HiSecEngine USG6000F

Typical Configuration Examples

Issue	01
Date	2024-07-15



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/ecolumnsweb/en/warranty-policy

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices.* For details about this document, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Huawei Enterprise End User License Agreement

This agreement is the end user license agreement between you (an individual, company, or any other entity) and Huawei for the use of the Huawei Software. Your use of the Huawei Software will be deemed as your acceptance of the terms mentioned in this agreement. For details about this agreement, visit the following web page:
https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

Contents

1 About This Document.....1

2 Comprehensive Configuration Examples in Typical Scenarios..... 7

3 Logging In to the Device.....8

3.1 CLI: Example for Configuring STelnet Login (RSA Authentication)..... 8
3.2 CLI: Example for Configuring STelnet Login (Password Authentication)..... 12
3.3 Web: Example for Configuring STelnet Login (Password Authentication)..... 17
3.4 CLI: Example for Configuring Telnet Login..... 22
3.5 CLI: Example for Logging In to the CLI Using STelnet (RADIUS)..... 25
3.6 CLI: Example for Logging In to the CLI Using STelnet (HWTACACS)..... 29
3.7 Web: Example for Configuring Web UI-based Login Through HTTPS (Default Certificate)..... 33
3.8 CLI: Example for Configuring Web UI-based Login Through HTTPS (Default Certificate)..... 36
3.9 CLI: Example for Configuring Web UI-based Login Through HTTPS (Specified Certificate)..... 38
3.10 Handling Administrator Password Loss..... 40
3.11 Handling BootLoader Password Loss..... 42

4 Accessing the Internet Using One Interface..... 45

4.1 Web: Example for Accessing the Internet Using a Static IPv4 Address.....45
4.2 CLI: Example for Accessing the Internet Using a Static IPv4 Address..... 49
4.3 Web: Example for Accessing the Internet Using DHCP..... 52
4.4 CLI: Example for Accessing the Internet Using DHCP..... 57
4.5 Web: Example for Configuring Static IPv6 Addresses for Devices to Communicate..... 60
4.6 CLI: Example for Configuring Static IPv6 Addresses for Devices to Communicate.....63

5 Accessing the Internet Using Multiple Interfaces..... 66

5.1 Web: Example for Configuring ISP Link Selection to Forward Traffic by ISPs..... 66
5.2 CLI: Example for Configuring ISP Link Selection to Forward Traffic by ISPs..... 73
5.3 Configuring PBR and PBR-based Intelligent Uplink Selection.....75
5.3.1 Web: Example for Configuring Protocol-Specific PBR.....75
5.3.2 CLI: Example for Configuring Protocol-Specific PBR..... 83
5.3.3 CLI: Example for Configuring Link Selection Based on Multi-Egress PBR Among Multiple ISP Outbound Interfaces..... 86
5.3.4 CLI: Example for Configuring Policy-based Routes for Internet Access from Multiple ISPs.....89
5.4 Configuring Equal Cost Route-based Intelligent Uplink Selection..... 93
5.4.1 Web: Example for Configuring Load Balancing Based on Link Bandwidth.....93

 Copyright © Huawei Technologies Co., Ltd.

5.4.2 CLI: Example for Configuring Load Balancing Based on Link Bandwidth....99
5.4.3 Web: Example for Configuring Load Balancing Based on Link Weight....103
5.4.4 CLI: Example for Configuring Load Balancing Based on Link Weight....108
5.4.5 Web: Example for Configuring Active/Standby Backup Based on Link Priority....112
5.4.6 CLI: Example for Configuring Active/Standby Backup Based on Link Priority....119

6 Virtual System....123

6.1 Web: Example for Configuring Communication Between a Virtual System and the Public System Based on Routing Tables....124
6.2 CLI: Example for Configuring Communication Between a Virtual System and the Public System Based on Routing Tables....132
6.3 CLI: Example for Configuring Communication Between a Virtual System and the Public System Based on a Traffic Diversion Table....137
6.4 Web: Example for Configuring Direct Communication Between Two Virtual Systems....141
6.5 CLI: Example for Configuring Direct Communication Between Two Virtual Systems....151
6.6 Web: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on Routing Tables....156
6.7 CLI: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on Routing Tables....168
6.8 CLI: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on a Traffic Diversion Table....174
6.9 CLI: Example for Configuring Communication Between Two Virtual Systems Across Another Virtual System....181
6.10 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through Independent Public Network Interfaces of the Virtual Systems....189
6.11 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through Independent WAN Interfaces of the Virtual Systems....202
6.12 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the Public Interface of the Public System (Performing NAT in the Public System)....208
6.13 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the WAN Interface of the Public System (Performing NAT in the Public System)....222
6.14 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the Public Network Interface of the Public System (Performing NAT in Each Virtual System)....229
6.15 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the WAN Interface of the Public System (Performing NAT in Each Virtual System)....247
6.16 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through Independent Public Network Interfaces of the Virtual Systems....255
6.17 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through Independent WAN Interfaces of the Virtual Systems....267
6.18 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the Public Network Interface of the Public System (Performing NAT in the Public System)....273
6.19 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the WAN Interface of the Public System (Performing NAT in the Public System)....286
6.20 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the Public Network Interface of the Public System (Performing NAT in Each Virtual System)....293
6.21 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the WAN Interface of the Public System (Performing NAT in Each Virtual System)....307
6.22 Web: Example for Configuring Layer 2 Access for Virtual Systems....313

 Copyright © Huawei Technologies Co., Ltd.

6.23 CLI: Example for Configuring Layer 2 Access for Virtual Systems....324
6.24 Web: Example for Configuring IPv6 User Access at Layer 3 Through Virtual Systems....330
6.25 CLI: Example for Configuring IPv6 User Access at Layer 3 Through Virtual Systems....339
6.26 CLI: Example for Configuring Telnet Login to a Virtual System....345
6.27 CLI: Example for Configuring STelnet Login to a Virtual System....347

7 Hot Standby....352

7.1 Configuring Hot Standby in Active/Standby Mode....352
7.1.1 Web: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions....352
7.1.2 CLI: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions....361
7.1.3 Web: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices....366
7.1.4 CLI: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices....377
7.1.5 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions....386
7.1.6 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions....395
7.1.7 Web: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively....401
7.1.8 CLI: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively....412
7.1.9 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction....418
7.1.10 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction....428
7.1.11 Web: Example for Connecting Devices to Switches Transparently in Upstream and Downstream Directions....433
7.1.12 CLI: Example for Connecting Devices to Switches Transparently in Upstream and Downstream Directions....439
7.2 Configuring Hot Standby in Load Sharing Mode....442
7.2.1 Web: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions....443
7.2.2 CLI: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions....452
7.2.3 Web: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices....458
7.2.4 CLI: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices....470
7.2.5 Web: Example for Load Balancing Networking in Which the Devices Work as the Gateways and Multi-ISP Accesses Are Provided....479
7.2.6 CLI: Example for Load Balancing Networking in Which the Devices Work as the Gateways and Multi-ISP Accesses Are Provided....488
7.2.7 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions....495

 Copyright © Huawei Technologies Co., Ltd.

7.2.8 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions..... 504
7.2.9 Web: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively..... 510
7.2.10 CLI: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively..... 521
7.2.11 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction..... 527
7.2.12 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction..... 537
7.2.13 Web: Example for Connecting Devices to Routers Transparently in the Upstream and Downstream Directions..... 542
7.2.14 CLI: Example for Connecting Devices to Routers Transparently in the Upstream and Downstream Directions..... 549
7.3 Configuring Hot Standby in Mirroring Mode..... 555
7.3.1 CLI: Example for Configuring Hot Standby in Mirroring Mode..... 555
7.4 Configuring Interworking Between Hot Standby and Health Check..... 561
7.4.1 CLI: Example for Configuring Interworking Between Hot Standby and Health Check..... 561
7.5 Configuring Association Between Hot Standby and BFD..... 567
7.5.1 CLI: Example for Configuring Interworking Between Hot Standby and BFD..... 567
7.6 Configuring Hot Standby of Virtual Systems..... 575
7.6.1 CLI: Example for Configuring Hot Standby (Active/Standby) of Virtual Systems on Devices Connecting to Switches in Upstream and Downstream Directions..... 575
7.6.2 CLI: Example for Configuring Hot Standby (Active/Standby) of Virtual Systems on Firewalls Connecting to Upstream Routers and Downstream Switches..... 585
7.6.3 CLI: Example for Configuring Hot Standby (Load Balancing) of Virtual Systems on Firewalls Connecting to Switches in Upstream and Downstream Directions..... 599
7.6.4 CLI: Example for Configuring Hot Standby (Load Balancing) of Virtual Systems on Firewalls Connecting to Upstream Routers and Downstream Switches..... 609
7.6.5 CLI: Example for Configuring Hot Standby (Load Balancing) of Virtual Systems on Firewalls Connecting to Upstream Routers Through the Public System and Downstream Subnets Through Virtual Systems..... 623
7.7 Configuring IPv6 Hot Standby..... 639
7.7.1 CLI: Example for Configuring IPv6 Hot Standby in Active/Standby Mode on Devices That Connect Switches in Upstream and Downstream Directions..... 639
7.7.2 CLI: Example for Configuring IPv6 Hot Standby in Load Balancing Mode on Devices That Connect Switches in Upstream and Downstream Directions..... 645
7.7.3 CLI: Example for Configuring IPv6 Hot Standby in Active/Standby Mode on Devices That Connect Routers in Upstream and Downstream Directions..... 651
7.7.4 CLI: Example for Configuring IPv6 Hot Standby in Load Balancing Mode on Devices That Connect Routers in Upstream and Downstream Directions..... 657
8 IPsec..... 664
8.1 Communication Between LANs Through IPsec Tunnels..... 664
8.1.1 Web: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using PSK Authentication)..... 664
8.1.2 CLI: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using PSK Authentication)..... 678
8.1.3 Web: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using Certificate Authentication)..... 687

 Copyright © Huawei Technologies Co., Ltd.

8.1.4 CLI: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using Certificate Authentication) 700
8.1.5 Web: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use the Same PSK for Authentication) 712
8.1.6 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use the Same PSK for Authentication) 727
8.1.7 Web: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use Different PSKs for Authentication) 740
8.1.8 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use Different PSKs for Authentication) 755
8.1.9 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Profile (Through PSK Authentication) 768
8.1.10 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Profile (Using Certificate Authentication) 778
8.1.11 Web: Example for Establishing an IPsec 6 Tunnel Based on Physical Interfaces Between Two Gateways 790
8.1.12 Web: Example for Establishing an IPsec 6 Tunnel Based on Tunnel Interfaces Between Two Gateways 803
8.1.13 Web: Example for Establishing an IPsec 6over4 Tunnel Based on Physical Interfaces Between Two Gateways 817
8.1.14 CLI: Example for Establishing an IPSec 6over4 Tunnel Based on Physical Interfaces Between Two Gateways 830
8.1.15 Web: Example for Establishing an IPsec 4over6 Tunnel Based on Physical Interfaces Between Two Gateways 839
8.2 Communication Between LANs Through GRE over IPsec Tunnels 853
8.2.1 CLI: Example for Establishing a GRE over IPsec Tunnel Using ISAKMP 853
8.2.2 CLI: Example for Establishing a GRE over IPsec Tunnel Using an IPsec Profile 862
8.3 IPsec in NAT Scenarios 871
8.3.1 CLI: Example for Establishing an IPsec Tunnel in a NAT Scenario (NAT Is Performed by the Headquarters Gateway) 871
8.3.2 Web: Example for Establishing an IPsec Tunnel in a NAT Scenario (NAT Is Performed by Each Branch's Gateway) 881
8.3.3 CLI: Example for Establishing an IPsec Tunnel in a NAT Scenario (NAT Is Performed by Each Branch's Gateway) 908
8.4 IPsec Virtualization 923
8.4.1 Web: Example for Configuring Virtual Systems to Use an Independent Public IP Address to Establish an IPsec Tunnel 923
8.4.2 CLI: Example for Configuring Virtual Systems to Use an Independent Public IP Address to Establish an IPsec Tunnel 940
8.4.3 CLI: Example for Establishing an IPsec Tunnel Within the Same VPN Instance 954
8.4.4 CLI: Example for Establishing an IPsec Tunnel Across VPN Instances 962
8.4.5 CLI: Example for Accessing Resources in Different VPN Instances Through an IPsec Tunnel 974
8.5 IPsec Dual-System Hot Standby 985
8.5.1 CLI: Example for Establishing an IPsec Tunnel in Active/Standby Mode 986
8.5.2 CLI: Example for Establishing an IPsec Tunnel in Load Balancing Mode (Routers Serving as Upstream and Downstream Devices) 998
8.6 IPsec Intelligent Uplink Selection 1015

 Copyright © Huawei Technologies Co., Ltd.

8.6.1 Web: Example for Configuring IPsec Intelligent Uplink Selection Based on Link Quality Detection (with Automatic Link Switchback Enabled)....1015
8.6.2 CLI: Example for Configuring IPsec Intelligent Uplink Selection Based on Link Quality Detection (with Automatic Link Switchback Disabled)....1032
8.6.3 CLI: Example for Configuring IPsec Intelligent Uplink Selection Based on Link Quality Detection (with Automatic Link Switchback Enabled)....1043
8.6.4 CLI: Example for Configuring IPsec Intelligent Uplink Selection Based on Route Status Changes..1054
8.7 Others....1064
8.7.1 Web: Example for Configuring a Base Station to Obtain an IP Address Using the IKEv2 Configuration Payload....1064
9 SSL VPN....1072
9.1 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (User Name + Password Authentication)....1073
9.2 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (User Name + Password Authentication)....1077
9.3 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Anonymous Authentication)....1083
9.4 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Anonymous Authentication)....1088
9.5 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Challenge Authentication)....1094
9.6 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Challenge Authentication)....1099
9.7 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + AD Authorization)....1106
9.8 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + AD Authorization)....1111
9.9 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + Local Authorization)....1121
9.10 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + Local Authorization)....1126
9.11 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + Local Authorization)....1135
9.12 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + Local Authorization)....1140
9.13 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + Local Authorization)....1149
9.14 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + Local Authorization)....1154
9.15 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + LDAP Authorization)....1163
9.16 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + LDAP Authorization)....1168
9.17 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + RADIUS Authorization)....1178
9.18 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + RADIUS Authorization)....1183

 Copyright © Huawei Technologies Co., Ltd.

9.19 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Two-Factor Authentication + Local Authorization) 1192
9.20 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Two-Factor Authentication + Local Authorization) 1198

10 Identity Management 1208
10.1 CLI: Example for Configuring RADIUS SSO (In-path Mode) 1208
10.2 CLI: Example for Configuring RADIUS SSO (Off-path Mode) 1213
10.3 CLI: Example for Configuring TSM SSO 1217

11 GRE 1223
11.1 Web: Example for Configuring a Static Route-based GRE Tunnel 1223
11.2 Web: Example for Configuring an OSPF-based GRE Tunnel 1233
11.3 CLI: Example for Configuring an IPv4 over IPv4 GRE Tunnel 1244
11.4 CLI: Example for Configuring an IPv6 over IPv4 GRE Tunnel 1251
11.5 Web: Example for Configuring an IPsec over GRE Tunnel 1258
11.6 CLI: Example for Configuring an IPsec over GRE Tunnel 1272

12 Security Policy 1282
12.1 Web: Example for Configuring Security Policies Based on IP Addresses and Ports 1282
12.2 CLI: Example for Configuring Security Policies Based on IP Addresses and Ports 1296
12.3 Web: Example for Configuring Application-based Security Policies 1299
12.4 CLI: Example for Configuring Application-based Security Policies 1306

13 Content Security 1310
13.1 Web: Example for Configuring Antivirus 1310
13.2 Web: Example for Configuring the IPS Function to Protect Intranet Servers 1314
13.3 Web: Example for Configuring the IPS Function to Protect Intranet Users 1326
13.4 CLI: Example for Configuring Intrusion Prevention 1334
13.5 CLI: Example for Configuring Antivirus 1337
13.6 Web: Example for Using URL Categories to Control Website Access 1341
13.7 CLI: Example for Using URL Categories to Control Website Access 1354
13.8 Web: Example for Using the Blacklist and Whitelist to Control Website Access 1362
13.9 CLI: Example for Using the Blacklist and Whitelist to Control Website Access 1369
13.10 CLI: Example for Using URL Categories, Blacklist, and Whitelist to Control Website Access 1374
13.11 Web: Example for Configuring Security Policies for Bypass Detection 1379
13.12 CLI: Example for Configuring Security Policies for Bypass Detection 1381

14 Security Protection 1384
14.1 CLI: Example for Configuring FTP ASPF 1384
14.2 Web: Example for Configuring SIP ALG 1387
14.3 CLI: Example for Configuring SIP ALG 1391
14.4 Web: Examples for DDoS Attack Defense 1394
14.5 CLI: Example for DDoS Attack Defense 1396
14.6 CLI: Examples for Dynamic Traffic Limiting for Defense Against Traffic Attacks 1398

 Copyright © Huawei Technologies Co., Ltd.

14.7 CLI: Example for Configuring Per-IP New Connection Rate Limiting and New Session Rate Limiting 1400

15 NAT 1406

15.1 Source NAT 1406
15.1.1 Web: Example for Configuring NAT No-PAT for Intranet Users to Access the Internet 1406
15.1.2 CLI: Example for Configuring NAT No-PAT for Intranet Users to Access the Internet 1414
15.1.3 Web: Example for Configuring NAPT for Intranet Users to Access the Internet 1417
15.1.4 CLI: Example for Configuring NAPT for Intranet Users to Access the Internet 1426
15.1.5 Web: Example for Configuring Easy IP for Intranet Users to Access the Internet 1430
15.1.6 CLI: Example for Configuring Easy IP for Intranet Users to Access the Internet 1435
15.1.7 CLI: Example for Configuring Smart NAT for Intranet Users to Access the Internet 1439
15.1.8 Web: Example for Configuring Triplet NAT for Intranet Users to Access the Internet 1443
15.1.9 CLI: Example for Configuring 3-Tuple NAT for Intranet Users to Access the Internet 1451
15.1.10 Web: Example for Configuring NAPT for Users on a Dual-Egress Intranet to Access the Internet 1455
15.1.11 CLI: Example for Configuring NAPT for Users on a Dual-Egress Intranet to Access the Internet 1468
15.1.12 Web: Example for Configuring NAPT for Users on a Layer-2 Intranet to Access the Internet 1473
15.1.13 CLI: Example for Configuring NAPT for Users on a Layer 2 Intranet to Access the Internet 1481
15.2 Policy-based Destination NAT 1485
15.2.1 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-one Mappings Between Public and Private IP Addresses) 1485
15.2.2 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mappings Between Public and Private Addresses) 1493
15.2.3 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mapping Between the Public and Private Ports) 1497
15.2.4 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mappings Between Public and Private Ports) 1503
15.2.5 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-one Mappings Between Public Ports and Private IP Addresses) 1506
15.2.6 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-one Mappings Between Public Ports and Private Addresses) 1514
15.2.7 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mapping Between the Public Address and Private Port) 1517
15.2.8 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mappings Between Public Addresses and Private Ports) 1523
15.2.9 CLI: Example for Configuring Destination NAT for Mobile Phone Users to Access Wireless Networks (Translating Public Addresses Randomly Into Addresses in a Destination Address Pool) 1527
15.2.10 Web: Example for Configuring NAT Policy for Internet Users to Access Servers on an Intranet with Two Egresses 1530
15.2.11 Example for Configuring a NAT Policy for Internet Users to Access a Server on an Intranet with Two Egresses in Different Security Zones 1541
15.2.12 CLI: Example for Configuring a NAT Policy for Internet Users to Access a Server on an Intranet with Two Egresses in the Same Security Zone 1545
15.2.13 Web: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP Address of a Server on a Dual-Egress Intranet (Sticky Load Balancing) 1549

 Copyright © Huawei Technologies Co., Ltd.

15.2.14 CLI: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP Address of a Server on a Dual-Egress Intranet (Sticky Load Balancing) 1560
15.3 NAT Server 1563
15.3.1 Web: Example for Configuring NAT Server for Internet Users to Access Intranet Servers 1564
15.3.2 CLI: Example for Configuring NAT Server for Internet Users to Access Intranet Servers 1570
15.3.3 Web: Example for Configuring NAT Server for Internet Users to Access Servers on an Intranet with Two Egresses in Different Security Zones 1574
15.3.4 CLI: Example for Configuring NAT Server for Internet Users to Access a Server on an Intranet with Two Egresses in Different Security Zones 1583
15.3.5 Web: Example for Configuring NAT Server for Internet Users to Access Servers on an Intranet with Two Egresses in the Same Security Zone 1587
15.3.6 CLI: Example for Configuring NAT Server for Internet Users to Access a Server on an Intranet with Two Egresses in the Same Security Zone 1595
15.3.7 Web: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP address of a Server on a Dual-Egress Intranet (Sticky Load Balancing) 1599
15.3.8 CLI: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP Address of a Server on a Dual-Egress Intranet (Sticky Load Balancing) 1607
15.4 Bidirectional NAT (Source NAT+Destination NAT) 1610
15.4.1 Web: Example for Configuring Bidirectional NAT (Source NAT + Static Destination NAT) for Internet Users to Access Intranet Servers 1610
15.4.2 CLI: Example for Configuring Bidirectional NAT (Source NAT + Static Destination NAT) for Internet Users to Access Intranet Servers 1619
15.4.3 Web: Example for Configuring Intranet Users to Access the Public Addresses of Intranet Servers (Source NAT+Static Destination NAT) 1623
15.4.4 CLI: Example for Configuring Intranet Users to Access Intranet Servers Using Public Addresses (Source NAT + Static Destination NAT) 1635
15.4.5 CLI: Example for Configuring Bidirectional NAT (Source NAT + Dynamic Destination NAT) for Internet Users to Access Intranet Servers 1638
15.5 Bidirectional NAT (Source NAT+NAT Server) 1642
15.5.1 Web: Example for Configuring NAPT and NAT Server for Internet Users to Access Intranet Servers 1642
15.5.2 CLI: Example for Configuring NAPT and NAT Server for Internet Users to Access Intranet Servers 1653
15.5.3 Web: Example for Configuring Intranet Users to Access the Public Addresses of Intranet Servers 1657
15.5.4 CLI: Example for Configuring Intranet Users to Access Intranet Servers Using Public Addresses 1669
15.6 NAT in Hot Standby Scenarios 1673
15.6.1 Web: Example for Configuring Source NAT in Load Balancing Scenarios (Active and Standby Devices Share One Address Pool) 1673
15.6.2 CLI: Example for Configuring Source NAT in a Load Balancing Scenario (Active and Standby Devices Share One Address Pool) 1689
15.6.3 CLI: Example for Configuring Source NAT in a Load Balancing Scenario (Active and Standby Devices Use Different Address Pools) 1697
16 CGN 1707
16.1 Web: Example for a Private IPv4 User Traversing the Carrier Network to Access the IPv4 Internet 1707
16.2 CLI: Example for Configuring NAT444 1715
16.3 CLI: Example for Configuring Static Mappings 1720

 Copyright © Huawei Technologies Co., Ltd.

16.4 CLI: Example for Applying Port Pre-Allocation and Incremental Allocation to a NAT444 Scenario 1727
16.5 Web: Example for Enabling an IPv6 User to Access an IPv4 Server 1733
16.6 CLI: Example for Enabling an IPv6 User to Access an IPv4 Server 1739
16.7 CLI: Example for Enabling an IPv4 User to Access an IPv6 Server 1742
16.8 CLI: Example for Applying Port Pre-Allocation and Incremental Allocation to a NAT64 Scenario 1745
16.9 CLI: Example for Configuring an IPv6 User in a Virtual System to Access an IPv4 Server 1749
16.10 CLI: Example for Configuring an IPv4 User in a Virtual System to Access an IPv6 Server 1752
16.11 CLI: Example for Configuring a Public IPv4 Network User to Access a Private IPv6 Network Server (Access from the Public System to a Virtual System) 1756
16.12 CLI: Example for Configuring a Private IPv6 Network User to Access a Public IPv4 Network Server (Access from a Virtual System to the Public System) 1759
16.13 CLI: Example for Configuring an IPv6 User on a Private Network to Access an IPv4 Server on Another Private Network (Access Between Virtual Systems) 1764

17 Traffic Management 1770

17.1 Web: Example for Configuring Maximum Bandwidth and Guaranteed Bandwidth 1770
17.2 CLI: Example for Configuring Maximum Bandwidth and Guaranteed Bandwidth 1777
17.3 Web: Example for Configuring the Connection Limit 1780
17.4 CLI: Example for Configuring the Connection Limit 1785
17.5 CLI: Example for Configuring Bandwidth Control Based on Public IP Addresses 1787

18 SLB 1792

18.1 CLI: Example for Configuring FTP SLB 1792

19 QoS 1796

19.1 Packet Filtering Configuration 1796
19.1.1 CLI: Example for Configuring MQC-based Packet Filtering 1796
19.2 Traffic Statistics Collection Configuration 1799
19.2.1 CLI: Example for Configuring MQC-based Traffic Statistics Collection 1799
19.3 Priority Mapping Configuration 1801
19.3.1 CLI: Example for Configuring Priority Mapping 1801

20 System Management and Monitoring 1806

20.1 Web: Example for Configuring a Device to Connect to eSight Using SNMPv3 1806
20.2 CLI: Example for Configuring a Device to Connect to eSight Using SNMPv3 1813
20.3 Web: Example for Configuring Devices to Connect to iMaster NCE-Campus 1819
20.4 CLI: Example for Sending IPv4 Session Logs to the SecoManager 1825
20.5 CLI: Example for Sending User Session Logs to the SecoManager 1832
20.6 CLI: Example for Sending Intrusion Prevention Logs to the SecoManager 1837
20.7 CLI: Example for Sending Virus Event Logs to the SecoManager 1843
20.8 CLI: Example for Sending Syslogs in Default or MTN Format to a Third-Party Log Host 1849
20.9 CLI: Example for Outputting Customized Syslog Session Logs to a Third-Party Log Host 1853
20.10 CLI: Example for Outputting Customized NetFlow Session Logs to a Third-Party Log Host 1857
20.11 CLI: Example for Sending Service Logs to a Third-Party Log Host 1861
20.12 CLI: Example for Outputting Packet Loss Logs to a Third-Party Log Host 1864

 Copyright © Huawei Technologies Co., Ltd.

20.13 CLI: Example for Sending IPv4 Session Logs to the SecoManager in Hot Standby Deployment of Loading Balancing Mode..... 1868

 Copyright © Huawei Technologies Co., Ltd.

1 About This Document

Related Version

The following table lists the product versions related to this document.

Product Name	Version
The USG6000F series have the following models: • USG6500F – USG6510F-D – USG6510F-DL – USG6510F-DPL – USG6525F – USG6530F-D – USG6530F-DL – USG6530F-DPL – USG6555F – USG6565F – USG6585F • USG6600F – USG6615F – USG6625F – USG6635F – USG6655F – USG6685F • USG6700F – USG6710F – USG6715F – USG6725F	V600R023C00 is used as an example. For details about other versions, see the product documentation.

 Copyright © Huawei Technologies Co., Ltd.

Intended Audience

This document describes the configuration methods in typical application scenarios of the firewall. This document does not cover all features. It focuses on typical configuration scenarios. You can adapt the examples to your conditions.

This document is intended for administrators who configure and manage firewalls. The administrators must have good Ethernet knowledge and network management experience.

Content Conventions

1. The purchased products, services and features are stipulated by the contract made between Huawei Technologies Co., Ltd. and the customer. Part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.
2. The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.
3. The screenshots in this document are for reference only. The settings are subject to the actual GUI. The GUI of different models may be different.
4. Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Encryption Algorithm Declaration

Currently, the device supports the following encryption algorithms: DES, 3DES, AES, DSA, RSA, DH, ECDH, HMAC, SHA1, SHA2, and MD5. Select an encryption algorithm according to the application scenario. Use the recommended encryption algorithm; otherwise, security protection requirements may not be met.

- Recommended symmetric encryption algorithm: AES (with a 128-bit or longer key).
- Recommended asymmetric encryption algorithm: RSA (with a 3072-bit or longer key). Use different key pairs for encryption and signature.
- Recommended encryption algorithm for the digital signature: RSA (with a 3072-bit or longer key).
- Recommended encryption algorithm for key negotiation: DH (with a 3072-bit or longer key) or ECDH (with a 256-bit or longer key).
- Recommended hash algorithm: SHA2 (256-bit or higher).
- Recommended hash-based message authentication code (HMAC) algorithm: HMAC-SHA2.
- The SHA1, SHA2, and MD5 encryption algorithms are irreversible, and the DES, 3DES, RSA, and AES encryption algorithms are reversible.
- SSH versions are classified into SSH1.X (earlier than SSH2.0) and SSH2.0, of which SSH2.0 is recommended. In SSH2.0, when the symmetric encryption algorithm in CBC mode is used, data may be subject to a plaintext-recovery

 Copyright © Huawei Technologies Co., Ltd.

attack, causing disclosure of encrypted data. Therefore, you are not advised to use the CBC mode for data encryption in SSH2.0.

- SSL provides a handshake mechanism that allows a client and a server to establish a session, authenticate each other's identity, and negotiate the key and cipher suite. It is recommended that a cipher suite of TLS 1.2 or a later version be used during communication. In TLS versions, when the symmetric encryption algorithm in CBC mode is used, data may be subject to a plaintext-recovery attack, causing disclosure of encrypted data. Therefore, you are not advised to use the CBC mode for data encryption in TLS versions.

Personal Data Declaration

Some personal data (such as MAC or IP addresses of terminals) may be obtained or used during operation or fault location of your purchased products, services, or features. Huawei does not independently collect or store user communication information. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information usage and storage, proper measures must be taken to protect user communication information.

Feature Usage Declaration

- For security purposes, you are not advised to use insecure protocols Telnet, FTP, and TFTP and weak security algorithms or weak security protocols in SSH, SNMP, IS-IS, IS-ISv6, RIP, SSL, NTP, OSPF, PKI, IPsec, logs, and keychain. If necessary, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA. By default, the device provides the weak security algorithm or protocol feature package WEAKEA. For details about how to install or uninstall the feature package, see "Upgrade Maintenance Configuration" in CLI Configuration Guide > System Management Configuration.
- After the FIPS mode is enabled, protocols and algorithms with low security cannot be used. For example, FTP, TFTP, and Telnet cannot be used. When the device connects to a gRPC client, an AD server, or an LDAP server, SSL encryption is required.

  After the FIPS mode is enabled, the device clears all certificates, keys, and passwords except the preset certificate and private key.

  After the FIPS mode is enabled, the weak security algorithm/protocol feature package can be installed on the device, but does not take effect. That is, the weak security algorithm/protocol still cannot be used.
- The device can transfer files through FTP, TFTP, SFTPv1, SFTPv2, and SCP. FTP, TFTP, and SFTPv1 have security risks. You are advised to use SFTPv2 or SCP to transfer files.
- Telnet, STelnet V1, and STelnet V2 can be used to log in to the device. Telnet and STelnet V1 have security risks. You are advised to use STelnet V2 to log in to the device.
- SNMPv1, SNMPv2c, and SNMPv3 can be used to manage the device. SNMPv1 and SNMPv2c have security risks. You are advised to use SNMPv3 to manage the device.

 Copyright © Huawei Technologies Co., Ltd.

- The device supports antivirus, URL filtering, data filtering, and intrusion prevention system (IPS), which may involve the collection of user communication content such as browsed web pages and transmitted files. To prevent communication information leakage, you are advised to delete unnecessary user information in a timely manner.
- The device supports SSL-encrypted traffic detection. This function decrypts SSL traffic and performs content security detection on the decrypted traffic, which may involve personal communication content. Huawei will never collect or store user communication information without prior user approval. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information usage and storage, proper measures must be taken to protect user communication information.
- The device supports the SSL uninstallation function to decrypt encrypted traffic and then forward the traffic to an intranet server, which may involve some communication information of individual users. Huawei does not independently collect or store user communication information. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information usage and storage, proper measures must be taken to protect user communication information.
- The device supports the zero trust function. As a proxy, the device works with other components to implement the zero trust solution, which involves obtaining device IDs and user information and may involve some communication information of individual users. Huawei does not independently collect or store user communication information. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information usage and storage, proper measures must be taken to protect user communication information.
- The device supports the mirroring function, which is used for network detection and fault management and may involve some communication information of individual users. Huawei does not independently collect or store user communication information. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information usage and storage, proper measures must be taken to protect user communication information.
- The device supports the packet obtaining function, which is used to detect transmission faults and errors. Huawei does not independently collect or store user communication information. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information collection and storage, proper measures must be taken to protect user communication information.
- Antivirus (AV) and intrusion prevention system (IPS) provide the attack evidence collection function to analyze virus or intrusion data packets. However, the attack evidence collection process may involve the collection of user communication information. To prevent user communication information leakage, clear attack evidence collection records in a timely manner.

 Copyright © Huawei Technologies Co., Ltd.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.

Copyright © Huawei Technologies Co., Ltd.

Convention	Description
{ x | y | ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

The GUI conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 01 (2024-07-15)

Initial commercial release.

 Copyright © Huawei Technologies Co., Ltd.

2 Comprehensive Configuration Examples in Typical Scenarios

As a basic security protection product, the firewall is used in various solutions and service scenarios. This section provides document links to various solutions for your reference.

The following table lists comprehensive application cases in typical scenarios or projects. The firewall versions and deployment schemes used in various projects are different. For details, see the documentation.

Typical Scenario	Documentation	Major Applications
HiSec Solution	For details about firewall applications in HiSec solution, see **Huawei HiSec Solution Product Documentation**.	The HiSec solution includes several security solutions. Firewalls are used in the solution. Currently, the following solutions are supported: • CloudFabric Data Center Network Solution • CloudCampus Solution • HUAWEI CLOUD Stack Solution

 Copyright © Huawei Technologies Co., Ltd.

3 Logging In to the Device

3.1 CLI: Example for Configuring STelnet Login (RSA Authentication)

3.2 CLI: Example for Configuring STelnet Login (Password Authentication)

3.3 Web: Example for Configuring STelnet Login (Password Authentication)

3.4 CLI: Example for Configuring Telnet Login

3.5 CLI: Example for Logging In to the CLI Using STelnet (RADIUS)

3.6 CLI: Example for Logging In to the CLI Using STelnet (HWTACACS)

3.7 Web: Example for Configuring Web UI-based Login Through HTTPS (Default Certificate)

3.8 CLI: Example for Configuring Web UI-based Login Through HTTPS (Default Certificate)

3.9 CLI: Example for Configuring Web UI-based Login Through HTTPS (Specified Certificate)

3.10 Handling Administrator Password Loss

3.11 Handling BootLoader Password Loss

3.1 CLI: Example for Configuring STelnet Login (RSA Authentication)

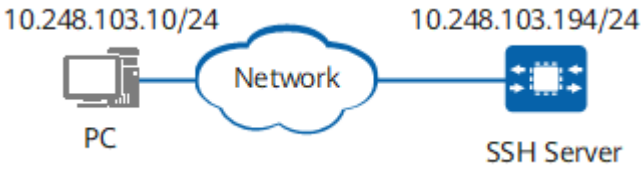
Networking Requirements

In **Figure 3-1**, after the STelnet server function is enabled on the device functioning as the SSH server, the PC functioning as the SSH client can connect to the SSH server in different authentication modes. This section uses the RSA authentication mode as an example to describe how to log in to the SSH server using STelnet.

To improve system security and prevent unauthorized users from logging in to the SSH server, you can configure an ACL rule on the SSH server.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Network diagram of STelnet login



Configuration Roadmap

The configuration roadmap is as follows:

1. Set the IP address of the management interface for the SSH server.
2. Configure the SSH server to generate a local key pair.
3. Configure a VTY user interface on the SSH server.
4. Create a local user and configure the user access type.
5. Create an SSH user and configure the authentication mode for the user.
6. On the SSH client, create a key pair based on the configured SSH user authentication mode and copy the public key to the SSH server.
7. On the SSH server, edit the public key and assign it to the user.
8. Enable STelnet on the SSH server and set the service type of the SSH user to STelnet.
9. On the SSH server, configure an ACL to allow access of the STelnet client.
10. Set parameters for STelnet login to the server.

Data Preparation

To complete the configuration, ensure that the following configurations have been completed:

NOTE

To ensure high security, you are advised to use the RSA key pair whose length is 3072 bits or longer.

- OpenSSH has been installed on the SSH client.
- The IP address of the management interface for the SSH server is 10.248.103.194/24.
- The local user's authentication mode is set to password authentication, and the user name and password are admin123 and YsHsjx_202206, respectively.
- The SSH user's authentication mode is RSA.
- ACL 2000 is configured to allow the clients on the network segment 10.248.103.0/24 to access the SSH server.

Procedure

Step 1 Set the IP address of the management interface for the SSH server.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> To log in to the device through a non-management interface, add this interface to a security zone and run the **service-manage ssh permit** command to allow access to the interface using SSH; or run the **undo service-manage enable** command to disable the interface access control function and configure a security policy that allows access to the interface. USG6510F-D, USG6530F-D use GE0/0/0 as the management interface and do not support MEth interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] interface meth 0/0/0
[SSH Server-MEth0/0/0] ip address 10.248.103.194 255.255.255.0
[SSH Server-MEth0/0/0] quit
```

Step 2 Configure the SSH server to generate a local key pair.

```
[SSH Server] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

Step 3 Configure a VTY user interface on the SSH server.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

> **NOTE**
>
> If SSH is configured as the login protocol, the device automatically disables the Telnet function.

Step 4 On the server, create a local user and configure the user access type.

```
[SSH Server] aaa
[SSH Server-aaa] local-user admin123 password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[SSH Server-aaa] local-user admin123 service-type ssh
[SSH Server-aaa] local-user admin123 privilege level 3
[SSH Server-aaa] quit
```

Step 5 Create an SSH user on the server and configure the authentication mode for the user.

```
[SSH Server] ssh user admin123
[SSH Server] ssh user admin123 authentication-type rsa
```

Step 6 Configure the public key algorithm, encryption algorithm, key exchange algorithm list, HMAC authentication algorithm, and minimum key length on the SSH server.

```
[SSH Server] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[SSH Server] ssh server hmac sha2_256 sha2_512
[SSH Server] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
[SSH Server] ssh server publickey rsa_sha2_256 rsa_sha2_512
[SSH Server] ssh server dh-exchange min-len 3072
```

Step 7 Use OpenSSH to create an RSA key pair on the SSH client and copy the public key to the SSH server.

Access the Windows CLI, create an RSA key pair, and save it to the local **id_rsa.pub** file. (The following information is for reference only.)

 Copyright © Huawei Technologies Co., Ltd.

```
C:\Users\User1> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\User1/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\User1/.ssh/id_rsa.
Your public key has been saved in C:\Users\User1/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:c43yubJjCUjY3JqH0aVZwJFM3gWJcH4YI5+4HUDAIqo
The key's randomart image is:
+---[RSA 3072]----+
| ..o==B=.o.      |
|o .  O=*+.       |
|o. +.oB=o        |
|. . =o=o   o     |
|.  ..*. S o .    |
|E   = o  = .     |
|     . . .o      |
|        =  .     |
|       ..+.      |
+----[SHA256]-----+
```

Step 8 On the SSH server, edit the public key generated using OpenSSH on the SSH client and assign it to the user.

```
[SSH Server] rsa peer-public-key rsa01 encoding-type openssh
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-public-key-rsa-key-code] ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCg5Ag490i6ilB7QuCVb35B8RJEh1DIYB88h2p1qjdh7qdMQv8rp
JaVAgQWxwzKZO0XdFuz4ReGQzTCSf7Det7Ajicddw3qi+6P8hRqZj6MPdLg/o3RN4aPCfr/
LFWCwqJ3gWGHlOC7qqjRk+6pySVoiWcSk5/elBkU7WVk/
cSWrt4qFXJV373OCesKcEVeDvAa1Tvx6L3LQroBqUO0EXzDgOthPCmOqiqvS5h3JipzqVsesdSKjeInooCQzS
Ov5eePpBcFcIvU6wFiLIZ5vnf6YtypgTVzHuje/sh4xM7Iuuon7AYXKHT8NpO9jd9zA/lKaRPXyDtei1O1Bt/
5lxnn
[SSH Server-rsa-public-key-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
[SSH Server] ssh user admin123 assign rsa-key rsa01
```

Step 9 Enable the STelnet function and set the user service type to STelnet.

```
[SSH Server] stelnet server enable
[SSH Server] ssh server-source all-interface
[SSH Server] ssh user admin123 service-type stelnet
```

Step 10 Configure an ACL rule. By default, the management interface is bound to VPN instance **_management_vpn_**.

```
[SSH Server] acl 2000
[SSH Server-acl4-basic-2000] rule permit vpn-instance _management_vpn_ source 10.248.103.0 24
[SSH Server-acl4-basic-2000] quit
[SSH Server] ssh server acl 2000
```

----End

Verifying the Configuration

Use the OpenSSH software to log in to the SSH server from the client. Access the Windows CLI and run the OpenSSH commands to access the device using STelnet.

```
C:\Users\User1> ssh admin123@10.248.103.194
Enter passphrase for key 'C:\Users\User/.ssh/id_rsa':
Info: The max number of VTY users is 21, the number of current VTY users online is 4, and total number of terminal users online is 4.
      The current login time is 2020-12-15 15:58:03.
<SSH Server>
```

Configuration Scripts

```
#
sysname SSH Server
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
acl number 2000
 rule 5 permit vpn-instance _management_vpn_ source 10.248.103.0 0.0.0.255
#
rsa peer-public-key rsa01 encoding-type openssh
 public-key-code begin
  ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCg5Ag490i6ilB7QuCVb35B8RJEh1DIYB88h2p1qjdh7qdMQv8rpJaVA
gQWxwzKZO0XdFuz4ReGQzTCSf7Det7Ajicddw3qi+6P8hRqZj6MPdLg/o3RN4aPCfr/
LFWCwqJ3gWGHlOC7qqjRk+6pySVoiWcSk5/elBkU7WVk/
cSWrt4qFXJV373OCesKcEVeDvAa1Tvx6L3LQroBqUO0EXzDgOthPCmOqiqvS5h3JipzqVsesdSKjeInooCQzSOv5e
ePpBcFcIvU6wFiLIZ5vnf6YtypgTVzHuje/sh4xM7Iuuon7AYXKHT8NpO9jd9zA/lKaRPXyDtei1O1Bt/5lxnn rsa-key
 public-key-code end
 peer-public-key end
#
aaa
 local-user admin123 password irreversible-cipher $1d$+,JS+))\
\2$KVNj(.3`_5x0FCKGv}H&.kUTI`Ff&H*eBqO.ua>)$
 local-user admin123 service-type terminal ssh
 local-user admin123 privilege level 3
#
interface MEth0/0/0
 ip address 10.248.103.194 255.255.255.0
#
stelnet server enable
ssh user admin123
ssh user admin123 authentication-type rsa
ssh user admin123 assign rsa-key rsa01
ssh user admin123 service-type stelnet
ssh server-source all-interface
ssh server acl 2000
#
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh server hmac sha2_256 sha2_512
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh server publickey rsa_sha2_256 rsa_sha2_512
ssh server dh-exchange min-len 3072
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

3.2 CLI: Example for Configuring STelnet Login (Password Authentication)

Networking Requirements

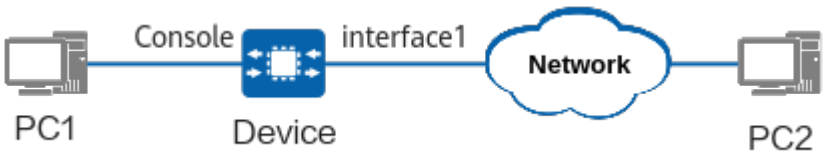
You must perform basic configurations after logging in to the device through the console port for the first time. You must also set the privilege level to 3 and the authentication mode to AAA authentication for users 0 to 4 who log in remotely through STelnet. This example assumes that there are reachable routes between PC2 and the device.

Figure 3-2 Performing basic configurations after the first login through the console port

NOTE

In this example, interface1 represents the management interface **MEth0/0/0**. USG6510F-D, USG6530F-D use GE0/0/0 as the management interface and do not support MEth interfaces.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

1. Log in to the device through the console port.
2. Perform basic configurations on the device.

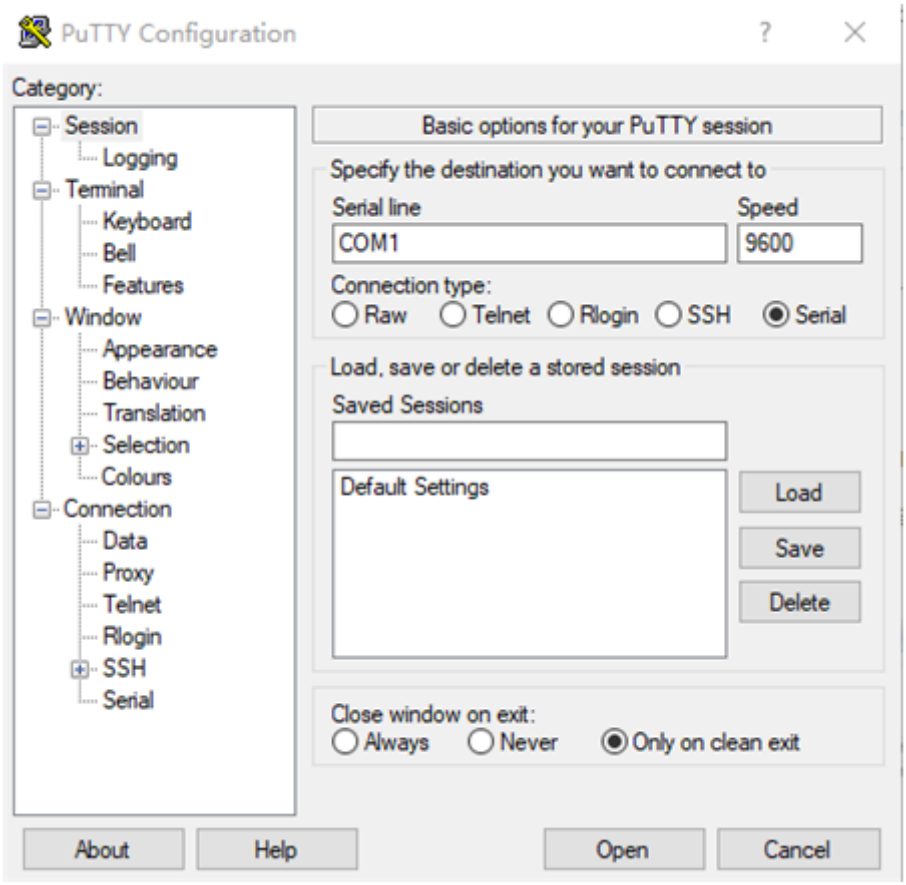
Procedure

Step 1 Connect the DB9 connector of the prepared console cable to the PC's serial port (COM), and the RJ45 connector to the device's console port. If there is no DB9 serial port on your terminal (PC), use a DB9-to-USB cable to connect the USB port to the terminal.

Step 2 Start a terminal emulation program on PC1. Create a connection and set the port and communication parameters. (This section uses the third-party software PuTTY as an example.)

1. Click **Session** to create a connection, as shown in **Figure 3-3**.

Figure 3-3 Creating a connection



2. Click **Serial** and set the port to be connected and the communication parameters, as shown in **Figure 3-4**.

 Copyright © Huawei Technologies Co., Ltd.

a. Select the port based on actual situations. For example, on Windows, you can open **Device Manager** to view port information and select the port to be connected.

b. Set the communication parameters. Ensure that the communication parameter settings in the terminal emulation software are consistent with the default parameter settings (9600 bit/s transmission rate, 8 data bits, 1 stop bit, no parity check, and no flow control) of the device's console port.

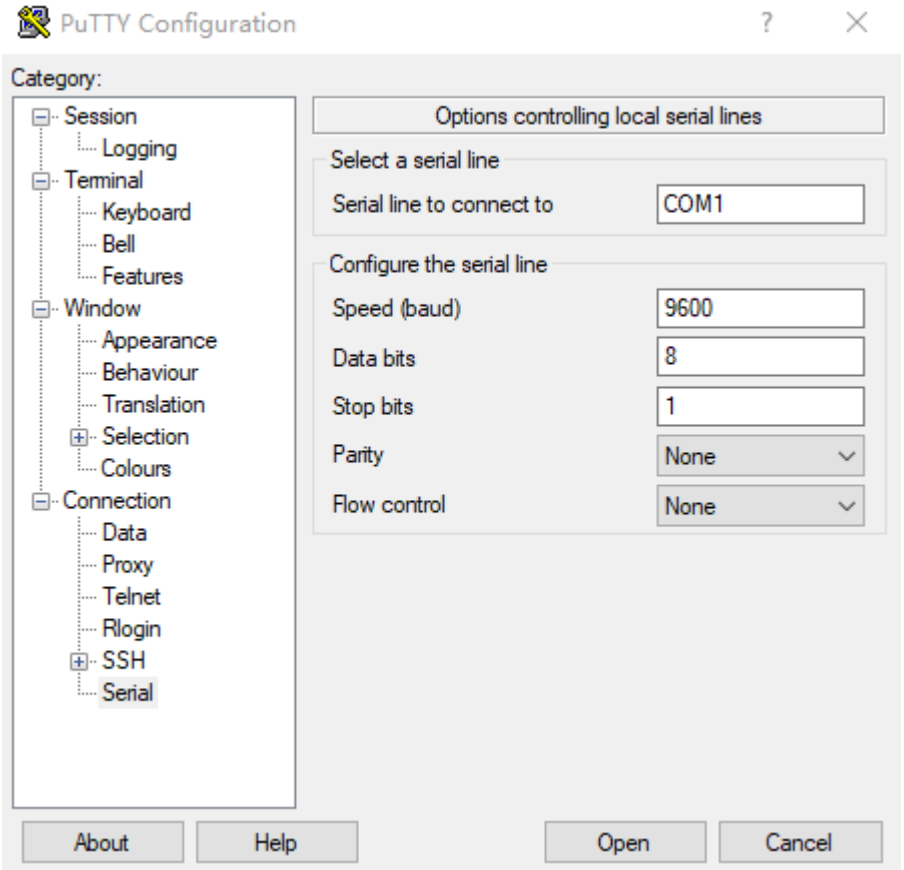
c. Click **Open**.

NOTE

PC1 may have multiple ports that can be connected to the device. In this step, you need to select the port to be connected to a console cable. In most cases, COM1 is used.

If the device's console port communication parameters are modified, you need to modify those on the PC accordingly and re-establish the connection.

Figure 3-4 Setting the connection port and communication parameters



Step 3 Press **Enter** until information similar to the following is displayed. Enter a password and confirm the password as prompted. (The following information is for reference only.)

```
User interface con0 is available

Please Press ENTER.

Please configure the login password (8-16)
```

 Copyright © Huawei Technologies Co., Ltd.

```
Enter Password:
Confirm Password:      //Enter the password for logging in to the device through the console port.
Info: Save the password now. Please wait for a moment.
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online is 2.
    The current login time is 2020-06-30 18:15:10+08:00
<HUAWEI>
```

NOTE

- You must set a login password upon first login to the device through the console port. By default, you can use the console port to perform administrator operations after successfully logging in to the device.
- The password is a string of 8 to 16 case-sensitive characters. It must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters. Special characters do not include question marks (?) or spaces.
- The password entered in interactive mode will not be displayed on the terminal screen.
- For security purposes, change the password periodically.

Step 4 Perform basic configurations on the device.

Set the date, time, and time zone.

```
<HUAWEI> clock timezone BJ add 08:00:00
<HUAWEI> clock datetime 20:20:00 2023-05-08
```

NOTICE

Before configuring the current time and date, run the **clock timezone** command to configure the time zone. If no time zone is configured, running the **clock datetime** command will configure the Coordinated Universal Time (UTC).

Set the device name and IP address of the management interface.

NOTE

To log in to the device through a non-management interface, add this interface to a security zone and run the **service-manage ssh permit** command to allow access to the interface using SSH; or run the **undo service-manage enable** command to disable the interface access control function and configure a security policy that allows access to the interface.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] interface meth 0/0/0
[Device-MEth0/0/0] ip binding vpn-instance _management_vpn_
[Device-MEth0/0/0] ip address 10.137.217.203 255.255.255.0
[Device-MEth0/0/0] quit
```

Configure a default route for the device with a gateway address of 10.137.217.1.

```
[Device] ip route-static vpn-instance _management_vpn_ 0.0.0.0 0 10.137.217.1
```

Configure the SSH client encryption algorithm, HMAC authentication algorithm, key exchange algorithm list, and public key algorithm.

```
[Device] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[Device] ssh server hmac sha2_256 sha2_512
[Device] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
[Device] ssh server publickey rsa_sha2_256 rsa_sha2_512
[Device] ssh server dh-exchange min-len 3072
```

Set parameters for the SSH user and the local user for SSH login.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device] user-interface vty 0 4
[Device-ui-vty0-4] authentication-mode aaa
[Device-ui-vty0-4] user privilege level 3
[Device-ui-vty0-4] protocol inbound ssh
[Device-ui-vty0-4] quit
[Device] aaa
[Device-aaa] local-user admin123 password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[Device-aaa] local-user admin123 service-type ssh
[Device-aaa] local-user admin123 privilege level 3
[Device-aaa] quit
[Device] ssh user admin123
[Device] ssh user admin123 authentication-type password
[Device] ssh user admin123 service-type stelnet
[Device] ssh server-source all-interface
[Device] stelnet server enable
```

----End

Verifying the Configuration

Log in to the device using STelnet from PC2. The third-party software OpenSSH and Windows CLI are used in the following example.

- For details about how to install OpenSSH, see the OpenSSH installation guide.
- To use OpenSSH to connect to the device using STelnet, run the OpenSSH commands. For details about OpenSSH commands, see the OpenSSH help.
- The Windows CLI can identify OpenSSH commands only when OpenSSH is installed on the terminal.

Access the Windows CLI and run the OpenSSH commands to connect to the device. (The following information is for reference only.)

```
C:\Users\User1> ssh admin123@10.137.217.203
Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.
Username:admin123
Password:
Warning: The initial password poses security risks.The password needs to be changed, Continue? [Y/N]:y
Please enter old password:
Please enter new password:
Please confirm new password:
The password has been changed successfully.
**************************************************************
*                   Copyright (C) 2012-2023                  *
*                Huawei Technologies Co., Ltd.               *
*                   All rights reserved.                     *
*          Without the owner's prior written consent,        *
*    no decompiling or reverse-engineering shall be allowed.  *
**************************************************************
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online is 2.
      The current login time is 2023-11-30 12:43:09.
Warnning: The current device can only be configured, it will discard all forwarding packets. Purchase license and active it on the web page to change device into forwarding state.
<Device>
```

Configuration Scripts

Device

 Copyright © Huawei Technologies Co., Ltd.

```
#
sysname Device
#
stelnet server enable
#
clock timezone BJ add 08:00:00
#
aaa
 local-user admin123 password irreversible-cipher $1d$+,JS+))\
\2$KVNj(.3`_5x0FCKGv}H&.kUTI`Ff&H*eBqO.ua>)$
 local-user admin123 service-type ssh
 local-user admin123 privilege level 3
#
interface MEth0/0/0
 ip binding vpn-instance _management_vpn_
 ip address 10.137.217.203 255.255.255.0
#
ip route-static vpn-instance _management_vpn_ 0.0.0.0 0.0.0.0 10.137.217.1
#
ssh user admin123
ssh user admin123 authentication-type password
ssh user admin123 service-type stelnet
ssh server-source all-interface
#
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh server hmac sha2_256 sha2_512
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh server publickey rsa_sha2_256 rsa_sha2_512
ssh server dh-exchange min-len 3072
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound ssh
#
return
```

3.3 Web: Example for Configuring STelnet Login (Password Authentication)

Networking Requirements

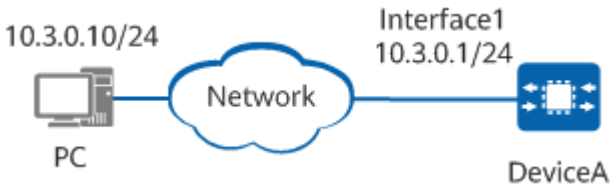
This section describes how to use the web UI to configure the administrator's PC (STelnet client) to connect to DeviceA (STelnet server) through STelnet in password authentication mode on an existing service network.

In **Figure 3-5**, the SSH account **admin123** is configured for DeviceA, which can be used to log in to DeviceA through SSH.

Figure 3-5 Network diagram of STelnet login

NOTE

Interface1 in this example represents GE0/0/1.



 Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item		Data
DeviceA	SSH account	admin123
	Password	YsHsjx_202206
	Authentication mode	Password authentication
	Service type	SSH
Administrator's PC		SSH client: OpenSSH software, which has been built in the Windows and Linux operating systems and can be directly used.

Configuration Roadmap

1. Configure a device login interface.
2. Create an SSH account for logging in to the device as an administrator.
3. Enable the SSH service function on the device.
4. Use the SSH account and password to log in to the device.

Procedure

Step 1 **Optional:** Configure the login interface.

NOTE

Skip this step if the default IP address of the management interface is used for login.

1. Choose **Network** > **Interface**.
2. Click in the **Edit** column of GE0/0/1 and set the parameters as follows.

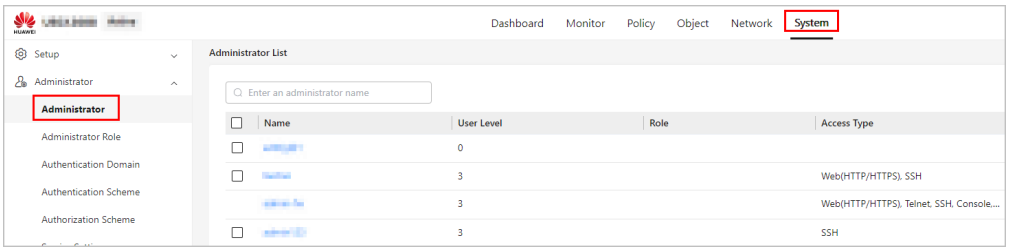
VPN Instance	public
Zone	trust
Mode	Routing
Connection Type	Static IP
IP Address	10.3.0.1/24
Access Management	SSH

3. Click **OK**.

Step 2 Create an SSH account.

1. Choose **System** > **Administrator** > **Administrator**.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **Add** and set parameters as follows.

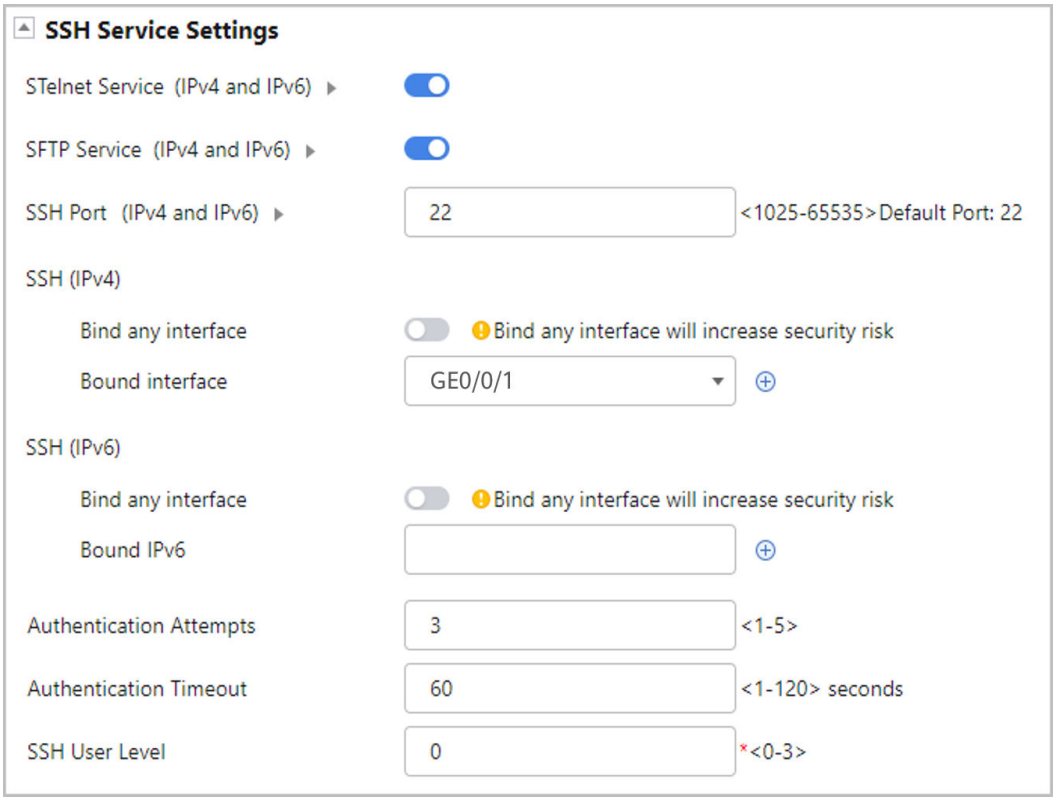
Name	admin123
Password	YsHsjx_202206
User Level	3
Role	Select or create a role corresponding to the administrator account. If **User Level** has been configured, you do not need to configure this parameter. Only one of them can be configured.
Advanced Settings	
Access Type	SSH
SSH Authentication	PASSWORD

3. Click **OK**.

Step 3 Enable the SSH service function.

1. Choose **System > Administrator > Service Settings**.
2. Expand **SSH Service Settings**, and enable **STelnet Service(IPv4 and IPv6)** and **SFTP Service(IPv4 and IPv6)**.

 Copyright © Huawei Technologies Co., Ltd.



3. Set the parameters by referring to the following table.

Parameter	Description
SSH Port(IPv4 and IPv6)	Service port number of the SSH server, that is, the port used by the STelnet and SFTP services. The default value is 22.
SSH (IPv4)	
Bind any interface	After this function is enabled, any interfaces configured with IPv4 addresses can access the SSH service. **NOTICE** Binding any interface increases security risks. Exercise caution when performing this operation.
Bound interface	Bind the interface specified in **Configuring the login interface**. A maximum of five interfaces can be bound.
SSH (IPv6)	
Bind any interface	After this function is enabled, any interfaces configured with IPv6 addresses can access the Telnet service. **NOTICE** Binding any interface increases security risks. Exercise caution when performing this operation.
Bound IPv6	IPv6 address to be bound. A maximum of five IPv6 addresses can be bound.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication Attempts	Maximum number of SSH authentication attempts allowed. The default value is 3.
Authentication Timeout	SSH authentication timeout interval. The default value is 60 seconds.
SSH User Level	Level of the administrator who can log in to the device through SSH. The default value is 3.

4. Click **Apply**.

Step 4 Configure the administrators' PC as the STelnet client to connect to the device.

1. Set the IP address of the administrator's PC to 10.3.0.10/24.
2. Run OpenSSH on the administrator's PC (Windows is used as an example) to access the Windows CLI.
3. Run OpenSSH commands to log in to the device through STelnet.

----End

Verifying the Configuration

The administrator's PC functions as a client and can connect to the device using OpenSSH. Access the Windows CLI and run the OpenSSH commands to access the device using STelnet. (The following information is for reference only.)

```
C:\Users\User1>ssh admin123@10.3.0.1
The authenticity of host '10.3.0.1 (10.3.0.1)' can't be established.
RSA key fingerprint is SHA256:HlePJh76z3meI4whXsxc2byEgBJlqkGIpzMgvxhNzVo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.3.0.1' (RSA) to the list of known hosts.
admin123@10.3.0.1's password:
                                                                  *
*                   Copyright (C) 2012-2023                     *
*                Huawei Technologies Co., Ltd.                  *
*                   All rights reserved.                        *
*          Without the owner's prior written consent,           *
*    no decompiling or reverse-engineering shall be allowed.    *
                                                                  *
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of
terminal users online is 1.
      The current login time is 2023-12-15 15:58:03.
<DeviceA>
```

Configuration Scripts

```
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
 service-manage enable
 service-manage ssh permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
```

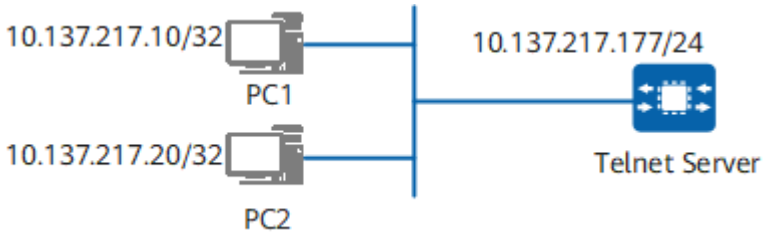
```
 protocol inbound ssh
#
aaa
local-user admin123 password irreversible-cipher ******
local-user admin123 service-type ssh
local-user admin123 privilege level 3
#
stelnet server enable
ssh user admin123
ssh user admin123 authentication-type password
ssh user admin123 service-type stelnet
ssh server port 22
ssh server-source -i GE0/0/1
ssh server timeout 60
ssh server authentication-retries 3
#
return
```

3.4 CLI: Example for Configuring Telnet Login

Networking Requirements

Users want to easily configure and manage the device shown in **Figure 3-6**. AAA authentication needs to be configured for Telnet users on the server, and an ACL policy needs to be configured to ensure that only the users matching the ACL can log in to the device.

Figure 3-6 Network diagram of Telnet login



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for the management interface on the Telnet server.
2. Configure Telnet login, that is, enable the Telnet server function and configure the server port number to remotely maintain network devices.
3. Set VTY user interface parameters, including an ACL policy, to ensure that only users matching the ACL can log in to the device.
4. Configure the user name and password for the administrator, and configure an AAA authentication policy to ensure that only users passing the authentication can log in to the device.

Configuration Precautions

In insecure network environments, you are advised to use a secure password authentication mode, encryption authentication algorithm, and protocol. For details about the configuration example of a secure protocol, see **3.1 CLI: Example for Configuring STelnet Login (RSA Authentication)**.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the device. If you log in to the device for the first time, perform operations in First Login Through the Console Port and then perform the following steps to set up the Telnet login environment.

Step 2 Run the **install feature-software WEAKEA** command in the user view to install the weak security algorithm/protocol feature package (WEAKEA).

Step 3 # Set the IP address of the management interface for the Telnet server.

NOTE

To log in to the device through a non-management interface, add this interface to a security zone and run the **service-manage telnet permit** command to allow access to the interface using Telnet; or run the **undo service-manage enable** command to disable the interface access control function and configure a security policy that allows access to the interface. USG6510F-D, USG6530F-D use GE0/0/0 as the management interface and do not support MEth interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname Telnet Server
[Telnet Server] interface meth 0/0/0
[Telnet Server-MEth0/0/0] ip address 10.137.217.177 255.255.255.0
[Telnet Server-MEth0/0/0] quit
```

Step 4 Set the server port number and enable the server function.

```
[Telnet Server] undo telnet server disable
[Telnet Server] telnet server port 1025
[Telnet Server] telnet server-source all-interface
```

Step 5 Set parameters for the VTY user interface.

Set the maximum number of VTY user interfaces.

```
[Telnet Server] user-interface maximum-vty 8
```

Configure an ACL rule that allows device login from specified host addresses. The IP address of PC1 is 10.137.217.10, and the IP address of PC2 is 10.137.217.20. By default, the management interface is bound to VPN instance **_management_vpn_**.

```
[Telnet Server] acl 2001
[Telnet Server-acl4-basic-2001] rule permit vpn-instance _management_vpn_ source 10.137.217.10 0
[Telnet Server-acl4-basic-2001] rule deny vpn-instance _management_vpn_ source 10.137.217.20 0
[Telnet Server-acl4-basic-2001] quit
[Telnet Server] user-interface vty 0 7
[Telnet Server-ui-vty0-7] acl 2001 inbound
```

Configure terminal attributes for the VTY user interface.

```
[Telnet Server-ui-vty0-7] shell
[Telnet Server-ui-vty0-7] idle-timeout 20
[Telnet Server-ui-vty0-7] screen-length 30
[Telnet Server-ui-vty0-7] history-command max-size 20
```

Configure the authentication mode for the VTY user interface.

```
[Telnet Server-ui-vty0-7] authentication-mode aaa
[Telnet Server-ui-vty0-7] user privilege level 3
[Telnet Server-ui-vty0-7] protocol inbound telnet
[Telnet Server-ui-vty0-7] quit
```

Step 6 Configure information about the administrator who logs in to the device.

Configure the authentication mode for the login user.

 Copyright © Huawei Technologies Co., Ltd.

```
[Telnet Server] aaa
[Telnet Server-aaa] local-user admin1234 password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[Telnet Server-aaa] local-user admin1234 service-type telnet
[Telnet Server-aaa] local-user admin1234 privilege level 3
[Telnet Server-aaa] quit
```

----End

Verifying the Configuration

Run the following command on the CLI of PC1 to telnet to the device:

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

Press **Enter**, and enter the user name and password configured for AAA authentication in the login window. If the authentication is successful, the command line prompt for the user view is displayed, indicating that you have successfully logged in to the device.

```
Username:admin1234
Password:
Info: The max number of VTY users is 8, the number of current VTY users online is 1, and total number of terminal users online is 1.
<Telnet Server>
```

Configuration Scripts

```
#
sysname Telnet Server
#
telnet server-source all-interface
telnet server port 1025
#
acl number 2001
 rule 5 permit vpn-instance _management_vpn_ source 10.137.217.10 0
 rule 10 deny vpn-instance _management_vpn_ source 10.137.217.20 0
#
aaa
 local-user admin1234 password irreversible-cipher $1d$g8wLJ`LjL!$CyE(V{3qg5DdU:PM[6=6O
$UF-.fQ,Q}>^)OBzgoU$
 local-user admin1234 service-type telnet
 local-user admin1234 privilege level 3
#
interface MEth0/0/0
 ip address 10.137.217.177 255.255.255.0
#
user-interface maximum-vty 8
#
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
 user privilege level 3
 protocol inbound telnet
 history-command max-size 20
 idle-timeout 20 0
 screen-length 30
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

3.5 CLI: Example for Logging In to the CLI Using STelnet (RADIUS)

Networking Requirements

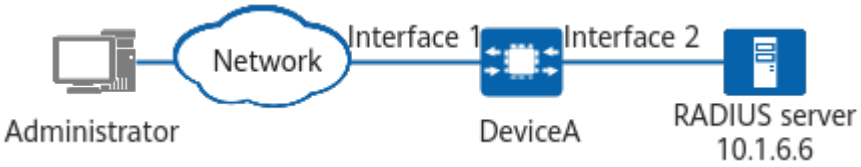
In Figure 3-7, a RADIUS server is deployed on an enterprise network. The enterprise requires that the administrator use RADIUS authentication to log in to DeviceA through STelnet. The specific requirements are as follows:

1. The administrator can log in to the device through STelnet only after entering a correct user name and password.
2. After the administrator logs in to the device through STelnet, the privilege level 3 is authorized to the administrator.

Figure 3-7 Configuring RADIUS authentication, authorization, and accounting

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

1. Configure STelnet login on DeviceA: Set the authentication mode for accessing VTY user interfaces to AAA, enable the STelnet service, and configure the authentication mode and service type for SSH users.
2. Configure RADIUS authentication on DeviceA: Create a RADIUS server template and AAA schemes, and apply the server template and AAA schemes to a domain.
3. Configure a RADIUS server.

Precautions

- Ensure that there are reachable routes between the user terminal and DeviceA before the configuration.
- Ensure that the shared key in the RADIUS server template is the same as that configured on the RADIUS server.
- After the domain is set as the global default administrative domain and the user name of the administrator contains the domain name or does not contain any domain name, the administrator uses AAA configuration in the global default administrative domain.
- If the RADIUS server does not support the user name containing a domain name, run the **undo radius-server user-name domain-included** command in the RADIUS server template view to configure the device to send packets that do not contain a domain name to the RADIUS server.

 Copyright © Huawei Technologies Co., Ltd.

- After the **undo radius-server user-name domain-included** command is run, the device changes only the user name format in the sent packet, without affecting the domain to which the user belongs. For example, after this command is run, the user with the user name **username@huawei.com** still uses AAA configuration in the domain named **huawei.com**.
- When the extended RADIUS attribute HW-Exec-Privilege (26-29) is used to authorize the priority of an administrator, the value ranges from 0 to 3. The value greater than or equal to 4 is invalid.

Procedure

Step 1 Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] portswitch
[DeviceA-GE0/0/1] port link-type trunk
[DeviceA-GE0/0/1] port trunk allow-pass vlan 10
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] portswitch
[DeviceA-GE0/0/2] port link-type trunk
[DeviceA-GE0/0/2] port trunk allow-pass vlan 20
[DeviceA-GE0/0/2] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.2 255.255.255.0
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.6.2 255.255.255.0
[DeviceA-Vlanif20] quit
```

Step 2 Add interfaces to security zones and configure interface access control and security policies.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface vlanif 10
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface vlanif 20
[DeviceA-zone-untrust] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] service-manage enable
[DeviceA-Vlanif10] service-manage ssh permit
[DeviceA-Vlanif10] quit
[DeviceA] security-policy
[DeviceA-policy-security] rule name sec_policy1
[DeviceA-policy-security-rule-sec_policy1] source-zone local
[DeviceA-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceA-policy-security-rule-sec_policy1] destination-address 10.1.6.6 24
[DeviceA-policy-security-rule-sec_policy1] action permit
[DeviceA-policy-security-rule-sec_policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure STelnet login.

Generate a local key pair on DeviceA.

```
[DeviceA] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 3072).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

Set the authentication mode and protocol for accessing VTY user interfaces 0 to 4 to AAA and SSH, respectively.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
[DeviceA-ui-vty0-4] protocol inbound ssh
[DeviceA-ui-vty0-4] quit
```

Enable the SSH server function on DeviceA.

```
[DeviceA] stelnet server enable
[DeviceA] ssh server-source -i vlanif 10
```

Set the authentication mode of all SSH users to password authentication.

```
[DeviceA] ssh authentication-type default password
```

Step 4 Configure RADIUS authentication, authorization, and accounting.

Configure a RADIUS server template for communication between DeviceA and RADIUS server.

```
[DeviceA] radius-server template 1
[DeviceA-radius-1] radius-server authentication 10.1.6.6 1812
[DeviceA-radius-1] radius-server accounting 10.1.6.6 1813
[DeviceA-radius-1] radius-server shared-key cipher YsHsjx_202206139
[DeviceA-radius-1] quit
```

Configure an AAA authentication scheme and set the authentication mode to RADIUS.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme auth1
[DeviceA-aaa-authen-auth1] authentication-mode radius
[DeviceA-aaa-authen-auth1] quit
```

Configure an AAA accounting scheme named **acc1** and set the accounting mode to RADIUS accounting.

```
[DeviceA-aaa] accounting-scheme acc1
[DeviceA-aaa-accounting-acc1] accounting-mode radius
[DeviceA-aaa-accounting-acc1] quit
```

Apply the AAA schemes and RADIUS server template to a domain.

```
[DeviceA-aaa] domain huawei.com
[DeviceA-aaa-domain-huawei.com] authentication-scheme auth1
[DeviceA-aaa-domain-huawei.com] accounting-scheme acc1
[DeviceA-aaa-domain-huawei.com] radius-server 1
[DeviceA-aaa-domain-huawei.com] quit
[DeviceA-aaa] quit
```

Step 5 Configure the domain to which the administrator belongs as the global default administrative domain so that the administrator does not need to enter the domain name during an STelnet login to DeviceA.

```
[DeviceA] domain huawei.com admin
```

Step 6 Configure a RADIUS server.

The configuration includes the following steps: add a device, add an administrator account, and set the administrator privilege level to 3.

----End

Verifying the Configuration

The administrator can log in to DeviceA through the STelnet client after entering the correct user name and password.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
radius-server template 1
 radius-server shared-key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!SKvr${[Fs.3t@/5k|BENhEu>W(3\~XG!!D;!!!!!2jp5!!!!!!
A!!!!3"pK8qv!}9M#(4$jGWvQF/R[CNe/+:W^jk8HUe&W%+%#
 radius-server authentication 10.1.6.6 1812 weight 80
 radius-server accounting 10.1.6.6 1813 weight 80
#
aaa
 authentication-scheme auth1
  authentication-mode radius
 accounting-scheme acc1
  accounting-mode radius
 domain huawei.com
  authentication-scheme auth1
  accounting-scheme acc1
  radius-server 1
#
domain huawei.com admin
#
vlan batch 10 20
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 service-manage enable
 service-manage ssh permit
#
interface Vlanif20
 ip address 10.1.6.2 255.255.255.0
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GE0/0/2
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 20
#
firewall zone trust
 add interface Vlanif 10
#
firewall zone untrust
 add interface Vlanif 20
#
security-policy
 rule name sec_policy1
  source-zone local
  destination-zone untrust
  destination-address 10.1.6.6 24
  action permit
#
stelnet server enable
ssh server-source -i Vlanif10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

3.6 CLI: Example for Logging In to the CLI Using STelnet (HWTACACS)

Networking Requirements

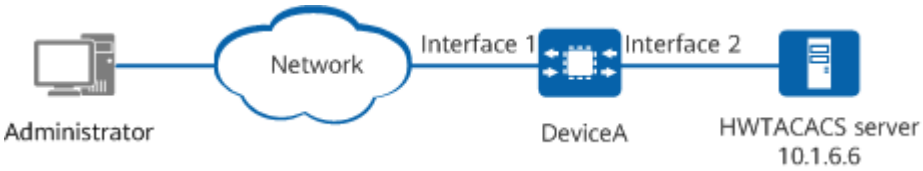
In **Figure 3-8**, an HWTACACS server is deployed on an enterprise network. The enterprise requires that the administrator use HWTACACS authentication to log in to DeviceA through STelnet.

1. The administrator can log in to the device through STelnet only after entering a correct user name and password.
2. After the administrator logs in to the device through STelnet, the privilege level 3 is authorized to the administrator, the commands that the administrator can execute are limited, and the commands that the administrator has executed are recorded.

Figure 3-8 Configuring HWTACACS authentication, authorization, and accounting

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

1. Configure STelnet login on DeviceA: Set the authentication mode for accessing VTY user interfaces to AAA, enable the STelnet service, and configure the authentication mode and service type for SSH users.
2. Configure HWTACACS authentication on DeviceA: Create an HWTACACS server template, configure AAA schemes and recording scheme, and enable command authorization.
3. Configure an HWTACACS server.

Precautions

Ensure that there are reachable routes between the user terminal and DeviceA before the configuration.

Procedure

Step 1 Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] portswitch
[DeviceA-GE0/0/1] port link-type trunk
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/1] port trunk allow-pass vlan 10
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] portswitch
[DeviceA-GE0/0/2] port link-type trunk
[DeviceA-GE0/0/2] port trunk allow-pass vlan 20
[DeviceA-GE0/0/2] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.2 255.255.255.0
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.6.2 255.255.255.0
[DeviceA-Vlanif20] quit
```

Step 2 Add interfaces to security zones and configure interface access control and security policies.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface vlanif 10
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface vlanif 20
[DeviceA-zone-untrust] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] service-manage enable
[DeviceA-Vlanif10] service-manage ssh permit
[DeviceA-Vlanif10] quit
[DeviceA] security-policy
[DeviceA-policy-security] rule name sec_policy1
[DeviceA-policy-security-rule-sec_policy1] source-zone local
[DeviceA-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceA-policy-security-rule-sec_policy1] destination-address 10.1.6.6 24
[DeviceA-policy-security-rule-sec_policy1] action permit
[DeviceA-policy-security-rule-sec_policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure STelnet login.

Generate a local key pair on DeviceA.

```
[DeviceA] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 3072).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

Set the authentication mode and protocol for accessing VTY user interfaces 0 to 4 to AAA and SSH, respectively.

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
[DeviceA-ui-vty0-4] protocol inbound ssh
[DeviceA-ui-vty0-4] quit
```

Enable the SSH server function on DeviceA.

```
[DeviceA] stelnet server enable
[DeviceA] ssh server-source -i vlanif 10
```

Set the authentication mode of all SSH users to password authentication.

```
[DeviceA] ssh authentication-type default password
```

Step 4 Configure HWTACACS authentication, authorization, and accounting.

Create an HWTACACS server template named **template1** for communication between DeviceA and the HWTACACS server.

```
[DeviceA] hwtacacs-server template template1
[DeviceA-hwtacacs-template1] hwtacacs-server authentication 10.1.6.6 49
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-hwtacacs-template1] hwtacacs-server authorization 10.1.6.6 49
[DeviceA-hwtacacs-template1] hwtacacs-server accounting 10.1.6.6 49
[DeviceA-hwtacacs-template1] hwtacacs-server shared-key cipher YsHsjx_202206139
[DeviceA-hwtacacs-template1] quit
```

Create an authentication scheme named **sch1** and set the authentication mode to HWTACACS authentication.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme sch1
[DeviceA-aaa-authen-sch1] authentication-mode hwtacacs
[DeviceA-aaa-authen-sch1] quit
```

Create an authorization scheme named **sch2**, set the authorization mode to HWTACACS authorization, and enable command authorization for the administrator with the privilege level 3.

```
[DeviceA-aaa] authorization-scheme sch2
[DeviceA-aaa-author-sch2] authorization-mode hwtacacs
[DeviceA-aaa-author-sch2] authorization-cmd 3 hwtacacs
[DeviceA-aaa-author-sch2] quit
```

Create a recording scheme named **sch0** to record the commands that the administrator has executed.

```
[DeviceA-aaa] recording-scheme sch0
[DeviceA-aaa-recording-sch0] recording-mode hwtacacs template1
[DeviceA-aaa-recording-sch0] quit
[DeviceA-aaa] cmd recording-scheme sch0
```

Create an accounting scheme named **sch3** and set the accounting mode to HWTACACS accounting.

```
[DeviceA-aaa] accounting-scheme sch3
[DeviceA-aaa-accounting-sch3] accounting-mode hwtacacs
[DeviceA-aaa-accounting-sch3] quit
```

Apply the HWTACACS server template and AAA schemes to the domain **huawei.com**.

```
[DeviceA-aaa] domain huawei.com
[DeviceA-aaa-domain-huawei.com] hwtacacs-server template1
[DeviceA-aaa-domain-huawei.com] authentication-scheme sch1
[DeviceA-aaa-domain-huawei.com] authorization-scheme sch2
[DeviceA-aaa-domain-huawei.com] accounting-scheme sch3
[DeviceA-aaa-domain-huawei.com] quit
[DeviceA-aaa] quit
```

Specify the domain **huawei.com** as a global default administrative domain.

```
[DeviceA] domain huawei.com admin
```

Step 5 Configure an HWTACACS server. Here, the Secure ACS is used as an example.

The configuration includes the following steps: add a device, add an administrator account, set the administrator privilege level to 3, and configure command authorization. Note that the **reset hwtacacs-server statistics all** command cannot be configured.

You can check logs recording command execution successes and failures of all users including non-HWTACACS-authenticated users under **Reports and Activity** > **TACACS+ Administration**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

- The administrator can log in to DeviceA through the STelnet client after entering the correct user name and password.
- After the administrator logs in to DeviceA, run the **reset hwtacacs-server statistics all** command. The system displays the message "Error: Failed to pass the authorization.", indicating that command authorization is successful.

```
[DeviceA] quit
<DeviceA> reset hwtacacs-server statistics all
 Error: Failed to pass the authorization.
```

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hwtacacs-server template template1
 hwtacacs-server authentication 10.1.6.6
 hwtacacs-server authorization 10.1.6.6
 hwtacacs-server accounting 10.1.6.6
 hwtacacs-server shared-key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!SKvr${[Fs."u,S-6a-X1'[X=L"cpF!5Oz`1!!!!!2jp5!!!!!!
A!!!!lx>cM8i{y6!);(8Dr9:dK`&BHfE(H2=.:SH{@pT%+%#
#
aaa
 authentication-scheme sch1
  authentication-mode hwtacacs
 authorization-scheme sch2
  authorization-mode hwtacacs
  authorization-cmd 3 hwtacacs
 accounting-scheme sch3
  accounting-mode hwtacacs
 recording-scheme sch0
  recording-mode hwtacacs template1
 cmd recording-scheme sch0
 domain huawei.com
  authentication-scheme sch1
  accounting-scheme sch3
  authorization-scheme sch2
  hwtacacs-server template1
#
domain huawei.com admin
#
vlan batch 10 20
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 service-manage enable
 service-manage ssh permit
#
interface Vlanif20
 ip address 10.1.6.2 255.255.255.0
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GE0/0/2
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 20
#
firewall zone trust
 add interface Vlanif 10
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
firewall zone untrust
 add interface Vlanif 20
#
security-policy
 rule name sec_policy1
  source-zone local
  destination-zone untrust
  destination-address 10.1.6.6 24
  action permit
#
stelnet server enable
ssh server-source -i Vlanif10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

3.7 Web: Example for Configuring Web UI-based Login Through HTTPS (Default Certificate)

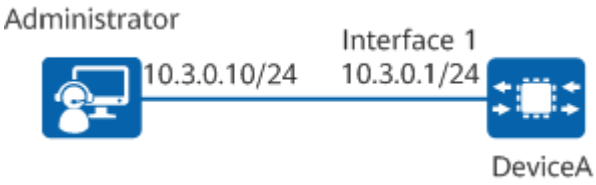
Networking Requirements

In Figure 3-9, the local account **admin123** is configured for DeviceA, which can be used to log in to the web UI of DeviceA through HTTPS.

Figure 3-9 Network diagram for logging in to the web UI through HTTPS (default certificate)

NOTE

In this example, interface 1 represents GE0/0/1.



Data Planning

Item	Data	Description
User name	admin123	-
Password	YsHsjx_202206	-
Service type	HTTPS	-

Configuration Roadmap

1. Configure a login interface for the device.
2. Create a local user account for logging in to the web UI of the device.

 Copyright © Huawei Technologies Co., Ltd.

3. Enable the web service function on the device.
4. Use the local user account to log in to the web UI of the device.

Procedure

Step 1 Configure the login interface.

NOTE

Skip this step if the default IP address of the management interface is used for login.

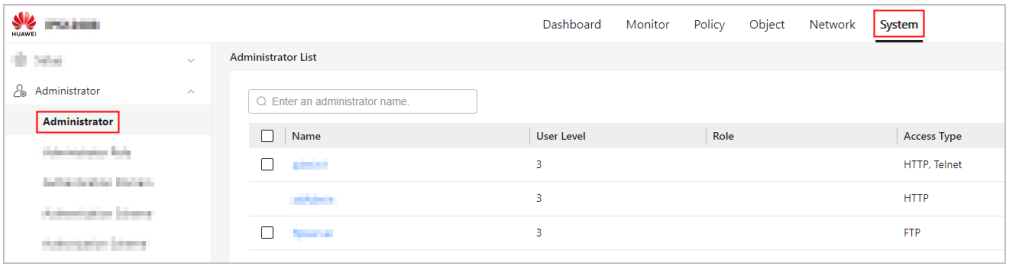
1. Choose **Network** > **Interface**.
2. Click for interface GE0/0/1 and set the parameters as follows:

VPN Instance	public
Zone	trust
Connect Type	Static IP
IP Address	10.3.0.1/24
Access Management	HTTPS

3. Click **OK**.

Step 2 Create a web user account.

1. Choose **System** > **Administrator** > **Administrator**.



2. Click **Add** and set parameters as follows:

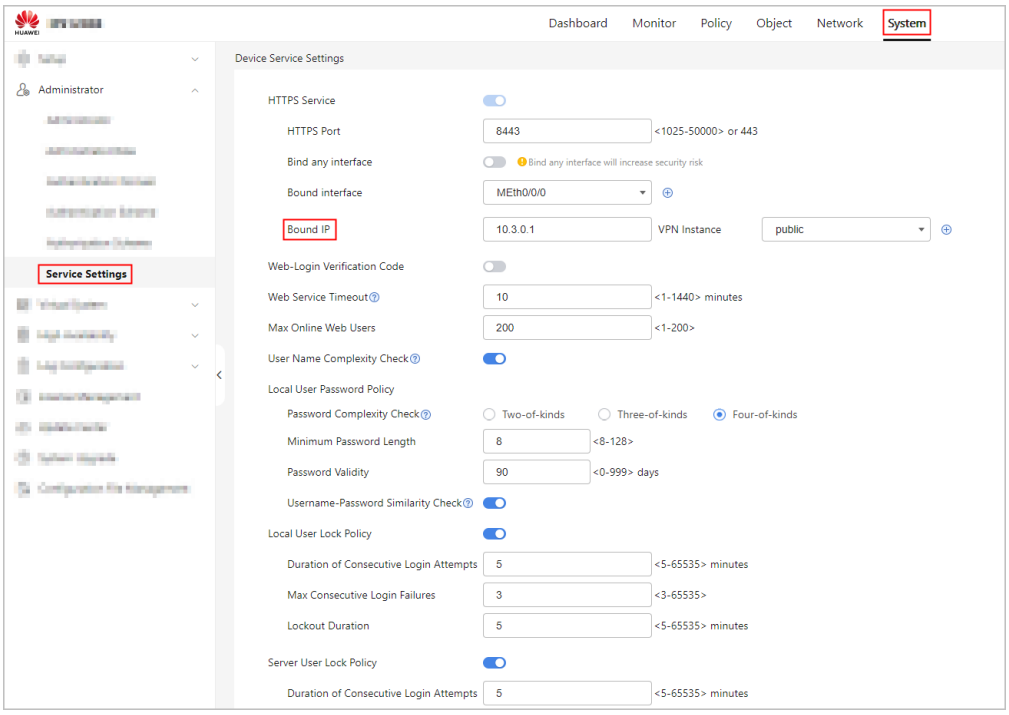
Name	admin123
Password	YsHsjx_202206
Advanced Settings	
Service Type	HTTP

3. Click **OK**.

Step 3 Enable the web service function.

1. Choose **System** > **Administrator** > **Service Settings**.
2. Set **Bound IP** to the IP address and VPN instance configured in **Configure the login interface** and retain the default values for other parameters.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **Apply**.

Step 4 Log in to the web UI.

1. Set the IP address of the PC used for web UI login to 10.3.0.10/24.
2. Open a browser and enter **https://10.3.0.1:8443**.
3. Enter the created web user account (user name: **admin123**; password: **YsHsjx_202206**) and click **Login**.

----End

Verifying the Configuration

Use a browser to access the web UI of the device, enter the user name and password, and check whether the login is successful.

Configuration Scripts

```
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
 service-manage https permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
aaa
local-user admin123 password irreversible-cipher ******
local-user admin123 service-type http
local-user admin123 privilege level 3
local-user admin123 state Active
#
web-manager enable port 8443
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

3.8 CLI: Example for Configuring Web UI-based Login Through HTTPS (Default Certificate)

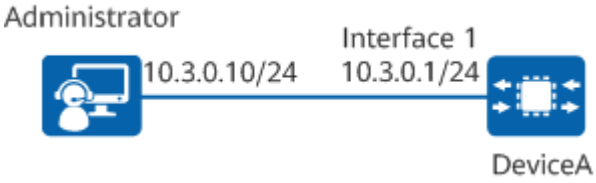
Networking Requirements

In Figure 3-10, the local account **admin123** is configured for DeviceA, which can be used to log in to the web UI of DeviceA through HTTPS.

Figure 3-10 Network diagram for logging in to the web UI through HTTPS (default certificate)

NOTE

In this example, interface 1 represents GE0/0/1.



Data Planning

Item	Data
User name	admin123
Password	YsHsjx_202206
Service type	HTTPS
User privilege level	3

Configuration Roadmap

1. Configure all interfaces to be used to access the web UI.
2. Configure a login interface for the device.
3. Create a local user account for logging in to the web UI of the device.
4. Enable the web service function on the device.
5. Use the local user account to log in to the web UI of the device.

Procedure

Step 1 Configure all interfaces to be used to access the web UI.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] web-manager server-source all-interface
```

Step 2 Configure a login interface for the device.

 Copyright © Huawei Technologies Co., Ltd.

1. Configure an IP address for the interface and enable the HTTPS service on it.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/1] service-manage enable
[DeviceA-GE0/0/1] service-manage https permit
[DeviceA-GE0/0/1] quit
```

2. Add the interface to a security zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Step 3 Create a web user account.

```
[DeviceA] aaa
[DeviceA-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[DeviceA-aaa] local-user admin123 service-type http
[DeviceA-aaa] local-user admin123 privilege level 3
[DeviceA-aaa] quit
```

Step 4 Enable the web service function.

1. Enable the HTTPS service.

```
[DeviceA] web-manager enable port 8443
```

2. Enable forcible redirection from HTTP to HTTPS.

```
[DeviceA] web-manager http forward enable
```

When this function is enabled, HTTPS is used even if you use HTTP to access the web UI.

Step 5 Log in to the web UI.

1. Set the IP address of the PC used for web UI login to 10.3.0.10/24.
2. Open a browser and enter **https://10.3.0.1:8443**.
3. Enter the created web user account (user name: **admin123**; password: **YsHsjx_202206**) and click **Login**.

----End

Verifying the Configuration

Use a browser to access the web UI of the device, enter the user name and password, and check whether the login is successful.

Configuration Scripts

```
#
sysname DeviceA
#
web-manager server-source all-interface
web-manager enable port 8443
web-manager http forward enable
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
 service-manage https permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
aaa
 local-user admin123 password irreversible-cipher $1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!
```

 Copyright © Huawei Technologies Co., Ltd.

```
ab48y=Ic*xEUR4pVhR2"9-~,$
 local-user admin123 service-type http
 local-user admin123 privilege level 3
#
return
```

3.9 CLI: Example for Configuring Web UI-based Login Through HTTPS (Specified Certificate)

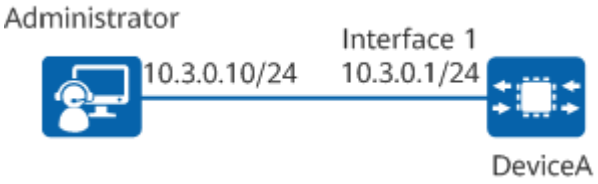
Networking Requirements

In Figure 3-11, the local account **admin123** is configured for DeviceA, which can be used to log in to the web UI of DeviceA through HTTPS.

Figure 3-11 Network diagram for logging in to the web UI through HTTPS (specified certificate)

NOTE

In this example, interface 1 represents GE 0/0/1.



Data Planning

Item	Data
User name	admin123
Password	YsHsjx_202206
Service type	HTTPS
User privilege level	3
Specified certificate	cep_local.cer

Configuration Roadmap

1. Configure a certificate for login authentication.
2. Configure a login interface for the device.
3. Create a local user account for logging in to the web UI of the device.
4. Enable the web service function on the device.
5. Use the local user account to log in to the web UI of the device.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure a certificate.

1. Generate a certificate request file on DeviceA and send the file to the CA server using methods such as the web UI, disks and emails. After the application is approved, the CA server will generate certificates. You can use HTTP, LDAP, or other methods to download the CA certificate and local certificate from the CA server to DeviceA and install them for them to take effect. For details, see "PKI Configuration" in CLI Configuration Guide > Security Protection.

   NOTE

   In the local certificate, the value of **Subject Alternative Name** must be the same as the IP address for logging in to the web UI of the device. If a domain name is used to access the web UI, set **Subject Alternative Name** to the domain name.

   Assume that the CA certificate and local certificate are **cep_ca.cer** and **cep_local.cer**, respectively.

2. Obtain the CA certificate of the CA server that issues certificates to the device and import it to the browser of the PC (client) used for web UI login.

   NOTE

   If the CA certificate is not imported to the browser, the client can still log in to the device through HTTPS. In this case, the client cannot verify the validity of the server's certificate and is vulnerable to attacks.

3. Configure the certificate sent by the device to the client during the client's login to the device through HTTPS.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] web-manager security server-certificate cep_local.cer
```

Step 2 Configure all interfaces to be used to access the web UI.

```
[DeviceA] web-manager server-source all-interface
```

Step 3 Configure a login interface for the device.

1. Configure an IP address for the interface and enable the HTTPS service on it.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/1] service-manage enable
[DeviceA-GE0/0/1] service-manage https permit
[DeviceA-GE0/0/1] quit
```

2. Add the interface to a security zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge0/0/1
[DeviceA-zone-trust] quit
```

Step 4 Create a web user account.

```
[DeviceA] aaa
[DeviceA-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[DeviceA-aaa] local-user admin123 service-type http
[DeviceA-aaa] local-user admin123 privilege level 3
[DeviceA-aaa] quit
```

Step 5 Enable the web service function.

1. Enable the HTTPS service.

```
[DeviceA] web-manager enable port 8443
```

 Copyright © Huawei Technologies Co., Ltd.

2. Enable forcible redirection from HTTP to HTTPS.

```
[DeviceA] web-manager http forward enable
```

When this function is enabled, HTTPS is used even if you use HTTP to access the web UI.

Step 6 Log in to the web UI of the device.

1. Set the IP address of the PC used for web UI login to 10.3.0.10/24.
2. Open a browser and enter **https://10.3.0.1:8443**.
3. Enter the created web user account (user name: **admin123**; password: **YsHsjx_202206**) and click **Login**.

----End

Verifying the Configuration

Use a browser to access the web UI of the device, enter the user name and password, and check whether the login is successful.

Configuration Scripts

```
#
sysname DeviceA
#
web-manager server-source all-interface
web-manager enable port 8443
web-manager http forward enable
web-manager security server-certificate cep_local.cer
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
 service-manage https permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
aaa
 local-user admin123 password irreversible-cipher $1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!
ab48y=Ic*xEUR4pVhR2"9-~,$
 local-user admin123 service-type http
 local-user admin123 privilege level 3
#
return
```

3.10 Handling Administrator Password Loss

Context

By default, the device does not have an account. You need to create an account upon the first login. If you forget the password of an account, you can log in to the device using another account or the console port to change the password of the target account. If you also forget the password of the console port, use the BootLoader menu to clear the password of the console port and log in to the device to change the password of the target account.

 Copyright © Huawei Technologies Co., Ltd.

Changing the Password of the Target Account

Log in to the device using another account or the console port to change the password of the target account. To ensure successful password change, you need to log in using an account whose level is at least level 3 and no lower than the target account. Assume that the target account is **admin123** and its password will be reset to **YsHsjx_202206**.

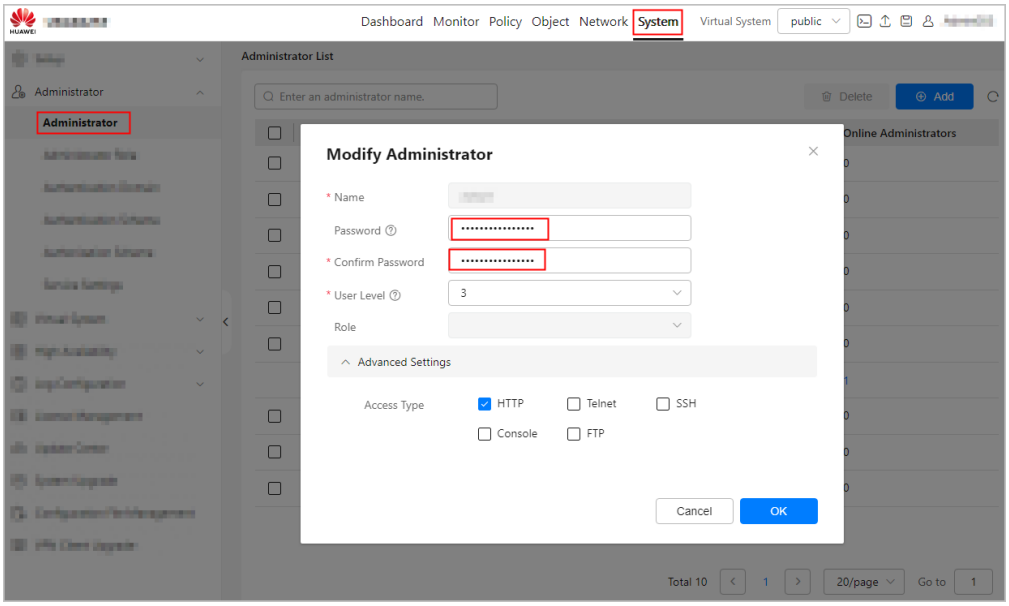
Changing the Password Through the CLI

Log in to the CLI of the device using another account or the console port to change the password of the target account.

```
<HUAWEI> system
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] quit
[HUAWEI]
```

Changing the Password on the Web UI

1. Choose **System** > **Administrator** > **Administrator**.
2. Click user name corresponding to the target account to change the password.



3. Click **OK**.

Clearing the Password of the Console Port

Clear the password of the console port through the BootLoader menu and log in to the device.

```
Press CTRL+B to enter BOOT menu: 3
Info: The password is empty. For security purposes, change the password.

New password:
Confirm password:

The password is changed successfully.

    Main Menu
```

 Copyright © Huawei Technologies Co., Ltd.

```
  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. List file
  6. Password manager submenu
  7. Restore factory defaults
  8. Reboot

Enter your choice(1-8): 6            //Access the password management submenu.

      Password manager submenu

  1. Modify bootloader password
  2. Clear the console login password
  3. Reset bootloader password
  0. Return

Enter your choice(0-3): 2


Caution: A new console password must be set after the restart.
Continue now? Yes(y) or No(n): y
Clear Console Lockword Successfully.

Please Press ENTER.


**********************************************************************
*                    Copyright (C) 2020-2020                         *
*                 Huawei Technologies Co., Ltd.                      *
*                    All rights reserved.                            *
*          Without the owner's prior written consent,                *
*    no decompiling or reverse-engineering shall be allowed.         *
**********************************************************************

Info: The max number of VTY users is 5, the number of current VTY users online is 0, and total number of
terminal users online is 1.
     The current login time is yyyy-mm-dd hh:mm:ss.
<HUAWEI>
```

3.11 Handling BootLoader Password Loss

Context

By default, the BootLoader has no password. You need to set a password when accessing the BootLoader main menu for the first time. If you forget the password, you need to first clear the password and then set a new one.

Clearing the BootLoader Password

Press and hold the **RESET** button to clear the BootLoader password.

Hold down the **RESET** button for 5s. Then the device restarts, After the restart, the BootLoader password is cleared.

NOTICE

After you press and hold down the **RESET** button, the device restarts with factory settings and deletes the current configuration file. To prevent the configuration file from being lost, back up the current configuration file before pressing the **RESET** button.

Press and hold down the **RESET** button to restart the device. Perform the following operations to set the backup configuration file as the configuration file for the next startup and restart the device.

1. Set the configuration file for the next startup to the configuration file backed up before pressing the **RESET** button.
   ```
   <HUAWEI> startup saved-configuration vrpcfg.zip    //The file name is the name of the backup configuration file.
   ```
2. Run the **reboot** command to restart the device. If the following information is displayed, enter **N** so the configuration changes generated during this operation will not be saved, avoiding overwriting the original configuration file.
   ```
   Warning: The configuration has been modified, and it will be saved to the next startup saved-configuration file flash:/vrpcfg.zip.
   Continue? [Y/N]:N
   ```
3. Set the **BootLoader** password during device restart.

   Log in to the device through the console port. When the message **Press Ctrl +B to enter BOOT menu** is displayed during device startup, press **Ctrl+B** within 3 seconds to access the BootLoader main menu. Access the password management submenu, enter the old password, and then enter the new password.
   ```
   Press Ctrl+B to enter BOOT menu: 3
   Password:

       Main Menu

     1. Default startup
     2. Serial submenu
     3. Ethernet submenu
     4. Startup parameters submenu
     5. List file
     6. Password manager submenu
     7. DFX submenu
     8. Reboot


   Enter your choice(1-8):  6          //Access the password manager submenu.

       Password manager submenu

     1. Modify bootloader password
     2. Clear the console login password
     3. Reset bootloader password
     0. Return

   Enter your choice(0-3): 1

   Old password:                       //Enter the old password.

   New password:                       //Enter a new password. The new password cannot be the same as the old password.
   Confirm password:
   Warning: The bootloader password will be written to the
   device.
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
Continue now? Yes(y) or No(n): y

The password is changed successfully.
```

 Copyright © Huawei Technologies Co., Ltd.

4 Accessing the Internet Using One Interface

4.1 Web: Example for Accessing the Internet Using a Static IPv4 Address
4.2 CLI: Example for Accessing the Internet Using a Static IPv4 Address
4.3 Web: Example for Accessing the Internet Using DHCP
4.4 CLI: Example for Accessing the Internet Using DHCP
4.5 Web: Example for Configuring Static IPv6 Addresses for Devices to Communicate
4.6 CLI: Example for Configuring Static IPv6 Addresses for Devices to Communicate

4.1 Web: Example for Accessing the Internet Using a Static IPv4 Address

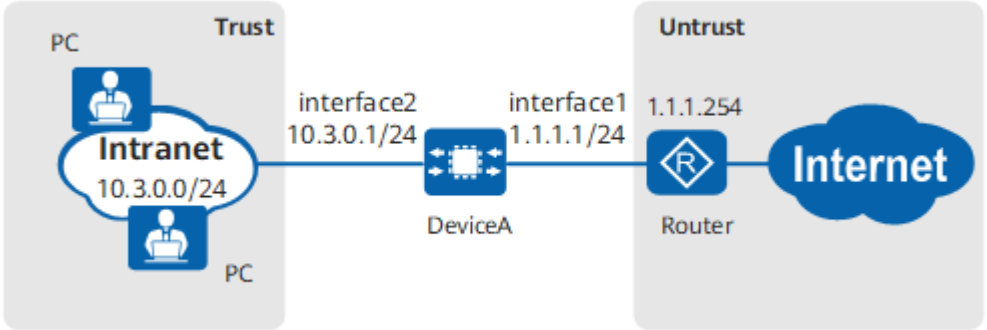
Networking Requirements

As shown in **Figure 4-1**, an enterprise deploys DeviceA as a security gateway on the network border and purchases broadband services from an ISP to implement intranet users' Internet access.

Figure 4-1 Network diagram of accessing the Internet through static IPv4 addresses

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

The following information is used as an example. Obtain the desired service information from your local ISP.

Table 4-1 Parameters provided by an ISP

Item	Data	Description
Enterprise address	1.1.1.1/24	Public network address that the ISP assigns to the enterprise
Default gateway address	1.1.1.254	Provided by the ISP

Configuration Roadmap

1. Configure IP addresses of interfaces and assign the interfaces to security zones.
2. Configure security policies to allow PCs to access the Internet.
3. Configure NAT policies for source address translation. As DeviceA translates private addresses into a fixed public network address that is assigned by the ISP, Easy IP is used to simplify the configuration.
4. Configure a default route on the DeviceA, so that traffic from the intranet can be forwarded to the ISP router.
5. Configure return routes on the ISP router. This operation is performed by the ISP. Therefore, the configuration details are not provided.
6. On the intranet PC, set the IP address to 10.3.0.100/24, gateway IP address to 10.3.0.1, and public DNS to 1.1.1.1/114.114.114.114.

   NOTE

   The device does not support the DNS proxy function. Therefore, the DNS of the intranet PC cannot be set to the IP address 10.3.0.1 of interface 2. Only the public DNS service can be used.

Procedure

Step 1 Configure the address for GE 0/0/1.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE 0/0/1 and set the following parameters.

Zone	untrust
Mode	Route
IPv4 Address	1.1.1.1/24

3. Repeat the preceding steps to set the parameters for GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

Security Zone	trust
Mode	Routing
IPv4 Address	10.3.0.1/24

Step 2 Configure security policies. In actual scenarios, more refined security policies can be configured to control Internet access of intranet users.

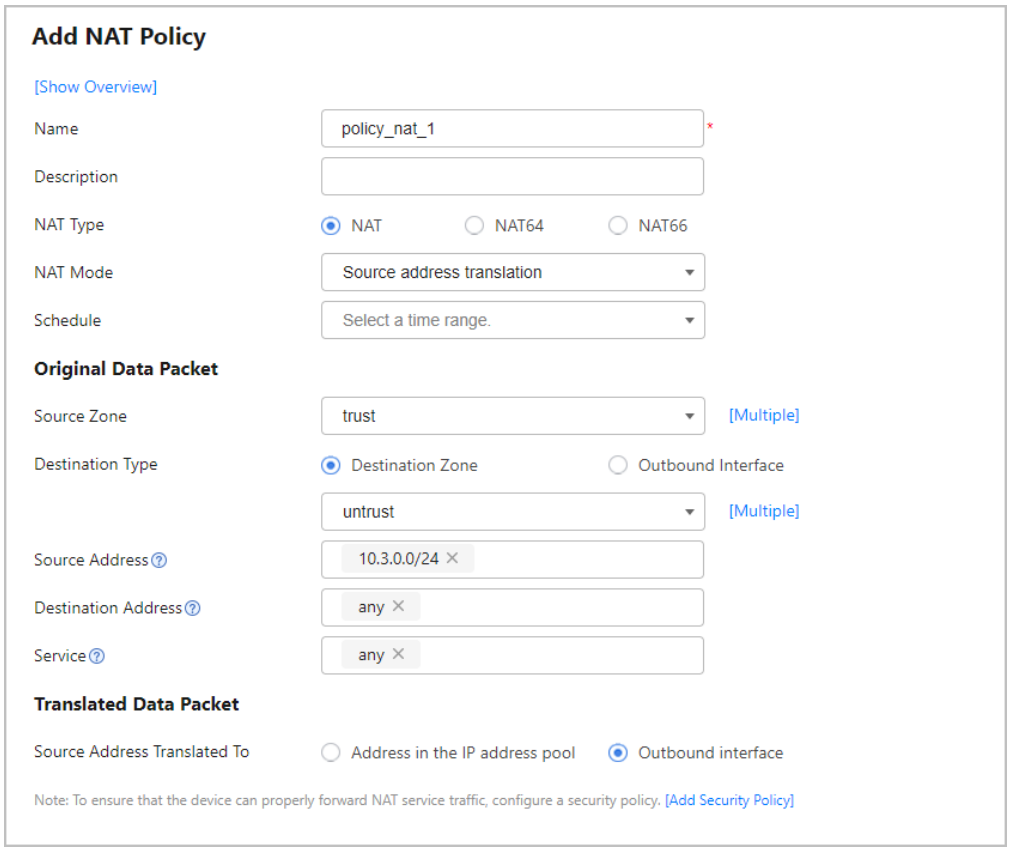
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Name	policy_sec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

Step 3 Configure a NAT policy, allowing PCs on the intranet to access the Internet by using the resulting public IP address of translation.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.
2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure the default route whose next hop IP address is 1.1.1.254.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

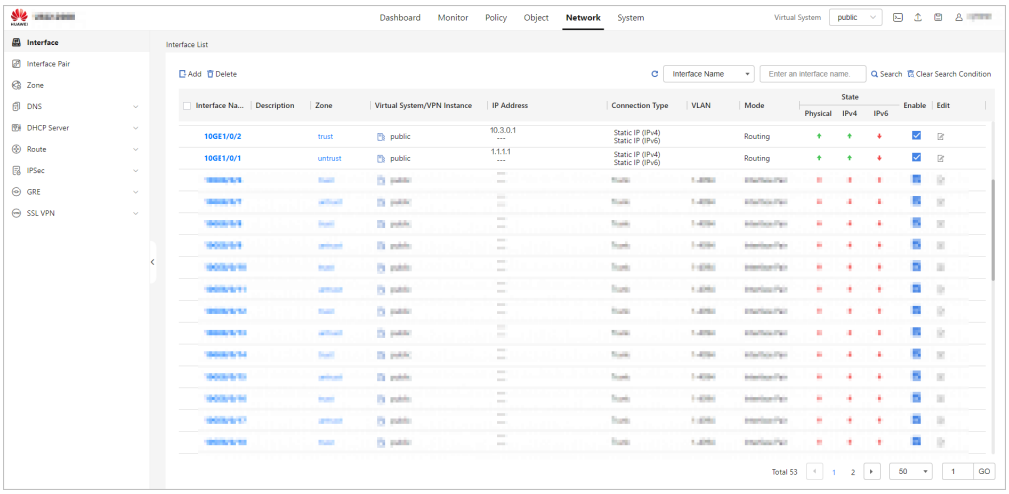
Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

----End

Verifying the Configuration

1. View details about **GE 0/0/1** and check whether the public network address of interface **GE 0/0/1** is correct and both the physical and IPv4 states are Up.

 Copyright © Huawei Technologies Co., Ltd.



2. Check whether an intranet PC can use a domain name to access the Internet. If the PC can access the Internet, the configuration is successful. If the PC fails to access the Internet, modify the configuration and try again.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
  rule name policy_sec_1
  source-address 10.3.0.0 24
  source-zone trust
  destination-zone untrust
  action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 10.3.0.0 24
    action source-nat easy-ip
#
return
```

4.2 CLI: Example for Accessing the Internet Using a Static IPv4 Address

 Copyright © Huawei Technologies Co., Ltd.

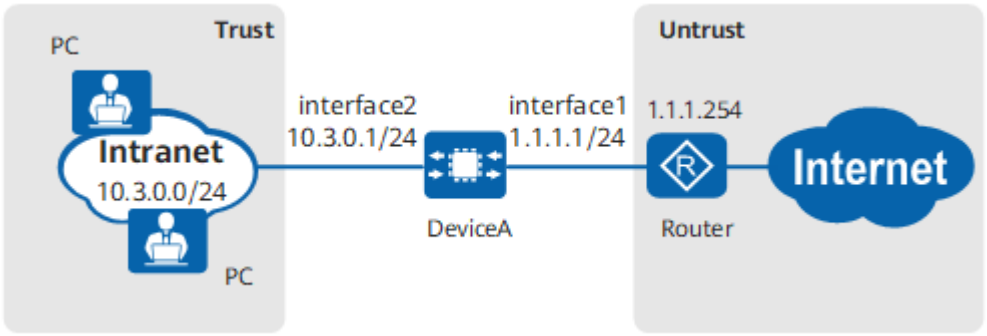
Networking Requirements

As shown in **Figure 4-2**, an enterprise deploys DeviceA as a security gateway on the network border and purchases broadband services from an ISP to implement intranet users' Internet access.

Figure 4-2 Network diagram of accessing the Internet through static IPv4 addresses

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



The following information is used as an example. Obtain the desired service information from your local ISP.

Table 4-2 Parameters provided by an ISP

Item	Data	Description
Enterprise address	1.1.1.1/24	Public network address that the ISP assigns to the enterprise
Default gateway address	1.1.1.254	Provided by the ISP

Configuration Roadmap

1. Configure IP addresses of interfaces and assign the interfaces to security zones.
2. Configure security policies to allow PCs to access the Internet.
3. Configure NAT policies for source address translation. As DeviceA translates private addresses into a fixed public network address that is assigned by the ISP, Easy IP is used to simplify the configuration.
4. Configure a default route on the DeviceA, so that traffic from the intranet can be forwarded to the ISP router.
5. Configure return routes on the ISP router. This operation is performed by the ISP. Therefore, the configuration details are not provided.

 Copyright © Huawei Technologies Co., Ltd.

6. On the intranet PC, set the IP address to 10.3.0.100/24, gateway IP address to 10.3.0.1, and public DNS to 1.1.1.1/114.114.114.114.

   NOTE

   The device does not support the DNS proxy function. Therefore, the DNS of the intranet PC cannot be set to the IP address 10.3.0.1 of interface 2. Only the public DNS service can be used.

Procedure

Step 1 Set the IP addresses of interfaces, and then assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies, allowing PCs on the intranet to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT policy, allowing PCs on the intranet to access the Internet by using the resulting public IP address of translation.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat_1
[DeviceA-policy-nat-rule-policy_nat_1] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-policy-nat-rule-policy_nat_1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat_1] action source-nat easy-ip
[DeviceA-policy-nat-rule-policy_nat_1] quit
[DeviceA-policy-nat] quit
```

Step 4 Configure the default route whose next hop IP address is 1.1.1.254.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

----End

Verifying the Configuration

1. View details about **GE 0/0/1** and check whether the public network address of interface **GE 0/0/1** is correct and both the physical and IPv4 states are Up.

```
<DeviceA> display ip interface brief ge 0/0/1
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(E): E-Trunk down
```

 Copyright © Huawei Technologies Co., Ltd.

```
Interface                   IP Address/Mask      Physical   Protocol
10GE 1/0/1                    1.1.1.1/24         UP         UP
```

2. Check whether an intranet PC can use a domain name to access the Internet. If the PC can access the Internet, the configuration is successful. If the PC fails to access the Internet, modify the configuration and try again.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name policy_sec_1
  source-address 10.3.0.0 24
  source-zone trust
  destination-zone untrust
  action permit
#
nat-policy
 rule name policy_nat_1
  source-zone trust
  source-address 10.3.0.0 24
  action source-nat easy-ip
#
return
```

4.3 Web: Example for Accessing the Internet Using DHCP

Networking Requirements

As shown in **Figure Networking diagram of accessing the Internet through DHCP**, the DeviceA functions as an egress gateway and connects PCs on an intranet to the Internet. The network plan is as follows:

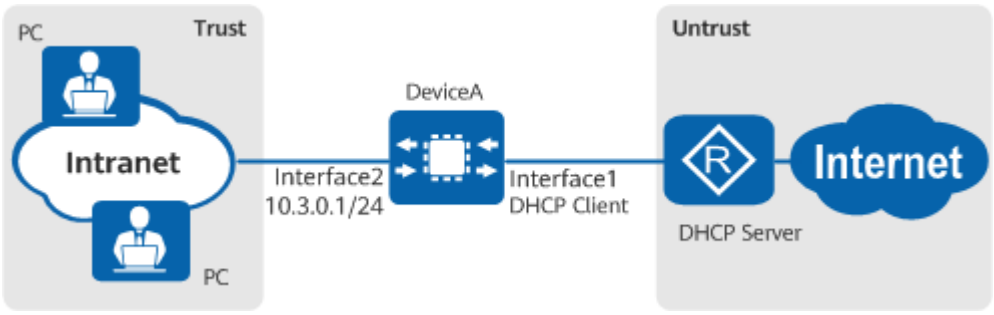
- The PCs on the intranet are deployed on the 10.3.0.0/24 network segment. The customer wants the DeviceA to assign IP addresses to intranet users and implement Internet access for intranet users.
- The DeviceA functions as a DHCP client and applies to a DHCP server (carrier device) for IPv4 and DNS addresses for Internet access of intranet users.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Networking diagram of accessing the Internet through DHCP

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

1. Enable the DHCP client function on interface1 of the DeviceA to obtain IPv4 and DNS server addresses from a DHCP server.
2. Configure an IPv4 address on interface2 of the DeviceA for connecting to the intranet.
3. Configure interface2 of the DeviceA as a DHCP server to dynamically assign IPv4 and DNS server addresses to the intranet. Configure intranet PCs to automatically obtain IP addresses and the DNS server address.
4. Configure a security policy and a NAT policy (easy-IP) on the DeviceA.

NOTE

After the DeviceA obtains IPv4 addresses from the DHCP server, the DHCP server sends the default route to the DHCP client. The next hop address of the default route is the carrier's device. Therefore, no extra default route is required in this networking.

Procedure

Step 1 Configure IP addresses of interfaces and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE 0/0/1 and set the parameters as follows.

Zone	untrust
Mode	Routing
IPv4	
Connection Type	DHCP

3. Repeat the preceding steps to set the parameters for GE 0/0/2.

Zone	trust
Mode	Routing
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

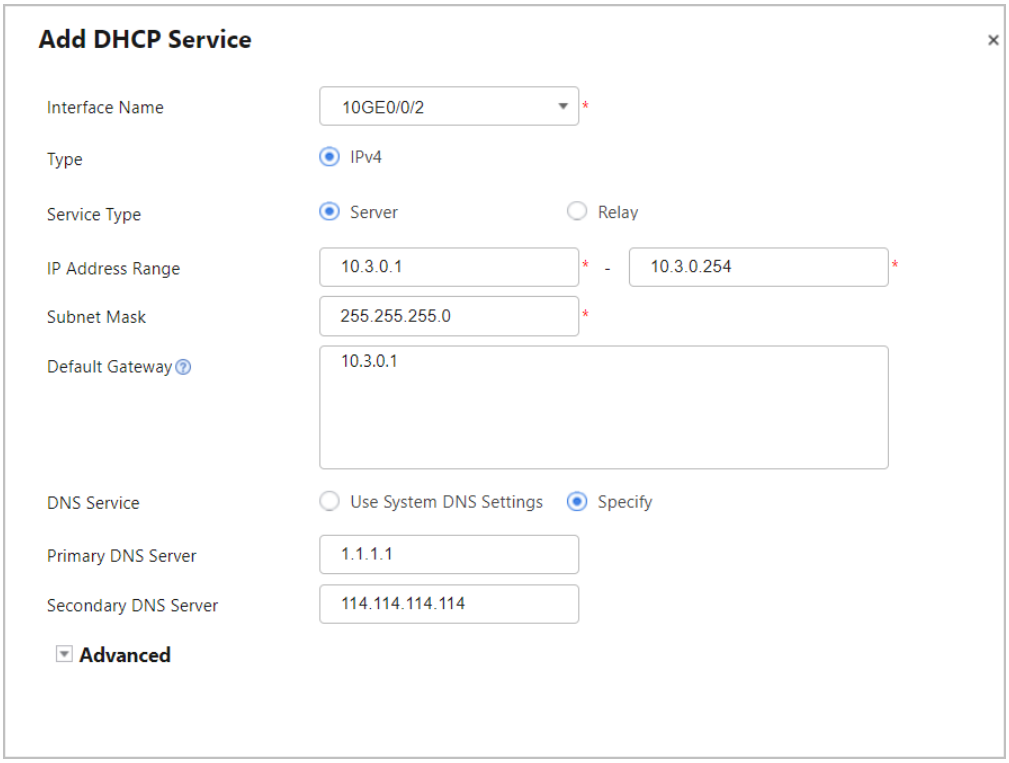
Connection Type	Static IP
IP Address	10.3.0.1/255.255.255.0

Step 2 Configure the dynamic DNS resolution. Currently, the configuration cannot be performed on the web UI. Click **CLI Console** in the lower right corner of the page to display the CLI configuration page and configure it on the CLI.

```
<HUAWEI> system-view
[HUAWEI] dns resolve
```

Step 3 Configure GE 0/0/2 as a DHCP server to assign IP addresses to the intranet.

1. Choose **Network** > **DHCP Server** > **Service**.
2. In **DHCP Service List**, click **Add** and configure the DHCP service as follows.



3. Click **OK**.

Step 4 Configure security policies so that intranet PCs can access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Name	sec_policy_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

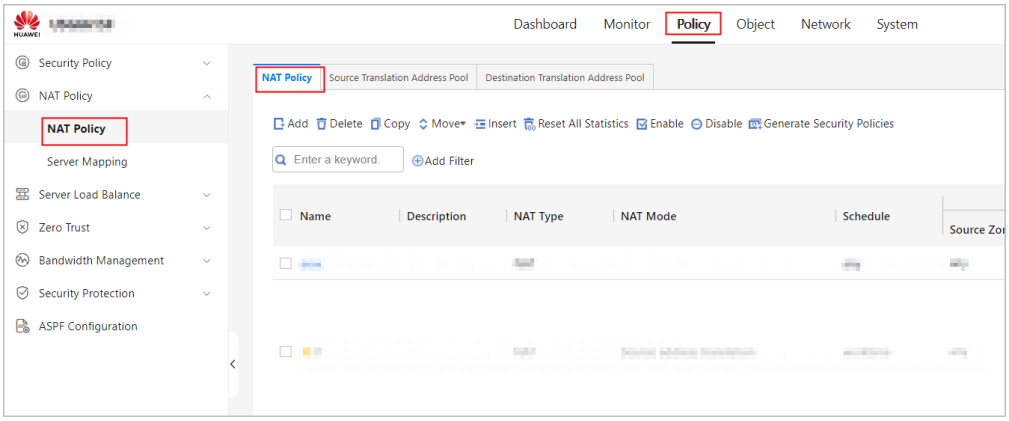
3. Repeat the preceding steps to create two security policies to allow users on the internal network segment 10.3.0.0/24 to access the Internet using domain names.

Name	sec_policy_2
Source Zone	trust
Destination Zone	local
Source Address	10.3.0.0/24
Service	dns
Action	Permit

Name	sec_policy_3
Source Zone	local
Destination Zone	untrust
Service	dns
Action	Permit

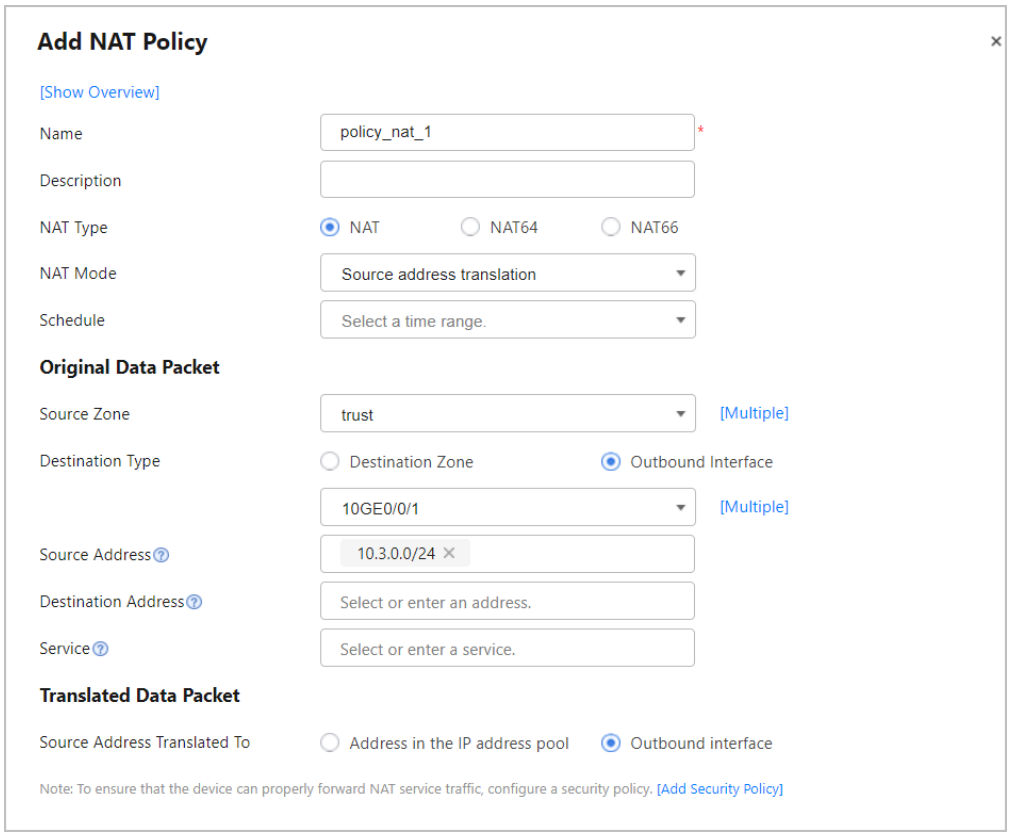
Step 5 Configure a NAT policy to translate private IP addresses into public IP addresses before intranet PCs access the Internet.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.



2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **OK**.

----End

Verification

1. Check the status of GE 0/0/1 (uplink).
   a. Choose **Network** > **Interface**.
   b. Verify that the physical status and IPv4 status of the interface are Up, the connection type is DHCP, and the interface has obtained an IPv4 address.
2. Check whether the PCs on the intranet can use domain names to access the Internet. If the PCs can access the Internet, the configuration is successful. If the PCs fail to access the Internet, modify the configuration and try again.

Configuration Scripts

```
#
sysname DeviceA
#
dns resolve
#
dhcp enable
#
interface GE0/0/1
 ip address dhcp-alloc
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
 dhcp select interface
 dhcp server mask 255.255.255.0
 dhcp server ip-range 10.3.0.1 10.3.0.254
```

 Copyright © Huawei Technologies Co., Ltd.

```
 dhcp server gateway-list 10.3.0.1
 dhcp server dns-list 1.1.1.1 114.114.114.114
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name sec_policy_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_2
  source-zone trust
  destination-zone local
  source-address 10.3.0.0 mask 255.255.255.0
  service dns
  action permit
 rule name sec_policy_3
  source-zone local
  destination-zone untrust
  service dns
  action permit
#
nat-policy
 rule name policy_nat_1
  source-zone trust
  egress-interface GE0/0/1
  source-address 10.3.0.0 24
  action nat easy-ip
#
return
```

4.4 CLI: Example for Accessing the Internet Using DHCP

Networking Requirements

Figure 4-4 shows that a DeviceA functions as an egress gateway and connect PCs in an intranet to the Internet. The network plan is as follows:

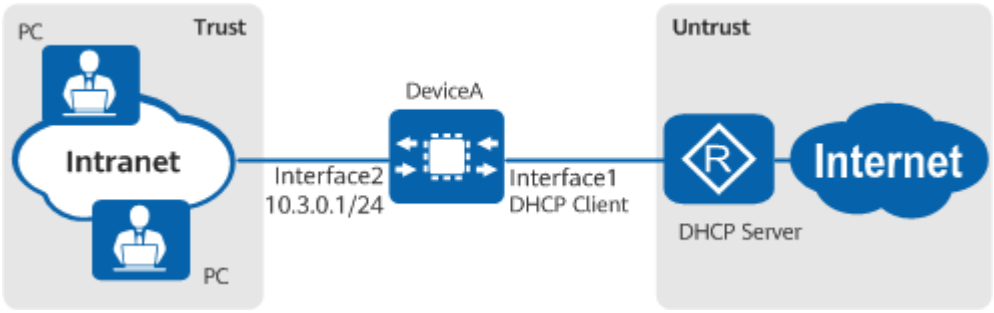
- An administrator manually specifies an IPv4 address for each PC on the network segment 10.3.0.0/24.
- An interface with a static IPv4 address connects the DeviceA to the intranet.
- Another interface on the DeviceA that functions as a DHCP client applies for a client IPv4 address and a DNS server IP address from a DHCP server and connects the intranet to the Internet.

Figure 4-4 Networking diagram for accessing the Internet using DHCP

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the DHCP client function on interface1 of the DeviceA to obtain a client IPv4 address and a DNS server address from a DHCP server.
2. Specify a static IPv4 address on interface2 that connects the DeviceA to the intranet.
3. Configure a security policy and a NAT policy (easy-IP) on the DeviceA.
4. Set the IP addresses of the PCs' gateway to 10.3.0.1, and DNS server is set to 1.1.1.1 and 114.114.114.114. This example provides the configuration procedure on the DeviceA. The configuration procedure for the PCs is not provided.

NOTE

After the DeviceA obtains an IPv4 address from a DHCP server, the DHCP server issues a default route to the DeviceA that function as a DHCP client. The next hop of the default route is a carrier's device. Therefore, there is no need to configure a default route.

Procedure

Step 1 Configure the IP address of the interface and assign the interfaces to the security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
<DeviceA> system-view
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.3.0.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Configure the DNS function.

```
[DeviceA] dns resolve
```

Step 3 Configure GE0/0/1 as a DHCP client.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE 0/0/1] ip address dhcp-alloc
[DeviceA-GE 0/0/1] quit
```

Step 4 Configure a security policy to allow the PCs to access the Internet.

```
[DeviceA] security-policy
[DeviceA-security-policy] rule name policy_sec_1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-security-policy-sec_policy_1] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-security-policy-sec_policy_1] source-zone trust
[DeviceA-security-policy-sec_policy_1] destination-zone untrust
[DeviceA-security-policy-sec_policy_1] action permit
[DeviceA-security-policy-sec_policy_1] quit
[DeviceA-security-policy] quit
[DeviceA-security-policy] rule name policy_sec_2
[DeviceA-security-policy-sec_policy_2] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-security-policy-sec_policy_2] source-zone trust
[DeviceA-security-policy-sec_policy_2] destination-zone local
[DeviceA-security-policy-sec_policy_2] action permit
[DeviceA-security-policy-sec_policy_2] quit
[DeviceA-security-policy] quit
[DeviceA-security-policy] rule name policy_sec_3
[DeviceA-security-policy-sec_policy_3] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-security-policy-sec_policy_3] source-zone local
[DeviceA-security-policy-sec_policy_3] destination-zone untrust
[DeviceA-security-policy-sec_policy_3] action permit
[DeviceA-security-policy-sec_policy_3] quit
[DeviceA-security-policy] quit
```

Step 5 Configure a NAT policy to translate private network IP addresses into public network IP addresses before PCs access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat_1
[DeviceA-policy-nat-rule-policy_nat_1] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-policy-nat-rule-policy_nat_1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat_1] egress-interface ge 0/0/1
[DeviceA-policy-nat-rule-policy_nat_1] action source-nat easy-ip
[DeviceA-policy-nat-rule-policy_nat_1] quit
[DeviceA-policy-nat] quit
```

----End

Configuration Verification

1. Check the status of GE 0/0/1 (uplink).
   a. Choose **Network** > **Interface**.
   b. Verify that the physical status and IPv4 status are Up, the connection type is DHCP, and the interface obtained an IPv4 address.
2. Check whether the PC on the intranet can use domain names to access the Internet. If the PC can access the Internet, the configuration is successful. If the PC fails to access the Internet, modify the configuration and try again.

Configuration Script

```
#
sysname DeviceA
#
dns resolve
#
interface GE 0/0/1
 ip address dhcp-alloc
#
interface GE 0/0/2
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254 preference 245
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
security-policy
 rule name policy_sec_2
  source-zone trust
  destination-zone local
  source-address 10.3.0.0 24
  action permit
#
security-policy
 rule name policy_sec_3
  source-zone local
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat_1
  source-zone trust
  egress-interface GE 0/0/1
  source-address 10.3.0.0 24
  action source-nat easy-ip
#
return
```

4.5 Web: Example for Configuring Static IPv6 Addresses for Devices to Communicate

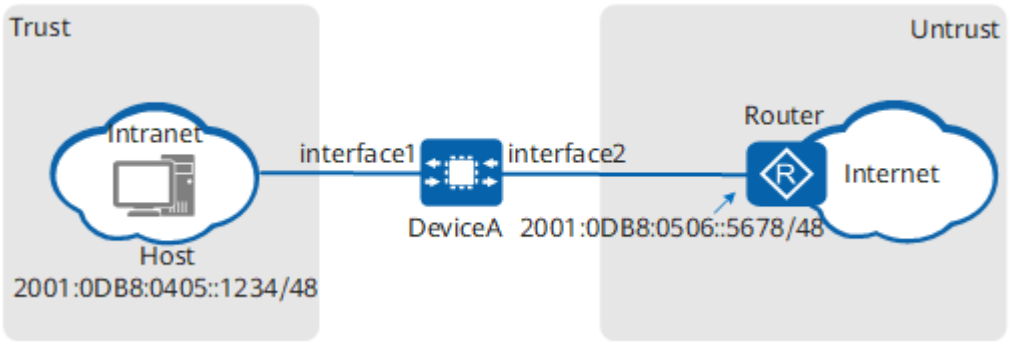
Networking Requirements

An enterprise deploys DeviceA as a security gateway on the network border and purchases broadband services from a carrier to implement intranet users' Internet access using IPv6 addresses.

Figure 4-5 Networking diagram of accessing the Internet through an IPv6 address

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

The following information is used as an example. Obtain the desired service information from your local ISP.

Table 4-3 Parameters provided by an ISP

Item	Data	Description
Enterprise address	2001:0DB8:0506::1234/48	Public network address that the ISP assigns to the enterprise, the IP address of interface2.
Default gateway address	2001:0DB8:0506::5678	Provided by the ISP

Configuration Roadmap

1. Configure IP addresses of interfaces and add the interfaces to security zones.
2. Configure a security policy so that intranet hosts can access the Internet.
3. Configure a default route on the DeviceA, so that traffic from the intranet can be forwarded to the ISP router.
4. Configure return routes on the ISP router, so that the router forwards return traffic from the Internet to the DeviceA. This operation is performed by the ISP. Therefore, the configuration details are not provided.
5. Configure the default gateway on each host on the intranet, so that the hosts send traffic to the DeviceA when they access the Internet.

   The configuration details are not provided.
6. Configure IP addresses and DNS server addresses on intranet PCs. The configuration details are not provided.

Procedure

Step 1 Configure the IPv6 address for GE 0/0/1.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE 0/0/1 and set the following parameters.

Zone	trust
Mode	Route
IPv6 Address	2001:0DB8:0405::5678/48

3. Repeat the preceding steps to set the parameters for GE 0/0/2.

Security Zone	untrust
Mode	Routing

 Copyright © Huawei Technologies Co., Ltd.

IPv6 Address	2001:0DB8:0506::1234/48

Step 2 Configure a security policy. In actual scenarios, more refined security policies can be configured to control Internet access of intranet users.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Name	policy_sec_1
Source Zone	trust
Destination Zone	untrust
Action	Permit

Step 3 Configure a default route on the DeviceA, so that traffic from the intranet can be forwarded to the ISP router.

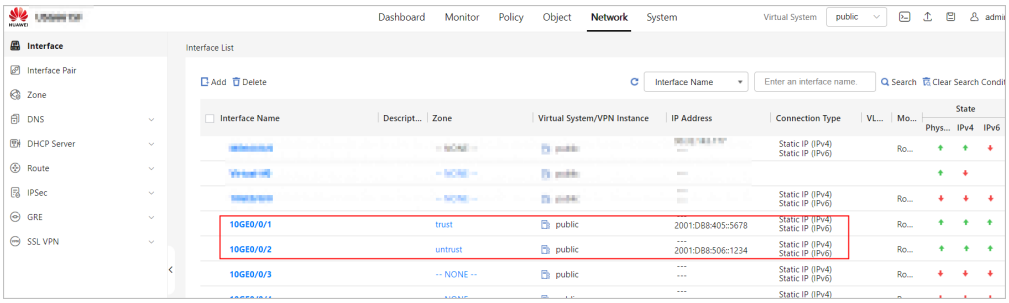
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv6
Destination Address/Mask	::/0
Next Hop	2001:0DB8:0506::5678

----End

Configuration Verification

1. Check the status of **GE 0/0/2**. If the configuration is successful, the configured global unicast address can be displayed. In addition, the physical status and IPv6 status of the interface is up.



2. Check whether intranet hosts can use domain names to access the Internet. If the hosts can access the Internet, the configurations are correct. If the hosts fail to access the Internet, modify the configuration and try again.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

Configuration script for DeviceA:

```
#
sysname DeviceA
#
interface GE 0/0/1
 ipv6 enable
 ipv6 address 2001:0DB8:0405::5678 48
#
interface GE 0/0/2
 ipv6 enable
 ipv6 address 2001:0DB8:0506::1234 48
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  action permit
#
ipv6 route-static :: 0 2001:DB8:506::5678
#
return
```

4.6 CLI: Example for Configuring Static IPv6 Addresses for Devices to Communicate

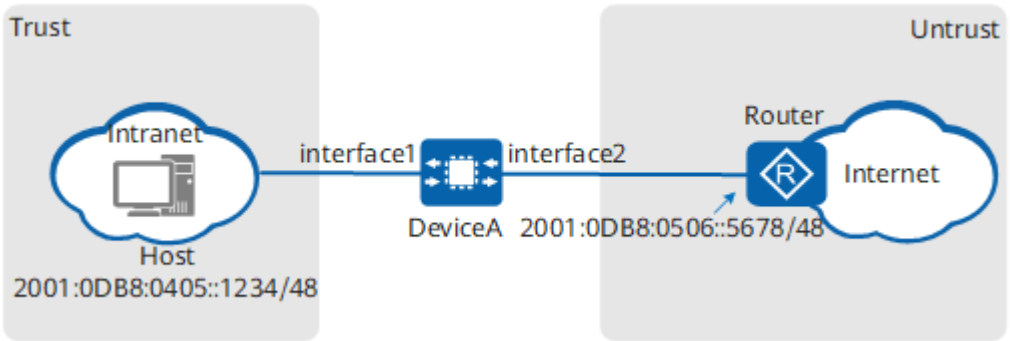
Networking Requirements

An enterprise deploys DeviceA as a security gateway on the network border and purchases broadband services from a carrier to implement intranet users' Internet access using IPv6 addresses.

Figure 4-6 Networking diagram of accessing the Internet through an IPv6 address

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

The following information is used as an example. Obtain the desired service information from your local ISP.

Table 4-4 Parameters provided by an ISP

Item	Data	Description
Enterprise address	2001:0DB8:0506::1234/48	Public network address that the ISP assigns to the enterprise, the IP address of interface2.
Default gateway address	2001:0DB8:0506::5678	Provided by the ISP

Configuration Roadmap

1. Configure IP addresses of interfaces and add the interfaces to security zones.
2. Configure a security policy so that intranet hosts can access the Internet.
3. Configure a default route on the DeviceA, so that traffic from the intranet can be forwarded to the ISP router.
4. Configure return routes on the ISP router, so that the router forwards return traffic from the Internet to the DeviceA. This operation is performed by the ISP. Therefore, the configuration details are not provided.
5. Configure the default gateway on each host on the intranet, so that the hosts send traffic to the DeviceA when they access the Internet.

   The configuration details are not provided.
6. Configure IP addresses and DNS server addresses on intranet PCs. The configuration details are not provided.

Procedure

Step 1 Configure the IPv6 address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipv6 enable
[DeviceA-GE0/0/1] ipv6 address 2001:0DB8:0405::5678 48
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Step 2 Configure the IPv6 address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:0DB8:0506::1234 48
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface  ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 3 Configure a security policy. In actual scenarios, more refined security policies can be configured to control Internet access of intranet users.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
[DeviceA-policy-security] quit
```

Step 4 Configure a default route on the DeviceA, so that traffic from the intranet can be forwarded to the ISP router.

```
[DeviceA] ipv6 route-static 0:0::0:0 0 2001:0DB8:0506::5678
```

----End

Configuration Verification

1. Check the status of **GE 0/0/1**. The following example uses **GE 0/0/1** on DeviceA. If the configuration is successful, the configured global unicast address can be displayed. In addition, the physical status and IPv6 status of the interface is up.

   ```
   [DeviceA] display ipv6 interface ge 0/0/1
   GE0/0/1 current state : UP
   IPv6 protocol current state : UP
   IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE00:1708
     Global unicast address(es):
       2001:DB8:405::5678, subnet is 2001:DB8:405::/48
   ```

2. Check whether intranet hosts can use domain names to access the Internet. If the hosts can access the Internet, the configurations are correct. If the hosts fail to access the Internet, modify the configuration and try again.

Configuration Scripts

Configuration script for DeviceA:

```
#
sysname DeviceA
#
interface ge 0/0/1
 ipv6 enable
 ipv6 address 2001:0DB8:0405::5678 48
#
interface GE 0/0/2
 ipv6 enable
 ipv6 address 2001:0DB8:0506::1234 48
#
firewall zone untrust
 set priority 5
 add interface ge0/0/1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  action permit
#
ipv6 route-static 0:0::0:0 0 2001:0DB8:0506::5678
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

5 Accessing the Internet Using Multiple Interfaces

5.1 Web: Example for Configuring ISP Link Selection to Forward Traffic by ISPs

5.2 CLI: Example for Configuring ISP Link Selection to Forward Traffic by ISPs

5.3 Configuring PBR and PBR-based Intelligent Uplink Selection

5.4 Configuring Equal Cost Route-based Intelligent Uplink Selection

5.1 Web: Example for Configuring ISP Link Selection to Forward Traffic by ISPs

Networking Requirements

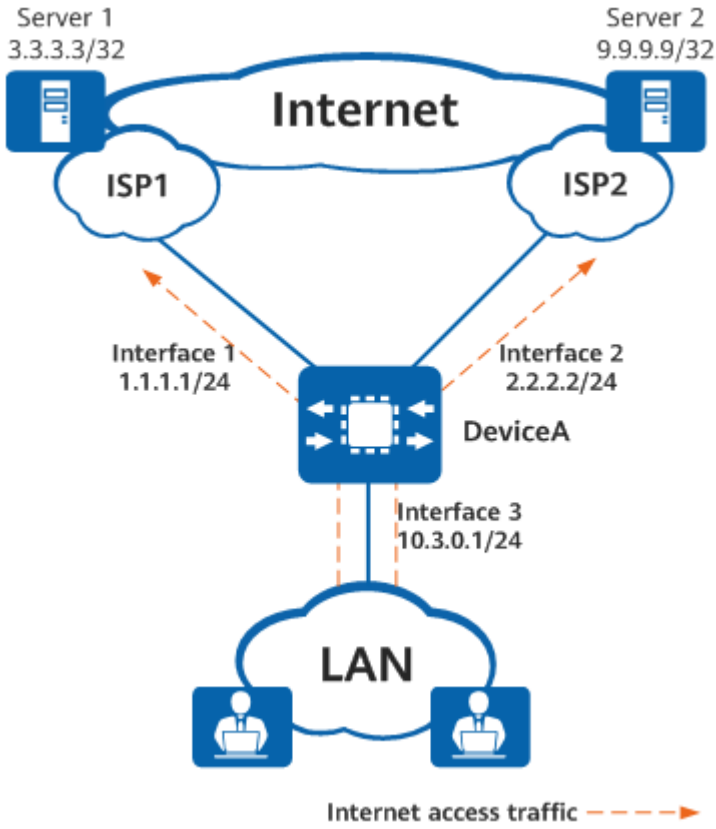
In **Figure 5-1**, DeviceA is deployed at the network egress as the security gateway. The enterprise has two links connected separately to ISP1 and ISP2. The enterprise requires that packets to Server 1 be forwarded on ISP1 link and packets to Server 2 be forwarded on ISP2 link.

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Networking diagram for configuring ISP link selection



Configuration Roadmap

1. Set interface IP addresses and security zones.
2. Create ISP address files **isp1.csv** and **isp2.csv**, write the IP address 3.3.3.3 of Server 1 into **isp1.csv** and the IP address 9.9.9.9 of Server 2 into **isp2.csv** based on the template, and import the two ISP address files to DeviceA.
3. Configure ISP link selection to forward packets destined for Server 1 from ISP1 link and packets destined for Server 2 link from ISP2 link.
4. Configure a basic security policy to allow intranet users to access the Internet.

NOTE

This example focuses on the configuration related to ISP link selection. Configure other data such as NAT based on the actual networking.

Procedure

Step 1 Assign IP addresses to interfaces, and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE0/0/1. Set parameters as follows.

Zone	untrust
Mode	Route

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
Connection Type	Static IP
IP Address	1.1.1.1/255.255.255.0

3. Repeat the previous operation and set interface parameters for GE0/0/2.

Zone	untrust
Mode	Route
IPv4	
Connection Type	Static IP
IP Address	2.2.2.2/255.255.255.0

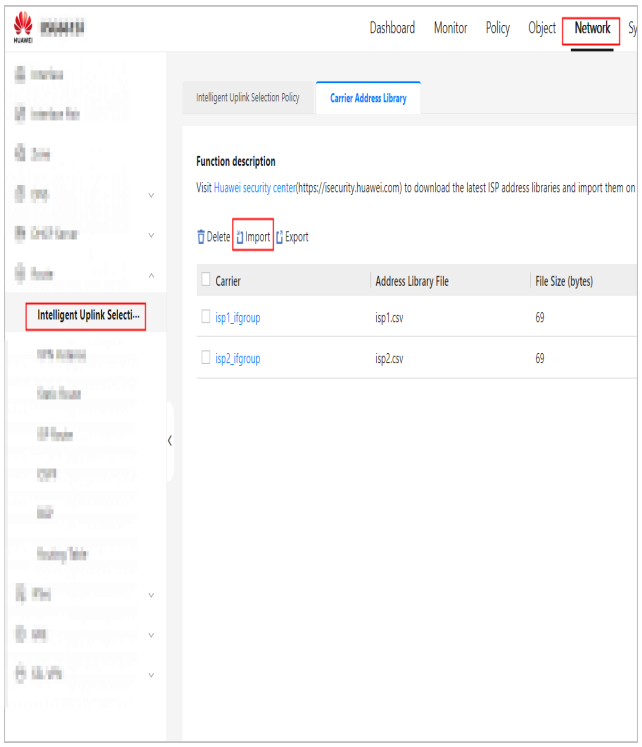
4. Repeat the previous operation and set interface parameters for GE0/0/3.

Zone	trust
Mode	Route
IPv4	
Connection Type	Static IP
IP Address	10.3.0.1/255.255.255.0

Step 2 Create carrier names **isp1_ifgrp** and **isp2_ifgrp** for ISP 1 and ISP 2, respectively, and import the ISP address files.

1. Choose **Network** > **Route** > **Intelligent Uplink Selection**, click the **Carrier Address Library** tab, and click **Import**.

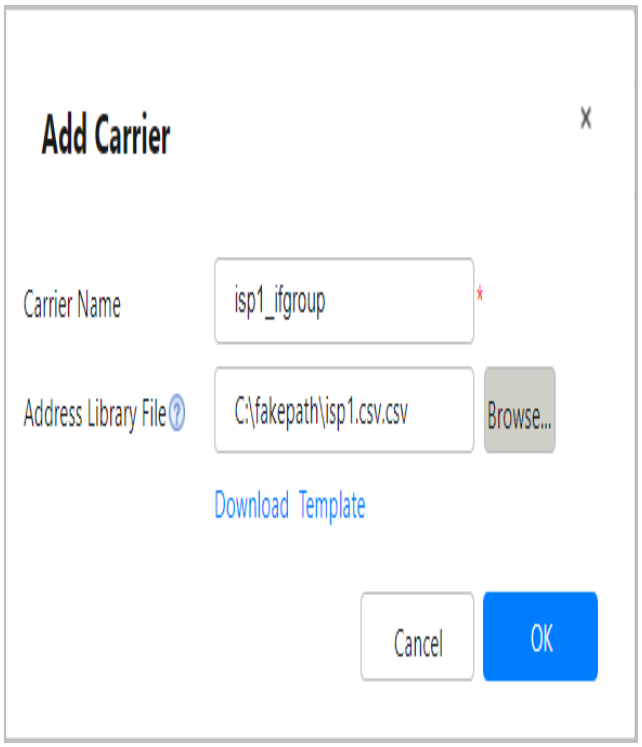
 Copyright © Huawei Technologies Co., Ltd.



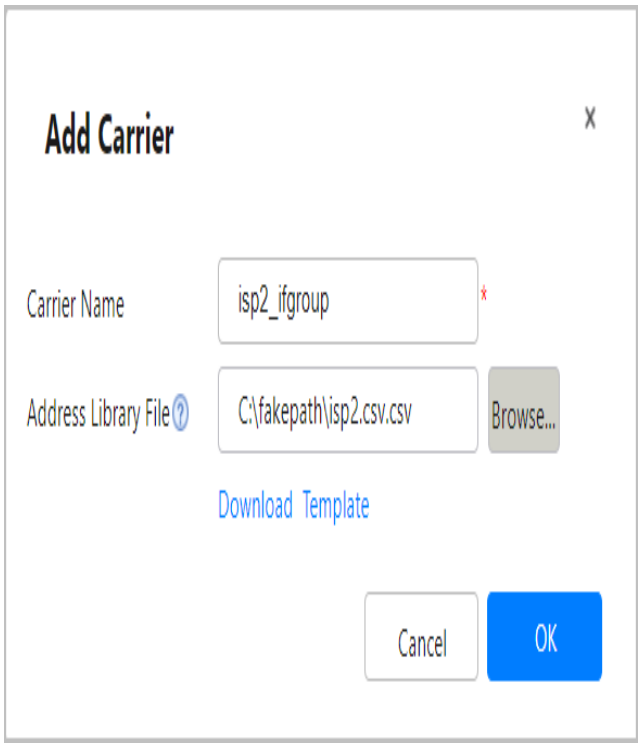
2. Create carrier names **isp1_ifgroup** and **isp2_ifgroup** for ISP 1 and ISP 2, respectively, and import the ISP address files.

   NOTE

   Create ISP address files **isp1.csv** and **isp2.csv**, and write the IP address 3.3.3.3/32 of Server 1 into **isp1.csv** and the IP address 9.9.9.9/32 of Server 2 into **isp2.csv**. You can obtain the ISP address file template from the **Carrier Address Library** tab page in **Network** > **Route** > **Intelligent Uplink Selection**.

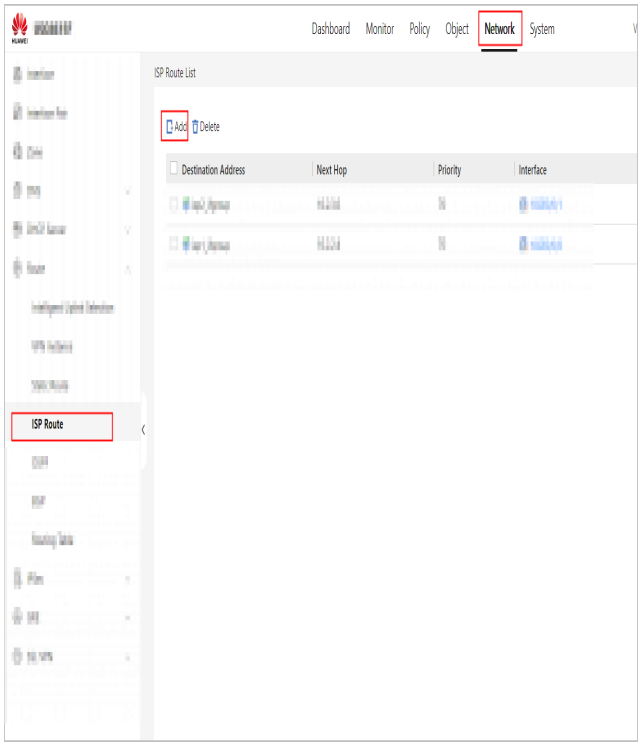


 Copyright © Huawei Technologies Co., Ltd.



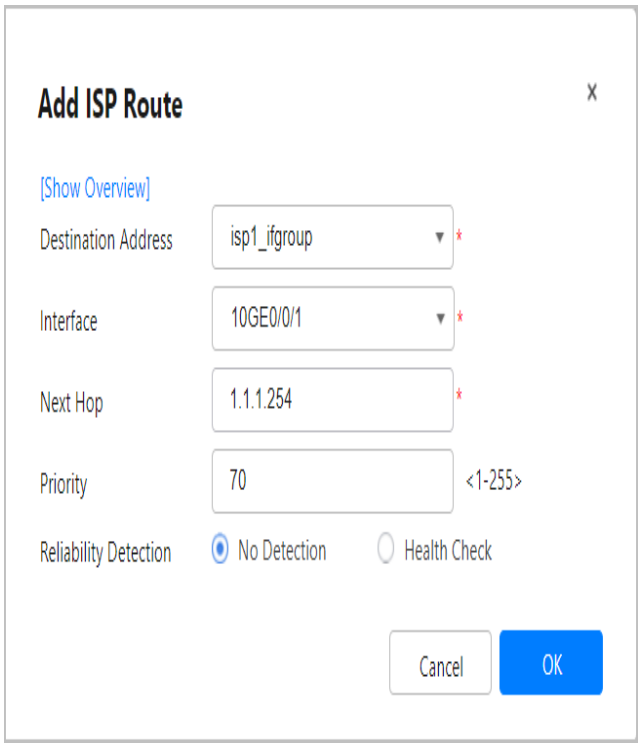
Step 3 Create an ISP route.

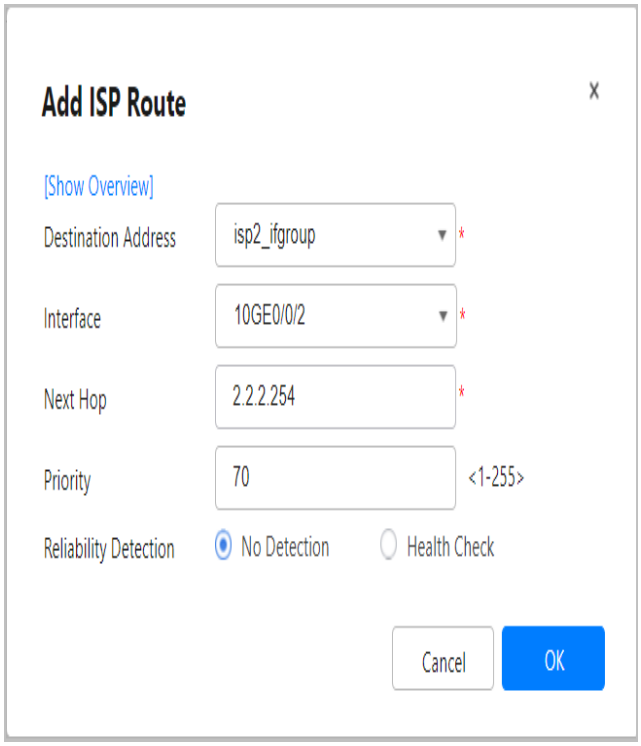
1. Choose **Network** > **Route** > **ISP Route** and click **Add** in **ISP Route List**.



2. Create an ISP route based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.





Step 4 Configure a Trust-to-Untrust interzone security policy to allow enterprise network users to access Internet resources. Assume that enterprise network users reside on 10.3.0.0/24.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	policy_sec_trust_untrust
Source Security Zone	trust
Destination Security Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

----End

Verifying the Configuration

- Run the **display firewall session table verbose destination inside 3.3.3.3** command to verify that the outbound interface of traffic destined for Server 1 is interface 1 (GE 0/0/1).
- Run the **display firewall session table verbose destination inside 9.9.9.9** command to verify that the outbound interface of traffic destined for Server 2 is interface 2 (GE 0/0/2).

Configuration Scripts

```
#
sysname DeviceA
#
 isp name isp1_ifgrp set filename isp1.csv
 isp name isp2_ifgrp set filename isp2.csv
 ip route-isp isp1_ifgrp interface GE0/0/1 nexthop 1.1.1.254
 ip route-isp isp2_ifgrp interface GE0/0/2 nexthop 2.2.2.254
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

5.2 CLI: Example for Configuring ISP Link Selection to Forward Traffic by ISPs

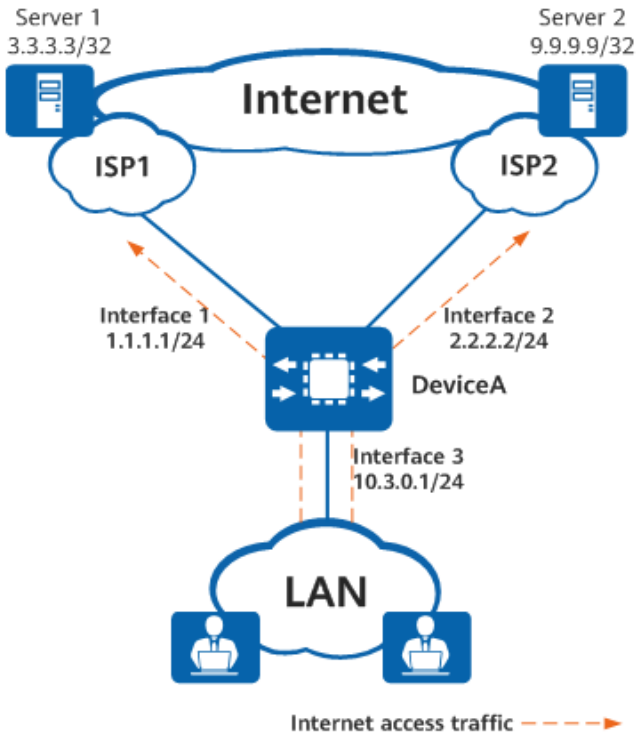
Networking Requirements

As shown in **Figure 5-2**, DeviceA is deployed at the network egress as the security gateway. The enterprise has two links connected respectively to ISP1 and ISP2. The enterprise requires that packets to Server 1 be forwarded on ISP1 link and packets to Server 2 be forwarded on ISP2 link.

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

Figure 5-2 Networking diagram for ISP link selection



Configuration Roadmap

1. Configure IP addresses for the interfaces and add them to security zones.
2. Make ISP address files **isp1.csv** and **isp2.csv**, write Server 1 IP address 3.3.3.3 into **isp1.csv** and Server 2 IP address 9.9.9.9 into **isp2.csv**, and upload the two ISP address files to DeviceA.
3. Configure ISP link selection to forward packets destined for Server 1 from ISP1 link and packets destined for Server 2 link from ISP2 link.
4. Configure a basic security policy to allow intranet users to access Internet resources.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This example focuses on the configuration of ISP link selection. Other configurations, such as NAT, need to be performed based on the actual networking.

Procedure

Step 1 Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 2.2.2.2 255.255.255.0
[DeviceA-GE0/0/2] quit
```

Step 2 Upload ISP address files to DeviceA using SFTP. Details are omitted.

Step 3 Create an ISP named **isp1_ifgrp** for ISP1 and an ISP named **isp2_ifgrp** for ISP2 and associate them with the corresponding ISP address files.

```
[DeviceA] isp name isp1_ifgrp set filename isp1.csv
[DeviceA] isp name isp2_ifgrp set filename isp2.csv
```

Step 4 Create ISP routes.

```
[DeviceA] ip route-isp isp1_ifgrp interface ge 0/0/1 nexthop 1.1.1.254
[DeviceA] ip route-isp isp2_ifgrp interface ge 0/0/2 nexthop 2.2.2.254
```

Step 5 Add interfaces to corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 6 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet. Assume that the intranet users reside on 10.3.0.0/24.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_trust_untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-zone trust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_trust_untrust] action permit
[DeviceA-policy-security-rule-policy_sec_trust_untrust] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

Run the **display firewall session table verbose destination inside 3.3.3.3** command to check whether the outbound interface of traffic destined for Server 1 is interface1 (GE0/0/1). Run the **display firewall session table verbose**

destination inside 9.9.9.9 command to check whether the outbound interface of traffic destined for Server 2 is interface2 (GE0/0/2).

Configuration Scripts

```
#
sysname DeviceA
#
 isp name isp1_ifgrp set filename isp1.csv
 isp name isp2_ifgrp set filename isp2.csv
 ip route-isp isp1_ifgrp interface GE0/0/1 nexthop 1.1.1.254
 ip route-isp isp2_ifgrp interface GE0/0/2 nexthop 2.2.2.254
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

5.3 Configuring PBR and PBR-based Intelligent Uplink Selection

5.3.1 Web: Example for Configuring Protocol-Specific PBR

Networking Requirements

In **Figure 5-3**, DeviceA is deployed at the intranet egress. DeviceA can access the Internet through Router_A of ISP_A or Router_B of ISP_B. ISP_A provides quick and stable Internet services but requires high charge. ISP_B requires low charge but provides slow Internet services.

- Service traffic is sent from interface 1 to the Internet through ISP_A.
- Entertainment traffic is sent from interface 2 to the Internet through ISP_B.

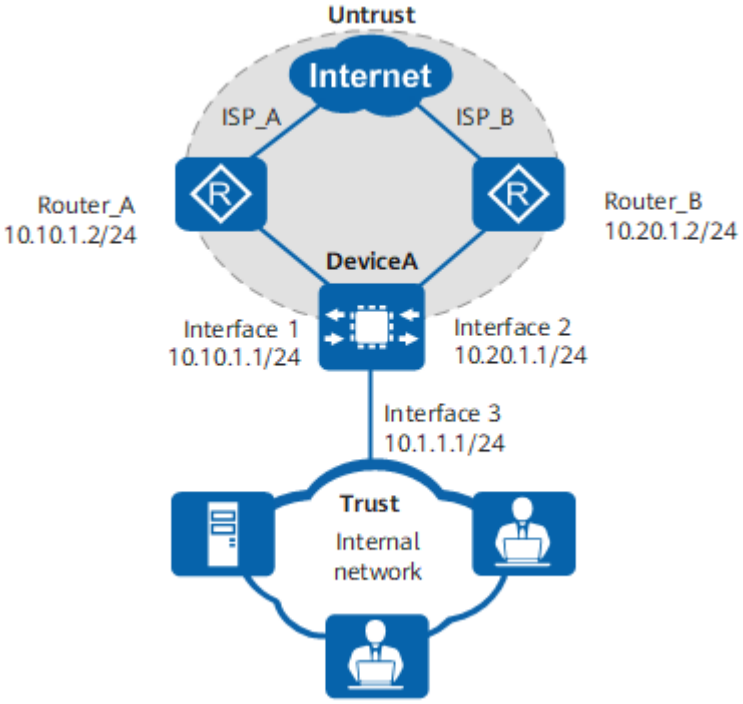
 Copyright © Huawei Technologies Co., Ltd.

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

This example focuses on the configuration related to PBR. Configure other data such as NAT based on the actual networking.

Figure 5-3 Networking diagram of protocol-specific PBR



Procedure

Step 1 Configure interfaces and complete basic network configurations.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE 0/0/1 and set the parameters as follows.

Security Zone	Untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	10.10.1.1/255.255.255.0

3. Repeat the preceding steps to configure GE 0/0/2.

Security Zone	Untrust
Mode	Routing

 Copyright © Huawei Technologies Co., Ltd.

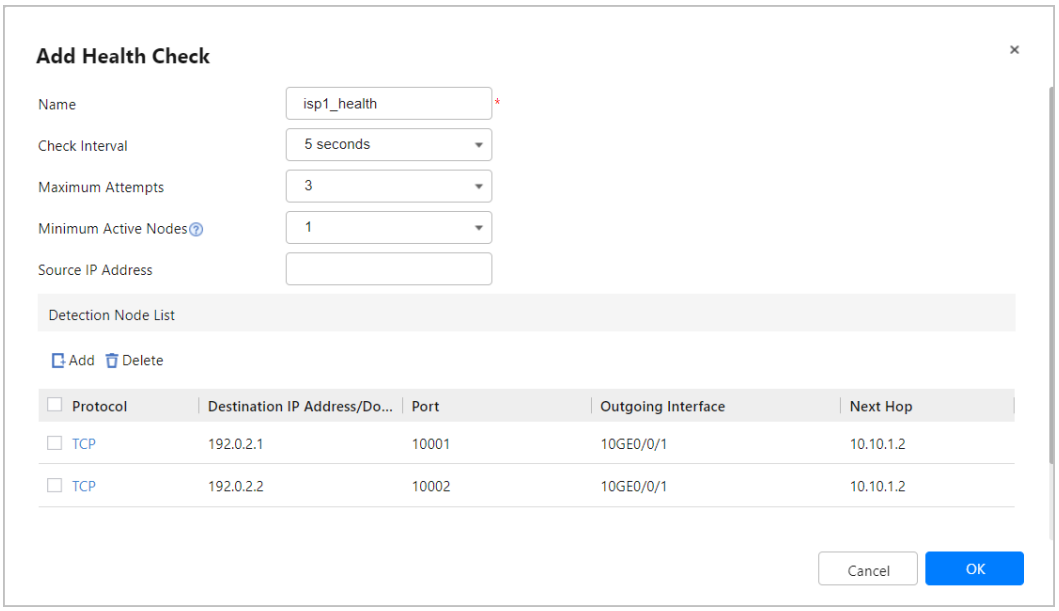
IPv4	
Connection Type	Static IP address
IP Address	10.20.1.1/255.255.255.0

4. Repeat the preceding steps to configure GE 0/0/3.

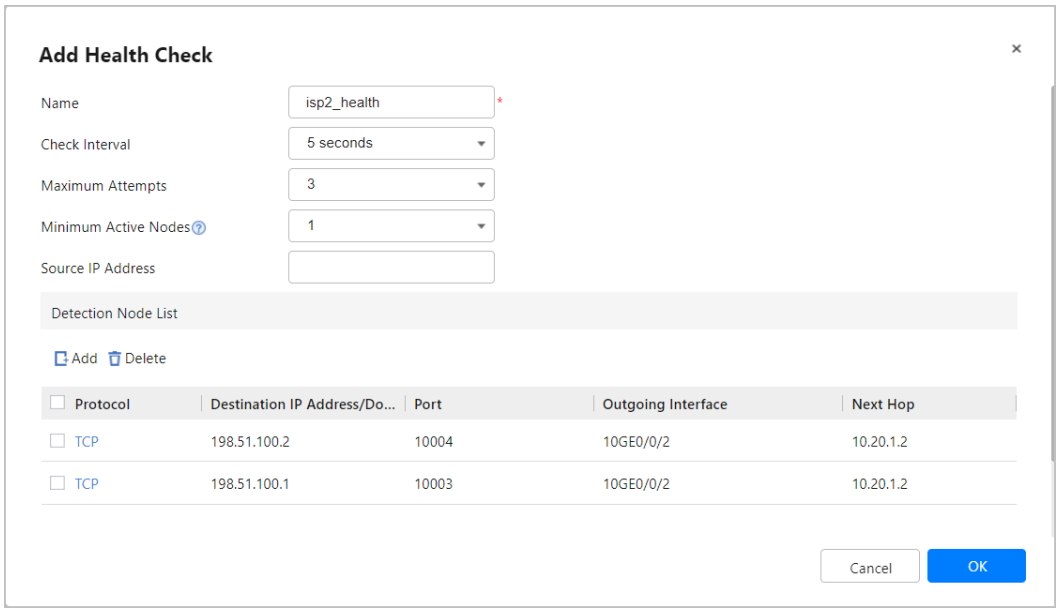
Security Zone	Trust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	10.1.1.1/255.255.255.0

Step 2 Enable the health check function and create a health check for the links to ISP_A and ISP_B respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP_A and is 198.51.100.0/24 for ISP_B.

1. Choose **Object** > **Health Check**.
2. In **Health Check List**, click **Add**.



 Copyright © Huawei Technologies Co., Ltd.



NOTE

Assume that 192.0.2.1 and 192.0.2.2 are known device addresses on the ISP_A network and that 198.51.100.1 and 198.51.100.2 are known device addresses on the ISP_B network.

If the state remains Down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 3 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access Internet resources. Assume that the intranet user network segment is 10.1.1.0/24.

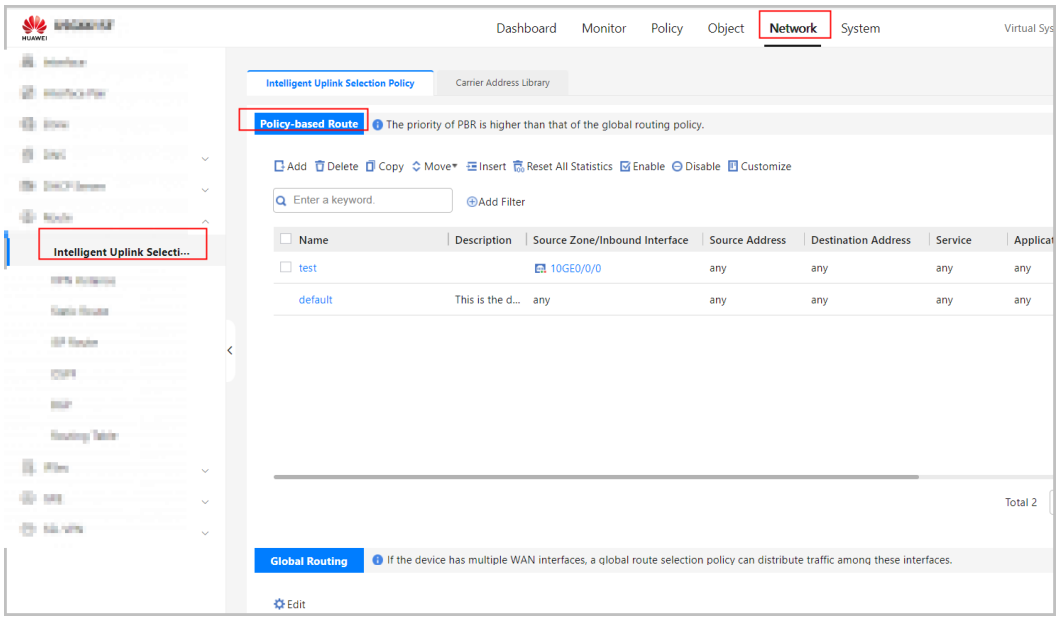
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Parameter	policy_sec_trust_untrust
Source Security Zone	Trust
Destination Security Zone	Untrust
Source Address	10.1.1.0/24
Action	Permit

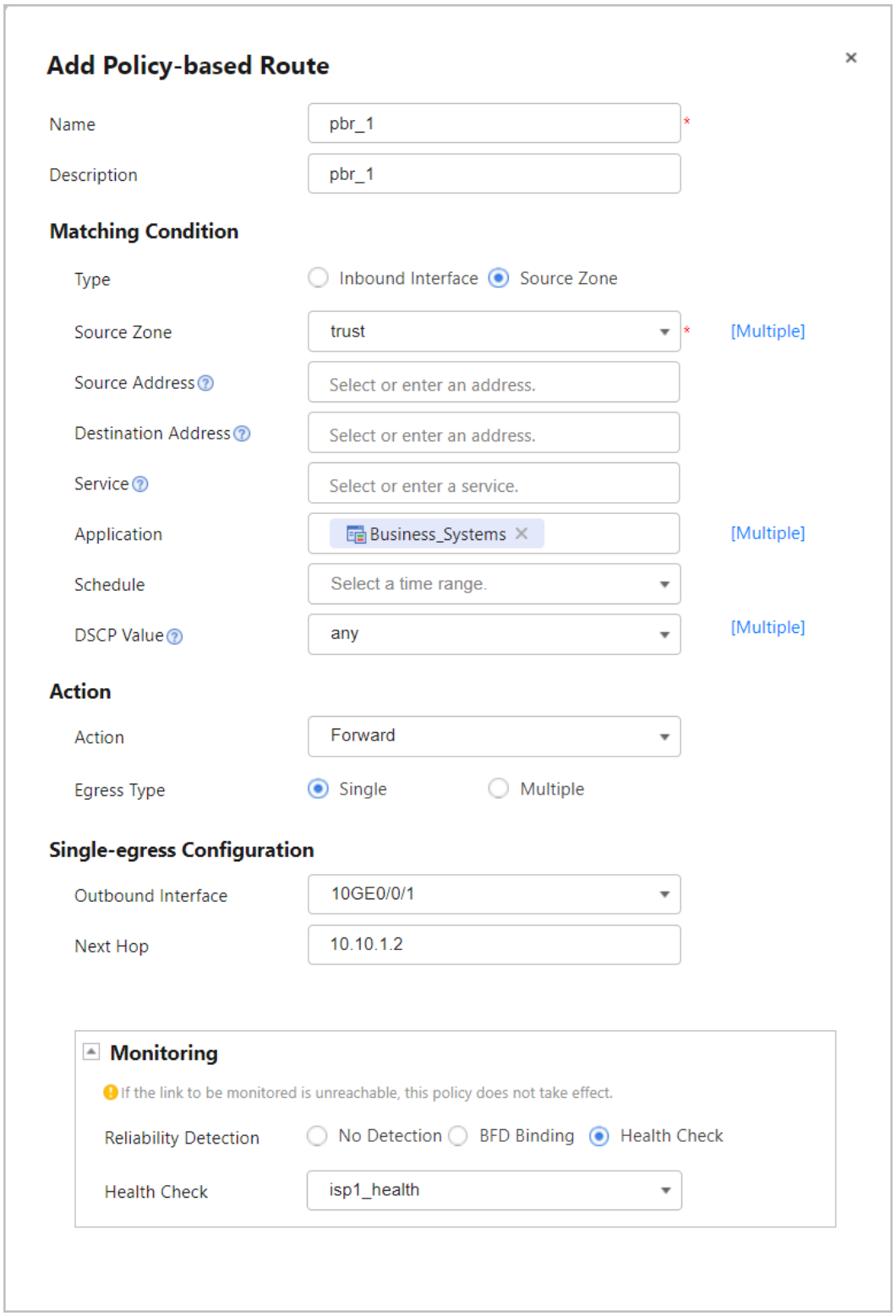
Step 4 Create PBR rule **pbr_1** to allow GE0/0/1 to forward service traffic to the Internet through ISP_A. Create PBR rule **pbr_2** to allow GE0/0/2 to forward entertainment traffic to the Internet through ISP_B.

1. Choose **Network** > **Route** > **Intelligent Uplink Selection**.

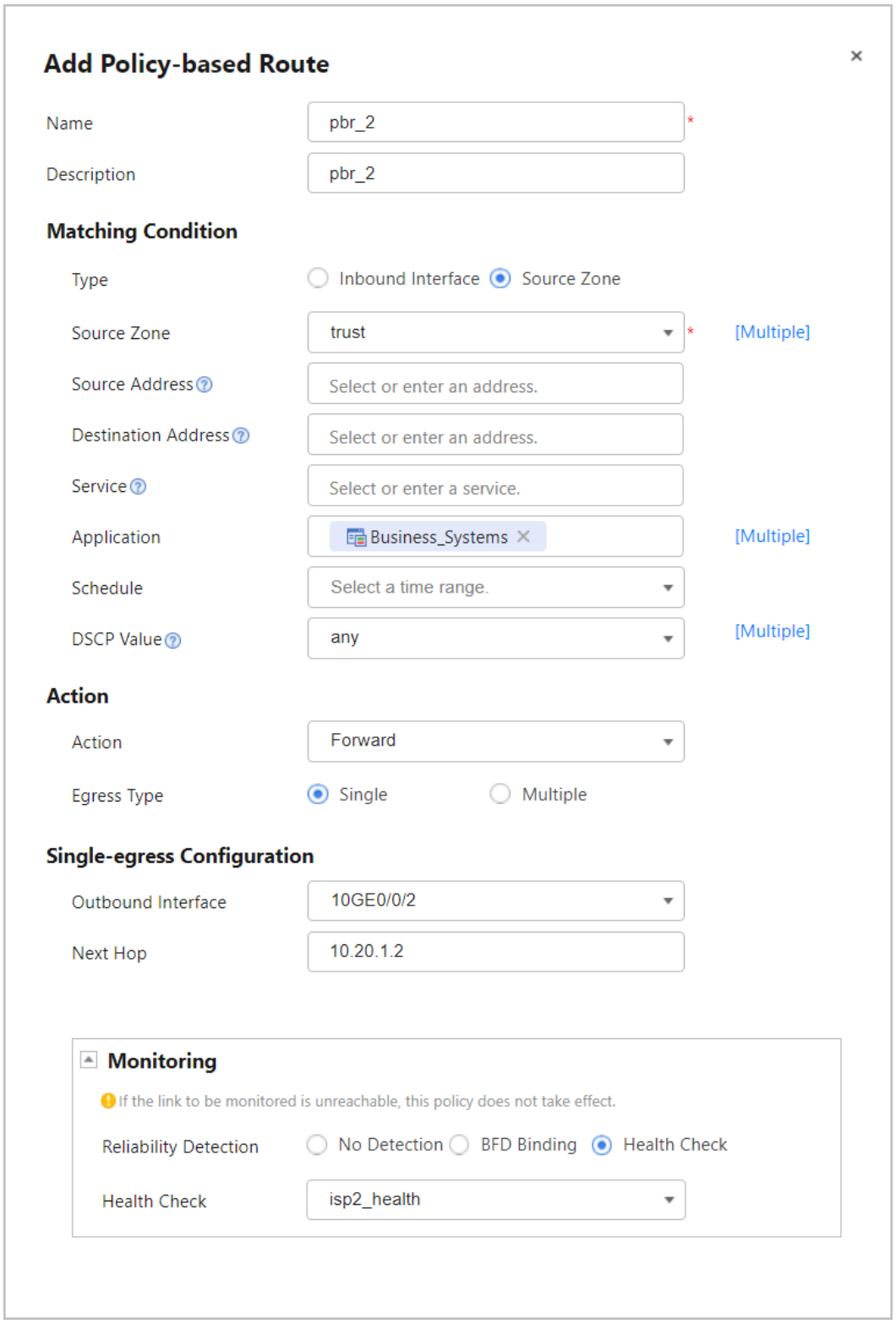
 Copyright © Huawei Technologies Co., Ltd.



2. On the **Intelligent Uplink Selection Policy-Policy-based Route** tab page, click **Create**.



 Copyright © Huawei Technologies Co., Ltd.



NOTE

Ensure that DeviceA has the route configuration that guides service traffic and entertainment traffic transmission even if PBR is unavailable.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

- Run the **display firewall session table verbose application BookMooch** command to verify that the outbound interface of service traffic is interface 1 (GE 0/0/1).
- Run the **display firewall session table verbose application Eyejot** command to verify that the outbound interface of entertainment traffic is interface 2 (GE 0/0/2).

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
#
healthcheck name isp1_health
 destination 192.0.2.1 interface GE0/0/1 next-hop 10.10.1.2 protocol tcp destination-port 10001
 destination 192.0.2.2 interface GE0/0/1 next-hop 10.10.1.2 protocol tcp destination-port 10002
healthcheck name isp2_health
 destination 198.51.100.1 interface GE0/0/2 next-hop 10.20.1.2 protocol tcp destination-port 10003
 destination 198.51.100.2 interface GE0/0/2 next-hop 10.20.1.2 protocol tcp destination-port 10004
#
interface GE0/0/1
 ip address 10.10.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.20.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
  action permit
#
policy-based-route
 rule name pbr_1
  description pbr_1
  source-zone trust
  application category Business_Systems
  track healthcheck isp1_health
  action pbr egress-interface GE0/0/1 next-hop 10.10.1.2
 rule name pbr_2
  description pbr_2
  source-zone trust
  application category Entertainment
  track healthcheck isp2_health
  action pbr egress-interface GE0/0/2 next-hop 10.20.1.2
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

5.3.2 CLI: Example for Configuring Protocol-Specific PBR

Networking Requirements

In Figure 5-4, DeviceA is deployed at the intranet egress. DeviceA can access the Internet through Router_A of ISP-A or Router_B of ISP-B. ISP-A provides quick and stable Internet services but requires high charge. ISP-B requires low charge but provides slow Internet services.

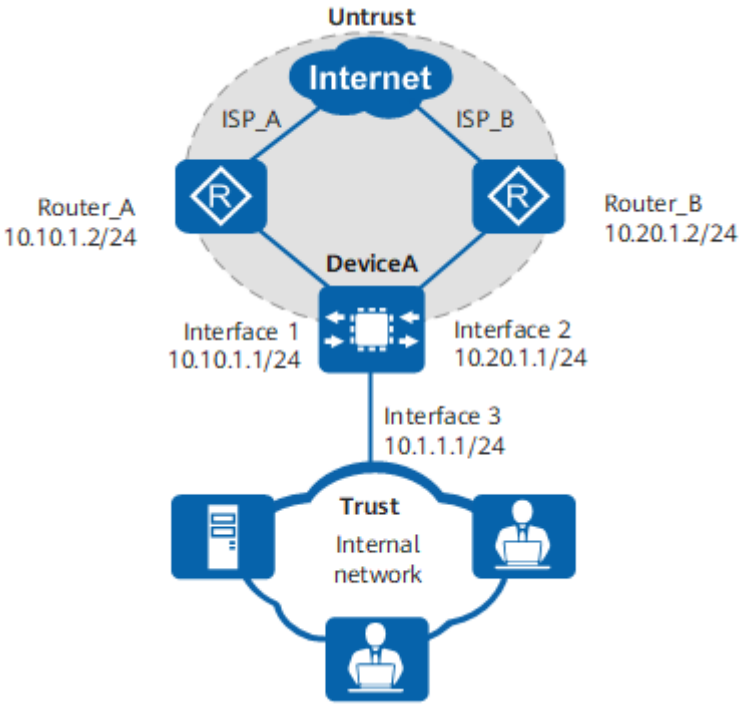
- Service traffic is sent from interface1 to the Internet through ISP-A.
- Entertainment traffic is sent from interface2 to the Internet through ISP-B.

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

This example focuses on the configuration related to PBR. Other configurations, such as NAT, need to be performed based on the actual networking.

Figure 5-4 Networking diagram of protocol-specific PBR



Procedure

Step 1 Set an IP address for each interface and assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.10.1.1 255.255.255.0
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.1.1.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.20.1.1 255.255.255.0
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Enable the health check function and create health check tasks for ISP-A and ISP-B links, respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP-A and 198.51.100.0/24 for ISP-B.

```
[DeviceA] healthcheck enable
[DeviceA] healthcheck name isp1_health
[DeviceA-healthcheck-isp1_health] destination 192.0.2.1 interface ge 0/0/1 next-hop 10.10.1.2 protocol tcp destination-port 10001
[DeviceA-healthcheck-isp1_health] quit
[DeviceA] healthcheck name isp2_health
[DeviceA-healthcheck-isp2_health] destination 198.51.100.1 interface ge 0/0/2 next-hop 10.20.1.2 protocol tcp destination-port 10003
[DeviceA-healthcheck-isp1_health] quit
```

NOTE

To check different IP addresses of the same interface, you can configure multiple health checks and reference them in different PBR rules.

Assume that 192.0.2.1 and 198.51.100.1 are known device addresses on the ISP-A network and ISP-B network, respectively.

If the state remains down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 3 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet. Assume that intranet users reside on 10.1.1.0/24.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_trust_untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-zone trust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy_sec_trust_untrust] action permit
[DeviceA-policy-security-rule-policy_sec_trust_untrust] quit
[DeviceA-policy-security] quit
```

Step 4 Create PBR rule **pbr_1** to allow GE0/0/1 to forward service traffic to the Internet through ISP-A. Create PBR rule **pbr_2** to allow GE0/0/2 to forward entertainment traffic to the Internet through ISP-B.

NOTE

Ensure that DeviceA has the route configuration that guides service traffic and entertainment traffic transmission even if PBR is unavailable.

```
[DeviceA] policy-based-route
[DeviceA-policy-pbr] rule name pbr_1
[DeviceA-policy-pbr-rule-pbr_1] description pbr_1
[DeviceA-policy-pbr-rule-pbr_1] source-zone trust
[DeviceA-policy-pbr-rule-pbr_1] application category Business_Systems
[DeviceA-policy-pbr-rule-pbr_1] track healthcheck isp1_health
[DeviceA-policy-pbr-rule-pbr_1] action pbr egress-interface ge 0/0/1 next-hop 10.10.1.2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-pbr-rule-pbr_1] quit
[DeviceA-policy-pbr] rule name pbr_2
[DeviceA-policy-pbr-rule-pbr_2] description pbr_2
[DeviceA-policy-pbr-rule-pbr_2] source-zone trust
[DeviceA-policy-pbr-rule-pbr_2] application category Entertainment
[DeviceA-policy-pbr-rule-pbr_2] track healthcheck isp2_health
[DeviceA-policy-pbr-rule-pbr_2] action pbr egress-interface ge 0/0/2 next-hop 10.20.1.2
[DeviceA-policy-pbr-rule-pbr_2] quit
```

----End

Verifying the Configuration

- Run the **display firewall session table verbose application BookMooch** command to verify that the outbound interface of service traffic is interface1 (GE0/0/1).
- Run the **display firewall session table verbose application Eyejot** command to verify that the outbound interface of entertainment traffic is interface2 (GE0/0/2).

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
healthcheck name isp1_health
 destination 192.0.2.1 interface GE0/0/1 next-hop 10.10.1.2 protocol tcp destination-port 10001
healthcheck name isp2_health
 destination 198.51.100.1 interface GE0/0/2 next-hop 10.20.1.2 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 10.10.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.20.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
  action permit
#
policy-based-route
 rule name pbr_1
  description pbr_1
  source-zone trust
  application category Business_Systems
  track healthcheck isp1_health
  action pbr egress-interface GE0/0/1 next-hop 10.10.1.2
 rule name pbr_2
  description pbr_2
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 application category Entertainment
 track healthcheck isp2_health
 action pbr egress-interface GE0/0/2 next-hop 10.20.1.2
#
return
```

5.3.3 CLI: Example for Configuring Link Selection Based on Multi-Egress PBR Among Multiple ISP Outbound Interfaces

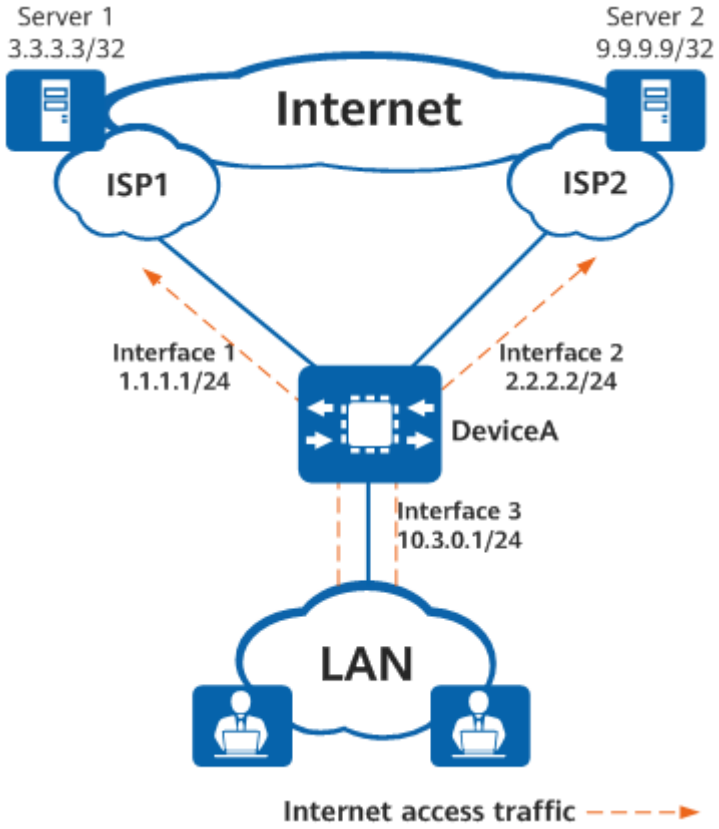
Networking Requirements

As shown in **Figure 5-5**, DeviceA is deployed at the network egress as the security gateway. The enterprise has two 50M links connected respectively to ISP1 and ISP2. The enterprise requires that packets to Server 1 be forwarded on ISP1 link and packets to Server 2 be forwarded on ISP2 link.

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

Figure 5-5 Networking diagram of multi-egress PBR link selection based on ISP destination addresses



Configuration Roadmap

After you configure ISP link selection and PBR-based intelligent uplink selection, DeviceA will select an outbound interface based on the ISP network of the packet

 Copyright © Huawei Technologies Co., Ltd.

destination address to forward traffic. The intelligent uplink selection mode is set to active/standby backup based on link priority. DeviceA needs to create a PBR for each of the two ISP networks. In the PBR to ISP1 network, the destination address matching condition is an ISP1 address set, and ISP1 link has higher priority than ISP2 link. In the PBR to ISP2 network, the destination address matching condition is an ISP2 address set, and ISP2 link has higher priority than ISP1 link.

1. Set IP addresses, security zones, gateway addresses, and bandwidth for interfaces.
2. Make ISP address files **isp1.csv** and **isp2.csv**, write Server 1 IP address 3.3.3.3 into **isp1.csv** and Server 2 IP address 9.9.9.9 into **isp2.csv**, and upload the two ISP address files to DeviceA.
3. Create ISPs for ISP1 and ISP2 respectively and associate them with their address files.
4. Configure PBR-based intelligent uplink selection and create a PBR for each of ISP1 and ISP2 networks.
5. Configure a basic security policy to allow intranet users to access Internet resources.

NOTE

This example focuses on the configuration of ISP link selection. Other configurations, such as NAT, need to be performed based on the actual networking.

Procedure

Step 1 Configure IP addresses and gateway addresses for interfaces, and configure the bandwidths of the links where the interfaces reside.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] bandwidth ingress 50000
[DeviceA-GE0/0/1] bandwidth egress 50000
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 2.2.2.2 255.255.255.0
[DeviceA-GE0/0/2] gateway 2.2.2.254
[DeviceA-GE0/0/2] bandwidth ingress 50000
[DeviceA-GE0/0/2] bandwidth egress 50000
[DeviceA-GE0/0/2] quit
```

Step 2 Upload ISP address files to DeviceA using SFTP. Details are omitted.

Step 3 Create an ISP named **isp1_ifgrp** for ISP1 and an ISP named **isp2_ifgrp** for ISP2 and associate them with the corresponding ISP address files.

```
[DeviceA] isp name isp1_ifgrp set filename isp1.csv
[DeviceA] isp name isp2_ifgrp set filename isp2.csv
```

Step 4 Add interfaces to corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 5 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet. Assume that the intranet users reside on 10.3.0.0/24.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_trust_untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-zone trust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_trust_untrust] action permit
[DeviceA-policy-security-rule-policy_sec_trust_untrust] quit
[DeviceA-policy-security] quit
```

Step 6 Configure PBR-based intelligent uplink selection for ISP1 and set the destination address to the ISP address of ISP1 so that packets destined for Server 1 will be forwarded over ISP1 link.

Select interface1 as the outbound interface and set its priority to 2. Set the priority of interface2 to 1.

```
[DeviceA] policy-based-route
[DeviceA-policy-pbr] rule name isp1_pbr
[DeviceA-policy-pbr-rule-isp1_pbr] ingress-interface ge 0/0/3
[DeviceA-policy-pbr-rule-isp1_pbr] destination-address isp isp1_ifgrp
[DeviceA-policy-pbr-rule-isp1_pbr] action pbr egress-interface multi-interface
[DeviceA-policy-pbr-rule-isp1_pbr-multi-inter] mode priority-of-userdefine
[DeviceA-policy-pbr-rule-isp1_pbr-multi-inter] add interface ge 0/0/1 priority 2
[DeviceA-policy-pbr-rule-isp1_pbr-multi-inter] add interface ge 0/0/2
[DeviceA-policy-pbr-rule-isp1_pbr-multi-inter] quit
[DeviceA-policy-pbr-rule-isp1_pbr] quit
```

Step 7 Configure PBR-based intelligent uplink selection for ISP2 and set the destination address to the ISP address of ISP2 so that packets destined for Server 2 will be forwarded over ISP2 link.

Select interface2 as the outbound interface and set its priority to 2. Set the priority of interface1 to 1.

```
[DeviceA-policy-pbr] rule name isp2_pbr
[DeviceA-policy-pbr-rule-isp2_pbr] ingress-interface ge 0/0/3
[DeviceA-policy-pbr-rule-isp2_pbr] destination-address isp isp2_ifgrp
[DeviceA-policy-pbr-rule-isp2_pbr] action pbr egress-interface multi-interface
[DeviceA-policy-pbr-rule-isp2_pbr-multi-inter] mode priority-of-userdefine
[DeviceA-policy-pbr-rule-isp2_pbr-multi-inter] add interface ge 0/0/2 priority 2
[DeviceA-policy-pbr-rule-isp2_pbr-multi-inter] add interface ge 0/0/1
[DeviceA-policy-pbr-rule-isp2_pbr-multi-inter] quit
[DeviceA-policy-pbr-rule-isp2_pbr] quit
```

----End

Verifying the Configuration

Run the **display firewall session table verbose destination inside 3.3.3.3** command to check whether the outbound interface of traffic destined for Server 1 is interface1 (GE0/0/1). Run the **display firewall session table verbose destination inside 9.9.9.9** command to check whether the outbound interface of traffic destined for Server 2 is interface2 (GE0/0/2).

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
sysname DeviceA
#
 isp name isp1_ifgrp set filename isp1.csv
 isp name isp2_ifgrp set filename isp2.csv
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
policy-based-route
 rule name isp1_pbr
  ingress-interface GE0/0/3
  destination-address isp isp1_ifgrp
  action pbr egress-interface multi-interface
   mode priority-of-userdefine
   add interface GE0/0/1 priority 2
   add interface GE0/0/2
 rule name isp2_pbr
  ingress-interface GE0/0/3
  destination-address isp isp2_ifgrp
  action pbr egress-interface multi-interface
   mode priority-of-userdefine
   add interface GE0/0/2 priority 2
   add interface GE0/0/1
#
return
```

5.3.4 CLI: Example for Configuring Policy-based Routes for Internet Access from Multiple ISPs

Networking Requirements

In **Figure 5-6**, a college connects to the Internet through an education network. The college also purchases broadband services from an ISP and connects to the Internet through the ISP network.

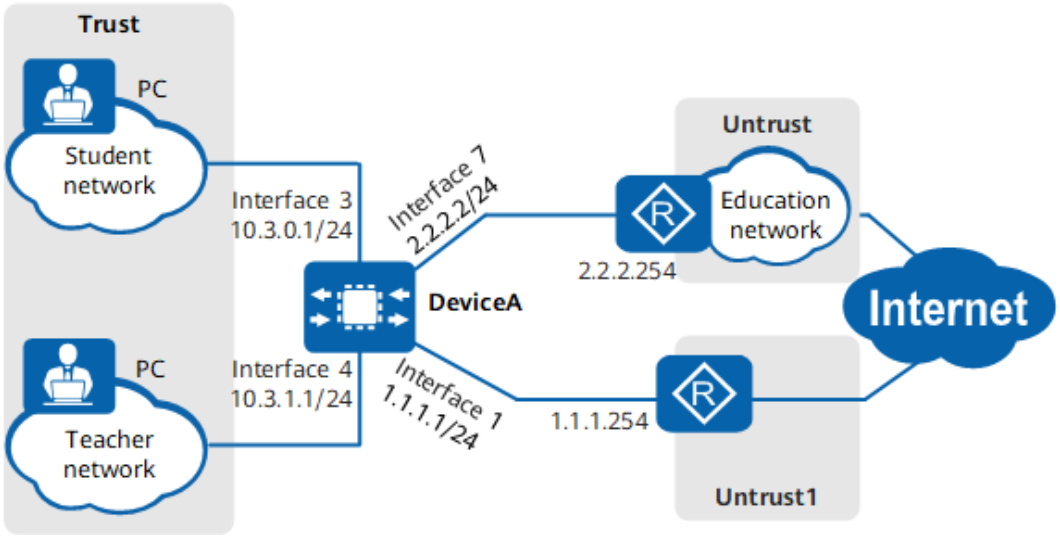
 Copyright © Huawei Technologies Co., Ltd.

PCs on the student network can access the Internet only through the education network, and PCs on the teacher network can access the Internet only through the ISP network.

NOTE

In this example, interface 1, interface 3, interface 4, and interface 7 represent GE 0/0/1, GE 0/0/3, GE 0/0/4, and GE 0/0/7, respectively.

Figure 5-6 Configuring policy-based routes for Internet access from multiple ISPs



Configuration Roadmap

1. Set the IP addresses of interfaces and add the interfaces to security zones.
2. Configure policy-based routes to enable PCs on the student network to access the Internet through interface 7 over the education network, and enable PCs on the teacher network to access the Internet through interface 1.
3. Configure security policies to allow PCs on the student network and teacher network to access the Internet.
4. Configure NAT policies for source address translation.

Procedure

Step 1 Set an IP address for each interface, assign interfaces to security zones, and complete basic parameter settings.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/4
[DeviceA-GE0/0/4] ip address 10.3.1.1 255.255.255.0
[DeviceA-GE0/0/4] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 255.255.255.0
```

```
[DeviceA-GE0/0/7] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] add interface ge 0/0/4
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/7
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone name untrust1
[DeviceA-zone-untrust1] set priority 10
[DeviceA-zone-untrust1] add interface ge 0/0/1
[DeviceA-zone-untrust1] quit
```

Step 2 Configure policy-based routes.

Configure a policy-based route to allow PCs on the student network to access the Internet through interface 7.

```
[DeviceA] policy-based-route
[DeviceA-policy-pbr] rule name policy_route_1
[DeviceA-policy-pbr-rule-policy_route_1] ingress-interface ge 0/0/3
[DeviceA-policy-pbr-rule-policy_route_1] source-address 10.3.0.0 24
[DeviceA-policy-pbr-rule-policy_route_1] action pbr egress-interface ge 0/0/7 next-hop 2.2.2.254
[DeviceA-policy-pbr-rule-policy_route_1] quit
```

Configure a policy-based route to allow PCs on the teacher network to access the Internet through interface 1.

```
[DeviceA-policy-pbr] rule name policy_route_2
[DeviceA-policy-pbr-rule-policy_route_2] ingress-interface ge 0/0/4
[DeviceA-policy-pbr-rule-policy_route_2] source-address 10.3.1.0 24
[DeviceA-policy-pbr-rule-policy_route_2] action pbr egress-interface ge 0/0/1 next-hop 1.1.1.254
[DeviceA-policy-pbr-rule-policy_route_2] quit
[DeviceA-policy-pbr] quit
```

Step 3 Configure security policies.

Configure a security policy to allow PCs on the student network to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
```

Configure a security policy to allow PCs on the teacher network to access the Internet.

```
[DeviceA-policy-security] rule name policy_sec_2
[DeviceA-policy-security-rule-policy_sec_2] source-zone trust
[DeviceA-policy-security-rule-policy_sec_2] destination-zone untrust1
[DeviceA-policy-security-rule-policy_sec_2] source-address 10.3.1.0 24
[DeviceA-policy-security-rule-policy_sec_2] action permit
[DeviceA-policy-security-rule-policy_sec_2] quit
[DeviceA-policy-security] quit
```

Step 4 Configure a NAT policy to translate addresses when PCs on the student network access the Internet.

Configure an address pool.

```
[DeviceA] nat address-group address_1
[DeviceA-address-group-address_1] section 0 2.2.2.10 2.2.2.15
[DeviceA-address-group-address_1] quit
```

Configure a NAT policy.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat_1
[DeviceA-policy-nat-rule-policy_nat_1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat_1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat_1] source-address 10.3.0.0 24
[DeviceA-policy-nat-rule-policy_nat_1] action source-nat address-group address_1
[DeviceA-policy-nat-rule-policy_nat_1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a NAT policy to translate addresses when PCs on the teacher network access the Internet.

Configure an address pool.

```
[DeviceA] nat address-group address_2
[DeviceA-address-group-address_2] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-address_2] quit
```

Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat_2
[DeviceA-policy-nat-rule-policy_nat_2] source-zone trust
[DeviceA-policy-nat-rule-policy_nat_2] destination-zone untrust1
[DeviceA-policy-nat-rule-policy_nat_2] source-address 10.3.1.0 24
[DeviceA-policy-nat-rule-policy_nat_2] action source-nat address-group address_2
[DeviceA-policy-nat-rule-policy_nat_2] quit
[DeviceA-policy-nat] quit
```

----End

Verifying the Configuration

Run the **display firewall session table verbose source inside 10.3.0.0** command to verify that the outbound interface of traffic from the student network is interface 7 (10GE 0/0/7). Run the **display firewall session table verbose source inside 10.3.1.0** command to verify that the outbound interface of traffic from the R&D department is interface 4 (10GE 0/0/4).

Configuration Scripts

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/4
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/7
#
firewall zone name untrust1
 set priority 10
 add interface GE0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 nat address-group address_1
  mode pat
  section 0 2.2.2.10 2.2.2.15
 nat address-group address_2
  mode pat
  section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.3.0.0 24
    action permit
  rule name policy_sec_2
    source-zone trust
    destination-zone untrust1
    source-address 10.3.1.0 24
    action permit
#
policy-based-route
  rule name policy_route_1
    ingress-interface GE0/0/3
    source-address 10.3.0.0 24
    action pbr egress-interface GE0/0/7 next-hop 2.2.2.254
  rule name policy_route_2
    ingress-interface GE0/0/4
    source-address 10.3.1.0 24
    action pbr egress-interface GE0/0/1 next-hop 1.1.1.254
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 10.3.0.0 255.255.255.0
    action source-nat address-group address_1
  rule name policy_nat_2
    source-zone trust
    destination-zone untrust1
    source-address 10.3.1.0 255.255.255.0
    action source-nat address-group address_2
#
return
```

5.4 Configuring Equal Cost Route-based Intelligent Uplink Selection

5.4.1 Web: Example for Configuring Load Balancing Based on Link Bandwidth

Networking Requirements

As shown in **Figure 5-7**, an enterprise has a 100M link connected to ISP1 and a 50M link connected to ISP2.

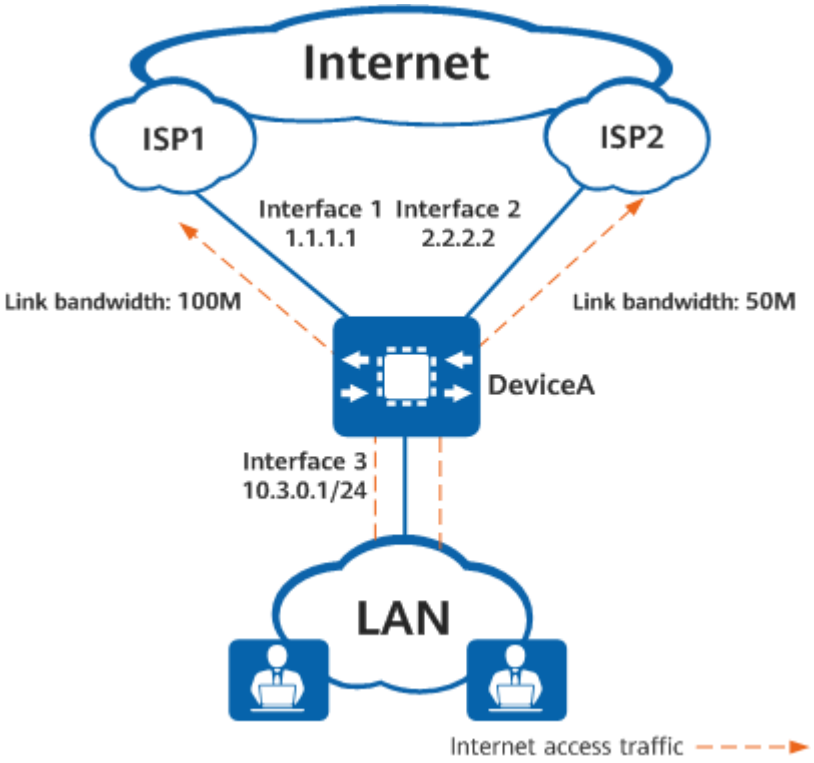
- The enterprise requires that traffic be forwarded to ISP1 and ISP2 links based on the bandwidth ratio to ensure that bandwidth resources are used to the greatest extent.
- When one ISP link is down, follow-up traffic will be forwarded on the other ISP link to ensure access availability.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

Figure 5-7 Networking diagram of load balancing based on link bandwidth



Configuration Roadmap

The enterprise requires traffic distribution based on the bandwidth ratio. Therefore, set the intelligent uplink selection mode to load balancing based on link bandwidth. To ensure that DeviceA can use other links to forward traffic when a link is faulty, you need to configure health check function.

1. Set interface IP addresses, security zones, gateway addresses, bandwidth.
2. **Optional:** Configure the health check function, and configure a health check task for ISP1 and ISP2, respectively.
3. Configure a global route selection policy. Set the intelligent uplink selection mode to load balancing based on link bandwidth, configure the outbound interfaces on DeviceA connecting to ISP1 and ISP2 networks as intelligent uplink selection member interfaces, and reference health check.
4. Configure a basic security policy to allow intranet users to access the Internet.

NOTE

This example focuses on the configuration related to intelligent uplink selection. Configure other data such as NAT based on the actual networking.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set IP addresses for interfaces on the firewall and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE 0/0/1 and set the parameters as follows.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	1.1.1.1/255.255.255.0
Default Gateway	1.1.1.254
Inbound Bandwidth	100 Mbit/s
Outbound Bandwidth	100 Mbit/s

3. Repeat the preceding steps to set the parameters for GE 0/0/2.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	2.2.2.2/255.255.255.0
Default Gateway	2.2.2.254
Inbound Bandwidth	50 Mbit/s
Outbound Bandwidth	50 Mbit/s

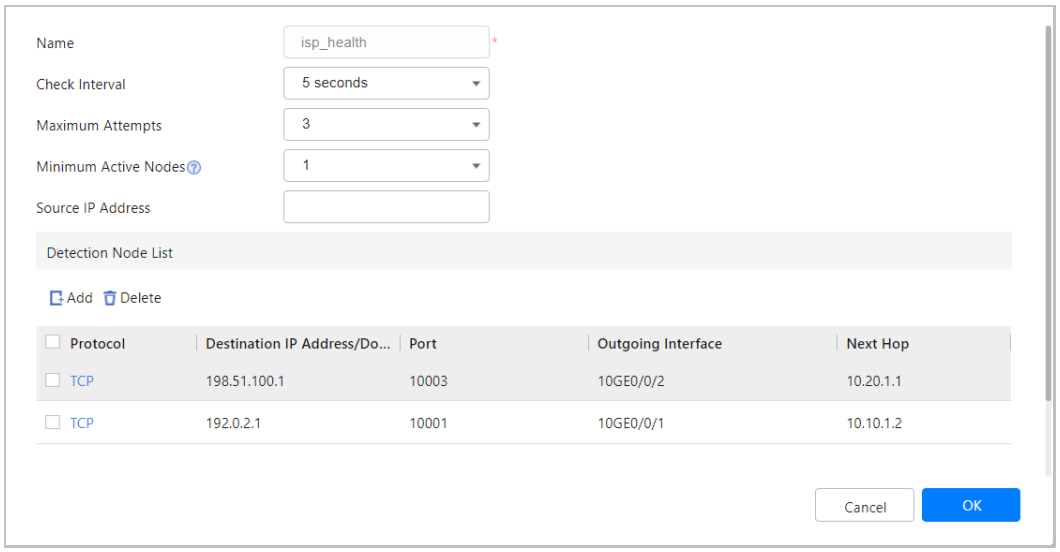
4. Repeat the preceding steps to set the parameters for GE 0/0/3.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	10.3.0.1/255.255.255.0

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Enable the health check function and create a health check for ISP1 and ISP2 link respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP1 and is 198.51.100.0/24 for ISP2.

1. Choose **Object** > **Health Check**.
2. In **Health Check List**, click **Create**.



NOTE

Assume that 192.0.2.1 and 198.51.100.1 are known device addresses on the ISP1 network and ISP2 network, respectively.

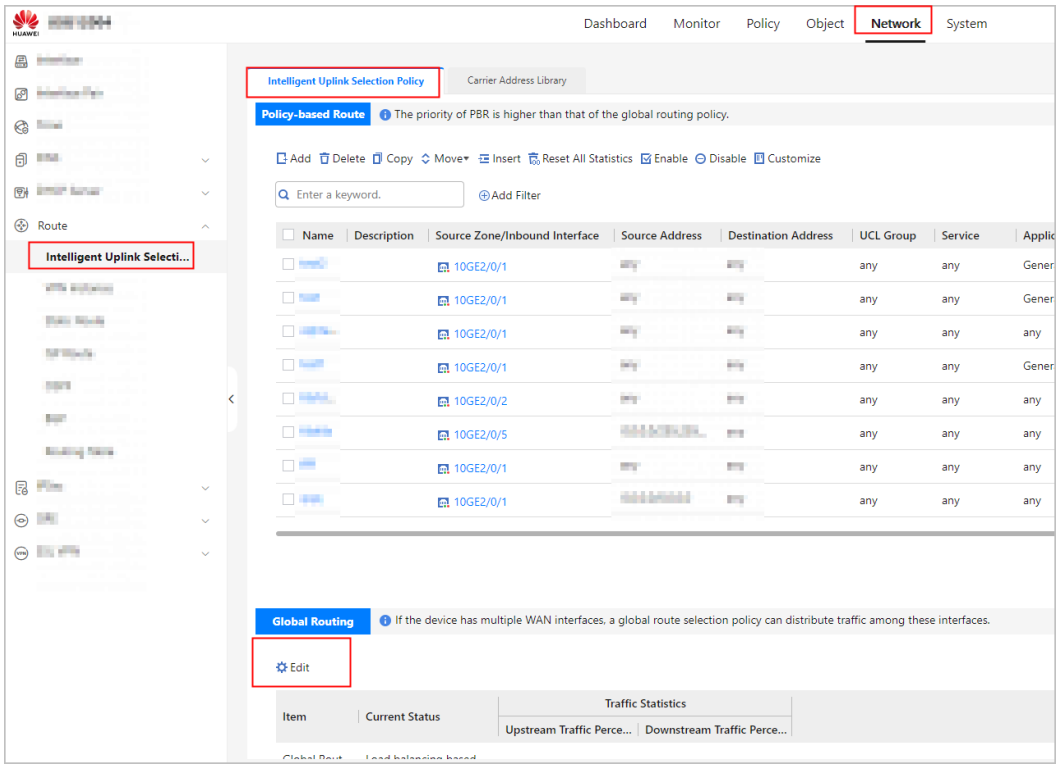
If the state remains Down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 3 Configure a global route selection policy to load balance traffic by link bandwidth and reference the health check.

1. Choose **Network** > **Route** > **Intelligent Uplink Selection**. On the **Intelligent Uplink Selection Policy** tab page, click **Edit** in **Global Routing Policy**.

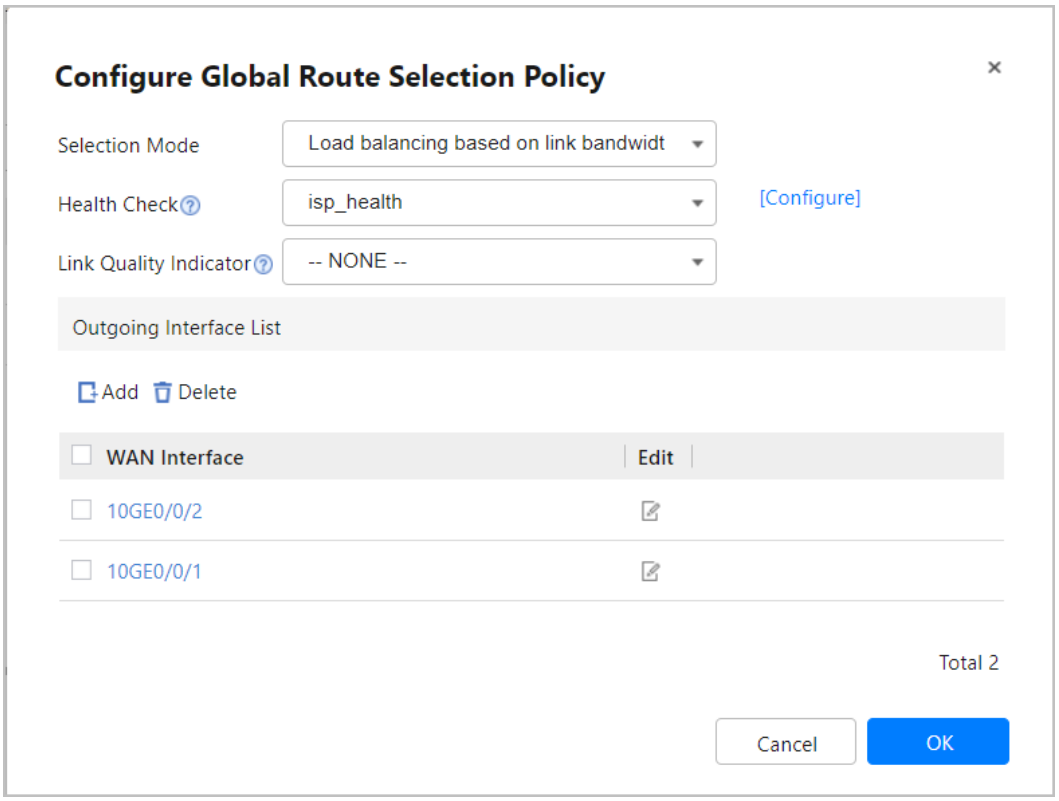
 Copyright © Huawei Technologies Co., Ltd.



NOTE

In multi-egress intelligent uplink selection, the availability of each link is determined based on each detection node in the health check instead of the status of the health check object.

2. Configure a global route selection policy.



Step 4 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access Internet resources. Assume that the intranet user network segment is 10.3.0.0/24.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Parameter	policy_sec_trust_untrust
Source Security Zone	trust
Destination Security Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

----End

Verifying the Configuration

- After the network has been running for a period of time, run the **display interface brief** command on interface 1 (GE 0/0/1) and interface 2 (GE 0/0/2) to check the average bandwidth usage (**OutUti** field) in the outbound direction within the last 300s and verify that the **OutUti** ratio (that is, the link bandwidth ratio) of the two interfaces is close to 2:1.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display firewall session table interface ge 0/0/1** and **display firewall session table interface ge 0/0/2** commands to check the number of sessions on the two interfaces and verify that the ratio is close to 2:1.

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
#
healthcheck name isp_health
 destination 192.0.2.1 interface GE0/0/1 next-hop 10.10.1.2 protocol tcp destination-port 10001
 destination 198.51.100.1 interface GE0/0/2 next-hop 10.20.1.2 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
 bandwidth ingress 100000
 bandwidth egress 100000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
multi-interface
  add interface GE0/0/1
  add interface GE0/0/2
  healthcheck isp_health
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

5.4.2 CLI: Example for Configuring Load Balancing Based on Link Bandwidth

Networking Requirements

In **Figure 5-8**, an enterprise has a 100M link connected to ISP1 and a 50M link connected to ISP2.

- The enterprise requires that traffic be forwarded to ISP1 and ISP2 links based on the bandwidth ratio to ensure full utilization of bandwidth resources.

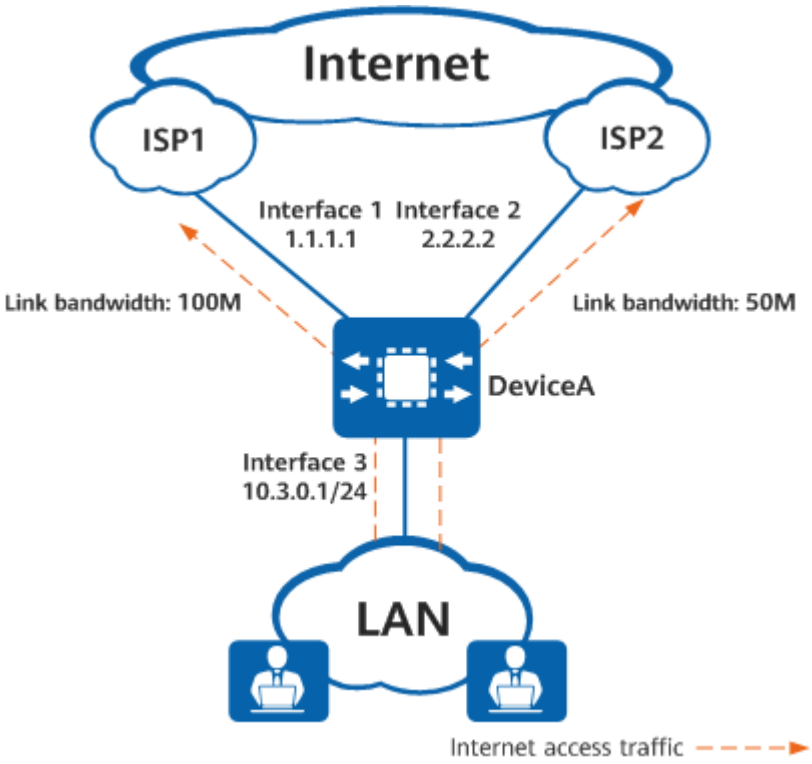
 Copyright © Huawei Technologies Co., Ltd.

- When one ISP link fails, follow-up traffic will be forwarded on the other ISP link to ensure access availability.

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

Figure 5-8 Networking diagram of load balancing by link bandwidth



Configuration Roadmap

The enterprise requires traffic distribution by bandwidth ratio. Therefore, set the intelligent uplink selection mode to load balancing by link bandwidth. To ensure that the DeviceA can use the other link to forward traffic when one link is faulty, configure the health check function.

1. Configure the health check function for ISP1 and ISP2 links respectively.
2. Set IP addresses, security zones, gateway addresses, and bandwidth for interfaces.
3. Configure a global route selection policy. Set the intelligent uplink selection mode to load balancing by link bandwidth, configure the outbound interfaces on DeviceA connecting to ISP1 and ISP2 networks as intelligent uplink selection member interfaces, and reference the health check.
4. Configure a basic security policy to allow intranet users to access Internet resources.

NOTE

This example focuses on the configuration of intelligent uplink selection. Other configurations, such as NAT, need to be performed based on the actual networking.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable the health check function and create health check tasks for ISP1 and ISP2 respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP1 and 198.51.100.0/24 for ISP2.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] healthcheck enable
[DeviceA] healthcheck name isp_health
[DeviceA-healthcheck-isp_health] destination 192.0.2.1 interface ge 0/0/1 protocol tcp destination-port 10001
[DeviceA-healthcheck-isp_health] destination 198.51.100.1 interface ge 0/0/2 protocol tcp destination-port 10003
[DeviceA-healthcheck-isp_health] quit
```

NOTE

Only one health check can be referenced for global route selection. In a health check, only one IP address of an interface can be checked. If extra IP addresses need to be checked, configure a PBR rule.

Assume that 192.0.2.1 and 198.51.100.1 are known device addresses on the ISP1 network and ISP2 network, respectively.

If the state remains down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 2 Configure IP addresses and gateway addresses for interfaces, and configure the bandwidths of the links where the interfaces reside.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] bandwidth ingress 100000
[DeviceA-GE0/0/1] bandwidth egress 100000
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 2.2.2.2 255.255.255.0
[DeviceA-GE0/0/2] gateway 2.2.2.254
[DeviceA-GE0/0/2] bandwidth ingress 50000
[DeviceA-GE0/0/2] bandwidth egress 50000
[DeviceA-GE0/0/2] quit
```

Step 3 Configure a global route selection policy to load balance traffic by link bandwidth and reference the health check.

```
[DeviceA] multi-interface
[DeviceA-multi-inter] mode proportion-of-bandwidth
[DeviceA-multi-inter] add interface ge 0/0/1
[DeviceA-multi-inter] add interface ge 0/0/2
[DeviceA-multi-inter] healthcheck isp_health
[DeviceA-multi-inter] quit
```

Step 4 Add interfaces to corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 5 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet. Assume that the intranet users reside on 10.3.0.0/24.

```
[DeviceA-policy-security] rule name policy_sec_trust_untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-zone trust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_trust_untrust] action permit
[DeviceA-policy-security-rule-policy_sec_trust_untrust] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

- After the network operates for a period of time, run the **display interface brief** command on interface1 (GE0/0/1) and interface2 (GE0/0/2) to check the average bandwidth usage (**OutUti** field) in the outbound direction within the last 300s. The **OutUti** ratio of the interfaces is close to 2:1 (link bandwidth ratio configured for the two interfaces).
- Run the **display firewall session table interface ge 0/0/1** and **display firewall session table interface ge 0/0/2** commands to check the number of sessions on the two interfaces. The session number ratio of the interfaces is close to 2:1.

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
healthcheck name isp_health
 destination 192.0.2.1 interface GE0/0/1 protocol tcp destination-port 10001
 destination 198.51.100.1 interface GE0/0/2 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
 bandwidth ingress 100000
 bandwidth egress 100000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
 multi-interface
  mode proportion-of-bandwidth
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/1
 add interface GE0/0/2
 healthcheck isp_health
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

5.4.3 Web: Example for Configuring Load Balancing Based on Link Weight

Networking Requirements

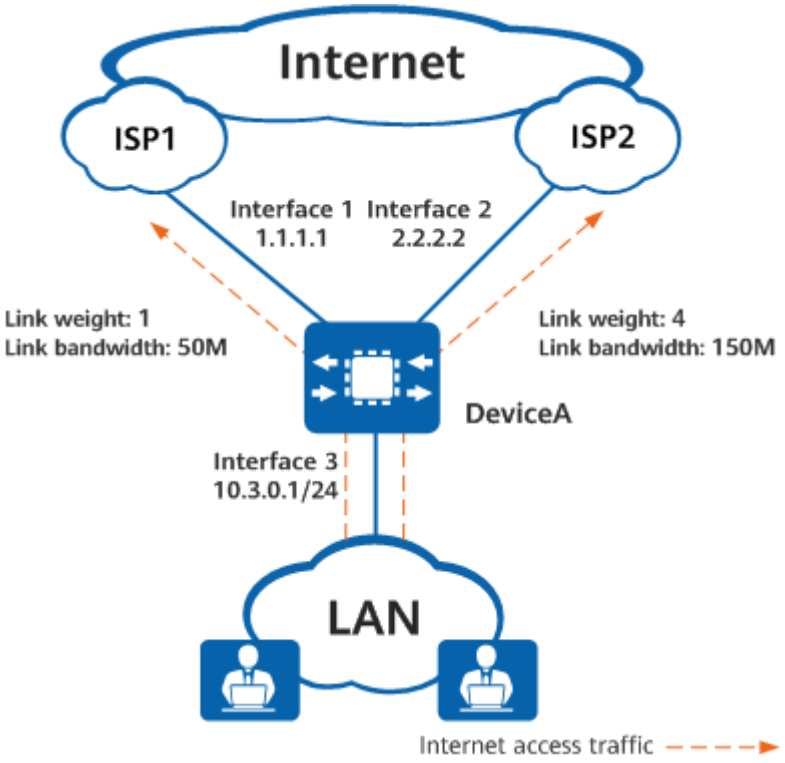
In **Figure 5-9**, an enterprise has a 50M link connected to ISP1, and a 150M link connected to ISP2.

- The enterprise requires that the ISP2 link forward 80% of the traffic and ISP1 link forward 20% of the traffic to improve the Internet access experience of most users.
- When one link becomes faulty, follow-up traffic will be forwarded on the other link to ensure transmission availability.

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

Figure 5-9 Networking diagram of load balancing based on link weight



Configuration Roadmap

The enterprise requires that the traffic ratio on ISP2 and ISP1 links is 4:1. Therefore, set the intelligent uplink selection mode to load balancing based on link weight and set the weights of ISP2 and ISP1 links to 4 and 1, respectively. To ensure that DeviceA can use other links to forward traffic when a link is faulty, you need to configure health check function.

1. Set interface IP addresses, security zones, gateway addresses, bandwidth.
2. **Optional:** Configure the health check function, and configure a health check task for ISP1 and ISP2, respectively.
3. Configure a global route selection policy. Set the intelligent uplink selection mode to load balancing based on link weight, configure the outbound interfaces on DeviceA connecting to ISP1 and ISP2 networks as intelligent uplink selection member interfaces, set weights for the interfaces, and reference health check.
4. Configure a basic security policy to allow intranet users to access the Internet.

NOTE

This example focuses on the configuration related to intelligent uplink selection. Configure other data such as NAT based on the actual networking.

Procedure

Step 1 Set IP addresses for interfaces on the firewall and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE 0/0/1 and set the parameters as follows.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	1.1.1.1/255.255.255.0
Default Gateway	1.1.1.254
Inbound Bandwidth	50 Mbit/s
Outbound Bandwidth	50 Mbit/s

3. Repeat the preceding steps to set the parameters for GE 0/0/2.

Security Zone	untrust
Mode	Routing
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

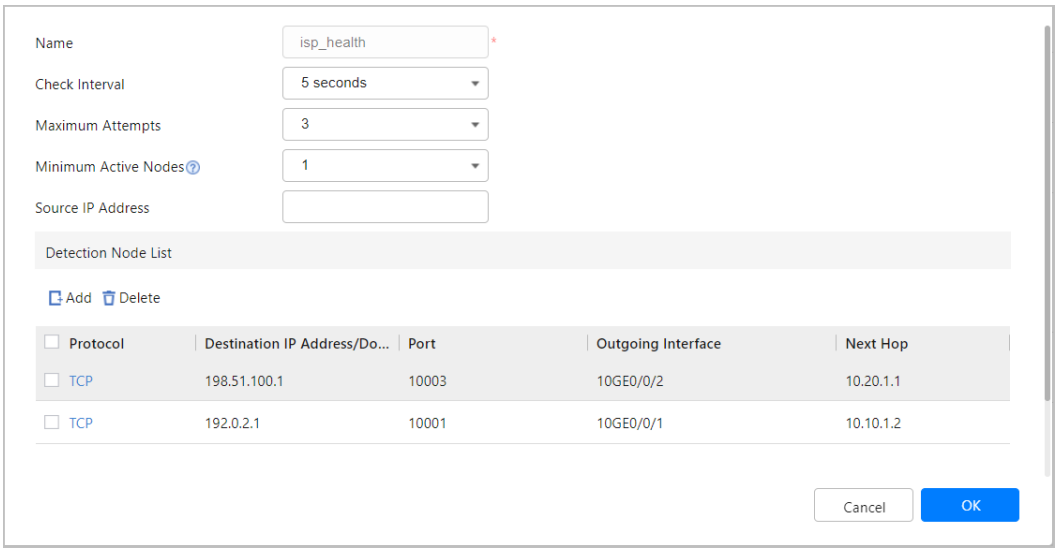
Connection Type	Static IP address
IP Address	2.2.2.2/255.255.255.0
Default Gateway	2.2.2.254
Inbound Bandwidth	50 Mbit/s
Outbound Bandwidth	50 Mbit/s

4. Repeat the preceding steps to set the parameters for GE 0/0/3.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	10.3.0.1/255.255.255.0

Step 2 Enable the health check function and create a health check for ISP1 and ISP2 link respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP1 and is 198.51.100.0/24 for ISP2.

1. Choose **Object** > **Health Check**.
2. In **Health Check List**, click **Create**.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

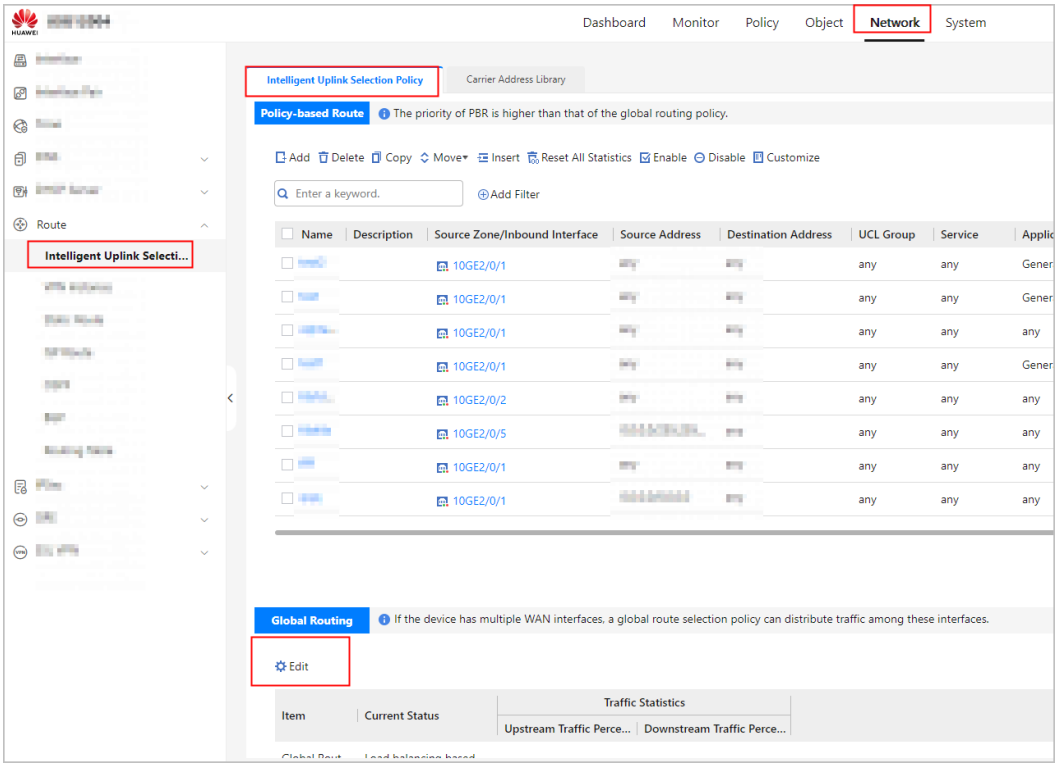
Assume that 192.0.2.1 and 198.51.100.1 are known device addresses on the ISP1 network and ISP2 network, respectively.

If the state remains Down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 3 Configure a global route selection policy to load balance traffic by link bandwidth and reference the health check.

1. Choose **Network** > **Route** > **Intelligent Uplink Selection**. On the **Intelligent Uplink Selection Policy** tab page, click **Edit** in **Global Routing Policy**.

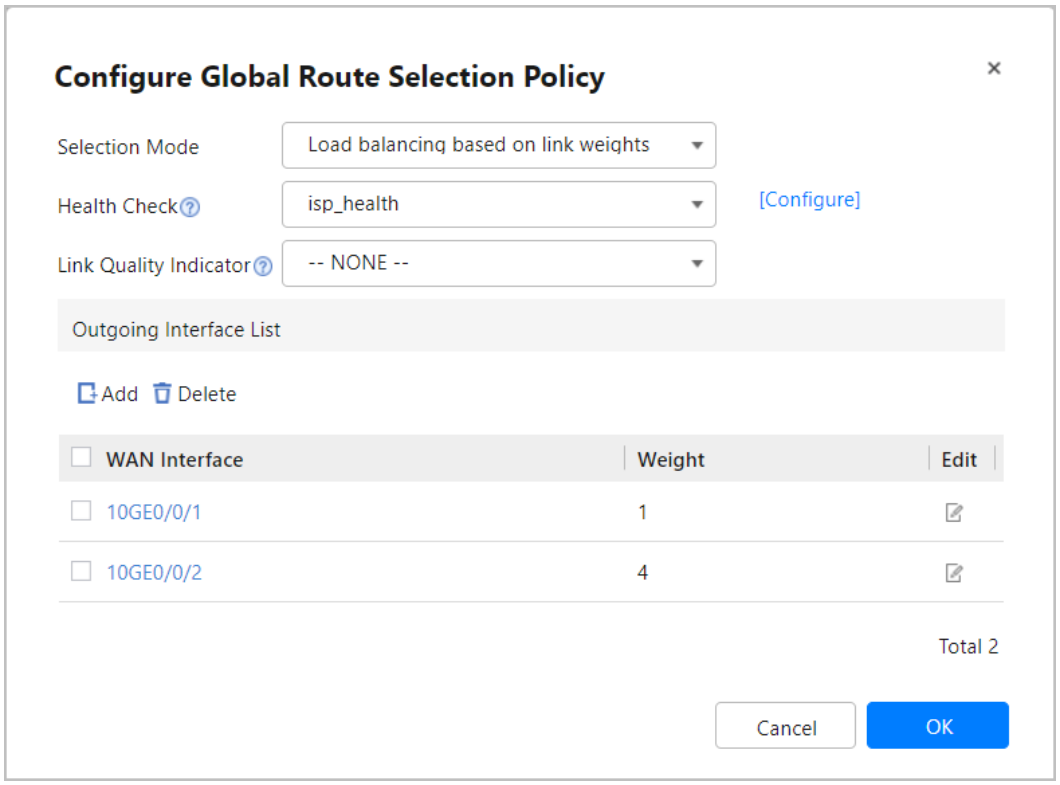


NOTE

In multi-egress intelligent uplink selection, the availability of each link is determined based on each detection node in the health check instead of the status of the health check object.

2. Configure a global route selection policy.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access Internet resources. Assume that the intranet user network segment is 10.3.0.0/24.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Parameter	policy_sec_trust_untrust
Source Security Zone	trust
Destination Security Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

----End

Verifying the Configuration

- After the network has been running for a period of time, run the **display interface brief** command on interface 1 (GE 0/0/1) and interface 2 (GE 0/0/2) to check the average bandwidth usage (**OutUti** field) in the outbound direction within the last 300s and verify that the **OutUti** ratio of the two interfaces is close to 1:4.
- Run the **display firewall session table interface ge 0/0/1** and **display firewall session table interface ge 0/0/2** commands to check the number of sessions on the two interfaces and verify that the ratio is close to 1:4.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
#
healthcheck name isp_health
 destination 192.0.2.1 interface GE0/0/1 next-hop 10.10.1.2 protocol tcp destination-port 10001
 destination 198.51.100.1 interface GE0/0/2 next-hop 10.20.1.2 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 150000
 bandwidth egress 150000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
 multi-interface
  mode proportion-of-weight
  add interface GE0/0/1
  add interface GE0/0/2 weight 4
  healthcheck isp_health

#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

5.4.4 CLI: Example for Configuring Load Balancing Based on Link Weight

Networking Requirements

As shown in **Figure 5-10**, an enterprise has a 50M link connected to ISP1. However, this link delivers poor forwarding performance. Therefore, the enterprise rents a 150M link from ISP2, which delivers good performance.

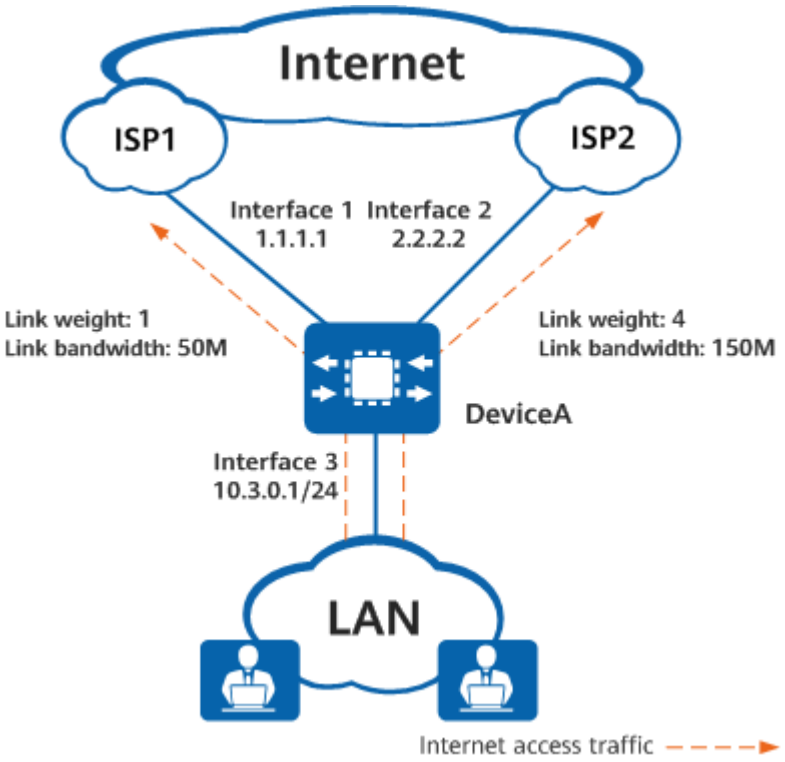
- The enterprise requires that the ISP2 link forwards 80% of the traffic and ISP1 link forwards 20% of the traffic to improve the Internet access experience of most users.
- When one link is faulty, follow-up traffic will be forwarded on the other link to ensure transmission availability.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

Figure 5-10 Networking diagram of load balancing by link weight



Configuration Roadmap

The enterprise requires that the traffic ratio on ISP2 and ISP1 links is 4:1. Therefore, set the intelligent uplink selection mode to load balancing by link weight and set the weights of ISP2 and ISP1 links to 4 and 1 respectively. To ensure that the DeviceA can use the other link to forward traffic when one link is faulty, configure the health check function.

1. Configure the health check function for ISP1 and ISP2 links respectively.
2. Set IP addresses, security zones, gateway addresses, and bandwidth for interfaces.
3. Configure a global route selection policy. Set the intelligent uplink selection mode to load balancing by link weight, configure the outbound interfaces on DeviceA connecting to ISP1 and ISP2 networks as intelligent uplink selection member interfaces, set weights for the interfaces, and reference the health check.
4. Configure a basic security policy to allow intranet users to access Internet resources.

NOTE

This example focuses on the configuration of intelligent uplink selection. Other configurations, such as NAT, need to be performed based on the actual networking.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable the health check function and create health check tasks for ISP1 and ISP2 respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP1 and 198.51.100.0/24 for ISP2.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] healthcheck enable
[DeviceA] healthcheck name isp_health
[DeviceA-healthcheck-isp_health] destination 192.0.2.1 interface ge 0/0/1 protocol tcp destination-port 10001
[DeviceA-healthcheck-isp_health] destination 198.51.100.1 interface ge 0/0/2 protocol tcp destination-port 10003
[DeviceA-healthcheck-isp_health] quit
```

NOTE

Only one health check can be referenced for global route selection. In a health check, only one IP address of an interface can be checked. If extra IP addresses need to be checked, configure a PBR rule.

Assume that 192.0.2.1 and 192.0.2.2 are known device addresses on the ISP1 network and that 198.51.100.1 and 198.51.100.2 are known device addresses on the ISP2 network.

If the state remains down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 2 Configure IP addresses and gateway addresses for interfaces, and configure the bandwidths of the links where the interfaces reside.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] bandwidth ingress 50000
[DeviceA-GE0/0/1] bandwidth egress 50000
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 2.2.2.2 255.255.255.0
[DeviceA-GE0/0/2] gateway 2.2.2.254
[DeviceA-GE0/0/2] bandwidth ingress 150000
[DeviceA-GE0/0/2] bandwidth egress 150000
[DeviceA-GE0/0/2] quit
```

Step 3 Configure a global route selection policy to load balance traffic by link weight and reference the health check.

```
[DeviceA] multi-interface
[DeviceA-multi-inter] mode proportion-of-weight
[DeviceA-multi-inter] add interface ge 0/0/1
[DeviceA-multi-inter] add interface ge 0/0/2 weight 4
[DeviceA-multi-inter] healthcheck isp_health
[DeviceA-multi-inter] quit
```

Step 4 Add interfaces to corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 5 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet. Assume that the intranet users reside on 10.3.0.0/24.

```
[DeviceA-policy-security] rule name policy_sec_trust_untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-zone trust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_trust_untrust] action permit
[DeviceA-policy-security-rule-policy_sec_trust_untrust] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

- After the network operates for a period of time, run the **display interface brief** command on interface1 (GE0/0/1) and interface2 (GE0/0/2) to check the average bandwidth usage (**OutUti** field) in the outbound direction within the last 300s. The **OutUti** ratio of the interfaces is close to 1:4.
- Run the **display firewall session table interface ge 0/0/1** and **display firewall session table interface ge 0/0/2** commands to check the number of sessions on the two interfaces. The session number ratio of the interfaces is close to 1:4.

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
healthcheck name isp_health
 destination 192.0.2.1 interface GE0/0/1 protocol tcp destination-port 10001
 destination 198.51.100.1 interface GE0/0/2 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 150000
 bandwidth egress 150000
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
 multi-interface
  mode proportion-of-weight
  add interface GE0/0/1
  add interface GE0/0/2 weight 4
```

 Copyright © Huawei Technologies Co., Ltd.

```
 healthcheck isp_health

#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

5.4.5 Web: Example for Configuring Active/Standby Backup Based on Link Priority

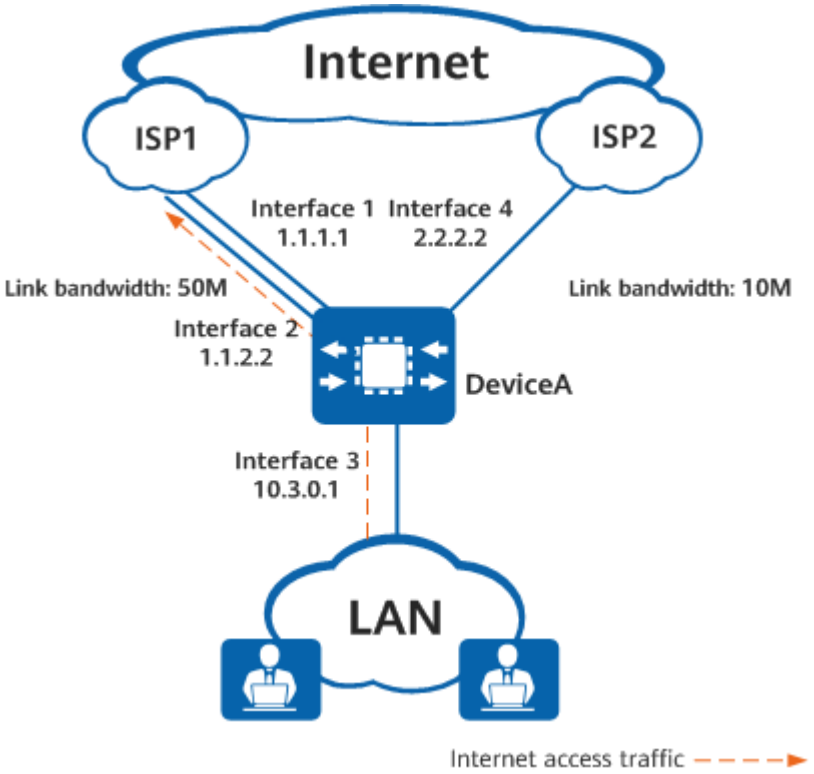
Networking Requirements

In Figure 5-11, an enterprise has two 50M links connected to ISP1 and one 10M link connected to ISP2. The enterprise requires that the two ISP1 links be used preferentially to forward Internet access traffic and ISP2 link be used only when both ISP1 links are faulty.

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, and GE 0/0/4, respectively.

Figure 5-11 Networking diagram of active/standby backup based on link priority



Configuration Roadmap

When the enterprise uses the ISP1 link preferentially, you need to set the global intelligent uplink selection mode to active/standby backup based on link priority

 Copyright © Huawei Technologies Co., Ltd.

and set the priorities of ISP1 and ISP2 links to 2 and 1, respectively. The tax declaration service needs to be transmitted on the ISP2 link preferentially. Therefore, configure PBR-based intelligent uplink selection for the tax declaration application, set the link selection mode to active/standby backup based on link priority, and set the priority of the ISP2 link to 2 and priorities of two ISP1 links to 1. To ensure that DeviceA can use the standby interface link to forward traffic when the active interface link is faulty, configure the health check function.

1. Set the interface IP addresses, security zones, gateway addresses, and bandwidth values for the links of the interfaces.
2. Configure the health check function, and configure a health check task for ISP1 and ISP2, respectively.
3. Configure a global link selection policy, set the intelligent uplink selection mode to active/standby backup based on link priority, and configure GE0/0/1, GE0/0/2, and GE0/0/4 as intelligent uplink selection member interfaces, apply health check.
4. Configure a basic security policy to allow intranet users to access the Internet.

NOTE

This example focuses on the configuration related to intelligent uplink selection. Configure other data such as NAT based on the actual networking.

Procedure

Step 1 Set IP addresses for interfaces on the firewall and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click GE 0/0/1 and set the parameters as follows.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	1.1.1.1/255.255.255.0
Default Gateway	1.1.1.254
Inbound Bandwidth	50 Mbit/s
Outbound Bandwidth	50 Mbit/s

3. Repeat the preceding steps to set the parameters for GE 0/0/2.

Security Zone	untrust
Mode	Routing
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

Connection Type	Static IP address
IP Address	1.1.2.2/255.255.255.0
Default Gateway	1.1.2.254
Inbound Bandwidth	50 Mbit/s
Outbound Bandwidth	50 Mbit/s

4. Repeat the preceding steps to set the parameters for GE 0/0/4.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	2.2.2.2/255.255.255.0
Default Gateway	2.2.2.254
Inbound Bandwidth	10 Mbit/s
Outbound Bandwidth	10 Mbit/s

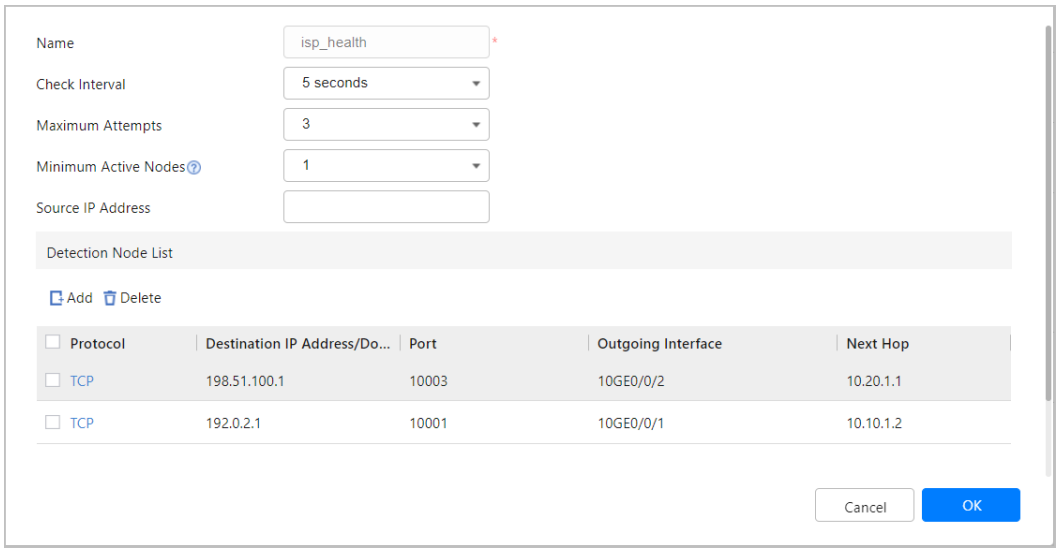
5. Repeat the preceding steps to set the parameters for GE 0/0/3.

Security Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP address
IP Address	10.3.0.1/255.255.255.0

Step 2 Enable the health check function and create a detection node for ISP1 and ISP2 link respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP1 and is 198.51.100.0/24 for ISP2.

1. Choose **Object** > **Health Check**.
2. In **Health Check List**, click **Create**.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

Assume that 192.0.2.1 and 198.51.100.1 are known device addresses on the ISPA network and ISPB network, respectively.

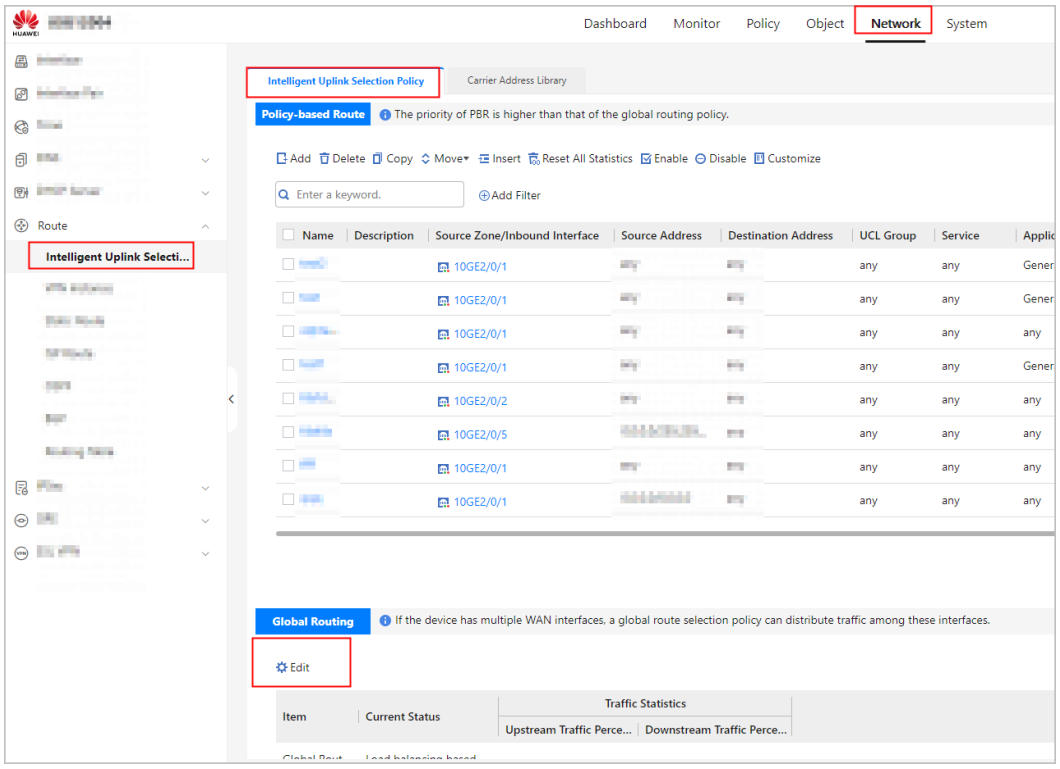
If the state remains Down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 3 Configure a global route selection policy for active/standby backup by link priority and reference the health check.

1. Choose **Network** > **Route** > **Intelligent Uplink Selection**. On the **Intelligent Uplink Selection Policy** tab page, click **Edit** in **Global Routing Policy**.

 Copyright © Huawei Technologies Co., Ltd.

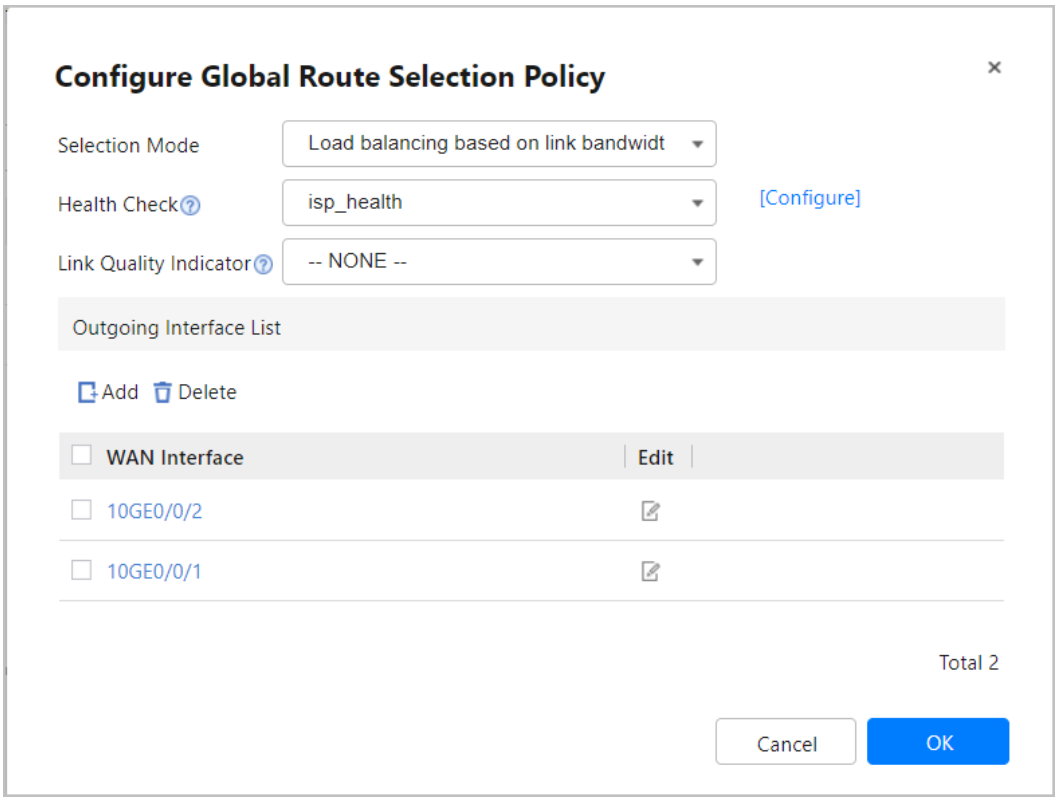


NOTE

In multi-egress intelligent uplink selection, the availability of each link is determined based on each detection node in the health check instead of the status of the health check object.

2. Configure a global route selection policy.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access Internet resources. Assume that the intranet user network segment is 10.3.0.0/24.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Parameter	policy_sec_trust_untrust
Source Security Zone	trust
Destination Security Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

----End

Verifying the Configuration

- After the network has been running for a period of time, run the **display interface brief** command on interface 1 (GE 0/0/1), interface 2 (GE 0/0/2) ,and interface4 (GE 0/0/4) to check the average bandwidth usage (**OutUti** field) in the outbound direction within the last 300s and verify that the **OutUti** ratio of the three interfaces is close to 1:1:0. That is, interface 1 and interface 2 forward traffic in 1:1 mode, and interface 4 does not forward traffic in normal cases.

 Copyright © Huawei Technologies Co., Ltd.

- When both links of ISP1 fail, all traffic is forwarded through interface 4.

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
healthcheck name isp1_health_01
 destination 192.0.2.1 interface GE0/0/1 protocol tcp destination-port 10001
 destination 192.0.2.1 interface GE0/0/2 protocol tcp destination-port 10002
 destination 198.51.100.1 interface GE0/0/4 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/2
 ip address 1.1.2.2 255.255.255.0
 gateway 1.1.2.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/4
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 10000
 bandwidth egress 10000
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
 add interface GE0/0/4
#
 multi-interface
  mode priority-of-userdefine
  add interface GE0/0/1 priority 2
  add interface GE0/0/2 priority 2
  add interface GE0/0/4
  healthcheck isp_health
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

5.4.6 CLI: Example for Configuring Active/Standby Backup Based on Link Priority

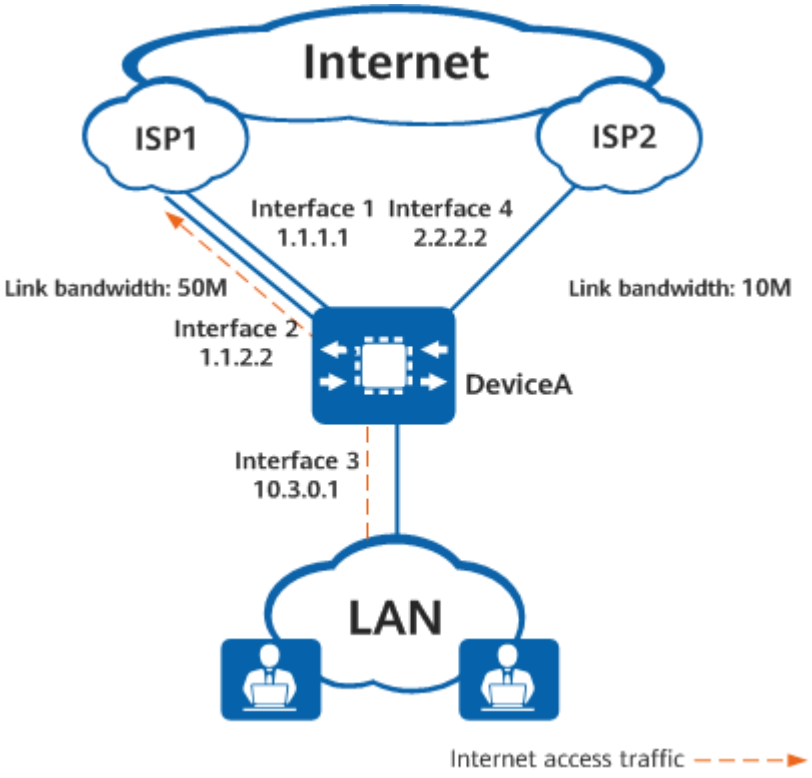
Networking Requirements

As shown in **Figure 5-12**, an enterprise has two 50M links connected to ISP1 and one 10M link connected to ISP2. The enterprise requires that the two ISP1 links be used preferentially to forward Internet access traffic and ISP2 link be used only when both ISP1 links are faulty.

NOTE

In this example, interface1, interface2, interface3, and interface4 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/4, respectively.

Figure 5-12 Networking diagram of active/standby backup by link priority



Configuration Roadmap

The enterprise needs to use ISP1 link preferentially. Therefore, set the global intelligent uplink selection mode to load balancing by link priority and set the priorities of ISP1 and ISP2 links to 2 and 1, respectively. To ensure that DeviceA can use the standby interface link to forward traffic when the active interface link is faulty, configure the health check function.

1. Configure the health check function for ISP1 and ISP2 links respectively.
2. Set IP addresses, security zones, gateway addresses, and bandwidth for interfaces.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure a global route selection policy. Set the intelligent uplink selection mode to active/standby backup by link priority, and configure GE0/0/1, GE0/0/2, and GE0/0/4 as intelligent uplink selection member interfaces. Reference the health check and set a priority for each interface.
4. Configure a basic security policy to allow intranet users to access Internet resources.

NOTE

This example focuses on the configuration of intelligent uplink selection. Other configurations, such as NAT, need to be performed based on the actual networking.

Procedure

Step 1 Enable the health check function and create health check tasks for ISP1 and ISP2 respectively. Assume that the destination network segment is 192.0.2.0/24 for ISP1 and 198.51.100.0/24 for ISP2.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] healthcheck enable
[DeviceA] healthcheck name isp_health
[DeviceA-healthcheck-isp_health] destination 192.0.2.1 interface ge 0/0/1 protocol tcp destination-port 10001
[DeviceA-healthcheck-isp_health] destination 192.0.2.3 interface ge 0/0/2 protocol tcp destination-port 10001
[DeviceA-healthcheck-isp_health] destination 198.51.100.1 interface ge 0/0/4 protocol tcp destination-port 10003
[DeviceA-healthcheck-isp_health] quit
```

NOTE

Only one health check can be referenced for global route selection. In a health check, only one IP address of an interface can be checked. If extra IP addresses need to be checked, configure a PBR rule.

Assume that 192.0.2.1 to 192.0.2.4 are known device addresses on the ISP1 network and that 198.51.100.1 and 198.51.100.2 are known device addresses on the ISP2 network.

If the state remains down after the health check configuration is complete, check the health check configuration.

Probe packets for health check are not controlled by security policies and are permitted by default. No security policy needs to be configured.

Step 2 Configure IP addresses and gateway addresses for interfaces, and configure the bandwidths of the links where the interfaces reside.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] bandwidth ingress 50000
[DeviceA-GE0/0/1] bandwidth egress 50000
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.2.2 255.255.255.0
[DeviceA-GE0/0/2] gateway 1.1.2.254
[DeviceA-GE0/0/2] bandwidth ingress 50000
[DeviceA-GE0/0/2] bandwidth egress 50000
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/4
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/4] undo portswitch
[DeviceA-GE0/0/4] ip address 2.2.2.2 255.255.255.0
[DeviceA-GE0/0/4] gateway 2.2.2.254
[DeviceA-GE0/0/4] bandwidth ingress 10000
[DeviceA-GE0/0/4] bandwidth egress 10000
[DeviceA-GE0/0/4] quit
```

Step 3 Configure a global route selection policy, configure active/standby backup for traffic based on link priorities, and reference the health check.

```
[DeviceA] multi-interface
[DeviceA-multi-inter] mode priority-of-userdefine
[DeviceA-multi-inter] add interface ge 0/0/1 priority 2
[DeviceA-multi-inter] add interface ge 0/0/2 priority 2
[DeviceA-multi-inter] add interface ge 0/0/4
[DeviceA-multi-inter] healthcheck isp_health
[DeviceA-multi-inter] quit
```

Step 4 Add interfaces to corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] add interface ge 0/0/4
[DeviceA-zone-untrust] quit
```

Step 5 Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet. Assume that the intranet users reside on 10.3.0.0/24.

```
[DeviceA-policy-security] rule name policy_sec_trust_untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-zone trust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_trust_untrust] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_trust_untrust] action permit
[DeviceA-policy-security-rule-policy_sec_trust_untrust] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

- After the network operates for a period of time, run the **display interface brief** command on interface1 (GE0/0/1), interface2 (GE0/0/2), and interface4 (GE0/0/4) to check the average bandwidth usage (**OutUti** field) in the outbound direction within the last 300s. The **OutUti** ratio of the interfaces is close to 1:1:0. That is, interface1 and interface2 forward traffic in a ratio of 1:1. In normal cases, interface4 does not forward traffic.
- When both ISP1 links fail, all traffic is forwarded through interface4.

Configuration Scripts

```
#
sysname DeviceA
#
healthcheck enable
healthcheck name isp_health
 destination 192.0.2.1 interface GE0/0/1 protocol tcp destination-port 10001
 destination 192.0.2.3 interface GE0/0/2 protocol tcp destination-port 10001
 destination 198.51.100.1 interface GE0/0/4 protocol tcp destination-port 10003
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
```

 Copyright © Huawei Technologies Co., Ltd.

```
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/2
 ip address 1.1.2.2 255.255.255.0
 gateway 1.1.2.254
 bandwidth ingress 50000
 bandwidth egress 50000
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/4
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
 bandwidth ingress 10000
 bandwidth egress 10000
#
 firewall zone trust
  set priority 85
  add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
 add interface GE0/0/4
#
 multi-interface
  mode priority-of-userdefine
  add interface GE0/0/1 priority 2
  add interface GE0/0/2 priority 2
  add interface GE0/0/4
  healthcheck isp_health
#
security-policy
 rule name policy_sec_trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

6 Virtual System

6.1 Web: Example for Configuring Communication Between a Virtual System and the Public System Based on Routing Tables

6.2 CLI: Example for Configuring Communication Between a Virtual System and the Public System Based on Routing Tables

6.3 CLI: Example for Configuring Communication Between a Virtual System and the Public System Based on a Traffic Diversion Table

6.4 Web: Example for Configuring Direct Communication Between Two Virtual Systems

6.5 CLI: Example for Configuring Direct Communication Between Two Virtual Systems

6.6 Web: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on Routing Tables

6.7 CLI: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on Routing Tables

6.8 CLI: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on a Traffic Diversion Table

6.9 CLI: Example for Configuring Communication Between Two Virtual Systems Across Another Virtual System

6.10 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through Independent Public Network Interfaces of the Virtual Systems

6.11 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through Independent WAN Interfaces of the Virtual Systems

6.12 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the Public Interface of the Public System (Performing NAT in the Public System)

6.13 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the WAN Interface of the Public System (Performing NAT in the Public System)

 Copyright © Huawei Technologies Co., Ltd.

6.14 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the Public Network Interface of the Public System (Performing NAT in Each Virtual System)

6.15 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the WAN Interface of the Public System (Performing NAT in Each Virtual System)

6.16 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through Independent Public Network Interfaces of the Virtual Systems

6.17 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through Independent WAN Interfaces of the Virtual Systems

6.18 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the Public Network Interface of the Public System (Performing NAT in the Public System)

6.19 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the WAN Interface of the Public System (Performing NAT in the Public System)

6.20 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the Public Network Interface of the Public System (Performing NAT in Each Virtual System)

6.21 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the WAN Interface of the Public System (Performing NAT in Each Virtual System)

6.22 Web: Example for Configuring Layer 2 Access for Virtual Systems

6.23 CLI: Example for Configuring Layer 2 Access for Virtual Systems

6.24 Web: Example for Configuring IPv6 User Access at Layer 3 Through Virtual Systems

6.25 CLI: Example for Configuring IPv6 User Access at Layer 3 Through Virtual Systems

6.26 CLI: Example for Configuring Telnet Login to a Virtual System

6.27 CLI: Example for Configuring STelnet Login to a Virtual System

6.1 Web: Example for Configuring Communication Between a Virtual System and the Public System Based on Routing Tables

Networking Requirements

As shown in **Figure 6-1**, the device is deployed between network A and the Internet, and **vsysa** functions as the gateway of network A to isolate and protect network A. The device connects to the Internet through the public network interface named interface 1 of the public system.

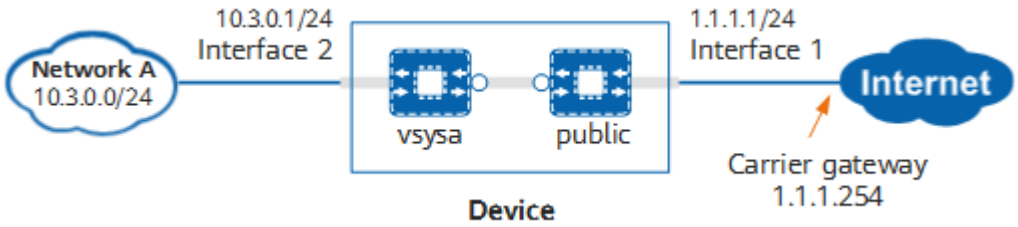
 Copyright © Huawei Technologies Co., Ltd.

You need to configure communication between **vsysa** and the public system based on routing tables so that network A and the Internet can communicate with each other.

Figure 6-1 Communication between a virtual system and the public system based on routing tables

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



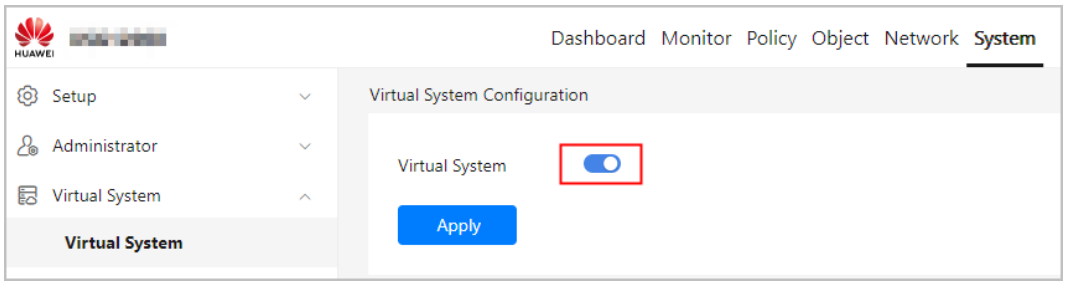
Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual system **vsysa**, and allocate resources to it.
2. Configure interfaces for the public system and **vsysa**, and add the interfaces to security zones.
3. Configure routes in the public system and **vsysa** to divert traffic between network A and the Internet.
4. Configure security policies in the public system and **vsysa** to permit the traffic between network A and the Internet.

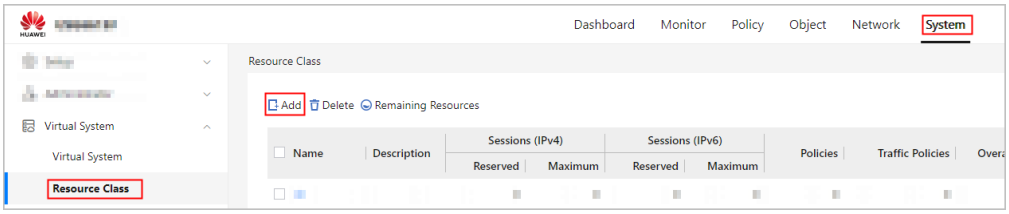
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



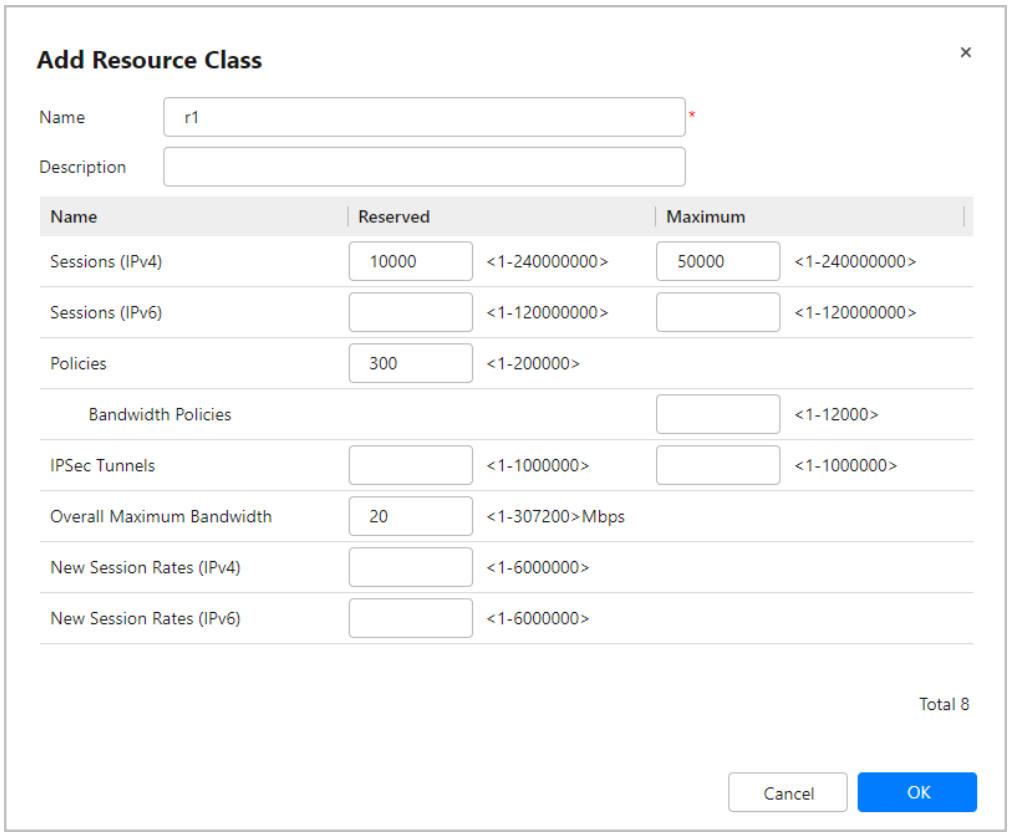
Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



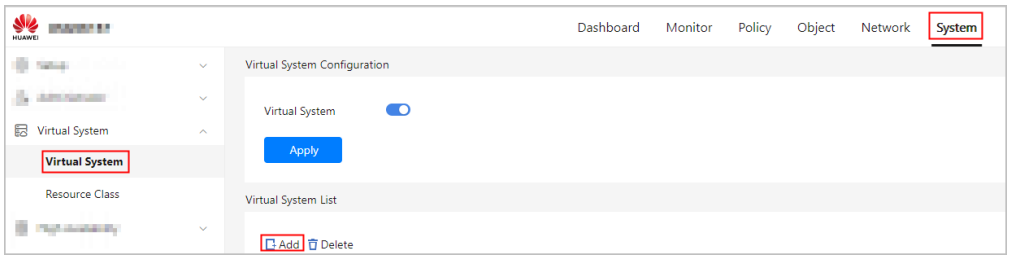
 Copyright © Huawei Technologies Co., Ltd.

2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



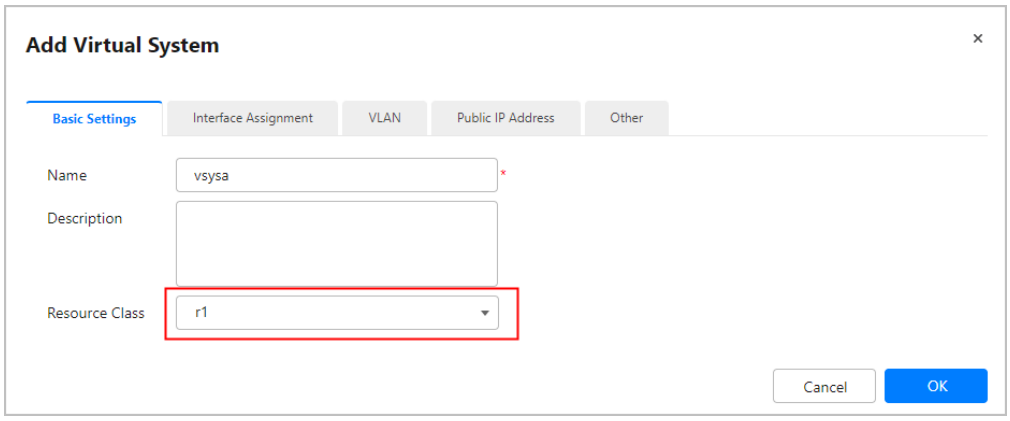
Step 3 In the public system, create virtual system **vsysa** and allocate resources. After completing the configuration, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

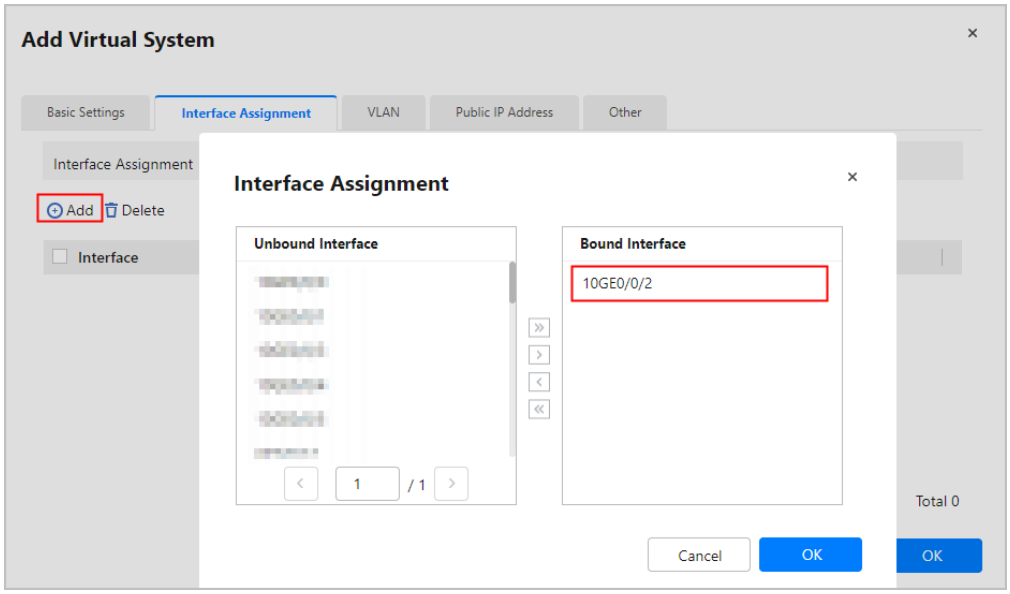


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



Step 4 Configure interfaces for the public system and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE 0/0/1 and set the following parameters. After completing the configuration, click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

3. Repeat the preceding steps and set the following parameters for Virtual-if0.

Zone	trust
IPv4	
IP Address	172.16.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure security policies in the public system.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network A to the Internet. After completing the configuration, click **OK**.

Name	trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

3. Repeat the preceding steps to configure an untrust-to-trust security policy to permit the traffic from the Internet to network A.

Name	untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.0.0/24
Action	Permit

Step 6 Configure routes in the public system.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the public system to the Internet, diverting the forward traffic of network A accessing the Internet or the return traffic for the Internet to access network A to the Internet. **1.1.1.254** is the next-hop address of the route from the public system to the Internet. After completing the configuration, click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

4. Repeat the preceding steps to configure a route from the public system to **vsysa**, diverting the forward traffic of the Internal accessing network A to **vsysa**.

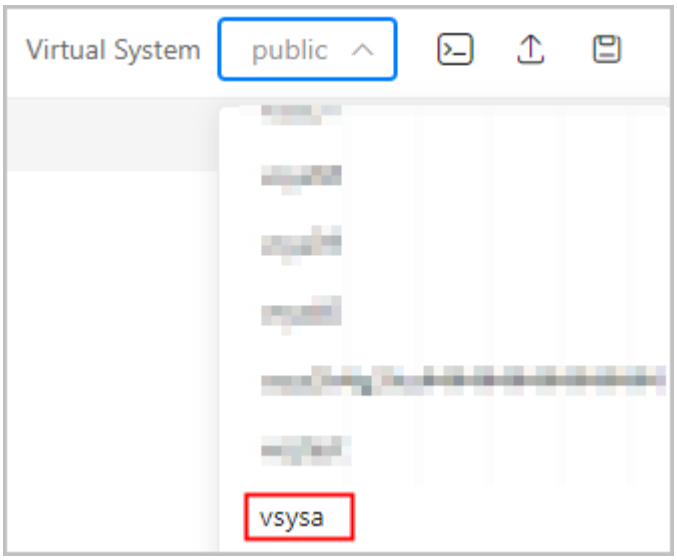
Protocol	IPv4

 Copyright © Huawei Technologies Co., Ltd.

Source Virtual Router	public
Destination Address/Mask	10.3.0.0/24
Destination Virtual Router	vsysa

Step 7 Set the IP addresses of interfaces in **vsysa** and add the interfaces to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/2 and set the following parameters. After completing the configuration, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps and set the following parameters for Virtual-if1.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 8 Configure security policies in **vsysa**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.

 Copyright © Huawei Technologies Co., Ltd.

2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network A to the Internet. After completing the configuration, click **OK**.

Name	vsysa_trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

3. Repeat the preceding steps to configure an untrust-to-trust security policy to permit the traffic from the Internet to network A.

Name	vsysa_untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.0.0/24
Action	Permit

Step 9 Configure routes in **vsysa**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysa** to the public system, diverting the forward traffic of network A accessing the Internet to the public system. After the configuration is complete, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysa
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

4. Repeat the preceding steps to configure a route from **vsysa** to network A, diverting the return traffic of network A accessing the Internet or the forward traffic for the Internet to access network A to network A. **10.3.0.254** is the next-hop address of the route from **vsysa** to network A.

Protocol	IPv4

 Copyright © Huawei Technologies Co., Ltd.

Destination Address/Mask	10.3.0.0/24
Next Hop	10.3.0.254

----End

Verifying the Configuration

Users on network A can proactively access the Internet, and users on the Internet can proactively access resources on network A.

In addition, you can view the sessions generated by the device by choosing **Monitor** > **Session Table** of **vsysa** and the public system.

Configuration Scripts

- public

```
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Virtual-if0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
```

- vsysa

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
```

6.2 CLI: Example for Configuring Communication Between a Virtual System and the Public System Based on Routing Tables

Networking Requirements

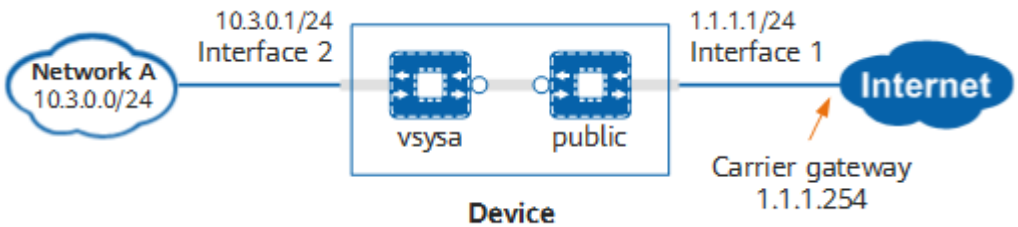
As shown in **Figure 6-2**, the device is deployed between network A and the Internet. Virtual system vsysa functions as the gateway of network A to isolate and protect network A. The device connects to the Internet through the WAN interface interface 1 of the public system.

You need to configure communication between vsysa and the public system based on routing tables so that network A and the Internet can communicate with each other.

Figure 6-2 Communication between a virtual system and the public system based on routing tables

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual system vsysa, and allocate resources to it.
2. Configure interfaces for the public system and vsysa, and add the interfaces to security zones.
3. Configure routes in the public system and vsysa to divert traffic between network A and the Internet.
4. Configure security policies in the public system and vsysa to permit the traffic between network A and the Internet.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Create virtual system vsysa and allocate GE 0/0/2 to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Step 3 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 1.1.1.1 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 4 Configure routes in the public system.

Configure a route from the public system to the Internet, diverting the forward traffic for network A to access the Internet or the return traffic for the Internet to access network A to the Internet. 1.1.1.254 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Configure a route from the public system to vsysa, diverting the forward traffic for the Internet to access network A to vsysa.

```
[Device] ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
```

Step 5 Configure security policies in the public system.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to the Internet.

```
[Device] security-policy
[Device-policy-security] rule name trust_to_untrust
[Device-policy-security-rule-trust_to_untrust] source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-policy-security-rule-trust_to_untrust] destination-zone untrust
[Device-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
[Device-policy-security-rule-trust_to_untrust] action permit
[Device-policy-security-rule-trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from the Internet to network A.

```
[Device-policy-security] rule name untrust_to_trust
[Device-policy-security-rule-untrust_to_trust] source-zone untrust
[Device-policy-security-rule-untrust_to_trust] destination-zone trust
[Device-policy-security-rule-untrust_to_trust] destination-address 10.3.0.0 24
[Device-policy-security-rule-untrust_to_trust] action permit
[Device-policy-security-rule-untrust_to_trust] quit
[Device-policy-security] quit
```

Step 6 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 7 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 8 Configure routes in vsysa.

Configure a route from vsysa to the public system, diverting the forward traffic for network A to access the Internet to the public system.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysa to network A, diverting the return traffic for network A to access the Internet or the forward traffic for the Internet to access network A to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 9 Configure security policies in vsysa.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name vsysa_trust_to_untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-zone trust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-zone untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] action permit
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from the Internet to network A.

```
[Device-vsysa-policy-security] rule name vsysa_untrust_to_trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-zone untrust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] action permit
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] quit
[Device-vsysa-policy-security] quit
```

----End

Verifying the Configuration

- A user on network A can access the Internet. In addition, the following sessions are created in vsysa and the public system.

  NOTE

  In the following command output, 3.3.3.3 is the IP address of the server on the Internet accessed by the user on network A, and 10.3.0.2 is the IP address of the user host on network A.

  Sessions in the public system:

  ```
  <Device> display firewall session table verbose destination global 3.3.3.3
  Current Total Sessions : 1
  icmp  VPN: public --> public  ID: xxxxxxxxxxxxxxxxxxxxx
  Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
  Interface: GE0/0/1  NextHop: 1.1.1.254  MAC: xxxx-xxxx-xxxx
  <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
  10.3.0.2:43999 --> 3.3.3.3:2048 PolicyName: trust_to_untrust
  ```

  Sessions in vsysa:

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 3.3.3.3
  Current Total Sessions : 1
  icmp  VPN: vsysa --> public  ID: xxxxxxxxxxxxxxxxxxxxx
  Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
  Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
  <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
  10.3.0.2:43999 --> 3.3.3.3:2048 PolicyName: vsysa_trust_to_untrust
  ```

- A user on the Internet can access network A. In addition, the following sessions are created in vsysa and the public system.

  NOTE

  In the following command output, 10.3.0.3 is the IP address of the server on network A accessed by the user on the Internet, and 2.2.2.2 is the IP address of the user host on the Internet.

  Sessions in the public system:

  ```
  <Device> display firewall session table verbose destination global 10.3.0.3
  Current Total Sessions : 1
  icmp  VPN: public --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
  Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
  Interface: Virtual-if0  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
  <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
  2.2.2.2:2048 --> 10.3.0.3:43999 PolicyName: untrust_to_trust
  ```

  Sessions in vsysa:

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 10.3.0.3
  Current Total Sessions : 1
  icmp  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
  Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
  Interface: GE0/0/2  NextHop: 10.3.0.254  MAC: xxxx-xxxx-xxxx
  <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
  2.2.2.2:2048 --> 10.3.0.3:43999 PolicyName: vsysa_untrust_to_trust
  ```

Configuration Scripts

- Public system (public)

 Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname Device
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/2
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Virtual-if0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

6.3 CLI: Example for Configuring Communication Between a Virtual System and the Public System Based on a Traffic Diversion Table

Networking Requirements

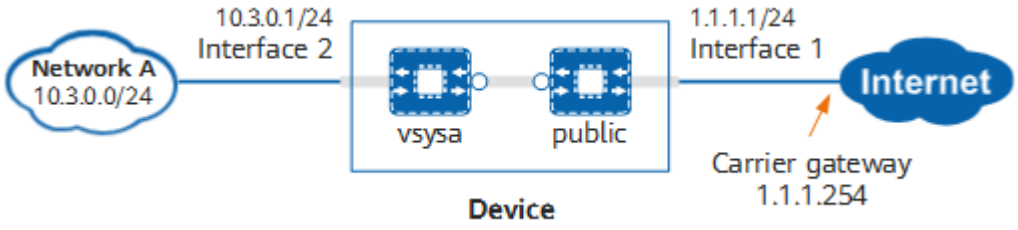
As shown in **Figure 6-3**, the device is deployed between network A and the Internet. Virtual system vsysa functions as the gateway of network A to isolate and protect network A. The device connects to the Internet through the WAN interface interface 1 of the public system.

You need to configure communication between vsysa and the public system based on a traffic diversion table so that network A and the Internet can communicate with each other.

Figure 6-3 Communication between a virtual system and the public system based on a traffic diversion table

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual system vsysa, and allocate resources to it.
2. Configure interfaces for the public system and vsysa, and add the interfaces to security zones.
3. Configure a traffic diversion table in the public system to divert traffic between network A and the Internet.
4. Configure routes in the public system and vsysa to divert traffic sent from the device to network A and the Internet.
5. Configure security policies in vsysa to permit the traffic between network A and the Internet.

NOTE

As no session is created in the public system, you do not need to configure security policies for the packets that match the traffic diversion table in the public system.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Create virtual system vsysa and allocate GE 0/0/2 to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Step 3 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 1.1.1.1 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 4 Configure a traffic diversion table.

Configure a traffic diversion table for diverting the forward traffic for the Internet to access network A or the return traffic of network A accessing the Internet to vsysa.

```
[Device] firewall import-flow public 10.3.0.0 10.3.0.255 vpn-instance vsysa
Warning: The destination of this IP range should be in this vsys network, otherwise it may cause flow loop!
Please select [Y/N]:Y
```

Step 5 Configure a route in the public system.

Configure a route from the public system to the Internet, diverting the forward traffic of network A accessing the Internet to the Internet. 1.1.1.254 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 6 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 7 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 8 Configure routes in vsysa.

Configure a route from vsysa to the public system, diverting the forward traffic for network A to access the Internet to the public system.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysa to network A, diverting the return traffic for network A to access the Internet or the forward traffic for the Internet to access network A to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 9 Configure security policies in vsysa.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name vsysa_trust_to_untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-zone trust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-zone untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] action permit
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from the Internet to network A.

```
[Device-vsysa-policy-security] rule name vsysa_untrust_to_trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-zone untrust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-zone trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] action permit
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] quit
[Device-vsysa-policy-security] quit
```

----End

Verifying the Configuration

- A user on network A can access the Internet. In addition, the following session is created in vsysa and no session is created in the public system.

  NOTE

  In the following command output, 3.3.3.3 is the IP address of the server on the Internet accessed by the user on network A, and 10.3.0.2 is the IP address of the user host on network A.

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 3.3.3.3
   Current Total Sessions : 1
   ICMP  VPN: vsysa --> public  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: trust --> untrust Slot: 0 CPU: 0 TTL: xx:xx:xx Left: xx:xx:xx
   Recv Interface: GE0/0/2 Rev Slot: 0 CPU: 1
   Interface: GE0/0/1 NextHop: 1.1.1.254
   <==packets: xxx bytes: xxx ==> packets: xxx bytes: xxx
   10.3.0.2:17408 --> 3.3.3.3:2048 PolicyName: vsysa_trust_to_untrust
  ```

- A user on the Internet can access network A. In addition, the following session is created in vsysa and no session is created in the public system.

  NOTE

  In the following command output, 10.3.0.3 is the IP address of the server on network A accessed by the user on the Internet, and 2.2.2.2 is the IP address of the user host on the Internet.

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 10.3.0.3
   Current Total Sessions : 1
   ICMP  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
Zone: untrust --> trust Slot: 0 CPU: 1 TTL: xx:xx:xx Left: xx:xx:xx
Recv Interface: GE0/0/1 Rev Slot: 0 CPU: 0
Interface: GE0/0/2 NextHop: 10.3.0.254
<==packets: xxx bytes: xxx ==> packets: xxx bytes: xxx
2.2.2.2:17408 --> 10.3.0.3:2048 PolicyName: vsysa_untrust_to_trust
```

- On the device, you can view the traffic diversion table configuration of vsysa or the traffic diversion table of a specified IP address on network A.

```
<Device> display firewall import-flow public vpn-instance vsysa
 Import Flow Tables:
 firewall import-flow public 10.3.0.0 10.3.0.255 vpn-instance vsysa
 ------------------------------------------------------------------
 Total:256
<Device> display firewall import-flow public 10.3.0.1
 Import Flow Tables:
 Source Instance   Destination Address   Destination Instance
 ------------------------------------------------------------------------------------------------------------
 public            10.3.0.1              vsysa
 ------------------------------------------------------------------------------------------------------------
 Total:1
```

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/2
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 firewall import-flow public 10.3.0.0 10.3.0.255 vpn-instance vsysa
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

6.4 Web: Example for Configuring Direct Communication Between Two Virtual Systems

Networking Requirements

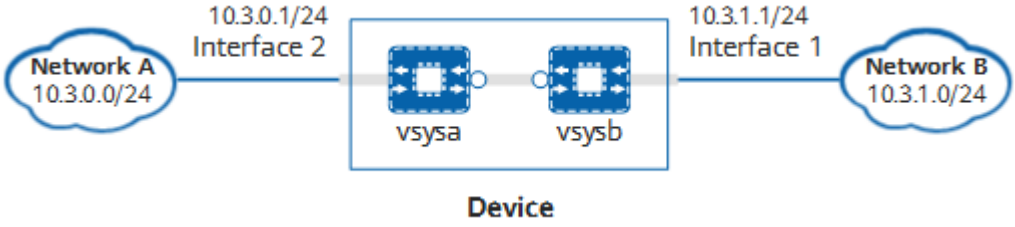
As shown in **Figure 6-4**, the device is deployed between network A and network B. Virtual systems **vsysa** and **vsysb** function as network A's gateway and network B's gateway, respectively, to isolate and protect their respective networks.

You need to configure direct communication between **vsysa** and **vsysb** so that networks A and B can communicate with each other.

Figure 6-4 Direct communication between two virtual systems

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

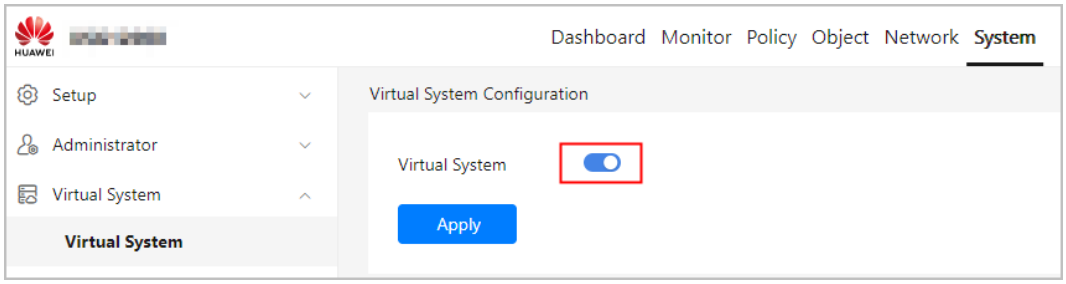
1. Enable the virtual system function, create virtual systems **vsysa** and **vsysb**, and allocate resources to them.
2. Configure interfaces for the public system, **vsysa**, and **vsysb**, and add the interfaces to security zones.
3. Configure routes in the public system to divert traffic between networks A and B.
4. Configure routes in **vsysa** and **vsysb** to divert traffic sent from the device to networks A and B.

 Copyright © Huawei Technologies Co., Ltd.

5. Configure security policies in **vsysa** and **vsysb** to permit the traffic between networks A and B.

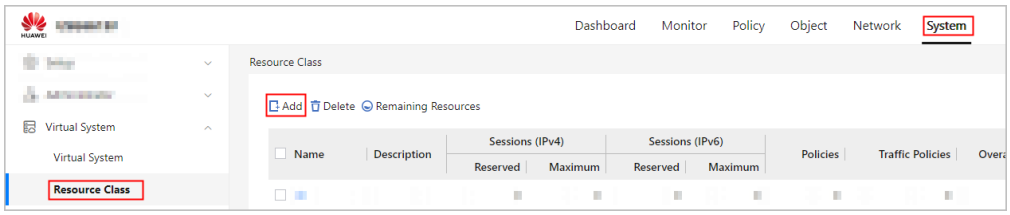
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



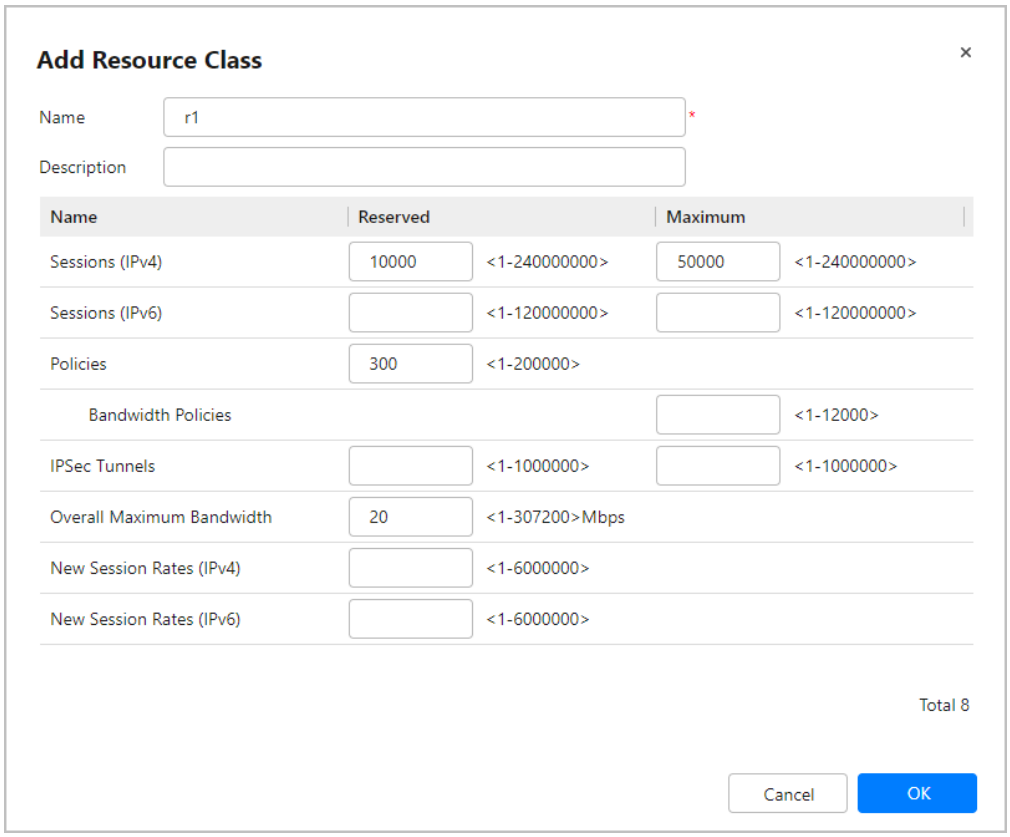
Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



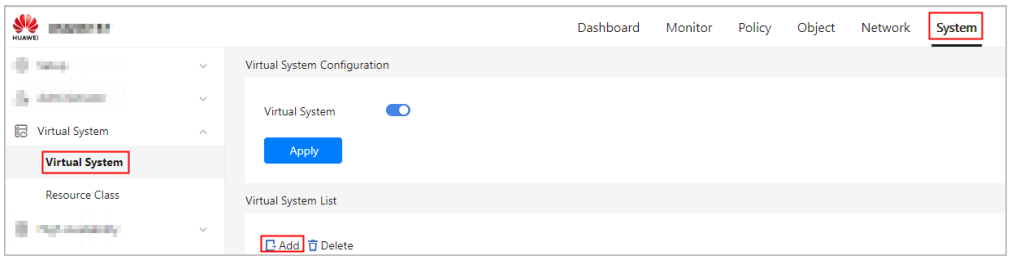
2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

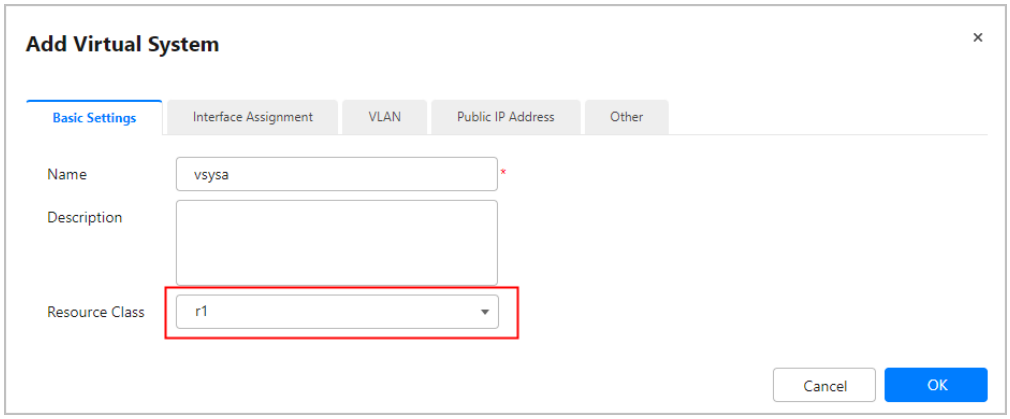


Step 3 In the public system, create virtual system **vsysa** and allocate resources. After completing the configuration, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

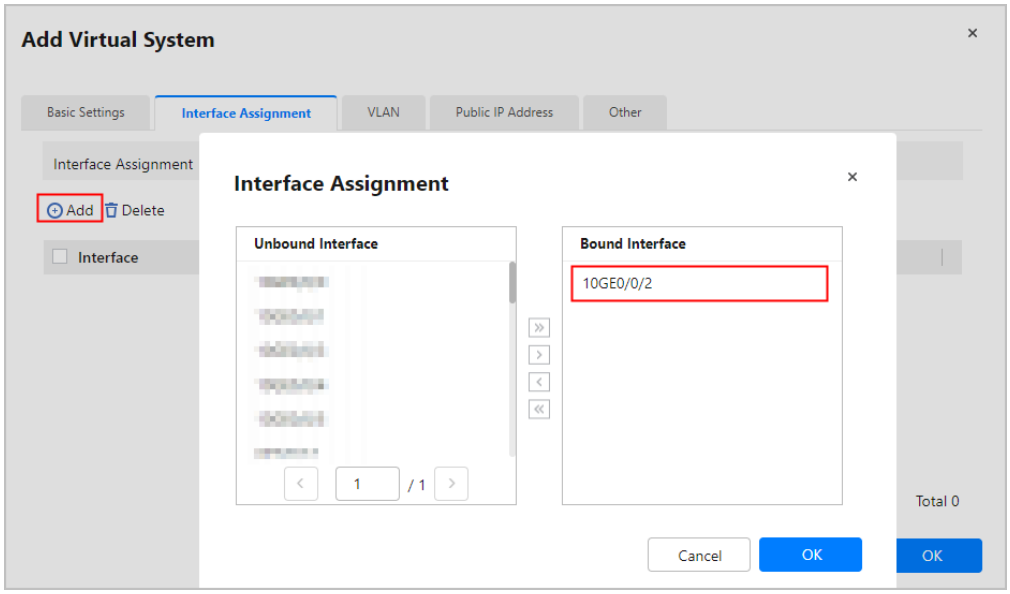


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



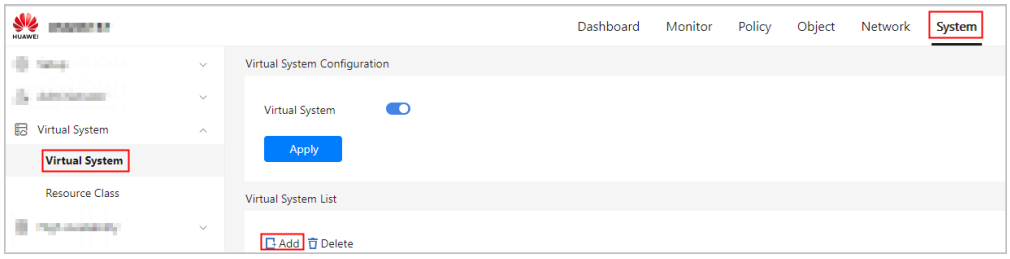
 Copyright © Huawei Technologies Co., Ltd.

3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.

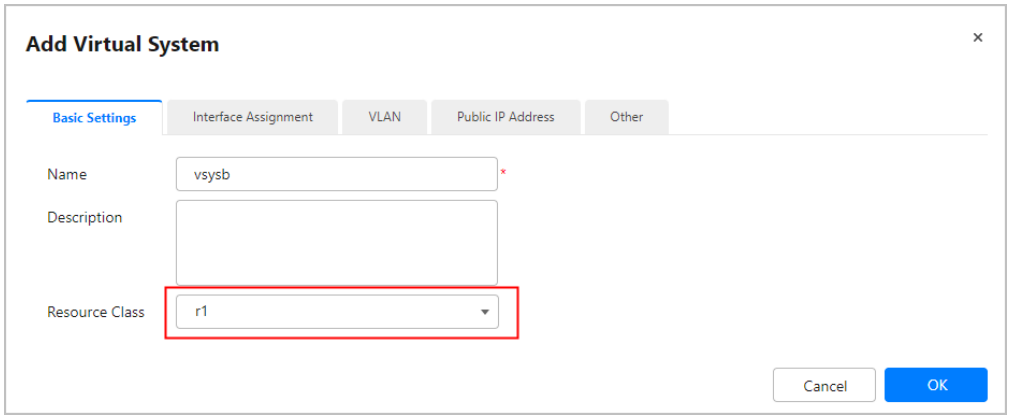


Step 4 In the public system, create virtual system **vsysb** and allocate resources. After completing the configuration, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

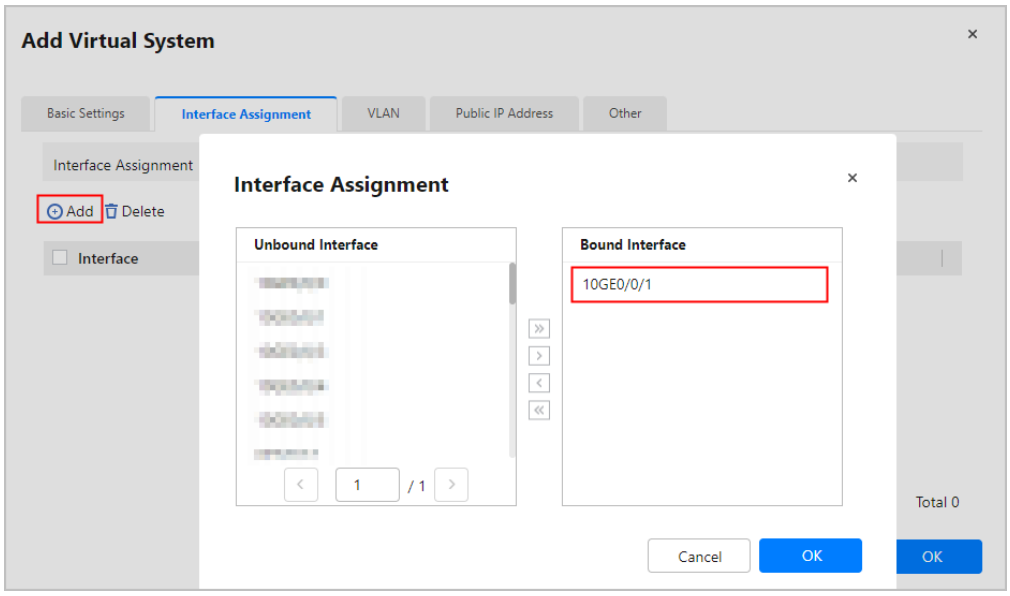


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 Configure the virtual interface Virtual-if0 for the public system and add the interface to a security zone.

1. Choose **Network** > **Interface**.
2. Click corresponding to Virtual-if0 and set the following parameters. After completing the configuration, click **OK**.

Zone	trust
IPv4	
IP Address	172.16.0.1/24

Step 6 Configure routes in the public system.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysa** to **vsysb**, diverting the forward traffic of network A accessing network B to **vsysb**. After completing the configuration, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysa
Destination Address/Mask	10.3.1.0/24
Destination Virtual Router	vsysb

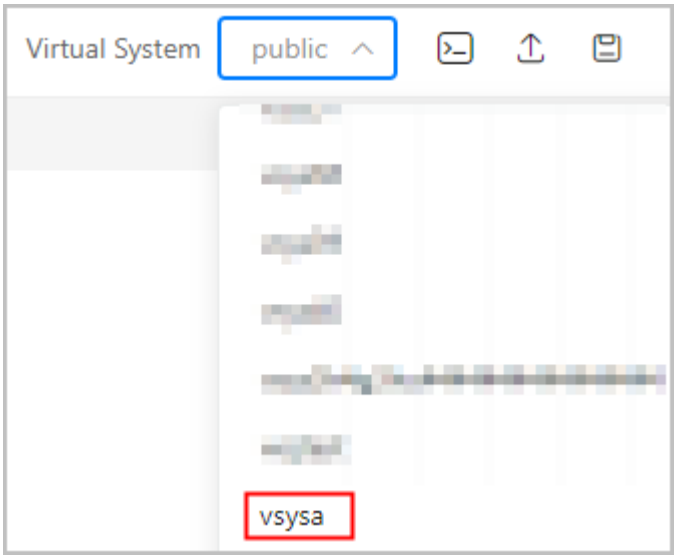
4. Repeat the preceding steps to configure a route from **vsysb** to **vsysa**, diverting the forward traffic of network B accessing network A to **vsysa**.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv4
Source Virtual Router	vsysb
Destination Address/Mask	10.3.0.0/24
Destination Virtual Router	vsysa

Step 7 Set the IP addresses of interfaces in **vsysa** and add the interfaces to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/2 and set the following parameters. After completing the configuration, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps and set the following parameters for Virtual-if1.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 8 Configure security policies in **vsysa**.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network A to network B. After completing the configuration, click **OK**.

Name	vsysa_trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Destination Address	10.3.1.0/24
Action	Permit

3. Repeat the preceding steps to configure an untrust-to-trust security policy to permit traffic from network B to network A.

Name	vsysa_untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Source Address	10.3.1.0/24
Destination Address	10.3.0.0/24
Action	Permit

Step 9 Configure routes in **vsysa**.

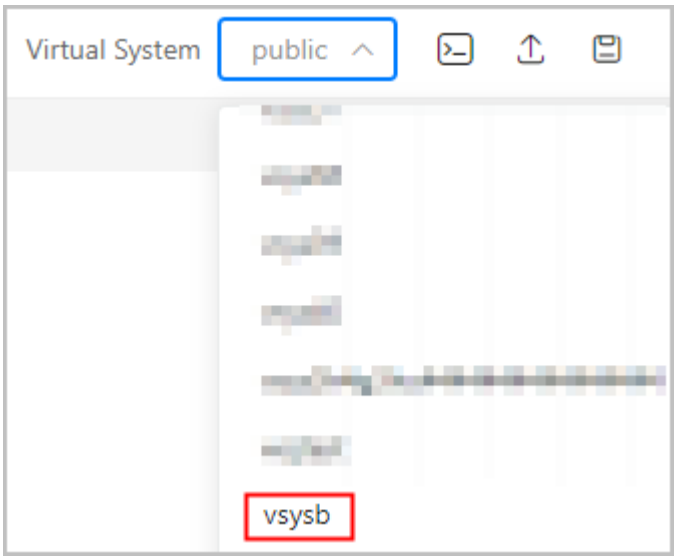
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysa** to network A, diverting the return traffic of network A accessing network B or the forward traffic for network B accessing network A to network A. **10.3.0.254** is the next-hop address of the route from **vsysa** to network A. After completing the configuration, click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.0.0/24
Next Hop	10.3.0.254

Step 10 Set the IP addresses of interfaces in **vsysb** and add the interfaces to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.

 Copyright © Huawei Technologies Co., Ltd.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/1 and set the following parameters. After completing the configuration, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

4. Repeat the preceding steps and set the following parameters for Virtual-if2.

Zone	untrust
IPv4	
IP Address	172.16.2.1/24

Step 11 Configure security policies in **vsysb**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network B to network A. After completing the configuration, click **OK**.

Name	vsysb_trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.1.0/24
Destination Address	10.3.0.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

3. Repeat the preceding steps to configure an untrust-to-trust security policy to permit traffic from network A to network B.

Name	vsysb_untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Source Address	10.3.0.0/24
Destination Address	10.3.1.0/24
Action	Permit

Step 12 Configure routes in **vsysb**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysb** to network B, diverting the forward traffic of network A accessing network B and the return traffic for network B accessing network A to network B. **10.3.1.254** is the next-hop address of the route from **vsysb** to network B. After completing the configuration, click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.1.0/24
Next Hop	10.3.1.254

----End

Verifying the Configuration

Users on network A can proactively access resources on network B, and users on network B can proactively access resources on network A.

In addition, you can view the sessions generated by the device by choosing **Monitor** > **Session Table** of **vsysa** and **vsysb**.

Configuration Scripts

- public

```
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
vsys name vsysb 2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 assign resource-class r1
 assign interface GE0/0/1
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
 ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysb
 ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysa
```

- vsysa

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
```

- vsysb

```
#
interface GE0/0/1
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
set priority 5
 add interface Virtual-if2
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name vsysb_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
rule name vsysb_untrust_to_trust
 source-zone untrust
 destination-zone trust
 source-address 10.3.0.0 mask 255.255.255.0
 destination-address 10.3.1.0 mask 255.255.255.0
 action permit
```

6.5 CLI: Example for Configuring Direct Communication Between Two Virtual Systems

Networking Requirements

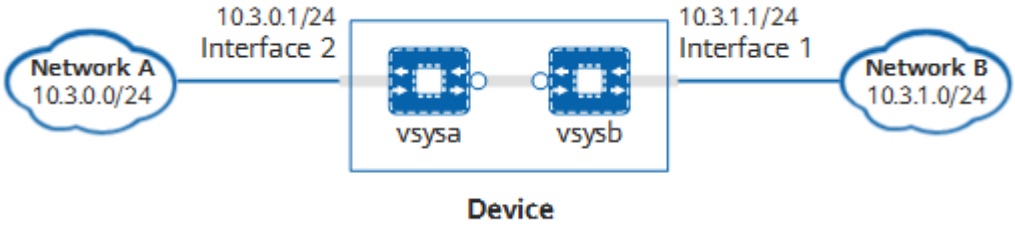
As shown in **Figure 6-5**, the device is deployed between network A and network B. Virtual systems vsysa and vsysb function as network A's gateway and network B's gateway respectively to isolate and protect their respective networks.

You need to configure direct communication between vsysa and vsysb so that networks A and B can communicate with each other.

Figure 6-5 Direct communication between two virtual systems

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual systems vsysa and vsysb, and allocate resources to them.
2. Configure interfaces for vsysa, and vsysb, and add the interfaces to security zones.
3. Configure routes in the public system to divert traffic between networks A and B.
4. Configure routes in vsysa and vsysb to divert traffic sent from the device to networks A and B.
5. Configure security policies in vsysa and vsysb to permit the traffic between networks A and B.

Procedure

Step 1 Enable the virtual system function.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate an interface to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate an interface to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign interface ge 0/0/1
[Device-vsys-vsysb] quit
```

Step 3 Configure routes in the public system.

Configure a route from vsysa to vsysb, diverting the forward traffic of network A accessing network B to vsysb.

```
[Device] ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysb
```

Configure a route from vsysb to vsysa, diverting the forward traffic of network B accessing network A to vsysa.

```
[Device] ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysa
```

Step 4 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 5 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 6 Configure a route in vsysa.

Configure a route from vsysa to network A, diverting the return traffic for network A to access network B or the forward traffic for network B to access network A to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 7 Configure security policies in vsysa.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to network B.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name vsysa_trust_to_untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-zone trust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-zone untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-address 10.3.0.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] action permit
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network B to network A.

```
[Device-vsysa-policy-security] rule name vsysa_untrust_to_trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-zone untrust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-zone trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] action permit
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] quit
[Device-vsysa-policy-security] quit
```

Step 8 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 9 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/1
[Device-vsysb-GE0/0/1] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/1] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/1
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

Step 10 Configure a route in vsysb.

Configure a route from vsysb to network B, diverting the forward traffic for network A to access network B and the return traffic for network B to access network A to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 11 Configure security policies in vsysb.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network B to network A.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name vsysb_trust_to_untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-zone trust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-zone untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] action permit
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network A to network B.

```
[Device-vsysb-policy-security] rule name vsysb_untrust_to_trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-zone untrust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-zone trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-address 10.3.1.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] action permit
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] quit
[Device-vsysb-policy-security] quit
```

----End

Verifying the Configuration

- A user on network A can access network B. In addition, the following sessions are created in vsysa and vsysb.

  NOTE

  In the following command output, 10.3.1.3 is the IP address of the server on network B accessed by the user on network A, and 10.3.0.2 is the IP address of the user host on network A.

  Sessions in vsysa:

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 10.3.1.3
   Current Total Sessions : 1
   icmp  VPN: vsysa --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysa_trust_to_untrust
  ```

  Sessions in vsysb:

  ```
  <Device> display firewall session table verbose vsys vsysb destination global 10.3.1.3
   Current Total Sessions : 1
   icmp  VPN: vsysb --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: GE0/0/1  NextHop: 10.3.1.254  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysb_untrust_to_trust
  ```

- A user on network B can access network A. In addition, the following sessions are created in vsysa and vsysb.

  NOTE

  In the following command output, 10.3.0.3 is the IP address of the server on network A accessed by the user on network B, and 10.3.1.2 is the IP address of the user host on network B.

  Sessions in vsysa:

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 10.3.0.3
   Current Total Sessions : 1
   icmp  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: GE0/0/2  NextHop: 10.3.0.254  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysa_untrust_to_trust
  ```

  Sessions in vsysb:

  ```
  <Device> display firewall session table verbose vsys vsysb destination global 10.3.0.3
   Current Total Sessions : 1
   icmp  VPN: vsysb --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysb_trust_to_untrust
  ```

Configuration Scripts

- Public system (public)

  ```
  #
   sysname Device
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign interface GE0/0/1
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
 ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysb
 ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/1
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
set priority 5
 add interface Virtual-if2
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name vsysb_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name vsysb_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
return
```

6.6 Web: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on Routing Tables

Networking Requirements

As shown in **Figure 6-6**, the device is deployed between network A and network B. Virtual systems **vsysa** and **vsysb** function as network A's gateway and network B's gateway, respectively, to isolate and protect their respective networks. The device connects to the Internet through the public network interface interface 1 of the public system.

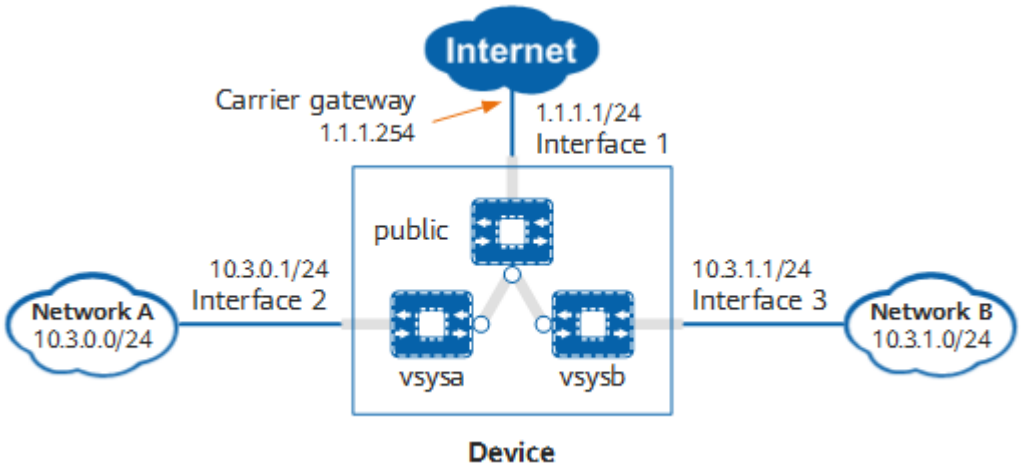
You need to configure communication between **vsysa** and **vsysb** across the public system based on routing tables so that networks A and B can communicate with each other. In addition, you need to configure communication between the public system and **vsysa** and the public system and **vsysb** based on routing tables so that networks A and B can access the Internet.

Figure 6-6 Communication between two virtual systems across the public system based on routing tables

NOTE

In this example, interface 1, interface 2, and interface3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



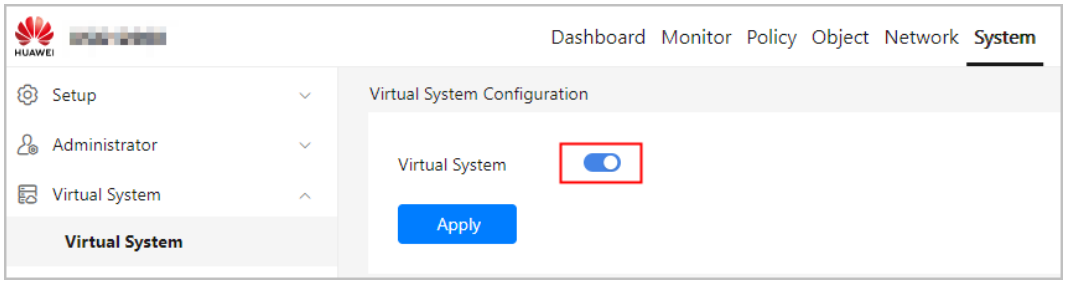
Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual systems **vsysa** and **vsysb**, and allocate resources to them.
2. Configure interfaces for the public system, **vsysa**, and **vsysb**, and add the interfaces to security zones.
3. Configure routes in the public system, **vsysa**, and **vsysb** to divert traffic between network A and network B as well as the traffic from the two networks to the Internet.
4. Configure security policies in the public system, **vsysa**, and **vsysb** to permit traffic between network A and network B as well as the traffic for the two networks to access the Internet.

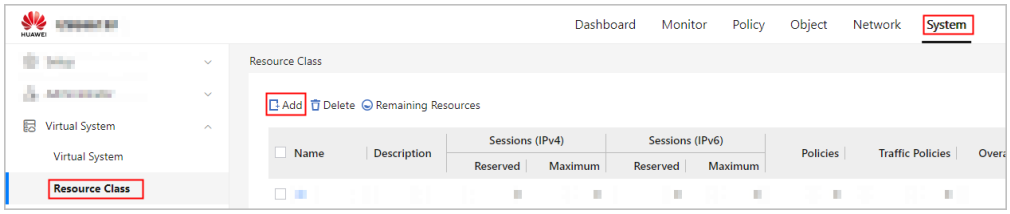
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



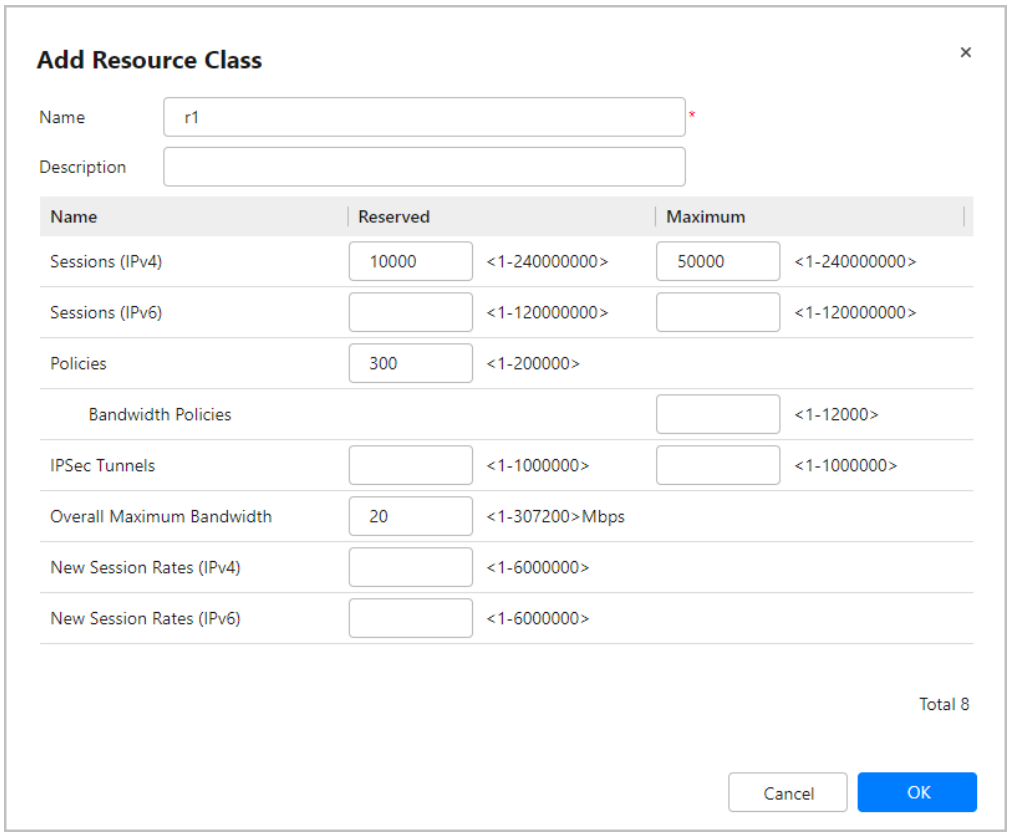
Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



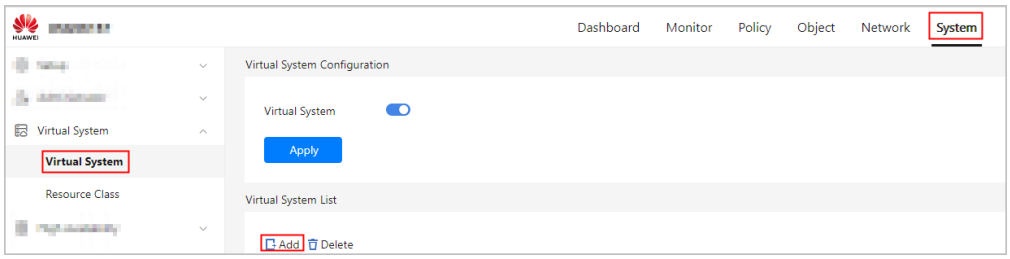
 Copyright © Huawei Technologies Co., Ltd.

2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



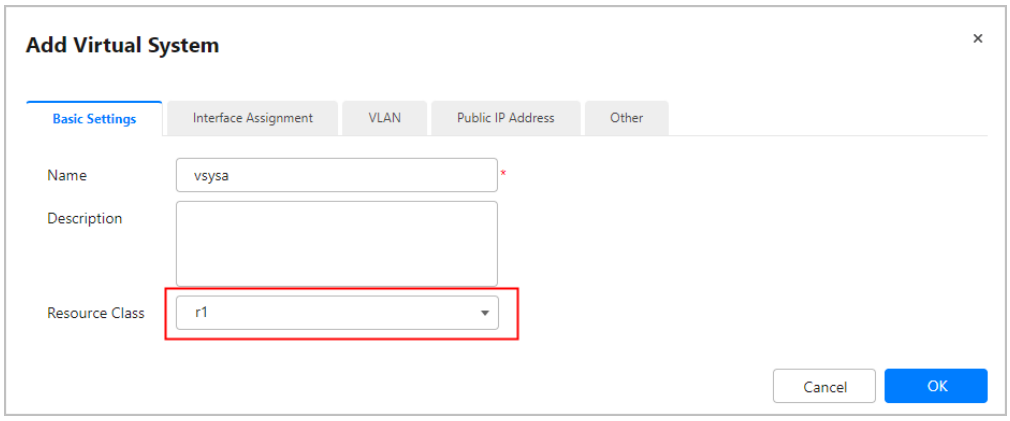
Step 3 In the public system, create virtual system **vsysa** and allocate resources. After completing the configuration, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

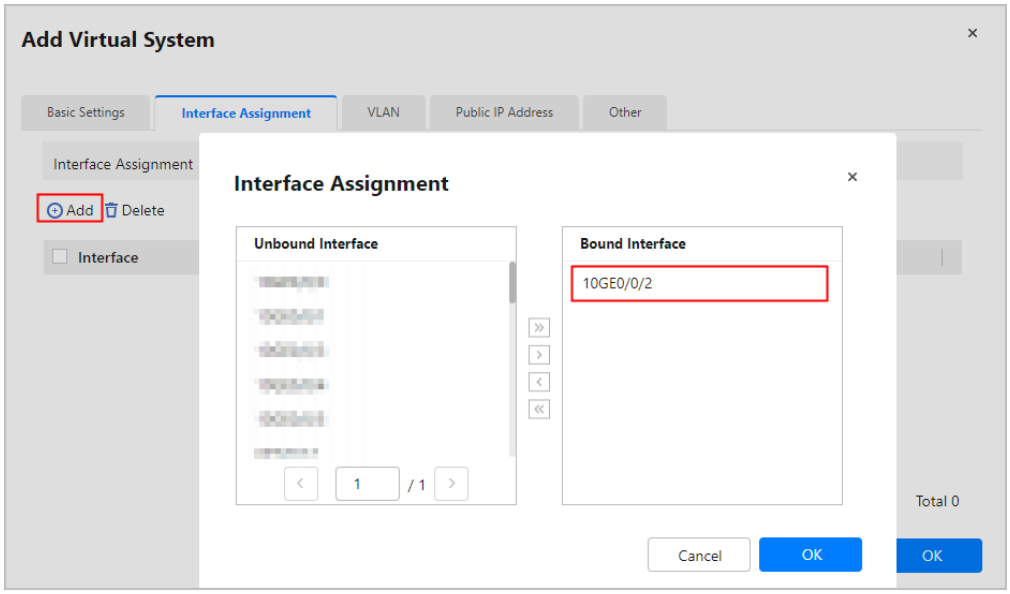


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

 Copyright © Huawei Technologies Co., Ltd.

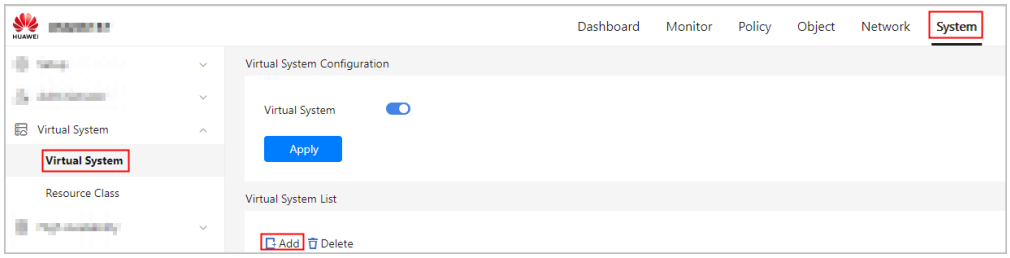


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



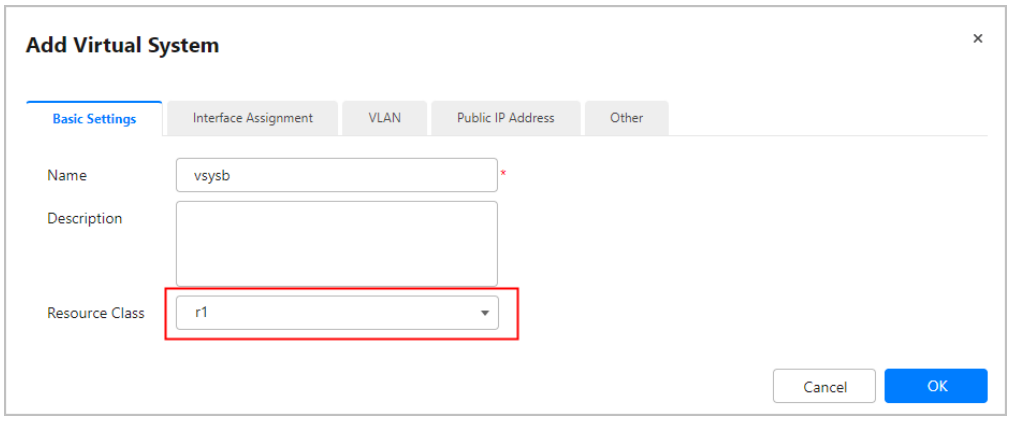
Step 4 In the public system, create virtual system **vsysb** and allocate resources. After completing the configuration, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

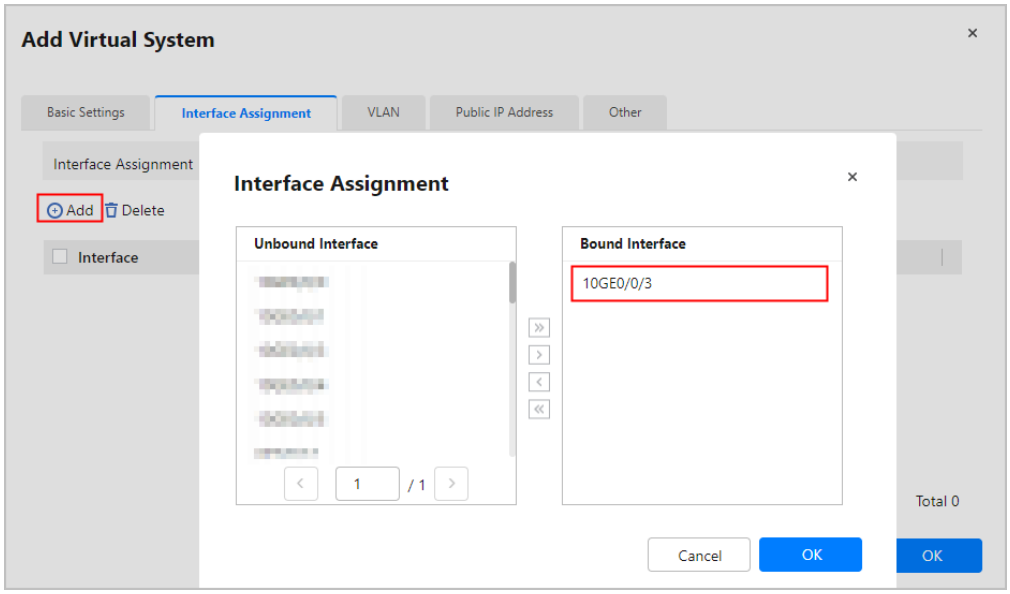


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



Step 5 Configure interfaces for the public system and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE 0/0/1 and set the following parameters. After completing the configuration, click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

3. Repeat the preceding steps and set the following parameters for Virtual-if0.

Zone	trust
IPv4	
IP Address	172.16.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure a security policy in the public system.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network A or B to the Internet. After completing the configuration, click **OK**.

Name	trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24 10.3.1.0/24
Destination Address	1.1.1.0/24
Action	Permit

Step 7 Configure routes in the public system.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the public system to the Internet, diverting the forward traffic from networks A and B to the Internet for access. **1.1.1.254** is the next-hop address of the route from the public system to the Internet. After completing the configuration, click **OK**.

Protocol	IPv4
Destination Address/Mask	0.00.0/0.00.0
Next Hop	1.1.1.254

4. Repeat the preceding steps to configure a route from the public system to **vsysb**, diverting the forward traffic of network A accessing network B to **vsysb.**

Protocol	IPv4
Source Virtual Router	public
Destination Address/Mask	10.3.1.0/24
Destination Virtual Router	vsysb

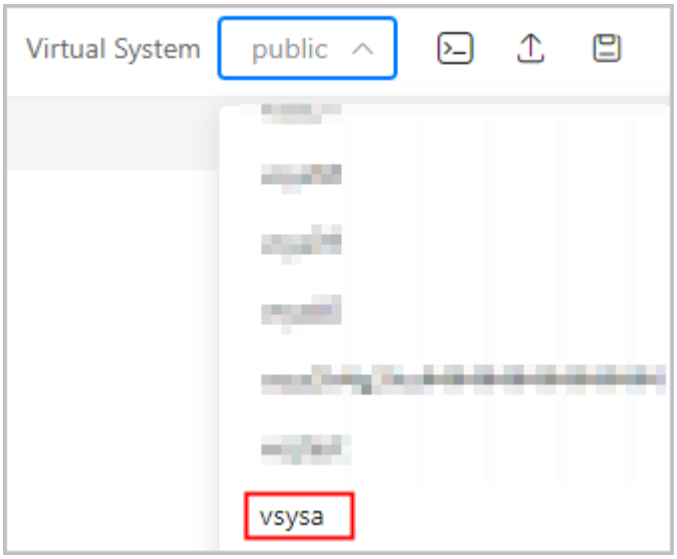
5. Repeat the preceding steps to configure a route from the public system to **vsysa**, diverting the forward traffic of network B accessing network A to **vsysa**.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv4
Source Virtual Router	public
Destination Address/Mask	10.3.0.0/24
Destination Virtual Router	vsysa

Step 8 Set the IP addresses of interfaces in **vsysa** and add the interfaces to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/2 and set the following parameters. After completing the configuration, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps and set the following parameters for Virtual-if1.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 9 Configure security policies in **vsysa**.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network A to network B or to the Internet. After completing the configuration, click **OK**.

Name	vsysa_trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

3. Repeat the preceding steps to configure an untrust-to-trust security policy to permit traffic from network B to network A.

Name	vsysa_untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Source Address	10.3.1.0/24
Destination Address	10.3.0.0/24
Action	Permit

Step 10 Configure a route in **vsysa**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysa** to the public system, diverting the forward traffic of network A accessing network B or the Internet to the public system. After the configuration is complete, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysa
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

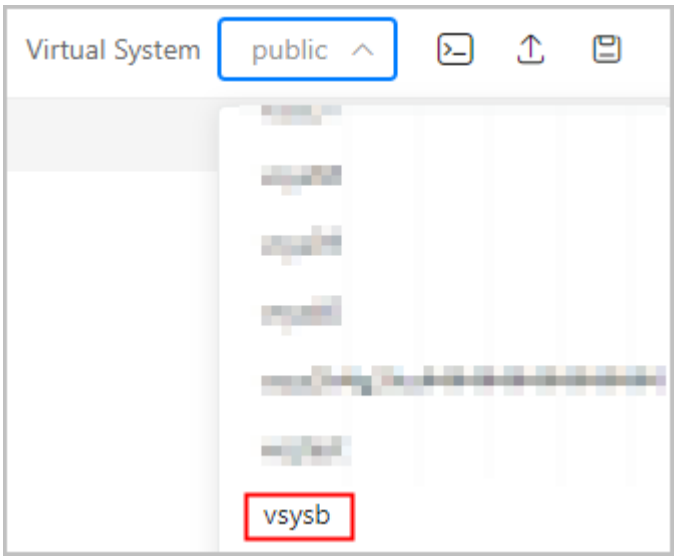
4. Repeat the preceding steps to configure a route from **vsysa** to network A, diverting the forward traffic of network B accessing network A and the return traffic of network A accessing network B to network A. **10.3.0.254** is the next-hop address of the route from **vsysa** to network A.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv4
Destination Address/Mask	10.3.0.0/24
Next Hop	10.3.0.254

Step 11 Set the IP addresses of interfaces in **vsysa** and add the interfaces to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/3 and set the following parameters. After completing the configuration, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

4. Repeat the preceding steps and set the following parameters for Virtual-if2.

Zone	untrust
IPv4	
IP Address	172.16.2.1/24

Step 12 Configure security policies in **vsysb**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy as follows to permit the traffic from network B to network A or the Internet. After completing the configuration, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Name	vsysb_trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.1.0/24
Action	Permit

3. Repeat the preceding steps to configure an untrust-to-trust security policy to permit traffic from network A to network B.

Name	vsysb_untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Source Address	10.3.0.0/24
Destination Address	10.3.1.0/24
Action	Permit

Step 13 Configure routes in **vsysb**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysb** to the public system, diverting the forward traffic of network B accessing network A or the Internet to the public system. After completing the configuration, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysb
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

4. Repeat the preceding steps to configure a route from **vsysb** to network B, diverting the forward traffic of network A accessing network B and the return traffic of network B accessing network A to network B. **10.3.1.254** is the next-hop address of the route from **vsysb** to network B.

Protocol	IPv4
Destination Address/Mask	10.3.1.0/24

 Copyright © Huawei Technologies Co., Ltd.

Next Hop	10.3.1.254

----End

Verifying the Configuration

Users on network A can proactively access network B and the Internet, and users on network B can proactively access network A and the Internet.

In addition, you can view the sessions generated by the device by choosing **Monitor** > **Session Table** of **vsysa** and **vsysb**.

Configuration Scripts

- public

```
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
#
interface GE0/0/1
 ip address 1.1.1.1 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 10.3.1.0 255.255.255.0 vpn-instance vsysb
 ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
```

- vsysa

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
```

- vsysb

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name vsysb_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name vsysb_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

6.7 CLI: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on Routing Tables

Networking Requirements

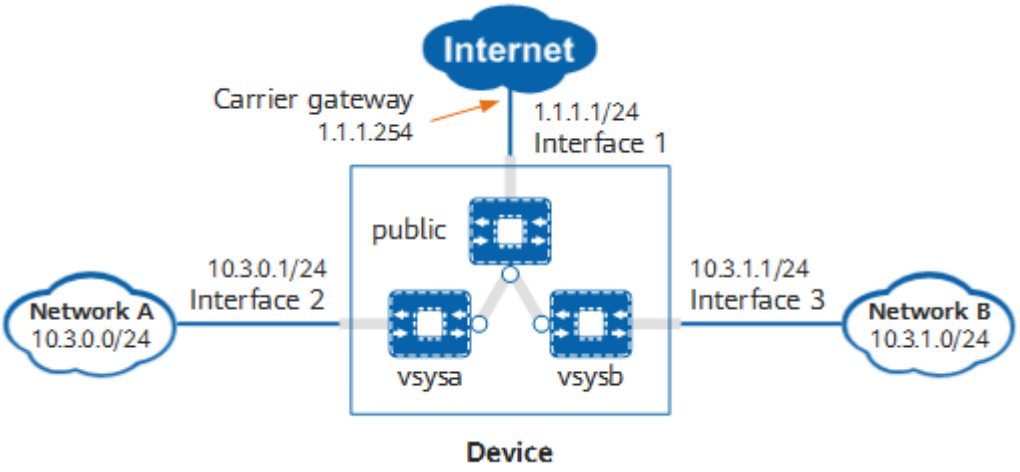
As shown in **Figure 6-7**, the device is deployed between network A and network B. Virtual systems vsysa and vsysb function as network A's gateway and network B's gateway respectively to isolate and protect their respective networks. The device connects to the Internet through the WAN interface interface 1 of the public system.

You need to configure communication between vsysa and vsysb across the public system based on routing tables so that networks A and B can communicate with each other. In addition, you need to configure communication between the public system and vsysa and the public system and vsysb based on routing tables so that networks A and B can access the Internet.

Figure 6-7 Communication between two virtual systems across the public system based on routing tables

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual systems vsysa and vsysb, and allocate resources to them.
2. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure routes in the public system, vsysa, and vsysb to divert traffic between network A and network B as well as the traffic for the two networks to access the Internet.
4. Configure security policies in the public system, vsysa, and vsysb to permit traffic between network A and network B as well as the traffic for the two networks to access the Internet.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate an interface to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate an interface to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] quit
```

Step 3 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 1.1.1.1 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 4 Configure routes in the public system.

Configure a route from the public system to the Internet, diverting the forward traffic of networks A and B accessing the Internet to the Internet. 1.1.1.254 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Configure a route from the public system to vsysb, diverting the forward traffic of network A accessing network B to vsysb.

```
[Device] ip route-static 10.3.1.0 255.255.255.0 vpn-instance vsysb
```

Configure a route from the public system to vsysa, diverting the forward traffic of network B accessing network A to vsysa.

```
[Device] ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
```

Step 5 Configure a security policy in the public system.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A or B to the Internet.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device] security-policy
[Device-policy-security] rule name trust_to_untrust
[Device-policy-security-rule-trust_to_untrust] source-zone trust
[Device-policy-security-rule-trust_to_untrust] destination-zone untrust
[Device-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
[Device-policy-security-rule-trust_to_untrust] source-address 10.3.1.0 24
[Device-policy-security-rule-trust_to_untrust] action permit
[Device-policy-security-rule-trust_to_untrust] quit
```

Step 6 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 7 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 8 Configure routes in vsysa.

Configure a route from vsysa to the public system, diverting the forward traffic of network A accessing network B or the Internet to the public system.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysa to network A, diverting the forward traffic of network B accessing network A and the return traffic of network A accessing network B to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 9 Configure security policies in vsysa.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to network B or the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name vsysa_trust_to_untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-zone trust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-zone untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] action permit
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network B to network A.

```
[Device-vsysa-policy-security] rule name vsysa_untrust_to_trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-zone untrust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-zone trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] action permit
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] quit
[Device-vsysa-policy-security] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 10 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 11 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

Step 12 Configure routes in vsysb.

Configure a route from vsysb to the public system, diverting the forward traffic of network B accessing network A or the Internet to the public system.

```
[Device-vsysb] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysb to network B, diverting the forward traffic of network A accessing network B and the return traffic of network B accessing network A to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 13 Configure security policies in vsysb.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network B to network A or the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name vsysb_trust_to_untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-zone trust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-zone untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] action permit
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network A to network B.

```
[Device-vsysb-policy-security] rule name vsysb_untrust_to_trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-zone untrust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-zone trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] action permit
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] quit
[Device-vsysb-policy-security] quit
```

----End

Verifying the Configuration

- A user on network A can access network B and the Internet. In addition, the following sessions are created in the public system, vsysa, and vsysb.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

10.3.1.3 is the IP address of the server on network B accessed by the user on network A. 3.3.3.3 is the IP address of the server on the Internet accessed by the user on network A. 10.3.0.2 is the IP address of the user host on network A.

Sessions in the public system:

```
<Device> display firewall session table verbose destination global 3.3.3.3
 Current Total Sessions : 1
 icmp  VPN: public --> public  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: GE0/0/1  NextHop: 1.1.1.254  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.0.2:43999 --> 3.3.3.3:2048 PolicyName: trust_to_untrust
```

Sessions in vsysa:

```
<Device> display firewall session table verbose vsys vsysa
 Current Total Sessions : 2
 icmp  VPN: vsysa --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysa_trust_to_untrust

 icmp  VPN: vsysa --> public  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.0.2:43999 --> 3.3.3.3:2048 PolicyName: vsysa_trust_to_untrust
```

Sessions in vsysb:

```
<Device> display firewall session table verbose vsys vsysb destination global 10.3.1.3
 Current Total Sessions : 1
 icmp  VPN: vsysb --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: GE0/0/3  NextHop: 10.3.1.254  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysb_untrust_to_trust
```

- A user on network B can access network A and the Internet. In addition, the following sessions are created in the public system, vsysa, and vsysb.

NOTE

10.3.0.3 is the IP address of the server on network A accessed by the user on network B. 3.3.3.3 is the IP address of the server on the Internet accessed by the user on network A. 10.3.1.2 is the IP address of the user host on network B.

Sessions in the public system:

```
<Device> display firewall session table verbose destination global 3.3.3.3
 Current Total Sessions : 1
 icmp  VPN: public --> public  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: GE0/0/1  NextHop: 1.1.1.254  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 3.3.3.3:2048 PolicyName: trust_to_untrust
```

Sessions in vsysa:

```
<Device> display firewall session table verbose vsys vsysa destination global 10.3.0.3
 Current Total Sessions : 1
 icmp  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: GE0/0/2  NextHop: 10.3.0.254  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysa_untrust_to_trust
```

Sessions in vsysb:

 Copyright © Huawei Technologies Co., Ltd.

```
<Device> display firewall session table verbose vsys vsysb
 Current Total Sessions : 2
 icmp  VPN: vsysb --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysb_trust_to_untrust

 icmp  VPN: vsysb --> public  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 3.3.3.3:2048 PolicyName: vsysb_trust_to_untrust
```

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign interface GE0/0/3
#
interface GE0/0/1
 ip address 1.1.1.1 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 10.3.1.0 255.255.255.0 vpn-instance vsysb
 ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name vsysb_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name vsysb_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
return
```

6.8 CLI: Example for Configuring Communication Between Two Virtual Systems Across the Public System Based on a Traffic Diversion Table

Networking Requirements

As shown in **Figure 6-8**, the device is deployed between network A and network B. Virtual systems vsysa and vsysb function as network A's gateway and network B's gateway respectively to isolate and protect their respective networks. The device

 Copyright © Huawei Technologies Co., Ltd.

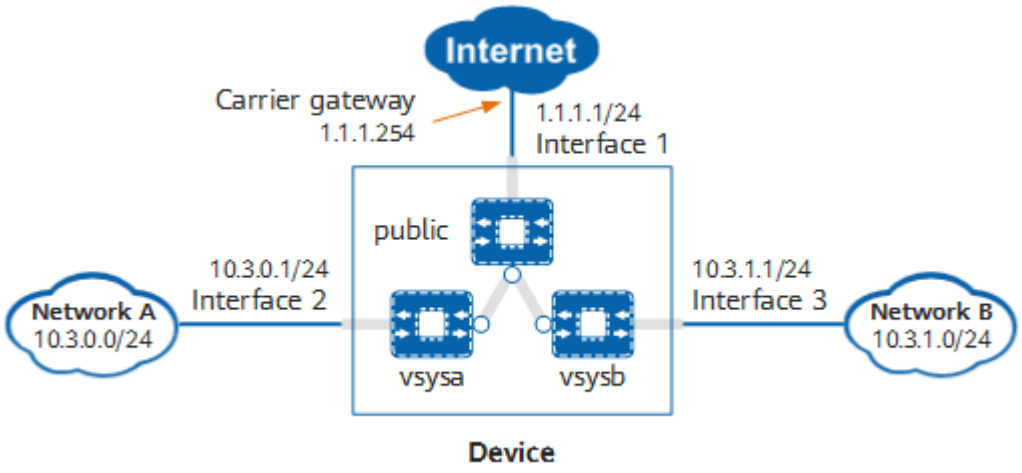
connects to the Internet through the WAN interface interface 1 of the public system.

You need to configure communication between vsysa and vsysb across the public system based on a traffic diversion table so that networks A and B can communicate with each other. In addition, you need to configure communication between the public system and vsysa and the public system and vsysb based on a traffic diversion table so that networks A and B can access the Internet.

Figure 6-8 Communication between two virtual systems across the public system based on a traffic diversion table

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function, create virtual systems vsysa and vsysb, and allocate resources to them.
2. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.
3. Configure a traffic diversion table in the public system to divert traffic between network A and network B as well as the traffic for the two networks to access the Internet.
4. Configure routes in the public system, vsysa, and vsysb to divert traffic sent from the device to network A, network B, and the Internet.
5. Configure security policies in the public system, vsysa, and vsysb to permit traffic between network A and network B as well as the traffic for the two networks to access the Internet.

Procedure

Step 1 Enable the virtual system function.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate an interface to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate an interface to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] quit
```

Step 3 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 1.1.1.1 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 4 Configure traffic diversion tables.

Configure a traffic diversion table for diverting the forward traffic of network B accessing network A or the return traffic of network A accessing network B or the Internet to vsysa.

```
[Device] firewall import-flow public 10.3.0.0 10.3.0.255 vpn-instance vsysa
Warning: The destination of this IP range should be in this vsys network, otherwise it may cause flow loop!
Please select [Y/N]:Y
```

Configure a traffic diversion table for diverting the forward traffic of network A accessing network B or the return traffic of network B accessing network A or the Internet to vsysb.

```
[Device] firewall import-flow public 10.3.1.0 10.3.1.255 vpn-instance vsysb
Warning: The destination of this IP range should be in this vsys network, otherwise it may cause flow loop!
Please select [Y/N]:Y
```

Step 5 Configure a route in the public system.

Configure a route from the public system to the Internet, diverting the forward traffic of networks A and B accessing the Internet to the Internet. 1.1.1.254 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 6 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 7 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 8 Configure routes in vsysa.

Configure a route from vsysa to the public system, diverting the forward traffic of network A accessing network B or the Internet to the public system.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysa to network A, diverting the forward traffic of network B accessing network A and the return traffic of network A accessing network B to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 9 Configure security policies in vsysa.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to network B or the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name vsysa_trust_to_untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-zone trust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-zone untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] action permit
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network B to network A.

```
[Device-vsysa-policy-security] rule name vsysa_untrust_to_trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-zone untrust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-zone trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] action permit
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] quit
[Device-vsysa-policy-security] quit
```

Step 10 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 11 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

Step 12 Configure routes in vsysb.

Configure a route from vsysb to the public system, diverting the forward traffic of network B accessing network A or the Internet to the public system.

```
[Device-vsysb] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysb to network B, diverting the forward traffic of network A accessing network B and the return traffic of network B accessing network A to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 13 Configure security policies in vsysb.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network B to network A or the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name vsysb_trust_to_untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-zone trust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-zone untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] action permit
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network A to network B.

```
[Device-vsysb-policy-security] rule name vsysb_untrust_to_trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-zone untrust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-zone trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] action permit
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] quit
[Device-vsysb-policy-security] quit
```

----End

Verifying the Configuration

- A user on network A can access network B and the Internet. In addition, the following sessions are created in vsysa and vsysb and no session is created in the public system.

  NOTE

  10.3.1.3 is the IP address of the server on network B accessed by the user on network A. 3.3.3.3 is the IP address of the server on the Internet accessed by the user on network A. 10.3.0.2 is the IP address of the user host on network A.

  Sessions in vsysa:

```
<Device> display firewall session table verbose vsys vsysa
 Current Total Sessions : 2
 icmp  VPN: vsysa --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysa_trust_to_untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
icmp  VPN: vsysa --> public  ID: xxxxxxxxxxxxxxxxxxxxx
Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
<--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
10.3.0.2:43999 --> 3.3.3.3:2048 PolicyName: vsysa_trust_to_untrust
```

Sessions in vsysb:

```
<Device> display firewall session table verbose vsys vsysb destination global 10.3.1.3
 Current Total Sessions : 1
 icmp  VPN: vsysb --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: GE0/0/3  NextHop: 10.3.1.254  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysb_untrust_to_trust
```

- A user on network B can access network A and the Internet. In addition, the following sessions are created in vsysa and vsysb and no session is created in the public system.

  NOTE

  10.3.0.3 is the IP address of the server on network A accessed by the user on network B. 3.3.3.3 is the IP address of the server on the Internet accessed by the user on network A. 10.3.1.2 is the IP address of the user host on network B.

  Sessions in vsysa:

```
<Device> display firewall session table verbose vsys vsysa destination global 10.3.0.3
 Current Total Sessions : 1
 icmp  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: GE0/0/2  NextHop: 10.3.0.254  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysa_untrust_to_trust
```

  Sessions in vsysb:

```
<Device> display firewall session table verbose vsys vsysb
 Current Total Sessions : 2
 icmp  VPN: vsysb --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysb_trust_to_untrust

 icmp  VPN: vsysb --> public  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
 Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
 <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
 10.3.1.2:43999 --> 3.3.3.3:2048 PolicyName: vsysb_trust_to_untrust
```

- On the device, you can view the traffic diversion table configuration of virtual systems or the traffic diversion table of a specified IP address on networks.

  View the traffic diversion table configuration of vsysa or the traffic diversion table of a specified IP address on network A.

```
<Device> display firewall import-flow public vpn-instance vsysa
 Import Flow Tables:
 firewall import-flow public 10.3.0.0 10.3.0.255 vpn-instance vsysa
 ------------------------------------------------------------------------
 Total:1
<Device> display firewall import-flow public 10.3.0.1
 Import Flow Tables:
 Source Instance   Destination Address   Destination Instance
 ------------------------------------------------------------------------------------------------
 public            10.3.0.1              vsysa
 ------------------------------------------------------------------------------------------------
 Total:1
```

  View the traffic diversion table configuration of vsysb or the traffic diversion table of a specified IP address on network B.

 Copyright © Huawei Technologies Co., Ltd.

```
<Device> display firewall import-flow public vpn-instance vsysb
 Import Flow Tables:
 firewall import-flow public 10.3.1.0 10.3.1.255 vpn-instance vsysb
 ------------------------------------------------------------------------
 Total:1
<Device> display firewall import-flow public 10.3.1.1
 Import Flow Tables:
 Source Instance   Destination Address   Destination Instance
 ------------------------------------------------------------------------------------------------------
 public            10.3.1.1              vsysb
 ------------------------------------------------------------------------------------------------------
 Total:1
```

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign interface GE0/0/3
#
interface GE0/0/1
 ip address 1.1.1.1 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 firewall import-flow public 10.3.0.0 10.3.0.255 vpn-instance vsysa
 firewall import-flow public 10.3.1.0 10.3.1.255 vpn-instance vsysb
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone trust
 destination-zone untrust
 source-address 10.3.0.0 mask 255.255.255.0
 action permit
rule name vsysa_untrust_to_trust
 source-zone untrust
 destination-zone trust
 source-address 10.3.1.0 mask 255.255.255.0
 destination-address 10.3.0.0 mask 255.255.255.0
 action permit
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name vsysb_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name vsysb_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
return
```

6.9 CLI: Example for Configuring Communication Between Two Virtual Systems Across Another Virtual System

Networking Requirements

As shown in **Figure 6-9**, the device is deployed between network A and network B. Virtual systems vsysa and vsysb function as network A's gateway and network B's gateway respectively to isolate and protect their respective networks. The device connects to a LAN through interface 1 of vsysc.

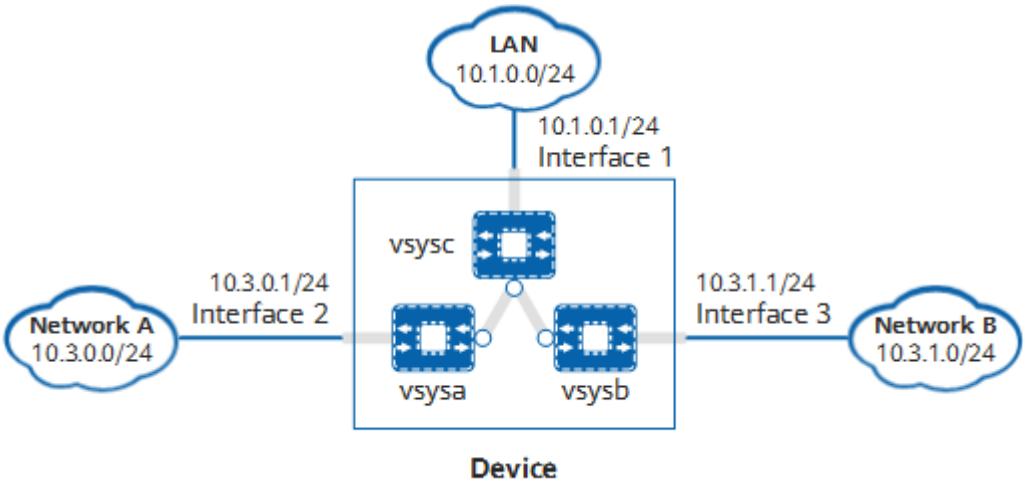
You need to configure communication between vsysa and vsysb across vsysc so that networks A and B can communicate with each other. In addition, you need to configure communication between vsysa and vsysc and between vsysb and vsysc so that networks A and B can access the LAN.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-9 Communication between two virtual systems across another virtual system

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function and configure the extended communication mode.
2. Create virtual systems vsysa, vsysb, and vsysc and allocate resources to them.
3. Configure interfaces for vsysa, vsysb, and vsysc, and add the interfaces to security zones.
4. Configure routes in the public system to divert traffic between network A and network B as well as the traffic for the two networks to access the LAN.
5. Configure routes in the vsysa, vsysb, and vsysc to divert traffic sent from the device to network A, network B, and the LAN.
6. Configure security policies in vsysa, vsysb, and vsysc to permit traffic between network A and network B as well as the traffic for the two networks to access the LAN.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure the extended communication mode.

```
[Device] firewall forward cross-vsys extended
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate an interface to it.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate an interface to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] quit
```

Create virtual system vsysc and allocate an interface to it.

```
[Device] vsys name vsysc
[Device-vsys-vsysc] assign interface ge 0/0/1
[Device-vsys-vsysc] quit
```

Step 4 Configure routes in the public system.

Configure a route from vsysa to vsysc, diverting the forward traffic of network A accessing network B to vsysc.

```
[Device] ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysc
```

Configure a route from vsysa to vsysc, diverting the forward traffic of network A accessing the LAN to vsysc.

```
[Device] ip route-static vpn-instance vsysa 10.1.0.0 255.255.255.0 vpn-instance vsysc
```

Configure a route from vsysb to vsysc, diverting the forward traffic of network B accessing network A to vsysc.

```
[Device] ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysc
```

Configure a route from vsysb to vsysc, diverting the forward traffic of network B accessing the LAN to vsysc.

```
[Device] ip route-static vpn-instance vsysb 10.1.0.0 255.255.255.0 vpn-instance vsysc
```

Configure a route from vsysc to vsysa, diverting the forward traffic of network B accessing network A to vsysa.

```
[Device] ip route-static vpn-instance vsysc 10.3.0.0 255.255.255.0 vpn-instance vsysa
```

Configure a route from vsysc to vsysb, diverting the forward traffic of network A accessing network B to vsysb.

```
[Device] ip route-static vpn-instance vsysc 10.3.1.0 255.255.255.0 vpn-instance vsysb
```

Step 5 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 6 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 7 Configure a route in vsysa.

 Copyright © Huawei Technologies Co., Ltd.

Configure a route from vsysa to network A, diverting the forward traffic of network B accessing network A and the return traffic of network A accessing network B or the LAN to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 8 Configure security policies in vsysa.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network A to network B or the LAN.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name vsysa_trust_to_untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-zone trust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-zone untrust
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] source-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] destination-address 10.1.0.0 24
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] action permit
[Device-vsysa-policy-security-rule-vsysa_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network B to network A.

```
[Device-vsysa-policy-security] rule name vsysa_untrust_to_trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-zone untrust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-zone trust
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] source-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] action permit
[Device-vsysa-policy-security-rule-vsysa_untrust_to_trust] quit
[Device-vsysa-policy-security] quit
```

Step 9 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 10 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

Step 11 Configure a route in vsysb.

Configure a route from vsysb to network B, diverting the forward traffic of network A accessing network B and the return traffic of network B accessing network A or the LAN to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 12 Configure security policies in vsysb.

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy for the Trust-to-Untrust interzone, permitting traffic from network B to network A or the LAN.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name vsysb_trust_to_untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-zone trust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-zone untrust
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] source-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] destination-address 10.1.0.0 24
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] action permit
[Device-vsysb-policy-security-rule-vsysb_trust_to_untrust] quit
```

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from network A to network B.

```
[Device-vsysb-policy-security] rule name vsysb_untrust_to_trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-zone untrust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-zone trust
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] source-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] destination-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] action permit
[Device-vsysb-policy-security-rule-vsysb_untrust_to_trust] quit
[Device-vsysb-policy-security] quit
```

Step 13 Switch to the system view of vsysc.

```
[Device-vsysb] quit
<Device-vsysb> quit
[Device] switch vsys vsysc
<Device-vsysc> system-view
```

Step 14 Configure interfaces for vsysc and add the interfaces to security zones.

```
[Device-vsysc] interface ge 0/0/1
[Device-vsysc-GE0/0/1] ip address 10.1.0.1 24
[Device-vsysc-GE0/0/1] quit
[Device-vsysc] interface Virtual-if 3
[Device-vsysc-Virtual-if2] ip address 172.16.3.1 24
[Device-vsysc-Virtual-if2] quit
[Device-vsysc] firewall zone trust
[Device-vsysc-zone-trust] add interface ge 0/0/1
[Device-vsysc-zone-trust] quit
[Device-vsysc] firewall zone untrust
[Device-vsysc-zone-untrust] add interface Virtual-if 3
[Device-vsysc-zone-untrust] quit
```

Step 15 Configure a route in vsysc.

Configure a route from vsysc to the LAN, diverting the forward traffic of networks A and B accessing the LAN to the LAN. 10.1.0.254 is the next-hop address of the route from vsysc to the LAN.

```
[Device-vsysc] ip route-static 10.1.0.0 255.255.255.0 10.1.0.254
```

Step 16 Configure security policies in vsysc.

Configure a security policy for the Untrust-to-Trust interzone, permitting traffic from networks A and B to the LAN.

```
[Device-vsysc] security-policy
[Device-vsysc-policy-security] rule name vsysc_untrust_to_trust
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] source-zone untrust
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] destination-zone trust
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] source-address 10.3.0.0 24
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] source-address 10.3.1.0 24
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] destination-address 10.1.0.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] action permit
[Device-vsysc-policy-security-rule-vsysc_untrust_to_trust] quit
```

----End

Verifying the Configuration

- A user on network A can access network B and the LAN. In addition, the following sessions are created in vsysa, vsysb, and vsysc.

  NOTE

  10.3.1.3 is the IP address of the server on network B accessed by the user on network A. 10.1.0.3 is the IP address of the server on the LAN accessed by the user on network A. 10.3.0.2 is the IP address of the user host on network A.

  Sessions in vsysa:

  ```
  <Device> display firewall session table verbose vsys vsysa
   Current Total Sessions : 2
   icmp  VPN: vsysa --> vsysc  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysa_trust_to_untrust

   icmp  VPN: vsysa --> vsysc  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: Virtual-if1  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.1.0.3:2048 PolicyName: vsysa_trust_to_untrust
  ```

  Sessions in vsysb:

  ```
  <Device> display firewall session table verbose vsys vsysb destination global 10.3.1.3
   Current Total Sessions : 1
   icmp  VPN: vsysb --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: GE0/0/3  NextHop: 10.3.1.254  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: vsysb_untrust_to_trust
  ```

  Sessions in vsysc:

  ```
  <Device> display firewall session table verbose vsys vsysc
   Current Total Sessions : 2
   icmp  VPN: vsysc --> vsysb  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: untrust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: Virtual-if3  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.3.1.3:2048 PolicyName: -

   icmp  VPN: vsysc --> vsysc  ID: xxxxxxxxxxxxxxxxxxxxx
   Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
   Interface: GE0/0/1  NextHop: 10.1.0.254  MAC: xxxx-xxxx-xxxx
   <--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
   10.3.0.2:43999 --> 10.1.0.3:2048 PolicyName: vsysc_untrust_to_trust
  ```

- A user on network B can access network A and the LAN. In addition, the following sessions are created in vsysa, vsysb, and vsysc.

  NOTE

  10.3.0.3 is the IP address of the server on network A accessed by the user on network B. 10.1.0.3 is the IP address of the server on the LAN accessed by the user on network B. 10.3.1.2 is the IP address of the user host on network B.

  Sessions in vsysa:

  ```
  <Device> display firewall session table verbose vsys vsysa destination global 10.3.0.3
   Current Total Sessions : 1
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
icmp  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
Interface: GE0/0/2  NextHop: 10.3.0.254  MAC: xxxx-xxxx-xxxx
<--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysa_untrust_to_trust
```

Sessions in vsysb:

```
<Device> display firewall session table verbose vsys vsysb
Current Total Sessions : 2
icmp  VPN: vsysb --> vsysc  ID: xxxxxxxxxxxxxxxxxxxxx
Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
<--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: vsysb_trust_to_untrust

icmp  VPN: vsysb --> vsysc  ID: xxxxxxxxxxxxxxxxxxxxx
Zone: trust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
Interface: Virtual-if2  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
<--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
10.3.1.2:43999 --> 10.1.0.3:2048 PolicyName: vsysb_trust_to_untrust
```

Sessions in vsysc:

```
<Device> display firewall session table verbose vsys vsysc
Current Total Sessions : 2
icmp  VPN: vsysc --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
Zone: untrust --> untrust  TTL: xx:xx:xx  Left: xx:xx:xx
Interface: Virtual-if3  NextHop: 0.0.0.0  MAC: xxxx-xxxx-xxxx
<--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
10.3.1.2:43999 --> 10.3.0.3:2048 PolicyName: -

icmp  VPN: vsysc --> vsysc  ID: xxxxxxxxxxxxxxxxxxxxx
Zone: untrust --> trust  TTL: xx:xx:xx  Left: xx:xx:xx
Interface: GE0/0/1  NextHop: 10.1.0.254  MAC: xxxx-xxxx-xxxx
<--packets: xxx bytes: xxx --> packets: xxx bytes: xxx
10.3.1.2:43999 --> 10.1.0.3:2048 PolicyName: vsysc_untrust_to_trust
```

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
 firewall forward cross-vsys extended
#
vsys name vsysa 1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign interface GE0/0/3
#
vsys name vsysc 3
 assign interface GE0/0/1
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
 ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysc
 ip route-static vpn-instance vsysa 10.1.0.0 255.255.255.0 vpn-instance vsysc
 ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysc
 ip route-static vpn-instance vsysb 10.1.0.0 255.255.255.0 vpn-instance vsysc
 ip route-static vpn-instance vsysc 10.3.0.0 255.255.255.0 vpn-instance vsysa
 ip route-static vpn-instance vsysc 10.3.1.0 255.255.255.0 vpn-instance vsysb
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name vsysa_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  destination-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name vsysa_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
set priority 5
 add interface Virtual-if2
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name vsysb_trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name vsysb_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

- Virtual system (vsysc)

```
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
#
interface Virtual-if 3
 ip address 172.16.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
set priority 5
 add interface Virtual-if3
#
 ip route-static 10.1.0.0 255.255.255.0 10.1.0.254
#
security-policy
 rule name vsysc_untrust_to_trust
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
#
return
```

6.10 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through Independent Public Network Interfaces of the Virtual Systems

Networking Requirements

In **Figure 6-10**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and therefore cannot communicate with each other.

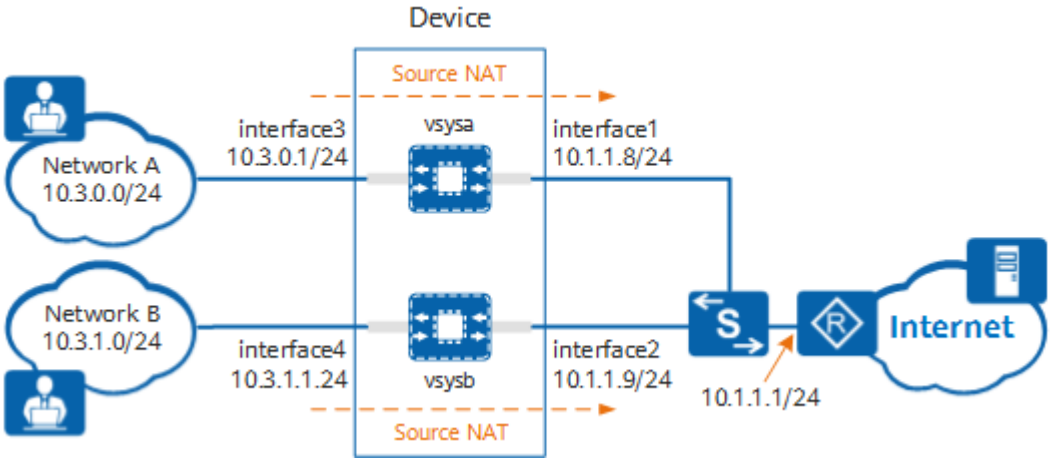
User hosts on network A access the Internet through interface 1 (independent public network interface) of vsysa, and user hosts on network B access the Internet through interface 2 (independent public network interface) of vsysb. On network A, only some user hosts can access the Internet. On network B, all user hosts can access the Internet. In addition, source NAT is performed in the two virtual systems separately to translate the source IP addresses of the packets from the intranet to the Internet into the public IP addresses of the device. In this way, the intranet IP addresses are hidden.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-10 Configuring intranet users of virtual systems to access the Internet through independent public network interfaces of the virtual systems

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/4, respectively.



Item	Data	Description
vsysa	Virtual system name: vsysa Public network interface: GE0/0/1 Public network interface IP address: 10.1.1.8/24 Security zone to which the public network interface belongs: Untrust Private network interface: GE0/0/3 Private network interface IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the private network interface belongs: Trust IP addresses allowed to access the Internet: 10.3.0.2 to 10.3.0.10	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb Public network interface: GE0/0/2 Public network interface IP address: 10.1.1.9/24 Security zone to which the public network interface belongs: Untrust Private network interface: GE0/0/4 Private network interface IP address: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the private network interface belongs: Trust	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

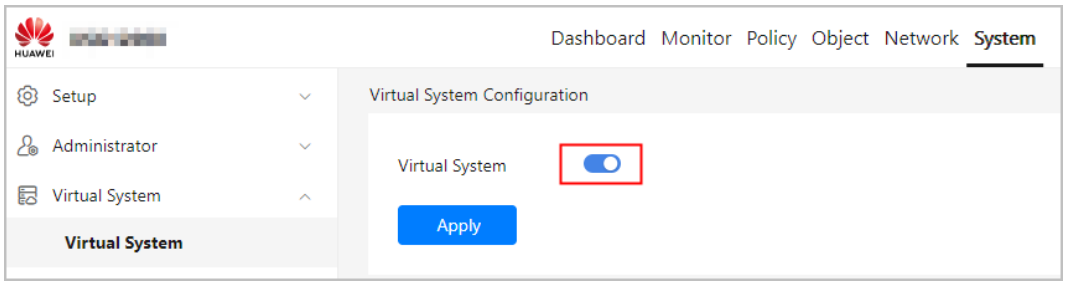
The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for vsysa and vsysb, and add the interfaces to security zones.
4. Configure routes in vsysa and vsysb to divert traffic from networks A and B to the Internet.
5. Configure security policies in vsysa and vsysb based on service requirements to permit traffic from user hosts on networks A and B to the Internet.
6. Configure source NAT policies in vsysa and vsysb to translate the source IP addresses of the packets from the intranet to the Internet into the IP addresses of the independent public network interfaces of the virtual systems.

Procedure

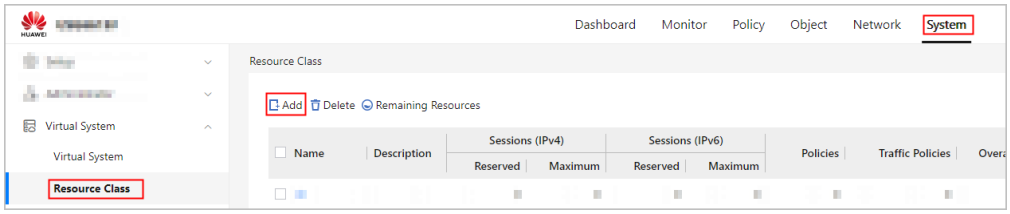
Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.

 Copyright © Huawei Technologies Co., Ltd.

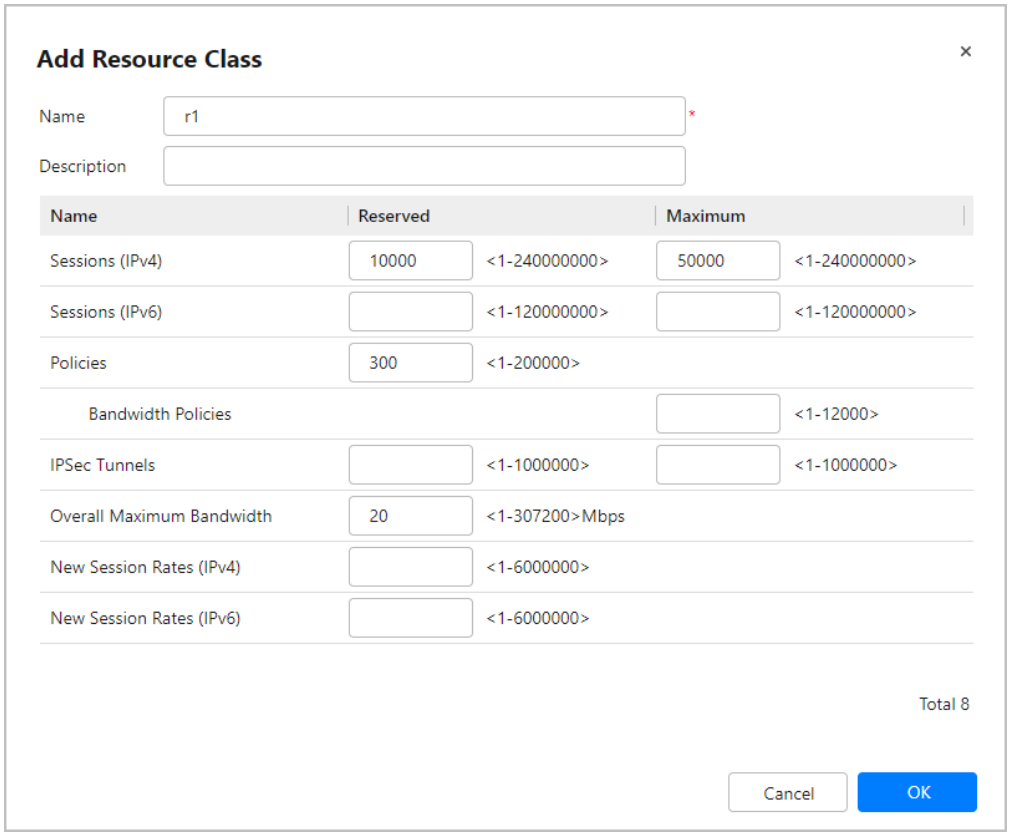


Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



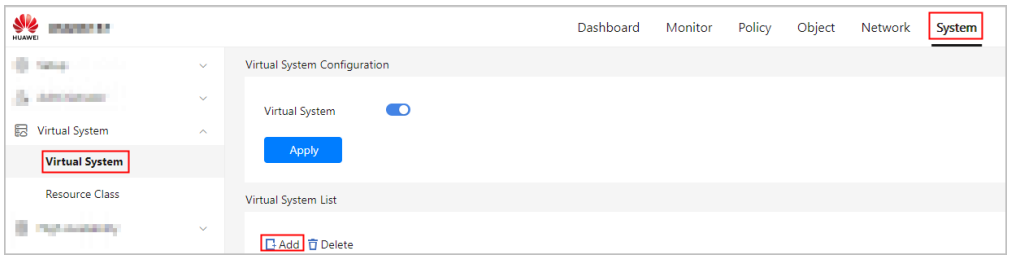
2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



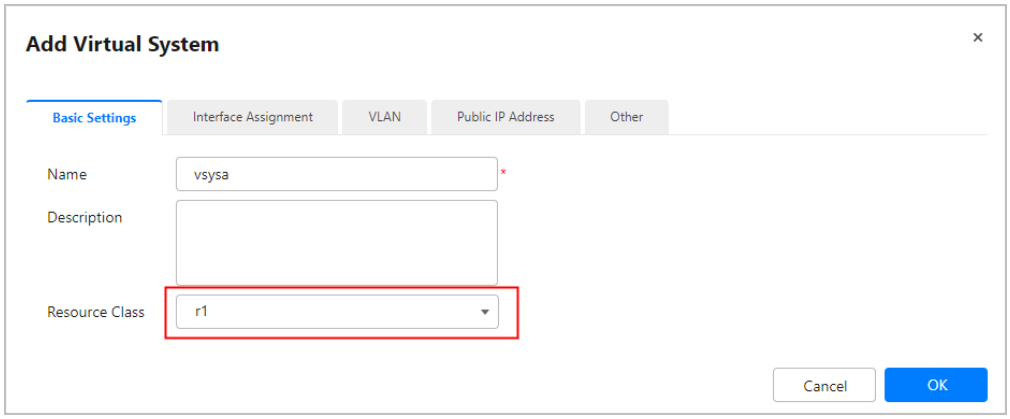
Step 3 In the public system, create virtual system vsysa and allocate resources to it. Click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

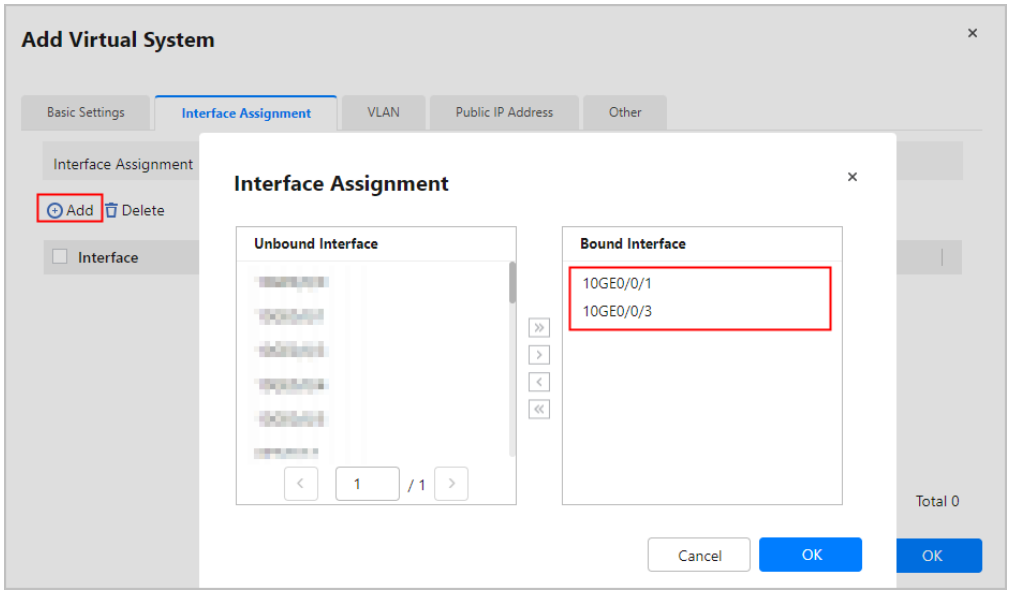
 Copyright © Huawei Technologies Co., Ltd.



2. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

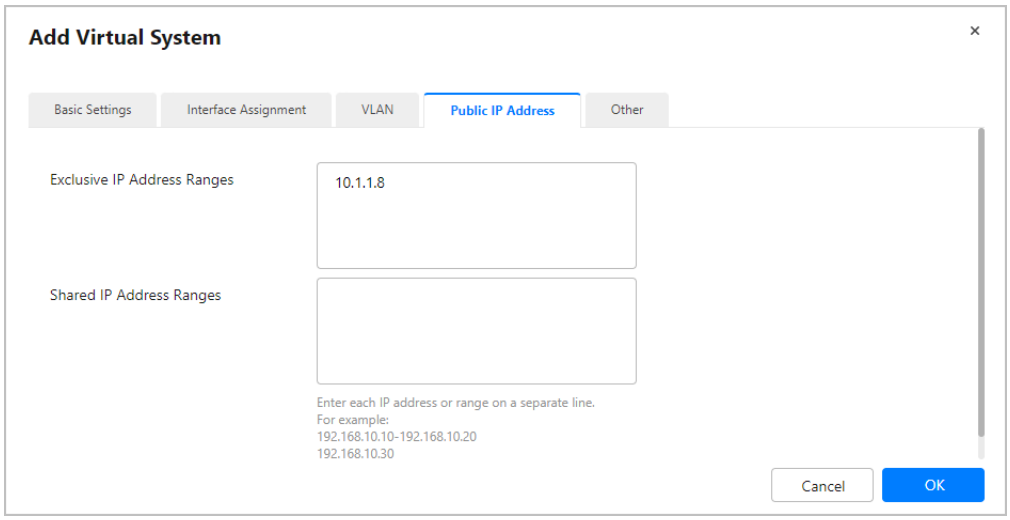


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



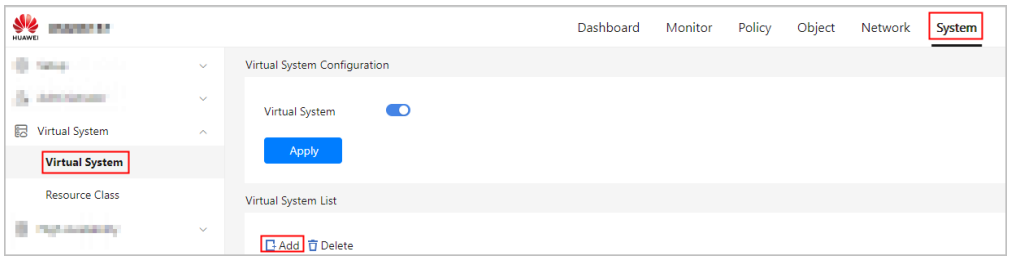
4. Click the **Public IP Address** tab, allocate public IP address to the virtual system.

 Copyright © Huawei Technologies Co., Ltd.

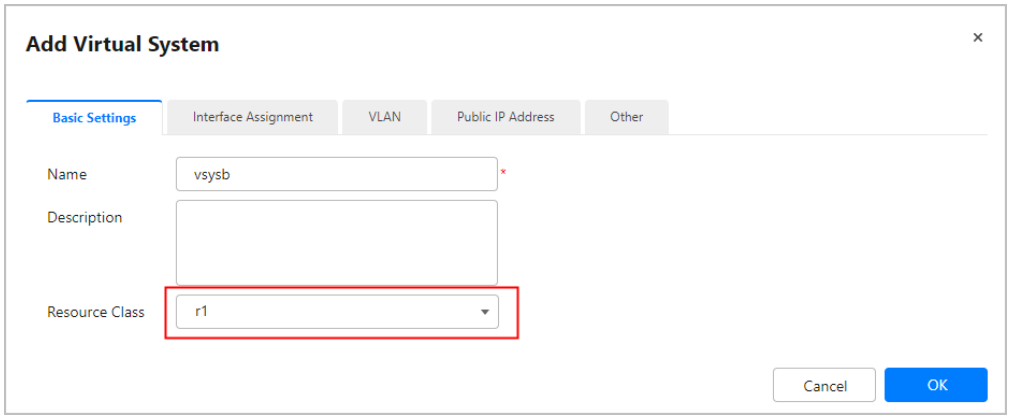


Step 4 In the public system, create virtual system vsysb and allocate resources to it. Click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

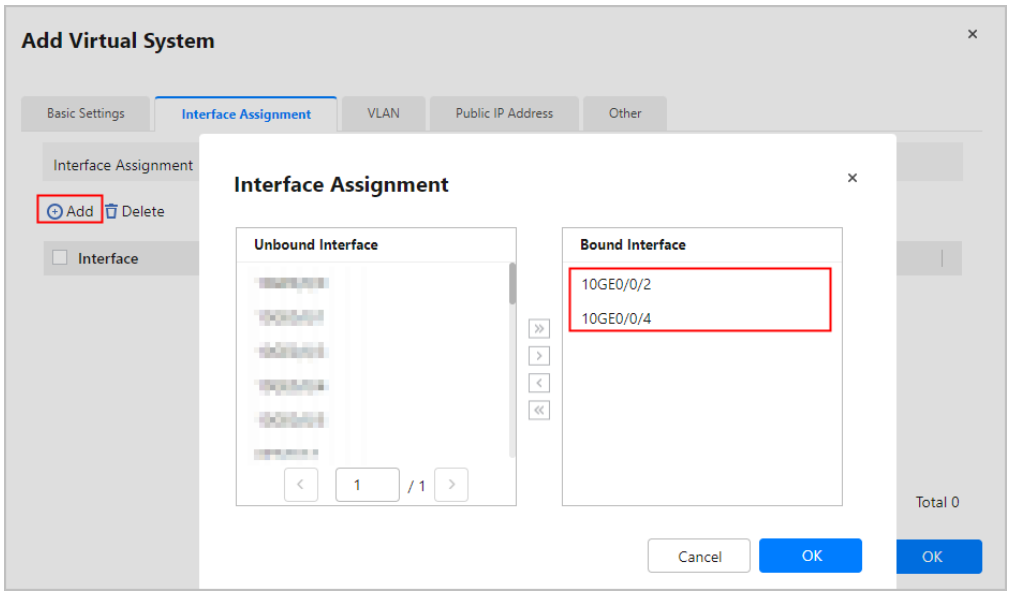


2. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

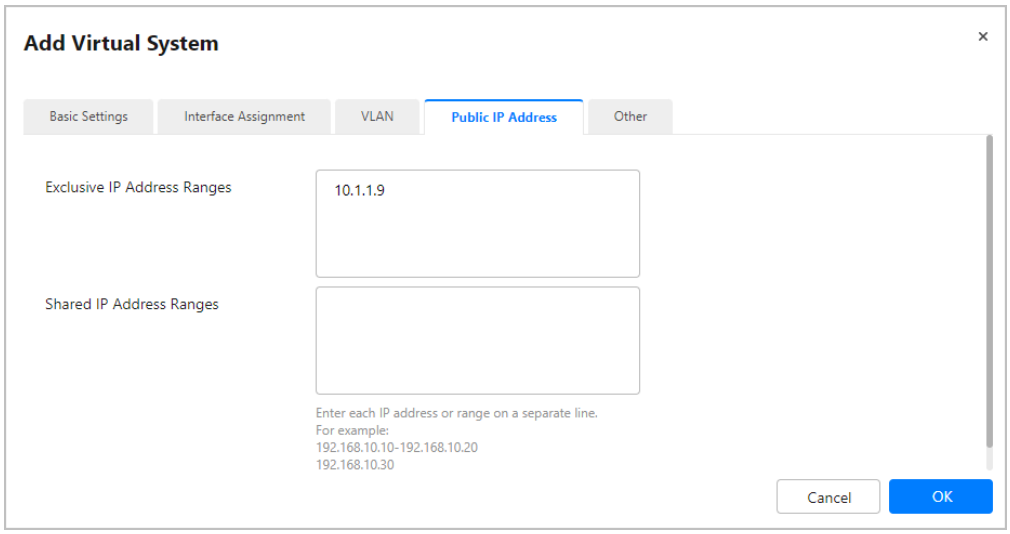


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



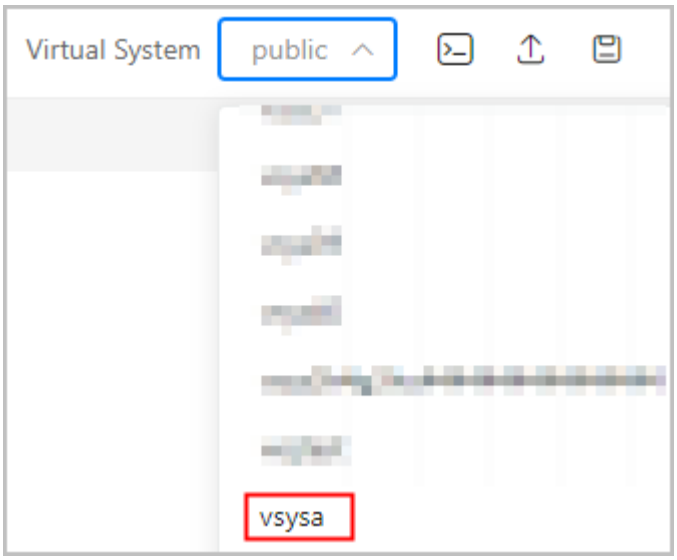
4. Click the **Public IP Address** tab, allocate public IP address to the virtual system.



Step 5 In vsysa, add GE0/0/1 and GE0/0/3 to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access vsysa.

 Copyright © Huawei Technologies Co., Ltd.



2. Choose **Network** > **Interface**.
3. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.1.8/24

4. Repeat the preceding steps to set the parameters for GE0/0/3.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

Step 6 Configure security policies in vsysa.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a Trust-to-Untrust interzone policy to allow user hosts on network segment 10.3.0.2 to 10.3.0.10 on network A to access the Internet. Click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.2-10.3.0.10
Action	Permit

3. Repeat the preceding steps to configure a Trust-to-Untrust interzone policy to prevent other user hosts on network segment 10.3.0.2 to 10.3.0.10 on network A from accessing the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Name	to_internet_block
Source Zone	trust
Destination Zone	untrust
Action	Deny

Step 7 Configure routes in vsysa.

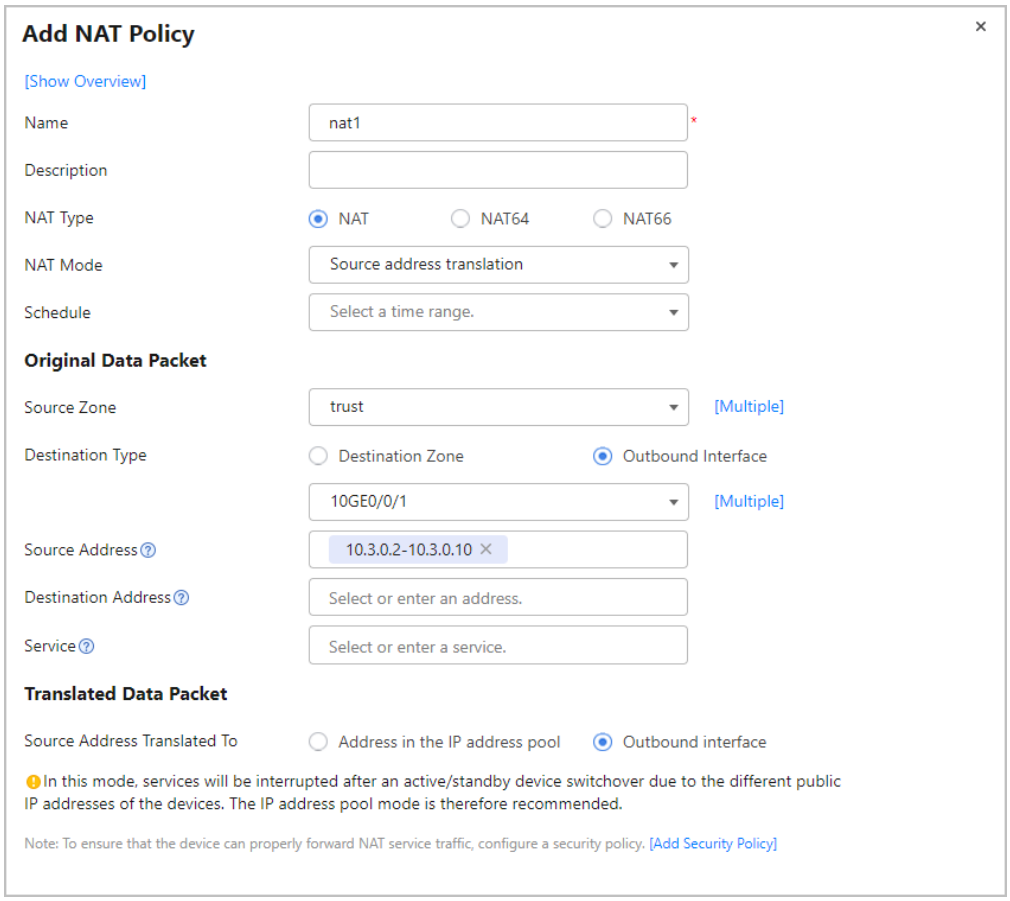
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a static route from network A to the Internet. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

Step 8 Configure a NAT policy in vsysa.

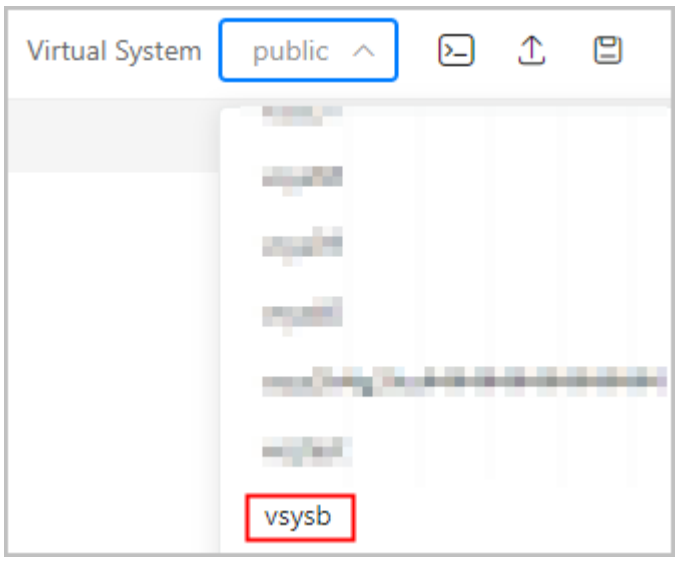
1. Choose **Policy** > **NAT Policy** > **NAT Policy**.
2. On the **NAT Policy** tab page, click **Add**.
3. Configure a source NAT policy to translate the source IP addresses of the packets from network A to the Internet into the IP address of the independent public network interface GE0/0/1 of vsysa. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 9 In vsysb, add GE0/0/2 and GE0/0/4 to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access vsysb.



2. Choose **Network** > **Interface**.
3. Click for GE0/0/2 and set the parameters as follows. Click **OK**.

Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.1.1.9/24

4. Repeat the preceding steps to set the parameters for GE0/0/4.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

Step 10 Configure security policies in vsysb.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a Trust-to-Untrust interzone policy to allow all user hosts on network B to access the Internet. Click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.1.0/24
Action	Permit

Step 11 Configure routes in vsysb.

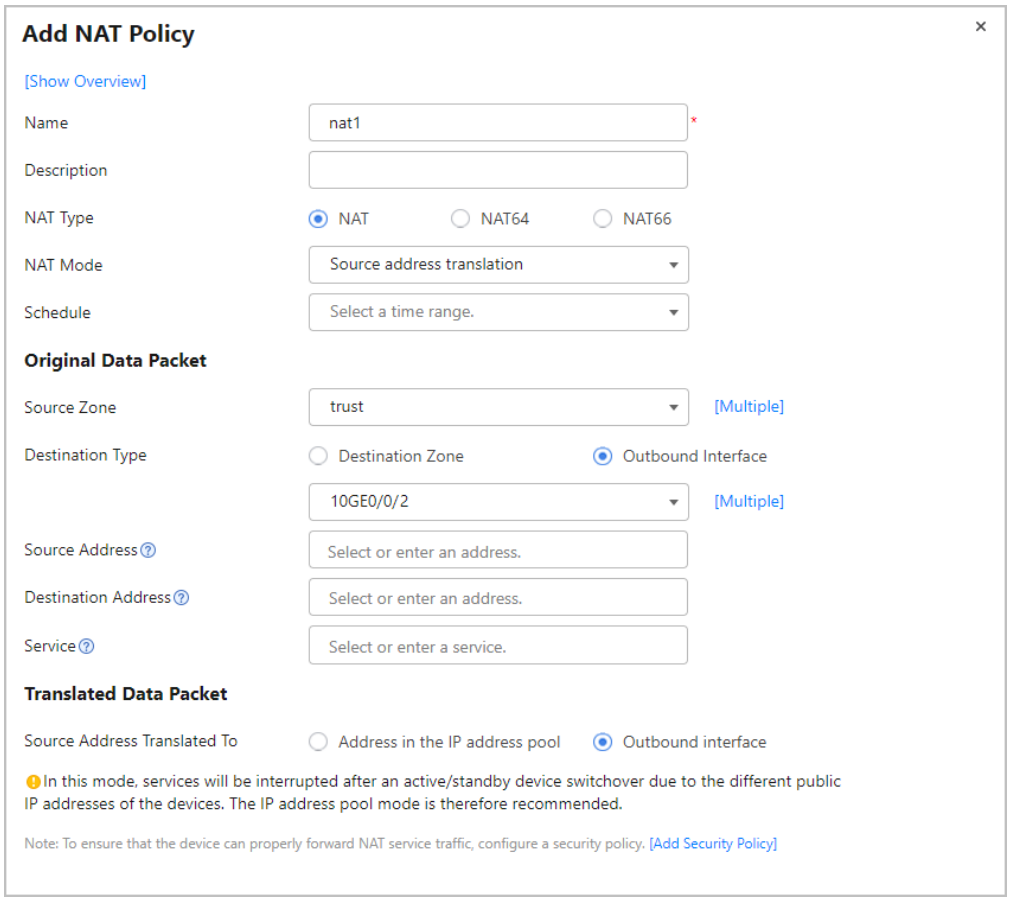
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a static route from network B to the Internet. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

Step 12 Configure a NAT policy in vsysb.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.
2. On the **NAT Policy** tab page, click **Add**.
3. Configure a source NAT policy to translate the source IP addresses of the packets from network B to the Internet into the IP address of the independent public network interface GE0/0/2 of vsysb. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



----End

Verifying the Configuration

- User hosts on network segment 10.3.0.2 to 10.3.0.10 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B can access the Internet.

Configuration Scripts

- public

```
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/1
 assign interface GE0/0/3
 assign global-ip 10.1.1.8 10.1.1.8 exclusive
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/2
 assign interface GE0/0/4
 assign global-ip 10.1.1.9 10.1.1.9 exclusive
```

 Copyright © Huawei Technologies Co., Ltd.

- vsysa

```
#
interface GE0/0/1
 ip address 10.1.1.8 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.0.2 10.3.0.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
nat-policy
 rule name nat1
  source-zone trust
  egress-interface GE0/0/1
  source-address range 10.3.0.2 10.3.0.10
  action source-nat easy-ip
```

- vsysb

```
#
interface GE0/0/2
 ip address 10.1.1.9 255.255.255.0
#
interface GE0/0/4
 ip address 10.3.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name nat1
  source-zone trust
  egress-interface GE0/0/2
  source-address 10.3.1.0 mask 255.255.255.0
  action source-nat easy-ip
```

 Copyright © Huawei Technologies Co., Ltd.

6.11 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through Independent WAN Interfaces of the Virtual Systems

Networking Requirements

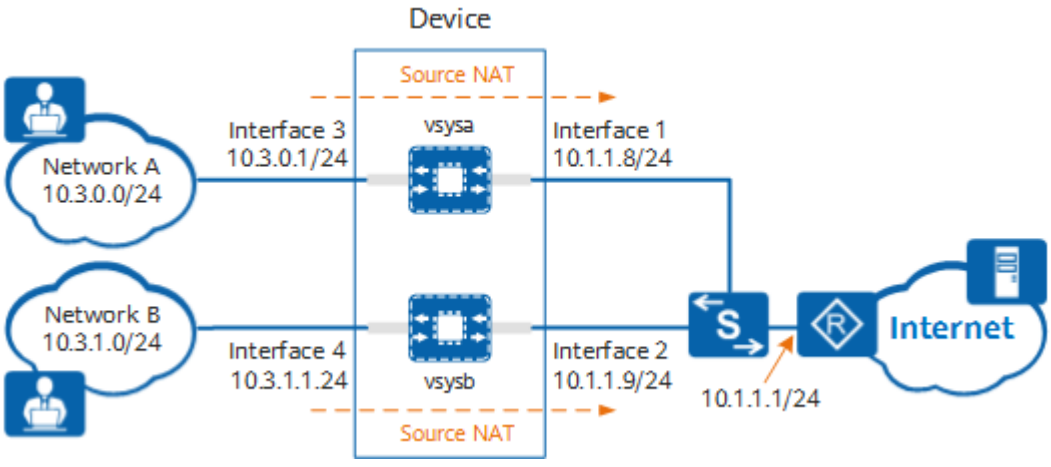
As shown in **Figure 6-11**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and therefore cannot communicate with each other.

User hosts on network A access the Internet through the independent WAN interface interface 1 of vsysa, and user hosts on network B access the Internet through the independent WAN interface interface 2 of vsysb. On network A, only some user hosts can access the Internet. On network B, all user hosts can access the Internet. In addition, source NAT is performed in the two virtual systems separately to translate the source IP addresses of the packets from the intranet to the Internet into the public IP addresses of the device. In this way, the intranet IP addresses are hidden.

Figure 6-11 Configuring intranet users of virtual systems to access the Internet through independent WAN interfaces of the virtual systems

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysa	Virtual system name: vsysa WAN interface: GE 0/0/1 WAN interface IP address: 10.1.1.8/24 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the LAN interface belongs: Trust IP addresses allowed to access the Internet: 10.3.0.2 to 10.3.0.10	-
vsysb	Virtual system name: vsysb WAN interface: GE 0/0/2 WAN interface IP address: 10.1.1.9/24 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/4 LAN interface IP address: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the LAN interface belongs: Trust	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for vsysa and vsysb, and add the interfaces to security zones.

 Copyright © Huawei Technologies Co., Ltd.

4. Configure routes in vsysa and vsysb to divert traffic from networks A and B to the Internet.
5. Configure security policies in vsysa and vsysb based on service requirements to permit traffic from user hosts on networks A and B to the Internet.
6. Configure source NAT policies in vsysa and vsysb to translate the source IP addresses of the packets from the intranet to the Internet into the IP addresses of the independent WAN interfaces of the virtual systems.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/1
[Device-vsys-vsysa] assign interface ge 0/0/3
[Device-vsys-vsysa] assign global-ip 10.1.1.8 10.1.1.8 exclusive
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/2
[Device-vsys-vsysb] assign interface ge 0/0/4
[Device-vsys-vsysb] assign global-ip 10.1.1.9 10.1.1.9 exclusive
[Device-vsys-vsysb] quit
```

Step 4 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 5 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/1
[Device-vsysa-GE0/0/1] ip address 10.1.1.8 24
[Device-vsysa-GE0/0/1] quit
[Device-vsysa] interface ge 0/0/3
[Device-vsysa-GE0/0/3] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/3] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/3
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface ge 0/0/1
[Device-vsysa-zone-untrust] quit
```

Step 6 Configure a static route from network A to the Internet.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Configure security policies for the traffic from network A to the Internet.

Allow user hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A to access the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_internet_allow
[Device-vsysa-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_allow] source-address range 10.3.0.2 10.3.0.10
[Device-vsysa-policy-security-rule-to_internet_allow] action permit
[Device-vsysa-policy-security-rule-to_internet_allow] quit
```

Forbid user hosts that are not in the IP address range of 10.3.0.2 to 10.3.0.10 on network A from accessing the Internet.

```
[Device-vsysa-policy-security] rule name to_internet_block
[Device-vsysa-policy-security-rule-to_internet_block] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_block] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_block] action deny
[Device-vsysa-policy-security-rule-to_internet_block] quit
[Device-vsysa-policy-security] quit
```

Step 8 Configure a source NAT policy to translate the source IP addresses of the packets from network A to the Internet into the IP address of the independent WAN interface GE 0/0/1 of vsysa.

```
[Device-vsysa] nat-policy
[Device-vsysa-policy-nat] rule name nat1
[Device-vsysa-policy-nat-rule-nat1] source-zone trust
[Device-vsysa-policy-nat-rule-nat1] egress-interface ge 0/0/1
[Device-vsysa-policy-nat-rule-nat1] source-address range 10.3.0.2 10.3.0.10
[Device-vsysa-policy-nat-rule-nat1] action source-nat easy-ip
[Device-vsysa-policy-nat-rule-nat1] quit
[Device-vsysa-policy-nat] quit
```

Step 9 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 10 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/2
[Device-vsysb-GE0/0/2] ip address 10.1.1.9 24
[Device-vsysb-GE0/0/2] quit
[Device-vsysb] interface ge 0/0/4
[Device-vsysb-GE0/0/4] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/4] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/4
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface ge 0/0/2
[Device-vsysb-zone-untrust] quit
```

Step 11 Configure a static route from network B to the Internet.

```
[Device-vsysb] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

Step 12 Configure a security policy for the network B-to-Internet interzone, allowing all user hosts on network B to access the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_internet_allow
[Device-vsysb-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysb-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysb-policy-security-rule-to_internet_allow] source-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-to_internet_allow] action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysb-policy-security-rule-to_internet_allow] quit
[Device-vsysb-policy-security] quit
```

Step 13 Configure a source NAT policy to translate the source IP addresses of the packets from network B to the Internet into the IP address of the independent WAN interface GE 0/0/2 of vsysb.

```
[Device-vsysb] nat-policy
[Device-vsysb-policy-nat] rule name nat1
[Device-vsysb-policy-nat-rule-nat1] source-zone trust
[Device-vsysb-policy-nat-rule-nat1] egress-interface ge 0/0/2
[Device-vsysb-policy-nat-rule-nat1] action source-nat easy-ip
[Device-vsysb-policy-nat-rule-nat1] quit
[Device-vsysb-policy-nat] quit
```

----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B can access the Internet.

Configuration Scripts

- Public system

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/1
 assign interface GE0/0/3
 assign global-ip 10.1.1.8 10.1.1.8 exclusive
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/2
 assign interface GE0/0/4
 assign global-ip 10.1.1.9 10.1.1.9 exclusive
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/1
 ip address 10.1.1.8 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.0.2 10.3.0.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
nat-policy
 rule name nat1
  source-zone trust
  egress-interface GE0/0/1
  source-address range 10.3.0.2 10.3.0.10
  action source-nat easy-ip
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/2
 ip address 10.1.1.9 255.255.255.0
#
interface GE0/0/4
 ip address 10.3.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name nat1
  source-zone trust
  egress-interface GE0/0/2
  source-address 10.3.1.0 mask 255.255.255.0
  action source-nat easy-ip
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

6.12 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the Public Interface of the Public System (Performing NAT in the Public System)

Networking Requirements

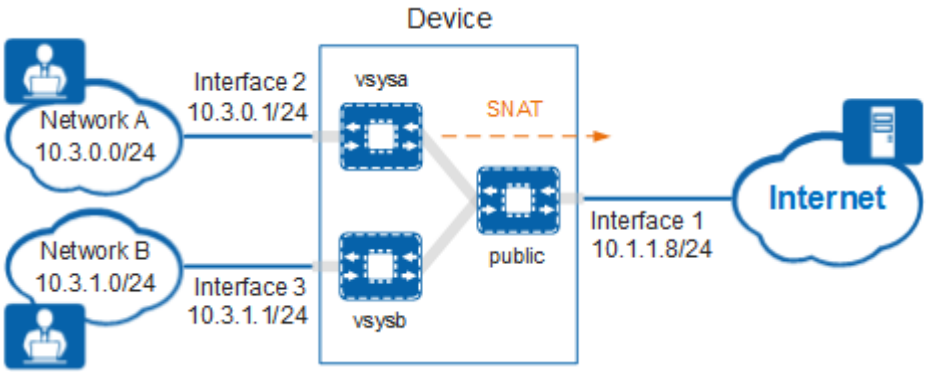
As shown in **Figure 6-12**, Device functions as a Layer 3 gateway and is deployed between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have no overlapping IP addresses.

User hosts on networks A and B access the Internet through the shared public network interface named interface 1 of the public system. On network A, only some user hosts are allowed to access the Internet. On network B, all user hosts are allowed to access the Internet. In addition, source NAT is performed in the public system to translate the source IP addresses of intranet-to-Internet packets into the public IP address of Device. In this way, the intranet IP addresses are hidden from the Internet.

Figure 6-12 Configuring intranet users of virtual systems to access the Internet through the public network interface of the public system (performing NAT in the public system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
public	Public network interface:GE0/0/1 IP address of the public network interface: 10.1.1.8/24 Security zone to which the public network interface belongs: Untrust Private network interface: Virtual-if0 of the public system Security zone to which the private network interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, intranet user hosts attached to virtual systems can access the Internet only through the public system. As the private IP addresses of networks A and B attached to the virtual systems do not overlap, you can configure a source NAT policy in the public system.
vsysa	Virtual system name: vsysa Public network interface: Virtual-if1 of vsysa Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/2 IP address of the private network interface: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the private network interface belongs: Trust IP addresses allowed to access the Internet: 10.3.0.2 to 10.3.0.10	-
vsysb	Virtual system name: vsysb Public network interface: virtual interface Virtual-if2 of vsysb Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/3 IP address of the private network interface: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the private network interface belongs: Trust	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

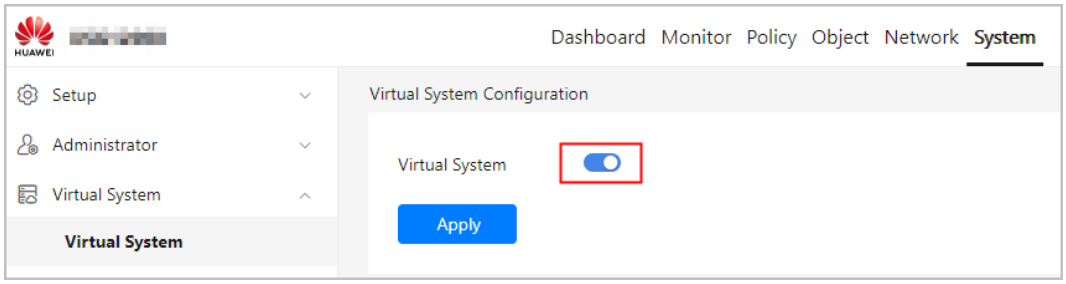
Configuration Roadmap

Do as follows on the public system, **vsysa**, and **vsysb** as required:

1. Enable the virtual system function.
2. Configure the resource class based on service requirements, create virtual systems **vsysa** and **vsysb** in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, **vsysa**, and **vsysb**, and add the interfaces to security zones.
4. Configure routes in the public system, **vsysa**, and **vsysb** to divert traffic from networks A and B to the Internet.
5. Configure security policies in the public system, **vsysa**, and **vsysb** based on service requirements to permit traffic from user hosts on networks A and B to the Internet.
6. Configure a source NAT policy in the public system to translate the source IP addresses of intranet-to-Internet packets into the IP address of the public network interface of the public system.

Procedure

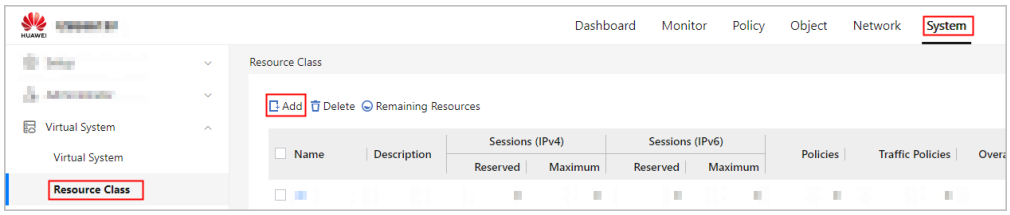
Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



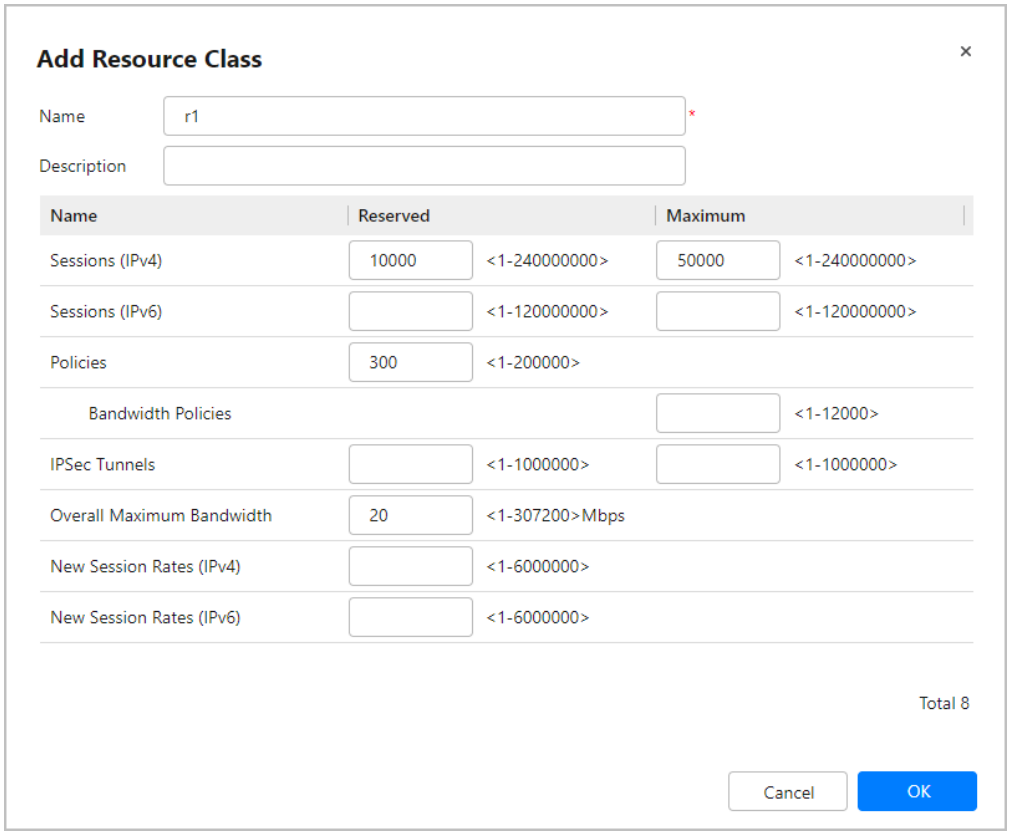
Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.

 Copyright © Huawei Technologies Co., Ltd.

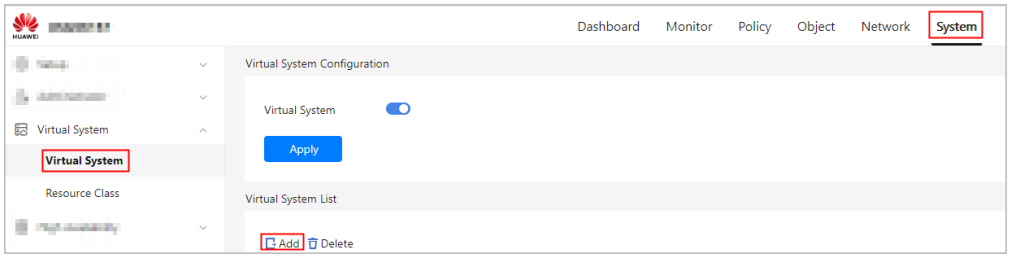


2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



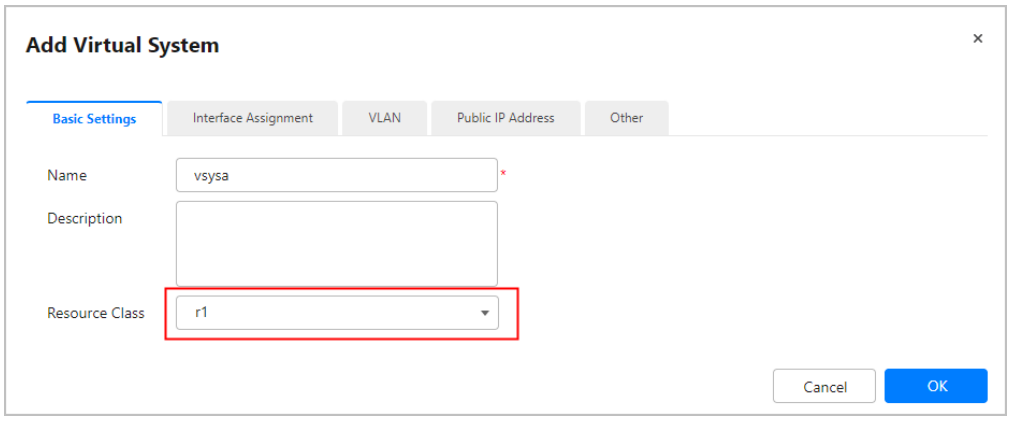
Step 3 In the public system, create virtual system **vsysa** and allocate resources. After the configuration is complete, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

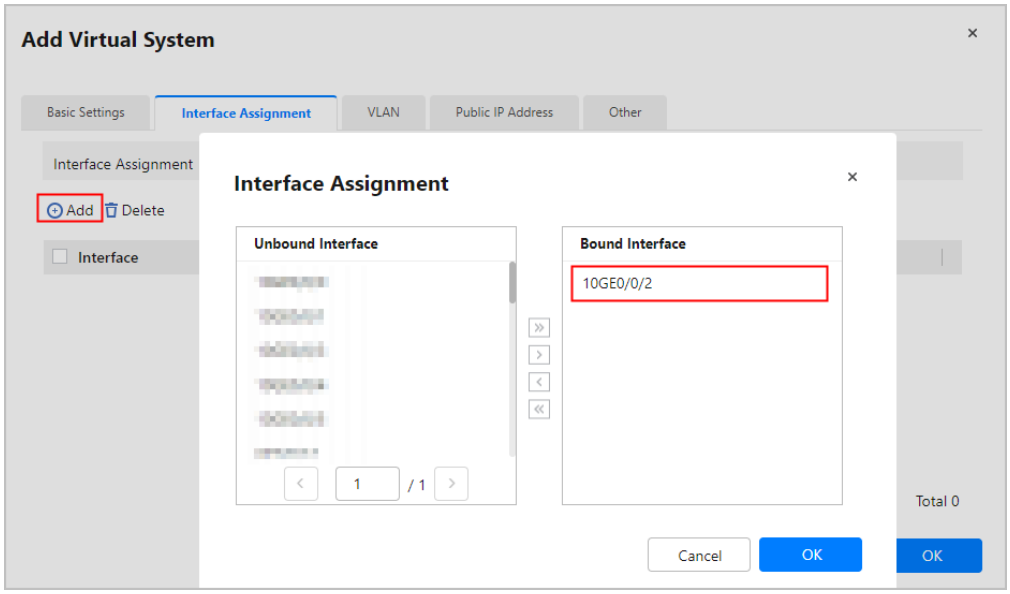


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

 Copyright © Huawei Technologies Co., Ltd.

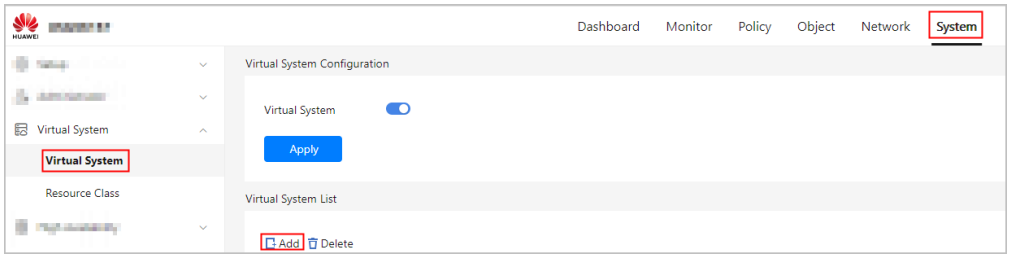


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



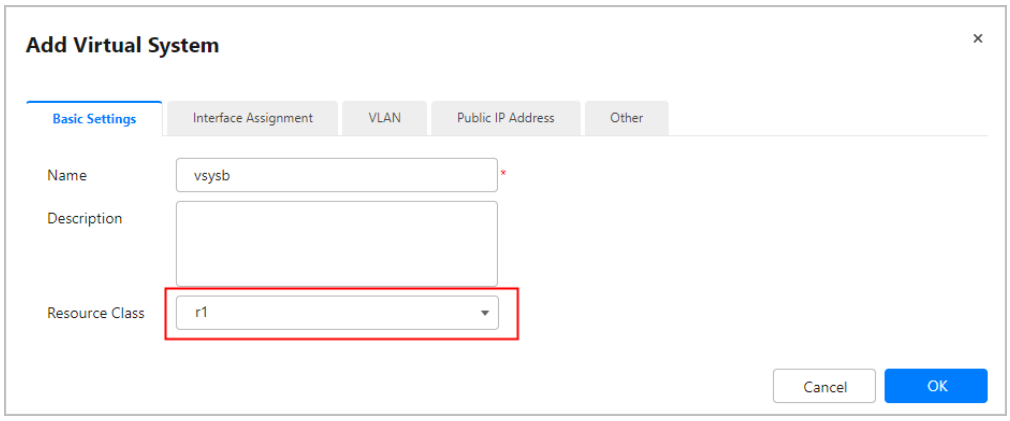
Step 4 In the public system, create virtual system **vsysb** and allocate resources. After the configuration is complete, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

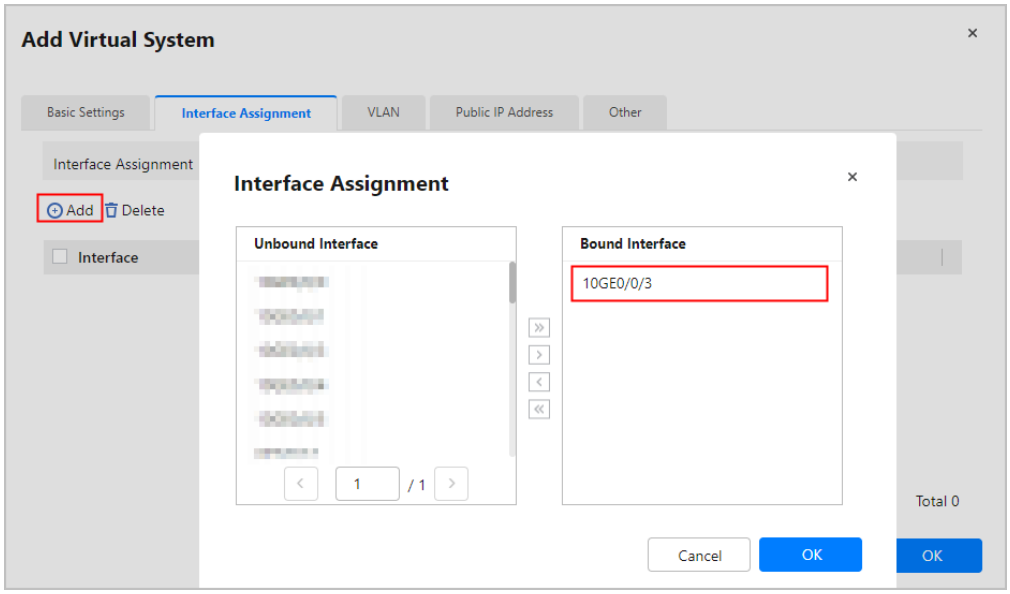


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



Step 5 Configure interfaces for the public system and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to the interface and set the following parameters. After the configuration is complete, click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.1.8/24

3. Repeat the preceding steps to configure **Virtual-if0**.

Zone	trust
IPv4	
IP Address	172.16.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure a security policy in the public system.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to permit user hosts from networks A and B to access the Internet. After the configuration is complete, click **OK**.

Name	trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24 10.3.1.0/24
Destination Address	10.1.1.0/24
Action	Permit

Step 7 Configure a route in the public system.

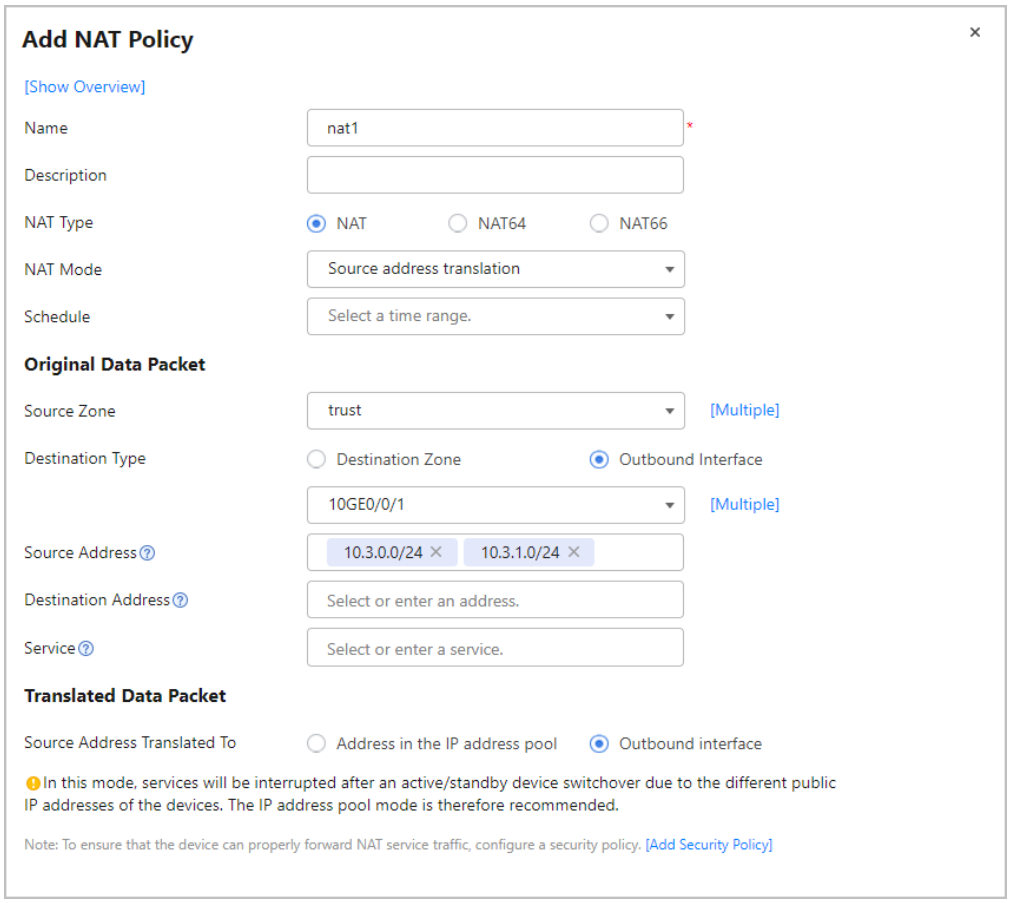
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the public system to the Internet to divert traffic from networks A and B to the Internet. **10.1.1.1** is the next-hop address of the route from the public system to the Internet. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

Step 8 Configure a NAT policy in the public system.

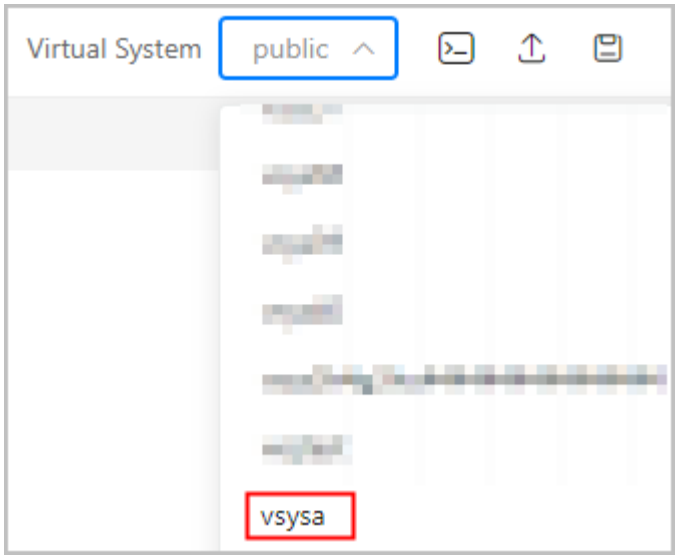
1. Choose **Policy** > **NAT Policy** > **NAT Policy**.
2. On the **NAT Policy** tab, click **Add**.
3. Configure a source NAT policy in the public system to translate the source IP addresses of packets sent from networks A and B to the Internet into the IP address of the public network interface of the public system. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 9 Add interfaces of **vsysa** to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click corresponding to the interface and set the following parameters. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps to configure **Virtual-if1**.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 10 Configure security policies in **vsysa**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to permit user hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A to access the Internet. After the configuration is complete, click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.2-10.3.0.10
Action	Permit

3. Repeat the preceding steps to configure a trust-to-untrust security policy to prevent user hosts that are not in the IP address range of 10.3.0.2 to 10.3.0.10 on network A from accessing the Internet.

Name	to_internet_block
Source Zone	trust
Destination Zone	untrust
Action	Deny

4. Repeat the preceding steps to configure a trust-to-untrust security policy to prevent the communication between network A and network B. Because a route has been configured in the public system to divert the return traffic to **vsysb**, **vsysa** and **vsysb** can communicate with each other through the public system. To isolate **vsysa** and **vsysb** from each other, you must configure this security policy in **vsysa**.

Name	to_vsysb_block
Source Zone	trust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	untrust
Destination Address	10.3.1.0/24
Action	Deny

Step 11 Configure routes in **vsysa**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysa** to the public system to divert the traffic of network A accessing the Internet to the public system. After the configuration is complete, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysa
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

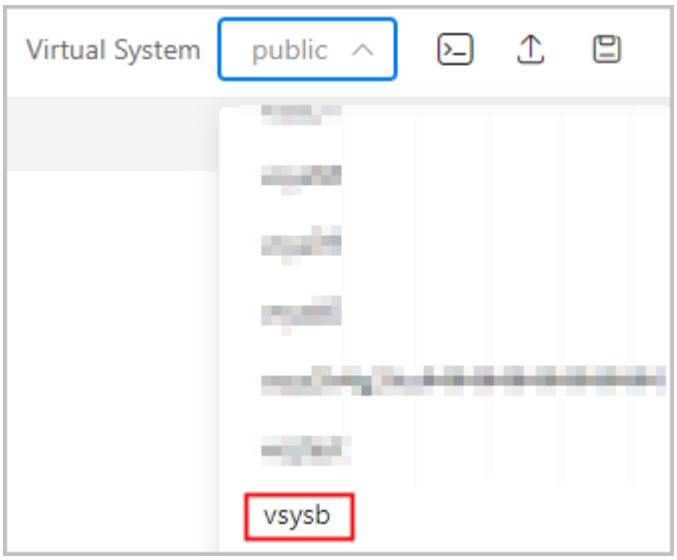
4. Repeat the preceding steps to configure a route from **vsysa** to network A. **10.3.0.254** is the next-hop address of the route from **vsysa** to network A.

Protocol	IPv4
Destination Address/Mask	10.3.0.0/24
Next Hop	10.3.0.254

Step 12 Add interfaces of **vsysb** to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.

 Copyright © Huawei Technologies Co., Ltd.



2. Choose **Network** > **Interface**.
3. Click and set the following parameters. After the configuration is complete, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

4. Repeat the preceding steps to configure **Virtual-if2**.

Zone	untrust
IPv4	
IP Address	172.16.2.1/24

Step 13 Configure security policies in **vsysb**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to permit user hosts on network B to access the Internet. After the configuration is complete, click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.1.0/24
Action	Permit

3. Repeat the preceding steps to configure a trust-to-untrust security policy to prevent the communication between network A and network B. Because a

 Copyright © Huawei Technologies Co., Ltd.

route has been configured in the public system to divert the return traffic to **vsysa**, **vsysa** and **vsysb** can communicate with each other across the public system. To isolate **vsysa** and **vsysb** from each other, you must configure this security policy in **vsysb**.

Name	to_vsysa_block
Source Zone	trust
Destination Zone	untrust
Destination Address	10.3.0.0/24
Action	Deny

Step 14 Configure routes in **vsysb**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysb** to the public system to divert the traffic of user hosts on network B accessing the Internet to the public system. After the configuration is complete, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysb
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

4. Repeat the preceding steps to configure a route from **vsysb** to network B. **10.3.1.254** is the next-hop address of the route from **vsysb** to network B.

Protocol	IPv4
Destination Address/Mask	10.3.1.0/24
Next Hop	10.3.1.254

----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A can access the Internet, but the other user hosts cannot.
- All user hosts on network B can access the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

- public:

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign resource-class r1
 assign interface
#
interface
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name nat1
  source-zone trust
  egress-interface
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  action source-nat easy-ip
#
return
```

- vsysa:

```
#
interface
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.0.2 10.3.0.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
 rule name to_vsysb_block
  source-zone trust
  destination-zone untrust
  destination-address 10.3.1.0 mask 255.255.255.0
  action deny
#
return
```

- vsysb:

```
#
interface
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name to_vsysa_block
  source-zone trust
  destination-zone untrust
  destination-address 10.3.0.0 mask 255.255.255.0
  action deny
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

6.13 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the WAN Interface of the Public System (Performing NAT in the Public System)

Networking Requirements

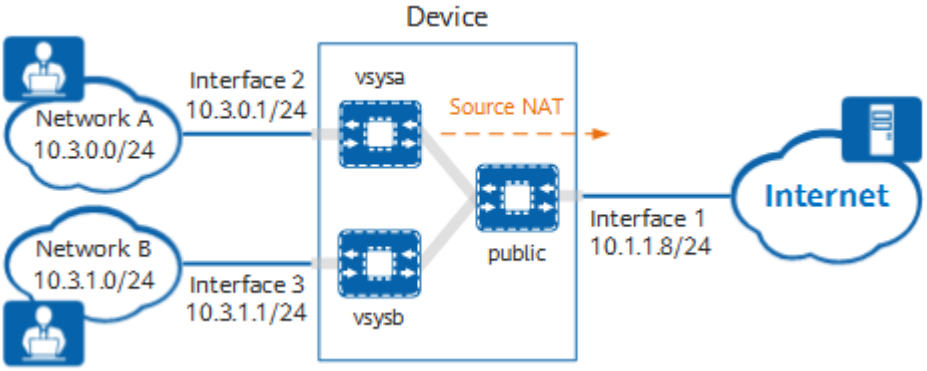
As shown in **Figure 6-13**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have no overlapping IP addresses.

User hosts on networks A and B access the Internet through the shared WAN interface interface 1 of the public system. On network A, only some user hosts can access the Internet. On network B, all user hosts can access the Internet. In addition, source NAT is performed in the public system to translate the source IP addresses of the packets from the intranet to the Internet into the public IP address of the device. In this way, the intranet IP addresses are hidden.

Figure 6-13 Configuring intranet users of virtual systems to access the Internet through the WAN interface of the public system (performing NAT in the public system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
public	WAN interface: GE 0/0/1 WAN interface IP address: 10.1.1.8/24 Security zone to which the WAN interface belongs: Untrust LAN interface: virtual interface Virtual-if0 of the public system Security zone to which the LAN interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, intranet user hosts attached to virtual systems can access the Internet only through the public system. As the private IP addresses of networks A and B attached to the virtual systems do not overlap, you can configure a source NAT policy in the public system.
vsysa	Virtual system name: vsysa WAN interface: virtual interface Virtual-if1 of vsysa Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 LAN interface IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the LAN interface belongs: Trust IP addresses allowed to access the Internet: 10.3.0.2 to 10.3.0.10	-
vsysb	Virtual system name: vsysb WAN interface: virtual interface Virtual-if2 of vsysb Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the LAN interface belongs: Trust	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.
4. Configure routes in the public system, vsysa, and vsysb to divert traffic from networks A and B to the Internet.
5. Configure security policies in the public system, vsysa, and vsysb based on service requirements to permit traffic from user hosts on networks A and B to the Internet.
6. Configure a source NAT policy in the public system to translate the source IP addresses of the packets from the intranet to the Internet into the IP address of the WAN interface of the public system.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] quit
```

Step 4 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 10.1.1.8 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 5 Configure a route from the public system to the Internet to divert traffic from networks A and B to the Internet. 10.1.1.1 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

Step 6 Configure a security policy in the public system to permit traffic from user hosts on networks A and B to the Internet.

```
[Device] security-policy
[Device-policy-security] rule name trust_to_untrust
[Device-policy-security-rule-trust_to_untrust] source-zone trust
[Device-policy-security-rule-trust_to_untrust] destination-zone untrust
[Device-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
[Device-policy-security-rule-trust_to_untrust] source-address 10.3.1.0 24
[Device-policy-security-rule-trust_to_untrust] action permit
[Device-policy-security-rule-trust_to_untrust] quit
[Device-policy-security] quit
```

Step 7 Configure a source NAT policy to translate the source IP addresses of the packets from networks A and B to the Internet into the IP address of the independent WAN interface GE 0/0/1 of the public system.

```
[Device] nat-policy
[Device-policy-nat] rule name nat1
[Device-policy-nat-rule-nat1] source-zone trust
[Device-policy-nat-rule-nat1] egress-interface ge 0/0/1
[Device-policy-nat-rule-nat1] source-address 10.3.0.0 24
[Device-policy-nat-rule-nat1] source-address 10.3.1.0 24
[Device-policy-nat-rule-nat1] action source-nat easy-ip
[Device-policy-nat-rule-nat1] quit
[Device-policy-nat] quit
```

Step 8 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 9 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 10 Configure routes in vsysa.

Configure a route from vsysa to the public system, diverting the traffic of network A accessing the Internet to the public system.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysa to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 11 Configure security policies in vsysa.

Allow user hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A to access the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_internet_allow
[Device-vsysa-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_allow] source-address range 10.3.0.2 10.3.0.10
[Device-vsysa-policy-security-rule-to_internet_allow] action permit
[Device-vsysa-policy-security-rule-to_internet_allow] quit
```

Forbid user hosts that are not in the IP address range of 10.3.0.2 to 10.3.0.10 on network A from accessing the Internet.

```
[Device-vsysa-policy-security] rule name to_internet_block
[Device-vsysa-policy-security-rule-to_internet_block] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_block] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_block] action deny
[Device-vsysa-policy-security-rule-to_internet_block] quit
```

Forbid communication between network A and network B. Because a route has been configured in the public system to divert the return traffic to vsysb, vsysa and vsysb can communicate with each other across the public system. To isolate vsysa and vsysb from each other, you must configure this security policy in vsysa.

```
[Device-vsysa-policy-security] rule name to_vsysb_block
[Device-vsysa-policy-security-rule-to_vsysb_block] source-zone trust
[Device-vsysa-policy-security-rule-to_vsysb_block] destination-zone untrust
[Device-vsysa-policy-security-rule-to_vsysb_block] destination-address 10.3.1.0 24
[Device-vsysa-policy-security-rule-to_vsysb_block] action deny
[Device-vsysa-policy-security-rule-to_vsysb_block] quit
[Device-vsysa-policy-security] quit
```

Step 12 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 13 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 14 Configure routes in vsysb.

Configure a route from vsysb to the public system, diverting the traffic of network B accessing the Internet to the public system.

```
[Device-vsysb] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysb to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 15 Configure security policies in vsysb.

Allow user hosts on network B to access the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_internet_allow
[Device-vsysb-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysb-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysb-policy-security-rule-to_internet_allow] source-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-to_internet_allow] action permit
[Device-vsysb-policy-security-rule-to_internet_allow] quit
```

Forbid communication between network A and network B. Because a route has been configured in the public system to divert the return traffic to vsysa, vsysa and vsysb can communicate with each other across the public system. To isolate vsysa and vsysb from each other, you must configure this security policy in vsysb.

```
[Device-vsysb-policy-security] rule name to_vsysa_block
[Device-vsysb-policy-security-rule-to_vsysa_block] source-zone trust
[Device-vsysb-policy-security-rule-to_vsysa_block] destination-zone untrust
[Device-vsysb-policy-security-rule-to_vsysa_block] destination-address 10.3.0.0 24
[Device-vsysb-policy-security-rule-to_vsysa_block] action deny
[Device-vsysb-policy-security-rule-to_vsysa_block] quit
[Device-vsysb-policy-security] quit
```

----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B can access the Internet.

Configuration Scripts

- Public system

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE0/0/1
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name nat1
  source-zone trust
  egress-interface GE0/0/1
  source-address 10.3.0.0 mask 255.255.255.0
  source-address 10.3.1.0 mask 255.255.255.0
  action source-nat easy-ip
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.0.2 10.3.0.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
 rule name to_vsysb_block
  source-zone trust
  destination-zone untrust
  destination-address 10.3.1.0 mask 255.255.255.0
  action deny
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
 rule name to_vsysa_block
  source-zone trust
  destination-zone untrust
  destination-address 10.3.0.0 mask 255.255.255.0
  action deny
#
return
```

6.14 Web: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the Public Network Interface of the Public System (Performing NAT in Each Virtual System)

Networking Requirements

As shown in **Figure 6-14**, Device functions as a Layer 3 gateway and is deployed between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have overlapping IP addresses.

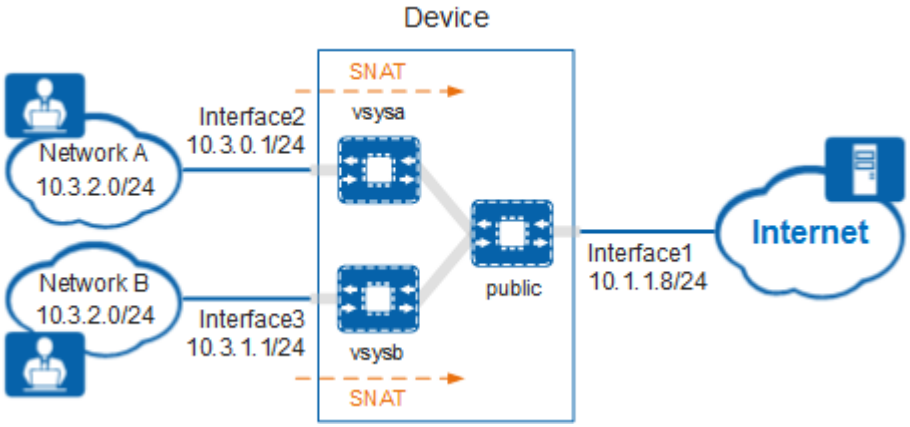
User hosts on networks A and B access the Internet through the shared public network interface named interface 1 of the public system. On network A, only some user hosts are allowed to access the Internet. On network B, all user hosts are allowed to access the Internet. In addition, source NAT is performed in the two virtual systems separately to translate the source IP addresses of intranet-to-Internet packets into the public IP address of Device. In this way, the intranet IP addresses are hidden from the Internet. Because public IP addresses are limited and NAT ports can be reused, the two virtual systems use the same public IP address but different ports.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-14 Configuring intranet users of virtual systems to access the Internet through the public network interface of the public system (performing NAT in each virtual system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Item	Data	Description
public	Public network interface:GE0/0/1 IP address of the public network interface: 10.1.1.8/24 Security zone to which the public network interface belongs: Untrust Private network interface: Virtual-if0 of the public system Security zone to which the private network interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, intranet user hosts attached to virtual systems can access the Internet only through the public system. As the private IP addresses of networks A and B attached to the virtual systems overlap, you need to configure a NAT policy in each virtual system.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysa	Virtual system name: vsysa Public network interface: virtual interface Virtual-if1 of vsysa Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/2 IP address of the private network interface: 10.3.0.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the private network interface belongs: Trust IP addresses allowed to access the Internet: 10.3.2.2 to 10.3.2.10 Public IP address after NAT: 10.10.1.1 (port range: 2048 to 30000)	-
vsysb	Virtual system name: vsysb Public network interface: virtual interface Virtual-if2 of vsysb Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/3 IP address of the private network interface: 10.3.1.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the private network interface belongs: Trust Public IP address after NAT: 10.10.1.1 (port range: 30001 to 65535)	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

Do as follows on the public system, **vsysa**, and **vsysb** as required:

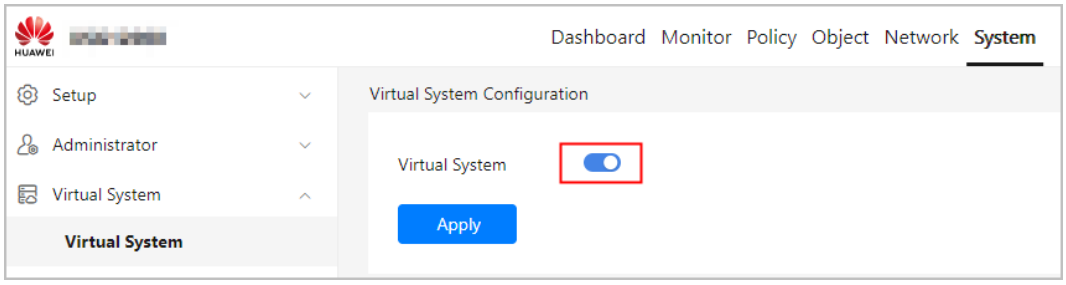
1. Enable the virtual system function.

 Copyright © Huawei Technologies Co., Ltd.

2. Configure the resource class based on service requirements, create virtual systems **vsysa** and **vsysb** in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, **vsysa**, and **vsysb**, and add the interfaces to security zones.
4. Configure routes in the public system, **vsysa**, and **vsysb** to divert traffic from networks A and B to the Internet.
5. Configure security policies in the public system, **vsysa**, and **vsysb** based on service requirements to permit traffic from user hosts on networks A and B to the Internet.
6. Configure source NAT policies in **vsysa** and **vsysb** to translate the source IP addresses of intranet-to-Internet packets into the IP addresses of the independent public network interfaces of the virtual systems.

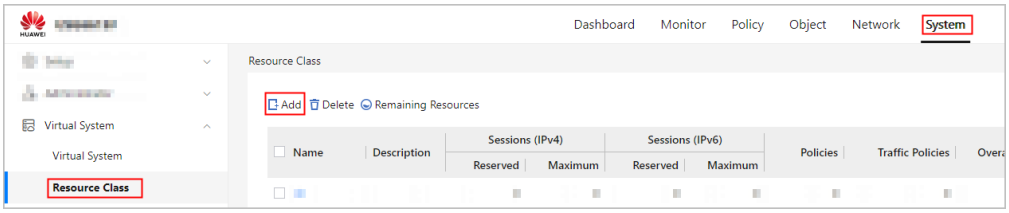
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



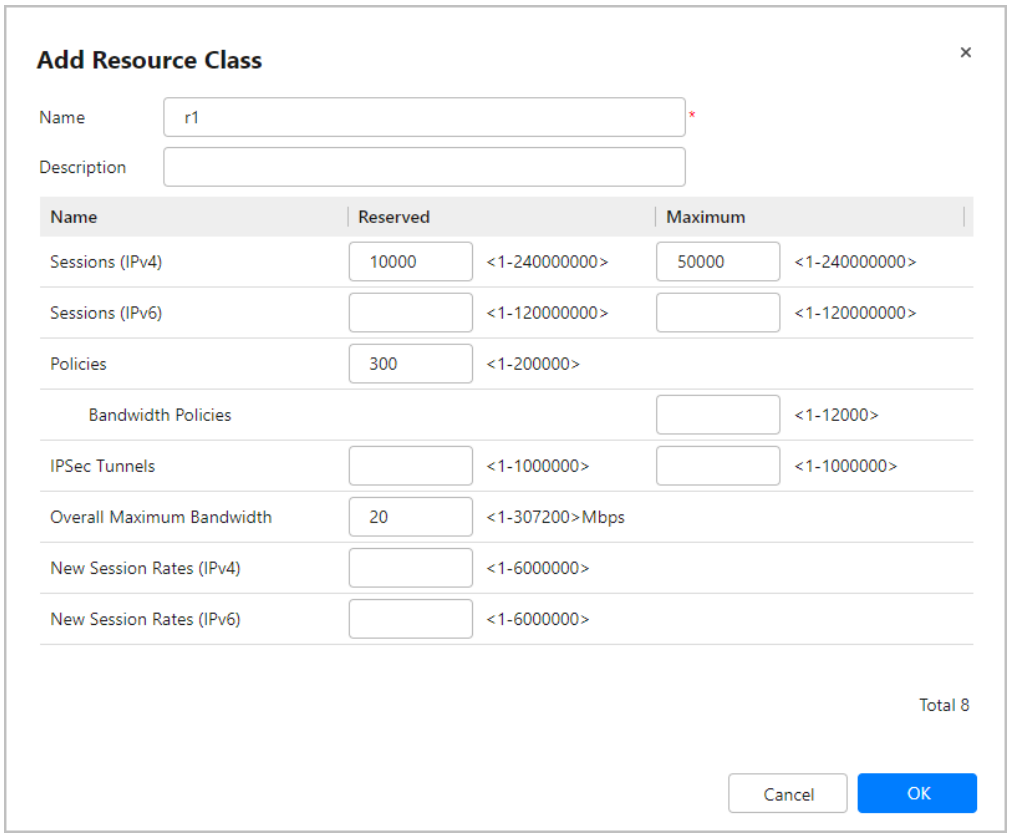
Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



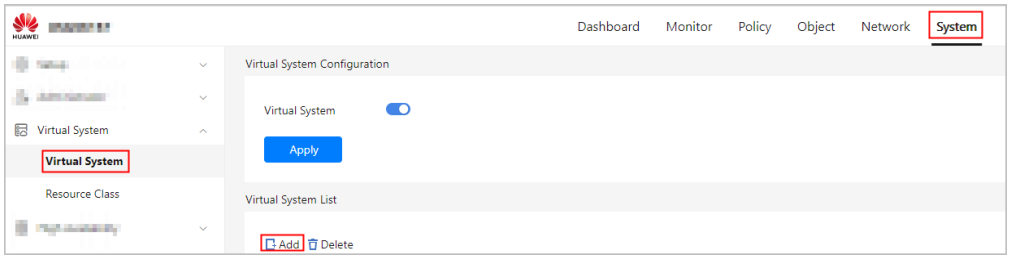
2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

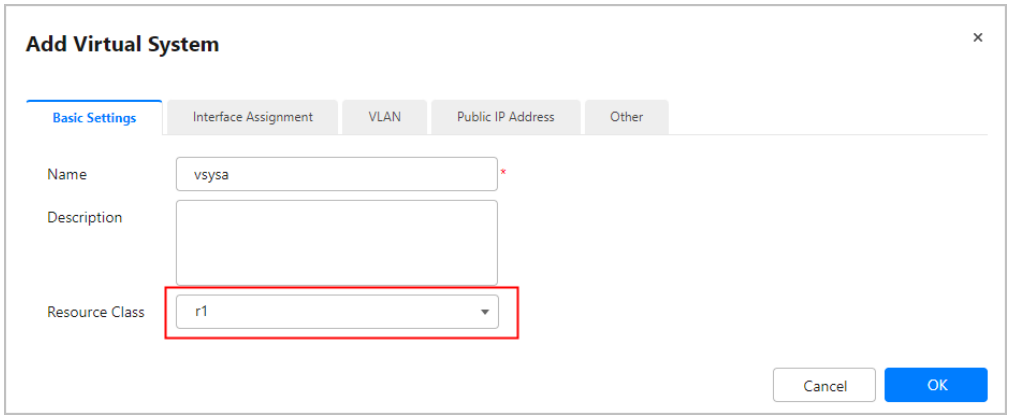


Step 3 In the public system, create virtual system **vsysa** and allocate resources. After the configuration is complete, click **OK**.

1. Choose **System > Virtual System >Virtual System**.

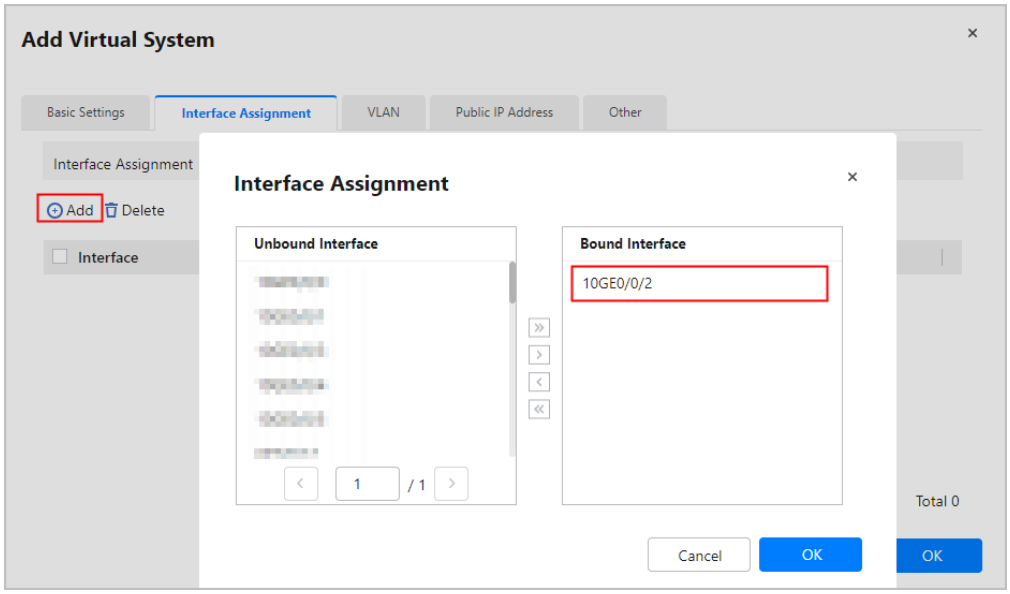


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

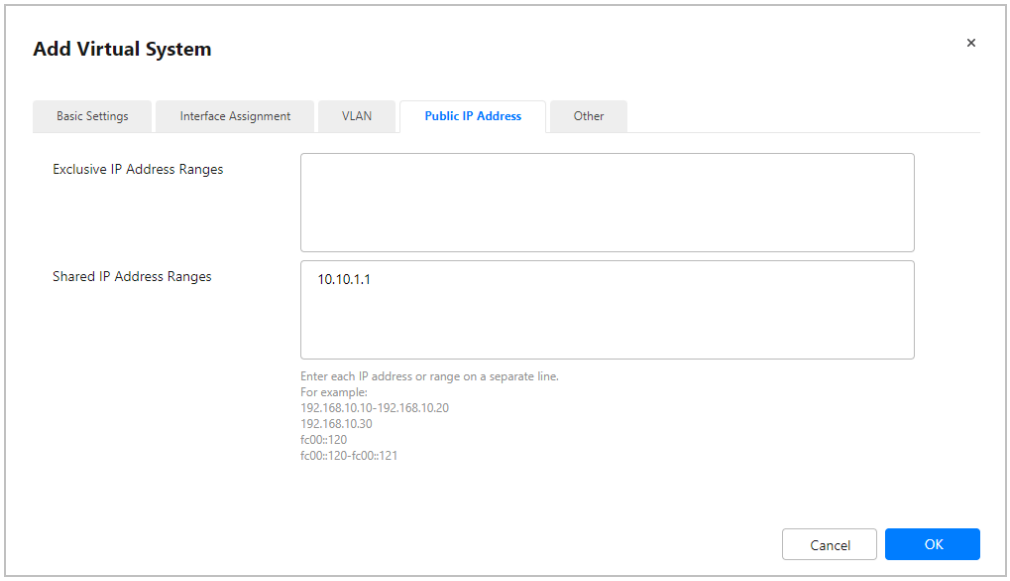


 Copyright © Huawei Technologies Co., Ltd.

3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.

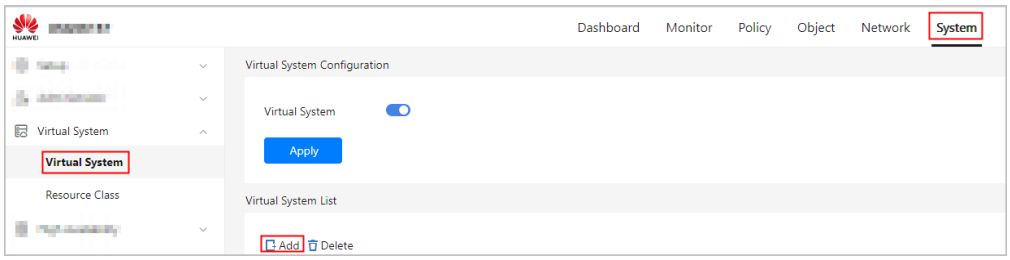


4. Click the **Public IP Address** tab and allocate a public IP address to the virtual system.



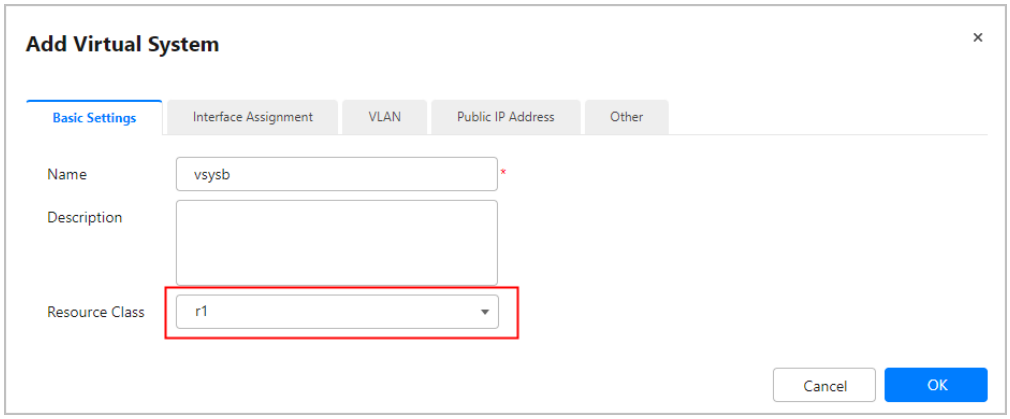
Step 4 In the public system, create virtual system **vsysb** and allocate resources. After the configuration is complete, click **OK**.

1. Choose **System > Virtual System >Virtual System**.

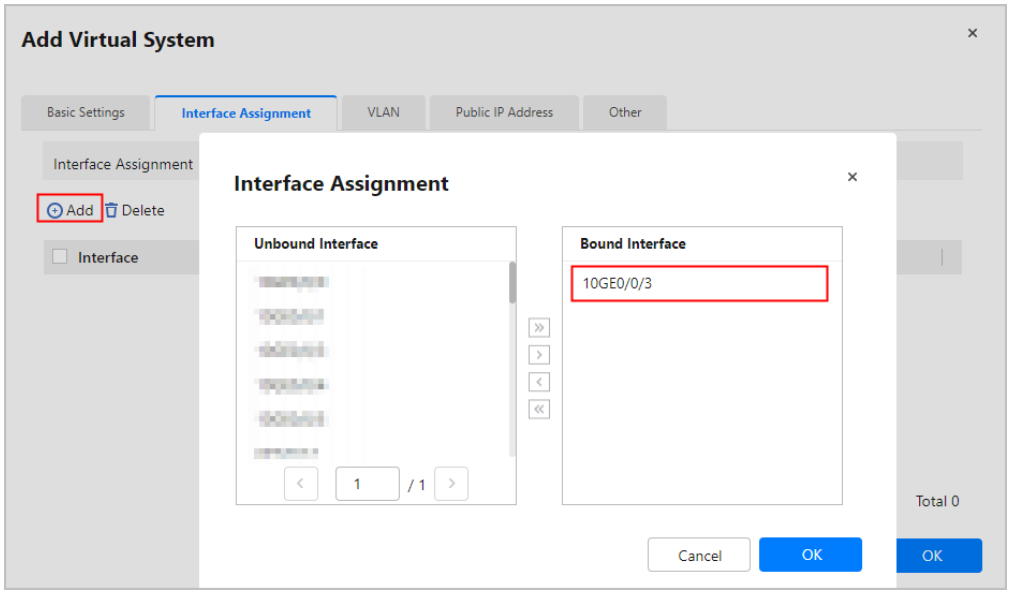


 Copyright © Huawei Technologies Co., Ltd.

2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

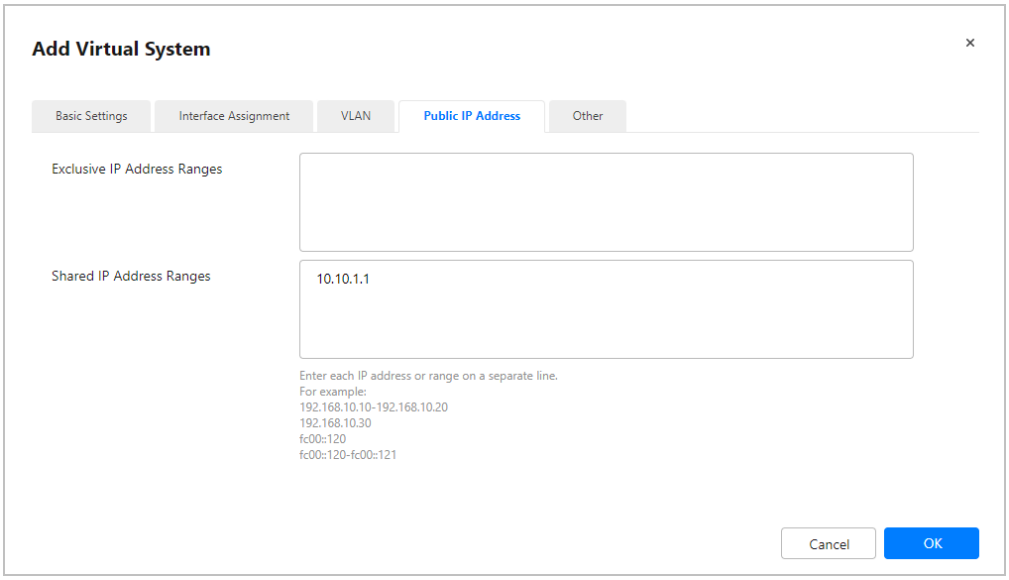


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



4. Click the **Public IP Address** tab and allocate a public IP address to the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 Configure interfaces for the public system and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/1 and setting the following parameters. After the configuration is complete, click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.1.8/24

3. Repeat the preceding steps to configure **Virtual-if0**.

Zone	trust
IPv4	
IP Address	172.16.0.1/24

Step 6 Configure a security policy in the public system.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to permit user hosts from networks A and B to access the Internet. After the configuration is complete, click **OK**.

Name	trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.10.1.1/32
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Configure a route in the public system.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the public system to the Internet to divert traffic from networks A and B to the Internet. **10.1.1.1** is the next-hop address of the route from the public system to the Internet. After the configuration is complete, click **OK**.

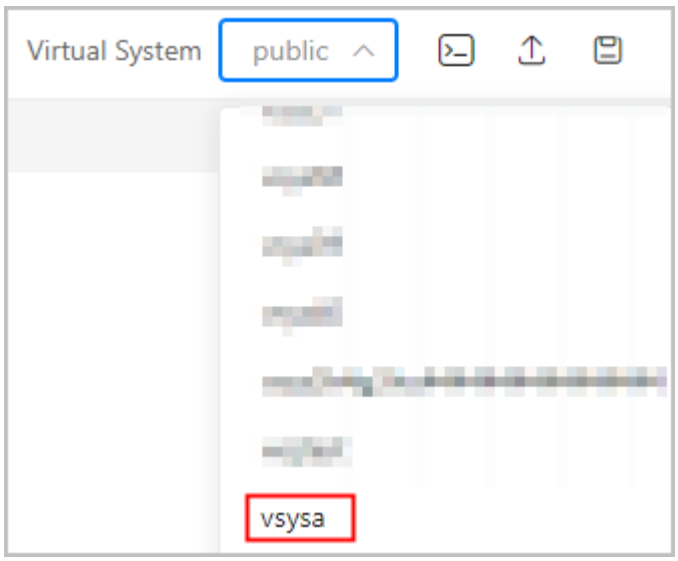
Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

4. Repeat the preceding steps to configure a blackhole route from the public system to the NAT address pool address to prevent network loops.

Protocol	IPv4
Destination Address/Mask	10.10.1.1/32
Interface	NULL0

Step 8 Add interfaces of **vsysa** to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/2 and set the following parameters. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps to configure **Virtual-if1**.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 9 Configure security policies in **vsysa**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to permit user hosts in the IP address range of 10.3.2.2 to 10.3.2.10 on network A to access the Internet. After the configuration is complete, click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.2-10.3.2.10
Action	Permit

3. Repeat the preceding steps to configure a trust-to-untrust security policy to prevent user hosts that are not in the IP address range of 10.3.2.2 to 10.3.2.10 on network A from accessing the Internet.

Name	to_internet_block
Source Zone	trust
Destination Zone	untrust
Action	Deny

Step 10 Configure routes in **vsysa**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.

   Configure a route from **vsysa** to the public system to divert the traffic of network A accessing the Internet to the public system. After the configuration is complete, click **OK**.

Protocol	IPv4

 Copyright © Huawei Technologies Co., Ltd.

Source Virtual Router	vsysa
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

3. Repeat the preceding steps to configure a route from **vsysa** to network A. **10.3.0.254** is the next-hop address of the route from **vsysa** to network A.

Protocol	IPv4
Destination Address/Mask	10.3.2.0/24
Next Hop	10.3.0.254

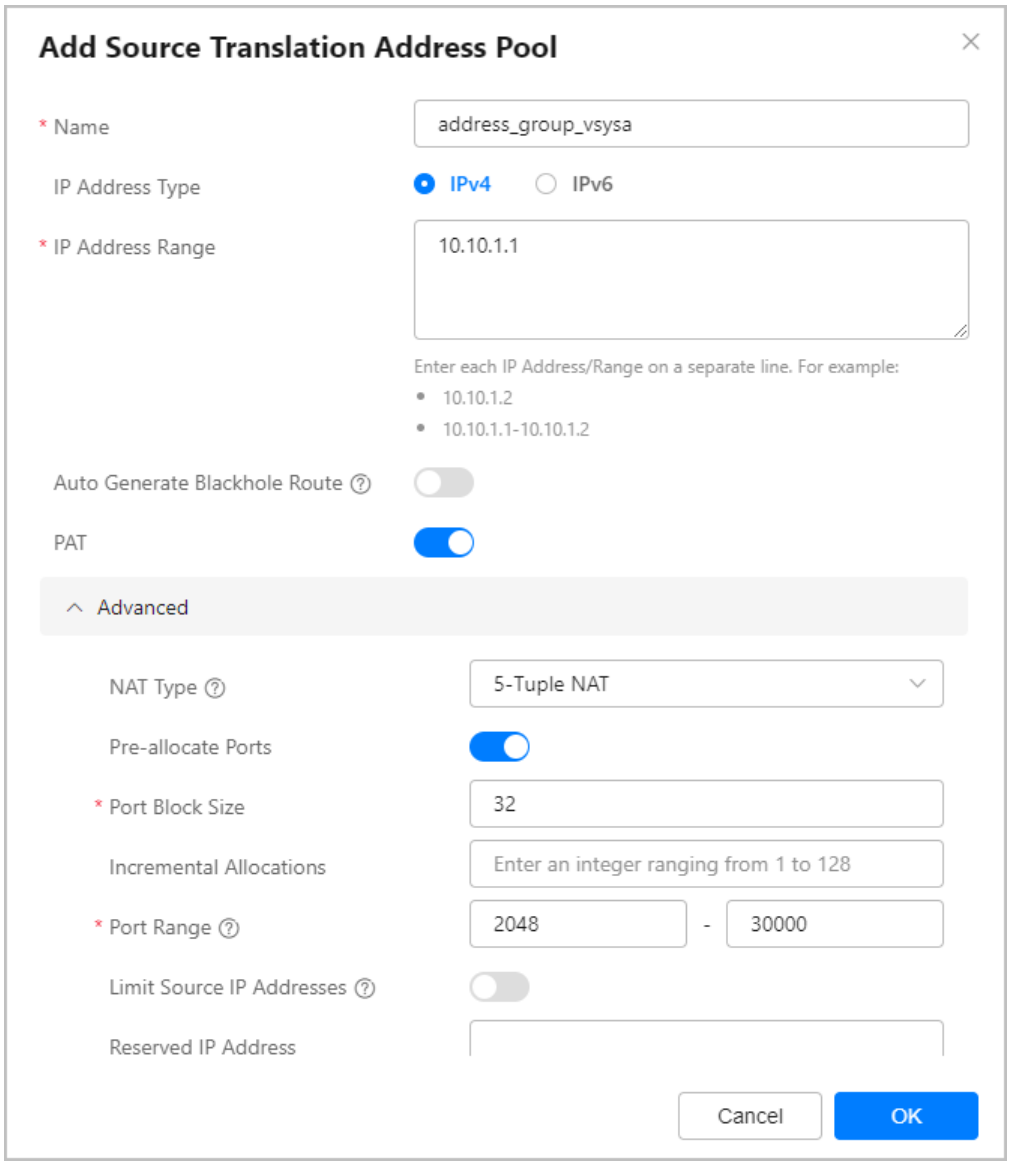
4. Repeat the preceding steps to configure a blackhole route from **vsysa** to the NAT address pool address to prevent network loops.

Protocol	IPv4
Destination Address/Mask	10.10.1.1/32
Interface	NULL0

Step 11 Configure security policies in **vsysa**.

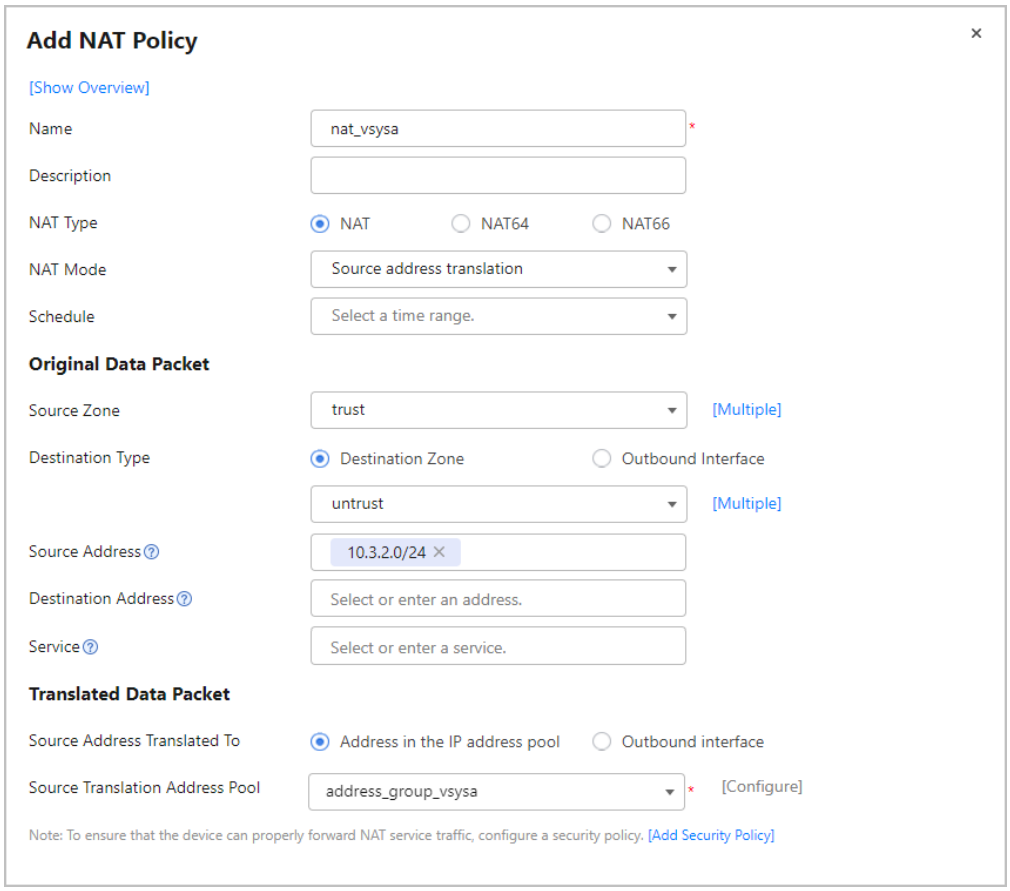
1. Choose **Policy** > **NAT Policy** > **NAT Policy**.
2. On the **Source Translation Address Pool** tab, click **Add**.
3. Create a source NAT address pool. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



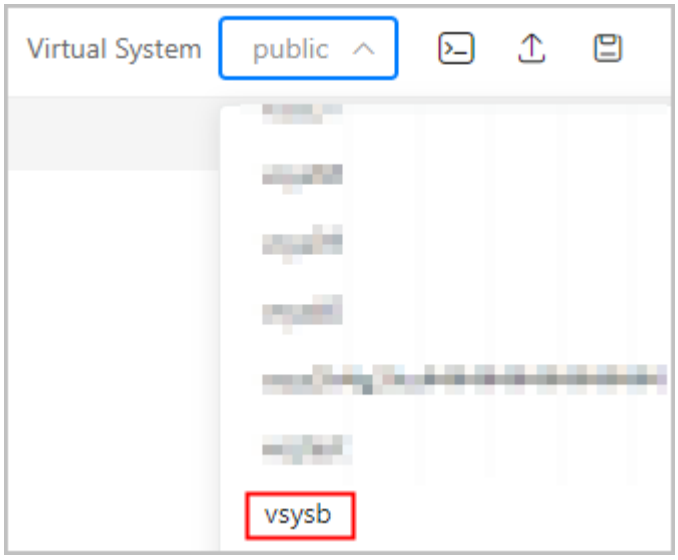
4. On the **NAT Policy** tab, click **Add**.
5. Configure a source NAT policy to translate the source IP addresses of packets sent from network A to the Internet into the IP address of the public of the virtual system. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 12 Add interfaces of **vsysb** to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/3 and set the following parameters. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

4. Repeat the preceding steps to configure **Virtual-if2**.

Zone	untrust
IPv4	
IP Address	172.16.2.1/24

Step 13 Configure security policies in **vsysb**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to permit user hosts on network B to access the Internet. After the configuration is complete, click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.0/24
Action	Permit

Step 14 Configure routes in **vsysb**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.

   Configure a route from **vsysb** to the public system to divert the traffic of user hosts on network B accessing the Internet to the public system. After the configuration is complete, click **OK**.

Protocol	IPv4
Source Virtual Router	vsysb
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public

3. Repeat the preceding steps to configure a route from **vsysb** to network B. **10.3.1.254** is the next-hop address of the route from **vsysb** to network B.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv4
Destination Address/Mask	10.3.2.0/24
Next Hop	10.3.1.254

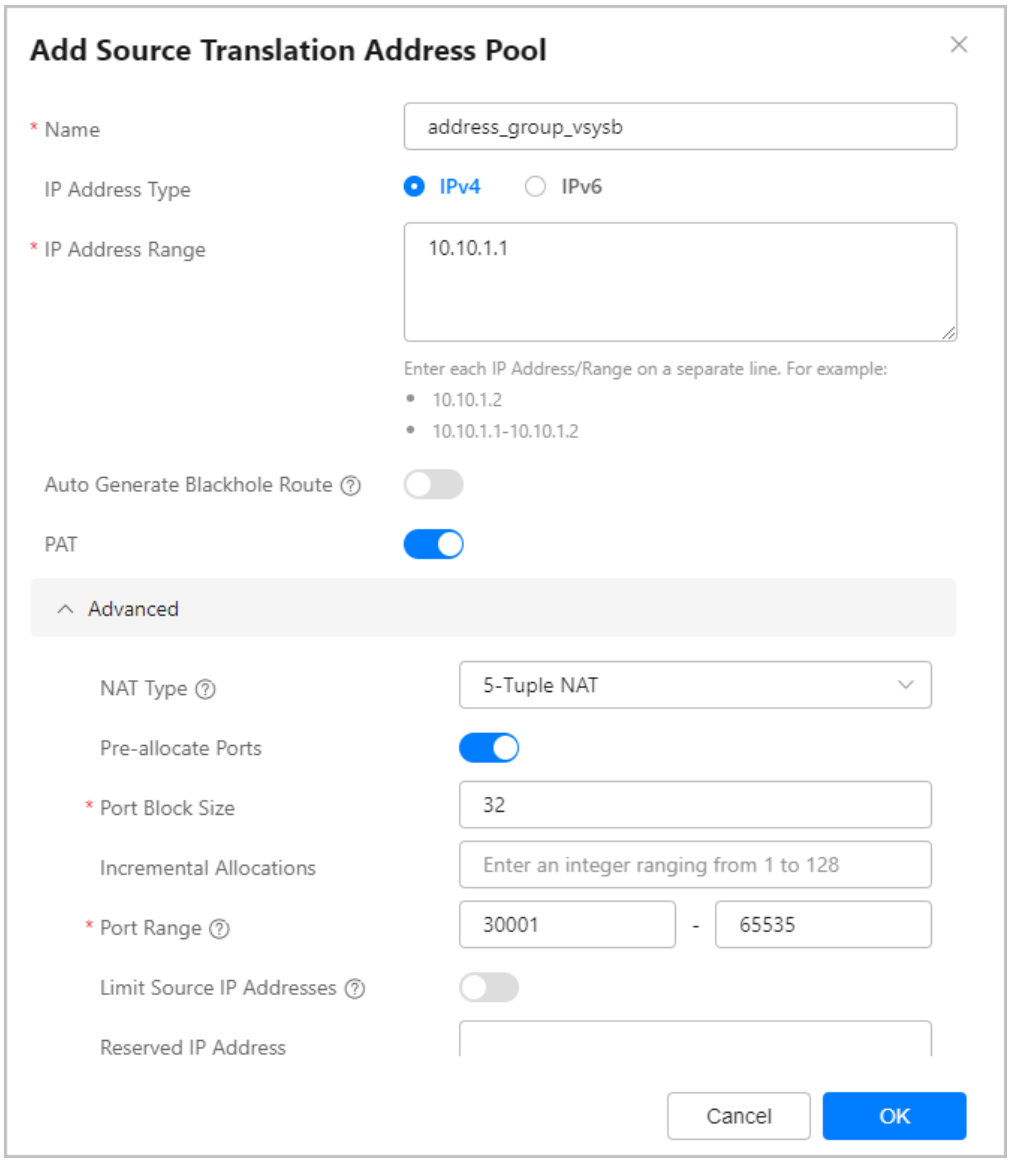
4. Repeat the preceding steps to configure a blackhole route from **vsysb** to the NAT address pool address to prevent network loops.

Protocol	IPv4
Destination Address/Mask	10.10.1.1/32
Interface	NULL0

Step 15 Configure a source NAT policy in **vsysb**.

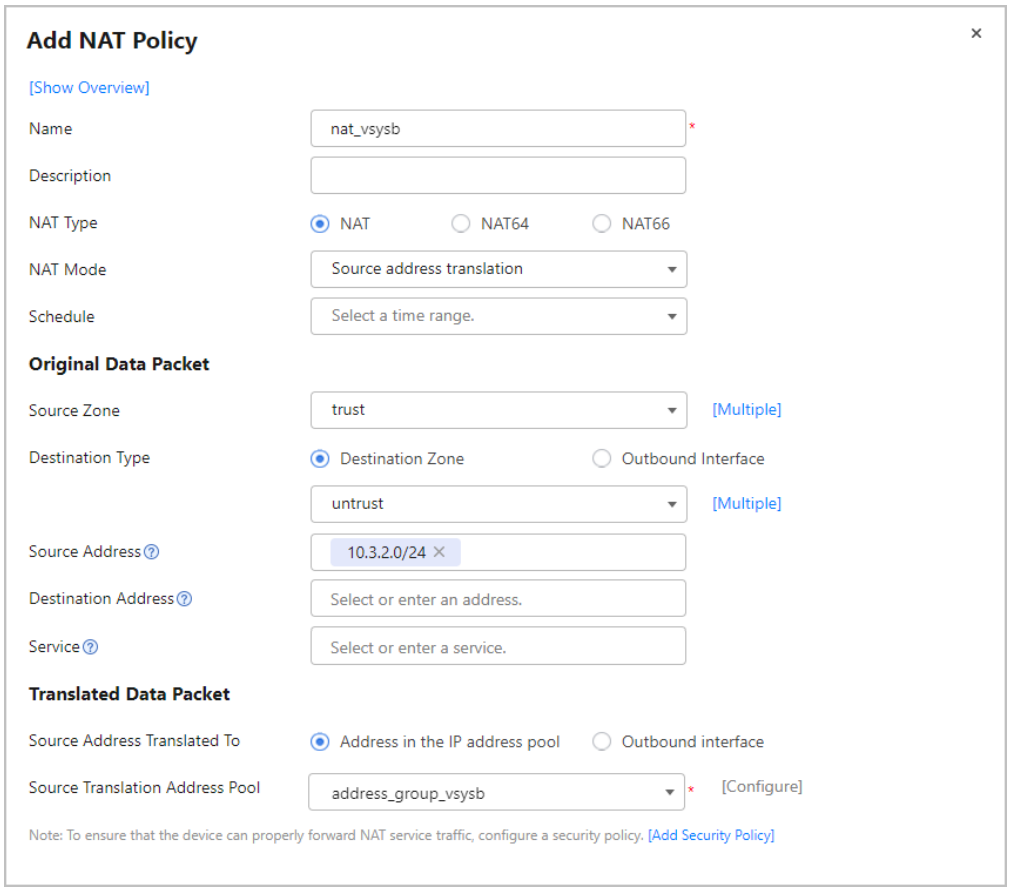
1. Choose **Policy** > **NAT Policy** > **NAT Policy**.
2. On the **Source Translation Address Pool** tab, click **Add**.
3. Create a source NAT address pool. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



4. On the **NAT Policy** tab, click **Add**.
5. Configure a source NAT policy to translate the source IP addresses of packets sent from network B to the Internet into the public IP address assigned to the virtual system. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.2.2 to 10.3.2.10 on network A can access the Internet, but the other user hosts cannot.
- All user hosts on network B can access the Internet.

Configuration Scripts

- public:

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
 assign global-ip 10.10.1.1 10.10.1.1 free
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
 assign global-ip 10.10.1.1 10.10.1.1 free
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/1
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
 ip route-static 10.10.1.1 255.255.255.255 NULL0
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.10.1.1 mask 255.255.255.255
  action permit
#
return
```

- vsysa:

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.2.0 255.255.255.0 10.3.0.254
 ip route-static 10.10.1.1 255.255.255.255 NULL0
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.2.2 10.3.2.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
nat address-group address_group_vsysa
 mode pat
 port-block-size 32 port-range 2048 30000
 section 0 10.10.1.1 10.10.1.1
#
nat-policy
 rule name nat_vsysa
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 mask 255.255.255.0
  action source-nat address-group address_group_vsysa
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

- vsysb:

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.2.0 255.255.255.0 10.3.1.254
 ip route-static 10.10.1.1 255.255.255.255 NULL0
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 mask 255.255.255.0
  action permit
#
nat address-group address_group_vsysb
 mode pat
 port-block-size 32 port-range 30001 65535
 section 0 10.10.1.1 10.10.1.1
#
nat-policy
 rule name nat_vsysb
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 mask 255.255.255.0
  action source-nat address-group address_group_vsysb
#
return
```

6.15 CLI: Example for Configuring Intranet Users of Virtual Systems to Access the Internet Through the WAN Interface of the Public System (Performing NAT in Each Virtual System)

Networking Requirements

As shown in **Figure 6-15**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have overlapping IP addresses.

User hosts on networks A and B access the Internet through the shared WAN interface interface 1 of the public system. On network A, only some user hosts can access the Internet. On network B, all user hosts can access the Internet. In addition, source NAT is performed in the two virtual systems separately to translate the source IP addresses of the packets from the intranet to the Internet into the public IP addresses of the device. In this way, the intranet IP addresses are

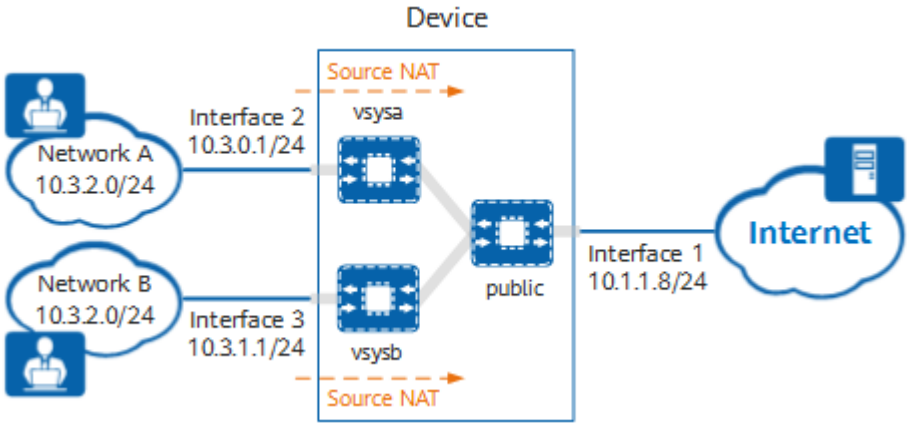
 Copyright © Huawei Technologies Co., Ltd.

hidden. Because public IP addresses are limited and NAT ports can be reused, the two virtual systems use the same public IP address but different ports.

Figure 6-15 Configuring intranet users of virtual systems to access the Internet through the WAN interface of the public system (performing NAT in each virtual system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Item	Data	Description
public	WAN interface: GE 0/0/1 WAN interface IP address: 10.1.1.8/24 Security zone to which the WAN interface belongs: Untrust LAN interface: virtual interface Virtual-if0 of the public system Security zone to which the LAN interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, intranet user hosts attached to virtual systems can access the Internet only through the public system. As the private IP addresses of networks A and B attached to the virtual systems overlap, you need to configure a NAT policy in each virtual system.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysa	Virtual system name: vsysa WAN interface: virtual interface Virtual-if1 of vsysa Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 LAN interface IP address: 10.3.0.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the LAN interface belongs: Trust IP addresses allowed to access the Internet: 10.3.2.2 to 10.3.2.10 Public IP address after NAT: 10.10.1.1 (port range: 2048-30000)	-
vsysb	Virtual system name: vsysb WAN interface: virtual interface Virtual-if2 of vsysb Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 10.3.1.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the LAN interface belongs: Trust Public IP address after NAT: 10.10.1.1 (port range: 30001-65535)	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.
4. Configure routes in the public system, vsysa, and vsysb to divert traffic from networks A and B to the Internet.
5. Configure security policies in the public system, vsysa, and vsysb based on service requirements to permit traffic from user hosts on networks A and B to the Internet.
6. Configure source NAT policies in vsysa and vsysb to translate the source IP addresses of the packets from the intranet to the Internet into the IP addresses of the independent WAN interfaces of the virtual systems.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] assign global-ip 10.10.1.1 10.10.1.1 free
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] assign global-ip 10.10.1.1 10.10.1.1 free
[Device-vsys-vsysb] quit
```

Step 4 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 10.1.1.8 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 5 Configure routes in the public system.

Configure a route from the public system to the Internet to divert traffic from networks A and B to the Internet. 10.1.1.1 is the next-hop address of the route from the public system to the Internet.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

Configure a blackhole route from the public system to the public IP address configured in the NAT address pool to prevent loops.

```
[Device] ip route-static 10.10.1.1 255.255.255.255 NULL0
```

Step 6 Configure a security policy in the public system to permit traffic from user hosts on networks A and B to the Internet.

```
[Device] security-policy
[Device-policy-security] rule name trust_to_untrust
[Device-policy-security-rule-trust_to_untrust] source-zone trust
[Device-policy-security-rule-trust_to_untrust] destination-zone untrust
[Device-policy-security-rule-trust_to_untrust] source-address 10.10.1.1 32
[Device-policy-security-rule-trust_to_untrust] action permit
[Device-policy-security-rule-trust_to_untrust] quit
[Device-policy-security] quit
```

Step 7 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 8 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 9 Configure routes in vsysa.

Configure a route from vsysa to the public system, diverting the traffic of network A accessing the Internet to the public system.

```
[Device-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysa to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.2.0 255.255.255.0 10.3.0.254
```

Configure a blackhole route from vsysa to the public IP address in the NAT address pool to prevent loops.

```
[Device-vsysa] ip route-static 10.10.1.1 255.255.255.255 NULL0
```

Step 10 Configure security policies in vsysa.

Allow user hosts in the IP address range of 10.3.2.2 to 10.3.2.10 on network A to access the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_internet_allow
[Device-vsysa-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_allow] source-address range 10.3.2.2 10.3.2.10
[Device-vsysa-policy-security-rule-to_internet_allow] action permit
[Device-vsysa-policy-security-rule-to_internet_allow] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Forbid user hosts that are not in the IP address range of 10.3.2.2 to 10.3.2.10 on network A from accessing the Internet.

```
[Device-vsysa-policy-security] rule name to_internet_block
[Device-vsysa-policy-security-rule-to_internet_block] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_block] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_block] action deny
[Device-vsysa-policy-security-rule-to_internet_block] quit
[Device-vsysa-policy-security] quit
```

Step 11 Configure a source NAT policy in vsysa to translate the source IP addresses of the packets from network A to the Internet into the public IP address assigned to vsysa.

Configure a NAT address pool and disable port translation.

```
[Device-vsysa] nat address-group address_group_vsysa
[Device-vsysa-address-group-address_group_vsysa] mode pat
[Device-vsysa-address-group-address_group_vsysa] port-block-size 32 port-range 2048 30000
[Device-vsysa-address-group-address_group_vsysa] section 0 10.10.1.1 10.10.1.1
[Device-vsysa-address-group-address_group_vsysa] quit
```

Configure a source NAT policy.

```
[Device-vsysa] nat-policy
[Device-vsysa-policy-nat] rule name nat_vsysa
[Device-vsysa-policy-nat-rule-nat_vsysa] source-zone trust
[Device-vsysa-policy-nat-rule-nat_vsysa] destination-zone untrust
[Device-vsysa-policy-nat-rule-nat_vsysa] source-address 10.3.2.0 24
[Device-vsysa-policy-nat-rule-nat_vsysa] action source-nat address-group address_group_vsysa
[Device-vsysa-policy-nat-rule-nat_vsysa] quit
[Device-vsysa-policy-nat] quit
```

Step 12 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 13 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

Step 14 Configure routes in vsysb.

Configure a route from vsysb to the public system, diverting the traffic of network B accessing the Internet to the public system.

```
[Device-vsysb] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a route from vsysb to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.2.0 255.255.255.0 10.3.1.254
```

Configure a blackhole route from vsysb to the public IP address configured in the NAT address pool to prevent loops.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysb] ip route-static 10.10.1.1 255.255.255.255 NULL0
```

Step 15 Configure security policies in vsysb.

Allow user hosts on network B to access the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_internet_allow
[Device-vsysb-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysb-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysb-policy-security-rule-to_internet_allow] source-address 10.3.2.0 24
[Device-vsysb-policy-security-rule-to_internet_allow] action permit
[Device-vsysb-policy-security-rule-to_internet_allow] quit
[Device-vsysb-policy-security] quit
```

Step 16 Configure a source NAT policy in vsysb to translate the source IP addresses of the packets from network B to the Internet into the public IP address assigned to vsysb.

Configure a NAT address pool and disable port translation.

```
[Device-vsysb] nat address-group address_group_vsysb
[Device-vsysb-address-group-address_group_vsysb] mode pat
[Device-vsysb-address-group-address_group_vsysb] port-block-size 32 port-range 30001 65535
[Device-vsysb-address-group-address_group_vsysb] section 0 10.10.1.1 10.10.1.1
[Device-vsysba-address-group-address_group_vsysb] quit
```

Configure a source NAT policy.

```
[Device-vsysb] nat-policy
[Device-vsysb-policy-nat] rule name nat_vsysb
[Device-vsysb-policy-nat-rule-nat_vsysb] source-zone trust
[Device-vsysb-policy-nat-rule-nat_vsysb] destination-zone untrust
[Device-vsysb-policy-nat-rule-nat_vsysb] source-address 10.3.2.0 24
[Device-vsysb-policy-nat-rule-nat_vsysb] action source-nat address-group address_group_vsysb
[Device-vsysb-policy-nat-rule-nat_vsysb] quit
[Device-vsysb-policy-nat] quit
```

----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.2.2 to 10.3.2.10 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B can access the Internet.

Configuration Scripts

- Public system

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
 assign global-ip 10.10.1.1 10.10.1.1 free
#
vsys name vsysb 2
 assign resource-class r1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 assign interface GE0/0/3
 assign global-ip 10.10.1.1 10.10.1.1 free
#
interface GE0/0/1
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
 ip route-static 10.10.1.1 255.255.255.255 NULL0
#
security-policy
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.10.1.1 mask 255.255.255.255
  action permit
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.2.0 255.255.255.0 10.3.0.254
 ip route-static 10.10.1.1 255.255.255.255 NULL0
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.2.2 10.3.2.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
nat address-group address_group_vsysa
 mode pat
 port-block-size 32 port-range 2048 30000
 section 0 10.10.1.1 10.10.1.1
#
nat-policy
 rule name nat_vsysa
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action source-nat address-group address_group_vsysa
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.2.0 255.255.255.0 10.3.1.254
 ip route-static 10.10.1.1 255.255.255.255 NULL0
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 mask 255.255.255.0
  action permit
#
nat address-group address_group_vsysb
 mode pat
 port-block-size 32 port-range 30001 65535
 section 0 10.10.1.1 10.10.1.1
#
nat-policy
 rule name nat_vsysb
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 mask 255.255.255.0
  action source-nat address-group address_group_vsysb
#
return
```

6.16 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through Independent Public Network Interfaces of the Virtual Systems

Networking Requirements

In **Figure 6-16**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and therefore cannot communicate with each other.

User hosts on the Internet access servers on networks A and B through interface 1 (public network interface) of vsysa and interface 2 (public network interface) of vsysb. In addition, NAT Server is configured for each virtual system. User hosts on

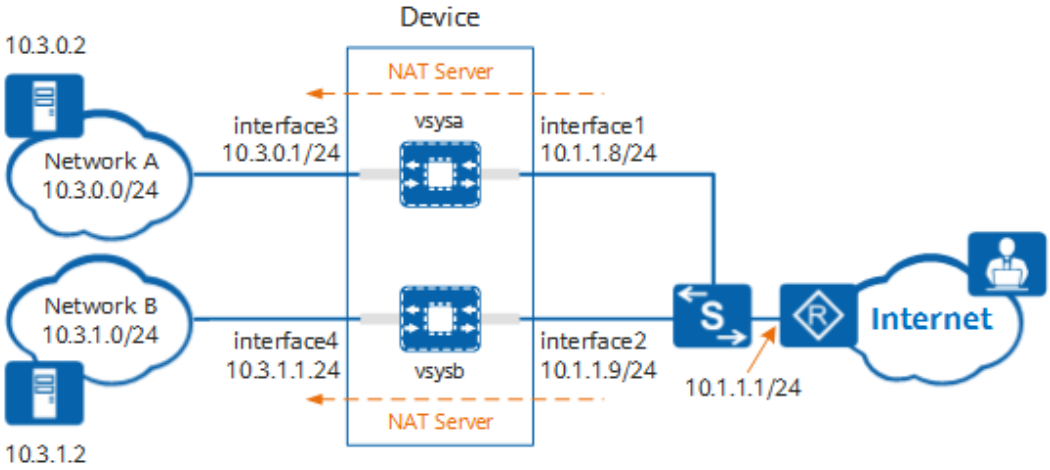
 Copyright © Huawei Technologies Co., Ltd.

the Internet can access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Figure 6-16 Configuring Internet users to access intranet servers of virtual systems through independent public network interfaces of the virtual systems

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/4, respectively.



Item	Data	Description
vsysa	Virtual system name: vsysa Public network interface: GE0/0/1 Public network interface IP address: 10.1.1.8/24 Security zone to which the public network interface belongs: Untrust Private network interface: GE0/0/3 Private network interface IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the private network interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.0.2:80 Public IP address and port of the intranet server for Internet users: 10.1.1.2:8080	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb Public network interface: GE0/0/2 Public network interface IP address: 10.1.1.9/24 Security zone to which the public network interface belongs: Untrust Private network interface: GE0/0/4 Private network interface IP address: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the private network interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.1.2:80 Public IP address and port of the intranet server for Internet users: 10.1.1.3:8080	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

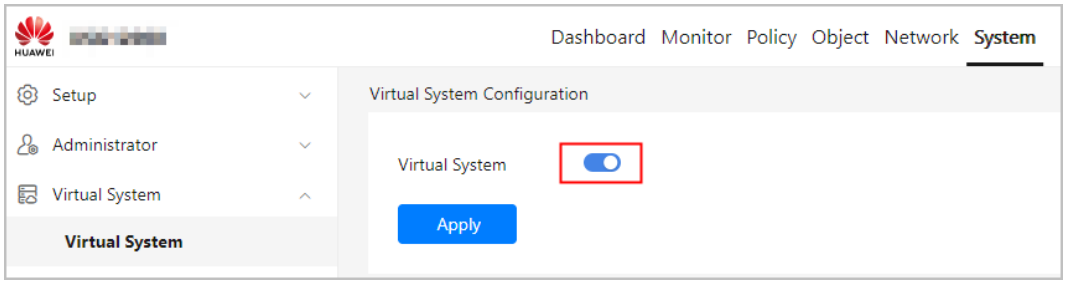
1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for vsysa and vsysb, and add the interfaces to security zones.
4. Configure routes in vsysa and vsysb to divert traffic from the Internet to networks A and B.
5. Configure security policies in vsysa and vsysb based on service requirements to permit traffic from user hosts on the Internet to servers on networks A and B.

 Copyright © Huawei Technologies Co., Ltd.

6. Configure NAT Server in both vsysa and vsysb to enable user hosts on the Internet to access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

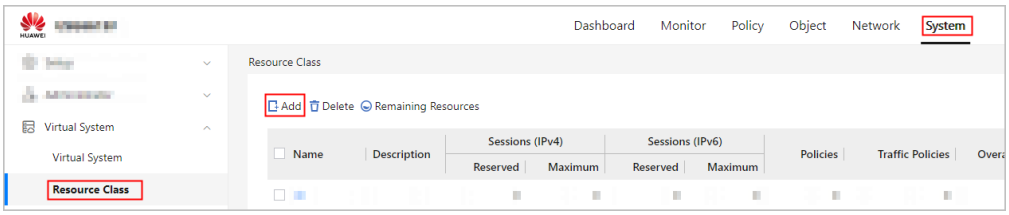
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



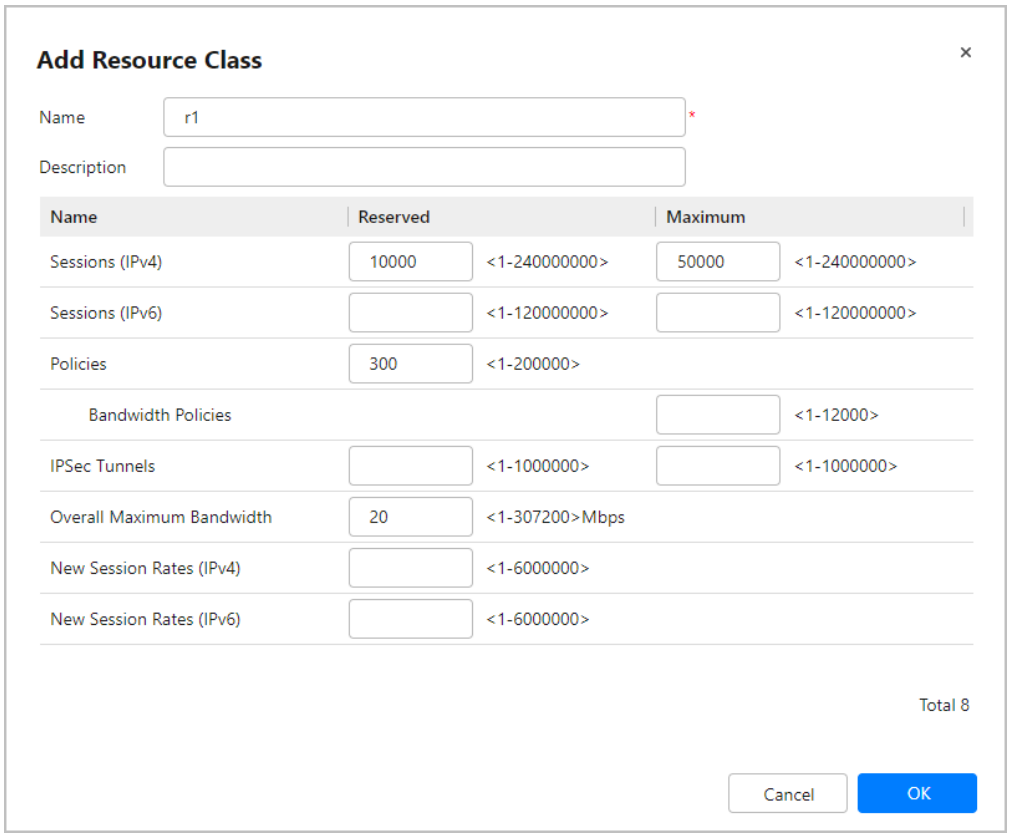
Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



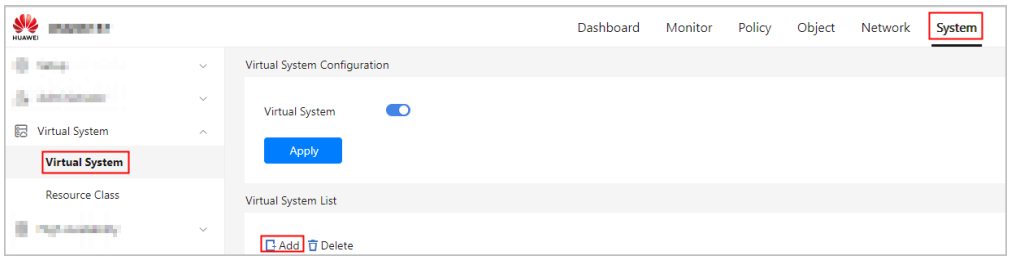
2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

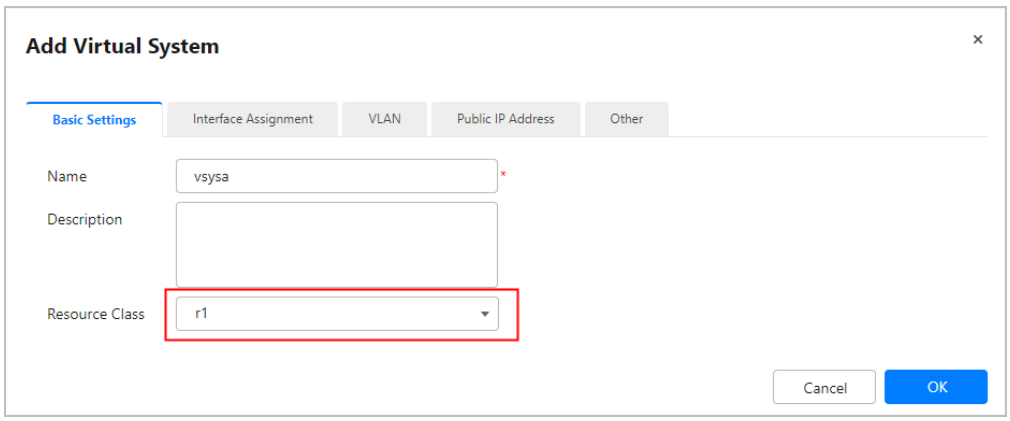


Step 3 In the public system, create virtual system vsysa and allocate resources to it. Click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

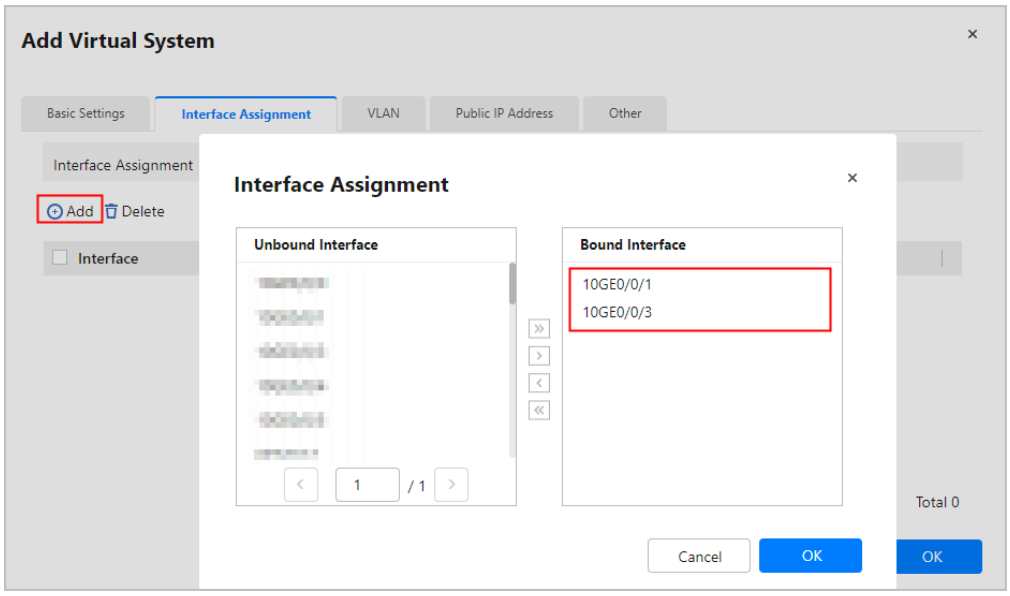


2. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

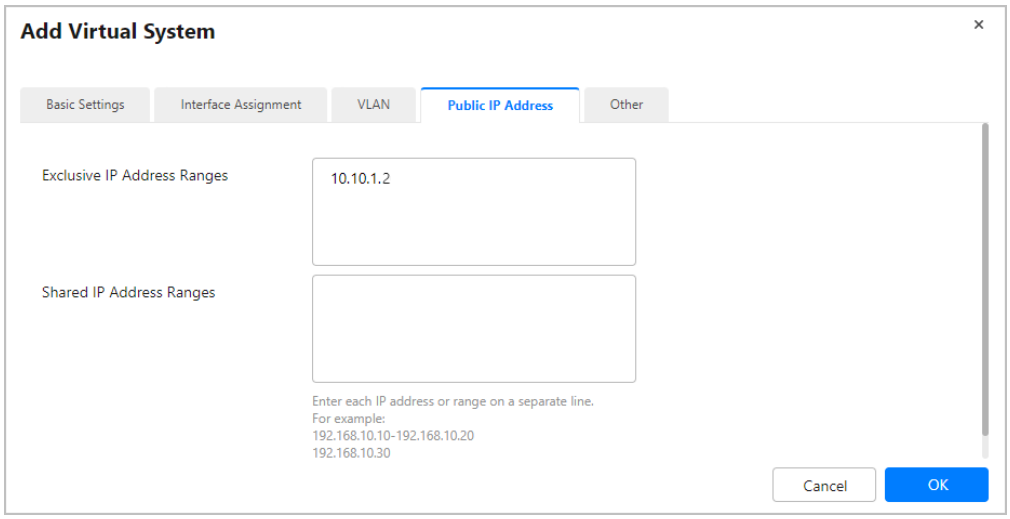


 Copyright © Huawei Technologies Co., Ltd.

3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.

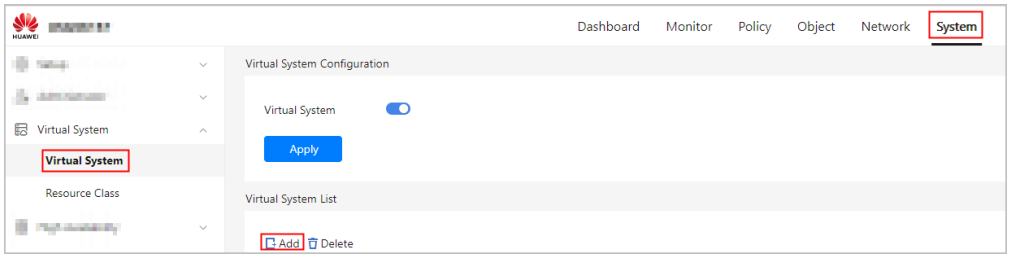


4. Click the **Public IP Address** tab, allocate public IP address to the virtual system.



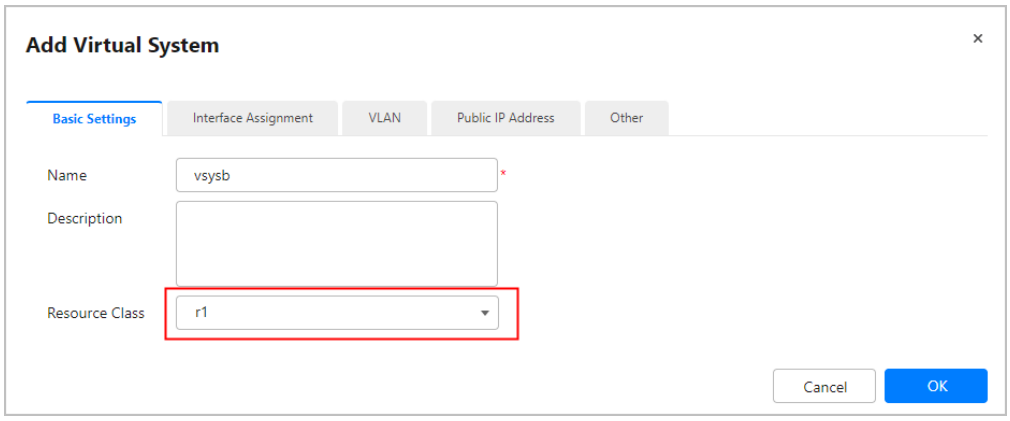
Step 4 In the public system, create virtual system vsysb and allocate resources to it. Click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

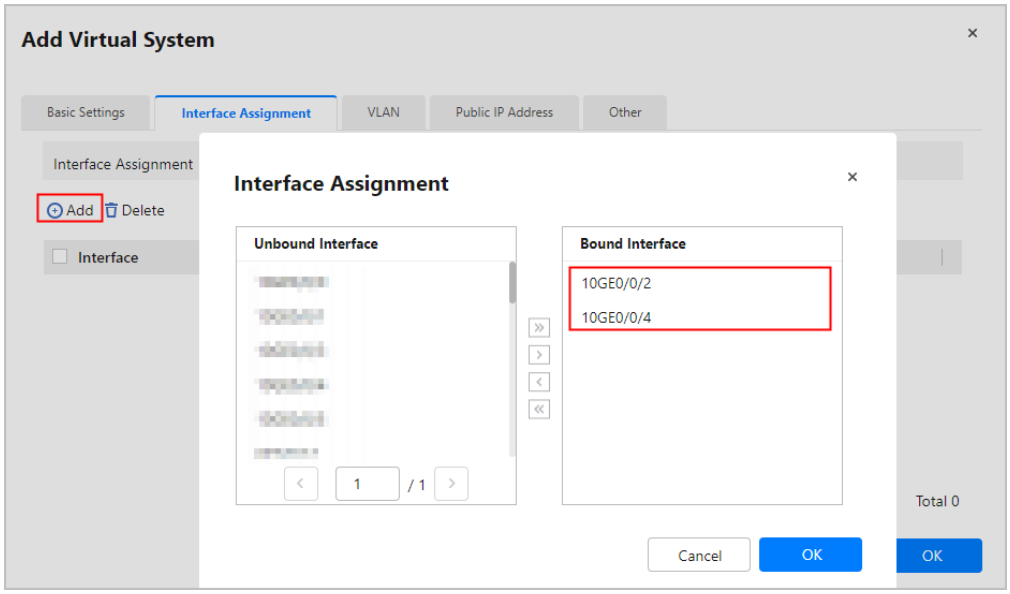


2. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

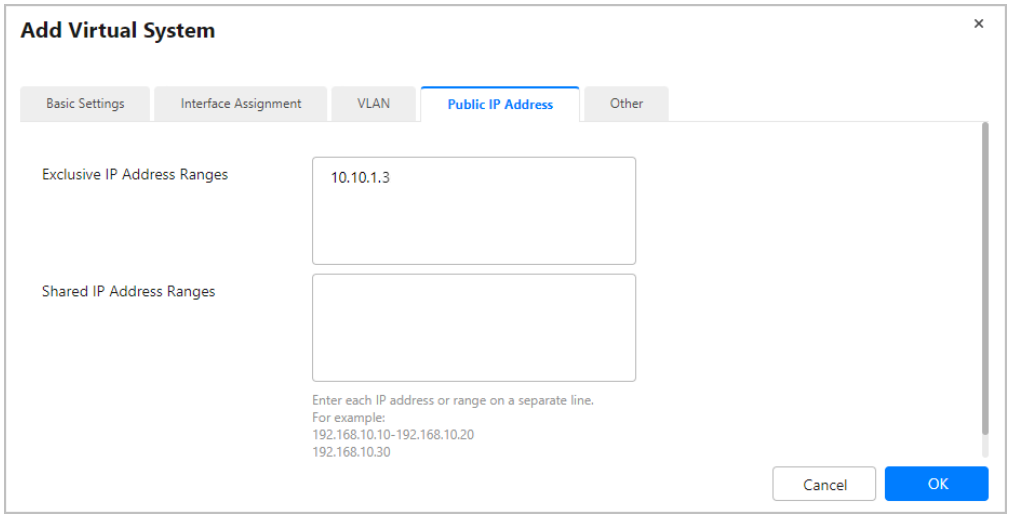
 Copyright © Huawei Technologies Co., Ltd.



3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



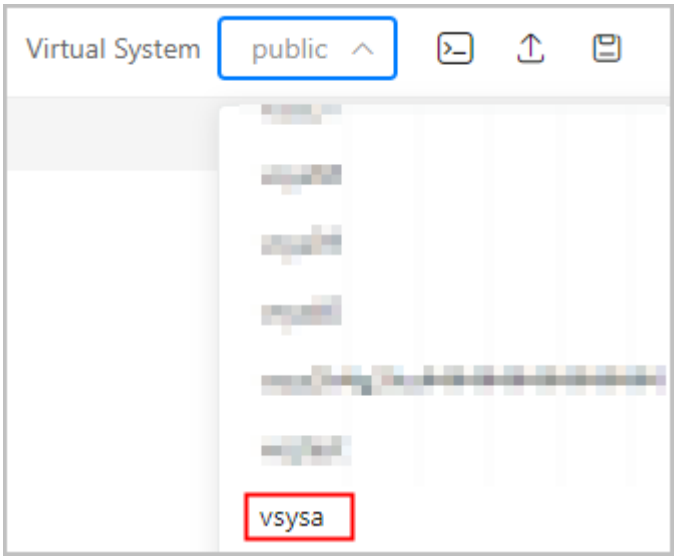
4. Click the **Public IP Address** tab, allocate public IP address to the virtual system.



Step 5 In vsysa, add GE0/0/1 and GE0/0/3 to security zones.

 Copyright © Huawei Technologies Co., Ltd.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access vsysa.



2. Choose **Network** > **Interface**.
3. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.1.8/24

4. Repeat the preceding steps to set the parameters for GE0/0/3.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

Step 6 Configure security policies in vsysa.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an Untrust-to-Trust interzone policy as follows to permit traffic from user hosts on the Internet to the servers on network A. Click **OK**.

Name	to_network_allow
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.0.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Configure routes in vsysa.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the Internet to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A. Click **OK**.

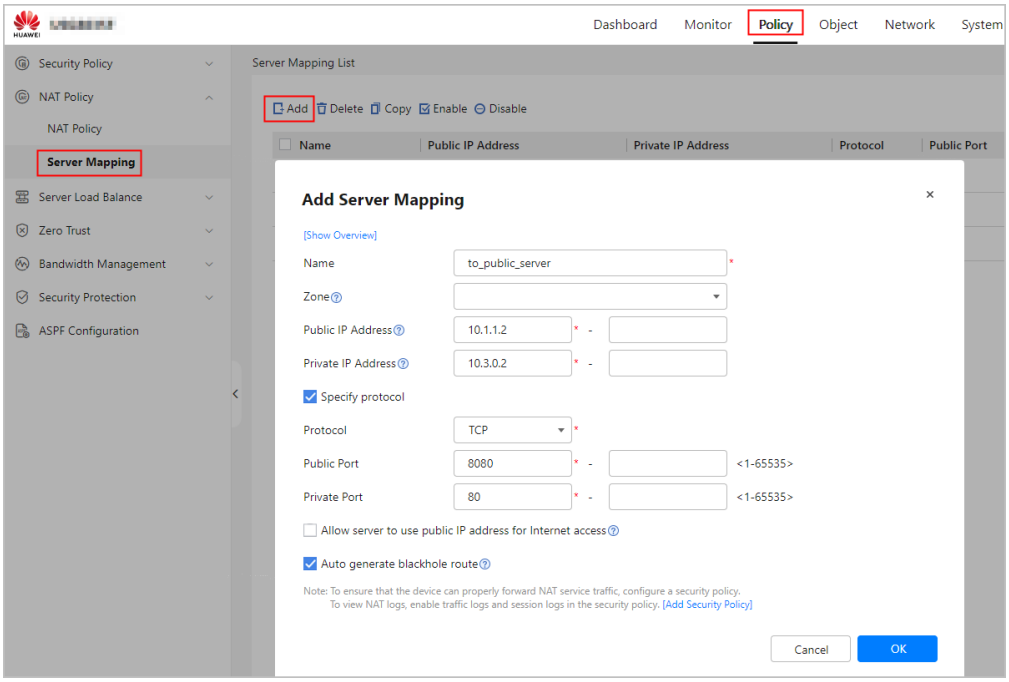
Protocol	IPv4
Destination Address/Mask	10.3.0.0/24
Next Hop	10.3.0.254

4. Configure a route from the vsysa to the Internet, diverting the return traffic for the Internet to access network A to the Internet. 10.1.1.1 is the next-hop address of the route from the vsysa to the Internet.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

Step 8 Configure server mapping (NAT Server) in vsysa.

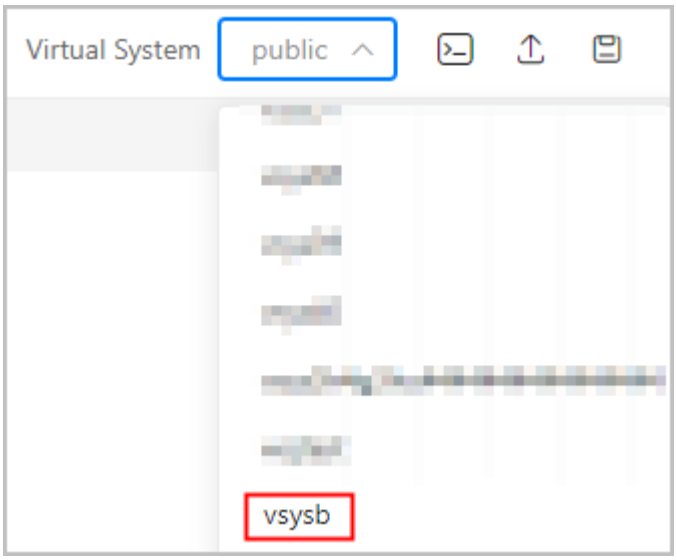
1. Choose **Policy** > **NAT Policy** > **Server Mapping**.
2. Click **Add**.
3. Configure NAT Server to enable user hosts on the Internet to access servers on network A through a public IP address. Click **OK**.



 Copyright © Huawei Technologies Co., Ltd.

Step 9 In vsysb, add GE0/0/2 and GE0/0/4 to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access vsysb.



2. Choose **Network** > **Interface**.
3. Click for GE0/0/2 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.1.9/24

4. Repeat the preceding steps to set the parameters for GE0/0/4.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

Step 10 Configure security policies in vsysb.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an Untrust-to-Trust interzone policy as follows to permit traffic from user hosts on the Internet to the servers on network B. Click **OK**.

Name	to_network_allow
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.1.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Step 11 Configure routes in vsysb.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the Internet to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.1.0/24
Next Hop	10.3.1.254

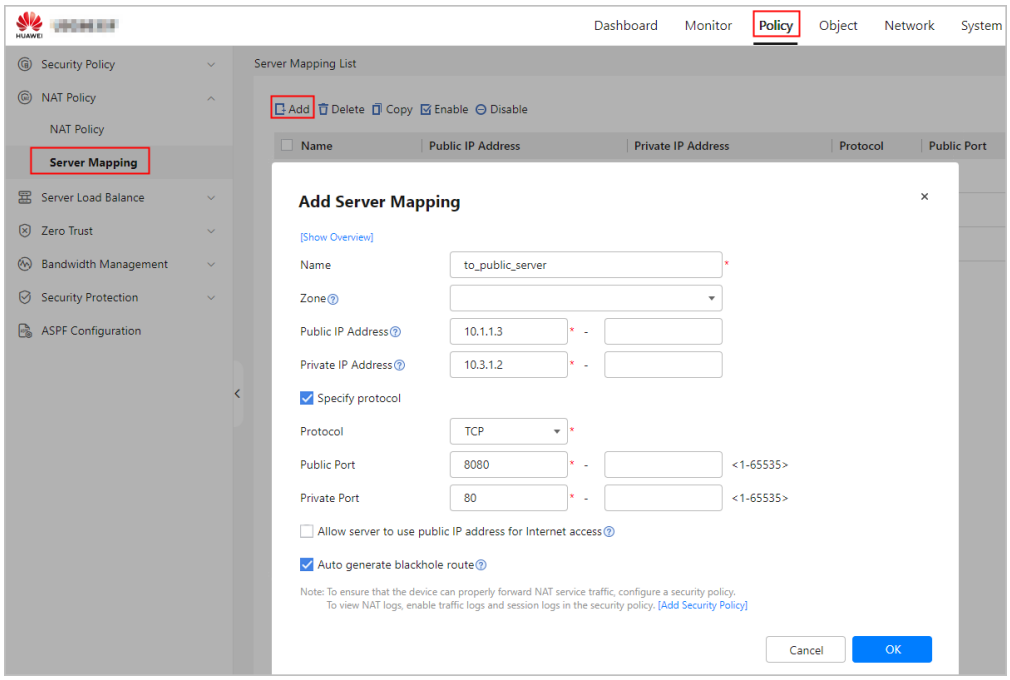
4. Configure a route from the vsysb to the Internet, diverting the return traffic for the Internet to access network B to the Internet. 10.1.1.1 is the next-hop address of the route from the vsysb to the Internet.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

Step 12 Configure server mapping (NAT Server) in vsysb.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.
2. Click **Add**.
3. Configure NAT Server to enable user hosts on the Internet to access servers on network B through a public IP address. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



----End

Verifying the Configuration

- User hosts on the Internet can access the web server at 10.3.0.2 on network A through http://10.1.1.2:8080.
- User hosts on the Internet can access the web server at 10.3.1.2 on network B through http://10.1.1.3:8080.

Configuration Scripts

- public

```
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/1
 assign interface GE0/0/3
 assign global-ip 10.1.1.2 10.1.1.2 exclusive
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/2
 assign interface GE0/0/4
 assign global-ip 10.1.1.3 10.1.1.3 exclusive
#
return
```

- vsysa

```
#
interface GE0/0/1
 ip address 10.1.1.8 255.255.255.0
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
 nat server to_public_server protocol tcp global 10.1.1.2 8080 inside 10.3.0.2 www no-reverse route
#
return
```

- vsysb

```
#
interface GE0/0/2
 ip address 10.1.1.9 255.255.255.0
#
interface GE0/0/4
 ip address 10.3.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
 nat server to_public_server protocol tcp global 10.1.1.3 8080 inside 10.3.1.2 www no-reverse route
#
return
```

6.17 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through Independent WAN Interfaces of the Virtual Systems

Networking Requirements

As shown in **Figure 6-17**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network

 Copyright © Huawei Technologies Co., Ltd.

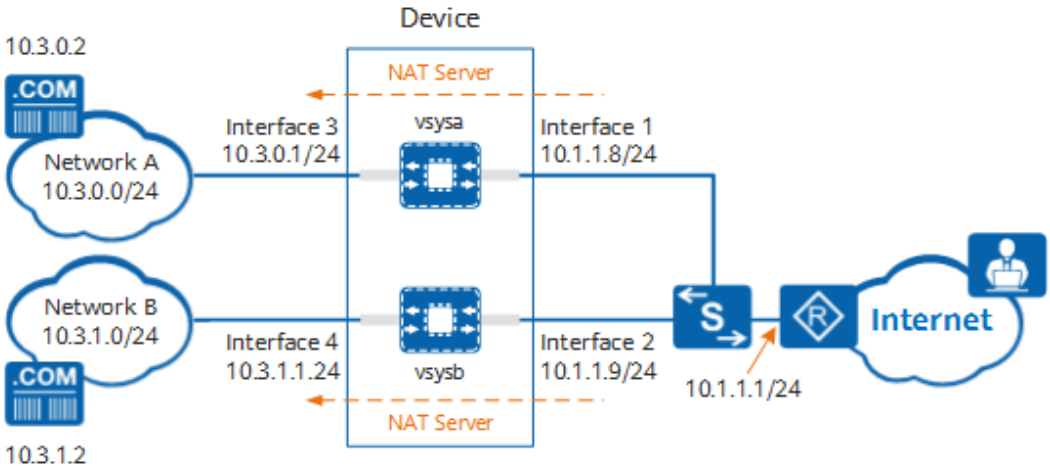
A and network B, which are isolated from each other and therefore cannot communicate with each other.

User hosts on the Internet access servers on networks A and B through the independent WAN interface interface 1 of vsysa and the independent WAN interface interface 2 of vsysb. In addition, NAT Server is configured for each virtual system. User hosts on the Internet can access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Figure 6-17 Configuring Internet users to access intranet servers of virtual systems through independent WAN interfaces of the virtual systems

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4, respectively.



Item	Data	Description
vsysa	Virtual system name: vsysa WAN interface: GE 0/0/1 WAN interface IP address: 10.1.1.8/24 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the LAN interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.0.2:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.1.1.2:8080	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb WAN interface: GE 0/0/2 WAN interface IP address: 10.1.1.9/24 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/4 LAN interface IP address: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the LAN interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.1.2:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.1.1.3:8080	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for vsysa and vsysb, and add the interfaces to security zones.
4. Configure routes in vsysa and vsysb to divert traffic from the Internet to networks A and B.
5. Configure security policies in vsysa and vsysb based on service requirements to permit traffic from user hosts on the Internet to servers on networks A and B.
6. Configure NAT Server in both vsysa and vsysb to enable user hosts on the Internet to access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/1
[Device-vsys-vsysa] assign interface ge 0/0/3
[Device-vsys-vsysa] assign global-ip 10.1.1.2 10.1.1.2 exclusive
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/2
[Device-vsys-vsysb] assign interface ge 0/0/4
[Device-vsys-vsysb] assign global-ip 10.1.1.3 10.1.1.3 exclusive
[Device-vsys-vsysb] quit
```

Step 4 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 5 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/1
[Device-vsysa-GE0/0/1] ip address 10.1.1.8 24
[Device-vsysa-GE0/0/1] quit
[Device-vsysa] interface ge 0/0/3
[Device-vsysa-GE0/0/3] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/3] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/3
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface ge 0/0/1
[Device-vsysa-zone-untrust] quit
```

Step 6 Configure a route from the Internet to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 7 Configure a route from the vsysa to the Internet, diverting the return traffic for the Internet to access network A to the Internet. 10.1.1.1 is the next-hop address of the route from the vsysa to the Internet.

```
[Device-vsysa] ip route-static 0.0.0.0 0 10.1.1.1
```

Step 8 Configure a security policy to permit traffic from user hosts on the Internet to servers on network A.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_network_allow
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-policy-security-rule-to_network_allow] source-zone untrust
[Device-vsysa-policy-security-rule-to_network_allow] destination-zone trust
[Device-vsysa-policy-security-rule-to_network_allow] destination-address 10.3.0.0 24
[Device-vsysa-policy-security-rule-to_network_allow] action permit
[Device-vsysa-policy-security-rule-to_network_allow] quit
[Device-vsysa-policy-security] quit
```

Step 9 Configure NAT Server to enable user hosts on the Internet to access servers on network A through a public IP address.

```
[Device-vsysa] nat server to_public_server protocol tcp global 10.1.1.2 8080 inside 10.3.0.2 www no-reverse route
```

Step 10 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 11 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/2
[Device-vsysb-GE0/0/2] ip address 10.1.1.9 24
[Device-vsysb-GE0/0/2] quit
[Device-vsysb] interface ge 0/0/4
[Device-vsysb-GE0/0/4] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/4] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/4
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface ge 0/0/2
[Device-vsysb-zone-untrust] quit
```

Step 12 Configure a route from the Internet to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 13 Configure a route from the vsysb to the Internet, diverting the return traffic for the Internet to access network B to the Internet. 10.1.1.1 is the next-hop address of the route from the vsysb to the Internet.

```
[Device-vsysb] ip route-static 0.0.0.0 0 10.1.1.1
```

Step 14 Configure a security policy to permit traffic from user hosts on the Internet to servers on network B.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_network_allow
[Device-vsysb-policy-security-rule-to_network_allow] source-zone untrust
[Device-vsysb-policy-security-rule-to_network_allow] destination-zone trust
[Device-vsysb-policy-security-rule-to_network_allow] destination-address 10.3.1.0 24
[Device-vsysb-policy-security-rule-to_network_allow] action permit
[Device-vsysb-policy-security-rule-to_network_allow] quit
[Device-vsysb-policy-security] quit
```

Step 15 Configure NAT Server to enable user hosts on the Internet to access servers on network B through a public IP address.

```
[Device-vsysb] nat server to_public_server protocol tcp global 10.1.1.3 8080 inside 10.3.1.2 www no-reverse route
```

----End

Verifying the Configuration

- User hosts on the Internet can access the web server at 10.3.0.2 on network A through http://10.1.1.2:8080.

 Copyright © Huawei Technologies Co., Ltd.

- User hosts on the Internet can access the web server at 10.3.1.2 on network B through http://10.1.1.3:8080.

Configuration Scripts

- Public system

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/1
 assign interface GE0/0/3
 assign global-ip 10.1.1.2 10.1.1.2 exclusive
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/2
 assign interface GE0/0/4
 assign global-ip 10.1.1.3 10.1.1.3 exclusive
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/1
 ip address 10.1.1.8 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
 nat server to_public_server protocol tcp global 10.1.1.2 8080 inside 10.3.0.2 www no-reverse route
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/2
 ip address 10.1.1.9 255.255.255.0
#
interface GE0/0/4
 ip address 10.3.1.1 255.255.255.0
#
firewall zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
 nat server to_public_server protocol tcp global 10.1.1.3 8080 inside 10.3.1.2 www no-reverse route
#
return
```

6.18 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the Public Network Interface of the Public System (Performing NAT in the Public System)

Networking Requirements

As shown in **Figure 6-18**, Device functions as a Layer 3 gateway and is deployed between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have no overlapping IP addresses.

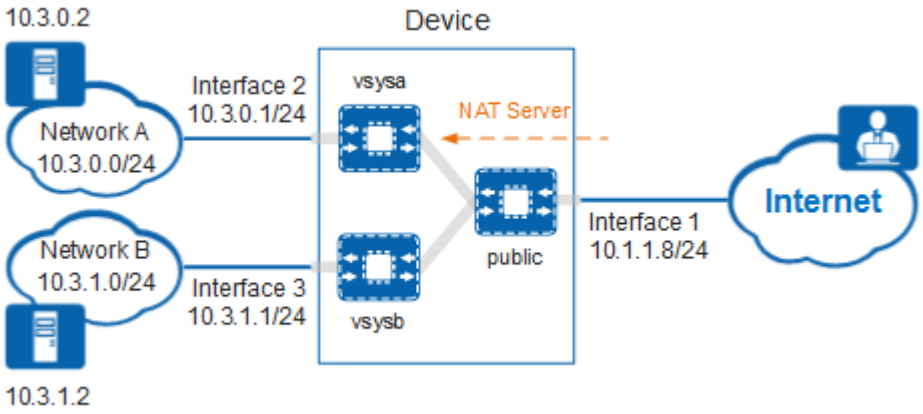
User hosts on the Internet access servers on networks A and B through the shared public network interface 1 of the public system. In addition, the NAT Server is configured for the public system. User hosts on the Internet can access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Figure 6-18 Configuring Internet users to access intranet servers of virtual systems through the public network interface of the public system (performing NAT in the public system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
public	Public network interface:GE0/0/1 IP address of the public network interface: 10.1.1.8/24 Security zone to which the public network interface belongs: Untrust Private network interface: Virtual-if0 of the public system Security zone to which the private network interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, all intranet servers provide services for Internet users through the public network interface of the public system. As the private IP addresses of networks A and B attached to the virtual systems do not overlap, you can configure the NAT Server in the public system.
vsysa	Virtual system name: vsysa Public network interface: virtual interface Virtual-if1 of vsysa Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/2 IP address of the private network interface: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the private network interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.0.2:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.1.1.2:8080	In this example, you can configure the NAT Server to enable user hosts on the Internet to access the server at 10.3.0.2 on network A through the IP address 10.1.1.2.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb Public network interface: virtual interface Virtual-if2 of vsysb Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/3 IP address of the private network interface: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the private network interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.1.2:80 Public IP address and port after NAT of the intranet server for Internet users: 10.1.1.3:8080	In this example, you can configure the NAT Server to enable user hosts on the Internet to access the server at 10.3.1.2 on network B through the IP address 10.1.1.3.
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

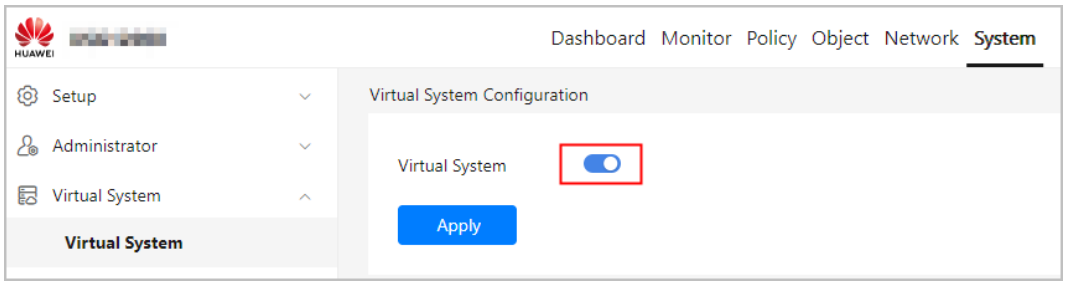
Do as follows on the public system, **vsysa**, and **vsysb** as required:

1. Enable the virtual system function.
2. Configure the resource class based on service requirements, create virtual systems **vsysa** and **vsysb** in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, **vsysa**, and **vsysb**, and add the interfaces to security zones.
4. Configure routes in the public system, **vsysa**, and **vsysb** to divert traffic from the Internet to networks A and B.
5. Configure security policies in the public system, **vsysa**, and **vsysb** based on service requirements to permit traffic from user hosts on the Internet to servers on networks A and B.
6. Configure the NAT Server in the public system to enable user hosts on the Internet to access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

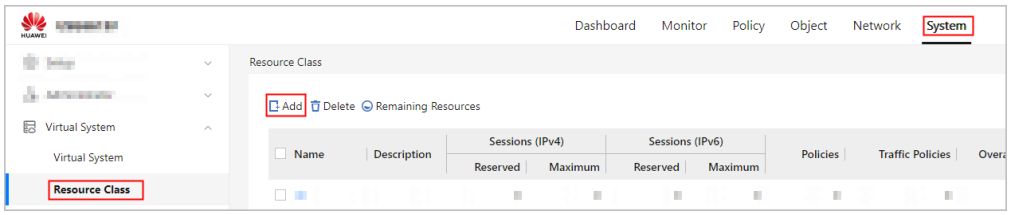
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.

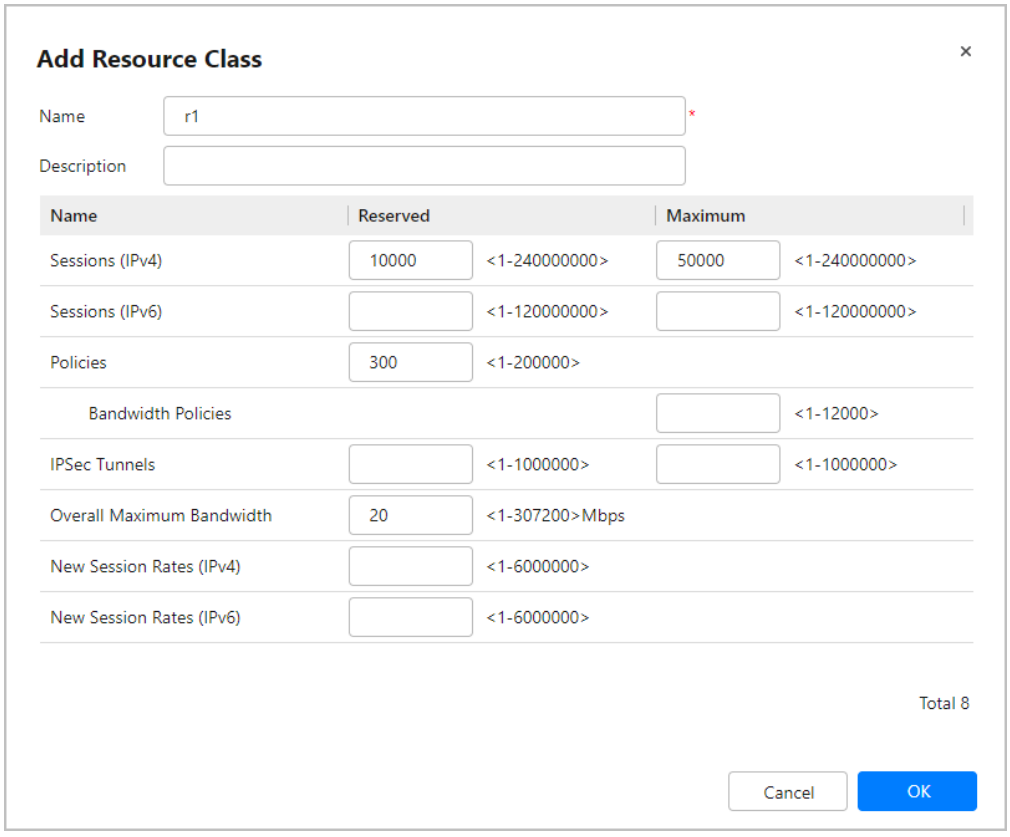


Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



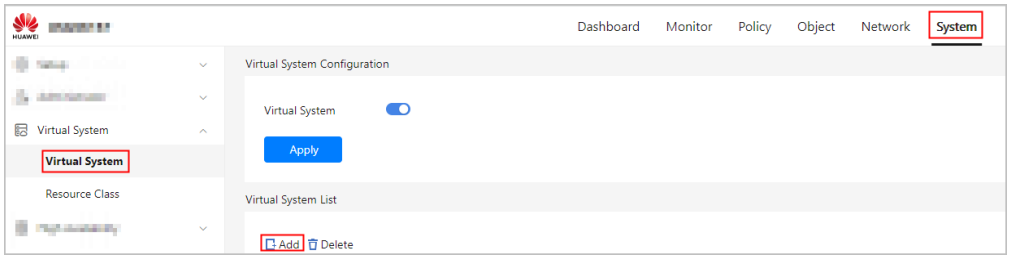
2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



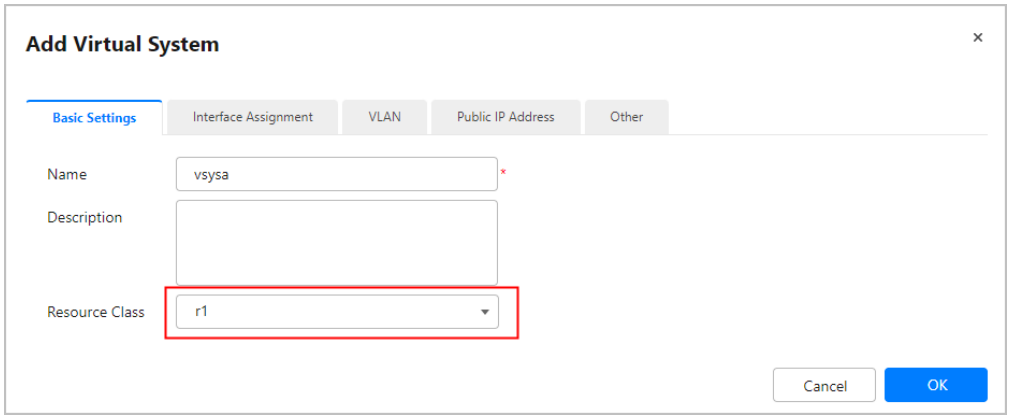
Step 3 In the public system, create virtual system **vsysa** and allocate resources. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

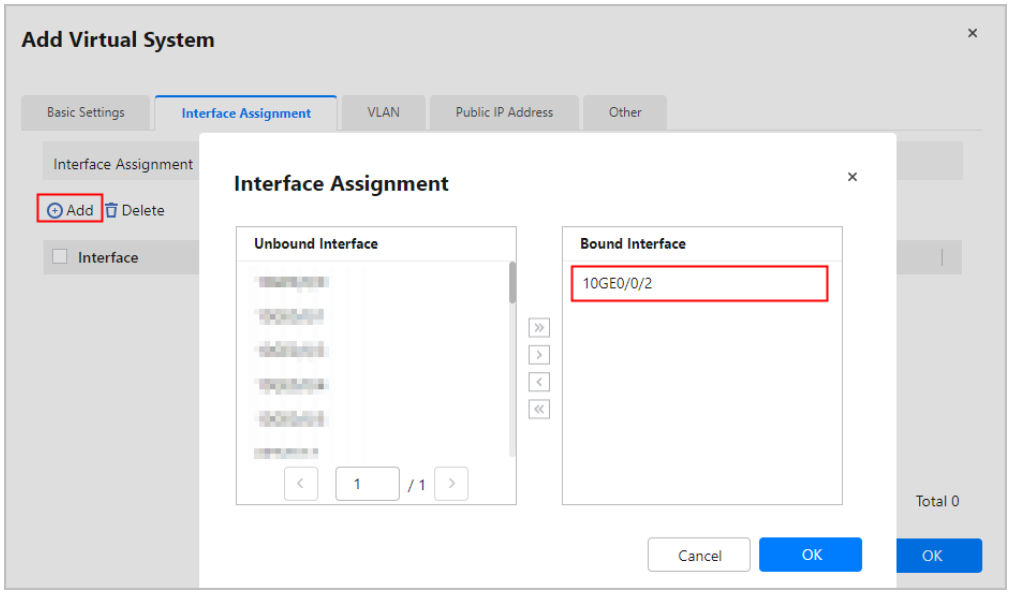
1. Choose **System** > **Virtual System** > **Virtual System**.



2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



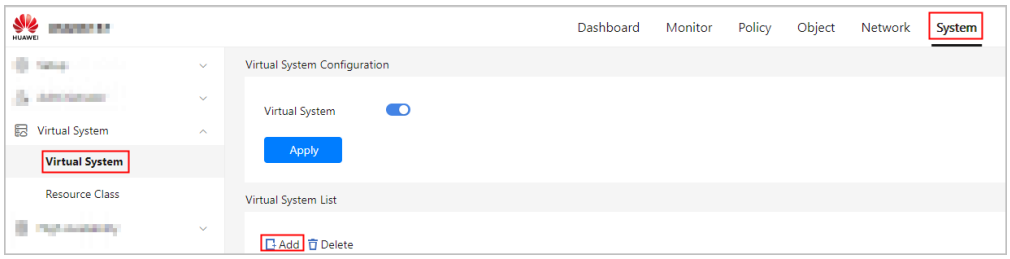
3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



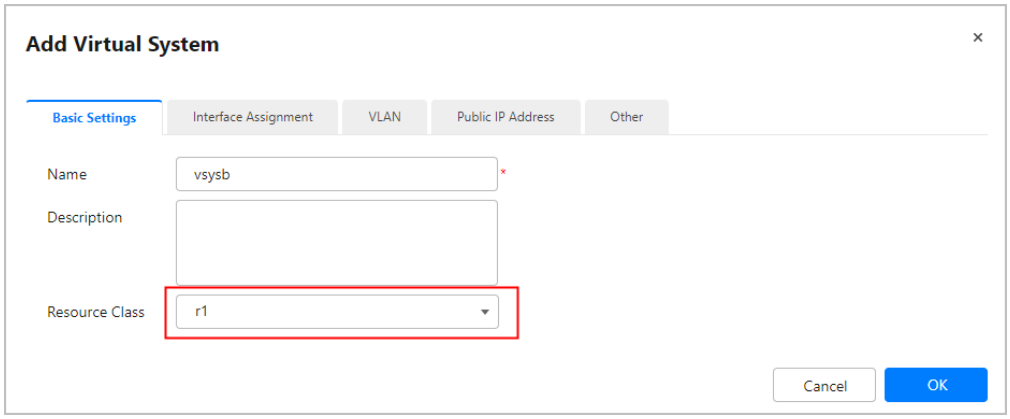
Step 4 In the public system, create virtual system **vsysb** and allocate resources. After the configuration is complete, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

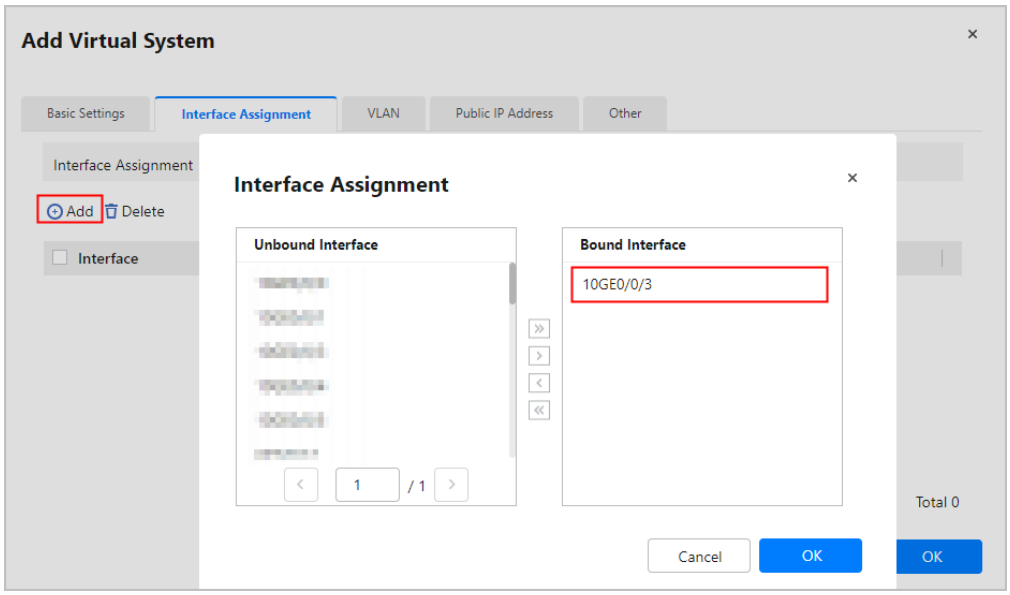
 Copyright © Huawei Technologies Co., Ltd.



2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



Step 5 Configure interfaces for the public system and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE 0/0/1 and set the following parameters. After the configuration is complete, click **OK**.

Zone	untrust
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

IP Address	10.1.1.8/24

3. Repeat the preceding steps to configure **Virtual-if0**.

Zone	trust
IPv4	
IP Address	172.16.0.1/24

Step 6 Configure a security policy in the public system.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an untrust-to-trust security policy to permit traffic of user hosts on the Internet to access servers of networks A and B. After the configuration is complete, click **OK**.

Name	untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.0.0/24
Destination Address	10.3.1.0/24
Action	Permit

Step 7 Configure routes in the public system.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the public system to the Internet. **10.1.1.1** is the next-hop address of the route from the public system to the Internet. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

4. Repeat the preceding steps to configure a route from the public network to **vsysa** to divert traffic from the Internet to the server of network A.

Protocol	IPv4
Source Virtual Router	public

 Copyright © Huawei Technologies Co., Ltd.

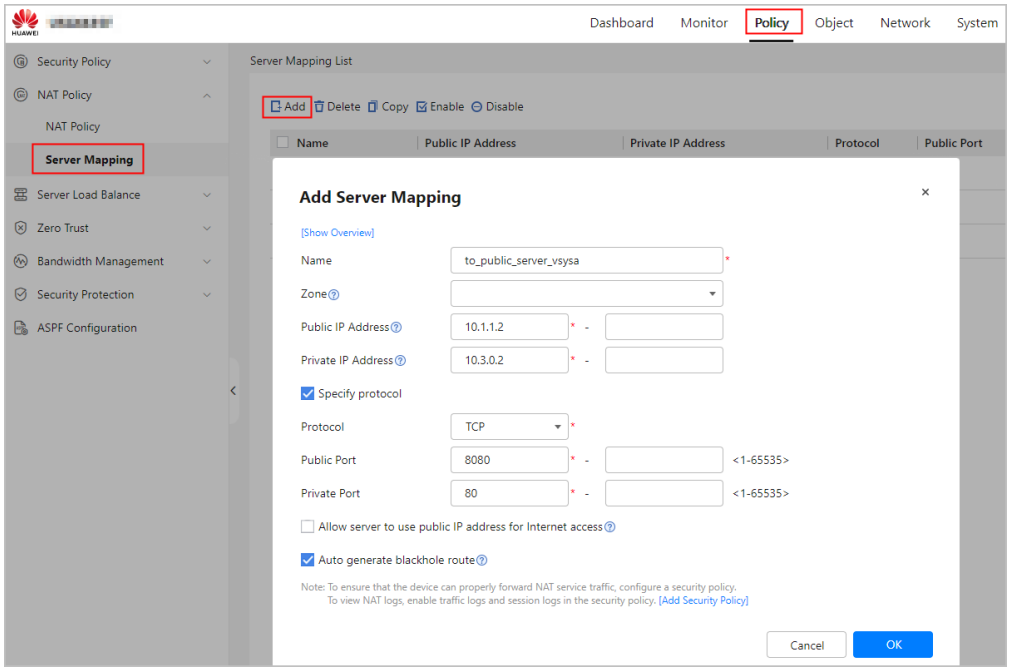
Destination Address/Mask	10.3.0.0/24
Destination Virtual Router	vsysa

5. Repeat the preceding steps to configure a route from the public network to **vsysb** to divert traffic from the Internet to the server of network B.

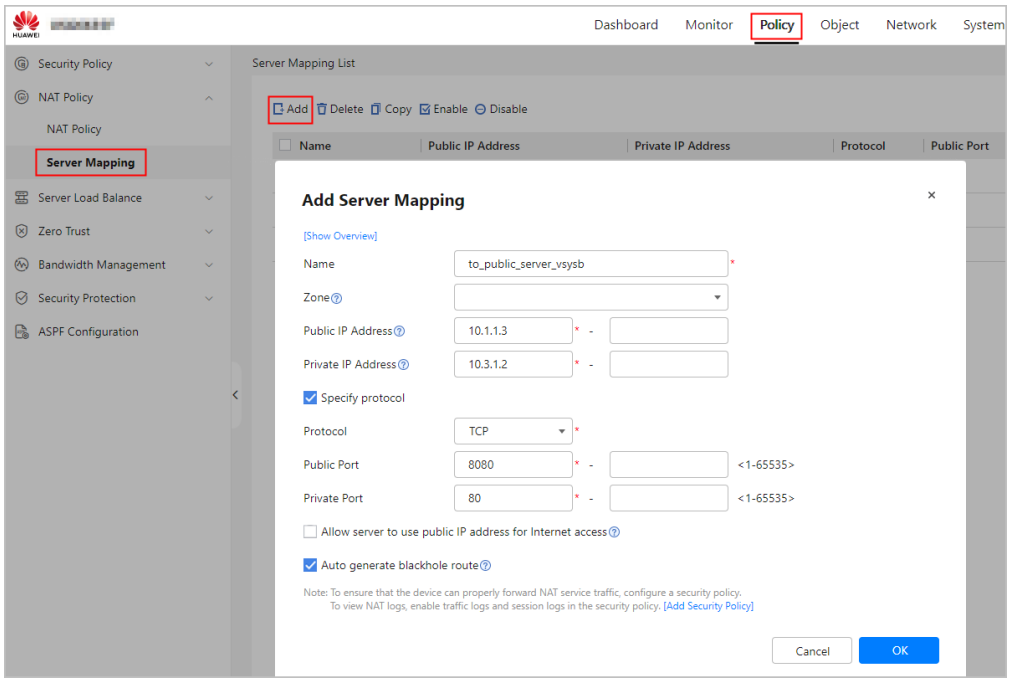
Protocol	IPv4
Source Virtual Router	public
Destination Address/Mask	10.3.1.0/24
Destination Virtual Router	vsysb

Step 8 Configure server mapping (NAT Server) in the public system.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.
2. Click **Add**.
3. Configure the NAT Server to enable user hosts on the Internet to access servers on networks A and B through public IP addresses. After the configuration is complete, click **OK**.

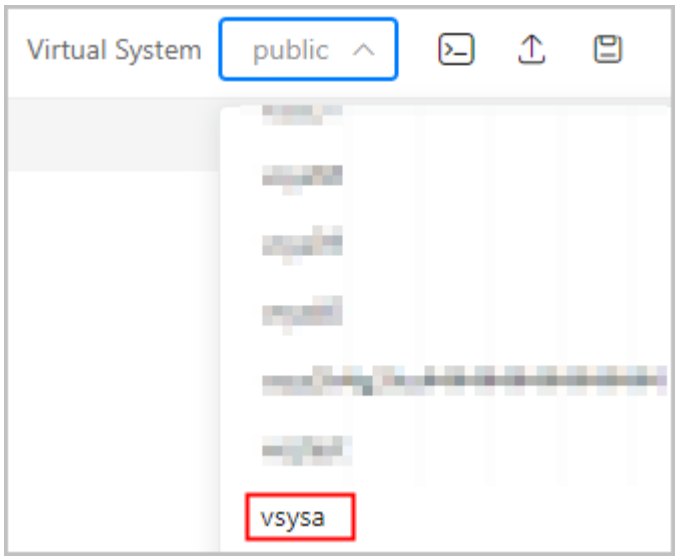


 Copyright © Huawei Technologies Co., Ltd.



Step 9 Add interfaces of **vsysa** to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/2 and set the following parameters. After the configuration is complete, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps to configure **Virtual-if1**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 10 Configure security policies in **vsysa**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an untrust-to-trust security policy to permit user hosts on the Internet to access servers of network A. After the configuration is complete, click **OK**.

Name	to_network_allow
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.0.2
Action	Permit

Step 11 Configure routes in **vsysa**.

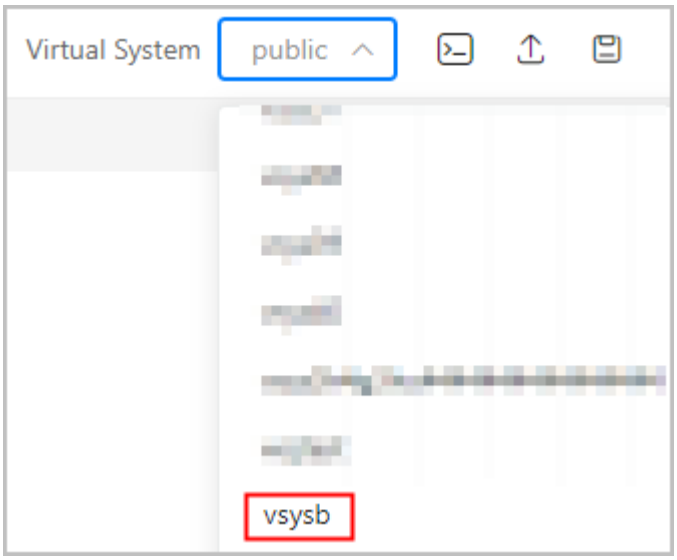
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysa** to network A. **10.3.0.254** is the next-hop address of the route from **vsysa** to network A. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.0.0/24
Next Hop	10.3.0.254

Step 12 Add interfaces of **vsysb** to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.

 Copyright © Huawei Technologies Co., Ltd.



2. Choose **Network** > **Interface**.
3. Click corresponding to GE 0/0/3 and set the following parameters. After the configuration is complete, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

4. Repeat the preceding steps to configure **Virtual-if2**.

Zone	untrust
IPv4	
IP Address	172.16.2.1/24

Step 13 Configure security policies in **vsysb**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an untrust-to-trust security policy to permit user hosts on the Internet to access servers of network B. After the configuration is complete, click **OK**.

Name	to_network_allow
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.1.2
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Step 14 Configure routes in **vsysb**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from **vsysb** to network B. **10.3.1.254** is the next-hop address of the route from **vsysb** to network B. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.1.0/24
Next Hop	10.3.1.254

----End

Verifying the Configuration

- User hosts on the Internet can access the web server at 10.3.0.2 on network A through http://10.1.1.2:8080.
- User hosts on the Internet can access the web server at 10.3.1.2 on network B through http://10.1.1.3:8080.

Configuration Scripts

- public:

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
#
interface GE0/0/1
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
 ip route-static 10.3.0.0 24 vpn-instance vsysa
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip route-static 10.3.1.0 24 vpn-instance vsysb
#
security-policy
 rule name untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
 nat server to_public_server_vsysa protocol tcp global 10.1.1.2 8080 inside 10.3.0.2 www no-reverse
route
 nat server to_public_server_vsysb protocol tcp global 10.1.1.3 8080 inside 10.3.1.2 www no-reverse
route
#
return
```

- vsysa:

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

- vsysb:

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

6.19 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the WAN Interface of the Public System (Performing NAT in the Public System)

Networking Requirements

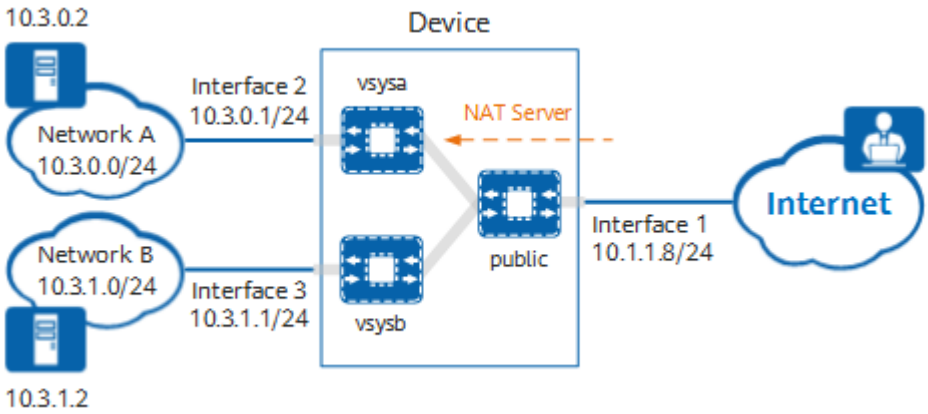
As shown in **Figure 6-19**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have no overlapping IP addresses.

User hosts on the Internet access servers on networks A and B through the shared WAN interface interface 1 of the public system. In addition, NAT Server is configured for the public system. User hosts on the Internet can access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Figure 6-19 Configuring Internet users to access intranet servers of virtual systems through the WAN interface of the public system (performing NAT in the public system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
public	WAN interface: GE 0/0/1 WAN interface IP address: 10.1.1.8/24 Security zone to which the WAN interface belongs: Untrust LAN interface: virtual interface Virtual-if0 of the public system Security zone to which the LAN interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, all intranet servers provide services for Internet users through the WAN interface of the public system. As the private IP addresses of networks A and B attached to the virtual systems do not overlap, you can configure NAT Server in the public system.
vsysa	Virtual system name: vsysa WAN interface: virtual interface Virtual-if1 of vsysa Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 LAN interface IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the LAN interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.0.2:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.1.1.2:8080	In this example, you can configure NAT Server to enable user hosts on the Internet to access the server at 10.3.0.2 on network A through the IP address 10.1.1.2.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb WAN interface: virtual interface Virtual-if2 of vsysb Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 10.3.1.1/24 Private IP address range: 10.3.1.0/24 Security zone to which the LAN interface belongs: Trust Private IP address and port of the intranet server for Internet users: 10.3.1.2:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.1.1.3:8080	In this example, you can configure NAT Server to enable user hosts on the Internet to access the server at 10.3.1.2 on network B through the IP address 10.1.1.3.
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.
4. Configure routes in the public system, vsysa, and vsysb to divert traffic from the Internet to networks A and B.
5. Configure security policies in the public system, vsysa, and vsysb based on service requirements to permit traffic from user hosts on the Internet to servers on networks A and B.
6. Configure NAT Server in the public system to enable user hosts on the Internet to access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] quit
```

Step 4 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 10.1.1.8 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 5 Configure routes in the public system.

Configure a route from the public system to the Internet. 10.1.1.1 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

Configure a route from the public system to vsysa to divert traffic from the Internet to network A.

```
[Device] ip route-static 10.3.0.0 24 vpn-instance vsysa
```

Configure a route from the public system to vsysb to divert traffic from the Internet to network B.

```
[Device] ip route-static 10.3.1.0 24 vpn-instance vsysb
```

Step 6 Configure a security policy in the public system to permit traffic from user hosts on the Internet to servers on networks A and B.

```
[Device] security-policy
[Device-policy-security] rule name untrust_to_trust
[Device-policy-security-rule-untrust_to_trust] source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-policy-security-rule-untrust_to_trust] destination-zone trust
[Device-policy-security-rule-untrust_to_trust] destination-address 10.3.0.0 24
[Device-policy-security-rule-untrust_to_trust] destination-address 10.3.1.0 24
[Device-policy-security-rule-untrust_to_trust] action permit
[Device-policy-security-rule-untrust_to_trust] quit
[Device-policy-security] quit
```

Step 7 Configure NAT Server to enable user hosts on the Internet to access servers on networks A and B through public IP addresses.

```
[Device] nat server to_public_server_vsysa protocol tcp global 10.1.1.2 8080 inside 10.3.0.2 www no-reverse route
[Device] nat server to_public_server_vsysb protocol tcp global 10.1.1.3 8080 inside 10.3.1.2 www no-reverse route
```

Step 8 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 9 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 10 Configure a route from vsysa to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
```

Step 11 Configure a security policy in vsysa to permit traffic from user hosts on the Internet to servers on network A.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_network_allow
[Device-vsysa-policy-security-rule-to_network_allow] source-zone untrust
[Device-vsysa-policy-security-rule-to_network_allow] destination-zone trust
[Device-vsysa-policy-security-rule-to_network_allow] destination-address 10.3.0.2 32
[Device-vsysa-policy-security-rule-to_network_allow] action permit
[Device-vsysa-policy-security-rule-to_network_allow] quit
[Device-vsysa-policy-security] quit
```

Step 12 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 13 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 14 Configure a route from vsysb to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
```

Step 15 Configure a security policy in vsysb to permit traffic from user hosts on the Internet to servers on network B.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_network_allow
[Device-vsysb-policy-security-rule-to_network_allow] source-zone untrust
[Device-vsysb-policy-security-rule-to_network_allow] destination-zone trust
[Device-vsysb-policy-security-rule-to_network_allow] destination-address 10.3.1.2 32
[Device-vsysb-policy-security-rule-to_network_allow] action permit
[Device-vsysb-policy-security-rule-to_network_allow] quit
[Device-vsysb-policy-security] quit
```

----End

Verifying the Configuration

- User hosts on the Internet can access the web server at 10.3.0.2 on network A through http://10.1.1.2:8080.
- User hosts on the Internet can access the web server at 10.3.1.2 on network B through http://10.1.1.3:8080.

Configuration Scripts

- Public system

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
#
interface GE0/0/1
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
 ip route-static 10.3.0.0 24 vpn-instance vsysa
 ip route-static 10.3.1.0 24 vpn-instance vsysb
#
security-policy
 rule name untrust_to_trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-zone trust
 destination-address 10.3.0.0 mask 255.255.255.0
 destination-address 10.3.1.0 mask 255.255.255.0
 action permit
#
 nat server to_public_server_vsysa protocol tcp global 10.1.1.2 8080 inside 10.3.0.2 www no-reverse
route
 nat server to_public_server_vsysb protocol tcp global 10.1.1.3 8080 inside 10.3.1.2 www no-reverse
route
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.0.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 10.3.1.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.1.0 mask 255.255.255.0
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

6.20 Web: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the Public Network Interface of the Public System (Performing NAT in Each Virtual System)

Networking Requirements

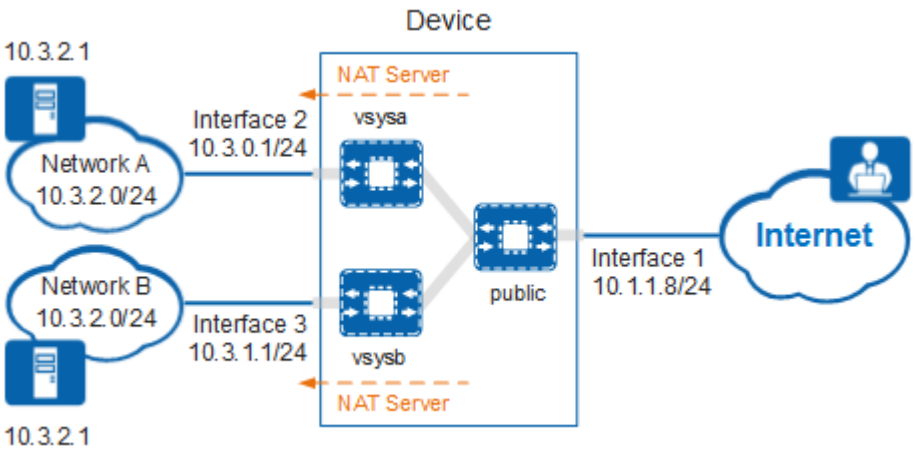
As shown in **Figure 6-20**, Device functions as a Layer 3 gateway and is deployed between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have overlapping IP addresses.

User hosts on the Internet access servers on networks A and B through the shared public network interface 1 of the public system. In addition, NAT Server is configured for each virtual system. User hosts on the Internet can access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Figure 6-20 Configuring Internet users to access intranet servers of virtual systems through the public network interface of the public system (performing NAT in each virtual system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
public	Public network interface:GE0/0/1 IP address of the public network interface: 10.1.1.8/24 Security zone to which the public network interface belongs: Untrust Private network interface: Virtual-if0 of the public system Security zone to which the private network interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, all intranet servers provide services for Internet users through the public network interface of the public system. As the private IP addresses of networks A and B attached to the virtual systems overlap, you need to configure the NAT Server for each virtual system.
vsysa	Virtual system name: vsysa Public network interface: virtual interface Virtual-if1 of vsysa Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/2 IP address of the private network interface: 10.3.0.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the private network interface belongs: Trust Private IP address and port of the intranet server: 10.3.2.1:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.10.1.1:8080	In this example, you can configure the NAT Server to enable user hosts on the Internet to access the server at 10.3.2.1 on network A through the IP address 10.10.1.1.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb Public network interface: virtual interface Virtual-if2 of vsysb Security zone to which the public network interface belongs: Untrust Private network interface:GE0/0/3 IP address of the private network interface: 10.3.1.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the private network interface belongs: Trust Private IP address and port of the intranet server: 10.3.2.1:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.10.1.2:8080	In this example, you can configure the NAT Server to enable user hosts on the Internet to access the server at 10.3.2.1 on network B through the IP address 10.10.1.2.
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

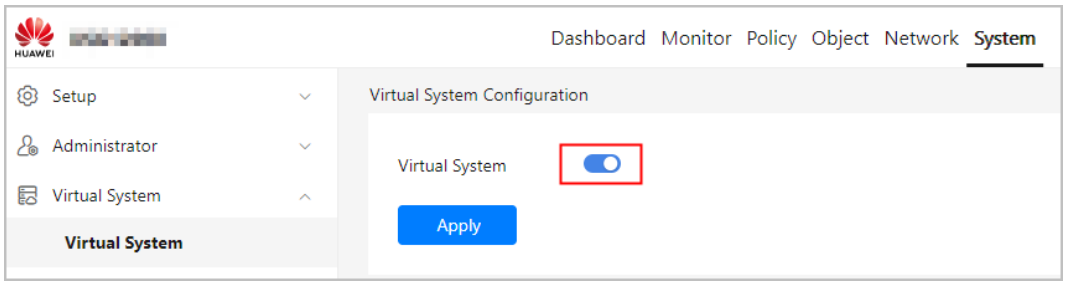
Do as follows on the public system, **vsysa**, and **vsysb** as required:

1. Enable the virtual system function.
2. Configure the resource class based on service requirements, create virtual systems **vsysa** and **vsysb** in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, **vsysa**, and **vsysb**, and add the interfaces to security zones.
4. Configure routes in the public system, **vsysa**, and **vsysb** to divert traffic from the Internet to networks A and B.
5. Configure security policies in the public system, **vsysa**, and **vsysb** based on service requirements to permit traffic from user hosts on the Internet to servers on networks A and B.
6. Configure server mapping (NAT Server) in both **vsysa** and **vsysb** to enable user hosts on the Internet to access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

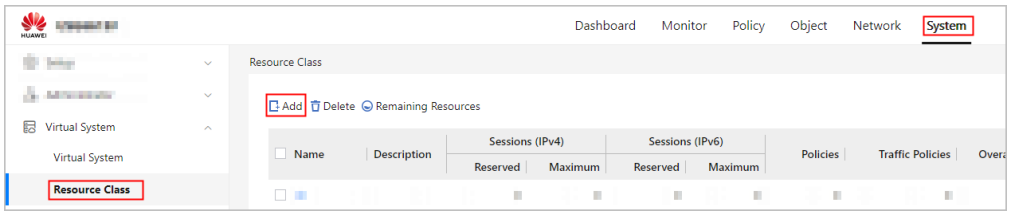
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.

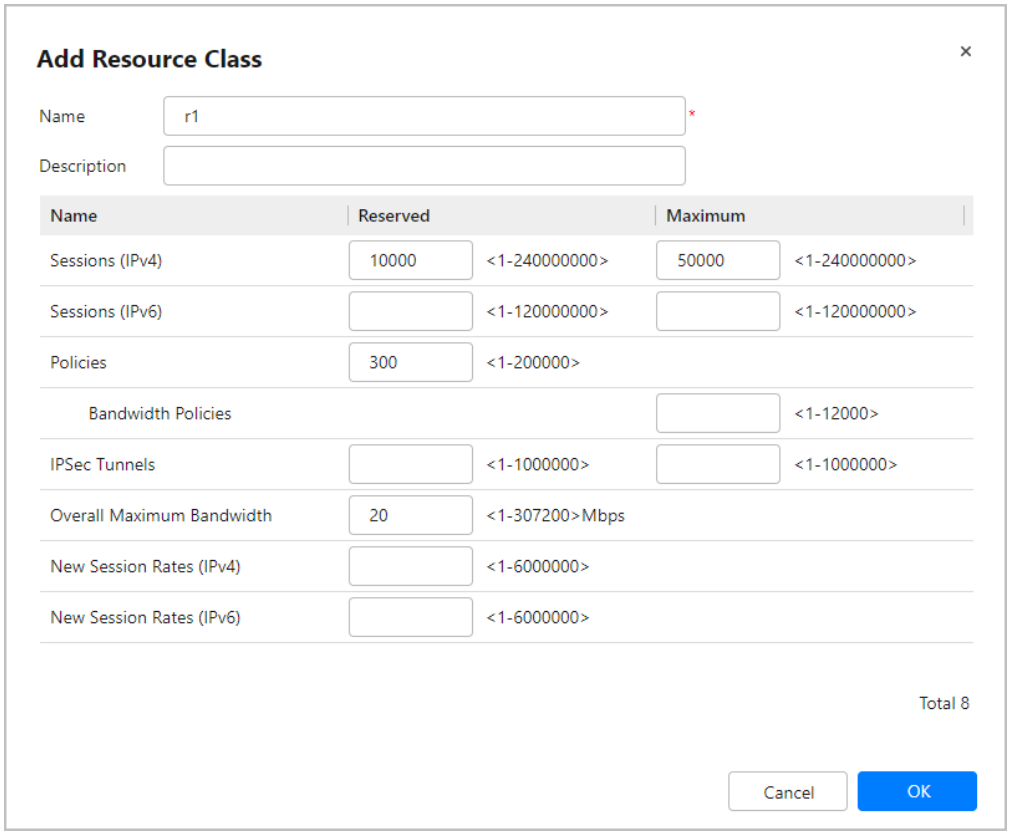


Step 2 Configure the virtual system resource class.

1. Choose **System** > **Virtual System** > **Resource Class**.



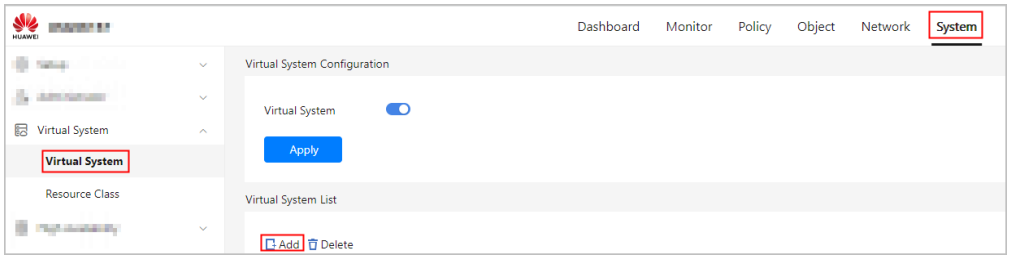
2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



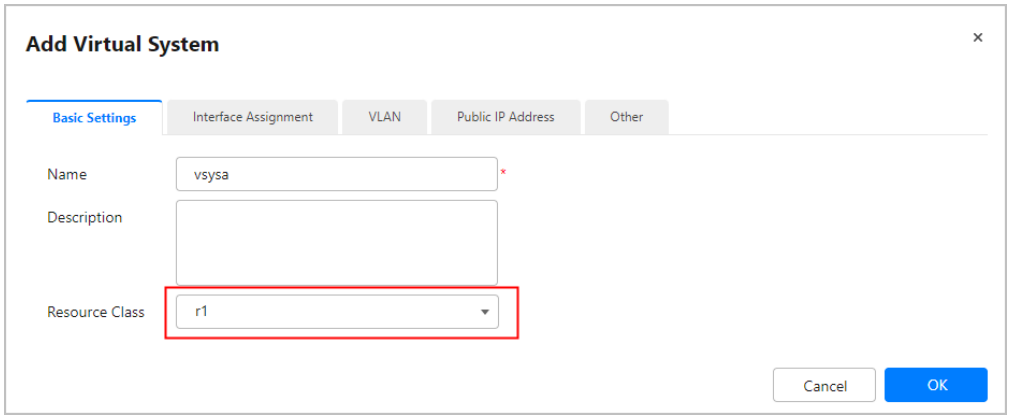
Step 3 In the public system, create virtual system **vsysa** and allocate resources. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

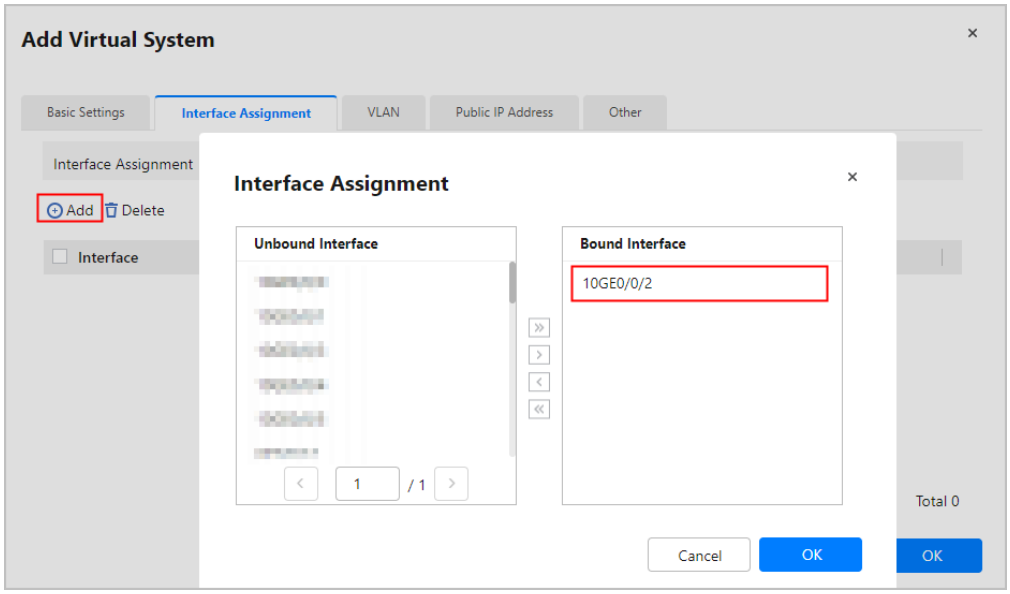
1. Choose **System** > **Virtual System** > **Virtual System**.



2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

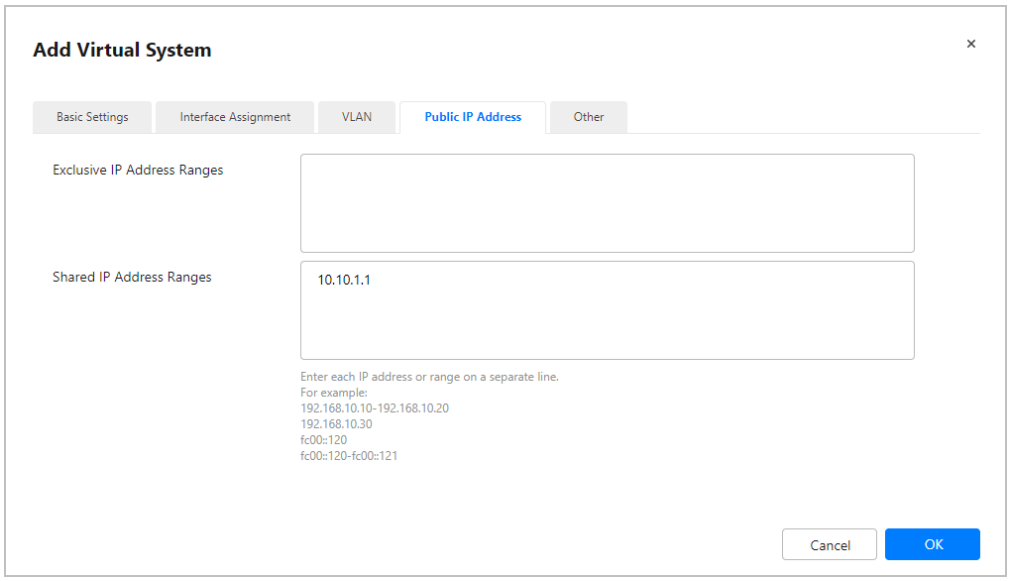


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



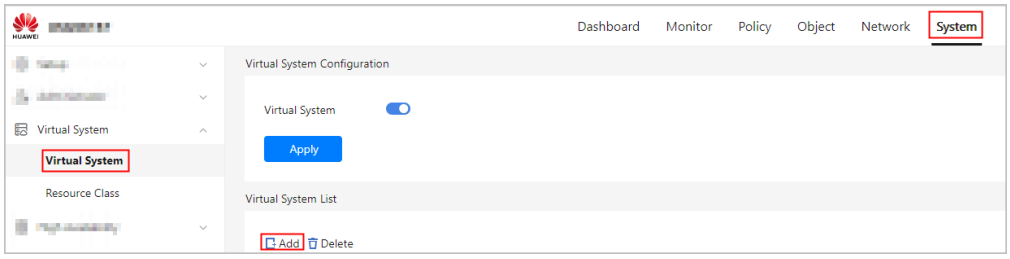
4. Click the **Public IP Address** tab and allocate a public IP address to the virtual system.

 Copyright © Huawei Technologies Co., Ltd.

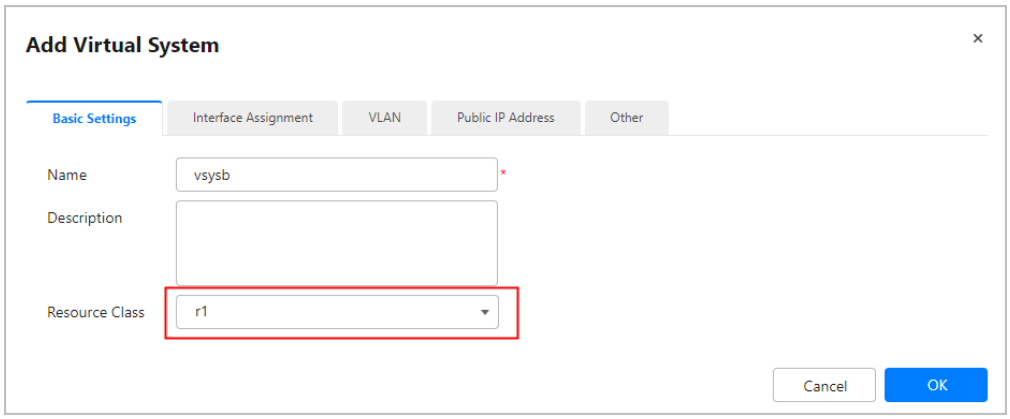


Step 4 In the public system, create virtual system **vsysb** and allocate resources. After the configuration is complete, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

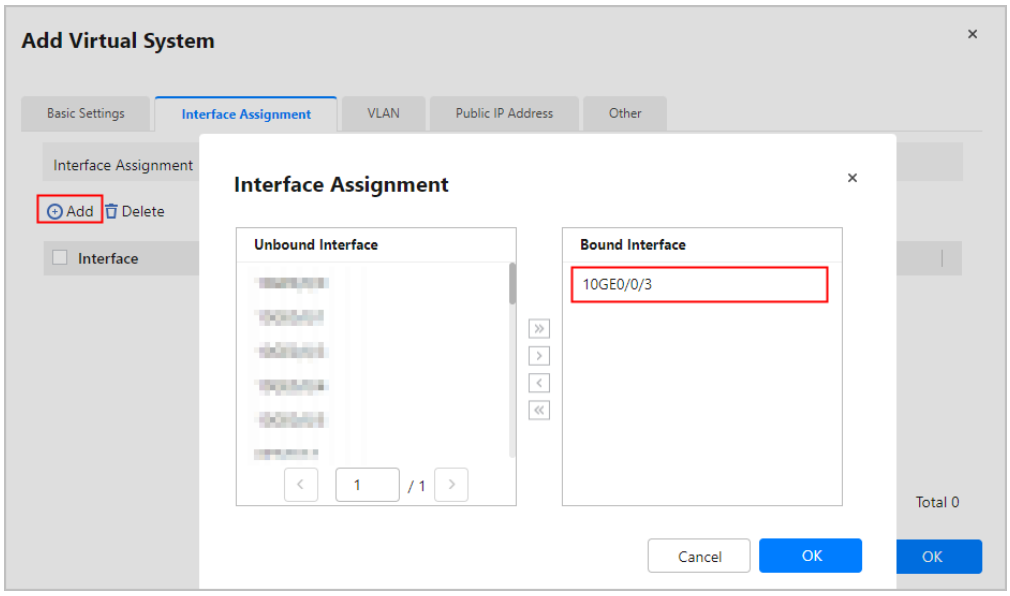


2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.

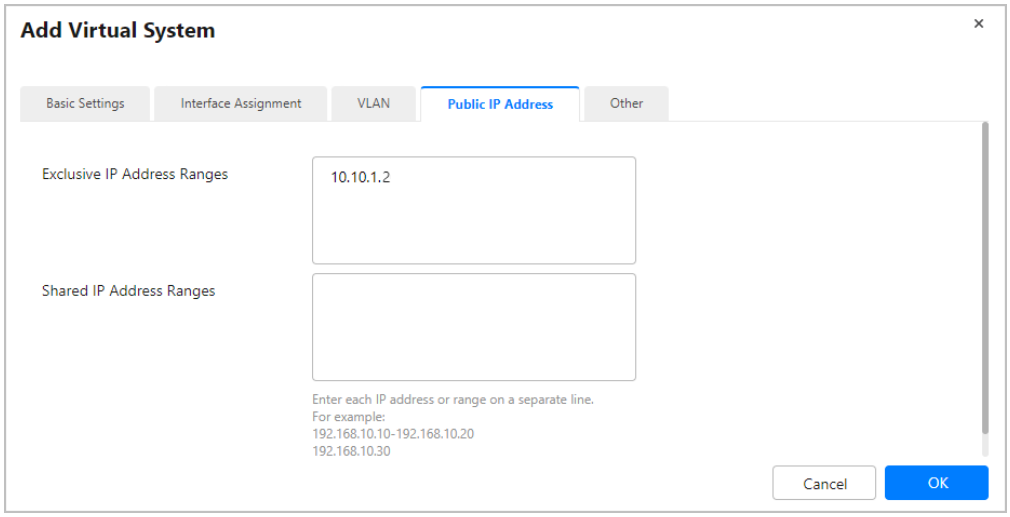


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.

 Copyright © Huawei Technologies Co., Ltd.



4. Click the **Public IP Address** tab and allocate a public IP address to the virtual system.



Step 5 Configure interfaces for the public system and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click and set the following parameters. After the configuration is complete, click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.1.8/24

3. Repeat the preceding steps to configure **Virtual-if0**.

Zone	trust
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

IP Address	172.16.0.1/24

Step 6 Configure a security policy in the public system.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an untrust-to-trust security policy to permit user hosts on the Internet to access servers of networks A and B. After the configuration is complete, click **OK**.

Name	untrust_to_trust
Source Zone	untrust
Destination Zone	trust
Destination Address	10.10.1.1/32
Destination Address	10.10.1.2/32
Action	Permit

Step 7 Configure routes in the public system.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a route from the public system to the Internet. **10.1.1.1** is the next-hop address of the route from the public system to the Internet. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.1

4. Repeat the preceding steps to configure a route from the public network to **vsysa** to divert traffic from the Internet to the server of network A.

Protocol	IPv4
Source Virtual Router	public
Destination Address/Mask	10.10.1.1/32
Destination Virtual Router	vsysa

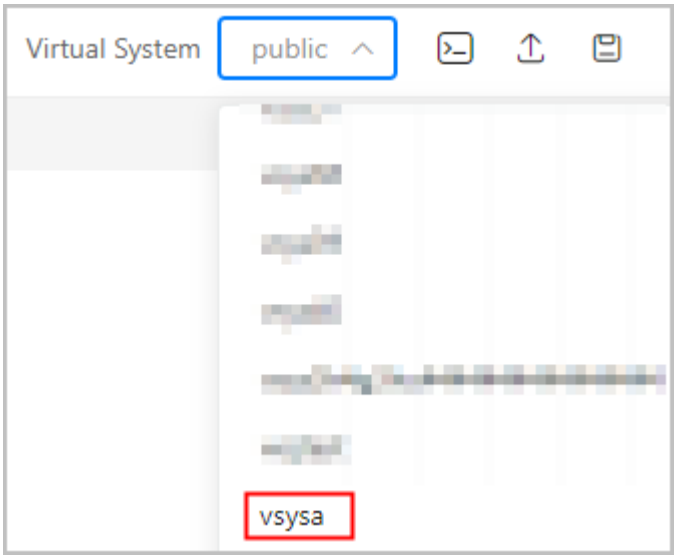
5. Repeat the preceding steps to configure a route from the public network to **vsysb** to divert traffic from the Internet to the server of network B.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv4
Source Virtual Router	public
Destination Address/Mask	10.10.1.2/32
Destination Virtual Router	vsysb

Step 8 Add interfaces of **vsysa** to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.



2. Choose **Network** > **Interface**.
3. Click and set the following parameters. After the configuration is complete, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

4. Repeat the preceding steps to configure **Virtual-if1**.

Zone	untrust
IPv4	
IP Address	172.16.1.1/24

Step 9 Configure security policies in **vsysa**.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an untrust-to-trust security policy to permit user hosts on the Internet to access servers of network A. After the configuration is complete, click **OK**.

Name	to_network_allow
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.2.1
Action	Permit

Step 10 Configure routes in **vsysa**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.

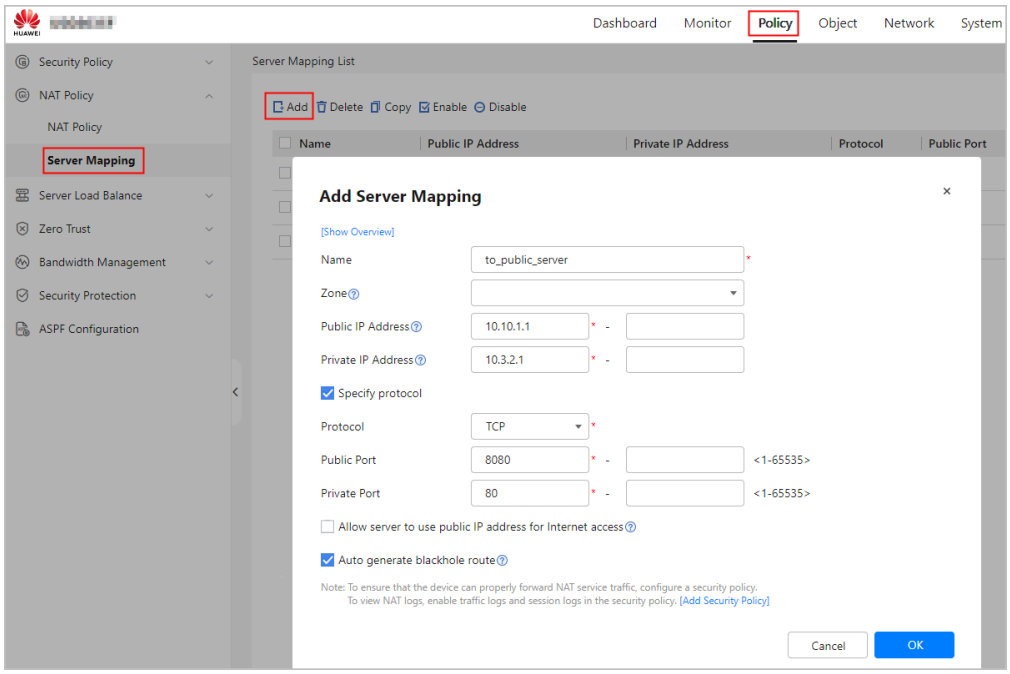
   Configure a route from **vsysa** to network A. 10.3.0.254 is the next-hop address of the route from **vsysa** to network A. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.2.0/24
Next Hop	10.3.0.254

Step 11 Configure server mapping (NAT Server) in **vsysa**.

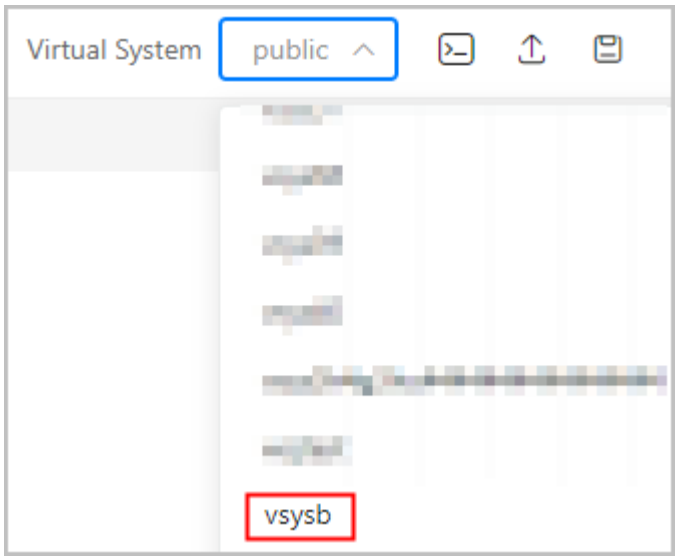
1. Choose **Policy** > **NAT Policy** > **Server Mapping**.
2. Click **Add**.
3. Configure the NAT Server to enable user hosts on the Internet to access servers on network A through a public IP address. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 12 Add interfaces of **vsysb** to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.



2. Choose **Network** > **Interface**.
3. Click and set the following parameters. After the configuration is complete, click **OK**.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

4. Repeat the preceding steps to configure **Virtual-if2**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv4	
IP Address	172.16.2.1/24

Step 13 Configure security policies in **vsysb**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure an untrust-to-trust security policy to permit user hosts on the Internet to access servers of network B. After the configuration is complete, click **OK**.

Name	to_network_allow
Source Zone	untrust
Destination Zone	trust
Destination Address	10.3.2.1
Action	Permit

Step 14 Configure routes in **vsysb**.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.

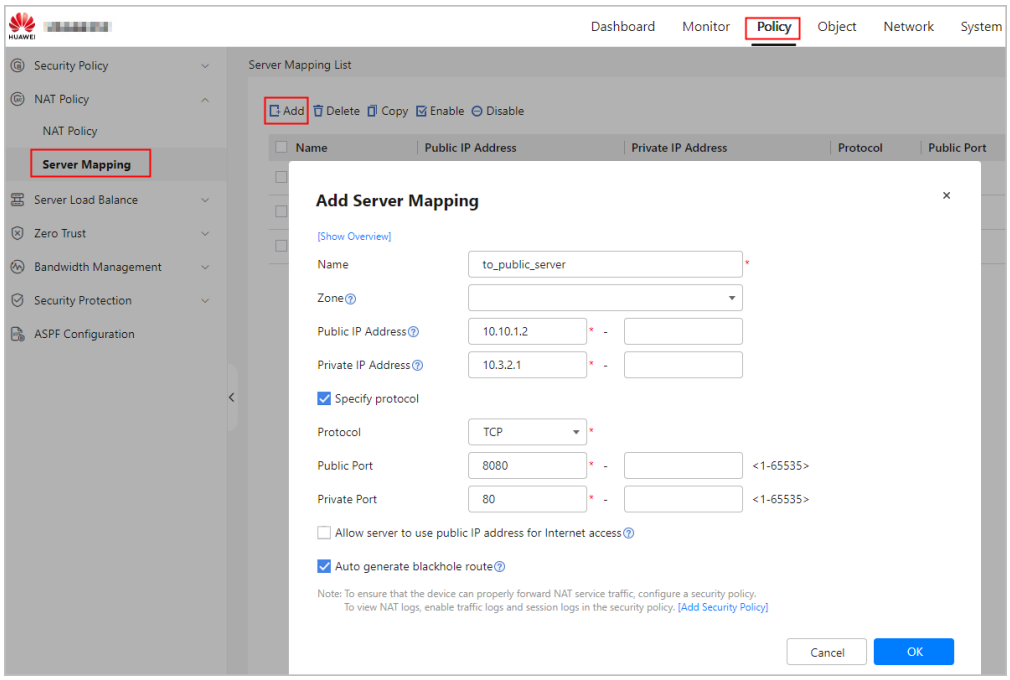
   Configure a route from **vsysb** to network B. **10.3.1.254** is the next-hop address of the route from **vsysb** to network B. After the configuration is complete, click **OK**.

Protocol	IPv4
Destination Address/Mask	10.3.2.0/24
Next Hop	10.3.1.254

Step 15 Configure server mapping (NAT Server) in **vsysb**.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.
2. Click **Add**.
3. Configure the NAT Server to enable user hosts on the Internet to access servers on network A through a public IP address. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



----End

Verifying the Configuration

- User hosts on the Internet can access the web server at 10.3.0.2 on network A through http://10.10.1.1:8080.
- User hosts on the Internet can access the web server at 10.3.1.2 on network B through http://10.10.1.2:8080.

Configuration Scripts

- public:

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
 assign global-ip 10.10.1.1 10.10.1.1 exclusive
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
 assign global-ip 10.10.1.2 10.10.1.2 exclusive
#
interface GE0/0/1
 ip address 10.1.1.8 24
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
 ip route-static 10.10.1.1 32 vpn-instance vsysa
 ip route-static 10.10.1.2 32 vpn-instance vsysb
#
security-policy
 rule name untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.10.1.1 mask 255.255.255.255
  destination-address 10.10.1.2 mask 255.255.255.255
  action permit
#
return
```

- vsysa:

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.2.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.2.1 mask 255.255.255.255
  action permit
#
 nat server to_public_server protocol tcp global 10.10.1.1 8080 inside 10.3.2.1 www no-reverse route
#
return
```

- vsysb:

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 10.3.2.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name to_network_allow
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-zone trust
 destination-address 10.3.2.1 mask 255.255.255.255
 action permit
#
 nat server to_public_server protocol tcp global 10.10.1.2 8080 inside 10.3.2.1 www no-reverse route
#
return
```

6.21 CLI: Example for Configuring Internet Users to Access Intranet Servers of Virtual Systems Through the WAN Interface of the Public System (Performing NAT in Each Virtual System)

Networking Requirements

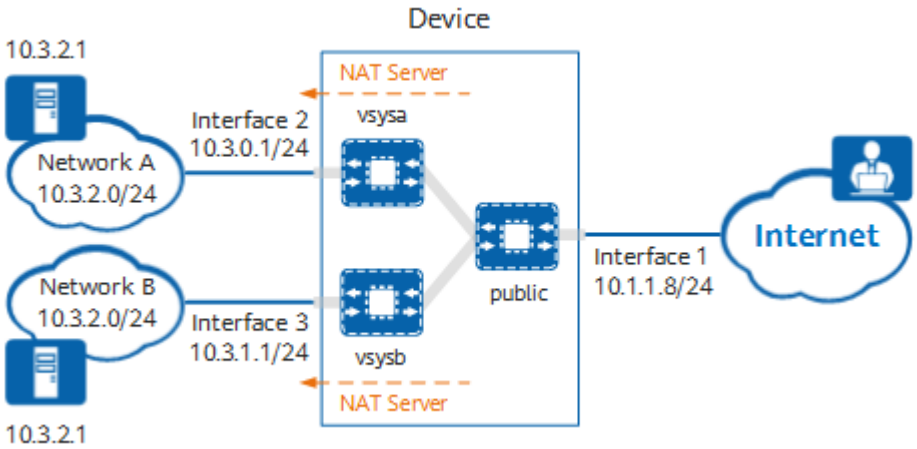
As shown in **Figure 6-21**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and have overlapping IP addresses.

User hosts on the Internet access servers on networks A and B through the shared WAN interface interface 1 of the public system. In addition, NAT Server is configured for each virtual system. User hosts on the Internet can access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Figure 6-21 Configuring Internet users to access intranet servers of virtual systems through the WAN interface of the public system (performing NAT in each virtual system)

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
public	WAN interface: GE 0/0/1 WAN interface IP address: 10.1.1.8/24 Security zone to which the WAN interface belongs: Untrust LAN interface: virtual interface Virtual-if0 of the public system Security zone to which the LAN interface belongs: Trust IP address of the carrier access gateway: 10.1.1.1/24	In this example, all intranet servers provide services for Internet users through the WAN interface of the public system. As the private IP addresses of networks A and B attached to the virtual systems overlap, you need to configure NAT Server for each virtual system.
vsysa	Virtual system name: vsysa WAN interface: virtual interface Virtual-if1 of vsysa Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 LAN interface IP address: 10.3.0.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the LAN interface belongs: Trust Private IP address and port of the intranet server: 10.3.2.1:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.10.1.1:8080	In this example, you can configure NAT Server to enable user hosts on the Internet to access the server at 10.3.2.1 on network A through the IP address 10.10.1.1.
vsysb	Virtual system name: vsysb WAN interface: virtual interface Virtual-if2 of vsysb Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 10.3.1.1/24 Private IP address range: 10.3.2.0/24 Security zone to which the LAN interface belongs: Trust Private IP address and port of the intranet server: 10.3.2.1:80 Post-NAT public IP address and port of the intranet server for Internet users: 10.10.1.2:8080	In this example, you can configure NAT Server to enable user hosts on the Internet to access the server at 10.3.2.1 on network B through the IP address 10.10.1.2.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.
4. Configure routes in the public system, vsysa, and vsysb to divert traffic from the Internet to networks A and B.
5. Configure security policies in the public system, vsysa, and vsysb based on service requirements to permit traffic from user hosts on the Internet to servers on networks A and B.
6. Configure NAT Server in both vsysa and vsysb to enable user hosts on the Internet to access specific servers on networks A and B attached to the virtual systems through independent public IP addresses.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/2
[Device-vsys-vsysa] assign global-ip 10.10.1.1 10.10.1.1 exclusive
[Device-vsys-vsysa] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/3
[Device-vsys-vsysb] assign global-ip 10.10.1.2 10.10.1.2 exclusive
[Device-vsys-vsysb] quit
```

Step 4 Configure interfaces for the public system and add the interfaces to security zones.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] ip address 10.1.1.8 24
[Device-GE0/0/1] quit
[Device] interface Virtual-if 0
[Device-Virtual-if0] ip address 172.16.0.1 24
[Device-Virtual-if0] quit
[Device] firewall zone trust
[Device-zone-trust] add interface Virtual-if 0
[Device-zone-trust] quit
[Device] firewall zone untrust
[Device-zone-untrust] add interface ge 0/0/1
[Device-zone-untrust] quit
```

Step 5 Configure routes in the public system.

Configure a route from the public system to the Internet. 10.1.1.1 is the next-hop address of the route from the public system to the Internet.

```
[Device] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

Configure a route from the public system to vsysa to divert traffic from the Internet to network A.

```
[Device] ip route-static 10.10.1.1 32 vpn-instance vsysa
```

Configure a route from the public system to vsysb to divert traffic from the Internet to network B.

```
[Device] ip route-static 10.10.1.2 32 vpn-instance vsysb
```

Step 6 Configure a security policy in the public system to permit traffic from user hosts on the Internet to servers on networks A and B.

```
[Device] security-policy
[Device-policy-security] rule name untrust_to_trust
[Device-policy-security-rule-untrust_to_trust] source-zone untrust
[Device-policy-security-rule-untrust_to_trust] destination-zone trust
[Device-policy-security-rule-untrust_to_trust] destination-address 10.10.1.1 32
[Device-policy-security-rule-untrust_to_trust] destination-address 10.10.1.2 32
[Device-policy-security-rule-untrust_to_trust] action permit
[Device-policy-security-rule-untrust_to_trust] quit
[Device-policy-security] quit
```

Step 7 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 8 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/2
[Device-vsysa-GE0/0/2] ip address 10.3.0.1 24
[Device-vsysa-GE0/0/2] quit
[Device-vsysa] interface Virtual-if 1
[Device-vsysa-Virtual-if1] ip address 172.16.1.1 24
[Device-vsysa-Virtual-if1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-zone-untrust] add interface Virtual-if 1
[Device-vsysa-zone-untrust] quit
```

Step 9 Configure a route from vsysa to network A. 10.3.0.254 is the next-hop address of the route from vsysa to network A.

```
[Device-vsysa] ip route-static 10.3.2.0 255.255.255.0 10.3.0.254
```

Step 10 Configure a security policy in vsysa to permit traffic from user hosts on the Internet to servers on network A.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_network_allow
[Device-vsysa-policy-security-rule-to_network_allow] source-zone untrust
[Device-vsysa-policy-security-rule-to_network_allow] destination-zone trust
[Device-vsysa-policy-security-rule-to_network_allow] destination-address 10.3.2.1 32
[Device-vsysa-policy-security-rule-to_network_allow] action permit
[Device-vsysa-policy-security-rule-to_network_allow] quit
[Device-vsysa-policy-security] quit
```

Step 11 Configure NAT Server in vsysa to enable user hosts on the Internet to access servers on network A through a public IP address.

```
[Device-vsysa] nat server to_public_server protocol tcp global 10.10.1.1 8080 inside 10.3.2.1 www no-reverse route
```

Step 12 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 13 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/3
[Device-vsysb-GE0/0/3] ip address 10.3.1.1 24
[Device-vsysb-GE0/0/3] quit
[Device-vsysb] interface Virtual-if 2
[Device-vsysb-Virtual-if2] ip address 172.16.2.1 24
[Device-vsysb-Virtual-if2] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/3
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface Virtual-if 2
[Device-vsysb-zone-untrust] quit
```

Step 14 Configure a route from vsysb to network B. 10.3.1.254 is the next-hop address of the route from vsysb to network B.

```
[Device-vsysb] ip route-static 10.3.2.0 255.255.255.0 10.3.1.254
```

Step 15 Configure a security policy in vsysb to permit traffic from user hosts on the Internet to servers on network B.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_network_allow
[Device-vsysb-policy-security-rule-to_network_allow] source-zone untrust
[Device-vsysb-policy-security-rule-to_network_allow] destination-zone trust
[Device-vsysb-policy-security-rule-to_network_allow] destination-address 10.3.2.1 32
[Device-vsysb-policy-security-rule-to_network_allow] action permit
[Device-vsysb-policy-security-rule-to_network_allow] quit
[Device-vsysb-policy-security] quit
```

Step 16 Configure NAT Server in vsysb to enable user hosts on the Internet to access servers on network B through a public IP address.

```
[Device-vsysb] nat server to_public_server protocol tcp global 10.10.1.2 8080 inside 10.3.2.1 www no-reverse route
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

- User hosts on the Internet can access the web server at 10.3.0.2 on network A through http://10.10.1.1:8080.
- User hosts on the Internet can access the web server at 10.3.1.2 on network B through http://10.10.1.2:8080.

Configuration Scripts

- Public system

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/2
 assign global-ip 10.10.1.1 10.10.1.1 exclusive
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/3
 assign global-ip 10.10.1.2 10.10.1.2 exclusive
#
interface GE0/0/1
 ip address 10.1.1.8 255.255.255.0
#
interface Virtual-if 0
 ip address 172.16.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
 ip route-static 10.10.1.1 255.255.255.255 vpn-instance vsysa
 ip route-static 10.10.1.2 255.255.255.255 vpn-instance vsysb
#
security-policy
 rule name untrust_to_trust
  source-zone untrust
  destination-zone trust
  destination-address 10.10.1.1 mask 255.255.255.255
  destination-address 10.10.1.2 mask 255.255.255.255
  action permit
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
interface Virtual-if 1
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface Virtual-if1
#
 ip route-static 10.3.2.0 255.255.255.0 10.3.0.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.2.1 mask 255.255.255.255
  action permit
#
 nat server to_public_server protocol tcp global 10.10.1.1 8080 inside 10.3.2.1 www no-reverse route
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface Virtual-if 2
 ip address 172.16.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtual-if2
#
 ip route-static 10.3.2.0 255.255.255.0 10.3.1.254
#
security-policy
 rule name to_network_allow
  source-zone untrust
  destination-zone trust
  destination-address 10.3.2.1 mask 255.255.255.255
  action permit
#
 nat server to_public_server protocol tcp global 10.10.1.2 8080 inside 10.3.2.1 www no-reverse route
#
return
```

6.22 Web: Example for Configuring Layer 2 Access for Virtual Systems

Networking Requirements

As shown in **Figure 6-22**, the device is deployed between the intranet and Internet and functions as a Layer 2 gateway. The intranet is divided into three independent LANs: network A, network B, and network C, which are isolated from one another and therefore cannot communicate with each other.

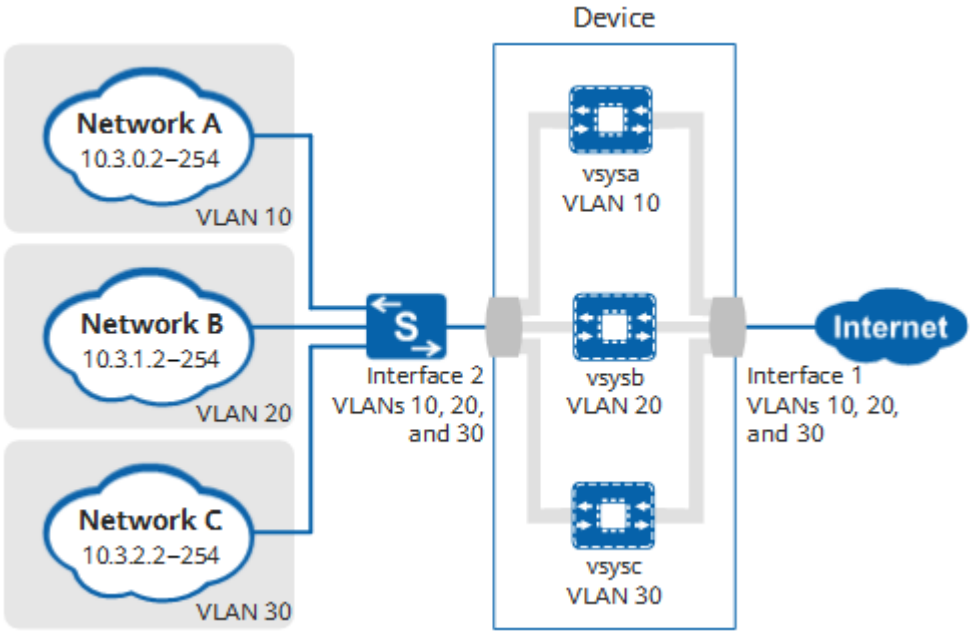
The three LANs belong to different VLANs and are isolated through virtual systems **vsysa**, **vsysb**, and **vsysc**. All user hosts on network C and some user hosts on network A are allowed to access the Internet, and all user hosts on network B are not allowed to access the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-22 Layer 2 access for virtual systems

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
vsysa	Virtual system name: vsysa Public network interface: GE 0/0/1 Security zone to which the public network interface belongs: Untrust Private network interface: GE 0/0/2 Security zone to which the public network interface belongs: Trust VLAN assigned: VLAN 10 IP addresses allowed to access the Internet: 10.3.0.2 to 10.3.0.10	-
vsysb	Virtual system name: vsysb Public network interface: GE 0/0/1 Security zone to which the public network interface belongs: Untrust Private network interface: GE 0/0/2 Security zone to which the public network interface belongs: Trust VLAN assigned: VLAN 20	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysc	Virtual system name: vsysc Public network interface: GE 0/0/1 Security zone to which the public network interface belongs: Untrust Private network interface: GE 0/0/2 Security zone to which the public network interface belongs: Trust VLAN assigned: VLAN 30	-
Resource Class	Name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A, B, and C have similar service resource usage requirements and therefore are allocated the same virtual system resources.

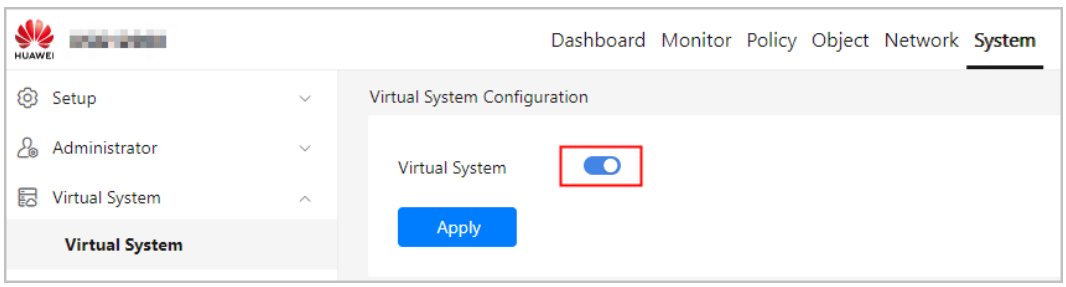
Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function and configure resource classes based on service requirements.
2. Create VLANs in the public system and add related interfaces to the VLANs.
3. Create virtual systems **vsysa**, **vsysb**, and **vsysc** in the public system and allocate resources to them.
4. Add interfaces of the virtual systems to security zones.
5. Configure security policies in the virtual systems.

Procedure

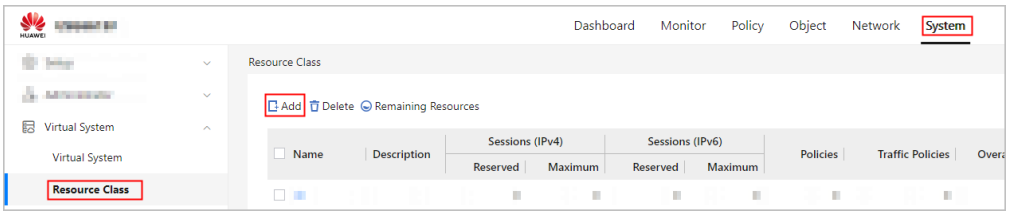
Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



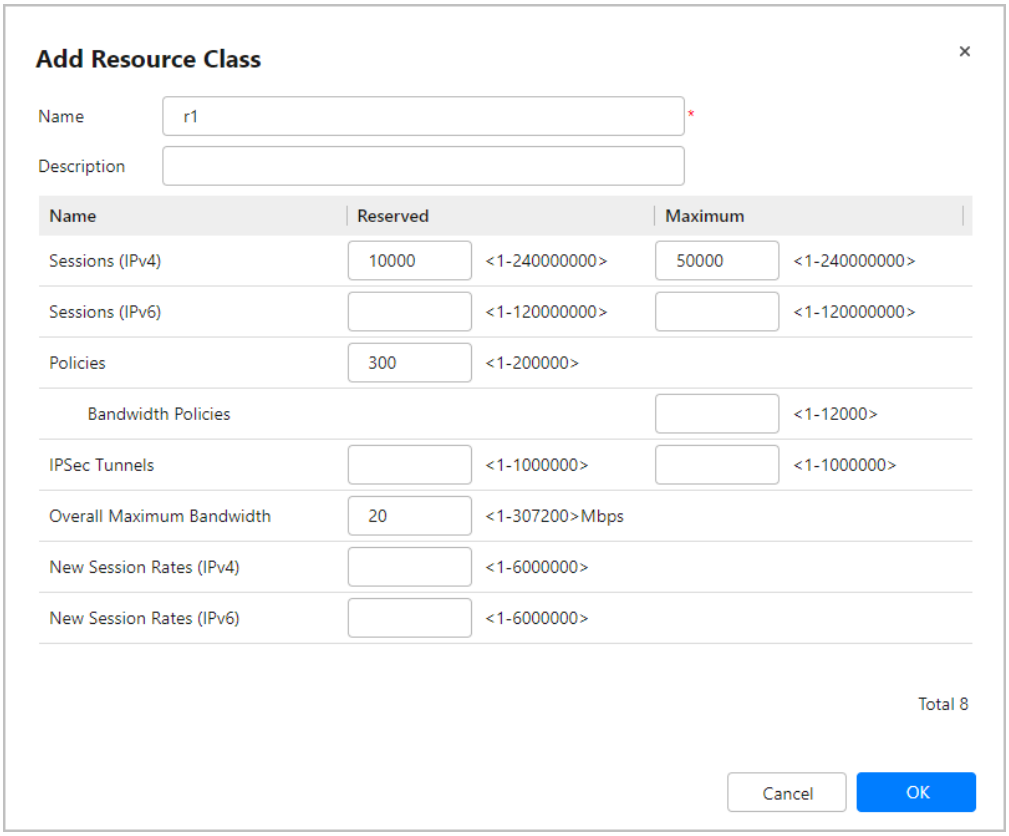
Step 2 Configure the virtual system resource class.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **System** > **Virtual System** > **Resource Class**.



2. Click **Add**, create the resource class **r1** by referring to the following figure, and set the guaranteed and maximum values of virtual system resources as required. After the configuration is complete, click **OK**.



Step 3 Configure GE 0/0/1 and GE 0/0/2 as trunk interfaces and add them to VLANs.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE 0/0/1 and set the following parameters. After the configuration is complete, click **OK**.

Zone	untrust
Mode	Switching
Connection Type	Trunk
Trunk VLAN ID	10, 20, and 30

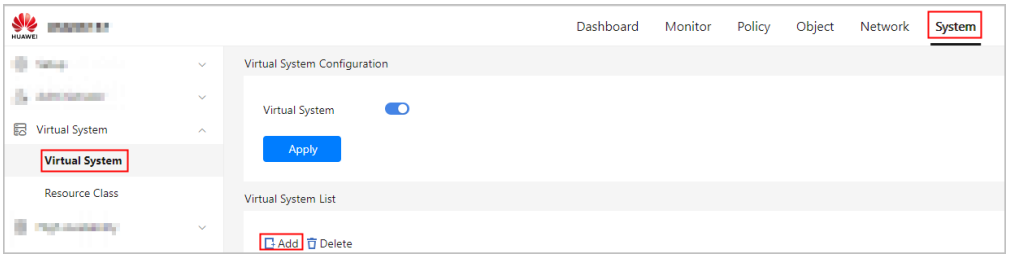
3. Repeat the preceding steps and set the following parameters for GE 0/0/2:

 Copyright © Huawei Technologies Co., Ltd.

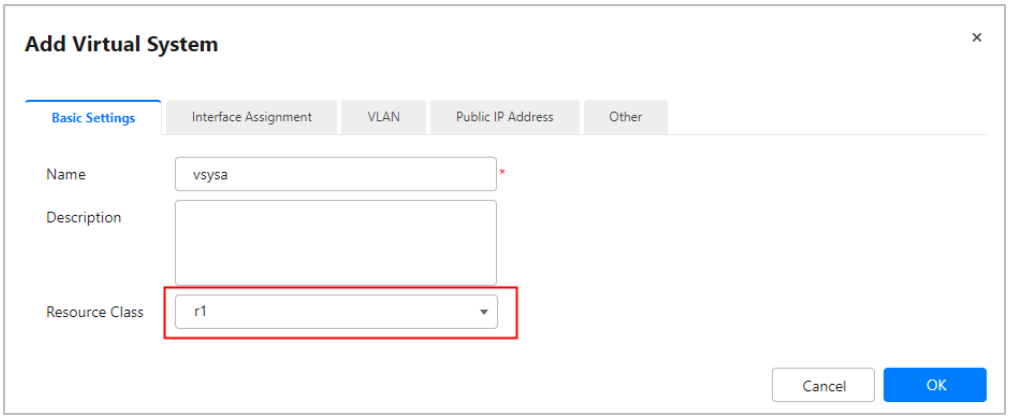
Zone	untrust
Mode	Switching
Connection Type	Trunk
Trunk VLAN ID	10, 20, and 30

Step 4 In the public system, create virtual system **vsysa** and allocate resources. After completing the configuration, click **OK**.

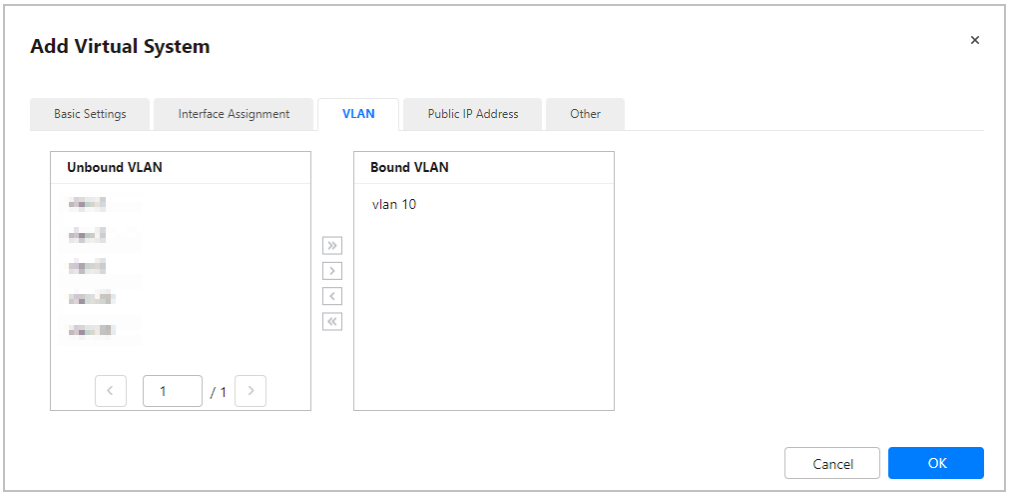
1. Choose **System** > **Virtual System** > **Virtual System**.



2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



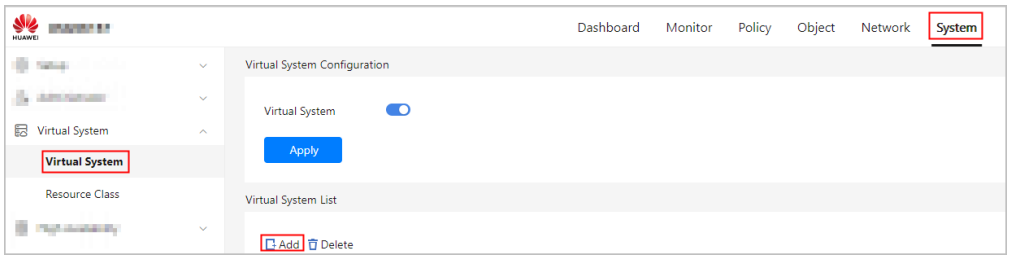
3. Click the **VLAN** tab and allocate a VLAN to the virtual system.



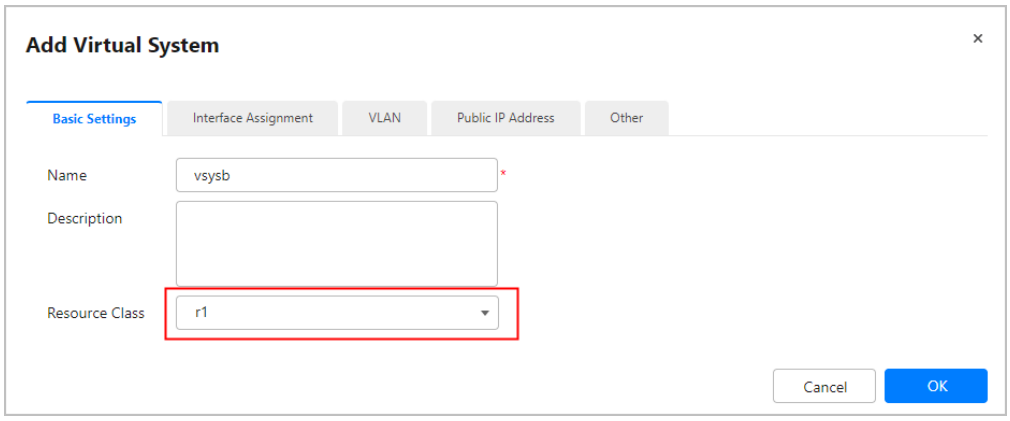
 Copyright © Huawei Technologies Co., Ltd.

Step 5 In the public system, create virtual system **vsysb** and allocate resources. After completing the configuration, click **OK**.

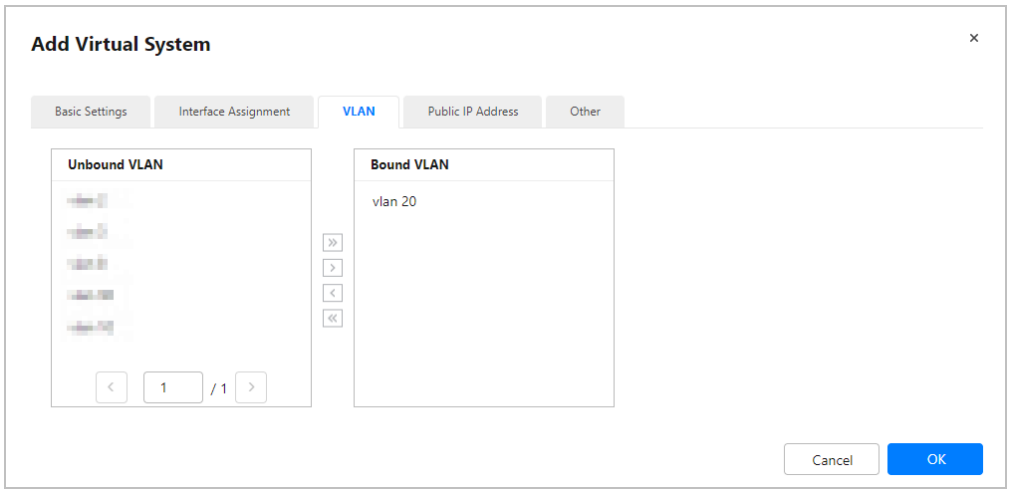
1. Choose **System** > **Virtual System** > **Virtual System**.



2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



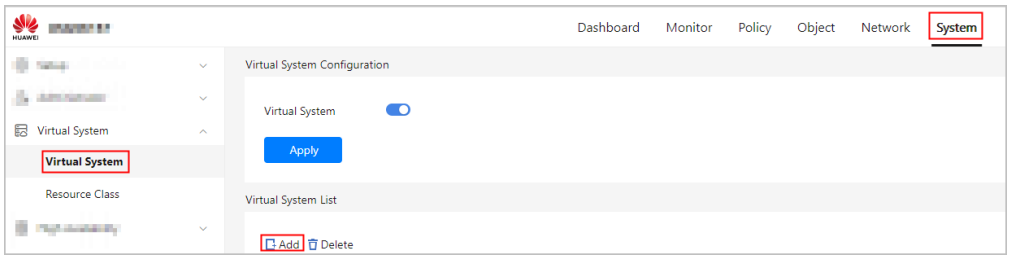
3. Click the **VLAN** tab, click **Add**, and allocate a VLAN to the virtual system.



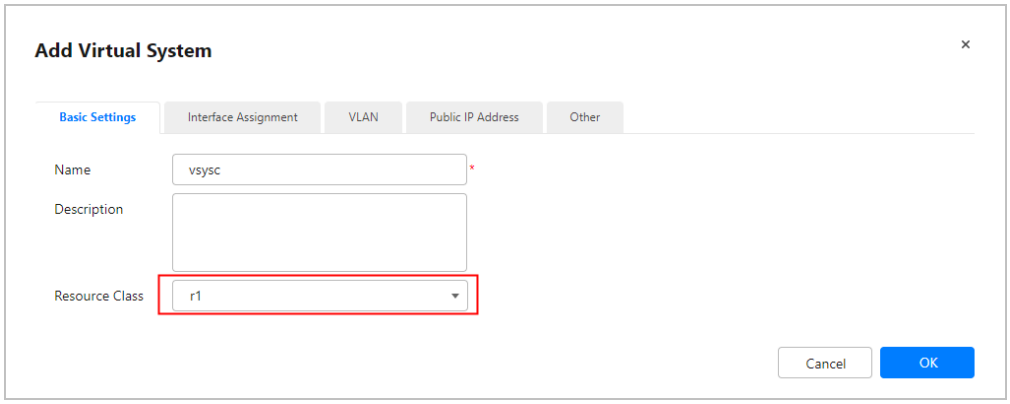
Step 6 In the public system, create virtual system **vsysc** and allocate resources. After completing the configuration, click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

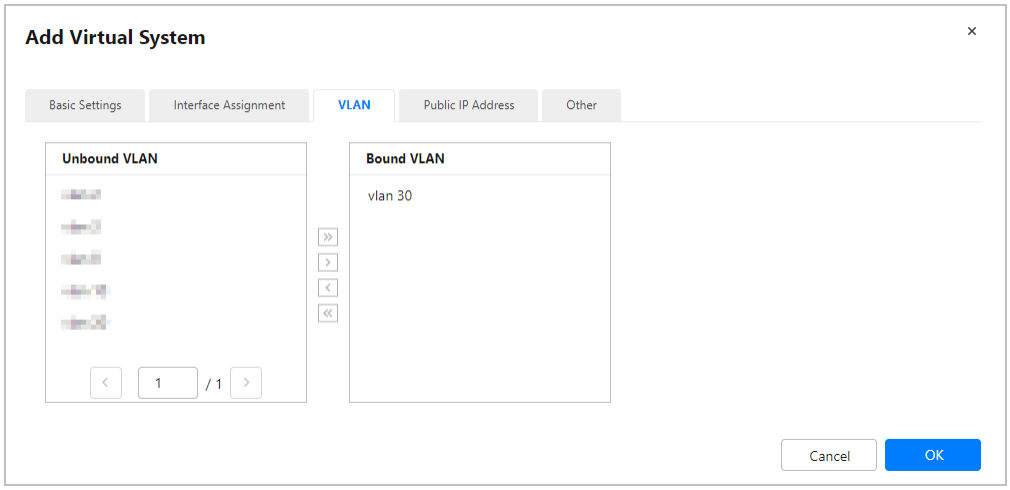
 Copyright © Huawei Technologies Co., Ltd.



2. Click **Add**, click the **Basic Settings** tab, and configure basic information about the virtual system.



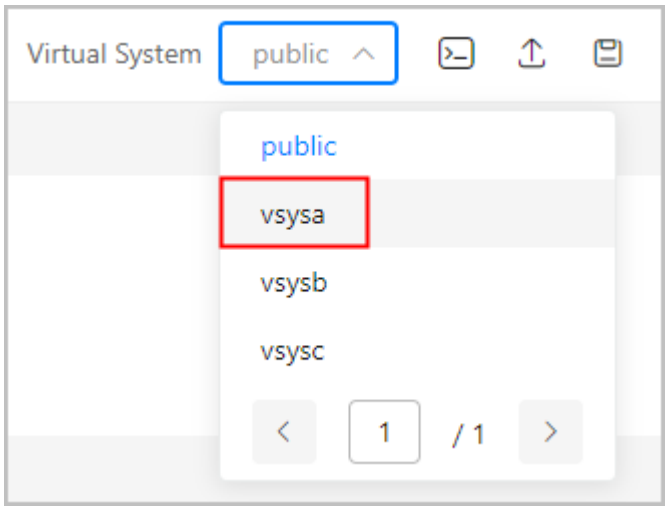
3. Click the **VLAN** tab and allocate a VLAN to the virtual system.



Step 7 Add GE 0/0/1 and GE 0/0/2 to security zones in virtual system **vsysa**.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access **vsysa**.

 Copyright © Huawei Technologies Co., Ltd.



2. Choose **Network** > **Interface**.
3. Click **-- NONE --** in the GE0/0/1**Zone** column and set the following parameters. After completing the configuration, click **OK**.

Interface Name	GE 0/0/1
Virtual System	vsysa
Zone	untrust

4. Repeat the preceding steps and set the following parameters for GE 0/0/2:

Interface Name	GE 0/0/2
Virtual System	vsysa
Zone	trust

Step 8 Configure security policies in **vsysa**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to allow hosts in the IP address range **10.3.0.2** to **10.3.0.10** to access the Internet. After completing the configuration, click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.2 to 10.3.0.10
Action	Permit

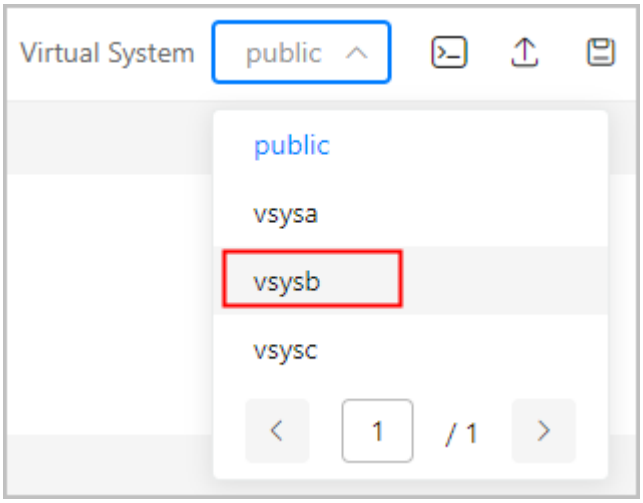
3. Repeat the preceding steps to configure a trust-to-untrust security policy to prevent hosts in the IP address range **10.3.0.2** to **10.3.0.10** on network A from accessing the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Name	to_internet_block
Source Zone	trust
Destination Zone	untrust
Action	Deny

Step 9 Add GE 0/0/1 and GE 0/0/2 to security zones in **vsysb**.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access **vsysb**.



2. Choose **Network** > **Interface**.
3. Click **-- NONE --** in the GE0/0/1**Zone** column and set the following parameters. After completing the configuration, click **OK**.

Interface Name	GE 0/0/1
Virtual System	vsysb
Zone	untrust

4. Repeat the preceding steps and set the following parameters for GE 0/0/2:

Interface Name	GE 0/0/2
Virtual System	vsysb
Zone	trust

Step 10 Configure security policies in **vsysb**.

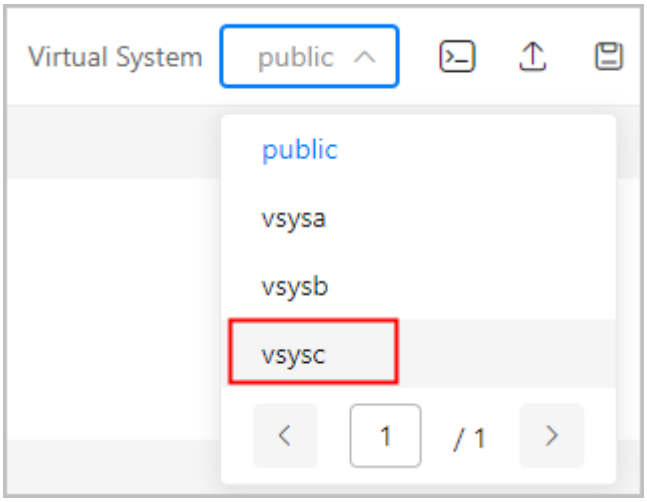
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to control the traffic from network B to the Internet based on service requirements and prevent all user hosts on network B from accessing the Internet. After completing the configuration, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Name	to_internet_block
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.1.2 to 10.3.1.254
Action	Deny

Step 11 Add GE 0/0/1 and GE 0/0/2 to security zones in **vsysc**.

1. Select **vsysc** from the **Virtual System** drop-down list in the upper right corner to access **vsysc**.



2. Choose **Network** > **Interface**.
3. Click **-- NONE --** in the GE0/0/1**Zone** column and set the following parameters. After completing the configuration, click **OK**.

Interface Name	GE 0/0/1
Virtual System	vsysc
Zone	untrust

4. Repeat the preceding steps and set the following parameters for GE 0/0/2:

Interface Name	GE0/0/2
Virtual System	vsysc
Zone	trust

Step 12 Configure security policies in **vsysc**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a trust-to-untrust security policy to control the traffic from network C to the Internet based on service

 Copyright © Huawei Technologies Co., Ltd.

requirements and allow all user hosts on network C to access the Internet. After completing the configuration, click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.2 to 10.3.2.254
Action	Permit

----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B cannot access the Internet.
- All user hosts on network C can access the Internet.

Configuration Scripts

- public

```
#
vlan batch 10 20 30
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign vlan 10
 assign resource-class r1
#
vsys name vsysb 2
 assign vlan 20
 assign resource-class r1
#
vsys name vsysc 3
 assign vlan 30
 assign resource-class r1
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
#
interface GE0/0/2
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
#
```

- vsysa

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.0.2 10.3.0.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
```

- vsysb

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface GE0/0/1
#
security-policy
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  source-address range 10.3.1.2 10.3.1.254
  action deny
#
```

- vsysc

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface GE0/0/1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.2.2 10.3.2.254
  action permit
#
```

6.23 CLI: Example for Configuring Layer 2 Access for Virtual Systems

Networking Requirements

As shown in **Figure 6-23**, the device is deployed as a Layer 2 gateway between the intranet and Internet. The intranet is divided into three independent LANs: network A, network B, and network C, which are isolated from each other and therefore cannot communicate with each other.

The three LANs belong to different VLANs and are isolated through virtual systems vsysa, vsysb, and vsysc. All user hosts on network C and some user hosts

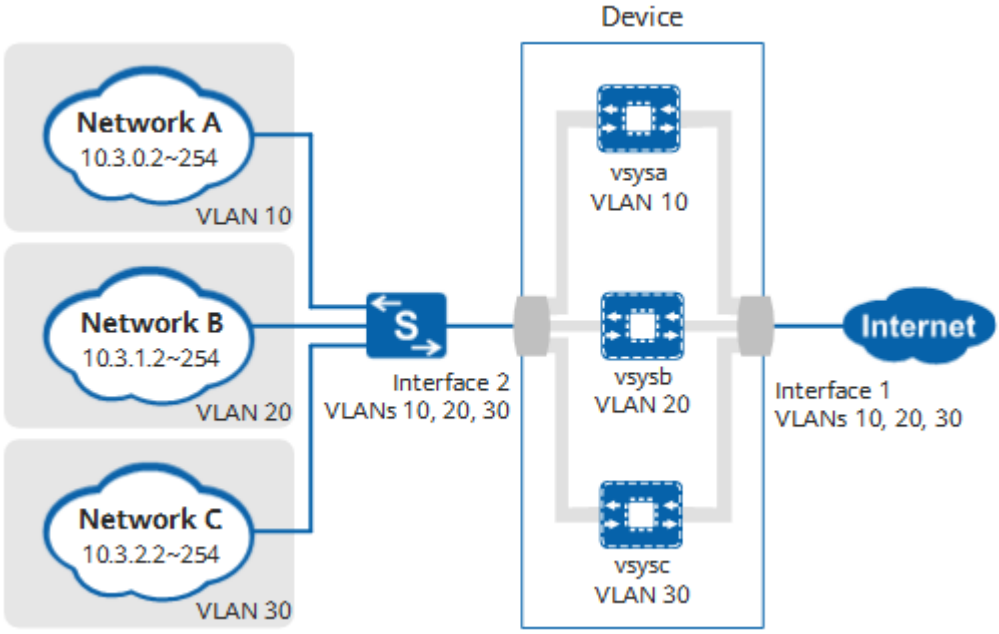
 Copyright © Huawei Technologies Co., Ltd.

on network A are allowed to access the Internet, and all user hosts on network B are not allowed to access the Internet.

Figure 6-23 Configuring Layer 2 access for virtual systems

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
vsysa	Virtual system name: vsysa WAN interface: GE 0/0/1 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 Security zone to which the LAN interface belongs: Trust VLAN assigned: VLAN 10 IP addresses allowed to access the Internet: 10.3.0.2 to 10.3.0.10	-
vsysb	Virtual system name: vsysb WAN interface: GE 0/0/1 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 Security zone to which the LAN interface belongs: Trust VLAN assigned: VLAN 20	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysc	Virtual system name: vsysc WAN interface: GE 0/0/1 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/2 Security zone to which the LAN interface belongs: Trust VLAN assigned: VLAN 30	-
Resource class	Resource class name: r1 Guaranteed number of IPv4 sessions: 10000 Maximum number of IPv4 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A, B, and C have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function and configure resource classes based on service requirements.
2. Create VLANs in the public system and add related interfaces to the VLANs.
3. Create virtual systems vsysa, vsysb, and vsysc in the public system and allocate resources to them.
4. Add interfaces of the virtual systems to security zones.
5. Configure security policies in the virtual systems.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create VLANs.

```
[Device] vlan 10
[Device-vlan10] quit
[Device] vlan 20
[Device-vlan20] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device] vlan 30
[Device-vlan30] quit
```

Step 4 Configure interfaces as trunk interfaces and add them to VLANs.

```
[Device] interface ge 0/0/1
[Device-GE0/0/1] portswitch
[Device-GE0/0/1] port link-type trunk
[Device-GE0/0/1] port trunk allow-pass vlan 10 20 30
[Device-GE0/0/1] quit
[Device] interface ge 0/0/2
[Device-GE0/0/2] portswitch
[Device-GE0/0/2] port link-type trunk
[Device-GE0/0/2] port trunk allow-pass vlan 10 20 30
[Device-GE0/0/2] quit
```

Step 5 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign vlan 10
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign vlan 20
[Device-vsys-vsysb] quit
```

Create virtual system vsysc and allocate resources to it.

```
[Device] vsys name vsysc
[Device-vsys-vsysc] assign resource-class r1
[Device-vsys-vsysc] assign vlan 30
[Device-vsys-vsysc] quit
```

Step 6 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 7 Add physical interfaces to security zones.

```
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/2
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface ge 0/0/1
[Device-vsysa-zone-untrust] quit
```

Step 8 Configure security policies to control the traffic from network A to the Internet based on service requirements.

Allow user hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A to access the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_internet_allow
[Device-vsysa-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_allow] source-address range 10.3.0.2 10.3.0.10
[Device-vsysa-policy-security-rule-to_internet_allow] action permit
[Device-vsysa-policy-security-rule-to_internet_allow] quit
```

Forbid user hosts that are not in the IP address range of 10.3.0.2 to 10.3.0.10 on network A from accessing the Internet.

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-policy-security] rule name to_internet_block
[Device-vsysa-policy-security-rule-to_internet_block] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_block] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_block] action deny
[Device-vsysa-policy-security-rule-to_internet_block] quit
[Device-vsysa-policy-security] quit
```

Step 9 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 10 Add physical interfaces to security zones.

```
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/2
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface ge 0/0/1
[Device-vsysb-zone-untrust] quit
```

Step 11 Configure a security policy to forbid all user hosts on network B from accessing the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_internet_block
[Device-vsysb-policy-security-rule-to_internet_block] source-zone trust
[Device-vsysb-policy-security-rule-to_internet_block] destination-zone untrust
[Device-vsysb-policy-security-rule-to_internet_block] source-address range 10.3.1.2 10.3.1.254
[Device-vsysb-policy-security-rule-to_internet_block] action deny
[Device-vsysb-policy-security-rule-to_internet_block] quit
[Device-vsysb-policy-security] quit
```

Step 12 Switch to the system view of vsysc.

```
[Device-vsysb] quit
<Device-vsysb> quit
[Device] switch vsys vsysc
<Device-vsysc> system-view
```

Step 13 Add physical interfaces to security zones.

```
[Device-vsysa] firewall zone trust
[Device-vsysc-zone-trust] add interface ge 0/0/2
[Device-vsysc-zone-trust] quit
[Device-vsysc] firewall zone untrust
[Device-vsysc-zone-untrust] add interface ge 0/0/1
[Device-vsysc-zone-untrust] quit
```

Step 14 Configure a security policy to allow all user hosts on network C to access the Internet.

```
[Device-vsysc] security-policy
[Device-vsysc-policy-security] rule name to_internet_allow
[Device-vsysc-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysc-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysc-policy-security-rule-to_internet_allow] source-address range 10.3.2.2 10.3.2.254
[Device-vsysc-policy-security-rule-to_internet_allow] action permit
[Device-vsysc-policy-security-rule-to_internet_allow] quit
[Device-vsysc-policy-security] quit
```

----End

Verifying the Configuration

- User hosts in the IP address range of 10.3.0.2 to 10.3.0.10 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B cannot access the Internet.

 Copyright © Huawei Technologies Co., Ltd.

- All user hosts on network C can access the Internet.

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
vlan batch 10 20 30
#
 vsys enable
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign vlan 10
 assign resource-class r1
#
vsys name vsysb 2
 assign vlan 20
 assign resource-class r1
#
vsys name vsysc 3
 assign vlan 30
 assign resource-class r1
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
#
interface GE0/0/2
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
#
return
```

- Virtual system (vsysa)

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.0.2 10.3.0.10
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
return
```

- Virtual system (vsysb)

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
firewall zone untrust
set priority 5
 add interface GE0/0/1
#
security-policy
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  source-address range 10.3.1.2 10.3.1.254
  action deny
#
return
```

- Virtual system (vsysc)

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
set priority 5
 add interface GE0/0/1
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 10.3.2.2 10.3.2.254
  action permit
#
return
```

6.24 Web: Example for Configuring IPv6 User Access at Layer 3 Through Virtual Systems

Networking Requirements

On the IPv6 network shown in **Figure 6-24**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and therefore cannot communicate with each other.

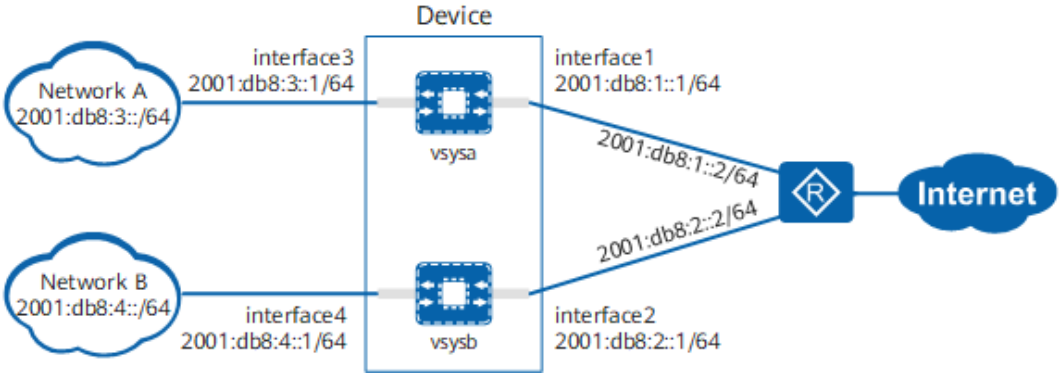
Network A accesses the Internet through interface 1 (independent public network interface) of vsysa, and network B accesses the Internet through interface 2 (independent public network interface) of vsysb. On network A, only some user hosts can access the Internet. On network B, all user hosts can access the Internet.

Figure 6-24 Configuring IPv6 user access at Layer 3 through virtual systems

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/4 respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
vsysa	Virtual system name: vsysa Public network interface: GE0/0/1 Public network interface IP address: 2001:db8:1::1/64 Security zone to which the public network interface belongs: Untrust Private network interface: GE0/0/3 Private network interface IP address: 2001:db8:3::1/64 Private IP address range: 2001:db8:3::/64 Security zone to which the private network interface belongs: Trust IP addresses allowed to access the Internet: 2001:db8:3::2-2001:db8:3::200	-
vsysb	Virtual system name: vsysb Public network interface: GE0/0/2 Public network interface IP address: 2001:db8:2::1/64 Security zone to which the public network interface belongs: Untrust Private network interface: GE0/0/4 Private network interface IP address: 2001:db8:4::1/64 Private IP address range: 2001:db8:4::/64 Security zone to which the private network interface belongs: Trust	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Resource class	Resource class name: r1 Guaranteed number of IPv6 sessions: 10000 Maximum number of IPv6 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

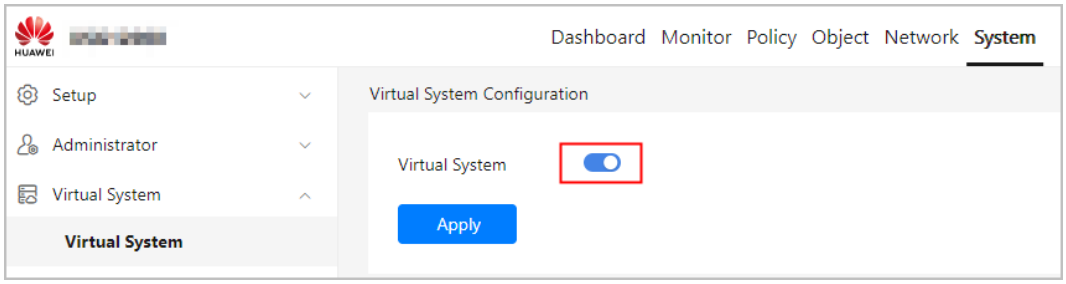
Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function and IPv6 unicast packet forwarding function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for vsysa and vsysb, and add the interfaces to security zones.
4. Configure routes in vsysa and vsysb to divert traffic from networks A and B to the Internet.
5. Configure security policies in vsysa and vsysb based on service requirements to permit traffic from user hosts on networks A and B to the Internet.

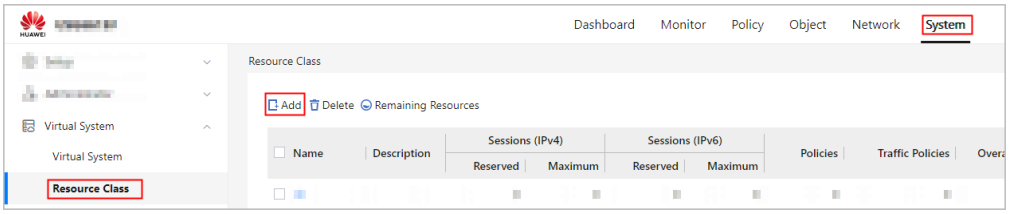
Procedure

Step 1 Choose **System** > **Virtual System** > **Virtual System**. In **Virtual System Configuration**, enable the virtual system function and click **Apply**.



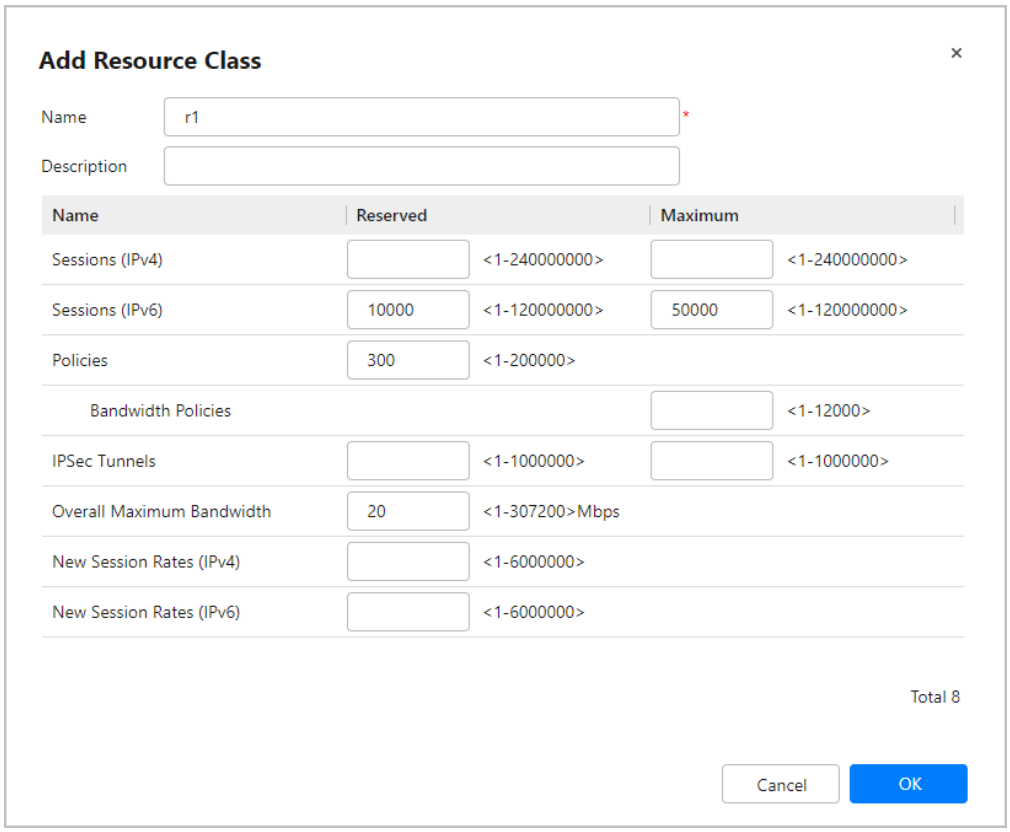
Step 2 Configure virtual system resource classes.

1. Choose **System** > **Virtual System** > **Resource Class**.



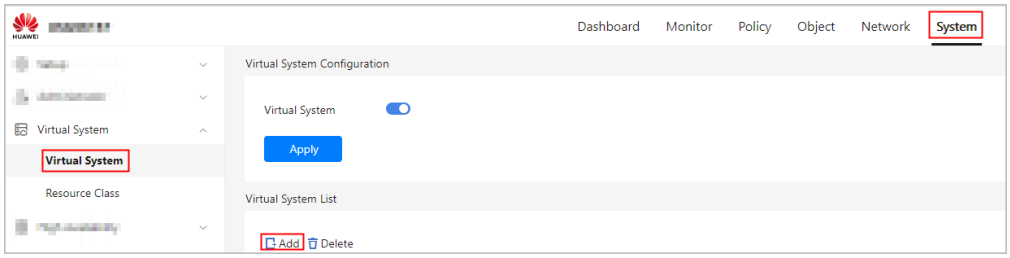
 Copyright © Huawei Technologies Co., Ltd.

2. Click **Add**. In the dialog box that is displayed, create system resource class r1 and set the guaranteed and maximum number of virtual system resources as follows. Click **OK**.



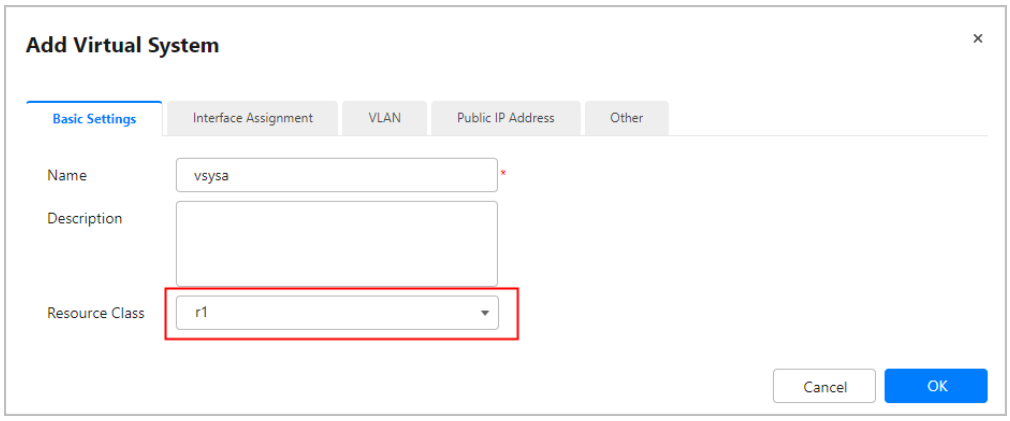
Step 3 In the public system, create virtual system vsysa and allocate resources to it. Click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

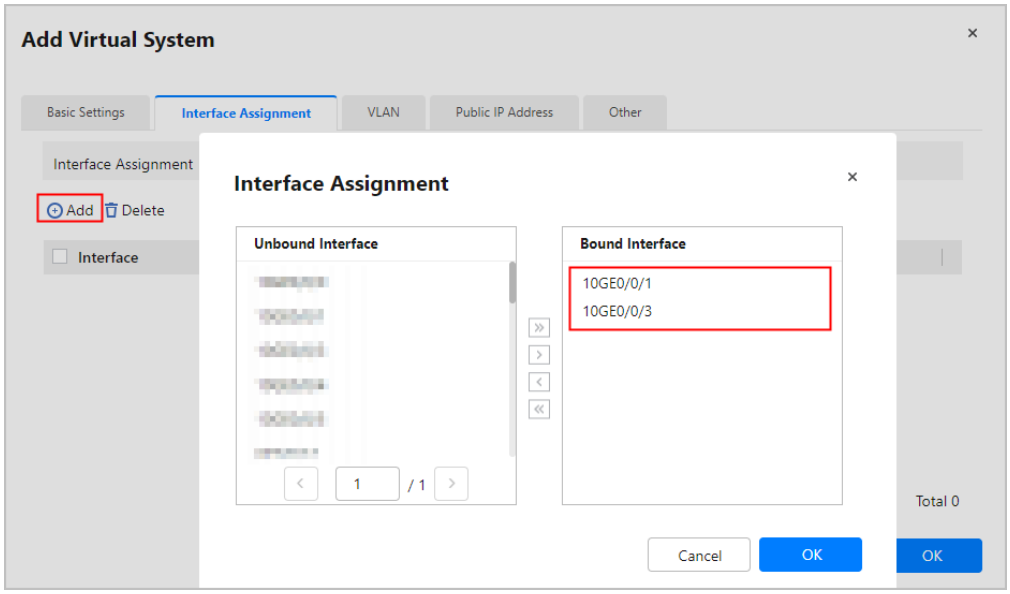


2. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

 Copyright © Huawei Technologies Co., Ltd.

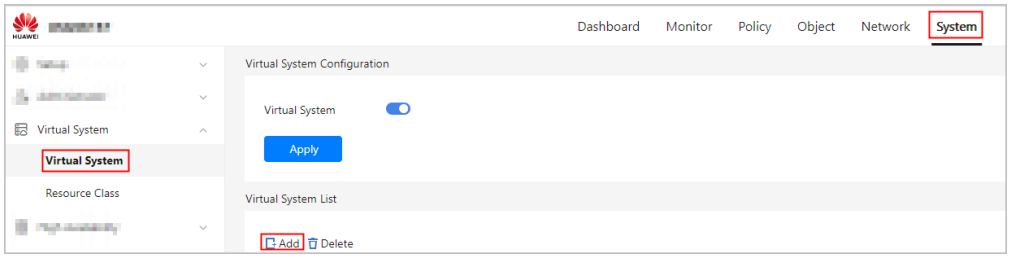


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



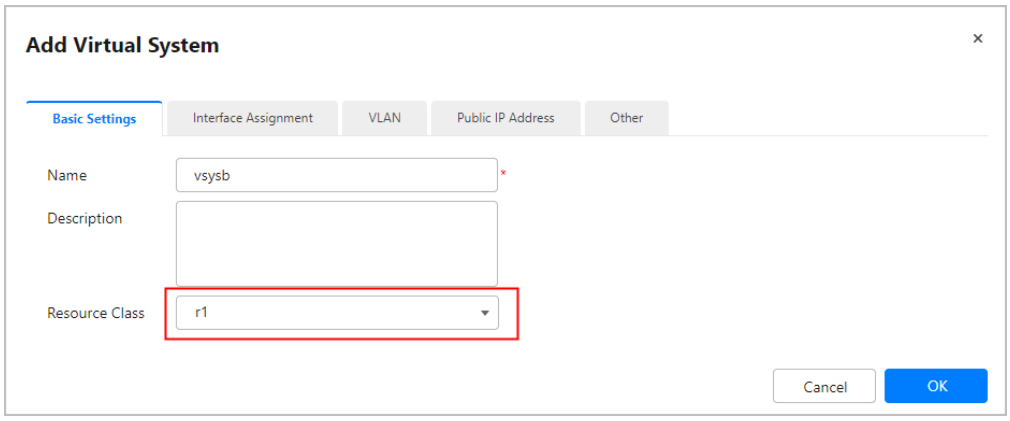
Step 4 In the public system, create virtual system vsysb and allocate resources to it. Click **OK**.

1. Choose **System** > **Virtual System** > **Virtual System**.

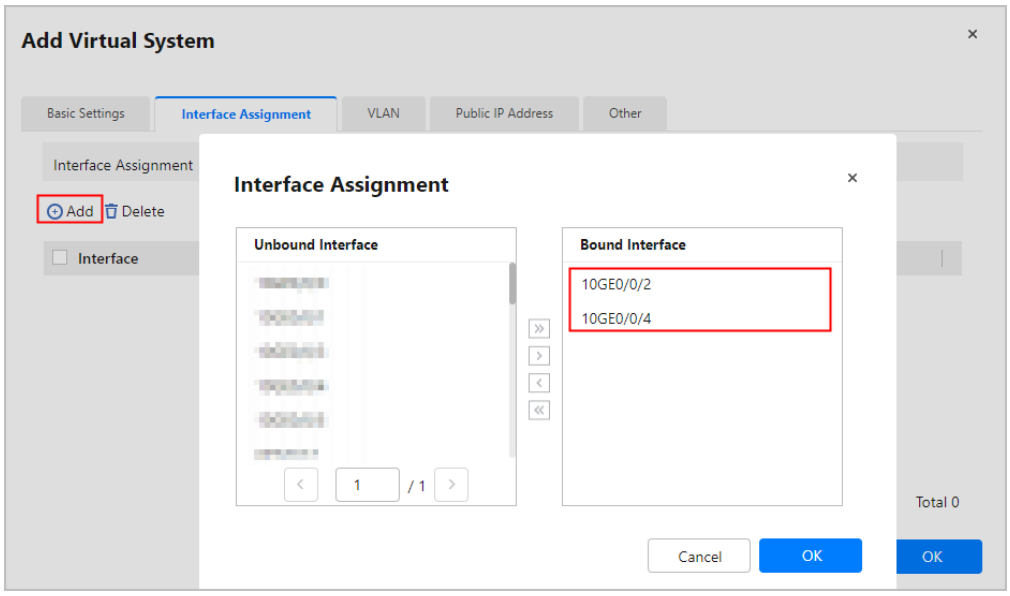


2. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

 Copyright © Huawei Technologies Co., Ltd.

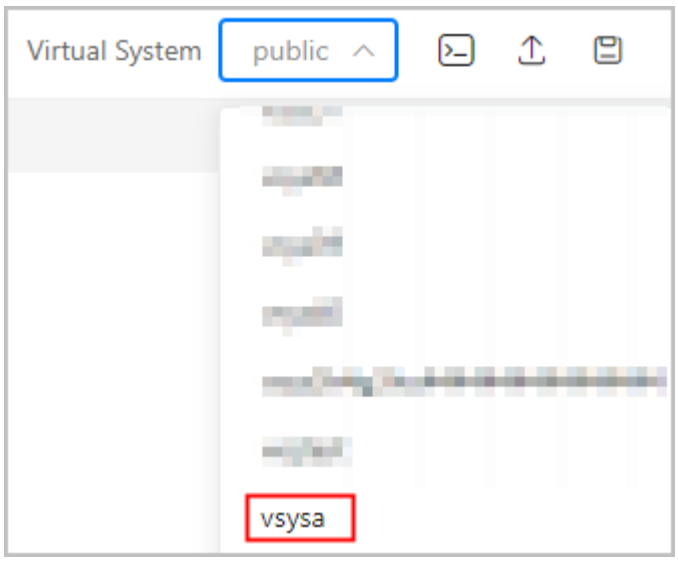


3. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



Step 5 In vsysa, configure GE0/0/1 and GE0/0/3 and add them to security zones.

1. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access vsysa.



 Copyright © Huawei Technologies Co., Ltd.

2. Choose **Network** > **Interface**.
3. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv6	
IP Address	2001:db8:1::1/64

4. Repeat the preceding steps to set the parameters for GE0/0/3.

Zone	trust
IPv6	
IP Address	2001:db8:3::1/64

Step 6 Configure security policies in vsysa.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a Trust-to-Untrust interzone policy to allow user hosts on network segment 2001:db8:3::2 to 2001:db8:3::200 on network A to access the Internet. Click **OK**.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	2001:db8:3::2-2001:db8:3::200
Action	Permit

3. Repeat the preceding steps to configure a Trust-to-Untrust interzone policy to prevent other user hosts on network segment 2001:db8:3::2 to 2001:db8:3::200 on network A from accessing the Internet.

Name	to_internet_block
Source Zone	trust
Destination Zone	untrust
Action	Deny

Step 7 Configure routes in vsysa.

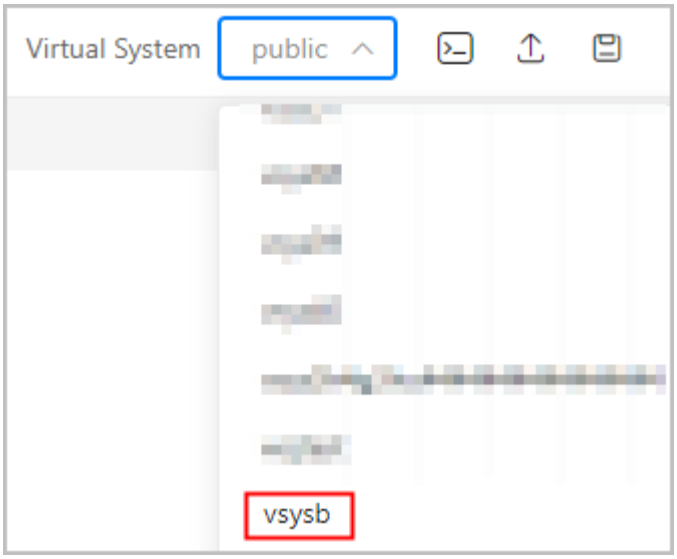
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a static route from network A to the Internet. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv6
Destination Address/Mask	::/0
Next Hop	2001:db8:1::2

Step 8 In vsysb, configure GE0/0/2 and GE0/0/4 and add them to security zones.

1. Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access vsysb.



2. Choose **Network** > **Interface**.
3. Click for GE0/0/2 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv6	
IP Address	2001:db8:2::1/64

4. Repeat the preceding steps to set the parameters for GE0/0/4.

Zone	trust
IPv6	
IP Address	2001:db8:4::1/64

Step 9 Configure security policies in vsysb.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a Trust-to-Untrust interzone policy to allow all user hosts on network B to access the Internet. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Name	to_internet_allow
Source Zone	trust
Destination Zone	untrust
Source Address	2001:db8:4::/64
Action	Permit

Step 10 Configure routes in vsysb.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a static route from network B to the Internet. Click **OK**.

Protocol	IPv6
Destination Address/Mask	::/0
Next Hop	2001:db8:2::2

----End

Verifying the Configuration

- On network A, the hosts whose IP addresses are in the range of 2001:db8:3::2-2001:db8:3::200 can access the Internet. Other hosts cannot access the Internet.
- Hosts on network B can access the Internet.

Configuration Scripts

- public

```
#
 vsys enable
#
resource-class r1
 resource-item-limit ipv6 session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/1
 assign interface GE0/0/3
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/2
 assign interface GE0/0/4
```

- vsysa

```
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:db8:1::1 64
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:db8:3::1 64
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
set priority 5
 add interface GE0/0/1
#
 ipv6 route-static :: 0 2001:db8:1::2
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 2001:db8:3::2 2001:db8:3::200
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
```

- vsysb

```
#
interface GE0/0/2
 ipv6 enable
 ipv6 address 2001:db8:2::1 64
#
interface GE0/0/4
 ipv6 enable
 ipv6 address 2001:db8:4::1 64
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
set priority 5
 add interface GE0/0/2
#
 ipv6 route-static :: 0 2001:db8:2::2
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:4:: 64
  action permit
```

6.25 CLI: Example for Configuring IPv6 User Access at Layer 3 Through Virtual Systems

Networking Requirements

On the IPv6 network shown in **Figure 6-25**, the device is deployed as a Layer 3 gateway between the intranet and Internet. The intranet is divided into two independent LANs: network A and network B, which are isolated from each other and therefore cannot communicate with each other.

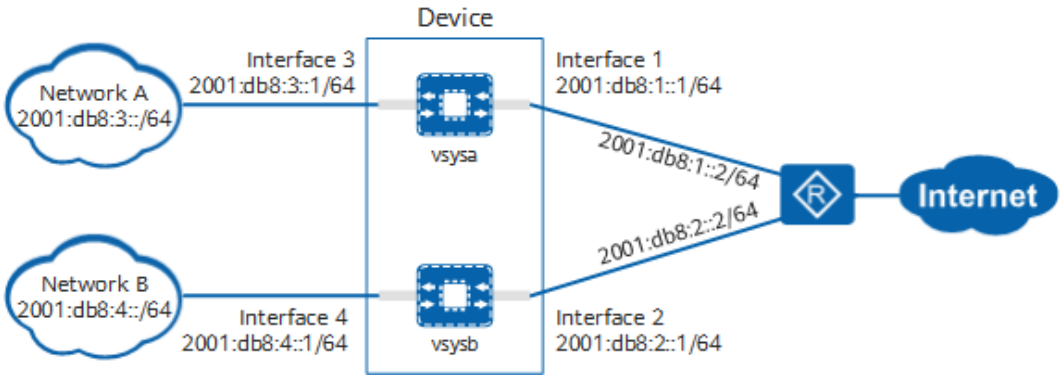
 Copyright © Huawei Technologies Co., Ltd.

Network A accesses the Internet through the independent WAN interface interface 1 of vsysa, and network B accesses the Internet through the independent WAN interface interface 2 of vsysb. On network A, only some user hosts can access the Internet. On network B, all user hosts can access the Internet.

Figure 6-25 Configuring IPv6 user access at Layer 3 through virtual systems

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4, respectively.



Item	Data	Description
vsysa	Virtual system name: vsysa WAN interface: GE 0/0/1 WAN interface IP address: 2001:db8:1::1/64 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/3 LAN interface IP address: 2001:db8:3::1/64 Private IP address range: 2001:db8:3::/64 Security zone to which the LAN interface belongs: Trust IP addresses allowed to access the Internet: 2001:db8:3::2-2001:db8:3::200	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
vsysb	Virtual system name: vsysb WAN interface: GE 0/0/2 WAN interface IP address: 2001:db8:2::1/64 Security zone to which the WAN interface belongs: Untrust LAN interface: GE 0/0/4 LAN interface IP address: 2001:db8:4::1/64 Private IP address range: 2001:db8:4::/64 Security zone to which the LAN interface belongs: Trust	-
Resource class	Resource class name: r1 Guaranteed number of IPv6 sessions: 10000 Maximum number of IPv6 sessions: 50000 Guaranteed number of policies: 300 Guaranteed total bandwidth: 20 Mbit/s	In this example, networks A and B have similar service resource usage requirements and therefore are allocated the same virtual system resources.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the virtual system function and IPv6 unicast packet forwarding function.
2. Configure resource classes based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for vsysa and vsysb, and add the interfaces to security zones.
4. Configure routes in vsysa and vsysb to divert traffic from networks A and B to the Internet.
5. Configure security policies in vsysa and vsysb based on service requirements to permit traffic from user hosts on networks A and B to the Internet.

Procedure

Step 1 Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] vsys enable
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure a resource class.

```
[Device] resource-class r1
[Device-resource-class-r1] resource-item-limit ipv6 session reserved-number 10000 maximum 50000
[Device-resource-class-r1] resource-item-limit policy reserved-number 300
[Device-resource-class-r1] resource-item-limit bandwidth 20 entire
[Device-resource-class-r1] quit
```

Step 3 Create virtual systems and allocate resources to them.

Create virtual system vsysa and allocate resources to it.

```
[Device] vsys name vsysa
[Device-vsys-vsysa] assign resource-class r1
[Device-vsys-vsysa] assign interface ge 0/0/1
[Device-vsys-vsysa] assign interface ge 0/0/3
[Device-vsys-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[Device] vsys name vsysb
[Device-vsys-vsysb] assign resource-class r1
[Device-vsys-vsysb] assign interface ge 0/0/2
[Device-vsys-vsysb] assign interface ge 0/0/4
[Device-vsys-vsysb] quit
```

Step 4 Switch to the system view of vsysa.

```
[Device] switch vsys vsysa
<Device-vsysa> system-view
```

Step 5 Configure interfaces for vsysa and add the interfaces to security zones.

```
[Device-vsysa] interface ge 0/0/1
[Device-vsysa-GE0/0/1] ipv6 enable
[Device-vsysa-GE0/0/1] ipv6 address 2001:db8:1::1 64
[Device-vsysa-GE0/0/1] quit
[Device-vsysa] interface ge 0/0/3
[Device-vsysa-GE0/0/3] ipv6 enable
[Device-vsysa-GE0/0/3] ipv6 address 2001:db8:3::1 64
[Device-vsysa-GE0/0/3] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/3
[Device-vsysa-zone-trust] quit
[Device-vsysa] firewall zone untrust
[Device-vsysa-zone-untrust] add interface ge 0/0/1
[Device-vsysa-zone-untrust] quit
```

Step 6 Configure a static route from network A to the Internet.

```
[Device-vsysa] ipv6 route-static :: 0 2001:db8:1::2
```

Step 7 Configure security policies for the traffic from network A to the Internet.

Allow user hosts in the IP address range of 2001:db8:3::2 to 2001:db8:3::200 on network A to access the Internet.

```
[Device-vsysa] security-policy
[Device-vsysa-policy-security] rule name to_internet_allow
[Device-vsysa-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysa-policy-security-rule-to_internet_allow] source-address range 2001:db8:3::2 2001:db8:3::200
[Device-vsysa-policy-security-rule-to_internet_allow] action permit
[Device-vsysa-policy-security-rule-to_internet_allow] quit
```

Forbid user hosts that are not in the IP address range of 2001:db8:3::2 to 2001:db8:3::200 on network A from accessing the Internet.

```
[Device-vsysa-policy-security] rule name to_internet_block
[Device-vsysa-policy-security-rule-to_internet_block] source-zone trust
[Device-vsysa-policy-security-rule-to_internet_block] destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-policy-security-rule-to_internet_block] action deny
[Device-vsysa-policy-security-rule-to_internet_block] quit
[Device-vsysa-policy-security] quit
```

Step 8 Switch to the system view of vsysb.

```
[Device-vsysa] quit
<Device-vsysa> quit
[Device] switch vsys vsysb
<Device-vsysb> system-view
```

Step 9 Configure interfaces for vsysb and add the interfaces to security zones.

```
[Device-vsysb] interface ge 0/0/2
[Device-vsysb-GE0/0/2] ipv6 enable
[Device-vsysb-GE0/0/2] ipv6 address 2001:db8:2::1 64
[Device-vsysb-GE0/0/2] quit
[Device-vsysb] interface ge 0/0/4
[Device-vsysb-GE0/0/4] ipv6 enable
[Device-vsysb-GE0/0/4] ipv6 address 2001:db8:4::1 64
[Device-vsysb-GE0/0/4] quit
[Device-vsysb] firewall zone trust
[Device-vsysb-zone-trust] add interface ge 0/0/4
[Device-vsysb-zone-trust] quit
[Device-vsysb] firewall zone untrust
[Device-vsysb-zone-untrust] add interface ge 0/0/2
[Device-vsysb-zone-untrust] quit
```

Step 10 Configure a static route from network B to the Internet.

```
[Device-vsysb] ipv6 route-static :: 0 2001:db8:2::2
```

Step 11 Configure a security policy for the network B-to-Internet interzone, allowing all user hosts on network B to access the Internet.

```
[Device-vsysb] security-policy
[Device-vsysb-policy-security] rule name to_internet_allow
[Device-vsysb-policy-security-rule-to_internet_allow] source-zone trust
[Device-vsysb-policy-security-rule-to_internet_allow] destination-zone untrust
[Device-vsysb-policy-security-rule-to_internet_allow] source-address 2001:db8:4:: 64
[Device-vsysb-policy-security-rule-to_internet_allow] action permit
[Device-vsysb-policy-security-rule-to_internet_allow] quit
[Device-vsysb-policy-security] quit
```

----End

Verifying the Configuration

- User hosts in the IP address range of 2001:db8:3::2 to 2001:db8:3::200 on network A can access the Internet, but other user hosts cannot.
- All user hosts on network B can access the Internet.

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
resource-class r1
 resource-item-limit ipv6 session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit bandwidth 20 entire
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GE0/0/1
 assign interface GE0/0/3
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GE0/0/2
 assign interface GE0/0/4
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:db8:1::1 64
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:db8:3::1 64
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
set priority 5
 add interface GE0/0/1
#
 ipv6 route-static :: 0 2001:db8:1::2
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address range 2001:db8:3::2 2001:db8:3::200
  action permit
 rule name to_internet_block
  source-zone trust
  destination-zone untrust
  action deny
#
return
```

- Virtual system (vsysb)

```
#
interface GE0/0/2
 ipv6 enable
 ipv6 address 2001:db8:2::1 64
#
interface GE0/0/4
 ipv6 enable
 ipv6 address 2001:db8:4::1 64
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
set priority 5
 add interface GE0/0/2
#
 ipv6 route-static :: 0 2001:db8:2::2
#
security-policy
 rule name to_internet_allow
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:4:: 64
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

6.26 CLI: Example for Configuring Telnet Login to a Virtual System

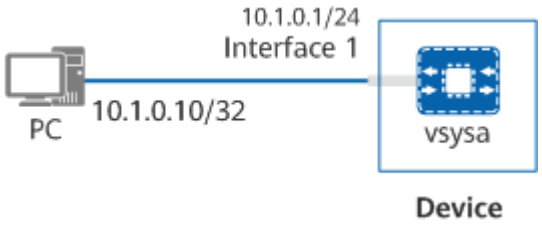
Networking Requirements

In **Figure 6-26**, the virtual system administrator wants to log in to a virtual system using Telnet to manage configurations in the virtual system. Before performing the configuration, ensure that the virtual system has been created, and interfaces and service resources have been allocated to the virtual system as required.

Figure 6-26 Network diagram for configuring Telnet login to a virtual system

NOTE

In this example, interface 1 represents GE 0/0/1.



Item	Data
Virtual system administrator	User name: vsysauser1@@vsysa Authentication type: local authentication Password: YsHsjx_202206 Trusted host: 10.1.0.10/32
Login interface	Interface number: GE 0/0/1 Security zone: Trust IP address: 10.1.0.1/24 Virtual system: vsysa
Login mode	Telnet **NOTE** If the network environment is not secure enough, a secure protocol is recommended. For details, see *Example for Configuring STelnet Login to a Virtual System*.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the Telnet server function and configure related parameters. For security purposes, Telnet is not recommended. If Telnet has to be used, run

 Copyright © Huawei Technologies Co., Ltd.

the install feature-software WEAKEA command to install the weak security algorithm/protocol feature package WEAKEA.

2. Configure parameters related to a VTY user interface, including the user privilege level, authentication mode, and supported protocol type.
3. Configure a login interface and add it to a security zone.
4. Create a virtual system administrator whose access type is telnet.

Procedure

Step 1 Enable the Telnet server function and configure related parameters.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] undo telnet server disable
[Device] telnet server-source -i ge0/0/1
```

Step 2 Configure parameters related to a VTY user interface, including the user privilege level, authentication mode, and supported protocol type.

Configure an IP address for the trusted host.

```
[Device] acl 2001
[Device-acl4-basic-2001] rule permit source 10.1.0.10 32
[Device-acl4-basic-2001] quit
```

Set parameters for the VTY user interface.

```
[Device] user-interface vty 0 5
[Device-ui-vty0-5] acl 2001 inbound
[Device-ui-vty0-5] user privilege level 3
[Device-ui-vty0-5] authentication-mode aaa
[Device-ui-vty0-5] protocol inbound telnet
[Device-ui-vty0-5] quit
```

Step 3 Enter the vsysa configuration view.

```
[Device] switch vsys vsysa
```

Step 4 Configure a login interface and add it to a security zone.

```
<Device-vsysa> system-view
[Device-vsysa] interface ge 0/0/1
[Device-vsysa-GE0/0/1] ip address 10.1.0.1 24
[Device-vsysa-GE0/0/1] service-manage enable
[Device-vsysa-GE0/0/1] service-manage telnet permit
[Device-vsysa-GE0/0/1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/1
[Device-vsysa-zone-trust] quit
```

Step 5 Create a virtual system administrator whose access type is telnet.

```
[Device-vsysa] aaa
[Device-vsysa-aaa] local-user vsysauser1@@vsysa password irreversible-cipher YsHsjx_202206
[Device-vsysa-aaa] local-user vsysauser1@@vsysa privilege level 3
[Device-vsysa-aaa] local-user vsysauser1@@vsysa access-limit 5
[Device-vsysa-aaa] local-user vsysauser1@@vsysa service-type telnet
[Device-vsysa-aaa] quit
```

----End

Verifying the Configuration

Log in to the virtual system from a terminal using Telnet as the virtual system administrator. For details, see "Example for Configuring Telnet Login" in CLI Configuration Guide > Basic Configuration > CLI-based Device Login Configuration.

 Copyright © Huawei Technologies Co., Ltd.

After logging in to a virtual system, you can configure service features in the virtual system as required. Function Availability for Virtual Systems lists the features supported by a virtual system.

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/1
#
undo telnet server disable
telnet server-source -i GE0/0/1
#
acl number 2001
 rule permit source 10.1.0.10 0
#
user-interface vty 0 5
 acl 2001 inbound
 user privilege level 3
 authentication-mode aaa
 protocol inbound telnet
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
 service-manage enable
 service-manage telnet permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
aaa
 local-user vsysauser1@@vsysa password irreversible-cipher $1b$\#Yy$EcLa.$@5+2%bvdTB[C
\{3g.TxJD`K_Jo+Un0+*Sm+-e&'Z$
 local-user vsysauser1@@vsysa privilege level 3
 local-user vsysauser1@@vsysa access-limit 5
 local-user vsysauser1@@vsysa service-type telnet
#
return
```

6.27 CLI: Example for Configuring STelnet Login to a Virtual System

Networking Requirements

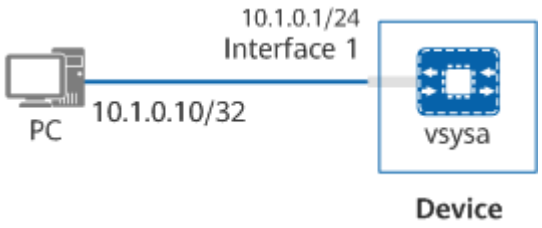
In **Figure 6-27**, the virtual system administrator wants to log in to a virtual system using STelnet to manage configurations in the virtual system. The device functions as an SSH server and uses the password authentication mode to authenticate the PC that functions as an SSH client. Before performing the configuration, ensure that the virtual system has been created, and interfaces and service resources have been allocated to the virtual system as required.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-27 Network diagram for configuring STelnet login to a virtual system

NOTE

In this example, interface 1 represents GE 0/0/1.



Item	Data
Virtual system administrator	User name: vsysauser1@@vsysa Authentication type: local authentication Password: YsHsjx_202206 Trusted host: 10.1.0.10/32
SSH user	User name: vsysauser1@@vsysa Authentication mode: password **NOTE** Only the password authentication mode is supported for STelnet login to a virtual system.
Login interface	Interface number: GE 0/0/1 Security zone: Trust IP address: 10.1.0.1/24 Virtual system: vsysa
Login mode	STelnet

Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair.
2. Enable the STelnet server function and configure related parameters.
3. Configure parameters related to a VTY user interface, including the user privilege level, authentication mode, and supported protocol type.
4. Create an SSH user, configure the authentication mode and service type, and set authentication parameters based on the configured authentication mode.
5. Configure a login interface and add it to a security zone.
6. Create a virtual system administrator whose access type is SSH.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Generate a local key pair.

```
[Device] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

Step 2 Enable the STelnet server function and configure related parameters.

Enable the STelnet server function.

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] stelnet server enable
```

Configure an IP address for the trusted host.

```
[Device] acl 2001
[Device-acl4-basic-2001] rule permit source 10.1.0.10 32
[Device-acl4-basic-2001] quit
```

Configure parameters related to the STelnet server function.

```
[Device] ssh server-source -i ge 0/0/1
[Device] ssh server acl 2000
```

Step 3 Configure parameters related to a VTY user interface, including the user privilege level, authentication mode, and supported protocol type.

```
[Device] user-interface vty 0 5
[Device-ui-vty0-5] user privilege level 3
[Device-ui-vty0-5] authentication-mode aaa
[Device-ui-vty0-5] protocol inbound ssh
[Device-ui-vty0-5] quit
```

NOTE

If SSH is configured as the login protocol, the device automatically disables the Telnet function.

Step 4 Create an SSH user, configure the authentication mode and service type, and set authentication parameters based on the configured authentication mode.

```
[Device] ssh user vsysauser1@@vsysa
[Device] ssh user vsysauser1@@vsysa authentication-type password
[Device] ssh user vsysauser1@@vsysa service-type stelnet
```

NOTE

- The SSH user must have the same name as the virtual system administrator created in the AAA view.
- As the **ssh user** command is case insensitive, the user names vsysauser1@@vsysa and vsysauser1@@VSYSA cannot be distinguished. However, after you run the **ssh user** command to create an SSH user named vsysauser1@@vsysa, the user can log in to vsysa or VSYSA with a corresponding password.

Step 5 Enter the vsysa configuration view.

```
[Device] switch vsys vsysa
```

Step 6 Configure a login interface and add it to a security zone.

```
<Device-vsysa> system-view
[Device-vsysa] interface ge 0/0/1
[Device-vsysa-GE0/0/1] ip address 10.1.0.1 24
[Device-vsysa-GE0/0/1] service-manage enable
[Device-vsysa-GE0/0/1] service-manage ssh permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Device-vsysa-GE0/0/1] quit
[Device-vsysa] firewall zone trust
[Device-vsysa-zone-trust] add interface ge 0/0/1
[Device-vsysa-zone-trust] quit
```

Step 7 Create a virtual system administrator whose access type is SSH.

```
[Device-vsysa] aaa
[Device-vsysa-aaa] local-user vsysauser1@@vsysa password irreversible-cipher YsHsjx_202206
[Device-vsysa-aaa] local-user vsysauser1@@vsysa privilege level 3
[Device-vsysa-aaa] local-user vsysauser1@@vsysa access-limit 5
[Device-vsysa-aaa] local-user vsysauser1@@vsysa service-type ssh
[Device-vsysa-aaa] quit
```

----End

Verifying the Configuration

Log in to the virtual system from a terminal using STelnet as the virtual system administrator. For details, see "Example for Configuring STelnet Login" in CLI Configuration Guide > Basic Configuration > CLI-based Device Login Configuration.

After logging in to a virtual system, you can configure service features in the virtual system as required. Function Availability for Virtual Systems lists the features supported by a virtual system.

Configuration Scripts

- Public system (public)

```
#
 sysname Device
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/1
#
stelnet server enable
ssh server-source -i GE0/0/1
ssh server acl 2000
#
acl number 2001
 rule permit source 10.1.0.10 0
#
user-interface vty 0 5
 user privilege level 3
 authentication-mode aaa
 protocol inbound ssh
#
ssh user vsysauser1@@vsysa
ssh user vsysauser1@@vsysa authentication-type password
ssh user vsysauser1@@vsysa service-type stelnet
#
return
```

- Virtual system (vsysa)

```
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
 service-manage enable
 service-manage ssh permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
aaa
```

 Copyright © Huawei Technologies Co., Ltd.

```
 local-user vsysauser1@@vsysa password irreversible-cipher $1b$\#Yy$EcLa.$@5+2%bvdTB[C
\{3g.TxJD`K_Jo+Un0+*Sm+-e&'Z$
 local-user vsysauser1@@vsysa privilege level 3
 local-user vsysauser1@@vsysa access-limit 5
 local-user vsysauser1@@vsysa service-type ssh
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7 Hot Standby

7.1 Configuring Hot Standby in Active/Standby Mode
7.2 Configuring Hot Standby in Load Sharing Mode
7.3 Configuring Hot Standby in Mirroring Mode
7.4 Configuring Interworking Between Hot Standby and Health Check
7.5 Configuring Association Between Hot Standby and BFD
7.6 Configuring Hot Standby of Virtual Systems
7.7 Configuring IPv6 Hot Standby

7.1 Configuring Hot Standby in Active/Standby Mode

7.1.1 Web: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions

Networking Requirements

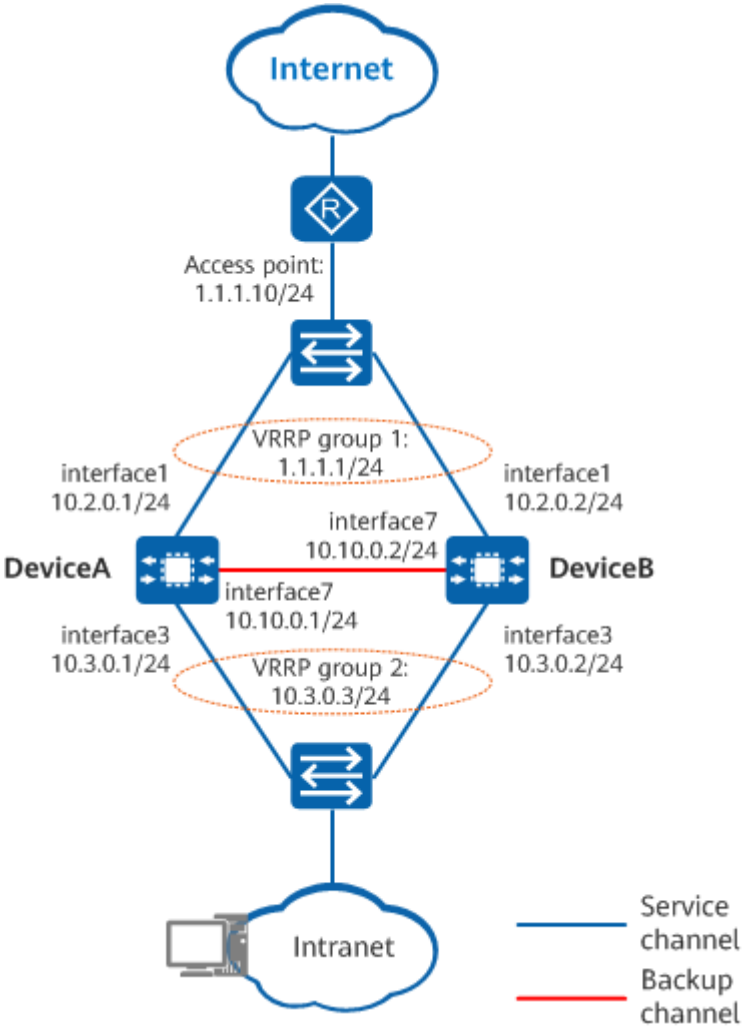
On the network shown in **Figure 7-1**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to Layer 2 switches. The upstream switch is connected to the carrier network, and the public IP address the carrier assigns to the enterprise is 1.1.1.1. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-1 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.2/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.2/24

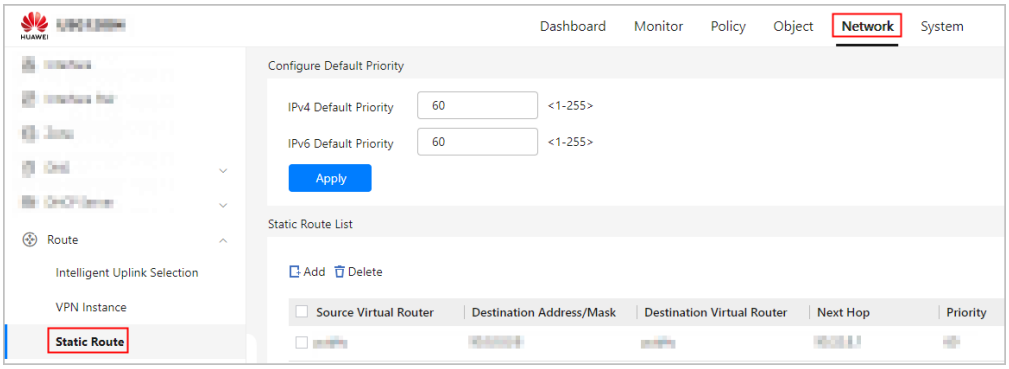
   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure static routes.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Network** > **Route** > **Static Route**.



 Copyright © Huawei Technologies Co., Ltd.

2. In **Static Route List**, click **Add**, configure a default route based on the following parameter values, and click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Interface	1.1.1.10
Next Hop	GE0/0/1

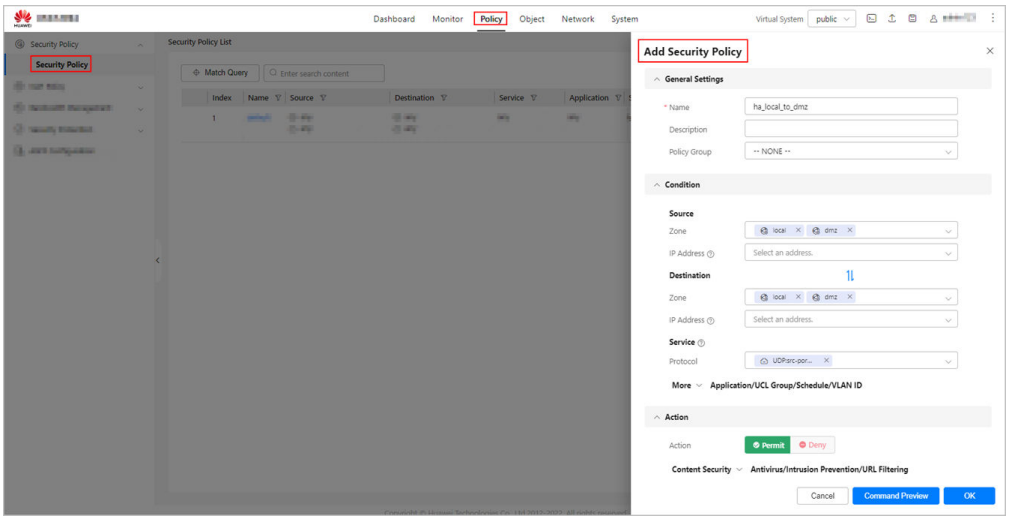
Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.



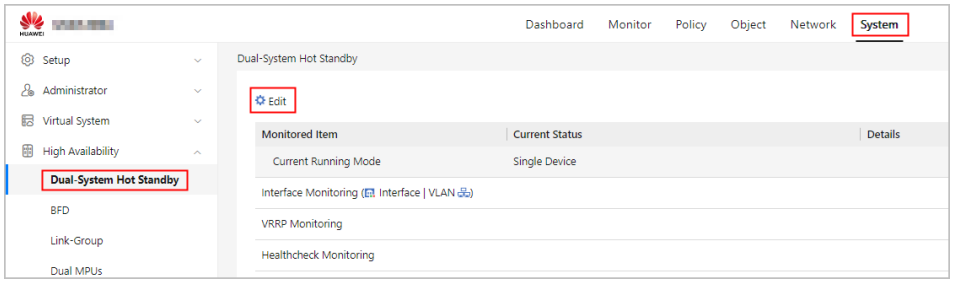
Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514

 Copyright © Huawei Technologies Co., Ltd.

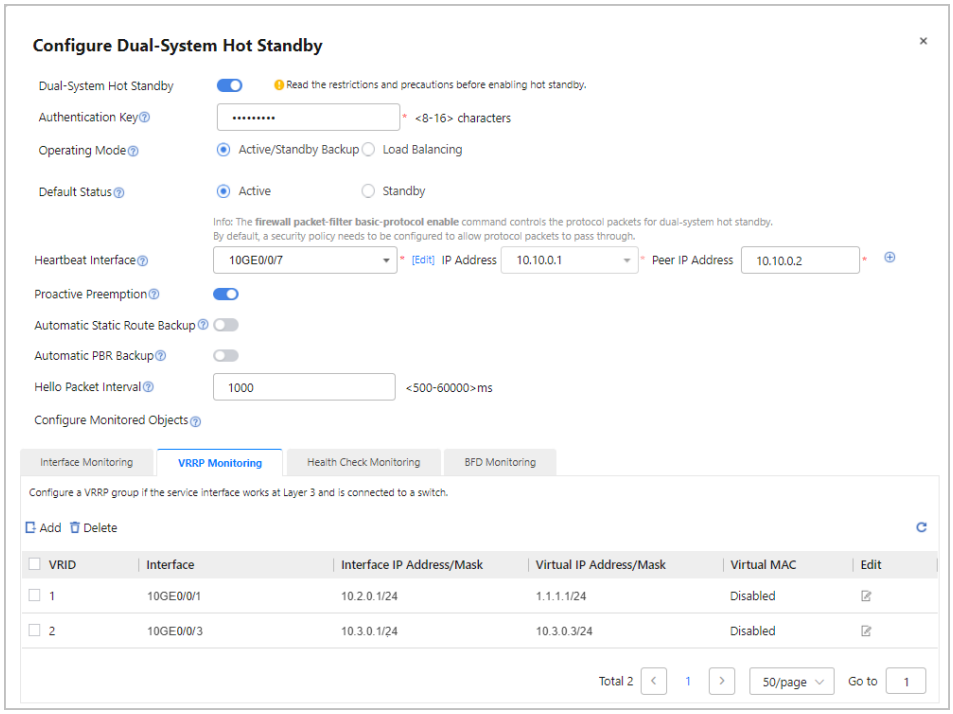
Action	Permit

Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

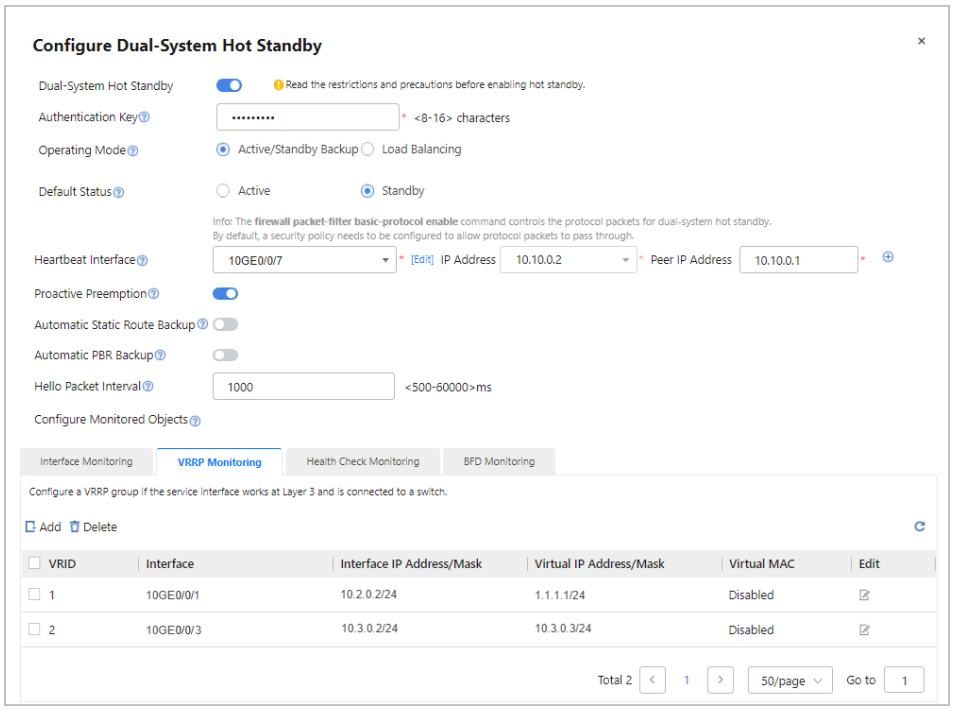


   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 Configure a security policy.

Configure a security policy on DeviceA to allow intranet users to access the Internet. After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

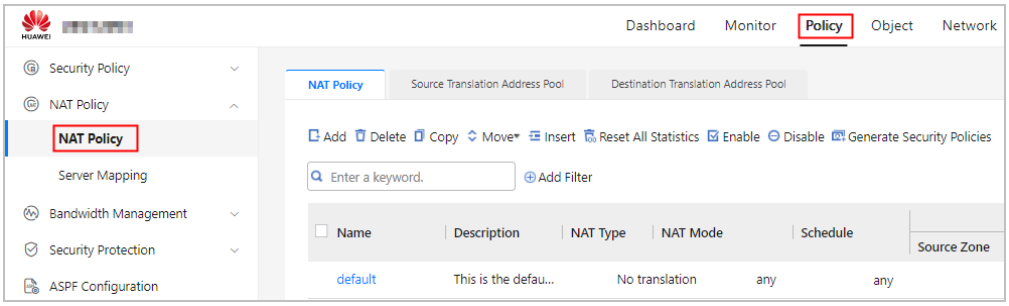
Name	trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

Step 6 Configure a NAT policy.

Configure a NAT policy on DeviceA to allow intranet users to access the Internet using the public IP address after NAT. That is, the source IP addresses on subnet 10.3.0.0/16 are translated into IP addresses in the NAT address pool (1.1.1.2 to 1.1.1.5) when intranet users access the Internet. After hot standby relationship is established, the NAT policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.



2. Click the **Source Translation Address Pool** tab, click **Add**, configure a NAT address pool and set the parameters as follows, and then click **OK**.

Name	addressgroup1
IP Address Range	1.1.1.2-1.1.1.5

3. Click the **NAT Policy** tab, click **Add**, configure a NAT policy and set the parameters as follows, and then click **OK**.

Name	policy_nat1
NAT Type	NAT
NAT Mode	Source address translation
Source Zone	trust
Destination Type	Destination Zone: untrust
Source Address	10.3.0.0/16
Source Address Translated To	IP Addresses in the IP Address Pool
Source Translation Address Pool	addressgroup1

Step 7 Configure the switches and PCs.

1. Add the three interfaces of the switches to the same VLANs accordingly. For configuration commands, refer to related documents of the switches.
2. On intranet PCs, specify the virtual IP address of VRRP group 2 as the default gateway address. Details are omitted.

Step 8 Configure the router.

Configure equal-cost routes to DeviceA and DeviceB, with the next hop being the virtual IP addresses of VRRP group 1.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

 Copyright © Huawei Technologies Co., Ltd.

- Normally, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0 active
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 10.3.0.3 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 16
  action source-nat address-group group1
#
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0 standby
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.3.0.3 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 16
  action source-nat address-group group1
#
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.2 CLI: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions

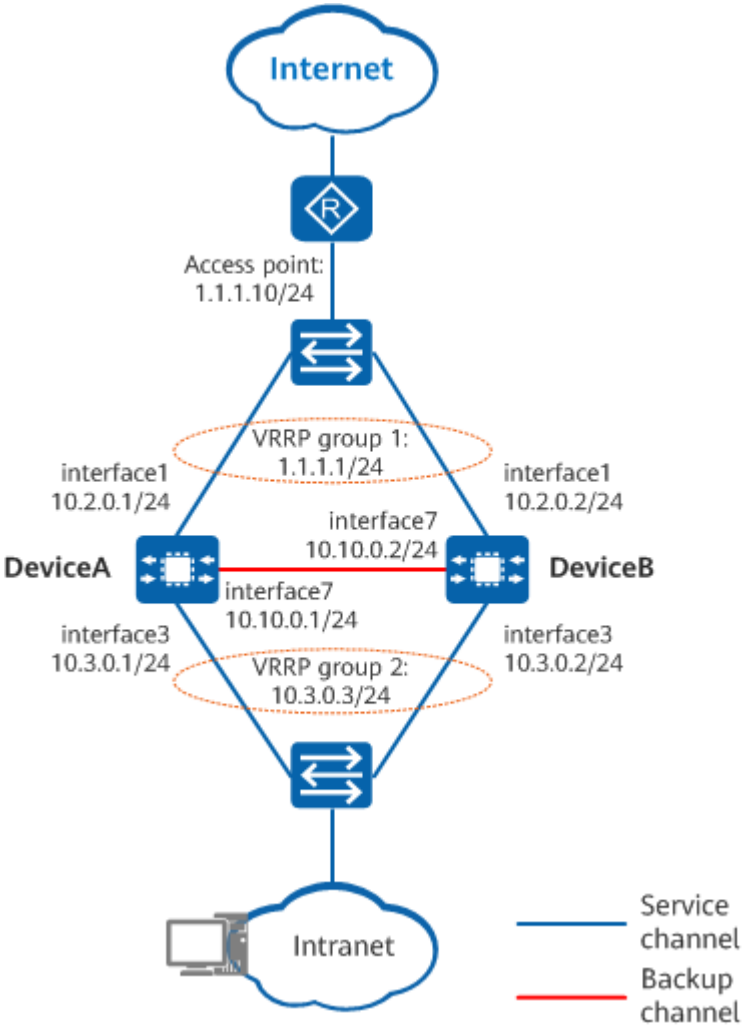
Networking Requirements

On the network shown in **Figure 7-2**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to Layer 2 switches. The upstream switch is connected to the carrier network, and the public IP address the carrier assigns to the enterprise is 1.1.1.1. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-2 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Configure an IP address for each interface on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.0.2 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Create a default route with next hop 1.1.1.10 on DeviceA and DeviceB to forward traffic of intranet users to the router.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.10**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.10**

Step 2 Configure VRRP groups.

DeviceA	DeviceB
# Configure VRRP group 1 on DeviceA's upstream service interface GE 0/0/1 and set its state to active. Configure VRRP group 1 on DeviceB's upstream service interface GE 0/0/1 and specify **standby** in the **vrrp vrid virtual-ip** command for the VRRP group. If the IP addresses of the interface and VRRP group are on different subnets, specify a mask when configuring the IP address of the VRRP group.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.1 24 active** [DeviceA-GE0/0/1] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.1 24 standby** [DeviceB-GE0/0/1] **quit**
# Configure VRRP group 2 on DeviceA's downstream service interface GE 0/0/3 and set its state to active. Configure VRRP group 2 on DeviceB's downstream service interface GE 0/0/3 and **standby** in the **vrrp vrid virtual-ip** command for the VRRP group.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 2 virtual-ip 10.3.0.3 active** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 2 virtual-ip 10.3.0.3 standby** [DeviceB-GE0/0/3] **quit**

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Specify the heartbeat interface, configure the authentication key, and enable hot standby.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Create a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name trust_to_untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] action permit
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure a NAT policy on DeviceA. After hot standby is enabled, the NAT policy on DeviceA will be automatically backed up to DeviceB.

Configure a NAT policy to translate source addresses on subnet 10.3.0.0/16 to IP addresses in the NAT address pool (1.1.1.2 to 1.1.1.5) when intranet users access the Internet.

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA] nat address-group group1
HRP_M[DeviceA-address-group-group1] section 0 1.1.1.2 1.1.1.5
HRP_M[DeviceA-address-group-group1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat1
HRP_M[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat1] source-address 10.3.0.0 16
HRP_M[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group group1
```

Step 7 Configure switches and intranet PCs.

1. Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.
2. On intranet PCs, specify the virtual IP address of VRRP group 2 as the default gateway address. Details are omitted.

Step 8 Configure the router.

Configure routes to DeviceA and DeviceB, with the next hop being the virtual IP addresses of VRRP group 1.

----End

Verifying the Configuration

1. Run the **display vrrp** command on DeviceA and DeviceB to check the status of interfaces in the VRRP group.
2. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
3. Ping Router in the untrust zone from the PC in the trust zone, and run the **display firewall session table** command to check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall session table** Current Total Sessions : 1 icmp VPN: public --> public 10.3.0.10:0[1.1.1.2:10298] --> 1.1.1.10:2048	HRP_S<DeviceB> **display firewall session table** Current Total Sessions : 1 icmp VPN:public --> public **Remote** 10.3.0.10:0[1.1.1.2:10298] --> 1.1.1.10:2048

The command output shows that sessions tagged with **Remote** are created on DeviceB, indicating that sessions are successfully backed up after hot standby is configured.

4. Run the **ping 1.1.1.10 -t** command on the PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is performed and whether ping packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0 active
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 10.3.0.3 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 16
  action source-nat address-group group1
#
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0 standby
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.3.0.3 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 16
  action source-nat address-group group1
#
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.3 Web: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices

Networking Requirements

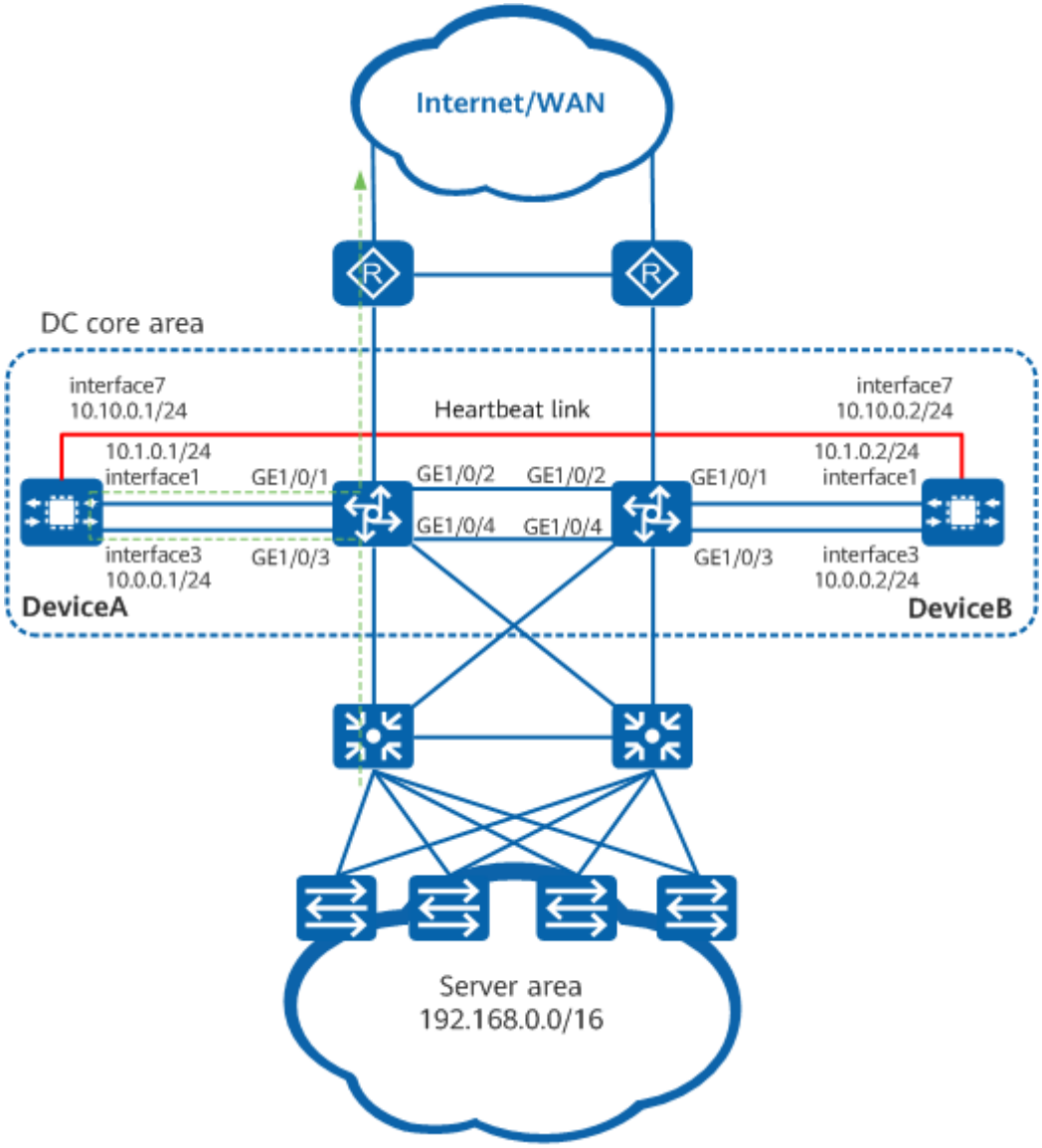
As shown in **Figure 7-3**, DeviceA and DeviceB are connected to core switches in the data center in off-path mode to ensure security of the data center network. All traffic on the core switches is diverted to DeviceA and DeviceB based on static routes for security checks. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-3 Network diagram of configuring hot standby when devices are deployed in off-path mode (using static routing for traffic diversion)

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



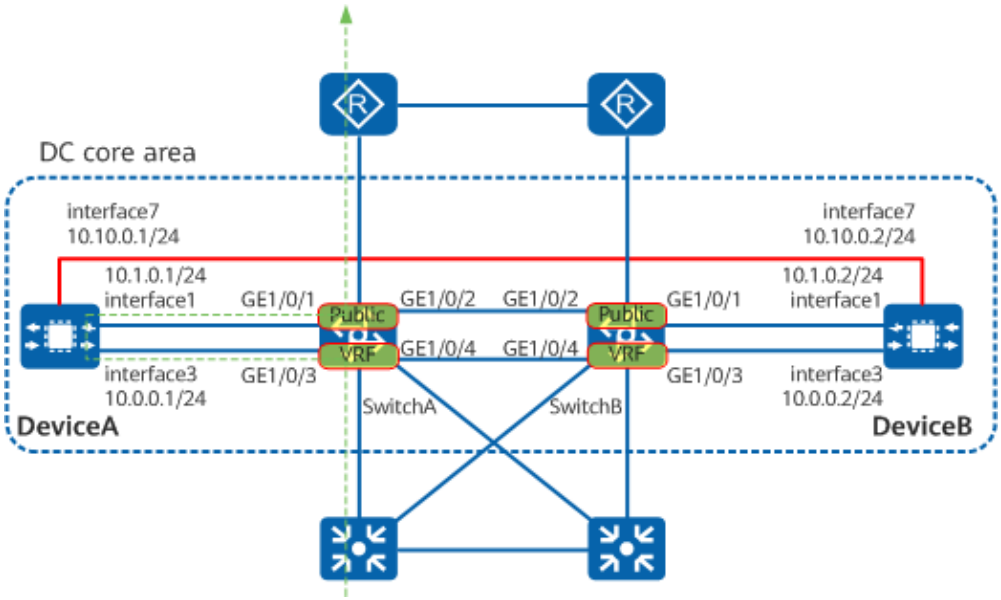
Configuration Roadmap

1. In **Figure 7-4**, if you want the core switches to divert traffic to DeviceA and DeviceB through static routes, you need to configure static routes and set the next hops to the IP addresses of interfaces of DeviceA and DeviceB. However, because the core switches, upstream routers, and downstream aggregation switches run OSPF, traffic cannot be diverted to DeviceA or DeviceB after reaching the core switches. Instead, the traffic is directly forwarded to upstream or downstream devices.

   Therefore, you must configure the virtual routing and forwarding (VRF) function on the core switches. This virtualizes each core switch into a public switch (Public) and a virtual switch (VRF), both of which are isolated. A public switch is used for connecting to the upstream device, whereas a VRF is used for connecting to the downstream device. In this way, traffic can be diverted to DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-4 Configuring VRF on switches

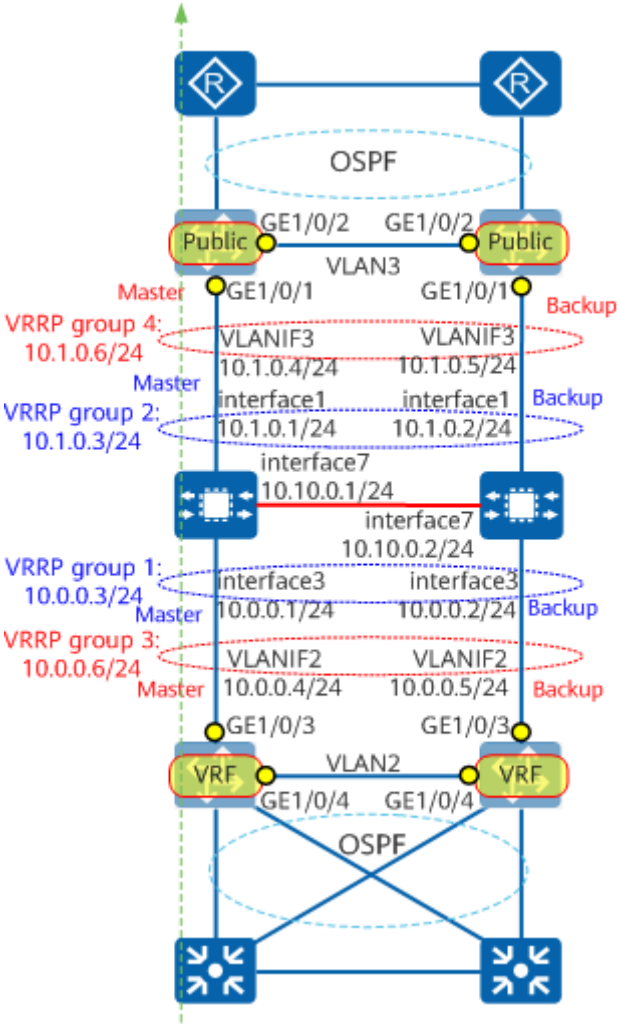


2. An abstract of **Figure 7-4** is shown in **Figure 7-5**. DeviceA and DeviceB run static routes to communicate with upstream and downstream switches (Public and VRF). To enable them to communicate using the virtual IP addresses of VRRP groups, you need to configure VRRP groups on DeviceA, DeviceB, and switches.

   As shown in **Figure 7-5**, configure static routes on DeviceA and DeviceB, and set the next hops to the IP addresses of VRRP groups 3 and 4. Configure a static route on the Public switch and set the next hop to the IP address of VRRP group 2. Then, configure a static route on the VRF switch and set the next hop to the IP address of VRRP group 1.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-5 Configuring VRRP on DeviceA, DeviceB, and switches



NOTE

The core switches run static routes to communicate with DeviceA and DeviceB and run OSPF to communicate with other devices. **Figure 7-5** lists only the core switch interfaces related to DeviceA and DeviceB.

3. Specify GE 0/0/7 on DeviceA and DeviceB as the heartbeat interface and enable hot standby.
4. After configuring hot standby, configure security functions such as security policies, IPS, and attack defense on DeviceA. DeviceA will automatically synchronize its configurations to DeviceB. This section describes only security policy configurations as an example.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv4	
IP Address	10.1.0.1/24

c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.0.0.1/24

d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.0.2/24

   c. Repeat the preceding steps to configure GE0/0/3.

Zone	trust
IPv4	
IP Address	10.0.0.2/24

   d. Repeat the preceding steps to configure GE0/0/7.

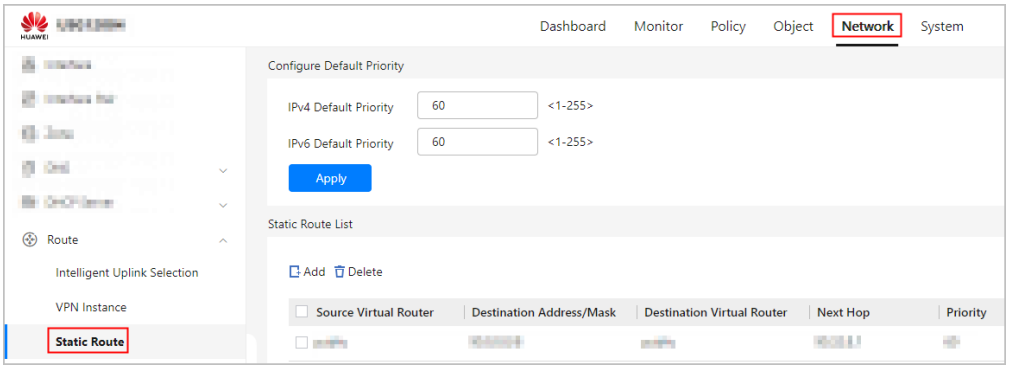
Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure static routes.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Network** > **Route** > **Static Route**.



2. In **Static Route List**, click **Add**, configure a static route (default route) for the upstream direction and set the next hop to the IP address of VRRP group 4, and then click **OK**.

Destination Address	0.0.0.0
Mask	0.0.0.0
Next Hop	10.1.0.6

3. Configure a static route for the downstream direction and set the destination address to an address in the server area and the next hop to the IP address of VRRP group 3.

Destination Address	192.168.0.0
Mask	255.255.0.0
Next Hop	10.0.0.6

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

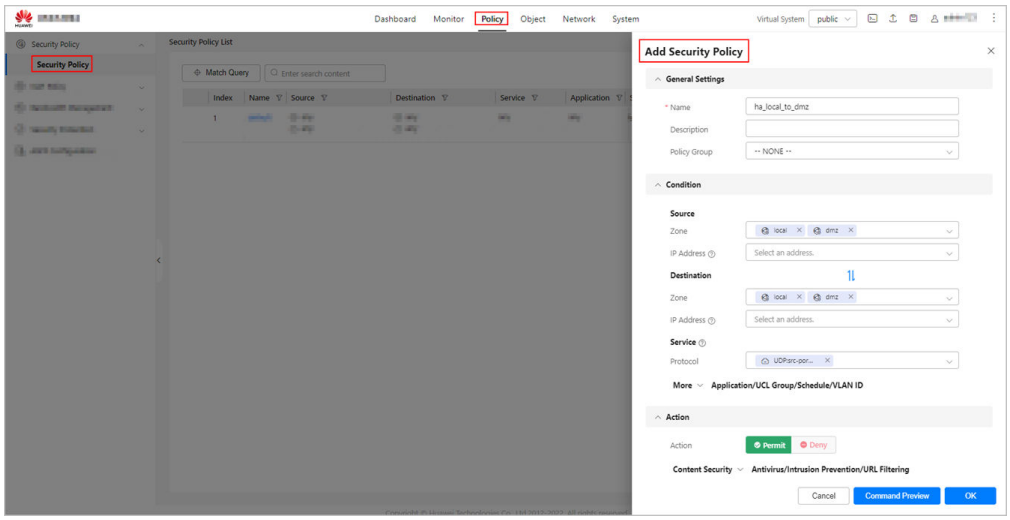
NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

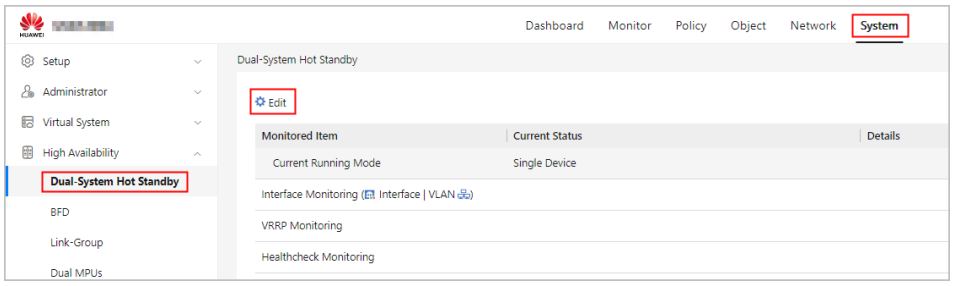
 Copyright © Huawei Technologies Co., Ltd.



Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

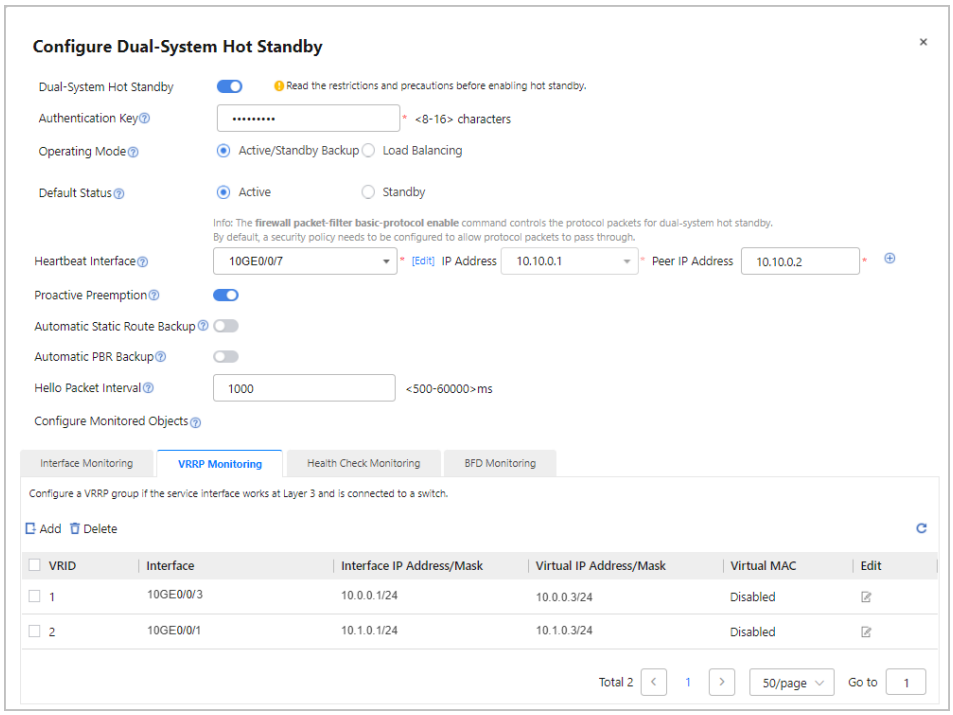
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.



   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

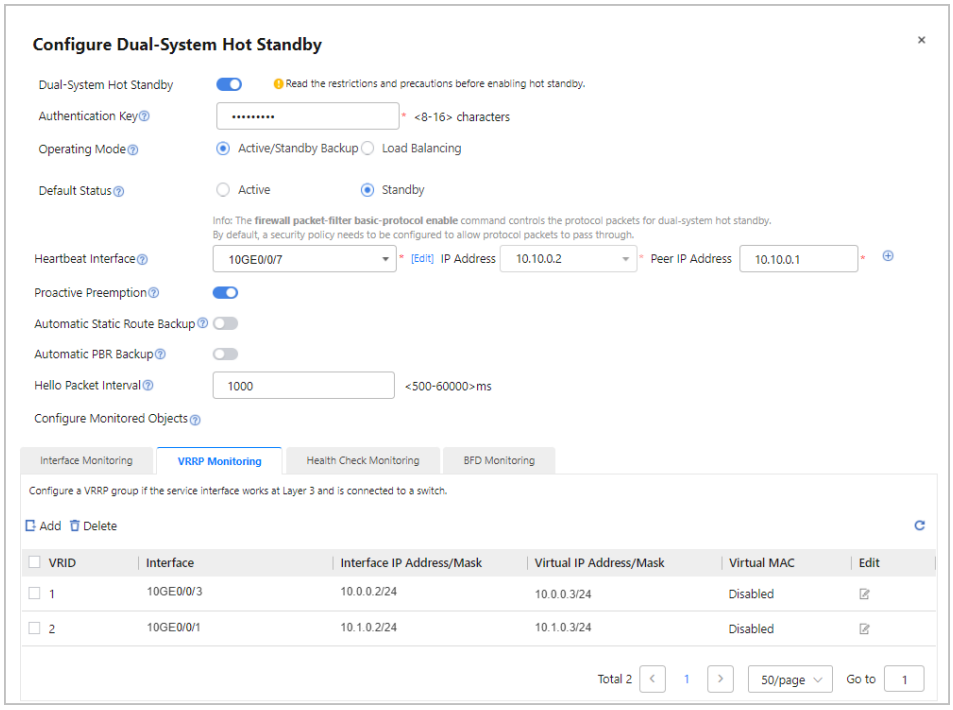
 Copyright © Huawei Technologies Co., Ltd.



2. Configure hot standby on DeviceB.

   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



Step 5 Configure a security policy.

Configure a security policy on DeviceA to allow Internet users to access the server area (subnet: 192.168.0.0/16, port: 80) in the data center. After hot standby

 Copyright © Huawei Technologies Co., Ltd.

relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

Name	policy_sec1
Source Zone	untrust
Destination Zone	trust
Destination Address	192.168.0.0/16
Service	http
Action	Permit

Step 6 Configure core switches.

NOTE

This example describes only the switch configurations for interconnection with DeviceA and DeviceB.

Configure SwitchA.

```
[SwitchA] ip vpn-instance VRF     //Create VRF.
[SwitchA-vpn-instance-VRF] ipv4-family
[SwitchA-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchA-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchA-vpn-instance-VRF-af-ipv4] quit
[SwitchA-vpn-instance-VRF] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/3 to 1/0/4     //Add the interface to VLAN2.
[SwitchA-vlan2] quit
[SwitchA] interface Vlanif 2
[SwitchA-Vlanif2] ip binding vpn-instance VRF     //Bind VLANIF2 to VRF.
[SwitchA-Vlanif2] ip address 10.0.0.4 24
[SwitchA-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6     //Create VRRP group 3.
[SwitchA-Vlanif2] vrrp vrid 3 priority 120     //Set the priority to 120. The VRRP group with a higher priority is active.
[SwitchA-Vlanif2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchA-vlan3] quit
[SwitchA] interface Vlanif 3
[SwitchA-Vlanif3] ip address 10.1.0.4 24
[SwitchA-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchA-Vlanif3] vrrp vrid 4 priority 120     //Set the priority to 120. The VRRP group with a higher priority is active.
[SwitchA-Vlanif3] quit
[SwitchA] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3     //Configure a default route on the virtual switch (VRF) and set the next hop to the virtual IP address of VRRP group 1.
[SwitchA] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3     //Configure a static route on the public switch (Public) and set the next hop to the virtual IP address of VRRP group 2.
```

Configure SwitchB.

```
[SwitchB] ip vpn-instance VRF     //Create VRF.
[SwitchB-vpn-instance-VRF] ipv4-family
[SwitchB-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchB-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
```

 Copyright © Huawei Technologies Co., Ltd.

```
[SwitchB-vpn-instance-VRF-af-ipv4] quit
[SwitchB-vpn-instance-VRF] quit
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/3 to 1/0/4     //Add the interface to VLAN2.
[SwitchB-vlan2] quit
[SwitchB] interface Vlanif 2
[SwitchB-Vlanif2] ip binding vpn-instance VRF     //Bind VLANIF2 to VRF.
[SwitchB-Vlanif2] ip address 10.0.0.5 24
[SwitchB-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6     //Create VRRP group 3.
[SwitchB-Vlanif2] vrrp vrid 3 priority 100     //Set the priority to 100. The VRRP group with a lower priority is standby.
[SwitchB-Vlanif2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchB-vlan3] quit
[SwitchB] interface Vlanif 3
[SwitchB-Vlanif3] ip address 10.1.0.5 24
[SwitchB-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchB-Vlanif3] vrrp vrid 4 priority 100     //Set the priority to 100. The VRRP group with a lower priority is standby.
[SwitchB-Vlanif3] quit
[SwitchB] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3     //Configure a default route on the virtual switch (VRF) and set the next hop to the virtual IP address of VRRP group 1.
[SwitchB] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3     //Configure a static route on the public switch (Public) and set the next hop to the virtual IP address of VRRP group 2.
```

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 active
#
interface GE0/0/3
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 standby
#
interface GE0/0/3
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.4 CLI: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices

Networking Requirements

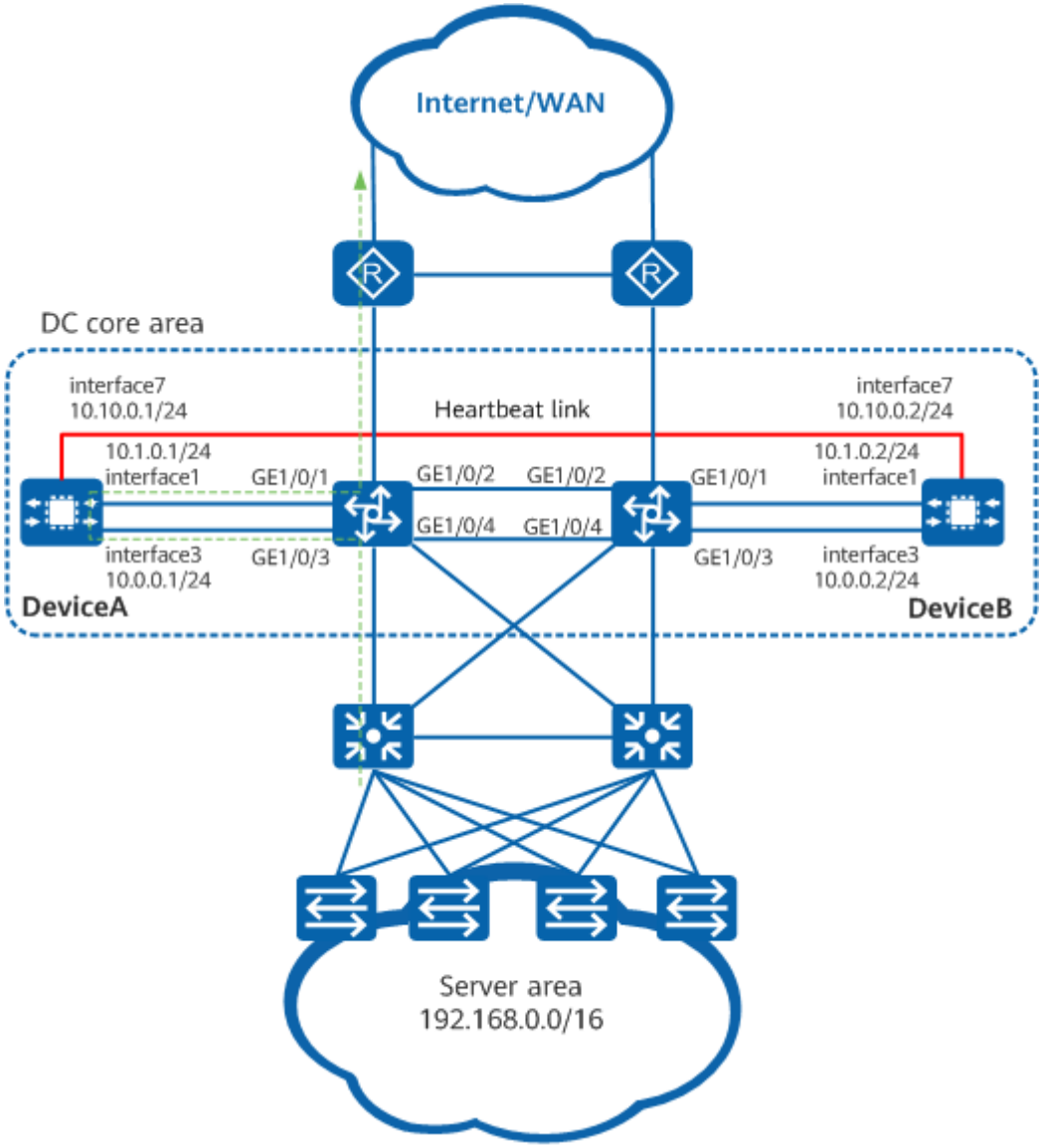
As shown in **Figure 7-6**, DeviceA and DeviceB are connected to core switches in the data center in off-path mode to ensure security of the data center network. All traffic on the core switches is diverted to DeviceA and DeviceB based on static routes for security checks. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-6 Network diagram of configuring hot standby when devices are deployed in off-path mode (using static routing for traffic diversion)

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



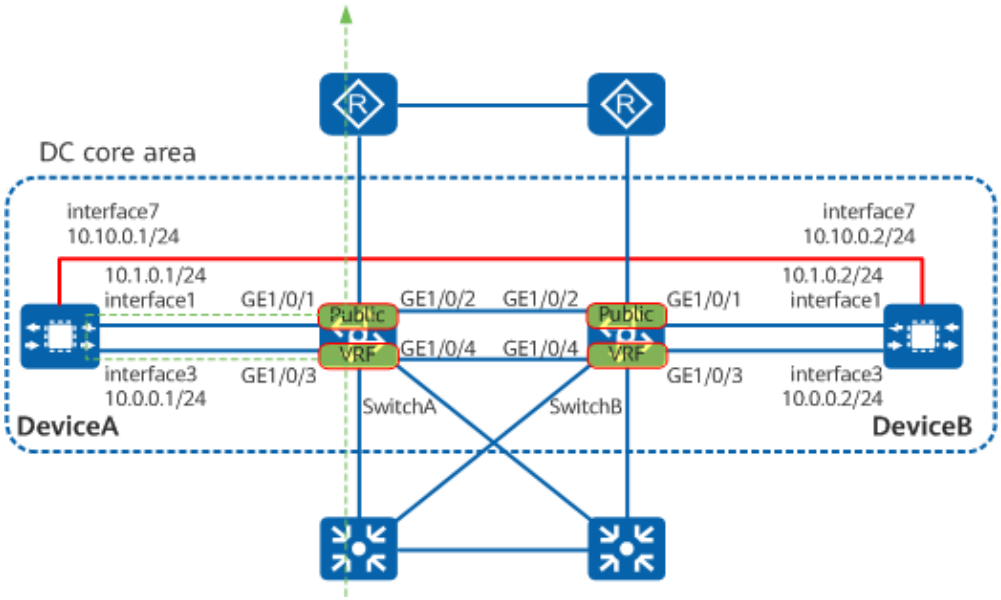
Configuration Roadmap

1. In **Figure 7-7**, if you want the core switches to divert traffic to DeviceA and DeviceB through static routes, you need to configure static routes and set the next hops to the IP addresses of interfaces of DeviceA and DeviceB. However, because the core switches, upstream routers, and downstream aggregation switches run OSPF, traffic cannot be diverted to DeviceA or DeviceB after reaching the core switches. Instead, the traffic is directly forwarded to upstream or downstream devices.

   Therefore, you must configure the virtual routing and forwarding (VRF) function on the core switches. This virtualizes each core switch into a public switch (Public) and a virtual switch (VRF), both of which are isolated. A public switch is used for connecting to the upstream device, whereas a VRF is used for connecting to the downstream device. In this way, traffic can be diverted to DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-7 Configuring VRF on switches

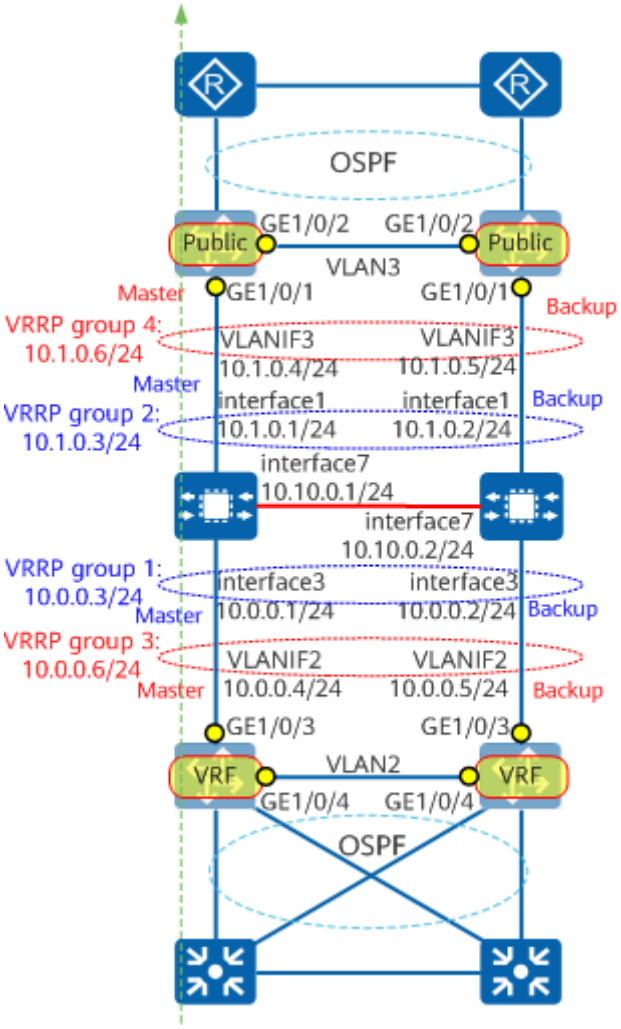


2. An abstract of **Figure 7-7** is shown in **Figure 7-8**. DeviceA and DeviceB run static routes to communicate with upstream and downstream switches (Public and VRF). To enable them to communicate using the virtual IP addresses of VRRP groups, you need to configure VRRP groups on DeviceA, DeviceB, and switches.

   As shown in **Figure 7-8**, configure static routes on DeviceA and DeviceB, and set the next hops to the IP addresses of VRRP groups 3 and 4. Configure a static route on the Public switch and set the next hop to the IP address of VRRP group 2. Then, configure a static route on the VRF switch and set the next hop to the IP address of VRRP group 1.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-8 Configuring VRRP on DeviceA, DeviceB, and switches



NOTE

The core switches run static routes to communicate with DeviceA and DeviceB and run OSPF to communicate with other devices. **Figure 7-8** lists only the core switch interfaces related to DeviceA and DeviceB.

3. Specify GE 0/0/7 on DeviceA and DeviceB as the heartbeat interface and enable hot standby.
4. After configuring hot standby, configure security functions such as security policies, IPS, and attack defense on DeviceA. DeviceA will automatically synchronize its configurations to DeviceB. This section describes only security policy configurations as an example.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.1.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.0.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.1.0.2 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.0.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

Step 2 Configure static routes.

DeviceA	DeviceB
# Configure a static route (default route) for the upstream direction and set the next hop to the IP address of VRRP group 4.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 10.1.0.6**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 10.1.0.6**
# Configure a static route for the downstream direction and set the destination address to an address in the server area and the next hop to the IP address of VRRP group 3.	
[DeviceA] **ip route-static 192.168.0.0 255.255.0.0 10.0.0.6**	[DeviceB] **ip route-static 192.168.0.0 255.255.0.0 10.0.0.6**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Configure hot standby.

DeviceA	DeviceB
# Configure VRRP groups on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp vrid 2 virtual-ip 10.1.0.3 active** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 1 virtual-ip 10.0.0.3 active** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp vrid 2 virtual-ip 10.1.0.3 standby** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 1 virtual-ip 10.0.0.3 standby** [DeviceB-GE0/0/3] **quit**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Configure a security policy on DeviceA. After hot standby is enabled, the security policy configuration on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow external network users to access the server area (subnet: 192.168.0.0/16, port: 80) in the data center.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec1
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-address 192.168.0.0 16
HRP_M[DeviceA-policy-security-rule-policy_sec1] service http
HRP_M[DeviceA-policy-security-rule-policy_sec1] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec1] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure core switches.

NOTE

This example describes only the switch configurations for interconnection with DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configure SwitchA.

```
[SwitchA] ip vpn-instance VRF     //Create VRF.
[SwitchA-vpn-instance-VRF] ipv4-family
[SwitchA-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchA-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchA-vpn-instance-VRF-af-ipv4] quit
[SwitchA-vpn-instance-VRF] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/3 to 1/0/4     //Add the interface to VLAN2.
[SwitchA-vlan2] quit
[SwitchA] interface Vlanif 2
[SwitchA-Vlanif2] ip binding vpn-instance VRF     //Bind VLANIF2 to VRF.
[SwitchA-Vlanif2] ip address 10.0.0.4 24
[SwitchA-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6     //Create VRRP group 3.
[SwitchA-Vlanif2] vrrp vrid 3 priority 120     //Set the priority to 120. The VRRP group with a higher priority is active.
[SwitchA-Vlanif2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchA-vlan3] quit
[SwitchA] interface Vlanif 3
[SwitchA-Vlanif3] ip address 10.1.0.4 24
[SwitchA-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchA-Vlanif3] vrrp vrid 4 priority 120     //Set the priority to 120. The VRRP group with a higher priority is active.
[SwitchA-Vlanif3] quit
[SwitchA] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3     //Configure a default route on the virtual switch (VRF) and set the next hop to the virtual IP address of VRRP group 1.
[SwitchA] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3     //Configure a static route on the public switch (Public) and set the next hop to the virtual IP address of VRRP group 2.
```

Configure SwitchB.

```
[SwitchB] ip vpn-instance VRF     //Create VRF.
[SwitchB-vpn-instance-VRF] ipv4-family
[SwitchB-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchB-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchB-vpn-instance-VRF-af-ipv4] quit
[SwitchB-vpn-instance-VRF] quit
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/3 to 1/0/4     //Add the interface to VLAN2.
[SwitchB-vlan2] quit
[SwitchB] interface Vlanif 2
[SwitchB-Vlanif2] ip binding vpn-instance VRF     //Bind VLANIF2 to VRF.
[SwitchB-Vlanif2] ip address 10.0.0.5 24
[SwitchB-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6     //Create VRRP group 3.
[SwitchB-Vlanif2] vrrp vrid 3 priority 100     //Set the priority to 100. The VRRP group with a lower priority is standby.
[SwitchB-Vlanif2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchB-vlan3] quit
[SwitchB] interface Vlanif 3
[SwitchB-Vlanif3] ip address 10.1.0.5 24
[SwitchB-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchB-Vlanif3] vrrp vrid 4 priority 100     //Set the priority to 100. The VRRP group with a lower priority is standby.
[SwitchB-Vlanif3] quit
[SwitchB] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3     //Configure a default route on the virtual switch (VRF) and set the next hop to the virtual IP address of VRRP group 1.
[SwitchB] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3     //Configure a static route on the public switch (Public) and set the next hop to the virtual IP address of VRRP group 2.
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Run the **display firewall session table** command on DeviceA and DeviceB. The command output shows that DeviceA has sessions and DeviceB has sessions tagged with **Remote**, indicating that core switch traffic is diverted to DeviceA, and hot standby in active/standby mode is successfully configured.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 active
#
interface GE0/0/3
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 standby
#
interface GE0/0/3
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.5 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions

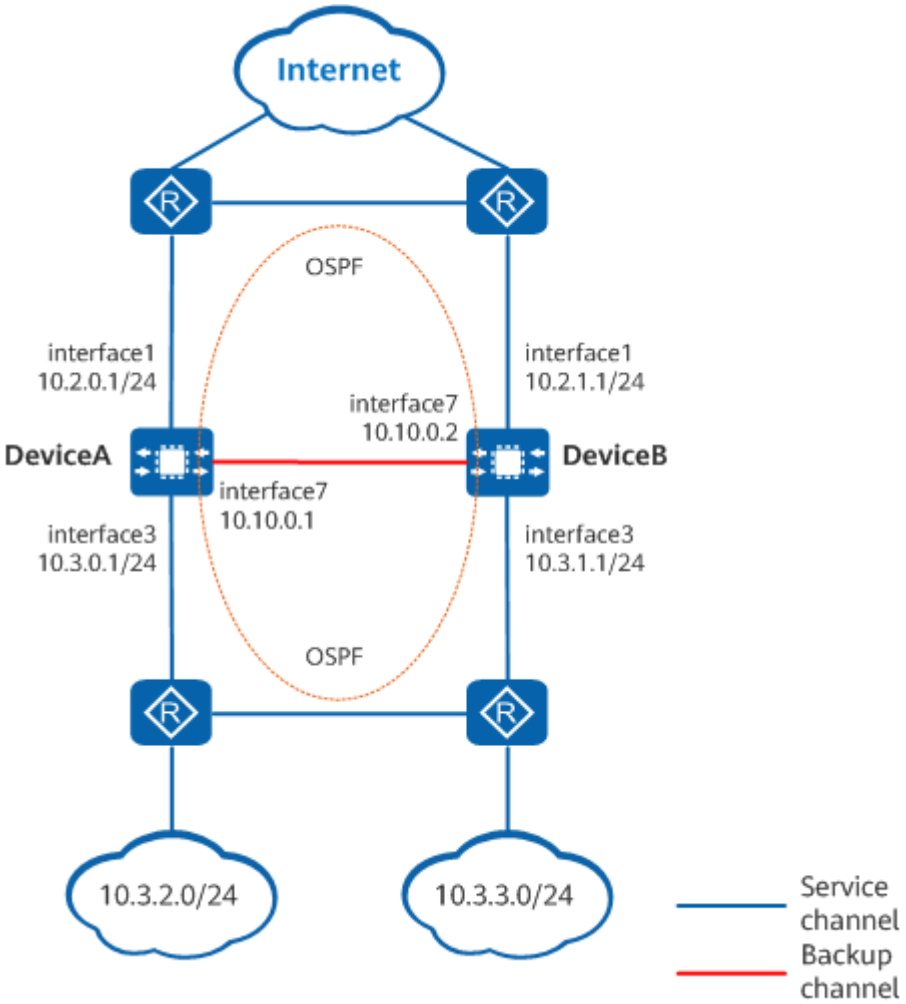
Networking Requirements

As shown in **Figure 7-9**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers. OSPF runs between the devices and upstream and downstream routers. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-9 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz

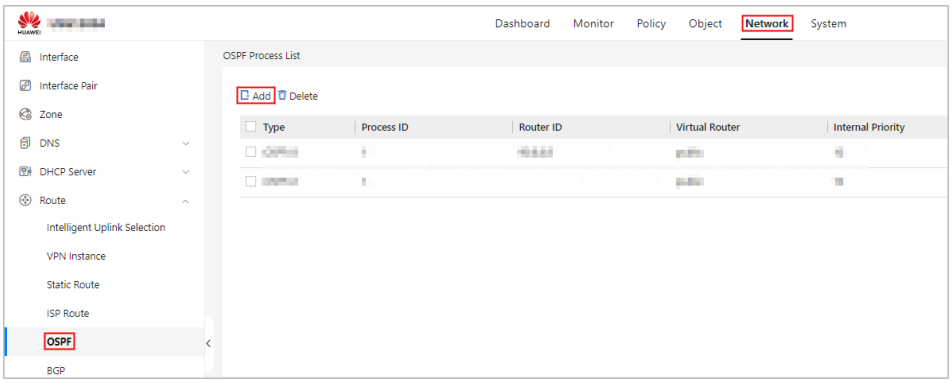
 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF to ensure IP connectivity.

1. Configure OSPF on DeviceA.

   a. Choose **Network** > **Route** > **OSPF** and click **Add**.



   b. Create an OSPF process, set the parameters as follows, and click **OK**.

Type	OSPFv2
Process ID	10

   c. Click , click **Add**, create an OSPF area and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.0.0
Mask/Wildcard Mask	255.255.255.0

   d. Choose **Basic Configuration** > **Network Settings**, click **Add**, create a network and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

2. Configure OSPF on DeviceB.

   a. Choose **Network** > **Route** > **OSPF**, click **Add**, create an OSPF process and set the parameters as follows, and then click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Type	OSPFv2
Process ID	10

b. Click , click **Add**, create an OSPF area and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.1.0
Mask/Wildcard Mask	255.255.255.0

c. Choose **Basic Configuration** > **Network Settings**, click **Add**, create a network and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.1.0
Mask/Wildcard Mask	255.255.255.0

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

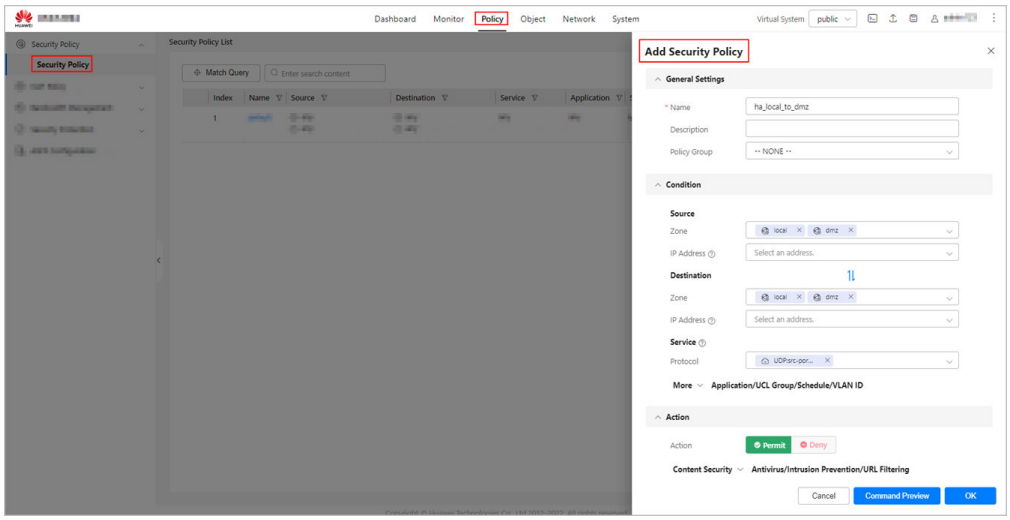
NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

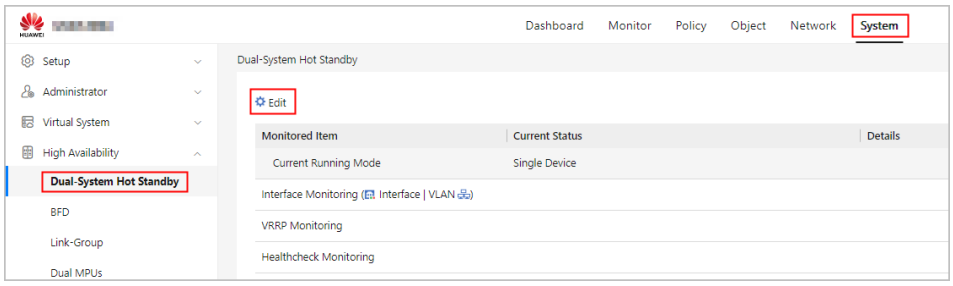
 Copyright © Huawei Technologies Co., Ltd.



Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

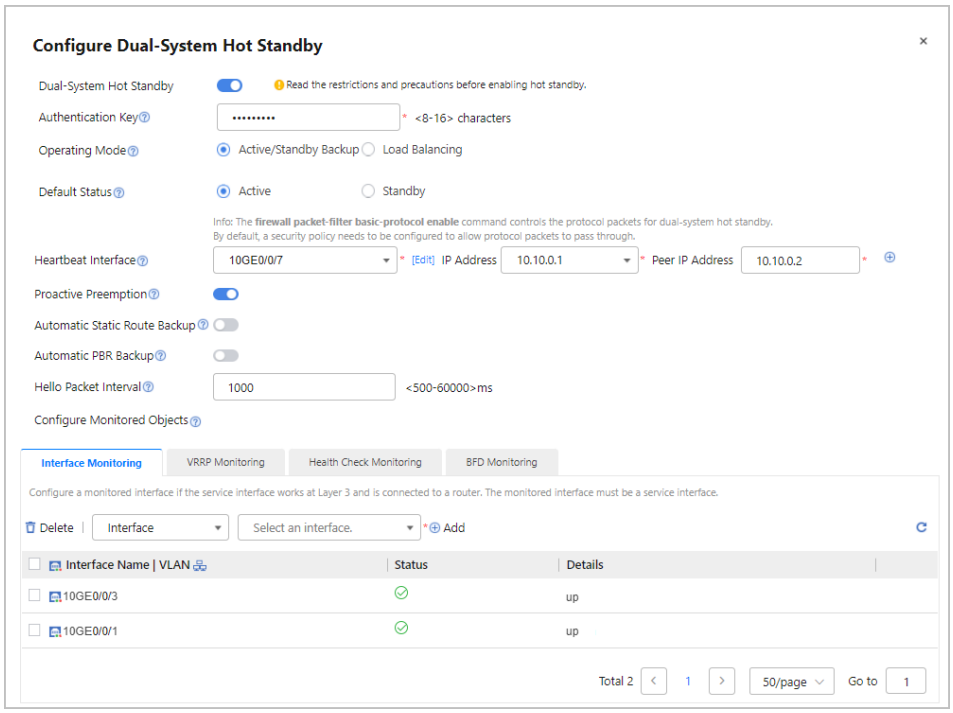
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

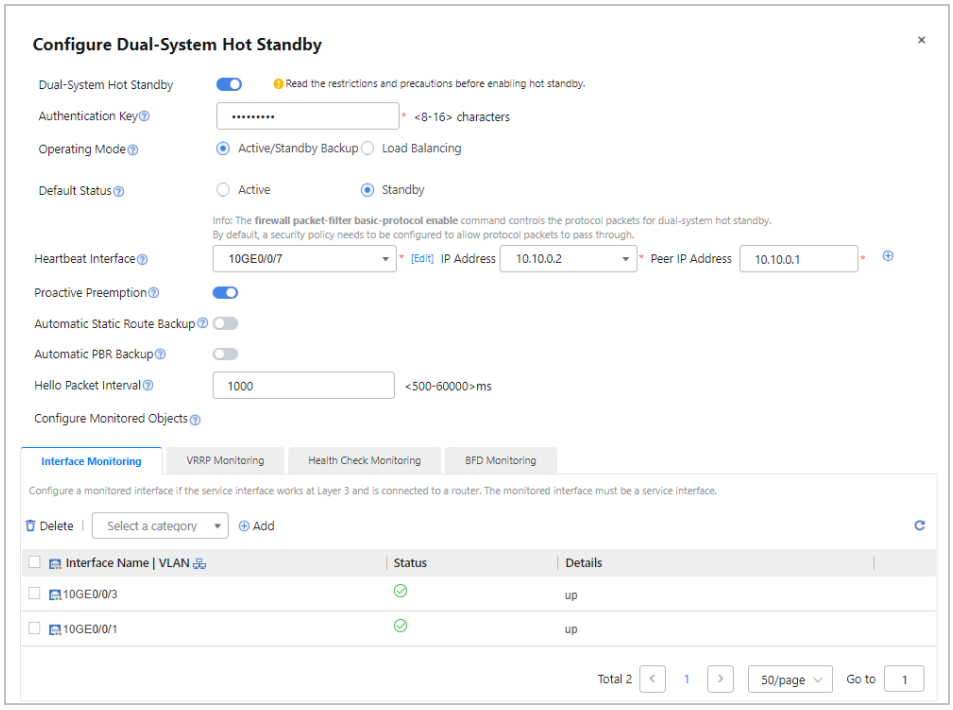


   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



Step 5 Configure the security policies.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure security policies and set the parameters as follows, and then click **OK**.

   # Configure security policies to allow the devices and the upstream/downstream routers to exchange OSPF packets.

   NOTE

   Controlling function of security policies for OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, OSPF packets are controlled by security policies. In this case, a security policy must be configured between the security zones where the upstream/downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_ospf_1
Source Zone	local
Destination Zone	trust,untrust
Service	ospf
Action	Permit

Name	policy_ospf_2
Source Zone	trust,untrust
Destination Zone	local
Service	ospf
Action	Permit

   # Configure a security policy to allow intranet users to access the Internet.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.0/24,10.3.3.0/24
Action	Permit

Step 6 Configure the routers.

 Copyright © Huawei Technologies Co., Ltd.

Configure OSPF on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 24
  source-address 10.3.3.0 24
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 24
  source-address 10.3.3.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action permit # return	action permit # return

7.1.6 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions

Networking Requirements

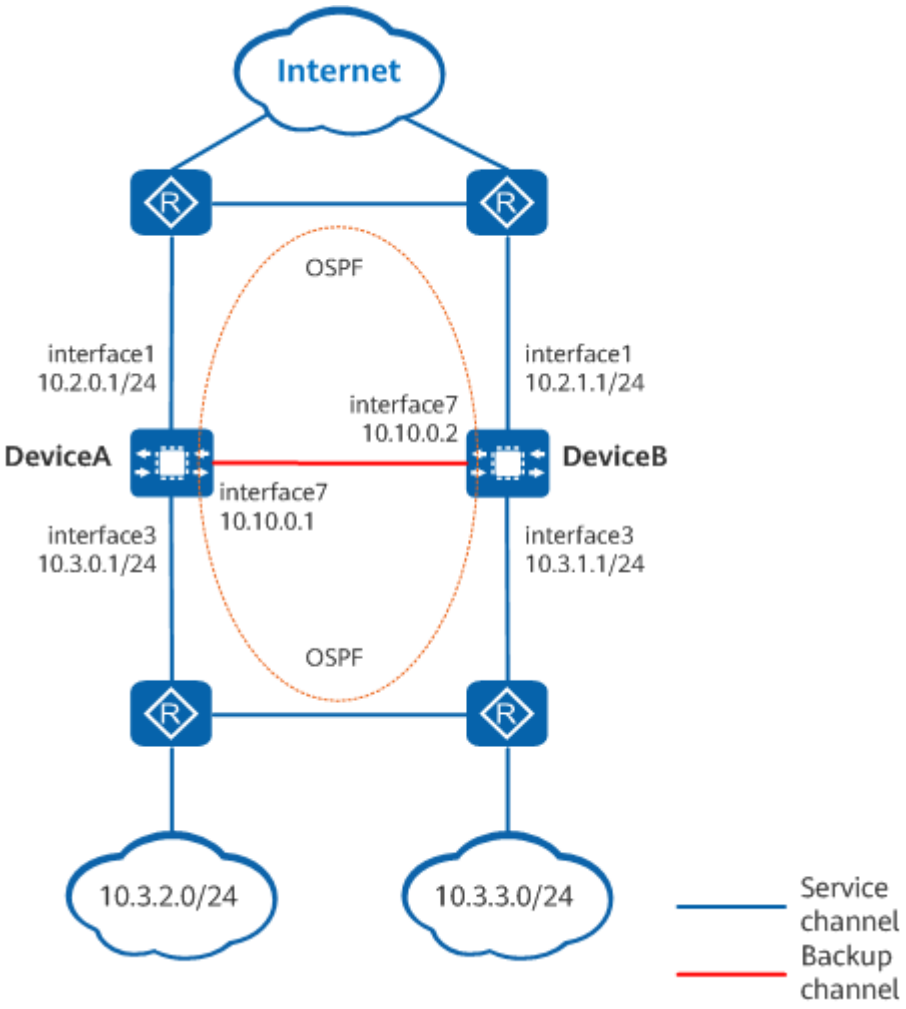
As shown in **Figure 7-10**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers. OSPF runs between the devices and upstream and downstream routers. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-10 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to adjust the OSPF cost values based on device priorities. After this command is run, a device determines whether it is the active or standby device when advertising OSPF routes. If the device is the active one, it directly advertises the routes that it has learned. If it is the standby device, it advertises the routes after increasing the cost values. In this way, when upstream and downstream routers calculate routes, the next hop points to the active device, and packets are forwarded to the active device.	
[DeviceA] **hrp adjust ospf-cost enable**	[DeviceB] **hrp adjust ospf-cost enable**
# Specify the heartbeat interface and device role, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Create a security policy on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow devices and the upstream and downstream routers to exchange OSPF packets.

NOTE

OSPF packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPF packets are controlled by security policies. As such, a security policy must be configured between the security zone where the upstream and downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.3.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
```

Step 5 Configure routers.

 Copyright © Huawei Technologies Co., Ltd.

Configure OSPF on the four routers to advertise routes. For configuration commands, see related documents of the routers.

----End

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA	DeviceB
# sysname **DeviceA** # hrp enable hrp device **active** hrp interface GE0/0/7 remote **10.10.0.2** hrp track interface GE0/0/1 hrp track interface GE0/0/3 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! J6+;U#>V\!_e1NY[iGLXjT %k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!! Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%# # interface GE0/0/1 ip address **10.2.0.1** 255.255.255.0 # interface GE0/0/3 ip address **10.3.0.1** 255.255.255.0 # interface GE0/0/7 ip address **10.10.0.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/3 # firewall zone untrust set priority 5 add interface GE0/0/1 # firewall zone dmz set priority 50 add interface GE0/0/7 # ospf 10 area 0.0.0.0 network **10.2.0.0** 0.0.0.255 network **10.3.0.0** 0.0.0.255 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_ospf_1 source-zone local destination-zone trust destination-zone untrust service ospf action permit rule name policy_ospf_2 source-zone trust source-zone untrust destination-zone local service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 source-address 10.3.3.0 24	# sysname **DeviceB** # hrp enable hrp device **standby** hrp interface GE0/0/7 remote **10.10.0.1** hrp track interface GE0/0/1 hrp track interface GE0/0/3 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! \FR0@B|5m51t2(SLB$(Yzq_KUB\| V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4 t;1e+vR$$U!!!!!%+%# # interface GE0/0/1 ip address **10.2.1.1** 255.255.255.0 # interface GE0/0/3 ip address **10.3.1.1** 255.255.255.0 # interface GE0/0/7 ip address **10.10.0.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/3 # firewall zone untrust set priority 5 add interface GE0/0/1 # firewall zone dmz set priority 50 add interface GE0/0/7 # ospf 10 area 0.0.0.0 network **10.2.1.0** 0.0.0.255 network **10.3.1.0** 0.0.0.255 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_ospf_1 source-zone local destination-zone trust destination-zone untrust service ospf action permit rule name policy_ospf_2 source-zone trust source-zone untrust destination-zone local service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 source-address 10.3.3.0 24

 Copyright © Huawei Technologies Co., Ltd.

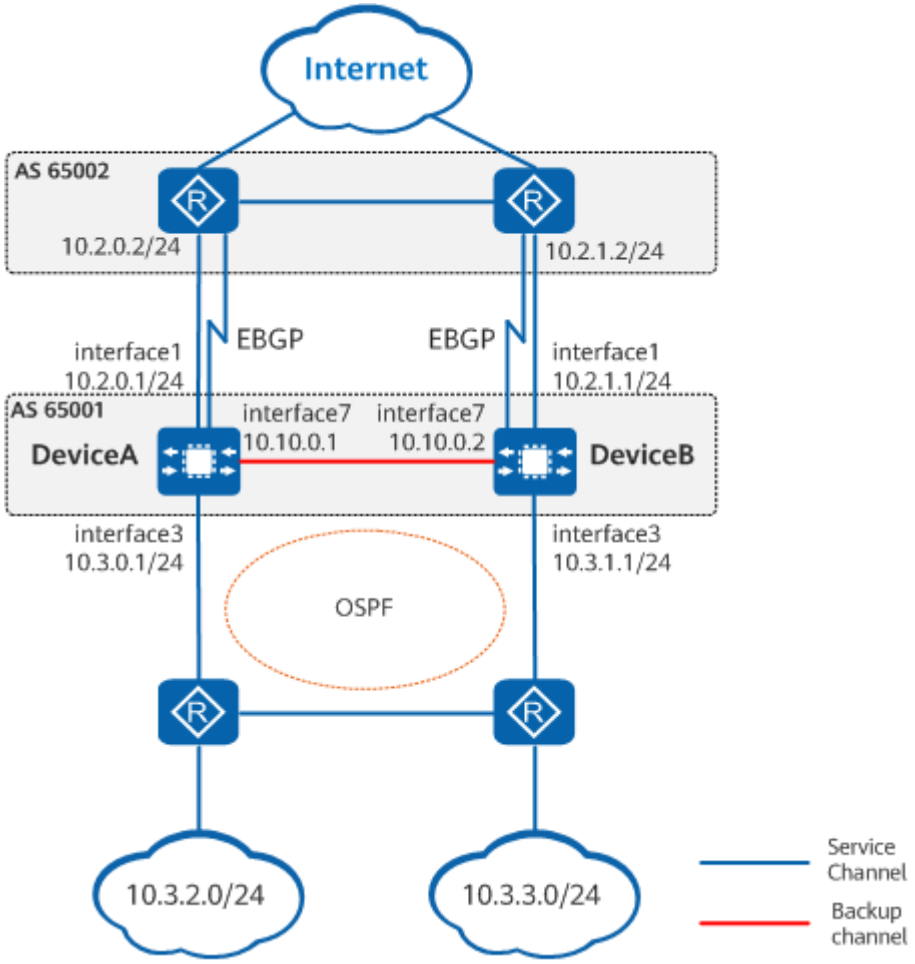
DeviceA	DeviceB
action permit # return	action permit # return

7.1.7 Web: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively

Networking Requirements

On the network shown in **Figure 7-11**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers through EBGP and OSPF respectively. DeviceA and DeviceB are expected to work in active/standby mode. In normal cases, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-11 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream routers



Procedure

Step 1 Set IP addresses for interfaces, and add the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click GE0/0/1, set the following parameters, and then click **OK**.

Security Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to set parameters for GE0/0/3.

Security Zone	trust
IPv4	
IP Address	10.3.0.1/24

   d. Repeat the preceding steps to set parameters for GE0/0/7.

Security Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click GE0/0/1, set parameters, and then click **OK**.

Security Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Repeat the preceding steps to set parameters for GE0/0/3.

Security Zone	trust
IPv4	
IP Address	10.3.1.1/24

   d. Repeat the preceding steps to set parameters for GE0/0/7.

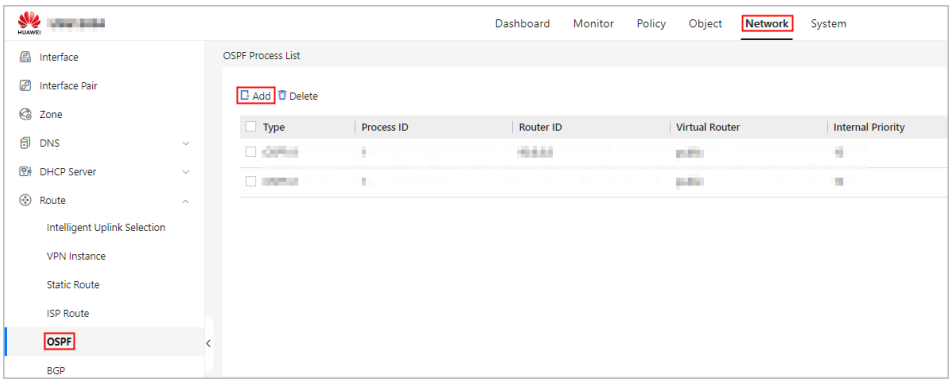
Security Zone	dmz

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF to ensure that the routes to the downstream routers are reachable.

1. Configure OSPF on DeviceA.
   a. Choose **Network** > **Route** > **OSPF**, and click **Add**.



   b. Set the following parameters for OSPF, and then click **OK**.

Type	OSPFv2
Process ID	10

   c. Click and choose **Area Settings**. In **Area List**, click **Add**, set the following parameters to create an area, and then click **OK**.

Area	0.0.0.0
Network Segment IP Address	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

   d. Click and choose **Route Import**. In **Route List**, click **Add**, set the type of the imported route to BGP, and then click **OK**.
2. Configure OSPF on DeviceB.
   a. Choose **Network** > **Route** > **OSPF**, click **Add**, set the following parameter for OSPF, and then click **OK**.

Type	OSPFv2
Process ID	10

   b. Click and choose **Area Settings**. In **Area List**, click **Add**, set the following parameters to create an area, and then click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

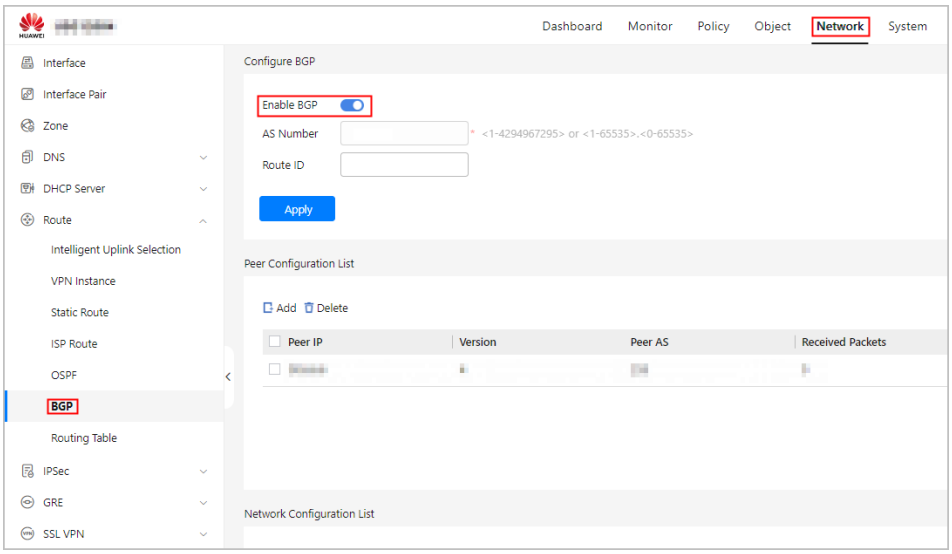
Zone	0.0.0.0
Network Segment IP Address	10.3.1.0
Mask/Wildcard Mask	255.255.255.0

c. Click and choose **Route Import**. In **Route List**, click **Add**, set the type of the imported route to BGP, and then click **OK**.

Step 3 Configure EBGP to ensure that the routes to the upstream routers are reachable. Assume that DeviceA and DeviceB belong to AS 65001 and that the upstream routers belong to AS 65002.

1. Configure EBGP on DeviceA.

a. Choose **Network** > **Route** > **BGP**, and click **Enable BGP**.



b. Set BGP **AS Number** to 65001 and **Route ID** to 10.2.0.1.

c. In **Peer Configuration List**, click **Add**, set the following parameters to add a peer relationship, and then click **OK**.

Peer IP	10.2.0.2
Peer AS	65002
Maximum EBGP Connection Hops	2

d. In **Network Configuration List**, click **Add**, enter the IP address and mask (10.2.0.1/24) of the route to be added to the BGP routing table, and then click **OK**.

e. In **Route List**, click **Add**, set the following parameters to import routes, and then click **OK**.

Protocol Type	OSPF

 Copyright © Huawei Technologies Co., Ltd.

Process ID	10

2. Configure EBGP on DeviceB.
   a. Choose **Network** > **Route** > **BGP**, and click **Enable BGP**.
   b. Set BGP **AS Number** to 65001 and **Route ID** to 10.2.1.1.
   c. In **Peer Configuration List**, click **Add**, set the following parameters to add a peer relationship, and then click **OK**.

Peer IP	10.2.1.2
Peer AS	65002
Maximum EBGP Connection Hops	2

   d. In **Network Configuration List**, click **Add**, enter the IP address and mask 10.2.1.1/24 of the route to be added to the BGP routing table, and then click **OK**.
   e. In **Route List**, click **Add**, set the following parameters to import routes, and then click **OK**.

Protocol Type	OSPF
Process ID	10

Step 4 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

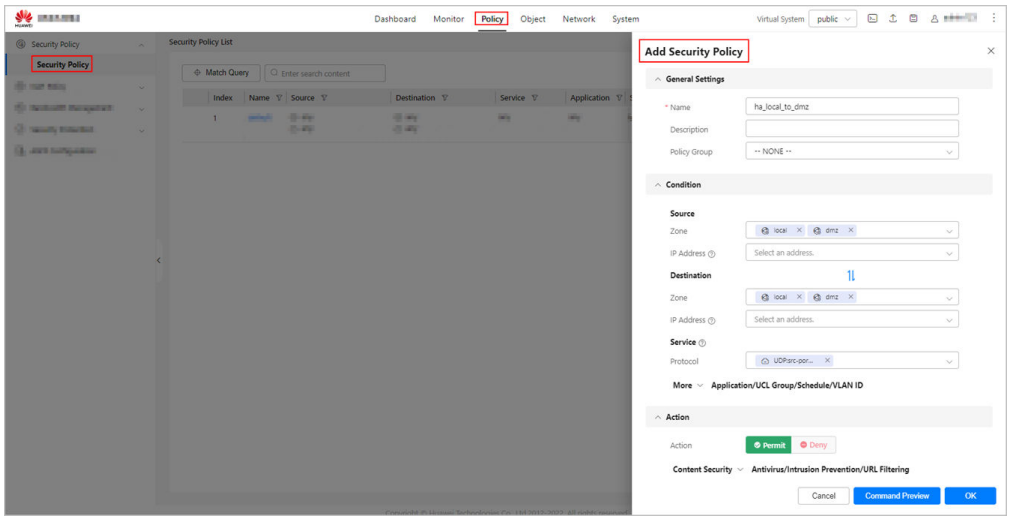
NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

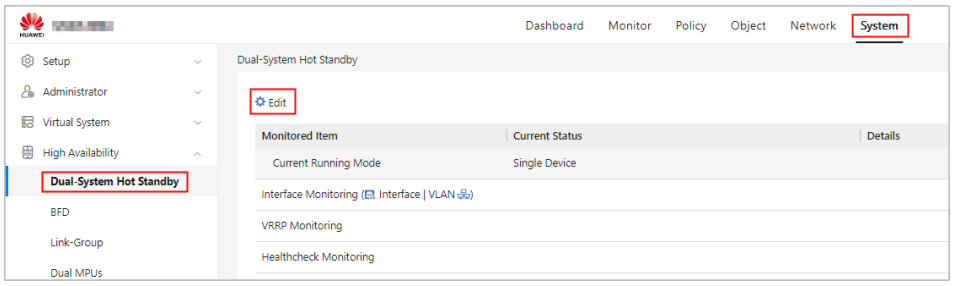
 Copyright © Huawei Technologies Co., Ltd.



Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

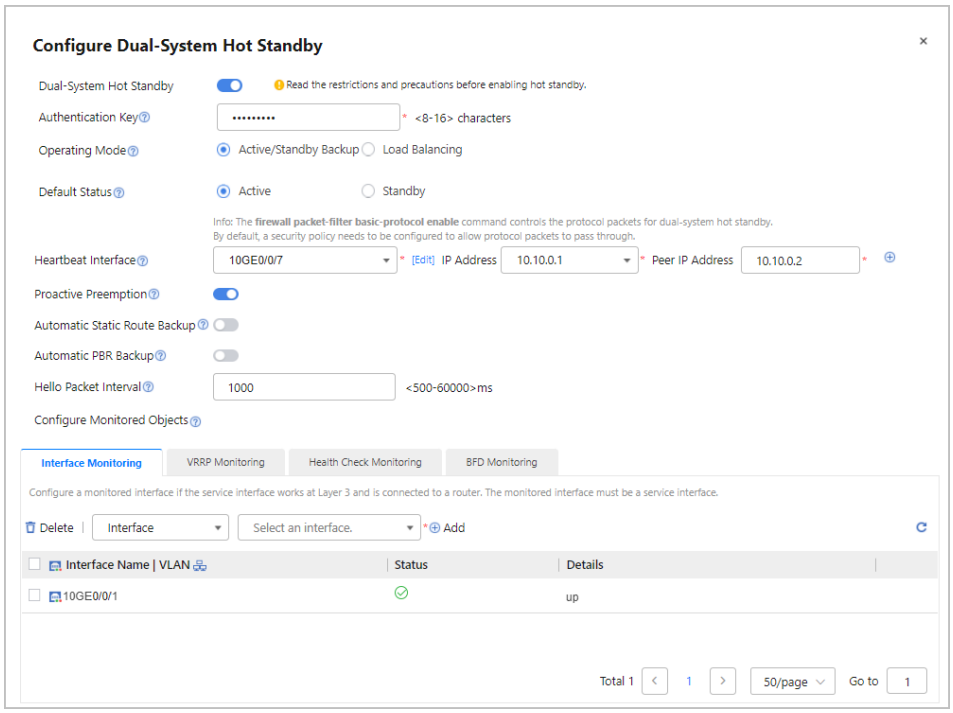
Step 5 Configure hot standby.

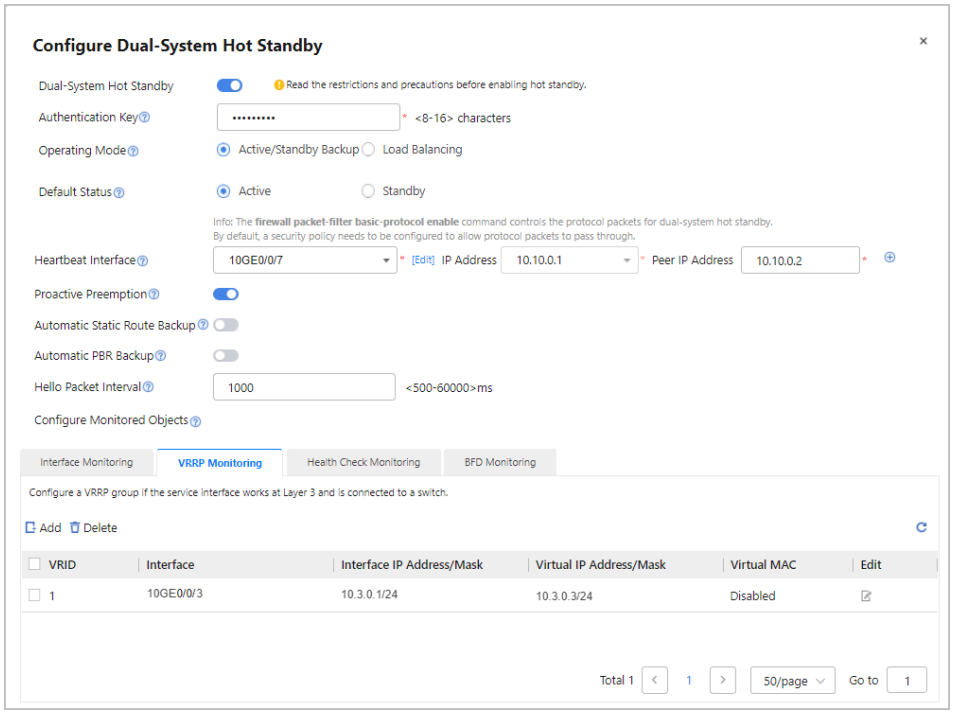
1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.



   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

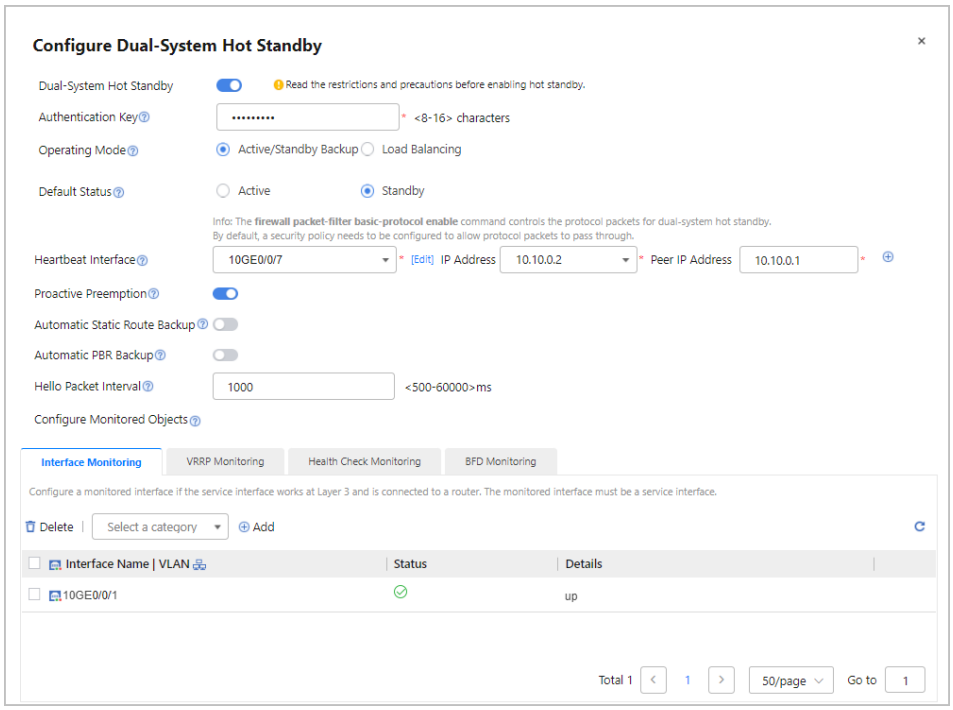
 Copyright © Huawei Technologies Co., Ltd.

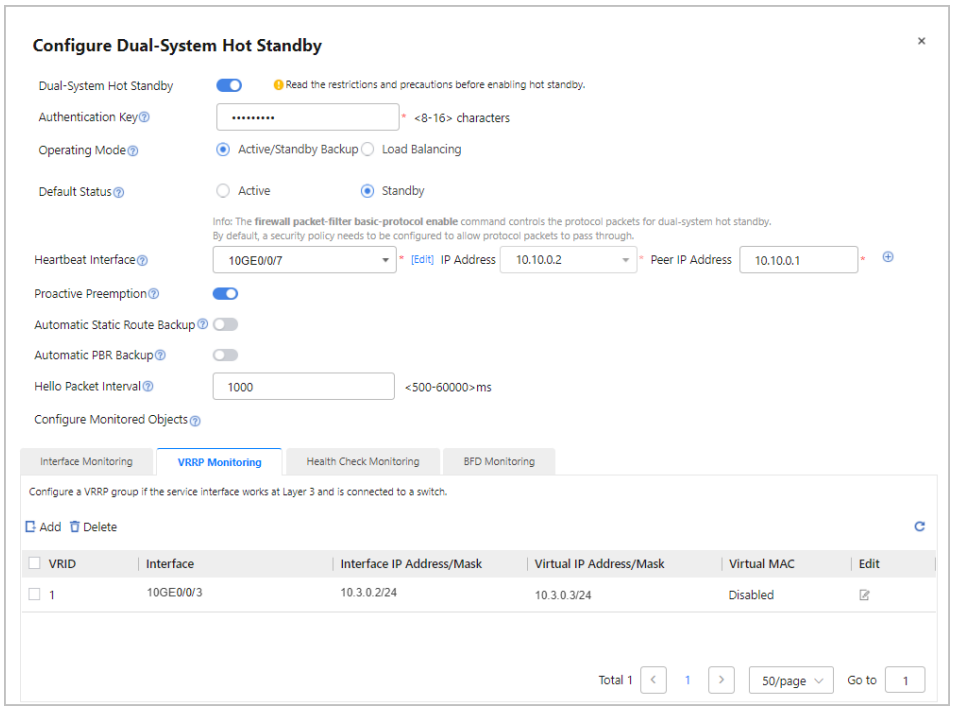




2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.





Step 6 Configure a security policy.

After the dual-system hot standby relationship is established, the security policies configured on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy List**.
2. Click **Add Security Policy**, set the following security policy parameters, and then click **OK**.

   # Configure security policies to allow the device to exchange OSPF packets with the downstream router and BGP messages with the upstream router.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Controlling function of security policies for BGP and OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command is enabled. That is, BGP and OSPF packets are controlled by security policies. In this case, a security policy must be configured between the local zone and the security zone where the outbound interface resides to allow BGP and OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_ospf_1
Source Zone	local
Destination Zone	trust
Destination Address	10.3.0.0/24,10.3.1.0/24
Service	ospf
Action	Permit

Name	policy_ospf_2
Source Zone	trust
Destination Zone	local
Source Address	10.3.0.0/24,10.3.1.0/24
Service	ospf
Action	Permit

Name	policy_bgp_1
Source Zone	local
Destination Zone	untrust
Destination Address	10.2.0.2/24,10.2.1.2/24
Service	bgp
Action	Permit

Name	policy_bgp_2
Source Zone	untrust
Destination Zone	local

 Copyright © Huawei Technologies Co., Ltd.

Source Address	10.2.0.2/24,10.2.1.2/24
Service	bgp
Action	Permit

Configure a security policy to allow intranet users to access the external network.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.0/24,10.3.3.0/24
Action	Permit

Step 7 Configure routers.

Configure OSPF on the downstream routers and BGP on the upstream routers to advertise neighboring network segments. For configuration commands, refer to the related router documents.

----End

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the dual-system hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.0.0 0.0.0.255
#
bgp 65001
 router-id 10.2.0.1
 peer 10.2.0.2 as-number 65002
 peer 10.2.0.2 ebgp-max-hop 2
 #
 ipv4-family unicast
  network 10.2.0.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
#
bgp 65001
 router-id 10.2.1.1
 peer 10.2.1.2 as-number 65002
 peer 10.2.1.2 ebgp-max-hop 2
 #
 ipv4-family unicast
  network 10.2.1.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-zone trust destination-zone local source-address 10.3.0.0 mask 255.255.255.0 source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 mask 255.255.255.0 destination-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 mask 255.255.255.0 source-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit #	source-zone trust destination-zone local source-address 10.3.0.0 mask 255.255.255.0 source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 mask 255.255.255.0 destination-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 mask 255.255.255.0 source-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit #

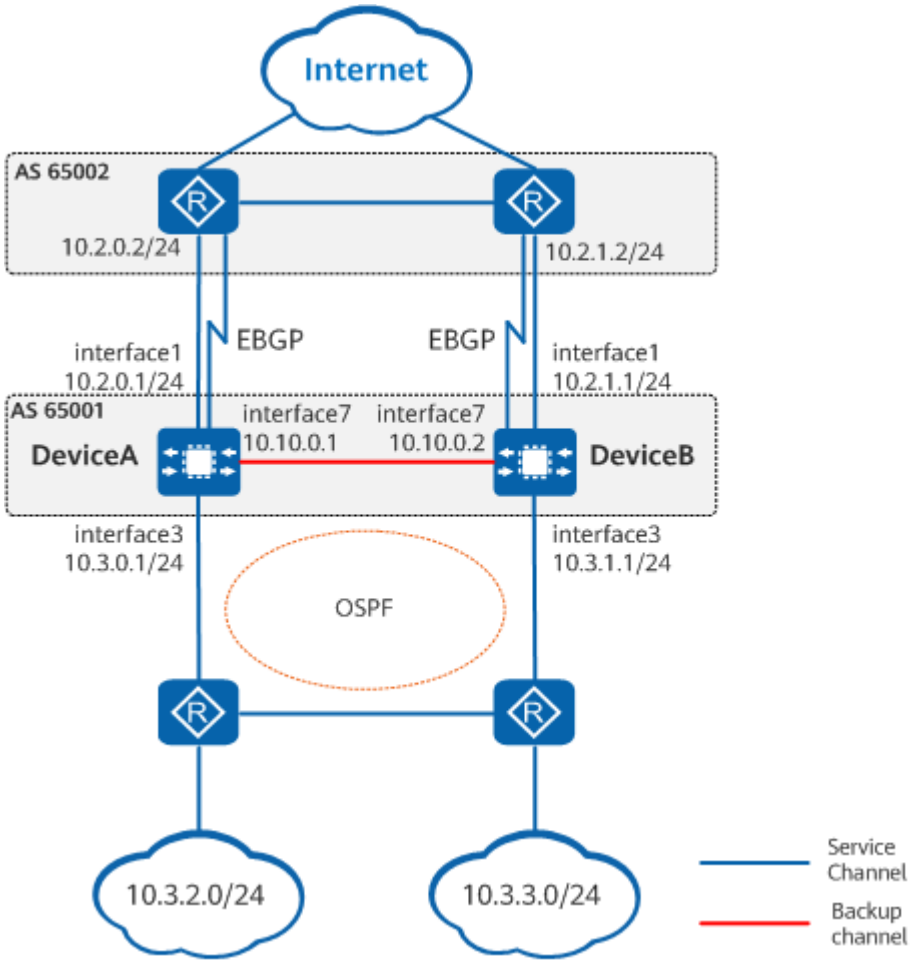
7.1.8 CLI: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively

Networking Requirements

On the network shown in **Figure 7-12**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers through EBGP and OSPF respectively. DeviceA and DeviceB are expected to work in active/standby mode. In normal cases, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-12 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream routers



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set an IP address for each interface on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Add the interfaces on DeviceA and DeviceB to security zones.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF on DeviceA and DeviceB and establish neighbor relationships with the downstream routers to ensure route reachability.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **import-route bgp** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceA-ospf-10] **import-route bgp** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**
# Configure EBGP on DeviceA and DeviceB to establish EBGP peer relationships with the upstream routers. Assume that DeviceA and DeviceB belong to AS 65001 and that the upstream routers belong to AS 65002.	
[DeviceA] **bgp 65001** [DeviceA-bgp] **router-id 10.2.0.1** [DeviceA-bgp] **peer 10.2.0.2 as-number 65002** [DeviceA-bgp] **peer 10.2.0.2 ebgp-max-hop 2** [DeviceA-bgp] **ipv4-family unicast** [DeviceA-bgp-af-ipv4] **network 10.2.0.1 24** [DeviceA-bgp-af-ipv4] **import-route ospf 10** [DeviceA-bgp-af-ipv4] **quit** [DeviceA-bgp] **quit**	[DeviceB] **bgp 65001** [DeviceB-bgp] **router-id 10.2.1.1** [DeviceB-bgp] **peer 10.2.1.2 as-number 65002** [DeviceB-bgp] **peer 10.2.1.2 ebgp-max-hop 2** [DeviceB-bgp] **ipv4-family unicast** [DeviceB-bgp-af-ipv4] **network 10.2.1.1 24** [DeviceA-bgp-af-ipv4] **import-route ospf 10** [DeviceB-bgp-af-ipv4] **quit** [DeviceB-bgp] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure dual-system hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# Configure DeviceA and DeviceB to adjust OSPF and BGP cost values based on the device role. After this command is run, a device determines whether it is the active or standby device when advertising OSPF or BGP routes. If the device is the active one, it directly advertises the routes that it has learned. If it is the standby device, it increases the cost values before advertising the routes. In this way, the next hop of the routes calculated by the upstream and downstream routers is the active device, and packets are forwarded to this device.	
[DeviceA] **hrp adjust ospf-cost enable** [DeviceA] **hrp adjust bgp-cost enable**	[DeviceB] **hrp adjust ospf-cost enable** [DeviceB] **hrp adjust bgp-cost enable**
# Specify the heartbeat interface and device role, configure the authentication key, and enable dual-system hot standby on DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Configure security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow the device to exchange OSPF packets with the downstream router and BGP messages with the upstream router.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> Controlling function of security policies for BGP and OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command is enabled. That is, BGP and OSPF packets are controlled by security policies. In this case, a security policy must be configured between the local zone and the security zone where the outbound interface resides to allow BGP and OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
HRP_M[DeviceA-policy-security] rule name policy_bgp_1
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] destination-address 10.2.0.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] destination-address 10.2.1.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] service bgp
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] quit
HRP_M[DeviceA-policy-security] rule name policy_bgp_2
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] source-address 10.2.0.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] source-address 10.2.1.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] service bgp
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.3.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers.

Configure OSPF on the downstream routers and BGP on the upstream routers to advertise neighboring network segments. For configuration commands, refer to the related router documents.

----End

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the dual-system hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.0.0 0.0.0.255
#
bgp 65001
 router-id 10.2.0.1
 peer 10.2.0.2 as-number 65002
 peer 10.2.0.2 ebgp-max-hop 2
 #
 ipv4-family unicast
  network 10.2.0.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
#
bgp 65001
 router-id 10.2.1.1
 peer 10.2.1.2 as-number 65002
 peer 10.2.1.2 ebgp-max-hop 2
 #
 ipv4-family unicast
  network 10.2.1.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-zone trust destination-zone local source-address 10.3.0.0 mask 255.255.255.0 source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 mask 255.255.255.0 destination-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 mask 255.255.255.0 source-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit #	source-zone trust destination-zone local source-address 10.3.0.0 mask 255.255.255.0 source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 mask 255.255.255.0 destination-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 mask 255.255.255.0 source-address 10.2.1.2 mask 255.255.255.0 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit #

7.1.9 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction

Networking Requirements

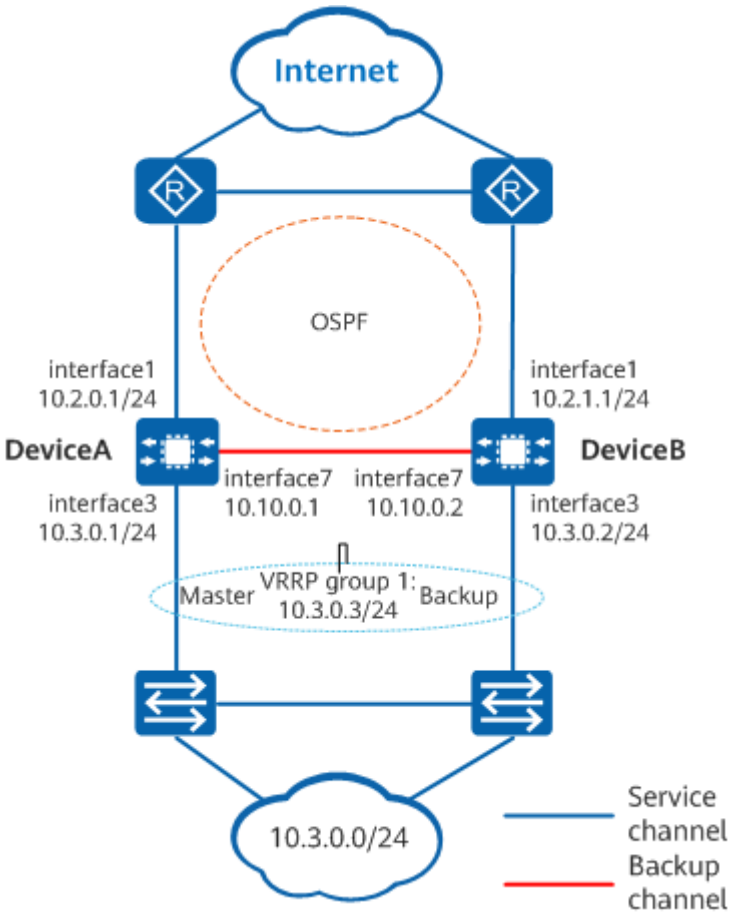
As shown in **Figure 7-13**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream routers and downstream Layer 2 switches. OSPF runs between the devices and upstream routers. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-13 Active/standby networking where service interfaces work at Layer 3 and connect to upstream routers and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

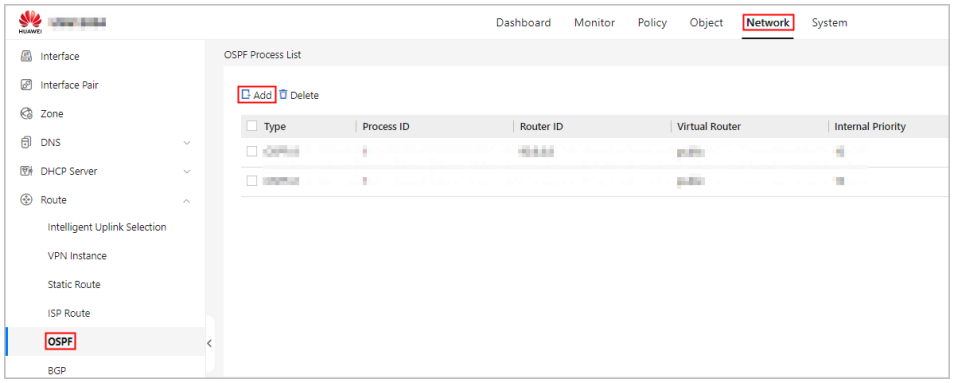
Zone	trust
IPv4	
IP Address	10.3.0.2/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF to ensure IP connectivity.

1. Configure OSPF on DeviceA.
   a. Choose **Network** > **Route** > **OSPF**.



   b. Click **Add**, set the parameters as follows to create an OSPF process, and click **OK**.

Type	OSPFv2
Process ID	10

c. Click , click **Add**, set the parameters as follows to create an OSPF area, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.0.0
Mask/Wildcard Mask	255.255.255.0

d. Choose **Basic Configuration** > **Network Settings**, click **Add**, set the parameters as follows to create a network, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

2. Configure OSPF on DeviceB.

a. Choose **Network** > **Route** > **OSPF**.

b. Click **Add**, set the parameters as follows to create an OSPF process, and click **OK**.

Type	OSPFv2
Process ID	10

c. Click , click **Add**, set the parameters as follows to create an OSPF area, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.1.0
Mask/Wildcard Mask	255.255.255.0

d. Choose **Basic Configuration** > **Network Settings**, click **Add**, set the parameters as follows to create a network, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.0.0

 Copyright © Huawei Technologies Co., Ltd.

Mask/Wildcard Mask	255.255.255.0

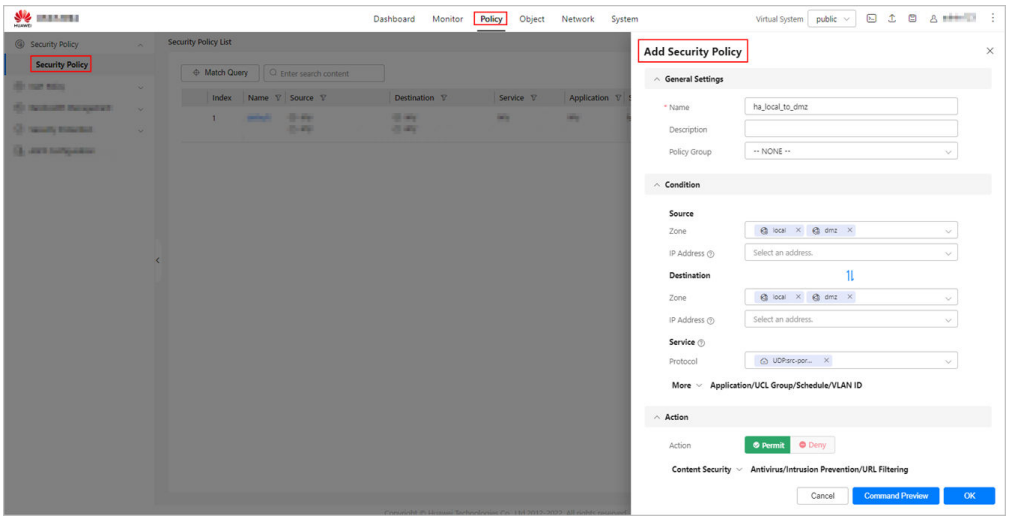
Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

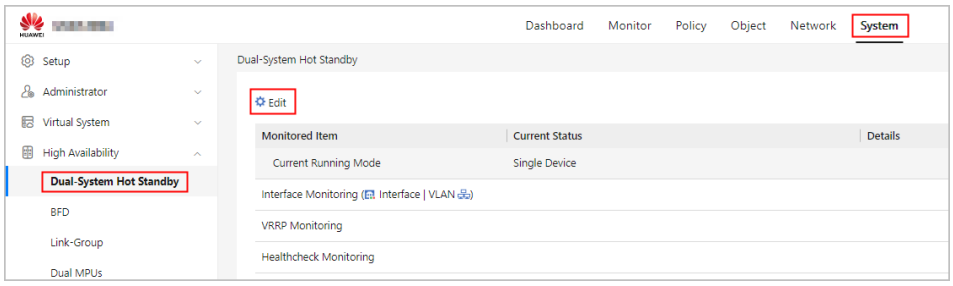


Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

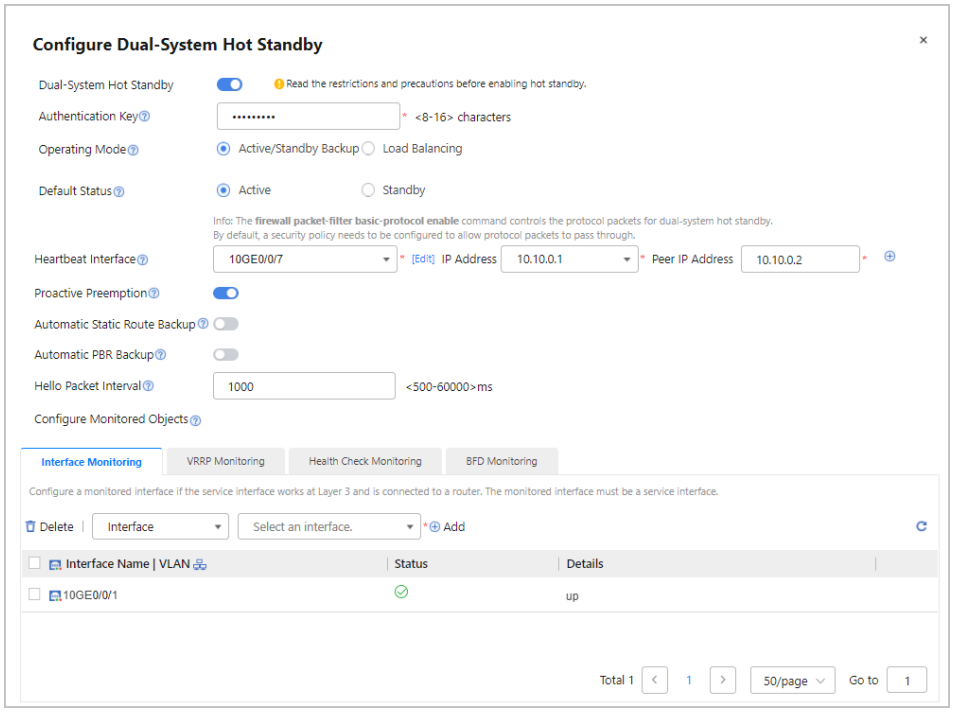
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

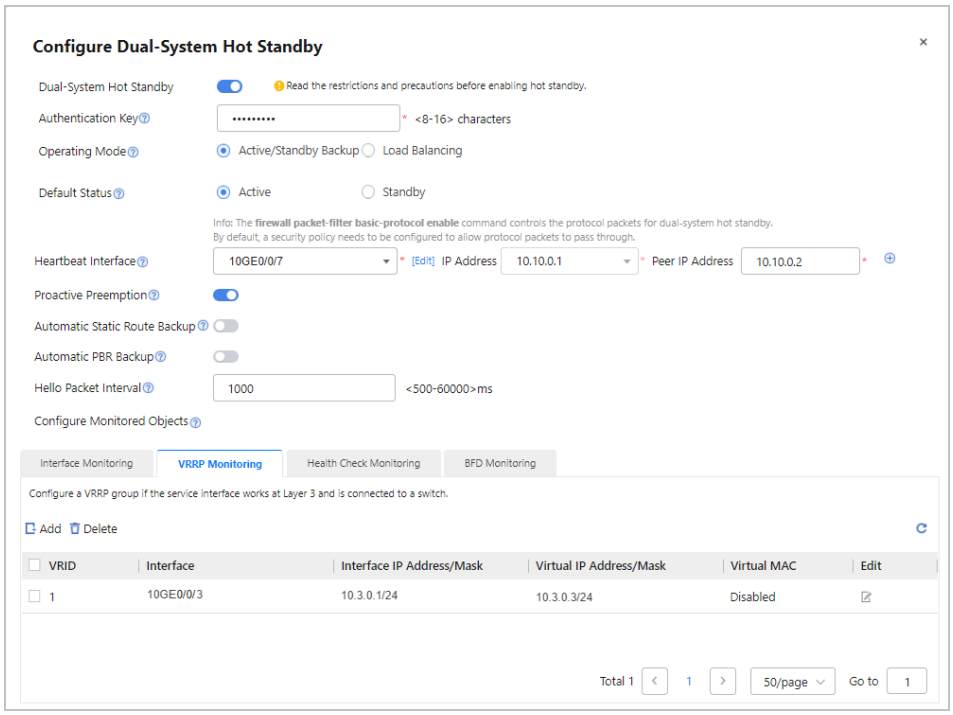
 Copyright © Huawei Technologies Co., Ltd.



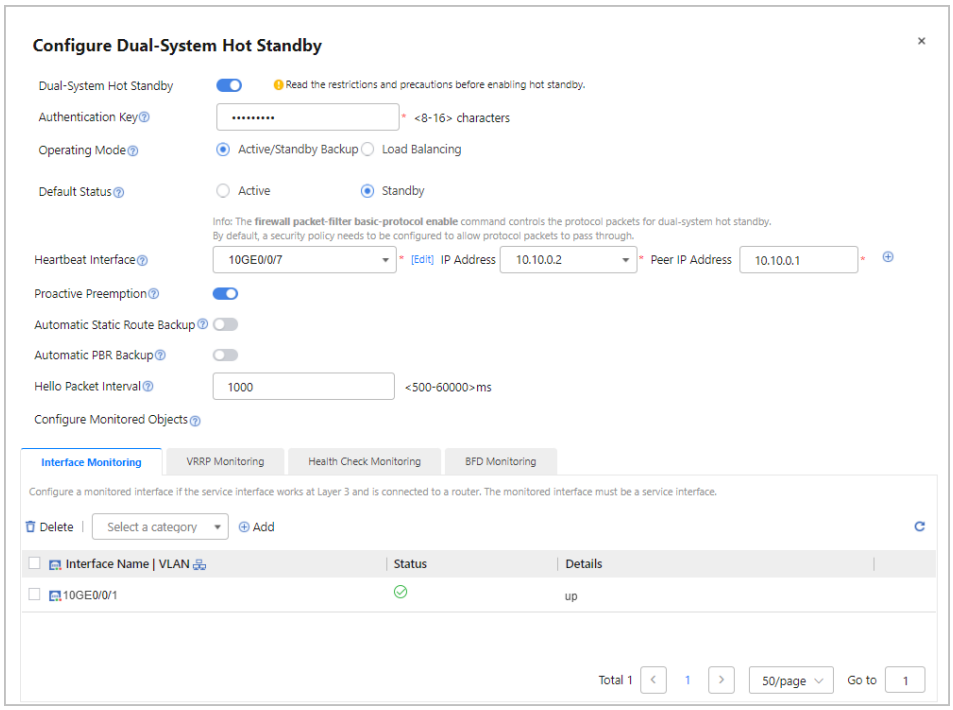
b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



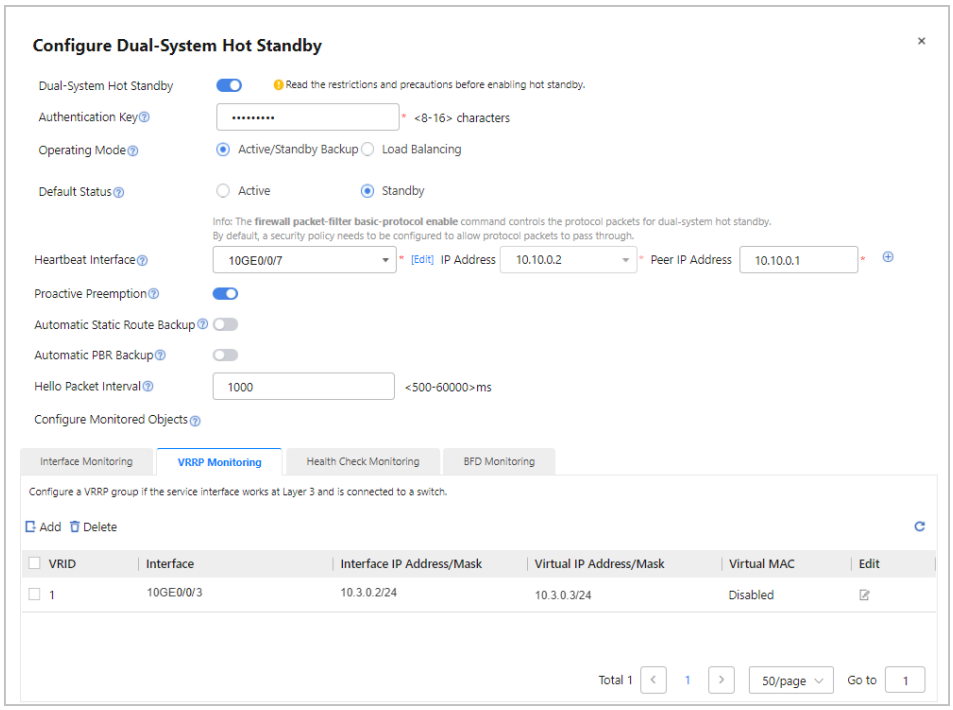
 Copyright © Huawei Technologies Co., Ltd.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



 Copyright © Huawei Technologies Co., Ltd.



Step 5 Configure the security policies.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure security policies and set the parameters as follows, and then click **OK**.

   # Configure a security policy to allow intranet users to access the Internet.

Name	policy_sec1
Source Zone	trust
Destination Zone	untrust
Service	10.3.0.0/24
Action	Permit

   # Configure a security policy to allow DeviceA and the upstream router (in the untrust zone) to exchange OSPF packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Controlling function of security policies for OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, OSPF packets are controlled by security policies. In this case, a security policy must be configured between the security zones where the upstream/downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_sec2
Source Zone	local,untrust
Destination Zone	local,untrust
Service	ospf
Action	Permit

Step 6 Configure the switches and PCs.

1. Add the three interfaces of the switches to the same VLANs accordingly. For configuration commands, refer to related documents of the switches.
2. Configure the default route whose next hop is the virtual IP address (10.3.0.3) of VRRP group 1 on the intranet device.

Step 7 Configure the routers.

Configure OSPF on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
  vrrp vrid 1 virtual-ip 10.3.0.3 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.10 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction

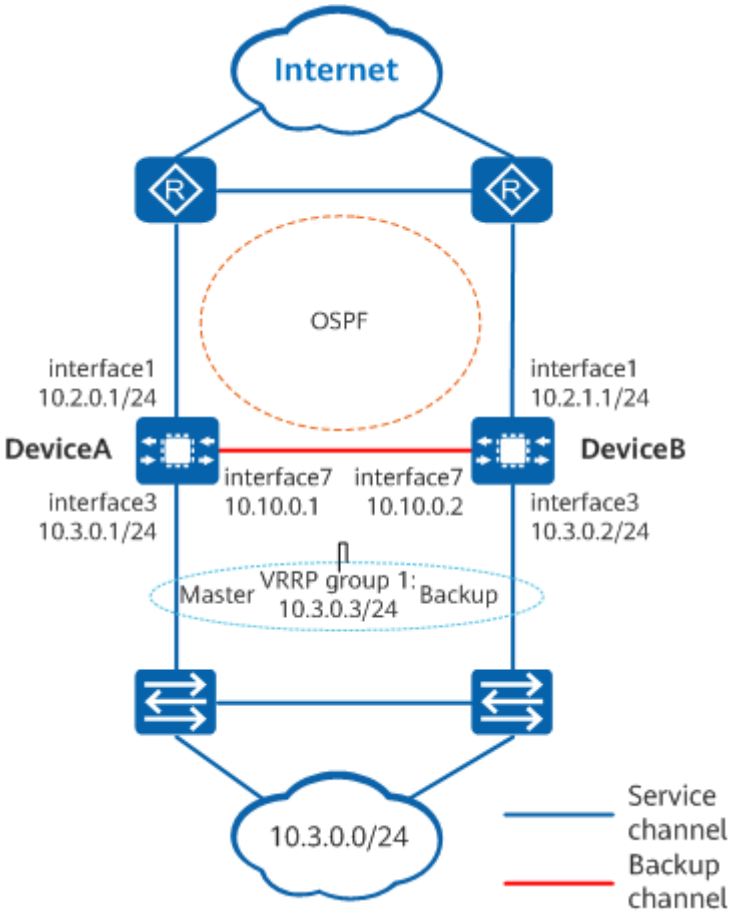
Networking Requirements

As shown in **Figure 7-14**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream routers and downstream Layer 2 switches. OSPF runs between the devices and upstream routers. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-14 Active/standby networking where service interfaces work at Layer 3 and connect to upstream routers and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



Procedure

Step 1 Complete basic network configurations.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

In this example, because DeviceA and DeviceB connect to upstream routers and downstream switches, you need to configure DeviceA and DeviceB to monitor the upstream interfaces and configure VRRP groups on downstream interfaces.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1**	[DeviceB] **hrp track interface ge 0/0/1**
# Configure VRRP group 1 on DeviceA's downstream service interface GE 0/0/3 and set its state to active. Configure VRRP group 1 on downstream service interface GE 0/0/3 of DeviceB and specify **standby** in the **vrrp vrid virtual-ip** command for the VRRP group.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 1 virtual-ip 10.3.0.3 active** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 1 virtual-ip 10.3.0.3 standby** [DeviceB-GE0/0/3] **quit**
# Configure DeviceA and DeviceB to adjust the OSPF cost values based on device priorities.	
[DeviceA] **hrp adjust ospf-cost enable**	[DeviceB] **hrp adjust ospf-cost enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Create a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec1
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec1] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec1] quit
```

Configure a security policy to allow DeviceA and the upstream router (in the untrust zone) to exchange OSPF packets.

NOTE

OSPF packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPF packets are controlled by security policies. As such, a security policy must be configured between the untrust zone where the upstream service interface resides and the local zone to allow OSPF packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA-policy-security] rule name policy_sec2
HRP_M[DeviceA-policy-security-rule-policy_sec2] source-zone local untrust
HRP_M[DeviceA-policy-security-rule-policy_sec2] destination-zone local untrust
HRP_M[DeviceA-policy-security-rule-policy_sec2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_sec2] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec2] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers and switches.

Configure OSPF on the routers to advertise routes. For configuration commands, see related documents of the routers.

Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.

----End

Verifying the Configuration

1. Run the **display vrrp** command on DeviceA and DeviceB to check the status of interfaces in the VRRP group.
2. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
  vrrp vrid 1 virtual-ip 10.3.0.3 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.11 Web: Example for Connecting Devices to Switches Transparently in Upstream and Downstream Directions

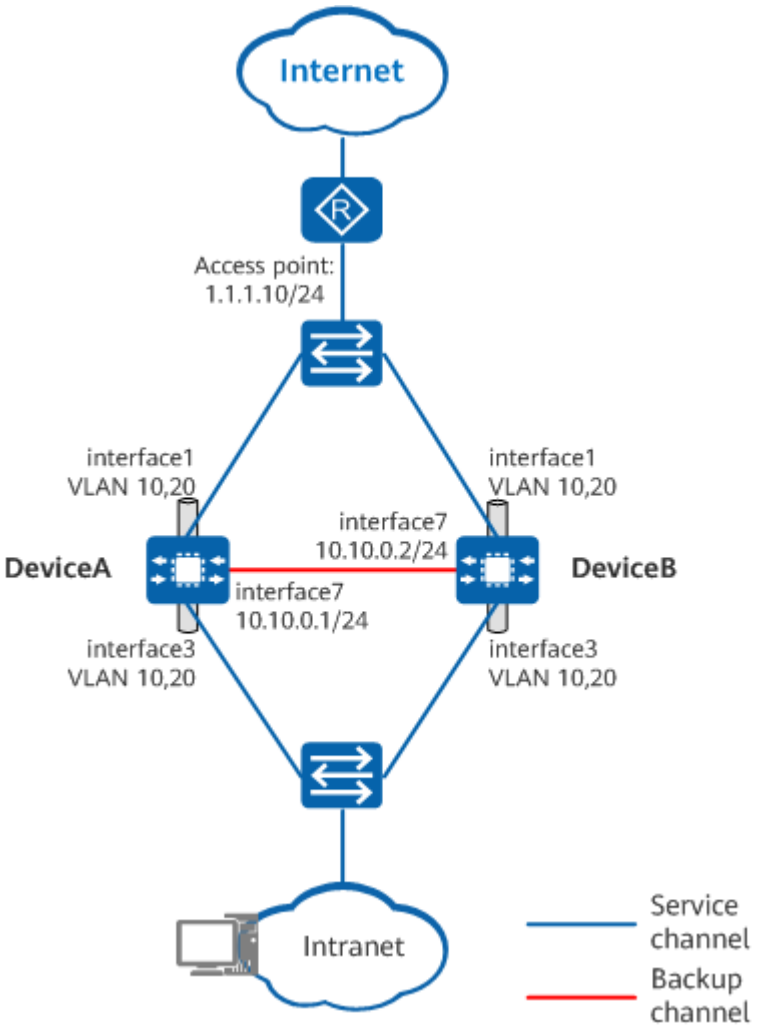
Networking Requirements

On the network shown in **Figure 7-15**, the upstream and downstream service interfaces of DeviceA and DeviceB work at Layer 2 and are connected to switches. The service interfaces of each device are added to VLAN 10 and VLAN 20. It is required that DeviceA and DeviceB work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-15 Active/standby networking where service interfaces work at Layer 2 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure interfaces and basic network configurations.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
Mode	Switching
Connection Type	Trunk
Trunk VLAN ID	10,20

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
Mode	Switching
Connection Type	Trunk
Trunk VLAN ID	10,20

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
Mode	Switching
Connection Type	Trunk
Trunk VLAN ID	10,20

   c. Repeat the preceding steps to configure GE0/0/3.

Zone	trust
Mode	Switching
Connection Type	Trunk

 Copyright © Huawei Technologies Co., Ltd.

Trunk VLAN ID	10,20

d. Repeat the preceding steps to configure GE0/0/7.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

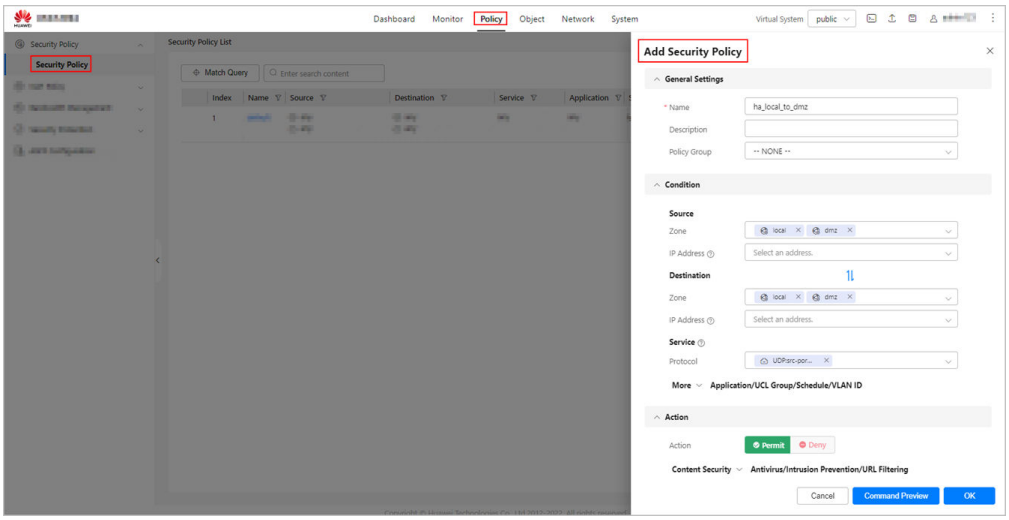
Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.



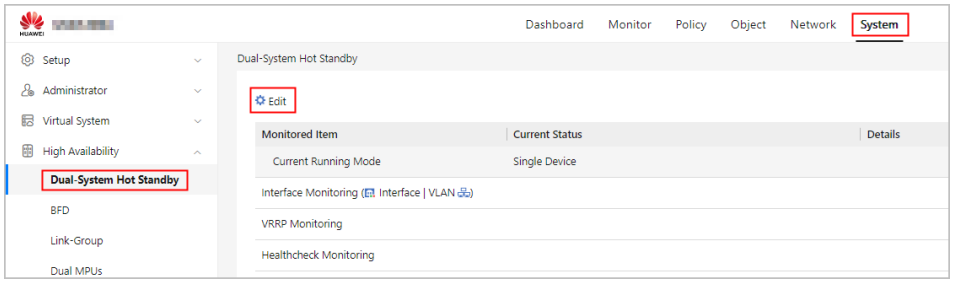
Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514

 Copyright © Huawei Technologies Co., Ltd.

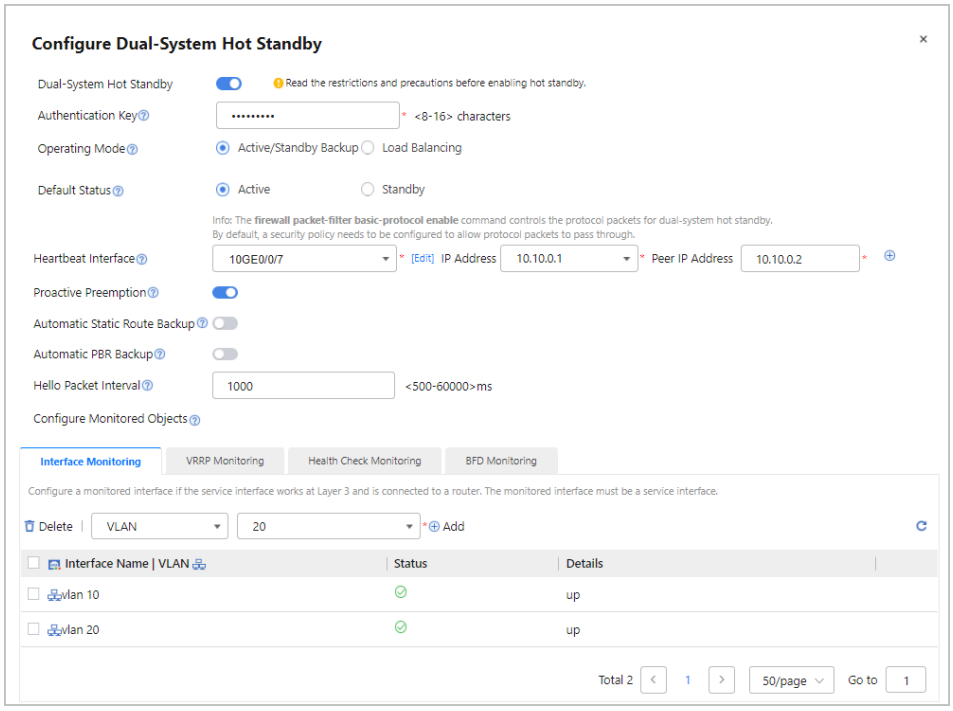
Action	Permit

Step 3 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

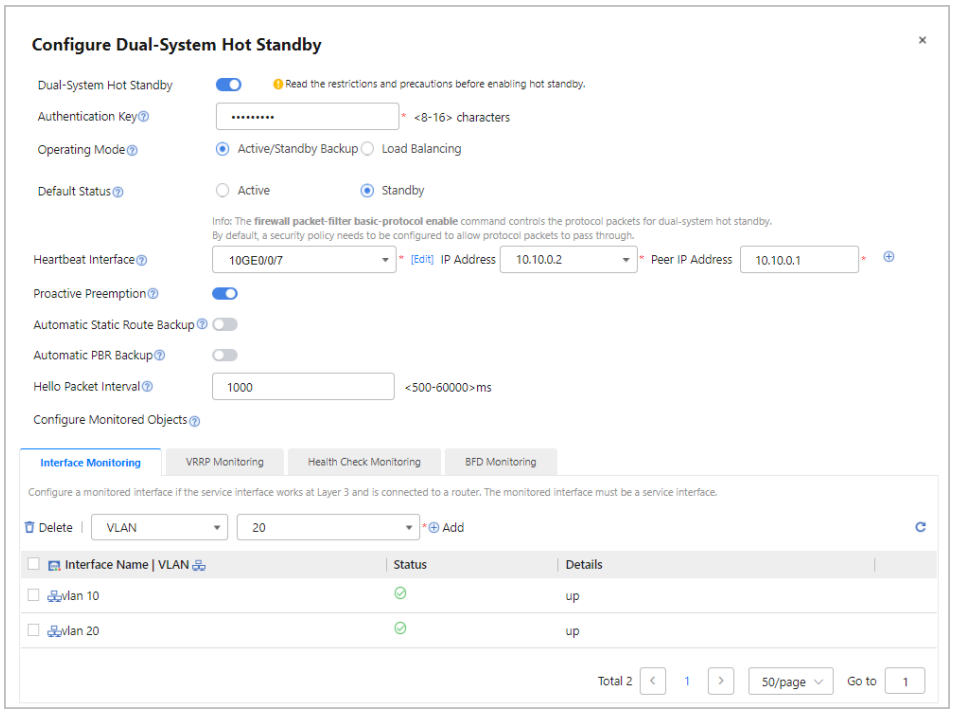


   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure a security policy.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, set the parameters as follows, and click **OK**.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Action	Permit

Step 5 Configure the switches.

Add the three interfaces of the switches to the same VLANs accordingly. For configuration commands, refer to related documents of the switches.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
vlan batch 10 20
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track vlan 10
hrp track vlan 20
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/3
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 10 20
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track vlan 10
hrp track vlan 20
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/3
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

7.1.12 CLI: Example for Connecting Devices to Switches Transparently in Upstream and Downstream Directions

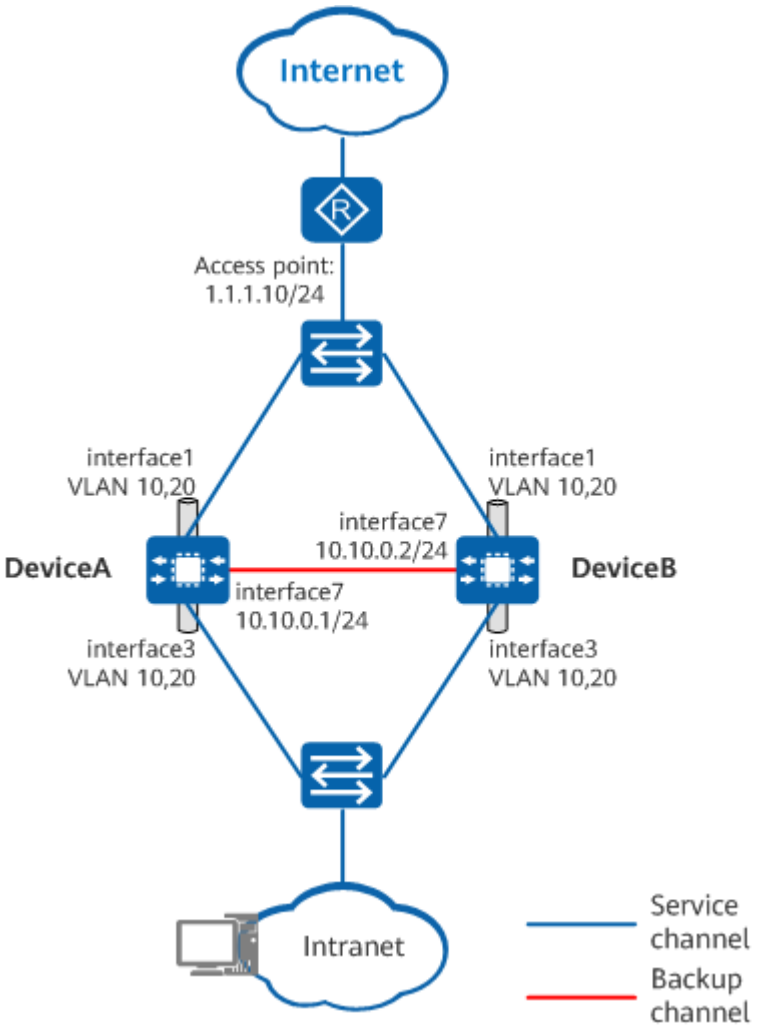
Networking Requirements

On the network shown in **Figure 7-16**, the upstream and downstream service interfaces of DeviceA and DeviceB work at Layer 2 and are connected to switches. The service interfaces of each device are added to VLAN 10 and VLAN 20. It is required that DeviceA and DeviceB work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-16 Active/standby networking where service interfaces work at Layer 2 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# On DeviceA, change the mode of upstream and downstream service interfaces to Layer 2 and add them to VLAN 10 and VLAN 20. On DeviceB, change the mode of upstream and downstream service interfaces to Layer 2 and add them to VLAN 10 and VLAN 20.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vlan batch 10 20** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **portswitch** [DeviceA-GE0/0/1] **port link-type trunk** [DeviceA-GE0/0/1] **port trunk allow-pass vlan 10 20** [DeviceA-GE0/0/1] **undo port trunk allow-pass vlan 1** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **portswitch** [DeviceA-GE0/0/3] **port link-type trunk** [DeviceA-GE0/0/3] **port trunk allow-pass vlan 10 20** [DeviceA-GE0/0/3] **undo port trunk allow-pass vlan 1** [DeviceA-GE0/0/3] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vlan batch 10 20** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **portswitch** [DeviceB-GE0/0/1] **port link-type trunk** [DeviceB-GE0/0/1] **port trunk allow-pass vlan 10 20** [DeviceB-GE0/0/1] **undo port trunk allow-pass vlan 1** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **portswitch** [DeviceB-GE0/0/3] **port link-type trunk** [DeviceB-GE0/0/3] **port trunk allow-pass vlan 10 20** [DeviceB-GE0/0/3] **undo port trunk allow-pass vlan 1** [DeviceB-GE0/0/3] **quit**
# Set an IP address for the heartbeat interface on each of DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor the VLAN status.	
[DeviceA] **hrp track vlan 10** [DeviceA] **hrp track vlan 20**	[DeviceB] **hrp track vlan 10** [DeviceB] **hrp track vlan 20**
# Specify the heartbeat interface and device role, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Configure a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec1
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec1] action permit
```

Step 5 Configure switches.

Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.

----End

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
vlan batch 10 20
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track vlan 10
hrp track vlan 20
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/3
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 10 20
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track vlan 10
hrp track vlan 20
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/3
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20
 undo port trunk allow-pass vlan 1
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
```

7.2 Configuring Hot Standby in Load Sharing Mode

 Copyright © Huawei Technologies Co., Ltd.

7.2.1 Web: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions

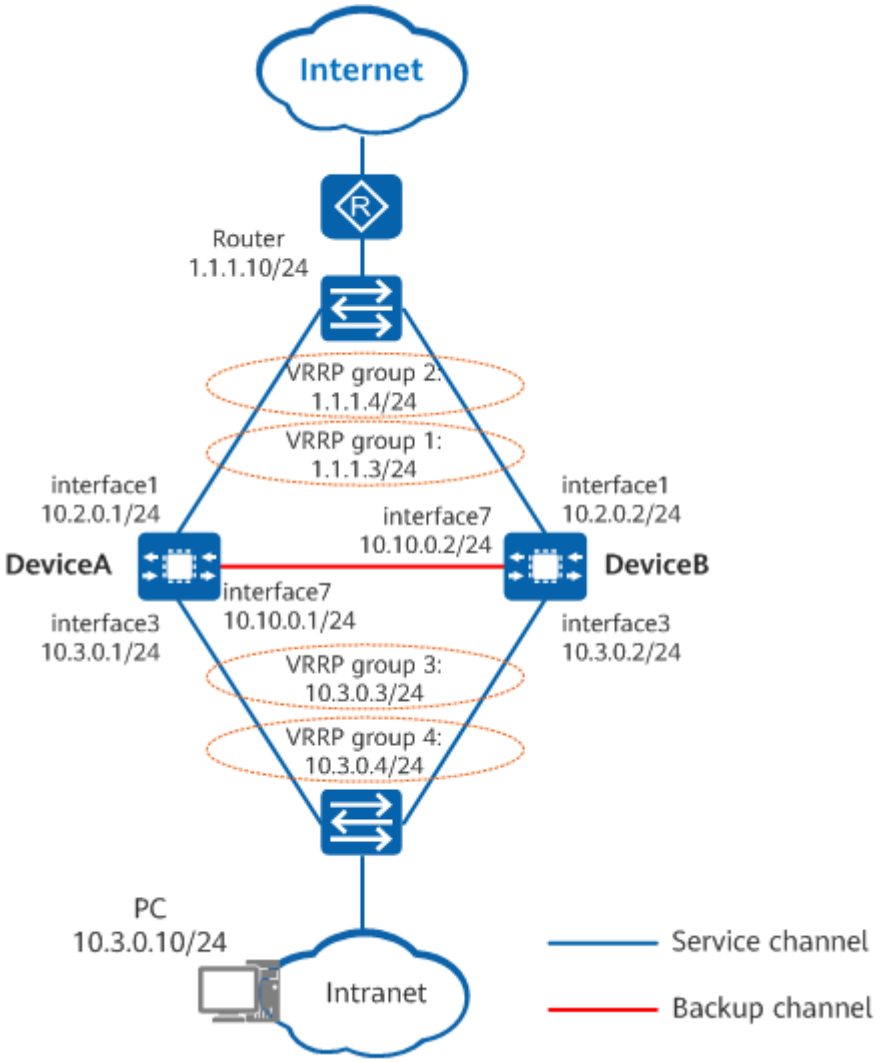
Networking Requirements

On the network shown in **Figure 7-17**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream Layer 2 switches. The upstream switch is connected to the carrier network, and the public IP addresses the carrier assigns to the enterprise are 1.1.1.3 and 1.1.1.4. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-17 Load sharing networking where service interfaces work at Layer 3 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.2/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.2/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz

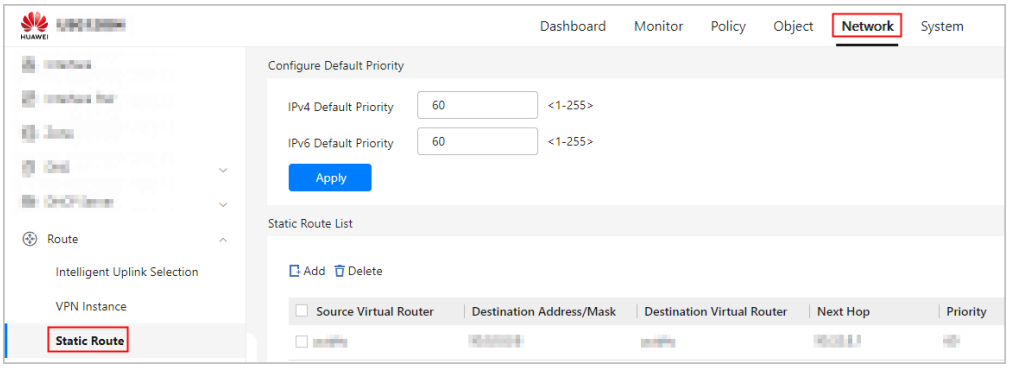
 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.10.0.2/24

Step 2 Configure static routes.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Network** > **Route** > **Static Route**.



2. In **Static Route List**, click **Add**, configure a default route based on the following parameter values, and click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Interface	1.1.1.10
Next Hop	**GE0/0/1**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

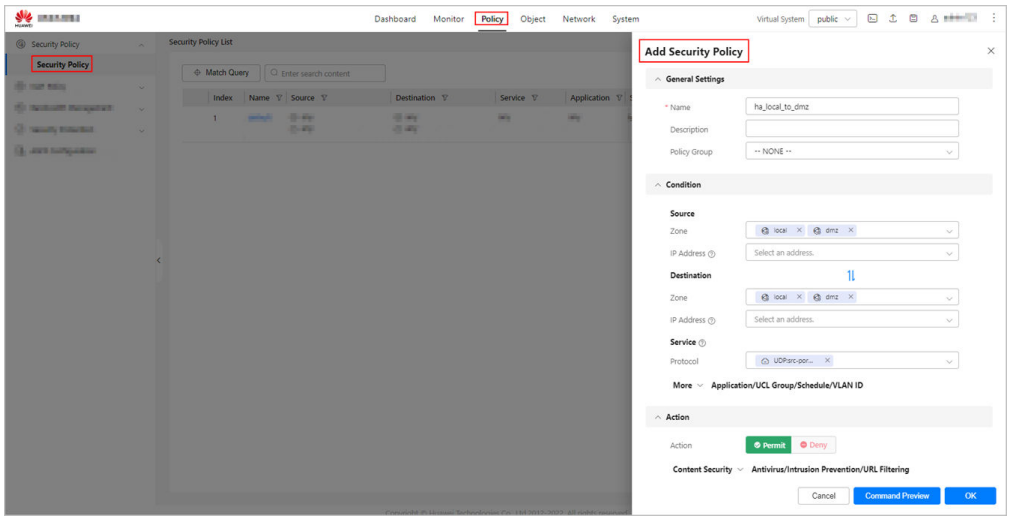
NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

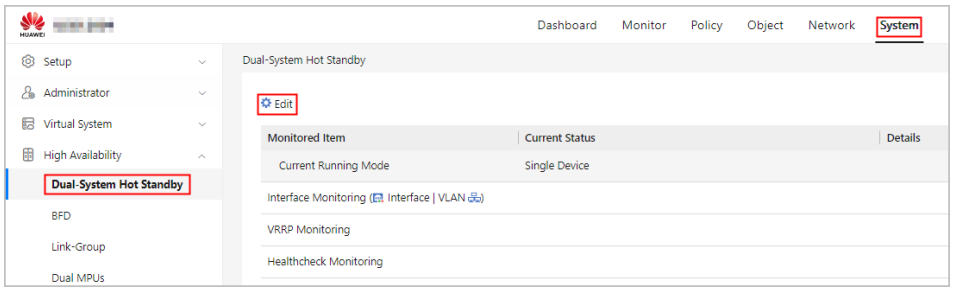
 Copyright © Huawei Technologies Co., Ltd.



Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

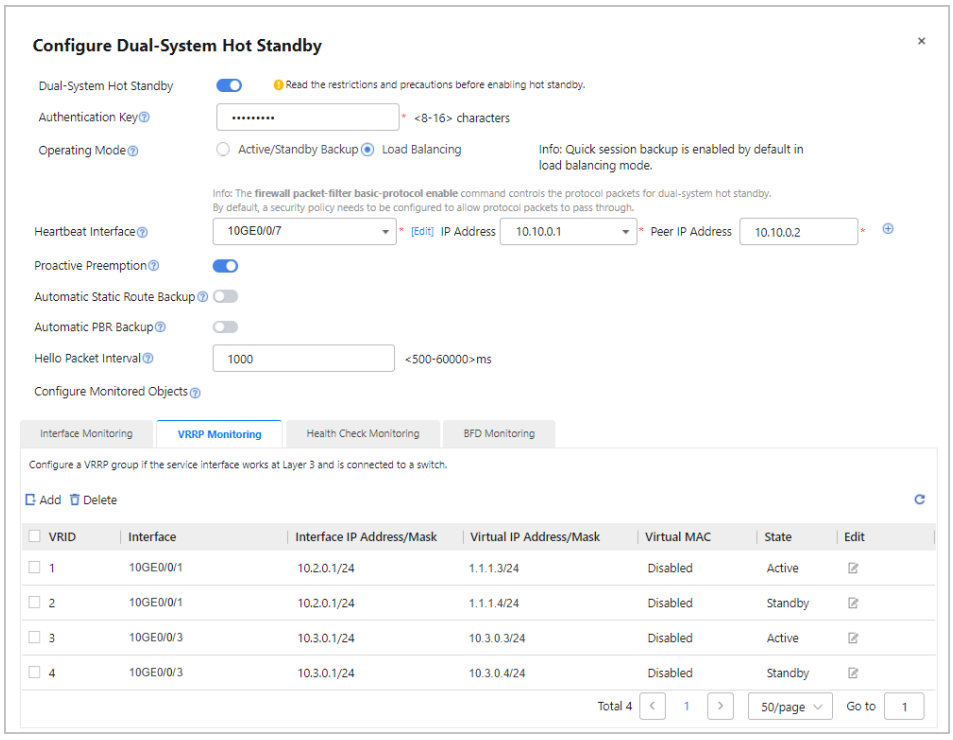
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.



   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

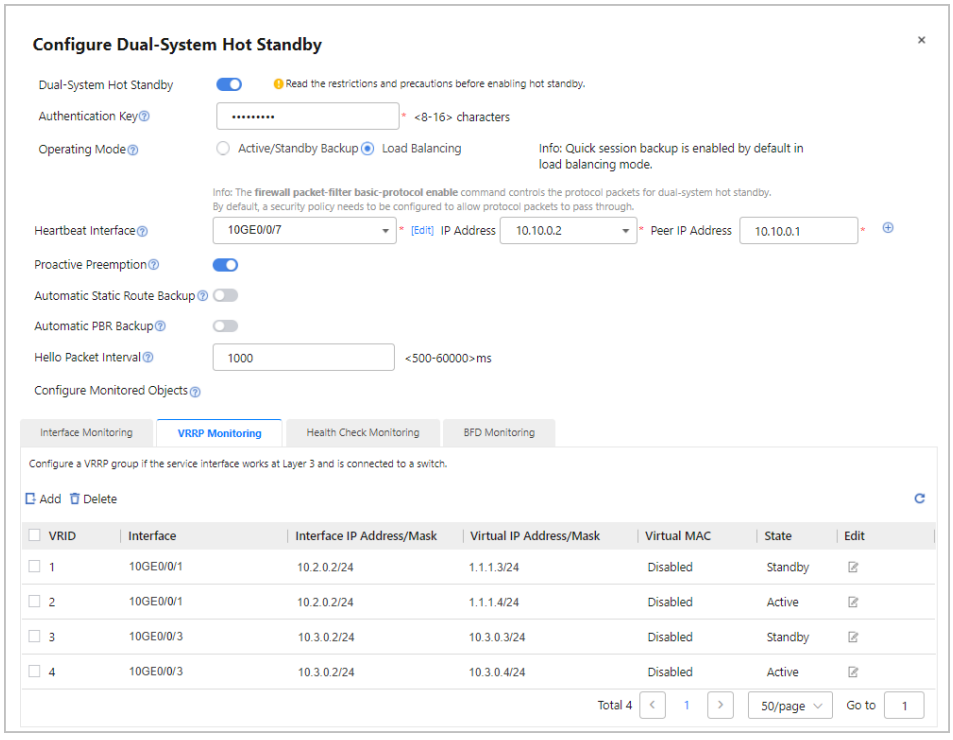
 Copyright © Huawei Technologies Co., Ltd.



2. Configure hot standby on DeviceB.

   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



3. To prevent port conflicts in address translation on the DeviceA and DeviceB in load balancing mode, configure available port ranges on DeviceA and

 Copyright © Huawei Technologies Co., Ltd.

DeviceB. Currently, the configuration cannot be performed on the web UI. Click **CLI Console** in the lower right corner of the page to display the CLI configuration page and configure it on the CLI.

NOTE

In the hot standby load balancing scenario, If NAPT is configured, the DeviceA and DeviceB may have conflicting public ports. To prevent such conflicts, configure respective NAT resources (including public IP addresses and ports) for the DeviceA and DeviceB. You can run the **hrp nat resource primary-group** command on the active device. The standby device will automatically generate the **hrp nat resource secondary-group** command (if you run the **hrp nat resource secondary-group** command on the active device, the standby device will automatically generate the **hrp nat resource primary-group** command).

Perform the following configuration on DeviceA:

```
HRP_M[DeviceA] hrp nat resource primary-group
```

Perform the following configuration on DeviceB:

```
HRP_S[DeviceB] hrp nat resource secondary-group
```

Step 5 Configure a security policy.

Configure a security policy on DeviceA to allow intranet users to access the Internet. After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

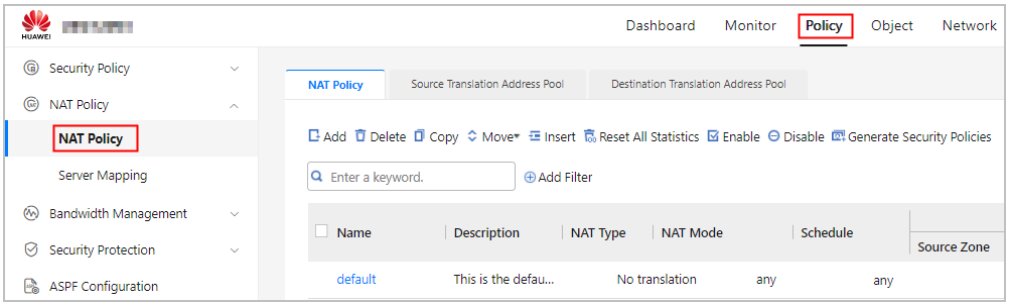
Name	trust_to_untrust
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

Step 6 Configure a NAT policy.

Configure a NAT policy on DeviceA to allow intranet users to access the Internet using the public IP address after NAT. That is, the source IP addresses on subnet 10.3.0.0/24 are translated into IP addresses in the NAT address pool (1.1.2.5 to 1.1.2.8) when intranet users access the Internet. After hot standby relationship is established, the NAT policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.



2. Click the **Source Translation Address Pool** tab, click **Add**, configure a NAT address pool and set the parameters as follows, and then click **OK**.

Name	addressgroup1
IP Address Range	1.1.2.5-1.1.2.8

3. Click the **NAT Policy** tab, click **Add**, configure a NAT policy and set the parameters as follows, and then click **OK**.

Name	policy_nat1
NAT Type	NAT
NAT Mode	Source address translation
Source Zone	trust
Destination Type	Destination Zone: untrust
Source Address	10.3.0.0/24
Source Address Translated To	IP Addresses in the IP Address Pool
Source Translation Address Pool	addressgroup1

Step 7 Configure the switches and PCs.

1. Add the three interfaces of the switches to the same VLANs accordingly. For configuration commands, refer to related documents of the switches.
2. On some intranet PCs, specify the IP address (10.3.0.3) of VRRP group 3 as the default gateway address and on some other intranet PCs, specify the IP address (10.3.0.4) of VRRP group 4 as the default gateway address to implement load balancing of intranet traffic.

Step 8 Configure the router.

Configure equal-cost routes to the NAT address pool, with the next hops being the virtual IP addresses of VRRP group 1 and VRRP group 2.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp nat resource primary-group
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 255.255.255.0 active
 vrrp vrid 2 virtual-ip 1.1.1.4 255.255.255.0 standby
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 active
 vrrp vrid 4 virtual-ip 10.3.0.4 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.2.5 1.1.2.8
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action source-nat address-group group1
#
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp nat resource secondary-group
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 255.255.255.0 standby
 vrrp vrid 2 virtual-ip 1.1.1.4 255.255.255.0 active
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 standby
 vrrp vrid 4 virtual-ip 10.3.0.4 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
 section 0 1.1.2.5 1.1.2.8
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  action source-nat address-group group1
#
```

 Copyright © Huawei Technologies Co., Ltd.

7.2.2 CLI: Example for Deploying Devices in In-path Mode and Connecting to Switches in Upstream and Downstream Directions

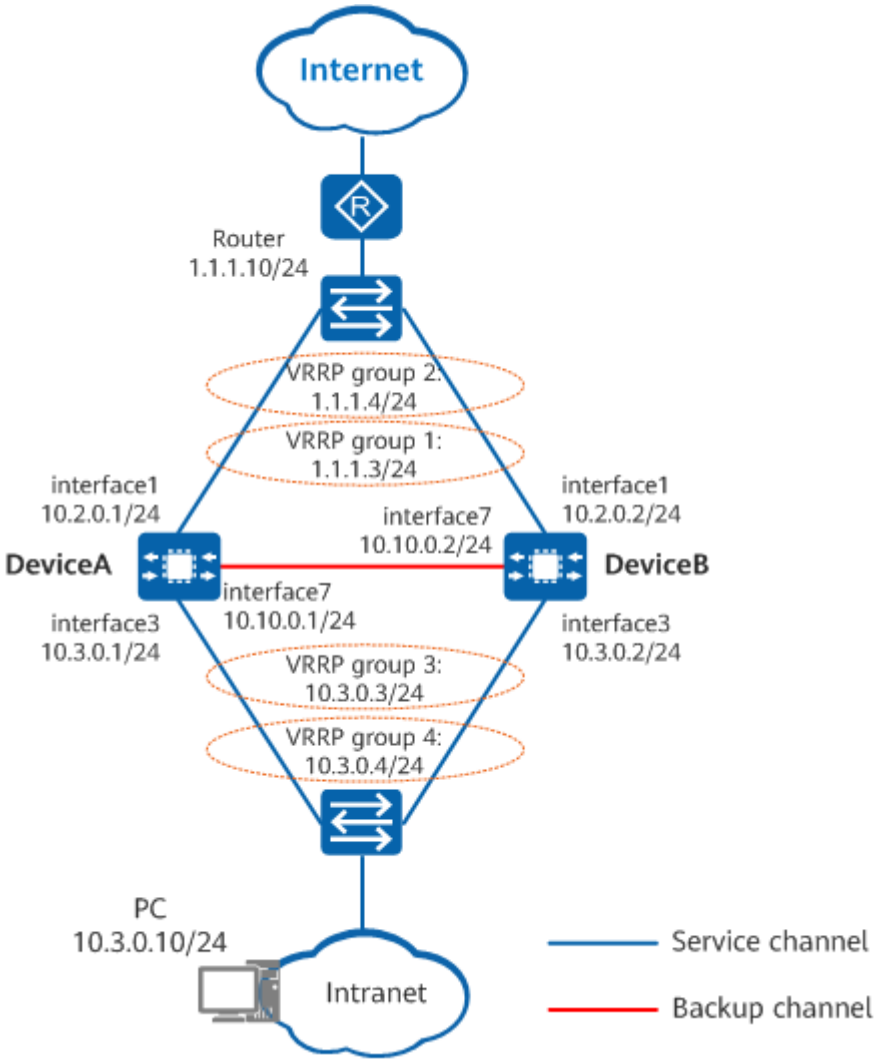
Networking Requirements

On the network shown in **Figure 7-18**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream Layer 2 switches. The upstream switch is connected to the carrier network, and the public IP addresses the carrier assigns to the enterprise are 1.1.1.3 and 1.1.1.4. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-18 Load sharing networking where service interfaces work at Layer 3 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.0.2 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Create a default route with next hop 1.1.1.10 on DeviceA and DeviceB to forward traffic of intranet users to Router.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.10**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.10**

Step 2 Configure VRRP groups.

To implement load sharing, configure two VRRP groups on each service interface and specify **active** in the **vrrp vrid virtual-ip** command for one VRRP group and **standby** in the command for the other VRRP group.

DeviceA	DeviceB
# Configure VRRP groups 1 and 2 on upstream service interface GE 0/0/1 of DeviceA and specify **active** in the **vrrp vrid virtual-ip** command for VRRP group 1 and **standby** in the command for VRRP group 2. Configure VRRP groups 1 and 2 on upstream service interface GE 0/0/1 of DeviceB and specify **standby** in the **vrrp vrid virtual-ip** command for VRRP group 1 and **active** in the command for VRRP group 2. If the IP addresses of the interface and VRRP group are on different subnets, specify a mask when configuring the IP address of the VRRP group.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.3 24 active** [DeviceA-GE0/0/1] **vrrp vrid 2 virtual-ip 1.1.1.4 24 standby** [DeviceA-GE0/0/1] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.3 24 standby** [DeviceB-GE0/0/1] **vrrp vrid 2 virtual-ip 1.1.1.4 24 active** [DeviceB-GE0/0/1] **quit**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure VRRP groups 3 and 4 on downstream service interface GE 0/0/3 of DeviceA and specify **active** in the **vrrp vrid virtual-ip** command for VRRP group 3 and **standby** in the command for VRRP group 4. Configure VRRP groups 3 and 4 on downstream service interface GE 0/0/3 of DeviceB and specify **standby** in the **vrrp vrid virtual-ip** command for VRRP group 3 and **active** in the command for VRRP group 4.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 3 virtual-ip 10.3.0.3 active** [DeviceA-GE0/0/3] **vrrp vrid 4 virtual-ip 10.3.0.4 standby** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 3 virtual-ip 10.3.0.3 standby** [DeviceB-GE0/0/3] **vrrp vrid 4 virtual-ip 10.3.0.4 active** [DeviceB-GE0/0/3] **quit**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Configure quick session backup, specify the heartbeat interface, and enable hot standby.

DeviceA	DeviceB
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Create a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name trust_to_untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] action permit
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure a NAT policy on DeviceA. After hot standby is enabled, the NAT policy on DeviceA will be automatically backed up to DeviceB.

Configure a NAT policy to translate source addresses on subnet 10.3.0.0/24 to IP addresses in the NAT address pool (1.1.2.5 to 1.1.2.8) when intranet users access the Internet.

```
HRP_M[DeviceA] nat address-group group1
HRP_M[DeviceA-address-group-group1] section 0 1.1.2.5 1.1.2.8
HRP_M[DeviceA-address-group-group1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat1
HRP_M[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat1] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group group1
HRP_M[DeviceA-policy-nat-rule-policy_nat1] quit
HRP_M[DeviceA-policy-nat] quit
```

To prevent port conflicts during NAT on the devices in load sharing mode, configure available port ranges on DeviceA and DeviceB. The configuration on DeviceA is as follows:

```
HRP_M[DeviceA] hrp nat resource primary-group
```

After the command is run on DeviceA, DeviceB will automatically back it up and convert it to the **hrp nat resource secondary-group** command.

Step 7 Configure switches and PCs.

1. Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.
2. Specify the IP address (10.3.0.3) of VRRP group 3 as the default gateway address on some intranet PCs, and specify the IP address (10.3.0.4) of VRRP group 4 as the default gateway address on some other intranet PCs. This implements load sharing of intranet traffic.

Step 8 Configure Router.

 Copyright © Huawei Technologies Co., Ltd.

Configure equal-cost routes to the NAT address pool, with the next hops being the virtual IP addresses of VRRP group 1 and VRRP group 2.

----End

Verifying the Configuration

1. Run the **display vrrp** command on DeviceA and DeviceB to check the status of interfaces in the VRRP group.
2. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
3. Ping Router in the untrust zone from the PC in the trust zone, and run the **display firewall session table** command to check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall session table** Current Total Sessions : 1 icmp VPN: public --> public 10.3.0.10:0[1.1.2.5:10298] --> 1.1.1.10:2048	HRP_S<DeviceB> **display firewall session table** Current Total Sessions : 1 icmp VPN:public --> public **Remote** 10.3.0.10:0[1.1.2.5:10298] --> 1.1.1.10:2048

   The command output shows that sessions tagged with **Remote** are created on DeviceB, indicating that sessions are successfully backed up after hot standby is configured.
4. Run the **ping 1.1.1.10 -t** command on the PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is performed and whether ping packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA	DeviceB
# sysname **DeviceA** # hrp enable hrp interface GE0/0/7 remote **10.10.0.2** hrp mirror session enable hrp nat resource **primary-group** hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!! J6+;U#>V\!_e1NY[iGLXjT %k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!! Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%# # interface GE0/0/1 ip address **10.2.0.1** 255.255.255.0 vrrp vrid 1 virtual-ip 1.1.1.3 255.255.255.0 **active** vrrp vrid 2 virtual-ip 1.1.1.4 255.255.255.0 **standby** # interface GE0/0/3 ip address **10.3.0.1** 255.255.255.0 vrrp vrid 3 virtual-ip 10.3.0.3 **active** vrrp vrid 4 virtual-ip 10.3.0.4 **standby** # interface GE0/0/7 ip address **10.10.0.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/3 # firewall zone untrust set priority 5 add interface GE0/0/1 # firewall zone dmz set priority 50 add interface GE0/0/7 # ip route-static 0.0.0.0 0.0.0.0 1.1.1.10 # nat address-group group1 section 0 1.1.2.5 1.1.2.8 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name trust_to_untrust source-zone trust destination-zone untrust source-address 10.3.0.0 24 action permit # nat-policy rule name policy_nat1 source-zone trust destination-zone untrust source-address 10.3.0.0 24 action source-nat address-group group1 #	# sysname **DeviceB** # hrp enable hrp interface GE0/0/7 remote **10.10.0.1** hrp mirror session enable hrp nat resource **secondary-group** hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!! \FR0@B|5m51t2(SLB$(Yzq_KUB\| V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4 t;1e+vR$$U!!!!!%+%# # interface GE0/0/1 ip address **10.2.0.2** 255.255.255.0 vrrp vrid 1 virtual-ip 1.1.1.3 255.255.255.0 **standby** vrrp vrid 2 virtual-ip 1.1.1.4 255.255.255.0 **active** # interface GE0/0/3 ip address **10.3.0.2** 255.255.255.0 vrrp vrid 3 virtual-ip 10.3.0.3 **standby** vrrp vrid 4 virtual-ip 10.3.0.4 **active** # interface GE0/0/7 ip address **10.10.0.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/3 # firewall zone untrust set priority 5 add interface GE0/0/1 # firewall zone dmz set priority 50 add interface GE0/0/7 # ip route-static 0.0.0.0 0.0.0.0 1.1.1.10 # nat address-group group1 section 0 1.1.2.5 1.1.2.8 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name trust_to_untrust source-zone trust destination-zone untrust source-address 10.3.0.0 24 action permit # nat-policy rule name policy_nat1 source-zone trust destination-zone untrust source-address 10.3.0.0 24 action source-nat address-group group1 #

 Copyright © Huawei Technologies Co., Ltd.

7.2.3 Web: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices

Networking Requirements

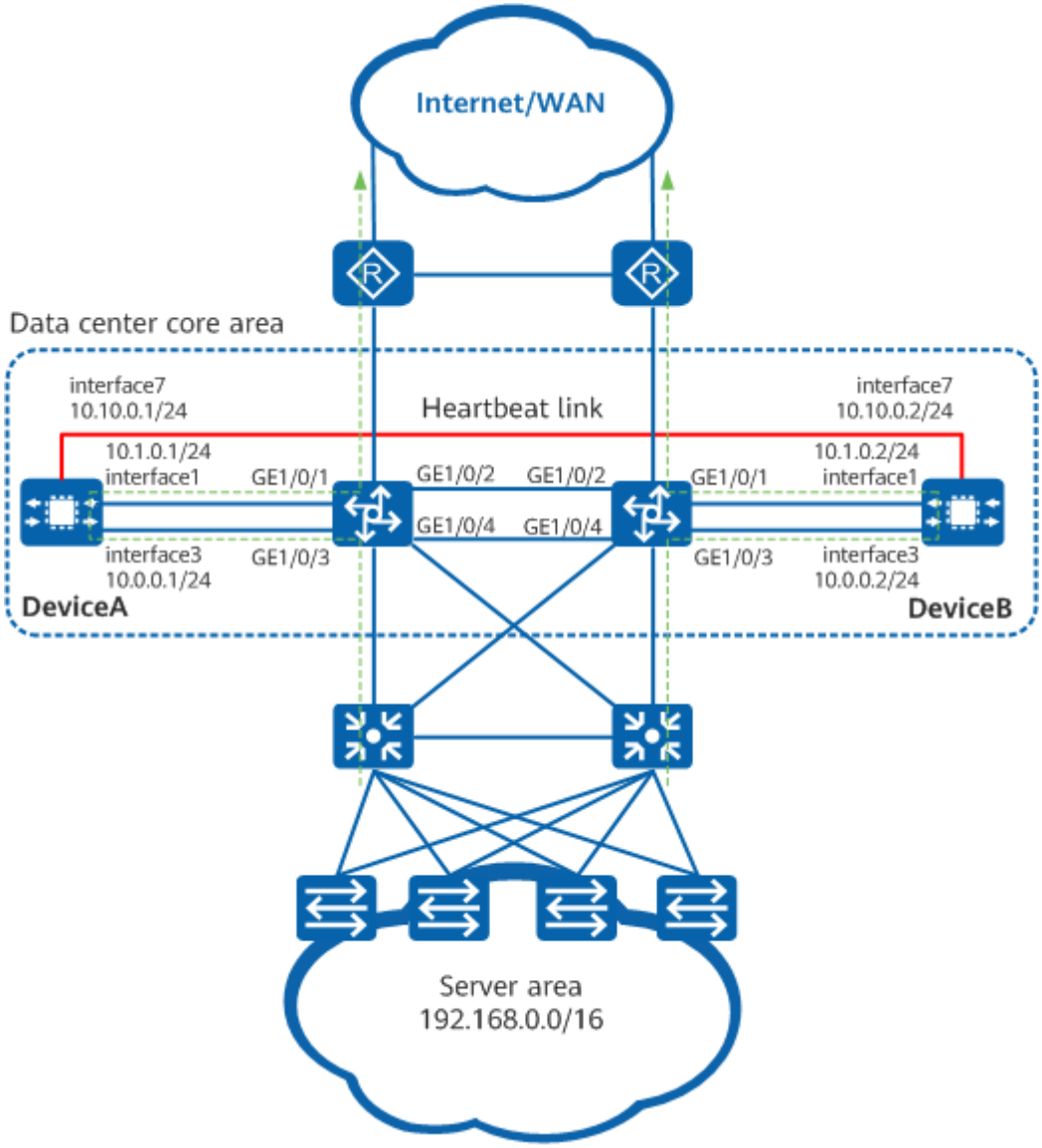
As shown in **Figure 7-19**, DeviceA and DeviceB are connected off-line to the core switches in the data center to secure the data center network. All traffic on the core switches is diverted to DeviceA and DeviceB based on static routes for security checks. DeviceA and DeviceB are expected to work in load sharing mode. Normally, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-19 Networking diagram for configuring hot standby when DeviceA and DeviceB are deployed in off-line mode (using static routing for traffic diversion)

NOTE

In this example, interfaces 1, 3, and 7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



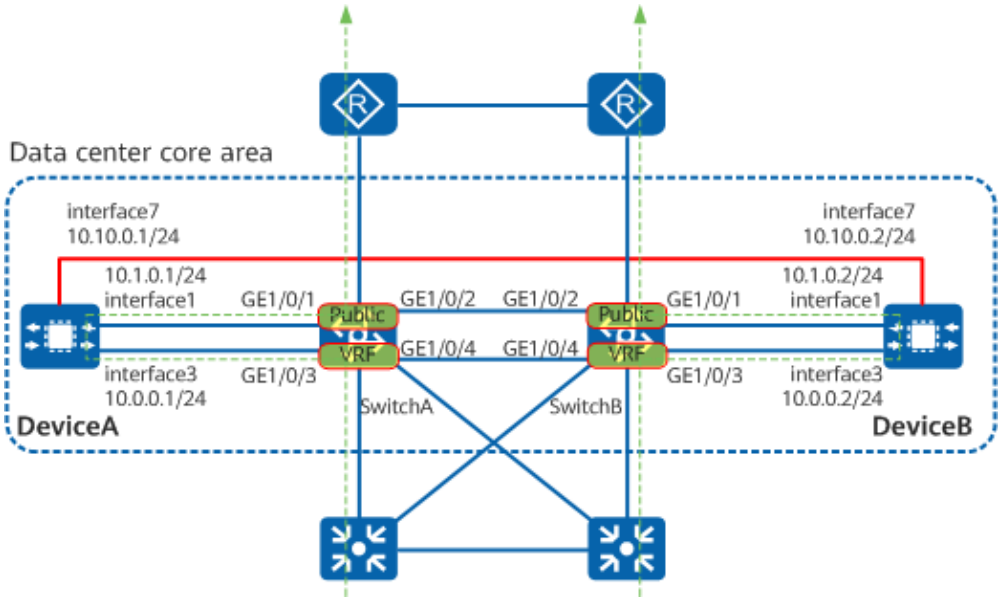
Configuration Roadmap

1. As shown in **Figure 7-20**, if the core switches need to use static routes to divert traffic to DeviceA and DeviceB, you need to configure static routes and set the next hops to the IP addresses of the interfaces of DeviceA and DeviceB. However, the core switches and upstream routers and downstream aggregation switches run OSPF. Therefore, traffic cannot be diverted to DeviceA and DeviceB after reaching the core switches. Instead, the traffic is directly forwarded to the upstream and downstream devices.

   Therefore, you must configure the virtual routing and forwarding (VRF) function on the core switches to virtualize each core switch into a public switch (Public) for connecting to the upstream switch and a virtual switch (VRF) for connecting to the downstream switch. The two virtualized switches are isolated. Therefore, traffic can be diverted to DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-20 Configuring VRF on the switches

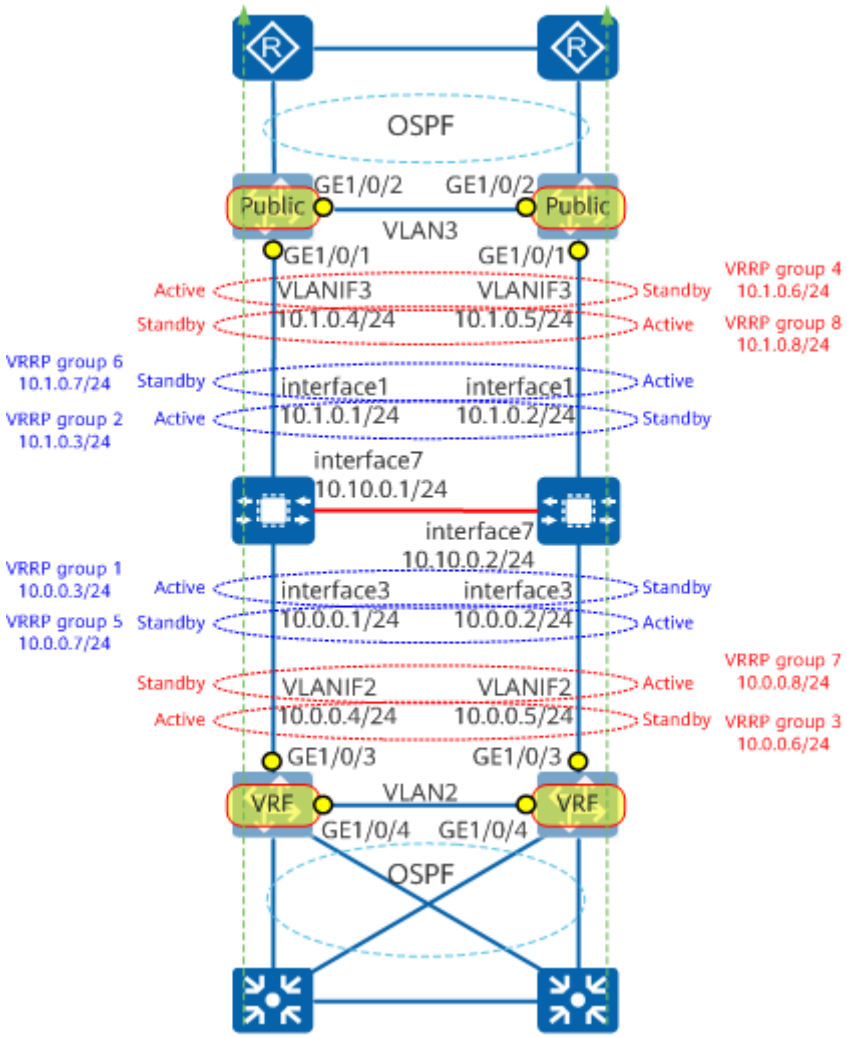


2. **Figure 7-20** can be abstracted as **Figure 7-21**. DeviceA and DeviceB run static routes with upstream and downstream switches (Public and VRF). Therefore, you need to configure VRRP groups on DeviceA, DeviceB and switches for them to communicate using the virtual IP addresses of VRRP groups.

   As shown in **Figure 7-21**, DeviceA and DeviceB work in load sharing mode. You need to configure two equal-cost static routes in the same direction on DeviceA and DeviceB and set the next hops respectively to the IP addresses of the two peer VRRP groups. Configure another two equal-cost static routes on the Public or VRF switch and set the next hops respectively to the IP addresses of the two VRRP groups on the interfaces of DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-21 Configuring VRRP on DeviceA, DeviceB and switches



NOTE

The core switches run static routes with the devices (DeviceA and DeviceB) and OSPF with other devices. **Figure 7-21** lists only the core switch interfaces related to the devices (DeviceA and DeviceB).

3. Specify GE 0/0/7 on DeviceA and DeviceB as the heartbeat interface and enable hot standby.
4. Configure security functions, such as security policies, IPS, and attack defense, on DeviceA. DeviceA will automatically synchronize its configurations to DeviceB. This section describes only security policy configurations as an example.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv4	
IP Address	10.1.0.1/24

c. Repeat the preceding steps to configure **GE0/0/3.**

Zone	trust
IPv4	
IP Address	10.0.0.1/24

d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.1.0.2/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.0.0.2/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

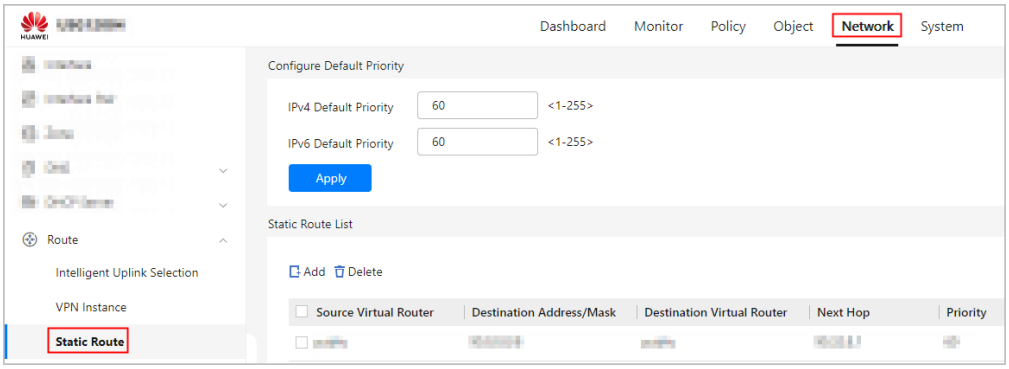
Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure static routes.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Network** > **Route** > **Static Route**.



2. In **Static Route List**, click **Add**, configure a static route (default route) for the upstream direction and set the next hops to the IP address of VRRP groups 4 and 8, and then click **OK**.

Destination Address	0.0.0.0
Mask	0.0.0.0
Next Hop	10.1.0.6

Destination Address	0.0.0.0
Mask	0.0.0.0
Next Hop	10.1.0.8

3. Configure a static route for the downstream direction and set the destination address to an address in the server area and the next hop to the IP address of VRRP groups 3 and 7.

Destination Address	192.168.0.0
Mask	255.255.0.0
Next Hop	10.0.0.6

Destination Address	192.168.0.0
Mask	255.255.0.0
Next Hop	10.0.0.8

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

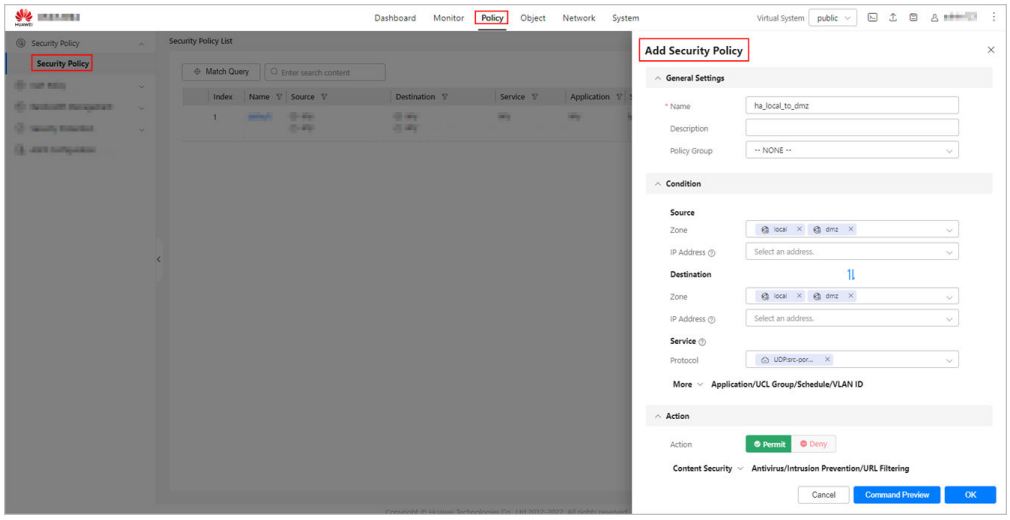
 Copyright © Huawei Technologies Co., Ltd.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

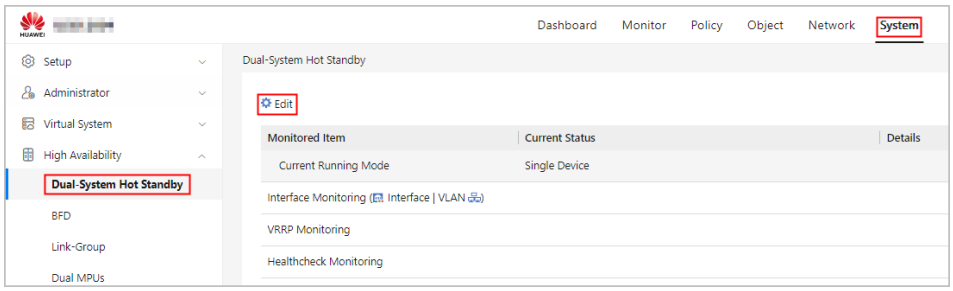


Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

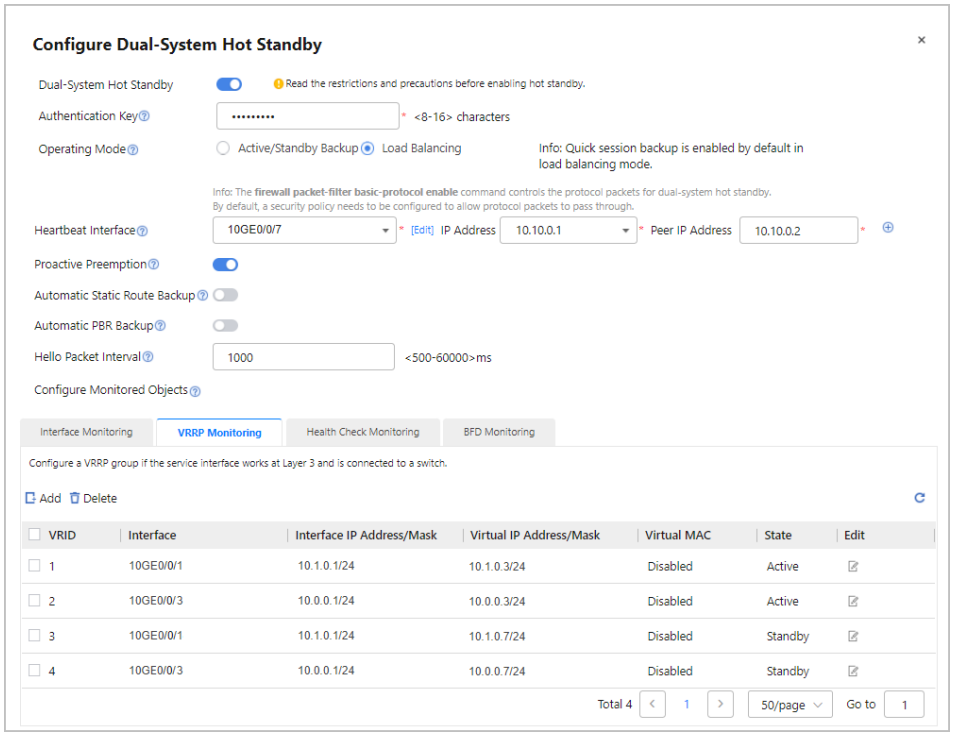
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

 Copyright © Huawei Technologies Co., Ltd.

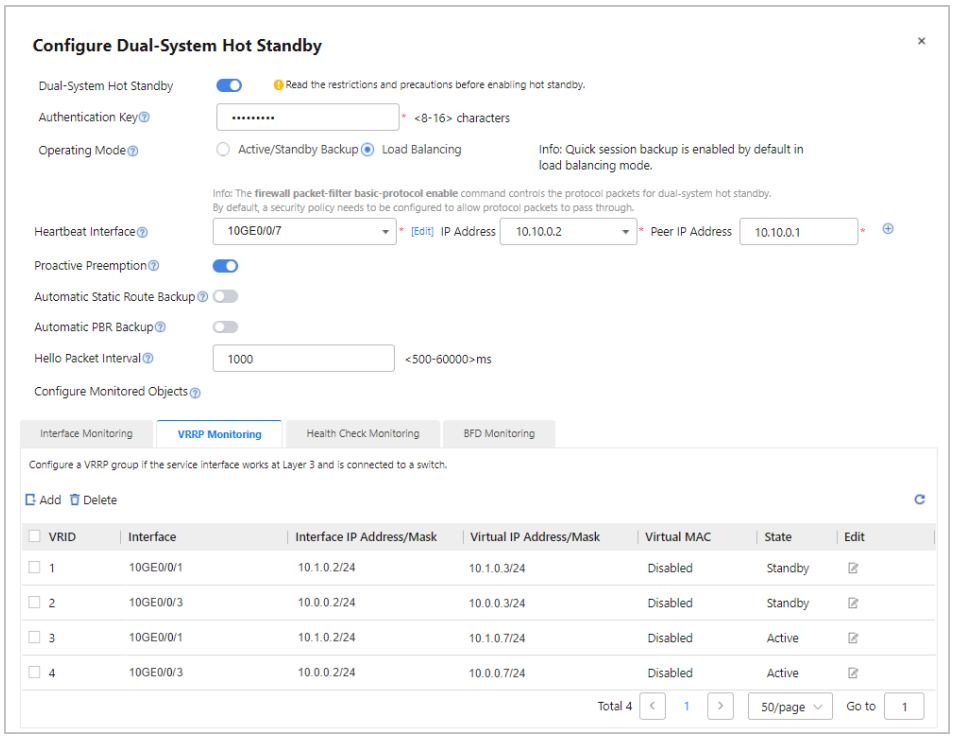


b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 Configure a security policy.

Configure a security policy on DeviceA to allow Internet users to access the server area (subnet: 192.168.0.0/16, port: 80) in the data center. After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

Name	policy_sec1
Source Zone	untrust
Destination Zone	trust
Destination Address	192.168.0.0/16
Service	http
Action	Permit

Step 6 Configure the core switches.

NOTE

This example describes only the switch configurations related to firewall connection.

Configure SwitchA.

```
[SwitchA] ip vpn-instance VRF     //Create VRF.
[SwitchA-vpn-instance-VRF] ipv4-family
[SwitchA-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[SwitchA-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchA-vpn-instance-VRF-af-ipv4] quit
[SwitchA-vpn-instance-VRF] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/3 to 1/0/4     //Add the interface to VLAN2.
[SwitchA-vlan2] quit
[SwitchA] interface Vlanif 2
[SwitchA-Vlanif2] ip binding vpn-instance VRF     //Bind VLANIF2 to VRF.
[SwitchA-Vlanif2] ip address 10.0.0.4 24
[SwitchA-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6     //Create VRRP group 3.
[SwitchA-Vlanif2] vrrp vrid 3 priority 120     //Set the priority to 120. The VRRP group with high priority is active.
[SwitchA-Vlanif2] vrrp vrid 7 virtual-ip 10.0.0.8     //Create VRRP group 7.
[SwitchA-Vlanif2] vrrp vrid 7 priority 100     //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchA-Vlanif2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchA-vlan3] quit
[SwitchA] interface Vlanif 3
[SwitchA-Vlanif3] ip address 10.1.0.4 24
[SwitchA-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchA-Vlanif3] vrrp vrid 4 priority 120     //Set the priority to 120. The VRRP group with high priority is active.
[SwitchA-Vlanif3] vrrp vrid 8 virtual-ip 10.1.0.8     //Create VRRP group 8.
[SwitchA-Vlanif3] vrrp vrid 8 priority 100     //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchA-Vlanif3] quit
[SwitchA] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3     //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 1.
[SwitchA] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.7     //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 5.
[SwitchA] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3     //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 2.
[SwitchA] ip route-static 192.168.0.0 255.255.0.0 10.1.0.7     //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 6.
```

Configure SwitchB.

```
[SwitchB] ip vpn-instance VRF     //Create VRF.
[SwitchB-vpn-instance-VRF] ipv4-family
[SwitchB-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchB-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchB-vpn-instance-VRF-af-ipv4] quit
[SwitchB-vpn-instance-VRF] quit
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/3 to 1/0/4     //Add the interface to VLAN2.
[SwitchB-vlan2] quit
[SwitchB] interface Vlanif 2
[SwitchB-Vlanif2] ip binding vpn-instance VRF     //Bind VLANIF2 to VRF.
[SwitchB-Vlanif2] ip address 10.0.0.5 24
[SwitchB-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6     //Create VRRP group 3.
[SwitchB-Vlanif2] vrrp vrid 3 priority 100     //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchB-Vlanif2] vrrp vrid 7 virtual-ip 10.0.0.8     //Create VRRP group 7.
[SwitchB-Vlanif2] vrrp vrid 7 priority 120     //Set the priority to 120. The VRRP group with high priority is active.
[SwitchB-Vlanif2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchB-vlan3] quit
[SwitchB] interface Vlanif 3
[SwitchB-Vlanif3] ip address 10.1.0.5 24
[SwitchB-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchB-Vlanif3] vrrp vrid 4 priority 100     //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchB-Vlanif3] vrrp vrid 8 virtual-ip 10.1.0.8     //Create VRRP group 8.
[SwitchB-Vlanif3] vrrp vrid 8 priority 120     //Set the priority to 120. The VRRP group with high priority is active.
[SwitchB-Vlanif3] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[SwitchB] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3    //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 1.
[SwitchB] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.7    //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 5.
[SwitchB] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3    //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 2.
[SwitchB] ip route-static 192.168.0.0 255.255.0.0 10.1.0.7    //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 6.
```

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 active
 vrrp vrid 6 virtual-ip 10.1.0.7 standby
#
interface GE0/0/3
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 active
 vrrp vrid 5 virtual-ip 10.0.0.7 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 0.0.0.0 0.0.0.0 10.1.0.8
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.8
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 standby
 vrrp vrid 6 virtual-ip 10.1.0.7 active
#
interface GE0/0/3
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 standby
 vrrp vrid 5 virtual-ip 10.0.0.7 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 0.0.0.0 0.0.0.0 10.1.0.8
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.8
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.2.4 CLI: Example for Connecting Devices to Switches in Out-of-path Mode and Configuring Static Routes on the Switches to Divert Traffic to the Devices

Networking Requirements

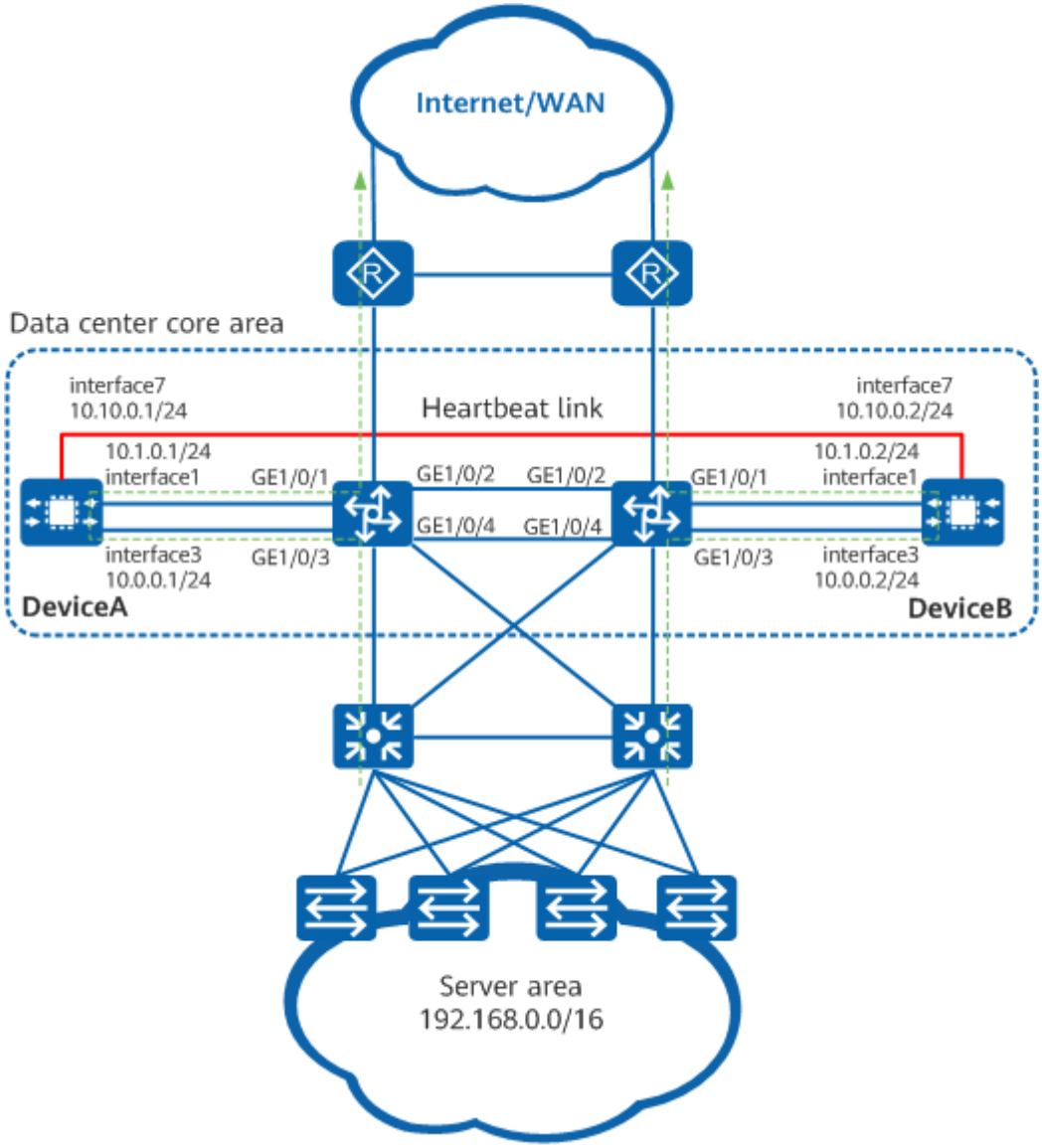
As shown in **Figure 7-22**, DeviceA and DeviceB are connected off-line to the core switches in the data center to secure the data center network. All traffic on the core switches is diverted to DeviceA and DeviceB based on static routes for security checks. DeviceA and DeviceB are expected to work in load sharing mode. Normally, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-22 Networking diagram for configuring hot standby when DeviceA and DeviceB are deployed in off-line mode (using static routing for traffic diversion)

NOTE

In this example, interfaces 1, 3, and 7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



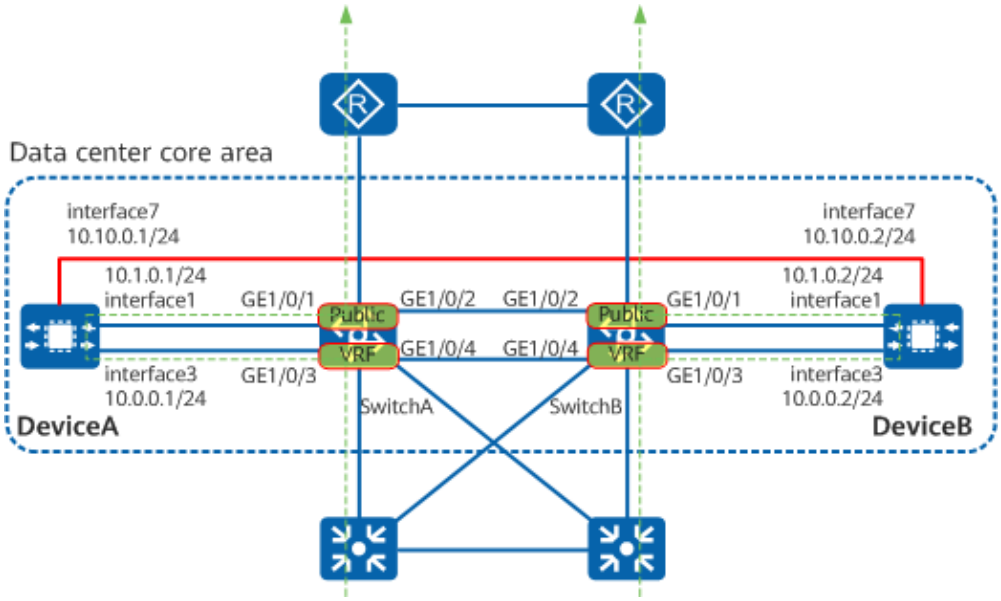
Configuration Roadmap

1. As shown in **Figure 7-23**, if the core switches need to use static routes to divert traffic to DeviceA and DeviceB, you need to configure static routes and set the next hops to the IP addresses of the interfaces of DeviceA and DeviceB. However, the core switches and upstream routers and downstream aggregation switches run OSPF. Therefore, traffic cannot be diverted to DeviceA and DeviceB after reaching the core switches. Instead, the traffic is directly forwarded to the upstream and downstream devices.

   Therefore, you must configure the virtual routing and forwarding (VRF) function on the core switches to virtualize each core switch into a public switch (Public) for connecting to the upstream switch and a virtual switch (VRF) for connecting to the downstream switch. The two virtualized switches are isolated. Therefore, traffic can be diverted to DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-23 Configuring VRF on the switches

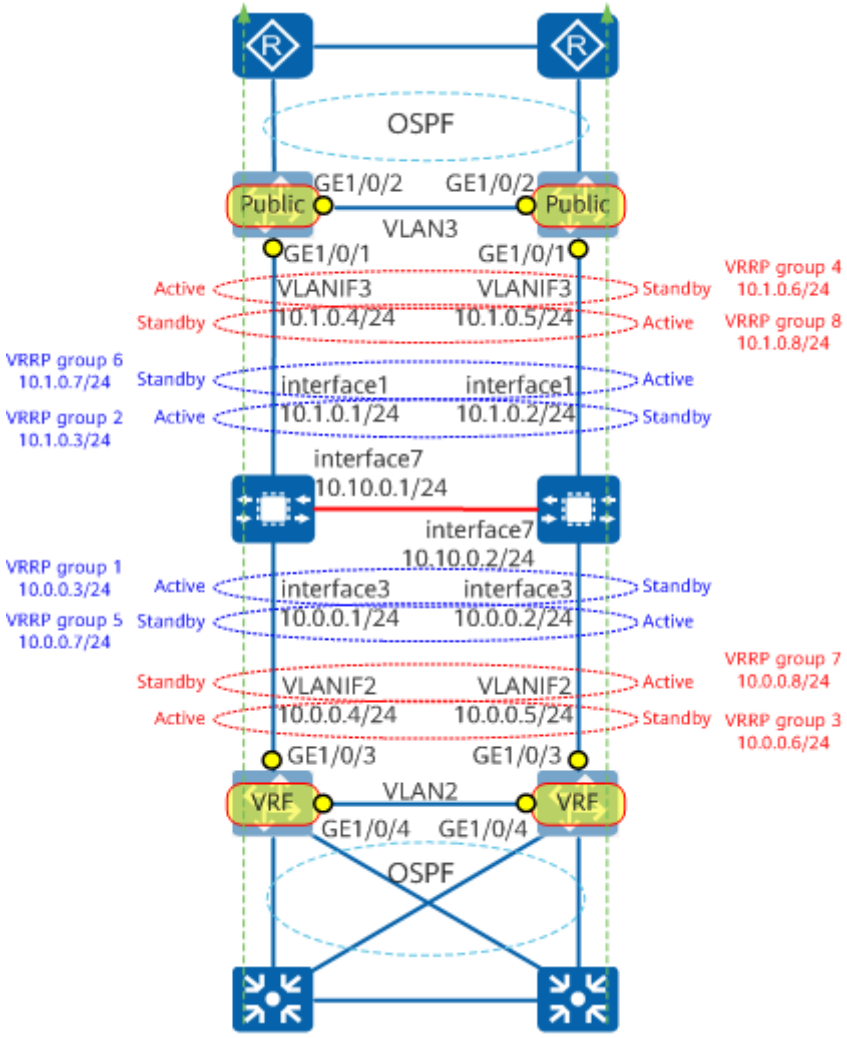


2. **Figure 7-23** can be abstracted as **Figure 7-24**. DeviceA and DeviceB run static routes with upstream and downstream switches (Public and VRF). Therefore, you need to configure VRRP groups on DeviceA, DeviceB and switches for them to communicate using the virtual IP addresses of VRRP groups.

   As shown in **Figure 7-24**, DeviceA and DeviceB work in load sharing mode. You need to configure two equal-cost static routes in the same direction on DeviceA and DeviceB and set the next hops respectively to the IP addresses of the two peer VRRP groups. Configure another two equal-cost static routes on the Public or VRF switch and set the next hops respectively to the IP addresses of the two VRRP groups on the interfaces of DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-24 Configuring VRRP on DeviceA, DeviceB and switches



NOTE

The core switches run static routes with the devices (DeviceA and DeviceB) and OSPF with other devices. **Figure 7-24** lists only the core switch interfaces related to the devices (DeviceA and DeviceB).

3. Specify GE 0/0/7 on DeviceA and DeviceB as the heartbeat interface and enable hot standby.
4. Configure security functions, such as security policies, IPS, and attack defense, on DeviceA. DeviceA will automatically synchronize its configurations to DeviceB. This section describes only security policy configurations as an example.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.1.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.0.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.1.0.2 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.0.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

Step 2 Create static routes.

DeviceA	DeviceB
# Configure two equal-cost static routes (default routes) for the upstream direction and set the next hops respectively to the IP addresses of VRRP groups 4 and 8.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 10.1.0.6** [DeviceA] **ip route-static 0.0.0.0 0.0.0.0 10.1.0.8**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 10.1.0.6** [DeviceB] **ip route-static 0.0.0.0 0.0.0.0 10.1.0.8**
# Configure two static routes for the downstream direction and set the destination addresses to addresses in the server area and the next hops respectively to the IP addresses of VRRP groups 3 and 7.	
[DeviceA] **ip route-static 192.168.0.0 255.255.0.0 10.0.0.6** [DeviceA] **ip route-static 192.168.0.0 255.255.0.0 10.0.0.8**	[DeviceB] **ip route-static 192.168.0.0 255.255.0.0 10.0.0.6** [DeviceB] **ip route-static 192.168.0.0 255.255.0.0 10.0.0.8**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Configure hot standby.

DeviceA	DeviceB
# Configure VRRP groups on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp vrid 2 virtual-ip 10.1.0.3 active** [DeviceA-GE0/0/1] **vrrp vrid 6 virtual-ip 10.1.0.7 standby** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 1 virtual-ip 10.0.0.3 active** [DeviceA-GE0/0/3] **vrrp vrid 5 virtual-ip 10.0.0.7 standby** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp vrid 2 virtual-ip 10.1.0.3 standby** [DeviceB-GE0/0/1] **vrrp vrid 6 virtual-ip 10.1.0.7 active** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 1 virtual-ip 10.0.0.3 standby** [DeviceB-GE0/0/3] **vrrp vrid 5 virtual-ip 10.0.0.7 active** [DeviceB-GE0/0/3] **quit**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on DeviceA and DeviceB.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Configure a security policy on DeviceA. After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow Internet users to access the server area (subnet: 192.168.0.0/16, port: 80) in the data center.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec1
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-address 192.168.0.0 16
HRP_M[DeviceA-policy-security-rule-policy_sec1] service http
HRP_M[DeviceA-policy-security-rule-policy_sec1] action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-policy-security-rule-policy_sec1] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure the core switches.

NOTE

This example describes only the switch configurations related to firewall connection.

Configure SwitchA.

```
[SwitchA] ip vpn-instance VRF    //Create VRF.
[SwitchA-vpn-instance-VRF] ipv4-family
[SwitchA-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchA-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchA-vpn-instance-VRF-af-ipv4] quit
[SwitchA-vpn-instance-VRF] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/3 to 1/0/4    //Add the interface to VLAN2.
[SwitchA-vlan2] quit
[SwitchA] interface Vlanif 2
[SwitchA-Vlanif2] ip binding vpn-instance VRF    //Bind VLANIF2 to VRF.
[SwitchA-Vlanif2] ip address 10.0.0.4 24
[SwitchA-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6    //Create VRRP group 3.
[SwitchA-Vlanif2] vrrp vrid 3 priority 120    //Set the priority to 120. The VRRP group with high priority is active.
[SwitchA-Vlanif2] vrrp vrid 7 virtual-ip 10.0.0.8    //Create VRRP group 7.
[SwitchA-Vlanif2] vrrp vrid 7 priority 100    //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchA-Vlanif2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/1 to 1/0/2    //Add the interface to VLAN3.
[SwitchA-vlan3] quit
[SwitchA] interface Vlanif 3
[SwitchA-Vlanif3] ip address 10.1.0.4 24
[SwitchA-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6    //Create VRRP group 4.
[SwitchA-Vlanif3] vrrp vrid 4 priority 120    //Set the priority to 120. The VRRP group with high priority is active.
[SwitchA-Vlanif3] vrrp vrid 8 virtual-ip 10.1.0.8    //Create VRRP group 8.
[SwitchA-Vlanif3] vrrp vrid 8 priority 100    //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchA-Vlanif3] quit
[SwitchA] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3    //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 1.
[SwitchA] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.7    //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 5.
[SwitchA] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3    //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 2.
[SwitchA] ip route-static 192.168.0.0 255.255.0.0 10.1.0.7    //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 6.
```

Configure SwitchB.

```
[SwitchB] ip vpn-instance VRF    //Create VRF.
[SwitchB-vpn-instance-VRF] ipv4-family
[SwitchB-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[SwitchB-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[SwitchB-vpn-instance-VRF-af-ipv4] quit
[SwitchB-vpn-instance-VRF] quit
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/3 to 1/0/4    //Add the interface to VLAN2.
[SwitchB-vlan2] quit
[SwitchB] interface Vlanif 2
[SwitchB-Vlanif2] ip binding vpn-instance VRF    //Bind VLANIF2 to VRF.
[SwitchB-Vlanif2] ip address 10.0.0.5 24
[SwitchB-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6    //Create VRRP group 3.
[SwitchB-Vlanif2] vrrp vrid 3 priority 100    //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchB-Vlanif2] vrrp vrid 7 virtual-ip 10.0.0.8    //Create VRRP group 7.
[SwitchB-Vlanif2] vrrp vrid 7 priority 120    //Set the priority to 120. The VRRP group with high priority is
```

 Copyright © Huawei Technologies Co., Ltd.

```
active.
[SwitchB-Vlanif2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1 to 1/0/2     //Add the interface to VLAN3.
[SwitchB-vlan3] quit
[SwitchB] interface Vlanif 3
[SwitchB-Vlanif3] ip address 10.1.0.5 24
[SwitchB-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6     //Create VRRP group 4.
[SwitchB-Vlanif3] vrrp vrid 4 priority 100     //Set the priority to 100. The VRRP group with low priority is standby.
[SwitchB-Vlanif3] vrrp vrid 8 virtual-ip 10.1.0.8     //Create VRRP group 8.
[SwitchB-Vlanif3] vrrp vrid 8 priority 120     //Set the priority to 120. The VRRP group with high priority is active.
[SwitchB-Vlanif3] quit
[SwitchB] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3     //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 1.
[SwitchB] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.7     //Configure a default route on the VRF and set the next hop to the virtual IP address of VRRP group 5.
[SwitchB] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3     //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 2.
[SwitchB] ip route-static 192.168.0.0 255.255.0.0 10.1.0.7     //Configure a static route on the Public switch and set the next hop to the virtual IP address of VRRP group 6.
```

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to view hot standby status.
2. Run the **display firewall session table** command on DeviceA and DeviceB. The command output shows that DeviceA and DeviceB have common sessions and sessions tagged with **Remote**, indicating that the traffic on the core switch is diverted to the devices, and hot standby in load sharing mode is successfully configured.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.1 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 active
 vrrp vrid 6 virtual-ip 10.1.0.7 standby
#
interface GE0/0/3
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 active
 vrrp vrid 5 virtual-ip 10.0.0.7 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 0.0.0.0 0.0.0.0 10.1.0.8
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.8
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.1.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.0.3 standby
 vrrp vrid 6 virtual-ip 10.1.0.7 active
#
interface GE0/0/3
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.3 standby
 vrrp vrid 5 virtual-ip 10.0.0.7 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ip route-static 0.0.0.0 0.0.0.0 10.1.0.6
ip route-static 0.0.0.0 0.0.0.0 10.1.0.8
ip route-static 192.168.0.0 255.255.0.0 10.0.0.6
ip route-static 192.168.0.0 255.255.0.0 10.0.0.8
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  destination-address 192.168.0.0 mask
255.255.0.0
  service http
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.2.5 Web: Example for Load Balancing Networking in Which the Devices Work as the Gateways and Multi-ISP Accesses Are Provided

Networking Requirements

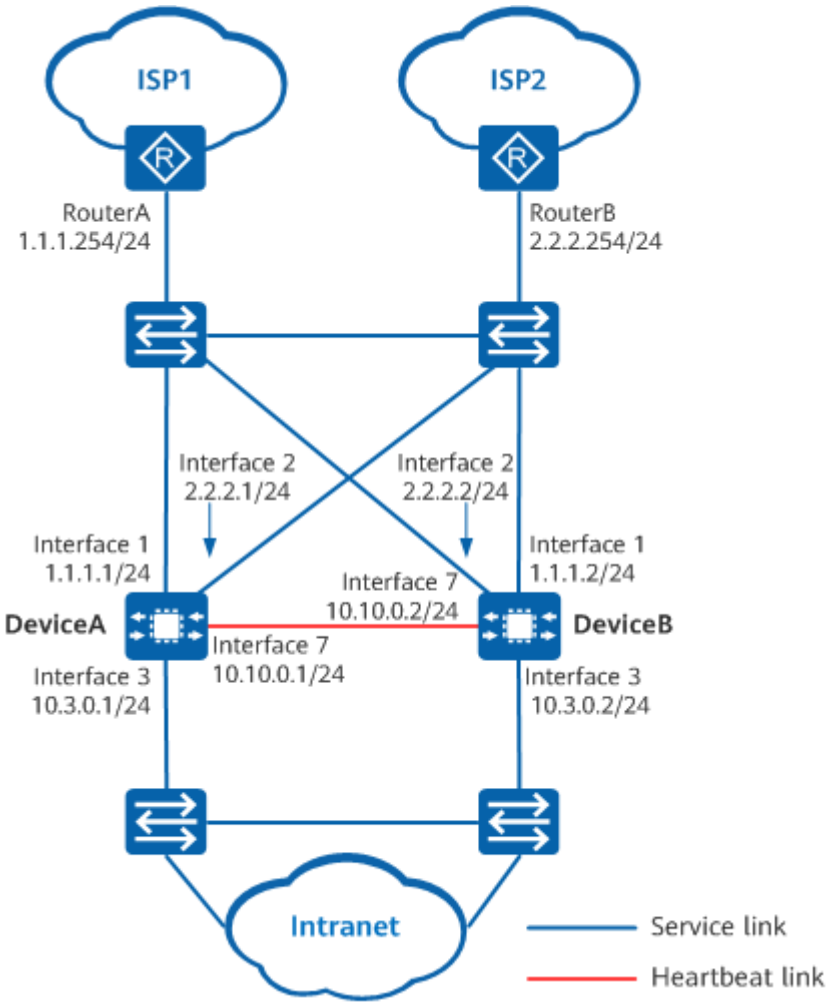
As shown in **Figure 7-25**, service interfaces of DeviceA and DeviceB work at Layer 3, having upstream and downstream connections to Layer-2 switches. The upstream two switches are connected to two ISPs. ISP1 assigns the IP addresses of 1.1.1.1, 1.1.1.2, and 1.1.1.3, and ISP2 assigns the IP addresses of 2.2.2.1, 2.2.2.2, and 2.2.2.3 to the enterprise. Now, DeviceA and DeviceB are supposed to work in load balancing mode so that traffic from Dept. A (IP address range: 10.3.0.51 to 10.3.0.100) goes to ISP1 and traffic from Dept. B (IP address range: 10.3.0.101 to 10.3.0.150) goes to ISP2. Normally, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-25 Load balancing networking in which the service interfaces work at Layer 3 and are upstream and downstream connected to switches

NOTE

In this example, interfaces 1, 2, 3, and 7 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.

   NOTE

   ISP1 and ISP2 are security zones that have been created.

   a. Choose **Network** > **Interface**.

   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	isp1
IPv4	
IP Address	1.1.1.1/24

   c. Repeat the preceding steps to configure **GE0/0/2**.

Zone	isp2

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	2.2.2.1/24

d. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

e. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	isp1
IPv4	
IP Address	1.1.1.2/24

   c. Repeat the preceding steps to configure **GE0/0/2**.

Zone	isp2
IPv4	
IP Address	2.2.2.2/24

   d. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.2/24

   e. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

IP Address	10.10.0.2/24

Step 2 Configure the routing function to ensure that routes are reachable.

Ensure consistent route configurations on DeviceA and DeviceB.

1. Choose **Network** > **Route** > **Intelligent Uplink Selection**.
2. On the **Intelligent Uplink Selection Policy** tab, click **Add** in the **Policy-based Route** list, configure a policy-based route (PBR) to ISP1 as follows, and click **OK**.

Name	route_policy_isp1
Type	Source Zone
Source Zone	trust
Source Address	10.3.0.51-10.3.0.100
Action	Forward
Egress Type	Single
Next Hop	1.1.1.254

3. Repeat the preceding steps and configure a PBR to ISP2.

Name	route_policy_isp2
Type	Source Zone
Source Zone	trust
Source Address	10.3.0.101-10.3.0.150
Action	Forward
Egress Type	Single
Next Hop	2.2.2.254

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

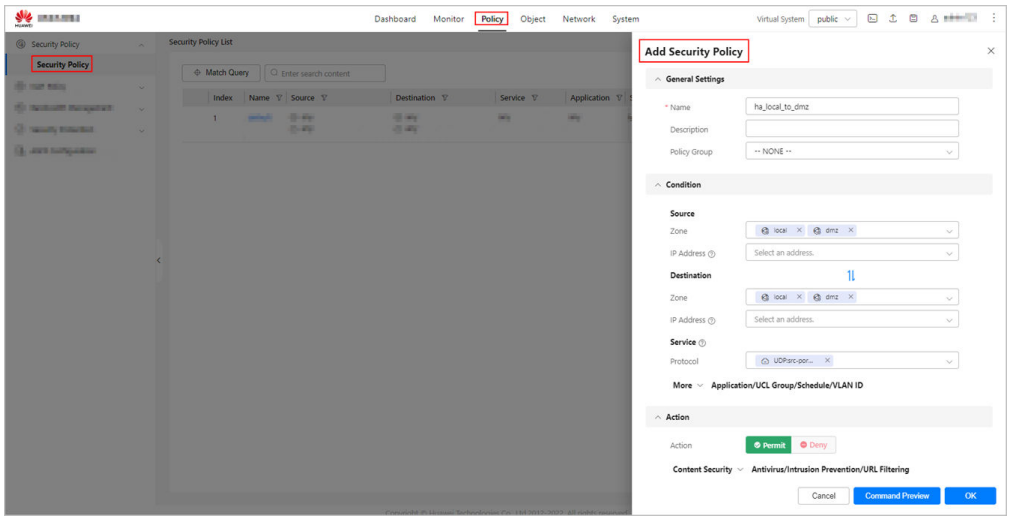
NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

 Copyright © Huawei Technologies Co., Ltd.

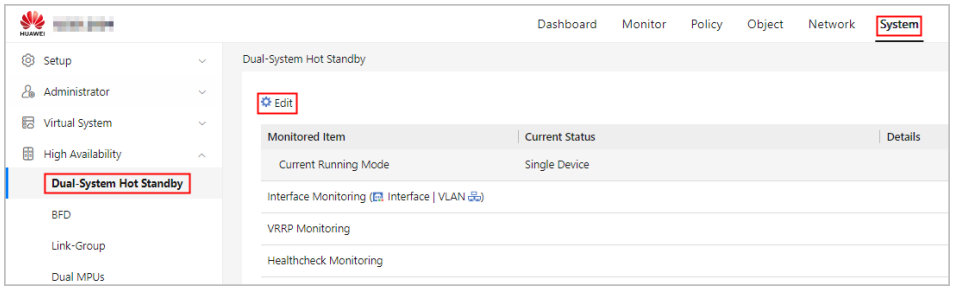
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.



Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

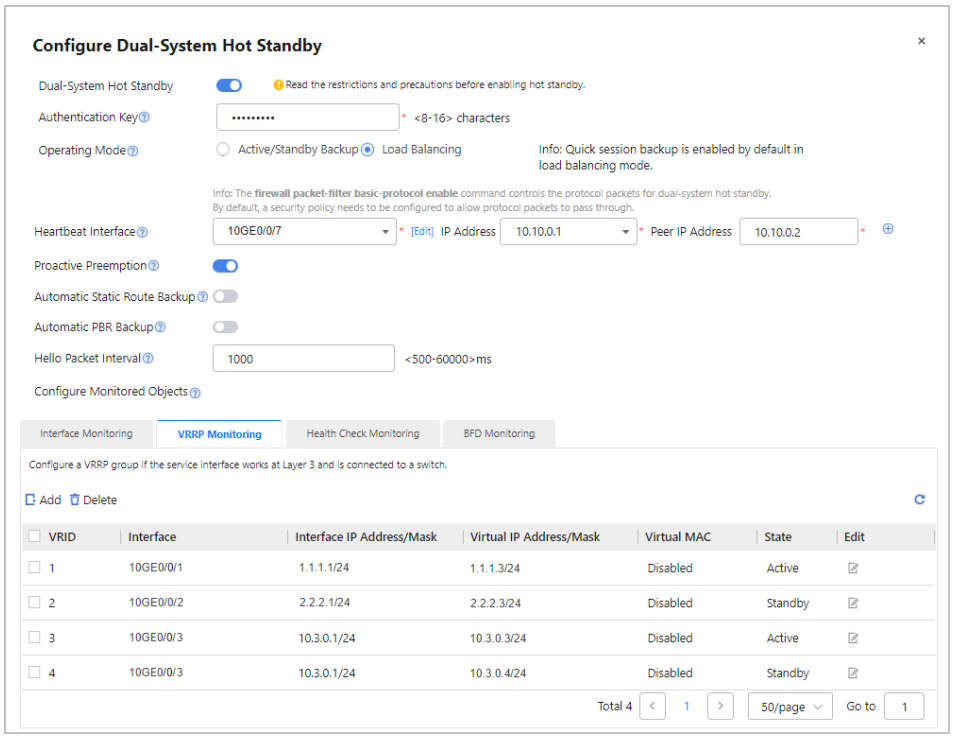
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.



   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

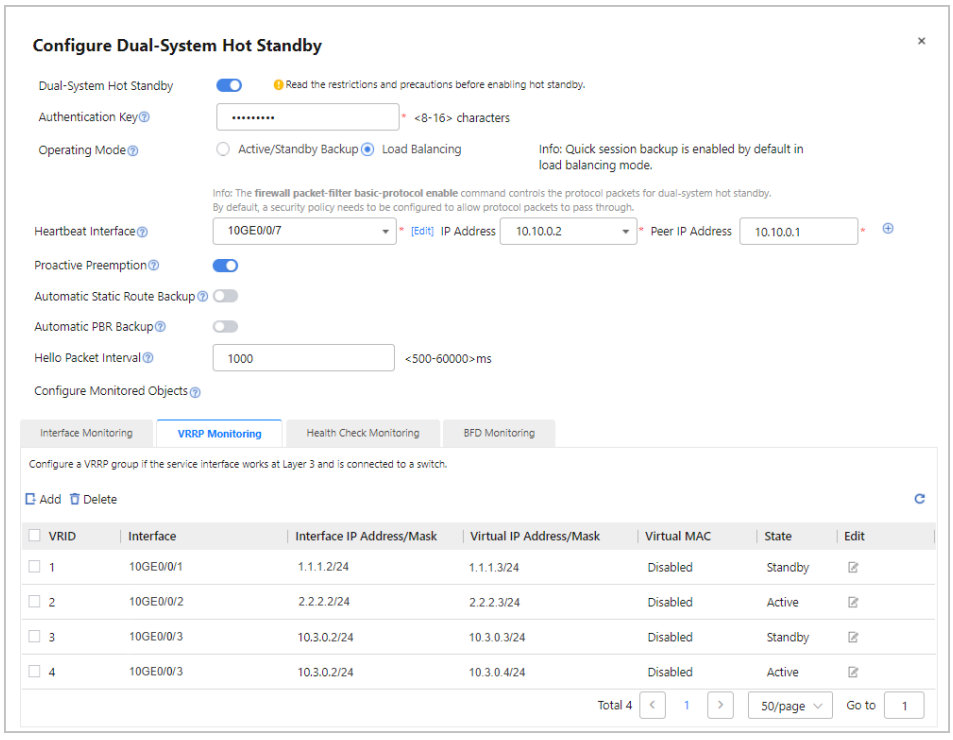
 Copyright © Huawei Technologies Co., Ltd.



2. Configure hot standby on DeviceB.

   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



Step 5 Configure a security policy.

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy on DeviceA to allow intranet users to access the Internet. After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

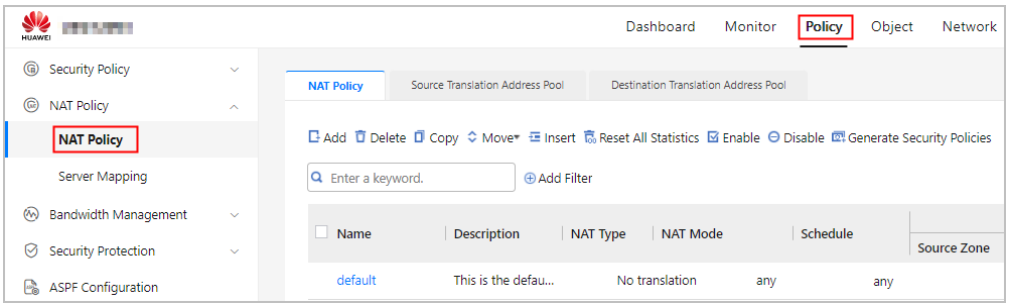
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

Name	policy_sec
Source Zone	trust
Destination Zone	isp1,isp2
Action	Permit

Step 6 Configure a NAT policy.

Configure a NAT policy on DeviceA to allow intranet users to access the Internet using the public IP address after NAT. After hot standby relationship is established, the NAT policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.



2. Click the **Source Translation Address Pool** tab, click **Add**, set the following parameters to configure NAT address pool 1, and click **OK**.

Name	1
IP Address Range	1.1.1.3-1.1.1.3

3. Repeat the preceding steps to configure NAT address pool 2.

Name	2
IP Address Range	2.2.2.3-2.2.2.3

4. Click the **NAT Policy** tab, click **Add**, set the following parameters to configure a NAT policy between the Trust zone and ISP1 zone, and click **OK**.

Name	policy_nat_1
NAT Type	NAT

 Copyright © Huawei Technologies Co., Ltd.

NAT Mode	Source address translation
Original Data Packet	
Source Zone	trust
Destination Type	Destination Zone: isp1
Translated Data Packet	
Source Address	Addresses in the IP Address Pool
Source Translation Address Pool	1

5. Repeat the preceding steps to configure a NAT policy between the Trust and ISP2 zones.

Name	policy_nat_2
NAT Type	NAT
NAT Mode	Source address translation
Original Data Packet	
Source Zone	trust
Destination Type	Destination Zone: isp2
Translated Data Packet	
Source Address	Addresses in the IP Address Pool
Source Translation Address Pool	2

Step 7 Configure default routes on the Intranet devices to set virtual IP address 10.3.0.3 of VRRP backup group 3 as the next hop for Dept. A and virtual IP address 10.3.0.4 of VRRP backup group 4 as the next hop for Dept. B.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.2
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 active
#
interface GE0/0/2
 ip address 2.2.2.1 255.255.255.0
 vrrp vrid 2 virtual-ip 2.2.2.3 standby
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 active
 vrrp vrid 4 virtual-ip 10.3.0.4 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone isp1
 set priority 10
 add interface GE0/0/1
#
firewall zone isp2
 set priority 15
 add interface GE0/0/2
#
 nat address-group 1
  section 0 1.1.1.3 1.1.1.3
 nat address-group 2
  section 0 2.2.2.3 2.2.2.3
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone isp1
  destination-zone isp2
  action permit
#
policy-based-route
 rule name route_policy_isp1
  source-zone trust
  source-address range 10.3.0.51 10.3.0.100
```

DeviceB

```
#
sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.1
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 standby
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 vrrp vrid 2 virtual-ip 2.2.2.3 active
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 standby
 vrrp vrid 4 virtual-ip 10.3.0.4 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone isp1
 set priority 10
 add interface GE0/0/1
#
firewall zone isp2
 set priority 15
 add interface GE0/0/2
#
 nat address-group 1
  section 0 1.1.1.3 1.1.1.3
 nat address-group 2
  section 0 2.2.2.3 2.2.2.3
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone isp1
  destination-zone isp2
  action permit
#
policy-based-route
 rule name route_policy_isp1
  source-zone trust
  source-address range 10.3.0.51 10.3.0.100
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action pbr next-hop 1.1.1.254 rule name route_policy_isp2 source-zone trust source-address range 10.3.0.101 10.3.0.150 action pbr next-hop 2.2.2.254 # nat-policy rule name policy_nat_1 source-zone trust destination-zone isp1 action source-nat address-group 1 rule name policy_nat_2 source-zone trust destination-zone isp2 action source-nat address-group 2	action pbr next-hop 1.1.1.254 rule name route_policy_isp2 source-zone trust source-address range 10.3.0.101 10.3.0.150 action pbr next-hop 2.2.2.254 # nat-policy rule name policy_nat_1 source-zone trust destination-zone isp1 action source-nat address-group rule name policy_nat_2 source-zone trust destination-zone isp2 action source-nat address-group 2

7.2.6 CLI: Example for Load Balancing Networking in Which the Devices Work as the Gateways and Multi-ISP Accesses Are Provided

Networking Requirements

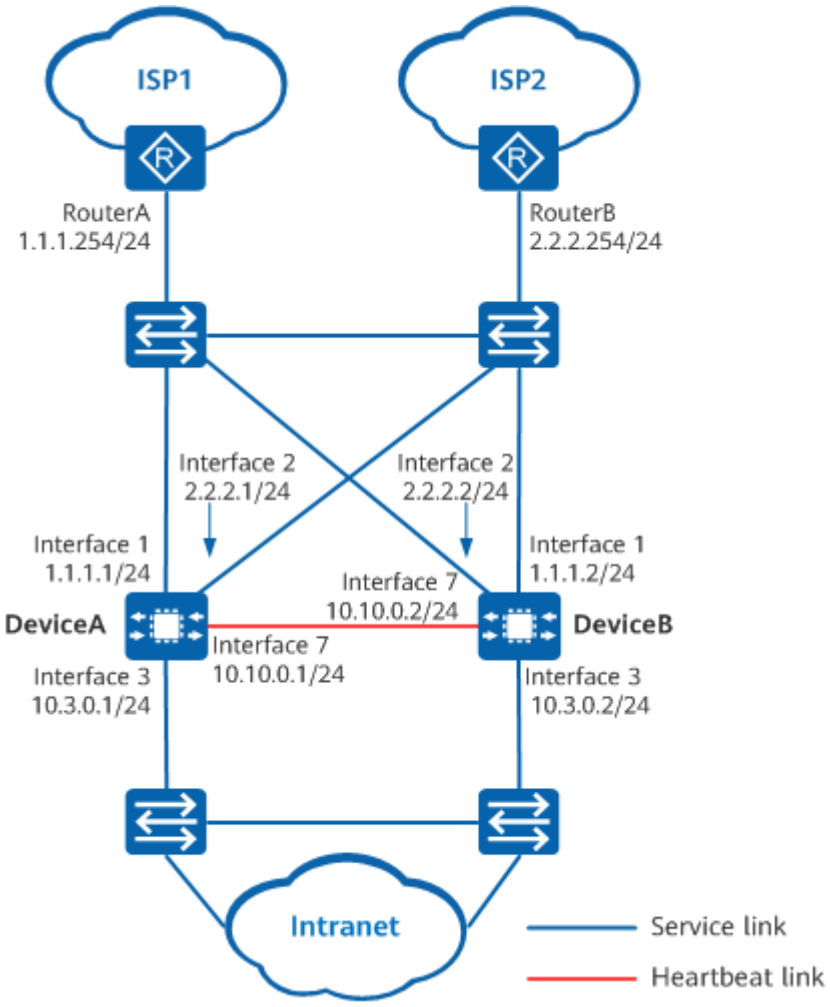
As shown in **Figure 7-26**, service interfaces of DeviceA and DeviceB work at Layer 3, having upstream and downstream connections to Layer-2 switches. The upstream two switches are connected to two ISPs. ISP1 assigns the IP addresses of 1.1.1.1, 1.1.1.2, and 1.1.1.3, and ISP2 assigns the IP addresses of 2.2.2.1, 2.2.2.2, and 2.2.2.3 to the enterprise. Now, DeviceA and DeviceB are supposed to work in load balancing mode so that traffic from Dept. A (IP address range: 10.3.0.51 to 10.3.0.100) goes to ISP1 and traffic from Dept. B (IP address range: 10.3.0.101 to 10.3.0.150) goes to ISP2. Normally, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-26 Load balancing networking in which the service interfaces work at Layer 3 and are upstream and downstream connected to switches

NOTE

In this example, interfaces 1, 2, 3, and 7 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set an IP address for each interface, assign interfaces to security zones, and complete basic parameter settings.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 1.1.1.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 2.2.2.1 24** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 1.1.1.2 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 2.2.2.2 24** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone name isp1** [DeviceA-zone-isp1] **set priority 10** [DeviceA-zone-isp1] **add interface ge 0/0/1** [DeviceA-zone-isp1] **quit** [DeviceA] **firewall zone name isp2** [DeviceA-zone-isp2] **set priority 15** [DeviceA-zone-isp2] **add interface ge 0/0/2** [DeviceA-zone-isp2] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone name isp1** [DeviceB-zone-isp1] **set priority 10** [DeviceB-zone-isp1] **add interface ge 0/0/1** [DeviceB-zone-isp1] **quit** [DeviceB] **firewall zone name isp2** [DeviceB-zone-isp2] **set priority 15** [DeviceB-zone-isp2] **add interface ge 0/0/2** [DeviceB-zone-isp2] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

Step 2 Configure PBR.

DeviceA	DeviceB
[DeviceA] **policy-based-route** [DeviceA-policy-pbr] **rule name route_policy_isp1** [DeviceA-policy-pbr-rule-route_policy_isp1] **source-zone trust** [DeviceA-policy-pbr-rule-route_policy_isp1] **source-address range 10.3.0.51 10.3.0.100** [DeviceA-policy-pbr-rule-route_policy_isp1] **action pbr next-hop 1.1.1.254** [DeviceA-policy-pbr-rule-route_policy_isp1] **quit** [DeviceA-policy-pbr] **rule name route_policy_isp2** [DeviceA-policy-pbr-rule-route_policy_isp2] **source-zone trust** [DeviceA-policy-pbr-rule-route_policy_isp2] **source-address range 10.3.0.101 10.3.0.150** [DeviceA-policy-pbr-rule-route_policy_isp2] **action pbr next-hop 2.2.2.254** [DeviceA-policy-pbr-rule-route_policy_isp2] **quit** [DeviceA-policy-pbr] **quit**	[DeviceB] **policy-based-route** [DeviceB-policy-pbr] **rule name route_policy_isp1** [DeviceB-policy-pbr-rule-route_policy_isp1] **source-zone trust** [DeviceB-policy-pbr-rule-route_policy_isp1] **source-address range 10.3.0.51 10.3.0.100** [DeviceB-policy-pbr-rule-route_policy_isp1] **action pbr next-hop 1.1.1.254** [DeviceB-policy-pbr-rule-route_policy_isp1] **quit** [DeviceB-policy-pbr] **rule name route_policy_isp2** [DeviceB-policy-pbr-rule-route_policy_isp2] **source-zone trust** [DeviceB-policy-pbr-rule-route_policy_isp2] **source-address range 10.3.0.101 10.3.0.150** [DeviceB-policy-pbr-rule-route_policy_isp2] **action pbr next-hop 2.2.2.254** [DeviceB-policy-pbr-rule-route_policy_isp2] **quit** [DeviceB-policy-pbr] **quit**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Configure hot standby.

DeviceA	DeviceB
# Configure VRRP group 1 on GE0/0/1 on DeviceA and set the status of VRRP group 1 to Active. Configure VRRP group 1 on GE0/0/1 on DeviceB and set the status of VRRP group 1 to Standby.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.3 active** [DeviceA-GE0/0/1] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.3 standby** [DeviceB-GE0/0/1] **quit**
# Configure VRRP group 2 on GE0/0/2 on DeviceA and set the status of VRRP group 2 to Standby. Configure VRRP group 2 on GE0/0/2 on DeviceB and set the status of VRRP group 2 to Active.	
[DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **vrrp vrid 2 virtual-ip 2.2.2.3 standby** [DeviceA-GE0/0/2] **quit**	[DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **vrrp vrid 2 virtual-ip 2.2.2.3 active** [DeviceB-GE0/0/2] **quit**
# Configure VRRP groups 3 and 4 on GE0/0/3 on DeviceA and set the status of VRRP group 3 to Active and status of VRRP group 4 to Standby. Configure VRRP group 3 and 4 on GE0/0/3 on DeviceB and set the status of VRRP group 3 to Standby and status of VRRP group 4 to Active.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 3 virtual-ip 10.3.0.3 active** [DeviceA-GE0/0/3] **vrrp vrid 4 virtual-ip 10.3.0.4 standby** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 3 virtual-ip 10.3.0.3 standby** [DeviceB-GE0/0/3] **vrrp vrid 4 virtual-ip 10.3.0.4 active** [DeviceB-GE0/0/3] **quit**
# Configure quick session backup on DeviceA and DeviceB in case of inconsistent forward and return packet paths.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Configure a security policy.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec
[DeviceA-policy-security-rule-policy_sec] source-zone trust
[DeviceA-policy-security-rule-policy_sec] destination-zone isp1 isp2
[DeviceA-policy-security-rule-policy_sec] action permit
[DeviceA-policy-security-rule-policy_sec] quit
[DeviceA-policy-security] quit
```

Step 6 Configure a NAT policy to allow intranet users to access the Internet by using the public IP address after NAT.

After hot standby relationship is established, NAT policies configured on DeviceA are automatically backed up to DeviceB.

Configure IP address pools.

```
HRP_M[DeviceA] nat address-group 1
HRP_M[DeviceA-address-group-1] section 0 1.1.1.3 1.1.1.3
HRP_M[DeviceA-address-group-1] quit
HRP_M[DeviceA] nat address-group 2
HRP_M[DeviceA-address-group-2] section 0 2.2.2.3 2.2.2.3
HRP_M[DeviceA-address-group-2] quit
```

Configure NAT policies.

```
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat_1
HRP_M[DeviceA-policy-nat-rule-policy_nat_1] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat_1] destination-zone isp1
HRP_M[DeviceA-policy-nat-rule-policy_nat_1] action source-nat address-group 1
HRP_M[DeviceA-policy-nat-rule-policy_nat_1] quit
HRP_M[DeviceA-policy-nat] rule name policy_nat_2
HRP_M[DeviceA-policy-nat-rule-policy_nat_2] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat_2] destination-zone isp2
HRP_M[DeviceA-policy-nat-rule-policy_nat_2] action source-nat address-group 2
HRP_M[DeviceA-policy-nat-rule-policy_nat_2] quit
HRP_M[DeviceA-policy-nat] quit
```

Step 7 Configure default routes on intranet devices. Set the next-hop address of the default route to the virtual IP address (10.3.0.3) of VRRP group 3 for a PC of department A and the virtual IP address (10.3.0.4) of VRRP group 4 for a PC of department B.

----End

Verifying the Configuration

1. Run the **display vrrp** command on DeviceA and DeviceB to check the status of the interfaces in the VRRP group.
2. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

3. Department A's PC in the trust zone can successfully ping 1.1.1.254 in ISP1, and department B's PC in the trust zone can successfully ping 2.2.2.254 in ISP2. Run the **display firewall session table** command on DeviceA and DeviceB to check the session. If a session exists on one device and the corresponding session with the Remote flag exists on the other device, hot standby load balancing is configured successfully.
4. When DeviceA or DeviceB is faulty, traffic can be switched to the other device and forwarded to the corresponding ISP, ensuring service continuity.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.2
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 active
#
interface GE0/0/2
 ip address 2.2.2.1 255.255.255.0
 vrrp vrid 2 virtual-ip 2.2.2.3 standby
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 active
 vrrp vrid 4 virtual-ip 10.3.0.4 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone isp1
 set priority 10
 add interface GE0/0/1
#
firewall zone isp2
 set priority 15
 add interface GE0/0/2
#
 nat address-group 1
  section 0 1.1.1.3 1.1.1.3
 nat address-group 2
  section 0 2.2.2.3 2.2.2.3
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone isp1
  destination-zone isp2
  action permit
#
policy-based-route
 rule name route_policy_isp1
  source-zone trust
  source-address range 10.3.0.51 10.3.0.100
```

DeviceB

```
#
sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.1
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 standby
#
interface GE0/0/2
 ip address 2.2.2.2 255.255.255.0
 vrrp vrid 2 virtual-ip 2.2.2.3 active
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 standby
 vrrp vrid 4 virtual-ip 10.3.0.4 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone isp1
 set priority 10
 add interface GE0/0/1
#
firewall zone isp2
 set priority 15
 add interface GE0/0/2
#
 nat address-group 1
  section 0 1.1.1.3 1.1.1.3
 nat address-group 2
  section 0 2.2.2.3 2.2.2.3
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone isp1
  destination-zone isp2
  action permit
#
policy-based-route
 rule name route_policy_isp1
  source-zone trust
  source-address range 10.3.0.51 10.3.0.100
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action pbr next-hop 1.1.1.254 rule name route_policy_isp2 source-zone trust source-address range 10.3.0.101 10.3.0.150 action pbr next-hop 2.2.2.254 # nat-policy rule name policy_nat_1 source-zone trust destination-zone isp1 action source-nat address-group 1 rule name policy_nat_2 source-zone trust destination-zone isp2 action source-nat address-group 2	action pbr next-hop 1.1.1.254 rule name route_policy_isp2 source-zone trust source-address range 10.3.0.101 10.3.0.150 action pbr next-hop 2.2.2.254 # nat-policy rule name policy_nat_1 source-zone trust destination-zone isp1 action source-nat address-group rule name policy_nat_2 source-zone trust destination-zone isp2 action source-nat address-group 2

7.2.7 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions

Networking Requirements

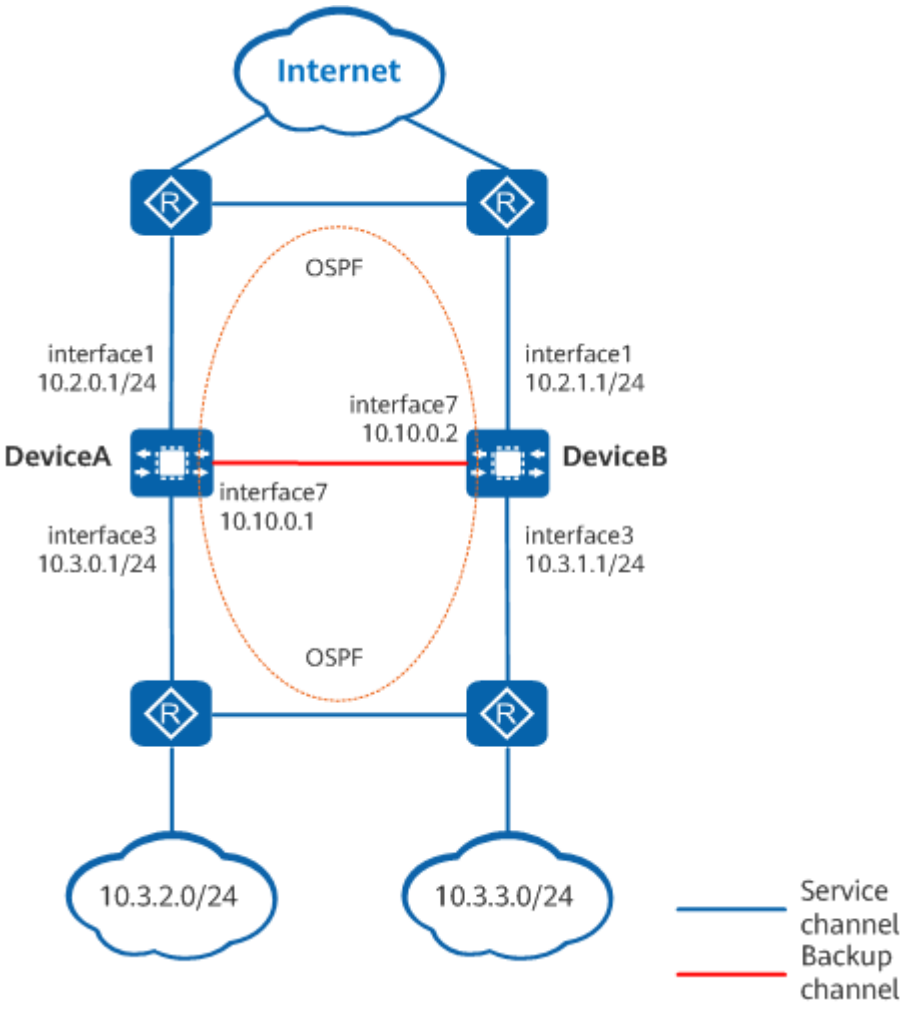
As shown in **Figure 7-27**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers. OSPF runs between the devices and routers. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-27 Load sharing networking where service interfaces work at Layer 3 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Repeat the preceding steps to configure **GE0/0/3.**

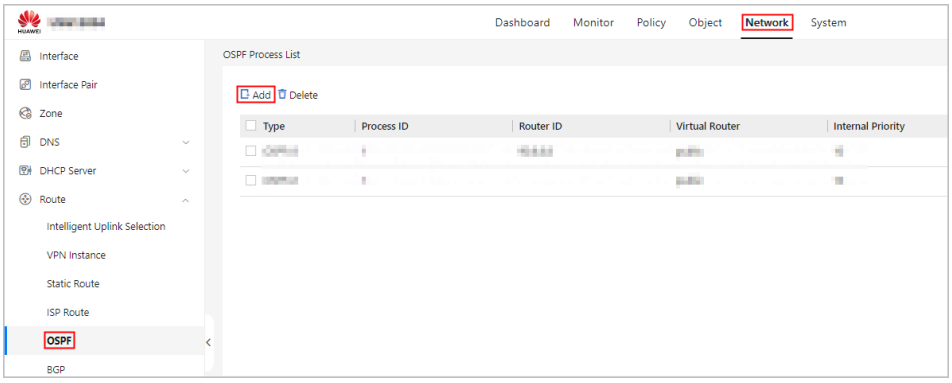
Zone	trust
IPv4	
IP Address	10.3.1.1/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF to ensure IP connectivity.

1. Configure OSPF on DeviceA.
   a. Choose **Network** > **Route** > **OSPF** and click **Add**.



   b. Create an OSPF process, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Type	OSPFv2
Process ID	10

c. Click , click **Add**, create an OSPF area and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.0.0
Mask/Wildcard Mask	255.255.255.0

d. Choose **Basic Configuration** > **Network Settings**, click **Add**, create a network and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

2. Configure OSPF on DeviceB.

a. Choose **Network** > **Route** > **OSPF** and click **Add**.

b. Create an OSPF process, set the parameters as follows, and click **OK**.

Type	OSPFv2
Process ID	10

c. Click , click **Add**, create an OSPF area and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.1.0
Mask/Wildcard Mask	255.255.255.0

d. Choose **Basic Configuration** > **Network Settings**, click **Add**, create a network and set the parameters as follows, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.1.0

 Copyright © Huawei Technologies Co., Ltd.

Mask/Wildcard Mask	255.255.255.0

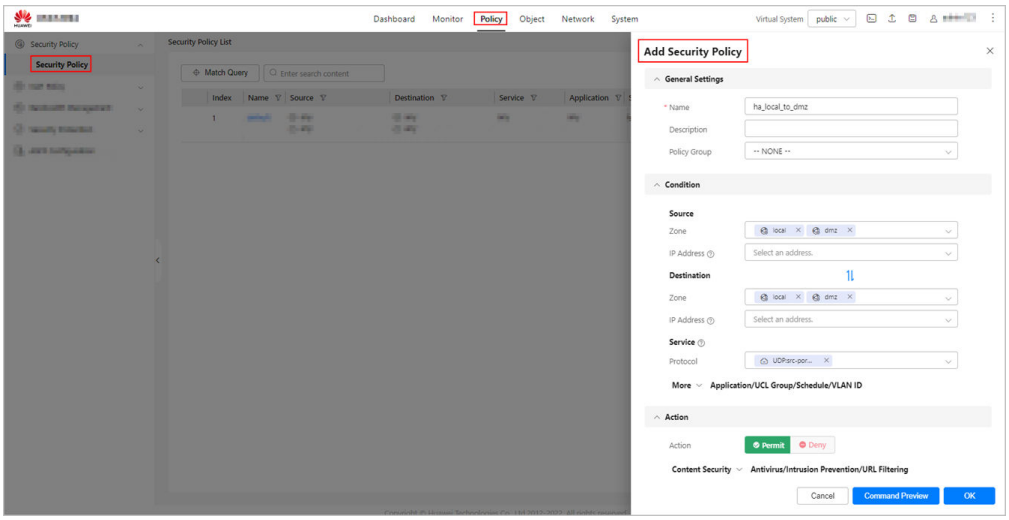
Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

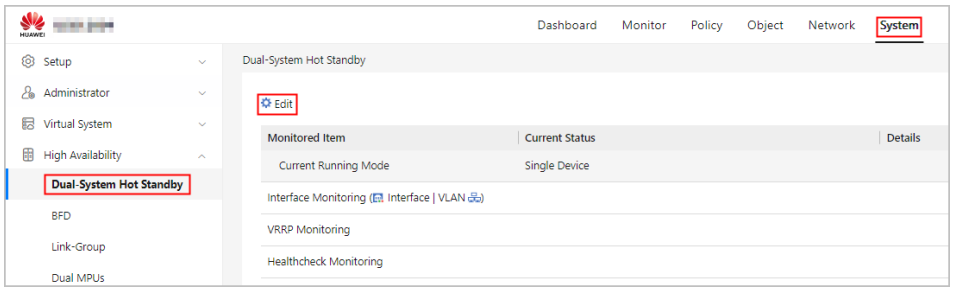


Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

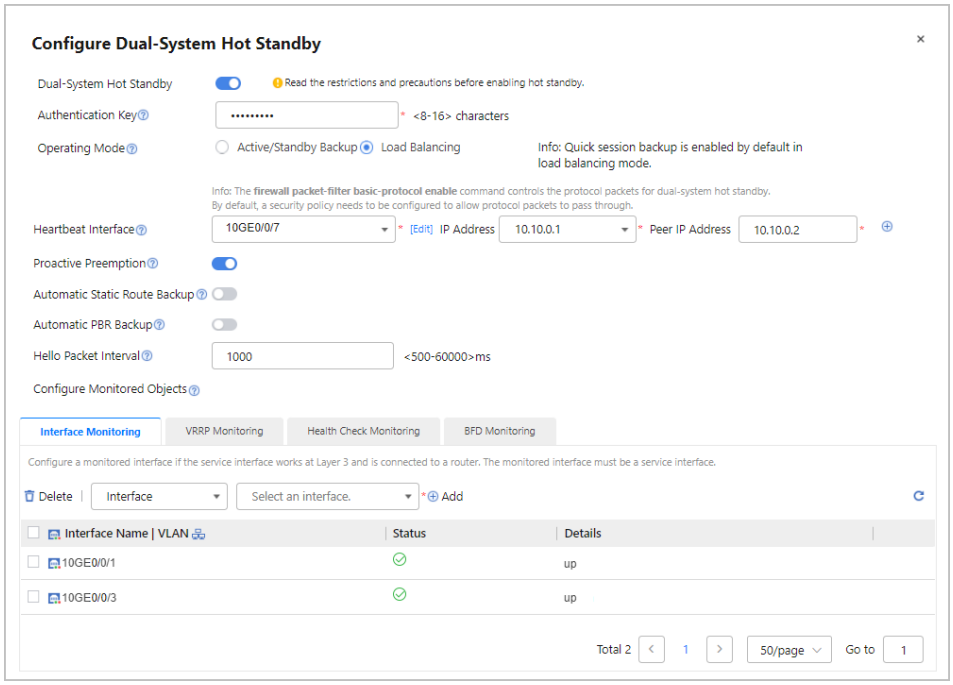
Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

 Copyright © Huawei Technologies Co., Ltd.

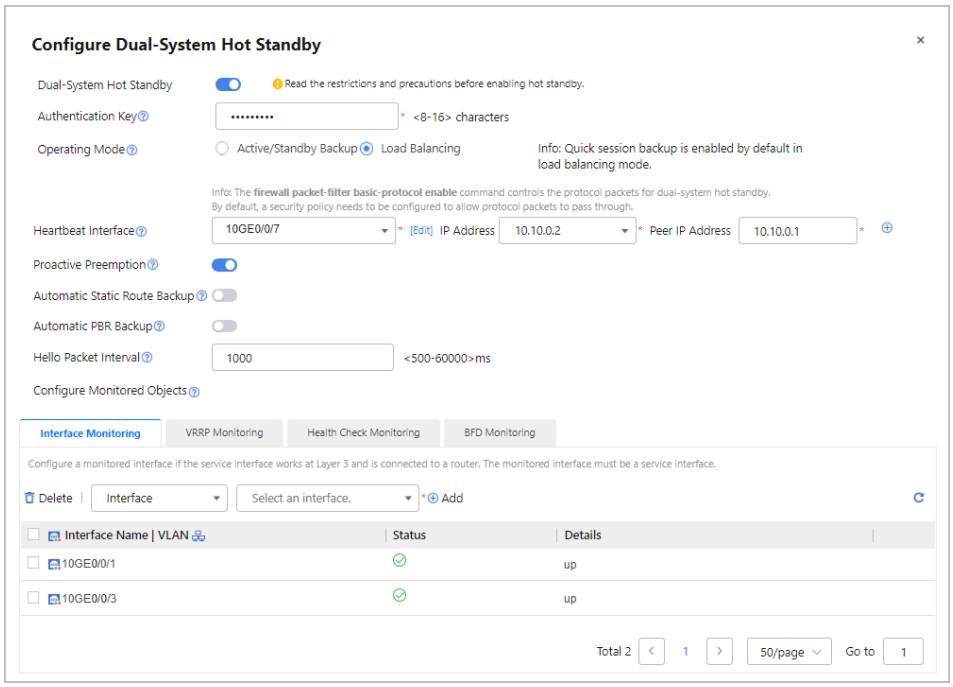


b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 Configure the security policies.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure security policies and set the parameters as follows, and then click **OK**.

   # Configure security policies to allow the devices and the upstream/downstream routers to exchange OSPF packets.

   NOTE

   Controlling function of security policies for OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, OSPF packets are controlled by security policies. In this case, a security policy must be configured between the security zones where the upstream/downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_ospf_1
Source Zone	local
Destination Zone	trust,untrust
Service	ospf
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Name	policy_ospf_2
Source Zone	trust,untrust
Destination Zone	local
Service	ospf
Action	Permit

Configure a security policy to allow intranet users to access the Internet.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Service	10.3.2.0/24,10.3.3.0/24
Action	Permit

Step 6 Configure the routers.

Configure OSPF on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 24
  source-address 10.3.3.0 24
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 24
  source-address 10.3.3.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action permit #	action permit #

7.2.8 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers in Upstream and Downstream Directions

Networking Requirements

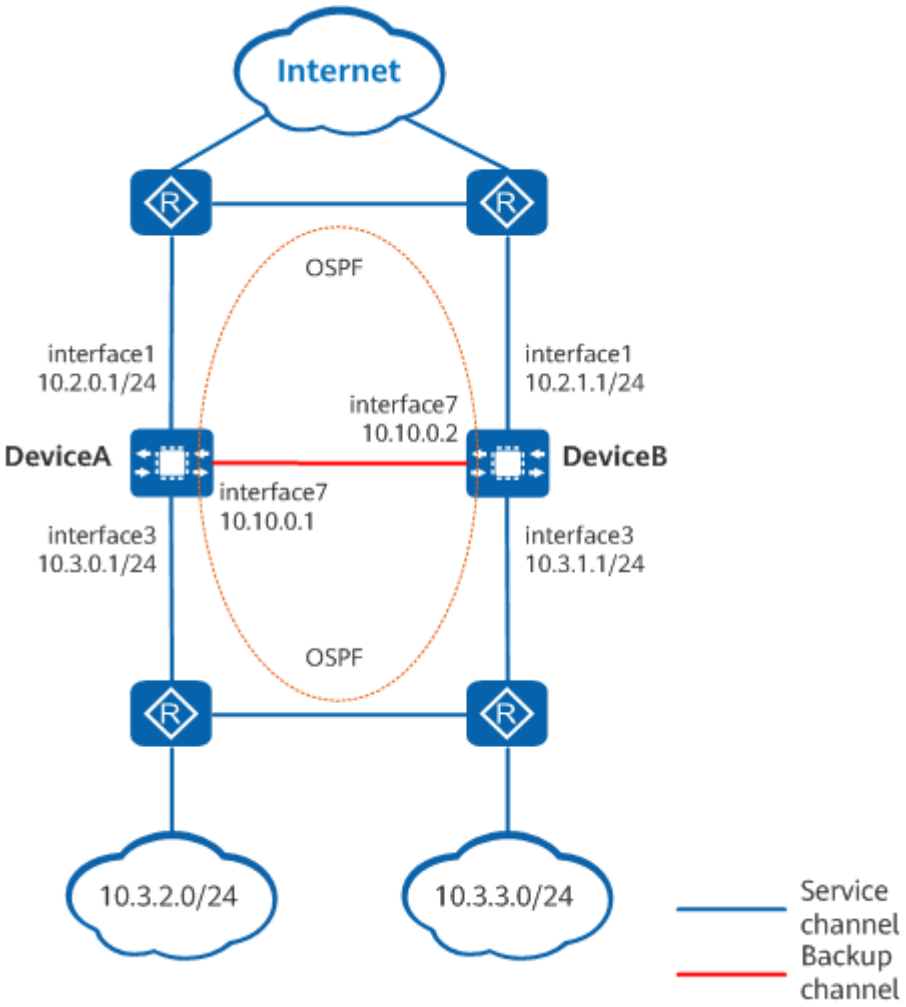
As shown in **Figure 7-28**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers. OSPF runs between the devices and routers. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-28 Load sharing networking where service interfaces work at Layer 3 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Configure a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow devices and upstream and downstream routers to exchange OSPF packets.

NOTE

OSPF packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPF packets are controlled by security policies. As such, a security policy must be configured between the security zone where the upstream and downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.3.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
```

Step 5 Configure routers.

Configure OSPF on the four routers to advertise routes. For configuration commands, see related documents of the routers.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 24
  source-address 10.3.3.0 24
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.2.0 24
  source-address 10.3.3.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

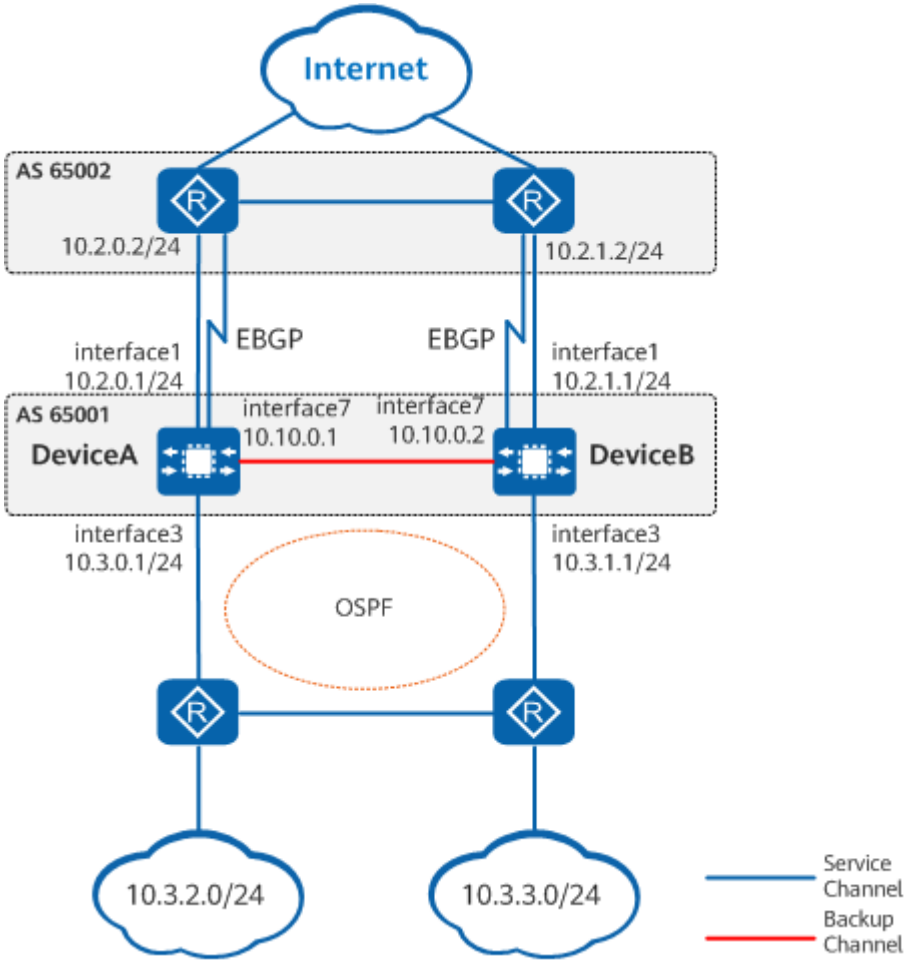
DeviceA	DeviceB
action permit #	action permit #

7.2.9 Web: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively

Networking Requirements

On the network shown in **Figure 7-29**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers through EBGP and OSPF respectively. DeviceA and DeviceB are expected to work in load balancing mode. In normal cases, traffic is forwarded by DeviceA and DeviceB together. When one of the devices fails, all services are forwarded by the other device to ensure service continuity.

Figure 7-29 Load balancing networking where service interfaces work at Layer 3 and connect to upstream and downstream routers



Procedure

Step 1 Set IP addresses for interfaces, and add the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click GE0/0/1, set the following parameters, and then click **OK**.

Security Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to set parameters for GE0/0/3.

Security Zone	trust
IPv4	
IP Address	10.3.0.1/24

   d. Repeat the preceding steps to set parameters for GE0/0/7.

Security Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click GE0/0/1, set parameters, and then click **OK**.

Security Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Repeat the preceding steps to set parameters for GE0/0/3.

Security Zone	trust
IPv4	
IP Address	10.3.1.1/24

   d. Repeat the preceding steps to set parameters for GE0/0/7.

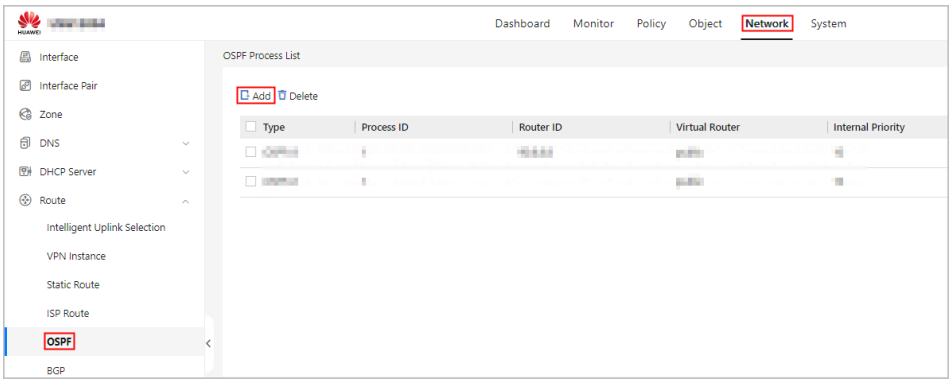
Security Zone	dmz

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF to ensure that the routes to the downstream routers are reachable.

1. Configure OSPF on DeviceA.
   a. Choose **Network** > **Route** > **OSPF**, and click **Add**.



   b. Set the following parameters for OSPF, and then click **OK**.

Type	OSPFv2
Process ID	10

   c. Click and choose **Area Settings**. In **Area List**, click **Add**, set the following parameters to create an area, and then click **OK**.

Area	0.0.0.0
Network Segment IP Address	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

   d. Click and choose **Route Import**. In **Route List**, click **Add**, set the type of the imported route to BGP, and then click **OK**.
2. Configure OSPF on DeviceB.
   a. Choose **Network** > **Route** > **OSPF**, click **Add**, set the following parameter for OSPF, and then click **OK**.

Type	OSPFv2
Process ID	10

   b. Click and choose **Area Settings**. In **Area List**, click **Add**, set the following parameters to create an area, and then click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

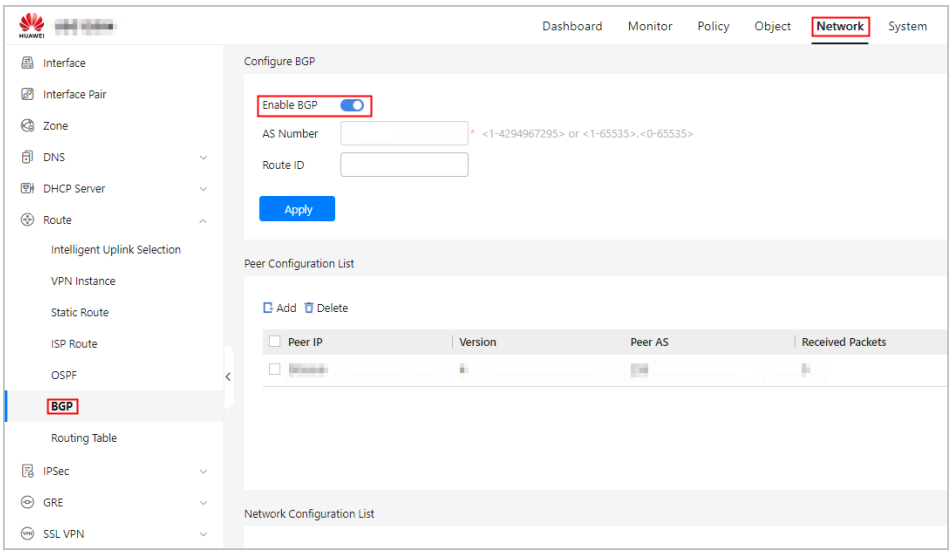
Zone	0.0.0.0
Network Segment IP Address	10.3.1.0
Mask/Wildcard Mask	255.255.255.0

c. Click and choose **Route Import**. In **Route List**, click **Add**, set the type of the imported route to BGP, and then click **OK**.

Step 3 Configure EBGP to ensure that the routes to the upstream routers are reachable. Assume that DeviceA and DeviceB belong to AS 65001 and that the upstream routers belong to AS 65002.

1. Configure EBGP on DeviceA.

a. Choose **Network** > **Route** > **BGP**, and click **Enable BGP**.



b. Set BGP **AS Number** to 65001 and **Route ID** to 10.2.0.1.

c. In **Peer Configuration List**, click **Add**, set the following parameters to add a peer relationship, and then click **OK**.

Peer IP	10.2.0.2
Peer AS	65002
Maximum EBGP Connection Hops	2

d. In **Network Configuration List**, click **Add**, enter the IP address and mask (10.2.0.1/24) of the route to be added to the BGP routing table, and then click **OK**.

e. In **Route List**, click **Add**, set the following parameters to import routes, and then click **OK**.

Protocol Type	OSPF

 Copyright © Huawei Technologies Co., Ltd.

Process ID	10

2. Configure EBGP on DeviceB.
   a. Choose **Network** > **Route** > **BGP**, and click **Enable BGP**.
   b. Set BGP **AS Number** to 65001 and **Route ID** to 10.2.1.1.
   c. In **Peer Configuration List**, click **Add**, set the following parameters to add a peer relationship, and then click **OK**.

Peer IP	10.2.1.2
Peer AS	65002
Maximum EBGP Connection Hops	2

   d. In **Network Configuration List**, click **Add**, enter the IP address and mask 10.2.1.1/24 of the route to be added to the BGP routing table, and then click **OK**.
   e. In **Route List**, click **Add**, set the following parameters to import routes, and then click **OK**.

Protocol Type	OSPF
Process ID	10

Step 4 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

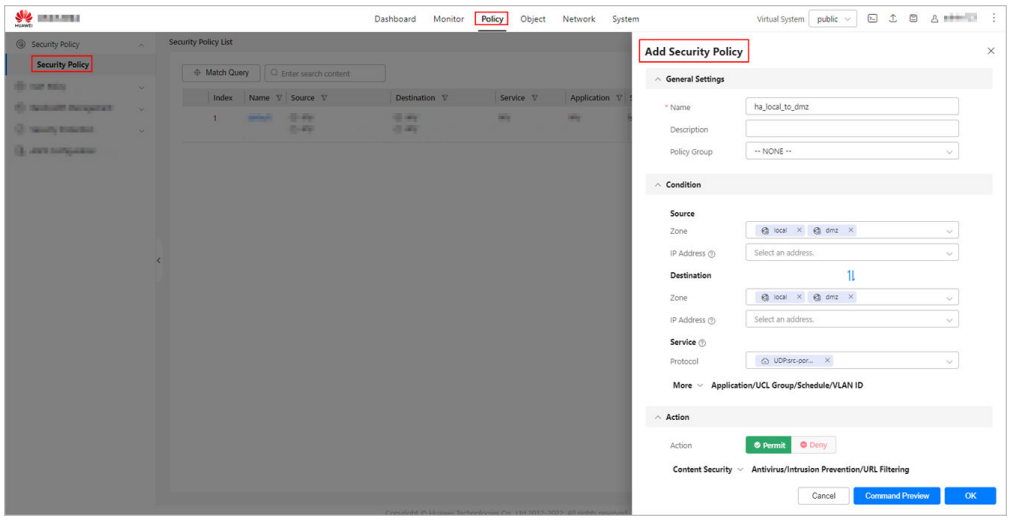
NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

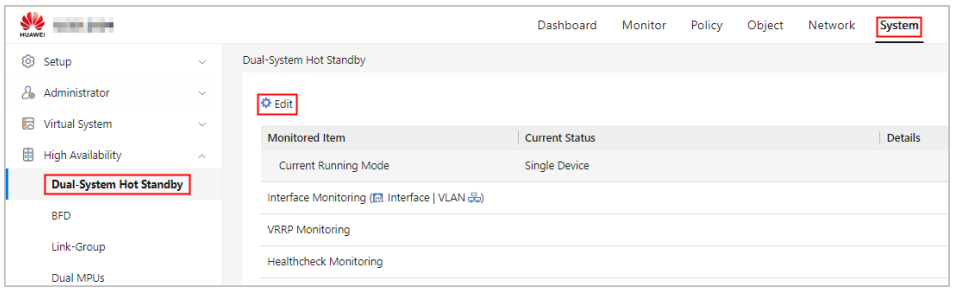
 Copyright © Huawei Technologies Co., Ltd.



Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

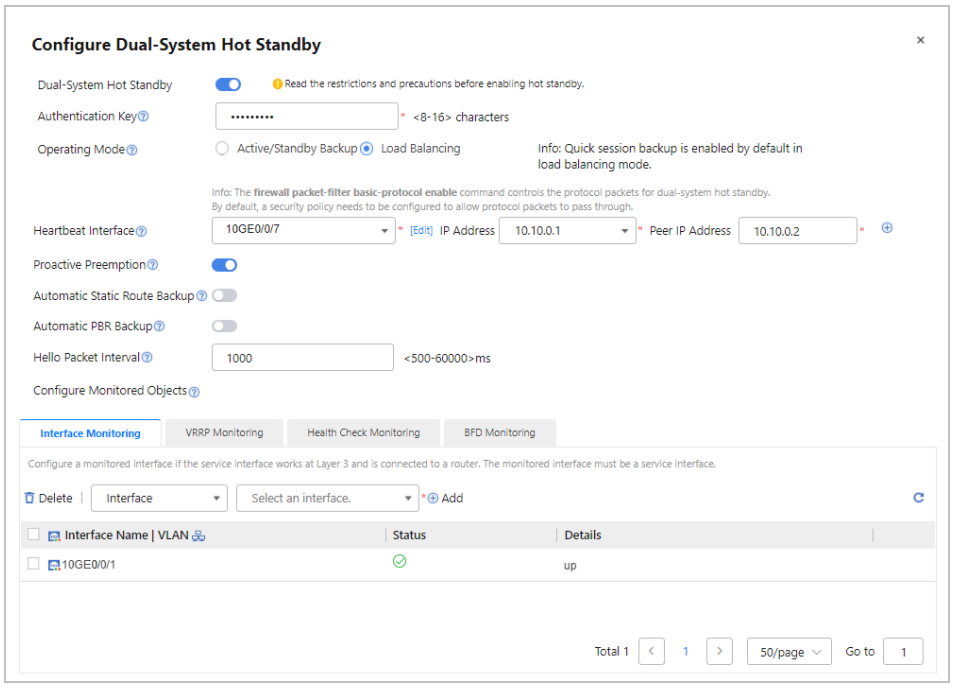
Step 5 Configure hot standby.

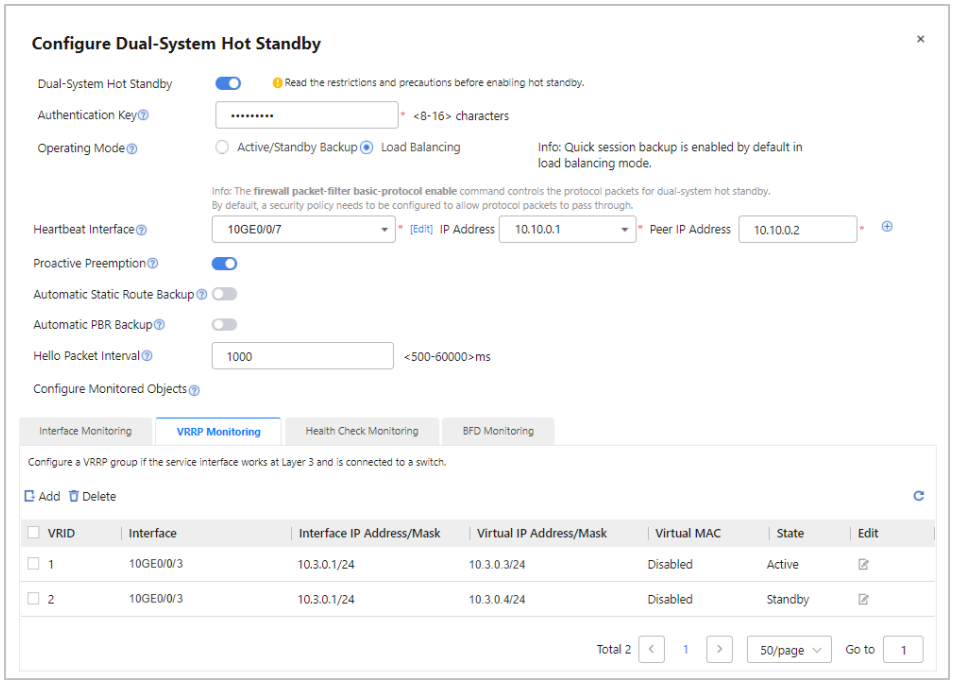
1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.



   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

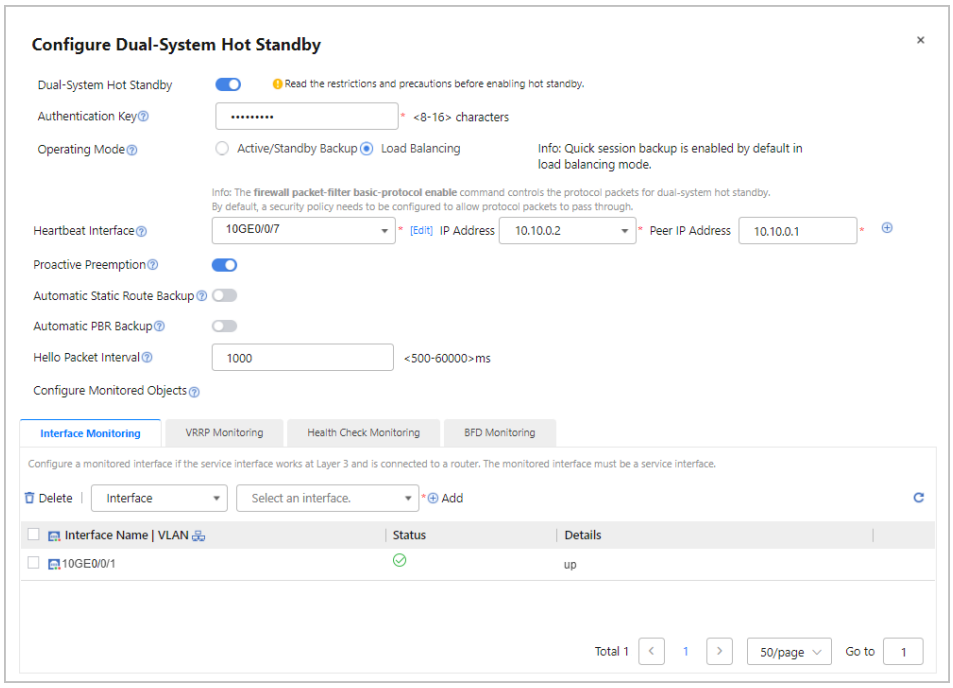
 Copyright © Huawei Technologies Co., Ltd.

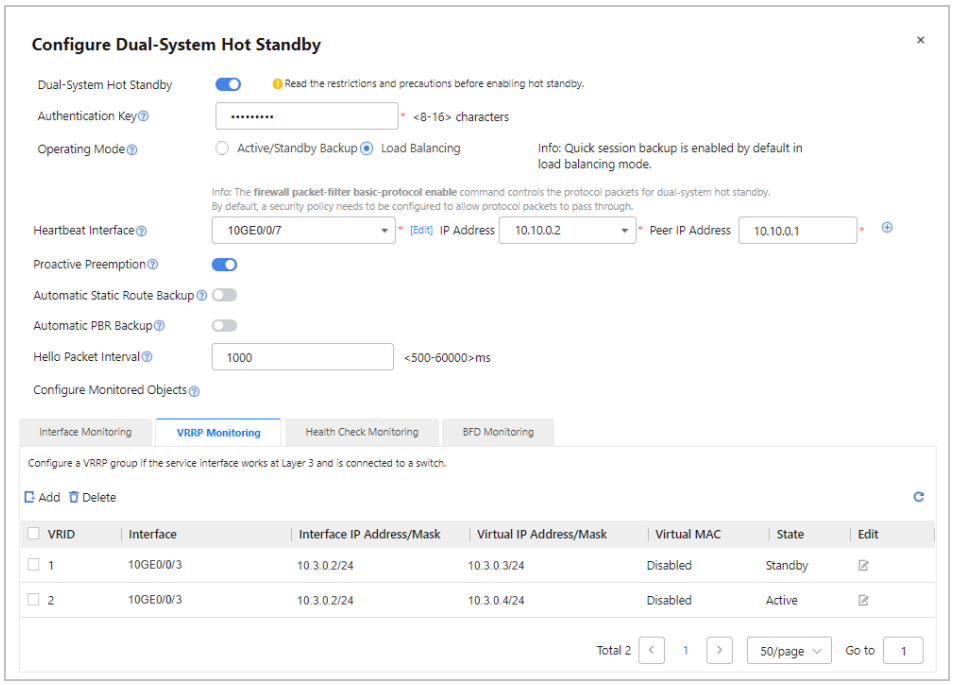




2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.





Step 6 Configure a security policy.

After the dual-system hot standby relationship is established, the security policies configured on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy List**.
2. Click **Add Security Policy**, set the following security policy parameters, and then click **OK**.

   # Configure security policies to allow the device to exchange OSPF packets with the downstream router and BGP messages with the upstream router.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Controlling function of security policies for BGP and OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command is enabled. That is, BGP and OSPF packets are controlled by security policies. In this case, a security policy must be configured between the local zone and the security zone where the outbound interface resides to allow BGP and OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_ospf_1
Source Zone	local
Destination Zone	trust
Destination Address	10.3.0.0/24,10.3.1.0/24
Service	ospf
Action	Permit

Name	policy_ospf_2
Source Zone	trust
Destination Zone	local
Source Address	10.3.0.0/24,10.3.1.0/24
Service	ospf
Action	Permit

Name	policy_bgp_1
Source Zone	local
Destination Zone	untrust
Destination Address	10.2.0.2/24,10.2.1.2/24
Service	bgp
Action	Permit

Name	policy_bgp_2
Source Zone	untrust
Destination Zone	local

 Copyright © Huawei Technologies Co., Ltd.

Source Address	10.2.0.2/24,10.2.1.2/24
Service	bgp
Action	Permit

Configure a security policy to allow intranet users to access the external network.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.0/24,10.3.3.0/24
Action	Permit

Step 7 Configure routers.

Configure OSPF on the downstream routers and BGP on the upstream routers to advertise neighboring network segments. For configuration commands, refer to the related router documents.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.2
 hrp mirror session enable
 hrp track interface GE0/0/1
 hrp track interface GE0/0/3
 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.0.0 0.0.0.255
#
bgp 65001
 router-id 10.2.0.1
 peer 10.2.0.2 as-number 65002
 peer 10.2.0.2 ebgp-max-hop 2
 ipv4-family unicast
  network 10.2.0.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  destination-zone local
  source-address 10.3.0.0 mask 255.255.255.0
```

DeviceB

```
#
sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.1
 hrp mirror session enable
 hrp track interface GE0/0/1
 hrp track interface GE0/0/3
 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
#
bgp 65001
 router-id 10.2.1.1
 peer 10.2.1.2 as-number 65002
 peer 10.2.1.2 ebgp-max-hop 2
 ipv4-family unicast
  network 10.2.1.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  destination-zone local
  source-address 10.3.0.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 24 destination-address 10.2.1.2 24 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 24 source-address 10.2.1.2 24 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 source-address 10.3.3.0 24 action permit #	source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 24 destination-address 10.2.1.2 24 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 24 source-address 10.2.1.2 24 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 source-address 10.3.3.0 24 action permit #

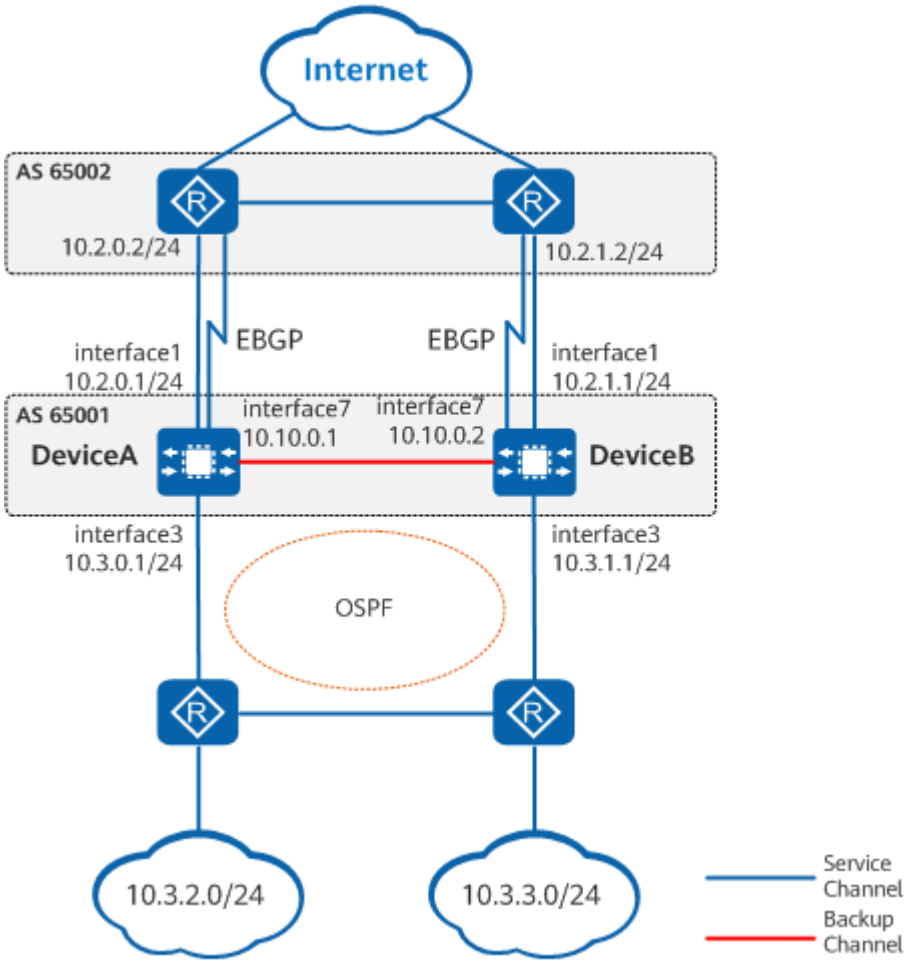
7.2.10 CLI: Example for Deploying Devices in In-Path Mode and Connecting to Upstream and Downstream Routers Through EBGP and OSPF Respectively

Networking Requirements

On the network shown in **Figure 7-30**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers through EBGP and OSPF respectively. DeviceA and DeviceB are expected to work in load balancing mode. In normal cases, traffic is forwarded by DeviceA and DeviceB together. When one of the devices fails, all services are forwarded by the other device to ensure service continuity.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-30 Load balancing networking where service interfaces work at Layer 3 and connect to upstream and downstream routers



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set an IP address for each interface on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Add the interfaces on DeviceA and DeviceB to security zones.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF on DeviceA and DeviceB and establish neighbor relationships with the downstream routers to ensure route reachability.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **import-route bgp** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceA-ospf-10] **import-route bgp** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**
# Configure EBGP on DeviceA and DeviceB to establish EBGP peer relationships with the upstream routers. Assume that DeviceA and DeviceB belong to AS 65001 and that the upstream routers belong to AS 65002.	
[DeviceA] **bgp 65001** [DeviceA-bgp] **router-id 10.2.0.1** [DeviceA-bgp] **peer 10.2.0.2 as-number 65002** [DeviceA-bgp] **peer 10.2.0.2 ebgp-max-hop 2** [DeviceA-bgp] **ipv4-family unicast** [DeviceA-bgp-af-ipv4] **network 10.2.0.1 24** [DeviceA-bgp-af-ipv4] **import-route ospf 10** [DeviceA-bgp-af-ipv4] **quit** [DeviceA-bgp] **quit**	[DeviceB] **bgp 65001** [DeviceB-bgp] **router-id 10.2.1.1** [DeviceB-bgp] **peer 10.2.1.2 as-number 65002** [DeviceB-bgp] **peer 10.2.1.2 ebgp-max-hop 2** [DeviceB-bgp] **ipv4-family unicast** [DeviceB-bgp-af-ipv4] **network 10.2.1.1 24** [DeviceA-bgp-af-ipv4] **import-route ospf 10** [DeviceB-bgp-af-ipv4] **quit** [DeviceB-bgp] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure dual-system hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# In load balancing networking, configure quick session backup on DeviceA and DeviceB to ensure round-trip forwarding path consistency.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface and device role, configure the authentication key, and enable dual-system hot standby on DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Configure security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow the device to exchange OSPF packets with the downstream router and BGP messages with the upstream router.

NOTE

Controlling function of security policies for BGP and OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command is enabled. That is, BGP and OSPF packets are controlled by security policies. In this case, a security policy must be configured between the local zone and the security zone where the outbound interface resides to allow BGP and OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
HRP_M[DeviceA-policy-security] rule name policy_bgp_1
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] destination-address 10.2.0.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] destination-address 10.2.1.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] service bgp
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_bgp_1] quit
HRP_M[DeviceA-policy-security] rule name policy_bgp_2
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] source-address 10.2.0.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] source-address 10.2.1.2 24
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] service bgp
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_bgp_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.3.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers.

Configure OSPF on the downstream routers and BGP on the upstream routers to advertise neighboring network segments. For configuration commands, refer to the related router documents.

----End

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the dual-system hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.2
 hrp mirror session enable
 hrp track interface GE0/0/1
 hrp track interface GE0/0/3
 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.0.0 0.0.0.255
#
bgp 65001
 router-id 10.2.0.1
 peer 10.2.0.2 as-number 65002
 peer 10.2.0.2 ebgp-max-hop 2
 ipv4-family unicast
  network 10.2.0.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  destination-zone local
  source-address 10.3.0.0 mask 255.255.255.0
```

DeviceB

```
#
sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.1
 hrp mirror session enable
 hrp track interface GE0/0/1
 hrp track interface GE0/0/3
 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 import-route bgp
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
#
bgp 65001
 router-id 10.2.1.1
 peer 10.2.1.2 as-number 65002
 peer 10.2.1.2 ebgp-max-hop 2
 ipv4-family unicast
  network 10.2.1.1 255.255.255.0
  import-route ospf 10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.3.1.0 mask 255.255.255.0
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  destination-zone local
  source-address 10.3.0.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 24 destination-address 10.2.1.2 24 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 24 source-address 10.2.1.2 24 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 source-address 10.3.3.0 24 action permit #	source-address 10.3.1.0 mask 255.255.255.0 service ospf action permit rule name policy_bgp_1 source-zone local destination-zone untrust destination-address 10.2.0.2 24 destination-address 10.2.1.2 24 service bgp action permit rule name policy_bgp_2 source-zone untrust destination-zone local source-address 10.2.0.2 24 source-address 10.2.1.2 24 service bgp action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 source-address 10.3.3.0 24 action permit #

7.2.11 Web: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction

Networking Requirements

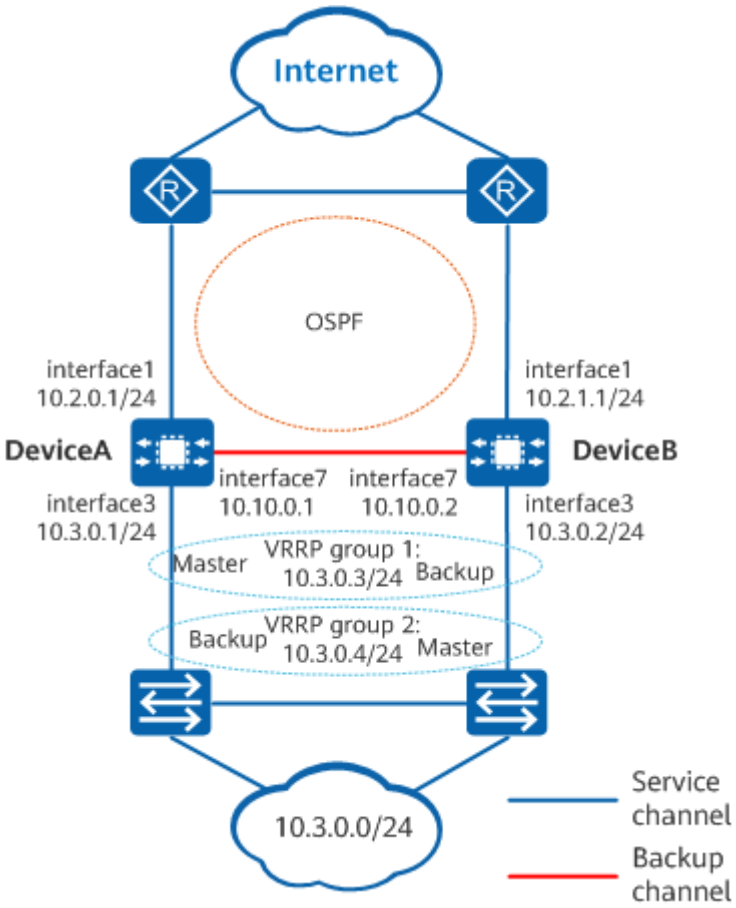
As shown in **Figure 7-31**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream routers and downstream Layer 2 switches. OSPF runs between the devices and routers. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-31 Load sharing networking where service interfaces work at Layer 3 and connect to upstream routers and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

 Copyright © Huawei Technologies Co., Ltd.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Repeat the preceding steps to configure **GE0/0/3**.

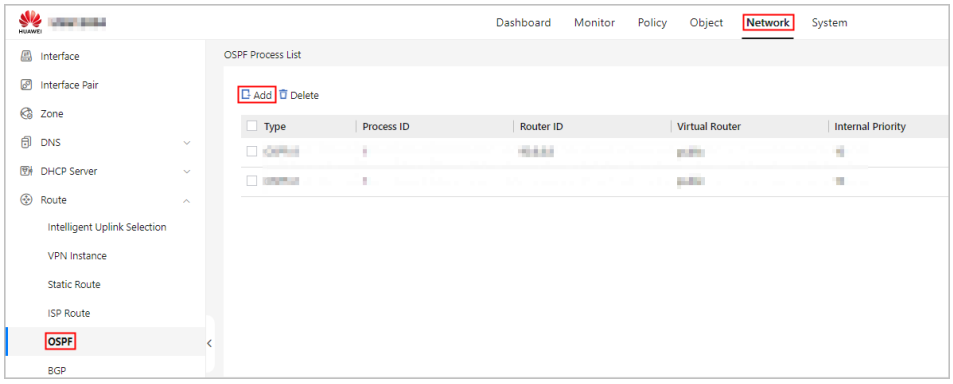
Zone	trust
IPv4	
IP Address	10.3.0.2/24

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF to ensure IP connectivity.

1. Configure OSPF on DeviceA.
   a. Choose **Network** > **Route** > **OSPF**.



   b. Click **Add**, set the parameters as follows to create an OSPF process, and click **OK**.

Type	OSPFv2
Process ID	10

c. Click , click **Add**, set the parameters as follows to create an OSPF area, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.0.0
Mask/Wildcard Mask	255.255.255.0

d. Choose **Basic Configuration** > **Network Settings**, click **Add**, set the parameters as follows to create a network, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

2. Configure OSPF on DeviceB.

a. Choose **Network** > **Route** > **OSPF**.

b. Click **Add**, set the parameters as follows to create an OSPF process, and click **OK**.

Type	OSPFv2
Process ID	10

c. Click , click **Add**, set the parameters as follows to create an OSPF area, and then click **OK**.

Area	0.0.0.0
IP Network	10.2.1.0
Mask/Wildcard Mask	255.255.255.0

d. Choose **Basic Configuration** > **Network Settings**, click **Add**, set the parameters as follows to create a network, and then click **OK**.

Area	0.0.0.0
IP Network	10.3.0.0

 Copyright © Huawei Technologies Co., Ltd.

Mask/Wildcard Mask	255.255.255.0

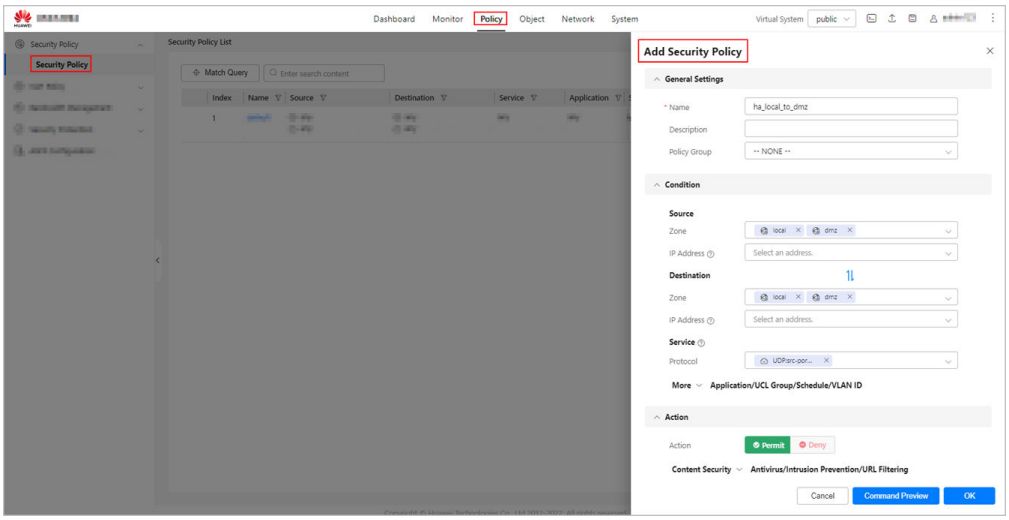
Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

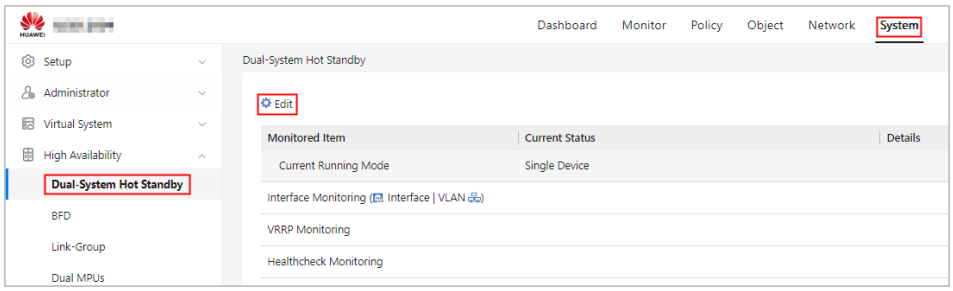


Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514
Action	Permit

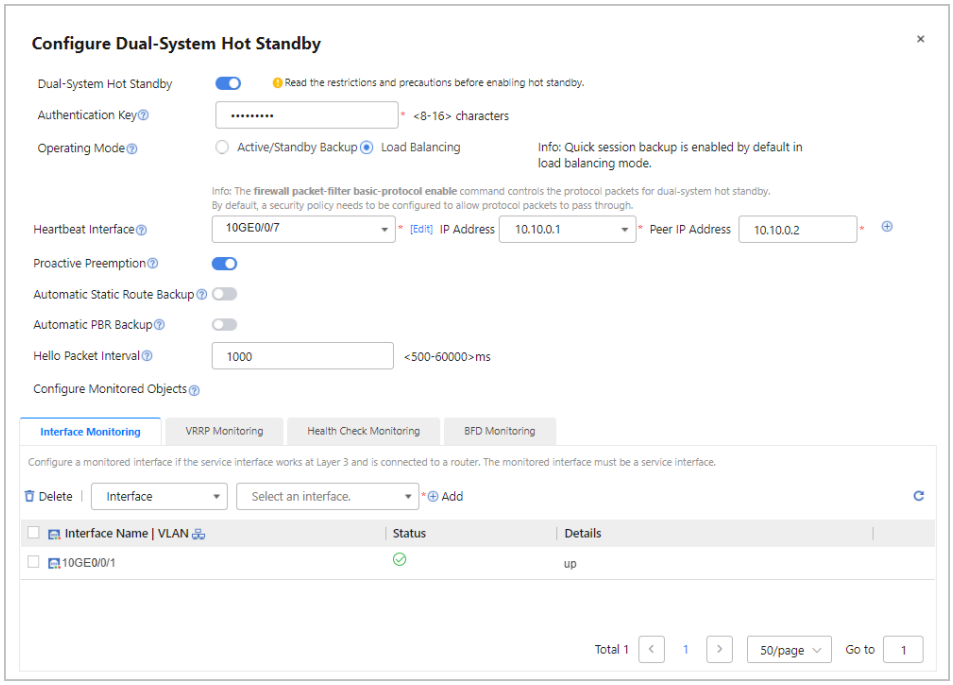
Step 4 Configure hot standby.

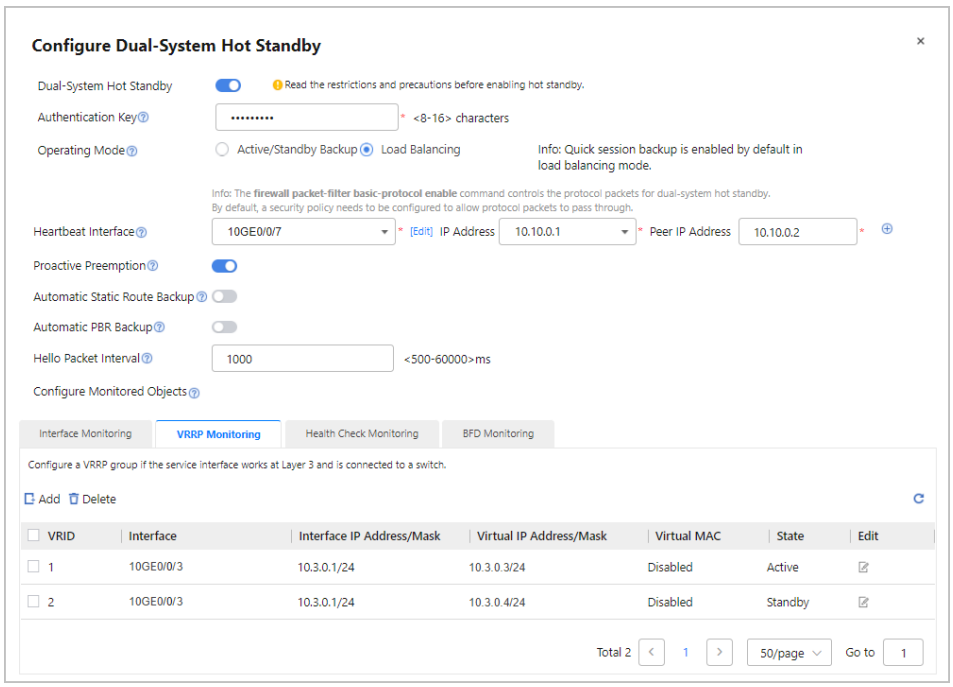
1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

 Copyright © Huawei Technologies Co., Ltd.



b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



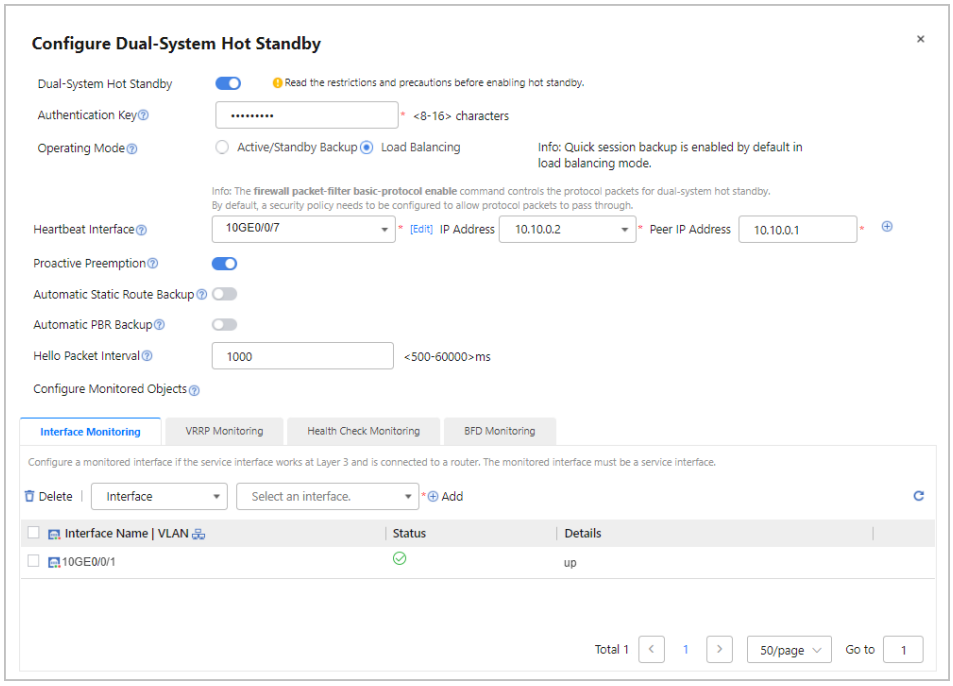


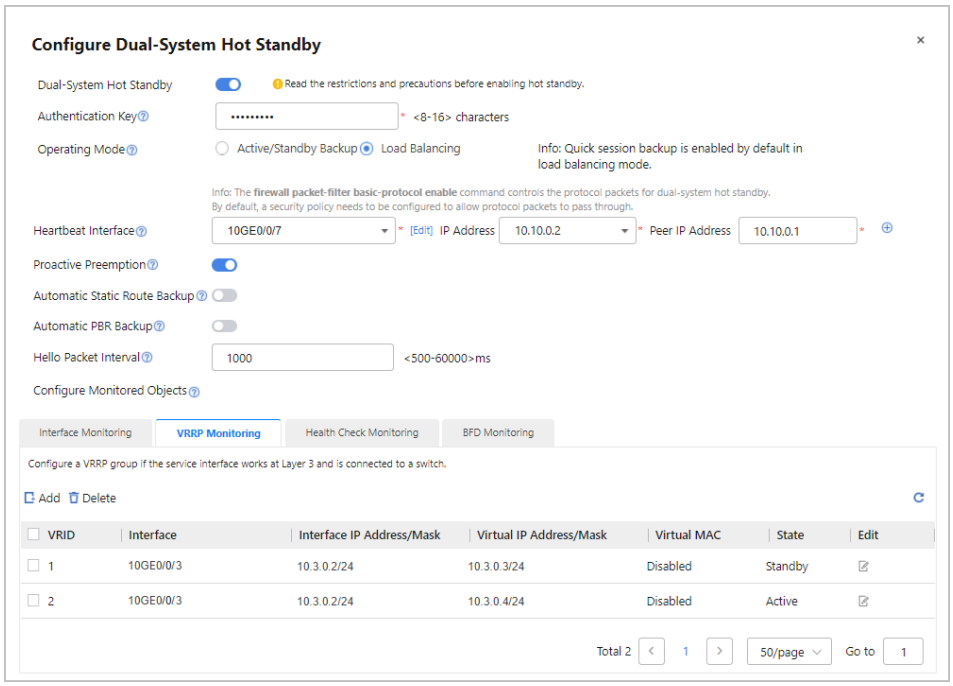
 Copyright © Huawei Technologies Co., Ltd.

2. Configure hot standby on DeviceB.

   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.

   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.





Step 5 Configure the security policies.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure security policies and set the parameters as follows, and then click **OK**.

   # Configure a security policy to allow intranet users to access the Internet.

Name	policy_sec1
Source Zone	trust
Destination Zone	untrust
Service	10.3.0.0/24
Action	Permit

   # Configure a security policy to allow DeviceA and the upstream router (in the untrust zone) to exchange OSPF packets.

   NOTE

   Controlling function of security policies for OSPF packets are configured by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, OSPF packets are controlled by security policies. In this case, a security policy must be configured between the security zones where the upstream/downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_sec2
Source Zone	local,untrust
Destination Zone	local,untrust
Service	ospf
Action	Permit

Step 6 Configure the switches and PCs.

1. Add the three interfaces of the switches to the same VLANs accordingly. For configuration commands, refer to related documents of the switches.
2. Configure the default routes on intranet devices. You can set the next hop of some devices to the virtual IP address (10.3.0.3) of VRRP group 1 and that of other devices to the virtual IP address (10.3.0.4) of VRRP group 2.

Step 7 Configure the routers.

Configure OSPF on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
 #
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 active
 vrrp vrid 2 virtual-ip 10.3.0.4 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 standby
 vrrp vrid 2 virtual-ip 10.3.0.4 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.2.12 CLI: Example for Deploying Devices in In-path Mode and Connecting to Routers Through OSPF in the Upstream Direction and Switches in the Downstream Direction

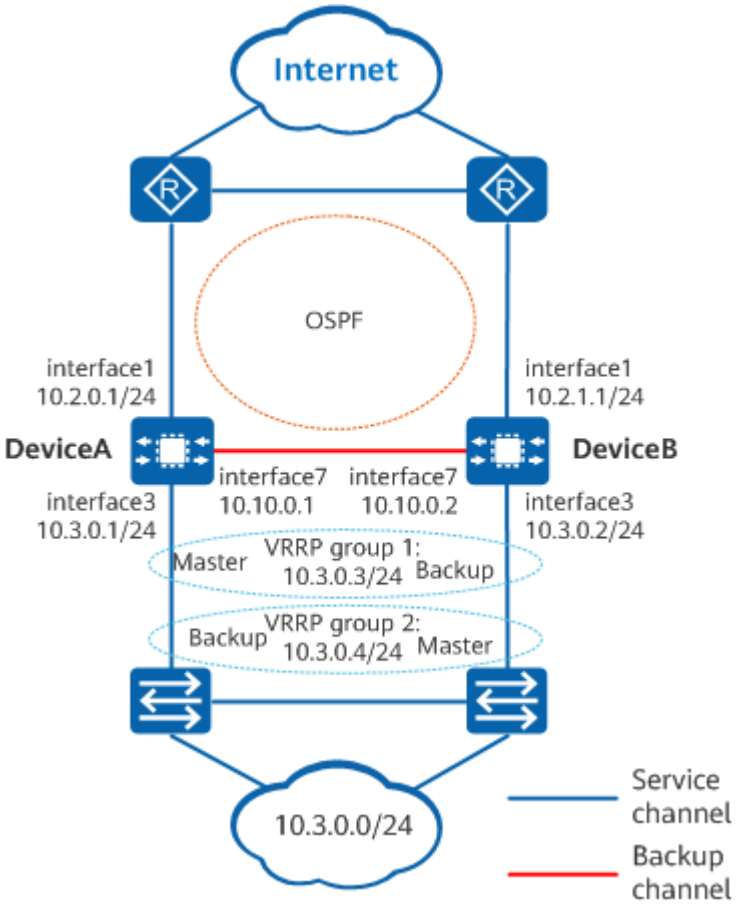
Networking Requirements

As shown in **Figure 7-32**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream routers and downstream Layer 2 switches. OSPF runs between the devices and routers. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-32 Load sharing networking where service interfaces work at Layer 3 and connect to upstream routers and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



Procedure

Step 1 Complete basic network configurations.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.0.2 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

In this example, because DeviceA and DeviceB connect to upstream routers and downstream switches, you need to configure DeviceA and DeviceB to monitor the upstream interfaces and configure VRRP groups on downstream interfaces.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1**	[DeviceB] **hrp track interface ge 0/0/1**
# Configure VRRP groups 1 and 2 on downstream service interface GE 0/0/3 of DeviceA and specify **active** in the **vrrp vrid virtual-ip** command for VRRP group 1 and **standby** in the command for VRRP group 2. Configure VRRP groups 1 and 2 on downstream service interface GE 0/0/3 of DeviceB and specify **standby** in the **vrrp vrid virtual-ip** command for VRRP group 1 and **active** in the command for VRRP group 2.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 1 virtual-ip 10.3.0.3 active** [DeviceA-GE0/0/3] **vrrp vrid 2 virtual-ip 10.3.0.4 standby** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 1 virtual-ip 10.3.0.3 standby** [DeviceB-GE0/0/3] **vrrp vrid 2 virtual-ip 10.3.0.4 active** [DeviceB-GE0/0/3] **quit**
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Create security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow intranet users to access the external network.

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec1
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec1] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec1] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec1] quit
```

Configure a security policy to allow DeviceA and the upstream router (in the untrust zone) to exchange OSPF packets.

NOTE

OSPF packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that OSPF packets are controlled by security policies. As such, a security policy must be configured between the untrust zone where the upstream service interface resides and the local zone to allow OSPF packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA-policy-security] rule name policy_sec2
HRP_M[DeviceA-policy-security-rule-policy_sec2] source-zone local untrust
HRP_M[DeviceA-policy-security-rule-policy_sec2] destination-zone local untrust
HRP_M[DeviceA-policy-security-rule-policy_sec2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_sec2] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec2] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers and switches.

Configure OSPF on the routers to advertise routes. For configuration commands, see related documents of the routers.

Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.

----End

Verifying the Configuration

1. Run the **display vrrp** command on DeviceA and DeviceB to check the status of interfaces in the VRRP groups.
2. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
 #
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 active
 vrrp vrid 2 virtual-ip 10.3.0.4 standby
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track interface GE0/0/1
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 standby
 vrrp vrid 2 virtual-ip 10.3.0.4 active
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name policy_sec2
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service ospf
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

7.2.13 Web: Example for Connecting Devices to Routers Transparently in the Upstream and Downstream Directions

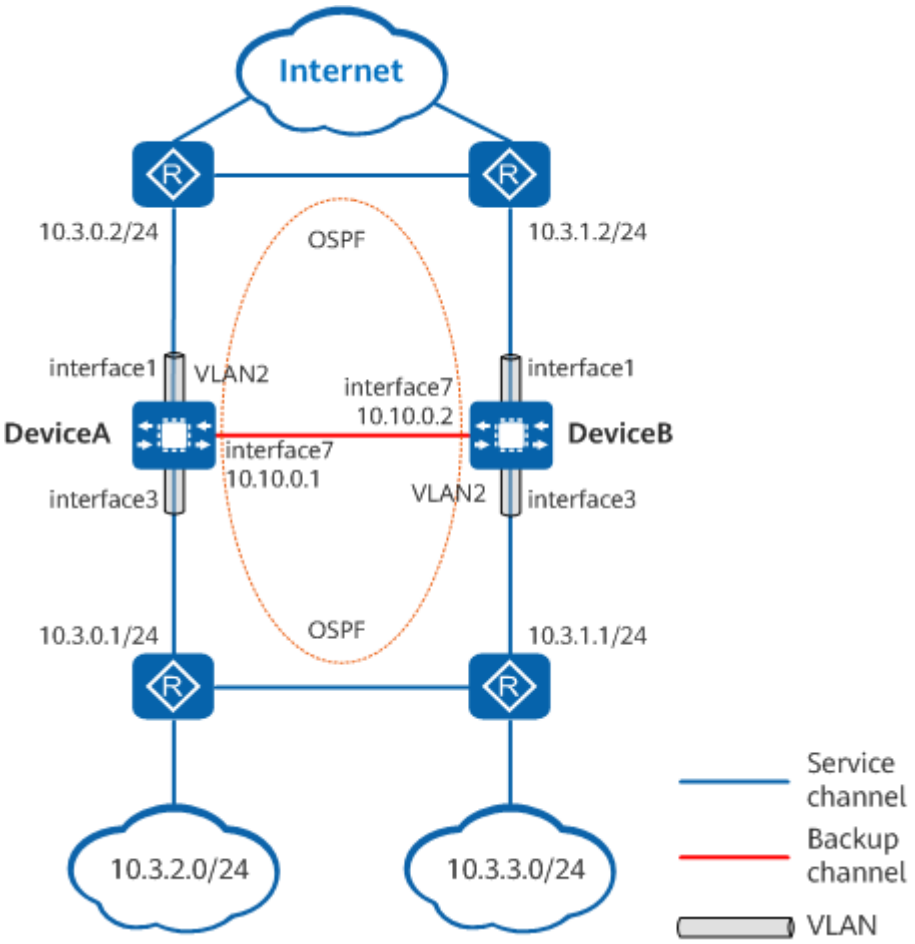
Networking Requirements

As shown in **Figure 7-33**, the upstream and downstream service interfaces of DeviceA and DeviceB work at Layer 2 and are connected to routers. The service interfaces are added to VLAN2. OSPF runs between upstream and downstream routers. DeviceA and DeviceB work as Layer-2 devices to transparently forward OSPF packets and do not participate in routing protocol calculation. It is required that DeviceA and DeviceB work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-33 Load sharing networking where service interfaces work at Layer 2 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure interfaces and basic network configurations.

1. Configure interfaces on DeviceA.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
Mode	Switching
Connection Type	Access
Access VLAN ID	2

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
Mode	Switching
Connection Type	Access
Access VLAN ID	2

   d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Configure interfaces on DeviceB.
   a. Choose **Network** > **Interface**.
   b. Click **GE0/0/1**, set the parameters as follows, click **OK**.

Zone	untrust
Mode	Switching
Connection Type	Access
Access VLAN ID	2

   c. Repeat the preceding steps to configure **GE0/0/3**.

Zone	trust
Mode	Switching
Connection Type	Access

 Copyright © Huawei Technologies Co., Ltd.

Access VLAN ID	2

d. Repeat the preceding steps to configure **GE0/0/7**.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

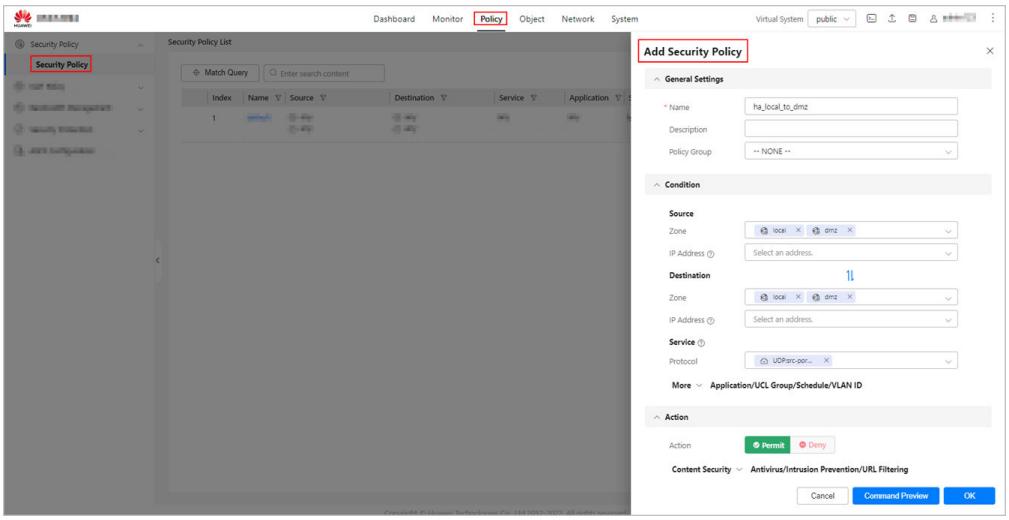
Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured by the **firewall packet-filter basic-protocol enable**. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the Local zone to allow HRP packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.



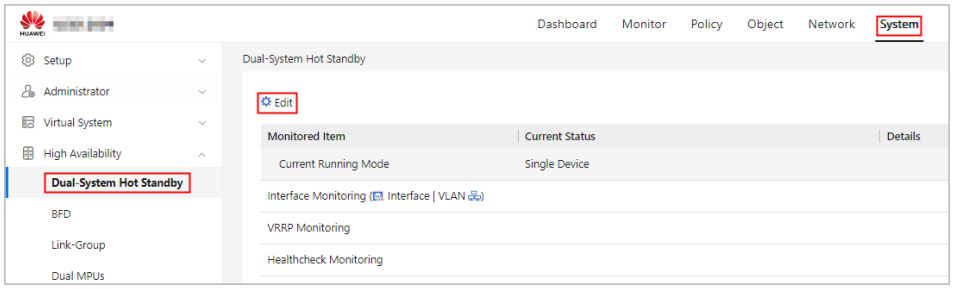
Name	ha_local_to_dmz
Source Zone	local, dmz
Destination Zone	local, dmz
Service/Protocol	UDP, Destination Port:18514

 Copyright © Huawei Technologies Co., Ltd.

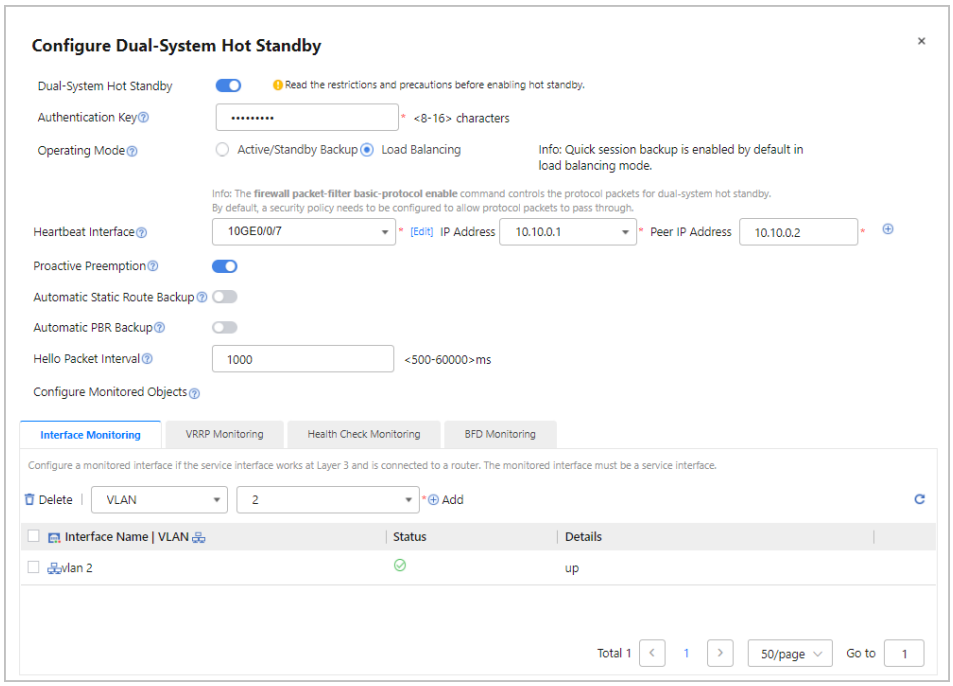
Action	Permit

Step 3 Configure hot standby.

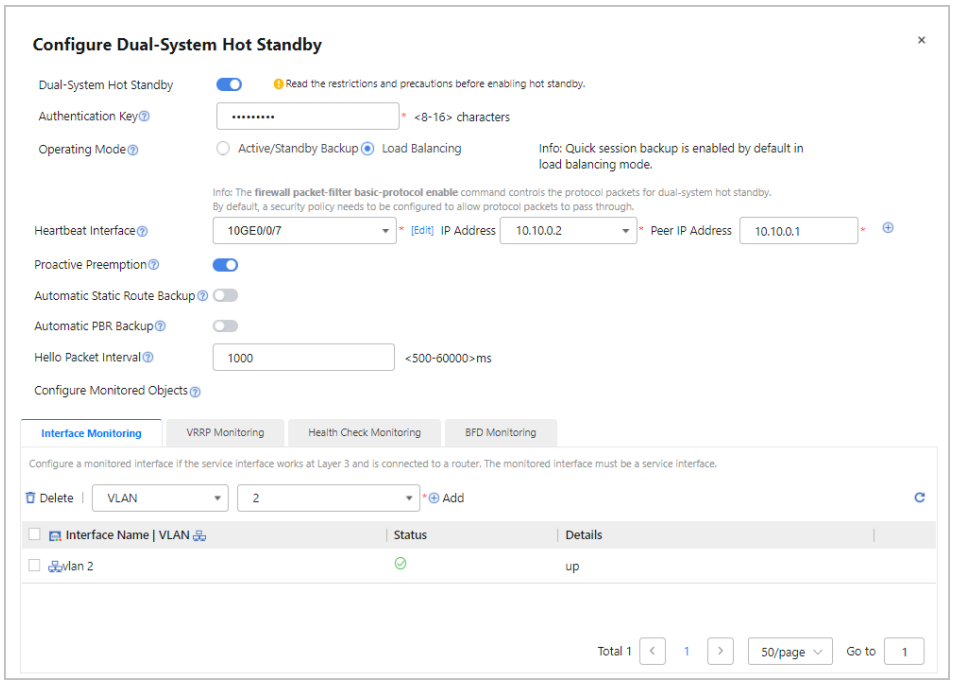
1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.



   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



2. Configure hot standby on DeviceB.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby** and click **Edit**.
   b. Enable **Dual-System Hot Standby**, set the parameters as follows, and click **OK**.



Step 4 Configure the security policies.

After hot standby relationship is established, the security policy on DeviceA will be automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, set the parameters as follows, and click **OK**.

   # Configure a security policy to allow OSPF packets transmitted between the upstream and downstream routers and the packets exchanged between the intranet and Internet.

   NOTE

   When the service interfaces of the devices (DeviceA and DeviceB) work at Layer 2, OSPF packets between upstream and downstream devices need to pass through the devices. Controlling function of security policies for OSPF packets are configured by the**firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, OSPF packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the upstream service interface resides and the security zone where the downstream service interface resides to allow OSPF packets to pass. In this example, enabling the **firewall packet-filter basic-protocol enable** command is used as an example.

Name	policy_ospf_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.1/32,10.3.1.1/32
Destination Address	10.3.0.2/32,10.3.1.2/32
Service	ospf

 Copyright © Huawei Technologies Co., Ltd.

Action	Permit

Name	policy_ospf_2
Source Zone	untrust
Destination Zone	trust
Source Address	10.3.0.2/32,10.3.1.2/32
Destination Address	10.3.0.1/32,10.3.1.1/32
Service	ospf
Action	Permit

Configure a security policy to allow intranet users to access the Internet.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.2.0/24,10.3.3.0/24
Action	Permit

Step 5 Configure the routers.

Configure OSPF on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

Verifying the Configuration

Choose **System** > **High Availability** > **Dual-System Hot Standby** to view the operating status of hot standby.

- Normally, the **Current Running Mode** of DeviceA is **Load Balancing** and the **Current Status** is **Active**. The **Current Running Mode** of DeviceB is **Load Balancing** and the **Current Status** is **Standby**. This shows that traffic is forwarded by DeviceA and DeviceB.
- When DeviceA goes faulty, the **Current Running Mode** of DeviceA is **Active/Standby Backup** and the **Current Status** is **Standby**. The **Current Running Mode** of DeviceB is **Active/Standby Backup** and the **Current Status** is **Active**. This shows that traffic is forwarded by DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track vlan 2
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
vlan batch 2
#
interface GE0/0/1
 portswitch
 port default vlan 2
#
interface GE0/0/3
 portswitch
 port default vlan 2
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.1 mask 255.255.255.255
  source-address 10.3.1.1 mask 255.255.255.255
  destination-address 10.3.0.2 mask
255.255.255.255
  destination-address 10.3.1.2 mask
255.255.255.255
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.2 mask 255.255.255.255
  source-address 10.3.1.2 mask 255.255.255.255
  destination-address 10.3.0.1 mask
255.255.255.255
  destination-address 10.3.1.1 mask
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track vlan 2
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
vlan batch 2
#
interface GE0/0/1
 portswitch
 port default vlan 2
#
interface GE0/0/3
 portswitch
 port default vlan 2
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.1 mask 255.255.255.255
  source-address 10.3.1.1 mask 255.255.255.255
  destination-address 10.3.0.2 mask
255.255.255.255
  destination-address 10.3.1.2 mask
255.255.255.255
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.2 mask 255.255.255.255
  source-address 10.3.1.2 mask 255.255.255.255
  destination-address 10.3.0.1 mask
255.255.255.255
  destination-address 10.3.1.1 mask
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
255.255.255.255 service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit # return	255.255.255.255 service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit # return

7.2.14 CLI: Example for Connecting Devices to Routers Transparently in the Upstream and Downstream Directions

Networking Requirements

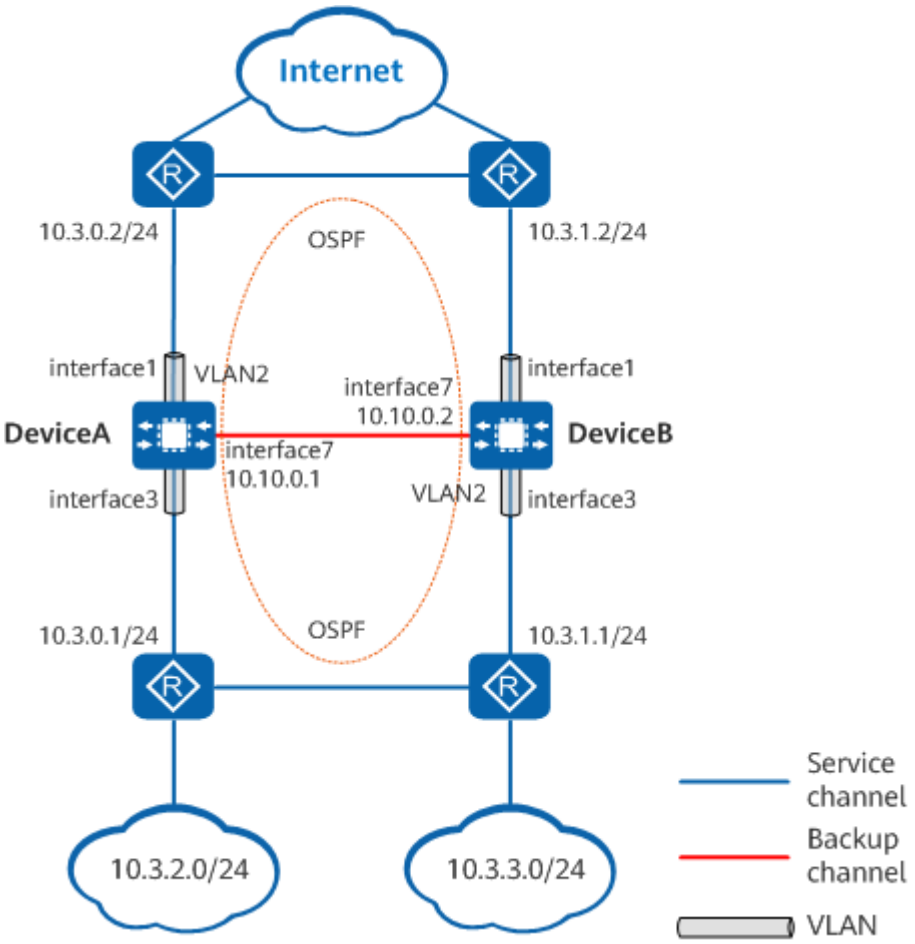
As shown in **Figure 7-34**, the upstream and downstream service interfaces of DeviceA and DeviceB work at Layer 2 and are connected to routers. The service interfaces are added to VLAN2. OSPF runs between upstream and downstream routers. DeviceA and DeviceB work as Layer-2 devices to transparently forward OSPF packets and do not participate in routing protocol calculation. It is required that DeviceA and DeviceB work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-34 Load sharing networking where service interfaces work at Layer 2 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# On DeviceA and DeviceB, change the mode of upstream and downstream service interfaces to Layer 2 and add them to the same VLAN.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vlan batch 2** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **portswitch** [DeviceA-GE0/0/1] **port link-type access** [DeviceA-GE0/0/1] **port default vlan 2** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **portswitch** [DeviceA-GE0/0/3] **port link-type access** [DeviceA-GE0/0/3] **port default vlan 2** [DeviceA-GE0/0/3] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vlan batch 2** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **portswitch** [DeviceB-GE0/0/1] **port link-type access** [DeviceB-GE0/0/1] **port default vlan 2** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **portswitch** [DeviceB-GE0/0/3] **port link-type access** [DeviceB-GE0/0/3] **port default vlan 2** [DeviceB-GE0/0/3] **quit**
# Set an IP address for the heartbeat interface on each of DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor the status of VLAN 2.	
[DeviceA] **hrp track vlan 2**	[DeviceB] **hrp track vlan 2**
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Create security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow OSPF packets exchanged between upstream and downstream routers and the packets exchanged between the intranet and external network to pass through.

NOTE

When the service interfaces of the devices (DeviceA and DeviceB) work at Layer 2, OSPF packets between upstream and downstream devices need to pass through the devices. OSPF packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that OSPF packets are controlled by security policies. As such, a security policy must be configured between the security zone where the upstream service interface resides and the security zone where the downstream service interface resides to allow OSPF packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-address 10.3.0.1 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-address 10.3.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-address 10.3.0.2 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-address 10.3.1.2 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-address 10.3.0.2 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-address 10.3.1.2 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-address 10.3.0.1 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-address 10.3.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.3.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers.

Configure OSPF on the four routers to advertise routes. For configuration commands, see related documents of the routers.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track vlan 2
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
vlan batch 2
#
interface GE0/0/1
 portswitch
 port default vlan 2
#
interface GE0/0/3
 portswitch
 port default vlan 2
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.1 mask 255.255.255.255
  source-address 10.3.1.1 mask 255.255.255.255
  destination-address 10.3.0.2 mask
255.255.255.255
  destination-address 10.3.1.2 mask
255.255.255.255
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.2 mask 255.255.255.255
  source-address 10.3.1.2 mask 255.255.255.255
  destination-address 10.3.0.1 mask
255.255.255.255
  destination-address 10.3.1.1 mask
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track vlan 2
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
vlan batch 2
#
interface GE0/0/1
 portswitch
 port default vlan 2
#
interface GE0/0/3
 portswitch
 port default vlan 2
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.1 mask 255.255.255.255
  source-address 10.3.1.1 mask 255.255.255.255
  destination-address 10.3.0.2 mask
255.255.255.255
  destination-address 10.3.1.2 mask
255.255.255.255
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.2 mask 255.255.255.255
  source-address 10.3.1.2 mask 255.255.255.255
  destination-address 10.3.0.1 mask
255.255.255.255
  destination-address 10.3.1.1 mask
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
255.255.255.255 service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit # return	255.255.255.255 service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 source-address 10.3.3.0 mask 255.255.255.0 action permit # return

7.3 Configuring Hot Standby in Mirroring Mode

7.3.1 CLI: Example for Configuring Hot Standby in Mirroring Mode

Networking Requirements

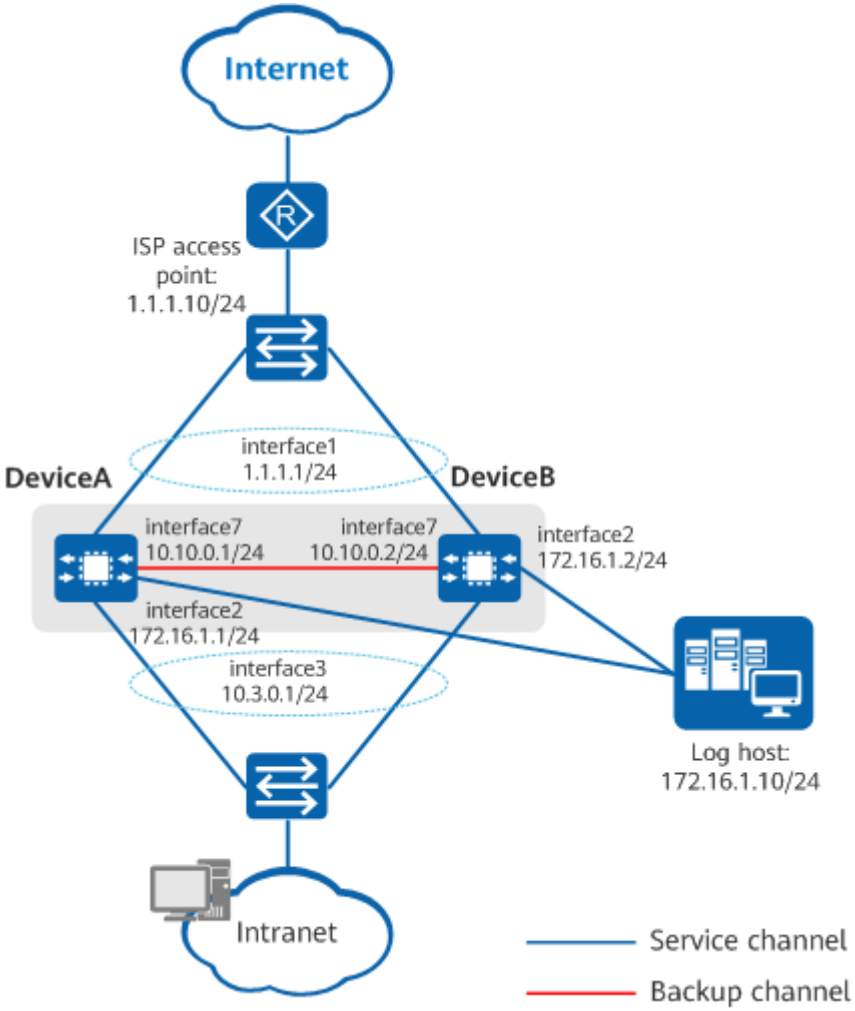
On the network shown in **Figure 7-35**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream Layer 2 switches. The two devices are connected to log hosts respectively. The upstream switch is connected to the carrier network, and the IP addresses that the carrier assigns to the enterprise are from 1.1.1.1 to 1.1.1.5. It is required that DeviceA and DeviceB form hot standby networking in mirroring mode and intranet users can access the Internet. In the mirroring mode, the two devices have the same service interface address and route configuration. Therefore, the two devices can be considered as one device.

Figure 7-35 Network diagram of hot standby networking in mirroring mode

NOTE

In this example, interface1, interface2, interface3, and interface7 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

Before configuring the mirroring mode, you need to complete network connections and basic configurations of hot standby, but not configurations such as service interfaces and routes. The configuration roadmap is as follows:

1. Complete basic hot standby configurations on DeviceA and DeviceB, including configuring devices to monitor service interfaces (**hrp track interface**), configuring the heartbeat interfaces, and enabling hot standby.
2. Enable the mirroring mode on DeviceA and DeviceB and perform manual batch backup.
3. Complete network configurations on one of the devices to ensure that intranet users can access the Internet.

   After the mirroring mode is formed, all configurations (including interface and route configurations) need to be performed on only one device. These configurations will be automatically backed up to the other device.

Procedure

Step 1 Configure heartbeat interfaces and hot standby management interfaces on DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only heartbeat interfaces and hot standby management interfaces need to be configured, and service interfaces do not need to be configured. This is because the service interface configurations will be automatically backed up after the mirroring mode is enabled.

Hot standby management interfaces are used to connect to log hosts and NMS devices.

DeviceA	DeviceB
# Configure IP addresses for heartbeat interfaces and hot standby management interfaces on DeviceA and DeviceB and assign these interfaces to security zones.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 172.16.1.1 24** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/2** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 172.16.1.2 24** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/2** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# Specify the heartbeat interface and device role, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp device active** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp device standby** [DeviceB] **hrp enable**

Step 4 Configure the mirroring mode and hot standby management interface on DeviceA. After hot standby is enabled, these configurations will be automatically backed up to DeviceB.

```
HRP_M[DeviceA] hrp mirror config enable
HRP_M[DeviceA] hrp mgt-interface ge 0/0/2
HRP_M[DeviceA] quit
```

Step 5 Perform manual batch backup to synchronize the configurations on DeviceA to DeviceB.

NOTE

The mirroring mode requires that the configurations of the two devices are the same. The configurations of the two devices may be different when mirroring is enabled. In this case, you can run the **hrp sync config** command to synchronize the configurations on the devices.

```
HRP_M<DeviceA> hrp sync config
```

Step 6 Complete network configurations on DeviceA to ensure that intranet users can access the Internet. The following configurations will be automatically backed up to DeviceB.

NOTE

After the mirroring mode is configured, the configuration on one device will be automatically backed up to the other device. Compared with traditional hot standby, hot standby in mirroring mode can back up interface and route configurations.

Assign IP addresses to interfaces.

```
HRP_M<DeviceA> system-view
HRP_M[DeviceA] interface ge 0/0/1
HRP_M[DeviceA-GE0/0/1] ip address 1.1.1.1 24
HRP_M[DeviceA-GE0/0/1] quit
HRP_M[DeviceA] interface ge 0/0/3
HRP_M[DeviceA-GE0/0/3] ip address 10.3.0.1 24
HRP_M[DeviceA-GE0/0/3] quit
```

Assign the interfaces to security zones.

```
HRP_M[DeviceA] firewall zone untrust
HRP_M[DeviceA-zone-untrust] add interface ge 0/0/1
HRP_M[DeviceA-zone-untrust] quit
HRP_M[DeviceA] firewall zone trust
HRP_M[DeviceA-zone-trust] add interface ge 0/0/3
HRP_M[DeviceA-zone-trust] quit
```

Create a default route with next-hop address 1.1.1.10.

```
HRP_M[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name trust_to_untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] action permit
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] quit
HRP_M[DeviceA-policy-security] quit
```

Configure a NAT policy to translate source addresses on subnet 10.3.0.0/24 to IP addresses in the NAT address pool (1.1.1.2 to 1.1.1.5) when intranet users access the Internet.

```
HRP_M[DeviceA] nat address-group group1
HRP_M[DeviceA-address-group-group1] section 0 1.1.1.2 1.1.1.5
HRP_M[DeviceA-address-group-group1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat1
HRP_M[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat1] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group group1
HRP_M[DeviceA-policy-nat-rule-policy_nat1] quit
HRP_M[DeviceA-policy-nat] quit
```

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Ping Router in the untrust zone from the PC in the trust zone, and run the **display firewall session table** command to check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall session table** Current Total Sessions : 1 icmp VPN: public --> public 10.3.0.10:0[1.1.1.2:10298] --> 1.1.1.10:2048	HRP_S<DeviceB> **display firewall session table** Current Total Sessions : 1 icmp VPN:public --> public **Remote** 10.3.0.10:0[1.1.1.2:10298] --> 1.1.1.10:2048

   The command output shows that sessions tagged with **Remote** exist on DeviceB, indicating that sessions are successfully backed up after you configure hot standby.
3. Run the **ping 1.1.1.10 -t** command on the PC, run the **shutdown** command to disable GE 0/0/1 on DeviceA, and then check whether an active/standby switchover is performed and whether ping packets are discarded. Run the **undo shutdown** command to enable GE 0/0/1 on DeviceA and check again whether an active/standby switchover is performed and whether ping packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror config enable
hrp mgt-interface GE0/0/2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
  section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone dmz
  destination-zone local
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror config enable
hrp mgt-interface GE0/0/2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.1.2 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
 add interface GE0/0/7
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
 nat address-group group1
  section 0 1.1.1.2 1.1.1.5
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone dmz
  destination-zone local
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action source-nat address-group group1 # 	action source-nat address-group group1 #

7.4 Configuring Interworking Between Hot Standby and Health Check

7.4.1 CLI: Example for Configuring Interworking Between Hot Standby and Health Check

Networking Requirements

As shown in **Figure 7-36**, all service interfaces on DeviceA and DeviceB work at Layer 3 and connect to upstream and downstream routers. The two devices work in active/standby mode. The requirements are as follows:

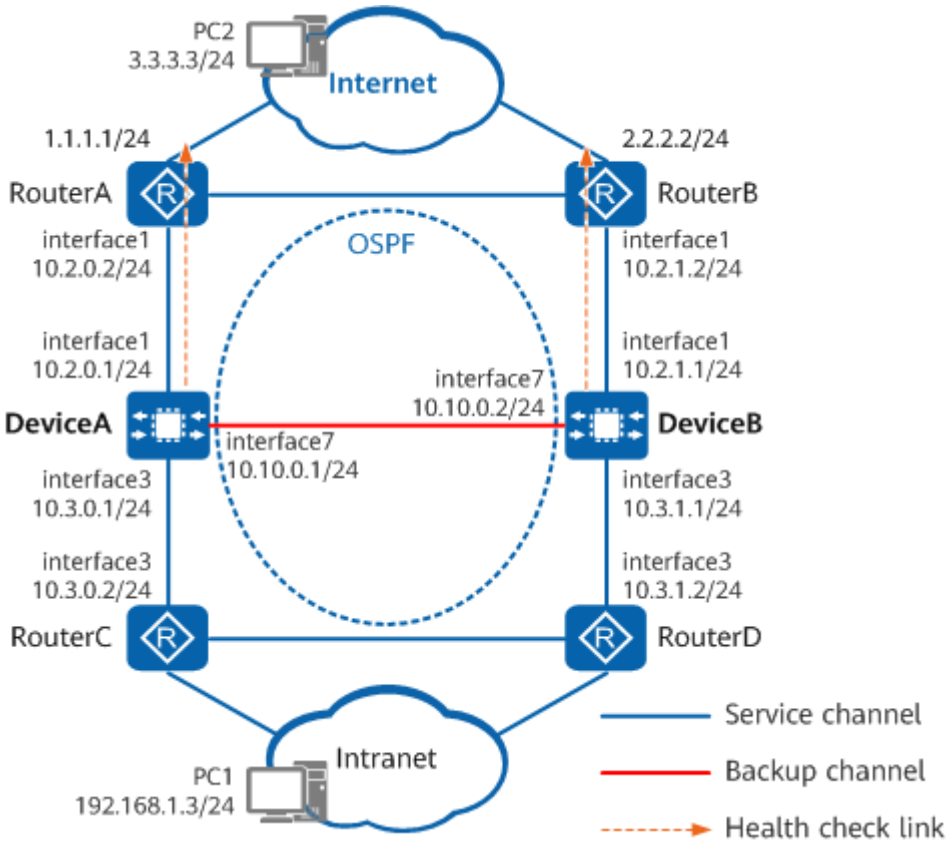
- OSPF runs between the two devices (DeviceA and DeviceB) and routers. Routers send service traffic to DeviceA based on the route calculation result.
- DeviceA and DeviceB monitor the network egress through association between hot standby and health check. If the network egress of the link where DeviceA resides is down, DeviceB becomes the active device and forwards service traffic.

Figure 7-36 Network diagram of configuring association between hot standby and health check

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set an IP address for each interface on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure OSPF on DeviceA and DeviceB to ensure that they are routable.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# Configure DeviceA and DeviceB to adjust the OSPF cost values based on device priorities. After this command is run, a device determines whether it is the active or standby device when advertising OSPF routes. If the device is the active one, it directly advertises the routes that it has learned. If it is the standby device, it advertises the routes after increasing the cost values. In this way, when upstream and downstream routers calculate routes, the next hop points to the active device, and packets are forwarded to the active device.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **hrp adjust ospf-cost enable**	[DeviceB] **hrp adjust ospf-cost enable**
# Specify the heartbeat interface and device role, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Configure interworking between hot standby and health check.

DeviceA	DeviceB
# Configure health check to monitor the network egress.	
HRP_M[DeviceA] **healthcheck enable** HRP_M[DeviceA] **healthcheck name test** HRP_M[DeviceA-healthcheck-test] **destination 1.1.1.1 interface ge 0/0/1 protocol icmp** HRP_M[DeviceA-healthcheck-test] **destination 2.2.2.2 interface ge 0/0/1 protocol icmp** HRP_M[DeviceA-healthcheck-test] **quit**	HRP_S[DeviceB] **healthcheck enable** HRP_S[DeviceB] **healthcheck name test** HRP_S[DeviceB-healthcheck-test] **destination 1.1.1.1 interface ge 0/0/1 protocol icmp** HRP_S[DeviceB-healthcheck-test] **destination 2.2.2.2 interface ge 0/0/1 protocol icmp** HRP_S[DeviceB-healthcheck-test] **quit**
# Configure interworking between hot standby and health check.	
HRP_M[DeviceA] **hrp track healthcheck test**	HRP_S[DeviceB] **hrp track healthcheck test**

Step 5 Configure security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow devices and the upstream and downstream routers to exchange OSPF packets.

NOTE

OSPF packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPF packets are controlled by security policies. As such, a security policy must be configured between the security zone where the upstream and downstream service interfaces reside and the local zone to allow OSPF packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
```

Configure a security policy to allow intranet users to access the external network.

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 192.168.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure routers.

Configure interface IP addresses and OSPF on the four routers to ensure that the routers are reachable. For details about the configuration commands, see related documents of the routers.

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Ping PC2 in the untrust zone from PC1 in the trust zone and run the **display firewall session table verbose** command on DeviceA and DeviceB to check sessions.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall session table verbose** icmp VPN: public --> public ID: a587f8591ef638b481757870e81 Zone: trust -> untrust TTL: 00:10:00 Left: 00:08:39 Output-interface: GE0/0/1 Nexthop: 10.2.0.2 MAC: 00-e0-fc-12-34-56 **<-- packets:14 bytes:1176 --> packets:14 bytes:1176** **192.168.1.3:55211 --> 3.3.3.3:2048** **PolicyName: policy_sec**	HRP_S<DeviceB> **display firewall session table verbose** icmp VPN: public --> public ID: c687f6e6827b3f018b2a357870de8 Zone: trust -> untrust **Remote** TTL: 00:10:00 Left: 00:09:00 Output-interface: GE0/0/1 Nexthop: 10.2.0.2 MAC: 00-e0-fc-12-34-56 **<-- packets:0 bytes:0 --> packets:0 bytes:0** **192.168.1.3:54955 --> 3.3.3.3:2048** **PolicyName: policy_sec**

The command output shows that sessions tagged with **Remote** are created on DeviceB, indicating that sessions are successfully backed up after hot standby is configured. If no traffic passes through DeviceB, DeviceB is in the standby state.

3. Run the **shutdown** command on the upstream interface 1.1.1.1/24 of RouterA to simulate a fault. DeviceA will detect that the remote interface 1.1.1.1/24 is unreachable. In this case, an active/standby switchover occurs between DeviceA and DeviceB. Then run the **display hrp state verbose** command on DeviceA and DeviceB to check the change in the hot standby status.

   Ping PC2 in the untrust zone from PC1 in the trust zone again, and run the **display firewall session table verbose** command on DeviceA and DeviceB to check sessions. The command output shows that sessions tagged with **Remote** exist on DeviceA and no traffic passes through DeviceA, indicating that DeviceA is in the standby state.

   After simulation of an active/standby switchover is completed, run the **undo shutdown** command in the corresponding interface view of RouterA to restore the interface state to Up.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp track healthcheck test
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
healthcheck enable
healthcheck name test
 destination 1.1.1.1 interface GE0/0/1 protocol
icmp
 destination 2.2.2.2 interface GE0/0/1 protocol
icmp
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp track healthcheck test
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
healthcheck enable
healthcheck name test
 destination 1.1.1.1 interface GE0/0/1 protocol
icmp
 destination 2.2.2.2 interface GE0/0/1 protocol
icmp
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
destination-zone local service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 192.168.1.0 mask 255.255.255.0 action permit #	destination-zone local service ospf action permit rule name policy_sec source-zone trust destination-zone untrust source-address 192.168.1.0 mask 255.255.255.0 action permit #

7.5 Configuring Association Between Hot Standby and BFD

7.5.1 CLI: Example for Configuring Interworking Between Hot Standby and BFD

Networking Requirements

As shown in **Figure 7-37**, all service interfaces on DeviceA and DeviceB work at Layer 3 and connect to upstream and downstream routers. The two devices work in active/standby mode. The requirements are as follows:

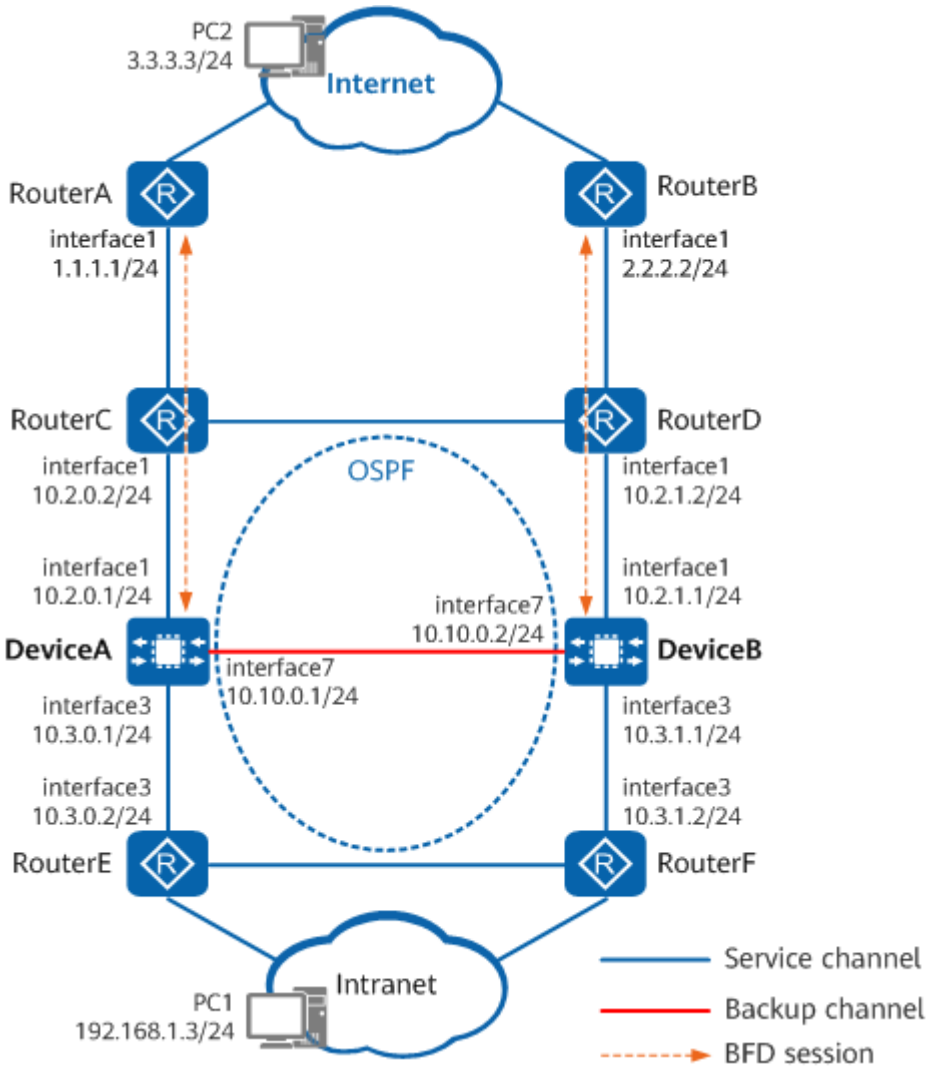
- OSPF runs between the two devices (DeviceA and DeviceB) and routers. Routers send service traffic to the active device based on the route calculation result.
- DeviceA and DeviceB monitor the network egress through association between hot standby and BFD. If the network egress of the link where DeviceA resides is down, DeviceB becomes the active device and forwards service traffic.

Figure 7-37 Network diagram of configuring association between BFD and hot standby

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set an IP address for each interface on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF on DeviceA and DeviceB to ensure that they are routable.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to adjust the OSPF cost values based on device priorities. After this command is run, a device determines whether it is the active or standby device when advertising OSPF routes. If the device is the active device, it directly advertises the learned routes. If the device is a standby device, it increases the cost and then advertises routes. In this way, when upstream and downstream routers calculate routes, the next hop points to the active device, and packets are forwarded to the active device.	
[DeviceA] **hrp adjust ospf-cost enable**	[DeviceB] **hrp adjust ospf-cost enable**
# Specify the heartbeat interface and device role, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Configure security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

NOTE

OSPF and BFD packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPF and BFD packets are controlled by security policies. As such, a security policy must be configured between the security zones where the upstream and downstream service interfaces reside and the local zone to allow OSPF packets to pass. In addition, a security policy needs to be configured between the security zone where the upstream service interface resides and the local zone to allow BFD packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

Configure security policies to allow the device to exchange OSPF packets with upstream and downstream routers.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospf_1
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] destination-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospf_2
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] source-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospf_2] quit
```

Configure security policies to allow the device to exchange BFD packets with the upstream router.

```
HRP_M[DeviceA-policy-security] rule name policy_bfd_1
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] source-address 10.2.0.1 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] source-address 10.2.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] destination-address 1.1.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] destination-address 2.2.2.2 32
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_bfd_1] quit
HRP_M[DeviceA-policy-security] rule name policy_bfd_2
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] source-address 1.1.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] source-address 2.2.2.2 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] destination-address 10.2.0.1 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] destination-address 10.2.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_bfd_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 192.168.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers.

Configure interface IP addresses and OSPF on the routers to ensure that the routers are reachable. For details about the configuration commands, see related documents of the routers.

Step 6 Create a BFD session.

BFD configurations cannot be backed up. You need to configure BFD on both DeviceA and DeviceB.

Configure BFD session 1 with peer IP address 1.1.1.1, local discriminator 10, and remote discriminator 20 on DeviceA. Configure BFD session 1 with peer IP address 10.2.0.1, local discriminator 20, and remote discriminator 10 on RouterA.

DeviceA	RouterA
HRP_M[DeviceA] **bfd** HRP_M[DeviceA-bfd] **quit** HRP_M[DeviceA] **bfd 1 bind peer-ip 1.1.1.1** HRP_M[DeviceA-bfd-session-1] **discriminator local 10** HRP_M[DeviceA-bfd-session-1] **discriminator remote 20** HRP_M[DeviceA-bfd-session-1] **quit**	<RouterA> **system-view** [RouterA] **bfd** [RouterA-bfd] **quit** [RouterA] **bfd 1 bind peer-ip 10.2.0.1** [RouterA-bfd-session-1] **discriminator local 20** [RouterA-bfd-session-1] **discriminator remote 10** [RouterA-bfd-session-1] **quit**

Configure BFD session 1 with peer IP address 2.2.2.2, local discriminator 10, and remote discriminator 20 on DeviceB. Configure BFD session 1 with peer IP address 10.2.1.1, local discriminator 20, and remote discriminator 10 on RouterB.

 Copyright © Huawei Technologies Co., Ltd.

DeviceB	RouterB
HRP_S[DeviceB] **bfd** HRP_S[DeviceB-bfd] **quit** HRP_S[DeviceB] **bfd 1 bind peer-ip 2.2.2.2** HRP_S[DeviceB-bfd-session-1] **discriminator local 10** HRP_S[DeviceB-bfd-session-1] **discriminator remote 20** HRP_S[DeviceB-bfd-session-1] **quit**	<RouterB> **system-view** [RouterB] **bfd** [RouterB-bfd] **quit** [RouterB] **bfd 1 bind peer-ip 10.2.1.1** [RouterB-bfd-session-1] **discriminator local 20** [RouterB-bfd-session-1] **discriminator remote 10** [RouterB-bfd-session-1] **quit**

Step 7 Configure association between hot standby and BFD.

DeviceA	DeviceB
HRP_M[DeviceA] **hrp track bfd-session 10**	HRP_S[DeviceB] **hrp track bfd-session 10**

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Ping PC2 in the untrust zone from PC1 in the trust zone and run the **display firewall session table verbose** command on DeviceA and DeviceB to check sessions.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall session table verbose** icmp VPN: public --> public ID: a587f8591ef638b481757870e81 Zone: trust -> untrust TTL: 00:10:00 Left: 00:08:39 Output-interface: GE0/0/1 Nexthop: 10.2.0.2 MAC: 00-e0-fc-12-34-56 **<-- packets:14 bytes:1176 --> packets:14 bytes:1176** **192.168.1.3:55211 --> 3.3.3.3:2048** **PolicyName: policy_sec**	HRP_S<DeviceB> **display firewall session table verbose** icmp VPN: public --> public ID: c687f6e6827b3f018b2a357870de8 Zone: trust -> untrust **Remote** TTL: 00:10:00 Left: 00:09:00 Output-interface: GE0/0/1 Nexthop: 10.2.0.2 MAC: 00-e0-fc-12-34-56 **<-- packets:0 bytes:0 --> packets:0 bytes:0** **192.168.1.3:54955 --> 3.3.3.3:2048** **PolicyName: policy_sec**

   The command output shows that sessions tagged with **Remote** are created on DeviceB, indicating that sessions are successfully backed up after hot standby is configured. If no traffic passes through DeviceB, DeviceB is in the standby state.
3. Run the **shutdown** command on GE 0/0/1 of RouterA to simulate a fault. DeviceA will detect that the remote interface 1.1.1.1/24 is unreachable. In this case, an active/standby switchover occurs between DeviceA and DeviceB. Then, run the **display hrp state verbose** command on DeviceA and DeviceB to check the change in the hot standby status.

   Ping PC2 in the untrust zone from PC1 in the trust zone again, and run the **display firewall session table verbose** command on DeviceA and DeviceB to check sessions. The command output shows that sessions tagged with

 Copyright © Huawei Technologies Co., Ltd.

Remote exist on DeviceA and no traffic passes through DeviceA, indicating that DeviceA is in the standby state.

After simulation of an active/standby switchover is completed, run the **undo shutdown** command in the corresponding interface view of RouterA to restore the interface state to Up.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp track bfd-session 10
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
bfd 1 bind peer-ip 1.1.1.1
 discriminator local 10
 discriminator remote 20
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp track bfd-session 10
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
bfd 1 bind peer-ip 2.2.2.2
 discriminator local 10
 discriminator remote 20
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
rule name policy_bfd_1 source-zone local destination-zone untrust source-address 10.2.0.1 32 source-address 10.2.1.1 32 destination-address 1.1.1.1 32 destination-address 2.2.2.2 32 action permit rule name policy_bfd_2 source-zone untrust destination-zone local source-address 1.1.1.1 32 source-address 2.2.2.2 32 destination-address 10.2.0.1 32 destination-address 10.2.1.1 32 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 192.168.1.0 24 action permit # 	rule name policy_bfd_1 source-zone local destination-zone untrust source-address 10.2.0.1 32 source-address 10.2.1.1 32 destination-address 1.1.1.1 32 destination-address 2.2.2.2 32 action permit rule name policy_bfd_2 source-zone untrust destination-zone local source-address 1.1.1.1 32 source-address 2.2.2.2 32 destination-address 10.2.0.1 32 destination-address 10.2.1.1 32 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 192.168.1.0 24 action permit #

7.6 Configuring Hot Standby of Virtual Systems

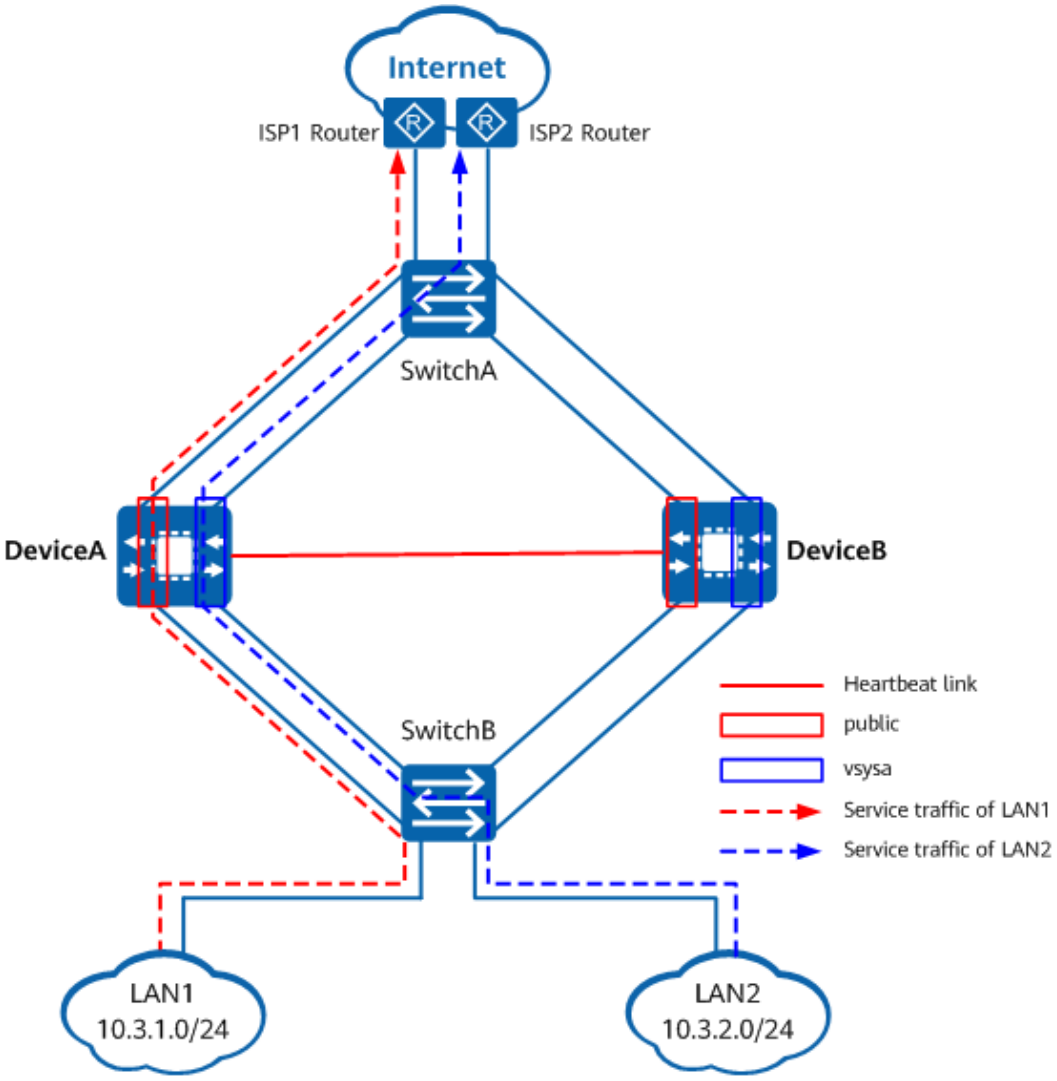
7.6.1 CLI: Example for Configuring Hot Standby (Active/Standby) of Virtual Systems on Devices Connecting to Switches in Upstream and Downstream Directions

Networking Requirements

As shown in **Figure 7-38**, two network segments on the enterprise network need to be separated. SwitchA and SwitchB use VLANs to separate the two network segments, and the devices (DeviceA and DeviceB) use virtual systems to separate them. The devices work in active/standby mode. In normal situations, DeviceA forwards traffic. When DeviceA fails, traffic is forwarded by DeviceB. This ensures that the services are not interrupted.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-38 Hot standby networking when virtual systems are configured



The detailed data planning is as follows.

Figure 7-39 Data planning scheme

NOTE

In this example, interfaces 1, 2, 3, 4, and 7 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.

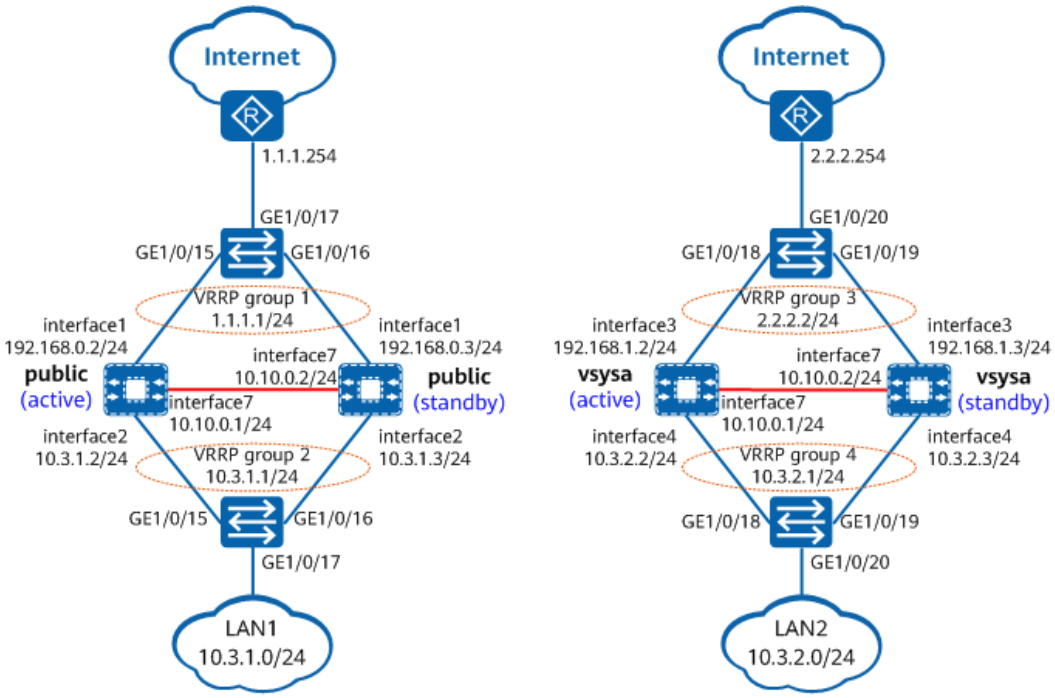


Table 7-1 Data planning of DeviceA and DeviceB

Item	Sub-item	Data of DeviceA	Data of DeviceB
Interfaces	Public interface of the public system	Interface number: GE 0/0/1 IP address: **192.168.0.2/24** Security zone: untrust	Interface number: GE 0/0/1 IP address: **192.168.0.3/24** Security zone: untrust
	Private interface of the public system	Interface number: GE 0/0/2 IP address: **10.3.1.2/24** Security zone: trust	Interface number: GE 0/0/2 IP address: **10.3.1.3/24** Security zone: trust
	Public interface of virtual system **vsysa**	Interface number: GE 0/0/3 IP address: **192.168.1.2/24** Security zone: untrust	Interface number: GE 0/0/3 IP address: **192.168.1.3/24** Security zone: untrust
	Private interface of virtual system **vsysa**	Interface number: GE 0/0/4 IP address: **10.3.2.2/24** Security zone: trust	Interface number: GE 0/0/4 IP address: **10.3.2.3/24** Security zone: trust
	Heartbeat interface	Interface number: GE 0/0/7 IP address: **10.10.0.1/24** Security zone: dmz	Interface number: GE 0/0/7 IP address: **10.10.0.2/24** Security zone: dmz

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Data of DeviceA	Data of DeviceB
VRRP groups	VRRP group 1	1.1.1.1/24 **active**	1.1.1.1/24 **standby**
	VRRP group 2	10.3.1.1/24 **active**	10.3.1.1/24 **standby**
	VRRP group 3	2.2.2.2/24 **active**	2.2.2.2/24 **standby**
	VRRP group 4	10.3.2.1/24 **active**	10.3.2.1/24 **standby**
Routes	Default route of the public system	Destination IP address: 0.0.0.0 Next hop: 1.1.1.254	Destination IP address: 0.0.0.0 Next hop: 1.1.1.254
	Default route of virtual system **vsysa**	Destination IP address: 0.0.0.0 Next hop: 2.2.2.254	Destination IP address: 0.0.0.0 Next hop: 2.2.2.254

Table 7-2 Data planning of switches

Device	VLAN	Member Interface 1	Member Interface 2	Member Interface 3
SwitchA	10 (public)	GE1/0/15	GE1/0/16	GE1/0/17
	30 (vsysa)	GE1/0/18	GE1/0/19	GE1/0/20
SwitchB	20 (public)	GE1/0/15	GE1/0/16	GE1/0/17
	40 (vsysa)	GE1/0/18	GE1/0/19	GE1/0/20

Procedure

Step 1 Create virtual system **vsysa** and assign interfaces to it.

NOTE

The virtual system names and IDs on DeviceA and DeviceB must be the same. You can run the **display vsys** command on both devices to compare the configurations after virtual systems are created.

DeviceA	DeviceB
# Enable the virtual system function on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vsys enable**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vsys enable**
# Create a virtual system on DeviceA and DeviceB and assign interfaces and a public address to it. The public address is used in the NAT address pool.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **vsys name vsysa** [DeviceA-vsys-vsysa] **assign interface ge 0/0/3** [DeviceA-vsys-vsysa] **assign interface ge 0/0/4** [DeviceA-vsys-vsysa] **assign global-ip 2.2.2.2 2.2.2.2 exclusive** [DeviceA-vsys-vsysa] **quit**	[DeviceB] **vsys name vsysa** [DeviceB-vsys-vsysa] **assign interface ge 0/0/3** [DeviceB-vsys-vsysa] **assign interface ge 0/0/4** [DeviceB-vsys-vsysa] **assign global-ip 2.2.2.2 2.2.2.2 exclusive** [DeviceB-vsys-vsysa] **quit**

Step 2 Configure interfaces.

DeviceA	DeviceB
# Configure IP addresses and VRRP groups for public system interfaces on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 192.168.0.2 24** [DeviceA-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.1 24 active** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 10.3.1.2 24** [DeviceA-GE0/0/2] **vrrp vrid 2 virtual-ip 10.3.1.1 active** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 192.168.0.3 24** [DeviceB-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.1 24 standby** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 10.3.1.3 24** [DeviceB-GE0/0/2] **vrrp vrid 2 virtual-ip 10.3.1.1 standby** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign public system interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/2** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/2** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure IP addresses and VRRP groups for virtual system interfaces on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 192.168.1.2 24** [DeviceA-GE0/0/3] **vrrp vrid 3 virtual-ip 2.2.2.2 24 active** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/4** [DeviceA-GE0/0/4] **ip address 10.3.2.2 24** [DeviceA-GE0/0/4] **vrrp vrid 4 virtual-ip 10.3.2.1 active** [DeviceA-GE0/0/4] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 192.168.1.3 24** [DeviceB-GE0/0/3] **vrrp vrid 3 virtual-ip 2.2.2.2 24 standby** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/4** [DeviceB-GE0/0/4] **ip address 10.3.2.3 24** [DeviceB-GE0/0/4] **vrrp vrid 4 virtual-ip 10.3.2.1 standby** [DeviceB-GE0/0/4] **quit**
# Assign virtual system interfaces to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **firewall zone untrust** [DeviceA-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceA-vsysa-zone-untrust] **quit** [DeviceA-vsysa] **firewall zone trust** [DeviceA-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceA-vsysa-zone-trust] **quit** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **firewall zone untrust** [DeviceB-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceB-vsysa-zone-untrust] **quit** [DeviceB-vsysa] **firewall zone trust** [DeviceB-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceB-vsysa-zone-trust] **quit** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 3 Configure static routes.

DeviceA	DeviceB
# Configure a default route from the public system to the Internet and set the next hop to the IP address of an ISP router on DeviceA and DeviceB.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.254**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.254**
# Configure a default route from the virtual system to the Internet and set the next hop to the IP address of an ISP router on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **ip route-static 0.0.0.0 0.0.0.0 2.2.2.254** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **ip route-static 0.0.0.0 0.0.0.0 2.2.2.254** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 4 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure hot standby.

Specify the heartbeat interface, configure the authentication key, and enable hot standby on DeviceA and DeviceB.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 6 Configure security policies.

After hot standby relationship is established, the security policy configured on DeviceA is automatically backed up to DeviceB.

Configure a security policy for the public system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Configure a security policy for the virtual system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] security-policy
HRP_M[DeviceA-vsysa-policy-security] rule name policy_sec
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-vsysa-policy-security] quit
HRP_M[DeviceA-vsysa] quit
HRP_M<DeviceA-vsysa> quit
```

Step 7 Configure NAT policies.

After hot standby relationship is established, the NAT policy configured on DeviceA is automatically backed up to DeviceB.

Configure a NAT policy for the public system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.1 1.1.1.1
HRP_M[DeviceA-address-group-addressgroup1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-policy-nat] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a NAT policy for the virtual system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] nat address-group addressgroup1
HRP_M[DeviceA-vsysa-address-group-addressgroup1] section 0 2.2.2.2 2.2.2.2
HRP_M[DeviceA-vsysa-address-group-addressgroup1] quit
HRP_M[DeviceA-vsysa] nat-policy
HRP_M[DeviceA-vsysa-policy-nat] rule name policy_nat
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-vsysa-policy-nat] quit
HRP_M[DeviceA-vsysa] quit
```

Step 8 Configure the switches.

NOTE

The following part uses Huawei switches to illustrate the configuration.

Configure SwitchA.

```
[SwitchA] vlan batch 10 30
[SwitchA] interface GigabitEthernet 1/0/15
[SwitchA-GigabitEthernet1/0/15] port link-type access
[SwitchA-GigabitEthernet1/0/15] port default vlan 10
[SwitchA-GigabitEthernet1/0/15] quit
[SwitchA] interface GigabitEthernet 1/0/16
[SwitchA-GigabitEthernet1/0/16] port link-type access
[SwitchA-GigabitEthernet1/0/16] port default vlan 10
[SwitchA-GigabitEthernet1/0/16] quit
[SwitchA] interface GigabitEthernet 1/0/17
[SwitchA-GigabitEthernet1/0/17] port link-type access
[SwitchA-GigabitEthernet1/0/17] port default vlan 10
[SwitchA-GigabitEthernet1/0/17] quit
[SwitchA] interface GigabitEthernet 1/0/18
[SwitchA-GigabitEthernet1/0/18] port link-type access
[SwitchA-GigabitEthernet1/0/18] port default vlan 30
[SwitchA-GigabitEthernet1/0/18] quit
[SwitchA] interface GigabitEthernet 1/0/19
[SwitchA-GigabitEthernet1/0/19] port link-type access
[SwitchA-GigabitEthernet1/0/19] port default vlan 30
[SwitchA-GigabitEthernet1/0/19] quit
[SwitchA] interface GigabitEthernet 1/0/20
[SwitchA-GigabitEthernet1/0/20] port link-type access
[SwitchA-GigabitEthernet1/0/20] port default vlan 30
[SwitchA-GigabitEthernet1/0/20] quit
```

Configure SwitchB.

```
[SwitchB] vlan batch 20 40
[SwitchB] interface GigabitEthernet 1/0/15
[SwitchB-GigabitEthernet1/0/15] port link-type access
[SwitchB-GigabitEthernet1/0/15] port default vlan 20
[SwitchB-GigabitEthernet1/0/15] quit
[SwitchB] interface GigabitEthernet 1/0/16
[SwitchB-GigabitEthernet1/0/16] port link-type access
[SwitchB-GigabitEthernet1/0/16] port default vlan 20
[SwitchB-GigabitEthernet1/0/16] quit
[SwitchB] interface GigabitEthernet 1/0/17
[SwitchB-GigabitEthernet1/0/17] port link-type trunk
[SwitchB-GigabitEthernet1/0/17] port trunk allow-pass vlan 20
[SwitchB-GigabitEthernet1/0/17] quit
[SwitchB] interface GigabitEthernet 1/0/18
[SwitchB-GigabitEthernet1/0/18] port link-type access
```

 Copyright © Huawei Technologies Co., Ltd.

```
[SwitchB-GigabitEthernet1/0/18] port default vlan 40
[SwitchB-GigabitEthernet1/0/18] quit
[SwitchB] interface GigabitEthernet 1/0/19
[SwitchB-GigabitEthernet1/0/19] port link-type access
[SwitchB-GigabitEthernet1/0/19] port default vlan 40
[SwitchB-GigabitEthernet1/0/19] quit
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] port link-type trunk
[SwitchB-GigabitEthernet1/0/20] port trunk allow-pass vlan 40
[SwitchB-GigabitEthernet1/0/20] quit
```

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Access the Internet from the enterprise network. The access succeeds. Check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M[DeviceA] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa 10.3.2.10:2057[2.2.2.2:2048]-->2.2.2.254:2048 icmp VPN:public -> public 10.3.1.10:2057[1.1.1.1:2048]-->1.1.1.254:2048	HRP_S[DeviceB] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa **Remote** 10.3.2.10:2057[2.2.2.2:2048]-->2.2.2.254:2048 icmp VPN:public -> public **Remote** 10.3.1.10:2057[1.1.1.1:2048]-->1.1.1.254:2048

   As shown in the previous information, a session tagged with **Remote** is created on DeviceB, indicating that the session is successfully synchronized after hot standby is configured.
3. Ping an IP address on the Internet from an intranet PC, remove the network cable from GE 0/0/1 on DeviceA, and check device status switchover and ping packet discard statistics. Then insert the network cable back to GE 0/0/1 on DeviceA and check device status switchover and ping packet discard statistics again.

Configuration Scripts

- Public system

 Copyright © Huawei Technologies Co., Ltd.

DeviceA

```
#
sysname DeviceA
#
vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/3
 assign interface GE0/0/4
 assign global-ip 2.2.2.2 2.2.2.2 exclusive
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+
%#
#
interface GE0/0/1
 ip address 192.168.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0
active
#
interface GE0/0/2
 ip address 10.3.1.2 255.255.255.0
 vrrp vrid 2 virtual-ip 10.3.1.1 active
#
interface GE0/0/3
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 3 virtual-ip 2.2.2.2 255.255.255.0
active
#
interface GE0/0/4
 ip address 10.3.2.2 255.255.255.0
 vrrp vrid 4 virtual-ip 10.3.2.1 active
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
```

DeviceB

```
#
sysname DeviceB
#
vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/3
 assign interface GE0/0/4
 assign global-ip 2.2.2.2 2.2.2.2 exclusive
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t
\i4 t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 192.168.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0
standby
#
interface GE0/0/2
 ip address 10.3.1.3 255.255.255.0
 vrrp vrid 2 virtual-ip 10.3.1.1 standby
#
interface GE0/0/3
 ip address 192.168.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 2.2.2.2 255.255.255.0
standby
#
interface GE0/0/4
 ip address 10.3.2.3 255.255.255.0
 vrrp vrid 4 virtual-ip 10.3.2.1 standby
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  source-address 10.3.1.0 mask 255.255.255.0
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 mask 255.255.255.0 action source-nat address-group addressgroup1 #	nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 mask 255.255.255.0 action source-nat address-group addressgroup1 #

- **vsysa**

DeviceA	DeviceB
# switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 0.0.0.0 0.0.0.0 2.2.2.254 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 action permit # nat address-group addressgroup1 section 0 2.2.2.2 2.2.2.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 action source-nat address-group addressgroup1 #	# switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 0.0.0.0 0.0.0.0 2.2.2.254 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 action permit # nat address-group addressgroup1 section 0 2.2.2.2 2.2.2.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 mask 255.255.255.0 action source-nat address-group addressgroup1 #

7.6.2 CLI: Example for Configuring Hot Standby (Active/Standby) of Virtual Systems on Firewalls Connecting to Upstream Routers and Downstream Switches

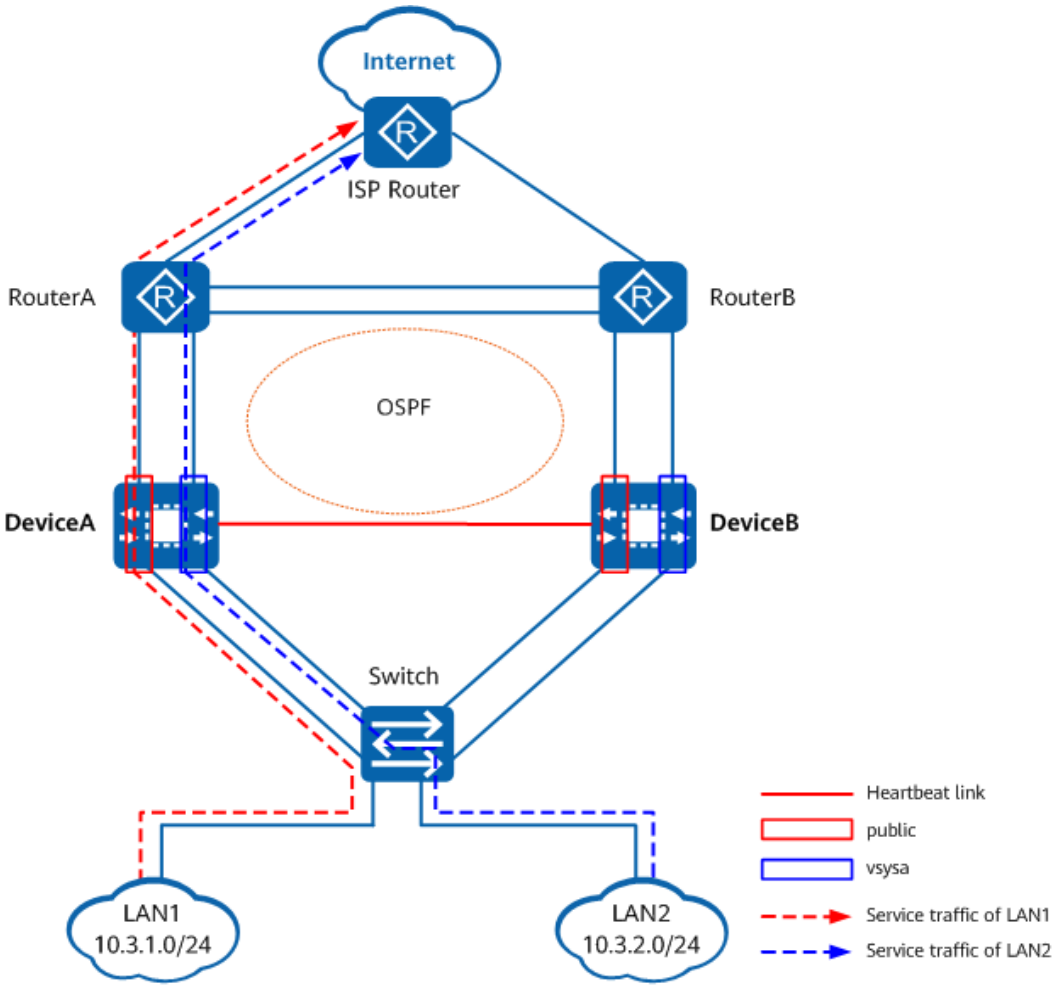
Networking Requirements

As shown in **Figure 7-40**, two network segments on the enterprise network need to be separated. Switches use VLANs to separate the two network segments, and the devices (DeviceA and DeviceB) use virtual systems to separate them. The

 Copyright © Huawei Technologies Co., Ltd.

devices connect to upstream routers, and OSPF runs between the devices and upstream routers. The two devices work in active/standby mode. In normal situations, DeviceA forwards traffic. When DeviceA fails, traffic is forwarded by DeviceB. This ensures that the services are not interrupted.

Figure 7-40 Hot standby networking when virtual systems are configured



The detailed data planning is as follows.

Figure 7-41 Data planning scheme

NOTE

In this example, interfaces 1, 2, 3, 4, and 7 represent GE0/0/1, GE0/0/2, GE0/0/3, GE0/0/4, and GE0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.

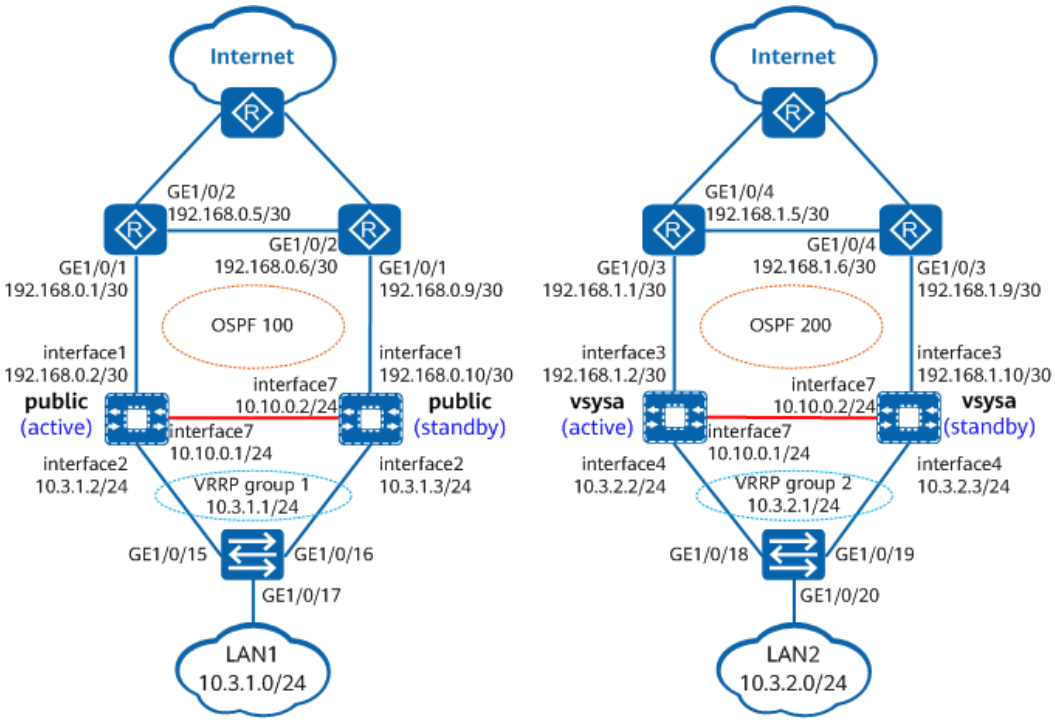


Table 7-3 Data planning of DeviceA and DeviceB

Item	Sub-item	Data of DeviceA	Data of DeviceB
Interfaces	Public interface of the public system	Interface number: GE0/0/1 IP address: **192.168.0.2/30** Security zone: untrust	Interface number: GE0/0/1 IP address: **192.168.0.10/30** Security zone: untrust
	Private interface of the public system	Interface number: GE0/0/2 IP address: **10.3.1.2/24** Security zone: trust	Interface number: GE0/0/2 IP address: **10.3.1.3/24** Security zone: trust
	Public interface of virtual system **vsysa**	Interface number: GE0/0/3 IP address: **192.168.1.2/30** Security zone: untrust	Interface number: GE0/0/3 IP address: **192.168.1.10/30** Security zone: untrust
	Private interface of virtual system **vsysa**	Interface number: GE0/0/4 IP address: **10.3.2.2/24** Security zone: trust	Interface number: GE0/0/4 IP address: **10.3.2.3/24** Security zone: trust
	Heartbeat interface	Interface number: GE0/0/7 IP address: **10.10.0.1/24** Security zone: dmz	Interface number: GE0/0/7 IP address: **10.10.0.2/24** Security zone: dmz

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Data of DeviceA	Data of DeviceB
VRRP groups	VRRP group 1	**10.3.1.1/24 active**	**10.3.1.1/24 standby**
	VRRP group 2	**10.3.2.1/24 active**	**10.3.2.1/24 standby**
Routes	Blackhole route configured for the NAT address pool of the public system to prevent route loops	Blackhole route Destination IP address: 1.1.1.1/32	Blackhole route Destination IP address: 1.1.1.1/32
	Blackhole route configured for the NAT address pool of **vsysa** to prevent route loops	Blackhole route Destination IP address: 1.1.1.2/32	Blackhole route Destination IP address: 1.1.1.2/32
	OSPF configuration of the public system	OSPF 100 Advertised network segment: **192.168.0.0/30** Static routes are imported.	OSPF 100 Advertised network segment: **192.168.0.8/30** Static routes are imported.
	OSPF configuration of **vsysa**	OSPF 200 Bound VPN instance: vsysa Advertised network segment: **192.168.1.0/30** Static routes are imported.	OSPF 200 Bound VPN instance: vsysa Advertised network segment: **192.168.1.8/30** Static routes are imported.

Table 7-4 Data planning of switches

VLAN	Member Interface 1	Member Interface 2	Member Interface 3
10 (public)	GE1/0/15	GE1/0/16	GE1/0/17
30 (vsysa)	GE1/0/18	GE1/0/19	GE1/0/20

 Copyright © Huawei Technologies Co., Ltd.

Table 7-5 Data planning of RouterA

Item	Data	Description
Interfaces	Interface number: GigabitEthernet 1/0/1 IP address: 192.168.0.1/30	Connecting to the public system on the DeviceA
	Interface number: GigabitEthernet 1/0/2 IP address: 192.168.0.5/30	Connecting to RouterB
	Interface number: GigabitEthernet 1/0/3 IP address: 192.168.1.1/30	Connecting to **vsysa** on the DeviceA
	Interface number: GigabitEthernet 1/0/4 IP address: 192.168.1.5/30	Connecting to RouterB
OSPF	OSPF 100 Advertised network segment: 192.168.0.0/30 and 192.168.0.4/30 Default routes are imported.	-
	OSPF 200 Advertised network segment: 192.168.1.0/30 and 192.168.1.4/30 Default routes are imported.	-

Table 7-6 Data planning of RouterB

Item	Data	Description
Interfaces	Interface number: GigabitEthernet 1/0/1 IP address: 192.168.0.9/30	Connecting to the public system on the DeviceB
	Interface number: GigabitEthernet 1/0/2 IP address: 192.168.0.6/30	Connecting to RouterA
	Interface number: GigabitEthernet 1/0/3 IP address: 192.168.1.9/30	Connecting to **vsysa** on the DeviceB

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
	Interface number: GigabitEthernet 1/0/4 IP address: 192.168.1.6/30	Connecting to RouterA
OSPF	OSPF 100 Advertised network segment: 192.168.0.8/30 and 192.168.0.4/30 Default routes are imported.	-
	OSPF 200 Advertised network segment: 192.168.1.8/30 and 192.168.1.4/30 Default routes are imported.	-

Procedure

Step 1 Create virtual system **vsysa** and assign interfaces to it.

NOTE

The virtual system names and IDs on DeviceA and DeviceB must be the same. You can run the **display vsys** command on both devices to compare the configurations after virtual systems are created.

DeviceA	DeviceB
# Enable the virtual system function on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vsys enable**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vsys enable**
# Create a virtual system on DeviceA and DeviceB and assign interfaces and a public address to it. The public address is used in the NAT address pool.	
[DeviceA] **vsys name vsysa** [DeviceA-vsys-vsysa] **assign interface ge 0/0/3** [DeviceA-vsys-vsysa] **assign interface ge 0/0/4** [DeviceA-vsys-vsysa] **assign global-ip 1.1.1.2 1.1.1.2 exclusive** [DeviceA-vsys-vsysa] **quit**	[DeviceB] **vsys name vsysa** [DeviceB-vsys-vsysa] **assign interface ge 0/0/3** [DeviceB-vsys-vsysa] **assign interface ge 0/0/4** [DeviceB-vsys-vsysa] **assign global-ip 1.1.1.2 1.1.1.2 exclusive** [DeviceB-vsys-vsysa] **quit**

Step 2 Configure interfaces.

DeviceA	DeviceB
# Configure interfaces of the public system on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 192.168.0.2 30** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 10.3.1.2 24** [DeviceA-GE0/0/2] **vrrp vrid 1 virtual-ip 10.3.1.1 active** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 192.168.0.10 30** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 10.3.1.3 24** [DeviceB-GE0/0/2] **vrrp vrid 1 virtual-ip 10.3.1.1 standby** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign public system interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/2** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/2** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure interfaces of the virtual system on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 192.168.1.2 30** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/4** [DeviceA-GE0/0/4] **ip address 10.3.2.2 24** [DeviceA-GE0/0/4] **vrrp vrid 2 virtual-ip 10.3.2.1 active** [DeviceA-GE0/0/4] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 192.168.1.10 30** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/4** [DeviceB-GE0/0/4] **ip address 10.3.2.3 24** [DeviceB-GE0/0/4] **vrrp vrid 2 virtual-ip 10.3.2.1 standby** [DeviceB-GE0/0/4] **quit**
# Assign virtual system interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **firewall zone untrust** [DeviceA-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceA-vsysa-zone-untrust] **quit** [DeviceA-vsysa] **firewall zone trust** [DeviceA-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceA-vsysa-zone-trust] **quit** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **firewall zone untrust** [DeviceB-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceB-vsysa-zone-untrust] **quit** [DeviceB-vsysa] **firewall zone trust** [DeviceB-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceB-vsysa-zone-trust] **quit** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 3 Configure static routes.

DeviceA	DeviceB
# Configure a blackhole route pointing to the addresses in the NAT address pool of the public system on DeviceA and DeviceB.	
[DeviceA] **ip route-static 1.1.1.1 32 null 0**	[DeviceB] **ip route-static 1.1.1.1 32 null 0**
# Configure a blackhole route pointing to the addresses in the NAT address pool of the virtual system on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **ip route-static 1.1.1.2 32 null 0** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **ip route-static 1.1.1.2 32 null 0** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 4 Configure OSPF.

DeviceA	DeviceB
[DeviceA] **ospf 100** [DeviceA-ospf-100] **import-route static** [DeviceA-ospf-100] **area 0** [DeviceA-ospf-100-area-0.0.0.0] **network 192.168.0.0 0.0.0.3** [DeviceA-ospf-100-area-0.0.0.0] **quit** [DeviceA-ospf-100] **quit** [DeviceA] **ospf 200 vpn-instance vsysa** [DeviceA-ospf-200] **import-route static** [DeviceA-ospf-200] **area 0** [DeviceA-ospf-200-area-0.0.0.0] **network 192.168.1.0 0.0.0.3** [DeviceA-ospf-200-area-0.0.0.0] **quit** [DeviceA-ospf-200] **quit**	[DeviceB] **ospf 100** [DeviceB-ospf-100] **import-route static** [DeviceB-ospf-100] **area 0** [DeviceB-ospf-100-area-0.0.0.0] **network 192.168.0.8 0.0.0.3** [DeviceB-ospf-100-area-0.0.0.0] **quit** [DeviceB-ospf-100] **quit** [DeviceB] **ospf 200 vpn-instance vsysa** [DeviceB-ospf-200] **import-route static** [DeviceB-ospf-200] **area 0** [DeviceB-ospf-200-area-0.0.0.0] **network 192.168.1.8 0.0.0.3** [DeviceB-ospf-200-area-0.0.0.0] **quit** [DeviceB-ospf-200] **quit**

Step 5 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 6 Configure hot standby.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3** [DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp adjust ospf-cost enable** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3** [DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp adjust ospf-cost enable** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 7 Configure security policies.

After hot standby relationship is established, the security policy configured on DeviceA is automatically backed up to DeviceB.

Configure a security policy for the public system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Configure a security policy for the virtual system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] security-policy
HRP_M[DeviceA-vsysa-policy-security] rule name policy_sec
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-vsysa-policy-security] quit
HRP_M[DeviceA-vsysa] quit
HRP_M<DeviceA-vsysa> quit
```

Step 8 Configure NAT policies.

After hot standby relationship is established, the NAT policy configured on DeviceA is automatically backed up to DeviceB.

Configure a NAT policy for the public system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.1 1.1.1.1
HRP_M[DeviceA-address-group-addressgroup1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-policy-nat] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a NAT policy for the virtual system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] nat address-group addressgroup1
HRP_M[DeviceA-vsysa-address-group-addressgroup1] section 0 1.1.1.2 1.1.1.2
HRP_M[DeviceA-vsysa-address-group-addressgroup1] quit
HRP_M[DeviceA-vsysa] nat-policy
HRP_M[DeviceA-vsysa-policy-nat] rule name policy_nat
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-vsysa-policy-nat-rule
-policy_nat] quit
HRP_M[DeviceA-vsysa-policy-nat] quit
HRP_M[DeviceA-vsysa] quit
```

Step 9 Configure the switch.

NOTE

The following part uses a Huawei switch to illustrate the configuration.

Configure the switch.

```
[Switch] vlan batch 10 30
[Switch] interface GigabitEthernet 1/0/15
[Switch-GigabitEthernet1/0/15] port link-type access
[Switch-GigabitEthernet1/0/15] port default vlan 10
[Switch-GigabitEthernet1/0/15] quit
[Switch] interface GigabitEthernet 1/0/16
[Switch-GigabitEthernet1/0/16] port link-type access
[Switch-GigabitEthernet1/0/16] port default vlan 10
[Switch-GigabitEthernet1/0/16] quit
[Switch] interface GigabitEthernet 1/0/17
[Switch-GigabitEthernet1/0/17] port link-type access
[Switch-GigabitEthernet1/0/17] port default vlan 10
[Switch-GigabitEthernet1/0/17] quit
[Switch] interface GigabitEthernet 1/0/18
[Switch-GigabitEthernet1/0/18] port link-type access
[Switch-GigabitEthernet1/0/18] port default vlan 30
[Switch-GigabitEthernet1/0/18] quit
[Switch] interface GigabitEthernet 1/0/19
[Switch-GigabitEthernet1/0/19] port link-type access
[Switch-GigabitEthernet1/0/19] port default vlan 30
[Switch-GigabitEthernet1/0/19] quit
[Switch] interface GigabitEthernet 1/0/20
[Switch-GigabitEthernet1/0/20] port link-type access
[Switch-GigabitEthernet1/0/20] port default vlan 30
[Switch-GigabitEthernet1/0/20] quit
```

Step 10 Configure the routers.

NOTE

The following part uses Huawei routers to illustrate the configuration.

 Copyright © Huawei Technologies Co., Ltd.

RouterA	RouterB
[RouterA] **interface GigabitEthernet 1/0/1** [RouterA-GigabitEthernet1/0/1] **ip address 192.168.0.1 30** [RouterA-GigabitEthernet1/0/1] **quit** [RouterA] **interface GigabitEthernet 1/0/2** [RouterA-GigabitEthernet1/0/2] **ip address 192.168.0.5 30** [RouterA-GigabitEthernet1/0/2] **quit** [RouterA] **interface GigabitEthernet 1/0/3** [RouterA-GigabitEthernet1/0/3] **ip address 192.168.1.1 30** [RouterA-GigabitEthernet1/0/3] **quit** [RouterA] **interface GigabitEthernet 1/0/4** [RouterA-GigabitEthernet1/0/4] **ip address 192.168.1.5 30** [RouterA-GigabitEthernet1/0/4] **quit** [RouterA] **ospf 100** [RouterA-ospf-100] **default-route-advertise** [RouterA-ospf-100] **area 0** [RouterA-ospf-100-area-0.0.0.0] **network 192.168.0.0 0.0.0.3** [RouterA-ospf-100-area-0.0.0.0] **network 192.168.0.4 0.0.0.3** [RouterA-ospf-100-area-0.0.0.0] **quit** [RouterA-ospf-100] **quit** [RouterA] **ospf 200** [RouterA-ospf-200] **default-route-advertise** [RouterA-ospf-200] **area 0** [RouterA-ospf-200-area-0.0.0.0] **network 192.168.1.0 0.0.0.3** [RouterA-ospf-200-area-0.0.0.0] **network 192.168.1.4 0.0.0.3** [RouterA-ospf-200-area-0.0.0.0] **quit** [RouterA-ospf-200] **quit**	[RouterB] **interface GigabitEthernet 1/0/1** [RouterB-GigabitEthernet1/0/1] **ip address 192.168.0.9 30** [RouterB-GigabitEthernet1/0/1] **quit** [RouterB] **interface GigabitEthernet 1/0/2** [RouterB-GigabitEthernet1/0/2] **ip address 192.168.0.6 30** [RouterB-GigabitEthernet1/0/2] **quit** [RouterB] **interface GigabitEthernet 1/0/3** [RouterB-GigabitEthernet1/0/3] **ip address 192.168.1.9 30** [RouterB-GigabitEthernet1/0/3] **quit** [RouterB] **interface GigabitEthernet 1/0/4** [RouterB-GigabitEthernet1/0/4] **ip address 192.168.1.6 30** [RouterB-GigabitEthernet1/0/4] **quit** [RouterB] **ospf 100** [RouterB-ospf-100] **default-route-advertise** [RouterB-ospf-100] **area 0** [RouterB-ospf-100-area-0.0.0.0] **network 192.168.0.8 0.0.0.3** [RouterB-ospf-100-area-0.0.0.0] **network 192.168.0.4 0.0.0.3** [RouterB-ospf-100-area-0.0.0.0] **quit** [RouterB-ospf-100] **quit** [RouterB] **ospf 200** [RouterB-ospf-200] **default-route-advertise** [RouterB-ospf-200] **area 0** [RouterB-ospf-200-area-0.0.0.0] **network 192.168.1.8 0.0.0.3** [RouterB-ospf-200-area-0.0.0.0] **network 192.168.1.4 0.0.0.3** [RouterB-ospf-200-area-0.0.0.0] **quit** [RouterB-ospf-200] **quit**

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Access the Internet from the enterprise network. The access succeeds. Check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M[DeviceA] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa 10.3.2.10:2057[1.1.1.2:2048]-->3.3.3.3:2048 icmp VPN:public -> public 10.3.1.10:2057[1.1.1.1:2048]-->3.3.3.3:2048	HRP_S[DeviceB] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa **Remote** 10.3.2.10:2057[1.1.1.2:2048]-->3.3.3.3:2048 icmp VPN:public -> public **Remote** 10.3.1.10:2057[1.1.1.1:2048]-->3.3.3.3:2048

   As shown in the previous information, a session tagged with **Remote** is created on DeviceB, indicating that the session is successfully synchronized after hot standby is configured.
3. Ping an IP address on the Internet from an intranet PC, remove the network cable from GE 0/0/1 on DeviceA, and check device status switchover and ping

 Copyright © Huawei Technologies Co., Ltd.

packet discard statistics. Then insert the network cable back to GE 0/0/1 on DeviceA and check device status switchover and ping packet discard statistics again.

Configuration Scripts

- Public system

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# sysname DeviceA # vsys enable # vsys name vsysa 1 assign interface GE0/0/3 assign interface GE0/0/4 assign global-ip 1.1.1.2 1.1.1.2 exclusive # hrp enable hrp device **active** hrp adjust ospf-cost enable hrp interface GE0/0/7 remote **10.10.0.2** hrp track interface GE0/0/1 hrp track interface GE0/0/3 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! J6+;U#>V\!_e1NY[iGLXjT %k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!! Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+ %# # interface GE0/0/1 ip address **192.168.0.2** 255.255.255.252 # interface GE0/0/2 ip address **10.3.1.2** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **active** # interface GE0/0/3 ip address **192.168.1.2** 255.255.255.252 # interface GE0/0/4 ip address **10.3.2.2** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **active** # interface GE0/0/7 ip address **10.10.0.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # ip route-static 1.1.1.1 255.255.255.255 null 0 # ospf 100 import-route static area 0.0.0.0 network **192.168.0.0** 0.0.0.3 # ospf 200 vpn-instance vsysa import-route static area 0.0.0.0 network **192.168.1.0** 0.0.0.3 # security-policy rule name ha_local_to_dmz source-zone local	# sysname DeviceB # vsys enable # vsys name vsysa 1 assign interface GE0/0/3 assign interface GE0/0/4 assign global-ip 1.1.1.2 1.1.1.2 exclusive # hrp enable hrp device **standby** hrp adjust ospf-cost enable hrp interface GE0/0/7 remote **10.10.0.1** hrp track interface GE0/0/1 hrp track interface GE0/0/3 hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! \FR0@B|5m51t2(SLB$(Yzq_KUB| V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t \i4 t;1e+vR$$U!!!!!%+%# # interface GE0/0/1 ip address **192.168.0.10** 255.255.255.252 # interface GE0/0/2 ip address **10.3.1.3** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **standby** # interface GE0/0/3 ip address **192.168.1.10** 255.255.255.252 # interface GE0/0/4 ip address **10.3.2.3** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **standby** # interface GE0/0/7 ip address **10.10.0.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # ip route-static 1.1.1.1 255.255.255.255 null 0 # ospf 100 import-route static area 0.0.0.0 network **192.168.0.8** 0.0.0.3 # ospf 200 vpn-instance vsysa import-route static area 0.0.0.0 network **192.168.1.8** 0.0.0.3 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 action source-nat address-group addressgroup1 #	destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 action source-nat address-group addressgroup1 #

- **vsysa**

DeviceA	DeviceB
# switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 1.1.1.2 255.255.255.255 null 0 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.2 1.1.1.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #	# switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 1.1.1.2 255.255.255.255 null 0 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.2 1.1.1.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #

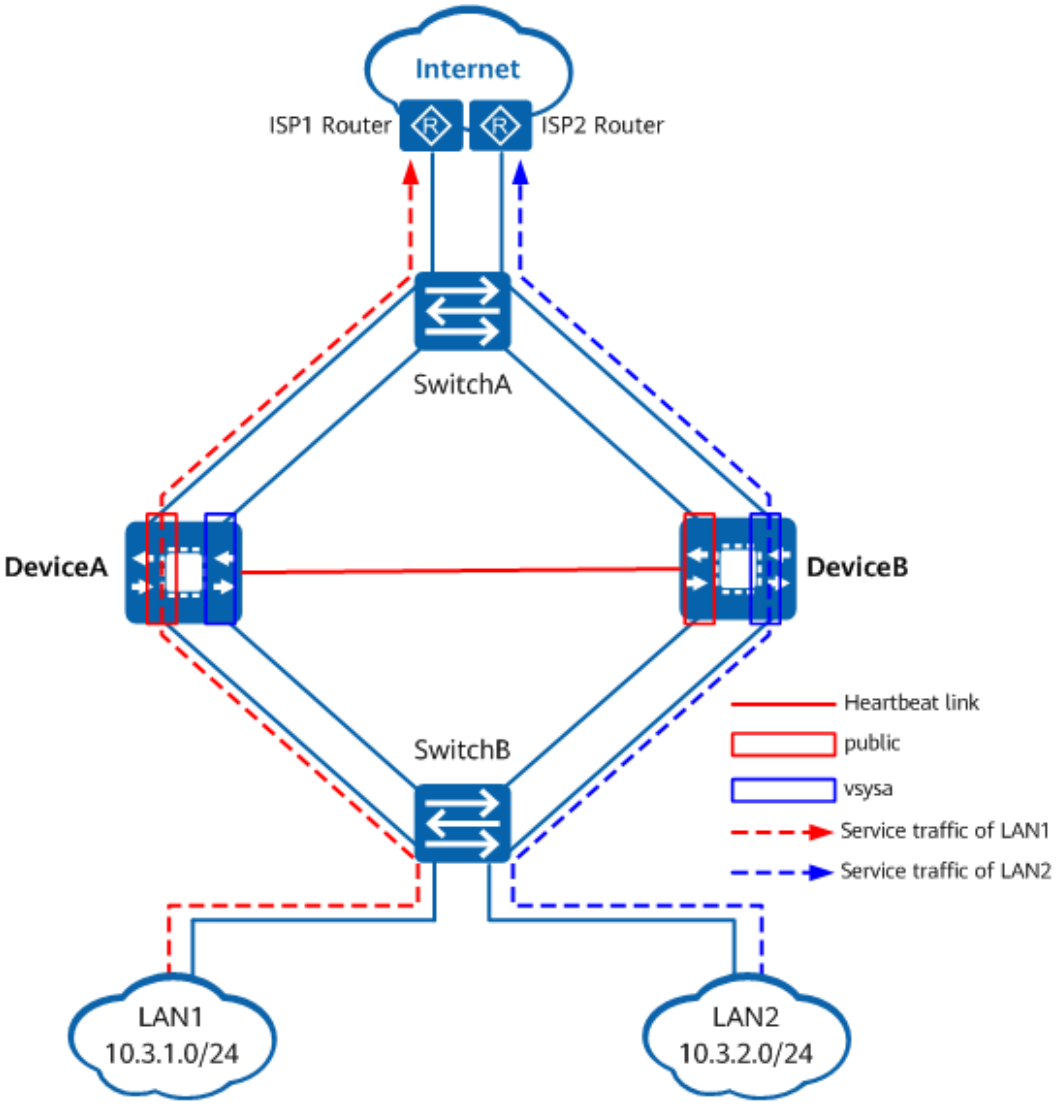
 Copyright © Huawei Technologies Co., Ltd.

7.6.3 CLI: Example for Configuring Hot Standby (Load Balancing) of Virtual Systems on Firewalls Connecting to Switches in Upstream and Downstream Directions

Networking Requirements

As shown in **Figure 7-42**, two network segments on the enterprise network need to be separated. SwitchA and SwitchB use VLANs to separate the two network segments, and the devices use virtual systems to separate them. The two devices work in load sharing mode. In normal situations, DeviceA forwards traffic from LAN1, and DeviceB forwards traffic from LAN2. If one device fails, traffic from both LAN1 and LAN2 is forwarded by the other device. This ensures that the services are not interrupted.

Figure 7-42 Hot standby networking when virtual systems are configured



The detailed data planning is as follows.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-43 Data planning scheme

NOTE

In this example, interfaces 1, 2, 3, 4, and 7 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/7, respectively.

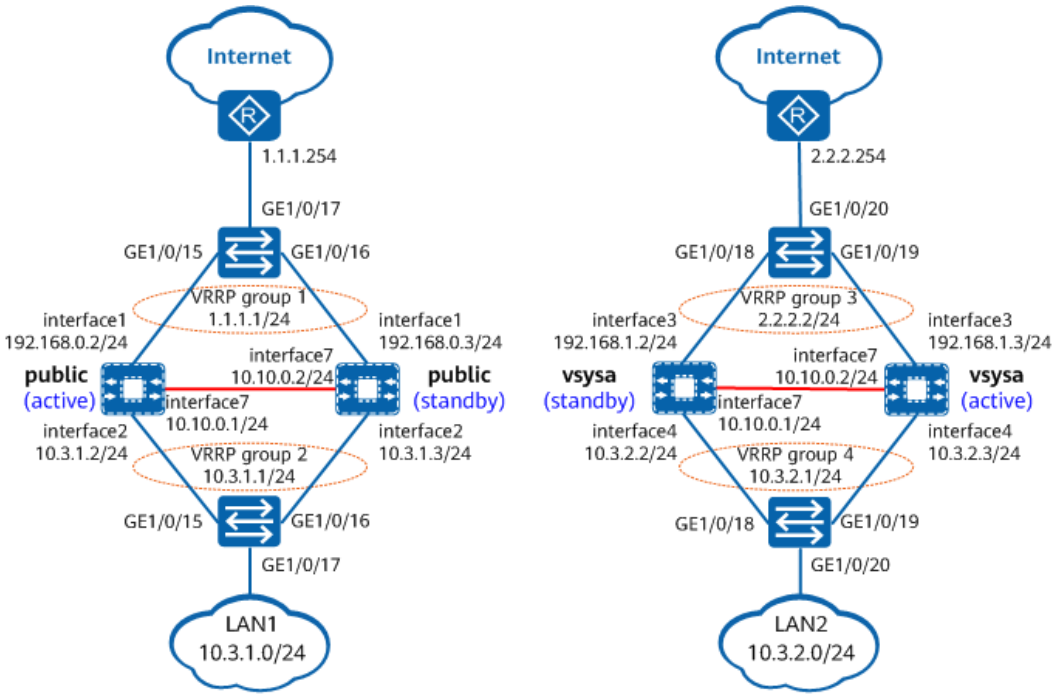


Table 7-7 Data planning of DeviceA and DeviceB

Item	Sub-item	Data of DeviceA	Data of DeviceB
Interfaces	Public interface of the public system	Interface number: GE 0/0/1 IP address: **192.168.0.2/24** Security zone: untrust	Interface number: GE 0/0/1 IP address: **192.168.0.3/24** Security zone: untrust
	Private interface of the public system	Interface number: GE 0/0/2 IP address: **10.3.1.2/24** Security zone: trust	Interface number: GE 0/0/2 IP address: **10.3.1.3/24** Security zone: trust
	Public interface of virtual system **vsysa**	Interface number: GE 0/0/3 IP address: **192.168.1.2/24** Security zone: untrust	Interface number: GE 0/0/3 IP address: **192.168.1.3/24** Security zone: untrust
	Private interface of virtual system **vsysa**	Interface number: GE 0/0/4 IP address: **10.3.2.2/24** Security zone: trust	Interface number: GE 0/0/4 IP address: **10.3.2.3/24** Security zone: trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Data of DeviceA	Data of DeviceB
	Heartbeat interface	Interface number: GE 0/0/7 IP address: **10.10.0.1/24** Security zone: DMZ	Interface number: GE 0/0/7 IP address: **10.10.0.2/24** Security zone: DMZ
VRRP groups	VRRP group 1	1.1.1.1/24 **active**	1.1.1.1/24 **standby**
	VRRP group 2	10.3.1.1/24 **active**	10.3.1.1/24 **standby**
	VRRP group 3	2.2.2.2/24 **standby**	2.2.2.2/24 **active**
	VRRP group 4	10.3.2.1/24 **standby**	10.3.2.1/24 **active**
Routes	Default route of the public system	Destination IP address: 0.0.0.0 Next hop: 1.1.1.254	Destination IP address: 0.0.0.0 Next hop: 1.1.1.254
	Default route of virtual system **vsysa**	Destination IP address: 0.0.0.0 Next hop: 2.2.2.254	Destination IP address: 0.0.0.0 Next hop: 2.2.2.254

Table 7-8 Data planning of switches

Device	VLAN	Member Interface 1	Member Interface 2	Member Interface 3
SwitchA	10 (public)	GE1/0/15	GE1/0/16	GE1/0/17
	30 (vsysa)	GE1/0/18	GE1/0/19	GE1/0/20
SwitchB	20 (public)	GE1/0/15	GE1/0/16	GE1/0/17
	40 (vsysa)	GE1/0/18	GE1/0/19	GE1/0/20

Procedure

Step 1 Create virtual system **vsysa** and assign interfaces to it.

NOTE

The virtual system names and IDs on DeviceA and DeviceB must be the same. You can run the **display vsys** command on both devices to compare the configurations after virtual systems are created.

DeviceA	DeviceB
# Enable the virtual system function on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vsys enable**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vsys enable**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Create a virtual system on DeviceA and DeviceB and assign interfaces and a public address to it. The public address is used in the NAT address pool.	
[DeviceA] **vsys name vsysa** [DeviceA-vsys-vsysa] **assign interface ge 0/0/3** [DeviceA-vsys-vsysa] **assign interface ge 0/0/4** [DeviceA-vsys-vsysa] **assign global-ip 2.2.2.2 2.2.2.2 exclusive** [DeviceA-vsys-vsysa] **quit**	[DeviceB] **vsys name vsysa** [DeviceB-vsys-vsysa] **assign interface ge 0/0/3** [DeviceB-vsys-vsysa] **assign interface ge 0/0/4** [DeviceB-vsys-vsysa] **assign global-ip 2.2.2.2 2.2.2.2 exclusive** [DeviceB-vsys-vsysa] **quit**

Step 2 Configure interfaces.

DeviceA	DeviceB
# Configure IP addresses and VRRP groups for public system interfaces on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 192.168.0.2 24** [DeviceA-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.1 24 active** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 10.3.1.2 24** [DeviceA-GE0/0/2] **vrrp vrid 2 virtual-ip 10.3.1.1 active** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 192.168.0.3 24** [DeviceB-GE0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.1 24 standby** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 10.3.1.3 24** [DeviceB-GE0/0/2] **vrrp vrid 2 virtual-ip 10.3.1.1 standby** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign public system interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/2** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/2** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure IP addresses and VRRP groups for virtual system interfaces on DeviceA and DeviceB.	
[Device] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 192.168.1.2 24** [DeviceA-GE0/0/3] **vrrp vrid 3 virtual-ip 2.2.2.2 24 standby** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/4** [DeviceA-GE0/0/4] **ip address 10.3.2.2 24** [DeviceA-GE0/0/4] **vrrp vrid 4 virtual-ip 10.3.2.1 standby** [DeviceA-GE0/0/4] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 192.168.1.3 24** [DeviceB-GE0/0/3] **vrrp vrid 3 virtual-ip 2.2.2.2 24 active** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/4** [DeviceB-GE0/0/4] **ip address 10.3.2.3 24** [DeviceB-GE0/0/4] **vrrp vrid 4 virtual-ip 10.3.2.1 active** [DeviceB-GE0/0/4] **quit**
# Assign virtual system interfaces to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **firewall zone untrust** [DeviceA-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceA-vsysa-zone-untrust] **quit** [DeviceA-vsysa] **firewall zone trust** [DeviceA-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceA-vsysa-zone-trust] **quit** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **firewall zone untrust** [DeviceB-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceB-vsysa-zone-untrust] **quit** [DeviceB-vsysa] **firewall zone trust** [DeviceB-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceB-vsysa-zone-trust] **quit** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 3 Configure static routes.

DeviceA	DeviceB
# Configure a default route from the public system to the Internet and set the next hop to the IP address of an ISP router on DeviceA and DeviceB.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.254**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.254**
# Configure a default route from the virtual system to the Internet and set the next hop to the IP address of an ISP router on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **ip route-static 0.0.0.0 0.0.0.0 2.2.2.254** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **ip route-static 0.0.0.0 0.0.0.0 2.2.2.254** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 4 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure hot standby.

DeviceA	DeviceB
# Configure quick session backup on DeviceA and DeviceB in case of inconsistent forward and return packet paths.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**
# To prevent port conflicts in address translation on the devices in load sharing mode, configure available port ranges on DeviceA and DeviceB. **NOTE** In the hot standby load sharing scenario, If NAPT is configured, DeviceA and DeviceB may have conflicting public ports. To prevent such conflicts, configure respective NAT resources (including public IP addresses and ports) for the devices. You can run the **hrp nat resource primary-group** command on the active device. The standby device will automatically generate the **hrp nat resource secondary-group** command (if you run the **hrp nat resource secondary-group** command on the active device, the standby device will automatically generate the **hrp nat resource primary-group** command).	
HRP_M[DeviceA] **hrp nat resource primary-group**	HRP_S[DeviceB] **hrp nat resource secondary-group**

Step 6 Configure security policies.

After hot standby relationship is established, the security policy configured on DeviceA is automatically backed up to DeviceB.

Configure a security policy for the public system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Configure a security policy for the virtual system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] security-policy
HRP_M[DeviceA-vsysa-policy-security] rule name policy_sec
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-vsysa-policy-security] quit
HRP_M[DeviceA-vsysa] quit
HRP_M<DeviceA-vsysa> quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Configure NAT policies.

After hot standby relationship is established, the NAT policy configured on DeviceA is automatically backed up to DeviceB.

Configure a NAT policy for the public system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.1 1.1.1.1
HRP_M[DeviceA-address-group-addressgroup1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-policy-nat] quit
```

Configure a NAT policy for the virtual system to allow intranet users to access the Internet.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] nat address-group addressgroup1
HRP_M[DeviceA-vsysa-address-group-addressgroup1] section 0 2.2.2.2 2.2.2.2
HRP_M[DeviceA-vsysa-address-group-addressgroup1] quit
HRP_M[DeviceA-vsysa] nat-policy
HRP_M[DeviceA-vsysa-policy-nat] rule name policy_nat
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-vsysa-policy-nat] quit
HRP_M[DeviceA-vsysa] quit
```

Step 8 Configure the switches.

NOTE

The following part uses Huawei switches to illustrate the configuration.

 Copyright © Huawei Technologies Co., Ltd.

SwitchA	SwitchB
[SwitchA] **vlan batch 10 30** [SwitchA] **interface GigabitEthernet 1/0/15** [SwitchA-GigabitEthernet1/0/15] **port link-type access** [SwitchA-GigabitEthernet1/0/15] **port default vlan 10** [SwitchA-GigabitEthernet1/0/15] **quit** [SwitchA] **interface GigabitEthernet 1/0/16** [SwitchA-GigabitEthernet1/0/16] **port link-type access** [SwitchA-GigabitEthernet1/0/16] **port default vlan 10** [SwitchA-GigabitEthernet1/0/16] **quit** [SwitchA] **interface GigabitEthernet 1/0/17** [SwitchA-GigabitEthernet1/0/17] **port link-type access** [SwitchA-GigabitEthernet1/0/17] **port default vlan 10** [SwitchA-GigabitEthernet1/0/17] **quit** [SwitchA] **interface GigabitEthernet 1/0/18** [SwitchA-GigabitEthernet1/0/18] **port link-type access** [SwitchA-GigabitEthernet1/0/18] **port default vlan 30** [SwitchA-GigabitEthernet1/0/18] **quit** [SwitchA] **interface GigabitEthernet 1/0/19** [SwitchA-GigabitEthernet1/0/19] **port link-type access** [SwitchA-GigabitEthernet1/0/19] **port default vlan 30** [SwitchA-GigabitEthernet1/0/19] **quit** [SwitchA] **interface GigabitEthernet 1/0/20** [SwitchA-GigabitEthernet1/0/20] **port link-type access** [SwitchA-GigabitEthernet1/0/20] **port default vlan 30** [SwitchA-GigabitEthernet1/0/20] **quit**	[SwitchB] **vlan batch 20 40** [SwitchB] **interface GigabitEthernet 1/0/15** [SwitchB-GigabitEthernet1/0/15] **port link-type access** [SwitchB-GigabitEthernet1/0/15] **port default vlan 20** [SwitchB-GigabitEthernet1/0/15] **quit** [SwitchB] **interface GigabitEthernet 1/0/16** [SwitchB-GigabitEthernet1/0/16] **port link-type access** [SwitchB-GigabitEthernet1/0/16] **port default vlan 20** [SwitchB-GigabitEthernet1/0/16] **quit** [SwitchB] **interface GigabitEthernet 1/0/17** [SwitchB-GigabitEthernet1/0/17] **port link-type trunk** [SwitchB-GigabitEthernet1/0/17] **port trunk allow-pass vlan 20** [SwitchB-GigabitEthernet1/0/17] **quit** [SwitchB] **interface GigabitEthernet 1/0/18** [SwitchB-GigabitEthernet1/0/18] **port link-type access** [SwitchB-GigabitEthernet1/0/18] **port default vlan 40** [SwitchB-GigabitEthernet1/0/18] **quit** [SwitchB] **interface GigabitEthernet 1/0/19** [SwitchB-GigabitEthernet1/0/19] **port link-type access** [SwitchB-GigabitEthernet1/0/19] **port default vlan 40** [SwitchB-GigabitEthernet1/0/19] **quit** [SwitchB] **interface GigabitEthernet 1/0/20** [SwitchB-GigabitEthernet1/0/20] **port link-type trunk** [SwitchB-GigabitEthernet1/0/20] **port trunk allow-pass vlan 40** [SwitchB-GigabitEthernet1/0/20] **quit**

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Access the Internet from the enterprise network. The access succeeds. Check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M[DeviceA] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa **Remote** 10.3.2.10:2057[2.2.2.2:2048]-->2.2.2.254:2048 icmp VPN:public -> public 10.3.1.10:2057[1.1.1.1:2048]-->1.1.1.254:2048	HRP_S[DeviceB] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa 10.3.2.10:2057[2.2.2.2:2048]-->2.2.2.254:2048 icmp VPN:public -> public **Remote** 10.3.1.10:2057[1.1.1.1:2048]-->1.1.1.254:2048

As shown in the previous information, a session tagged with **Remote** is created on DeviceA and DeviceB, indicating that the session is successfully synchronized after hot standby is configured.

 Copyright © Huawei Technologies Co., Ltd.

3. Ping an IP address on the Internet from an intranet PC, remove the network cable from GE 0/0/1 on DeviceA, and check device status switchover and ping packet discard statistics. Then insert the network cable back to GE 0/0/1 on DeviceA and check device status switchover and ping packet discard statistics again.

Configuration Scripts

- Public system

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# sysname DeviceA # vsys enable # vsys name vsysa 1 assign interface GE0/0/3 assign interface GE0/0/4 assign global-ip 2.2.2.2 2.2.2.2 exclusive # hrp enable hrp interface GE0/0/7 remote **10.10.0.2** hrp mirror session enable hrp nat resource **primary-group** hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! J6+;U#>V\!_e1NY[iGLXjT %k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!! Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+ %# # interface GE0/0/1 ip address **192.168.0.2** 255.255.255.0 vrrp vrid 1 virtual-ip 1.1.1.1 24 **active** # interface GE0/0/2 ip address **10.3.1.2** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.1.1 **active** # interface GE0/0/3 ip address **192.168.1.2** 255.255.255.0 vrrp vrid 3 virtual-ip 2.2.2.2 24 **standby** # interface GE0/0/4 ip address **10.3.2.2** 255.255.255.0 vrrp vrid 4 virtual-ip 10.3.2.1 **standby** # interface GE0/0/7 ip address **10.10.0.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # ip route-static 0.0.0.0 0.0.0.0 1.1.1.254 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit	# sysname DeviceB # vsys enable # vsys name vsysa 1 assign interface GE0/0/3 assign interface GE0/0/4 assign global-ip 2.2.2.2 2.2.2.2 exclusive # hrp enable hrp interface GE0/0/7 remote **10.10.0.1** hrp mirror session enable hrp nat resource **secondary-group** hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! \FR0@B|5m51t2(SLB$(Yzq_KUB\| V43Td3,.!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t \i4 t;1e+vR$$U!!!!!%+%# # interface GE0/0/1 ip address **192.168.0.3** 255.255.255.0 vrrp vrid 1 virtual-ip 1.1.1.1 24 **standby** # interface GE0/0/2 ip address **10.3.1.3** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.1.1 **standby** # interface GE0/0/3 ip address **192.168.1.3** 255.255.255.0 vrrp vrid 3 virtual-ip 2.2.2.2 24 **active** # interface GE0/0/4 ip address **10.3.2.3** 255.255.255.0 vrrp vrid 4 virtual-ip 10.3.2.1 **active** # interface GE0/0/7 ip address **10.10.0.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # ip route-static 0.0.0.0 0.0.0.0 1.1.1.254 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit #

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 action source-nat address-group addressgroup1 #	nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 action source-nat address-group addressgroup1 #

- **vsysa**

DeviceA	DeviceB
# switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 0.0.0.0 0.0.0.0 2.2.2.254 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit # nat address-group addressgroup1 section 0 2.2.2.2 2.2.2.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #	# switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 0.0.0.0 0.0.0.0 2.2.2.254 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit # nat address-group addressgroup1 section 0 2.2.2.2 2.2.2.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #

7.6.4 CLI: Example for Configuring Hot Standby (Load Balancing) of Virtual Systems on Firewalls Connecting to Upstream Routers and Downstream Switches

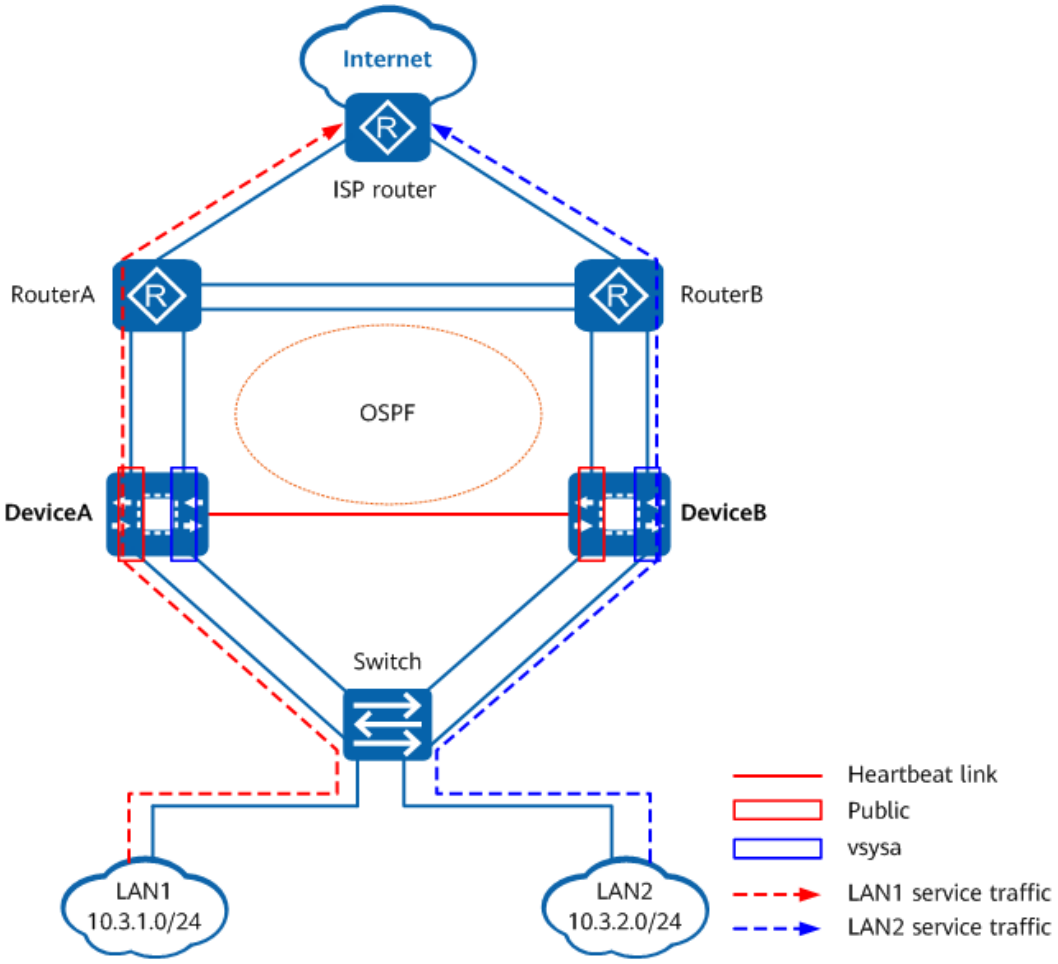
Networking Requirements

As shown in **Figure 7-44**, two network segments on the enterprise intranet need to be isolated. To isolate them, the switch uses VLANs, whereas DeviceA and DeviceB use virtual systems. DeviceA and DeviceB connect to upstream routers,

 Copyright © Huawei Technologies Co., Ltd.

and OSPF runs between them and the routers. The two devices work in load sharing mode. During normal operation, DeviceA forwards traffic from LAN1, and DeviceB forwards traffic from LAN2. If one device fails, traffic from both LAN1 and LAN2 is forwarded by the other device. This ensures that the services are not interrupted.

Figure 7-44 Hot standby networking where virtual systems are configured



The detailed data plan is as follows.

Figure 7-45 Data plan scheme

NOTE

In this example, interface1, interface2, interface3, interface4, and interface7 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.

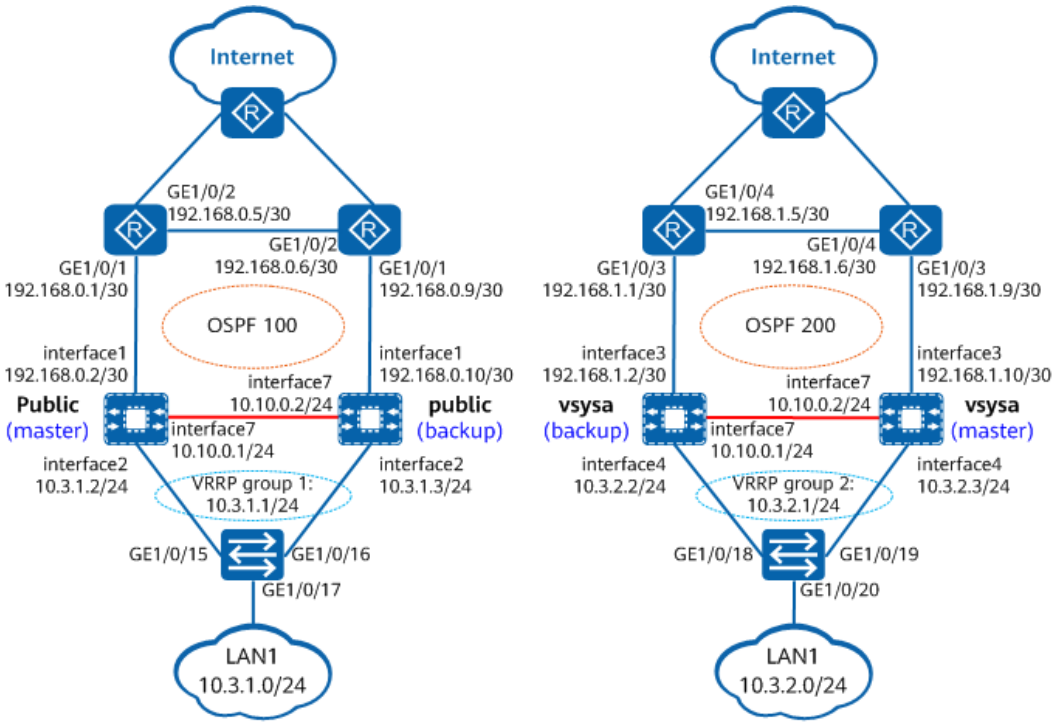


Table 7-9 Data plan of DeviceA and DeviceB

Item	Sub-item	Data of DeviceA	Data of DeviceB
Interfaces	Public network interface of the public system	Interface number: GE 0/0/1 IP address: 192.168.0.2/30 Security zone: untrust	Interface number: GE 0/0/1 IP address: 192.168.0.10/30 Security zone: untrust
	Private network interface of the public system	Interface number: GE 0/0/2 IP address: 10.3.1.2/24 Security zone: trust	Interface number: GE 0/0/2 IP address: 10.3.1.3/24 Security zone: trust
	Public network interface of virtual system **vsysa**	Interface number: GE 0/0/3 IP address: 192.168.1.2/30 Security zone: untrust	Interface number: GE 0/0/3 IP address: 192.168.1.10/30 Security zone: untrust
	Private network interface of virtual system **vsysa**	Interface number: GE 0/0/4 IP address: 10.3.2.2/24 Security zone: trust	Interface number: GE 0/0/4 IP address: 10.3.2.3/24 Security zone: trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Data of DeviceA	Data of DeviceB
	Heartbeat interface	Interface number: GE 0/0/7 IP address: 10.10.0.1/24 Security zone: dmz	Interface number: GE 0/0/7 IP address: 10.10.0.2/24 Security zone: dmz
VRRP groups	VRRP group 1	**10.3.1.1/24 active**	**10.3.1.1/24 standby**
	VRRP group 2	**10.3.2.1/24 standby**	**10.3.2.1/24 active**
Routes	Blackhole route configured for the NAT address pool of public system **public** to prevent route loops	Blackhole route Destination IP address: 1.1.1.1/32	Blackhole route Destination IP address: 1.1.1.1/32
	Blackhole route configured for the NAT address pool of virtual system **vsysa** to prevent route loops	Blackhole route Destination IP address: 1.1.1.2/32	Blackhole route Destination IP address: 1.1.1.2/32
	OSPF configuration of public system **public**	OSPF 100 Advertised network segment: 192.168.0.0/30 Static routes imported	OSPF 100 Advertised network segment: 192.168.0.8/30 Static routes imported
	OSPF configuration of virtual system **vsysa**	OSPF 200 Bound VPN instance: vsysa Advertised network segment: 192.168.1.0/30 Static routes imported	OSPF 200 Bound VPN instance: vsysa Advertised network segment: 192.168.1.8/30 Static routes imported

Table 7-10 Data plan of the switch

VLAN	Member Interface 1	Member Interface 2	Member Interface 3
10 (public)	GE 1/0/15	GE 1/0/16	GE 1/0/17

 Copyright © Huawei Technologies Co., Ltd.

VLAN	Member Interface 1	Member Interface 2	Member Interface 3
30 (vsys a)	GE 1/0/18	GE 1/0/19	GE 1/0/20

Table 7-11 Data plan of RouterA

Item	Data	Description
Interfaces	Interface number: GigabitEthernet 1/0/1 IP address: 192.168.0.1/30	Connecting to public system **public** on DeviceA
	Interface number: GigabitEthernet 1/0/2 IP address: 192.168.0.5/30	Connecting to RouterB
	Interface number: GigabitEthernet 1/0/3 IP address: 192.168.1.1/30	Connecting to virtual system **vsysa** on DeviceA
	Interface number: GigabitEthernet 1/0/4 IP address: 192.168.1.5/30	Connecting to RouterB
OSPF	OSPF 100 Advertised network segments: 192.168.0.0/30 and 192.168.0.4/30 Default routes imported	-
	OSPF 200 Advertised network segments: 192.168.1.0/30 and 192.168.1.4/30 Default routes imported	-

Table 7-12 Data plan of RouterB

Item	Data	Description
Interfaces	Interface number: GigabitEthernet 1/0/1 IP address: 192.168.0.9/30	Connecting to public system **public** on DeviceB

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
	Interface number: GigabitEthernet 1/0/2 IP address: 192.168.0.6/30	Connecting to RouterA
	Interface number: GigabitEthernet 1/0/3 IP address: 192.168.1.9/30	Connecting to virtual system **vsysa** on DeviceB
	Interface number: GigabitEthernet 1/0/4 IP address: 192.168.1.6/30	Connecting to RouterA
OSPF	OSPF 100 Advertised network segments: 192.168.0.8/30 and 192.168.0.4/30 Default routes imported	-
	OSPF 200 Advertised network segments: 192.168.1.8/30 and 192.168.1.4/30 Default routes imported	-

Procedure

Step 1 Create virtual system **vsysa** and assign interfaces to it.

NOTE

The virtual system names and IDs on DeviceA and DeviceB must be the same. You can run the **display vsys** command on both devices to compare the configurations after virtual systems are created.

DeviceA	DeviceB
# Enable the virtual system function on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vsys enable**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vsys enable**
# Create a virtual system on DeviceA and DeviceB and assign interfaces and a public address to it. The public address is used in the NAT address pool.	
[DeviceA] **vsys name vsysa** [DeviceA-vsys-vsysa] **assign interface ge 0/0/3** [DeviceA-vsys-vsysa] **assign interface ge 0/0/4** [DeviceA-vsys-vsysa] **assign global-ip 1.1.1.2 1.1.1.2 exclusive** [DeviceA-vsys-vsysa] **quit**	[DeviceB] **vsys name vsysa** [DeviceB-vsys-vsysa] **assign interface ge 0/0/3** [DeviceB-vsys-vsysa] **assign interface ge 0/0/4** [DeviceB-vsys-vsysa] **assign global-ip 1.1.1.2 1.1.1.2 exclusive** [DeviceB-vsys-vsysa] **quit**

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure interfaces.

DeviceA	DeviceB
# Configure public system interfaces and VRRP groups on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 192.168.0.2 30** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 10.3.1.2 24** [DeviceA-GE0/0/2] **vrrp vrid 1 virtual-ip 10.3.1.1 active** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 192.168.0.10 30** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 10.3.1.3 24** [DeviceB-GE0/0/2] **vrrp vrid 1 virtual-ip 10.3.1.1 standby** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign public system interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/2** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/2** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure virtual system interfaces and VRRP groups on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 192.168.1.2 30** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/4** [DeviceA-GE0/0/4] **ip address 10.3.2.2 24** [DeviceA-GE0/0/4] **vrrp vrid 2 virtual-ip 10.3.2.1 standby** [DeviceA-GE0/0/4] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 192.168.1.10 30** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/4** [DeviceB-GE0/0/4] **ip address 10.3.2.3 24** [DeviceB-GE0/0/4] **vrrp vrid 2 virtual-ip 10.3.2.1 active** [DeviceB-GE0/0/4] **quit**
# Assign virtual system interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **firewall zone untrust** [DeviceA-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceA-vsysa-zone-untrust] **quit** [DeviceA-vsysa] **firewall zone trust** [DeviceA-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceA-vsysa-zone-trust] **quit** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **firewall zone untrust** [DeviceB-vsysa-zone-untrust] **add interface ge 0/0/3** [DeviceB-vsysa-zone-untrust] **quit** [DeviceB-vsysa] **firewall zone trust** [DeviceB-vsysa-zone-trust] **add interface ge 0/0/4** [DeviceB-vsysa-zone-trust] **quit** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 3 Configure static routes.

DeviceA	DeviceB
# Configure a blackhole route pointing to the addresses in the NAT address pool of the public system on DeviceA and DeviceB.	
[DeviceA] **ip route-static 1.1.1.1 32 null 0**	[DeviceB] **ip route-static 1.1.1.1 32 null 0**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure a blackhole route pointing to the addresses in the NAT address pool of the virtual system on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **ip route-static 1.1.1.2 32 null 0** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **ip route-static 1.1.1.2 32 null 0** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

Step 4 Configure OSPF.

DeviceA	DeviceB
[DeviceA] **ospf 100** [DeviceA-ospf-100] **import-route static** [DeviceA-ospf-100] **area 0** [DeviceA-ospf-100-area-0.0.0.0] **network 192.168.0.0 0.0.0.3** [DeviceA-ospf-100-area-0.0.0.0] **quit** [DeviceA-ospf-100] **quit** [DeviceA] **ospf 200 vpn-instance vsysa** [DeviceA-ospf-200] **import-route static** [DeviceA-ospf-200] **area 0** [DeviceA-ospf-200-area-0.0.0.0] **network 192.168.1.0 0.0.0.3** [DeviceA-ospf-200-area-0.0.0.0] **quit** [DeviceA-ospf-200] **quit**	[DeviceB] **ospf 100** [DeviceB-ospf-100] **import-route static** [DeviceB-ospf-100] **area 0** [DeviceB-ospf-100-area-0.0.0.0] **network 192.168.0.8 0.0.0.3** [DeviceB-ospf-100-area-0.0.0.0] **quit** [DeviceB-ospf-100] **quit** [DeviceB] **ospf 200 vpn-instance vsysa** [DeviceB-ospf-200] **import-route static** [DeviceB-ospf-200] **area 0** [DeviceB-ospf-200-area-0.0.0.0] **network 192.168.1.8 0.0.0.3** [DeviceB-ospf-200-area-0.0.0.0] **quit** [DeviceB-ospf-200] **quit**

Step 5 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 6 Configure hot standby.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**
# To prevent port conflicts during NAT on the devices in load sharing mode, configure available port ranges on DeviceA and DeviceB. **NOTE** In hot standby load sharing networking, if two devices share one NAT address pool and NAPT is configured, the devices may have conflicting public ports. To prevent such conflicts, configure respective NAT resources (including public IP addresses and port numbers) for the devices. If the **hrp nat resource primary-group** command is run on the active device, the **hrp nat resource secondary-group** command is automatically generated on the standby device. Similarly, if the **hrp nat resource secondary-group** command is run on the active device, the **hrp nat resource primary-group** command is automatically generated on the standby device.	
HRP_M[DeviceA] **hrp nat resource primary-group**	HRP_S[DeviceB] **hrp nat resource secondary-group**

Step 7 Configure security policies.

After hot standby relationship is established, the security policies configured on DeviceA are automatically backed up to DeviceB.

Configure a security policy for the public system to allow intranet users to access the public network.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Configure a security policy for the virtual system to allow intranet users to access the public network.

```
HRP_M[DeviceA] Switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] security-policy
HRP_M[DeviceA-vsysa-policy-security] rule name policy_sec
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-address 10.3.2.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-vsysa-policy-security] quit
HRP_M[DeviceA-vsysa] quit
HRP_M<DeviceA-vsysa> quit
```

Step 8 Configure NAT policies.

After hot standby is enabled, the NAT policies on DeviceA will be automatically backed up to DeviceB.

Configure a NAT policy for the public system to allow intranet users to access the public network.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.1 1.1.1.1
HRP_M[DeviceA-address-group-addressgroup1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-policy-nat] quit
```

Configure a NAT policy for the virtual system to allow intranet users to access the public network.

```
HRP_M[DeviceA] switch vsys vsysa
HRP_M<DeviceA-vsysa> system-view
HRP_M[DeviceA-vsysa] nat address-group addressgroup1
HRP_M[DeviceA-vsysa-address-group-addressgroup1] section 0 1.1.1.2 1.1.1.2
HRP_M[DeviceA-vsysa-address-group-addressgroup1] quit
HRP_M[DeviceA-vsysa] nat-policy
HRP_M[DeviceA-vsysa-policy-nat] rule name policy_nat
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] source-address 10.3.2.0 24
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-vsysa-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-vsysa-policy-nat] quit
HRP_M[DeviceA-vsysa] quit
```

Step 9 Configure the switch.

NOTE

The following part uses a Huawei switch to illustrate the configuration.

Configure the switch.

```
[Switch] vlan batch 10 30
[Switch] interface GigabitEthernet 1/0/15
[Switch-GigabitEthernet1/0/15] port link-type access
[Switch-GigabitEthernet1/0/15] port default vlan 10
[Switch-GigabitEthernet1/0/15] quit
[Switch] interface GigabitEthernet 1/0/16
[Switch-GigabitEthernet1/0/16] port link-type access
[Switch-GigabitEthernet1/0/16] port default vlan 10
[Switch-GigabitEthernet1/0/16] quit
[Switch] interface GigabitEthernet 1/0/17
[Switch-GigabitEthernet1/0/17] port link-type access
[Switch-GigabitEthernet1/0/17] port default vlan 10
[Switch-GigabitEthernet1/0/17] quit
[Switch] interface GigabitEthernet 1/0/18
[Switch-GigabitEthernet1/0/18] port link-type access
[Switch-GigabitEthernet1/0/18] port default vlan 30
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Switch-GigabitEthernet1/0/18] quit
[Switch] interface GigabitEthernet 1/0/19
[Switch-GigabitEthernet1/0/19] port link-type access
[Switch-GigabitEthernet1/0/19] port default vlan 30
[Switch-GigabitEthernet1/0/19] quit
[Switch] interface GigabitEthernet 1/0/20
[Switch-GigabitEthernet1/0/20] port link-type access
[Switch-GigabitEthernet1/0/20] port default vlan 30
[Switch-GigabitEthernet1/0/20] quit
```

Step 10 Configure routers.

NOTE

This example uses Huawei routers.

RouterA	RouterB
[RouterA] **interface GigabitEthernet 1/0/1** [RouterA-GigabitEthernet1/0/1] **ip address 192.168.0.1 30** [RouterA-GigabitEthernet1/0/1] **quit** [RouterA] **interface GigabitEthernet 1/0/2** [RouterA-GigabitEthernet1/0/2] **ip address 192.168.0.5 30** [RouterA-GigabitEthernet1/0/2] **quit** [RouterA] **interface GigabitEthernet 1/0/3** [RouterA-GigabitEthernet1/0/3] **ip address 192.168.1.1 30** [RouterA-GigabitEthernet1/0/3] **quit** [RouterA] **interface GigabitEthernet 1/0/4** [RouterA-GigabitEthernet1/0/4] **ip address 192.168.1.5 30** [RouterA-GigabitEthernet1/0/4] **quit** [RouterA] **ospf 100** [RouterA-ospf-100] **default-route-advertise** [RouterA-ospf-100] **area 0** [RouterA-ospf-100-area-0.0.0.0] **network 192.168.0.0 0.0.0.3** [RouterA-ospf-100-area-0.0.0.0] **network 192.168.0.4 0.0.0.3** [RouterA-ospf-100-area-0.0.0.0] **quit** [RouterA-ospf-100] **quit** [RouterA] **ospf 200** [RouterA-ospf-200] **default-route-advertise** [RouterA-ospf-200] **area 0** [RouterA-ospf-200-area-0.0.0.0] **network 192.168.1.0 0.0.0.3** [RouterA-ospf-200-area-0.0.0.0] **network 192.168.1.4 0.0.0.3** [RouterA-ospf-200-area-0.0.0.0] **quit** [RouterA-ospf-200] **quit**	[RouterB] **interface GigabitEthernet 1/0/1** [RouterB-GigabitEthernet1/0/1] **ip address 192.168.0.9 30** [RouterB-GigabitEthernet1/0/1] **quit** [RouterB] **interface GigabitEthernet 1/0/2** [RouterB-GigabitEthernet1/0/2] **ip address 192.168.0.6 30** [RouterB-GigabitEthernet1/0/2] **quit** [RouterB] **interface GigabitEthernet 1/0/3** [RouterB-GigabitEthernet1/0/3] **ip address 192.168.1.9 30** [RouterB-GigabitEthernet1/0/3] **quit** [RouterB] **interface GigabitEthernet 1/0/4** [RouterB-GigabitEthernet1/0/4] **ip address 192.168.1.6 30** [RouterB-GigabitEthernet1/0/4] **quit** [RouterB] **ospf 100** [RouterB-ospf-100] **default-route-advertise** [RouterB-ospf-100] **area 0** [RouterB-ospf-100-area-0.0.0.0] **network 192.168.0.8 0.0.0.3** [RouterB-ospf-100-area-0.0.0.0] **network 192.168.0.4 0.0.0.3** [RouterB-ospf-100-area-0.0.0.0] **quit** [RouterB-ospf-100] **quit** [RouterB] **ospf 200** [RouterB-ospf-200] **default-route-advertise** [RouterB-ospf-200] **area 0** [RouterB-ospf-200-area-0.0.0.0] **network 192.168.1.8 0.0.0.3** [RouterB-ospf-200-area-0.0.0.0] **network 192.168.1.4 0.0.0.3** [RouterB-ospf-200-area-0.0.0.0] **quit** [RouterB-ospf-200] **quit**

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Access the public network from the private network. The access succeeds. Check session information on DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
HRP_M[DeviceA] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa **Remote** 10.3.2.10:2057[1.1.1.2:2048]-->3.3.3.3:2048 icmp VPN:public -> public 10.3.1.10:2057[1.1.1.1:2048]-->3.3.3.3:2048	HRP_S[DeviceB] **display firewall session table** Current Total Sessions : 2 icmp VPN:vsysa --> vsysa 10.3.2.10:2057[1.1.1.2:2048]-->3.3.3.3:2048 icmp VPN:public -> public **Remote** 10.3.1.10:2057[1.1.1.1:2048]-->3.3.3.3:2048

The command output shows that a session tagged with **Remote** is created on DeviceA and DeviceB, indicating that the session is successfully backed up after hot standby is configured.

3. Continuously ping an IP address on the public network from a private network PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is performed and whether ping packets are discarded.

Configuration Scripts

- Public system

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# sysname DeviceA # vsys enable # vsys name vsysa 1 assign interface GE0/0/3 assign interface GE0/0/4 assign global-ip 1.1.1.2 1.1.1.2 exclusive # hrp enable hrp interface GE0/0/7 remote **10.10.0.2** hrp track interface GE0/0/1 hrp track interface GE0/0/3 hrp mirror session enable hrp nat resource **primary-group** hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! J6+;U#>V\!_e1NY[iGLXjT %k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!! Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+ %# # interface GE0/0/1 ip address **192.168.0.2** 255.255.255.252 # interface GE0/0/2 ip address **10.3.1.2** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **active** # interface GE0/0/3 ip address **192.168.1.2** 255.255.255.252 # interface GE0/0/4 ip address **10.3.2.2** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **standby** # interface GE0/0/7 ip address **10.10.0.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # ip route-static 1.1.1.1 255.255.255.255 null 0 # ospf 100 import-route static area 0.0.0.0 network **192.168.0.0** 0.0.0.3 # ospf 200 vpn-instance vsysa import-route static area 0.0.0.0 network **192.168.1.0** 0.0.0.3 # security-policy rule name ha_local_to_dmz source-zone local	# sysname DeviceB # vsys enable # vsys name vsysa 1 assign interface GE0/0/3 assign interface GE0/0/4 assign global-ip 1.1.1.2 1.1.1.2 exclusive # hrp enable hrp interface GE0/0/7 remote **10.10.0.1** hrp track interface GE0/0/1 hrp track interface GE0/0/3 hrp mirror session enable hrp nat resource **secondary-group** hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! \FR0@B|5m51t2(SLB$(Yzq_KUB| V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t \i4 t;1e+vR$$U!!!!!%+%# # interface GE0/0/1 ip address **192.168.0.10** 255.255.255.252 # interface GE0/0/2 ip address **10.3.1.3** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **standby** # interface GE0/0/3 ip address **192.168.1.10** 255.255.255.252 # interface GE0/0/4 ip address **10.3.2.3** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **active** # interface GE0/0/7 ip address **10.10.0.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # ip route-static 1.1.1.1 255.255.255.255 null 0 # ospf 100 import-route static area 0.0.0.0 network **192.168.0.8** 0.0.0.3 # ospf 200 vpn-instance vsysa import-route static area 0.0.0.0 network **192.168.1.8** 0.0.0.3 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 action source-nat address-group addressgroup1 #	destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 action source-nat address-group addressgroup1 #

- Virtual system **vsysa**

DeviceA	DeviceB
# Switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 1.1.1.2 255.255.255.255 null 0 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.2 1.1.1.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #	# Switch vsys vsysa # firewall zone trust set priority 85 add interface GE0/0/4 # firewall zone untrust set priority 5 add interface GE0/0/3 # ip route-static 1.1.1.2 255.255.255.255 null 0 # security-policy rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit # nat address-group addressgroup1 section 0 1.1.1.2 1.1.1.2 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #

 Copyright © Huawei Technologies Co., Ltd.

7.6.5 CLI: Example for Configuring Hot Standby (Load Balancing) of Virtual Systems on Firewalls Connecting to Upstream Routers Through the Public System and Downstream Subnets Through Virtual Systems

Networking Requirements

As shown in **Figure 7-46**, an enterprise deploys two devices as egress gateways to connect the intranet to the Internet. The two devices work in hot standby mode for high availability. The service interfaces of both DeviceA and DeviceB work at Layer 3 and connect to upstream routers (with OSPF running between the devices and routers) and downstream switches (to connect to different subnets isolated from each other). Specific requirements are as follows:

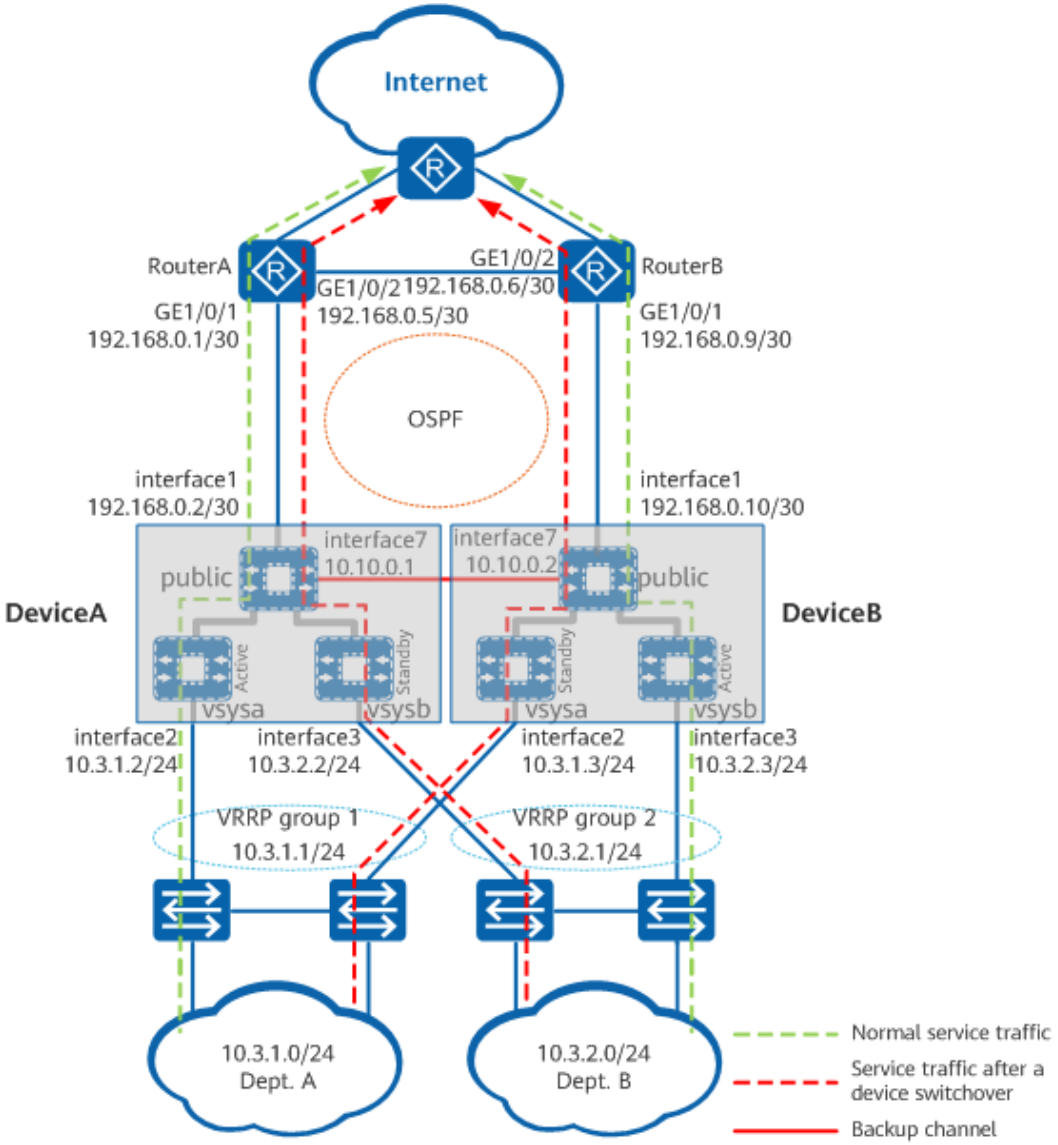
- The enterprise has only one upstream interface. All departments need to access the Internet through this interface.
- Different departments on the intranet need to be isolated from and cannot communicate with each other.
- The two devices work in load sharing mode. In normal cases, DeviceA forwards traffic from department A, and DeviceB forwards traffic from department B. If one device fails, traffic from both departments is forwarded by the other device. This ensures that the services are not interrupted.
- The upstream and downstream links of DeviceA and DeviceB must be in the same state, so that when the interface of one device is down, the interface of the other device can take over to ensure service continuity.

Figure 7-46 Hot standby networking where virtual systems are configured

NOTE

In this example, interface1, interface2, interface3, and interface7 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, andGE0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



The detailed data plan is as follows.

Table 7-13 Data plan of DeviceA and DeviceB

Item	Sub-item	Data of DeviceA	Data of DeviceB
Interfaces	Upstream interface of public system **public**	Interface number: GE 0/0/1 IP address: 192.168.0.2/30 Security zone: untrust	Interface number: GE 0/0/1 IP address: 192.168.0.10/30 Security zone: untrust
	Downstream interface of virtual system **vsysa**	Interface number: GE 0/0/2 IP address: 10.3.1.2/24 Security zone: trust	Interface number: GE 0/0/2 IP address: 10.3.1.3/24 Security zone: trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Data of DeviceA	Data of DeviceB
	Downstream interface of virtual system **vsysb**	Interface number: GE 0/0/3 IP address: 10.3.2.2/24 Security zone: trust	Interface number: GE 0/0/3 IP address: 10.3.2.3/24 Security zone: trust
	Heartbeat interface	Interface number: GE 0/0/7 IP address: 10.10.0.1/24 Security zone: DMZ	Interface number: GE 0/0/7 IP address: 10.10.0.2/24 Security zone: DMZ
VRRP groups	VRRP group 1	10.3.1.1/24 **active**	10.3.1.1/24 **standby**
	VRRP group 2	10.3.2.1/24 **standby**	10.3.2.1/24 **active**
Routes	Blackhole route configured for the NAT address pool of public system **public** to prevent route loops	Blackhole route Destination IP address: 1.1.1.1/32	Blackhole route Destination IP address: 1.1.1.1/32
	OSPF configuration of public system **public**	OSPF 100 Advertised network segment: 192.168.0.0/30 Static routes imported	OSPF 100 Advertised network segment: 192.168.0.8/30 Static routes imported

Table 7-14 Data plan of RouterA

Item	Data	Description
Interfaces	Interface number: GigabitEthernet 1/0/1 IP address: 192.168.0.1/30	Connecting to public system **public** of DeviceA
	Interface number: GigabitEthernet 1/0/2 IP address: 192.168.0.5/30	Connecting to RouterB
OSPF	OSPF 100 Advertised network segment: 192.168.0.0/30 Default routes imported	-

 Copyright © Huawei Technologies Co., Ltd.

Table 7-15 Data plan of RouterB

Item	Data	Description
Interfaces	Interface number: GigabitEthernet 1/0/1 IP address: 192.168.0.9/30	Connecting to public system **public** of DeviceB
	Interface number: GigabitEthernet 1/0/2 IP address: 192.168.0.6/30	Connecting to RouterA
OSPF	OSPF 100 Advertised network segment: 192.168.0.8/30 Default routes imported	-

Configuration Roadmap

The configuration roadmap is as follows:

1. Create different virtual systems on DeviceA and DeviceB to isolate networks of different departments.
2. Configure mutual communication between the virtual systems and the public system on DeviceA and DeviceB so that different virtual systems can share the interface of the public system to access the Internet.
3. The service interfaces of DeviceA and DeviceB work at Layer 3 in load sharing mode, connect to upstream routers, and run OSPF. Therefore, you need to configure OSPF and configure the devices to monitor service interfaces. That is, configure OSPF-based hot standby in load sharing mode. The service interfaces also connect to downstream switches. Therefore, you need to configure VRRP groups. In addition, you also need to complete basic configurations, such as configuring heartbeat interfaces and enabling hot standby.
4. Configure a Link-Group on DeviceA and DeviceB and add the upstream interface of the public system and the downstream interfaces of the virtual systems to this Link-Group to ensure that the upstream and downstream interfaces are in the same state.
5. After hot standby is deployed, configure security and NAT policies for intranet users to access the Internet on DeviceA. You do not need to configure the policies on DeviceB because they can be automatically synchronized from DeviceA.

Procedure

Step 1 Create virtual systems **vsysa** and **vsysb** and assign interfaces to them.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The virtual system names and IDs on DeviceA and DeviceB must be the same. You can run the **display vsys** command on both devices to compare the configurations after virtual systems are created.

This example describes only virtual system configurations closely related to hot standby. For details about other virtual system configurations, see **"Virtual System Configuration"** in *CLI Configuration Guide > Virtualization Configuration*.

DeviceA	DeviceB
# Enable the virtual system function on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **vsys enable**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **vsys enable**
# Create virtual system **vsysa** on each of DeviceA and DeviceB and assign interface GE 0/0/2 to it.	
[DeviceA] **vsys name vsysa** [DeviceA-vsys-vsysa] **assign interface ge 0/0/2** [DeviceA-vsys-vsysa] **quit**	[DeviceB] **vsys name vsysa** [DeviceB-vsys-vsysa] **assign interface ge 0/0/2** [DeviceB-vsys-vsysa] **quit**
# Create virtual system **vsysb** on DeviceA and DeviceB and assign interface GE 0/0/3 to it.	
[DeviceA] **vsys name vsysb** [DeviceA-vsys-vsysb] **assign interface ge 0/0/3** [DeviceA-vsys-vsysb] **quit**	[DeviceB] **vsys name vsysb** [DeviceB-vsys-vsysb] **assign interface ge 0/0/3** [DeviceB-vsys-vsysb] **quit**

Step 2 Configure interfaces.

1. Configure the public system interfaces on DeviceA and DeviceB and assign the interfaces to security zones.

DeviceA	DeviceB
# Set the IP addresses for the upstream and heartbeat interfaces of the public system on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 192.168.0.2 30** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 192.168.0.10 30** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Set the IP address for virtual interface **Virtual-if0** of the public system on DeviceA and DeviceB. The IP address can be any value that is not in conflict with the IP addresses of other interfaces.	
[DeviceA] **interface Virtual-if 0** [DeviceA-Virtual-if0] **ip address 172.16.0.1 24** [DeviceA-Virtual-if0] **quit**	[DeviceB] **interface Virtual-if 0** [DeviceB-Virtual-if0] **ip address 172.16.0.2 24** [DeviceB-Virtual-if0] **quit**
# Assign the interfaces of the public system to security zones on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface Virtual-if 0** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface Virtual-if 0** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**

2. Configure the interfaces of virtual system **vsysa** on DeviceA and DeviceB and assign the interfaces to security zones.

DeviceA	DeviceB
# Configure IP addresses and VRRP groups for the downstream interfaces of virtual system **vsysa** on DeviceA and DeviceB.	
[DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 10.3.1.2 24** [DeviceA-GE0/0/2] **vrrp vrid 1 virtual-ip 10.3.1.1 24 active** [DeviceA-GE0/0/2] **quit**	[DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 10.3.1.3 24** [DeviceB-GE0/0/2] **vrrp vrid 1 virtual-ip 10.3.1.1 24 standby** [DeviceB-GE0/0/2] **quit**
# Set an IP address for virtual interface **Virtual-if1** of virtual system **vsysa** on DeviceA and DeviceB. The IP address can be any value that is not in conflict with the IP addresses of other interfaces.	
[DeviceA] **interface Virtual-if 1** [DeviceA-Virtual-if1] **ip address 172.16.1.1 24** [DeviceA-Virtual-if1] **quit**	[DeviceB] **interface Virtual-if 1** [DeviceB-Virtual-if1] **ip address 172.16.1.2 24** [DeviceB-Virtual-if1] **quit**
# Assign the interfaces of virtual system **vsysa** to security zones on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **firewall zone trust** [DeviceA-vsysa-zone-trust] **add interface ge 0/0/2** [DeviceA-vsysa-zone-trust] **quit** [DeviceA-vsysa] **firewall zone untrust** [DeviceA-vsysa-zone-untrust] **add interface Virtual-if1** [DeviceA-vsysa-zone-untrust] **quit** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **firewall zone trust** [DeviceB-vsysa-zone-trust] **add interface ge 0/0/2** [DeviceB-vsysa-zone-trust] **quit** [DeviceB-vsysa] **firewall zone untrust** [DeviceB-vsysa-zone-untrust] **add interface Virtual-if1** [DeviceB-vsysa-zone-untrust] **quit** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**

3. Configure the interfaces of virtual system **vsysb** on DeviceA and DeviceB and assign the interfaces to security zones.

DeviceA	DeviceB
# Configure IP addresses and VRRP groups for the downstream interfaces of virtual system **vsysb** on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.2.2 24** [DeviceA-GE0/0/3] **vrrp vrid 2 virtual-ip 10.3.2.1 24 standby** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.2.3 24** [DeviceB-GE0/0/3] **vrrp vrid 2 virtual-ip 10.3.2.1 24 active** [DeviceB-GE0/0/3] **quit**
# Set an IP address for virtual interface **Virtual-if2** of virtual system **vsysb** on DeviceA and DeviceB. The IP address can be any value that is not in conflict with the IP addresses of other interfaces.	
[DeviceA] **interface Virtual-if 2** [DeviceA-Virtual-if2] **ip address 172.16.2.1 24** [DeviceA-Virtual-if2] **quit**	[DeviceB] **interface Virtual-if 2** [DeviceB-Virtual-if2] **ip address 172.16.2.2 24** [DeviceB-Virtual-if2] **quit**
# Assign the interfaces of virtual system **vsysb** to security zones on DeviceA and DeviceB.	
[DeviceA] **switch vsys vsysb** <DeviceA-vsysb> **system-view** [DeviceA-vsysb] **firewall zone trust** [DeviceA-vsysb-zone-trust] **add interface ge 0/0/3** [DeviceA-vsysb-zone-trust] **quit** [DeviceA-vsysb] **firewall zone untrust** [DeviceA-vsysb-zone-untrust] **add interface Virtual-if2** [DeviceA-vsysb-zone-untrust] **quit** [DeviceA-vsysb] **quit** <DeviceA-vsysb> **quit**	[DeviceB] **switch vsys vsysb** <DeviceB-vsysb> **system-view** [DeviceB-vsysb] **firewall zone trust** [DeviceB-vsysb-zone-trust] **add interface ge 0/0/3** [DeviceB-vsysb-zone-trust] **quit** [DeviceB-vsysb] **firewall zone untrust** [DeviceB-vsysb-zone-untrust] **add interface Virtual-if2** [DeviceB-vsysb-zone-untrust] **quit** [DeviceB-vsysb] **quit** <DeviceB-vsysb> **quit**

Step 3 Configures static routes.

DeviceA	DeviceB
# On DeviceA and DeviceB, configure a blackhole route pointing to the addresses in the NAT address pool of the public system. 1.1.1.1 32 shall be consistent with the address in the NAT address pool specified in **Step 9**.	
[DeviceA] **ip route-static 1.1.1.1 32 null 0**	[DeviceB] **ip route-static 1.1.1.1 32 null 0**
# Configure a static route to guide return traffic of employees in **vsysa** from the Internet to **vsysa**.	
[DeviceA] **ip route-static 10.3.1.0 24 vpn-instance vsysa**	[DeviceB] **ip route-static 10.3.1.0 24 vpn-instance vsysa**
# Configure a static route to guide return traffic of employees in **vsysb** from the Internet to **vsysb**.	
[DeviceA] **ip route-static 10.3.2.0 24 vpn-instance vsysb**	[DeviceB] **ip route-static 10.3.2.0 24 vpn-instance vsysb**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure a static route to guide Internet access traffic from employees in **vsysa** to the public system. **NOTE** In this example, the network topology and route configuration are simplified. If **vsysa** requires only communication between its connected private networks and the Internet, set **Destination Address/Mask** to **0.0.0.0 0.0.0.0**. That is, all packets are sent to the public system. In practice, for accurate routing information, you shall set **Destination Address/Mask** to a specific Internet address range that the intranet users are allowed to access. Incorrect route configuration may result in communication failure of multiple private networks connected with **vsysa**.	
[DeviceA] **switch vsys vsysa** <DeviceA-vsysa> **system-view** [DeviceA-vsysa] **ip route-static 0.0.0.0 0.0.0.0 public** [DeviceA-vsysa] **quit** <DeviceA-vsysa> **quit**	[DeviceB] **switch vsys vsysa** <DeviceB-vsysa> **system-view** [DeviceB-vsysa] **ip route-static 0.0.0.0 0.0.0.0 public** [DeviceB-vsysa] **quit** <DeviceB-vsysa> **quit**
# Configure a static route to guide Internet access traffic from employees in **vsysb** to the public system. **NOTE** In this example, the network topology and route configuration are simplified. If **vsysb** only needs to communicate with the Internet, set **Destination Address/Mask** to **0.0.0.0 0.0.0.0**. That is, all packets are sent to the public system. In practice, for accurate routing information, you shall set **Destination Address/Mask** to a specific Internet address range that the intranet users are allowed to access. Incorrect route configuration may result in communication failure of multiple LANs connected with **vsysb**.	
[DeviceA] **switch vsys vsysb** <DeviceA-vsysb> **system-view** [DeviceA-vsysb] **ip route-static 0.0.0.0 0.0.0.0 public** [DeviceA-vsysb] **quit** <DeviceA-vsysb> **quit**	[DeviceB] **switch vsys vsysb** <DeviceB-vsysb> **system-view** [DeviceB-vsysb] **ip route-static 0.0.0.0 0.0.0.0 public** [DeviceB-vsysb] **quit** <DeviceB-vsysb> **quit**

Step 4 Configure OSPF.

DeviceA	DeviceB
[DeviceA] **ospf 100** [DeviceA-ospf-100] **import-route static** [DeviceA-ospf-100] **area 0** [DeviceA-ospf-100-area-0.0.0.0] **network 192.168.0.0 0.0.0.3** [DeviceA-ospf-100-area-0.0.0.0] **quit** [DeviceA-ospf-100] **quit**	[DeviceB] **ospf 100** [DeviceB-ospf-100] **import-route static** [DeviceB-ospf-100] **area 0** [DeviceB-ospf-100-area-0.0.0.0] **network 192.168.0.8 0.0.0.3** [DeviceB-ospf-100-area-0.0.0.0] **quit** [DeviceB-ospf-100] **quit**

Step 5 Configure the Link-Group function to ensure that the upstream and downstream interfaces are in the same state.

Add the public system interface (upstream interface) and virtual system interfaces (downstream interfaces) to the same Link-Group on DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **link-group 1** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **link-group public 1** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **link-group public 1** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **link-group 1** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **link-group public 1** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **link-group public 1** [DeviceB-GE0/0/3] **quit**

Step 6 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 7 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1**	[DeviceB] **hrp track interface ge 0/0/1**
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# To prevent port conflicts during NAT on the devices in load sharing mode, configure available port ranges on DeviceA and DeviceB. **NOTE** In hot standby load sharing networking, if two devices share one NAT address pool and NAPT is configured, the devices may have conflicting public ports. To prevent such conflicts, configure respective NAT resources (including public IP addresses and port numbers) for the devices. If the **hrp nat resource primary-group** command is run on the active device, the **hrp nat resource secondary-group** command is automatically generated on the standby device. If the **hrp nat resource secondary-group** command is run on the active device, the **hrp nat resource primary-group** command is automatically generated on the standby device.	
HRP_M[DeviceA] **hrp nat resource primary-group**	HRP_S[DeviceB] **hrp nat resource secondary-group**

Step 8 Configure security policies.

NOTE

Security policies can be backed up. That is, policies configured on DeviceA can be automatically backed up to DeviceB. If you have configured security policies separately on DeviceA and DeviceB before configuring hot standby, ensure that their configurations and the sequences in which they are configured are the same on DeviceA and DeviceB. Otherwise, services may become abnormal after an active/standby switchover.

1. Configure a security policy for the public system.

   # On DeviceA, configure a security policy for the public system to allow intranet users to access the Internet. When configuring the security policy for the public system, you do not need to specify the IP address range. When configuring the security policy for the virtual system, you need to specify the IP addresses of the intranet employees to configure a strict security policy.

   ```
   HRP_M[DeviceA] security-policy
   HRP_M[DeviceA-policy-security] rule name policy_sec
   HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
   HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
   HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
   HRP_M[DeviceA-policy-security-rule-policy_sec] quit
   HRP_M[DeviceA-policy-security] quit
   ```

2. Configure security policies in virtual system **vsysa**.

   # In **vsysa** of DeviceA, configure a security policy to isolate **vsysa** from **vsysb**. Because routes have been configured in the public system to divert the return traffic to **vsysa** and **vsysb**, **vsysa** and **vsysb** can communicate with each other through the public system. To isolate them from each other, you must configure this security policy in **vsysa**.

   ```
   HRP_M[DeviceA] switch vsys vsysa
   HRP_M<DeviceA-vsysa> system-view
   HRP_M[DeviceA-vsysa] security-policy
   HRP_M[DeviceA-vsysa-policy-security] rule name vsysa_to_vsysb
   HRP_M[DeviceA-vsysa-policy-security-rule-vsysa_to_vsysb] source-zone trust
   HRP_M[DeviceA-vsysa-policy-security-rule-vsysa_to_vsysb] destination-zone untrust
   HRP_M[DeviceA-vsysa-policy-security-rule-vsysa_to_vsysb] source-address 10.3.1.0 24
   HRP_M[DeviceA-vsysa-policy-security-rule-vsysa_to_vsysb] destination-address 10.3.2.0 24
   HRP_M[DeviceA-vsysa-policy-security-rule-vsysa_to_vsysb] action deny
   HRP_M[DeviceA-vsysa-policy-security-rule-vsysa_to_vsysb] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

On DeviceA, configure a security policy for virtual system **vsysa** to allow intranet users to access the Internet.

```
HRP_M[DeviceA-vsysa-policy-security] rule name policy_sec
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] source-address 10.3.1.0 24
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-vsysa-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-vsysa-policy-security] quit
HRP_M[DeviceA-vsysa] quit
HRP_M<DeviceA-vsysa> quit
```

3. Configure security policies in virtual system **vsysb**.

   # In **vsysb** of DeviceA, configure a security policy to isolate **vsysa** from **vsysb**. Because routes have been configured in the public system to divert the return traffic to **vsysa** and **vsysb**, **vsysa** and **vsysb** can communicate with each other through the public system. To isolate them from each other, you must configure this security policy in **vsysb**.

   ```
   HRP_M[DeviceA] switch vsys vsysb
   HRP_M<DeviceA-vsysb> system-view
   HRP_M[DeviceA-vsysb] security-policy
   HRP_M[DeviceA-vsysb-policy-security] rule name vsysb_to_vsysa
   HRP_M[DeviceA-vsysb-policy-security-rule-vsysb_to_vsysa] source-zone trust
   HRP_M[DeviceA-vsysb-policy-security-rule-vsysb_to_vsysa] destination-zone untrust
   HRP_M[DeviceA-vsysb-policy-security-rule-vsysb_to_vsysa] source-address 10.3.2.0 24
   HRP_M[DeviceA-vsysb-policy-security-rule-vsysb_to_vsysa] destination-address 10.3.1.0 24
   HRP_M[DeviceA-vsysb-policy-security-rule-vsysb_to_vsysa] action deny
   HRP_M[DeviceA-vsysb-policy-security-rule-vsysb_to_vsysa] quit
   ```

   # On DeviceA, configure a security policy for virtual system **vsysb** to allow intranet users to access the Internet.

   ```
   HRP_M[DeviceA-vsysb-policy-security] rule name policy_sec
   HRP_M[DeviceA-vsysb-policy-security-rule-policy_sec] source-zone trust
   HRP_M[DeviceA-vsysb-policy-security-rule-policy_sec] destination-zone untrust
   HRP_M[DeviceA-vsysb-policy-security-rule-policy_sec] source-address 10.3.2.0 24
   HRP_M[DeviceA-vsysb-policy-security-rule-policy_sec] action permit
   HRP_M[DeviceA-vsysb-policy-security-rule-policy_sec] quit
   HRP_M[DeviceA-vsysb-policy-security] quit
   HRP_M[DeviceA-vsysb] quit
   HRP_M<DeviceA-vsysb> quit
   ```

Step 9 Configure a NAT policy.

On DeviceA, configure a NAT policy for the public system to allow intranet users to access the Internet. The NAT policy configured on DeviceA can be automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.1 1.1.1.1
HRP_M[DeviceA-address-group-addressgroup1] quit
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-zone trust
HRP_M[DeviceA-policy-nat-rule-policy_nat] destination-zone untrust
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-address 10.3.1.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-nat-rule-policy_nat] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-rule-policy_nat] quit
HRP_M[DeviceA-policy-nat] quit
```

Step 10 Configure routers.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This example uses Huawei routers.

RouterA	RouterB
[RouterA] **interface GigabitEthernet 1/0/1** [RouterA-GigabitEthernet1/0/1] **ip address 192.168.0.1 30** [RouterA-GigabitEthernet1/0/1] **quit** [RouterA] **interface GigabitEthernet 1/0/2** [RouterA-GigabitEthernet1/0/2] **ip address 192.168.0.5 30** [RouterA-GigabitEthernet1/0/2] **quit** [RouterA] **ospf 100** [RouterA-ospf-100] **default-route-advertise** [RouterA-ospf-100] **area 0** [RouterA-ospf-100-area-0.0.0.0] **network 192.168.0.0 0.0.0.3** [RouterA-ospf-100-area-0.0.0.0] **quit** [RouterA-ospf-100] **quit**	[RouterB] **interface GigabitEthernet 1/0/1** [RouterB-GigabitEthernet1/0/1] **ip address 192.168.0.9 30** [RouterB-GigabitEthernet1/0/1] **quit** [RouterB] **interface GigabitEthernet 1/0/2** [RouterB-GigabitEthernet1/0/2] **ip address 192.168.0.6 30** [RouterB-GigabitEthernet1/0/2] **quit** [RouterB] **ospf 100** [RouterB-ospf-100] **default-route-advertise** [RouterB-ospf-100] **area 0** [RouterB-ospf-100-area-0.0.0.0] **network 192.168.0.8 0.0.0.3** [RouterB-ospf-100-area-0.0.0.0] **quit** [RouterB-ospf-100] **quit**

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Access the public network from the private network. The access succeeds. Check session information on DeviceA and DeviceB.

DeviceA	DeviceB
HRP_M[DeviceA] **display firewall session table all-systems** Current Total Sessions : 4 udp VPN: vsysb --> public **Remote** 10.3.2.4:1001 --> 3.3.3.4:2001 udp VPN: public --> public **Remote** 10.3.2.4:1001[1.1.1.1:2049] --> 3.3.3.4:2001 udp VPN: vsysa --> public 10.3.1.4:1000 --> 3.3.3.3:2000 udp VPN: public --> public 10.3.1.4:1000[1.1.1.1:2119] --> 3.3.3.3:2000	HRP_S[DeviceB] **display firewall session table all-systems** Current Total Sessions : 4 udp VPN: vsysb --> public 10.3.2.4:1001 --> 3.3.3.4:2001 udp VPN: public --> public 10.3.2.4:1001[1.1.1.1:2049] --> 3.3.3.4:2001 udp VPN: vsysa --> public **Remote** 10.3.1.4:1000 --> 3.3.3.3:2000 udp VPN: public --> public **Remote** 10.3.1.4:1000[1.1.1.1:2119] --> 3.3.3.3:2000

   The command output shows that a session tagged with **Remote** is created on DeviceA and DeviceB, indicating that the session is successfully backed up after hot standby is configured.
3. Continuously ping an IP address on the Internet from an intranet PC and pull out the network cable from GE 0/0/2 on DeviceA. An active/standby device switchover occurs, the state of DeviceA changes from **HRP_M** to **HRP_S**, and no ping packets are discarded. Then, run the **display link-group** command. The state of upstream interface GE 0/0/1 also changes to **Down**, which is consistent with that of GE 0/0/2.

```
HRP_S[DeviceA] display link-group
 link group 1, total 3, fault 1
 --------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Interface                   Vsys                State
--------------------------------------------------------------------------------
GE0/0/1                     public              down
GE0/0/2                     vsysa               fault
GE0/0/3                     vsysb               down
--------------------------------------------------------------------------------
```

Then, plug the cable back into GE 0/0/2 on DeviceA. The state of DeviceA changes from **HRP_S** to **HRP_M**, no ping packets are discarded, and the interfaces in the Link-Group become up again.

```
HRP_M[DeviceA] display link-group
link group 1, total 3, fault 0
--------------------------------------------------------------------------------
Interface                   Vsys                State
--------------------------------------------------------------------------------
GE0/0/1                     public              up
GE0/0/2                     vsysa               up
GE0/0/3                     vsysb               up
--------------------------------------------------------------------------------
```

4. Continuously ping an IP address on the Internet from an intranet PC and pull out the network cable from GE 0/0/3 on DeviceB. Device status switchover occurs, the state of DeviceB changes from **HRP_M** to **HRP_S**, and no ping packets are discarded. Then, run the **display link-group** command. The state of upstream interface GE 0/0/1 also changes to **Down**, which is consistent with that of GE 0/0/3.

```
HRP_S[DeviceB] display link-group
link group 1, total 3, fault 1
--------------------------------------------------------------------------------
Interface                   Vsys                State
--------------------------------------------------------------------------------
GE0/0/1                     public              down
GE0/0/2                     vsysa               down
GE0/0/3                     vsysb               fault
--------------------------------------------------------------------------------
```

Then, plug the cable back into GE 0/0/3 on DeviceB. The state of DeviceB changes from **HRP_S** to **HRP_M**, no ping packets are discarded, and the interfaces in the Link-Group become up again.

```
HRP_M[DeviceB] display link-group
link group 1, total 3, fault 0
--------------------------------------------------------------------------------
Interface                   Vsys                State
--------------------------------------------------------------------------------
GE0/0/1                     public              up
GE0/0/2                     vsysa               up
GE0/0/3                     vsysb               up
--------------------------------------------------------------------------------
```

Configuration Scripts

- Public system

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# sysname DeviceA # vsys enable # vsys name vsysa 1 assign interface GE0/0/2 # vsys name vsysb 2 assign interface GE0/0/3 # hrp enable hrp interface GE0/0/7 remote **10.10.0.2** hrp track interface GE0/0/1 hrp mirror session enable hrp nat resource **primary-group** hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! J6+;U#>V\!_e1NY[iGLXjT %k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!! Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+ %# # interface GE0/0/1 ip address **192.168.0.2** 255.255.255.252 link-group 1 # interface GE0/0/2 ip binding vpn-instance vsysa ip address **10.3.1.2** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **active** link-group public 1 # interface GE0/0/3 ip binding vpn-instance vsysb ip address **10.3.2.2** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **standby** link-group public 1 # interface GE0/0/7 ip address **10.10.0.1** 255.255.255.0 # interface Virtual-if0 ip address **172.16.0.1** 255.255.255.0 # interface Virtual-if1 ip address **172.16.1.1** 255.255.255.0 # interface Virtual-if2 ip address **172.16.2.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 add interface Virtual-if0 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # vsys enable resource-class r0 #	# sysname DeviceB # vsys enable # vsys name vsysa 1 assign interface GE0/0/2 # vsys name vsysb 2 assign interface GE0/0/3 # hrp enable hrp interface GE0/0/7 remote **10.10.0.1** hrp track interface GE0/0/1 hrp mirror session enable hrp nat resource **secondary-group** hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!! \FR0@B|5m51t2(SLB$(Yzq_KUB\| V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t \i4 t;1e+vR$$U!!!!!%+%# # interface GE0/0/1 ip address **192.168.0.10** 255.255.255.252 link-group 1 # interface GE0/0/2 ip binding vpn-instance vsysa ip address **10.3.1.3** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **standby** link-group public 1 # interface GE0/0/3 ip binding vpn-instance vsysb ip address **10.3.2.3** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **active** link-group public 1 # interface GE0/0/7 ip address **10.10.0.2** 255.255.255.0 # interface Virtual-if0 ip address **172.16.0.2** 255.255.255.0 # interface Virtual-if1 ip address **172.16.1.2** 255.255.255.0 # interface Virtual-if2 ip address **172.16.2.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 add interface Virtual-if0 # firewall zone dmz set priority 50 add interface GE0/0/7 # firewall zone untrust set priority 5 add interface GE0/0/1 # vsys enable resource-class r0 # ip route-static 1.1.1.1 255.255.255.255 null 0

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
ip route-static 1.1.1.1 255.255.255.255 null 0 ip route-static 10.3.1.0 255.255.255.0 vpn-instance vsysa ip route-static 10.3.2.0 255.255.255.0 vpn-instance vsysb # ospf 100 import-route static area 0.0.0.0 network **192.168.0.0** 0.0.0.3 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust action permit # nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #	ip route-static 10.3.1.0 255.255.255.0 vpn-instance vsysa ip route-static 10.3.2.0 255.255.255.0 vpn-instance vsysb # ospf 100 import-route static area 0.0.0.0 network **192.168.0.8** 0.0.0.3 # security-policy rule name ha_local_to_dmz source-zone local source-zone dmz destination-zone local destination-zone dmz service protocol udp destination-port 18514 action permit rule name policy_sec source-zone trust destination-zone untrust action permit # nat address-group addressgroup1 section 0 1.1.1.1 1.1.1.1 # nat-policy rule name policy_nat source-zone trust destination-zone untrust source-address 10.3.1.0 24 source-address 10.3.2.0 24 action source-nat address-group addressgroup1 #

- Virtual system **vsysa**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# switch vsys vsysa # interface GE0/0/2 ip binding vpn-instance vsysa ip address **10.3.1.2** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **active** link-group public 1 # interface Virtual-if1 ip address **172.16.1.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone untrust set priority 5 add interface Virtual-if1 # ip route-static 0.0.0.0 0.0.0.0 public # security-policy rule name vsysa_to_vsysb source-zone trust destination-zone untrust source-address 10.3.1.0 24 destination-address 10.3.2.0 24 action deny rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit #	# switch vsys vsysa # interface GE0/0/2 ip binding vpn-instance vsysa ip address **10.3.1.3** 255.255.255.0 vrrp vrid 1 virtual-ip 10.3.1.1 **standby** link-group public 1 # interface Virtual-if1 ip address **172.16.1.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/2 # firewall zone untrust set priority 5 add interface Virtual-if1 # ip route-static 0.0.0.0 0.0.0.0 public # security-policy rule name vsysa_to_vsysb source-zone trust destination-zone untrust source-address 10.3.1.0 24 destination-address 10.3.2.0 24 action deny rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.1.0 24 action permit #

- Virtual system **vsysb**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# switch vsys vsysb # interface GE0/0/3 ip binding vpn-instance vsysb ip address **10.3.2.2** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **standby** link-group public 1 # interface Virtual-if2 ip address **172.16.2.1** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/3 # firewall zone untrust set priority 5 add interface Virtual-if2 # ip route-static 0.0.0.0 0.0.0.0 public # security-policy rule name vsysb_to_vsysa source-zone trust destination-zone untrust source-address 10.3.2.0 24 destination-address 10.3.1.0 24 action deny rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit #	# switch vsys vsysb # interface GE0/0/3 ip binding vpn-instance vsysb ip address **10.3.2.3** 255.255.255.0 vrrp vrid 2 virtual-ip 10.3.2.1 **active** link-group public 1 # interface Virtual-if2 ip address **172.16.2.2** 255.255.255.0 # firewall zone trust set priority 85 add interface GE0/0/3 # firewall zone untrust set priority 5 add interface Virtual-if2 # ip route-static 0.0.0.0 0.0.0.0 public # security-policy rule name vsysb_to_vsysa source-zone trust destination-zone untrust source-address 10.3.2.0 24 destination-address 10.3.1.0 24 action deny rule name policy_sec source-zone trust destination-zone untrust source-address 10.3.2.0 24 action permit #

7.7 Configuring IPv6 Hot Standby

7.7.1 CLI: Example for Configuring IPv6 Hot Standby in Active/Standby Mode on Devices That Connect Switches in Upstream and Downstream Directions

Networking Requirements

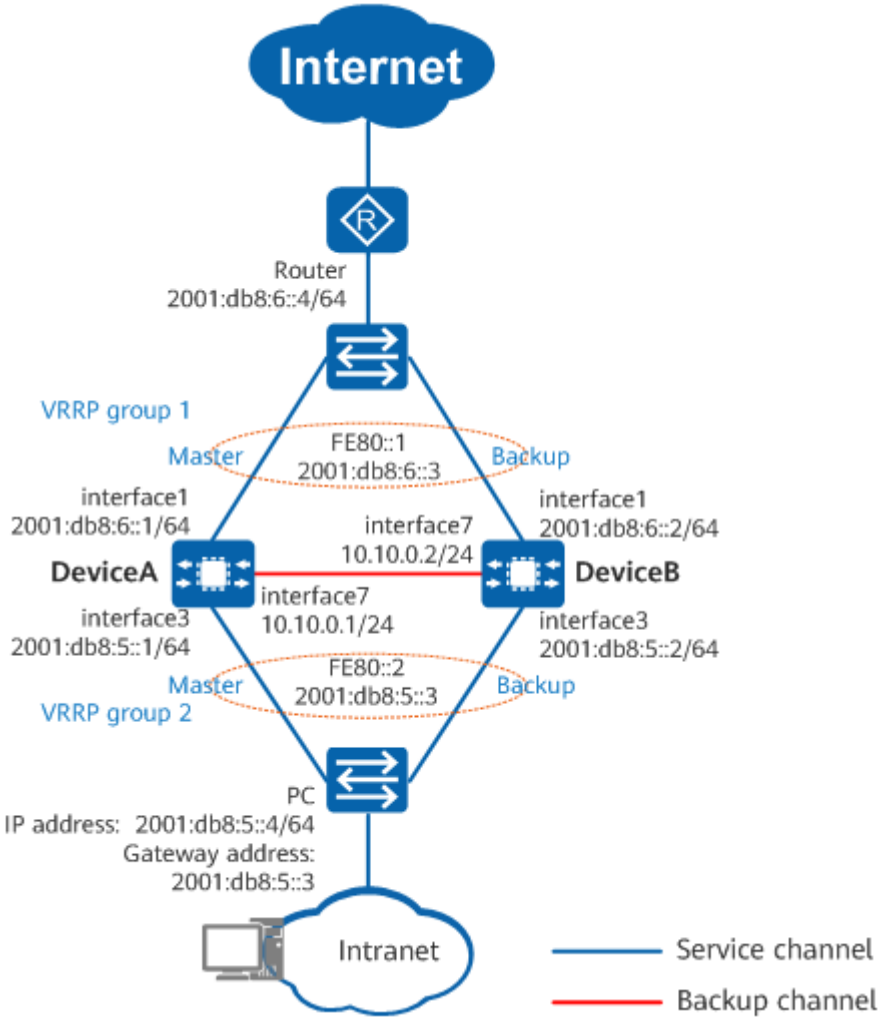
On the network shown in **Figure 7-47**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream Layer 2 switches. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-47 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Enable the IPv6 packet forwarding function of upstream and downstream service interfaces on DeviceA and DeviceB, and configure IP addresses for the interfaces.	

DeviceA	DeviceB
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ipv6 enable** [DeviceA-GE0/0/1] **ipv6 address 2001:db8:6::1 64** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ipv6 enable** [DeviceA-GE0/0/3] **ipv6 address 2001:db8:5::1 64** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ipv6 enable** [DeviceB-GE0/0/1] **ipv6 address 2001:db8:6::2 64** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ipv6 enable** [DeviceB-GE0/0/3] **ipv6 address 2001:db8:5::2 64** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Create a default route with next hop 2001:db8:6::4 on DeviceA and DeviceB to forward traffic of intranet users to Router.	
[DeviceA] **ipv6 route-static :: 0 2001:db8:6::4**	[DeviceB] **ipv6 route-static :: 0 2001:db8:6::4**

Step 2 Configure VRRP6 groups.

DeviceA	DeviceB
# Configure VRRP6 group 1 on upstream service interface GE 0/0/1 of DeviceA and specify **active** in the **vrrp vrid virtual-ip** command for the VRRP group. Configure VRRP6 group 1 on upstream service interface GE 0/0/1 of DeviceB and specify **standby** in the **vrrp vrid virtual-ip** command for the VRRP group.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp6 vrid 1 virtual-ip FE80::1 link-local active** [DeviceA-GE0/0/1] **vrrp6 vrid 1 virtual-ip 2001:db8:6::3** [DeviceA-GE0/0/1] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp6 vrid 1 virtual-ip FE80::1 link-local standby** [DeviceB-GE0/0/1] **vrrp6 vrid 1 virtual-ip 2001:db8:6::3** [DeviceB-GE0/0/1] **quit**
# Configure VRRP6 group 2 on downstream service interface GE 0/0/3 of DeviceA and set the VRRP6 group state to Active. Configure VRRP6 group 2 on downstream service interface GE 0/0/3 of DeviceB and set the VRRP6 group state to Standby.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp6 vrid 2 virtual-ip FE80::2 link-local active** [DeviceA-GE0/0/3] **vrrp6 vrid 2 virtual-ip 2001:db8:5::3** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp6 vrid 2 virtual-ip FE80::2 link-local standby** [DeviceB-GE0/0/3] **vrrp6 vrid 2 virtual-ip 2001:db8:5::3** [DeviceB-GE0/0/3] **quit**

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Specify the heartbeat interface, configure the authentication key, and enable hot standby.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Create a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name trust_to_untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-address 2001:db8:5:: 64
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] action permit
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure switches and intranet PCs.

1. Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.
2. On intranet PCs, specify the virtual IPv6 address of VRRP6 group 2 as the default gateway address. Details are omitted.

Step 7 Configure Router.

 Copyright © Huawei Technologies Co., Ltd.

Configure routes to DeviceA and DeviceB on Router, with the next hop being the virtual IPv6 addresses of VRRP6 group 1.

----End

Verifying the Configuration

1. Run the **display vrrp6** command to check the status of interfaces in the VRRP6 group.
2. Run the **display hrp state verbose** command to check the hot standby status.
3. Run the **ping 2001:db8:6::4** command on the PC in the trust zone to ping Router in the untrust zone. The ping operation is successful. Run the **display firewall ipv6 session table** command on DeviceA and DeviceB. Sessions between the two devices are successfully created and backed up.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall ipv6 session table** Current Total Sessions : 1 icmpv6 VPN: public --> public 2001:DB8:5::4.0 --> 2001:DB8:6::4.2048	HRP_S<DeviceB> **display firewall ipv6 session table** Current Total Sessions : 1 icmpv6 VPN: public --> public **Remote** 2001:DB8:5::4.0 --> 2001:DB8:6::4.2048

   The preceding command output shows that sessions tagged with **Remote** are created on DeviceB. This indicates that the sessions are successfully backed up after hot standby is configured.
4. Run the **ping 2001:db8:6::4 -t** command on the PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is performed and whether ping packets are discarded. During the entire process, the ping operation is not interrupted.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::1/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local active
 vrrp6 vrid 1 virtual-ip 2001:DB8:6::3
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::1/64
 vrrp6 vrid 2 virtual-ip FE80::2 link-local active
 vrrp6 vrid 2 virtual-ip 2001:DB8:5::3
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ipv6 route-static :: 0 2001:db8:6::4
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:5:: 64
  action permit
#
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::2/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local standby
 vrrp6 vrid 1 virtual-ip 2001:DB8:6::3
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::2/64
 vrrp6 vrid 2 virtual-ip FE80::2 link-local standby
 vrrp6 vrid 2 virtual-ip 2001:DB8:5::3
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ipv6 route-static :: 0 2001:db8:6::4
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:5:: 64
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

7.7.2 CLI: Example for Configuring IPv6 Hot Standby in Load Balancing Mode on Devices That Connect Switches in Upstream and Downstream Directions

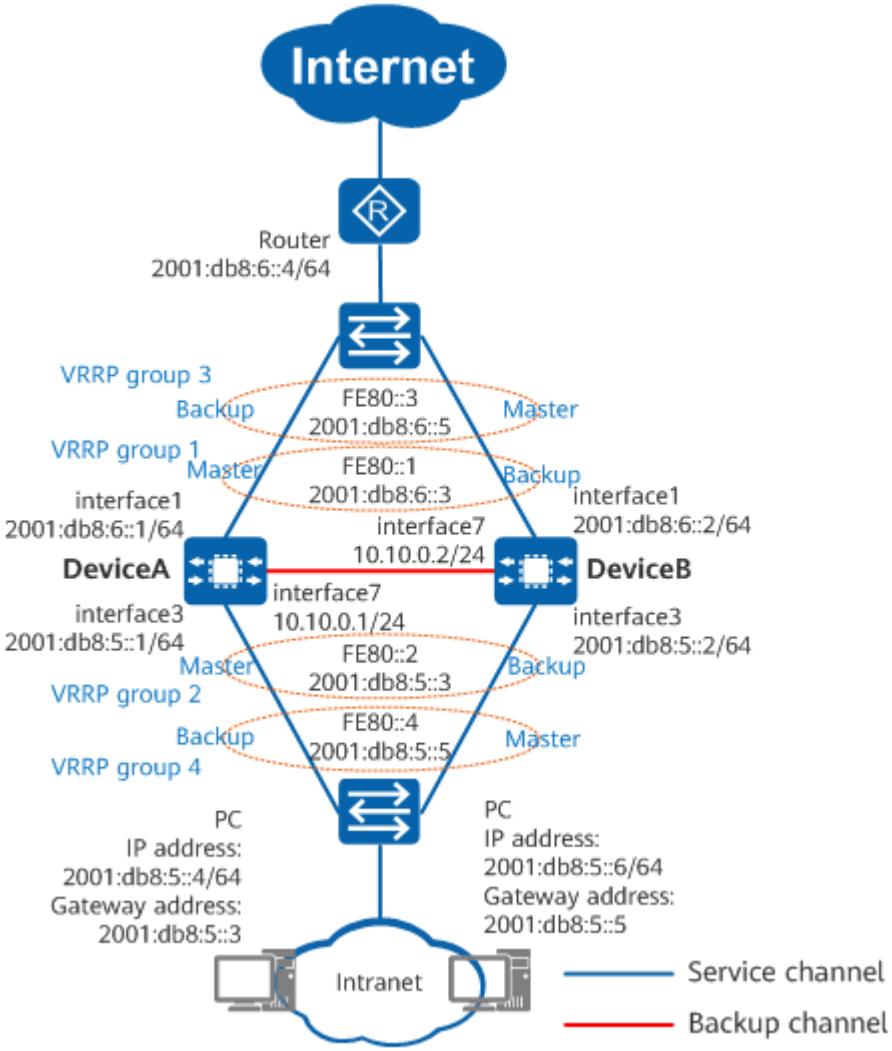
Networking Requirements

On the network shown in **Figure 7-48**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream Layer 2 switches. DeviceA and DeviceB are expected to work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-48 Load sharing networking where service interfaces work at Layer 3 and connect to upstream and downstream switches

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Enable the IPv6 packet forwarding function of the upstream and downstream service interfaces on DeviceA and DeviceB, and configure IP addresses for the interfaces.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ipv6 enable** [DeviceA-GE0/0/1] **ipv6 address 2001:db8:6::1 64** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ipv6 enable** [DeviceA-GE0/0/3] **ipv6 address 2001:db8:5::1 64** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ipv6 enable** [DeviceB-GE0/0/1] **ipv6 address 2001:db8:6::2 64** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ipv6 enable** [DeviceB-GE0/0/3] **ipv6 address 2001:db8:5::2 64** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Create a default route with next hop 2001:db8:6::4 on DeviceA and DeviceB to forward traffic of intranet users to Router.	
[DeviceA] **ipv6 route-static 0:0::0:0 0 2001:db8:6::4**	[DeviceB] **ipv6 route-static 0:0::0:0 0 2001:db8:6::4**

Step 2 Configure VRRP6 groups.

DeviceA	DeviceB
# Configure VRRP6 groups 1 and 3 on upstream service interface GE 0/0/1 of DeviceA and specify **active** for VRRP group 1 and **standby** for VRRP group 3. Configure VRRP6 groups 1 and 3 on upstream service interface GE 0/0/1 of DeviceB and specify **standby** for VRRP group 1 and **active** for VRRP group 3.	
[DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **vrrp6 vrid 1 virtual-ip FE80::1 link-local active** [DeviceA-GE0/0/1] **vrrp6 vrid 1 virtual-ip 2001:db8:6::3** [DeviceA-GE0/0/1] **vrrp6 vrid 3 virtual-ip FE80::3 link-local standby** [DeviceA-GE0/0/1] **vrrp6 vrid 3 virtual-ip 2001:db8:6::5** [DeviceA-GE0/0/1] **quit**	[DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **vrrp6 vrid 1 virtual-ip FE80::1 link-local standby** [DeviceB-GE0/0/1] **vrrp6 vrid 1 virtual-ip 2001:db8:6::3** [DeviceB-GE0/0/1] **vrrp6 vrid 3 virtual-ip FE80::3 link-local active** [DeviceB-GE0/0/1] **vrrp6 vrid 3 virtual-ip 2001:db8:6::5** [DeviceB-GE0/0/1] **quit**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure VRRP6 groups 2 and 4 on downstream service interface GE 0/0/3 of DeviceA and specify **active** in the **vrrp vrid virtual-ip** command for VRRP group 2 and **standby** in the command for VRRP group 4. Configure VRRP groups 2 and 4 on downstream service interface GE 0/0/3 of DeviceB and specify **standby** in the **vrrp vrid virtual-ip** command for VRRP group 2 and **active** in the command for VRRP group 4.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp6 vrid 2 virtual-ip FE80::2 link-local active** [DeviceA-GE0/0/3] **vrrp6 vrid 2 virtual-ip 2001:db8:5::3** [DeviceA-GE0/0/3] **vrrp6 vrid 4 virtual-ip FE80::4 link-local standby** [DeviceA-GE0/0/3] **vrrp6 vrid 4 virtual-ip 2001:db8:5::5** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp6 vrid 2 virtual-ip FE80::2 link-local standby** [DeviceB-GE0/0/3] **vrrp6 vrid 2 virtual-ip 2001:db8:5::3** [DeviceB-GE0/0/3] **vrrp6 vrid 4 virtual-ip FE80::4 link-local active** [DeviceB-GE0/0/3] **vrrp6 vrid 4 virtual-ip 2001:db8:5::5** [DeviceB-GE0/0/3] **quit**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Configure quick session backup, specify the heartbeat interface, configure the authentication key, and enable hot standby.

DeviceA	DeviceB
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 5 Create a security policy on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure a security policy to allow intranet users to access the Internet.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name trust_to_untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] source-address 2001:db8:5:: 64
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] action permit
HRP_M[DeviceA-policy-security-rule-trust_to_untrust] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure switches and intranet PCs.

1. Add three interfaces of each switch to the same VLAN. For configuration commands, see related documents of the switches.
2. On some intranet PCs, specify the virtual IPv6 address of VRRP6 group 2 as the default gateway address and on some other intranet PCs, specify the virtual IPv6 address of VRRP6 group 4 as the default gateway address to implement load sharing of intranet traffic.

Step 7 Configure Router.

Configure equal-cost routes to DeviceA and DeviceB on Router, with the next hops being the virtual IPv6 addresses of VRRP6 group 1 and VRRP6 group 3.

----End

Verifying the Configuration

1. Run the **display vrrp6** command on DeviceA and DeviceB to check the status of interfaces in the VRRP6 group.
2. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
3. In the trust zone, select two PCs with the default gateways set to the virtual IPv6 addresses of VRRP6 group 2 and VRRP6 group 4 respectively and run the **ping 2001:db8:6::4** command on the two PCs to ping Router in the untrust zone. The ping operation is successful. Run the **display firewall ipv6 session table** command on DeviceA and DeviceB. Sessions between the two devices are successfully created and backed up.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall ipv6 session table** Current Total Sessions : 2 icmpv6 VPN: public --> public 2001:DB8:5::4.0 --> 2001:DB8:6::4.2048 icmpv6 VPN: public --> public **Remote** 2001:DB8:5::6.0 --> 2001:DB8:6::4.2048	HRP_S<DeviceB> **display firewall ipv6 session table** Current Total Sessions : 2 icmpv6 VPN: public --> public **Remote** 2001:DB8:5::4.0 --> 2001:DB8:6::4.2048 icmpv6 VPN: public --> public 2001:DB8:5::6.0 --> 2001:DB8:6::4.2048

The preceding command output shows that sessions tagged with **Remote** are created on the two devices. This indicates that the sessions between the two devices are successfully backed up after hot standby is configured.

4. Run the **ping 2001:db8:6::4 -t** command on the PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is performed and whether ping packets are discarded. During the entire process, the ping operation is not interrupted.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::1/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local active
 vrrp6 vrid 1 virtual-ip 2001:DB8:6::3
 vrrp6 vrid 3 virtual-ip FE80::3 link-local standby
 vrrp6 vrid 3 virtual-ip 2001:DB8:6::5
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::1/64
 vrrp6 vrid 2 virtual-ip FE80::2 link-local active
 vrrp6 vrid 2 virtual-ip 2001:DB8:5::3
 vrrp6 vrid 4 virtual-ip FE80::4 link-local standby
 vrrp6 vrid 4 virtual-ip 2001:DB8:5::5
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ipv6 route-static 0:0::0:0 0 2001:db8:6::4
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:5:: 64
  action permit
#
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::2/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local standby
 vrrp6 vrid 1 virtual-ip 2001:DB8:6::3
 vrrp6 vrid 3 virtual-ip FE80::3 link-local active
 vrrp6 vrid 3 virtual-ip 2001:DB8:6::5
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::2/64
 vrrp6 vrid 2 virtual-ip FE80::2 link-local standby
 vrrp6 vrid 2 virtual-ip 2001:DB8:5::3
 vrrp6 vrid 4 virtual-ip FE80::4 link-local active
 vrrp6 vrid 4 virtual-ip 2001:DB8:5::5
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
 ipv6 route-static 0:0::0:0 0 2001:db8:6::4
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:5:: 64
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

7.7.3 CLI: Example for Configuring IPv6 Hot Standby in Active/Standby Mode on Devices That Connect Routers in Upstream and Downstream Directions

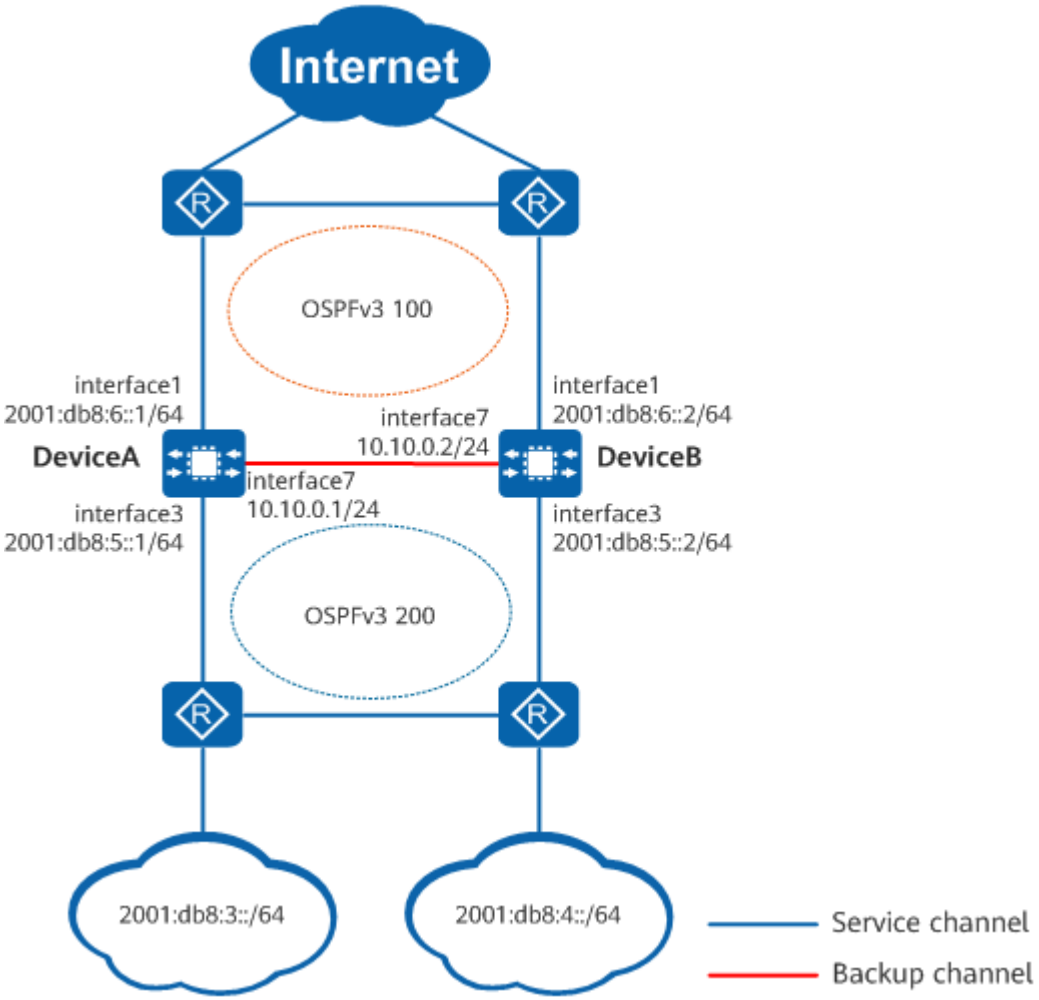
Networking Requirements

As shown in **Figure 7-49**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers. OSPFv3 runs between the devices and routers. DeviceA and DeviceB are expected to work in active/standby mode. During normal operation, traffic is forwarded by DeviceA. If DeviceA fails, DeviceB takes over to ensure service continuity.

Figure 7-49 Active/standby networking where service interfaces work at Layer 3 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Enable the IPv6 packet forwarding function of the upstream and downstream service interfaces on DeviceA and DeviceB, and configure IP addresses for the interfaces.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ipv6 enable** [DeviceA-GE0/0/1] **ipv6 address 2001:db8:6::1 64** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ipv6 enable** [DeviceA-GE0/0/3] **ipv6 address 2001:db8:5::1 64** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ipv6 enable** [DeviceB-GE0/0/1] **ipv6 address 2001:db8:6::2 64** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ipv6 enable** [DeviceB-GE0/0/3] **ipv6 address 2001:db8:5::2 64** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPFv3 to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospfv3 100** [DeviceA-ospfv3-100] **router-id 1.1.1.1** [DeviceA-ospfv3-100] **quit** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ospfv3 100 area 0.0.0.0** [DeviceA-GE0/0/1] **quit** [DeviceA] **ospfv3 200** [DeviceA-ospfv3-200] **router-id 10.1.1.1** [DeviceA-ospfv3-200] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ospfv3 200 area 0.0.0.0** [DeviceA-GE0/0/3] **quit**	[DeviceB] **ospfv3 100** [DeviceB-ospfv3-100] **router-id 1.1.1.2** [DeviceB-ospfv3-100] **quit** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ospfv3 100 area 0.0.0.0** [DeviceB-GE0/0/1] **quit** [DeviceB] **ospfv3 200** [DeviceB-ospfv3-200] **router-id 10.1.1.2** [DeviceB-ospfv3-200] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ospfv3 200 area 0.0.0.0** [DeviceB-GE0/0/3] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# Configure DeviceA and DeviceB to adjust the OSPFv3 cost values based on device priorities. After this command is run, a device determines whether it is the active or standby device when advertising OSPFv3 routes. If the device is the active one, it directly advertises the routes that it has learned. If it is the standby device, it advertises the routes after increasing the cost values. In this way, when upstream and downstream routers calculate routes, the next hop points to the active device, and packets are forwarded to the active device.	
[DeviceA] **hrp adjust ospfv3-cost enable**	[DeviceB] **hrp adjust ospfv3-cost enable**
# Specify the heartbeat interface and device role, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp device active** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp device standby** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Create security policies on DeviceA. After hot standby is enabled, the security policy on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow devices and the upstream and downstream routers to exchange OSPFv3 packets.

NOTE

OSPFv3 packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPFv3 packets are controlled by security policies. In this case, a security policy must be configured between the security zones where the upstream and downstream service interfaces reside and the local zone to allow OSPFv3 packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospfv3_1
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] destination-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospfv3_2
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] source-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 2001:db8:3:: 64
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 2001:db8:4:: 64
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec] quit
HRP_M[DeviceA-policy-security] quit
```

Step 5 Configure routers.

Configure OSPFv3 on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Run the **ping 2001:db8:6::4** command on the PC in the trust zone to ping a router in the untrust zone. The ping operation is successful. Run the **display firewall ipv6 session table** command on DeviceA and DeviceB. Sessions between the two devices are successfully created and backed up.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall ipv6 session table** Current Total Sessions : 2 icmpv6 VPN: public --> public 2001:DB8:3::4.0 --> 2001:DB8:6::4.2048 icmpv6 VPN: public --> public 2001:DB8:4::4.0 --> 2001:DB8:6::4.2048	HRP_S<DeviceB> **display firewall ipv6 session table** Current Total Sessions : 2 icmpv6 VPN: public --> public **Remote** 2001:DB8:3::4.0 --> 2001:DB8:6::4.2048 icmpv6 VPN: public --> public **Remote** 2001:DB8:4::4.0 --> 2001:DB8:6::4.2048

The preceding command output shows that sessions tagged with **Remote** are created on DeviceB. This indicates that the sessions are successfully backed up after the hot standby function is configured.

3. Run the **ping 2001:db8:6::4 -t** command on the PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is

 Copyright © Huawei Technologies Co., Ltd.

performed and whether ping packets are discarded. During the entire process, the ping operation is not interrupted.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp device active
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::1/64
 ospfv3 100 area 0.0.0.0
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::1/64
 ospfv3 200 area 0.0.0.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospfv3 100
 router-id 1.1.1.1
 area 0.0.0.0
ospfv3 200
 router-id 10.1.1.1
 area 0.0.0.0
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospfv3_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospfv3_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp device standby
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::2/64
 ospfv3 100 area 0.0.0.0
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::2/64
 ospfv3 200 area 0.0.0.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospfv3 100
 router-id 1.1.1.2
 area 0.0.0.0
ospfv3 200
 router-id 10.1.1.2
 area 0.0.0.0
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospfv3_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospfv3_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action permit rule name policy_sec source-zone trust destination-zone untrust source-address 2001:db8:3:: 64 source-address 2001:db8:4:: 64 action permit #	action permit rule name policy_sec source-zone trust destination-zone untrust source-address 2001:db8:3:: 64 source-address 2001:db8:4:: 64 action permit #

7.7.4 CLI: Example for Configuring IPv6 Hot Standby in Load Balancing Mode on Devices That Connect Routers in Upstream and Downstream Directions

Networking Requirements

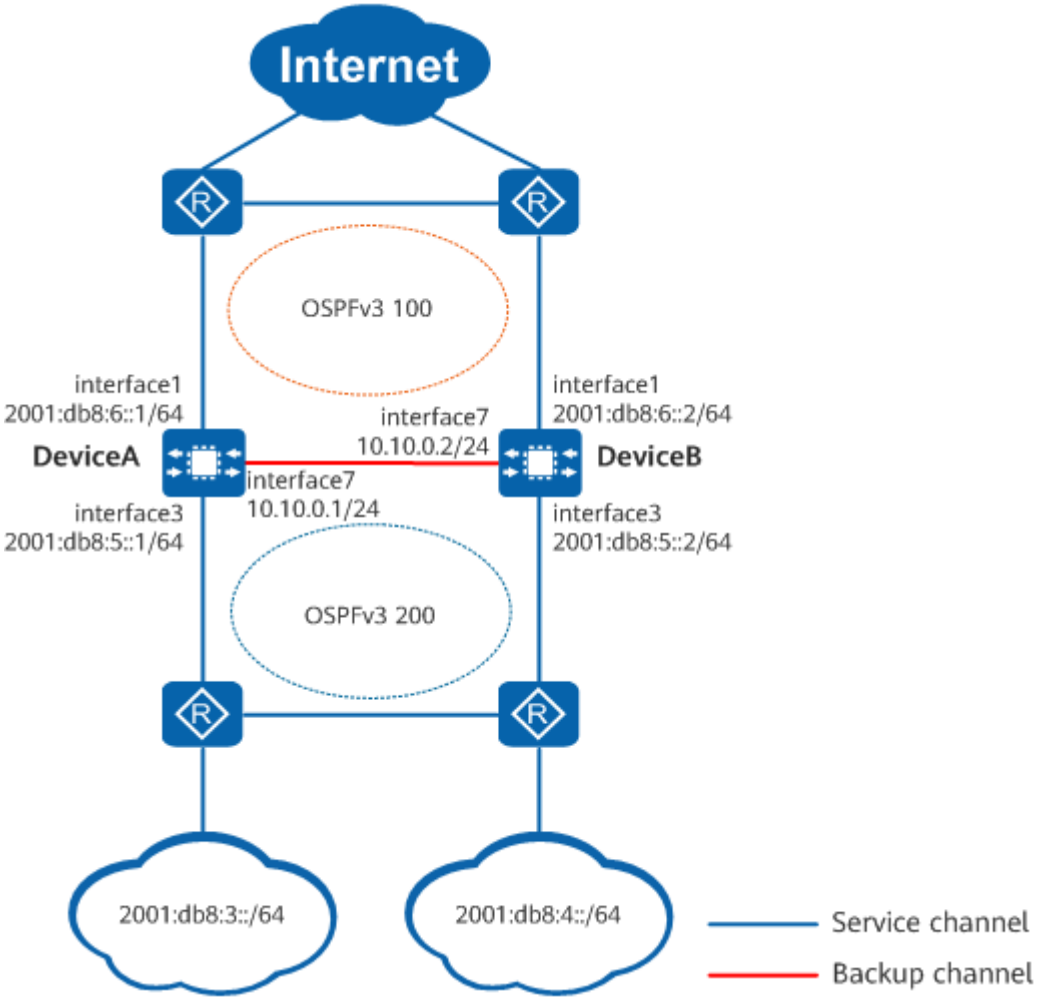
As shown in **Figure 7-50**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are connected to upstream and downstream routers. OSPFv3 runs between the devices and routers. It is required that DeviceA and DeviceB work in load sharing mode. During normal operation, both DeviceA and DeviceB forward traffic. If either device fails, the other device forwards all traffic to ensure service continuity.

Figure 7-50 Load sharing networking where service interfaces work at Layer 3 and connect to upstream and downstream routers

NOTE

In this example, interface1, interface3, and interface7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Enable the IPv6 packet forwarding function of the upstream and downstream service interfaces on DeviceA and DeviceB, and configure IP addresses for the interfaces.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ipv6 enable** [DeviceA-GE0/0/1] **ipv6 address 2001:db8:6::1 64** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ipv6 enable** [DeviceA-GE0/0/3] **ipv6 address 2001:db8:5::1 64** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ipv6 enable** [DeviceB-GE0/0/1] **ipv6 address 2001:db8:6::2 64** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ipv6 enable** [DeviceB-GE0/0/3] **ipv6 address 2001:db8:5::2 64** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPFv3 to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospfv3 100** [DeviceA-ospfv3-100] **router-id 1.1.1.1** [DeviceA-ospfv3-100] **quit** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ospfv3 100 area 0.0.0.0** [DeviceA-GE0/0/1] **quit** [DeviceA] **ospfv3 200** [DeviceA-ospfv3-200] **router-id 10.1.1.1** [DeviceA-ospfv3-200] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ospfv3 200 area 0.0.0.0** [DeviceA-GE0/0/3] **quit**	[DeviceB] **ospfv3 100** [DeviceB-ospfv3-100] **router-id 1.1.1.2** [DeviceB-ospfv3-100] **quit** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ospfv3 100 area 0.0.0.0** [DeviceB-GE0/0/1] **quit** [DeviceB] **ospfv3 200** [DeviceB-ospfv3-200] **router-id 10.1.1.2** [DeviceB-ospfv3-200] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ospfv3 200 area 0.0.0.0** [DeviceB-GE0/0/3] **quit**

Step 2 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure DeviceA and DeviceB to monitor upstream and downstream service interfaces.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# In load sharing networking, configure quick session backup on DeviceA and DeviceB in case of inconsistent paths for forward and return packets.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on each of DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

Step 4 Create security policies on DeviceA. After hot standby is enabled, the security policies on DeviceA will be automatically backed up to DeviceB.

Configure security policies to allow devices and the upstream and downstream routers to exchange OSPFv3 packets.

NOTE

OSPFv3 packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of this command is enabled, meaning that OSPFv3 packets are controlled by security policies. In this case, a security policy must be configured between the security zones where the upstream and downstream service interfaces reside and the local zone to allow OSPFv3 packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ospfv3_1
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] destination-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ospfv3_2
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] source-zone trust untrust
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] service ospf
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ospfv3_2] quit
```

Configure a security policy to allow intranet users to access the external network.

```
HRP_M[DeviceA-policy-security] rule name policy_sec
HRP_M[DeviceA-policy-security-rule-policy_sec] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 2001:db8:3:: 64
HRP_M[DeviceA-policy-security-rule-policy_sec] source-address 2001:db8:4:: 64
HRP_M[DeviceA-policy-security-rule-policy_sec] action permit
```

Step 5 Configure routers.

 Copyright © Huawei Technologies Co., Ltd.

Configure OSPFv3 on the routers to advertise routes. For configuration commands, refer to the related documents of the routers.

----End

Verifying the Configuration

1. Run the **display hrp state verbose** command on DeviceA and DeviceB to check the hot standby status.
2. Run the **ping 2001:db8:6::4** command on the PC in the trust zone to ping a router in the untrust zone. The ping operation is successful. Run the **display firewall ipv6 session table** command on DeviceA and DeviceB. Sessions between the two devices are successfully created and backed up.

DeviceA	DeviceB
HRP_M<DeviceA> **display firewall ipv6 session table** Current Total Sessions : 1 icmpv6 VPN: public --> public 2001:DB8:3::4.0 --> 2001:DB8:6::4.2048 icmpv6 VPN: public --> public **Remote** 2001:DB8:4::4.0 --> 2001:DB8:6::4.2048	HRP_S<DeviceB> **display firewall ipv6 session table** Current Total Sessions : 1 icmpv6 VPN: public --> public **Remote** 2001:DB8:3::4.0 --> 2001:DB8:6::4.2048 icmpv6 VPN: public --> public 2001:DB8:4::4.0 --> 2001:DB8:6::4.2048

   The preceding command output shows that sessions tagged with **Remote** are created on the two devices. This indicates that the sessions between the two devices are successfully backed up after hot standby is configured.
3. Run the **ping 2001:db8:6::4 -t** command on the PC. Then, pull out the cable from GE 0/0/1 on DeviceA and check whether an active/standby switchover is performed and whether ping packets are discarded. Plug the cable back into GE 0/0/1 on DeviceA and then check whether an active/standby switchover is performed and whether ping packets are discarded. During the entire process, the ping operation is not interrupted.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp mirror session enable
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::1/64
 ospfv3 100 area 0.0.0.0
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::1/64
 ospfv3 200 area 0.0.0.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospfv3 100
 router-id 1.1.1.1
 area 0.0.0.0
ospfv3 200
 router-id 10.1.1.1
 area 0.0.0.0
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospfv3_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospfv3_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
```

DeviceB

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp mirror session enable
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::2/64
 ospfv3 100 area 0.0.0.0
#
interface GE0/0/3
 ipv6 enable
 ipv6 address 2001:DB8:5::2/64
 ospfv3 200 area 0.0.0.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospfv3 100
 router-id 1.1.1.2
 area 0.0.0.0
ospfv3 200
 router-id 10.1.1.2
 area 0.0.0.0
#
security-policy
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_ospfv3_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospfv3_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
action permit rule name policy_sec source-zone trust destination-zone untrust source-address 2001:db8:3:: 64 source-address 2001:db8:4:: 64 action permit #	action permit rule name policy_sec source-zone trust destination-zone untrust source-address 2001:db8:3:: 64 source-address 2001:db8:4:: 64 action permit #

 Copyright © Huawei Technologies Co., Ltd.

8 IPsec

8.1 Communication Between LANs Through IPsec Tunnels
8.2 Communication Between LANs Through GRE over IPsec Tunnels
8.3 IPsec in NAT Scenarios
8.4 IPsec Virtualization
8.5 IPsec Dual-System Hot Standby
8.6 IPsec Intelligent Uplink Selection
8.7 Others

8.1 Communication Between LANs Through IPsec Tunnels

8.1.1 Web: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using PSK Authentication)

Networking Requirements

As shown in **Figure 8-1**, network A is connected to the Internet through DeviceA, and network B is connected to the Internet through DeviceB. The networking is described as follows:

- Network A belongs to the subnet 10.1.1.0/24 and is connected to DeviceA through interface 2.
- Network B belongs to the subnet 10.1.2.0/24 and is connected to DeviceB through interface 4.
- There are reachable routes between DeviceA and DeviceB.

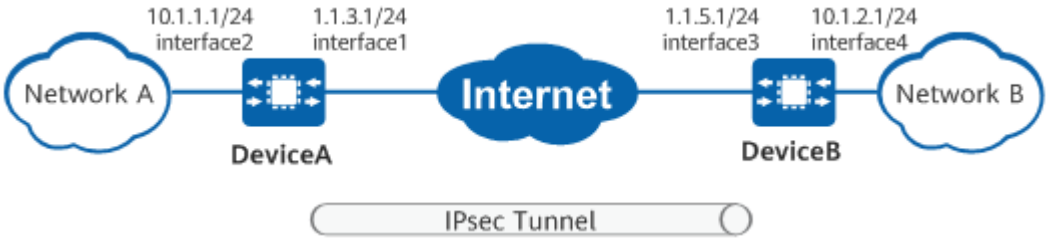
The networking must meet the following requirements: Establish an ISAKMP IPsec tunnel between DeviceA and DeviceB so that users on networks A and B can communicate with each other through the IPsec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-1 Establishing an IPsec tunnel in ISAKMP mode (using PSK authentication)

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.



Item	Data
DeviceA	Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	Interface number: GE0/0/1 IP address: 1.1.3.1/24 Security zone: Untrust
	IPsec configuration Scenario: point-to-point Remote address: 1.1.5.1 Authentication mode: pre-shared key (PSK) authentication PSK: Test!1234 Local ID: IP address Remote ID: IP address
DeviceB	Interface number: GE0/0/1 IP address: 1.1.5.1/24 Security zone: Untrust
	Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Scenario: point-to-point Remote address: 1.1.3.1 Authentication mode: PSK authentication PSK: Test!1234 Local ID: IP address Remote ID: IP address

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes between network A and network B.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.3.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy_ipsec_2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

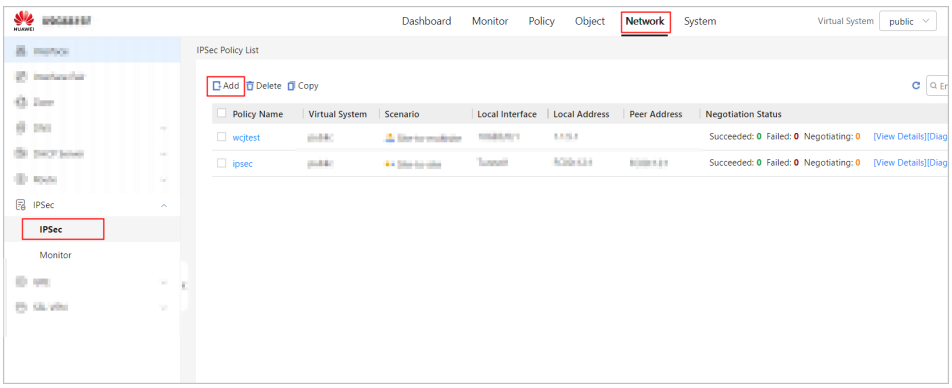
3. Configure static routes on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a static route to network B to divert encrypted data packets transmitted through the tunnel as follows. In this example, the next-hop IP address is 1.1.3.2. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.1.2.0/24
Next Hop	1.1.3.2

   d. Configure a static route to DeviceB to divert tunnel negotiation packets as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	1.1.5.0/24
Next Hop	1.1.3.2

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

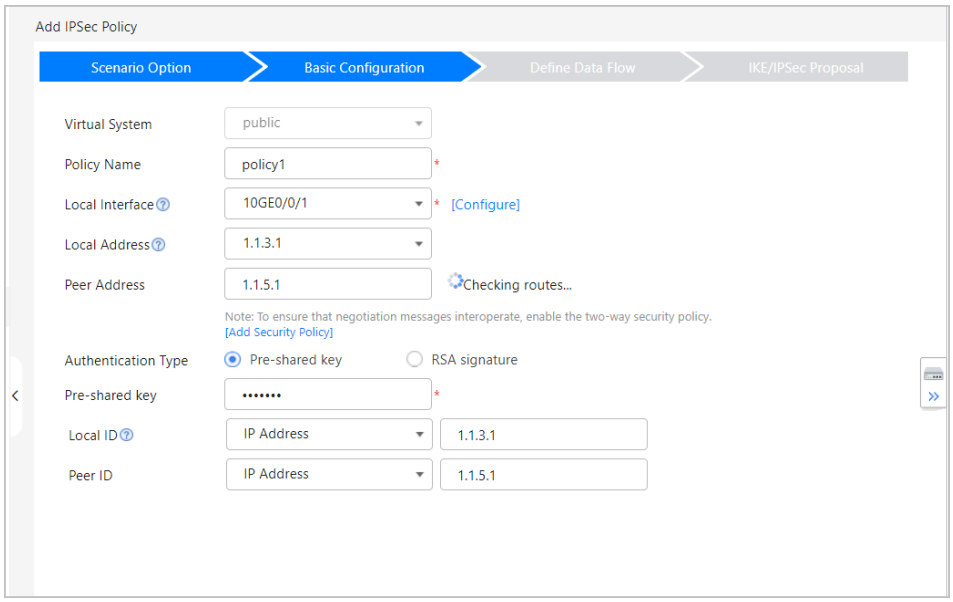


 Copyright © Huawei Technologies Co., Ltd.

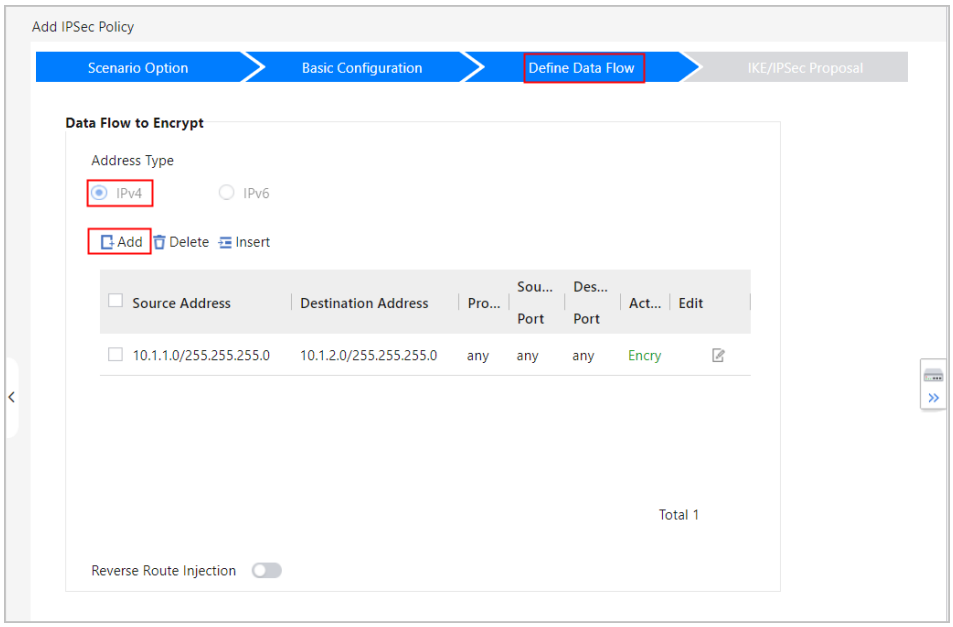
b. Click **Add** to create an IPsec policy as prompted.



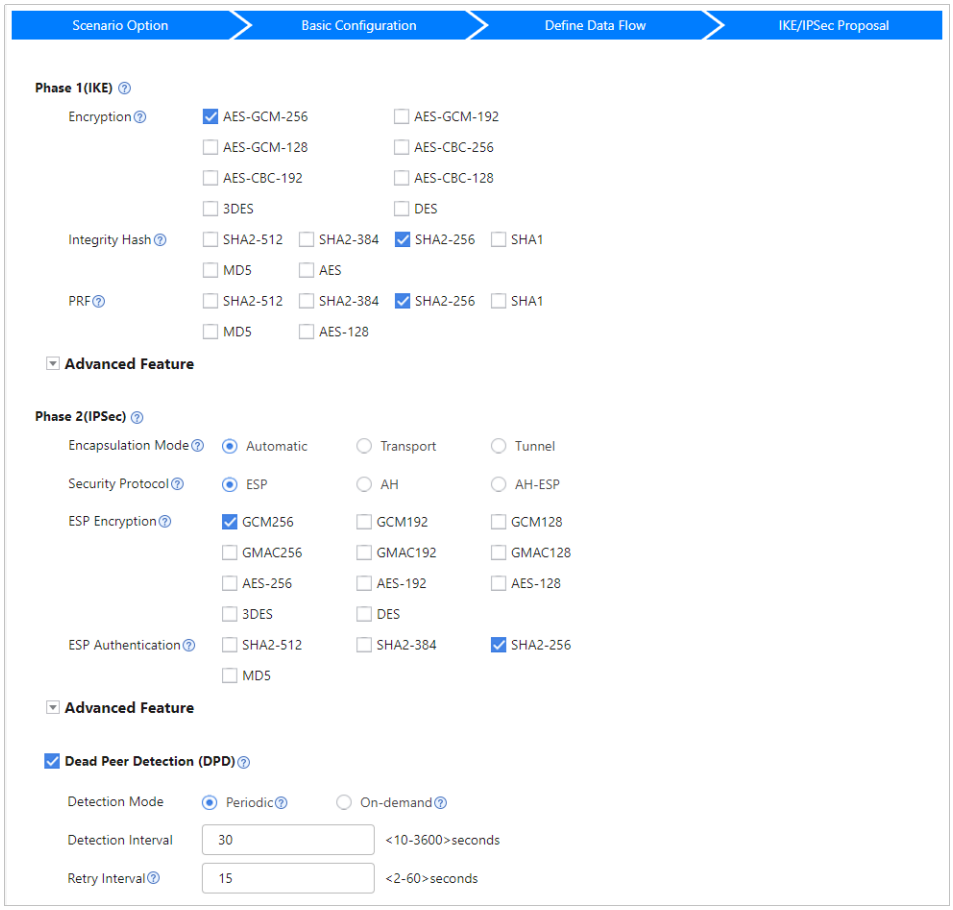
The PSK is Test!1234.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

Step 2 Configure DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.5.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy_ipsec_2
Source Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	trust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

3. Configure static routes on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceB to DeviceA as follows. Click **OK**.
   d. Configure a static route to network A to divert encrypted data packets transmitted through the tunnel as follows. In this example, the next-hop IP address is 1.1.5.2. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.1.1.0/24

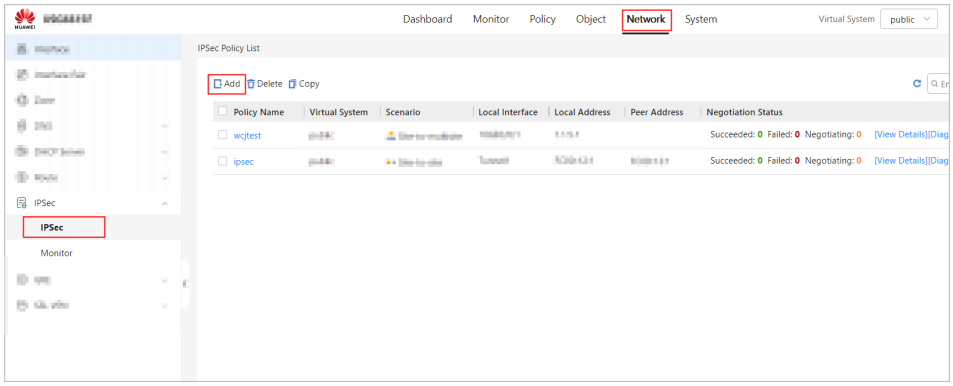
 Copyright © Huawei Technologies Co., Ltd.

Next Hop	1.1.5.2

e. Configure a static route to DeviceB to divert tunnel negotiation packets as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	1.1.3.0/24
Next Hop	1.1.5.2

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

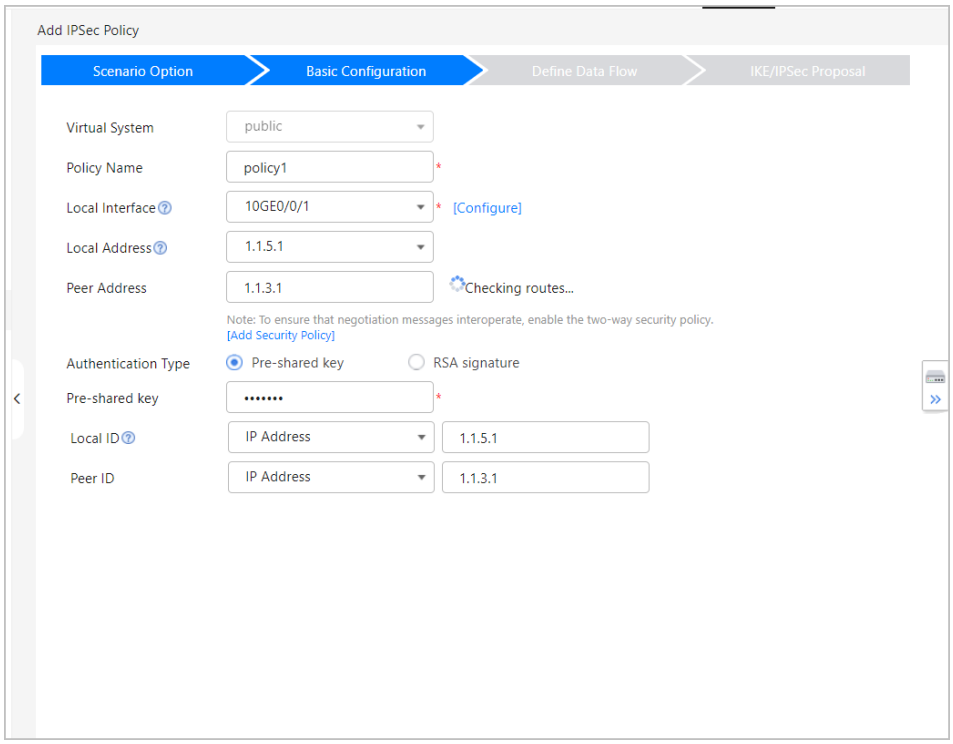


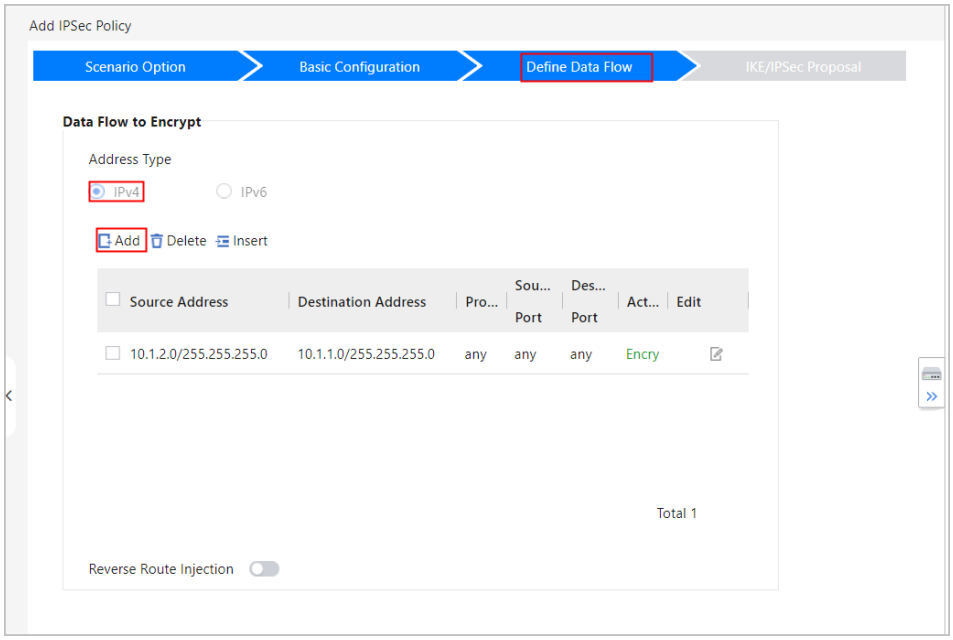
   b. Click **Add** to create an IPsec policy as prompted.



   The PSK is Test!1234.

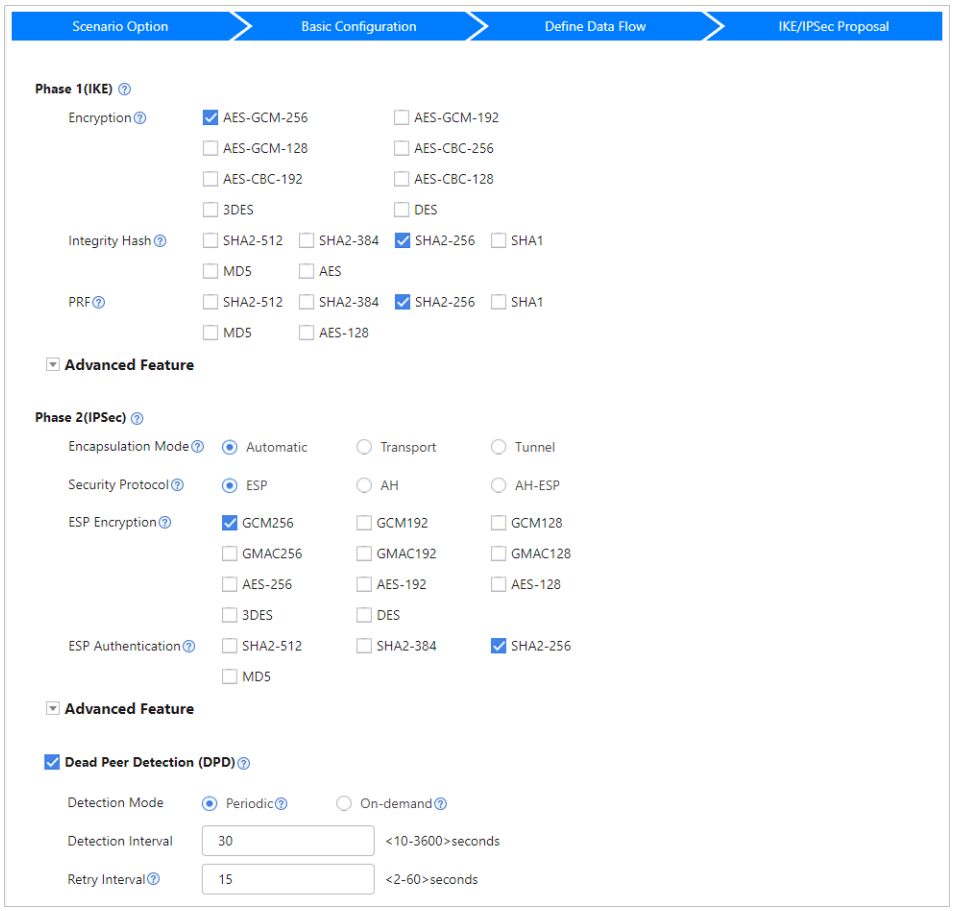
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

----End

Verifying the Configuration

1. Access a host or server on the headquarters network from a host on the branch network. The access succeeds.
2. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

Policy Name	Status	Local Address	Peer Address
policy1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.3.1	1.1.5.1

3. On DeviceB, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Policy Name	Status	Local Address	Peer Address
policy1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.5.1	1.1.3.1

Configuration Scripts

- DeviceA

```
#
acl number 3000
 rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop6117323732
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike6117323732
 pre-shared-key %$%$c([VET@941t/q_4tS-f7,ri/%$%$
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.5.1
 local-id 1.1.3.1
 remote-address 1.1.5.1
#
ipsec policy policy1 1 isakmp
 security acl 3000
 ike-peer ike6117323732
 proposal prop6117323732
 tunnel local 1.1.3.1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.3.1 255.255.255.0
 ipsec policy policy1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 10.1.2.0 255.255.255.0 1.1.3.2
ip route-static 1.1.5.0 255.255.255.0 1.1.3.2
#
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-address 10.1.2.0 24
 action permit
rule name policy_ipsec_2
 source-zone untrust
 destination-zone trust
 source-address 10.1.2.0 24
 destination-address 10.1.1.0 24
 action permit
rule name policy_ipsec_3
 source-zone untrust
 destination-zone local
 source-address 1.1.5.1 32
 destination-address 1.1.3.1 32
 action permit
rule name policy_ipsec_4
 source-zone local
 destination-zone untrust
 source-address 1.1.3.1 32
 destination-address 1.1.5.1 32
 action permit
```

- DeviceB

```
#
acl number 3000
 rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop6117323732
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike6117323732
 pre-shared-key %$%$pFR^=%xE/P^}NS*sN5e(,wne%$%$
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.3.1
 local-id 1.1.5.1
 remote-address 1.1.3.1
#
ipsec policy policy1 1 isakmp
 security acl 3000
 ike-peer ike6117323732
 proposal prop6117323732
 tunnel local 1.1.5.1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
 ipsec policy policy1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 10.1.1.0 255.255.255.0 1.1.5.2
ip route-static 1.1.3.0 255.255.255.0 1.1.5.2
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 24
  destination-address 10.1.1.0 24
  action permit
 rule name policy_ipsec_2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 24
  destination-address 10.1.2.0 24
  action permit
 rule name policy_ipsec_3
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 32
  destination-address 1.1.5.1 32
  action permit
 rule name policy_ipsec_4
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 32
  destination-address 1.1.3.1 32
  action permit
```

8.1.2 CLI: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using PSK Authentication)

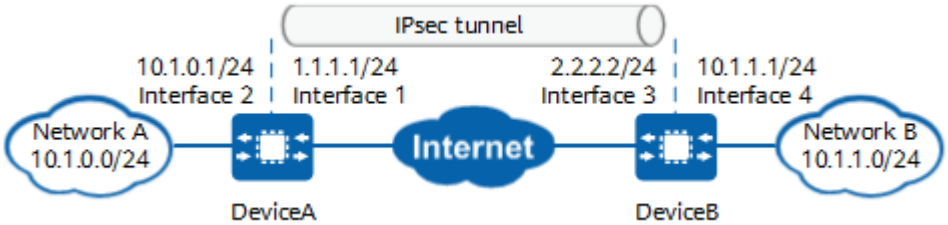
Networking Requirements

In **Figure 8-2**, networks A and B connect to the Internet through DeviceA and DeviceB respectively, and there are reachable routes between the two devices. An Internet Security Association and Key Management Protocol (ISAKMP) IPsec tunnel needs to be established between public network interfaces (interface 1 and interface 3) on the two devices. The two ends of the tunnel use pre-shared key (PSK) authentication to ensure secure transmission of data flows on specific network segments in networks A and B.

Figure 8-2 Establishing an IPsec tunnel in ISAKMP mode (using PSK authentication)

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 on DeviceA, and interface 3 and interface 4 represent GE 0/0/1 and GE 0/0/2 on DeviceB.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data
DeviceA	Interface: GE 0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.0.1/24 Security zone: Trust
	IPsec configuration Remote address: 2.2.2.2 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceB	Interface: GE 0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	IPsec configuration Remote address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure static routes to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
4. Configure ISAKMP IPsec policies and apply an IPsec policy group to an interface.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure static routes on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

Configure a static route to DeviceB to divert tunnel negotiation packets.

```
[DeviceA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
```

Configure a static route to network B to divert encrypted data packets transmitted through the tunnel.

```
[DeviceA] ip route-static 10.1.1.0 255.255.255.0 1.1.1.254
```

Step 4 Configure ISAKMP IPsec policies on DeviceA and apply an IPsec policy group to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.0.0/24 to access the network segment 10.1.1.0/24.

   ```
   [DeviceA] acl 3000
   [DeviceA-acl4-advance-3000] rule 5 permit ip source 10.1.0.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
   [DeviceA-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceA] ipsec proposal tran1
   [DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceA-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceA] ike proposal 10
   [DeviceA-ike-proposal-10] authentication-method pre-share
   [DeviceA-ike-proposal-10] prf hmac-sha2-256
   [DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceA-ike-proposal-10] dh group14
   [DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceA-ike-proposal-10] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

4. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] remote-address 2.2.2.2
[DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-b] quit
```

5. Configure an IPsec policy.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer b
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
```

Step 5 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.1.1 24
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 6 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 7 Configure static routes on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.254.

Configure a static route to DeviceA to divert tunnel negotiation packets.

```
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
```

Configure a static route to network A to divert encrypted data packets transmitted through the tunnel.

```
[DeviceB] ip route-static 10.1.0.0 255.255.255.0 2.2.2.254
```

Step 8 Configure ISAKMP IPsec policies on DeviceB and apply an IPsec policy group to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.0.0/24.

   ```
   [DeviceB] acl 3000
   [DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
   [DeviceB-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceB-ipsec-proposal-tran1] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

3. Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] remote-address 1.1.1.1
[DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-a] quit
```

5. Configure an IPsec policy.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on the device in the protected network segment of network A or network B to trigger IKE negotiation.

   If IKE negotiation succeeds, devices in the protected network segments at both ends of the tunnel can ping each other successfully. Otherwise, IKE negotiation fails.

2. On DeviceA and DeviceB, run the **display ike sa** and **display ipsec sa** commands to check SA establishment information. The following example uses the command output on DeviceB, which shows that IKE SAs and IPsec SAs have been established successfully.

```
<DeviceB> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU : 1
Total number of phase 2 SA in all CPU : 1

Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
  ------------------------------------------------------------------------------
    Conn-ID     Peer           VPN   Flag(s)  Phase  RemoteType  RemoteID
  ------------------------------------------------------------------------------
    16777239    1.1.1.1:500          RD|ST|A  v2:2   IP          1.1.1.1
    16777232    1.1.1.1:500          RD|ST|A  v2:1   IP          1.1.1.1
  ------------------------------------------------------------------------------
<DeviceB> display ipsec sa

ipsec sa information:
```

 Copyright © Huawei Technologies Co., Ltd.

```
==============================
Interface: GE0/0/1

==============================

 -----------------------------
 IPsec policy name: "map1"
 Sequence number  : 10
 Acl group        : 3000
 Acl rule         : 5
 Mode             : ISAKMP
 -----------------------------
   Connection ID     : 83903371
   Encapsulation mode: Tunnel
   Tunnel local      : 2.2.2.2
   Tunnel remote     : 1.1.1.1
   Flow source       : 10.1.1.0-10.1.1.255 0-65535 0
   Flow destination  : 10.1.0.0-10.1.0.255 0-65535 0

   [Outbound ESP SAs]
     SPI: 763065754 (0x2d7b759a)
     Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
     SA remaining key duration (kilobytes/sec): 0/3079
     Max sent sequence-number: 1
     UDP encapsulation used for NAT traversal: N
     SA encrypted packets (number/kilobytes): 4/0

   [Inbound ESP SAs]
     SPI: 163241969 (0x9badff1)
     Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
     SA remaining key duration (kilobytes/sec): 0/3079
     Max received sequence-number: 3203668
     UDP encapsulation used for NAT traversal: N
     SA decrypted packets (number/kilobytes): 4/0
     Anti-replay : Enable
     Anti-replay window size: 1024
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.0.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
  pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
  ike-proposal 10
  remote-address 2.2.2.2
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer b
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
 ip route-static 10.1.1.0 255.255.255.0 1.1.1.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
```

 Copyright © Huawei Technologies Co., Ltd.

```
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
 ip route-static 10.1.0.0 255.255.255.0 2.2.2.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
return
```

8.1.3 Web: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using Certificate Authentication)

Networking Requirements

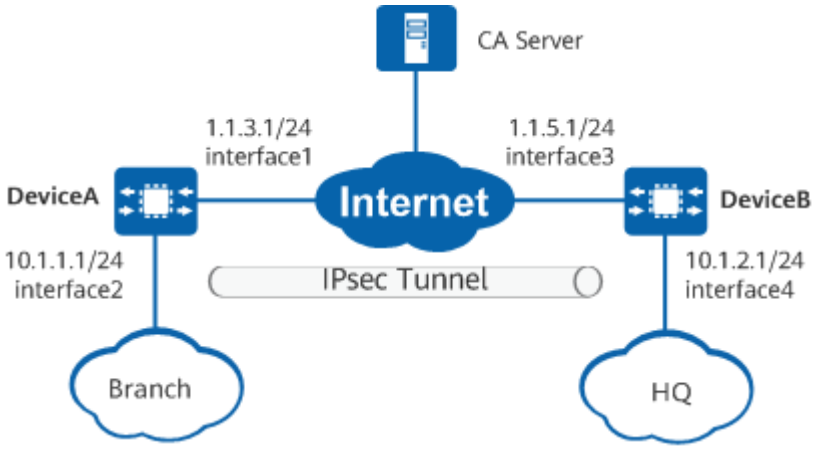
As shown in **Figure 8-3**, the enterprise branch is connected to the Internet through DeviceA, and the headquarters is connected to the Internet through DeviceB. To enhance communication security, the enterprise requires that an IPsec tunnel be established between the branch and headquarters using certificate authentication.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-3 Establishing an IPsec tunnel in ISAKMP mode (using certificate authentication)

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.



Item	DeviceA	DeviceB
Interface configuration	Interface number: GE0/0/1 IP address: 1.1.3.1/24 Security zone: Untrust	Interface number: GE0/0/1 IP address: 1.1.5.1/24 Security zone: Untrust
	Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust	Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
IPsec configuration	Scenario: point-to-point Remote IP address: 1.1.5.1 Authentication method: RSA signature Local ID: IP address Remote ID: IP address	Scenario: point-to-point Remote IP address: 1.1.3.1 Authentication method: RSA signature Local ID: IP address Remote ID: IP address

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes between network A and network B.
4. Configure DeviceA and DeviceB to apply for local and CA certificates.

 Copyright © Huawei Technologies Co., Ltd.

5. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

   You need to import the local and CA certificates when configuring an IPsec policy.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.3.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24

 Copyright © Huawei Technologies Co., Ltd.

Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy_ipsec_2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.3.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceA to DeviceB as follows. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.3.2

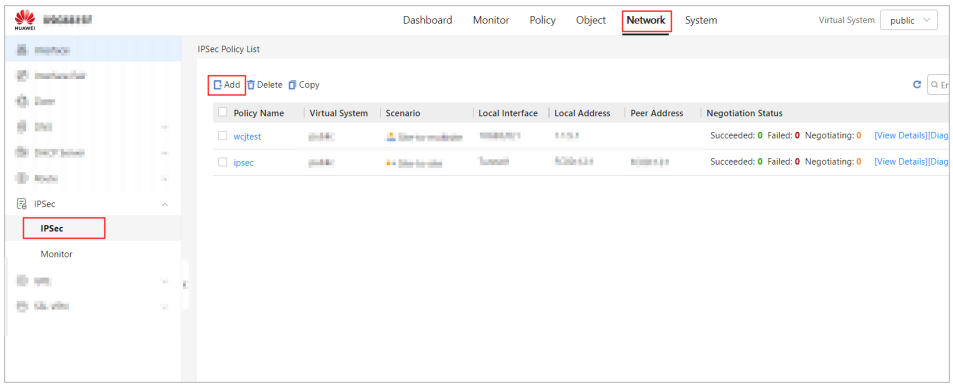
4. Apply for and import the local and CA certificates.

   For details about how to apply for and import local and CA certificates, see the Web Configuration Guide > Object > Certificates.

   During local certificate application, the IP address in the application file must be set to the IP address used by DeviceA to establish an IPsec tunnel.

5. Configure an IPsec policy.

   a. Choose **Network** > **IPSec** > **IPSec**.

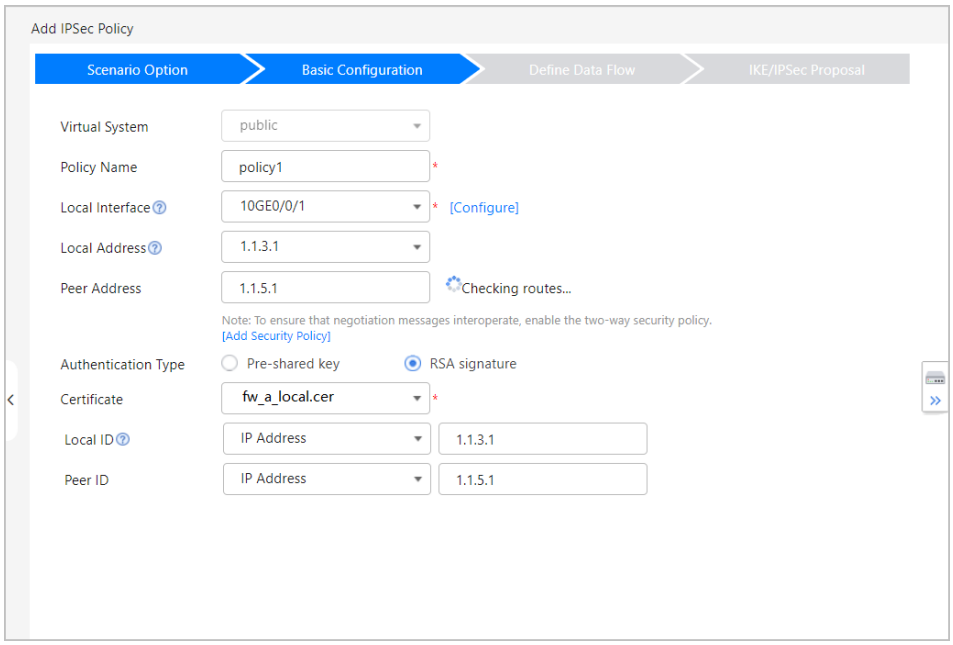
   

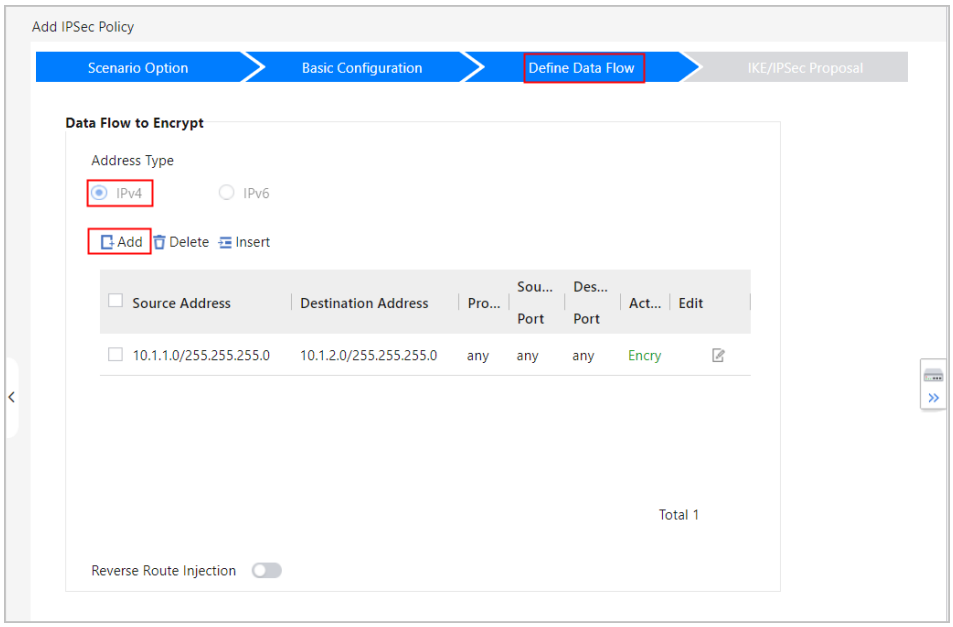
   b. Click **Add** to create an IPsec policy as prompted.

   Select the imported local certificate from the **Certificate** drop-down list.

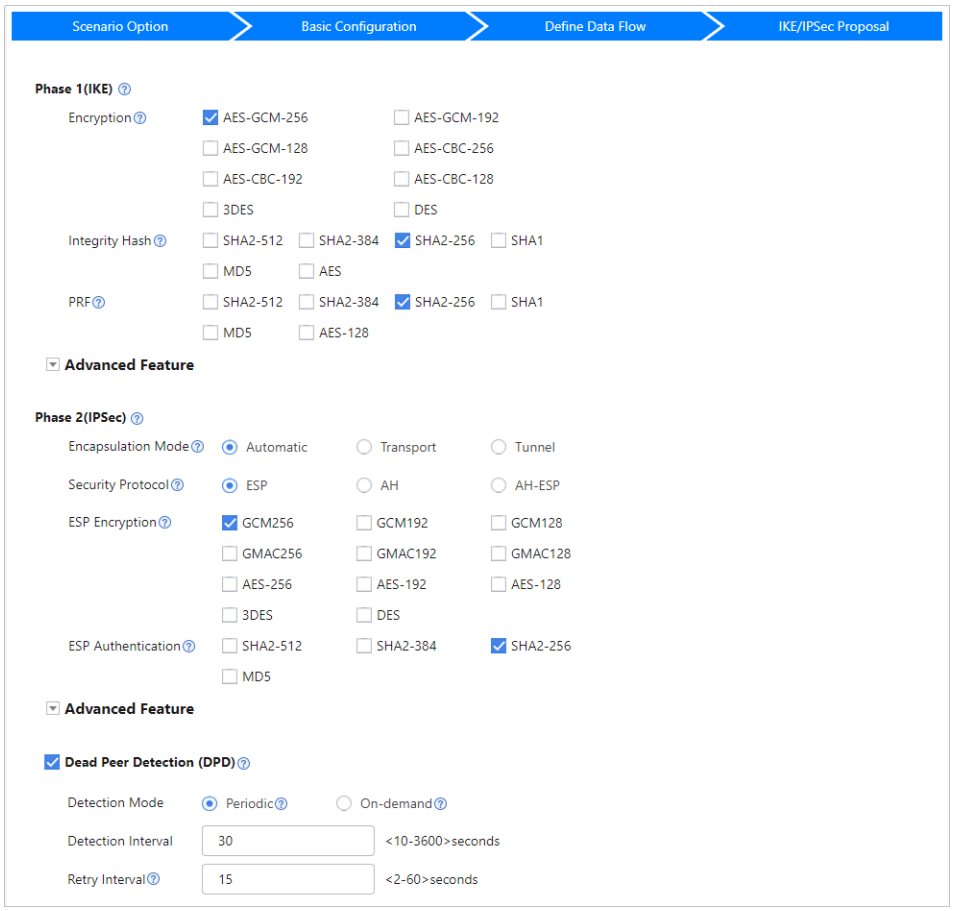
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

Step 2 Configure DeviceB.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.5.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy_ipsec_2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

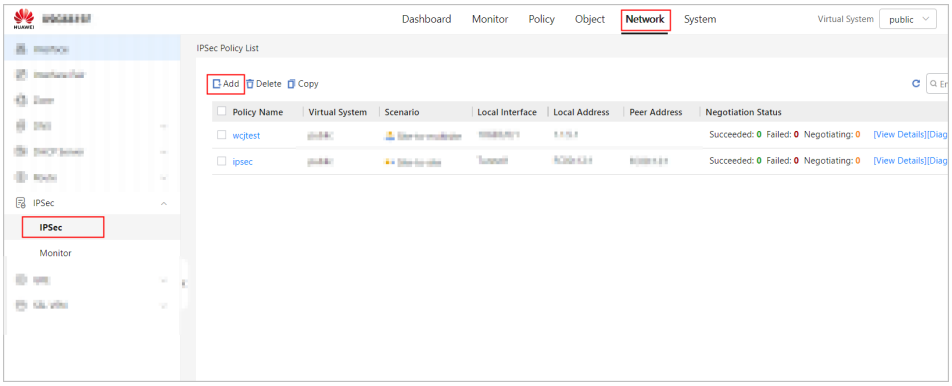
3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.5.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceB to DeviceA as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.5.2

4. Apply for and import the local and CA certificates.

   For details about how to apply for and import local and CA certificates, see the Web Configuration Guide > Object > Certificates.

   During local certificate application, the IP address in the application file must be set to the IP address used by DeviceB to establish an IPsec tunnel.
5. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

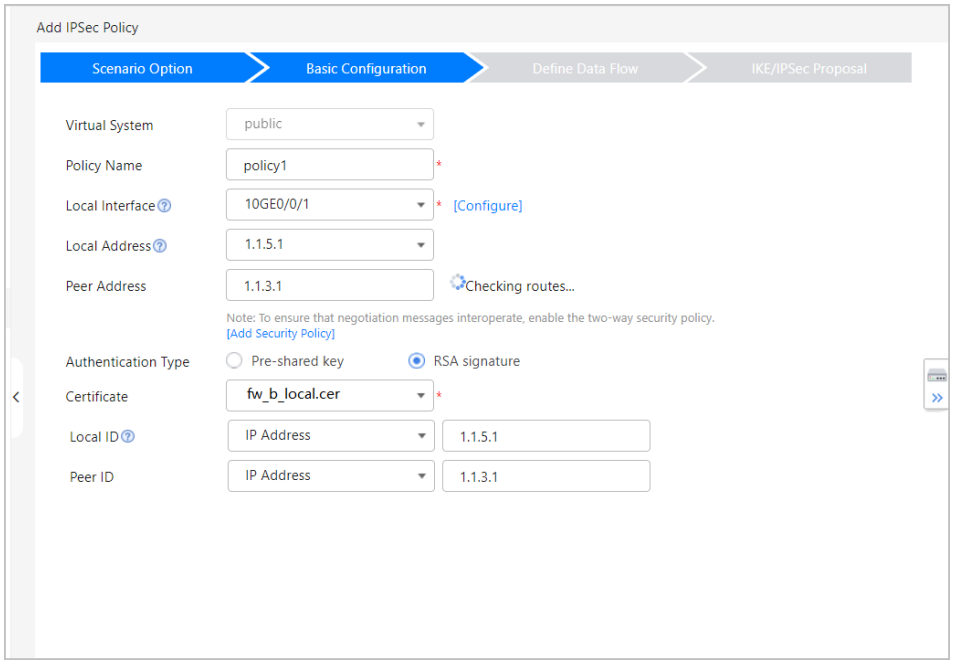


   b. Click **Add** to create an IPsec policy as prompted.

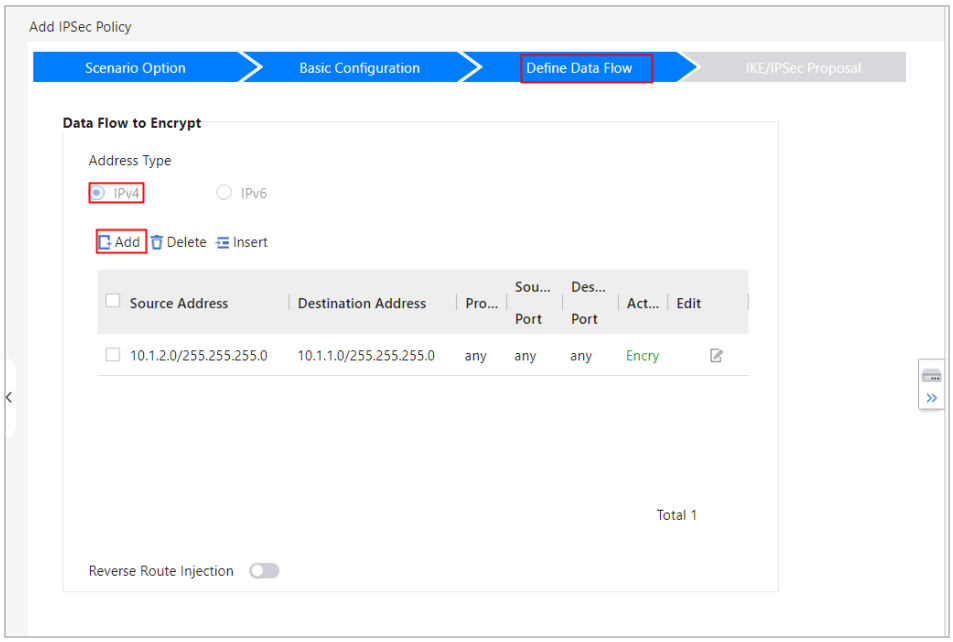
 Copyright © Huawei Technologies Co., Ltd.



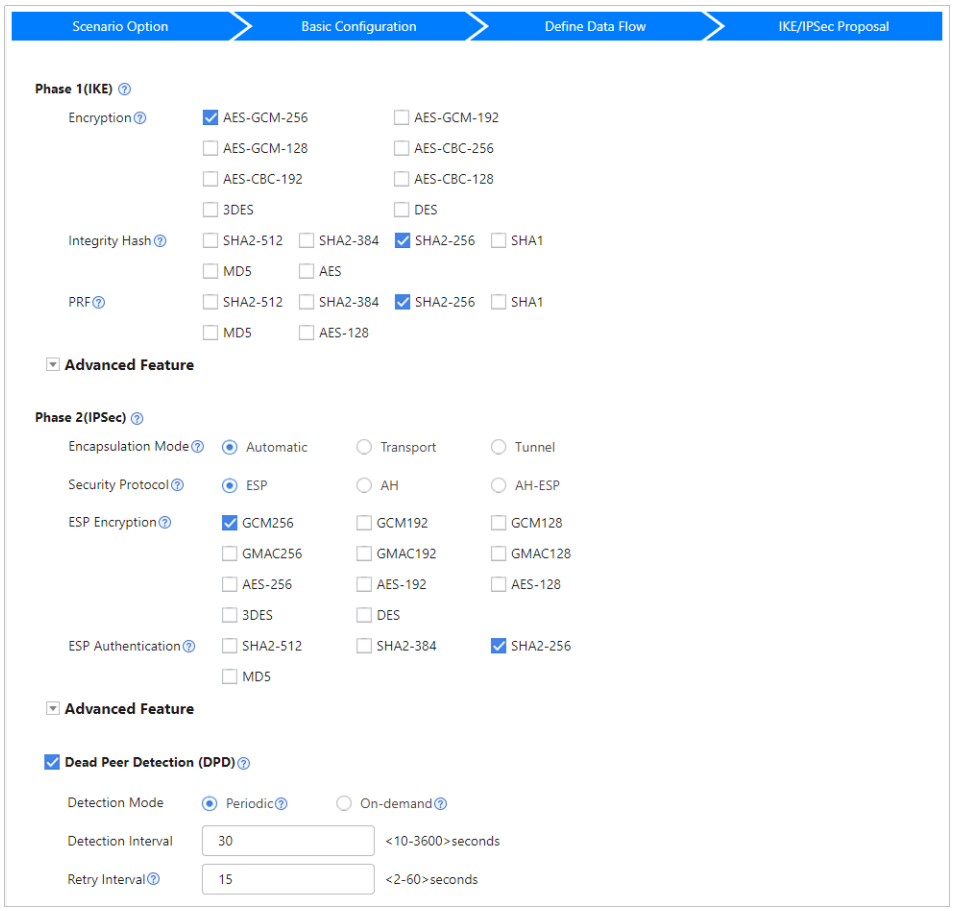
Select the imported local certificate from the **Certificate** drop-down list.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Access a host or server on the headquarters network from a host on the branch network. The access succeeds.
2. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

Policy Name	Status	Local Address	Peer Address
policy1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.3.1	1.1.5.1

3. On DeviceB, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

Policy Name	Status	Local Address	Peer Address
policy1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.5.1	1.1.3.1

Configuration Scripts

- DeviceA

```
#
acl number 3000
 rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop21115403936
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method rsa-signature
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike211154039363
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.5.1
 local-id 1.1.3.1
 remote-address 1.1.5.1
 certificate local-filename fw_a_local.cer
#
ipsec policy policy1 1 isakmp
 security acl 3000
 ike-peer ike211154039363
 proposal prop21115403936
 tunnel local 1.1.3.1
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.3.1 255.255.255.0
 ipsec policy policy1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.3.2
#
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_3
  source-zone untrust
  destination-zone local
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy_ipsec_4
  source-zone local
  destination-zone untrust
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
```

- DeviceB

```
#
acl number 3000
 rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop2111540184
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method rsa-signature
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike41117138841
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.3.1
 local-id 1.1.5.1
 remote-address 1.1.3.1
 certificate local-filename fw_b_local.cer
#
ipsec policy policy1 1 isakmp
 security acl 3000
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ike-peer ike41117138841
 proposal prop2111540184
 tunnel local 1.1.5.1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.5.1 255.255.255.0
 ipsec policy policy1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.5.2
#
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_3
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
 rule name policy_ipsec_4
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
```

8.1.4 CLI: Example for Establishing an IPsec Tunnel in ISAKMP Mode (Using Certificate Authentication)

Networking Requirements

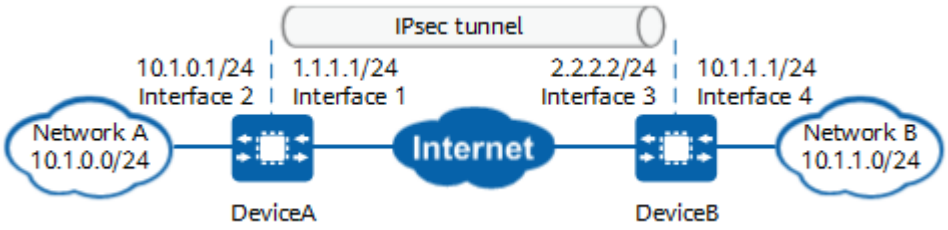
In **Figure 8-4**, networks A and B connect to the Internet through DeviceA and DeviceB respectively, and there are reachable routes between the two devices. An ISAKMP IPsec tunnel needs to be established between public network interfaces (interface 1 and interface 3) on the two devices. The two ends of the tunnel use Rivest-Shamir-Adleman (RSA) signature authentication to ensure secure transmission of data flows on specific network segments in networks A and B.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-4 Establishing an IPsec tunnel in ISAKMP mode (using certificate authentication)

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 on DeviceA, and interface 3 and interface 4 represent GE 0/0/1 and GE 0/0/2 on DeviceB.



Item	Data
DeviceA	Interface: GE 0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.0.1/24 Security zone: Trust
	IPsec configuration Remote address: 2.2.2.2 Authentication mode: RSA signature authentication Local ID: DN Remote ID: DN
DeviceB	Interface: GE 0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	IPsec configuration Remote address: 1.1.1.1 Authentication mode: RSA signature authentication Local ID: DN Remote ID: DN

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
3. Configure static routes to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
4. Apply for the local certificate and CA certificate in offline mode and import the certificates to the devices.
5. Configure ISAKMP IPsec policies and apply an IPsec policy group to an interface.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure static routes on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

Configure a static route to DeviceB to divert tunnel negotiation packets.

```
[DeviceA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
```

Configure a static route to network B to divert encrypted data packets transmitted through the tunnel.

```
[DeviceA] ip route-static 10.1.1.0 255.255.255.0 1.1.1.254
```

Step 4 Apply for the local certificate and CA certificate in offline mode and import the certificates to the device.

1. Create a 3072-bit RSA key pair and allow it to be exported from the device.

```
[DeviceA] pki rsa local-key-pair create rsakey_a exportable
 Info: The name of the new key-pair will be: rsakey_a
```

```
The size of the public key ranges from 2048 to 4096.
Input the bits in the modules:3072
Generating key-pairs...
Generating key-pairs finished
```

2. Configure a PKI entity to identify a certificate applicant.

```
[DeviceA] pki entity user_a
[DeviceA-pki-entity-user_a] common-name devicea
[DeviceA-pki-entity-user_a] country cn
[DeviceA-pki-entity-user_a] email testa@user.com
[DeviceA-pki-entity-user_a] fqdn testa.abc.com
[DeviceA-pki-entity-user_a] ip-address 1.1.1.1
[DeviceA-pki-entity-user_a] state beijing
[DeviceA-pki-entity-user_a] organization huawei
[DeviceA-pki-entity-user_a] organization-unit dev
[DeviceA-pki-entity-user_a] quit
```

3. Apply for a local certificate for the PKI entity in offline mode.

   # Create a PKI realm.

```
[DeviceA] pki realm a
[DeviceA-pki-realm-a] entity user_a
[DeviceA-pki-realm-a] rsa local-key-pair rsakey_a
[DeviceA-pki-realm-a] quit
```

   # Save certificate application information to a certificate request file in PKCS#10 format.

```
[DeviceA] pki enroll-certificate realm a pkcs10 filename cer_req
 Info: Creating certificate request file...
 Info: Create certificate request file successfully.
```

4. Download the certificate request file using a file transfer protocol, and send the file to the CA server in out-of-band mode, such as through the web system, using a disk, or through an email, to apply for a local certificate from the CA server.

   After a local certificate is successfully requested, download the local certificate **a_local.cer** and CA certificate **a_ca.cer** in out-of-band mode. Transfer the certificates to the device storage using a file transfer protocol.

5. Import the CA certificate into the device memory.

   After the certificate is imported, the **a_ca.cer** file is deleted from the storage medium by default. To keep it, select **N** as prompted.

```
[DeviceA] pki import-certificate ca filename a_ca.cer
 The CA's Subject is /CN=ca_root
 The CA's fingerprint is:
   MD5  fingerprint:1135 25D8 96D3 5936 C382 35EA 2CEE 80EB
   SHA1 fingerprint:6330 974F B2FE 3C52 D16B DAC4 0140 918B 4BCD 3EC7
 Is the fingerprint correct?(Y/N):y
 Info: Succeeded in importing the certificate.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select
[Y/N]:y
 Info: Delete Success.
```

6. Import the local certificate into the device memory.

   After the certificate is imported, the **a_local.cer** file is deleted from the storage medium by default. To keep it, select **N** as prompted.

```
[DeviceA] pki import-certificate local filename a_local.cer
 Info: Succeeded in importing file.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select
[Y/N]:y
 Info: Delete Success
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure ISAKMP IPsec policies on DeviceA and apply an IPsec policy group to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.0.0/24 to access the network segment 10.1.1.0/24.

```
[DeviceA] acl 3000
[DeviceA-acl4-advance-3000] rule 5 permit ip source 10.1.0.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceA-acl4-advance-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method rsa-signature
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] local-id-type dn
[DeviceA-ike-peer-b] remote-id-type dn
[DeviceA-ike-peer-b] certificate local-filename a_local.cer
[DeviceA-ike-peer-b] remote-address 2.2.2.2
[DeviceA-ike-peer-b] remote-id /C=CN/ST=beijing/O=huawei/OU=dev/CN=deviceb
[DeviceA-ike-peer-b] quit
```

5. Configure an IPsec policy.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer b
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
```

Step 6 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.1.1 24
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 7 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 8 Configure static routes on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.254.

 Copyright © Huawei Technologies Co., Ltd.

Configure a static route to DeviceA to divert tunnel negotiation packets.

```
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
```

Configure a static route to network A to divert encrypted data packets transmitted through the tunnel.

```
[DeviceB] ip route-static 10.1.0.0 255.255.255.0 2.2.2.254
```

Step 9 Apply for the local certificate and CA certificate in offline mode and import the certificates to the device.

1. Create a 3072-bit RSA key pair and allow it to be exported from the device.

```
[DeviceB] pki rsa local-key-pair create rsakey_b exportable
 Info: The name of the new key-pair will be: rsakey_b
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:3072
 Generating key-pairs...
 Generating key-pairs finished
```

2. Configure a PKI entity to identify a certificate applicant.

```
[DeviceB] pki entity user_b
[DeviceB-pki-entity-user_b] common-name deviceb
[DeviceB-pki-entity-user_b] country cn
[DeviceB-pki-entity-user_b] email testb@user.com
[DeviceB-pki-entity-user_b] fqdn testb.abc.com
[DeviceB-pki-entity-user_b] ip-address 1.1.1.1
[DeviceB-pki-entity-user_b] state beijing
[DeviceB-pki-entity-user_b] organization huawei
[DeviceB-pki-entity-user_b] organization-unit dev
[DeviceB-pki-entity-user_b] quit
```

3. Apply for a local certificate for the PKI entity in offline mode.

   # Create a PKI realm.

```
[DeviceB] pki realm b
[DeviceB-pki-realm-b] entity user_b
[DeviceB-pki-realm-b] rsa local-key-pair rsakey_b
[DeviceB-pki-realm-b] quit
```

   # Save certificate application information to a certificate request file in PKCS#10 format.

```
[DeviceB] pki enroll-certificate realm b pkcs10 filename cer_req
 Info: Creating certificate request file...
 Info: Create certificate request file successfully.
```

4. Download the certificate request file using a file transfer protocol, and send the file to the CA server in out-of-band mode, such as through the web system, using a disk, or through an email, to apply for a local certificate from the CA server.

   After a local certificate is successfully requested, download the local certificate **b_local.cer** and CA certificate **b_ca.cer** in out-of-band mode. Transfer the certificates to the device storage using a file transfer protocol.

5. Import the CA certificate into the device memory.

```
[DeviceB] pki import-certificate ca filename b_ca.cer
 The CA's Subject is /CN=ca_root
 The CA's fingerprint is:
   MD5  fingerprint:1135 25D8 96D3 5936 C382 35EA 2CEE 80EB
   SHA1 fingerprint:6330 974F B2FE 3C52 D16B DAC4 0140 918B 4BCD 3EC7
 Is the fingerprint correct?(Y/N):y
 Info: Succeeded in importing file.
```

6. Import the local certificate into the device memory.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] pki import-certificate local filename b_local.cer
 Info: Succeeded in importing file.
```

Step 10 Configure ISAKMP IPsec policies on DeviceB and apply an IPsec policy group to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.0.0/24.

```
[DeviceB] acl 3000
[DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
[DeviceB-acl4-advance-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method rsa-signature
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] local-id-type dn
[DeviceB-ike-peer-a] remote-id-type dn
[DeviceB-ike-peer-a] certificate local-filename b_local.cer
[DeviceB-ike-peer-a] remote-address 1.1.1.1
[DeviceB-ike-peer-a] remote-id /C=CN/ST=beijing/O=huawei/OU=dev/CN=devicea
[DeviceB-ike-peer-a] quit
```

5. Configure an IPsec policy.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on the device in the protected network segment of network A or network B to trigger IKE negotiation.

   If IKE negotiation succeeds, devices in the protected network segments at both ends of the tunnel can ping each other successfully. Otherwise, IKE negotiation fails.

2. On DeviceA and DeviceB, run the **display ike sa** and **display ipsec sa** commands to check SA establishment information. The following example

 Copyright © Huawei Technologies Co., Ltd.

uses the command output on DeviceB, which shows that IKE SAs and IPsec SAs have been established successfully.

```
<DeviceB> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU : 1
Total number of phase 2 SA in all CPU : 1

Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
 -------------------------------------------------------------------------------
   Conn-ID     Peer           VPN   Flag(s)  Phase  RemoteType  RemoteID
 -------------------------------------------------------------------------------
   16777239    1.1.1.1:500          RD|ST|A  v2:2   DN          /C=CN/ST=beijing/O=huawei/OU=dev/
CN=devicea
   16777232    1.1.1.1:500          RD|ST|A  v2:1   DN          /C=CN/ST=beijing/O=huawei/OU=dev/
CN=devicea
  -------------------------------------------------------------------------------
<DeviceB> display ipsec sa

ipsec sa information:

================================
Interface: GE0/0/1

================================

  ----------------------------
  IPsec policy name: "map1"
  Sequence number  : 10
  Acl group        : 3000
  Acl rule         : 5
  Mode             : ISAKMP
  ----------------------------
    Connection ID     : 83903371
    Encapsulation mode: Tunnel
    Tunnel local      : 2.2.2.2
    Tunnel remote     : 1.1.1.1
    Flow source       : 10.1.1.0-10.1.1.255 0-65535 0
    Flow destination  : 10.1.0.0-10.1.0.255 0-65535 0

    [Outbound ESP SAs]
      SPI: 763065754 (0x2d7b759a)
      Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 0/3079
      Max sent sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      SA encrypted packets (number/kilobytes): 4/0

    [Inbound ESP SAs]
      SPI: 163241969 (0x9badff1)
      Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 0/3079
      Max received sequence-number: 3203668
      UDP encapsulation used for NAT traversal: N
      SA decrypted packets (number/kilobytes): 4/0
      Anti-replay : Enable
      Anti-replay window size: 1024
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
acl number 3000
 rule 5 permit ip source 10.1.0.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method rsa-signature
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 ike-proposal 10
 local-id-type dn
 remote-id-type dn
 remote-id /C=CN/ST=beijing/O=huawei/OU=dev/CN=deviceb
 remote-address 2.2.2.2
 certificate local-filename a_local.cer
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer b
 proposal tran1
#
pki entity user_a
 common-name devicea
 country cn
 email testa@user.com
 fqdn testa.abc.com
 ip-address 1.1.1.1
 state beijing
 organization huawei
 organization-unit dev
#
pki realm a
 entity user_a
 rsa local-key-pair rsakey_a
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
 ip route-static 10.1.1.0 255.255.255.0 1.1.1.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone trust
 source-address 10.1.1.0 mask 255.255.255.0
 destination-address 10.1.0.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 1.1.1.1 mask 255.255.255.255
 destination-address 2.2.2.2 mask 255.255.255.255
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 2.2.2.2 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method rsa-signature
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 ike-proposal 10
 local-id-type dn
 remote-id-type dn
 remote-id /C=CN/ST=beijing/O=huawei/OU=dev/CN=devicea
 remote-address 1.1.1.1
 certificate local-filename b_local.cer
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
pki entity user_b
 common-name deviceb
 country cn
 email testb@user.com
 fqdn testb.abc.com
 ip-address 1.1.1.1
 state beijing
 organization huawei
 organization-unit dev
#
pki realm b
 entity user_b
 rsa local-key-pair rsakey_b
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec policy map1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
 ip route-static 10.1.0.0 255.255.255.0 2.2.2.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
return
```

8.1.5 Web: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use the Same PSK for Authentication)

Networking Requirements

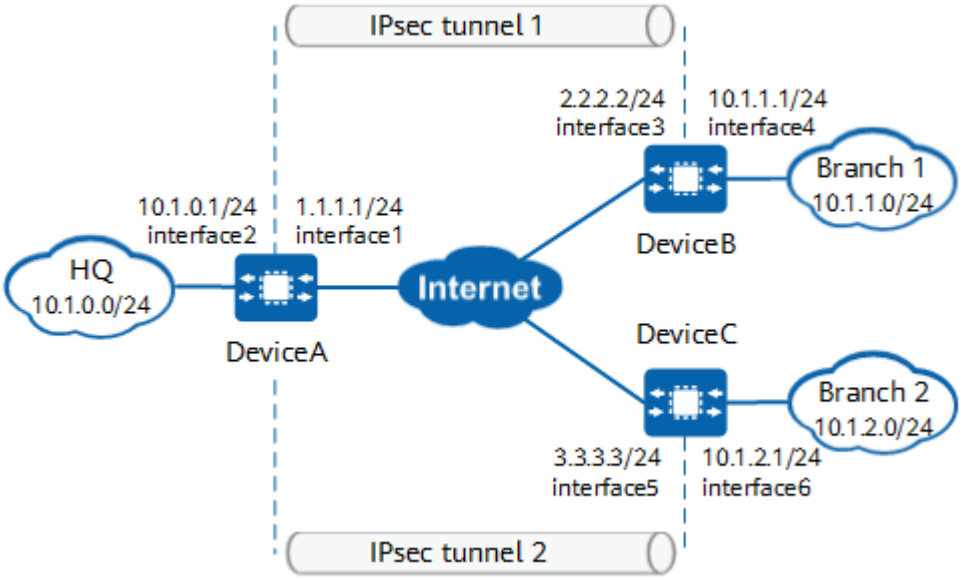
As shown in **Figure 8-5**, an enterprise has a headquarters and multiple branches. DeviceA is the egress gateway of the headquarters, and DeviceB and DeviceC are the egress gateways of the branches. The IP address of DeviceA is fixed. The networking must meet the following requirements: IPsec tunnels need to be established between the headquarters and multiple branches to implement secure communication between them. Different branches use the same PSK for identity authentication.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-5 Establishing an IPsec tunnel using an IPsec policy template (branches use the same PSK for authentication)

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively; interface 5 and interface 6 represent GE0/0/1 and GE0/0/2 of DeviceC, respectively.



Item	DeviceA	DeviceB	DeviceC
Interface configuration	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust Interface number: GE0/0/2 IP address: 10.1.0.1/24 Security zone: Trust	Interface number: GE0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust	Interface number: GE0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	DeviceA	DeviceB	DeviceC
IPsec configuration	Scenario: point-to-multipoint Remote address: not configured Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: Any	Scenario: point-to-point Remote address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: Any	Scenario: point-to-point Remote address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: Any

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB and DeviceC.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes between the headquarters and branches.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

   Note that you do not need to set the remote IP address when configuring DeviceA, because the remote IP address is not fixed. When configuring DeviceB and DeviceC, you need to set the peer IP address.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

IP Address	10.1.0.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.

   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.0.0/24
Destination Address	10.1.1.0/24 10.1.2.0/24
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.1.0/24 10.1.2.0/24
Destination Address	10.1.0.0/24
Action	Permit

Name	policy3
Source Zone	untrust

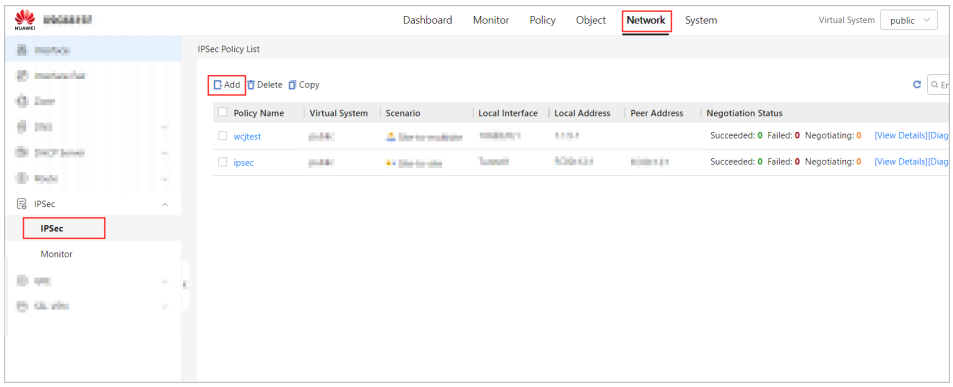
 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	local
Source Address	2.2.2.2/32 3.3.3.3/32
Destination Address	1.1.1.1/32
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.1.254.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a route from DeviceA to the Internet as follows. Click **OK**.

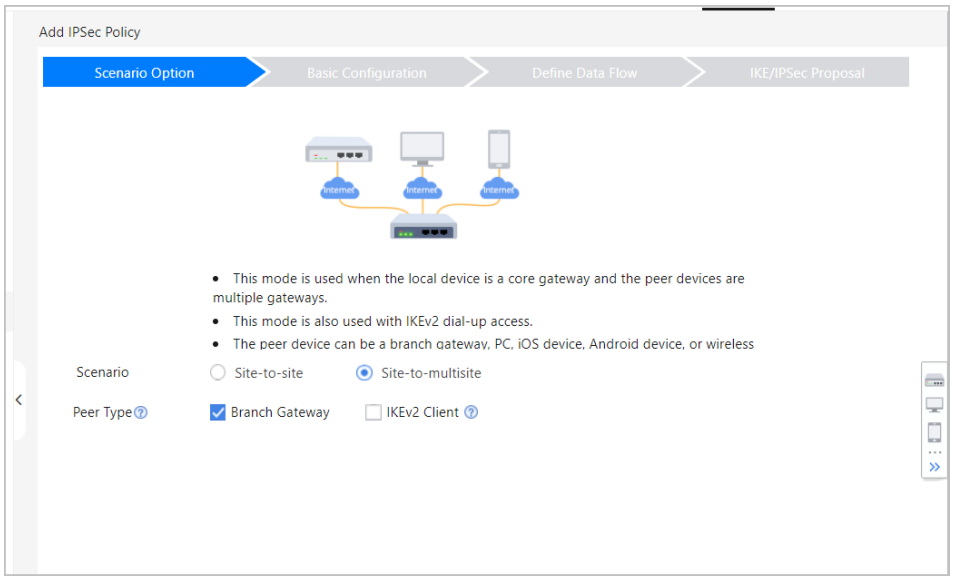
Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

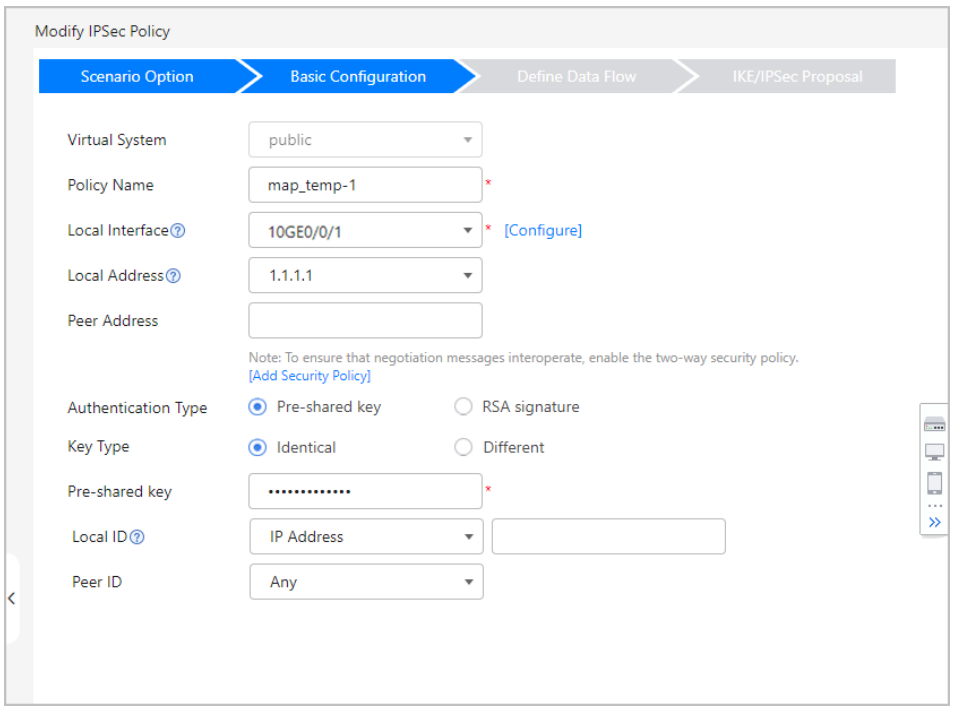


   b. Click **Add** to create an IPsec policy as prompted.

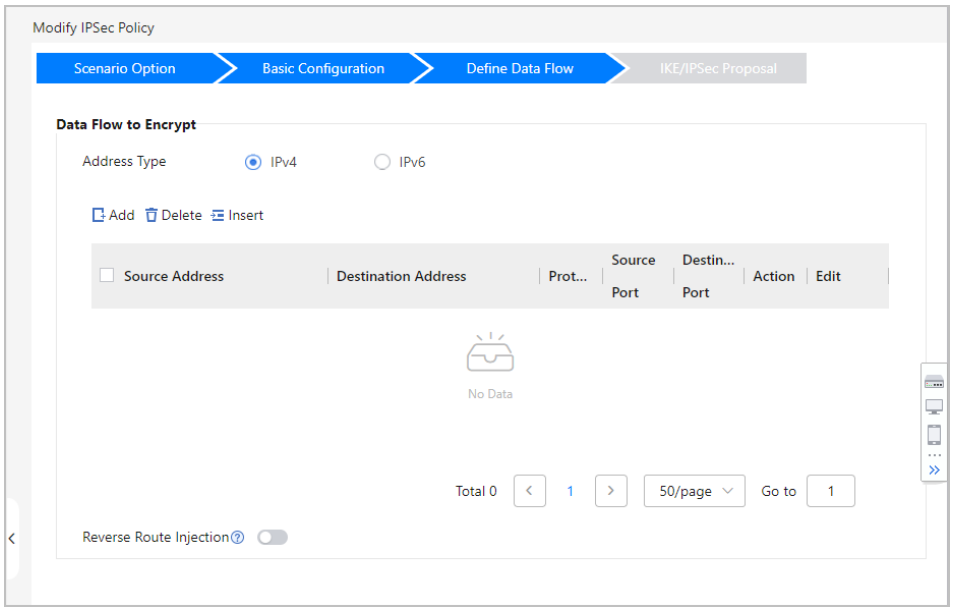
 Copyright © Huawei Technologies Co., Ltd.



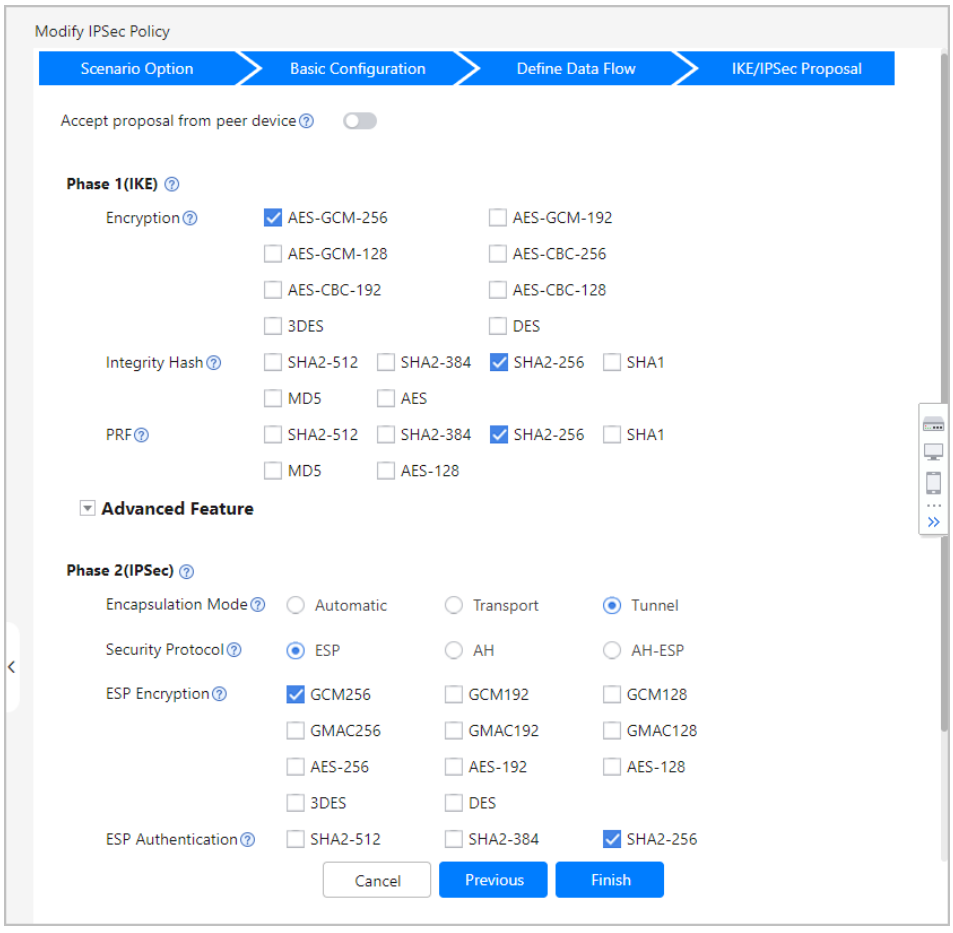
The PSK is YsHsjx_202206.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

Step 2 Configure DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	2.2.2.2/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Destination Address	10.1.0.0/24
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	trust
Source Address	10.1.0.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2.2.2.2/32
Destination Address	1.1.1.1/32
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.1.1/32
Destination Address	2.2.2.2/32
Action	Permit

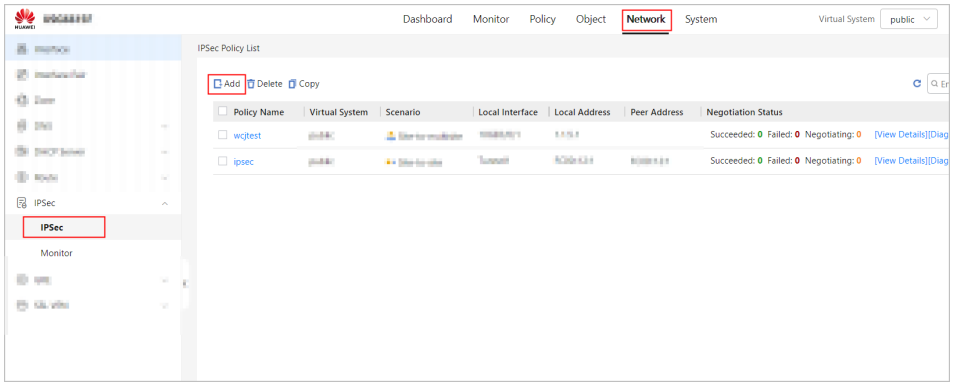
3. Create a static route to the Internet. In this example, the next-hop IP address is 2.2.2.254.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a route from DeviceB to the Internet as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	2.2.2.254

4. Configure an IPsec policy.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Network** > **IPSec** > **IPSec**.

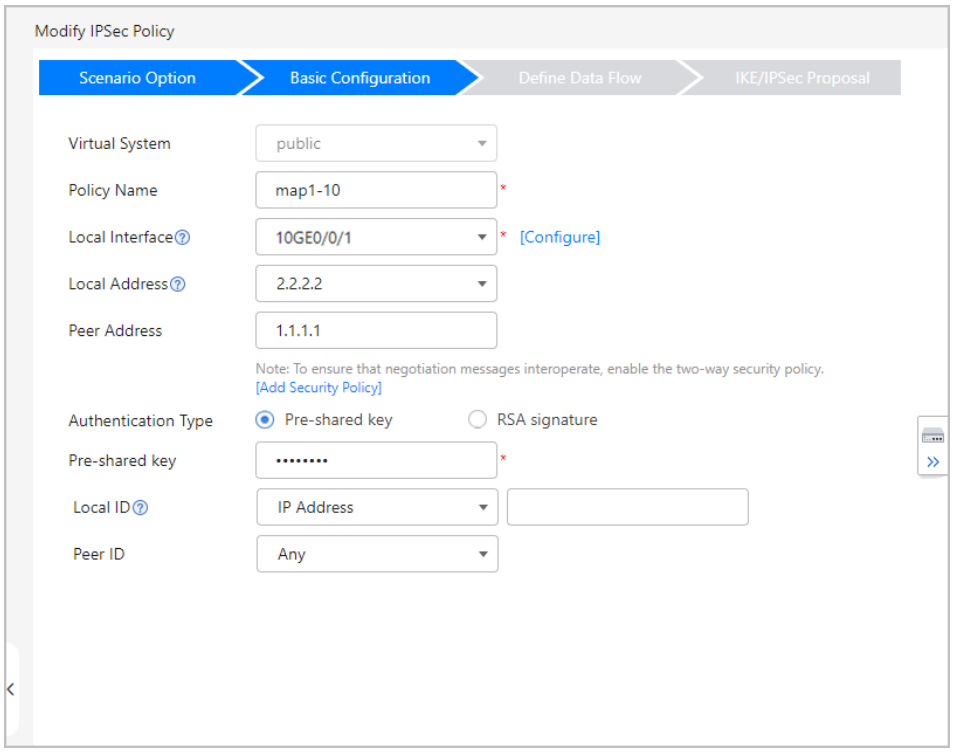


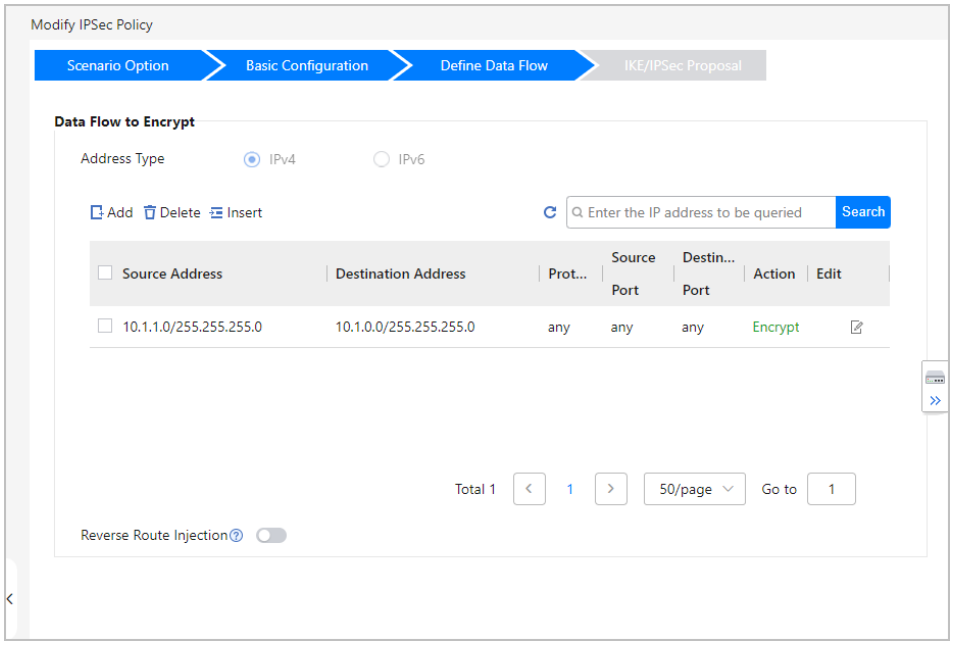
b. Click **Add** to create an IPsec policy as prompted.



The PSK is YsHsjx_202206.

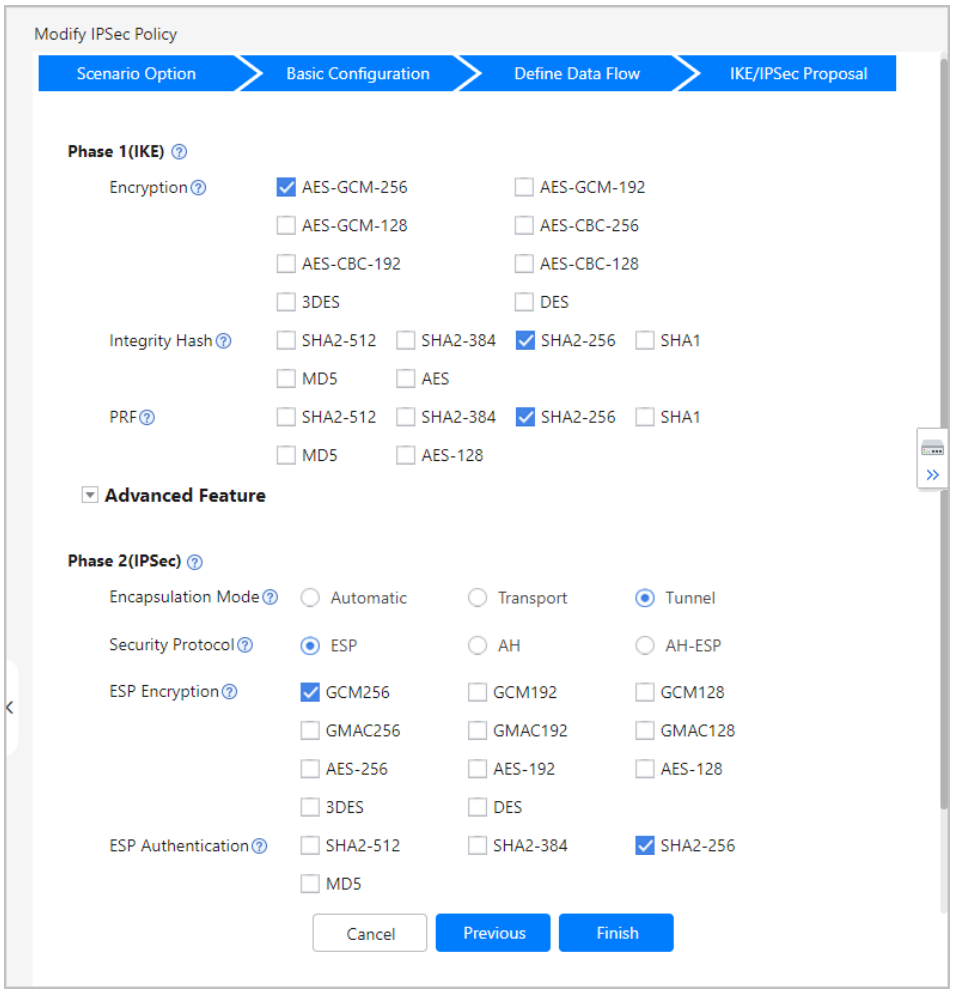
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

Step 3 Configure DeviceC.

Configure DeviceC by referring to the configurations of DeviceB.

----End

Verifying the Configuration

1. After the configuration is complete, ping the branches from the headquarters. The ping operations succeed.
2. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

Policy Name	Status	Local Address	Peer Address
map_temp-1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.1.1	2.2.2.2

 Copyright © Huawei Technologies Co., Ltd.

Policy Name	Status	Local Address	Peer Address
map_temp-1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.1.1	3.3.3.3

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
 ike-proposal 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
 tunnel local 1.1.1.1
#
ipsec policy map1 10 isakmp template map_temp
#
interface 10GE1/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface 10GE1/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface
#
firewall zone untrust
 set priority 5
 add interface
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone trust
 source-address 10.1.1.0 mask 255.255.255.0
 source-address 10.1.2.0 mask 255.255.255.0
 destination-address 10.1.0.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone untrust
 destination-zone local
 source-address 2.2.2.2 mask 255.255.255.255
 source-address 3.3.3.3 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
 tunnel local 2.2.2.2
#
interface
 ip address 10.1.1.1 255.255.255.0
#
interface
 ip address 2.2.2.2 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface
#
firewall zone untrust
 set priority 5
 add interface
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-zone trust
 source-address 10.1.0.0 mask 255.255.255.0
 destination-address 10.1.1.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 2.2.2.2 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.1.1 mask 255.255.255.255
 destination-address 2.2.2.2 mask 255.255.255.255
 action permit
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
 tunnel local 3.3.3.3
#
interface
 ip address 10.1.2.1 255.255.255.0
#
interface
 ip address 3.3.3.3 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface
#
firewall zone untrust
 set priority 5
 add interface
#
 ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
#
security-policy
 rule name policy1
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone untrust
 source-address 10.1.2.0 mask 255.255.255.0
 destination-address 10.1.0.0 mask 255.255.255.0
 action permit
rule name policy2
 source-zone untrust
 destination-zone trust
 source-address 10.1.0.0 mask 255.255.255.0
 destination-address 10.1.2.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 3.3.3.3 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.1.1 mask 255.255.255.255
 destination-address 3.3.3.3 mask 255.255.255.255
 action permit
#
return
```

8.1.6 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use the Same PSK for Authentication)

Networking Requirements

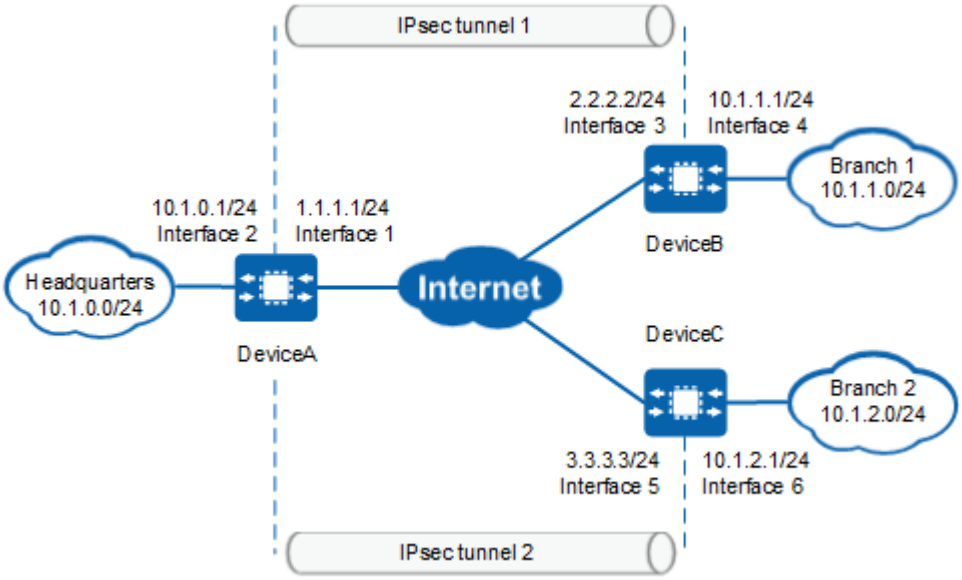
In **Figure 8-6**, the headquarters and two branches (branch1 and branch 2) connect to the Internet through DeviceA, DeviceB, and DeviceC respectively. There are reachable routes between DeviceA and DeviceB, and between DeviceA and DeviceC. An IPsec tunnel needs to be established between DeviceA and DeviceB and between DeviceA and DeviceC through public network interfaces. The same PSK is used for identity authentication to ensure secure transmission of data flows on specific network segments between the headquarters and two branches.

Figure 8-6 Establishing an IPsec tunnel using an IPsec policy template (branches use the same PSK for authentication)

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 on DeviceA, interface 3 and interface 4 represent GE 0/0/1 and GE 0/0/2 on DeviceB, and interface 5 and interface 6 represent GE 0/0/1 and GE 0/0/2 on DeviceC.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data
DeviceA	Interface number: GE 0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface number: GE 0/0/2 IP address: 10.1.0.1/24 Security zone: Trust
	IPsec configuration Remote IP address: IP address of the public network interface used by DeviceB and DeviceC to establish an IPsec tunnel Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceB	Interface number: GE 0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust
	Interface number: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote IP address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceC	Interface number: GE 0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust
	Interface number: GE 0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	IPsec configuration Remote IP address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA, DeviceB, and DeviceC must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
3. Configure static routes to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
4. Configure IPsec policies and apply an IPsec policy group to an interface. Template IPsec policies need to be configured on DeviceA at the headquarters, and ISAKMP IPsec policies need to be configured on DeviceB and DeviceC in the branches.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the trusted and untrusted zones to permit data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure a security policy between the local and untrusted zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone untrust
[DeviceA-policy-security-rule-policy3] destination-zone local
[DeviceA-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a default static route on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 4 Configure template IPsec policies on DeviceA and apply an IPsec policy group to GE 0/0/1.

1. Configure an IPsec proposal.

   ```
   [DeviceA] ipsec proposal tran1
   [DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceA-ipsec-proposal-tran1] quit
   ```

2. Configure an IKE proposal.

   ```
   [DeviceA] ike proposal 10
   [DeviceA-ike-proposal-10] authentication-method pre-share
   [DeviceA-ike-proposal-10] prf hmac-sha2-256
   [DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceA-ike-proposal-10] dh group14
   [DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceA-ike-proposal-10] quit
   ```

3. Configure an IKE peer.

   ```
   [DeviceA] ike peer b
   [DeviceA-ike-peer-b] ike-proposal 10
   [DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
   [DeviceA-ike-peer-b] quit
   ```

4. Configure an IPsec policy template **map_temp**.

   ```
   [DeviceA] ipsec policy-template map_temp 1
   [DeviceA-ipsec-policy-templet-map_temp-1] proposal tran1
   [DeviceA-ipsec-policy-templet-map_temp-1] ike-peer b
   [DeviceA-ipsec-policy-templet-map_temp-1] quit
   ```

5. Reference the IPsec policy template **map_temp** in the IPsec policy numbered 10 in the IPsec policy group **map1**.

   ```
   [DeviceA] ipsec policy map1 10 isakmp template map_temp
   ```

6. Apply an IPsec policy group to GE 0/0/1.

   ```
   [DeviceA] interface ge 0/0/1
   [DeviceA-GE0/0/1] ipsec policy map1
   [DeviceA-GE0/0/1] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.1.1 24
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 6 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the trusted and untrusted zones to permit data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure a security policy between the local and untrusted zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policy between the local and untrusted zones ensures that IKE negotiation packets can pass through DeviceB. This policy can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 7 Configure a default static route on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.254.

```
[DeviceB] ip route-static 0.0.0.0 0.0.0.0 2.2.2.254
```

Step 8 Configure ISAKMP IPsec policies on DeviceB and apply an IPsec policy group to GE 0/0/1.

1. Create an advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.0.0/24.

   ```
   [DeviceB] acl 3000
   [DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
   [DeviceB-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceB-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method pre-share
   [DeviceB-ike-proposal-10] prf hmac-sha2-256
   [DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceB-ike-proposal-10] dh group14
   [DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceB-ike-proposal-10] quit
   ```

4. Configure an IKE peer.

   ```
   [DeviceB] ike peer a
   [DeviceB-ike-peer-a] ike-proposal 10
   [DeviceB-ike-peer-a] remote-address 1.1.1.1
   [DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
   [DeviceB-ike-peer-a] quit
   ```

5. Configure an IPsec policy.

   ```
   [DeviceB] ipsec policy map1 10 isakmp
   [DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
   [DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
   [DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
   [DeviceB-ipsec-policy-isakmp-map1-10] quit
   ```

6. Apply an IPsec policy group to GE 0/0/1.

   ```
   [DeviceB] interface ge 0/0/1
   [DeviceB-GE0/0/1] ipsec policy map1
   [DeviceB-GE0/0/1] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

Step 9 Configure public and private network interfaces on DeviceC, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] undo portswitch
[DeviceC-GE0/0/1] ip address 3.3.3.3 24
[DeviceC-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceC] interface ge 0/0/2
[DeviceC-GE0/0/2] undo portswitch
[DeviceC-GE0/0/2] ip address 10.1.2.1 24
[DeviceC-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
```

Step 10 Configure security policies on DeviceC to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the trusted and untrusted zones to permit data flows to be encrypted.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy1
[DeviceC-policy-security-rule-policy1] source-zone trust
[DeviceC-policy-security-rule-policy1] destination-zone untrust
[DeviceC-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceC-policy-security-rule-policy1] action permit
[DeviceC-policy-security-rule-policy1] quit
[DeviceC-policy-security] rule name policy2
[DeviceC-policy-security-rule-policy2] source-zone untrust
[DeviceC-policy-security-rule-policy2] destination-zone trust
[DeviceC-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceC-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy2] action permit
[DeviceC-policy-security-rule-policy2] quit
```

Configure a security policy between the local and untrusted zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policy between the local and untrusted zones ensures that IKE negotiation packets can pass through DeviceC. This policy can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceC-policy-security] rule name policy3
[DeviceC-policy-security-rule-policy3] source-zone local
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-policy-security-rule-policy3] destination-zone untrust
[DeviceC-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceC-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceC-policy-security-rule-policy3] action permit
[DeviceC-policy-security-rule-policy3] quit
[DeviceC-policy-security] quit
[DeviceC-policy-security] rule name policy4
[DeviceC-policy-security-rule-policy4] source-zone untrust
[DeviceC-policy-security-rule-policy4] destination-zone local
[DeviceC-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceC-policy-security-rule-policy4] destination-address 3.3.3.3 32
[DeviceC-policy-security-rule-policy4] action permit
[DeviceC-policy-security-rule-policy4] quit
[DeviceC-policy-security] quit
```

Step 11 Configure a default static route on DeviceC to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceC to the Internet is 3.3.3.254.

```
[DeviceC] ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
```

Step 12 Configure ISAKMP IPsec policies on DeviceC and apply an IPsec policy group to GE 0/0/1.

1. Create an advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.2.0/24 to access the network segment 10.1.0.0/24.

   ```
   [DeviceC] acl 3000
   [DeviceC-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
   [DeviceC-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceC] ipsec proposal tran1
   [DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceC-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceC] ike proposal 10
   [DeviceC-ike-proposal-10] authentication-method pre-share
   [DeviceC-ike-proposal-10] prf hmac-sha2-256
   [DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceC-ike-proposal-10] dh group14
   [DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceC-ike-proposal-10] quit
   ```

4. Configure an IKE peer.

   ```
   [DeviceC] ike peer a
   [DeviceC-ike-peer-a] ike-proposal 10
   [DeviceC-ike-peer-a] remote-address 1.1.1.1
   [DeviceC-ike-peer-a] pre-shared-key YsHsjx_202206
   [DeviceC-ike-peer-a] quit
   ```

5. Configure an IPsec policy.

   ```
   [DeviceC] ipsec policy map1 10 isakmp
   [DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
   [DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
   [DeviceC-ipsec-policy-isakmp-map1-10] ike-peer a
   [DeviceC-ipsec-policy-isakmp-map1-10] quit
   ```

6. Apply an IPsec policy group to GE 0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ipsec policy map1
[DeviceC-GE0/0/1] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on the devices in the protected network segments of branches 1 and 2 to trigger IKE negotiation.

   If IKE negotiation succeeds, devices in the protected network segments at both ends of the IPsec tunnel can ping each other successfully. Otherwise, IKE negotiation fails.

2. View IKE SAs and IPsec SAs on DeviceA at the headquarters. The following command output indicates that two pairs of IKE SAs and IPsec SAs have been established.

```
<DeviceA> display ike sa
Total number of IKE SA in all CPU : 4
Total number of phase 1 SA in all CPU :
2
Total number of phase 2 SA in all CPU : 2

Flag Description: RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 4,  number of IKE SA1: 2,  number of IKE SA2: 2
-------------------------------------------------------------------------------
  Conn-ID    Peer           VPN     Flag(s)      Phase   RemoteType  RemoteID
-------------------------------------------------------------------------------
  83886142   2.2.2.2/500            RD|A         v2:2    IP          2.2.2.2
  83886137   2.2.2.2/500            RD|A         v2:1    IP          2.2.2.2
  134217773  3.3.3.3/500            RD|A         v2:2    IP          3.3.3.3
  134217765  3.3.3.3/500            RD|A         v2:1    IP          3.3.3.3
-------------------------------------------------------------------------------
<DeviceA> display ipsec sa brief
Slot 0, cpu 0 IPSec SA information:
  Src address   Dst address     SPI      VPN  Protocol     Algorithm
-------------------------------------------------------------------------------
    1.1.1.1       2.2.2.2     16423687          ESP       E:AES-256-GCM-128
    2.2.2.2       1.1.1.1     274624861         ESP       E:AES-256-GCM-128
    1.1.1.1       3.3.3.3     7787885           ESP       E:AES-256-GCM-128
    3.3.3.3       1.1.1.1     15539132          ESP       E:AES-256-GCM-128
Number of IPSec SA : 4
-------------------------------------------------------------------------------
Total number of IPSec SA in all CPU : 4
```

3. View IKE SAs and IPsec SAs on DeviceB and DeviceC in the branches. The following example uses the command output on DeviceB, which indicates that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU :
1
Total number of phase 2 SA in all CPU : 1

Flag Description: RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Conn-ID    Peer           VPN     Flag(s)      Phase   RemoteType  RemoteID
-------------------------------------------------------------------------------
  16782416   1.1.1.1/500            RD|ST|A      v2:2    IP          1.1.1.1
  16782415   1.1.1.1/500            RD|ST|A      v2:1    IP          1.1.1.1
-------------------------------------------------------------------------------
<DeviceB> display ipsec sa brief
Slot 0, cpu 0 IPSec SA information:
  Src address   Dst address     SPI      VPN  Protocol     Algorithm
-------------------------------------------------------------------------------
    1.1.1.1       2.2.2.2    16423687          ESP       E:AES-256-GCM-128
    2.2.2.2       1.1.1.1    274624861         ESP       E:AES-256-GCM-128
Number of IPSec SA : 2
-------------------------------------------------------------------------------
Total number of IPSec SA in all CPU : 2
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
 ike-proposal 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
#
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-zone trust
 source-address 10.1.1.0 mask 255.255.255.0
 source-address 10.1.2.0 mask 255.255.255.0
 destination-address 10.1.0.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone untrust
 destination-zone local
 source-address 2.2.2.2 mask 255.255.255.255
 source-address 3.3.3.3 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-zone trust
 source-address 10.1.0.0 mask 255.255.255.0
 destination-address 10.1.1.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 2.2.2.2 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.1.1 mask 255.255.255.255
 destination-address 2.2.2.2 mask 255.255.255.255
 action permit
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-address 10.1.2.0 mask 255.255.255.0
 destination-address 10.1.0.0 mask 255.255.255.0
 action permit
rule name policy2
 source-zone untrust
 destination-zone trust
 source-address 10.1.0.0 mask 255.255.255.0
 destination-address 10.1.2.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 3.3.3.3 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.1.1 mask 255.255.255.255
 destination-address 3.3.3.3 mask 255.255.255.255
 action permit
#
return
```

8.1.7 Web: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use Different PSKs for Authentication)

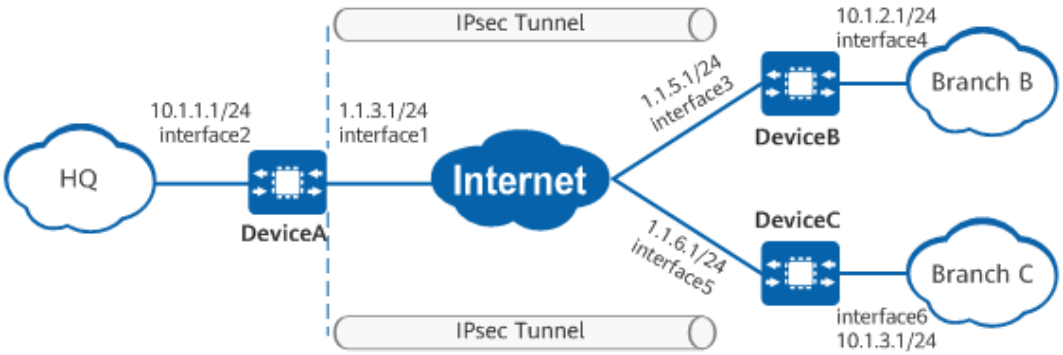
Networking Requirements

As shown in **Figure 8-7**, an enterprise has a headquarters and multiple branches. DeviceA is the egress gateway of the headquarters, and DeviceB and DeviceC are the egress gateways of the branches. The IP address of DeviceA is fixed. The networking must meet the following requirements: IPsec tunnels need to be established between the headquarters and multiple branches to implement secure communication between them. Different branches use different PSKs for identity authentication.

Figure 8-7 Establishing IPsec tunnels using an IPsec policy template (branches use different PSKs for authentication)

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively; interface 5 and interface 6 represent GE0/0/1 and GE0/0/2 of DeviceC, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	DeviceA	DeviceB	DeviceC
Interface configuration	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust Interface number: GE0/0/2 IP address: 10.1.0.1/24 Security zone: Trust	Interface number: GE0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust	Interface number: GE0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
IPsec configuration	Scenario: point-to-multipoint Remote address: not configured Authentication mode: PSK authentication PSKs: YsHsjx_202206, Admin@456 Local ID: IP address Remote ID: Any	Scenario: point-to-point Remote address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: Any	Scenario: point-to-point Remote address: 1.1.1.1 Authentication mode: PSK authentication PSK: Admin@456 Local ID: IP address Remote ID: Any

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB and DeviceC.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes between the headquarters and branches.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

   Note that you do not need to set the remote IP address when configuring DeviceA, because the remote IP address is not fixed. When configuring DeviceB and DeviceC, you need to set the peer IP address.

   Configure an IKE user table on DeviceA to configure different PSKs for different branches.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.0.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.0.0/24
Destination Address	10.1.1.0/24 10.1.2.0/24
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

 Copyright © Huawei Technologies Co., Ltd.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.1.0/24 10.1.2.0/24
Destination Address	10.1.0.0/24
Action	Permit

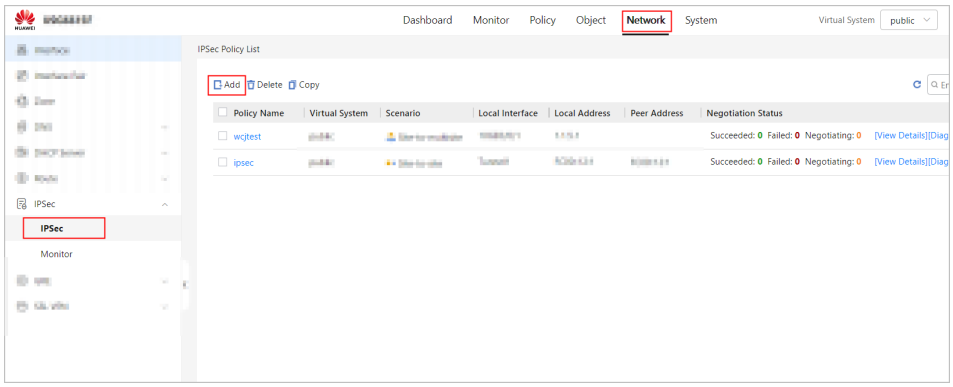
Name	policy3
Source Zone	untrust
Destination Zone	local
Source Address	2.2.2.2/32 3.3.3.3/32
Destination Address	1.1.1.1/32
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.1.254.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a route from DeviceA to the Internet as follows. Click **OK**.

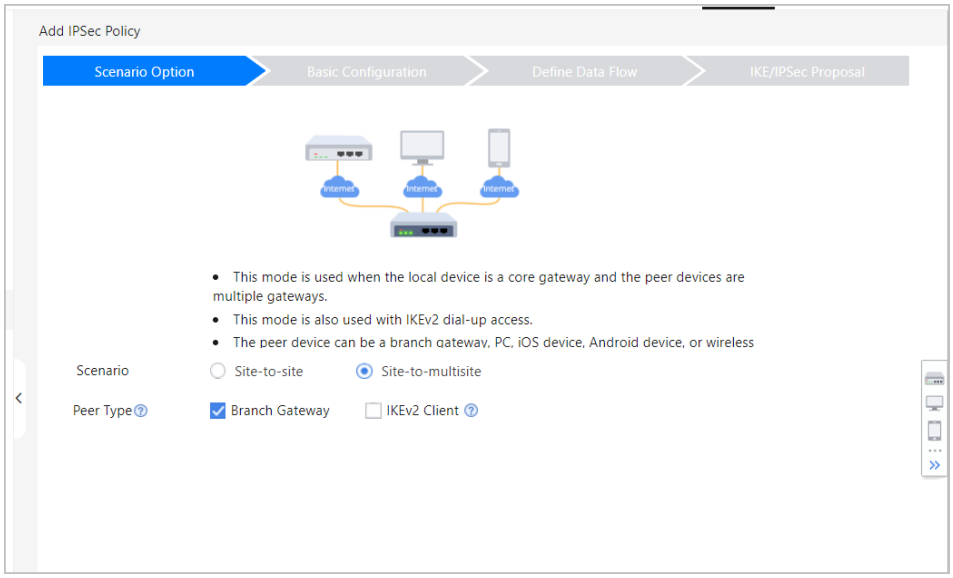
Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

 Copyright © Huawei Technologies Co., Ltd.

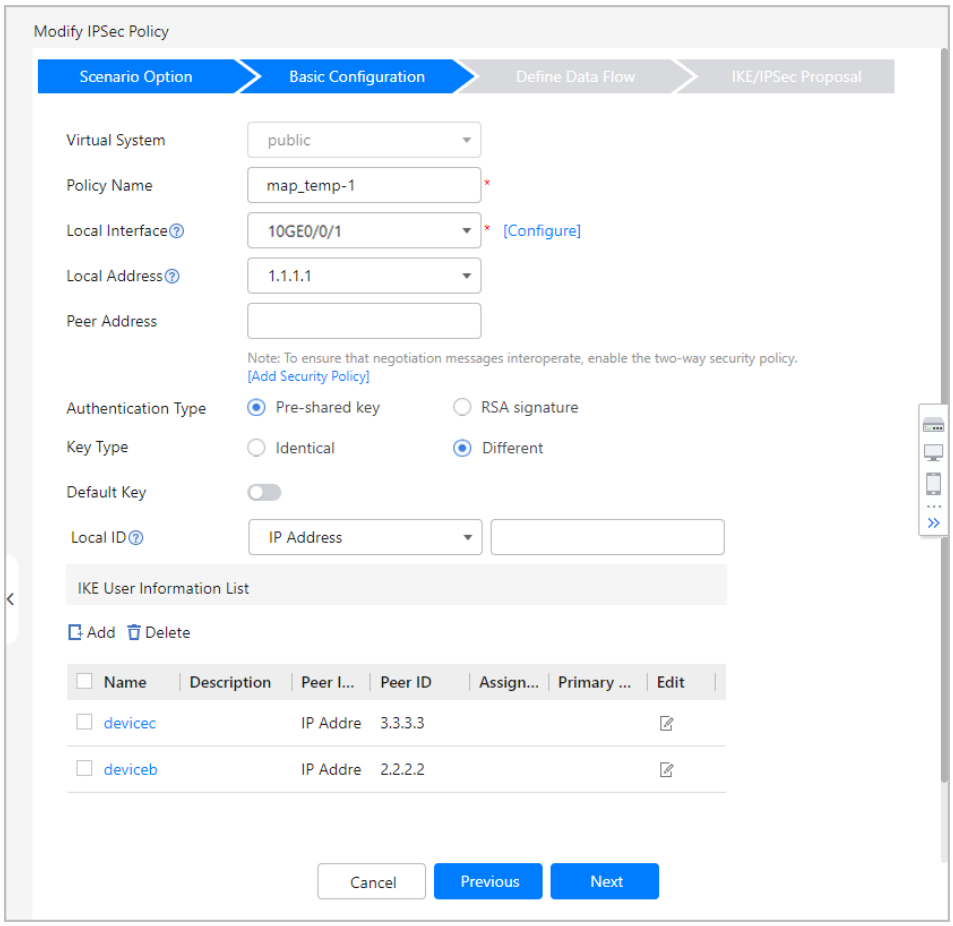


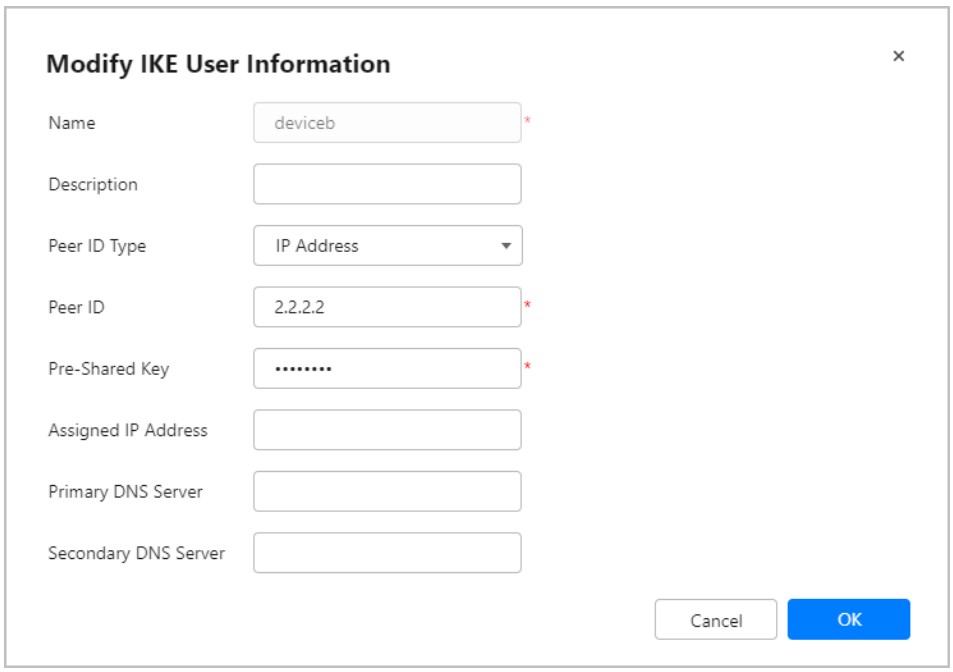
b. Click **Add** to create an IPsec policy as prompted.



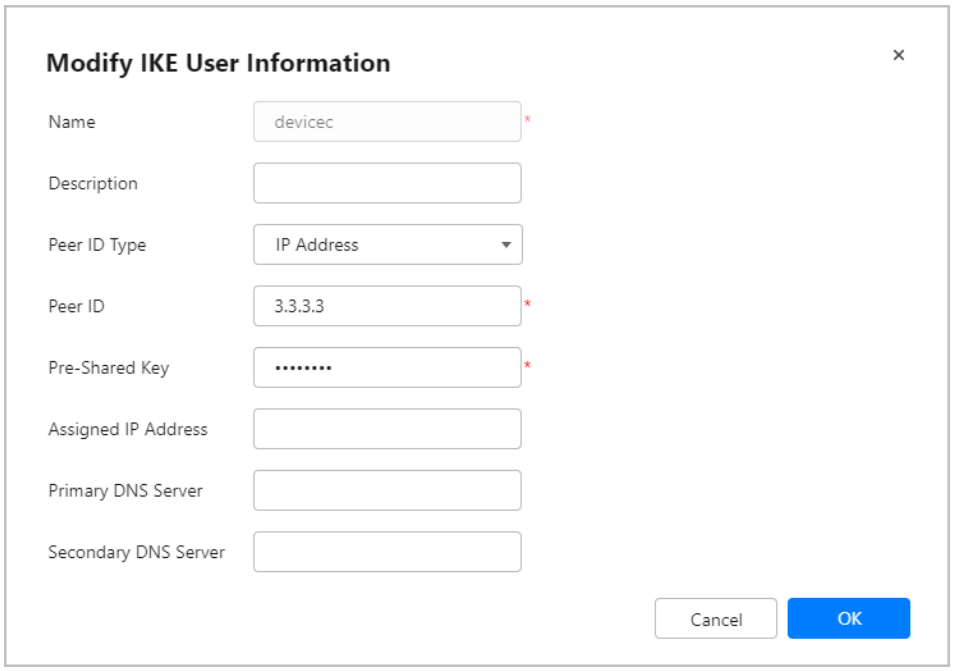
Click **Add** in **IKE User Information List** to create an IKE user. The PSK of deviceb is YsHsjx_202206 and that of devicec is Admin@456.

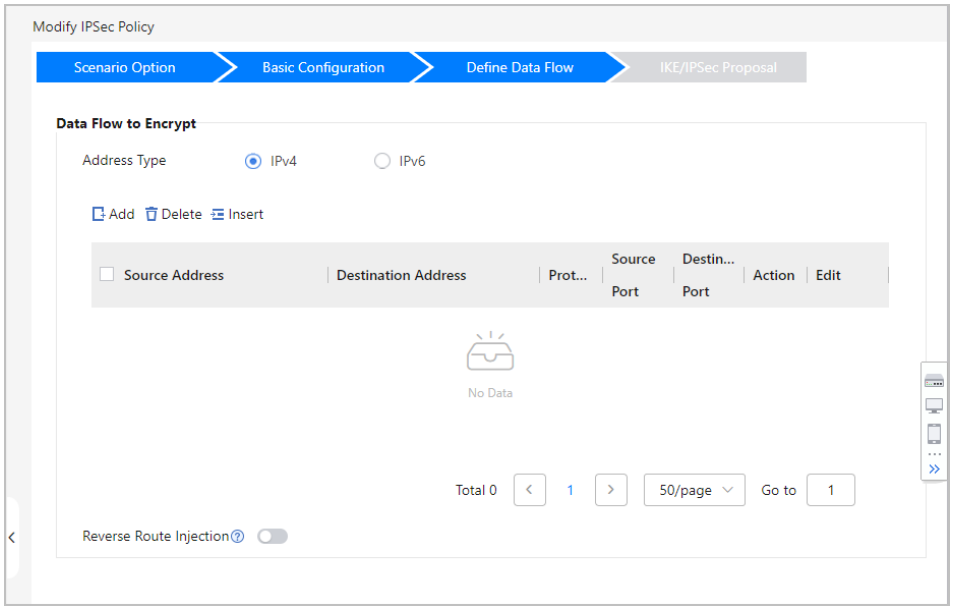
 Copyright © Huawei Technologies Co., Ltd.





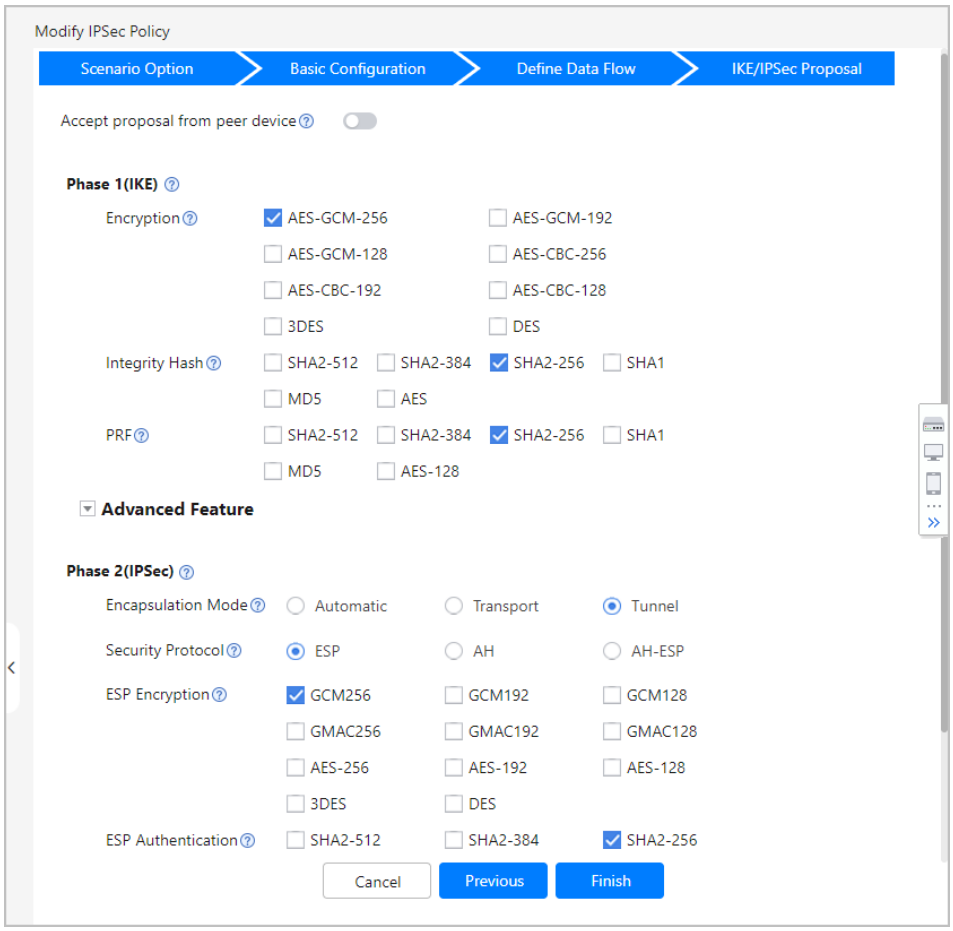
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

Step 2 Configure DeviceB.

1. Set interface IP addresses and add the interfaces to security zones.

   a. Choose **Network** > **Interface**.

   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.5.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Destination Address	10.1.0.0/24
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.0.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2.2.2.2/32
Destination Address	1.1.1.1/32
Action	Permit

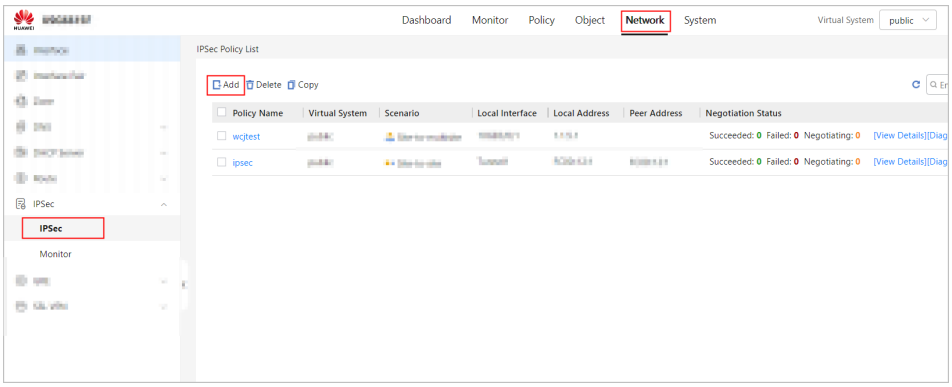
 Copyright © Huawei Technologies Co., Ltd.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.1.1/32
Destination Address	2.2.2.2/32
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.5.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a route from DeviceB to the Internet as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.5.2

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

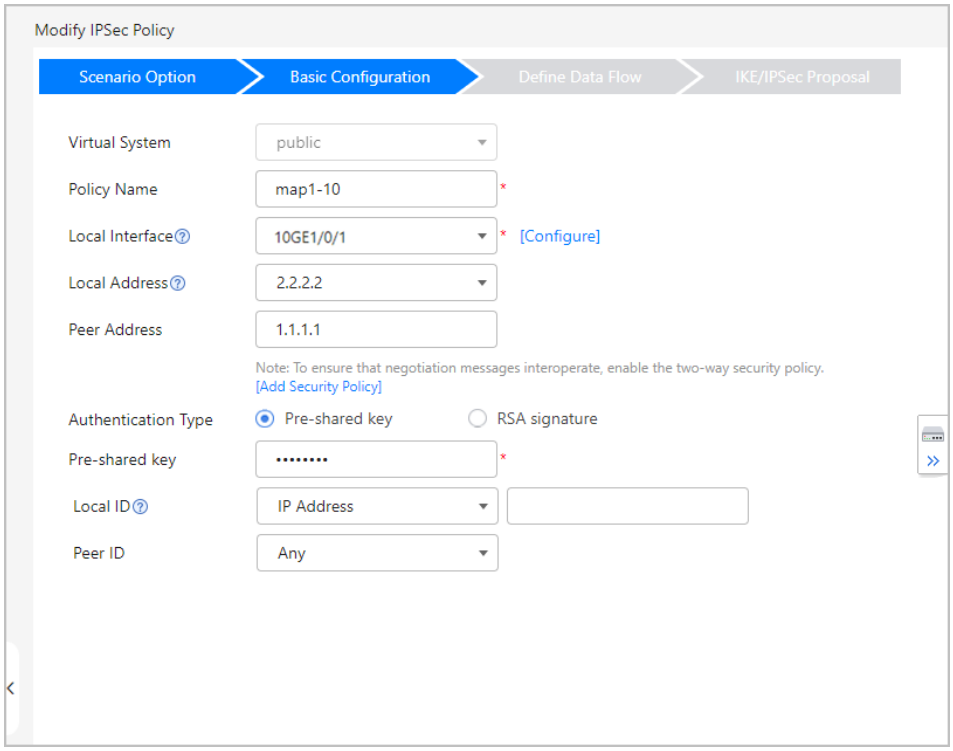


   b. Click **Add** to create an IPsec policy as prompted.

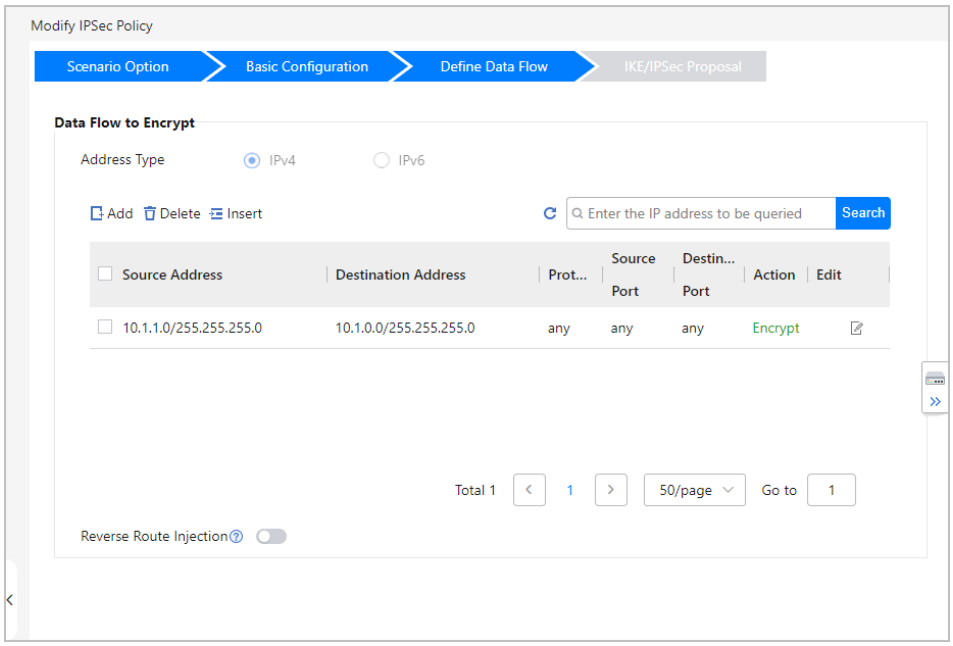
 Copyright © Huawei Technologies Co., Ltd.



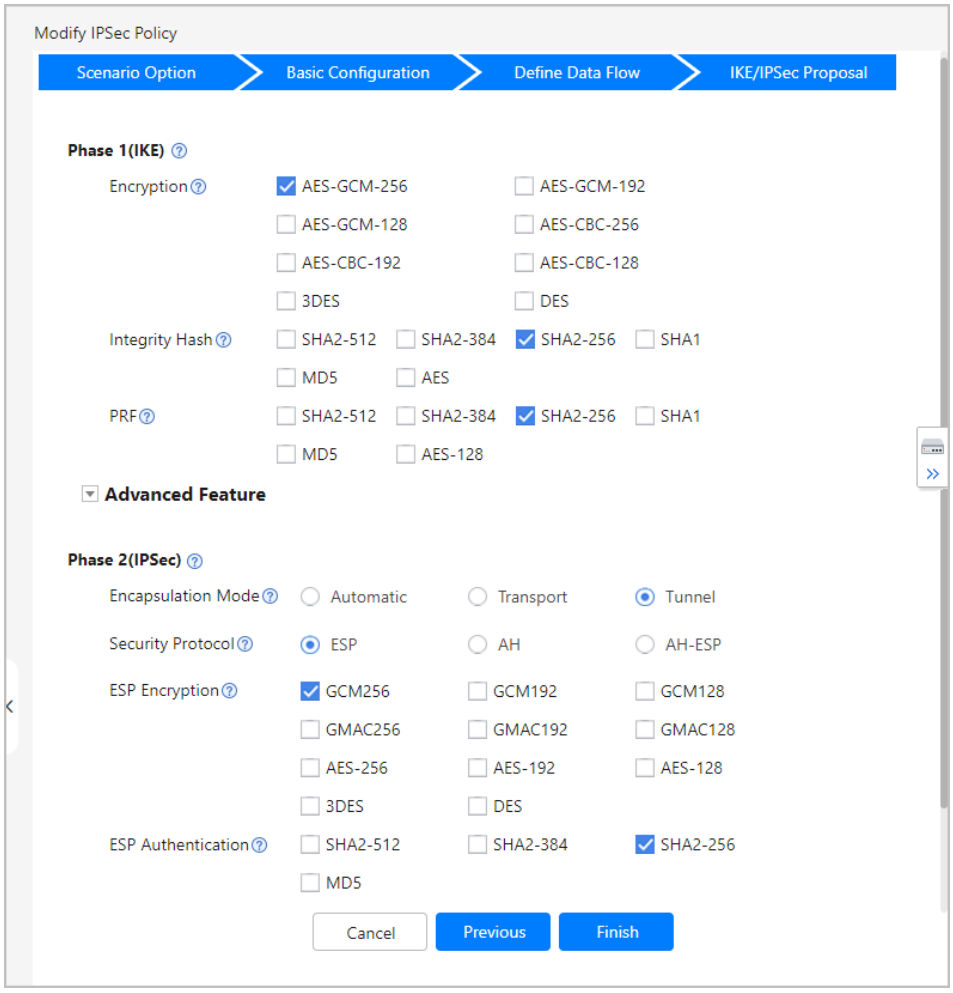
The PSK is YsHsjx_202206.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



 Copyright © Huawei Technologies Co., Ltd.

c. Click **Finish**.

Step 3 Configure DeviceC.

Configure DeviceC by referring to the configurations of DeviceB.

----End

Verifying the Configuration

1. After the configuration is complete, ping the branches from the headquarters. The ping operations succeed.
2. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

Policy Name	Status	Local Address	Peer Address
map_temp-1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.1.1	2.2.2.2
map_temp-1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.1.1	3.3.3.3

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike user-table 10
 user deviceb
  id-type ip 2.2.2.2
  pre-shared-key %+%#W)04NhZ:bP=~"=KQu\CN6KcK#NE5:(Os2L57]r5I%+%#
 user devicec
  id-type ip 3.3.3.3
  pre-shared-key %+%#Z"m.4U|TGN$'4c7~m'7FFo\A9q-smXqS8B"w;=w~%+%#
#
ike peer b
 ike-proposal 10
 user-table 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
```

 Copyright © Huawei Technologies Co., Ltd.

```
 tunnel local 1.1.1.1
#
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#W)04NhZ:bP=~"=KQu\CN6KcK#NE5:(Os2L57]r5I%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
```

 Copyright © Huawei Technologies Co., Ltd.

```
 security acl 3000
 ike-peer a
 proposal tran1
 tunnel local 2.2.2.2
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#Z"m.4U|TGN$'4c7~m'7FFo\A9q-smXqS8B"w;=w~%+%#
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
 tunnel local 3.3.3.3
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
#
return
```

8.1.8 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Policy Template (Branches Use Different PSKs for Authentication)

Networking Requirements

In **Figure 8-8**, the headquarters and two branches (branch1 and branch 2) connect to the Internet through DeviceA, DeviceB, and DeviceC respectively. There are reachable routes between DeviceA and DeviceB, and between DeviceA and DeviceC. An IPsec tunnel needs to be established between DeviceA and DeviceB and between DeviceA and DeviceC through public network interfaces. Different

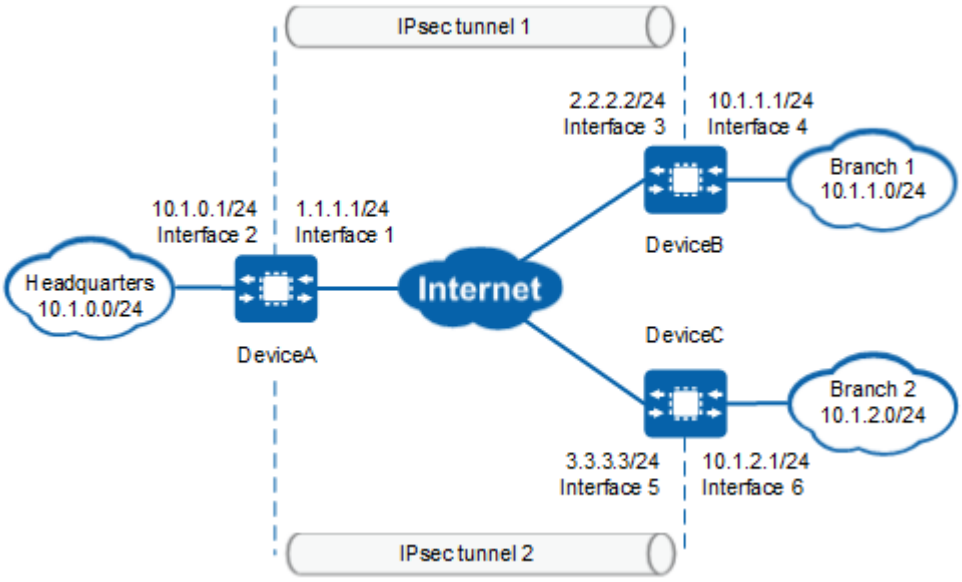
 Copyright © Huawei Technologies Co., Ltd.

pre-shared keys (PSKs) are used for identity authentication to ensure secure transmission of data flows on specific network segments between the headquarters and two branches.

Figure 8-8 Establishing IPsec tunnels using an IPsec policy template (branches use different PSKs for authentication)

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 on DeviceA, interface 3 and interface 4 represent GE 0/0/1 and GE 0/0/2 on DeviceB, and interface 5 and interface 6 represent GE 0/0/1 and GE 0/0/2 on DeviceC.



Item	Data
DeviceA	Interface number: GE 0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface number: GE 0/0/2 IP address: 10.1.0.1/24 Security zone: Trust
	IPsec configuration Remote IP address: IP address of the public network interface used by DeviceB and DeviceC to establish an IPsec tunnel Authentication mode: PSK authentication PSKs: YsHsjx_202206, Admin@456
DeviceB	Interface number: GE 0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	Interface number: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	IPsec configuration Remote IP address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceC	Interface number: GE 0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust
	Interface number: GE 0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	IPsec configuration Remote IP address: 1.1.1.1 Authentication mode: PSK authentication PSK: Admin@456 Local ID type: IP address Remote ID type: any

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA, DeviceB, and DeviceC must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
3. Configure static routes to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

4. Configure IPsec policies and apply an IPsec policy group to an interface. Template IPsec policies need to be configured on DeviceA at the headquarters, and ISAKMP IPsec policies need to be configured on DeviceB and DeviceC in the branches. The branches use different PSKs to access the headquarters. Therefore, you need to configure an IKE user table on DeviceA and configure different PSKs for different branches to initiate tunnel negotiation.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the trusted and untrusted zones to permit data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy between the local and untrusted zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone untrust
[DeviceA-policy-security-rule-policy3] destination-zone local
[DeviceA-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a default static route on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 4 Configure template IPsec policies on DeviceA and apply an IPsec policy group to GE 0/0/1.

1. Configure an IPsec proposal.

   ```
   [DeviceA] ipsec proposal tran1
   [DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceA-ipsec-proposal-tran1] quit
   ```

2. Configure an IKE proposal.

   ```
   [DeviceA] ike proposal 10
   [DeviceA-ike-proposal-10] authentication-method pre-share
   [DeviceA-ike-proposal-10] prf hmac-sha2-256
   [DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceA-ike-proposal-10] dh group14
   [DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceA-ike-proposal-10] quit
   ```

3. Configure an IKE user table and configure different PSKs for different branches.

   NOTE

   When the IKEv1 main mode and PSK authentication are used, **id-type** can only be set to an IP address, and in NAT traversal scenarios, the IP address must be set to a post-NAT address. If the branches dynamically obtain IP addresses, you must use the IKEv1 or IKEv2 aggressive mode and are advised to set **id-type** to an FQDN.

   ```
   [DeviceA] ike user-table 10
   [DeviceA-ike-user-table-10] user deviceb
   [DeviceA-ike-user-table-10-deviceb] id-type ip 2.2.2.2
   [DeviceA-ike-user-table-10-deviceb] pre-shared-key YsHsjx_202206
   [DeviceA-ike-user-table-10-deviceb] quit
   [DeviceA-ike-user-table-10] user devicec
   [DeviceA-ike-user-table-10-devicec] id-type ip 3.3.3.3
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-ike-user-table-10-devicec] pre-shared-key Admin@456
[DeviceA-ike-user-table-10-devicec] quit
```

4. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] user-table 10
[DeviceA-ike-peer-b] quit
```

5. Configure an IPsec policy template **map_temp**.

```
[DeviceA] ipsec policy-template map_temp 1
[DeviceA-ipsec-policy-templet-map_temp-1] proposal tran1
[DeviceA-ipsec-policy-templet-map_temp-1] ike-peer b
[DeviceA-ipsec-policy-templet-map_temp-1] quit
```

6. Reference the IPsec policy template **map_temp** in the IPsec policy numbered 10 in the IPsec policy group **map1**.

```
[DeviceA] ipsec policy map1 10 isakmp template map_temp
```

7. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
```

Step 5 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.1.1 24
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 6 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the trusted and untrusted zones to permit data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure a security policy between the local and untrusted zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policy between the local and untrusted zones ensures that IKE negotiation packets can pass through DeviceB. This policy can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 7 Configure a default static route on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.254.

```
[DeviceB] ip route-static 0.0.0.0 0.0.0.0 2.2.2.254
```

Step 8 Configure ISAKMP IPsec policies on DeviceB and apply an IPsec policy group to GE 0/0/1.

1. Create an advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.0.0/24.

   ```
   [DeviceB] acl 3000
   [DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
   [DeviceB-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceB-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method pre-share
   [DeviceB-ike-proposal-10] prf hmac-sha2-256
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] remote-address 1.1.1.1
[DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-a] quit
```

5. Configure an IPsec policy.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

Step 9 Configure public and private network interfaces on DeviceC, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] undo portswitch
[DeviceC-GE0/0/1] ip address 3.3.3.3 24
[DeviceC-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceC] interface ge 0/0/2
[DeviceC-GE0/0/2] undo portswitch
[DeviceC-GE0/0/2] ip address 10.1.2.1 24
[DeviceC-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
```

Step 10 Configure security policies on DeviceC to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the trusted and untrusted zones to permit data flows to be encrypted.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy1
[DeviceC-policy-security-rule-policy1] source-zone trust
[DeviceC-policy-security-rule-policy1] destination-zone untrust
[DeviceC-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceC-policy-security-rule-policy1] action permit
[DeviceC-policy-security-rule-policy1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-policy-security] rule name policy2
[DeviceC-policy-security-rule-policy2] source-zone untrust
[DeviceC-policy-security-rule-policy2] destination-zone trust
[DeviceC-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceC-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy2] action permit
[DeviceC-policy-security-rule-policy2] quit
```

Configure a security policy between the local and untrusted zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policy between the local and untrusted zones ensures that IKE negotiation packets can pass through DeviceC. This policy can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceC-policy-security] rule name policy3
[DeviceC-policy-security-rule-policy3] source-zone local
[DeviceC-policy-security-rule-policy3] destination-zone untrust
[DeviceC-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceC-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceC-policy-security-rule-policy3] action permit
[DeviceC-policy-security-rule-policy3] quit
[DeviceC-policy-security] rule name policy4
[DeviceC-policy-security-rule-policy4] source-zone untrust
[DeviceC-policy-security-rule-policy4] destination-zone local
[DeviceC-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceC-policy-security-rule-policy4] destination-address 3.3.3.3 32
[DeviceC-policy-security-rule-policy4] action permit
[DeviceC-policy-security-rule-policy4] quit
[DeviceC-policy-security] quit
```

Step 11 Configure a default static route on DeviceC to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceC to the Internet is 3.3.3.254.

```
[DeviceC] ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
```

Step 12 Configure ISAKMP IPsec policies on DeviceC and apply an IPsec policy group to GE 0/0/1.

1. Create an advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.2.0/24 to access the network segment 10.1.0.0/24.

   ```
   [DeviceC] acl 3000
   [DeviceC-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
   [DeviceC-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceC] ipsec proposal tran1
   [DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceC-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceC] ike proposal 10
   [DeviceC-ike-proposal-10] authentication-method pre-share
   [DeviceC-ike-proposal-10] prf hmac-sha2-256
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceC-ike-proposal-10] dh group14
[DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceC-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceC] ike peer a
[DeviceC-ike-peer-a] ike-proposal 10
[DeviceC-ike-peer-a] remote-address 1.1.1.1
[DeviceC-ike-peer-a] pre-shared-key Admin@456
[DeviceC-ike-peer-a] quit
```

5. Configure an IPsec policy.

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ipsec policy map1
[DeviceC-GE0/0/1] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on the devices in the protected network segments of branches 1 and 2 to trigger IKE negotiation.

   If IKE negotiation succeeds, devices in the protected network segments at both ends of the IPsec tunnel can ping each other successfully. Otherwise, IKE negotiation fails.

2. View IKE SAs and IPsec SAs on DeviceA at the headquarters. The following command output indicates that two pairs of IKE SAs and IPsec SAs have been established.

```
<DeviceA> display ike sa
Total number of IKE SA in all CPU : 4
Total number of phase 1 SA in all CPU :
2
Total number of phase 2 SA in all CPU : 2

Flag Description: RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 4,  number of IKE SA1: 2,  number of IKE SA2: 2
-------------------------------------------------------------------------------
  Conn-ID    Peer           VPN     Flag(s)      Phase   RemoteType  RemoteID
-------------------------------------------------------------------------------
  83886142   2.2.2.2/500            RD|A         v2:2    IP          2.2.2.2
  83886137   2.2.2.2/500            RD|A         v2:1    IP          2.2.2.2
  134217773  3.3.3.3/500            RD|A         v2:2    IP          3.3.3.3
  134217765  3.3.3.3/500            RD|A         v2:1    IP          3.3.3.3
-------------------------------------------------------------------------------
<DeviceA> display ipsec sa brief
Slot 0, cpu 0 IPSec SA information:
  Src address   Dst address     SPI      VPN  Protocol     Algorithm
-------------------------------------------------------------------------------
  1.1.1.1       2.2.2.2     16423687          ESP       E:AES-256-GCM-128
  2.2.2.2       1.1.1.1     274624861         ESP       E:AES-256-GCM-128
  1.1.1.1       3.3.3.3     7787885           ESP       E:AES-256-GCM-128
  3.3.3.3       1.1.1.1     15539132          ESP       E:AES-256-GCM-128
```

 Copyright © Huawei Technologies Co., Ltd.

```
Number of IPSec SA : 4
--------------------------------------------------------------------------------
Total number of IPSec SA in all CPU : 4
```

3. View IKE SAs and IPsec SAs on DeviceB and DeviceC in the branches. The following example uses the command output on DeviceB, which indicates that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU :
1
Total number of phase 2 SA in all CPU : 1

Flag Description: RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
--------------------------------------------------------------------------------
  Conn-ID    Peer           VPN     Flag(s)      Phase   RemoteType  RemoteID
--------------------------------------------------------------------------------
  16782416   1.1.1.1/500            RD|ST|A      v2:2    IP          1.1.1.1
  16782415   1.1.1.1/500            RD|ST|A      v2:1    IP          1.1.1.1
--------------------------------------------------------------------------------
<DeviceB> display ipsec sa brief
Slot 0, cpu 0 IPSec SA information:
  Src address   Dst address     SPI      VPN  Protocol     Algorithm
--------------------------------------------------------------------------------
    1.1.1.1       2.2.2.2     16423687          ESP       E:AES-256-GCM-128
    2.2.2.2       1.1.1.1     274624861         ESP       E:AES-256-GCM-128
Number of IPSec SA : 2
--------------------------------------------------------------------------------
Total number of IPSec SA in all CPU : 2
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike user-table 10
 user deviceb
  id-type ip 2.2.2.2
  pre-shared-key %+%#W)04NhZ:bP=~"=KQu\CN6KcK#NE5:(Os2L57]r5I%+%#
 user devicec
  id-type ip 3.3.3.3
  pre-shared-key %+%#Z"m.4U|TGN$'4c7~m'7FFo\A9q-smXqS8B"w;=w~%+%#
#
ike peer b
 ike-proposal 10
 user-table 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#W)04NhZ:bP=~"=KQu\CN6KcK#NE5:(Os2L57]r5I%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
```

 Copyright © Huawei Technologies Co., Ltd.

```
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#Z"m.4U|TGN$'4c7~m'7FFo\A9q-smXqS8B"w;=w~%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
#
return
```

8.1.9 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Profile (Through PSK Authentication)

Networking Requirements

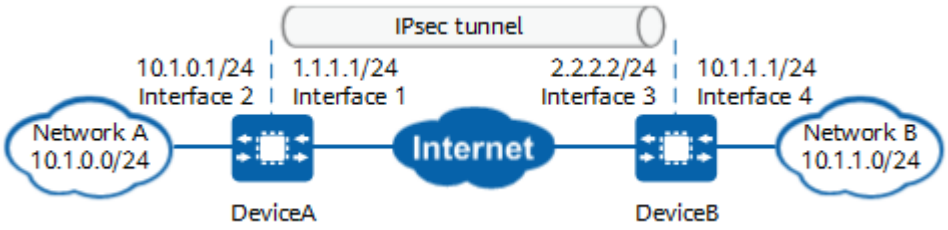
In **Figure 8-9**, networks A and B connect to the Internet through DeviceA and DeviceB respectively, and there are reachable routes between the two devices. The two devices need to establish an IPsec tunnel using an IPsec profile through tunnel interfaces. The two ends of the tunnel use PSK authentication to ensure secure transmission of data flows that are diverted to the tunnel through static routes.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-9 Establishing an IPsec tunnel using an IPsec profile (through PSK authentication)

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, and interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB.



Item	Data
DeviceA	Interface: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.1.0.1/24 Security zone: Trust
	Tunnel interface configuration Encapsulation protocol: IPsec Source IP address: 1.1.1.1 Destination IP address: 2.2.2.2 IP address of the interface: any IP address that is not in use
	IPsec profile configuration Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: IP address
DeviceB	Interface: GE0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	Tunnel interface configuration Encapsulation protocol: IPsec Source IP address: 2.2.2.2 Destination IP address: 1.1.1.1 IP address of the interface: any IP address that is not in use
	IPsec profile configuration Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: IP address

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
3. Configure a static route to divert tunnel negotiation packets.
4. Configure an IPsec tunnel interface, divert encrypted data packets to the tunnel interface through a static route, and apply an IPsec profile to the tunnel interface.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the Trust and Untrust zones to permit data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a static route to DeviceB to divert tunnel negotiation packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

```
[DeviceA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
```

Step 4 Configure an IPsec tunnel interface and add the interface to a security zone.

```
[DeviceA] interface Tunnel 1
[DeviceA-Tunnel1] tunnel-protocol ipsec
[DeviceA-Tunnel1] source 1.1.1.1
[DeviceA-Tunnel1] destination 2.2.2.2
[DeviceA-Tunnel1] ip address 172.16.0.1 24
[DeviceA-Tunnel1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface tunnel 1
[DeviceA-zone-untrust] quit
```

Step 5 Configure a static route to divert encrypted data packets to the tunnel interface.

```
[DeviceA] ip route-static 10.1.1.0 24 Tunnel 1
```

Step 6 Configure an IPsec profile.

1. Configure an IPsec proposal.

   ```
   [DeviceA] ipsec proposal tran1
   [DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceA-ipsec-proposal-tran1] quit
   ```

2. Configure an IKE proposal.

   ```
   [DeviceA] ike proposal 10
   [DeviceA-ike-proposal-10] authentication-method pre-share
   [DeviceA-ike-proposal-10] prf hmac-sha2-256
   [DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceA-ike-proposal-10] dh group14
   [DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceA-ike-proposal-10] quit
   ```

3. Configure an IKE peer.

   ```
   [DeviceA] ike peer b
   [DeviceA-ike-peer-b] ike-proposal 10
   [DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
   [DeviceA-ike-peer-b] quit
   ```

4. Configure an IPsec profile.

   ```
   [DeviceA] ipsec profile pro1
   [DeviceA-ipsec-profile-pro1] proposal tran1
   [DeviceA-ipsec-profile-pro1] ike-peer b
   [DeviceA-ipsec-profile-pro1] quit
   ```

Step 7 Apply the IPsec profile to the tunnel interface.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] ipsec profile pro1
[DeviceA-Tunnel1] quit
```

Step 8 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.1.1 24
[DeviceB-GE0/0/2] quit
```

Add GE0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 9 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the Trust and Untrust zones to permit data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 10 Configure a static route to DeviceA to divert tunnel negotiation packets.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.254.

```
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
```

Step 11 Configure an IPsec tunnel interface and add the interface to a security zone.

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] tunnel-protocol ipsec
[DeviceB-Tunnel1] source 2.2.2.2
[DeviceB-Tunnel1] destination 1.1.1.1
[DeviceB-Tunnel1] ip address 172.16.0.2 24
[DeviceB-Tunnel1] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface tunnel 1
[DeviceB-zone-untrust] quit
```

Step 12 Configure a static route to divert encrypted data packets to the tunnel interface.

```
[DeviceB] ip route-static 10.1.0.0 24 Tunnel1
```

Step 13 Configure an IPsec profile.

1. Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

2. Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

3. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-a] quit
```

4. Configure an IPsec profile.

```
[DeviceB] ipsec profile pro1
[DeviceB-ipsec-profile-pro1] proposal tran1
[DeviceB-ipsec-profile-pro1] ike-peer a
[DeviceB-ipsec-profile-pro1] quit
```

Step 14 Apply the IPsec profile to the tunnel interface.

```
[DeviceB] interface tunnel 1
[DeviceB-Tunnel1] ipsec profile pro1
[DeviceB-Tunnel1] quit
```

----End

Verifying the Configuration

On DeviceA and DeviceB, run the **display ike sa** and **display ipsec sa** commands to check SA establishment information. The following shows the command output of DeviceB for your reference. If the following information is displayed, IKE SAs and IPsec SAs have been successfully established.

```
<DeviceB> display ike sa
IKE SA information :
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Conn-ID     Peer           VPN   Flag(s)  Phase  RemoteType  RemoteID
 ------------------------------------------------------------------------------
  16777239    1.1.1.1:500          RD|ST|A  v2:2   IP          1.1.1.1
  16777232    1.1.1.1:500          RD|ST|A  v2:1   IP          1.1.1.1

 Number of IKE SA : 2
 ------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceB> display ipsec sa

ipsec sa information:

===============================
Interface: Tunnel1

===============================

 ------------------------------
 IPsec profile name: "pro1"
 Mode              : PROF-ISAKMP
 ------------------------------
  Connection ID     : 83903371
  Encapsulation mode: Tunnel
  Tunnel local      : 2.2.2.2
  Tunnel remote     : 1.1.1.1

  [Outbound ESP SAs]
    SPI: 763065754 (0x2d7b759a)
    Proposal: ESP-ENCRYPT-AES-256 SHA2-256-128
    SA remaining key duration (kilobytes/sec): 20971520/3551
    Max sent sequence-number: 1
    UDP encapsulation used for NAT traversal: N
    SA encrypted packets (number/kilobytes): 4/0

  [Inbound ESP SAs]
    SPI: 163241969 (0x9badff1)
    Proposal: ESP-ENCRYPT-AES-256 SHA2-256-128
    SA remaining key duration (kilobytes/sec): 20971520/3551
    Max received sequence-number: 1
    UDP encapsulation used for NAT traversal: N
    SA decrypted packets (number/kilobytes): 4/0
    Anti-replay : Disable
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
  pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
  ike-proposal 10
#
ipsec profile pro1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ike-peer b
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel 1
 ip address 172.16.0.1 255.255.255.0
 tunnel-protocol ipsec
 source 1.1.1.1
 destination 2.2.2.2
 ipsec profile pro1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel1
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
 ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
#
ipsec profile pro1
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
#
interface Tunnel 1
 ip address 172.16.0.2 255.255.255.0
 tunnel-protocol ipsec
 source 2.2.2.2
 destination 1.1.1.1
 ipsec profile pro1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel1
#
 ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
 ip route-static 10.1.0.0 255.255.255.0 Tunnel1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

8.1.10 CLI: Example for Establishing an IPsec Tunnel Using an IPsec Profile (Using Certificate Authentication)

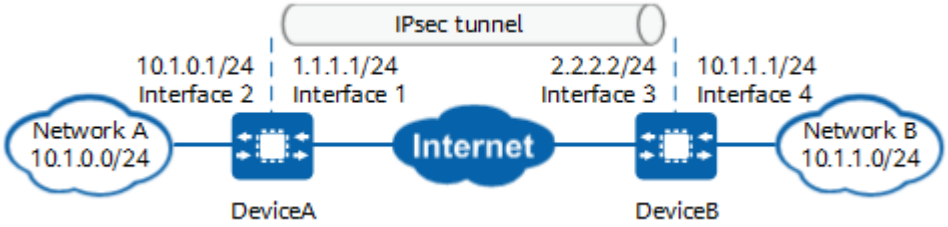
Networking Requirements

In Figure 8-10, networks A and B connect to the Internet through DeviceA and DeviceB respectively, and there are reachable routes between the two devices. The two devices need to establish an IPsec tunnel using an IPsec profile through tunnel interfaces. The two ends of the tunnel use RSA signature authentication to ensure secure transmission of data flows that are diverted to the tunnel through static routes.

Figure 8-10 Establishing an IPsec tunnel using an IPsec profile (using certificate authentication)

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, and interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB.



Item	Data
DeviceA	Interface: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.1.0.1/24 Security zone: Trust
	Tunnel interface configuration Encapsulation protocol: IPsec Source IP address: 1.1.1.1 Destination IP address: 2.2.2.2 IP address of the interface: any IP address that is not in use
	IPsec configuration Authentication mode: RSA signature authentication Local ID: IP address Remote ID: IP address

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
DeviceB	Interface: GE0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	Tunnel interface configuration Encapsulation protocol: IPsec Source IP address: 2.2.2.2 Destination IP address: 1.1.1.1 IP address of the interface: any IP address that is not in use
	IPsec configuration Authentication mode: RSA signature authentication Local ID: IP address Remote ID: IP address

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.
3. Configure a static route to divert tunnel negotiation packets.
4. Apply for the local certificate and CA certificate in offline mode and import the certificates to the devices.
5. Configure an IPsec tunnel interface, divert encrypted data packets to the tunnel interface through a static route, and apply an IPsec profile to the tunnel interface.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the Trust and Untrust zones to permit data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a static route to DeviceB to divert tunnel negotiation packets.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.2.

```
[DeviceA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
```

Step 4 Configure an IPsec tunnel interface and add the interface to a security zone.

```
[DeviceA] interface Tunnel 1
[DeviceA-Tunnel1] tunnel-protocol ipsec
[DeviceA-Tunnel1] source 1.1.1.1
[DeviceA-Tunnel1] destination 2.2.2.2
[DeviceA-Tunnel1] ip address 172.16.0.1 24
[DeviceA-Tunnel1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface tunnel 1
[DeviceA-zone-untrust] quit
```

Step 5 Configure a static route to divert encrypted data packets to the tunnel interface.

```
[DeviceA] ip route-static 10.1.1.0 24 Tunnel 1
```

Step 6 Apply for the local certificate and CA certificate in offline mode and import the certificates to the device.

1. Create a 3072-bit RSA key pair and allow it to be exported from the device.

   ```
   [DeviceA] pki rsa local-key-pair create rsakey_a exportable
   Info: The name of the new key-pair will be: rsakey_a
   The size of the public key ranges from 2048 to 4096.
   Input the bits in the modules:3072
   Generating key-pairs...
   Generating key-pairs finished
   ```

2. Configure a PKI entity to identify a certificate applicant.

   ```
   [DeviceA] pki entity user_a
   [DeviceA-pki-entity-user_a] common-name devicea
   [DeviceA-pki-entity-user_a] country cn
   [DeviceA-pki-entity-user_a] email testa@user.com
   [DeviceA-pki-entity-user_a] fqdn testa.abc.com
   [DeviceA-pki-entity-user_a] ip-address 1.1.1.1
   [DeviceA-pki-entity-user_a] state beijing
   [DeviceA-pki-entity-user_a] organization huawei
   [DeviceA-pki-entity-user_a] organization-unit dev
   [DeviceA-pki-entity-user_a] quit
   ```

3. Apply for a local certificate for the PKI entity in offline mode.

   # Create a PKI realm.

   ```
   [DeviceA] pki realm a
   [DeviceA-pki-realm-a] entity user_a
   [DeviceA-pki-realm-a] rsa local-key-pair rsakey_a
   [DeviceA-pki-realm-a] quit
   ```

   # Save certificate application information to a certificate request file in PKCS#10 format.

   ```
   [DeviceA] pki enroll-certificate realm a pkcs10 filename cer_req
   Info: Creating certificate request file...
   Info: Create certificate request file successfully.
   ```

 Copyright © Huawei Technologies Co., Ltd.

4. Download the certificate request file using a file transfer protocol, and send the file to the CA server in out-of-band mode, such as through the web system, using a disk, or through an email, to apply for a local certificate from the CA server.

   After a local certificate is successfully requested, download the local certificate **a_local.cer** and CA certificate **a_ca.cer** in out-of-band mode. Transfer the certificates to the device storage using a file transfer protocol.

5. Import the CA certificate into the device memory.

   After the certificate is imported, the **a_ca.cer** file is deleted from the storage medium by default. To keep it, select **N** as prompted.

```
[DeviceA] pki import-certificate ca filename a_ca.cer
 The CA's Subject is /CN=ca_root
 The CA's fingerprint is:
   MD5  fingerprint:1135 25D8 96D3 5936 C382 35EA 2CEE 80EB
   SHA1 fingerprint:6330 974F B2FE 3C52 D16B DAC4 0140 918B 4BCD 3EC7
 Is the fingerprint correct?(Y/N):y
 Info: Succeeded in importing the certificate.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select
[Y/N]:y
 Info: Delete Success.
```

6. Import the local certificate into the device memory.

   After the certificate is imported, the **a_local.cer** file is deleted from the storage medium by default. To keep it, select **N** as prompted.

```
[DeviceA] pki import-certificate local filename a_local.cer
 Info: Succeeded in importing file.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select
[Y/N]:y
 Info: Delete Success
```

Step 7 Configure an IPsec profile.

1. Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

2. Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method rsa-signature
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

3. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] certificate local-filename a_local.cer
[DeviceA-ike-peer-b] quit
```

4. Configure an IPsec profile.

```
[DeviceA] ipsec profile pro1
[DeviceA-ipsec-profile-pro1] proposal tran1
[DeviceA-ipsec-profile-pro1] ike-peer b
[DeviceA-ipsec-profile-pro1] quit
```

Step 8 Apply the IPsec profile to the tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] ipsec profile pro1
[DeviceA-Tunnel1] quit
```

Step 9 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.1.1 24
[DeviceB-GE0/0/2] quit
```

Add GE0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 10 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the Trust and Untrust zones to permit data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through DeviceB. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 11 Configure a static route to DeviceA to divert tunnel negotiation packets.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.3.

```
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 2.2.2.3
```

Step 12 Configure an IPsec tunnel interface and add the interface to a security zone.

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] tunnel-protocol ipsec
[DeviceB-Tunnel1] source 2.2.2.2
[DeviceB-Tunnel1] destination 1.1.1.1
[DeviceB-Tunnel1] ip address 172.16.0.2 24
[DeviceB-Tunnel1] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface tunnel 1
[DeviceB-zone-untrust] quit
```

Step 13 Configure a static route to divert encrypted data packets to the tunnel interface.

```
[DeviceB] ip route-static 10.1.0.0 24 Tunnel1
```

Step 14 Apply for the local certificate and CA certificate in offline mode and import the certificates to the device.

1. Create a 3072-bit RSA key pair and allow it to be exported from the device.

```
[DeviceB] pki rsa local-key-pair create rsakey_b exportable
 Info: The name of the new key-pair will be: rsakey_b
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:3072
 Generating key-pairs...
 Generating key-pairs finished
```

2. Configure a PKI entity to identify a certificate applicant.

```
[DeviceB] pki entity user_b
[DeviceB-pki-entity-user_a] common-name deviceb
[DeviceB-pki-entity-user_a] country cn
[DeviceB-pki-entity-user_a] email testb@user.com
[DeviceB-pki-entity-user_a] fqdn testb.abc.com
[DeviceB-pki-entity-user_a] ip-address 1.1.1.1
[DeviceB-pki-entity-user_a] state beijing
[DeviceB-pki-entity-user_a] organization huawei
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-pki-entity-user_a] organization-unit dev
[DeviceB-pki-entity-user_a] quit
```

3. Apply for a local certificate for the PKI entity in offline mode.

   # Create a PKI realm.

   ```
   [DeviceB] pki realm b
   [DeviceB-pki-realm-b] entity user_b
   [DeviceB-pki-realm-b] rsa local-key-pair rsakey_b
   [DeviceB-pki-realm-b] quit
   ```

   # Save certificate application information to a certificate request file in PKCS#10 format.

   ```
   [DeviceB] pki enroll-certificate realm a pkcs10 filename cer_req
    Info: Creating certificate request file...
    Info: Create certificate request file successfully.
   ```

4. Download the certificate request file using a file transfer protocol, and send the file to the CA server in out-of-band mode, such as through the web system, using a disk, or through an email, to apply for a local certificate from the CA server.

   After a local certificate is successfully requested, download the local certificate **b_local.cer** and CA certificate **b_ca.cer** in out-of-band mode. Transfer the certificates to the device storage using a file transfer protocol.

5. Import the CA certificate into the device memory.

   After the certificate is imported, the **b_ca.cer** file is deleted from the storage medium by default. To keep it, select **N** as prompted.

   ```
   [DeviceB] pki import-certificate ca filename b_ca.cer
    The CA's Subject is /CN=ca_root
    The CA's fingerprint is:
      MD5  fingerprint:1135 25D8 96D3 5936 C382 35EA 2CEE 80EB
      SHA1 fingerprint:6330 974F B2FE 3C52 D16B DAC4 0140 918B 4BCD 3EC7
    Is the fingerprint correct?(Y/N):y
    Info: Succeeded in importing the certificate.
    Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select
   [Y/N]:y
    Info: Delete Success.
   ```

6. Import the local certificate into the device memory.

   After the certificate is imported, the **b_local.cer** file is deleted from the storage medium by default. To keep it, select **N** as prompted.

   ```
   [DeviceB] pki import-certificate local filename b_local.cer
    Info: Succeeded in importing file.
    Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select
   [Y/N]:y
    Info: Delete Success
   ```

Step 15 Configure an IPsec profile.

1. Configure an IPsec proposal.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceB-ipsec-proposal-tran1] quit
   ```

2. Configure an IKE proposal.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method rsa-signature
   [DeviceB-ike-proposal-10] prf hmac-sha2-256
   [DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

3. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] certificate local-filename b_local.cer
[DeviceB-ike-peer-a] quit
```

4. Configure an IPsec profile.

```
[DeviceB] ipsec profile pro1
[DeviceB-ipsec-profile-pro1] proposal tran1
[DeviceB-ipsec-profile-pro1] ike-peer a
[DeviceB-ipsec-profile-pro1] quit
```

Step 16 Apply the IPsec profile to the tunnel interface.

```
[DeviceB] interface tunnel 1
[DeviceB-Tunnel1] ipsec profile pro1
[DeviceB-Tunnel1] quit
```

----End

Verifying the Configuration

On DeviceA and DeviceB, run the **display ike sa** and **display ipsec sa** commands to check SA establishment information. The following shows the command output of DeviceB for your reference. If the following information is displayed, IKE SAs and IPsec SAs have been successfully established.

```
<DeviceB> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SAs in all CPU : 1
Total number of phase 2 SAs in all CPU : 1

Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
    Conn-ID     Peer           VPN   Flag(s)  Phase  RemoteType  RemoteID
  -------------------------------------------------------------------------------
    16777239    1.1.1.1/500          RD|ST|A  v2:2   IP          1.1.1.1
    16777232    1.1.1.1/500          RD|ST|A  v2:1   IP          1.1.1.1
  -------------------------------------------------------------------------------
<DeviceB> display ipsec sa

ipsec sa information:

===============================
Interface: Tunnel1

===============================

  ------------------------------
  IPsec profile name: "pro1"
  Mode              : PROF-ISAKMP
  ------------------------------
    Connection ID     : 83903371
    Encapsulation mode: Tunnel
    Tunnel local      : 2.2.2.2
    Tunnel remote     : 1.1.1.1

    [Outbound ESP SAs]
      SPI: 763065754 (0x2d7b759a)
      Proposal: ESP-ENCRYPT-AES-256 SHA2-256-128
```

 Copyright © Huawei Technologies Co., Ltd.

```
  SA remaining key duration (kilobytes/sec): 20971520/3551
  Max sent sequence-number: 1
  UDP encapsulation used for NAT traversal: N
  SA encrypted packets (number/kilobytes): 4/0

[Inbound ESP SAs]
  SPI: 163241969 (0x9badff1)
  Proposal: ESP-ENCRYPT-AES-256 SHA2-256-128
  SA remaining key duration (kilobytes/sec): 20971520/3551
  Max received sequence-number: 1
  UDP encapsulation used for NAT traversal: N
  SA decrypted packets (number/kilobytes): 4/0
  Anti-replay : Disable
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method rsa-signature
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer b
 ike-proposal 10
 certificate local-filename a_local.cer
#
ipsec profile pro1
 ike-peer b
 proposal tran1
#
pki entity user_a
 country CN
 state beijing
 organization huawei
 organization-unit dev
 common-name devicea
 fqdn testa.abc.com
 ip-address 1.1.1.1
 email testa@user.com
#
pki realm a
 entity user_a
 rsa local-key-pair rsakey_a
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel 1
 ip address 172.16.0.1 255.255.255.0
 tunnel-protocol ipsec
 source 1.1.1.1
 destination 2.2.2.2
 ipsec profile pro1
#
firewall zone trust
 set priority 85
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel1
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
 ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method rsa-signature
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer a
 ike-proposal 10
 certificate local-filename b_local.cer
#
ipsec profile pro1
 ike-peer a
 proposal tran1
#
pki entity user_b
 country CN
 state beijing
 organization huawei
 organization-unit dev
 common-name deviceb
 fqdn testb.abc.com
 ip-address 1.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 email testb@user.com
#
pki realm b
 entity user_b
 rsa local-key-pair rsakey_b
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
#
interface Tunnel 1
 ip address 172.16.0.2 255.255.255.0
 tunnel-protocol ipsec
 source 2.2.2.2
 destination 1.1.1.1
 ipsec profile pro1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel1
#
 ip route-static 1.1.1.0 255.255.255.0 2.2.2.3
 ip route-static 10.1.0.0 255.255.255.0 Tunnel1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

8.1.11 Web: Example for Establishing an IPsec 6 Tunnel Based on Physical Interfaces Between Two Gateways

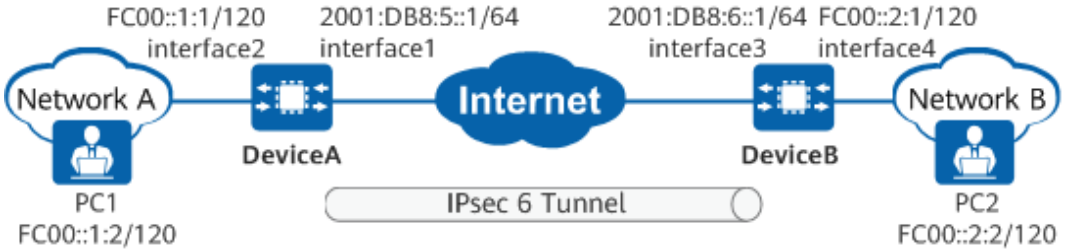
Networking Requirements

As shown in **Figure 8-11**, DeviceA and DeviceB serve as the egress gateways of two IPv6 networks. To enhance communication security, IPsec protection is performed on traffic between the IPv6 networks.

Figure 8-11 Establishing an IPsec 6 tunnel based on physical interfaces between two gateways

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.



Item	DeviceA	DeviceB
Interface configuration	Interface number: GE0/0/1 IP address: 2001:DB8:5::1/64 Security zone: Untrust	Interface number: GE0/0/1 IP address: 2001:DB8:6::1/64 Security zone: Untrust
	Interface number: GE0/0/2 IP address: FC00::1:1/120 Security zone: Trust	Interface number: GE0/0/2 IP address: FC00::2:1/120 Security zone: Trust
IPsec configuration	Scenario: point-to-point Remote IP address: 2001:DB8:6::1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address	Scenario: point-to-point Remote IP address: 2001:DB8:5::1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes, including the public network routes between DeviceA and DeviceB and the private network route from DeviceA or DeviceB to its peer private network.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv6	
IP Address	2001:DB8:5::1/64

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv6	
IP Address	FC00::1:1/120

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Source Address	fc00::1:0/120
Destination Address	fc00::2:0/120
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	fc00::2:0/120
Destination Address	fc00::1:0/120
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2001:DB8:5::1/64
Destination Address	2001:DB8:6::1/64
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	2001:DB8:6::1/64
Destination Address	2001:DB8:5::1/64
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 2001:DB8:5::2.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Network** > **Route** > **Static Route**.

b. In **Static Route List**, click **Add**.

c. Configure a public network route from DeviceA to DeviceB as follows. Click **OK**.

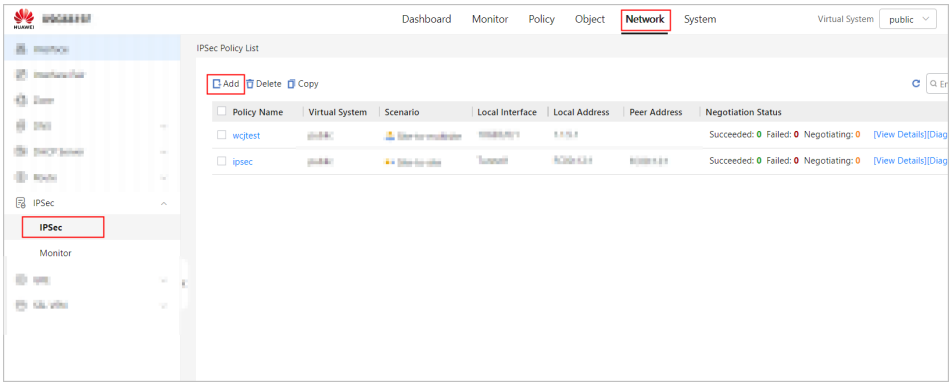
Protocol	IPv6
Destination Address/Mask	2001:DB8:6::0/120
Next Hop	2001:DB8:5::2

d. Repeat the preceding steps to configure a route from DeviceA's private network to DeviceB's private network as follows.

Protocol	IPv6
Destination Address/Mask	FC00::2:0/120
Next Hop	2001:DB8:5::2

4. Configure an IPsec policy.

a. Choose **Network** > **IPSec** > **IPSec**.

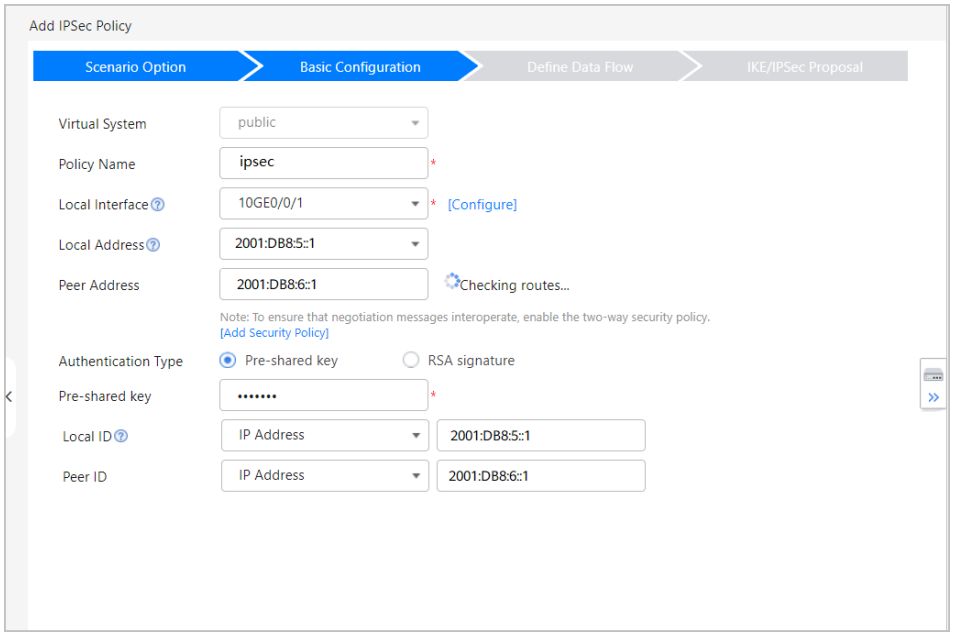


b. Click **Add** to create an IPsec policy as prompted.

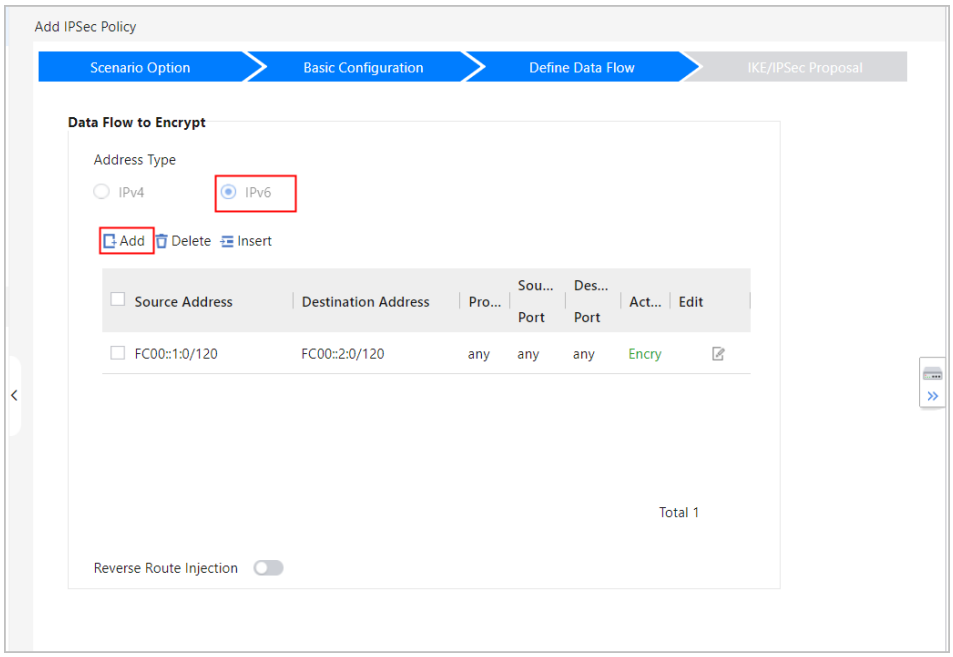
 Copyright © Huawei Technologies Co., Ltd.



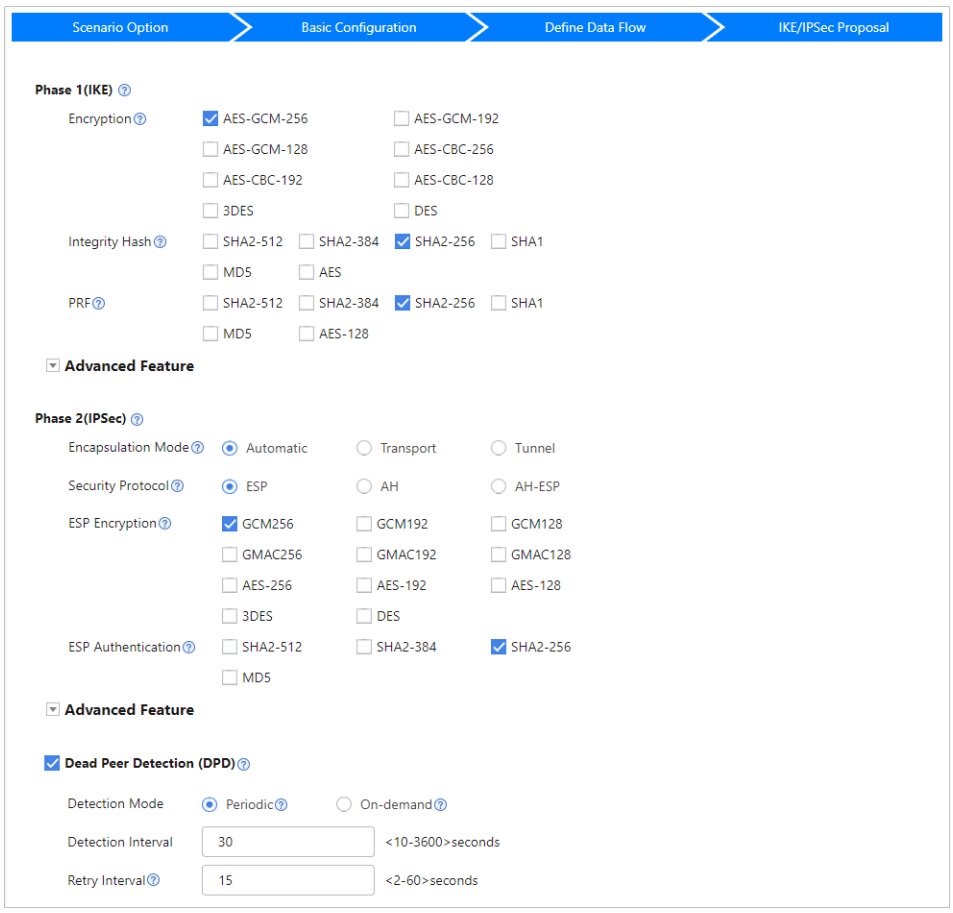
The PSK is Hello123.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

Step 2 Configure DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv6	
IP Address	2001:DB8:6::1/64

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv6	
IP Address	FC00::2:1/120

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	fc00::2:0/120
Destination Address	fc00::1:0/120
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	trust
Source Address	fc00::1:0/120
Destination Address	fc00::2:0/120
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2001:DB8:6::1/64
Destination Address	2001:DB8:5::1/64
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	2001:DB8:5::1/64
Destination Address	2001:DB8:6::1/64
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 2001:DB8:6::2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   a. Configure a public network route from DeviceB to DeviceA as follows. Click **OK**.

Protocol	IPv6
Destination Address/Mask	2001:DB8:5::0/120
Next Hop	2001:DB8:6::2

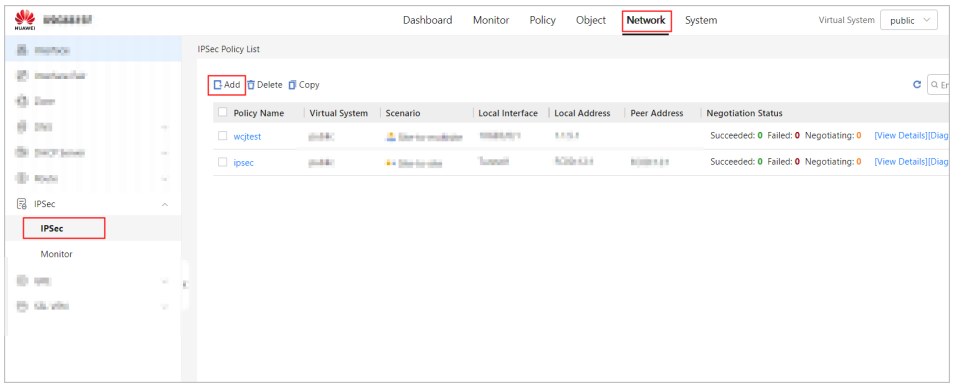
 Copyright © Huawei Technologies Co., Ltd.

b. Repeat the preceding steps to configure a route from DeviceB's private network to DeviceA's private network as follows.

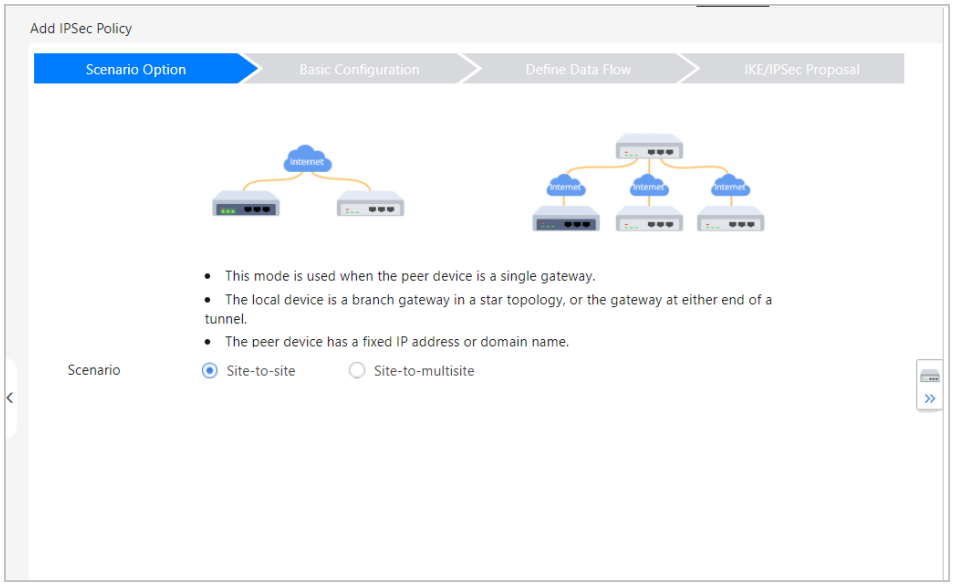
Protocol	IPv6
Destination Address/Mask	FC00::1:0/120
Next Hop	2001:DB8:6::2

4. Configure an IPsec policy.

a. Choose **Network** > **IPSec** > **IPSec**.

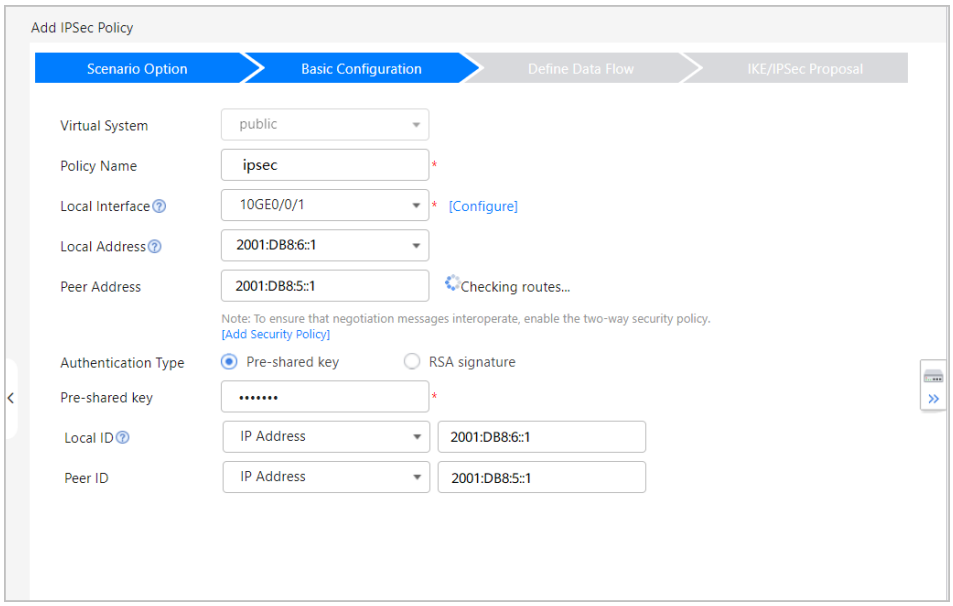


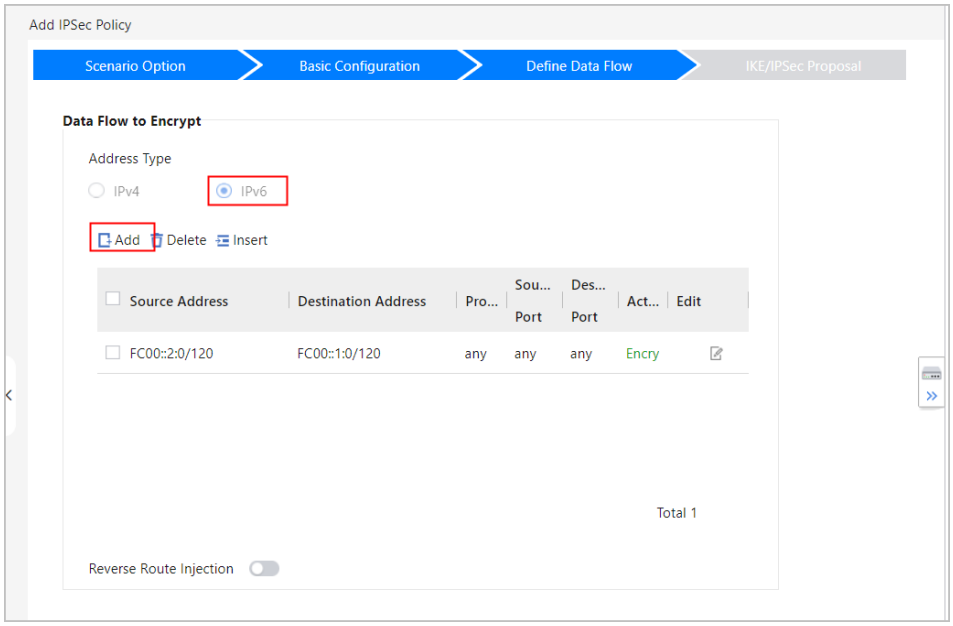
b. Click **Add** to create an IPsec policy as prompted.



The PSK is Hello123.

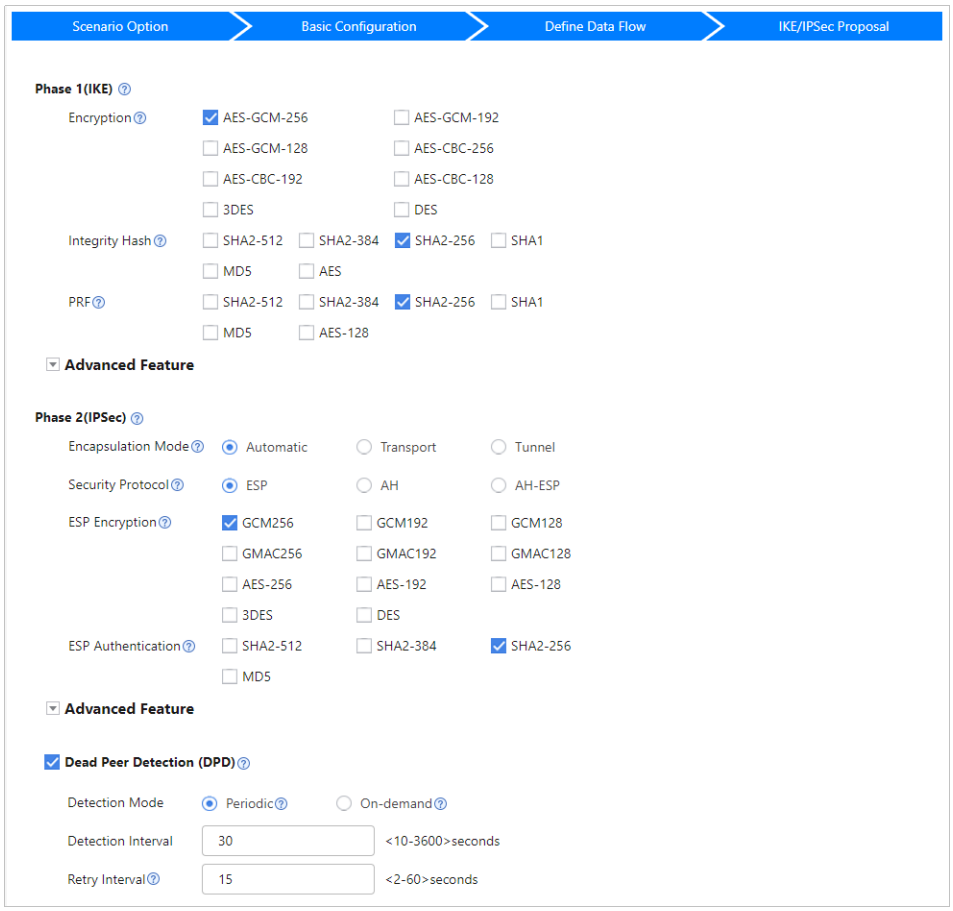
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

----End

Verifying the Configuration

1. Take DeviceA as an example. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. If "IKE negotiation succeeded" or "IPSec negotiation succeeded" is displayed in the **Status** column, the tunnel is successfully established.
2. Access a host on network B from a host on network A. The access succeeds.

Configuration Scripts

- DeviceA

```
#
acl ipv6 number 3000
 rule 5 permit ipv6 source FC00::1:0/120 destination FC00::2:0/120
#
ipsec proposal prop28111627842
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ike peer ike281116278421
 pre-shared-key %+%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%+%#
 ike-proposal 1
 remote-id-type ip
 remote-id 2001:DB8:6::1
 local-id 2001:DB8:5::1
 remote-address 2001:DB8:6::1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278421
 proposal prop28111627842
 tunnel local 2001:DB8:5::1
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:5::1/64
 ipsec policy ipsec
#
interface GE0/0/2
 ipv6 enable
 ipv6 address fc00::1:1/120
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ipv6 route-static 2001:DB8:6::0 64 2001:DB8:5::2
ipv6 route-static FC00::2:0 120 2001:DB8:5::2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address FC00::1:0 120
  destination-address FC00::2:0 120
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address FC00::2:0 120
  destination-address FC00::1:1 120
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2001:DB8:5::1 64
  destination-address 2001:DB8:6::1 64
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2001:DB8:6::1 64
  destination-address 2001:DB8:5::1 64
  action permit
#
return
```

- DeviceB

```
#
acl ipv6 number 3000
 rule 5 permit ipv6 source FC00::2:0/120 destination FC00::1:0/120
#
ipsec proposal prop28111627844
 esp authentication-algorithm sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike281116278423
 pre-shared-key %+%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%+%#
 ike-proposal 1
 remote-id-type ip
 remote-id 2001:DB8:5::1
 local-id 2001:DB8:6::1
 remote-address 2001:DB8:5::1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278423
 proposal prop28111627844
 tunnel local 2001:DB8:6::1
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::1/64
 ipsec policy ipsec
#
interface GE0/0/2
 ipv6 enable
 ipv6 address fc00::2:1/120
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ipv6 route-static 2001:DB8:5::0 64 2001:DB8:6::2
ipv6 route-static FC00::1:0 120 2001:DB8:6::2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address FC00::2:0 120
  destination-address FC00::1:0 120
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address FC00::1:1 120
  destination-address FC00::2:0 120
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2001:DB8:6::1 64
  destination-address 2001:DB8:5::1 64
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2001:DB8:5::1 64
  destination-address 2001:DB8:6::1 64
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

8.1.12 Web: Example for Establishing an IPsec 6 Tunnel Based on Tunnel Interfaces Between Two Gateways

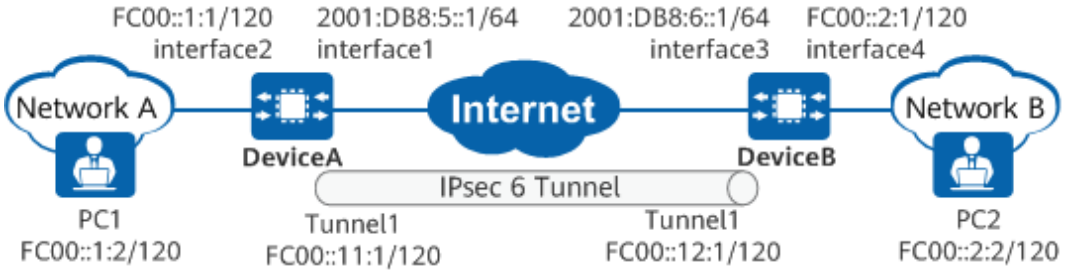
Networking Requirements

As shown in **Figure 8-12**, DeviceA and DeviceB serve as the egress gateways of two IPv6 networks. To enhance communication security, IPsec protection is performed on traffic between the IPv6 networks. For tunnel stability, tunnel interfaces are used to establish an IPsec tunnel.

Figure 8-12 Establishing an IPsec 6 tunnel based on tunnel interfaces between two gateways

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.



Item	DeviceA	DeviceB
Interface configuration	Interface number: GE0/0/1 IP address: 2001:DB8:5::1/64 Security zone: Untrust	Interface number: GE0/0/1 IP address: 2001:DB8:6::1/64 Security zone: Untrust
	Interface number: GE0/0/2 IP address: FC00::1:1/120 Security zone: Trust	Interface number: GE0/0/2 IP address: FC00::2:1/120 Security zone: Trust
	Interface: Tunnel 1 IP address: FC00::11:1/120 Security zone: Untrust	Interface: Tunnel 1 IP address: FC00::12:1/120 Security zone: Untrust
IPsec configuration	Scenario: point-to-point Remote IP address: FC00::12:1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address	Scenario: point-to-point Peer IP address: FC00::11:1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes, including the public network routes between DeviceA and DeviceB and the private network route from DeviceA or DeviceB to its peer private network.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

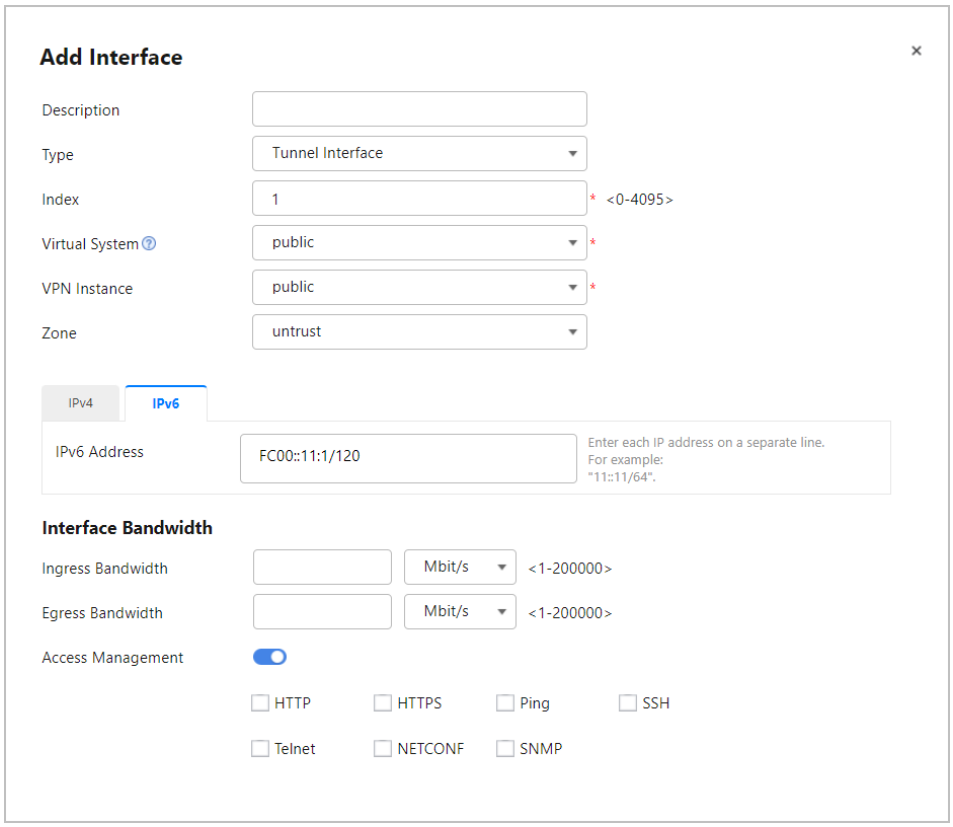
Zone	untrust
IPv6	
IP Address	2001:DB8:5::1/64

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv6	
IP Address	FC00::1:1/120

   d. Click **Add** and set parameters as follows to create a tunnel interface. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.

   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	fc00::1:0/120
Destination Address	fc00::2:0/120
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	fc00::2:0/120
Destination Address	fc00::1:0/120
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	FC00::11:1/120
Destination Address	FC00::12:1/120
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	FC00::12:1/120
Destination Address	FC00::11:1/120
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 2001:DB8:5::2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceA to DeviceB as follows. Click **OK**.

Protocol	IPv6

 Copyright © Huawei Technologies Co., Ltd.

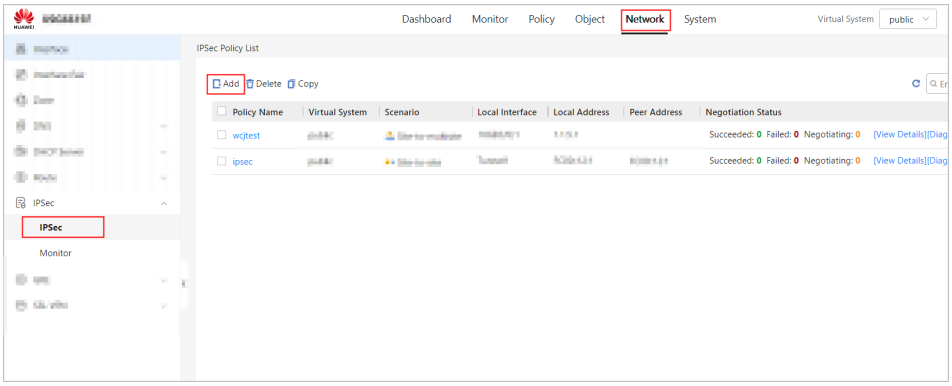
Destination Address/Mask	2001:DB8:6::1/64
Next Hop	2001:DB8:5::2

d. Repeat the preceding steps to configure a route from DeviceA's private network to DeviceB's private network as follows.

Protocol	IPv6
Destination Address/Mask	FC00::2:0/120
Interface	Tunnel1

Protocol	IPv6
Destination Address/Mask	FC00::12:0/120
Next Hop	2001:DB8:5::2

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

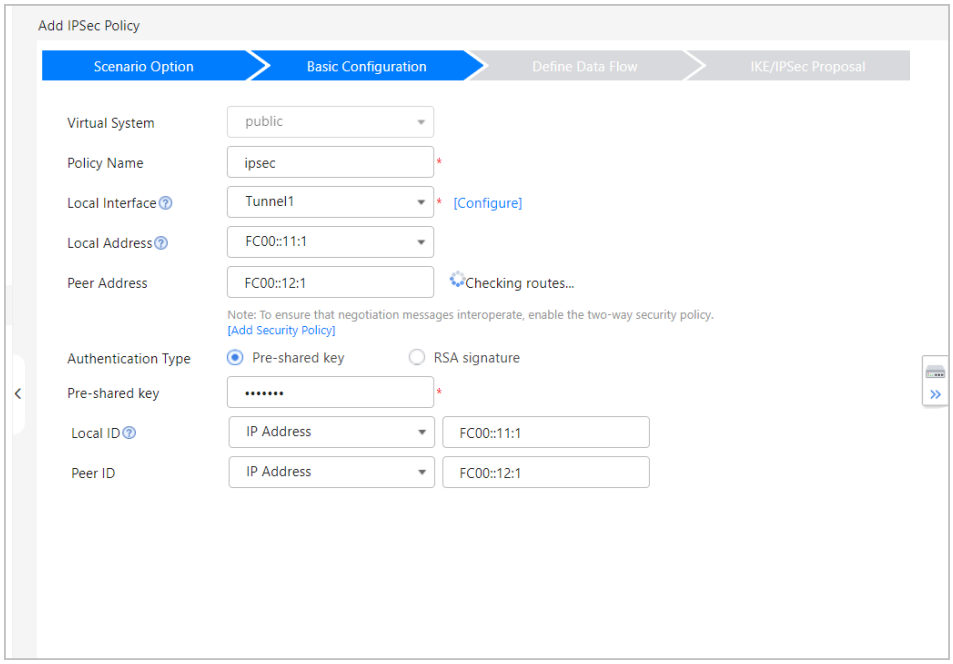


   b. Click **Add** to create an IPsec policy as prompted.

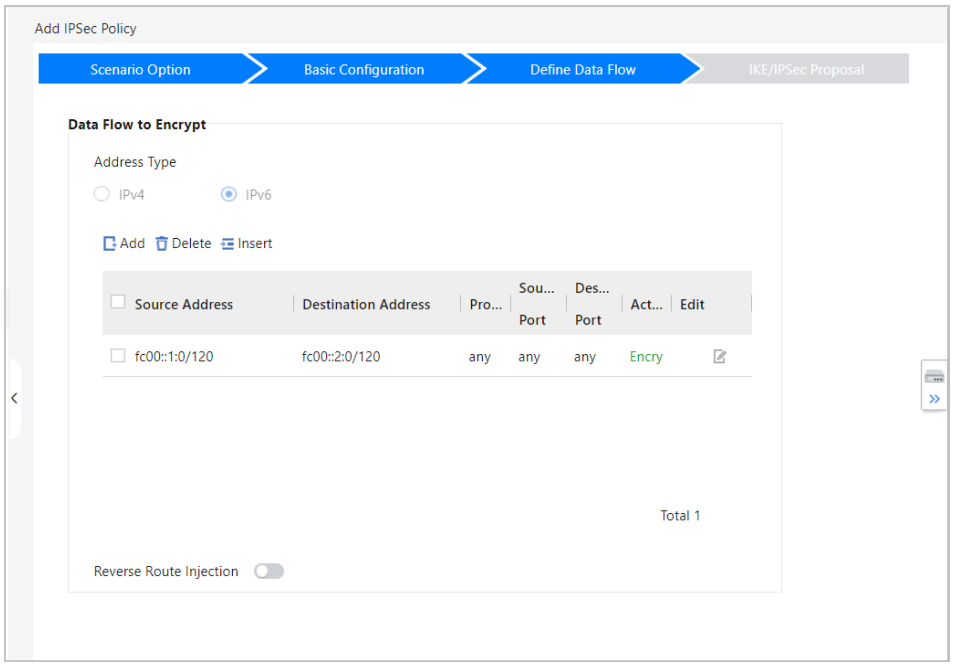
 Copyright © Huawei Technologies Co., Ltd.



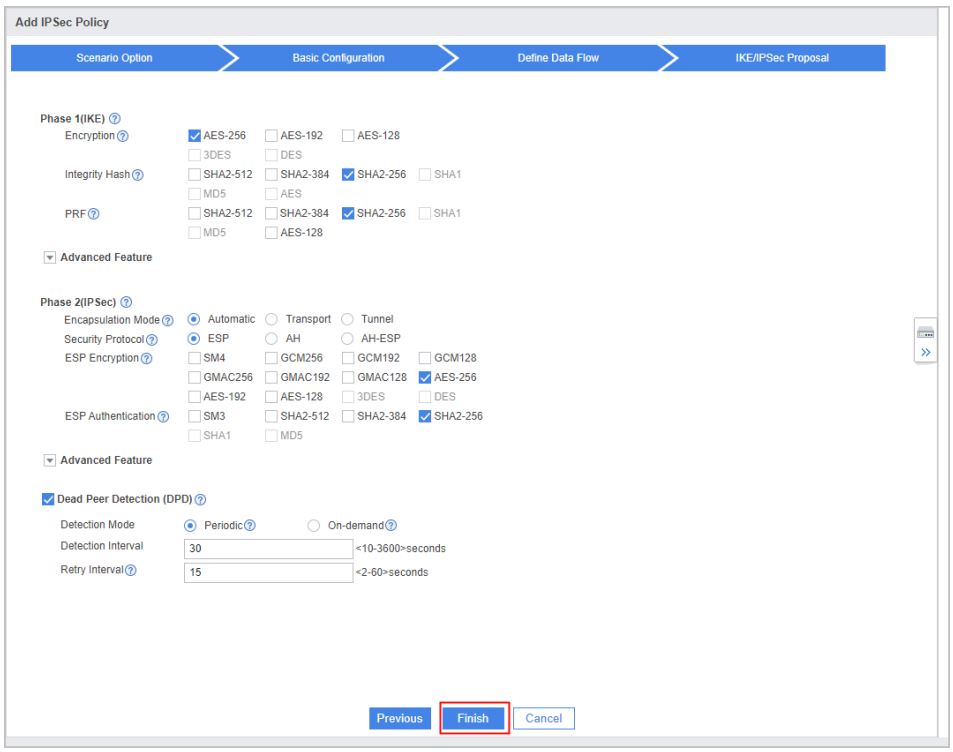
The PSK is Hello123.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

Step 2 Configure DeviceB.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click  for GE0/0/1 and set the parameters as follows. Click **OK**.

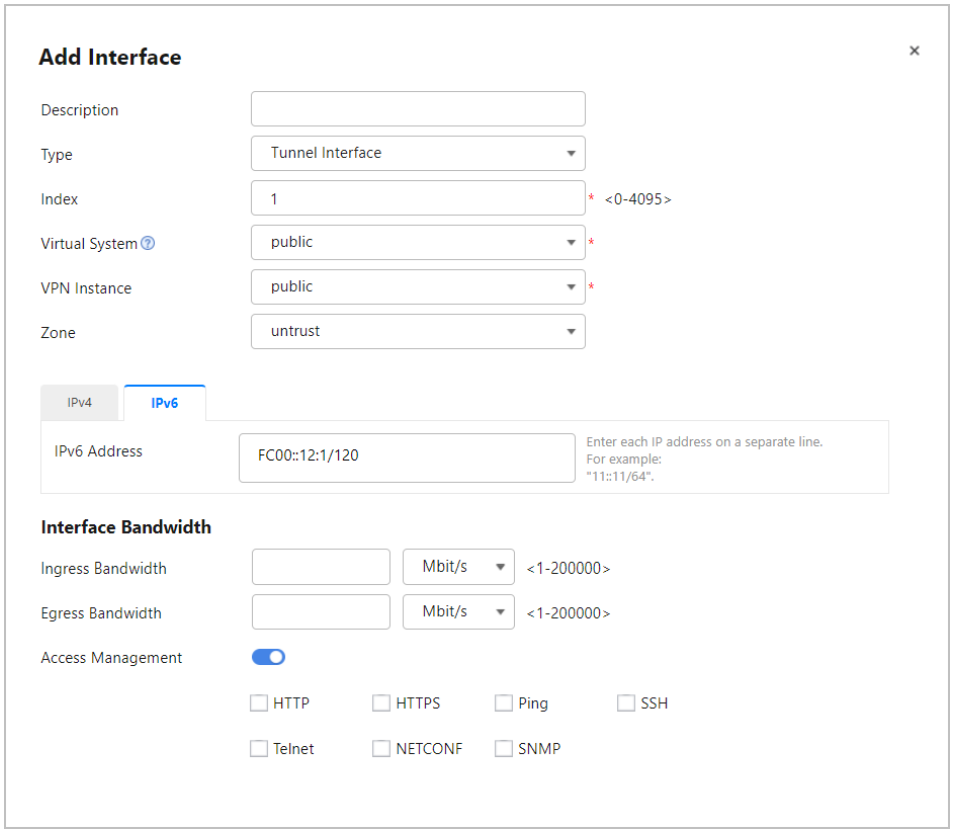
 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv6	
IP Address	2001:DB8:6::1/64

c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv6	
IP Address	FC00::2:1/120

d. Click **Add** and set parameters as follows to create a tunnel interface. Click **OK**.



2. Configure security policies to permit IPsec negotiation packets and service packets.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	fc00::2:0/120
Destination Address	fc00::1:0/120
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	fc00::1:0/120
Destination Address	fc00::2:0/120
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	FC00::12:0/120
Destination Address	FC00::11:0/120
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local

 Copyright © Huawei Technologies Co., Ltd.

Source Address	FC00::11:0/120
Destination Address	FC00::12:0/120
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 2001:DB8:6::2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceB to DeviceA as follows. Click **OK**.

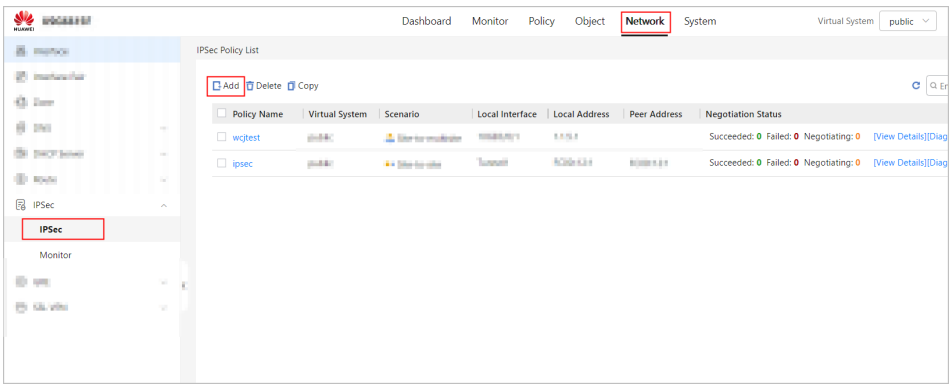
Protocol	IPv6
Destination Address/Mask	2001:DB8:5::0/120
Next Hop	2001:DB8:6::2

   d. Repeat the preceding steps to configure a route from DeviceB's private network to DeviceA's private network as follows.

Protocol	IPv6
Destination Address/Mask	FC00::1:0/120
Interface	Tunnel1

Protocol	IPv6
Destination Address/Mask	FC00::11:0/120
Next Hop	2001:DB8:6::2

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

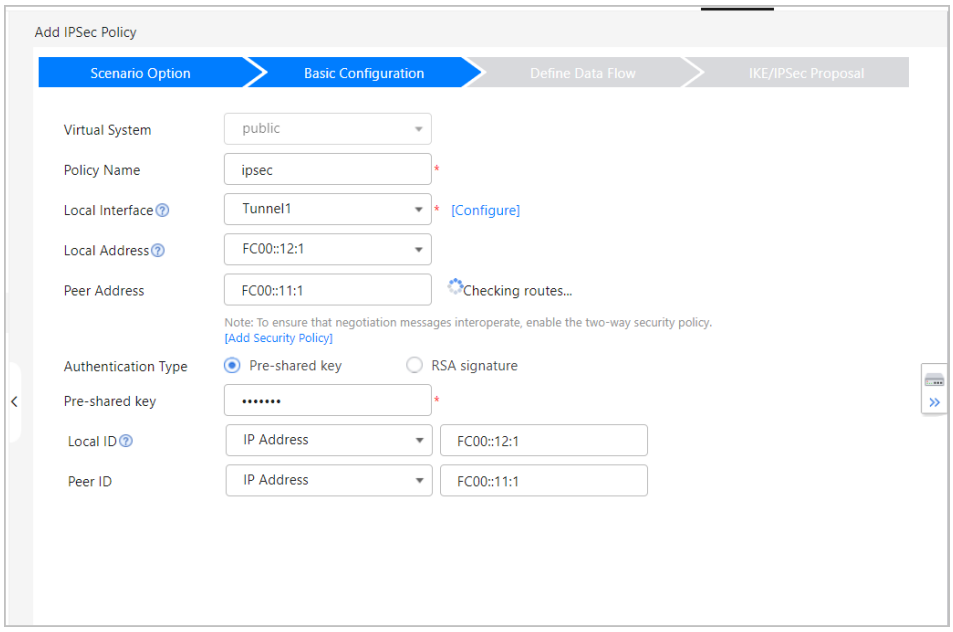


 Copyright © Huawei Technologies Co., Ltd.

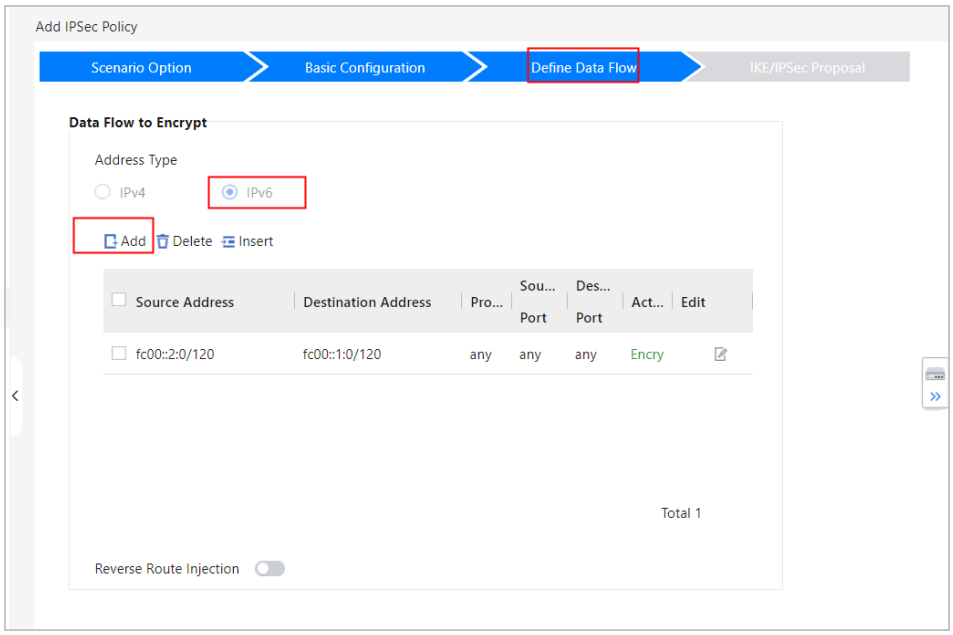
b. Click **Add** to create an IPsec policy as prompted.



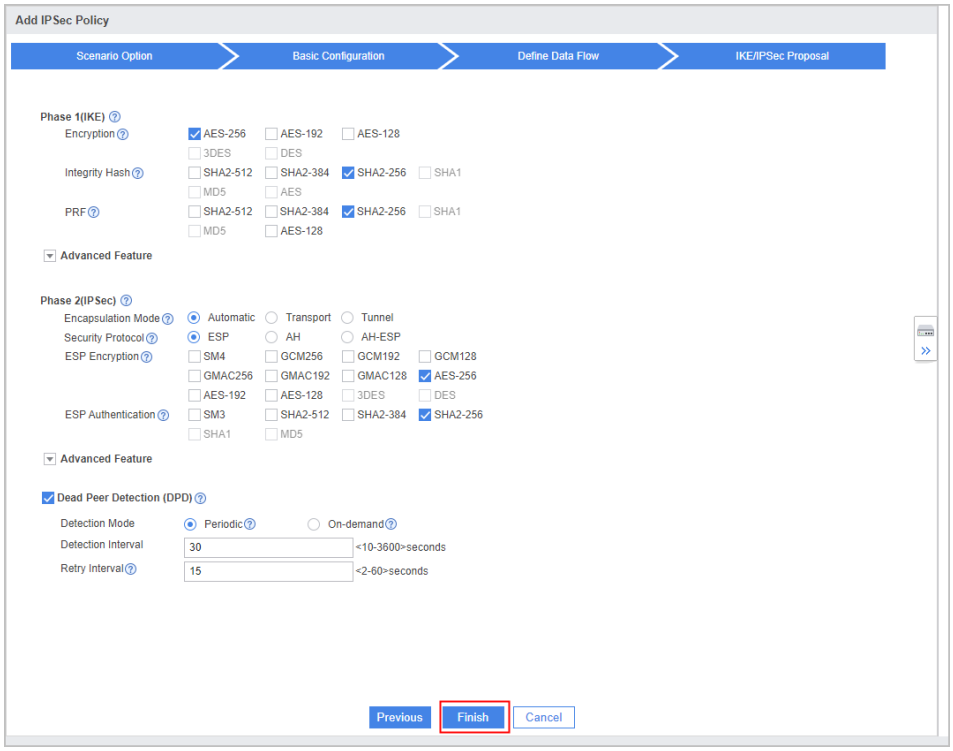
The PSK is Hello123.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish.**

----End

Verifying the Configuration

1. Take DeviceA as an example. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. If "IKE

 Copyright © Huawei Technologies Co., Ltd.

negotiation succeeded" or "IPSec negotiation succeeded" is displayed in the **Status** column, the tunnel is successfully established.

2. Access a host on network B from a host on network A. The access succeeds.

Configuration Scripts

- DeviceA

```
#
acl ipv6 number 3000
 rule 5 permit ipv6 source FC00::1:0/120 destination FC00::2:0/120
#
ipsec proposal prop28111627842
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike281116278421
 pre-shared-key %^%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id FC00::12:1
 local-id FC00::11:1
 remote-address FC00::12:1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278421
 proposal prop28111627842
 tunnel local FC00::11:1
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:5::1/64
#
interface GE0/0/2
 ipv6 enable
 ipv6 address fc00::1:1/120
#
interface Tunnel1
 ipv6 enable
 ipv6 address fc00::11:1/120
 tunnel-protocol ipsec
 ipsec policy ipsec
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface Tunnel1
#
 ipv6 route-static 2001:DB8:6::0 64 2001:DB8:5::2
 ipv6 route-static FC00::2:0 120 Tunnel1
 ipv6 route-static FC00::12:0 120 2001:DB8:5::2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-address FC00::1:0 120
 destination-address FC00::2:0 120
 action permit
rule name policy2
 source-zone untrust
 destination-zone trust
 source-address FC00::2:0 120
 destination-address FC00::1:1 120
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address FC00::11:1 120
 destination-address FC00::12:1 120
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address FC00::12:1 120
 destination-address FC00::11:1 120
 action permit
#
return
```

- DeviceB

```
#
acl ipv6 number 3000
 rule 5 permit ipv6 source FC00::2:0/120 destination FC00::1:0/120
#
ipsec proposal prop28111627844
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike281116278423
 pre-shared-key %^%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id FC00::11:1
 local-id FC00::12:1
 remote-address FC00::11:1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278423
 proposal prop28111627844
 tunnel local FC00::12:1
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:6::1/64
#
interface GE0/0/2
 ipv6 enable
 ipv6 address fc00::2:1/120
#
interface Tunnel1
 ipv6 enable
 ipv6 address fc00::12:1/120
 tunnel-protocol ipsec
 ipsec policy ipsec
#
firewall zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface Tunnel1
#
 ipv6 route-static 2001:DB8:5::0 64 2001:DB8:6::2
 ipv6 route-static FC00::1:0 120 Tunnel1
 ipv6 route-static FC00::11:0 120 2001:DB8:6::2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address FC00::2:0 120
  destination-address FC00::1:0 120
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address FC00::1:1 120
  destination-address FC00::2:0 120
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address FC00::12:0 120
  destination-address FC00::11:0 120
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address FC00::11:0 120
  destination-address FC00::12:0 120
  action permit
#
return
```

8.1.13 Web: Example for Establishing an IPsec 6over4 Tunnel Based on Physical Interfaces Between Two Gateways

Networking Requirements

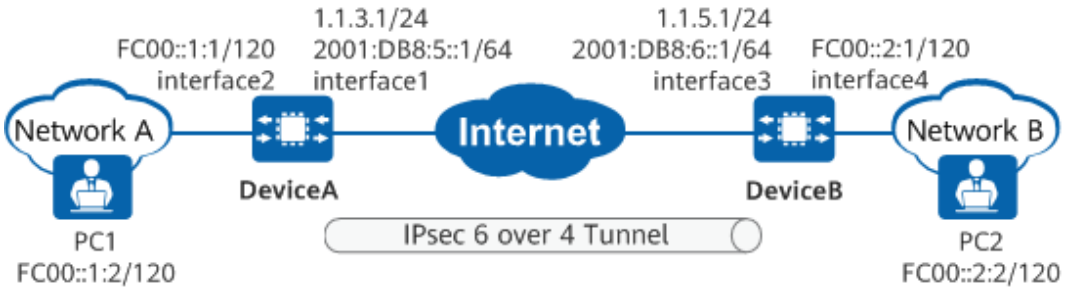
As shown in **Figure 8-13**, two IPv6 networks connect to an IPv4 public network through DeviceA and DeviceB, respectively. IPsec protection is performed on traffic between the IPv6 networks. The IPv6 networks communicate with each other over the IPv4 public network. An IPsec 6over4 tunnel needs to be established between DeviceA and DeviceB so that users on the IPv6 networks can communicate with each other over the IPsec tunnel.

Figure 8-13 Establishing an IPsec 6over4 tunnel based on physical interfaces between two gateways

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	DeviceA	DeviceB
Interface configuration	Interface number: GE0/0/1 IPv4 address: 1.1.3.1/24 IPv6 address: 2001:DB8:5::1/64 Security zone: Untrust	Interface number: GE0/0/1 IPv4 address: 1.1.5.1/24 IPv6 address: 2001:DB8:6::1/64 Security zone: Untrust
	Interface number: GE0/0/2 IP address: FC00::1:1/120 Security zone: Trust	Interface number: GE0/0/2 IP address: FC00::2:1/120 Security zone: Trust
IPsec configuration	Scenario: point-to-point Remote IP address: 1.1.5.1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address	Scenario: point-to-point Remote IP address: 1.1.3.1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.
3. Configure routes, including the public network routes between DeviceA and DeviceB and the private network route from DeviceA or DeviceB to its peer private network.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Set the IPv4 address to 1.1.3.1/24 and IPv6 address to 2001:DB8:5::1/64.

Zone	untrust
IP Type	IPv4
IP Address	1.1.3.1/24
IP Type	IPv6
IP Address	2001:DB8:5::1/64

c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv6	
IP Address	FC00::1:1/120

2. Configure security policies to permit IPsec negotiation packets and service packets.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	fc00::1:0/120
Destination Address	fc00::2:0/120
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2

 Copyright © Huawei Technologies Co., Ltd.

Source Zone	untrust
Destination Zone	trust
Source Address	fc00::2:0/120
Destination Address	fc00::1:0/120
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	1.1.3.1/24, 2001:DB8:5::1/64
Destination Address	1.1.5.1/24, 2001:DB8:6::1/64
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.5.1/24, 2001:DB8:6::1/64
Destination Address	1.1.3.1/24, 2001:DB8:5::1/64
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.3.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceA to DeviceB as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	1.1.5.0/24
Next Hop	1.1.3.2

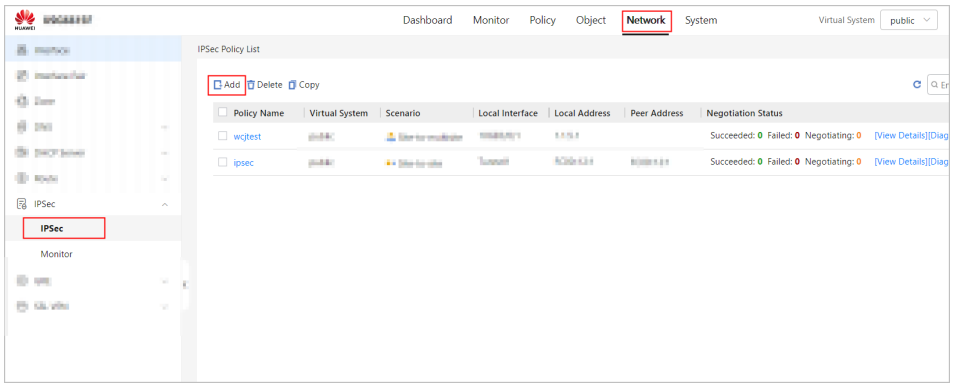
 Copyright © Huawei Technologies Co., Ltd.

d. Repeat the preceding steps to configure a route from DeviceA's private network to DeviceB's private network as follows.

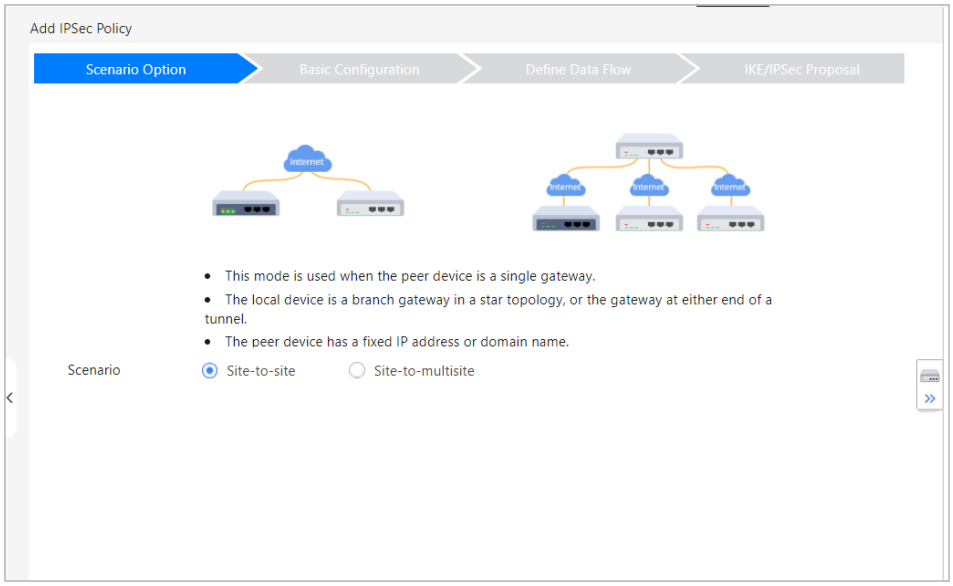
Protocol	IPv6
Destination Address/Mask	FC00::2:0/120
Interface	GE0/0/1

4. Configure an IPsec policy.

a. Choose **Network** > **IPSec** > **IPSec**.

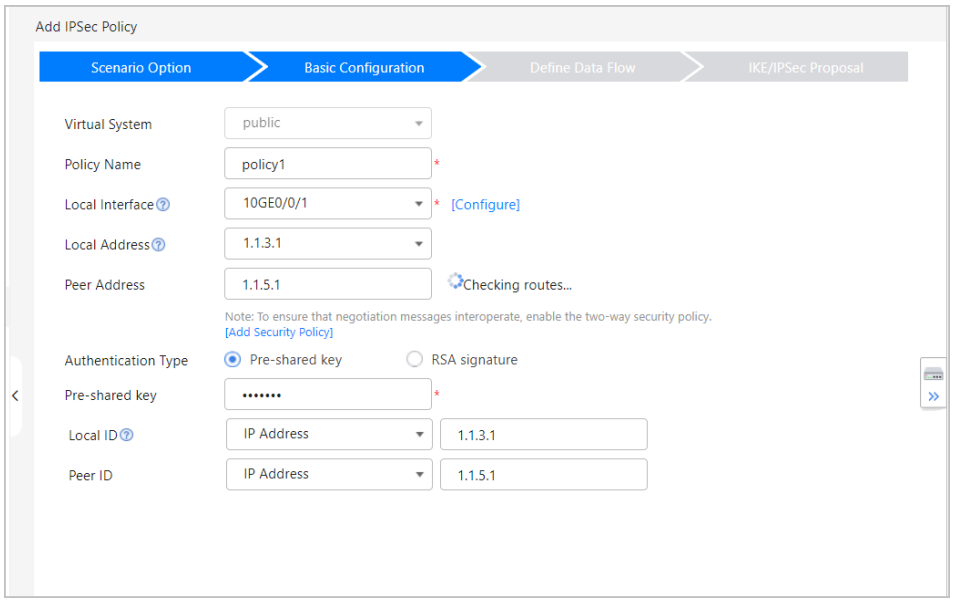


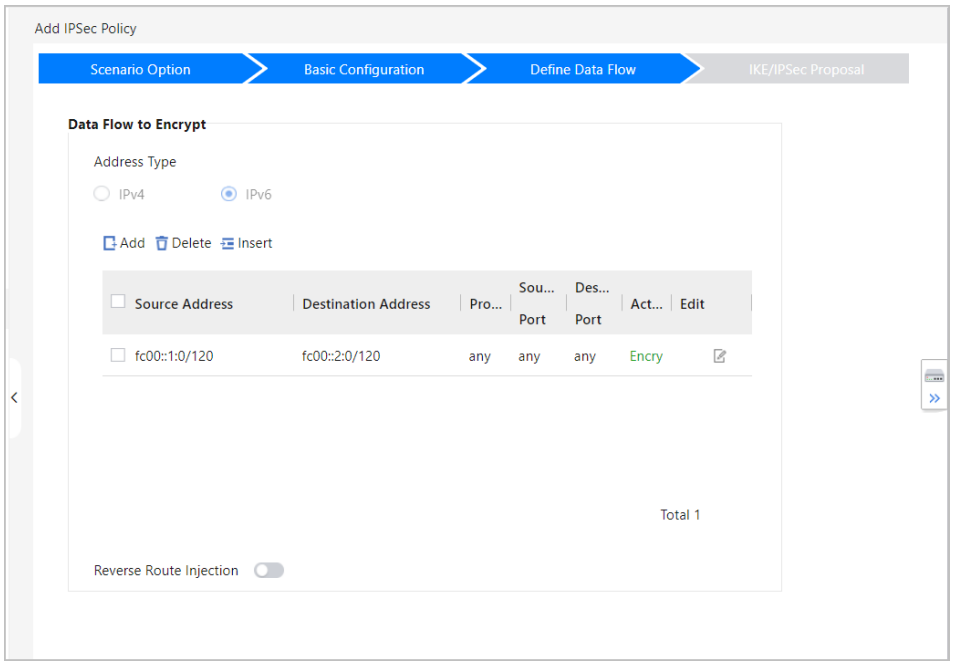
b. Click **Add** to create an IPsec policy as prompted.



The PSK is Hello123.

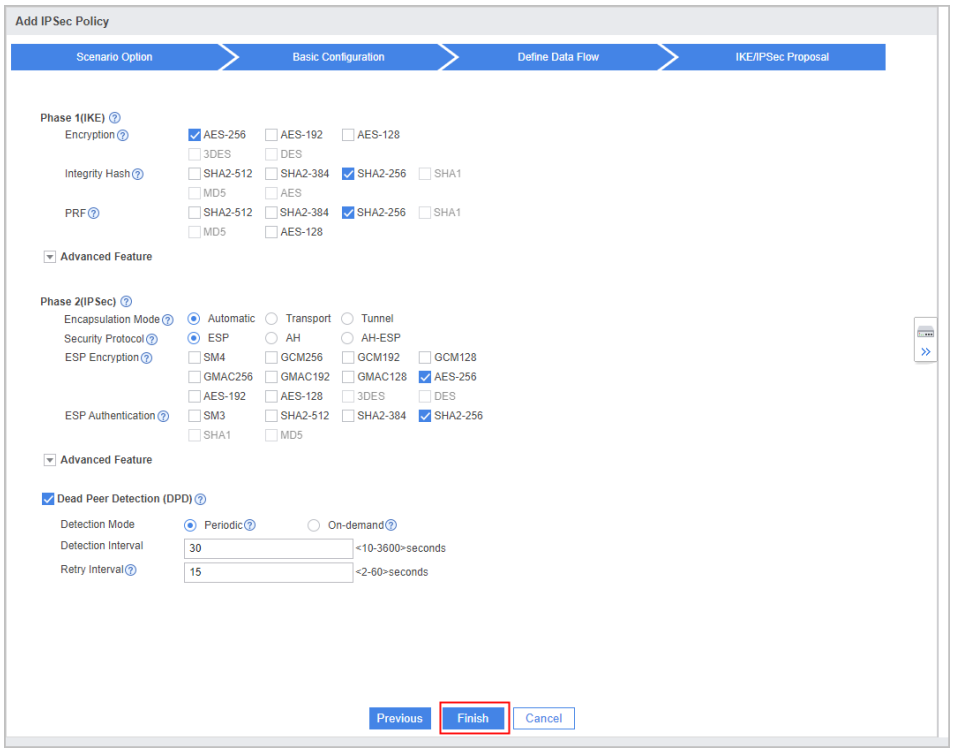
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

Step 2 Configure DeviceB.

1. Set interface IP addresses and add the interfaces to security zones.

   a. Choose **Network** > **Interface**.

   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

   Set the IPv4 address to 1.1.5.1/24 and IPv6 address to 2001:DB8:6::1/64.

Zone	untrust
IP Type	IPv4
IP Address	1.1.5.1/24
IP Type	IPv6
IP Address	2001:DB8:6::1/64

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv6	
IP Address	FC00::2:1/120

2. Configure security policies to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	fc00::2:0/120
Destination Address	fc00::1:0/120
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	fc00::1:0/120
Destination Address	fc00::2:0/120
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2001:DB8:6::1/64, 1.1.5.1/24
Destination Address	2001:DB8:5::1/64, 1.1.3.1/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	2001:DB8:5::1/64, 1.1.3.1/24
Destination Address	2001:DB8:6::1/64, 1.1.5.1/24
Action	Permit

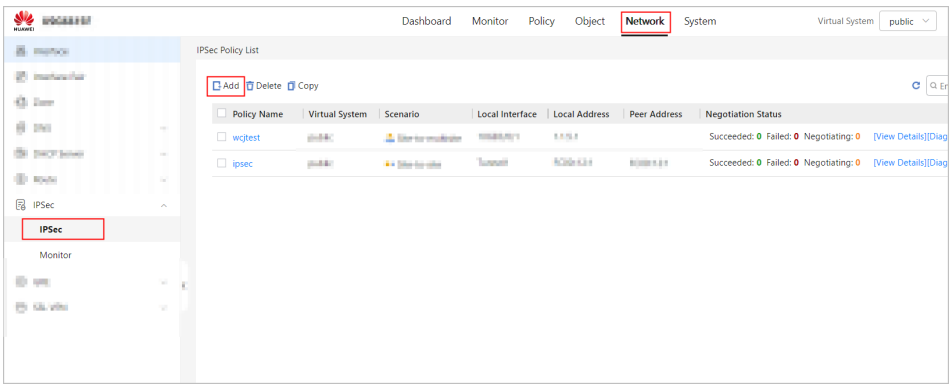
3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.5.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceB to DeviceA as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	1.1.3.0/24
Next Hop	1.1.5.2

   d. Repeat the preceding steps to configure a route from DeviceB's private network to DeviceA's private network as follows.

Protocol	IPv6
Destination Address/Mask	FC00::1:0/120
Interface	GE0/0/1

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

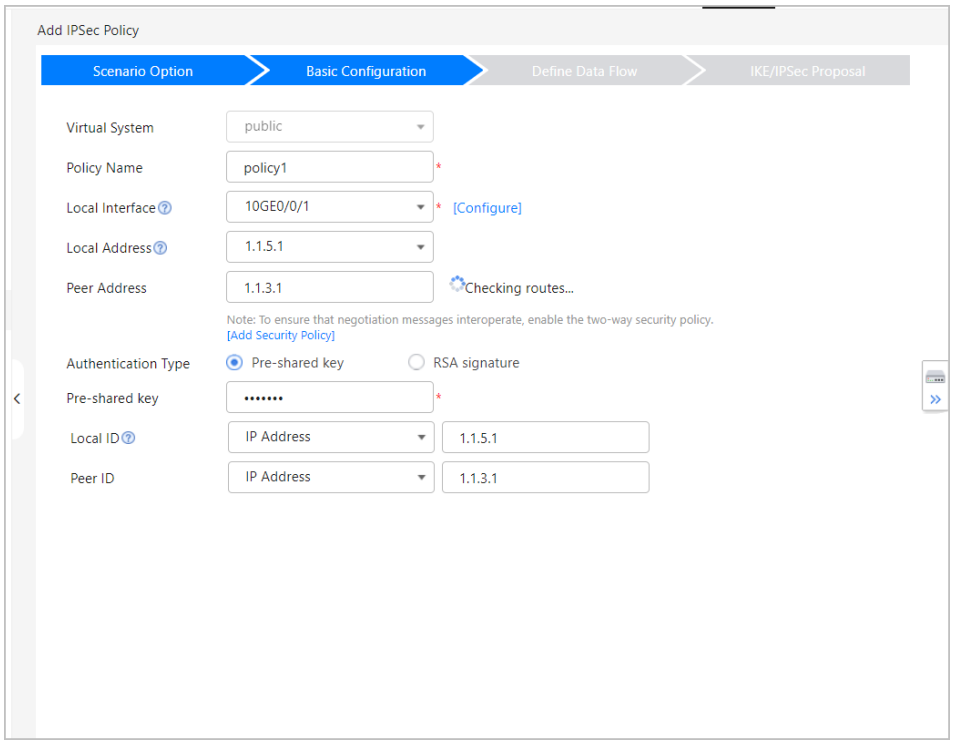


 Copyright © Huawei Technologies Co., Ltd.

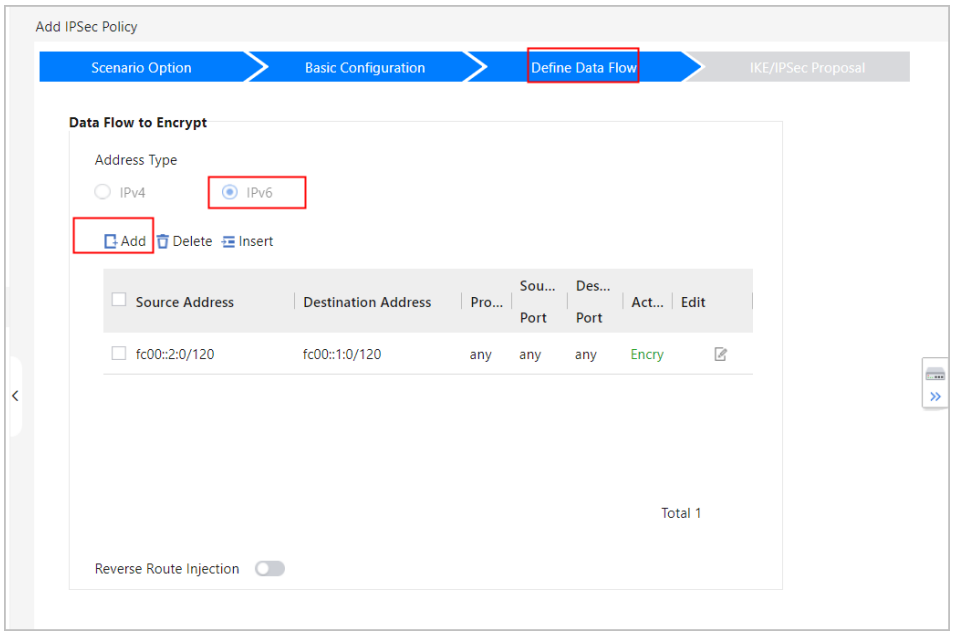
b. Click **Add** to create an IPsec policy as prompted.



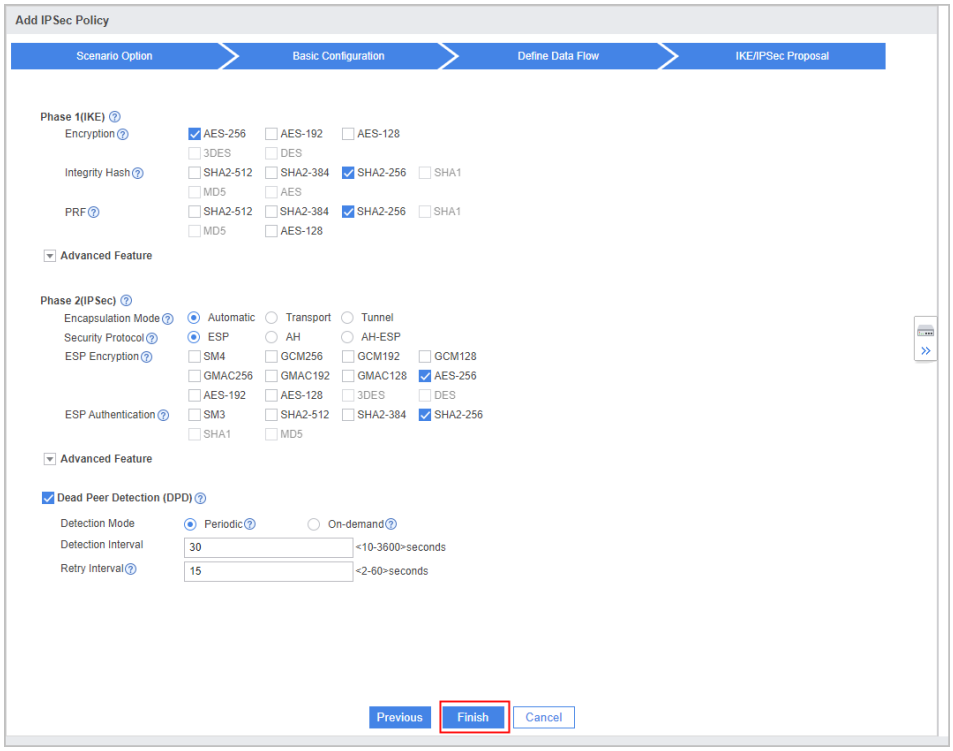
The PSK is Hello123.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

----End

Verifying the Configuration

1. Take DeviceA as an example. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. If "IKE

 Copyright © Huawei Technologies Co., Ltd.

negotiation succeeded" or "IPSec negotiation succeeded" is displayed in the **Status** column, the tunnel is successfully established.

2. Access a host on network B from a host on network A. The access succeeds.

Configuration Scripts

- DeviceA

```
#
acl ipv6 number 3000
 rule 5 permit ipv6 source FC00::1:0/120 destination FC00::2:0/120
#
ipsec proposal prop28111627842
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike281116278421
 pre-shared-key %^%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.5.1
 local-id 1.1.3.1
 dpd type periodic
 remote-address 1.1.5.1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278421
 proposal prop28111627842
 tunnel local applied-interface
 alias ipsec
 sa trigger-mode auto
 sa duration traffic-based 83886080
 sa duration time-based 3600
#
interface GE0/0/1
 ipv6 enable
 ip address 1.1.3.1 255.255.255.0
 ipv6 address 2001:DB8:5::1/64
 ipsec policy ipsec
#
interface GE0/0/2
 ipv6 enable
 ipv6 address fc00::1:1/120
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 1.1.5.0 255.255.255.0 1.1.3.2
#
ipv6 route-static FC00::2:0 120 GE0/0/1
#
security-policy
 rule name policy1
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone untrust
 source-address FC00::1:0 120
 destination-address FC00::2:0 120
 action permit
rule name policy2
 source-zone untrust
 destination-zone trust
 source-address FC00::2:0 120
 destination-address FC00::1:0 120
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 1.1.3.0 mask 255.255.255.0
 source-address 2001:DB8:5::0 64
 destination-address 1.1.5.0 mask 255.255.255.0
 destination-address 2001:DB8:6::0 64
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.5.0 mask 255.255.255.0
 source-address 2001:DB8:6::0 64
 destination-address 1.1.3.0 mask 255.255.255.0
 destination-address 2001:DB8:5::0 64
 action permit
#
return
```

- DeviceB

```
#
acl ipv6 number 3000
 rule 5 permit ipv6 source FC00::2:0/120 destination FC00::1:0/120
#
ipsec proposal prop28111627844
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike281116278423
 pre-shared-key %^%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.3.1
 local-id 1.1.5.1
 dpd type periodic
 remote-address 1.1.3.1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278423
 proposal prop28111627844
 tunnel local applied-interface
 alias ipsec
 sa trigger-mode auto
 sa duration traffic-based 83886080
 sa duration time-based 3600
#
interface GE0/0/1
 ipv6 enable
 ip address 1.1.5.1 255.255.255.0
 ipv6 address 2001:DB8:6::1/64
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ipsec policy ipsec
#
interface GE0/0/2
 ipv6 enable
 ipv6 address fc00::2:1/120
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 1.1.3.0 255.255.255.0 1.1.5.2
#
ipv6 route-static FC00::1:0 120 GE0/0/1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address FC00::2:0 120
  destination-address FC00::1:0 120
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address FC00::1:0 120
  destination-address FC00::2:0 120
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.5.0 mask 255.255.255.0
  source-address 2001:DB8:6::0 64
  destination-address 1.1.3.0 mask 255.255.255.0
  destination-address 2001:DB8:5::0 64
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.0 mask 255.255.255.0
  source-address 2001:DB8:5::0 64
  destination-address 1.1.5.0 mask 255.255.255.0
  destination-address 2001:DB8:6::0 64
  action permit
#
return
```

8.1.14 CLI: Example for Establishing an IPSec 6over4 Tunnel Based on Physical Interfaces Between Two Gateways

Networking Requirements

As shown in **Figure 8-14**, two IPv6 networks are connected to an IPv4 public network through DeviceA and DeviceB respectively. Security protection is desired for mutual access traffic between the IPv6 networks.

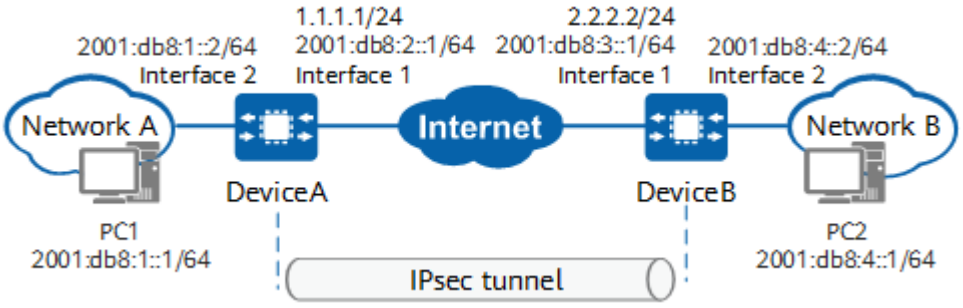
The IPv6 networks communicate with each other over the IPv4 public network. An IPsec 6over4 tunnel needs to be established between DeviceA and DeviceB so that users on the IPv6 networks can communicate with each other over the IPsec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-14 Network diagram for establishing an IPsec 6over4 tunnel based on physical interfaces between two gateways

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 on DeviceA, and interface 3 and interface 4 represent GE 0/0/1 and GE 0/0/2 on DeviceB.



Item	Data
DeviceA	Interface: GE 0/0/1 IPv4 address: 1.1.1.1/24 IPv6 address: 2001:db8:2::1/64 Security zone: Untrust
	Interface: GE 0/0/2 IPv6 address: 2001:db8:1::2/64 Security zone: Trust
	IPsec configuration Remote address: 2.2.2.2 Authentication type: Pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceB	Interface: GE 0/0/1 IPv4 address: 2.2.2.2/24 IPv6 address: 2001:db8:3::1/64 Security zone: Untrust
	Interface: GE 0/0/2 IPv6 address: 2001:db8:4::2/64 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote address: 1.1.1.1 Authentication type: Pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID type: any

Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Perform basic interface configurations.
2. Configure security policies to allow devices on specified private network segments to exchange packets.
3. Configure routes to the peer intranet.
4. Configure IPsec policies, including basic information of IPsec policies, data flows to be encrypted, and IPsec proposal negotiation parameters.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] ipv6 enable
[DeviceA-GE0/0/1] ipv6 address 2001:db8:2::1/64
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:db8:1::2/64
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 2001:db8:1::2 64
[DeviceA-policy-security-rule-policy1] destination-address 2001:db8:4::2 64
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 2001:db8:4::2 64
[DeviceA-policy-security-rule-policy2] destination-address 2001:db8:1::2 64
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy3] source-address 2001:db8:2::1 64
[DeviceA-policy-security-rule-policy3] destination-address 2.2.2.2 24
[DeviceA-policy-security-rule-policy4] destination-address 2001:db8:3::1 64
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 2.2.2.2 24
[DeviceA-policy-security-rule-policy4] source-address 2001:db8:3::1 64
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy4] destination-address 2001:db8:2::1 64
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure static routes on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

Configure a static route to DeviceB to divert tunnel negotiation packets.

```
[DeviceA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
```

Configure a static route to network B to divert encrypted data packets transmitted through the tunnel.

```
[DeviceA] ipv6 route-static 2001:db8:4::0 64 ge 0/0/1
```

Step 4 Configure an ISAKMP IPsec policy on DeviceA and apply an IPsec policy to GE 0/0/1.

1. Create advanced ACL 3000 to define the data flow to be protected.

```
[DeviceA] acl ipv6 3000
[DeviceA-acl6-advance-3000] rule 5 permit ipv6 source 2001:db8:1::0/64 destination 2001:db8:4::0/64
[DeviceA-acl6-advance-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] remote-address 2.2.2.2
[DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-b] quit
```

5. Configure an IPsec policy.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl ipv6 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer b
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy to GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
```

Step 5 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 2.2.2.2 24
[DeviceB-GE0/0/1] ipv6 enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-GE0/0/1] ipv6 address 2001:db8:3::1/64
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ipv6 enable
[DeviceB-GE0/0/2] ipv6 address 2001:db8:4::2/64
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 6 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 2001:db8:4::2 64
[DeviceB-policy-security-rule-policy1] destination-address 2001:db8:1::2 64
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 2001:db8:1::2 64
[DeviceB-policy-security-rule-policy2] destination-address 2001:db8:4::2 64
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as matching criteria, enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] source-address 2001:db8:3::1 24
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 24
[DeviceB-policy-security-rule-policy3] destination-address 2001:db8:2::1 64
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 24
[DeviceB-policy-security-rule-policy4] source-address 2001:db8:2::1 64
[DeviceB-policy-security-rule-policy4] destination-address 2.2.2.2 24
[DeviceB-policy-security-rule-policy4] destination-address 2001:db8:3::1 64
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 7 Configure static routes on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 2.2.2.254.

Configure a static route to DeviceA to divert tunnel negotiation packets.

```
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
```

Configure a static route to network A to divert encrypted data packets transmitted through the tunnel.

```
[DeviceB] ipv6 route-static 2001:db8:1::0 64 ge 0/0/1
```

Step 8 Configure an ISAKMP IPsec policy on DeviceB and apply an IPsec policy to GE 0/0/1.

1. Create advanced ACL 3000 to define the data flow to be protected.

   ```
   [DeviceB] acl ipv6 3000
   [DeviceB-acl6-advance-3000] rule 5 permit ipv6 source 2001:db8:4::0/64 destination
   2001:db8:1::0/64
   [DeviceB-acl6-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceB-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method pre-share
   [DeviceB-ike-proposal-10] prf hmac-sha2-256
   [DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceB-ike-proposal-10] dh group14
   [DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceB-ike-proposal-10] quit
   ```

4. Configure an IKE peer.

   ```
   [DeviceB] ike peer a
   [DeviceB-ike-peer-a] ike-proposal 10
   [DeviceB-ike-peer-a] remote-address 1.1.1.1
   [DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
   [DeviceB-ike-peer-a] quit
   ```

5. Configure an IPsec policy.

   ```
   [DeviceB] ipsec policy map1 10 isakmp
   [DeviceB-ipsec-policy-isakmp-map1-10] security acl ipv6 3000
   [DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
   [DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
   [DeviceB-ipsec-policy-isakmp-map1-10] quit
   ```

6. Apply an IPsec policy to GE 0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on a device in the protected network segment of network A or network B to trigger IKE negotiation.

   If IKE negotiation succeeds, devices in the protected network segments at both ends of the IPsec tunnel can ping each other successfully. Otherwise, IKE negotiation fails.

2. On DeviceA and DeviceB, run the **display ike sa** and **display ipsec sa** commands to check SA establishment information. The following example uses the command output on DeviceB, which indicates that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa
IKE SA information :
  Conn-ID     Peer           VPN   Flag(s)  Phase  RemoteType  RemoteID
 -------------------------------------------------------------------------------
  16777239    1.1.1.1:500          RD|ST|A  v2:2   IP          1.1.1.1
  16777232    1.1.1.1:500          RD|ST|A  v2:1   IP          1.1.1.1

 Number of IKE SA : 2
 -------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
acl ipv6 number 3000
 rule 5 permit ipv6 source 2001:db8:1::0 64 destination 2001:db8:4::0 64
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
  pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
  ike-proposal 10
  remote-address 2.2.2.2
#
ipsec policy map1 10 isakmp
 security acl ipv6 3000
 ike-peer b
 proposal tran1
#
interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ipv6 enable
 ip address 2001:db8:2::1/64
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:db8:2::1/64
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.254
 ipv6 route-static 2001:db8:4::0 64 GE0/0/1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:1::2 64
  destination-address 2001:db8:4::2 64
   action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 2001:db8:4::2 64
  destination-address 2001:db8:1::2 64
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2001:db8:2::1 64
  destination-address 2.2.2.2 mask 255.255.255.255  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  source-address 2001:db8:3::1 64
  destination-address 1.1.1.1 mask 255.255.255.255  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl ipv6 number 3000
 rule 5 permit ipv6 source 2001:db8:4::0 64 destination 2001:db8:1::0 64
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ipsec policy map1 10 isakmp
 security acl ipv6 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ipv6 enable
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 2.2.2.2 255.255.255.0
 ipv6 enable
 ipv6 address 2001:db8:3::1/64
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 1.1.1.0 255.255.255.0 2.2.2.254
 ip route-static 2001:db8:1::0 64 GE0/0/1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 2001:db8:4::2 64
  destination-address 2001:db8:1::2 64
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 2001:db8:1::2 64
  destination-address 2001:db8:4::2 64
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  source-address 2001:db8:3::1 24
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2001:db8:2::1 64
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2001:db8:2::1 64
  destination-address 2.2.2.2 mask 255.255.255.255
  destination-address 2001:db8:3::1 64
  action permit
#
return
```

8.1.15 Web: Example for Establishing an IPsec 4over6 Tunnel Based on Physical Interfaces Between Two Gateways

Networking Requirements

As shown in **Figure 8-15**, two IPv4 networks connect to an IPv6 public network through DeviceA and DeviceB, respectively. IPsec protection is performed on traffic

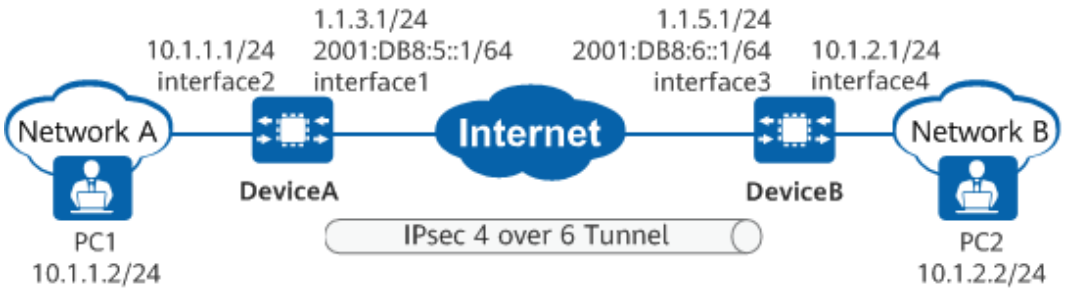
 Copyright © Huawei Technologies Co., Ltd.

between the IPv4 networks. The IPv4 networks communicate with each other over the IPv6 public network. An IPsec 4over6 tunnel needs to be established between DeviceA and DeviceB so that users on the IPv4 networks can communicate with each other over the IPsec tunnel.

Figure 8-15 Establishing an IPsec 4over6 tunnel based on physical interfaces between two gateways

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.



Item	DeviceA	DeviceB
Interface configuration	Interface number: GE0/0/1 IPv4 address: 1.1.3.1/120 IPv6 address: 2001:DB8:5::1/64 Security zone: Untrust	Interface number: GE0/0/1 IPv4 address: 1.1.5.1/120 IPv6 address: 2001:DB8:6::1/64 Security zone: Untrust
	Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust	Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
IPsec configuration	Scenario: point-to-point Remote IP address: 2001:DB8:6::1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address	Scenario: point-to-point Remote IP address: 2001:DB8:5::1 Authentication mode: PSK authentication Local ID: IP address Remote ID: IP address

Configuration Roadmap

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Set IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure routes, including the public network routes between DeviceA and DeviceB and the private network route from DeviceA or DeviceB to its peer private network.
4. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.
   Set the IPv4 address to 1.1.3.1/24 and IPv6 address to 2001:DB8:5::1/64.

Zone	untrust
IP Type	IPv4
IP Address	1.1.3.1/24
IP Type	IPv6
IP Address	2001:DB8:5::1/64

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2001:DB8:5::1/64, 1.1.3.1/24
Destination Address	2001:DB8:6::1/64, 1.1.5.1/24
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	2001:DB8:6::1/64, 1.1.5.1/24
Destination Address	2001:DB8:5::1/64, 1.1.3.1/24
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 2001:DB8:5::2.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Network** > **Route** > **Static Route**.

b. In **Static Route List**, click **Add**.

c. Configure a public network route from DeviceA to DeviceB as follows. Click **OK**.

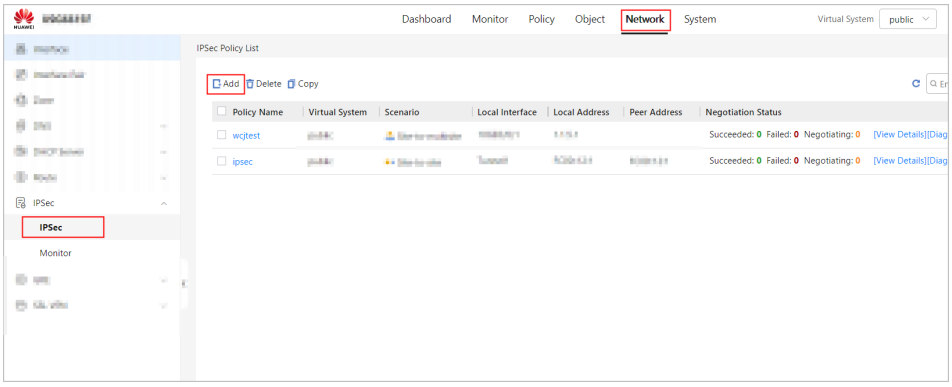
Protocol	IPv6
Destination Address/Mask	2001:DB8:6::0/120
Next Hop	2001:DB8:5::2

d. Repeat the preceding steps to configure a route from DeviceA's private network to DeviceB's private network as follows.

Protocol	IPv4
Destination Address/Mask	10.1.2.0/24
Interface	GE0/0/1

4. Configure an IPsec policy.

a. Choose **Network** > **IPSec** > **IPSec**.

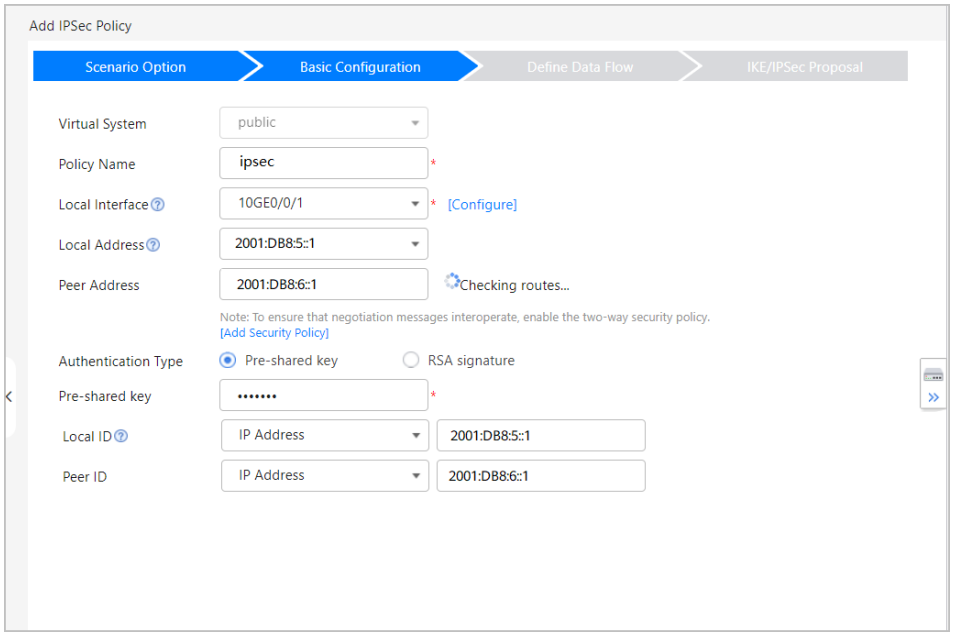


b. Click **Add** to create an IPsec policy as prompted.

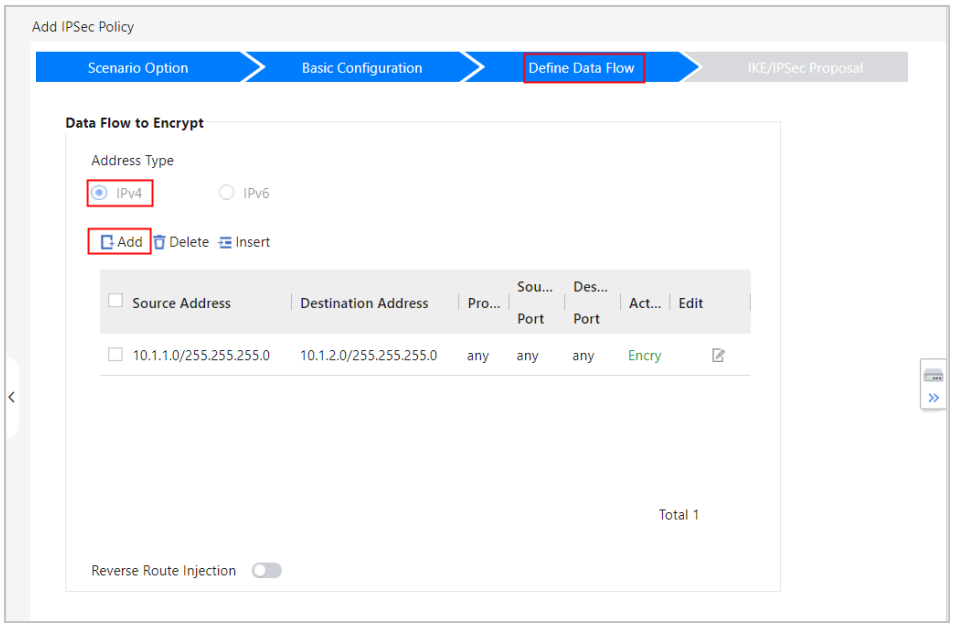
 Copyright © Huawei Technologies Co., Ltd.



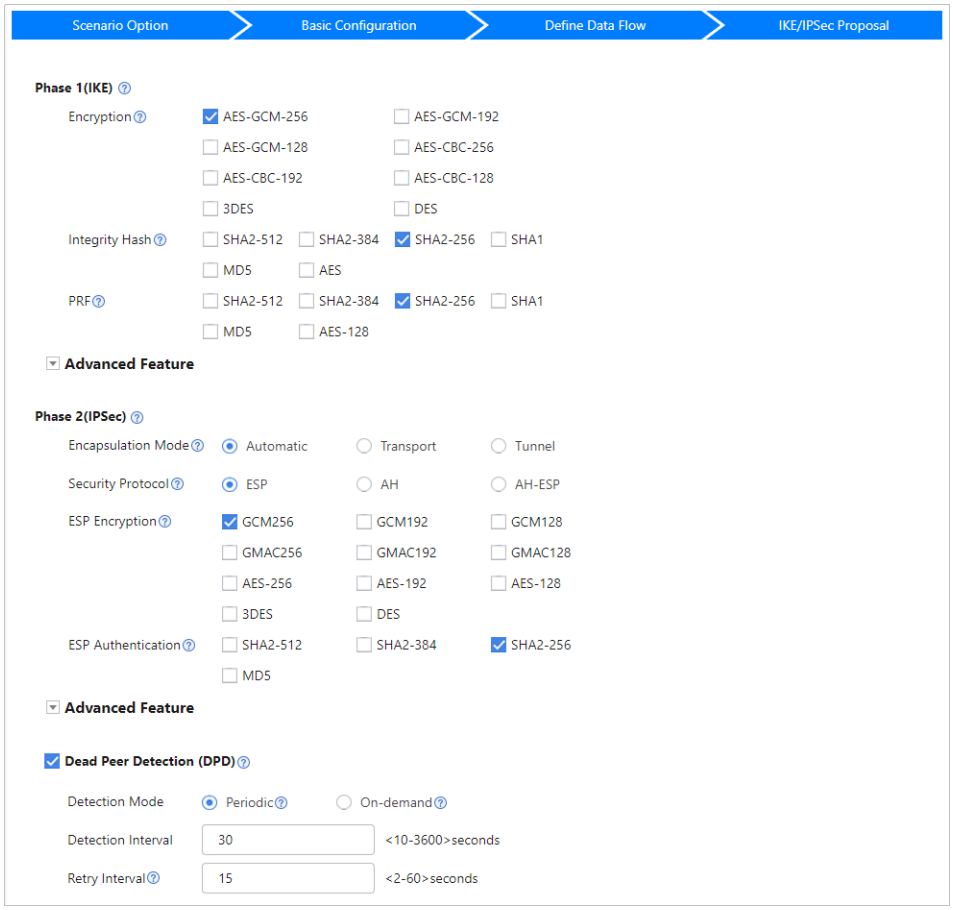
The PSK is Hello123.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

Step 2 Configure DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.
      Set the IPv4 address to 1.1.5.1/24 and IPv6 address to 2001:DB8:6::1/64.

Zone	untrust
IP Type	IPv4
IP Address	1.1.5.1/24
IP Type	IPv6
IP Address	2001:DB8:6::1/64

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

 Copyright © Huawei Technologies Co., Ltd.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	2001:DB8:6::1/64, 1.1.5.1/24
Destination Address	2001:DB8:5::1/64, 1.1.3.1/24
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	2001:DB8:5::1/64, 1.1.3.1/24
Destination Address	2001:DB8:6::1/64, 1.1.5.1/24
Action	Permit

3. Create a static route to the Internet. In this example, the next-hop IP address is 2001:DB8:6::2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a public network route from DeviceB to DeviceA as follows. Click **OK**.

Protocol	IPv6
Destination Address/Mask	2001:DB8:5::0/120

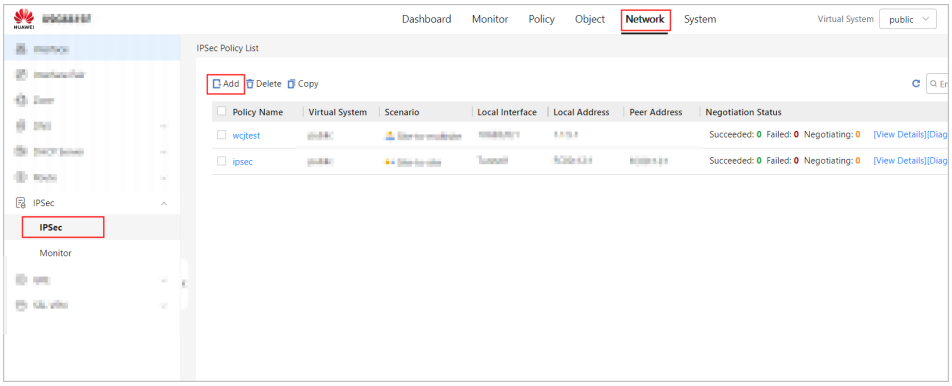
 Copyright © Huawei Technologies Co., Ltd.

Next Hop	2001:DB8:6::2

d. Repeat the preceding steps to configure a route from DeviceB's private network to DeviceA's private network as follows.

Protocol	IPv4
Destination Address/Mask	10.1.1.0/24
Interface	GE0/0/1

4. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

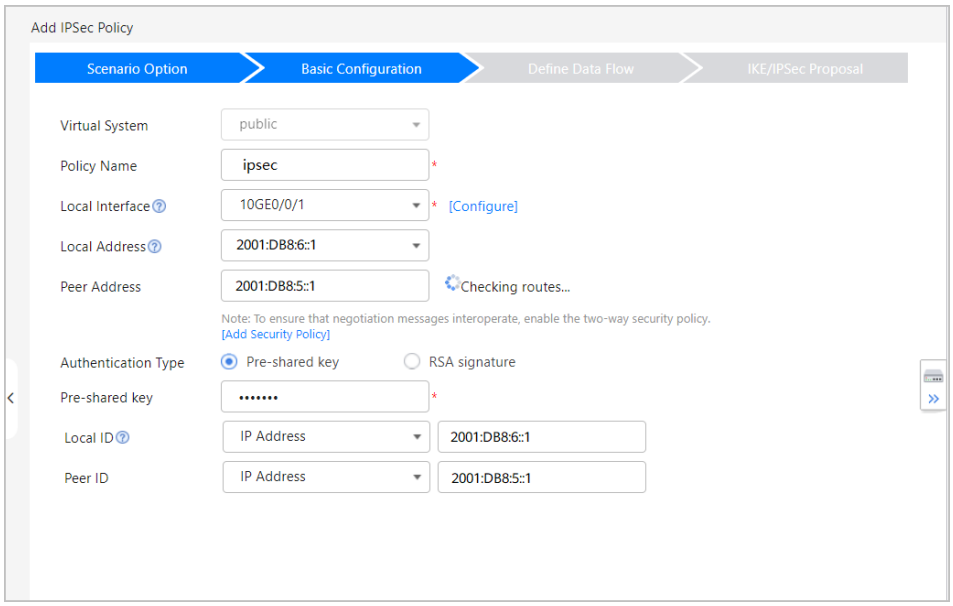


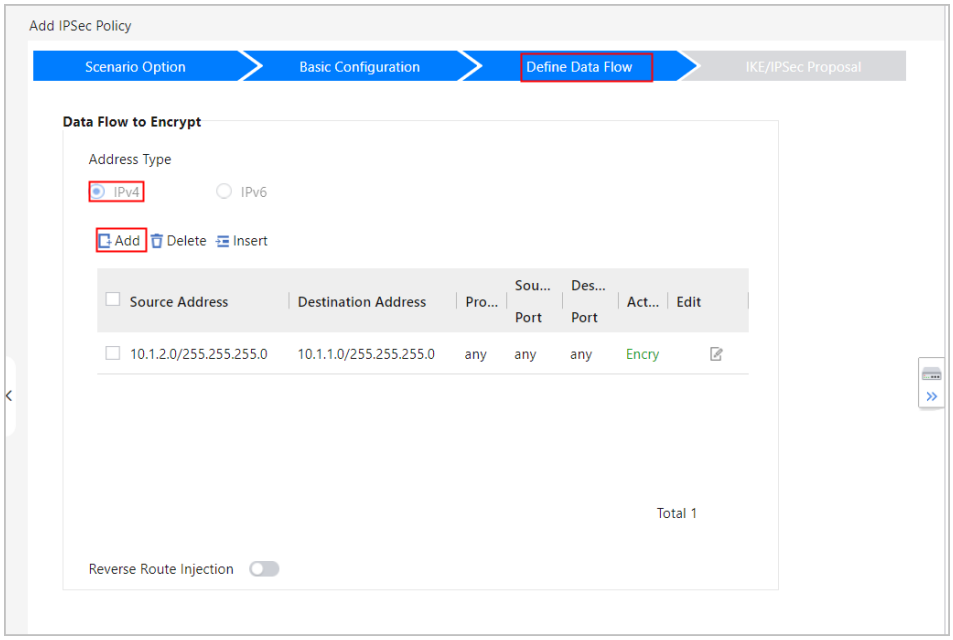
   b. Click **Add** to create an IPsec policy as prompted.



   The PSK is Hello123.

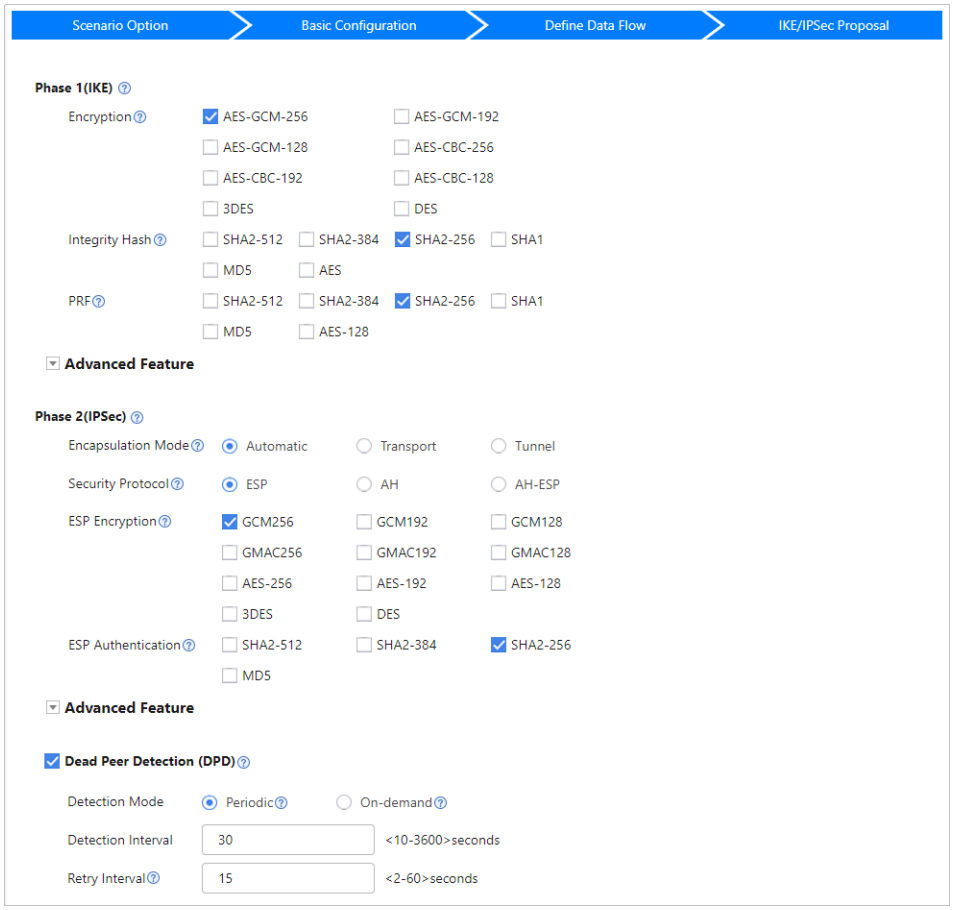
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

----End

Verifying the Configuration

1. Take DeviceA as an example. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. If "IKE negotiation succeeded" or "IPSec negotiation succeeded" is displayed in the **Status** column, the tunnel is successfully established.
2. Access a host on network B from a host on network A. The access succeeds.

Configuration Scripts

- DeviceA

```
#
acl ipv6 number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop28111627842
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ike peer ike281116278421
 pre-shared-key %^%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id 2001:DB8:6::1
 local-id 2001:DB8:5::1
 remote-address 2001:DB8:6::1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278421
 proposal prop28111627842
 tunnel local 2001:DB8:5::1
#
interface GE0/0/1
 ipv6 enable
 ip address 1.1.3.1 255.255.255.0
 ipv6 address 2001:DB8:5::1/64
 ipsec policy ipsec
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 10.1.2.0 255.255.255.0 GE0/0/1
#
ipv6 route-static 2001:DB8:6::0 64 2001:DB8:5::2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.3.0 mask 255.255.255.0
  source-address 2001:DB8:5::1 64
  destination-address 1.1.5.1 mask 255.255.255.0
  destination-address 2001:DB8:6::1 64
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 2001:DB8:6::1 64
  source-address 1.1.5.1 mask 255.255.255.0
  destination-address 2001:DB8:5::1 64
  destination-address 1.1.3.0 mask 255.255.255.0
  action permit
#
return
```

- DeviceB

 Copyright © Huawei Technologies Co., Ltd.

```
#
acl ipv6 number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop28111627844
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike281116278423
 pre-shared-key %^%#ljD3B%+u|Ci%<,Tk7FE*xzPWG:Y`$O1(oZVea8/S%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id 2001:DB8:5::1
 local-id 2001:DB8:6::1
 remote-address 2001:DB8:5::1
#
ipsec policy ipsec 1 isakmp
 security acl ipv6 3000
 ike-peer ike281116278423
 proposal prop28111627844
 tunnel local 2001:DB8:6::1
#
interface GE0/0/1
 ipv6 enable
 ip address 1.1.5.1 255.255.255.0
 ipv6 address 2001:DB8:6::1/64
 ipsec policy ipsec
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 10.1.1.0 255.255.255.0 GE0/0/1
#
ipv6 route-static 2001:DB8:5::0 64 2001:DB8:6::2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 mask 255.255.255.0
  source-address 2001:DB8:6::1 64
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-address 1.1.3.0 mask 255.255.255.0
 destination-address 2001:DB8:5::1 64
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.3.0 mask 255.255.255.0
 source-address 2001:DB8:5::1 64
 destination-address 1.1.5.1 mask 255.255.255.0
 destination-address 2001:DB8:6::1 64
 action permit
#
return
```

8.2 Communication Between LANs Through GRE over IPsec Tunnels

8.2.1 CLI: Example for Establishing a GRE over IPsec Tunnel Using ISAKMP

Networking Requirements

As shown in **Figure 8-16**, Network A and Network B are connected through DeviceA and DeviceB. Users on Network A need to securely access resources on Network B through a GRE tunnel. GRE cannot authenticate or encrypt packets. Therefore, IPsec needs to be configured to protect traffic from Network A to Network B.

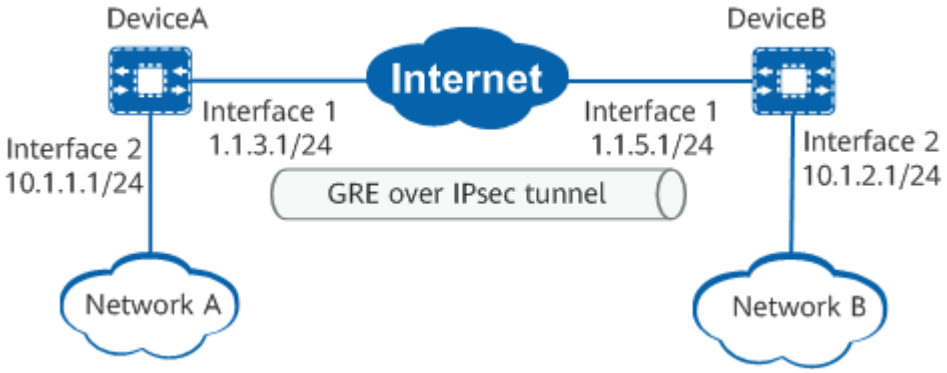
The networking requirements are as follows:

- Network A is in the network segment 10.1.1.0/24 and connects to DeviceA through interface 2.
- Network B is in the network segment 10.1.2.0/24 and connects to DeviceB through interface 2.
- DeviceA and DeviceB have reachable routes to each other.

Figure 8-16 GRE over IPsec networking

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data
DeviceA	Interface number: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	Interface number: GE 0/0/1 IP address: 1.1.3.1/24 Security zone: Untrust
	GRE tunnel interface configuration Source IP address: 1.1.3.1 Destination IP address: 1.1.5.1 IP address: any address that does not conflict with other IP addresses
	IPsec policy configuration Authentication type: Pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID: IP address
DeviceB	Interface number: GE 0/0/1 IP address: 1.1.5.1/24 Security zone: Untrust
	Interface number: GE 0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	GRE tunnel interface configuration Source IP address: 1.1.5.1 Destination IP address: 1.1.3.1 IP address: any address that does not conflict with other IP addresses
	IPsec policy configuration Authentication type: Pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID: IP address

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Perform basic interface configurations.
2. Configure security policies to allow devices on specified private network segments to exchange packets and allow IKE negotiation packets.
3. Configure static routes to ensure that there are reachable routes between both ends.
4. Configure a GRE tunnel interface and a forwarding route for the tunnel interface.
5. Configure ACL-based IPsec policies. In GRE over IPsec, the source and destination of the data flow to be protected by IPsec are the GRE tunnel source and destination addresses, respectively. Therefore, the source and destination IP addresses in the ACL on DeviceA are 1.1.3.1 and 1.1.5.1, respectively. The source and destination IP addresses in the ACL on DeviceB are 1.1.5.1 and 1.1.3.1, respectively.

Procedure

Step 1 Perform basic interface configurations on DeviceA.

1. Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.3.1 24
[DeviceA-GE0/0/1] quit
```

2. Add interfaces to security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Configure security policies to allow devices on specified private network segments to exchange packets and allow IKE negotiation packets.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy3] destination-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination IP addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Step 3 Configure a GRE tunnel interface on DeviceA.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] tunnel-protocol gre
[DeviceA-Tunnel1] ip address 2.1.1.1 24
[DeviceA-Tunnel1] source 1.1.3.1
[DeviceA-Tunnel1] destination 1.1.5.1
[DeviceA-Tunnel1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface tunnel 1
[DeviceA-zone-untrust] quit
```

NOTE

The IP address of the tunnel interface can be any idle IP address. When routes with the tunnel interface as the next hop need to be generated through dynamic routing protocols, the IP addresses of the interfaces at both ends of the GRE tunnel must belong to the same network segment.

Step 4 Configure a static route from DeviceA to Network B with the next hop Tunnel 1 and outbound interface GE 0/0/1. The following assumes that the next hop of the route with the outbound interface GE 0/0/1 is 1.1.3.2.

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 tunnel 1
[DeviceA] ip route-static 1.1.5.0 255.255.255.0 ge 0/0/1 1.1.3.2
```

Step 5 Configure an IPsec policy and apply it to an interface on DeviceA.

1. Create advanced ACL 3000, and configure a rule for packets whose source IP address is 1.1.3.1 and destination IP address is 1.1.5.1.

   ```
   [DeviceA] acl 3000
   [DeviceA-acl4-advance-3000] rule 5 permit ip source 1.1.3.1 0 destination 1.1.5.1 0
   [DeviceA-acl4-advance-3000] quit
   ```

   NOTE

   The source and destination IP addresses are those of Tunnel 1.

 Copyright © Huawei Technologies Co., Ltd.

2. Configure the IPsec proposal **tran1** and use the default parameter settings.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal and use the default parameter settings.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] remote-address 1.1.5.1
[DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-b] quit
```

5. Configure an IPsec policy using the IKE negotiation mode.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer b
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

6. Apply the IPsec policy **map1** to GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
[DeviceA] quit
```

Step 6 Perform basic interface configurations on DeviceB.

1. Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] ip address 10.1.2.1 24
[DeviceB-GE0/0/2] quit
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ip address 1.1.5.1 24
[DeviceB-GE0/0/1] quit
```

2. Add interfaces to security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Step 7 Configure interzone security policies.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy3] source-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy4] destination-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination IP addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Step 8 Configure a GRE tunnel interface on DeviceB.

```
[DeviceB] interface tunnel 1
[DeviceB-Tunnel1] tunnel-protocol gre
[DeviceB-Tunnel1] ip address 2.1.1.2 24
[DeviceB-Tunnel1] source 1.1.5.1
[DeviceB-Tunnel1] destination 1.1.3.1
[DeviceB-Tunnel1] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface tunnel 1
[DeviceB-zone-untrust] quit
```

NOTE

The IP address of the tunnel interface can be any idle IP address. When routes with the tunnel interface as the next hop need to be generated through dynamic routing protocols, the IP addresses of the interfaces at both ends of the GRE tunnel must belong to the same network segment.

Step 9 Configure a static route from DeviceB to Network A with the next hop Tunnel 1 and outbound interface GE 0/0/1. The following assumes that the next hop of the route with the outbound interface GE 0/0/1 is 1.1.5.2.

```
[DeviceB] ip route-static 1.1.3.0 255.255.255.0 ge 0/0/1 1.1.5.2
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 tunnel 1
```

Step 10 Configure an IPsec policy and apply it to an interface on DeviceB.

1. Create advanced ACL 3000, and configure a rule for packets whose source IP address is 1.1.5.1 and destination IP address is 1.1.3.1.

   ```
   [DeviceB] acl 3000
   [DeviceB-acl4-advance-3000] rule 5 permit ip source 1.1.5.1 0 destination 1.1.3.1 0
   [DeviceB-acl4-advance-3000] quit
   ```

   NOTE

   The source and destination IP addresses are those of Tunnel 1.

2. Configure the IPsec proposal **tran1** and use the default parameter settings.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal and use the default parameter settings.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method pre-share
   [DeviceB-ike-proposal-10] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

4. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] remote-address 1.1.3.1
[DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-a] quit
```

5. Configure an IPsec policy using the IKE negotiation mode.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

6. Apply the IPsec policy **map1** to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
[DeviceB] quit
```

----End

Verifying the Configuration

Users on Network A can successfully access Network B. Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB to check the establishment of IKE SAs and IPsec SAs. The following shows the command output of DeviceA. If information similar to the following is displayed, IKE SAs and IPsec SAs have been established.

```
<DeviceA> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU : 1
Total number of phase 2 SA in all CPU : 1

Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING

Slot 0, cpu 1 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
-------------------------------------------------------------------------------
 Conn-ID    Peer            VPN        Flag(s)       Phase  RemoteType  RemoteID
-------------------------------------------------------------------------------
 33554442   1.1.5.1/500                RD|A          v2:2   IP          1.1.5.1
 33554440   1.1.5.1/500                RD|ST|A       v2:1   IP          1.1.5.1
-------------------------------------------------------------------------------
<DeviceA> display ipsec sa
Slot 0, cpu 1 ipsec sa information:

===============================
Interface: GE0/0/1
===============================

  ----------------------------
  IPSec policy name: "map1"
  Sequence number  : 10
  Acl group        : 3000/IPv4
  Acl rule         : 5
  Mode             : ISAKMP
  ----------------------------
    Connection ID     : 33554456
    Encapsulation mode: Tunnel
    Holding time      : 0d 13h 30m 13s
    Tunnel local      : 1.1.3.1/500
    Tunnel remote     : 1.1.5.1/500
```

 Copyright © Huawei Technologies Co., Ltd.

```
Flow source      : 1.1.3.1/255.255.255.255 0/0-65535
Flow destination  : 1.1.5.1/255.255.255.255 0/0-65535

[Outbound ESP SAs]
  SPI: 10914757 (0xa68bc5)
  Proposal: ESP-ENCRYPT-AES-GCM-256
  SA remaining soft duration (kilobytes/sec): 0/512054
  SA remaining hard duration (kilobytes/sec): 0/602772
  Max sent sequence-number: 5
  UDP encapsulation used for NAT traversal: N
  SA encrypted packets (number/bytes): 5/540

[Inbound ESP SAs]
  SPI: 276363621 (0x1078f965)
  Proposal: ESP-ENCRYPT-AES-GCM-256
  SA remaining soft duration (kilobytes/sec): 0/530198
  SA remaining hard duration (kilobytes/sec): 0/602772
  Max received sequence-number: 5
  UDP encapsulation used for NAT traversal: N
  SA decrypted packets (number/bytes): 5/540
  Anti-replay : Enable
  Anti-replay window size: 1024
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 1.1.3.1 0 destination 1.1.5.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer b
  pre-shared-key %^%#o3Z7,b[Ox7Sc#r-f+WDC:D=s%^%#
  ike-proposal 10
  remote-address 1.1.5.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer b
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.3.1 255.255.255.0
 ipsec policy map1
#
interface Tunnel1
 ip address 2.1.1.1 255.255.255.0
 tunnel-protocol gre
 source 1.1.3.1
 destination 1.1.5.1
#
firewall zone trust
 set priority 85
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel 1
#
 ip route-static 10.1.2.0 255.255.255.0 tunnel 1
 ip route-static 1.1.5.0 255.255.255.0 GE 0/0/1 1.1.3.2
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    destination-address 10.1.2.0 mask 255.255.255.0
    action permit
  rule name policy2
    source-zone untrust
    destination-zone trust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 mask 255.255.255.0
    action permit
  rule name policy3
    source-zone local
    destination-zone untrust
    source-address 1.1.3.1 mask 255.255.255.255
    destination-address 1.1.5.1 mask 255.255.255.255
    action permit
  rule name policy4
    source-zone untrust
    destination-zone local
    source-address 1.1.5.1 mask 255.255.255.255
    destination-address 1.1.3.1 mask 255.255.255.255
    action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 1.1.5.1 0 destination 1.1.3.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer a
 pre-shared-key %^%#2@@y~:)7dX56AoVG1S@&0)Xf%^%#
 ike-proposal 10
 remote-address 1.1.3.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
 ipsec policy map1
#
interface Tunnel1
 ip address 2.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 1.1.5.1
 destination 1.1.3.1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel 1
#
 ip route-static 10.1.1.0 255.255.255.0 tunnel 1
 ip route-static 1.1.3.0 255.255.255.0 GE 0/0/1 1.1.5.2
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 mask 255.255.255.0
    action permit
  rule name policy2
    source-zone untrust
    destination-zone trust
    source-address 10.1.1.0 mask 255.255.255.0
    destination-address 10.1.2.0 mask 255.255.255.0
    action permit
  rule name policy3
    source-zone local
    destination-zone untrust
    source-address 1.1.5.1 mask 255.255.255.255
    destination-address 1.1.3.1 mask 255.255.255.255
    action permit
  rule name policy4
    source-zone untrust
    destination-zone local
    source-address 1.1.3.1 mask 255.255.255.255
    destination-address 1.1.5.1 mask 255.255.255.255
    action permit
#
return
```

8.2.2 CLI: Example for Establishing a GRE over IPsec Tunnel Using an IPsec Profile

Networking Requirements

As shown in **Figure 8-17**, Network A and Network B are connected through DeviceA and DeviceB. Users on Network A need to securely access resources on Network B through a GRE tunnel. GRE cannot authenticate or encrypt packets. Therefore, IPsec needs to be configured to protect traffic from Network A to Network B.

The networking requirements are as follows:

- Network A is in the network segment 10.1.1.0/24 and connects to DeviceA through interface 2.

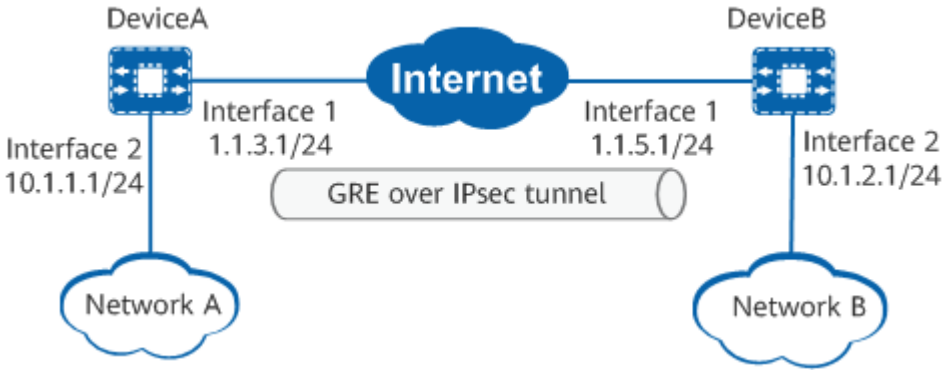
 Copyright © Huawei Technologies Co., Ltd.

- Network B is in the network segment 10.1.2.0/24 and connects to DeviceB through interface 2.
- DeviceA and DeviceB have reachable routes to each other.

Figure 8-17 GRE over IPsec networking

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data
DeviceA	Interface number: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	Interface number: GE 0/0/1 IP address: 1.1.3.1/24 Security zone: Untrust
	GRE tunnel interface configuration Source IP address: 1.1.3.1 Destination IP address: 1.1.5.1 IP address: any address that does not conflict with other IP addresses
	IPsec policy configuration Authentication type: Pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID: IP address
DeviceB	Interface number: GE 0/0/1 IP address: 1.1.5.1/24 Security zone: Untrust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	Interface number: GE 0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	GRE tunnel interface configuration Source IP address: 1.1.5.1 Destination IP address: 1.1.3.1 IP address: any address that does not conflict with other IP addresses
	IPsec policy configuration Authentication type: Pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID: IP address

Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The roadmap for configuring DeviceA is the same as that for configuring DeviceB.

1. Perform basic interface configurations.
2. Configure security policies to allow devices on specified private network segments to exchange packets and allow IKE negotiation packets.
3. Configure static routes to ensure that there are reachable routes between both ends.
4. Configure a GRE tunnel interface and a forwarding route for the tunnel interface to direct the data flows to be protected by IPsec to the interface.
5. Configure an IPsec profile.

Procedure

Step 1 Perform basic interface configurations on DeviceA.

1. Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.3.1 24
[DeviceA-GE0/0/1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

2. Add interfaces to security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Configure security policies to allow devices on specified private network segments to exchange packets and allow IKE negotiation packets.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy3] destination-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination IP addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Step 3 Configure a GRE tunnel interface on DeviceA.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] tunnel-protocol gre
[DeviceA-Tunnel1] ip address 2.1.1.1 24
[DeviceA-Tunnel1] source 1.1.3.1
[DeviceA-Tunnel1] destination 1.1.5.1
[DeviceA-Tunnel1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface tunnel 1
[DeviceA-zone-untrust] quit
```

NOTE

The IP address of the tunnel interface can be any idle IP address. When routes with the tunnel interface as the next hop need to be generated through dynamic routing protocols, the IP addresses of the interfaces at both ends of the GRE tunnel must belong to the same network segment.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure a static route from DeviceA to Network B. The following assumes that the next hop of the route with the outbound interface GE 0/0/1 is 1.1.3.2. Configure a forwarding route for the tunnel interface to direct the data flows to be protected by IPsec to the interface.

```
[DeviceA] ip route-static 1.1.5.0 255.255.255.0 ge 0/0/1 1.1.3.2
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 tunnel 1
```

Step 5 Configure an IPsec profile and apply it to the tunnel interface.

1. Configure an IPsec proposal. You do not need to set default parameters.

   ```
   [DeviceA] ipsec proposal tran1
   [DeviceA-ipsec-proposal-tran1] quit
   ```

2. Configure an IKE proposal. You do not need to set default parameters.

   ```
   [DeviceA] ike proposal 10
   [DeviceA-ike-proposal-10] authentication-method pre-share
   [DeviceA-ike-proposal-10] quit
   ```

3. Configure an IKE peer.

   ```
   [DeviceA] ike peer b
   [DeviceA-ike-peer-b] ike-proposal 10
   [DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
   [DeviceA-ike-peer-b] quit
   ```

4. Configure an IPsec profile.

   ```
   [DeviceA] ipsec profile pro1
   [DeviceA-ipsec-profile-pro1] proposal tran1
   [DeviceA-ipsec-profile-pro1] ike-peer b
   [DeviceA-ipsec-profile-pro1] quit
   ```

5. Apply the IPsec profile **pro1** to the tunnel interface.

   ```
   [DeviceA] interface tunnel 1
   [DeviceA-Tunnel1] ipsec profile pro1
   [DeviceA-Tunnel1] quit
   [DeviceA] quit
   ```

Step 6 Perform basic interface configurations on DeviceB.

1. Configure IP addresses for interfaces.

   ```
   <HUAWEI> system-view
   [HUAWEI] sysname DeviceB
   [DeviceB] interface ge 0/0/2
   [DeviceB-GE0/0/2] ip address 10.1.2.1 24
   [DeviceB-GE0/0/2] quit
   [DeviceB] interface ge 0/0/1
   [DeviceB-GE0/0/1] ip address 1.1.5.1 24
   [DeviceB-GE0/0/1] quit
   ```

2. Add interfaces to security zones.

   ```
   [DeviceB] firewall zone trust
   [DeviceB-zone-trust] add interface ge 0/0/2
   [DeviceB-zone-trust] quit
   [DeviceB] firewall zone untrust
   [DeviceB-zone-untrust] add interface ge 0/0/1
   [DeviceB-zone-untrust] quit
   ```

Step 7 Configure interzone security policies.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy4] destination-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination IP addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Step 8 Configure a GRE tunnel interface on DeviceB.

```
[DeviceB] interface tunnel 1
[DeviceB-Tunnel1] tunnel-protocol gre
[DeviceB-Tunnel1] ip address 2.1.1.2 24
[DeviceB-Tunnel1] source 1.1.5.1
[DeviceB-Tunnel1] destination 1.1.3.1
[DeviceB-Tunnel1] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface tunnel 1
[DeviceB-zone-untrust] quit
```

NOTE

The IP address of the tunnel interface can be any idle IP address. When routes with the tunnel interface as the next hop need to be generated through dynamic routing protocols, the IP addresses of the interfaces at both ends of the GRE tunnel must belong to the same network segment.

Step 9 Configure a static route from DeviceB to Network A. The following assumes that the next hop of the route with the outbound interface GE 0/0/1 is 1.1.5.2. Configure a forwarding route for the tunnel interface to direct the data flows to be protected by IPsec to the interface.

```
[DeviceB] ip route-static 1.1.3.0 255.255.255.0 ge 0/0/1 1.1.5.2
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 Tunnel1
```

Step 10 Configure an IPsec profile and apply it to the tunnel interface.

1. Configure an IPsec proposal. You do not need to set default parameters.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] quit
   ```

2. Configure an IKE proposal. You do not need to set default parameters.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method pre-share
   [DeviceB-ike-proposal-10] quit
   ```

 Copyright © Huawei Technologies Co., Ltd.

3. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-b] ike-proposal 10
[DeviceB-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-b] quit
```

4. Configure an IPsec profile.

```
[DeviceB] ipsec profile pro1
[DeviceB-ipsec-profile-pro1] proposal tran1
[DeviceB-ipsec-profile-pro1] ike-peer a
[DeviceB-ipsec-profile-pro1] quit
```

5. Apply the IPsec profile **pro1** to the tunnel interface.

```
[DeviceB] interface tunnel 1
[DeviceB-Tunnel1] ipsec profile pro1
[DeviceB-Tunnel1] quit
[DeviceB] quit
```

----End

Verifying the Configuration

Users on Network A can successfully access Network B. Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB to check the establishment of IKE SAs and IPsec SAs. The following shows the command output of DeviceA. If information similar to the following is displayed, IKE SAs and IPsec SAs have been established.

```
<DeviceA> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU : 1
Total number of phase 2 SA in all CPU : 1

Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING

Slot 0, cpu 1 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
-------------------------------------------------------------------------------
 Conn-ID    Peer            VPN        Flag(s)       Phase  RemoteType  RemoteID
-------------------------------------------------------------------------------
 33554442   1.1.5.1/500                RD|A          v2:2   IP          1.1.5.1
 33554440   1.1.5.1/500                RD|ST|A       v2:1   IP          1.1.5.1
-------------------------------------------------------------------------------
<DeviceA> display ipsec sa
Slot 0, cpu 1 ipsec sa information:

===============================
Interface: GE0/0/1
===============================

  ----------------------------
  IPSec policy name: "map1"
  Sequence number  : 10
  Acl group        : 3000/IPv4
  Acl rule         : 5
  Mode             : ISAKMP
  ----------------------------
    Connection ID     : 33554456
    Encapsulation mode: Tunnel
    Holding time      : 0d 13h 30m 13s
    Tunnel local      : 1.1.3.1/500
    Tunnel remote     : 1.1.5.1/500
    Flow source       : 1.1.3.1/255.255.255.255 0/0-65535
    Flow destination  : 1.1.5.1/255.255.255.255 0/0-65535
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Outbound ESP SAs]
  SPI: 10914757 (0xa68bc5)
  Proposal: ESP-ENCRYPT-AES-GCM-256
  SA remaining soft duration (kilobytes/sec): 0/512054
  SA remaining hard duration (kilobytes/sec): 0/602772
  Max sent sequence-number: 5
  UDP encapsulation used for NAT traversal: N
  SA encrypted packets (number/bytes): 5/540

[Inbound ESP SAs]
  SPI: 276363621 (0x1078f965)
  Proposal: ESP-ENCRYPT-AES-GCM-256
  SA remaining soft duration (kilobytes/sec): 0/530198
  SA remaining hard duration (kilobytes/sec): 0/602772
  Max received sequence-number: 5
  UDP encapsulation used for NAT traversal: N
  SA decrypted packets (number/bytes): 5/540
  Anti-replay : Enable
  Anti-replay window size: 1024
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer b
  pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!0wh:W'|^cWVEaw==)"2Zwo_o2GIV8LeaRb>!!!!!2jp5!!!!!!9!!!!
NI4E((n_/HFtL35tXwpVh+h#IMXhhW!!!!!!!!!!%+%#
  ike-proposal 10
#
ipsec profile pro1
 ike-peer b
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.3.1 255.255.255.0
#
interface Tunnel1
 ip address 2.1.1.1 255.255.255.0
 tunnel-protocol gre
 source 1.1.3.1
 destination 1.1.5.1
 ipsec profile pro1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 ip route-static 10.1.2.0 255.255.255.0 tunnel 1
 ip route-static 1.1.5.0 255.255.255.0 GE 0/0/1 1.1.3.2
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    destination-address 10.1.2.0 mask 255.255.255.0
    action permit
  rule name policy2
    source-zone untrust
    destination-zone trust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 mask 255.255.255.0
    action permit
  rule name policy3
    source-zone local
    destination-zone untrust
    source-address 1.1.3.1 mask 255.255.255.255
    destination-address 1.1.5.1 mask 255.255.255.255
    action permit
  rule name policy4
    source-zone untrust
    destination-zone local
    source-address 1.1.5.1 mask 255.255.255.255
    destination-address 1.1.3.1 mask 255.255.255.255
    action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!0wh:W'|^cWVEaw==)"2Zwo_o2GIV8LeaRb>!!!!!2jp5!!!!!!9!!!!
NI4E((n_/HFtL35tXwpVh+h#IMXhhW!!!!!!!!!!%+%#
 ike-proposal 10
#
ipsec profile pro1
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
#
interface Tunnel1
 ip address 2.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 1.1.5.1
 destination 1.1.3.1
 ipsec profile pro1
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface tunnel 1
#
 ip route-static 10.1.1.0 255.255.255.0 Tunnel 1
 ip route-static 1.1.3.0 255.255.255.0 GE 0/0/1 1.1.5.2
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 mask 255.255.255.0
    action permit
  rule name policy2
    source-zone untrust
    destination-zone trust
    source-address 10.1.1.0 mask 255.255.255.0
    destination-address 10.1.2.0 mask 255.255.255.0
    action permit
  rule name policy3
    source-zone local
    destination-zone untrust
    source-address 1.1.5.1 mask 255.255.255.255
    destination-address 1.1.3.1 mask 255.255.255.255
    action permit
  rule name policy4
    source-zone untrust
    destination-zone local
    source-address 1.1.3.1 mask 255.255.255.255
    destination-address 1.1.5.1 mask 255.255.255.255
    action permit
#
return
```

8.3 IPsec in NAT Scenarios

8.3.1 CLI: Example for Establishing an IPsec Tunnel in a NAT Scenario (NAT Is Performed by the Headquarters Gateway)

Networking Requirements

On the network shown in **Figure 8-18**:

- The HQ belongs to the subnet 10.1.1.0/24 and is connected to DeviceA through GE 0/0/1.
- The branch belongs to the subnet 10.1.2.0/24 and is connected to DeviceC through GE 0/0/1.
- There are reachable routes between DeviceA and DeviceC.
- DeviceB is a NAT gateway. Branch users can access the HQ only through the NAT gateway.

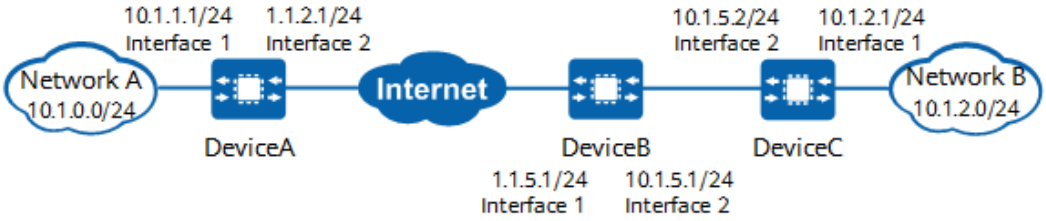
Employees at the branch need to access the servers at the HQ. The information obtained from the servers is confidential and needs to be encrypted for secure transmission over the Internet through an IPsec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-18 Network diagram for establishing an IPsec tunnel in a NAT scenario

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 of DeviceA, respectively.



Item	Data
DeviceA	Interface: GE 0/0/1 IP address: 10.1.1.1/24 Security zone: Trust
	Interface: GE 0/0/2 IP address: 1.1.2.1/24 Security zone: Untrust
	IPsec configuration Remote address: 2.2.2.2 Authentication mode: PSK authentication PSK: YsHsjx_202206 Remote ID type: any
DeviceB	Interface: GE 0/0/1 IP address: 1.1.5.1/24 Security zone: Trust
	Interface: GE 0/0/2 IP address: 10.1.5.1/24 Security zone: Untrust
	NAT configuration Easy IP
DeviceC	Interface: GE 0/0/1 IP address: 2.2.2.2/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote address: 1.1.1.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceC must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

- If there is a NAT device between the HQ and branch, configure a template IPsec policy at the HQ and do not specify the peer IP address when configuring an IKE peer.
- When configuring an IPsec proposal, retain the default security protocol, Encapsulating Security Payload (ESP).

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the private network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the public network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.2.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.2.1 32
[DeviceA-policy-security-rule-policy3] destination-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.2.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure static routes on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.2.2.

Configure a static route to DeviceC to divert tunnel negotiation packets.

```
[DeviceA] ip route-static 10.1.5.0 255.255.255.0 1.1.2.2
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a static route to network B to divert encrypted data packets transmitted through the tunnel.

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 1.1.2.2
```

Step 4 Configure an ISAKMP IPsec policy on DeviceA and apply an IPsec policy to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.2.0/24.

```
[DeviceA] acl 3000
[DeviceA-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl4-advance-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceA] ike peer c
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-b] quit
```

5. Configure an IPsec policy.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer c
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

6. Apply the IPsec policy to GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipsec policy map1
[DeviceA-GE0/0/2] quit
```

Step 5 Configure public and private network interfaces on DeviceC, and add the interfaces to security zones.

Configure the private network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] undo portswitch
[DeviceC-GE0/0/1] ip address 10.1.2.1 24
[DeviceC-GE0/0/1] quit
```

Configure the interface GE 0/0/2 connected to the NAT gateway.

```
[DeviceC] interface ge 0/0/2
[DeviceC-GE0/0/2] undo portswitch
[DeviceC-GE0/0/2] ip address 10.1.5.2 24
[DeviceC-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Add GE 0/0/1 to the Trust zone.

```
[DeviceC] firewall zone trust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceC] firewall zone untrust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
```

Step 6 Configure security policies on DeviceC to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy1
[DeviceC-policy-security-rule-policy1] source-zone trust
[DeviceC-policy-security-rule-policy1] destination-zone untrust
[DeviceC-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceC-policy-security-rule-policy1] action permit
[DeviceC-policy-security-rule-policy1] quit
[DeviceC-policy-security] rule name policy2
[DeviceC-policy-security-rule-policy2] source-zone untrust
[DeviceC-policy-security-rule-policy2] destination-zone trust
[DeviceC-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceC-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy2] action permit
[DeviceC-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceC-policy-security] rule name policy3
[DeviceC-policy-security-rule-policy3] source-zone local
[DeviceC-policy-security-rule-policy3] destination-zone untrust
[DeviceC-policy-security-rule-policy3] source-address 10.1.5.2 32
[DeviceC-policy-security-rule-policy3] destination-address 1.1.2.1 32
[DeviceC-policy-security-rule-policy3] action permit
[DeviceC-policy-security-rule-policy3] quit
[DeviceC-policy-security] rule name policy4
[DeviceC-policy-security-rule-policy4] source-zone untrust
[DeviceC-policy-security-rule-policy4] destination-zone local
[DeviceC-policy-security-rule-policy4] source-address 1.1.2.1 32
[DeviceC-policy-security-rule-policy4] destination-address 10.1.5.2 32
[DeviceC-policy-security-rule-policy4] action permit
[DeviceC-policy-security-rule-policy4] quit
[DeviceC-policy-security] quit
```

Step 7 Configure static routes on DeviceC to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Assume that the next-hop IP address of the route from DeviceC to the Internet is 2.2.2.254.

Configure a static route to DeviceA to divert tunnel negotiation packets.

```
[DeviceC] ip route-static 1.1.2.0 255.255.255.0 10.1.5.1
```

Configure a static route to network A to divert encrypted data packets transmitted through the tunnel.

```
[DeviceC] ip route-static 10.1.1.0 255.255.255.0 10.1.5.1
```

Step 8 Configure an ISAKMP IPsec policy on DeviceC and apply an IPsec policy to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.0.0/24.

```
[DeviceC] acl 3000
[DeviceC-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceC-acl4-advance-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceC] ipsec proposal tran1
[DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceC-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceC] ike proposal 10
[DeviceC-ike-proposal-10] authentication-method pre-share
[DeviceC-ike-proposal-10] prf hmac-sha2-256
[DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceC-ike-proposal-10] dh group14
[DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceC-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceC] ike peer a
[DeviceC-ike-peer-a] ike-proposal 10
[DeviceC-ike-peer-a] remote-address 1.1.2.1
[DeviceC-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceC-ike-peer-a] quit
```

5. Configure an IPsec policy.

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

6. Apply the IPsec policy to GE 0/0/2.

```
[DeviceC] interface ge 0/0/2
[DeviceC-GE0/0/2] ipsec policy map1
[DeviceC-GE0/0/2] quit
```

Step 9 Configure interfaces GE 0/0/1 and GE 0/0/2 on DeviceB (NAT gateway), and add GE 0/0/1 and GE 0/0/2 to the Trust zone and Untrust zone respectively. For details, see the configurations of DeviceA and DeviceC.

Step 10 Configure security policies on DeviceB (NAT gateway) to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.5.2 32
[DeviceB-policy-security-rule-policy1] destination-address 1.1.2.1 32
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 1.1.2.1 32
[DeviceB-policy-security-rule-policy2] destination-address 10.1.5.2 32
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
[DeviceB-policy-security] quit
```

Step 11 Configure a NAT policy on DeviceB.

```
[DeviceB] nat-policy
[DeviceB-policy-nat] rule name policy_nat1
[DeviceB-policy-nat-rule-policy_nat1] source-zone trust
[DeviceB-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceB-policy-nat-rule-policy_nat1] source-address 10.1.5.0 24
[DeviceB-policy-nat-rule-policy_nat1] action source-nat easy-ip
[DeviceB-policy-nat-rule-policy_nat1] quit
[DeviceB-policy-nat] quit
```

Step 12 Configure static routes from DeviceB (NAT gateway) to the branch network and HQ network.

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.5.2
[DeviceB] ip route-static 10.1.2.0 255.255.255.0 10.1.5.2
[DeviceB] ip route-static 1.1.2.0 255.255.255.0 ge 0/0/1
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on a device in the protected network segment of network A or network B to trigger IKE negotiation.

   If IKE negotiation succeeds, devices in the protected network segments at both ends of the tunnel can ping each other successfully. Otherwise, IKE negotiation fails.

2. The device on network B can ping the IP address 1.1.2.1 of GE 0/0/1 on DeviceA, and NAT session entries can be viewed on DeviceB.

   ```
   <DeviceB> display firewall session table
    Current Total Sessions : 2
    udp  VPN:public --> public 10.1.5.2:500[1.1.5.1:2048]-->1.1.2.1:500
    udp  VPN:public --> public 10.1.5.2:4500[1.1.5.1:2048]-->1.1.2.1:4500
   ```

3. On DeviceA and DeviceC, run the **display ike sa** and **display ipsec sa** commands to check SA establishment information. The following example uses the command output on DeviceC, which shows that IKE SAs and IPsec SAs have been established successfully.

   ```
   <DeviceB> display ike sa
   IKE SA information :
     Conn-ID     Peer          VPN   Flag(s)  Phase  RemoteType  RemoteID
   -------------------------------------------------------------------------
     16777239    1.1.5.1:500         RD|ST|A  v2:2   IP          1.1.5.1
     16777232    1.1.5.1:500         RD|ST|A  v2:1   IP          1.1.5.1

   Number of IKE SA : 2
   -------------------------------------------------------------------------
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer c
  pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
  ike-proposal 10
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer c
 proposal tran1
#
interface GE0/0/2
 ip address 1.1.2.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 10.1.2.0 255.255.255.0 1.1.2.2
 ip route-static 10.1.5.0 255.255.255.0 1.1.2.2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-address 1.1.2.1 mask 255.255.255.255
 destination-address 1.1.5.1 mask 255.255.255.255
 action permit
 rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.5.1 mask 255.255.255.255
 destination-address 1.1.2.1 mask 255.255.255.255
 action permit
#
return
```

- Device B (NAT gateway)

```
#
 sysname DeviceB
#
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.5.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
ip route-static 10.1.1.0 255.255.255.0 1.1.5.2
ip route-static 10.1.2.0 255.255.255.0 10.1.5.2
ip route-static 1.1.2.0 255.255.255.0 GE0/0/1
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.5.2 mask 255.255.255.255
    destination-address 1.1.2.1 mask 255.255.255.255
    action permit
  rule name policy2
    source-zone untrust
    destination-zone trust
    source-address 1.1.2.1 mask 255.255.255.255
    destination-address 10.1.5.2 mask 255.255.255.255
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.5.0 24
    action source-nat easy-ip
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.2.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.5.2 255.255.255.0
 ipsec policy map1
#
interface GE0/0/1
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 1.1.2.0 255.255.255.0 10.1.5.1
 ip route-static 10.1.1.0 255.255.255.0 10.1.5.1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 10.1.5.2 mask 255.255.255.255
  destination-address 1.1.2.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.2.1 mask 255.255.255.255
  destination-address 10.1.5.2 mask 255.255.255.255
  action permit
#
return
```

8.3.2 Web: Example for Establishing an IPsec Tunnel in a NAT Scenario (NAT Is Performed by Each Branch's Gateway)

Networking Requirements

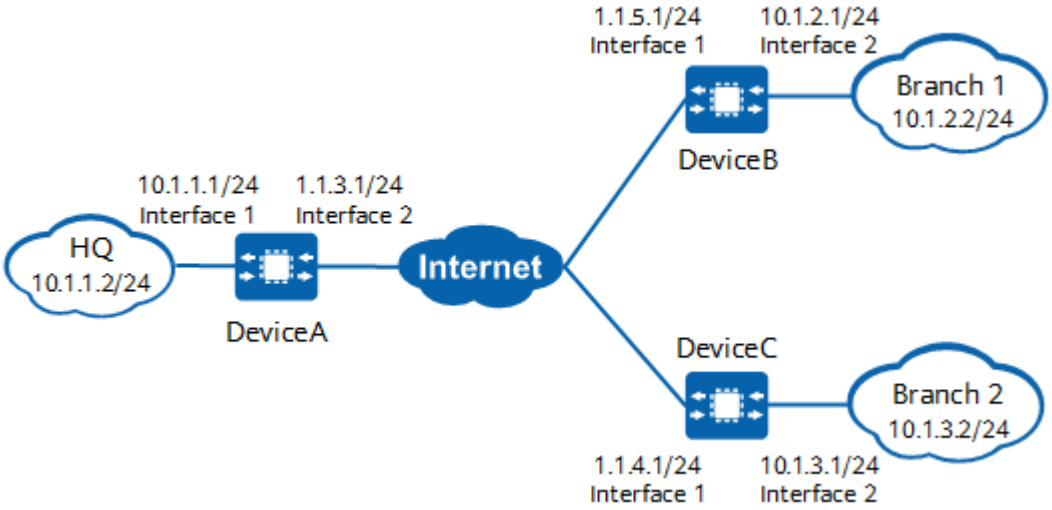
In Figure 1, an enterprise has the HQ and two branches (branch 1 and branch 2).

Employees at the branches need to access the servers at the HQ. The information obtained from the servers is confidential and needs to be encrypted for secure transmission over the Internet through an IPsec tunnel. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not. Therefore, distinguish the data flows when configuring NAT.

Figure 8-19 Establishing an IPsec tunnel in a NAT scenario (NAT is performed by each branch's gateway)

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data
DeviceA	Private network interface: GE0/0/1 IP address: 10.1.1.1/24 Security zone: Trust
	Public network interface: GE0/0/2 IP address: 1.1.3.1/24 Security zone: Untrust
	IPsec configuration Scenario: point-to-multipoint Peer IP address: not configured Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Peer ID: any peer ID

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	NAT configuration • Name: policy_nat1 Source IP address: 10.1.1.0/24 Destination IP address: 10.1.2.0/24 Destination IP address: 10.1.3.0/24 Action: no-nat • Name: policy_nat2 Source IP address: 10.1.1.0/24 Action: easy-ip
DeviceB	Interface number: GE0/0/1 IP address: 1.1.5.1/24 Security zone: Untrust
	Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	IPsec configuration Scenario: point-to-point Remote address: 1.1.3.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Peer ID: any peer ID
	NAT configuration • Name: policy_nat1 Source IP address: 10.1.2.0/24 Destination IP address: 10.1.1.0/24 Destination IP address: 10.1.3.0/24 Action: no-nat • Name: policy_nat2 Source IP address: 10.1.2.0/24 Action: easy-ip
DeviceC	Interface number: GE0/0/1 IP address: 1.1.4.1/24 Security zone: Untrust
	Interface number: GE0/0/2 IP address: 10.1.3.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote address: 1.1.3.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Peer ID: any peer ID
	NAT configuration • Name: policy_nat1 Source IP address: 10.1.3.0/24 Destination IP address: 10.1.1.0/24 Destination IP address: 10.1.2.0/24 Action: no-nat • Name: policy_nat2 Source IP address: 10.1.3.0/24 Action: easy-ip

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceC must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
3. Configure static routes to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
4. Configure an IPsec policy.
5. Configure source NAT. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not. Therefore, you need to configure different actions in a NAT policy to distinguish the data flows.

Procedure

Step 1 Configure the private network interface GE0/0/1 and public network interface GE0/0/2 on DeviceA, and add the interfaces to security zones.

1. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

2. Click corresponding to GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	Trust
IPv4	
IP Address	10.1.1.1/24

3. Repeat the preceding steps to set parameters for GE0/0/2.

Zone	Untrust
IPv4	
IP Address	1.1.3.1/24

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted. Click **OK**.

Name	policy1
Source Zone	Trust
Destination Zone	Untrust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24, 10.1.3.0/24
Action	Permit

Name	policy2
Source Zone	Untrust
Destination Zone	Trust
Source Address	10.1.2.0/24, 10.1.3.0/24
Destination Address	10.1.1.0/24
Action	Permit

3. Configure security policies between the Local and Untrust zones by referring to the preceding steps to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	1.1.3.1/32
Destination Address	1.1.4.1/32, 1.1.5.1/32
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.4.1/32, 1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

Step 3 Configure a default static route on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

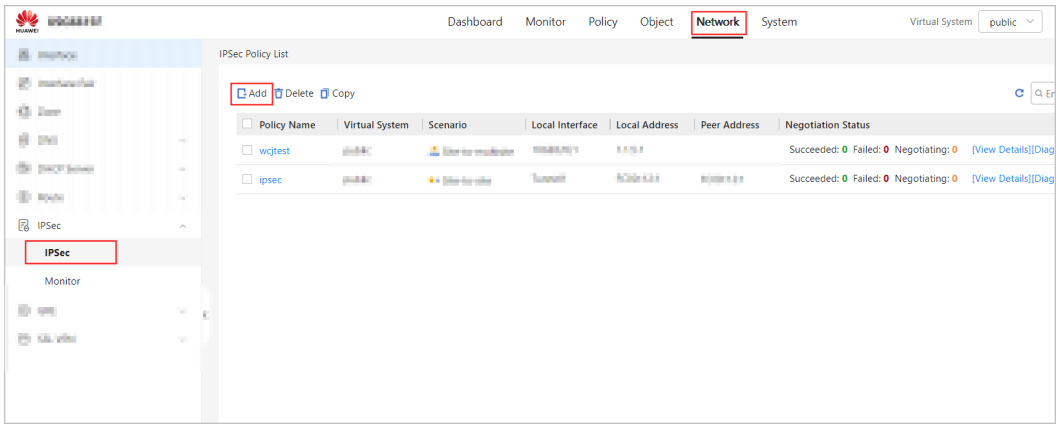
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. The following assumes that the next-hop IP address to the public network is 1.1.3.254. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0
Next Hop	1.1.3.254

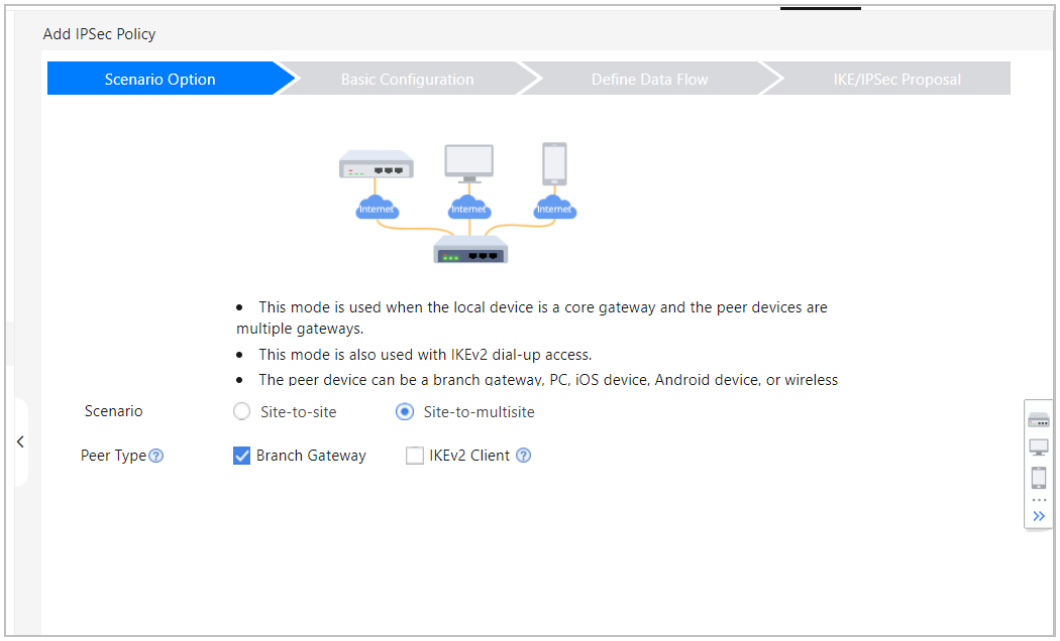
Step 4 Configure an IPsec policy on DeviceA and apply the corresponding IPsec policy group to GE0/0/2.

1. Choose **Network** > **IPSec** > **IPSec**.

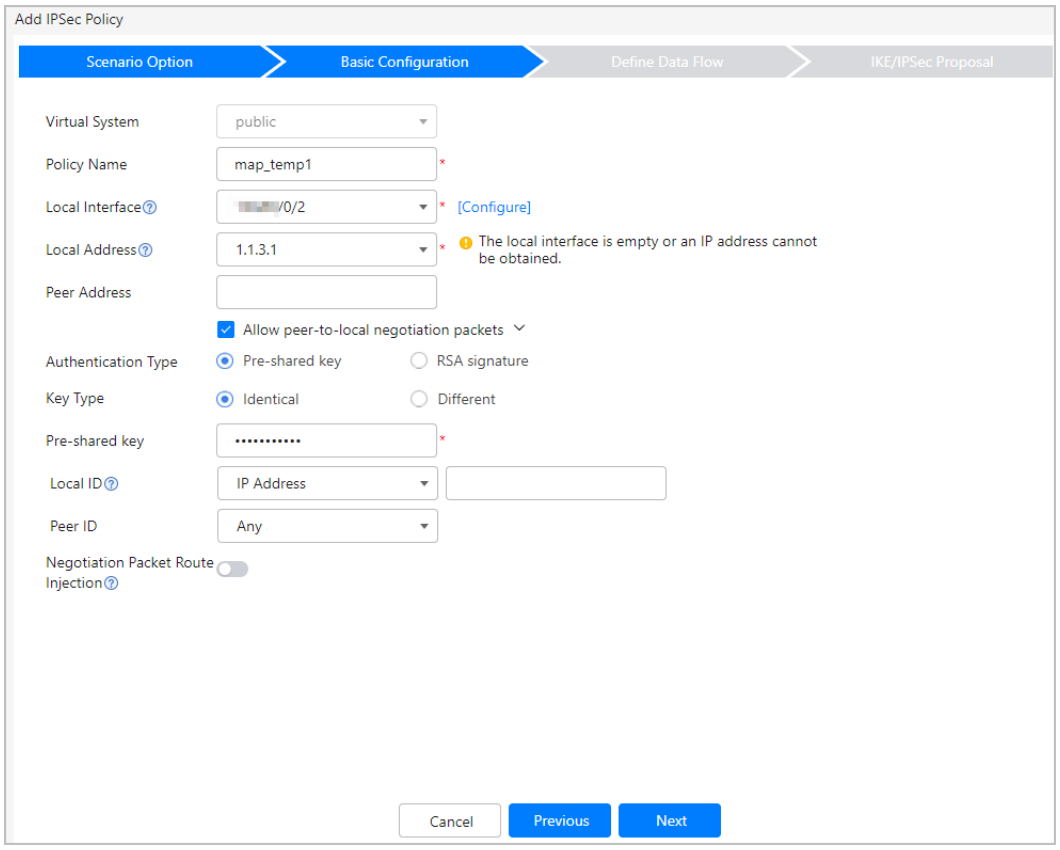
 Copyright © Huawei Technologies Co., Ltd.

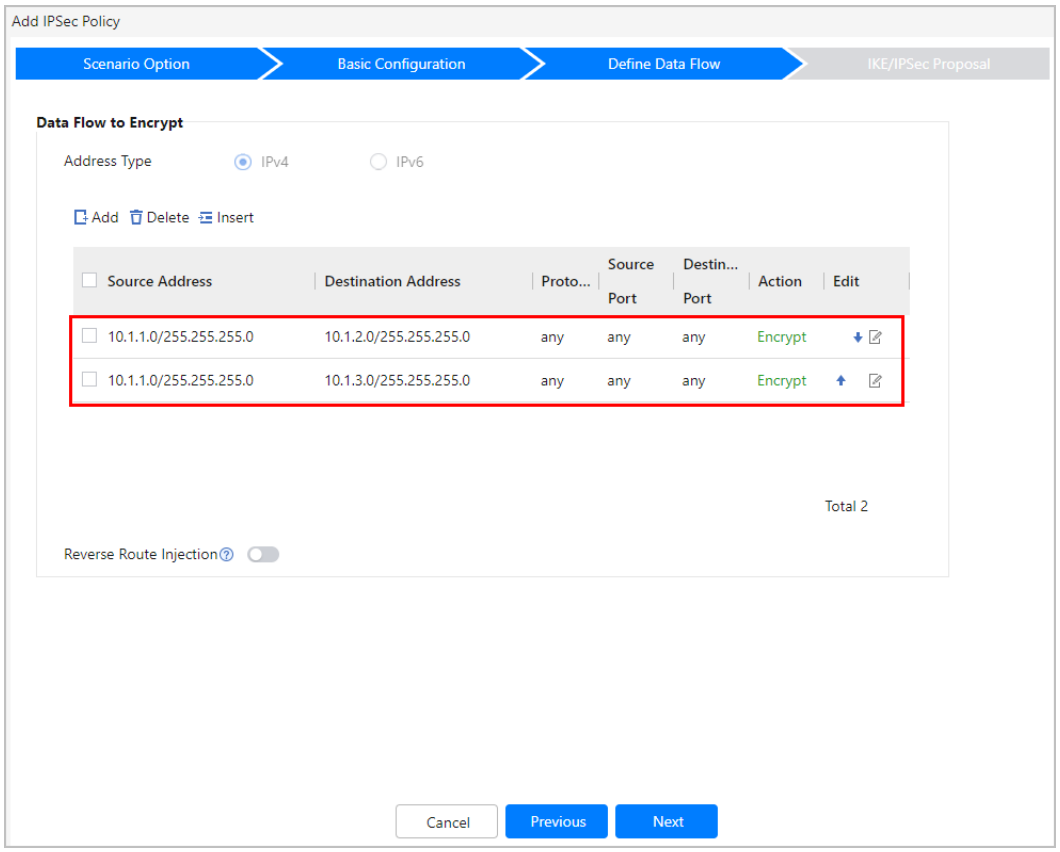


2. Click **Add** to create an IPsec policy as prompted.

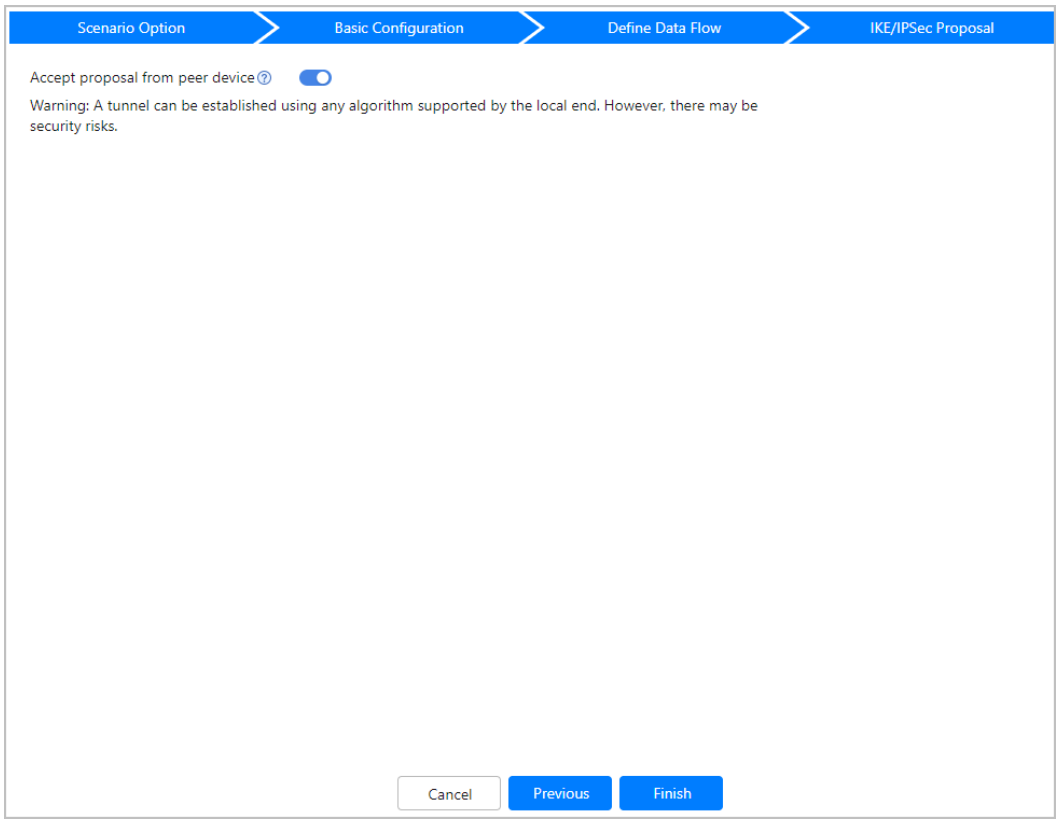


 Copyright © Huawei Technologies Co., Ltd.



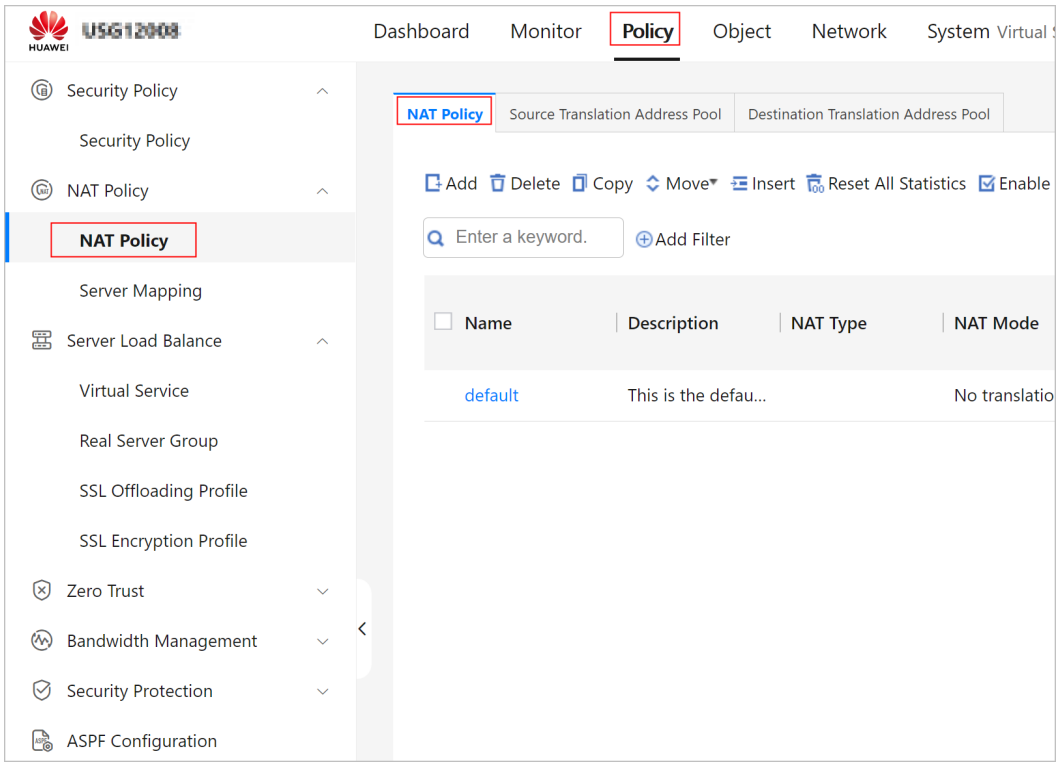


 Copyright © Huawei Technologies Co., Ltd.

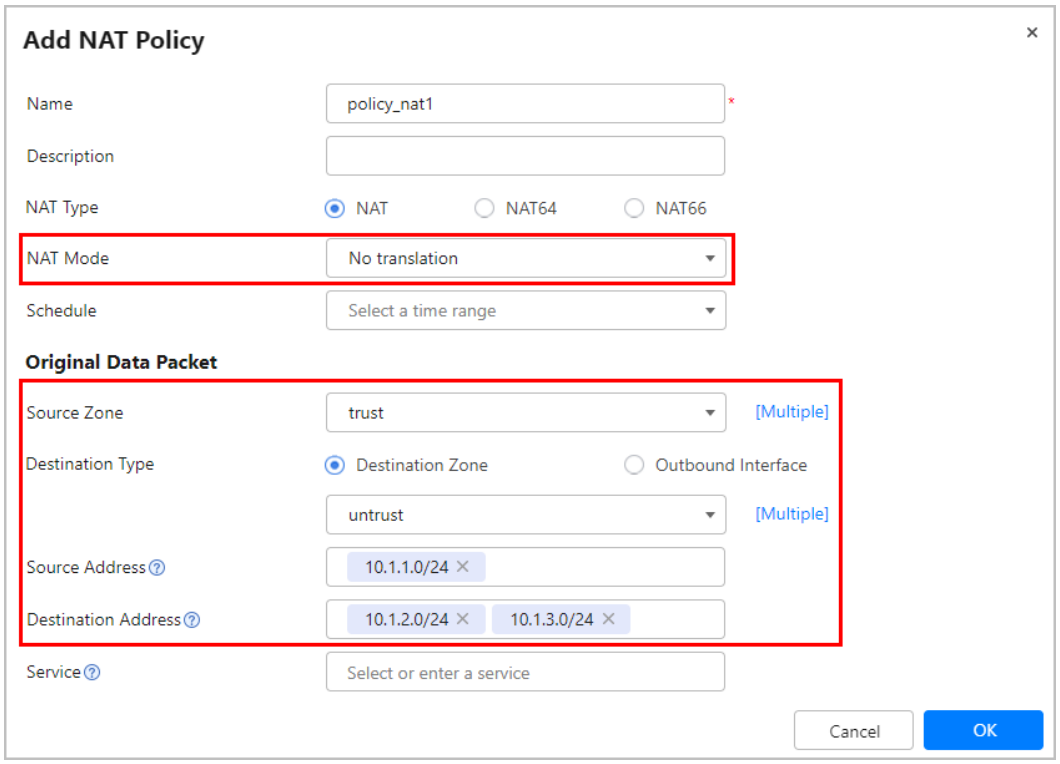


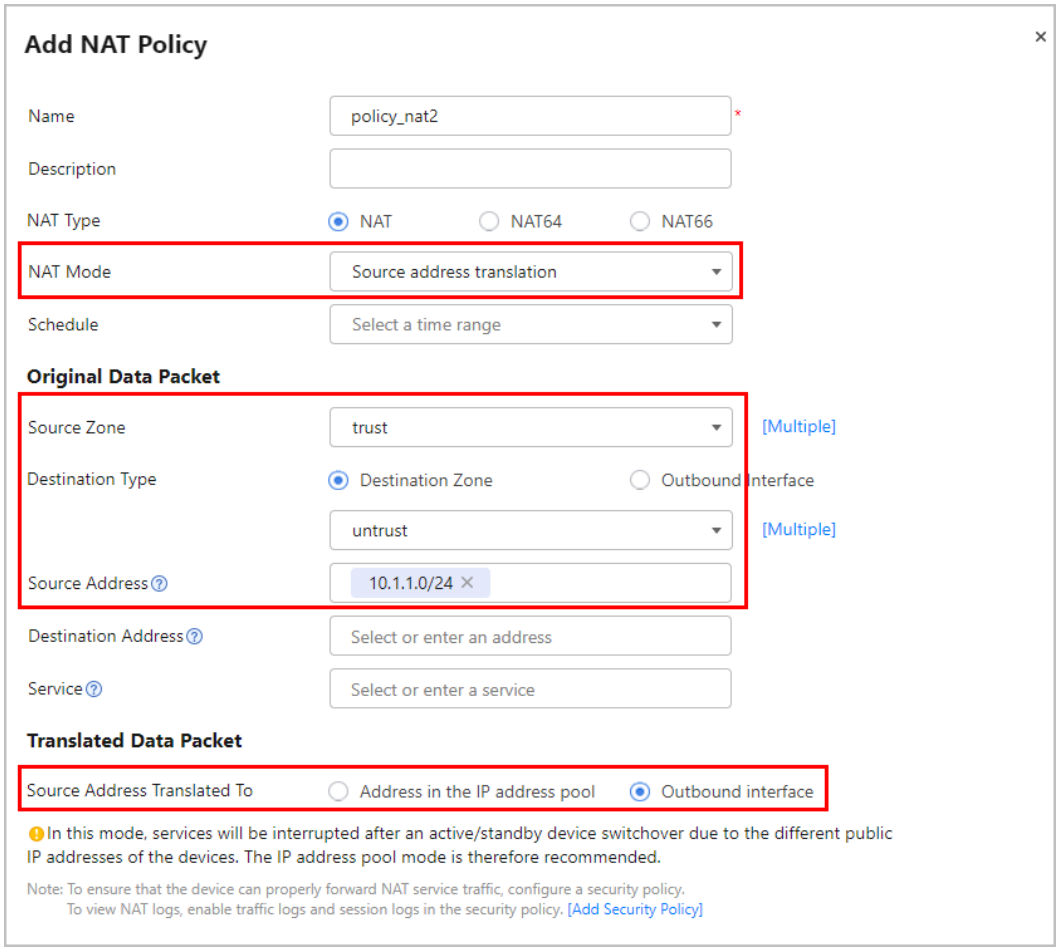
Step 5 Configure NAT on DeviceA. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



2. Click **Add** and configure a NAT policy as follows:





 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure the private network interface GE0/0/2 and public network interface GE0/0/1 on DeviceB, and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.5.1/24

3. Repeat the preceding steps to set parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

Step 7 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24, 10.1.3.0/24
Action	Permit

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.1.0/24, 10.1.3.0/24
Destination Address	10.1.2.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

3. Configure security policies between the Local and Untrust zones by referring to the preceding steps to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Name	policy3
Source Zone	local
Destination Zone	unrtust
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

Step 8 Configure a default static route on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

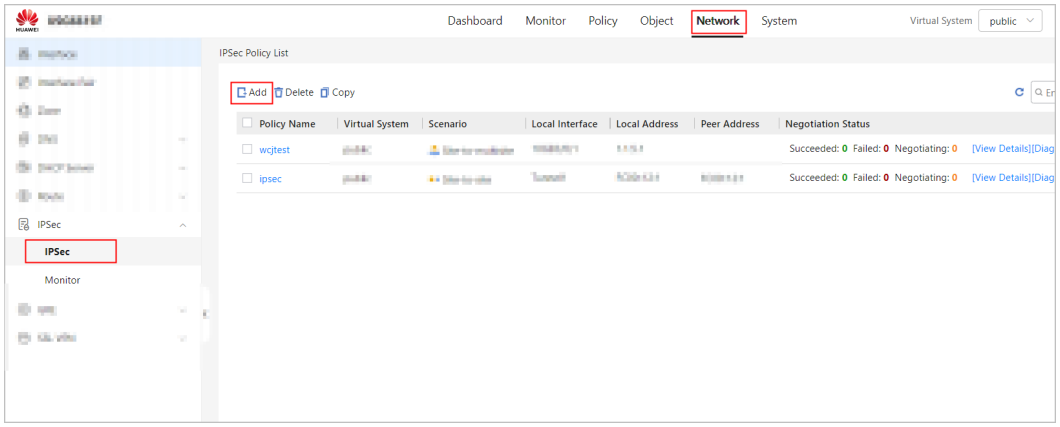
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. The following assumes that the next-hop IP address to the public network is 1.1.5.254. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0
Next Hop	1.1.5.254

Step 9 Configure an IPsec policy on DeviceB and apply the corresponding IPsec policy group to GE0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

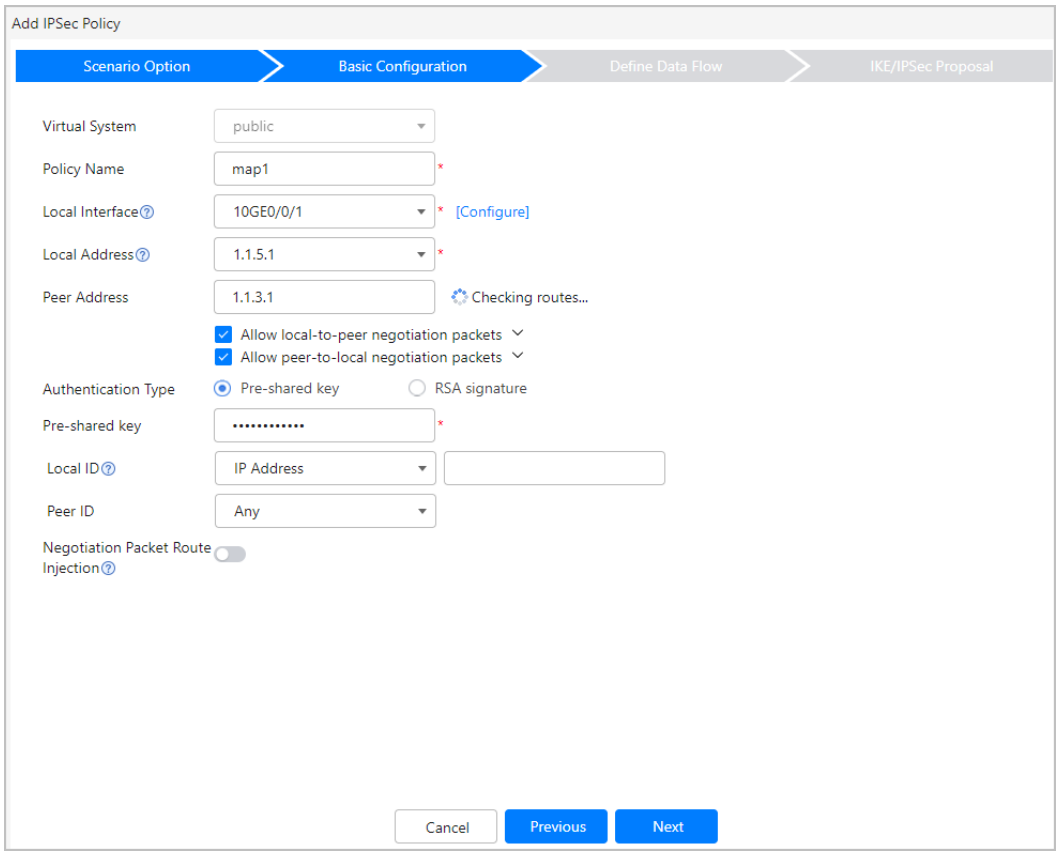
1. Choose **Network** > **IPSec** > **IPSec**.

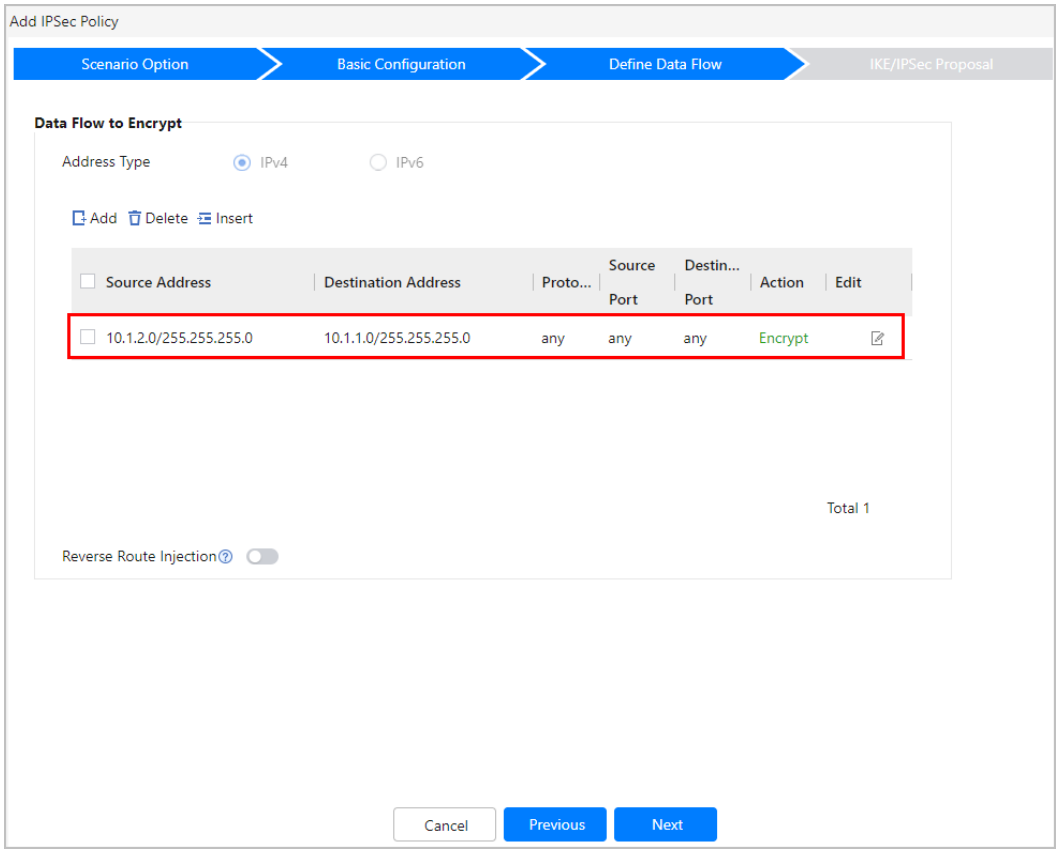


2. Click **Add** to create an IPsec policy as prompted.

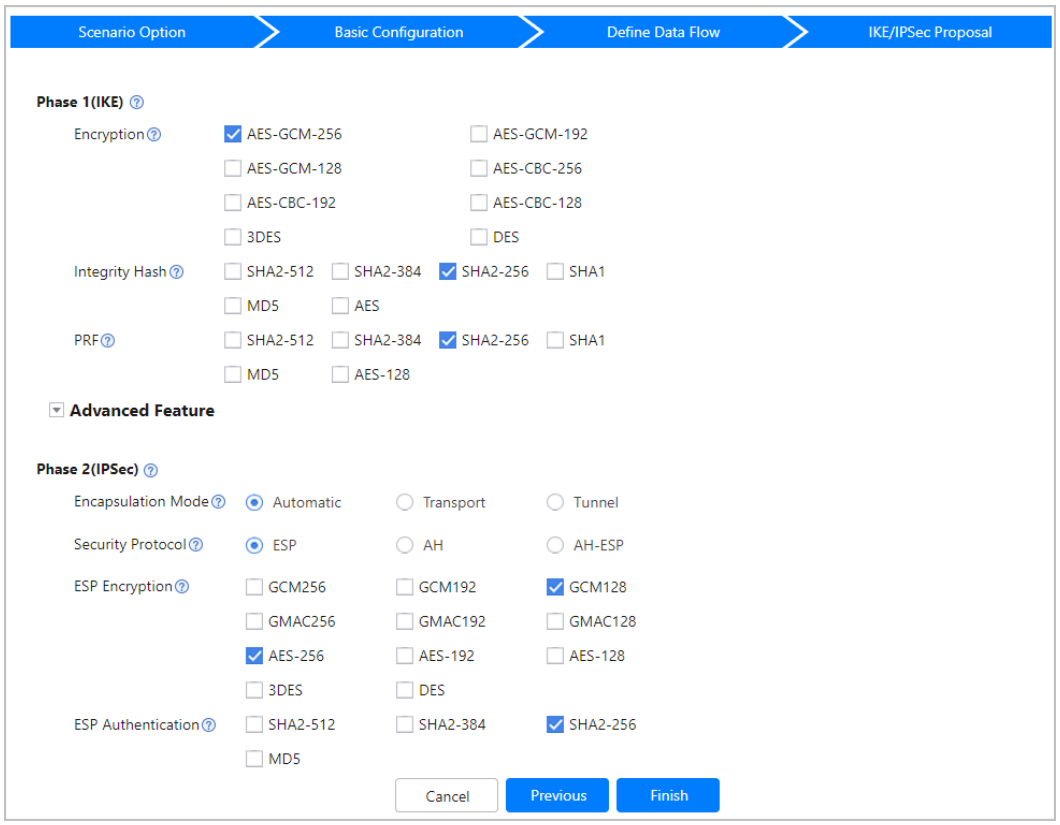


 Copyright © Huawei Technologies Co., Ltd.



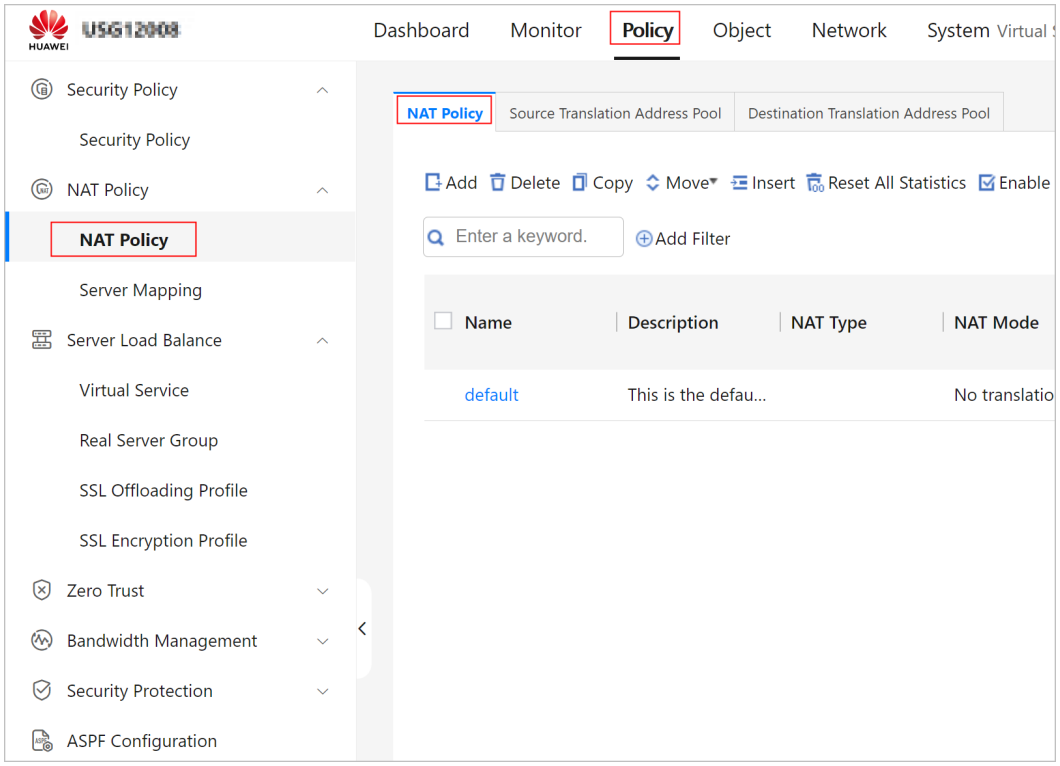


 Copyright © Huawei Technologies Co., Ltd.



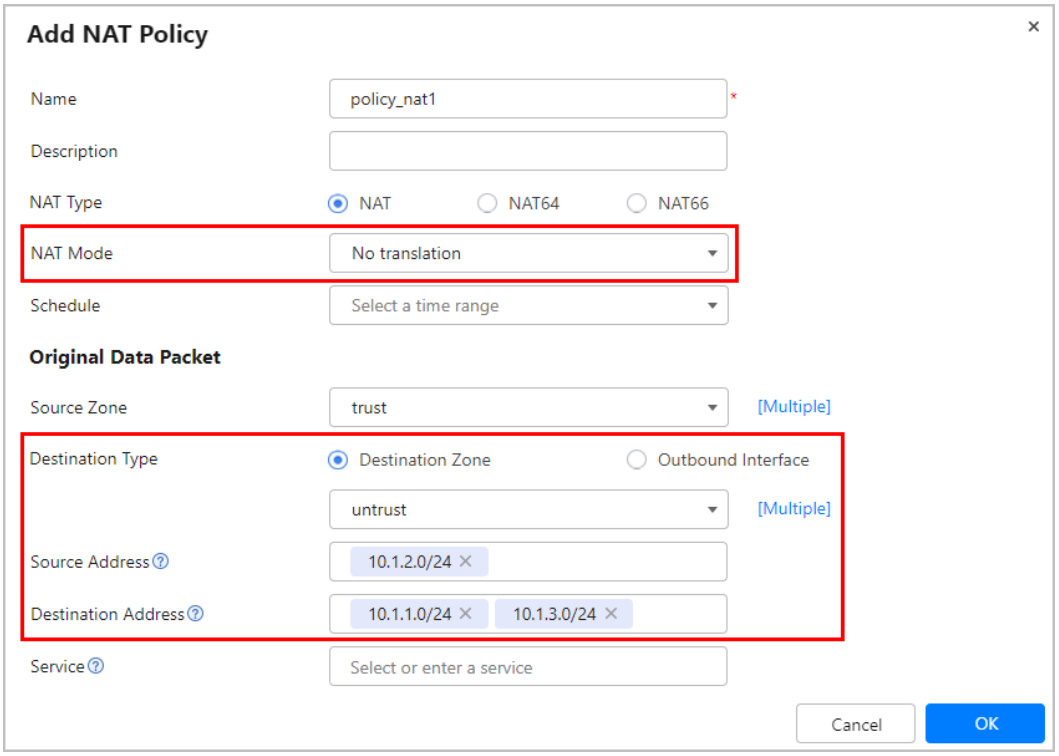
Step 10 Configure NAT on DeviceB. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not.

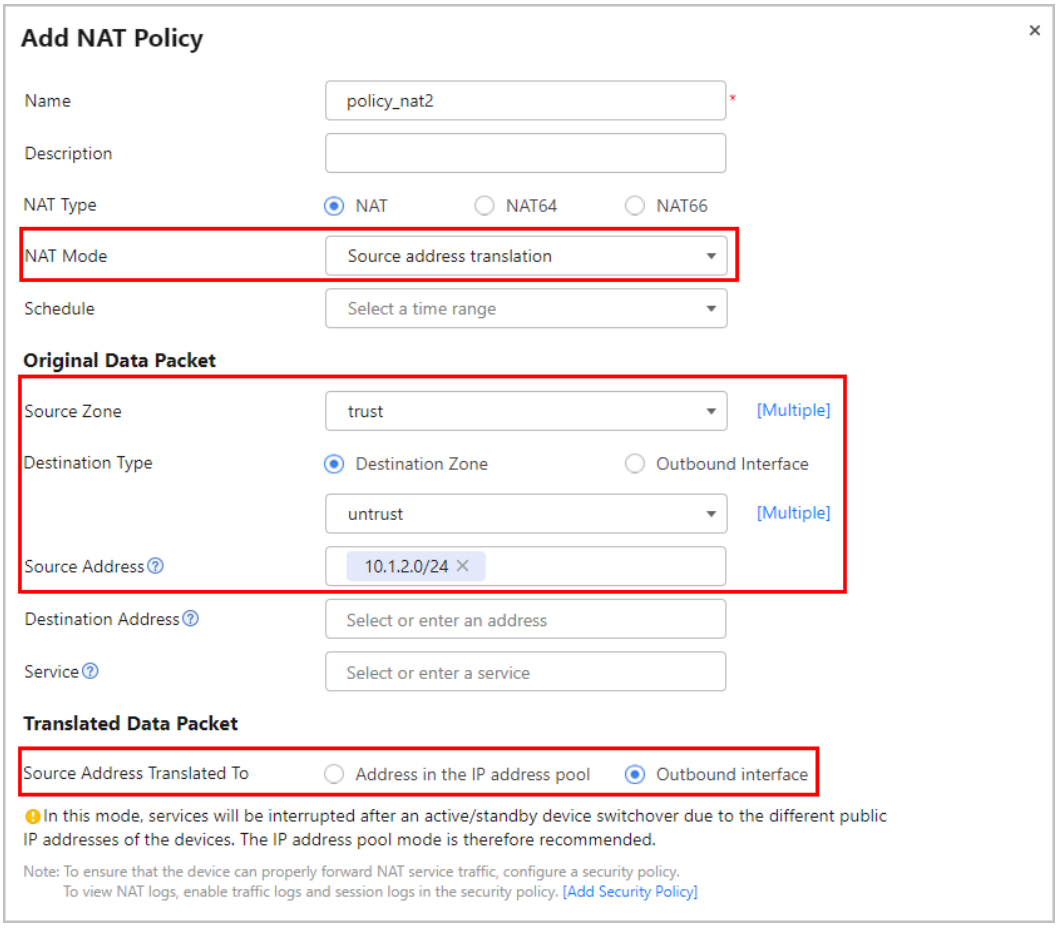
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



 Copyright © Huawei Technologies Co., Ltd.

2. Click **Add** and configure a NAT policy as follows:





 Copyright © Huawei Technologies Co., Ltd.

Step 11 Configure the private network interface GE0/0/2 and public network interface GE0/0/1 on DeviceC, and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.4.1/24

3. Repeat the preceding steps to set parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.3.1/24

Step 12 Configure security policies on DeviceC to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.3.0/24
Destination Address	10.1.1.0/24, 10.1.2.0/24
Action	Permit

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.1.0/24, 10.1.2.0/24
Destination Address	10.1.3.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

3. Configure security policies between the Local and Untrust zones by referring to the preceding steps to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Name	policy3
Source Zone	local
Destination Zone	unrtust
Source Address	1.1.4.1/32
Destination Address	1.1.3.1/32
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.3.1/32
Destination Address	1.1.4.1/32
Action	Permit

Step 13 Configure a default static route on DeviceC to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

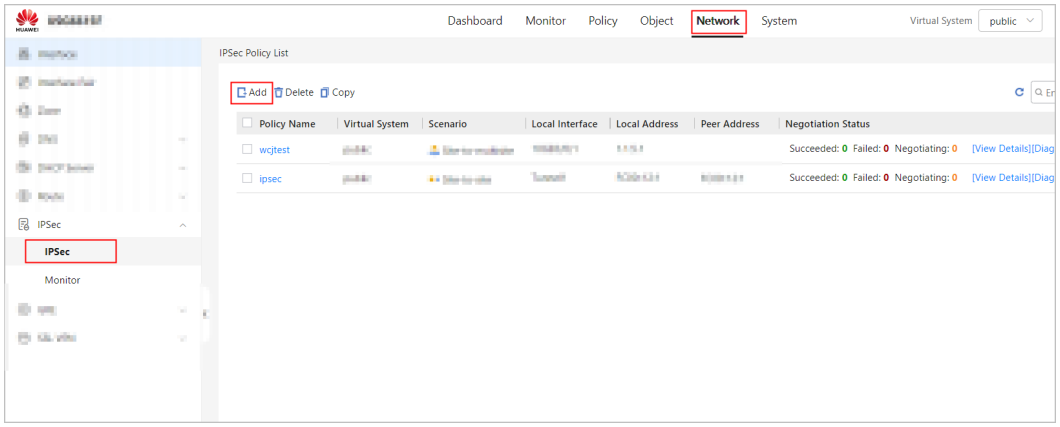
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. The following assumes that the next-hop IP address to the public network is 1.1.4.254. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0
Next Hop	1.1.4.254

Step 14 Configure an IPsec policy on DeviceC.

 Copyright © Huawei Technologies Co., Ltd.

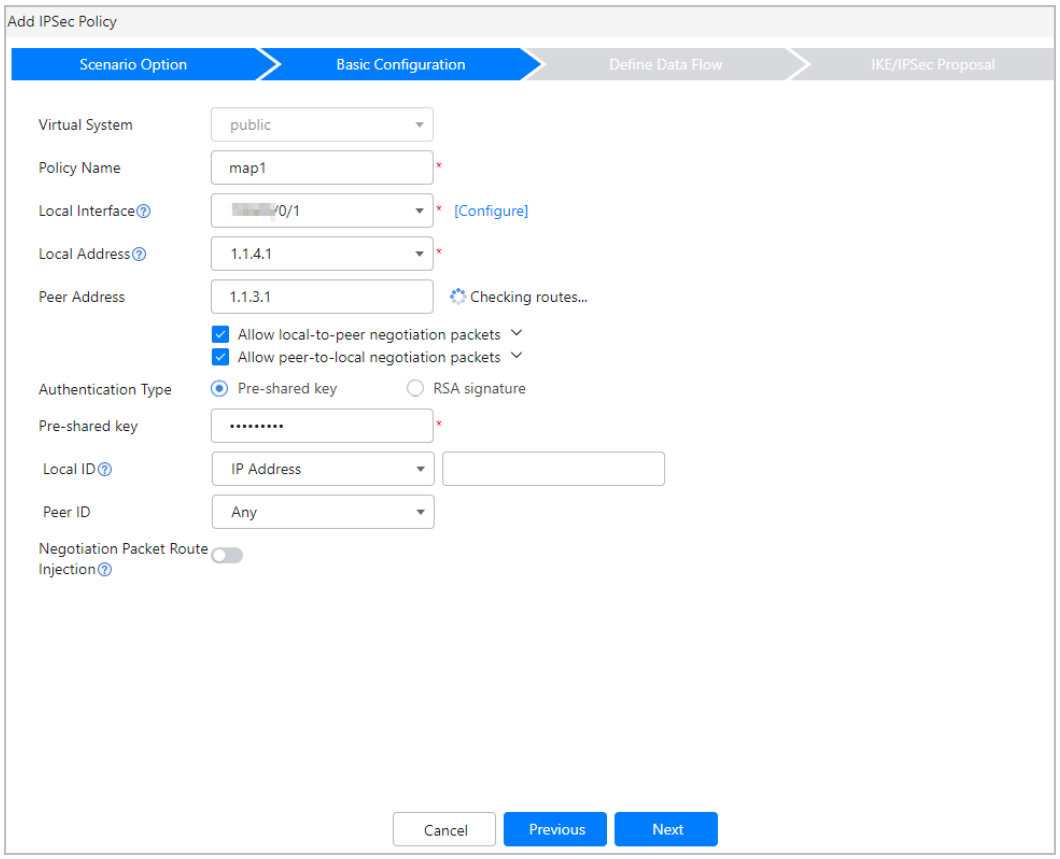
1. Choose **Network** > **IPSec** > **IPSec**.

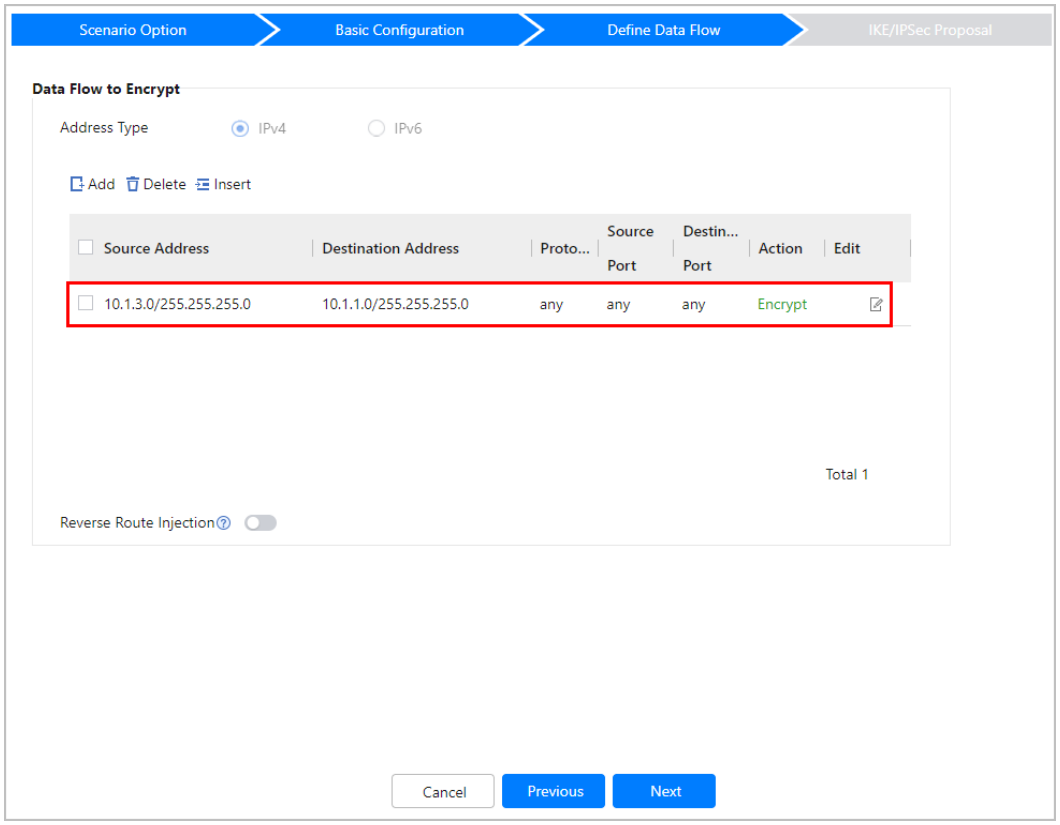


2. Click **Add** to create an IPsec policy as prompted.

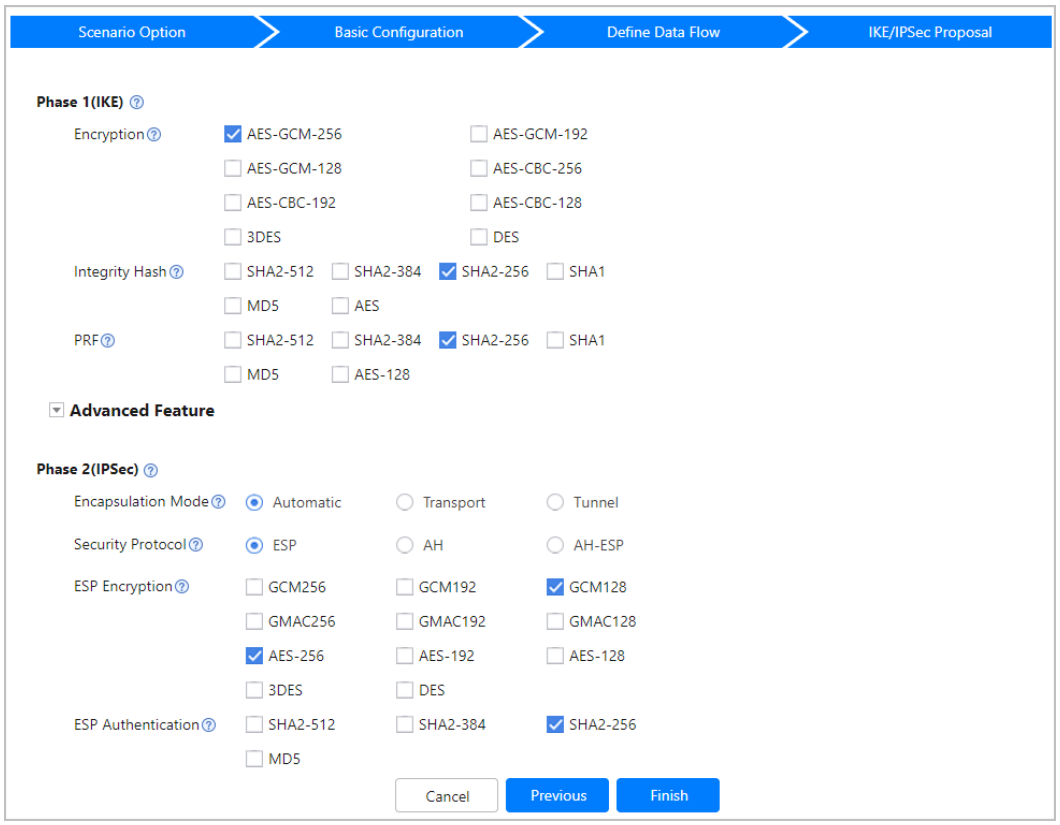


 Copyright © Huawei Technologies Co., Ltd.



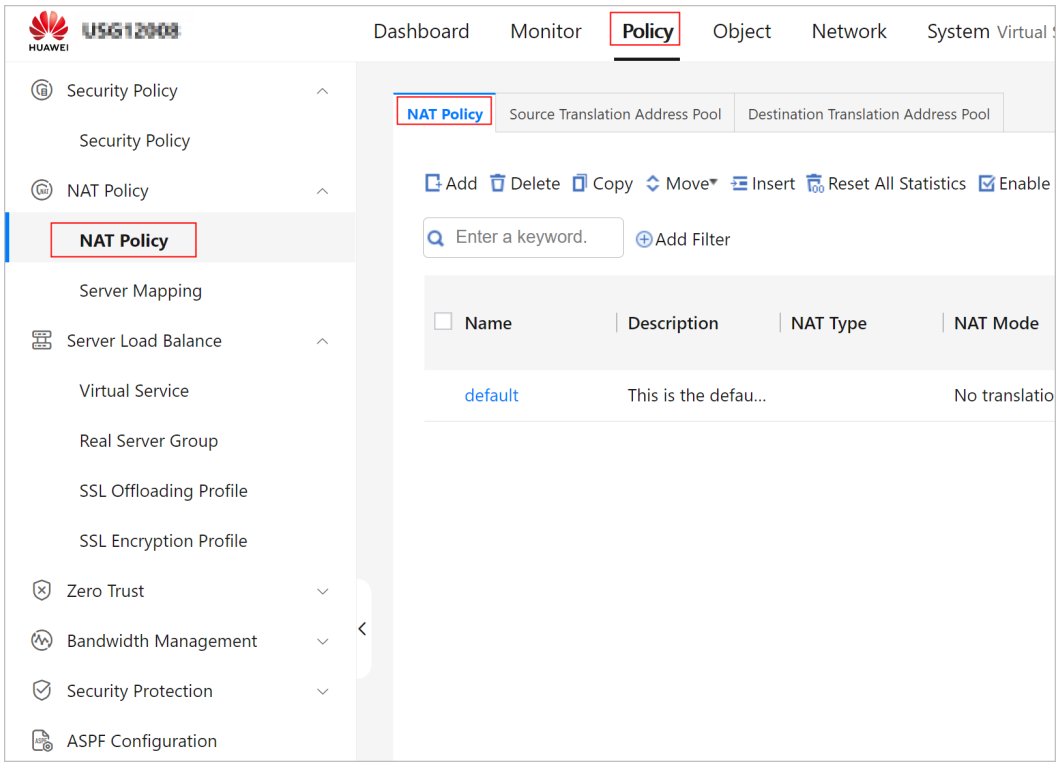


 Copyright © Huawei Technologies Co., Ltd.



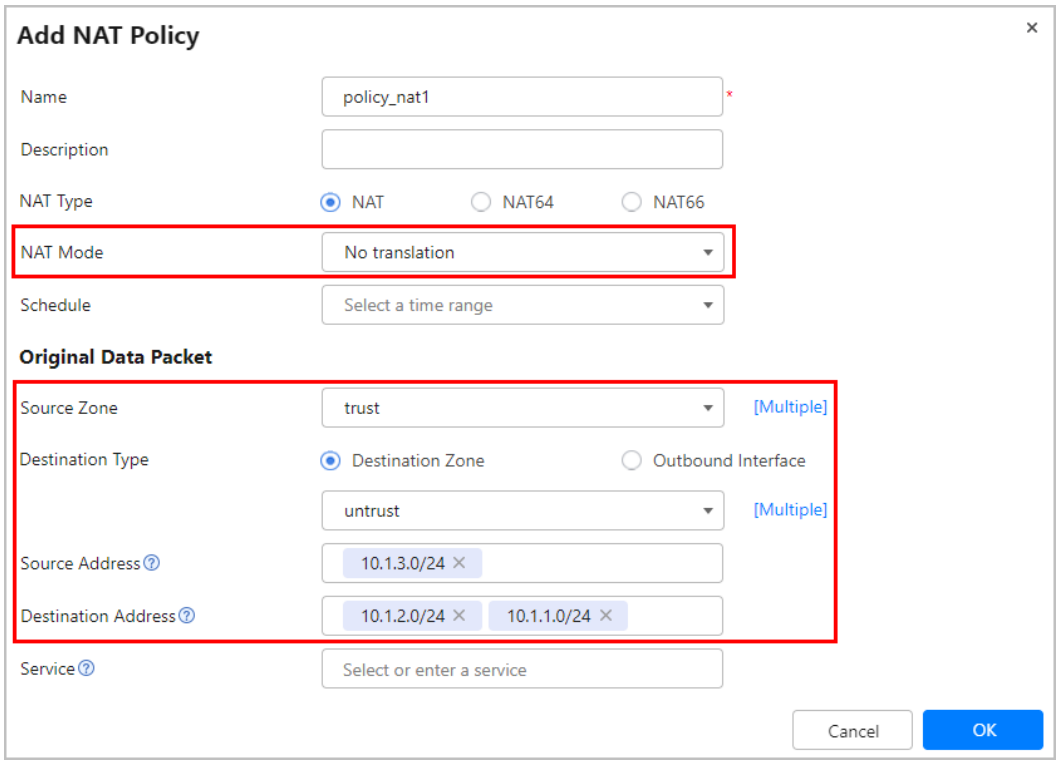
Step 15 Configure NAT on DeviceC. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not.

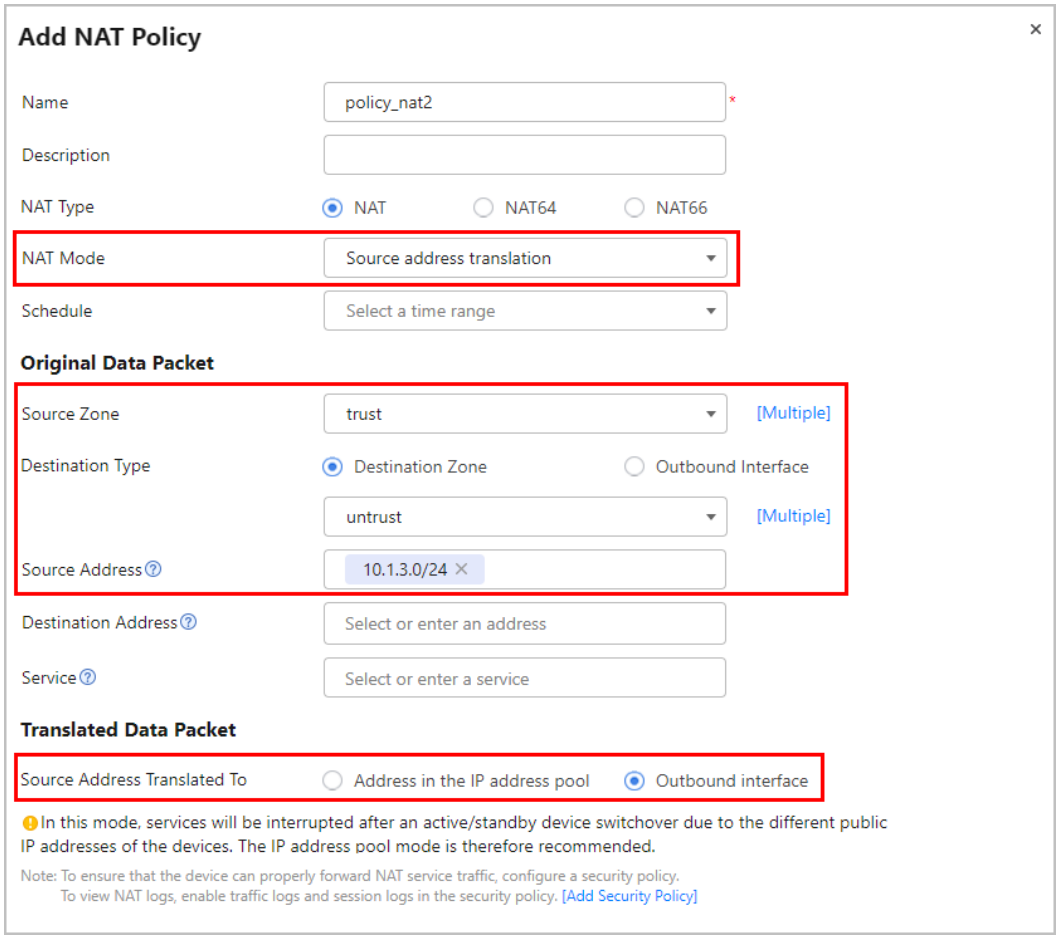
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



2. Click **Add** and configure a NAT policy as follows:

 Copyright © Huawei Technologies Co., Ltd.





----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. After the configuration is complete, employees at the HQ and branches can access the Internet at any time, and the post-NAT source IP address is the IP address of the public network interface on the gateway.
2. Employees at the HQ can access the branch networks, and employees at the branches can also access the HQ network. Choose **Network** > **IPSec** > **Monitor** on DeviceA, DeviceB, and DeviceC to check IPsec tunnel monitoring information.

Table 8-1 IPsec monitoring information on DeviceA

Policy Name	Status	Local Address	Peer Address
map_temp1	IKE negotiation succeeds. IPsec negotiation succeeds.	1.1.3.1	1.1.5.1
map_temp1	IKE negotiation succeeds. IPsec negotiation succeeds.	1.1.3.1	1.1.4.1

Table 8-2 IPsec monitoring information on DeviceB

Policy Name	Status	Local Address	Peer Address
map1	IKE negotiation succeeds. IPsec negotiation succeeds.	1.1.5.1	1.1.3.1

Table 8-3 IPsec monitoring information on DeviceC

Policy Name	Status	Local Address	Peer Address
map1	IKE negotiation succeeds. IPsec negotiation succeeds.	1.1.4.1	1.1.3.1

Configuration Scripts

- DeviceA

 Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 10 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ike proposal 3
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
 #
 ipsec proposal prop29215224150
  encapsulation-mode auto
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-128-gcm-128 aes-256
 #
 ike peer ike29215224150
  pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:g)bb4No&q9eh$d/U[;vG-X-PM!!!!!2jp5!!!!!>!!!!
f1hm>L-to.<2g@+clB*8(<o]+4cxS8E[fm=/XF)C%+%#
  ike-proposal 3
  remote-id-type none
  ike negotiate compatible
 #
 ipsec policy-template tpl29215224150 1
  security acl 3000
  ike-peer ike29215224150
  proposal prop29215224150
  tunnel local applied-interface
  alias map1
  sa duration traffic-based 83886080
  sa duration time-based 3600
 #
 ipsec policy ipsec2921034235 2 isakmp template tpl29215224150
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.3.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule name policy3
  source-zone untrust
  destination-zone local
  source-address 1.1.4.1 mask 255.255.255.255
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone local
  destination-zone untrust
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.4.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
#
nat-policy
 rule name policy_nat1
   source-zone trust
   destination-zone untrust
   source-address 10.1.1.0 mask 255.255.255.0
   destination-address 10.1.2.0 24 mask 255.255.255.0
   destination-address 10.1.3.0 24 mask 255.255.255.0
   action no-nat
 rule name policy_nat2
   source-zone trust
   destination-zone untrust
   source-address 10.1.1.0 mask 255.255.255.0
   action source-nat easy-ip
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ike proposal 1
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
 #
 ipsec proposal prop29215224150
  encapsulation-mode auto
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-128-gcm-128 aes-256
 #
 ike peer ike29215224150
  pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:g)bb4No&q9eh$d/U[;vG-X-PM!!!!!2jp5!!!!!!>!!!!
f1hm>L-to.<2g@+clB*8(<o]+4cxS8E[fm=/XF)C%+%#
  ike-proposal 1
  remote-id-type none
```

 Copyright © Huawei Technologies Co., Ltd.

```
 remote-address 1.1.3.1
 #
 ipsec policy-template tpl29215224150 1
  security acl 3000
  ike-peer ike29215224150
  proposal prop29215224150
  tunnel local applied-interface
  alias map1
  sa duration traffic-based 83886080
  sa duration time-based 3600
 #
 ipsec policy ipsec2921034235 2 isakmp template tpl29215224150
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.5.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 24 mask 255.255.255.0
    destination-address 10.1.3.0 24 mask 255.255.255.0
    action no-nat
  rule name policy_nat2
    source-zone trust
    destination-zone untrust
    source-address 10.1.2.0 mask 255.255.255.0
    action source-nat easy-ip
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
interface GE0/0/1
 ip address 1.1.4.1 255.255.255.0
#
interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ike proposal 1
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
 #
 ipsec proposal prop29215224150
  encapsulation-mode auto
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-128-gcm-128 aes-256
 #
 ike peer ike29215224150
  pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:g)bb4No&q9eh$d/U[;vG-X-PM!!!!!2jp5!!!!!!>!!!!
f1hm>L-to.<2g@+clB*8(<o]+4cxS8E[fm=/XF)C%+%#
  ike-proposal 1
  remote-id-type none
  remote-address 1.1.3.1
 #
 ipsec policy-template tpl29215224150 1
  security acl 3000
  ike-peer ike29215224150
  proposal prop29215224150
  tunnel local applied-interface
  alias map1
  sa duration traffic-based 83886080
  sa duration time-based 3600
 #
 ipsec policy ipsec2921034235 2 isakmp template tpl29215224150
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.4.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.4.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.4.1 mask 255.255.255.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.1.0 24 mask 255.255.255.0
  destination-address 10.1.2.0 24 mask 255.255.255.0
  action no-nat
 rule name policy_nat2
  source-zone trust
  destination-zone untrust
  source-address 10.1.3.0 mask 255.255.255.0
  action source-nat easy-ip
#
return
```

8.3.3 CLI: Example for Establishing an IPsec Tunnel in a NAT Scenario (NAT Is Performed by Each Branch's Gateway)

Networking Requirements

In **Figure 8-20**, an enterprise has the HQ and two branches (branch 1 and branch 2).

- DeviceB connects branch 1 to the Internet, and DeviceC connects branch 2 to the Internet.
- There are reachable routes between DeviceA and DeviceB, and between DeviceA and DeviceC.
- DeviceA is the NAT gateway of the HQ, while DeviceB and DeviceC are the NAT gateways of branch 1 and branch 2, respectively.

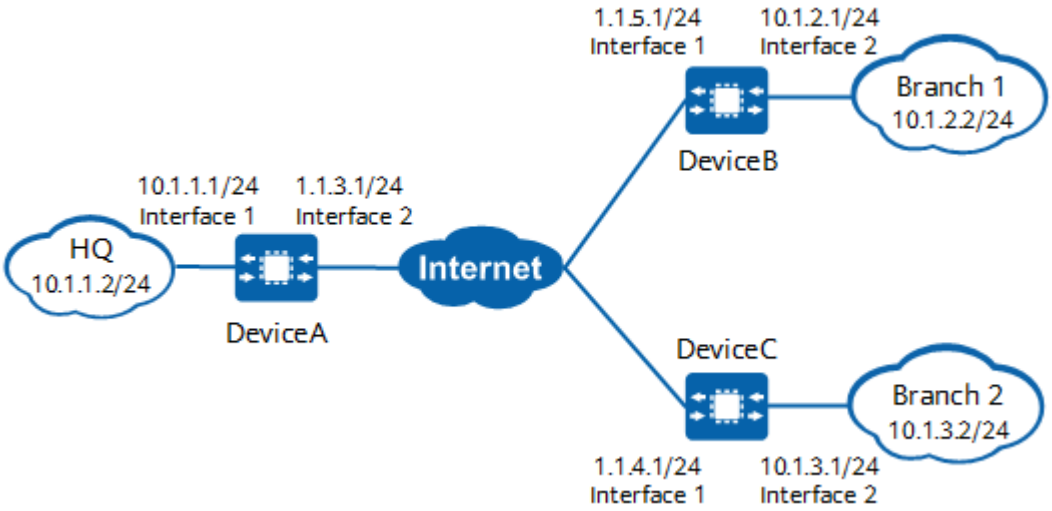
Employees at the branches need to access the servers at the HQ. The information obtained from the servers is confidential and needs to be encrypted for secure transmission over the Internet through an IPsec tunnel. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not. Therefore, distinguish the data flows when configuring NAT.

Figure 8-20 Establishing an IPsec tunnel in a NAT scenario (NAT is performed by each branch's gateway)

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data
DeviceA	Interface: GE 0/0/1 IP address: 10.1.1.1/24 Security zone: Trust
	Interface: GE 0/0/2 IP address: 1.1.3.1/24 Security zone: Untrust
	IPsec configuration Authentication mode: PSK authentication PSK: YsHsjx_202206
	NAT configuration • Name: policy_nat1 Source IP address: 10.1.1.0/24 Destination IP address: 10.1.2.0/24 Destination IP address: 10.1.3.0/24 Action: no-nat • Name: policy_nat2 Source IP address: 10.1.1.0/24 Action: easy-ip
DeviceB	Interface: GE 0/0/1 IP address: 1.1.5.1/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.2.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote address: 1.1.3.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
	NAT configuration • Name: policy_nat1 Source IP address: 10.1.2.0/24 Destination IP address: 10.1.1.0/24 Destination IP address: 10.1.3.0/24 Action: no-nat • Name: policy_nat2 Source IP address: 10.1.2.0/24 Action: easy-ip
DeviceC	Interface: GE 0/0/1 IP address: 1.1.4.1/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.3.1/24 Security zone: Trust
	IPsec configuration Remote address: 1.1.3.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
	NAT configuration • Name: policy_nat1 Source IP address: 10.1.3.0/24 Destination IP address: 10.1.1.0/24 Destination IP address: 10.1.2.0/24 Action: no-nat • Name: policy_nat2 Source IP address: 10.1.3.0/24 Action: easy-ip

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on devices at both ends of a tunnel must be the same.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

The configuration roadmap is as follows:

1. Configure interfaces and add the interfaces to security zones.
2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
3. Configure static routes to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.
4. Configure an IPsec policy and apply an IPsec policy group to an interface. Template IPsec policies need to be configured on DeviceA at the HQ, and ISAKMP IPsec policies need to be configured on DeviceB and DeviceC at the branches.
5. Configure source NAT. Data flows destined for the Internet require NAT, but data flows passing through the IPsec tunnel do not. Therefore, you need to configure different actions in a NAT policy to distinguish the data flows.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.3.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.3.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] source-address 10.1.3.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone untrust
[DeviceA-policy-security-rule-policy3] destination-zone local
[DeviceA-policy-security-rule-policy3] source-address 1.1.4.1 32
[DeviceA-policy-security-rule-policy3] source-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone local
[DeviceA-policy-security-rule-policy4] destination-zone untrust
[DeviceA-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.4.1 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a default static route on DeviceA to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.3.254.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.3.254
```

Step 4 Configure a template IPsec policy on DeviceA and apply an IPsec policy group to GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

1. Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

2. Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

3. Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 10
[DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-b] quit
```

4. Configure an IPsec policy template.

```
[DeviceA] ipsec policy-template map_temp 1
[DeviceA-ipsec-policy-templet-map_temp-1] proposal tran1
[DeviceA-ipsec-policy-templet-map_temp-1] ike-peer b
[DeviceA-ipsec-policy-templet-map_temp-1] quit
```

5. Reference the IPsec policy template **map_temp** in the IPsec policy numbered 10 in the IPsec policy group **map1**.

```
[DeviceA] ipsec policy map1 10 isakmp template map_temp
```

6. Apply the IPsec policy group to GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipsec policy map1
[DeviceA-GE0/0/2] quit
```

Step 5 Configure NAT on DeviceA.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] destination-address 10.1.2.0 24
[DeviceA-policy-nat-rule-policy_nat1] destination-address 10.1.3.0 24
[DeviceA-policy-nat-rule-policy_nat1] action no-nat
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] rule name policy_nat2
[DeviceA-policy-nat-rule-policy_nat2] source-zone trust
[DeviceA-policy-nat-rule-policy_nat2] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat2] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat2] action source-nat easy-ip
[DeviceA-policy-nat-rule-policy_nat2] quit
[DeviceA-policy-nat] quit
```

Step 6 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 1.1.5.1 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.2.1 24
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Step 7 Configure security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.3.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] source-address 10.1.3.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy4] destination-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy4] action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 8 Configure a default static route on DeviceB to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 1.1.5.254.

```
[DeviceB] ip route-static 0.0.0.0 0.0.0.0 1.1.5.254
```

Step 9 Configure an ISAKMP IPsec policy on DeviceB and apply an IPsec policy group to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.2.0/24 to access the network segment 10.1.1.0/24.

```
[DeviceB] acl 3000
[DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl4-advance-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 10
[DeviceB-ike-peer-a] remote-address 1.1.3.1
[DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-a] quit
```

5. Configure an IPsec policy.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

Step 10 Configure NAT on DeviceB.

```
[DeviceB] nat-policy
[DeviceB-policy-nat] rule name policy_nat1
[DeviceB-policy-nat-rule-policy_nat1] source-zone trust
[DeviceB-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceB-policy-nat-rule-policy_nat1] source-address 10.1.2.0 24
[DeviceB-policy-nat-rule-policy_nat1] destination-address 10.1.1.0 24
[DeviceB-policy-nat-rule-policy_nat1] destination-address 10.1.3.0 24
[DeviceB-policy-nat-rule-policy_nat1] action no-nat
[DeviceB-policy-nat-rule-policy_nat1] quit
[DeviceB-policy-nat] rule name policy_nat2
[DeviceB-policy-nat-rule-policy_nat2] source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-nat-rule-policy_nat2] destination-zone untrust
[DeviceB-policy-nat-rule-policy_nat2] source-address 10.1.2.0 24
[DeviceB-policy-nat-rule-policy_nat2] action source-nat easy-ip
[DeviceB-policy-nat-rule-policy_nat2] quit
[DeviceB-policy-nat] quit
```

Step 11 Configure public and private network interfaces on DeviceC, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] undo portswitch
[DeviceC-GE0/0/1] ip address 1.1.4.1 24
[DeviceC-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceC] interface ge 0/0/2
[DeviceC-GE0/0/2] undo portswitch
[DeviceC-GE0/0/2] ip address 10.1.3.1 24
[DeviceC-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
```

Step 12 Configure security policies on DeviceC to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure security policies between the Trust and Untrust zones to permit the data flows to be encrypted.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy1
[DeviceC-policy-security-rule-policy1] source-zone trust
[DeviceC-policy-security-rule-policy1] destination-zone untrust
[DeviceC-policy-security-rule-policy1] source-address 10.1.3.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy1] action permit
[DeviceC-policy-security-rule-policy1] quit
[DeviceC-policy-security] rule name policy2
[DeviceC-policy-security-rule-policy2] source-zone untrust
[DeviceC-policy-security-rule-policy2] destination-zone trust
[DeviceC-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceC-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy2] destination-address 10.1.3.0 24
[DeviceC-policy-security-rule-policy2] action permit
[DeviceC-policy-security-rule-policy2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceC-policy-security] rule name policy3
[DeviceC-policy-security-rule-policy3] source-zone local
[DeviceC-policy-security-rule-policy3] destination-zone untrust
[DeviceC-policy-security-rule-policy3] source-address 1.1.4.1 32
[DeviceC-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceC-policy-security-rule-policy3] action permit
[DeviceC-policy-security-rule-policy3] quit
[DeviceC-policy-security] rule name policy4
[DeviceC-policy-security-rule-policy4] source-zone untrust
[DeviceC-policy-security-rule-policy4] destination-zone local
[DeviceC-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceC-policy-security-rule-policy4] destination-address 1.1.4.1 32
[DeviceC-policy-security-rule-policy4] action permit
[DeviceC-policy-security-rule-policy4] quit
[DeviceC-policy-security] quit
```

Step 13 Configure a default static route on DeviceC to divert tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceC to the Internet is 1.1.4.254.

```
[DeviceC] ip route-static 0.0.0.0 0.0.0.0 1.1.4.254
```

Step 14 Configure an ISAKMP IPsec policy on DeviceC and apply an IPsec policy group to GE 0/0/1.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.3.0/24 to access the network segment 10.1.1.0/24.

   ```
   [DeviceC] acl 3000
   [DeviceC-acl4-advance-3000] rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
   [DeviceC-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceC] ipsec proposal tran1
   [DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceC-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceC] ike proposal 10
   [DeviceC-ike-proposal-10] authentication-method pre-share
   [DeviceC-ike-proposal-10] prf hmac-sha2-256
   [DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceC-ike-proposal-10] dh group14
   [DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceC-ike-proposal-10] quit
   ```

4. Configure an IKE peer.

   ```
   [DeviceC] ike peer a
   [DeviceC-ike-peer-a] ike-proposal 10
   [DeviceC-ike-peer-a] remote-address 1.1.3.1
   [DeviceC-ike-peer-a] pre-shared-key YsHsjx_202206
   [DeviceC-ike-peer-a] quit
   ```

5. Configure an IPsec policy.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

6. Apply an IPsec policy group to GE 0/0/1.

```
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ipsec policy map1
[DeviceC-GE0/0/1] quit
```

Step 15 Configure NAT on DeviceC.

```
[DeviceC] nat-policy
[DeviceC-policy-nat] rule name policy_nat1
[DeviceC-policy-nat-rule-policy_nat1] source-zone trust
[DeviceC-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceC-policy-nat-rule-policy_nat1] source-address 10.1.3.0 24
[DeviceC-policy-nat-rule-policy_nat1] destination-address 10.1.2.0 24
[DeviceC-policy-nat-rule-policy_nat1] destination-address 10.1.1.0 24
[DeviceC-policy-nat-rule-policy_nat1] action no-nat
[DeviceC-policy-nat-rule-policy_nat1] quit
[DeviceC-policy-nat] rule name policy_nat2
[DeviceC-policy-nat-rule-policy_nat2] source-zone trust
[DeviceC-policy-nat-rule-policy_nat2] destination-zone untrust
[DeviceC-policy-nat-rule-policy_nat2] source-address 10.1.3.0 24
[DeviceC-policy-nat-rule-policy_nat2] action source-nat easy-ip
[DeviceC-policy-nat-rule-policy_nat2] quit
[DeviceC-policy-nat] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, employees at the HQ and branches can access the Internet at any time. Check for the session entries with source addresses as the private addresses of intranet PCs. The following assumes that a PC on the HQ intranet accesses IP address 3.3.3.3. If a session entry with the source address as the private addresses of the PC is found and the post-NAT IP address is the public IP address of the public network interface, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.1.1.3:2474[1.1.3.1:3761]-->3.3.3.3:80
```

2. View IKE SAs and IPsec SAs on DeviceB and DeviceC at the branches. The following example uses the command output on DeviceB, which shows that IKE SAs and IPsec SAs have been established successfully.

```
<DeviceB> display ike sa
Total number of IKE SA in all CPU : 2
Total number of phase 1 SA in all CPU :
1
Total number of phase 2 SA in all CPU : 1

Flag Description: RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING

Slot 0, cpu 0 IKE SA information :
  Number of IKE SA : 2,  number of IKE SA1: 1,  number of IKE SA2: 1
-------------------------------------------------------------------------------
  Conn-ID    Peer          VPN     Flag(s)     Phase   RemoteType  RemoteID
-------------------------------------------------------------------------------
  16782416   1.1.3.1/500           RD|ST|A     v2:2    IP          1.1.3.1
  16782415   1.1.3.1/500           RD|ST|A     v2:1    IP          1.1.3.1
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
<DeviceB> display ipsec sa brief
Slot 0, cpu 0 IPSec SA information:
  Src address   Dst address     SPI      VPN  Protocol     Algorithm
-------------------------------------------------------------------------------
  1.1.3.1       1.1.5.1    16423687          ESP       E:AES-256-GCM-128
  1.1.5.1       1.1.3.1    274624861         ESP       E:AES-256-GCM-128
Number of IPSec SA : 2
-------------------------------------------------------------------------------
Total number of IPSec SA in all CPU : 2
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 pre-shared-key %@%@'OMi3SPl%@TJdx5uDE(44*I^%@%@
 ike-proposal 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
#
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.3.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.3.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
 rule name policy3
  source-zone untrust
  destination-zone local
  source-address 1.1.4.1 mask 255.255.255.255
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone local
  destination-zone untrust
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.4.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
#
nat-policy
 rule name policy_nat1
   source-zone trust
   destination-zone untrust
   source-address 10.1.1.0 mask 255.255.255.0
   destination-address 10.1.2.0 24 mask 255.255.255.0
   destination-address 10.1.3.0 24 mask 255.255.255.0
   action no-nat
 rule name policy_nat2
   source-zone trust
   destination-zone untrust
   source-address 10.1.1.0 mask 255.255.255.0
   action source-nat easy-ip
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.3.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.5.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 24 mask 255.255.255.0
    destination-address 10.1.3.0 24 mask 255.255.255.0
    action no-nat
  rule name policy_nat2
    source-zone trust
    destination-zone untrust
    source-address 10.1.2.0 mask 255.255.255.0
    action source-nat easy-ip
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ike peer a
 pre-shared-key %@%@W[QD:1tV\'f"!1W&yrX6v$B>%@%@
 ike-proposal 10
 remote-address 1.1.3.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/2
 ip address 10.1.3.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.4.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.4.254
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.4.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.4.1 mask 255.255.255.255
  action permit
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.3.0 mask 255.255.255.0
    destination-address 10.1.1.0 24 mask 255.255.255.0
    destination-address 10.1.2.0 24 mask 255.255.255.0
    action no-nat
  rule name policy_nat2
    source-zone trust
    destination-zone untrust
    source-address 10.1.3.0 mask 255.255.255.0
    action source-nat easy-ip
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

8.4 IPsec Virtualization

8.4.1 Web: Example for Configuring Virtual Systems to Use an Independent Public IP Address to Establish an IPsec Tunnel

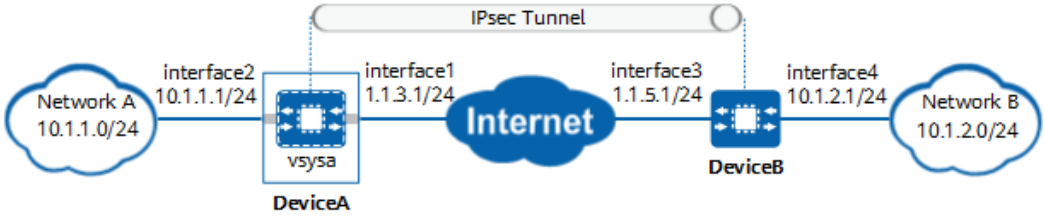
Networking Requirements

As shown in **Figure 8-21**, create vsysa on DeviceA and assign interface 1 (public network interface) to vsysa. Configure an IPsec policy in the virtual system and establish an IPsec tunnel between interface1 and the peer gateway to implement secure communication between network A attached to vsysa and network B.

Figure 8-21 Each virtual system using an independent public IP address to establish an IPsec tunnel

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively; interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB, respectively.



Item		Data
DeviceA	Virtual system: vsysa	Public network interface: GE0/0/1 Public network interface IP address: 1.1.3.1/24 Security zone to which the public network interface belongs: Untrust
		Private network interface: GE0/0/2 Private network interface IP address: 10.1.1.1/24 Security zone to which the private network interface belongs: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item		Data
		IPsec configuration Scenario: point-to-point Remote address: 1.1.5.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: IP address
DeviceB		Interface number: GE0/0/1 IP address: 1.1.5.1/24 Security zone to which the interface belongs: Untrust
		Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone to which the interface belongs: Trust
		IPsec configuration Scenario: point-to-point Remote address: 1.1.3.1 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID: IP address Remote ID: IP address

Configuration Roadmap

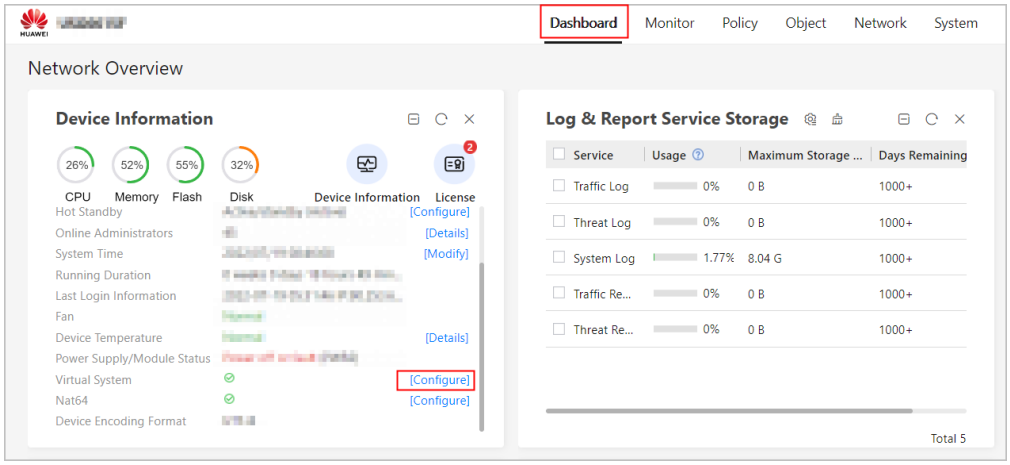
- On DeviceA:
  a. In the public system, create virtual system vsysa and allocate resources to the virtual system.
  b. Complete basic configuration, including interfaces, routes, and security policies in vsysa.
  c. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal in vsysa.
- On DeviceB:
  a. Set IP addresses for interfaces and add the interfaces to security zones.
  b. Configure security policies to permit IPsec negotiation packets and service packets.
  c. Configure routes between network A and network B.
  d. Configure IPsec policies, including the basic IPsec policy information, data flow to be protected by IPsec, and IPsec proposal.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

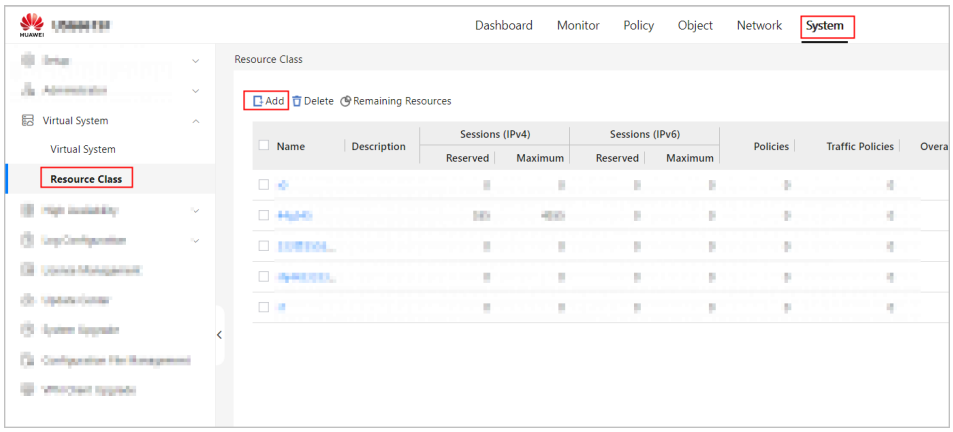
Step 1 Configure DeviceA.

1. Choose **Dashboard** > **Device Information**. Click **Configure** next to **Virtual System** to enable the virtual system function.



2. Configure virtual system resource classes.

   a. Choose **System** > **Virtual System** > **Resource Class**.

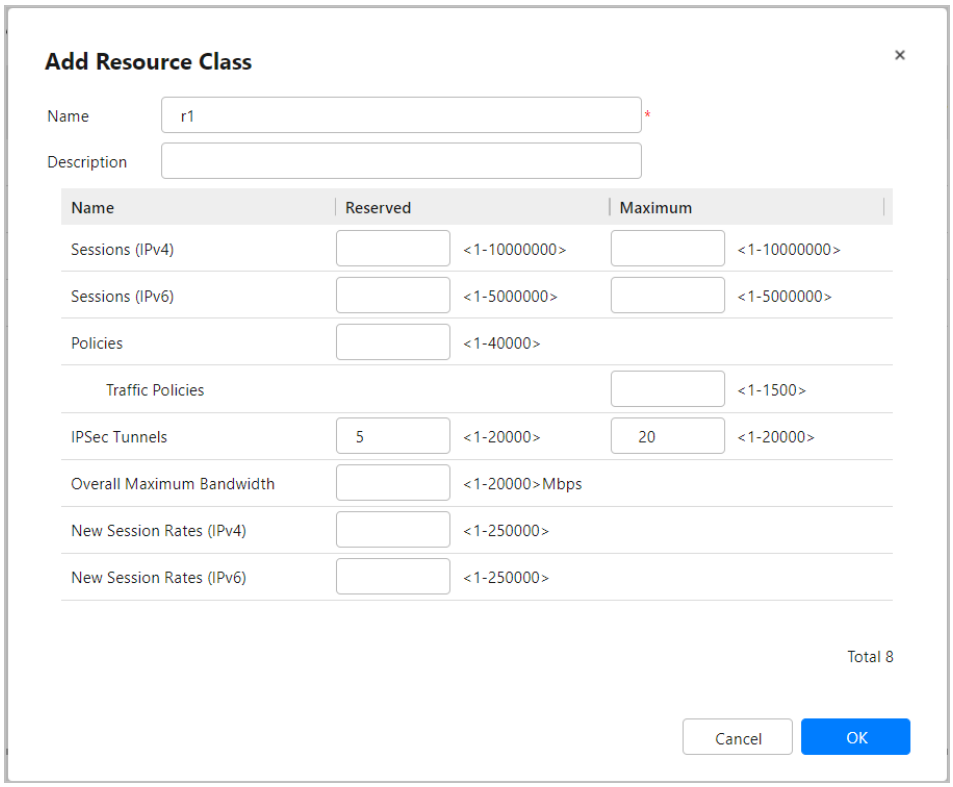


   b. Click **Add**. In the dialog box that is displayed, create system resource class r1 and set the guaranteed and maximum number of IPsec tunnels as follows. Click **OK**.

   NOTE

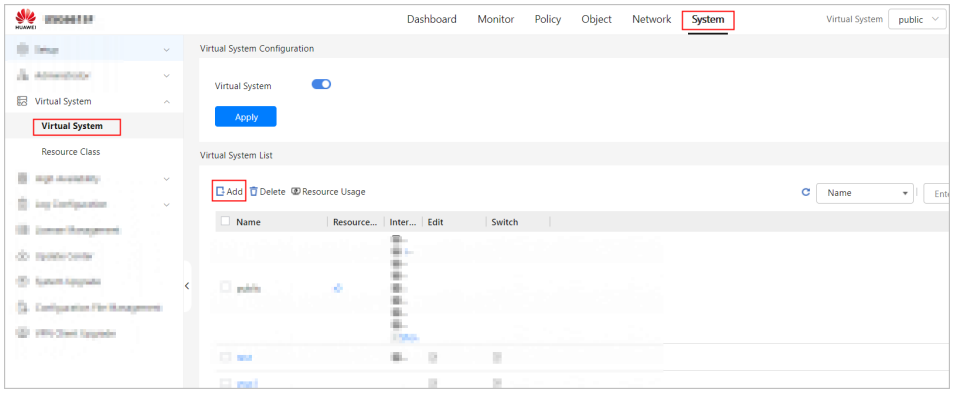
   The guaranteed number of IPsec tunnels cannot be greater than the maximum number of IPsec tunnels.

 Copyright © Huawei Technologies Co., Ltd.



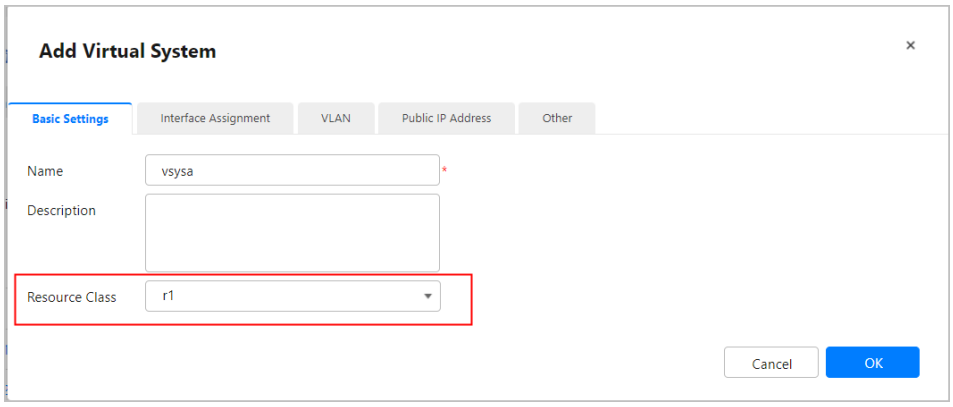
3. In the public system, create virtual system vsysa and allocate resources to it. Click **OK**.

   a. Choose **System** > **Virtual System** > **Virtual System**.

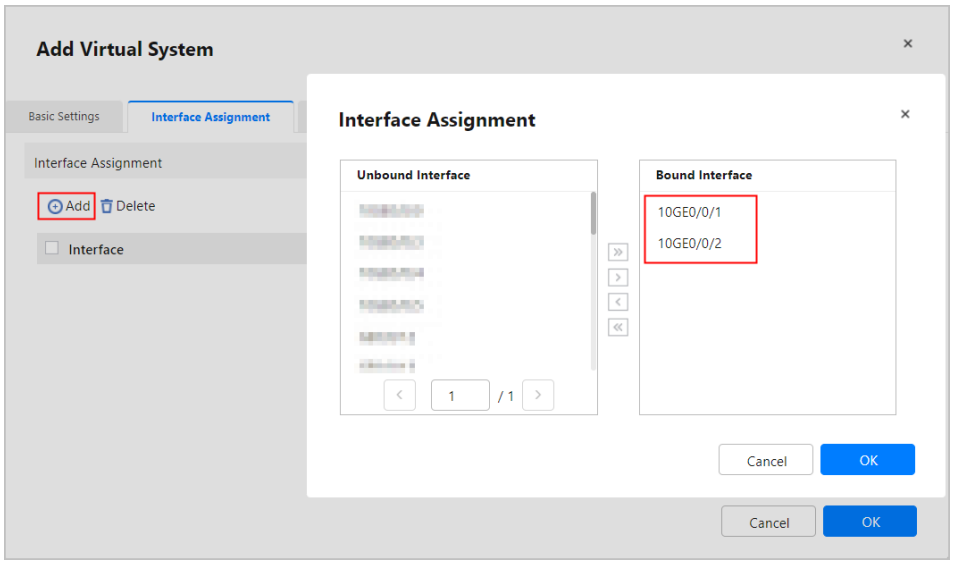


   b. Click **Add**. In the dialog box displayed, click the **Basic Settings** tab and complete basic virtual system configurations as follows.

 Copyright © Huawei Technologies Co., Ltd.

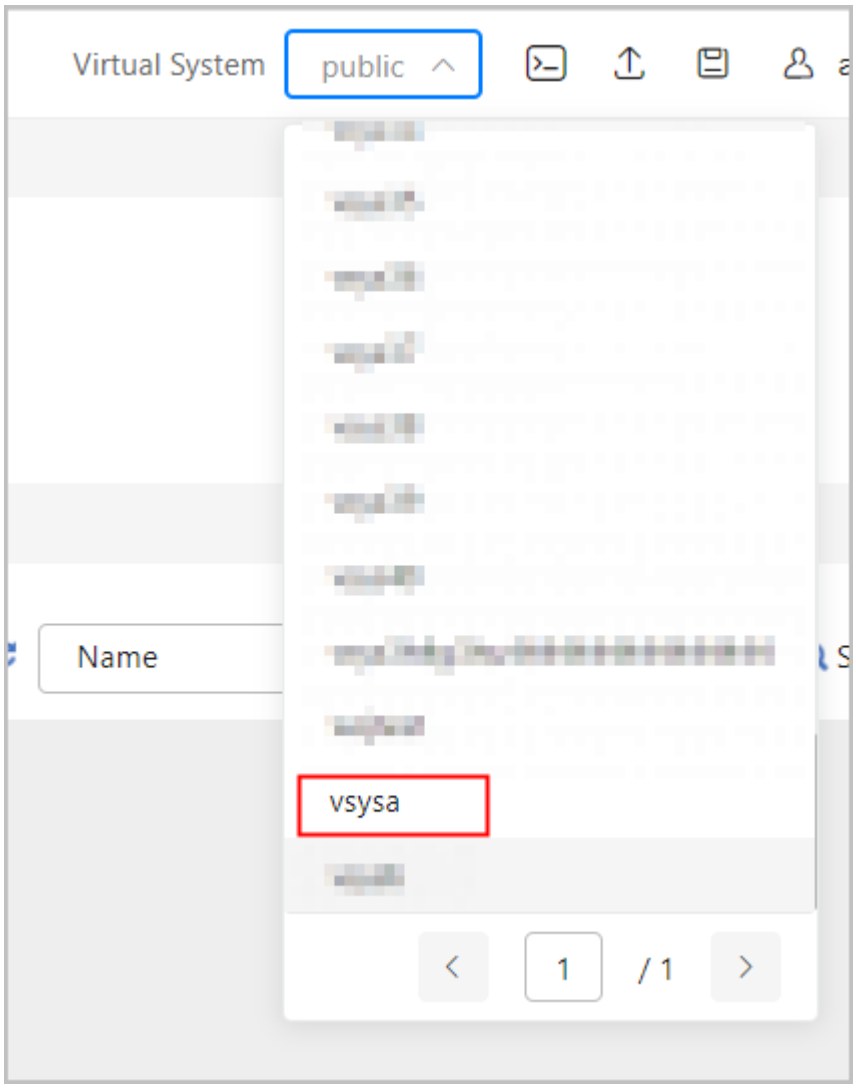


c. Click the **Interface Assignment** tab, click **Add**, and allocate interfaces to the virtual system.



4. Configure IP addresses for interfaces in vsysa, and assign the interfaces to security zones.
   a. Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access vsysa.

 Copyright © Huawei Technologies Co., Ltd.



b. Choose **Network** > **Interface**.

c. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.3.1/24

d. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

5. Configure security policies in vsysa to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy_ipsec_2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

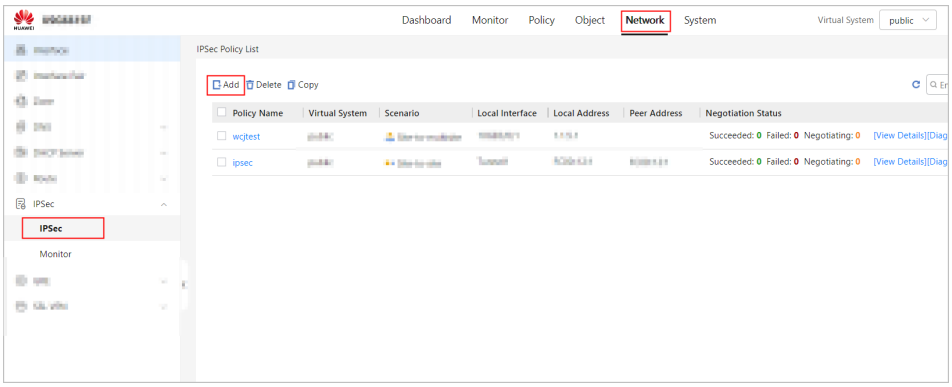
 Copyright © Huawei Technologies Co., Ltd.

Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

6. Create a static route to the Internet in vsysa. In this example, the next-hop IP address is 1.1.3.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a route from vsysa to the Internet as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.3.2

7. Configure an IPsec policy in vsysa.
   a. Choose **Network** > **IPSec** > **IPSec**.

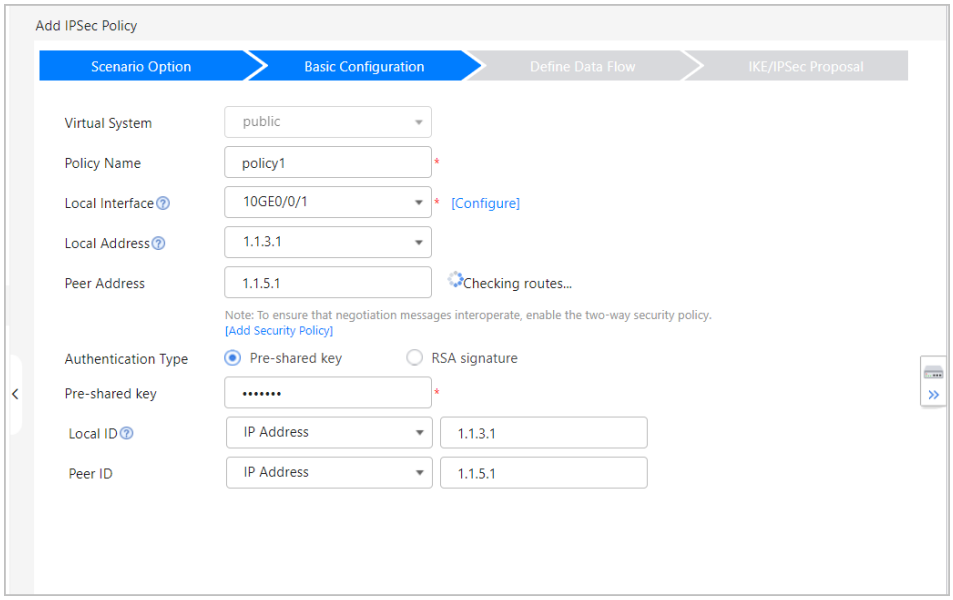


   b. Click **Add** to create an IPsec policy as prompted.

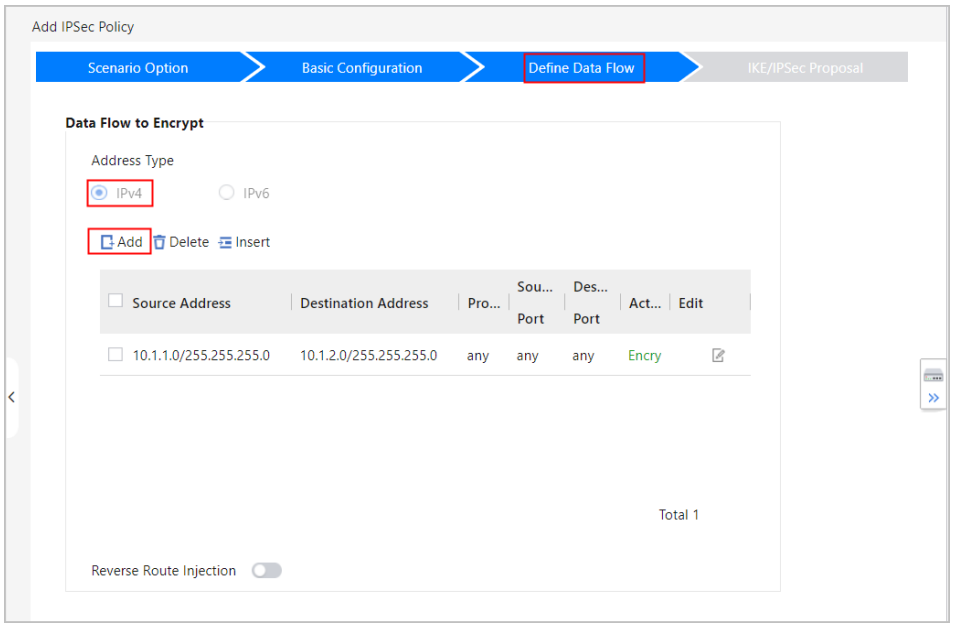
 Copyright © Huawei Technologies Co., Ltd.



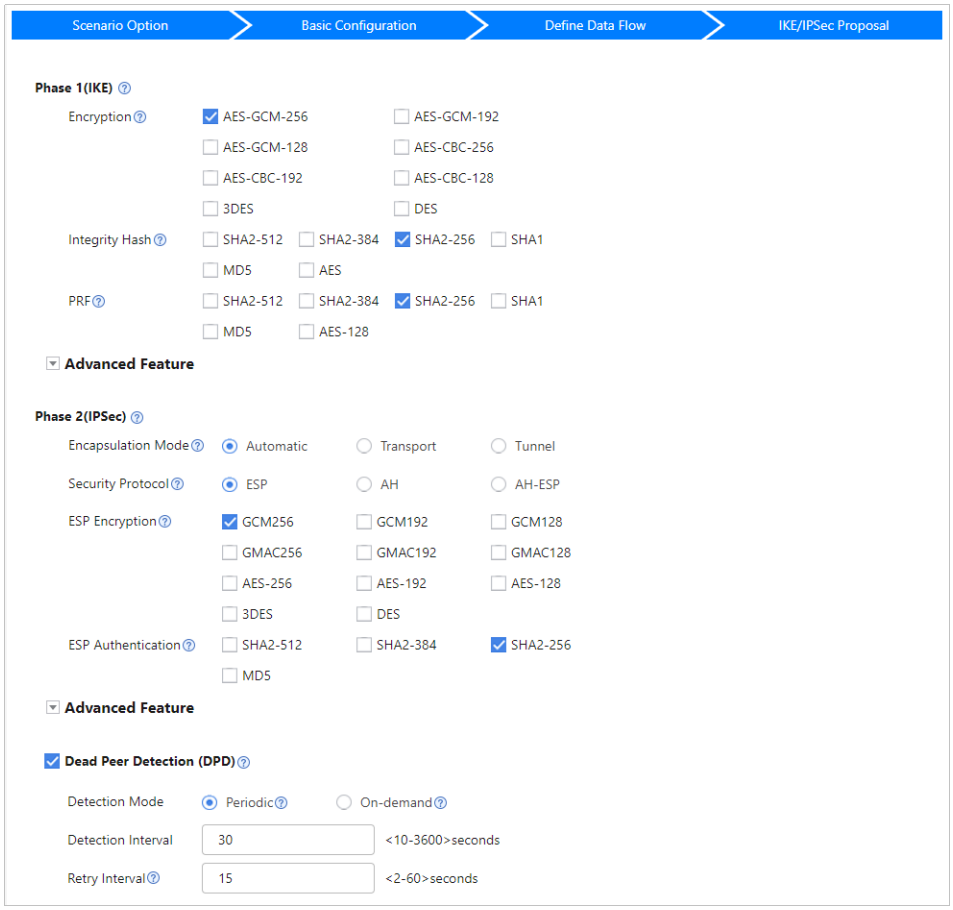
The pre-shared key is YsHsjx_202206.



 Copyright © Huawei Technologies Co., Ltd.



In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.



c. Click **Finish**.

Step 2 Configure DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.5.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Configure security policies to permit IPsec negotiation packets and service packets.

   NOTE

   The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

   c. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy_ipsec_2
Source Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	trust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Source Address	1.1.3.1/32
Destination Address	1.1.5.1/32
Action	Permit

Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address	1.1.5.1/32
Destination Address	1.1.3.1/32
Action	Permit

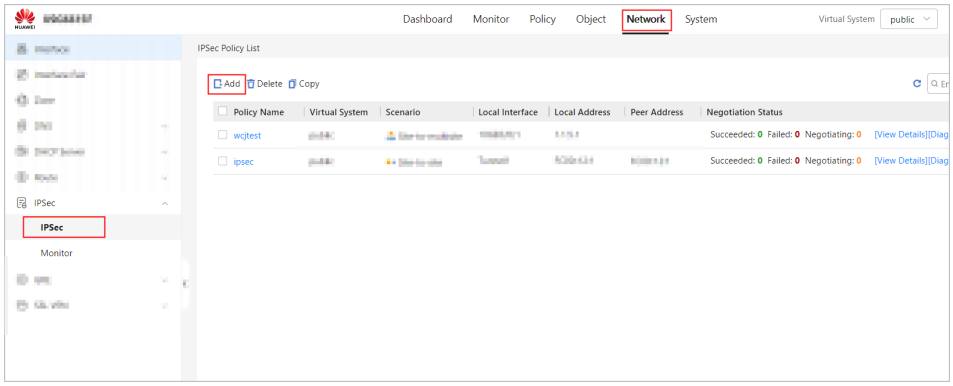
3. Create a static route to the Internet. In this example, the next-hop IP address is 1.1.5.2.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a route from DeviceB to the Internet as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.5.2

4. Configure an IPsec policy.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Network** > **IPSec** > **IPSec**.

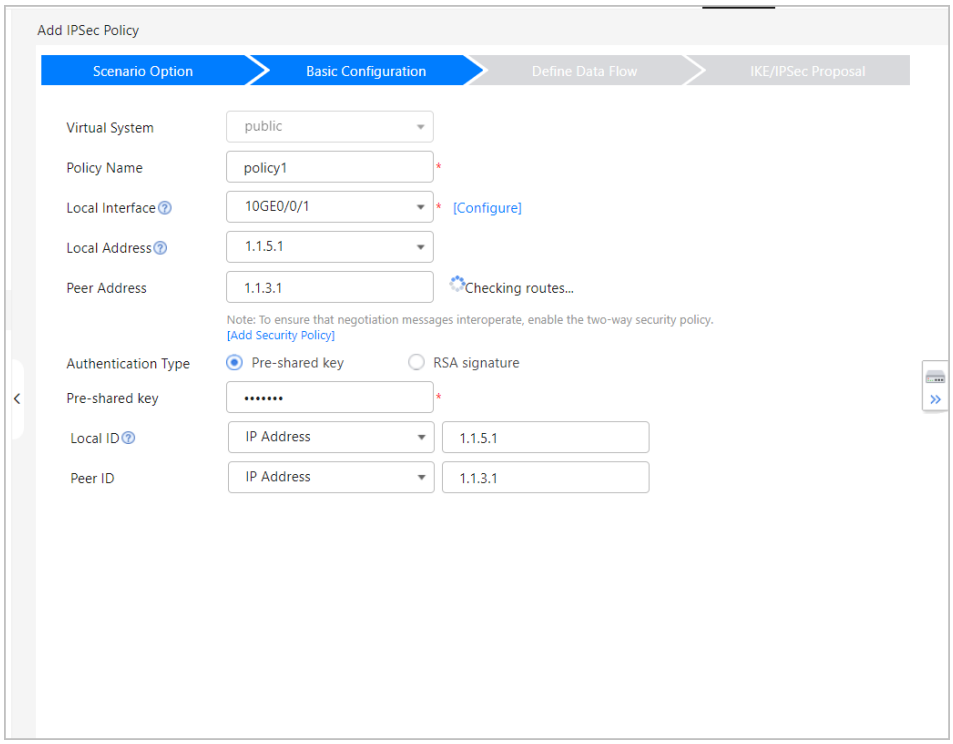


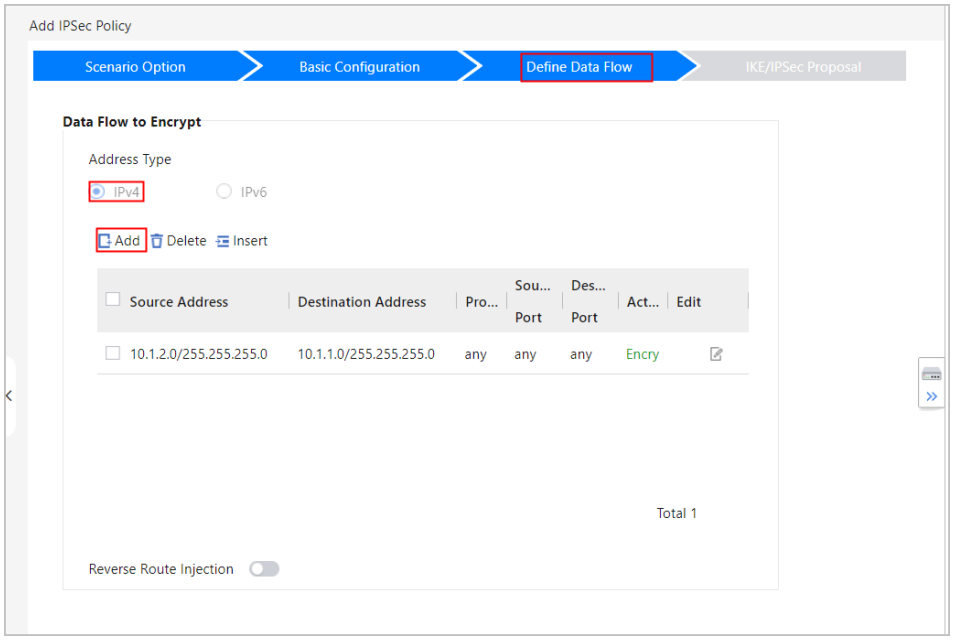
b. Click **Add** to create an IPsec policy as prompted.



The pre-shared key is YsHsjx_202206.

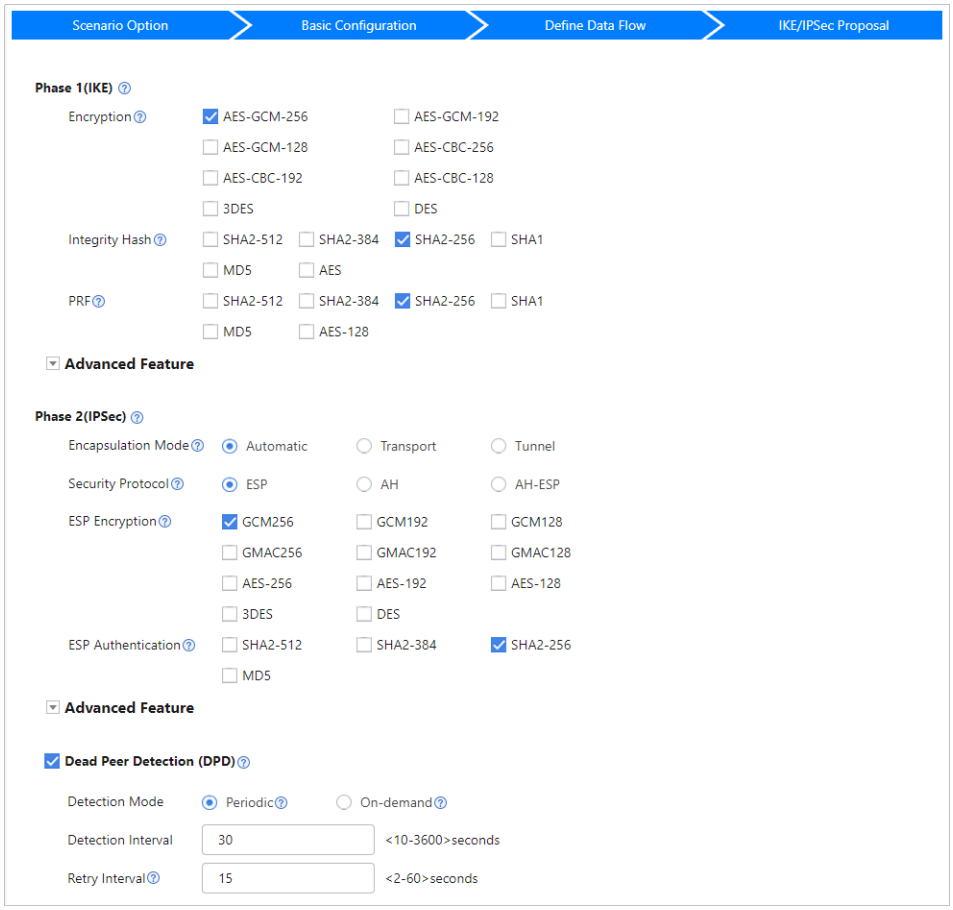
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

----End

Verifying the Configuration

1. Access a host or server on network B from a host on network A. The access succeeds.
2. In vsysa on DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

Policy Name	Status	Local Address	Peer Address
policy1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.3.1	1.1.5.1

3. On DeviceB, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following tunnel information is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Policy Name	Status	Local Address	Peer Address
policy1	IKE negotiation succeeded IPSec negotiation succeeded	1.1.5.1	1.1.3.1

Configuration Scripts

- public of DeviceA

```
#
vsys enable
resource-class r1
 resource-item-limit ipsec-tunnel reserved-number 5 maximum 20
#
vsys name vsysa 1
 assign interface GE0/0/1
 assign interface GE0/0/2
 assign resource-class r1
#
interface GE0/0/1
 ip binding vpn-instance vsysa
 ip address 1.1.3.1 255.255.255.0
 ipsec policy policy1
#
interface GE0/0/2
 ip binding vpn-instance vsysa
 ip address 10.1.1.1 255.255.255.0
```

- vsysa of DeviceA

```
#
switch vsys vsysa
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop2792077960
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 3
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike2792077960
 pre-shared-key %^%#m`wdHMo4eVMY2&*+hDV~BbN&<=zoQ@d{n%=**qR6%^%#
 ike-proposal 3
 remote-id-type ip
 remote-id 1.1.5.1
 local-id 1.1.3.1
 remote-address 1.1.5.1
#
ipsec policy ipsec2792077900 1 isakmp
 security acl 3000
 ike-peer ike2792077960
 proposal prop2792077960
 tunnel local applied-interface
#
interface GE0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip binding vpn-instance vsysa
 ip address 1.1.3.1 255.255.255.0
 ipsec policy ipsec2792077900
#
interface GE0/0/2
 ip binding vpn-instance vsysa
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_3
  source-zone untrust
  destination-zone local
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
 rule name policy_ipsec_4
  source-zone local
  destination-zone untrust
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
#
return
```

- DeviceB

```
#
acl number 3000
 rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop2792077960
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike2792077960
 pre-shared-key %^%#m`wdHMo4eVMY2&*+hDV~BbN&<=zoQ@d{n%=**qR6%^%#
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.3.1
 local-id 1.1.5.1
 remote-address 1.1.3.1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ipsec policy ipsec2792077900 1 isakmp
 security acl 3000
 ike-peer ike2792077960
 proposal prop2792077960
 tunnel local 1.1.3.1
#
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
 ipsec policy ipsec2792077900
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.5.2
#
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_3
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 mask 255.255.255.255
  destination-address 1.1.5.1 mask 255.255.255.255
  action permit
 rule name policy_ipsec_4
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 mask 255.255.255.255
  destination-address 1.1.3.1 mask 255.255.255.255
  action permit
#
return
```

8.4.2 CLI: Example for Configuring Virtual Systems to Use an Independent Public IP Address to Establish an IPsec Tunnel

Networking Requirements

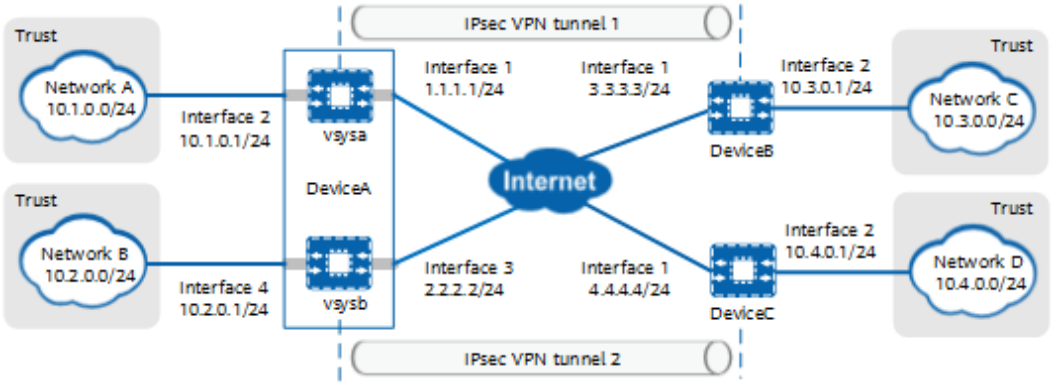
In **Figure 8-22**, multiple public network interfaces are configured on DeviceA, and each interface has a unique public IP address. These public network interfaces need to be allocated to different virtual systems, and an IPsec policy needs to be configured in each virtual system and applied to the corresponding public network interface. Each virtual system can then use a unique public IP address to establish an IPsec VPN tunnel with the remote gateway, securing communication between the virtual system network and the remote network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-22 Establishing IPsec VPN tunnels with remote gateways using unique public IP addresses

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4, respectively.



Item		Data
DeviceA	vsysa	Public network interface: GE 0/0/1 Public network interface IP address: 1.1.1.1/24 Security zone to which the public network interface belongs: Untrust
		Private network interface: GE 0/0/2 Private network interface IP address: 10.1.0.1/24 Private IP address range: 10.1.0.0/24 Security zone to which the private network interface belongs: Trust
		IPsec configuration Remote IP address: 3.3.3.3/24 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
	vsysb	Public network interface: GE 0/0/3 Public network interface IP address: 2.2.2.2/24 Security zone to which the public network interface belongs: Untrust

 Copyright © Huawei Technologies Co., Ltd.

Item		Data
		Private network interface: GE 0/0/4 Private network interface IP address: 10.2.0.1/24 Private address range: 10.2.0.0/24 Security zone to which the private network interface belongs: Trust
		IPsec configuration Remote IP address: 4.4.4.4/24 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceB		Interface: GE 0/0/1 IP address: 3.3.3.3/24 Security zone to which the interface belongs: Untrust
		Interface: GE 0/0/2 IP address: 10.3.0.1/24 Private IP address range: 10.3.0.0/24 Security zone to which the interface belongs: Trust
		IPsec configuration Remote IP address: 1.1.1.1/24 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any
DeviceC		Interface: GE 0/0/1 IP address: 4.4.4.4/24 Security zone to which the interface belongs: Untrust
		Interface: GE 0/0/2 IP address: 10.4.0.1/24 Private IP address range: 10.4.0.0/24 Security zone to which the interface belongs: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote IP address: 2.2.2.2/24 Authentication mode: PSK authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any

Configuration Roadmap

NOTE

The configuration roadmaps for vsysa and vsysb, and those for DeviceB and DeviceC are similar. This example describes how to configure vsysa and DeviceB to use unique public IP addresses to establish an IPsec VPN tunnel with remote gateways. For details about how to configure vsysb and DeviceC, see the configurations of vsysa and DeviceB.

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

- On DeviceA:
  a. In the public system, create virtual system vsysa and allocate resources to vsysa.
  b. In vsysa, configure interfaces, routes, and security policies.
  c. Configure an IPsec policy in vsysa, including basic IPsec policy information, data flows to be protected, and IPsec proposal negotiation parameters.
- On DeviceB:
  a. Perform basic interface configurations.
  b. Configure security policies to allow devices on specified private network segments to exchange packets.
  c. Configure a route to the remote virtual system.
  d. Configure an IPsec policy, including basic IPsec policy information, data flows to be protected, and IPsec proposal negotiation parameters.

Procedure

- Configure DeviceA.
  a. Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vsys enable
```

  b. Create virtual system vsysa and allocate resources to it.

     # Configure resource class **r1**, and set the guaranteed number and maximum number of IPsec tunnels.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] resource-class r1
[DeviceA-resource-class-r1] resource-item-limit ipsec-tunnel reserved-number 10 maximum
500
[DeviceA-resource-class-r1] quit
```

Create virtual system vsysa.

```
[DeviceA] vsys name vsysa
[DeviceA-vsys-vsysa] assign interface ge 0/0/1
[DeviceA-vsys-vsysa] assign interface ge 0/0/2
[DeviceA-vsys-vsysa] assign resource-class r1
[DeviceA-vsys-vsysa] quit
```

c. Access vsysa, configure GE 0/0/1 and GE 0/0/2 and configure parameters for the interfaces.

Configure GE 0/0/1.

```
[Device] switch vsys vsysa
<DeviceA-vsysa> system-view
[DeviceA-vsysa] interface ge 0/0/1
[DeviceA-vsysa-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-vsysa-GE0/0/1] quit
```

Configure GE 0/0/2.

```
[DeviceA-vsysa] interface ge 0/0/2
[DeviceA-vsysa-GE0/0/2] ip address 10.1.0.1 255.255.255.0
[DeviceA-vsysa-GE0/0/2] quit
```

d. Add interfaces to security zones.

Add GE 0/0/2 to the Trust zone.

```
[DeviceA-vsysa] firewall zone trust
[DeviceA-vsysa-zone-trust] add interface ge 0/0/2
[DeviceA-vsysa-zone-trust] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA-vsysa] firewall zone untrust
[DeviceA-vsysa-zone-untrust] add interface ge 0/0/1
[DeviceA-vsysa-zone-untrust] quit
```

e. Configure a static route to the remote network and a default route to the Internet. Assume that the next-hop IP address of the route from vsysa to the Internet is 1.1.1.2.

Configure a static route to the remote network.

```
[DeviceA-vsysa] ip route-static 10.3.0.0 255.255.255.0 1.1.1.2
```

Configure a default route destined for the Internet.

```
[DeviceA-vsysa] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

f. Configure security policies.

Configure a security policy between the Trust and Untrust zones to allow users in network A to access the resources of network C.

```
[DeviceA-vsysa] security-policy
[DeviceA-vsysa-policy-security] rule name sec_policy_1
[DeviceA-vsysa-policy-security-rule-sec_policy_1] source-zone trust
[DeviceA-vsysa-policy-security-rule-sec_policy_1] destination-zone untrust
[DeviceA-vsysa-policy-security-rule-sec_policy_1] source-address 10.1.0.0 mask 255.255.255.0
[DeviceA-vsysa-policy-security-rule-sec_policy_1] destination-address 10.3.0.0 mask
255.255.255.0
[DeviceA-vsysa-policy-security-rule-sec_policy_1] action permit
[DeviceA-vsysa-policy-security-rule-sec_policy_1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy between the Untrust and Trust zones to allow users in network C to access the resources of network A.

```
[DeviceA-vsysa-policy-security] rule name sec_policy_2
[DeviceA-vsysa-policy-security-rule-sec_policy_2] source-zone untrust
[DeviceA-vsysa-policy-security-rule-sec_policy_2] destination-zone trust
[DeviceA-vsysa-policy-security-rule-sec_policy_2] source-address 10.3.0.0 mask 255.255.255.0
[DeviceA-vsysa-policy-security-rule-sec_policy_2] destination-address 10.1.0.0 mask
255.255.255.0
[DeviceA-vsysa-policy-security-rule-sec_policy_2] action permit
[DeviceA-vsysa-policy-security-rule-sec_policy_2] quit
```

Configure a security policy between the Local and Untrust zones to allow vsysa to establish an IPsec tunnel with the remote device.

```
[DeviceA-vsysa-policy-security] rule name sec_policy_3
[DeviceA-vsysa-policy-security-rule-sec_policy_3] source-zone local
[DeviceA-vsysa-policy-security-rule-sec_policy_3] destination-zone untrust
[DeviceA-vsysa-policy-security-rule-sec_policy_3] source-address 1.1.1.1 mask 255.255.255.255
[DeviceA-vsysa-policy-security-rule-sec_policy_3] destination-address 3.3.3.3 mask
255.255.255.255
[DeviceA-vsysa-policy-security-rule-sec_policy_3] action permit
[DeviceA-vsysa-policy-security-rule-sec_policy_3] quit
```

Configure a security policy between the Untrust and Local zones to allow the remote device to establish an IPsec tunnel with vsysa.

```
[DeviceA-vsysa-policy-security] rule name sec_policy_4
[DeviceA-vsysa-policy-security-rule-sec_policy_4] source-zone untrust
[DeviceA-vsysa-policy-security-rule-sec_policy_4] destination-zone local
[DeviceA-vsysa-policy-security-rule-sec_policy_4] source-address 3.3.3.3 mask 255.255.255.255
[DeviceA-vsysa-policy-security-rule-sec_policy_4] destination-address 1.1.1.1 mask
255.255.255.255
[DeviceA-vsysa-policy-security-rule-sec_policy_4] action permit
[DeviceA-vsysa-policy-security-rule-sec_policy_4] quit
[DeviceA-vsysa-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

g. Configure an IPsec policy on vsysa and apply the policy to an interface.

Define data flows to be protected. Configure advanced ACL 3000 to allow users on network segment 10.1.0.0/24 to access network segment 10.3.0.0/24.

```
[DeviceA-vsysa] acl 3000
[DeviceA-vsysa-acl4-advance-3000] rule 5 permit ip source 10.1.0.0 0.0.0.255 destination
10.3.0.0 0.0.0.255
[DeviceA-vsysa-acl4-advance-3000] quit
```

Configure an IPsec proposal. You can use the default parameter settings.

```
[DeviceA-vsysa] ipsec proposal tran1
[DeviceA-vsysa-ipsec-proposal-tran1] encapsulation-mode auto
[DeviceA-vsysa-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-vsysa-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-vsysa-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceA-vsysa] ike proposal 1
[DeviceA-vsysa-ike-proposal-1] encryption-algorithm aes-gcm-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-vsysa-ike-proposal-1] authentication-algorithm sha2-256
[DeviceA-vsysa-ike-proposal-1] authentication-method pre-share
[DeviceA-vsysa-ike-proposal-1] integrity-algorithm hmac-sha2-256
[DeviceA-vsysa-ike-proposal-1] prf hmac-sha2-256
[DeviceA-vsysa-ike-proposal-1] dh group2
[DeviceA-vsysa-ike-proposal-1] quit
```

Configure an IKE peer.

```
[DeviceA-vsysa] ike peer a
[DeviceA-vsysa-ike-peer-a] ike-proposal 1
[DeviceA-vsysa-ike-peer-a] remote-address 3.3.3.3
[DeviceA-vsysa-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceA-vsysa-ike-peer-a] quit
```

Configure an IPsec policy.

```
[DeviceA-vsysa] ipsec policy ipsec1 1 isakmp
[DeviceA-vsysa-ipsec-policy-isakmp-ipsec1-1] security acl 3000
[DeviceA-vsysa-ipsec-policy-isakmp-ipsec1-1] proposal tran1
[DeviceA-vsysa-ipsec-policy-isakmp-ipsec1-1] ike-peer a
[DeviceA-vsysa-ipsec-policy-isakmp-ipsec1-1] quit
```

Apply IPsec policy group **ipsec1** to GE 0/0/1.

```
[DeviceA-vsysa] interface ge 0/0/1
[DeviceA-vsysa-GE0/0/1] ipsec policy ipsec1
[DeviceA-vsysa-GE0/0/1] quit
```

- Configure DeviceB.
  a. Configure IP addresses for interfaces and add interfaces to security zones.

     # Configure GE 0/0/1.

     ```
     <HUAWEI> system-view
     [HUAWEI] sysname DeviceB
     [DeviceB] interface ge 0/0/1
     [DeviceB-GE0/0/1] ip address 3.3.3.3 255.255.255.0
     [DeviceB-GE0/0/1] quit
     ```

     # Configure GE 0/0/2.

     ```
     [DeviceB] interface ge 0/0/2
     [DeviceB-GE0/0/2] ip address 10.3.0.1 255.255.255.0
     [DeviceB-GE0/0/2] quit
     ```

     # Add GE 0/0/2 to the Trust zone.

     ```
     [DeviceB] firewall zone trust
     [DeviceB-zone-trust] add interface ge 0/0/2
     [DeviceB-zone-trust] quit
     ```

     # Add GE 0/0/1 to the Untrust zone.

     ```
     [DeviceB] firewall zone untrust
     [DeviceB-zone-untrust] add interface ge 0/0/1
     [DeviceB-zone-untrust] quit
     ```

  b. Configure a static route to the remote network and a default route to the Internet. Assume that the next-hop IP address of the route from DeviceB to the Internet is 3.3.3.4.

     # Configure a static route to the remote network.

     ```
     [DeviceB] ip route-static 10.1.0.0 255.255.255.0 3.3.3.4
     ```

     # Configure a default route destined for the Internet.

     ```
     [DeviceB] ip route-static 0.0.0.0 0.0.0.0 3.3.3.4
     ```

  c. Configure security policies.

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy between the Trust and Untrust zones to allow users in network C to access the resources of network A.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name sec_policy_1
[DeviceB-policy-security-rule-sec_policy_1] source-zone trust
[DeviceB-policy-security-rule-sec_policy_1] destination-zone untrust
[DeviceB-policy-security-rule-sec_policy_1] source-address 10.3.0.0 mask 255.255.255.0
[DeviceB-policy-security-rule-sec_policy_1] destination-address 10.1.0.0 mask 255.255.255.0
[DeviceB-policy-security-rule-sec_policy_1] action permit
[DeviceB-policy-security-rule-sec_policy_1] quit
```

Configure a security policy between the Untrust and Trust zones to allow users in network A to access the resources of network C.

```
[DeviceB-policy-security] rule name sec_policy_2
[DeviceB-policy-security-rule-sec_policy_2] source-zone untrust
[DeviceB-policy-security-rule-sec_policy_2] destination-zone trust
[DeviceB-policy-security-rule-sec_policy_2] source-address 10.1.0.0 mask 255.255.255.0
[DeviceB-policy-security-rule-sec_policy_2] destination-address 10.3.0.0 mask 255.255.255.0
[DeviceB-policy-security-rule-sec_policy_2] action permit
[DeviceB-policy-security-rule-sec_policy_2] quit
```

Configure an interzone security policy between the Local zone and Untrust zone to allow DeviceB to establish an IPsec tunnel with the remote device.

```
[DeviceB-policy-security] rule name sec_policy_3
[DeviceB-policy-security-rule-sec_policy_3] source-zone local
[DeviceB-policy-security-rule-sec_policy_3] destination-zone untrust
[DeviceB-policy-security-rule-sec_policy_3] source-address 3.3.3.3 mask 255.255.255.255
[DeviceB-policy-security-rule-sec_policy_3] destination-address 1.1.1.1 mask 255.255.255.255
[DeviceB-policy-security-rule-sec_policy_3] action permit
[DeviceB-policy-security-rule-sec_policy_3] quit
```

Configure an interzone security policy between the Untrust zone and Local zone to allow the remote device to establish an IPsec tunnel with DeviceB.

```
[DeviceB-policy-security] rule name sec_policy_4
[DeviceB-policy-security-rule-sec_policy_4] source-zone untrust
[DeviceB-policy-security-rule-sec_policy_4] destination-zone local
[DeviceB-policy-security-rule-sec_policy_4] source-address 1.1.1.1 mask 255.255.255.255
[DeviceB-policy-security-rule-sec_policy_4] destination-address 3.3.3.3 mask 255.255.255.255
[DeviceB-policy-security-rule-sec_policy_4] action permit
[DeviceB-policy-security-rule-sec_policy_4] quit
[DeviceB-policy-security] quit
```

d. Configure an IPsec policy and apply it to an interface.

Define data flows to be protected. Configure advanced ACL 3000 to allow users on network segment 10.3.0.0/24 to access network segment 10.1.0.0/24.

```
[DeviceB] acl 3000
[DeviceB-acl4-advance-3000] rule 5 permit ip source 10.3.0.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
[DeviceB-acl4-advance-3000] quit
```

Configure an IPsec proposal. You can use the default parameter settings.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] encapsulation-mode auto
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] encryption-algorithm aes-gcm-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-ike-proposal-1] authentication-algorithm sha2-256
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-1] prf hmac-sha2-256
[DeviceB-ike-proposal-1] dh group2
[DeviceB-ike-proposal-1] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 1
[DeviceB-ike-peer-a] remote-address 1.1.1.1
[DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-a] quit
```

Configure an IPsec policy.

```
[DeviceB] ipsec policy ipsec1 1 isakmp
[DeviceB-ipsec-policy-isakmp-ipsec1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-ipsec1-1] proposal tran1
[DeviceB-ipsec-policy-isakmp-ipsec1-1] ike-peer a
[DeviceB-ipsec-policy-isakmp-ipsec1-1] quit
```

Apply IPsec policy group **ipsec1** to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy ipsec1
[DeviceB-GE0/0/1] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping** command on the PC on network A to enable the PC to access the PC on network C, triggering IKE negotiation.

   If IKE negotiation is successful, an IPsec tunnel can be established and the ping will be successful. If IKE negotiation fails, no IPsec tunnel can be established and the ping will fail.

2. Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB to check SA information. The following shows the command outputs of DeviceB, which if similar, indicate that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa

Ike sa information :
   Conn-ID      Peer          VPN          Flag(s)             Phase
 -------------------------------------------------------------------------------
   16777239     1.1.1.1                    RD|ST|A             v2:2
   16777232     1.1.1.1                    RD|ST|A             v2:1

  Number of SA entries  : 2

  Number of SA entries of all cpu : 2

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceB> display ipsec sa

ipsec sa information:

===============================
Interface: GE0/0/1
===============================

  ----------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
IPsec policy name: "ipsec1"
Sequence number  : 1
Acl group        : 3000
Acl rule         : 5
Mode             : ISAKMP
-----------------------------
  Connection ID     : 83903371
  Encapsulation mode: Tunnel
  Tunnel local      : 3.3.3.3
  Tunnel remote     : 1.1.1.1
  Flow source       : 10.3.0.1/255.255.255.255 0/0
  Flow destination  : 10.1.0.1/255.255.255.255 0/0

  [Outbound ESP SAs]
    SPI: 763065754 (0x2d7b759a)
    Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
    SA remaining key duration (kilobytes/sec): 0/3079
    Max sent sequence-number: 1
    UDP encapsulation used for NAT traversal: N
    SA encrypted packets (number/kilobytes): 4/0

  [Inbound ESP SAs]
    SPI: 163241969 (0x9badff1)
    Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
    SA remaining key duration (kilobytes/sec): 0/3079
    Max received sequence-number: 3203668
    UDP encapsulation used for NAT traversal: N
    SA decrypted packets (number/kilobytes): 4/0
    Anti-replay : Disable
```

Configuration Scripts

- DeviceA public system

```
#
sysname DeviceA
#
vsys enable
#
resource-class r1
 resource-item-limit ipsec-tunnel reserved-number 10 maximum 500
#
vsys name vsysa 1
 assign interface GE0/0/1
 assign interface GE0/0/2
 assign resource-class r1
#
vsys name vsysb 2
 assign interface GE0/0/3
 assign interface GE0/0/4
 assign resource-class r1
#
interface GE0/0/1
 ip binding vpn-instance vsysa
 ip address 1.1.1.1 255.255.255.0
 ipsec policy ipsec1
#
interface GE0/0/2
 ip binding vpn-instance vsysa
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/3
 ip binding vpn-instance vsysb
 ip address 2.2.2.2 255.255.255.0
 ipsec policy ipsec2
#
interface GE0/0/4
 ip binding vpn-instance vsysb
 ip address 10.2.0.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

- DeviceA virtual system vsysa

```
#
switch vsys vsysa
#
acl number 3000
 rule 5 permit ip source 10.1.0.0 0.0.0.255 destination 10.3.0.0 0.0.0.255
#
ipsec proposal tran1
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group2
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#m`wdHMo4eVMY2&*+hDV~BbN&<=zoQ@d{n%=**qR6%+%#
 ike-proposal 1
 remote-id-type ip
 remote-id 3.3.3.3
 local-id 1.1.1.1
 remote-address 3.3.3.3
#
ipsec policy ipsec1 1 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/1
 ip binding vpn-instance vsysa
 ip address 1.1.1.1 255.255.255.0
 ipsec policy ipsec1
#
interface GE0/0/2
 ip binding vpn-instance vsysa
 ip address 10.1.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name sec_policy_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_2
  source-zone untrust
  destination-zone trust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule name sec_policy_4
  source-zone untrust
  destination-zone local
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
ip route-static 10.3.0.0 255.255.255.0 1.1.1.2
#
return
```

- DeviceA virtual system vsysb

```
#
switch vsys vsysb
#
acl number 3001
 rule 5 permit ip source 10.2.0.0 0.0.0.255 destination 10.4.0.0 0.0.0.255
#
ipsec proposal tran2
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 2
 encryption-algorithm aes-gcm-256
 dh group2
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 pre-shared-key %+%#m`wdHMo4eVMY2&*+hDV~BbN&<=zoQ@d{n%=**qR6%+%#
 ike-proposal 2
 remote-id-type ip
 remote-id 4.4.4.4
 local-id 2.2.2.2
 remote-address 4.4.4.4
#
ipsec policy ipsec2 1 isakmp
 security acl 3001
 ike-peer b
 proposal tran2
#
interface GE0/0/3
 ip binding vpn-instance vsysb
 ip address 2.2.2.2 255.255.255.0
 ipsec policy ipsec2
#
interface GE0/0/4
 ip binding vpn-instance vsysb
 ip address 10.2.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/3
#
security-policy
 rule name sec_policy_1
  source-zone trust
  destination-zone untrust
  source-address 10.2.0.0 mask 255.255.255.0
  destination-address 10.4.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-zone trust
 source-address 10.4.0.0 mask 255.255.255.0
 destination-address 10.2.0.0 mask 255.255.255.0
 action permit
rule name sec_policy_3
 source-zone local
 destination-zone untrust
 source-address 2.2.2.2 mask 255.255.255.255
 destination-address 4.4.4.4 mask 255.255.255.255
 action permit
rule name sec_policy_4
 source-zone untrust
 destination-zone local
 source-address 4.4.4.4 mask 255.255.255.255
 destination-address 2.2.2.2 mask 255.255.255.255
 action permit
#
ip route-static 0.0.0.0 0.0.0.0 2.2.2.3
ip route-static 10.4.0.0 255.255.255.0 2.2.2.3
#
return
```

- DeviceB

```
#
sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.3.0.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group2
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#@ama1^ws3/PX+B.f~tnNDy(q~gjoR%dmP6.\U#5~%+%#
 ike-proposal 1
 remote-id-type ip
 remote-id 1.1.1.1
 local-id 3.3.3.3
 remote-address 1.1.1.1
#
ipsec policy ipsec1 1 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
 ipsec policy ipsec1
#
interface GE0/0/2
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.4
ip route-static 10.1.0.0 255.255.255.0 3.3.3.4
#
security-policy
 rule name sec_policy_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.1.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 mask 255.255.255.0
  destination-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  action permit
 rule name sec_policy_4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
#
return
```

- DeviceC

```
#
sysname FW_C
#
acl number 3000
 rule 5 permit ip source 10.4.0.0 0.0.0.255 destination 10.2.0.0 0.0.0.255
#
ipsec proposal tran1
 encapsulation-mode auto
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group2
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#@ama1^ws3/PX+B.f~tnNDy(q~gjoR%dmP6.\U#5~%+%#
 ike-proposal 1
 remote-id-type ip
 remote-id 2.2.2.2
 local-id 4.4.4.4
 remote-address 2.2.2.2
#
ipsec policy ipsec1 1 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
interface GE0/0/1
 ip address 4.4.4.4 255.255.255.0
 ipsec policy ipsec1
#
interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 10.4.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.5
ip route-static 10.1.0.0 255.255.255.0 4.4.4.5
#
security-policy
 rule name sec_policy_1
  source-zone trust
  destination-zone untrust
  source-address 10.4.0.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_2
  source-zone untrust
  destination-zone trust
  source-address 10.2.0.0 mask 255.255.255.0
  destination-address 10.4.0.0 mask 255.255.255.0
  action permit
 rule name sec_policy_3
  source-zone local
  destination-zone untrust
  source-address 4.4.4.4 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name sec_policy_4
  source-zone untrust
  destination-zone local
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 4.4.4.4 mask 255.255.255.255
  action permit
#
return
```

8.4.3 CLI: Example for Establishing an IPsec Tunnel Within the Same VPN Instance

Context

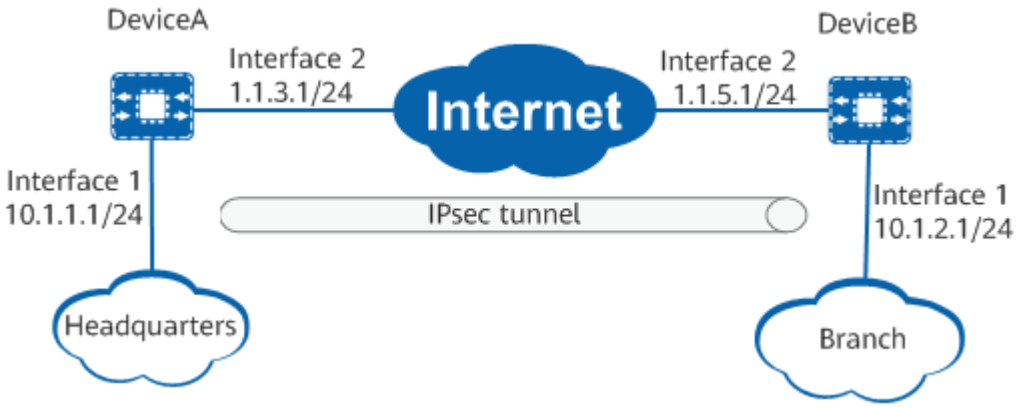
In **Figure 8-23**, the headquarters is connected to the Internet through DeviceA, and the branch is connected to the Internet through DeviceB. DeviceA and DeviceB establish an IPsec tunnel for secure communication. To prevent IPsec services on DeviceA from being affected by other services, the enterprise requires that a VPN instance be created on DeviceA and bound to the IPsec tunnel for service isolation.

Figure 8-23 Configuring an IPsec tunnel in a VPN instance

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

1. Create a VPN instance named **vpn1** on DeviceA.
2. Configure routes for the VPN instance.
3. Set IPsec policy parameters for the VPN instance. When configuring an IKE peer, you need to bind an IPsec tunnel to a VPN instance.

Procedure

- Configure DeviceA (at the headquarters).
  a. Configure a VPN instance named **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] ip vpn-instance vpn1
[DeviceA-vpn-instance-vpn1] route-distinguisher 100:1
[DeviceA-vpn-instance-vpn1] quit
```

  b. Configure IP addresses for interfaces and add interfaces to security zones.

Configure an IP address for GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip binding vpn-instance vpn1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip binding vpn-instance vpn1
[DeviceA-GE0/0/2] ip address 1.1.3.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

c. Configure a static route destined for DeviceB. The following assumes that the next-hop IP address is 1.1.3.2. This route instructs DeviceA to forward packets from the headquarters to the branch.

```
[DeviceA] ip route-static vpn-instance vpn1 1.1.5.0 24 1.1.3.2
[DeviceA] ip route-static vpn-instance vpn1 10.1.2.0 24 1.1.3.2
```

d. Configure security policies.

Configure security policies between the Trust and Untrust zones to permit pre-encapsulated and decapsulated packets.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name 1
[DeviceA-policy-security-rule-1] source-zone untrust
[DeviceA-policy-security-rule-1] destination-zone trust
[DeviceA-policy-security-rule-1] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-1] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-1] action permit
[DeviceA-policy-security-rule-1] quit
[DeviceA-policy-security] rule name 2
[DeviceA-policy-security-rule-2] source-zone trust
[DeviceA-policy-security-rule-2] destination-zone untrust
[DeviceA-policy-security-rule-2] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-2] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-2] action permit
[DeviceA-policy-security-rule-2] quit
```

Configure security policies between the Local and Untrust zones to permit IKE negotiation packets.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name 3
[DeviceA-policy-security-rule-3] source-zone local
[DeviceA-policy-security-rule-3] destination-zone untrust
[DeviceA-policy-security-rule-3] source-address 1.1.3.1 32
[DeviceA-policy-security-rule-3] destination-address 1.1.5.1 32
[DeviceA-policy-security-rule-3] action permit
[DeviceA-policy-security-rule-3] quit
[DeviceA-policy-security] rule name 4
[DeviceA-policy-security-rule-4] source-zone untrust
[DeviceA-policy-security-rule-4] destination-zone local
[DeviceA-policy-security-rule-4] source-address 1.1.5.1 32
[DeviceA-policy-security-rule-4] destination-address 1.1.3.1 32
[DeviceA-policy-security-rule-4] action permit
[DeviceA-policy-security-rule-4] quit
[DeviceA-policy-security] quit
```

e. Configure IPsec.

Configure an ACL to define the data flows to be protected, and bind the ACL to the specified VPN instance.

```
[DeviceA] acl 3000
[DeviceA-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255 vpn-instance vpn1
[DeviceA-acl4-advance-3000] quit
```

Configure an IPsec proposal.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] transform esp
[DeviceA-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

Create an IKE proposal. You can use the default parameter settings.

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] dh group14
[DeviceA-ike-proposal-1] quit
```

Configure an IKE peer.

```
[DeviceA] ike peer b
[DeviceA-ike-peer-b] ike-proposal 1
[DeviceA-ike-peer-b] pre-shared-key Key123
[DeviceA-ike-peer-b] remote-address vpn-instance vpn1 1.1.5.1
[DeviceA-ike-peer-b] sa binding vpn-instance vpn1
[DeviceA-ike-peer-b] quit
```

Configure an ISAKMP IPsec policy.

```
[DeviceA] ipsec policy map1 1 isakmp
[DeviceA-ipsec-policy-isakmp-map1-1] ike-peer b
[DeviceA-ipsec-policy-isakmp-map1-1] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-1] quit
```

Apply an IPsec policy to GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipsec policy map1
[DeviceA-GE0/0/2] quit
```

- Configure DeviceB (at the branch).
  a. Configure IP addresses for interfaces and add interfaces to security zones.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ip address 10.1.2.1 24
[DeviceB-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] ip address 1.1.5.1 24
[DeviceB-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/1
[DeviceB-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/2
[DeviceB-zone-untrust] quit
```

  b. Configure a static route destined for DeviceA. The following assumes that the next-hop IP address is 1.1.5.2. This route instructs DeviceB to forward packets from the branch to the headquarters.

```
[DeviceB] ip route-static 10.1.1.0 24 1.1.5.2
[DeviceB] ip route-static 1.1.3.0 24 1.1.5.2
```

  c. Configure security policies.

Configure security policies between the Trust and Untrust zones to permit pre-encapsulated and decapsulated packets.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name 1
[DeviceB-policy-security-rule-1] source-zone untrust
[DeviceB-policy-security-rule-1] destination-zone trust
[DeviceB-policy-security-rule-1] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-1] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-1] action permit
[DeviceB-policy-security-rule-1] quit
[DeviceB-policy-security] rule name 2
[DeviceB-policy-security-rule-2] source-zone trust
[DeviceB-policy-security-rule-2] destination-zone untrust
[DeviceB-policy-security-rule-2] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-2] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-2] action permit
[DeviceB-policy-security-rule-2] quit
```

Configure security policies between the Local and Untrust zones to permit IKE negotiation packets.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name 3
[DeviceB-policy-security-rule-3] source-zone local
[DeviceB-policy-security-rule-3] destination-zone untrust
[DeviceB-policy-security-rule-3] source-address 1.1.5.1 32
[DeviceB-policy-security-rule-3] destination-address 1.1.3.1 32
[DeviceB-policy-security-rule-3] action permit
[DeviceB-policy-security-rule-3] quit
[DeviceB-policy-security] rule name 4
[DeviceB-policy-security-rule-4] source-zone untrust
[DeviceB-policy-security-rule-4] destination-zone local
[DeviceB-policy-security-rule-4] source-address 1.1.3.1 32
[DeviceB-policy-security-rule-4] destination-address 1.1.5.1 32
[DeviceB-policy-security-rule-4] action permit
[DeviceB-policy-security-rule-4] quit
[DeviceB-policy-security] quit
```

d. Configure IPsec.

Configure an ACL to define the data flow to be protected.

```
[DeviceB] acl 3000
[DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl4-advance-3000] quit
```

Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] transform esp
[DeviceB-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Create an IKE proposal. You can use the default parameter settings.

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer a
[DeviceB-ike-peer-a] ike-proposal 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-ike-peer-a] pre-shared-key Key123
[DeviceB-ike-peer-a] remote-address 1.1.3.1
[DeviceB-ike-peer-a] quit
```

Configure a non-template IPsec policy.

```
[DeviceB] ipsec policy map1 1 isakmp
[DeviceB-ipsec-policy-isakmp-map1-1] ike-peer a
[DeviceB-ipsec-policy-isakmp-map1-1] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-1] quit
```

Apply an IPsec policy to GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] ipsec policy map1
[DeviceB-GE0/0/2] quit
```

----End

Verifying the Configuration

After the configuration is complete, users at the headquarters and branch can communicate with each other. Run the **display ike sa** and **display ipsec sa brief** commands on DeviceA and DeviceB to check SA information. The following shows the command outputs of DeviceA, which if similar, indicate that IKE SAs and IPsec SAs have been established.

```
<DeviceA> display ike sa
IKE SA information :
  Conn-ID     Peer           VPN   Flag(s)  Phase  RemoteType  RemoteID
 -------------------------------------------------------------------------------
  10         1.1.5.1:500     vpn1  RD|ST|A  V2:2   IP          1.1.5.1
  9          1.1.5.1:500     vpn1  RD|ST|A  V2:1   IP          1.1.5.1

 Number of IKE SA : 2
 -------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceA> display ipsec sa brief
Current ipsec sa num:2

Spu board slot 0, cpu 0 ipsec sa information:
Number of SAs:4
  Src address   Dst address      SPI       VPN   Protocol     Algorithm
-------------------------------------------------------------------------------
  1.1.5.1       1.1.3.1      4001819557  vpn1    ESP      E:AES-256-GCM-128 A:SHA2-256-128
  1.1.3.1       1.1.5.1      3923280450  vpn1    ESP      E:AES-256-GCM-128 A:SHA2-256-128
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ip vpn-instance vpn1
 route-distinguisher 100:1
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 vpn-instance vpn1
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 pre-shared-key %+%#cnEDZkL3}#J"qG/2iTb&P9q/%+%#
 ike-proposal 1
 remote-address vpn-instance vpn1 1.1.5.1
 sa binding vpn-instance vpn1
#
ipsec policy map1 1 isakmp
 security acl 3000
 ike-peer b
 proposal tran1

#
interface GE0/0/1
 ip binding vpn-instance vpn1
 ip address 10.1.1.1 24
#
interface GE0/0/2
 ip binding vpn-instance vpn1
 ip address 1.1.3.1 255.255.255.0
 ipsec policy map1
#
firewall zone trust
 add interface GE0/0/1
#
firewall zone untrust
 add interface GE0/0/2
#
ip route-static vpn-instance vpn1 1.1.5.0 255.255.255.0 1.1.3.2
ip route-static vpn-instance vpn1 10.1.2.0 255.255.255.0 1.1.3.2
#
security-policy
 rule name 1
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 24
  destination-address 10.1.1.0 24
  action permit
 rule name 2
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
  destination-address 10.1.2.0 24
  action permit
 rule name 3
  source-zone local
  destination-zone untrust
  source-address 1.1.3.1 32
  destination-address 1.1.5.1 32
  action permit
 rule name 4
  source-zone untrust
  destination-zone local
  source-address 1.1.5.1 32
  destination-address 1.1.3.1 32
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%#1tx/S9a;iF[L)QFz!$p;y]Lg%+%#
 ike-proposal 1
 remote-address 1.1.3.1
#
ipsec policy map1 1 isakmp
 security acl 3000
 ike-peer a
 proposal tran1

#
interface GE0/0/1
 ip address 10.1.2.1 24
#
interface GE0/0/2
 ip address 1.1.5.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/1
#
firewall zone untrust
 add interface GE0/0/2
#
 ip route-static 10.1.1.0 255.255.255.0 1.1.5.2
 ip route-static 1.1.3.0 255.255.255.0 1.1.5.2
#
security-policy
 rule name 1
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 24
  destination-address 10.1.2.0 24
  action permit
 rule name 2
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 24
  destination-address 10.1.1.0 24
  action permit
 rule name 3
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 32
  destination-address 1.1.3.1 32
  action permit
 rule name 4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 32
  destination-address 1.1.5.1 32
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

8.4.4 CLI: Example for Establishing an IPsec Tunnel Across VPN Instances

Networking Requirements

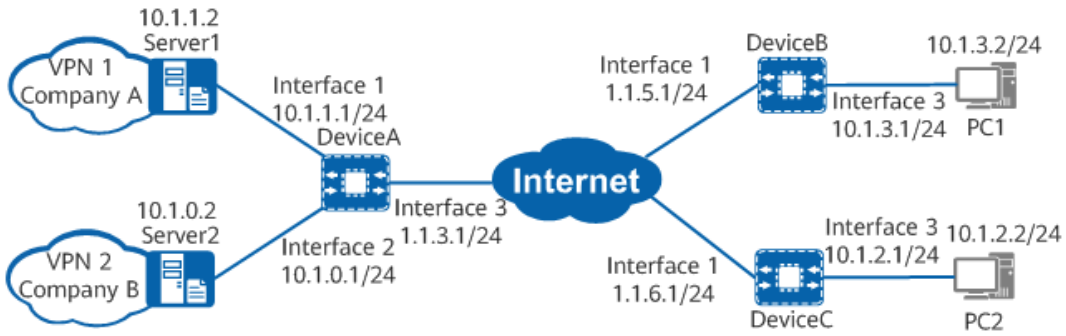
DeviceA is deployed by a carrier as an IPsec gateway, and is leased by multiple small companies to create VPN instances for them. Each company has an independent VPN network granting secure access to the headquarters' network for branch employees or those working remotely.

In **Figure 8-24**, PC1 is located on the branch network of company A, and PC2 is located on the branch network of company B. Branches of companies A and B are connected to the Internet through their respective IPsec gateways. On DeviceA, create VPN 1 for company A so that PC1 can securely access VPN 1, and create VPN 2 for company B so that PC2 can securely access VPN 2. There are reachable routes between DeviceA and DeviceB, and between DeviceA and DeviceC.

Figure 8-24 IPsec multi-instance

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

1. GE 0/0/3 of DeviceA is connected to the Internet and belongs to the public network, that is, the public system. GE 0/0/1 is connected to the intranet of company A and is bound to the VPN instance **vpn1**. GE 0/0/2 is connected to the intranet of company B and is bound to the VPN instance **vpn2**.
2. Configure two tunnel interfaces (Tunnel 0 and Tunnel 1), and bind Tunnel 0 to **vpn1** and Tunnel 1 to **vpn2**. This example uses tunnel interfaces to implement inter-VPN IPsec forwarding.
3. Configure two IPsec policies with the local IP address set to the IP address of GE 0/0/3. Use the local and remote IP addresses (IP address of GE 0/0/1 on

 Copyright © Huawei Technologies Co., Ltd.

DeviceB and IP address of GE 0/0/1 on DeviceC) for tunnel negotiation. These interfaces belong to the public system.

4. Apply the IPsec policies to the tunnel interfaces.

Procedure

- Configure DeviceA.
  a. Configure VPN instances **vpn1** and **vpn2**.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] ip vpn-instance vpn1
[DeviceA-vpn-instance-vpn1] route-distinguisher 100:1
[DeviceA-vpn-instance-vpn1] quit
[DeviceA] ip vpn-instance vpn2
[DeviceA-vpn-instance-vpn2] route-distinguisher 200:1
[DeviceA-vpn-instance-vpn2] quit
```

  b. Configure IP addresses for interfaces and add interfaces to security zones.

     # Configure IP addresses for intranet interfaces GE 0/0/1 and GE 0/0/2.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip binding vpn-instance vpn1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip binding vpn-instance vpn2
[DeviceA-GE0/0/2] ip address 10.1.0.1 24
[DeviceA-GE0/0/2] quit
```

     # Configure an IP address for the public network interface GE 0/0/3.

```
[DeviceA] interface ge 0/0/3
[Device-GE0/0/3] ip address 1.1.3.1 24
[DeviceA-GE0/0/3] quit
```

     # Create and bind Tunnel 0 and Tunnel 1 to VPN instances **vpn1** and **vpn2**, respectively.

```
[DeviceA] interface Tunnel 0
[DeviceA-tunnel0] tunnel-protocol ipsec
[DeviceA-tunnel0] ip binding vpn-instance vpn1
[DeviceA-tunnel0] ip address 10.10.1.2 24
[DeviceA-tunnel0] source 1.1.3.1
[DeviceA-tunnel0] quit
[DeviceA] interface Tunnel 1
[DeviceA-tunnel1] tunnel-protocol ipsec
[DeviceA-tunnel1] ip binding vpn-instance vpn2
[DeviceA-tunnel1] ip address 10.10.1.1 24
[DeviceA-tunnel1] source 1.1.3.1
[DeviceA-tunnel1] quit
```

     # Add GE 0/0/1 and GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

     # Add Tunnel 0, Tunnel 1, and GE 0/0/3 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface tunnel 0
[DeviceA-zone-untrust] add interface tunnel 1
[DeviceA-zone-untrust] add interface ge 0/0/3
[DeviceA-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

c. Configure security policies.

Configure a security policy between the Local zone and Untrust zone where the public network interface resides.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone local
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 1.1.3.1 32
[DeviceA-policy-security-rule-policy1] destination-address 1.1.5.1 32
[DeviceA-policy-security-rule-policy1] destination-address 1.1.6.1 32
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
```

Configure security policies between the Trust and Untrust zones. The Untrust zone is a security zone where tunnel interfaces reside.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone trust
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy3] destination-address 10.1.3.0 24
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone trust
[DeviceA-policy-security-rule-policy4] source-address 10.1.3.0 24
[DeviceA-policy-security-rule-policy4] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] rule name policy5
[DeviceA-policy-security-rule-policy5] source-zone trust
[DeviceA-policy-security-rule-policy5] destination-zone untrust
[DeviceA-policy-security-rule-policy5] source-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy5] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy5] action permit
[DeviceA-policy-security-rule-policy5] quit
[DeviceA-policy-security] rule name policy6
[DeviceA-policy-security-rule-policy6] source-zone untrust
[DeviceA-policy-security-rule-policy6] destination-zone trust
[DeviceA-policy-security-rule-policy6] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy6] destination-address 10.1.0.0 24
[DeviceA-policy-security-rule-policy6] action permit
[DeviceA-policy-security-rule-policy6] quit
[DeviceA-policy-security] quit
```

d. Configure routes destined for the branch.

```
[DeviceA] ip route-static vpn-instance vpn1 10.1.3.0 255.255.255.0 tunnel0
[DeviceA] ip route-static vpn-instance vpn2 10.1.2.0 255.255.255.0 tunnel1
```

e. Configure two IPsec policies and apply them to tunnel interfaces.

Define data flows to be protected.

```
[DeviceA] acl 3000
[DeviceA-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
0.0.0.255 vpn-instance vpn1
[DeviceA-acl4-advance-3000] quit
[DeviceA] acl 3001
[DeviceA-acl4-advance-3001] rule 10 permit ip source 10.1.0.0 0.0.0.255 destination 10.1.2.0
0.0.0.255 vpn-instance vpn2
[DeviceA-acl4-advance-3001] quit
```

Configure an IPsec proposal. You can use the default parameter settings.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

Configure IKE proposal 10. You can use the default parameter settings.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

Configure IKE peers.

```
[DeviceA] ike peer vpn1
[DeviceA-ike-peer-vpn1] ike-proposal 10
[DeviceA-ike-peer-vpn1] remote-address 1.1.5.1
[DeviceA-ike-peer-vpn1] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-vpn1] sa binding vpn-instance vpn1
[DeviceA-ike-peer-vpn1] quit
[DeviceA] ike peer vpn2
[DeviceA-ike-peer-vpn2] ike-proposal 10
[DeviceA-ike-peer-vpn2] remote-address 1.1.6.1
[DeviceA-ike-peer-vpn2] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-vpn2] sa binding vpn-instance vpn2
[DeviceA-ike-peer-vpn2] quit
```

Configure two IPsec policies.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer vpn1
[DeviceA-ipsec-policy-isakmp-map1-10] tunnel local 1.1.3.1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
[DeviceA] ipsec policy map2 10 isakmp
[DeviceA-ipsec-policy-isakmp-map2-10] security acl 3001
[DeviceA-ipsec-policy-isakmp-map2-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map2-10] ike-peer vpn2
[DeviceA-ipsec-policy-isakmp-map2-10] tunnel local 1.1.3.1
[DeviceA-ipsec-policy-isakmp-map2-10] quit
```

Apply the IPsec policy **map1** to Tunnel 0 and IPsec policy **map2** to Tunnel 1.

```
[DeviceA] interface tunnel 0
[DeviceA-tunnel0] ipsec policy map1
[DeviceA-tunnel0] quit
[DeviceA] interface tunnel 1
[DeviceA-tunnel1] ipsec policy map2
[DeviceA-tunnel1] quit
```

- Configure DeviceB.
  a. Configure IP addresses for interfaces and add interfaces to security zones.

     # Configure an IP address for GE 0/0/3.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/3
[DeviceB-GE0/0/3] ip address 10.1.3.1 24
[DeviceB-GE0/0/3] quit
```

Configure an IP address for GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ip address 1.1.5.1 24
[DeviceB-GE0/0/1] quit
```

Add GE 0/0/3 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/3
[DeviceB-zone-trust] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

b. Configure security policies.

Configure security policies between the Trust and Untrust zones.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.3.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.3.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Untrust and Local zones.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceB-policy-security-rule-policy4] destination-address 1.1.5.1 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can configure security policies between the Local and Untrust zones to allow devices on both ends of an IPsec tunnel to communicate with each other.

c. Configure a static route destined for the network where the headquarters of company A resides. The following assumes that the next-hop IP address of the static route is 1.1.5.2.

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.5.2
```

d. Configure an IPsec policy and apply it to an interface.

Configure advanced ACL 3000 to allow users on network segment 10.1.3.0/24 to access network segment 10.1.1.0/24.

```
[DeviceB] acl 3000
[DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl4-advance-3000] quit
```

Configure an IPsec proposal named **tran1**. You can use the default parameter settings.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Configure IKE proposal 10. You can use the default parameter settings.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer vpn1
[DeviceB-ike-peer-vpn1] ike-proposal 10
[DeviceB-ike-peer-vpn1] remote-address 1.1.3.1
[DeviceB-ike-peer-vpn1] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-vpn1] quit
```

Configure an IPsec policy with the name **map1** and ID 10.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer vpn1
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy **map1** to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

- # Configure DeviceC.

a. Configure IP addresses for interfaces and add interfaces to security zones.

Configure an IP address for GE 0/0/3.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/3
[DeviceC-GE0/0/3] ip address 10.1.2.1 24
[DeviceC-GE0/0/3] quit
```

Configure an IP address for GE 0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ip address 1.1.6.1 24
[DeviceC-GE0/0/1] quit
```

Add GE 0/0/3 to the Trust zone.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/3
[DeviceC-zone-trust] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

b. Configure security policies.

Configure security policies between the Trust and Untrust zones.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy1
[DeviceC-policy-security-rule-policy1] source-zone trust
[DeviceC-policy-security-rule-policy1] destination-zone untrust
[DeviceC-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.0.0 24
[DeviceC-policy-security-rule-policy1] action permit
[DeviceC-policy-security-rule-policy1] quit
[DeviceC-policy-security] rule name policy2
[DeviceC-policy-security-rule-policy2] source-zone untrust
[DeviceC-policy-security-rule-policy2] destination-zone trust
[DeviceC-policy-security-rule-policy2] source-address 10.1.0.0 24
[DeviceC-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceC-policy-security-rule-policy2] action permit
[DeviceC-policy-security-rule-policy2] quit
```

Configure security policies between the Untrust and Local zones.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceC-policy-security] rule name policy3
[DeviceC-policy-security-rule-policy3] source-zone local
[DeviceC-policy-security-rule-policy3] destination-zone untrust
[DeviceC-policy-security-rule-policy3] source-address 1.1.6.1 32
[DeviceC-policy-security-rule-policy3] destination-address 1.1.3.1 32
[DeviceC-policy-security-rule-policy3] action permit
[DeviceC-policy-security-rule-policy3] quit
[DeviceC-policy-security] rule name policy4
[DeviceC-policy-security-rule-policy4] source-zone untrust
[DeviceC-policy-security-rule-policy4] destination-zone local
[DeviceC-policy-security-rule-policy4] source-address 1.1.3.1 32
[DeviceC-policy-security-rule-policy4] destination-address 1.1.6.1 32
[DeviceC-policy-security-rule-policy4] action permit
[DeviceC-policy-security-rule-policy4] quit
[DeviceC-policy-security] quit
```

NOTE

You can configure security policies between the Local and Untrust zones to allow devices on both ends of an IPsec tunnel to communicate with each other.

c. Configure a static route destined for the network where the headquarters of company B resides. The following assumes that the next-hop IP address of the static route is 1.1.6.2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC] ip route-static 10.1.0.0 255.255.255.0 1.1.6.2
```

d. Configure an IPsec policy and apply it to an interface.

Configure advanced ACL 3001 to allow users on network segment 10.1.2.0/24 to access network segment 10.1.0.0/24.

```
[DeviceC] acl 3001
[DeviceC-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
[DeviceC-acl4-advance-3000] quit
```

Configure an IPsec proposal named **tran1**. You can use the default parameter settings.

```
[DeviceC] ipsec proposal tran1
[DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceC-ipsec-proposal-tran1] quit
```

Configure IKE proposal 10. You can use the default parameter settings.

```
[DeviceC] ike proposal 10
[DeviceC-ike-proposal-10] authentication-method pre-share
[DeviceC-ike-proposal-10] prf hmac-sha2-256
[DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceC-ike-proposal-10] dh group14
[DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceC-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceC] ike peer vpn2
[DeviceC-ike-peer-vpn1] ike-proposal 10
[DeviceC-ike-peer-vpn1] remote-address 1.1.3.1
[DeviceC-ike-peer-vpn1] pre-shared-key YsHsjx_202206
[DeviceC-ike-peer-vpn1] quit
```

Configure an IPsec policy with the name **map1** and ID 10.

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3001
[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer vpn2
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy **map1** to GE 0/0/1.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

----End

Verifying the Configuration

The following assumes that PC1 needs to access resources (Server1) at the headquarters of company A. Run the **display ike sa** and **display ipsec sa brief** commands on DeviceA and DeviceB to check SA information. The following shows the command outputs of DeviceA, which if similar, indicate that IKE SAs and IPsec SAs have been established.

```
<DeviceA> display ike sa
IKE SA information :
  Conn-ID     Peer          VPN   Flag(s)  Phase  RemoteType  RemoteID
-------------------------------------------------------------------------
  117477244   1.1.5.1:500         RD|A     v2:2   IP          1.1.5.1
  117477243   1.1.5.1:500         RD|A     v2:1   IP          1.1.5.1

 Number of IKE SA : 2
-------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceA> display ipsec sa

==============================
Interface: Tunnel0
==============================

  ----------------------------
  IPSec policy name: "map1"
  Sequence number  : 10
  Acl group        : 3000
  Acl rule         : 5
  Mode             : ISAKMP
  ----------------------------
    Connection ID     : 150994963
    Encapsulation mode: Tunnel
    Tunnel local      : 1.1.3.1
    Tunnel remote     : 1.1.5.1
    Flow source       : 10.1.1.0/255.255.255.0 0/0
    Flow destination  : 10.1.3.0/255.255.255.0 0/0
    Flow vpn          : vpn1
    [Outbound ESP SAs]
      SPI: 120037772 (0x727a18c)
      Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 1843200/1031
      Max sent sequence-number: 9
      UDP encapsulation used for NAT traversal: N
      SA decrypted packets (number/kilobytes): 4/0

    [Inbound ESP SAs]
      SPI: 215352593 (0xcd60511)
      Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 1843196/1031
      Max received sequence-number: 49
      UDP encapsulation used for NAT traversal: N
      SA decrypted packets (number/kilobytes): 4/0
      Anti-replay : Enable
      Anti-replay window size: 1024
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ip vpn-instance vpn1
 route-distinguisher 100:1
ip vpn-instance vpn2
 route-distinguisher 200:1
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255 vpn-instance vpn1
acl number 3001
 rule 5 permit ip source 10.1.0.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 vpn-instance vpn2
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ike peer vpn1
 pre-shared-key cnEDZkL3}#J"qG/2iTb&P9q/
 ike-proposal 10
 remote-address 1.1.5.1
 sa binding vpn-instance vpn1
ike peer vpn2
 pre-shared-key cnEDZkL3}#J"qG/2iTb&P9q/
 ike-proposal 10
 remote-address 1.1.6.1
 sa binding vpn-instance vpn2
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer vpn1
 proposal tran1
 tunnel local 1.1.3.1
ipsec policy map2 10 isakmp
 security acl 3001
 ike-peer vpn2
 proposal tran1
 tunnel local 1.1.3.1
#
interface GE0/0/1
 ip binding vpn-instance vpn1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip binding vpn-instance vpn2
 ip address 10.1.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 1.1.3.1 255.255.255.0
#
interface Tunnel0
 ip binding vpn-instance vpn1
 ip address 10.10.1.2 255.255.255.0
 tunnel-protocol ipsec
 source 1.1.3.1
 ipsec policy map1
#
interface Tunnel1
 ip binding vpn-instance vpn2
 ip address 10.10.1.1 255.255.255.0
 tunnel-protocol ipsec
 source
1.1.3.1

 ipsec policy map2
#
firewall zone trust
 add interface GE0/0/1
 add interface GE0/0/2
#
firewall zone untrust
 add interface GE0/0/3
 add interface Tunnel0
 add interface Tunnel1
#
ip route-static vpn-instance vpn1 10.1.3.0 255.255.255.0 Tunnel0
ip route-static vpn-instance vpn2 10.1.2.0 255.255.255.0 Tunnel1
#
security-policy
 rule name policy1
  source-zone local
  destination-zone untrust
  source-address 1.1.3.1 255.255.255.255
  destination-address 1.1.5.1 255.255.255.255
  destination-address 1.1.6.1 255.255.255.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
rule name policy2
 source-zone untrust
 destination-zone local
 source-address 1.1.5.1 255.255.255.255
 source-address 1.1.6.1 255.255.255.255
 destination-address 1.1.3.1 255.255.255.255
 action permit
rule name policy3
 source-zone trust
 destination-zone untrust
 source-address 10.1.1.0 255.255.255.0
 destination-address 10.1.3.0 255.255.255.0
 action permit
rule name policy4
 source-zone untrust
 destination-zone trust
 source-address 10.1.3.0 255.255.255.0
 destination-address 10.1.1.0 255.255.255.0
 action permit
rule name policy5
 source-zone trust
 destination-zone untrust
 source-address 10.1.0.0 255.255.255.0
 destination-address 10.1.2.0 255.255.255.0
 action permit
rule name policy6
 source-zone untrust
 destination-zone trust
 source-address 10.1.2.0 255.255.255.0
 destination-address 10.1.0.0 255.255.255.0
 action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer vpn1
 pre-shared-key 1tx/S9a;iF[L)QFz!$p;y]Lg
 ike-proposal 10
 remote-address 1.1.3.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer vpn1
 proposal tran1

#
interface GE0/0/1
 ip address 1.1.5.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/3
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
ip route-static 10.1.1.0 255.255.255.0 1.1.5.2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.3.0 255.255.255.0
  destination-address 10.1.1.0 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 255.255.255.0
  destination-address 10.1.3.0 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.5.1 255.255.255.255
  destination-address 1.1.3.1 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 255.255.255.255
  destination-address 1.1.5.1 255.255.255.255
  action permit
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3001
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer vpn2
 pre-shared-key 1tx/S9a;iF[L)QFz!$p;y]Lg
 ike-proposal 10
 remote-address 1.1.3.1
#
ipsec policy map2 10 isakmp
 security acl 3001
 ike-peer vpn2
 proposal tran1

#
interface GE0/0/1
 ip address 1.1.6.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ipsec policy map1
#
interface GE0/0/3
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
ip route-static 10.1.0.0 255.255.255.0 1.1.6.2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 255.255.255.0
  destination-address 10.1.0.0 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 255.255.255.0
  destination-address 10.1.2.0 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.6.1 255.255.255.255
  destination-address 1.1.3.1 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.3.1 255.255.255.255
  destination-address 1.1.6.1 255.255.255.255
  action permit
#
return
```

8.4.5 CLI: Example for Accessing Resources in Different VPN Instances Through an IPsec Tunnel

Networking Requirements

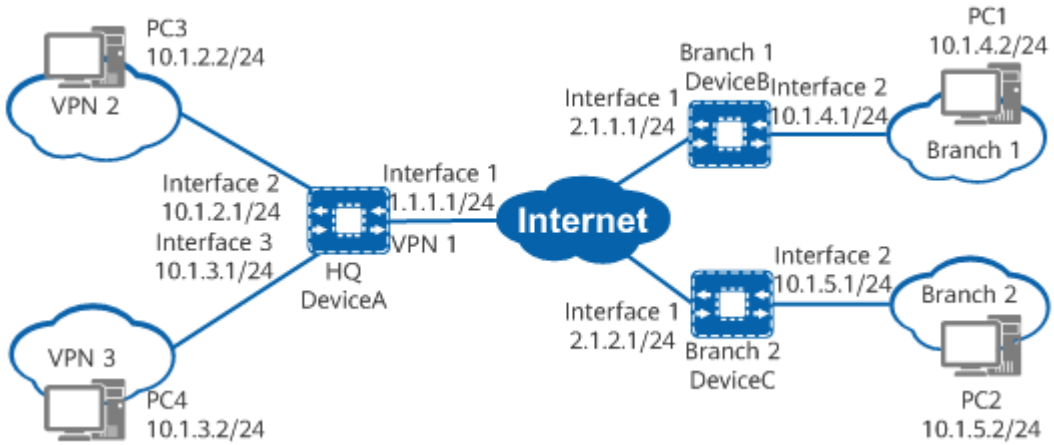
In **Figure 8-25**, DeviceA is the gateway of the enterprise headquarters, DeviceB is the gateway of branch 1, and DeviceC is the gateway of branch 2. The VPNs isolate different resources at the headquarters. It is required that branches securely access these resources through IPsec tunnels.

Figure 8-25 Configuring branches to access headquarters resources in different VPN instances through IPsec tunnels

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

On DeviceA, configure a template IPsec policy to respond to the access requests of the branches.

1. Perform basic configurations, including configuring VPN instances, configuring IP addresses for interfaces, adding interfaces to security zones, configuring security policies, and configuring static routes.
2. Configure an IPsec policy, including an IPsec proposal, IKE proposal, and IKE user table.

On DeviceB and DeviceC:

1. Perform basic configurations, including configuring IP addresses for interfaces, adding interfaces to security zones, configuring security policies, and configuring static routes.
2. Configure an IPsec policy, including the data flows to be encrypted, IPsec proposal, and IKE proposal.

Procedure

- Configure DeviceA.
  a. Configure VPN instances.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] ip vpn-instance vpn1
[DeviceA-vpn-instance-vpn1] route-distinguisher 100:1
[DeviceA-vpn-instance-vpn1-af-ipv4] quit
[DeviceA-vpn-instance-vpn1] quit
[DeviceA] ip vpn-instance vpn2
[DeviceA-vpn-instance-vpn2] route-distinguisher 200:1
[DeviceA-vpn-instance-vpn2-af-ipv4] quit
[DeviceA-vpn-instance-vpn2] quit
[DeviceA] ip vpn-instance vpn3
[DeviceA-vpn-instance-vpn3] route-distinguisher 300:1
```

```
[DeviceA-vpn-instance-vpn3-af-ipv4] quit
[DeviceA-vpn-instance-vpn3] quit
```

b. Configure IP addresses for interfaces and add interfaces to security zones.

Configure IP addresses for interfaces.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip binding vpn-instance vpn1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip binding vpn-instance vpn2
[DeviceA-GE0/0/2] ip address 10.1.2.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip binding vpn-instance vpn3
[DeviceA-GE0/0/3] ip address 10.1.3.1 24
[DeviceA-GE0/0/3] quit
```

Add interfaces to security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

c. Configure security policies.

Configure security policies between the Local zone and the Untrust zone where GE 0/0/1 resides.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone local
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy1] destination-address 2.1.1.1 24
[DeviceA-policy-security-rule-policy1] destination-address 2.1.2.1 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone local
[DeviceA-policy-security-rule-policy2] source-address 2.1.1.1 24
[DeviceA-policy-security-rule-policy2] source-address 2.1.2.1 24
[DeviceA-policy-security-rule-policy2] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
[DeviceA-policy-security] quit
```

Configure security policies between the Trust and Untrust zones.

```
[DeviceA] security-policy
[Device-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone trust
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 10.1.0.0 16
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy3] destination-address 10.1.4.0 24
[DeviceA-policy-security-rule-policy3] destination-address 10.1.5.0 24
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone trust
[DeviceA-policy-security-rule-policy4] source-address 10.1.4.0 24
[DeviceA-policy-security-rule-policy4] source-address 10.1.5.0 24
[DeviceA-policy-security-rule-policy4] destination-address 10.1.0.0 16
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

d. Configure static routes destined for the branches. The following assumes that the next-hop address is 1.1.1.2.

```
[DeviceA] ip route-static vpn-instance vpn1 2.1.1.0 255.255.255.0 1.1.1.2
[DeviceA] ip route-static vpn-instance vpn1 2.1.2.0 255.255.255.0 1.1.1.2
```

e. Configure routes between VPNs so that there are reachable routes between VPN 1, VPN 2 and VPN 3.

```
[DeviceA] ip route-static vpn-instance vpn1 10.1.2.0 24 vpn-instance vpn2 10.1.2.2
[DeviceA] ip route-static vpn-instance vpn1 10.1.3.0 24 vpn-instance vpn3 10.1.3.2
[DeviceA] ip route-static vpn-instance vpn2 10.1.4.0 24 vpn-instance vpn1 1.1.1.2
[DeviceA] ip route-static vpn-instance vpn3 10.1.5.0 24 vpn-instance vpn1 1.1.1.2
```

f. Configure an IPsec policy.

Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] authentication-algorithm sha2-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

Create an IKE user table.

```
[DeviceA] ike user-table 1
[DeviceA-ike-user-table-1] user vpn2
[DeviceA-ike-user-table-1-vpn2] pre-shared-key YsHsjx_202206
[DeviceA-ike-user-table-1-vpn2] vpn-instance-traffic name vpn2
[DeviceA-ike-user-table-1-vpn2] id-type ip 2.1.1.1
[DeviceA-ike-user-table-1-vpn2] quit
[DeviceA-ike-user-table-1] user vpn3
[DeviceA-ike-user-table-1-vpn3] pre-shared-key YsHsjx_202206
[DeviceA-ike-user-table-1-vpn3] vpn-instance-traffic name vpn3
[DeviceA-ike-user-table-1-vpn3] id-type ip 2.1.2.1
[DeviceA-ike-user-table-1-vpn3] quit
[DeviceA-ike-user-table-1] quit
```

Configure an IKE peer.

```
[DeviceA] ike peer vpn
[DeviceA-ike-peer-vpn] ike-proposal 10
[DeviceA-ike-peer-vpn] local-id 1.1.1.1
[DeviceA-ike-peer-vpn] user-table 1
[DeviceA-ike-peer-vpn] quit
```

Configure an IPsec policy.

```
[DeviceA] ipsec policy-template use1 10
[DeviceA-ipsec-policy-templet-use1-10] proposal tran1
[DeviceA-ipsec-policy-templet-use1-10] ike-peer vpn
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-ipsec-policy-templet-use1-10] flow-vrf check disable
[DeviceA-ipsec-policy-templet-use1-10] quit
[DeviceA] ipsec policy map1 10 isakmp template use1
```

NOTE

If VPNs import routes from each other for inter-VPN traffic forwarding, you need to run the **flow-vrf check disable** command to disable the function of checking the VPN instance in data flows during IPsec encryption and decryption.

Apply the IPsec policy to an interface.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
```

- Configure DeviceB.
  a. Configure IP addresses for interfaces and add interfaces to security zones.

Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ip address 2.1.1.1 24
[DeviceB-GE0/0/1] quit
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] ip address 10.1.4.1 24
[DeviceB-GE0/0/2] quit
```

Add interfaces to security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

  b. Configure security policies.

Configure security policies between the Trust and Untrust zones.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.4.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.0.0 16
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.0.0 16
[DeviceB-policy-security-rule-policy2] destination-address 10.1.4.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure security policies between the Untrust and Local zones.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 2.1.1.1 24
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 24
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 1.1.1.1 24
[DeviceB-policy-security-rule-policy4] destination-address 2.1.1.1 24
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

NOTE

You can configure security policies between the Local and Untrust zones to allow devices on both ends of an IPsec tunnel to communicate with each other.

c. Configure static routes to the headquarters. The following assumes that the next-hop address is 2.1.1.2.

```
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 2.1.1.2
[DeviceB] ip route-static 10.1.0.0 255.255.0.0 2.1.1.2
```

d. Configure an IPsec policy.

Configure advanced ACL 3000.

```
[DeviceB] acl 3000
[DeviceB-acl4-advance-3000] rule 10 permit ip source 10.1.4.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceB-acl4-advance-3000] rule 15 permit ip source 10.1.4.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
[DeviceB-acl4-advance-3000] quit
```

Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] authentication-algorithm sha2-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer vpn
[DeviceB-ike-peer-vpn] ike-proposal 10
[DeviceB-ike-peer-vpn] remote-address 1.1.1.1
[DeviceB-ike-peer-vpn] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-vpn] quit
```

Configure an IPsec policy.

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-peer vpn
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy **map1** to an interface.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ipsec policy map1
[DeviceB-GE0/0/1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

- Configure DeviceC.
  a. Configure IP addresses for interfaces and add interfaces to security zones.

     # Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ip address 2.1.2.1 24
[DeviceC-GE0/0/1] quit
[DeviceC] interface ge 0/0/2
[DeviceC-GE0/0/2] ip address 10.1.5.1 24
[DeviceC-GE0/0/2] quit
```

     # Add interfaces to security zones.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

  b. Configure security policies.

     # Configure security policies between the Trust and Untrust zones.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy1
[DeviceC-policy-security-rule-policy1] source-zone trust
[DeviceC-policy-security-rule-policy1] destination-zone untrust
[DeviceC-policy-security-rule-policy1] source-address 10.1.5.0 24
[DeviceC-policy-security-rule-policy1] destination-address 10.1.0.0 16
[DeviceC-policy-security-rule-policy1] action permit
[DeviceC-policy-security-rule-policy1] quit
[DeviceC-policy-security] rule name policy2
[DeviceC-policy-security-rule-policy2] source-zone untrust
[DeviceC-policy-security-rule-policy2] destination-zone trust
[DeviceC-policy-security-rule-policy2] source-address 10.1.0.0 16
[DeviceC-policy-security-rule-policy2] destination-address 10.1.5.0 24
[DeviceC-policy-security-rule-policy2] action permit
[DeviceC-policy-security-rule-policy2] quit
```

     # Configure security policies between the Untrust and Local zones.

     NOTE

     The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as match conditions and use protocols and ports as additional match conditions. This example configures source and destination addresses as match conditions. To use protocols and ports as additional match conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceC-policy-security] rule name policy3
[DeviceC-policy-security-rule-policy3] source-zone local
[DeviceC-policy-security-rule-policy3] destination-zone untrust
[DeviceC-policy-security-rule-policy3] source-address 2.1.2.1 24
[DeviceC-policy-security-rule-policy3] destination-address 1.1.1.1 24
[DeviceC-policy-security-rule-policy3] action permit
[DeviceC-policy-security-rule-policy3] quit
[DeviceC-policy-security] rule name policy4
[DeviceC-policy-security-rule-policy4] source-zone untrust
[DeviceC-policy-security-rule-policy4] destination-zone local
[DeviceC-policy-security-rule-policy4] source-address 1.1.1.1 24
[DeviceC-policy-security-rule-policy4] destination-address 2.1.2.1 24
[DeviceC-policy-security-rule-policy4] action permit
[DeviceC-policy-security-rule-policy4] quit
[DeviceC-policy-security] quit
```

 Copyright © Huawei Technologies Co., Ltd.

> NOTE
>
> You can configure security policies between the Local and Untrust zones to allow devices on both ends of an IPsec tunnel to communicate with each other.

c. Configure static routes to the headquarters. The following assumes that the next-hop address is 2.1.2.2.

```
[DeviceC] ip route-static 1.1.1.0 255.255.255.0 2.1.2.2
[DeviceC] ip route-static 10.1.0.0 255.255.0.0 2.1.2.2
```

d. Configure an IPsec policy.

Configure advanced ACL 3000.

```
[DeviceC] acl 3000
[DeviceC-acl4-advance-3000] rule 10 permit ip source 10.1.5.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceC-acl4-advance-3000] rule 15 permit ip source 10.1.5.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
[DeviceC-acl4-advance-3000] quit
```

Configure an IPsec proposal.

```
[DeviceC] ipsec proposal tran1
[DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceC-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceC] ike proposal 10
[DeviceC-ike-proposal-10] authentication-method pre-share
[DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceC-ike-proposal-10] authentication-algorithm sha2-256
[DeviceC-ike-proposal-10] dh group14
[DeviceC-ike-proposal-10] prf hmac-sha2-256
[DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceC-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceC] ike peer vpn
[DeviceC-ike-peer-vpn] ike-proposal 10
[DeviceC-ike-peer-vpn] remote-address 1.1.1.1
[DeviceC-ike-peer-vpn] pre-shared-key YsHsjx_202206
[DeviceC-ike-peer-vpn] quit
```

Configure an IPsec policy.

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer vpn
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy **map1** to an interface.

```
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ipsec policy map1
[DeviceC-GE0/0/1] quit
```

----End

Verifying the Configuration

1. Ping PC3 from PC1 and PC4 from PC2. The pings are successful.
2. Run the **display ike sa** command to check SA information. The following shows the command output of DeviceA.

```
<DeviceA> display ike sa

IKE SA information:
```

 Copyright © Huawei Technologies Co., Ltd.

```
Conn-ID    Peer     VPN   Flag(s)  Phase  RemoteType  RemoteID
-------------------------------------------------------------------------
117477245  2.1.1.1  vpn1  RD|A     v2:2   IP          2.1.1.1
117477244  2.1.1.1  vpn1  RD|A     v2:2   IP          2.1.1.1
117477243  2.1.1.1  vpn1  RD|A     v2:1   IP          2.1.1.1

Number of IKE SA : 2
-------------------------------------------------------------------------

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Configuration Scripts

- DeviceA

```
#
 sysname DeviceA
#
ip vpn-instance vpn1
 route-distinguisher 100:1
#
ip vpn-instance vpn2
 route-distinguisher 200:1
#
ip vpn-instance vpn3
 route-distinguisher 300:1
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike user-table 1
 user vpn2
  pre-shared-key %+%#KdY"Ac_06J"\KzUi_Bl>5zI}Gse+~>zba6#8q%xU%+%#
  vpn-instance-traffic name vpn2
  id-type ip 2.1.1.1
 user vpn3
  pre-shared-key %+%#zWlRJ$]-I3o7!2+0]uA:C<%<2e3L:$V|\tS(.+9)%+%#
  vpn-instance-traffic name vpn3
  id-type ip 2.1.2.1
#
ike peer vpn
 ike-proposal 10
 local-id 1.1.1.1
 user-table 1
#
ipsec policy-template use1 10
 ike-peer vpn
 proposal tran1
 flow-vrf check disable
#
ipsec policy map1 10 isakmp template use1
#
interface GE0/0/1
 ip binding vpn-instance vpn1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip binding vpn-instance vpn2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/3
 ip binding vpn-instance vpn3
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
ip route-static vpn-instance vpn1 2.1.1.0 255.255.255.0 1.1.1.2
ip route-static vpn-instance vpn1 2.1.2.0 255.255.255.0 1.1.1.2
ip route-static vpn-instance vpn1 10.1.2.0 24 vpn-instance vpn2 10.1.2.2
ip route-static vpn-instance vpn1 10.1.3.0 24 vpn-instance vpn3 10.1.3.2
ip route-static vpn-instance vpn2 10.1.4.0 24 vpn-instance vpn1 1.1.1.2
ip route-static vpn-instance vpn3 10.1.5.0 24 vpn-instance vpn1 1.1.1.2
#
security-policy
 rule name policy1
  source-zone local
  destination-zone untrust
  source-address 1.1.1.0 255.255.255.0
  destination-address 2.1.1.0 255.255.255.0
  destination-address 2.1.2.0 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone local
  source-address 2.1.1.0 255.255.255.0
  source-address 2.1.2.0 255.255.255.0
  destination-address 1.1.1.0 255.255.255.0
  action permit
 rule name policy3
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 255.255.0.0
  destination-address 10.1.4.0 255.255.255.0
  destination-address 10.1.5.0 255.255.255.0
  action permit
 rule name policy4
  source-zone untrust
  destination-zone trust
  source-address 10.1.4.0 255.255.255.0
  source-address 10.1.5.0 255.255.255.0
  destination-address 10.1.0.0 255.255.0.0
  action permit
#
return
```

- DeviceB

```
#
 sysname DeviceB
#
acl number 3000
 rule 10 permit ip source 10.1.4.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 15 permit ip source 10.1.4.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
```

 Copyright © Huawei Technologies Co., Ltd.

```
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer vpn
 pre-shared-key %+%#5$\vJ~&IS==EJ=Eq^`3@GA[a!Xa}eIm'-GPK]_K@%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer vpn
 proposal tran1

#
interface GE0/0/2
 ip address 2.1.1.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/1
 ip address 10.1.4.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/2
#
firewall zone untrust
 add interface GE0/0/1
#
ip route-static 1.1.1.0 255.255.255.0 2.1.1.2
ip route-static 10.1.0.0 255.255.0.0 2.1.1.2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.4.0 255.255.255.0
  destination-address 10.1.0.0 255.255.0.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 255.255.0.0
  destination-address 10.1.4.0 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.1.1.0 255.255.255.0
  destination-address 1.1.1.0 255.255.255.0
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.0 255.255.255.0
  destination-address 2.1.1.0 255.255.255.0
  action permit
#
return
```

- DeviceC

```
#
 sysname DeviceC
#
acl number 3000
 rule 10 permit ip source 10.1.5.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 15 permit ip source 10.1.5.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer vpn
 pre-shared-key %+%#5$\vJ~&IS==EJ=Eq^`3@GA[a!Xa}eIm'-GPK]_K@%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer vpn
 proposal tran1

#
interface GE0/0/2
 ip address 2.1.2.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/1
 ip address 10.1.5.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/2
#
firewall zone untrust
 add interface GE0/0/1
#
ip route-static 1.1.1.0 255.255.255.0 2.1.2.2
ip route-static 10.1.0.0 255.255.0.0 2.1.2.2
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.5.0 255.255.255.0
  destination-address 10.1.0.0 255.255.0.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.0.0 255.255.0.0
  destination-address 10.1.5.0 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 2.1.2.0 255.255.255.0
  destination-address 1.1.1.0 255.255.255.0
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.0 255.255.255.0
  destination-address 2.1.2.0 255.255.255.0
  action permit
#
return
```

8.5 IPsec Dual-System Hot Standby

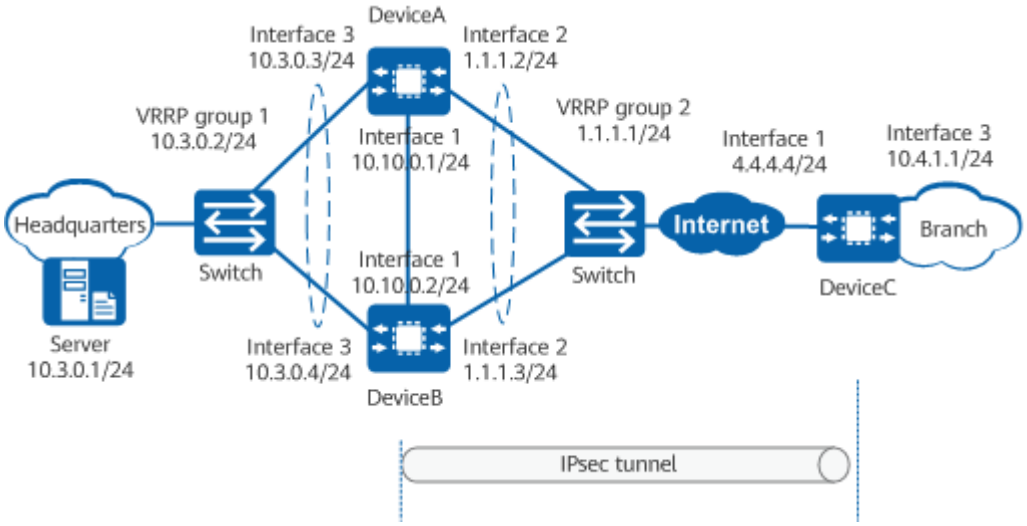
 Copyright © Huawei Technologies Co., Ltd.

8.5.1 CLI: Example for Establishing an IPsec Tunnel in Active/Standby Mode

Networking Requirements

As shown in **Figure 8-26**, the enterprise headquarters connects to the Internet through DeviceA and DeviceB. A branch connects to the headquarters through DeviceC. The branch needs to securely access the IPsec-protected headquarters intranet servers. The enterprise has multiple branches. This example describes IPsec communication between the headquarters and one branch, of which the gateway is DeviceC. To improve availability, DeviceA and DeviceB are configured to work in active/standby mode. Both the upstream and downstream devices are switches.

Figure 8-26 Establishing IPsec tunnels on devices in active/standby mode



Item	Data
DeviceA	Interface: GE0/0/1 IP address: 10.10.0.1/24 Security zone: DMZ
	Interface: GE0/0/2 IP address: 1.1.1.2/24 VRRP group 2 IP address: 1.1.1.1/24 Security zone: Untrust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	Interface: GE0/0/3 IP address: 10.3.0.3/24 VRRP group 1 IP address: 10.3.0.2/24 Security zone: Trust
	IPsec configuration Method of creating an IPsec policy: IPsec policy template PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: IP address
DeviceB	Interface: GE0/0/1 IP address: 10.10.0.2/24 Security zone: DMZ
	Interface: GE0/0/2 IP address: 1.1.1.3/24 VRRP group 2 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE0/0/3 IP address: 10.3.0.4/24 VRRP group 1 IP address: 10.3.0.2/24 Security zone: Trust
	IPsec configuration Method of creating an IPsec policy: IPsec policy template PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: IP address
DeviceC	Interface: GE0/0/1 IP address: 4.4.4.4/24 Security zone: Untrust
	Interface: GE0/0/3 IP address: 10.4.1.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

1. Configure Huawei Redundancy Protocol (HRP) on DeviceA and DeviceB.
2. Configure security policies and an IPsec policy on DeviceA. After HRP is enabled on DeviceA and DeviceB, the security policies and IPsec policy of DeviceA are automatically backed up to DeviceB.
3. Configure an IPsec policy on DeviceC.

Procedure

Step 1 Complete basic network configurations on DeviceA and DeviceB.

DeviceA	DeviceB
# Configure an IP address for each interface on DeviceA and DeviceB.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **ip address 10.10.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **ip address 1.1.1.2 24** [DeviceA-GE0/0/2] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **ip address 10.3.0.3 24** [DeviceA-GE0/0/3] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.10.0.2 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **ip address 1.1.1.3 24** [DeviceB-GE0/0/2] **quit** [DeviceB] **interface ge0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.0.4 24** [DeviceB-GE0/0/3] **quit**
# Add each interface on DeviceA and DeviceB to a security zone.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/2** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/1** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/2** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/1** [DeviceB-zone-dmz] **quit**
# Configure a default route with the next hop 1.1.1.254 on DeviceA and DeviceB. Configure a static route to the branch intranet and set the next hop to 1.1.1.254.	
[DeviceA] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.254** [DeviceA] **ip route-static 10.4.1.0 255.255.255.0 1.1.1.254**	[DeviceB] **ip route-static 0.0.0.0 0.0.0.0 1.1.1.254** [DeviceB] **ip route-static 10.4.1.0 255.255.255.0 1.1.1.254**

Step 2 Configure a VRRP group on DeviceA and DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# Configure VRRP group 1 on the service interface GE0/0/3 of DeviceA and set its state to **active**. # Configure VRRP group 1 on the service interface GE0/0/3 of DeviceB and set its state to **standby**. If the IP addresses of the interfaces and VRRP group are on different network segments, specify a mask when configuring the IP address of the VRRP group.	
[DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **vrrp vrid 1 virtual-ip 10.3.0.2 active** [DeviceA-GE0/0/3] **quit**	[DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **vrrp vrid 1 virtual-ip 10.3.0.2 standby** [DeviceB-GE0/0/3] **quit**
# Configure VRRP group 2 on the service interface GE0/0/2 of DeviceA and set its state to **active**. # Configure VRRP group 2 on the service interface GE0/0/2 of DeviceB and set its state to **standby**.	
[DeviceA] **interface ge 0/0/2** [DeviceA-GE0/0/2] **vrrp vrid 2 virtual-ip 1.1.1.1 active** [DeviceA-GE0/0/2] **quit**	[DeviceB] **interface ge 0/0/2** [DeviceB-GE0/0/2] **vrrp vrid 2 virtual-ip 1.1.1.1 standby** [DeviceB-GE0/0/2] **quit**

Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 4 Specify heartbeat interfaces, configure authentication keys, and enable HRP on DeviceA and DeviceB.

DeviceA	DeviceB
[DeviceA] **hrp interface ge 0/0/1 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/1 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206** [DeviceB] **hrp enable**

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure security policies on DeviceA. After HRP is enabled, the security policy configuration on DeviceA will be automatically backed up to DeviceB.

Configure security policies between the Trust and Untrust zones to allow pre-encapsulated and decapsulated packets to pass through DeviceA.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_ipsec_1
HRP_M[DeviceA-policy-security-rule-policy_ipsec_1] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ipsec_1] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_ipsec_1] source-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_ipsec_1] destination-address 10.4.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_ipsec_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_ipsec_1] quit
HRP_M[DeviceA-policy-security] rule name policy_ipsec_2
HRP_M[DeviceA-policy-security-rule-policy_ipsec_2] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_ipsec_2] destination-zone trust
HRP_M[DeviceA-policy-security-rule-policy_ipsec_2] source-address 10.4.1.0 24
HRP_M[DeviceA-policy-security-rule-policy_ipsec_2] destination-address 10.3.0.0 24
HRP_M[DeviceA-policy-security-rule-policy_ipsec_2] action permit
HRP_M[DeviceA-policy-security-rule-policy_ipsec_2] quit
```

Configure security policies between the Local and Untrust zones to allow IKE negotiation packets to pass through DeviceA.

```
HRP_M[DeviceA-policy-security] rule name policy_ipsec_3
HRP_M[DeviceA-policy-security-rule-policy_ipsec_3] source-zone local
HRP_M[DeviceA-policy-security-rule-policy_ipsec_3] destination-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_ipsec_3] source-address 1.1.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_ipsec_3] destination-address 4.4.4.4 32
HRP_M[DeviceA-policy-security-rule-policy_ipsec_3] action permit
HRP_M[DeviceA-policy-security-rule-policy_ipsec_3] quit
HRP_M[DeviceA-policy-security] rule name policy_ipsec_4
HRP_M[DeviceA-policy-security-rule-policy_ipsec_4] source-zone untrust
HRP_M[DeviceA-policy-security-rule-policy_ipsec_4] destination-zone local
HRP_M[DeviceA-policy-security-rule-policy_ipsec_4] source-address 4.4.4.4 32
HRP_M[DeviceA-policy-security-rule-policy_ipsec_4] destination-address 1.1.1.1 32
HRP_M[DeviceA-policy-security-rule-policy_ipsec_4] action permit
HRP_M[DeviceA-policy-security-rule-policy_ipsec_4] quit
HRP_M[DeviceA-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Step 6 Configure an IPsec policy on DeviceA and apply the policy to an interface.

1. Create an advanced ACL, define the data flow to be protected, and allow devices on the network segment 10.3.0.0/24 to access the network segment 10.4.1.0/24.

   ```
   HRP_M[DeviceA] acl 3000
   HRP_M[DeviceA-acl4-advance-3000] rule 5 permit ip source 10.3.0.0 0.0.0.255 destination 10.4.1.0 0.0.0.255
   HRP_M[DeviceA-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   HRP_M[DeviceA] ipsec proposal tran1
   HRP_M[DeviceA-ipsec-proposal-tran1] encapsulation-mode tunnel
   HRP_M[DeviceA-ipsec-proposal-tran1] transform esp
   HRP_M[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
HRP_M[DeviceA-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
HRP_M[DeviceA] ike proposal 10
HRP_M[DeviceA-ike-proposal-10] authentication-method pre-share
HRP_M[DeviceA-ike-proposal-10] prf hmac-sha2-256
HRP_M[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
HRP_M[DeviceA-ike-proposal-10] dh group14
HRP_M[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
HRP_M[DeviceA-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
HRP_M[DeviceA] ike peer any
HRP_M[DeviceA-ike-peer-any] ike-proposal 10
HRP_M[DeviceA-ike-peer-any] pre-shared-key YsHsjx_202206
HRP_M[DeviceA-ike-peer-any] quit
```

5. Configure an IPsec policy template.

```
HRP_M[DeviceA] ipsec policy-template policy1 1
HRP_M[DeviceA-ipsec-policy-templet-policy1-1] security acl 3000
HRP_M[DeviceA-ipsec-policy-templet-policy1-1] proposal tran1
HRP_M[DeviceA-ipsec-policy-templet-policy1-1] ike-peer any
HRP_M[DeviceA-ipsec-policy-templet-policy1-1] tunnel local 1.1.1.1
HRP_M[DeviceA-ipsec-policy-templet-policy1-1] quit
```

6. Reference the IPsec policy template **policy1** in the IPsec policy numbered 10 in the IPsec policy group **map1**.

```
HRP_M[DeviceA] ipsec policy map1 10 isakmp template policy1
```

7. Apply the IPsec policy to GE0/0/2.

```
HRP_M[DeviceA] interface ge0/0/2
HRP_M[DeviceA-GE0/0/2] ipsec policy map1
HRP_M[DeviceA-GE0/0/2] quit
```

Step 7 Configure DeviceC (at the branch).

1. Configure IP addresses for interfaces and add interfaces to security zones.

   # Configure IP addresses for interfaces.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface ge 0/0/3
[DeviceC-GE0/0/3] ip address 10.4.1.1 24
[DeviceC-GE0/0/3] quit
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ip address 4.4.4.4 24
[DeviceC-GE0/0/1] quit
```

   # Add interfaces to security zones.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/3
[DeviceC-zone-trust] quit
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
```

2. Configure security policies to permit tunnel negotiation packets and encrypted data packets transmitted through the IPsec tunnel.

   # Configure security policies between the Trust and Untrust zones to permit data flows to be encrypted.

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name policy_ipsec_1
[DeviceC-policy-security-rule-policy_ipsec_1] source-zone trust
[DeviceC-policy-security-rule-policy_ipsec_1] destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-policy-security-rule-policy_ipsec_1] source-address 10.4.1.0 24
[DeviceC-policy-security-rule-policy_ipsec_1] destination-address 10.3.0.0 24
[DeviceC-policy-security-rule-policy_ipsec_1] action permit
[DeviceC-policy-security-rule-policy_ipsec_1] quit
[DeviceC-policy-security] rule name policy_ipsec_2
[DeviceC-policy-security-rule-policy_ipsec_2] source-zone untrust
[DeviceC-policy-security-rule-policy_ipsec_2] destination-zone trust
[DeviceC-policy-security-rule-policy_ipsec_2] source-address 10.3.0.0 24
[DeviceC-policy-security-rule-policy_ipsec_2] destination-address 10.4.1.0 24
[DeviceC-policy-security-rule-policy_ipsec_2] action permit
[DeviceC-policy-security-rule-policy_ipsec_2] quit
```

Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

```
[DeviceC-policy-security] rule name policy_ipsec_3
[DeviceC-policy-security-rule-policy_ipsec_3] source-zone local
[DeviceC-policy-security-rule-policy_ipsec_3] destination-zone untrust
[DeviceC-policy-security-rule-policy_ipsec_3] source-address 4.4.4.4 32
[DeviceC-policy-security-rule-policy_ipsec_3] destination-address 1.1.1.1 32
[DeviceC-policy-security-rule-policy_ipsec_3] action permit
[DeviceC-policy-security-rule-policy_ipsec_3] quit
[DeviceC-policy-security] rule name policy_ipsec_4
[DeviceC-policy-security-rule-policy_ipsec_4] source-zone untrust
[DeviceC-policy-security-rule-policy_ipsec_4] destination-zone local
[DeviceC-policy-security-rule-policy_ipsec_4] source-address 1.1.1.1 32
[DeviceC-policy-security-rule-policy_ipsec_4] destination-address 4.4.4.4 32
[DeviceC-policy-security-rule-policy_ipsec_4] action permit
[DeviceC-policy-security-rule-policy_ipsec_4] quit
[DeviceC-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

3. Configure static routes.

   # Configure a default route with the next hop 4.4.4.254.

   ```
   [DeviceC] ip route-static 0.0.0.0 0.0.0.0 4.4.4.254
   ```

   # Configure a static route to the headquarters intranet with the next hop 4.4.4.254.

   ```
   [DeviceC] ip route-static 10.3.0.0 255.255.255.0 4.4.4.254
   ```

4. Configure an IPsec policy.

   # Create an advanced ACL to define the data flows to be protected.

   ```
   [DeviceC] acl 3000
   [DeviceC-acl4-advance-3000] rule 5 permit ip source 10.4.1.0 0.0.0.255 destination 10.3.0.0
   0.0.0.255
   [DeviceC-acl4-advance-3000] quit
   ```

   # Configure an IPsec proposal.

   ```
   [DeviceC] ipsec proposal tran1
   [DeviceC-ipsec-proposal-tran1] encapsulation-mode tunnel
   [DeviceC-ipsec-proposal-tran1] transform esp
   [DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceC-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceC] ike proposal 10
[DeviceC-ike-proposal-10] authentication-method pre-share
[DeviceC-ike-proposal-10] prf hmac-sha2-256
[DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceC-ike-proposal-10] dh group14
[DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceC-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceC] ike peer a
[DeviceC-ike-peer-a] ike-proposal 10
[DeviceC-ike-peer-a] remote-address 1.1.1.1
[DeviceC-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceC-ike-peer-a] quit
```

NOTE

The IP address specified by **remote-address** must be set to the VRRP group virtual IP address of the peer.

Configure an IPsec policy.

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy to GE0/0/1.

```
[DeviceC] interface ge 0/0/1
[DeviceC-GE0/0/1] ipsec policy map1
[DeviceC-GE0/0/1] quit
```

Step 8 Configure switches.

Add the interfaces of switches in **Figure 8-26** to the same VLAN. For configuration details, see the documents of the switches.

----End

Verifying the Configuration

1. Enable branch devices on the network segment 10.4.1.0/24 to access the servers on the network segment 10.3.0.0/24 at the headquarters. The branch devices can successfully access the headquarters servers.
2. Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB. The command outputs show that IPsec SAs have been generated, indicating that the IPsec tunnel has been established and backed up successfully.
3. Disconnect GE0/0/3 or GE0/0/2 of DeviceA. Services can be properly switched to DeviceB.

Configuration Scripts

- DeviceA (at the headquarters)

```
#
sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
hrp enable
hrp interface GE0/0/1 remote 10.10.0.2
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4lqCB.ZE~lJJ`kv&=Du9:}^>aY!!!!!!!!!!!!!!!:!!!!
&P*JDAZ\&O=VY`FDa)\W#`d47_S=MAd$C*8!!!!!%+%#
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
acl number 3000
 rule 5 permit ip source 10.3.0.0 0.0.0.255 destination 10.4.1.0 0.0.0.255
#
interface GE0/0/1
 ip address 10.10.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.2 255.255.255.0
 vrrp vrid 2 virtual-ip 1.1.1.1 active
 ipsec policy map1
#
interface GE0/0/3
 ip address 10.3.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.2 active
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
ip route-static 10.4.1.0 255.255.255.0 1.1.1.254
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer any
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4z1Y~+B1$6HK#=<)TbjAC#D;]B!!!!!!!!!!!!!!!:!!!!
OZ"$HYj.6/bsbT~![qY.SyLs7OZsL<loti-!!!!!%+%#
 ike-proposal 10
#
ipsec policy-template policy1 1
 security acl 3000
 ike-peer any
 proposal tran1
 tunnel local 1.1.1.1
#
ipsec policy map1 10 isakmp template policy1
#
security-policy
 rule name ha_local_to_dmz
  source-zone dmz
  source-zone local
  destination-zone dmz
  destination-zone local
  service protocol udp destination-port 18514
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.4.1.0 mask 255.255.255.0
  action permit
 rule name policy_ipsec_2
   source-zone untrust
   destination-zone trust
   source-address 10.4.1.0 mask 255.255.255.0
   destination-address 10.3.0.0 mask 255.255.255.0
   action permit
 rule name policy_ipsec_3
   source-zone local
   destination-zone untrust
   source-address 1.1.1.1 mask 255.255.255.255
   destination-address 4.4.4.4 mask 255.255.255.255
   action permit
 rule name policy_ipsec_4
   source-zone untrust
   destination-zone local
   source-address 4.4.4.4 mask 255.255.255.255
   destination-address 1.1.1.1 mask 255.255.255.255
   action permit
#
return
```

- DeviceB (at the headquarters)

```
#
sysname DeviceB
#
hrp enable
hrp interface GE0/0/1 remote 10.10.0.1
hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4lqCB.ZE~lJJ`kv&=Du9:}^>aY!!!!!!!!!!!!!!!:!!!!
&P*JDAZ\&O=VY`FDa)\W#`d47_S=MAd$C*8!!!!!%+%#
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
acl number 3000
 rule 5 permit ip source 10.3.0.0 0.0.0.255 destination 10.4.1.0 0.0.0.255
#
interface GE0/0/1
 ip address 10.10.0.2 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.3 255.255.255.0
 vrrp vrid 2 virtual-ip 1.1.1.1 standby
 ipsec policy map1
#
interface GE0/0/3
 ip address 10.3.0.4 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.2 standby
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
ip route-static 10.4.1.0 255.255.255.0 1.1.1.254
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer any
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4z1Y~+B1$6HK#=<)TbjAC#D;]B!!!!!!!!!!!!!!!:!!!!
OZ"$HYj.6/bsbT~![qY.SyLs7OZsL<loti-!!!!!%+%#
 ike-proposal 10
#
ipsec policy-template policy1 1
 security acl 3000
 ike-peer any
 proposal tran1
 tunnel local 1.1.1.1
#
ipsec policy map1 10 isakmp template policy1
#
security-policy
 rule name ha_local_to_dmz
   source-zone dmz
   source-zone local
   destination-zone dmz
   destination-zone local
   service protocol udp destination-port 18514
   action permit
 rule name policy_ipsec_1
   source-zone trust
   destination-zone untrust
   source-address 10.3.0.0 mask 255.255.255.0
   destination-address 10.4.1.0 mask 255.255.255.0
   action permit
 rule name policy_ipsec_2
   source-zone untrust
   destination-zone trust
   source-address 10.4.1.0 mask 255.255.255.0
   destination-address 10.3.0.0 mask 255.255.255.0
   action permit
 rule name policy_ipsec_3
   source-zone local
   destination-zone untrust
   source-address 1.1.1.1 mask 255.255.255.255
   destination-address 4.4.4.4 mask 255.255.255.255
   action permit
 rule name policy_ipsec_4
   source-zone untrust
   destination-zone local
   source-address 4.4.4.4 mask 255.255.255.255
   destination-address 1.1.1.1 mask 255.255.255.255
   action permit
#
return
```

- DeviceC (at the branch)

```
#
sysname DeviceC
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
acl 3000
 rule 5 permit ip source 10.4.1.0 0.0.0.255 destination 10.3.0.0 0.0.0.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE0/0/3
 ip address 10.4.1.1 255.255.255.0
#
interface GE0/0/1

 ip address 4.4.4.4 255.255.255.0
 ipsec policy map1
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.254
ip route-static 10.3.0.0 255.255.255.0 4.4.4.254
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer a
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4ST[pC*<yh-&9W|)2lfVLf7%5I!!!!!!!!!!!!!!!:!!!!n7dU
%;7acX'M9k5uxAt3m;tC=T\OM!B:3QY!!!!!%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
#
security-policy
  rule name policy_ipsec_1
    source-zone trust
    destination-zone untrust
    source-address 10.4.1.0 mask 255.255.255.0
    destination-address 10.3.0.0 mask 255.255.255.0
    action permit
  rule name policy_ipsec_2
    source-zone untrust
    destination-zone trust
    source-address 10.3.0.0 mask 255.255.255.0
    destination-address 10.4.1.0 mask 255.255.255.0
    action permit
  rule name policy_ipsec_3
    source-zone local
    destination-zone untrust
    source-address 4.4.4.4 mask 255.255.255.255
    destination-address 1.1.1.1 mask 255.255.255.255
    action permit
  rule name policy_ipsec_4
    source-zone untrust
    destination-zone local
    source-address 1.1.1.1 mask 255.255.255.255
    destination-address 4.4.4.4 mask 255.255.255.255
    action permit
#
return
```

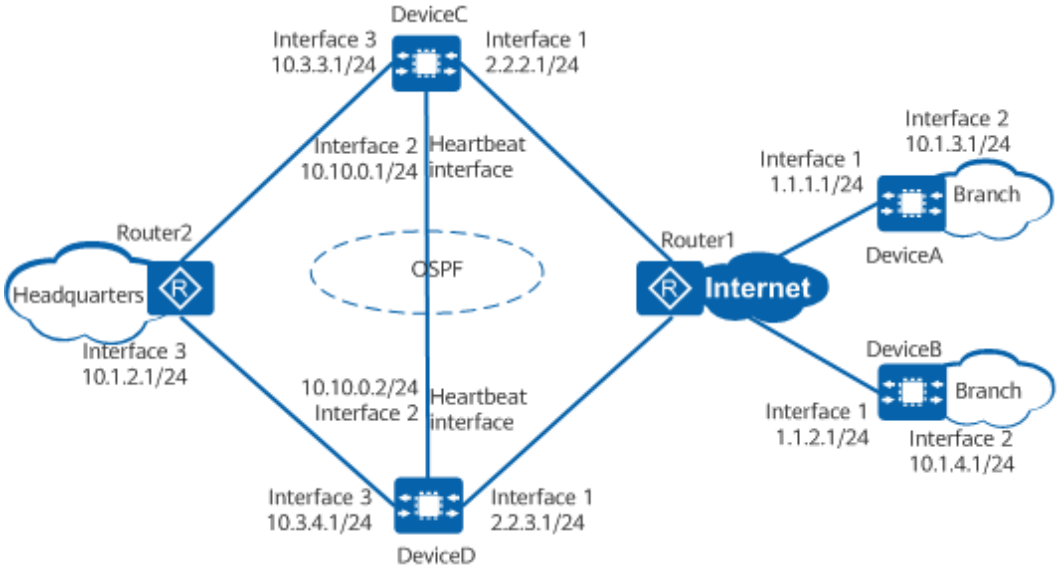
 Copyright © Huawei Technologies Co., Ltd.

8.5.2 CLI: Example for Establishing an IPsec Tunnel in Load Balancing Mode (Routers Serving as Upstream and Downstream Devices)

Networking Requirements

As shown in **Figure 8-27**, the headquarters and branches connect to the Internet through IPsec gateways. IPsec gateways (DeviceC and DeviceD) at the headquarters work in load balancing mode. Their service interfaces work in Layer 3 mode, and OSPF is used between these gateways and upstream as well as downstream routers. The enterprise requires that an IPsec tunnel be established to protect traffic from the branches to the headquarters, that DeviceC preferentially process the traffic sent from DeviceA to the headquarters, and that DeviceD preferentially process the traffic sent from DeviceB to the headquarters. If DeviceC or DeviceD fails, all the traffic sent from the branches to the headquarters is switched to the other operational device.

Figure 8-27 Establishing IPsec tunnels on devices in load balancing mode



Item	Data
DeviceA	Interface: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.1.3.1/24 Security zone: Trust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Method of creating an IPsec policy: ISAKMP PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: IP address
DeviceB	Interface: GE0/0/1 IP address: 1.1.2.1/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.1.4.1/24 Security zone: Trust
	IPsec configuration Method of creating an IPsec policy: ISAKMP PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: IP address
DeviceC	Interface: GE0/0/1 IP address: 2.2.2.1/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.10.0.1/24 (heartbeat interface) Security zone: DMZ
	Interface: GE0/0/3 IP address: 10.3.3.1/24 Security zone: Trust
	Tunnel 1 IP address: 2.2.4.1/24 Security zone: Untrust
	Tunnel 2 IP address: 2.2.5.1/24 Security zone: Untrust
	IPsec configuration Method of creating an IPsec policy: ISAKMP PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: IP address

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
DeviceD	Interface: GE0/0/1 IP address: 2.2.3.1/24 Security zone: Untrust
	Interface: GE0/0/2 IP address: 10.10.0.2/24 (heartbeat interface) Security zone: DMZ
	Interface: GE0/0/3 IP address: 10.3.4.1/24 Security zone: Trust
	Tunnel 1 IP address: 2.2.4.1/24 Security zone: Untrust
	Tunnel 2 IP address: 2.2.5.1/24 Security zone: Untrust
	IPsec configuration Method of creating an IPsec policy: ISAKMP PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: IP address

Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

1. Configure DeviceC and DeviceD to work in load balancing mode.
2. Create two tunnel interfaces Tunnel 1 and Tunnel 2 on each of DeviceC and DeviceD. The IP address of Tunnel 1 is the same on the two devices, and the IP address of Tunnel 2 is the same on the two devices. Tunnel 1 on DeviceC is used to establish a primary IPsec tunnel with DeviceA, and Tunnel 1 on DeviceD is used to establish a backup IPsec tunnel with DeviceA. Similarly, Tunnel 2 on DeviceD is used to establish a primary IPsec tunnel with DeviceB, and Tunnel 2 on DeviceC is used to establish a backup IPsec tunnel with DeviceB. Then DeviceA and DeviceB each have two IPsec tunnels, one with DeviceC and the other with DeviceD. When DeviceC and DeviceD are working properly, DeviceA and DeviceB send traffic to the headquarters through their

 Copyright © Huawei Technologies Co., Ltd.

respective primary IPsec tunnels. If DeviceC or DeviceD fails, DeviceA or DeviceB sends traffic to the headquarters through their respective backup IPsec tunnels.

3. Configure routing policies on DeviceC and DeviceD to change the route preference following the device state change. When DeviceC and DeviceD are working properly, the traffic sent from the headquarters to DeviceA is directed to DeviceC, and the traffic sent from the headquarters to DeviceB is directed to DeviceD. If DeviceC fails, all the traffic sent from the headquarters to DeviceA and DeviceB is directed to DeviceD.
4. Apply IPsec policies to the public network interfaces of DeviceA and DeviceB to establish IPsec tunnels with DeviceC and DeviceD, respectively.

Procedure

Step 1 Complete basic network configurations on DeviceC and DeviceD.

DeviceC	DeviceD
# Configure an IP address for each interface on DeviceC and DeviceD.	
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceC** [DeviceC] **interface ge 0/0/1** [DeviceC-GE0/0/1] **ip address 2.2.2.1 24** [DeviceC-GE0/0/1] **quit** [DeviceC] **interface ge 0/0/2** [DeviceC-GE0/0/2] **ip address 10.10.0.1 24** [DeviceC-GE0/0/2] **quit** [DeviceC] **interface ge 0/0/3** [DeviceC-GE0/0/3] **ip address 10.3.3.1 24** [DeviceC-GE0/0/3] **quit** [DeviceC] **interface Tunnel 1** [DeviceC-Tunnel1] **tunnel-protocol ipsec** [DeviceC-Tunnel1] **ip address 2.2.4.1 24** [DeviceC-Tunnel1] **quit** [DeviceC] **interface Tunnel 2** [DeviceC-Tunnel2] **tunnel-protocol ipsec** [DeviceC-Tunnel2] **ip address 2.2.5.1 24** [DeviceC-Tunnel2] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceD** [DeviceD] **interface ge 0/0/1** [DeviceD-GE0/0/1] **ip address 2.2.3.1 24** [DeviceD-GE0/0/1] **quit** [DeviceD] **interface ge 0/0/2** [DeviceD-GE0/0/2] **ip address 10.10.0.2 24** [DeviceD-GE0/0/2] **quit** [DeviceD] **interface ge0/0/3** [DeviceD-GE0/0/3] **ip address 10.3.4.1 24** [DeviceD-GE0/0/3] **quit** [DeviceD] **interface Tunnel 1** [DeviceD-Tunnel1] **tunnel-protocol ipsec** [DeviceD-Tunnel1] **ip address 2.2.4.1 24** [DeviceD-Tunnel1] **quit** [DeviceD] **interface Tunnel 2** [DeviceD-Tunnel2] **tunnel-protocol ipsec** [DeviceD-Tunnel2] **ip address 2.2.5.1 24** [DeviceD-Tunnel2] **quit**
# Add each interface on DeviceC and DeviceD to a security zone.	
[DeviceC] **firewall zone untrust** [DeviceC-zone-untrust] **add interface ge 0/0/1** [DeviceC-zone-untrust] **add interface Tunnel 1** [DeviceC-zone-untrust] **add interface Tunnel 2** [DeviceC-zone-untrust] **quit** [DeviceC] **firewall zone trust** [DeviceC-zone-trust] **add interface ge 0/0/3** [DeviceC-zone-trust] **quit** [DeviceC] **firewall zone dmz** [DeviceC-zone-dmz] **add interface ge 0/0/2** [DeviceC-zone-dmz] **quit**	[DeviceD] **firewall zone untrust** [DeviceD-zone-untrust] **add interface ge 0/0/1** [DeviceD-zone-untrust] **add interface Tunnel 1** [DeviceD-zone-untrust] **add interface Tunnel 2** [DeviceD-zone-untrust] **quit** [DeviceD] **firewall zone trust** [DeviceD-zone-trust] **add interface ge 0/0/3** [DeviceD-zone-trust] **quit** [DeviceD] **firewall zone dmz** [DeviceD-zone-dmz] **add interface ge 0/0/2** [DeviceD-zone-dmz] **quit**
# Configure static routes on DeviceC and DeviceD.	
[DeviceC] **ip route-static 10.1.3.0 24 tunnel 1** [DeviceC] **ip route-static 10.1.4.0 24 tunnel 2**	[DeviceD] **ip route-static 10.1.3.0 24 tunnel 1** [DeviceD] **ip route-static 10.1.4.0 24 tunnel 2**

Step 2 Configure security policies on DeviceC and DeviceD to allow heartbeat interfaces to exchange Huawei Redundancy Protocol (HRP) packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Whether HRP packets are controlled by security policies depends on the configuration of the **firewall packet-filter basic-protocol enable** command. By default, the controlling function of security policies for HRP packets is enabled. In this case, you need to configure security policies between the security zone where the heartbeat interface resides and the Local zone to permit HRP packets. In this example, the controlling function of security policies for HRP packets (configured using the **firewall packet-filter basic-protocol enable** command) is enabled.

DeviceC	DeviceD
[DeviceC] **security-policy** [DeviceC-policy-security] **rule name ha_local_to_dmz** [DeviceC-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceC-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceC-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceC-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceC-policy-security-rule-ha_local_to_dmz] **quit** [DeviceC-policy-security] **quit**	[DeviceD] **security-policy** [DeviceD-policy-security] **rule name ha_local_to_dmz** [DeviceD-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceD-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceD-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceD-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceD-policy-security-rule-ha_local_to_dmz] **quit** [DeviceD-policy-security] **quit**

Step 3 Configure HRP on DeviceC and DeviceD.

DeviceC	DeviceD
[DeviceC] **hrp interface ge 0/0/2 remote 10.10.0.2** [DeviceC] **hrp auto-sync config** [DeviceC] **hrp mirror session enable** [DeviceC] **hrp track interface ge 0/0/1** [DeviceC] **hrp track interface ge 0/0/3** [DeviceC] **hrp adjust ospf-cost enable** [DeviceC] **hrp authentication-key YsHsjx_202206** [DeviceC] **hrp enable**	[DeviceD] **hrp interface ge 0/0/2 remote 10.10.0.1** [DeviceD] **hrp auto-sync config** [DeviceD] **hrp mirror session enable** [DeviceD] **hrp track interface ge 0/0/1** [DeviceD] **hrp track interface ge 0/0/3** [DeviceD] **hrp adjust ospf-cost enable** [DeviceD] **hrp authentication-key YsHsjx_202206** [DeviceD] **hrp enable**

Step 4 # Configure OSPF on DeviceC and DeviceD.

To ensure that the traffic sent from DeviceA to the headquarters is transmitted along the path DeviceA -> Router1 -> DeviceC -> Router2 and the traffic from DeviceB to the headquarters along the path DeviceB -> Router1 -> DeviceD -> Router2, configure routing policies on DeviceC and DeviceD to control routing information of Router1 and Router2.

When DeviceC and DeviceD work in load balancing mode, DeviceC and DeviceD advertise the direct routes destined for Tunnel 1 to Router1 and advertise the private network routes (static routes) destined for DeviceA to Router2. To forward different flows based on different routes, you need to control the direct routes and static routes advertised by DeviceC and DeviceD.

When DeviceC works in load balancing mode, Router1 needs to send the traffic of DeviceA to Tunnel 1 of DeviceC instead of Tunnel 1 of DeviceD. Therefore, when DeviceC advertises the route destined for Tunnel 1, the route cost will be reduced by 10. When DeviceD advertises the route destined for Tunnel 1, the route cost

 Copyright © Huawei Technologies Co., Ltd.

will be increased by 10. In this way, Router1 sends the traffic of DeviceA to DeviceC based on the route cost.

In addition, Router2 needs to send the return traffic destined for DeviceA to DeviceC instead of DeviceD. Therefore, when DeviceC advertises the private network route (static route) destined for DeviceA, the route cost will be reduced by 10. When DeviceD advertises the private network route (static route) destined for DeviceA, the route cost will be increased by 10. In this way, Router2 sends the return traffic destined for DeviceA to DeviceC based on the route cost.

If DeviceD fails, the OSPF costs of routes are adjusted based on HRP active/standby states, enabling all the traffic of DeviceA and DeviceB to be sent to DeviceC.

If DeviceC fails, the OSPF costs of routes are adjusted based on HRP active/standby states, enabling all the traffic of DeviceA and DeviceB to be sent to DeviceD.

Perform the following configurations on the HRP active device. The configurations will be automatically synchronized to the HRP standby device.

Configure the ACLs used in routing policies.

```
HRP_M[DeviceC] acl 2000
HRP_M[DeviceC-acl4-basic-2000] rule permit source 2.2.4.0 0.0.0.255
HRP_M[DeviceC-acl4-basic-2000] rule permit source 10.1.3.0 0.0.0.255
HRP_M[DeviceC-acl4-basic-2000] quit
HRP_M[DeviceC] acl 2001
HRP_M[DeviceC-acl4-basic-2001] rule permit source 2.2.5.0 0.0.0.255
HRP_M[DeviceC-acl4-basic-2001] rule permit source 10.1.4.0 0.0.0.255
HRP_M[DeviceC-acl4-basic-2001] quit
```

Perform the following configurations on both the HRP active and standby devices.

Configure a routing policy on the HRP active device.

```
HRP_M[DeviceC] route-policy rp permit node 1
HRP_M[DeviceC-route-policy] if-match acl 2000
HRP_M[DeviceC-route-policy] apply cost - 10
HRP_M[DeviceC-route-policy] quit
HRP_M[DeviceC] route-policy rp permit node 2
HRP_M[DeviceC-route-policy] if-match acl 2001
HRP_M[DeviceC-route-policy] apply cost + 10
HRP_M[DeviceC-route-policy] quit
HRP_M[DeviceC] ospf 1
HRP_M[DeviceC-ospf-1] import-route direct type 1 route-policy rp
HRP_M[DeviceC-ospf-1] import-route static type 1 route-policy rp
HRP_M[DeviceC-ospf-1] area 0.0.0.0
HRP_M[DeviceC-ospf-1-area-0.0.0.0] network 10.3.3.0 0.0.0.255
HRP_M[DeviceC-ospf-1-area-0.0.0.0] network 2.2.2.0 0.0.0.255
HRP_M[DeviceC-ospf-1-area-0.0.0.0] quit
HRP_M[DeviceC-ospf-1] quit
```

Configure a routing policy on the HRP standby device.

```
HRP_S[DeviceD] route-policy rp permit node 1
HRP_S[DeviceD-route-policy] if-match acl 2000
HRP_S[DeviceD-route-policy] apply cost + 10
HRP_S[DeviceD-route-policy] quit
HRP_S[DeviceD] route-policy rp permit node 2
HRP_S[DeviceD-route-policy] if-match acl 2001
HRP_S[DeviceD-route-policy] apply cost - 10
HRP_S[DeviceD-route-policy] quit
HRP_S[DeviceD] ospf 1
HRP_S[DeviceD-ospf-1] import-route direct type 1 route-policy rp
HRP_S[DeviceD-ospf-1] import-route static type 1 route-policy rp
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_S[DeviceD-ospf-1] area 0.0.0.0
HRP_S[DeviceD-ospf-1-area-0.0.0.0] network 10.3.4.0 0.0.0.255
HRP_S[DeviceD-ospf-1-area-0.0.0.0] network 2.2.3.0 0.0.0.255
HRP_S[DeviceD-ospf-1-area-0.0.0.0] quit
HRP_S[DeviceD-ospf-1] quit
```

NOTICE

When configuring OSPF, configure inter-zone security policies correctly to prevent normal routing protocol packets from being blocked.

Step 5 Configure security policies on DeviceC. After HRP is enabled, the security policy configuration on DeviceC will be automatically backed up to DeviceD.

Configure security policies between the Trust and Untrust zones to allow pre-encapsulated and decapsulated packets to pass through DeviceC.

```
HRP_M[DeviceC] security-policy
HRP_M[DeviceC-policy-security] rule name 1
HRP_M[DeviceC-policy-security-rule-1] source-zone untrust
HRP_M[DeviceC-policy-security-rule-1] destination-zone trust
HRP_M[DeviceC-policy-security-rule-1] source-address 10.1.3.0 24
HRP_M[DeviceC-policy-security-rule-1] source-address 10.1.4.0 24
HRP_M[DeviceC-policy-security-rule-1] destination-address 10.1.2.0 24
HRP_M[DeviceC-policy-security-rule-1] action permit
HRP_M[DeviceC-policy-security-rule-1] quit
HRP_M[DeviceC-policy-security] rule name 2
HRP_M[DeviceC-policy-security-rule-2] source-zone trust
HRP_M[DeviceC-policy-security-rule-2] destination-zone untrust
HRP_M[DeviceC-policy-security-rule-2] source-address 10.1.2.0 24
HRP_M[DeviceC-policy-security-rule-2] destination-address 10.1.3.0 24
HRP_M[DeviceC-policy-security-rule-2] destination-address 10.1.4.0 24
HRP_M[DeviceC-policy-security-rule-2] action permit
HRP_M[DeviceC-policy-security-rule-2] quit
```

Configure a security policy to allow the device to exchange OSPF packets with upstream and downstream routers.

NOTE

Whether OSPF packets are controlled by security policies depends on the configuration of the **firewall packet-filter basic-protocol enable** command. By default, the controlling function of security policies for OSPF packets is enabled. In this case, you need to configure a security policy between the security zone where the upstream and downstream service interfaces reside and the Local zone to permit OSPF packets. In this example, the controlling function of security policies for OSPF packets (configured using the **firewall packet-filter basic-protocol enable** command) is enabled.

```
HRP_M[DeviceC-policy-security] rule name policy_ospf_1
HRP_M[DeviceC-policy-security-rule-policy_ospf_1] source-zone local
HRP_M[DeviceC-policy-security-rule-policy_ospf_1] destination-zone trust untrust
HRP_M[DeviceC-policy-security-rule-policy_ospf_1] service ospf
HRP_M[DeviceC-policy-security-rule-policy_ospf_1] action permit
HRP_M[DeviceC-policy-security-rule-policy_ospf_1] quit
HRP_M[DeviceC-policy-security] rule name policy_ospf_2
HRP_M[DeviceC-policy-security-rule-policy_ospf_2] source-zone trust untrust
HRP_M[DeviceC-policy-security-rule-policy_ospf_2] destination-zone local
HRP_M[DeviceC-policy-security-rule-policy_ospf_2] service ospf
HRP_M[DeviceC-policy-security-rule-policy_ospf_2] action permit
HRP_M[DeviceC-policy-security-rule-policy_ospf_2] quit
```

Configure security policies between the Local and Untrust zones to allow IKE negotiation packets to pass through DeviceC.

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceC-policy-security] rule name 3
HRP_M[DeviceC-policy-security-rule-3] source-zone local
HRP_M[DeviceC-policy-security-rule-3] destination-zone untrust
HRP_M[DeviceC-policy-security-rule-3] source-address 2.2.0.0 16
HRP_M[DeviceC-policy-security-rule-3] destination-address 1.1.0.0 16
HRP_M[DeviceC-policy-security-rule-3] action permit
HRP_M[DeviceC-policy-security-rule-3] quit
HRP_M[DeviceC-policy-security] rule name 4
HRP_M[DeviceC-policy-security-rule-4] source-zone untrust
HRP_M[DeviceC-policy-security-rule-4] destination-zone local
HRP_M[DeviceC-policy-security-rule-4] source-address 1.1.0.0 16
HRP_M[DeviceC-policy-security-rule-4] destination-address 2.2.0.0 16
HRP_M[DeviceC-policy-security-rule-4] action permit
HRP_M[DeviceC-policy-security-rule-4] quit
HRP_M[DeviceC-policy-security] quit
```

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Step 6 Configure IPsec policies on DeviceC and apply the policies to tunnel interfaces. After HRP is enabled, the IPsec policy configuration on DeviceC will be automatically backed up to DeviceD.

Configure ACLs.

```
HRP_M[DeviceC] acl 3005
HRP_M[DeviceC-acl4-advance-3005] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.3.0
0.0.0.255
HRP_M[DeviceC-acl4-advance-3005] quit
HRP_M[DeviceC] acl 3006
HRP_M[DeviceC-acl4-advance-3006] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.4.0
0.0.0.255
HRP_M[DeviceC-acl4-advance-3006] quit
```

Configure an IPsec proposal.

```
HRP_M[DeviceC] ipsec proposal tran1
HRP_M[DeviceC-ipsec-proposal-tran1] encapsulation-mode tunnel
HRP_M[DeviceC-ipsec-proposal-tran1] transform esp
HRP_M[DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
HRP_M[DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
HRP_M[DeviceC-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
HRP_M[DeviceC] ike proposal 10
HRP_M[DeviceC-ike-proposal-10] authentication-method pre-share
HRP_M[DeviceC-ike-proposal-10] prf hmac-sha2-256
HRP_M[DeviceC-ike-proposal-10] encryption-algorithm aes-gcm-256
HRP_M[DeviceC-ike-proposal-10] dh group14
HRP_M[DeviceC-ike-proposal-10] integrity-algorithm hmac-sha2-256
HRP_M[DeviceC-ike-proposal-10] quit
```

Configure IKE peers.

```
HRP_M[DeviceC] ike peer fw_a
HRP_M[DeviceC-ike-peer-fw_a] ike-proposal 10
HRP_M[DeviceC-ike-peer-fw_a] remote-address 1.1.1.1
HRP_M[DeviceC-ike-peer-fw_a] pre-shared-key YsHsjx_202206
HRP_M[DeviceC-ike-peer-fw_a] quit
HRP_M[DeviceC] ike peer fw_b
HRP_M[DeviceC-ike-peer-fw_b] ike-proposal 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceC-ike-peer-fw_b] remote-address 1.1.2.1
HRP_M[DeviceC-ike-peer-fw_b] pre-shared-key YsHsjx_202206
HRP_M[DeviceC-ike-peer-fw_b] quit
```

Configure two IPsec policies.

```
HRP_M[DeviceC] ipsec policy map1 10 isakmp
HRP_M[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3005
HRP_M[DeviceC-ipsec-policy-isakmp-map1-10] proposal tran1
HRP_M[DeviceC-ipsec-policy-isakmp-map1-10] ike-peer fw_a
HRP_M[DeviceC-ipsec-policy-isakmp-map1-10] quit
HRP_M[DeviceC] ipsec policy map2 10 isakmp
HRP_M[DeviceC-ipsec-policy-isakmp-map2-10] security acl 3006
HRP_M[DeviceC-ipsec-policy-isakmp-map2-10] proposal tran1
HRP_M[DeviceC-ipsec-policy-isakmp-map2-10] ike-peer fw_b
HRP_M[DeviceC-ipsec-policy-isakmp-map2-10] quit
```

Apply the IPsec policies to tunnel interfaces.

```
HRP_M[DeviceC] interface tunnel 1
HRP_M[DeviceC-Tunnel1] ipsec policy map1 master
HRP_M[DeviceC-Tunnel1] quit
HRP_M[DeviceC] interface tunnel 2
HRP_M[DeviceC-Tunnel2] ipsec policy map2 slave
HRP_M[DeviceC-Tunnel2] quit
```

Step 7 Configure branch gateways.

The following provides the configuration of DeviceA. The configuration of DeviceB is similar to that of DeviceA.

1. Complete basic network configurations, including configuring IP addresses for interfaces, adding interfaces to security zones, configuring inter-zone security policies, and configuring routes.

   # Configure IP addresses for interfaces and add interfaces to security zones.

   ```
   <HUAWEI> system-view
   [HUAWEI] sysname DeviceA
   [DeviceA] interface ge 0/0/1
   [DeviceA-GE0/0/1] ip address 1.1.1.1 24
   [DeviceA-GE0/0/1] quit
   [DeviceA] interface ge 0/0/2
   [DeviceA-GE0/0/2] ip address 10.1.3.1 24
   [DeviceA-GE0/0/2] quit
   [DeviceA] firewall zone untrust
   [DeviceA-zone-untrust] add interface ge 0/0/1
   [DeviceA-zone-untrust] quit
   [DeviceA] firewall zone trust
   [DeviceA-zone-trust] add interface ge 0/0/2
   [DeviceA-zone-trust] quit
   ```

   # Configure security policies between the Trust and Untrust zones to permit pre-encapsulated and decapsulated packets.

   ```
   [DeviceA] security-policy
   [DeviceA-policy-security] rule name 1
   [DeviceA-policy-security-rule-1] source-zone trust
   [DeviceA-policy-security-rule-1] destination-zone untrust
   [DeviceA-policy-security-rule-1] source-address 10.1.3.0 24
   [DeviceA-policy-security-rule-1] destination-address 10.1.2.0 24
   [DeviceA-policy-security-rule-1] action permit
   [DeviceA-policy-security-rule-1] quit
   [DeviceA-policy-security] rule name 2
   [DeviceA-policy-security-rule-2] source-zone untrust
   [DeviceA-policy-security-rule-2] destination-zone trust
   [DeviceA-policy-security-rule-2] source-address 10.1.2.0 24
   [DeviceA-policy-security-rule-2] destination-address 10.1.3.0 24
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-2] action permit
[DeviceA-policy-security-rule-2] quit
```

Configure security policies between the Local and Untrust zones to permit IKE negotiation packets.

```
[DeviceA-policy-security] rule name 3
[DeviceA-policy-security-rule-3] source-zone local
[DeviceA-policy-security-rule-3] destination-zone untrust
[DeviceA-policy-security-rule-3] source-address 1.1.0.0 16
[DeviceA-policy-security-rule-3] destination-address 2.2.0.0 16
[DeviceA-policy-security-rule-3] action permit
[DeviceA-policy-security-rule-3] quit
[DeviceA-policy-security] rule name 4
[DeviceA-policy-security-rule-4] source-zone untrust
[DeviceA-policy-security-rule-4] destination-zone local
[DeviceA-policy-security-rule-4] source-address 2.2.0.0 16
[DeviceA-policy-security-rule-4] destination-address 1.1.0.0 16
[DeviceA-policy-security-rule-4] action permit
[DeviceA-policy-security-rule-4] quit
[DeviceA-policy-security] quit
```

Configure a default route to the Internet with the next hop 1.1.1.2.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

2. Configure an IPsec policy.

   # Configure an ACL.

```
[DeviceA] acl 3000
[DeviceA-acl4-advance-3000] rule permit ip source 10.1.3.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl4-advance-3000] quit
```

   # Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceA-ipsec-proposal-tran1] transform esp
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

   # Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

   # Configure an IKE peer.

```
[DeviceA] ike peer fw_c
[DeviceA-ike-peer-fw_c] ike-proposal 10
[DeviceA-ike-peer-fw_c] remote-address 2.2.4.1
[DeviceA-ike-peer-fw_c] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-fw_c] quit
```

   # Configure an IPsec policy.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer fw_c
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

   # Apply the IPsec policy to an interface.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ipsec policy map1
[DeviceA-GE0/0/1] quit
```

----End

Verifying the Configuration

1. Enable devices on a branch private network to ping the headquarters private network to trigger IKE negotiation.

   If IKE negotiation succeeds, data transmitted between the branch and headquarters is encrypted after an IPsec tunnel is established.

2. Run the **display ipsec sa** command on DeviceA and DeviceB to check IPsec SA information. The following shows the command output of DeviceA. If information similar to the following is displayed, IPsec SAs have been established.

```
<DeviceA> display ipsec sa brief
IPsec SA information:
  Src address      Dst address      SPI          VPN      Protocol        Algorithm
-------------------------------------------------------------------------------------------------
  1.1.1.1          2.2.4.1          194639781             ESP             E:AES-256 A:SHA2_256_128
  2.2.4.1          1.1.1.1          184618952             ESP             E:AES-256 A:SHA2_256_128

 Number of IPsec SA : 2
-------------------------------------------------------------------------------------------------
```

3. Check whether services are normal during an HRP switchover.

   If the branches can access the headquarters resources normally in the following three scenarios, service configurations are correct:

   a. When DeviceA and DeviceB are operational, enable the PCs connected to the two devices to access the headquarters resources. If the access is successful, the configurations are correct.

   b. Disable the interface of DeviceC and then check whether the PCs can access the headquarters resources normally. If the access is successful, traffic can be switched from DeviceC to DeviceD.

   c. Enable the interface of DeviceC, disable the interface of DeviceD, and then check whether the PCs can access the headquarters resources normally. If the access is successful, traffic can be switched from DeviceD to DeviceC.

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/2
 ip address 10.1.3.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
ipsec proposal tran1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer fw_c
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4xMClN{a:!;.qs:RZcA'!R8>4+!!!!!!!!!!!!!!!!:!!!!
%Vnj&xWzxQ]:)$ME(2&8gjfs-Y7S[(M[)a;!!!!!%+%#
 ike-proposal 10
 remote-address 2.2.4.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer fw_c
 proposal tran1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name 1
  source-zone trust
  destination-zone untrust
  source-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name 2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
 rule name 3
  source-zone local
  destination-zone untrust
  source-address 1.1.0.0 mask 255.255.0.0
  destination-address 2.2.0.0 mask 255.255.0.0
  action permit
 rule name 4
  source-zone untrust
  destination-zone local
  source-address 2.2.0.0 mask 255.255.0.0
  destination-address 1.1.0.0 mask 255.255.0.0
  action permit
#
return
```

- DeviceB

```
#
sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.4.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
interface GE0/0/1
 ip address 1.1.2.1 255.255.255.0
 ipsec policy map1
#
interface GE0/0/2
 ip address 10.1.4.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer fw_d
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4xMClN{a:!;.qs:RZcA'!R8>4+!!!!!!!!!!!!!!:!!!!
%Vnj&xWzxQ]:)$ME(2&8gjfs-Y7S[(M[)a;!!!!!%+%#
 ike-proposal 10
 remote-address 2.2.5.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer fw_d
 proposal tran1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name 1
  source-zone trust
  destination-zone untrust
  source-address 10.1.4.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name 2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.4.0 mask 255.255.255.0
  action permit
 rule name 3
  source-zone local
  destination-zone untrust
  source-address 1.1.0.0 mask 255.255.0.0
  destination-address 2.2.0.0 mask 255.255.0.0
  action permit
 rule name 4
  source-zone untrust
  destination-zone local
  source-address 2.2.0.0 mask 255.255.0.0
  destination-address 1.1.0.0 mask 255.255.0.0
  action permit
#
return
```

- DeviceC

```
#
sysname DeviceC
#
hrp enable
hrp mirror session enable
hrp auto-sync config
hrp interface GE0/0/2 remote 10.10.0.2
hrp track interface GE0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!\FR0@B|5m51t2(SLB$(Yzq_KUB|V43Td3,.!!!!!!!!!!!!!!!:!!!!>
$P4S-0S{KqT>VWoG2!K9t\i4 t;1e+vR$$U!!!!!%+%#
#
acl number 2000
 rule 5 permit source 2.2.4.0 0.0.0.255
 rule 10 permit source 10.1.3.0 0.0.0.255
#
acl number 2001
 rule 5 permit source 2.2.5.0 0.0.0.255
 rule 10 permit source 10.1.4.0 0.0.0.255
#
acl number 3005
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
acl number 3006
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.4.0 0.0.0.255
#
interface GE0/0/1
 ip address 2.2.2.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.10.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.3.1 255.255.255.0
#
interface Tunnel 1
 ip address 2.2.4.1 255.255.255.0
 tunnel-protocol ipsec
 ipsec policy map1 master
#
interface Tunnel 2
 ip address 2.2.5.1 255.255.255.0
 tunnel-protocol ipsec
 ipsec policy map2 slave
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface Tunnel 1
 add interface Tunnel 2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer fw_a
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4pgwAD<nBQ=#tM1S7+g\~)*FxY!!!!!!!!!!!!!!!:!!!!
[2H>WK!;I-wz_13{Wn,*^~JU9mp2oV:<r{N!!!!!%+%#
 ike-proposal 10
 remote-address 1.1.1.1
ike peer fw_b
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4+boLPy7`h%y%2#">%;6~3!)Y@!!!!!!!!!!!!!!!:!!!!
```

 Copyright © Huawei Technologies Co., Ltd.

```
Evp2(J")o*^s0*~j]F8>]^;t-}'XjK3O_w=!!!!!%+%#
 ike-proposal 10
 remote-address 1.1.2.1
#
ipsec policy map1 10 isakmp
 security acl 3005
 ike-peer fw_a
 proposal tran1
ipsec policy map2 10 isakmp
 security acl 3006
 ike-peer fw_b
 proposal tran1
#
ospf 1
 import-route direct type 1 route-policy rp
 import-route static type 1 route-policy rp
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
  network 10.3.3.0 0.0.0.255
#
route-policy rp permit node 1
 if-match acl 2000
 apply cost - 10
#
route-policy rp permit node 2
 if-match acl 2001
 apply cost + 10
#
ip route-static 10.1.3.0 255.255.255.0 Tunnel1
ip route-static 10.1.4.0 255.255.255.0 Tunnel2
#
security-policy
 rule name ha_local_to_dmz
  source-zone dmz
  source-zone local
  destination-zone dmz
  destination-zone local
  service protocol udp destination-port 18514
  action permit
 rule name 1
  source-zone untrust
  destination-zone trust
  source-address 10.1.3.0 mask 255.255.255.0
  source-address 10.1.4.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name 2
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.4.0 mask 255.255.255.0
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
  action permit
 rule name policy_ospf_2
  source-zone trust
  source-zone untrust
  destination-zone local
  service ospf
  action permit
 rule name 3
  source-zone local
  destination-zone untrust
  source-address 2.2.0.0 mask 255.255.0.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-address 1.1.0.0 mask 255.255.0.0
 action permit
 rule name 4
 source-zone untrust
 destination-zone local
 source-address 1.1.0.0 mask 255.255.0.0
 destination-address 2.2.0.0 mask 255.255.0.0
 action permit
#
return
```

- DeviceD

```
#
sysname DeviceD
#
hrp enable
hrp mirror session enable
hrp auto-sync config
hrp interface GE0/0/2 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!J6+;U#>V\!_e1NY[iGLXjT%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
acl number 2000
 rule 5 permit source 2.2.4.0 0.0.0.255
 rule 10 permit source 10.1.3.0 0.0.0.255
#
acl number 2001
 rule 5 permit source 2.2.5.0 0.0.0.255
 rule 10 permit source 10.1.4.0 0.0.0.255
#
acl number 3005
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
acl number 3006
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.4.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer fw_a
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4pgwAD<nBQ=#tM1S7+g\~)*FxY!!!!!!!!!!!!!!!:!!!!
[2H>WK!;I-wz_13{Wn,*^~JU9mp2oV:<r{N!!!!!%+%#
 ike-proposal 10
 remote-address 1.1.1.1
ike peer fw_b
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!obe:Xx9B~4+boLPy7`h%y%2#">%;6~3!)Y@!!!!!!!!!!!!!!!:!!!!
Evp2(J")o*^s0*~j]F8>]^;t-}'XjK3O_w=!!!!!%+%#
 ike-proposal 10
 remote-address 1.1.2.1
#
ipsec policy map1 10 isakmp
 security acl 3005
 ike-peer fw_a
 proposal tran1
ipsec policy map2 10 isakmp
 security acl 3006
 ike-peer fw_b
 proposal tran1
#
interface GE0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 2.2.3.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.10.0.2 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.4.1 255.255.255.0
#
 ip address 2.2.4.1 255.255.255.0
 tunnel-protocol ipsec
 ipsec policy map1 slave
#
interface Tunnel 2
 ip address 2.2.5.1 255.255.255.0
 tunnel-protocol ipsec
 ipsec policy map2 master
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface Tunnel 1
 add interface Tunnel 2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
ospf 1
 import-route direct type 1 route-policy rp
 import-route static type 1 route-policy rp
 area 0.0.0.0
  network 2.2.3.0 0.0.0.255
  network 10.3.4.0 0.0.0.255
#
route-policy rp permit node 1
 if-match acl 2000
 apply cost + 10
#
route-policy rp permit node 2
 if-match acl 2001
 apply cost - 10
#
ip route-static 10.1.3.0 255.255.255.0 Tunnel1
ip route-static 10.1.4.0 255.255.255.0 Tunnel2
#
security-policy
 rule name 1
  source-zone untrust
  destination-zone trust
  source-address 10.1.3.0 mask 255.255.255.0
  source-address 10.1.4.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name 2
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.3.0 mask 255.255.255.0
  destination-address 10.1.4.0 mask 255.255.255.0
  action permit
 rule name policy_ospf_1
  source-zone local
  destination-zone trust
  destination-zone untrust
  service ospf
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
rule name policy_ospf_2
 source-zone trust
 source-zone untrust
 destination-zone local
 service ospf
 action permit
rule name 3
 source-zone local
 destination-zone untrust
 source-address 2.2.0.0 mask 255.255.0.0
 destination-address 1.1.0.0 mask 255.255.0.0
 action permit
rule name 4
 source-zone untrust
 destination-zone local
 source-address 1.1.0.0 mask 255.255.0.0
 destination-address 2.2.0.0 mask 255.255.0.0
 action permit
#
return
```

8.6 IPsec Intelligent Uplink Selection

8.6.1 Web: Example for Configuring IPsec Intelligent Uplink Selection Based on Link Quality Detection (with Automatic Link Switchback Enabled)

Networking Requirements

As shown in **Figure 8-28**, the HQ and branch are connected to the Internet through DeviceA and DeviceB. DeviceA is connected to the Internet through two links, and DeviceB is connected to the Internet through one link.

The requirements are as follows:

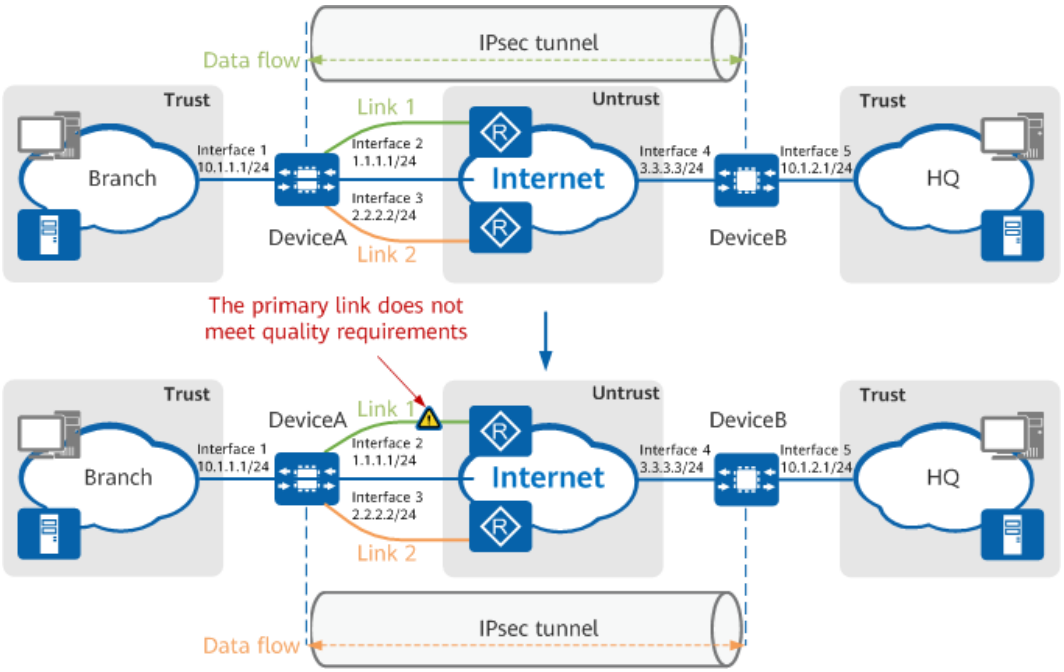
- An IPsec tunnel needs to be established between DeviceA and DeviceB for communication between the HQ and branch.
- DeviceA first establishes an IPsec tunnel with the HQ based on Link 1. If the IPsec tunnel has a high packet loss rate or delay, DeviceA automatically establishes another IPsec tunnel based on Link 2.
- When automatic link switchback is enabled on DeviceA, after Link 1 recovers, DeviceA automatically switches traffic back from the IPsec tunnel established based on Link 2 to that established based on Link 1.

Figure 8-28 Network diagram of IPsec intelligent uplink selection

NOTE

In this example, interface 1, interface 2, interface 3, interface 4, and interface 5 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/5, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item		DeviceA	DeviceB
Intranet interface		Interface: GE 0/0/1 IP address: 10.1.1.1/24 Security zone: Trust	Interface: GE 0/0/5 IP address: 10.1.2.1/24 Security zone: Trust
External network interface		• Interface: GE 0/0/2 IP address: 1.1.1.1/24 Security zone: Untrust • Interface: GE 0/0/3 IP address: 2.2.2.2/24 Security zone: Untrust	Interface: GE 0/0/4 IP address: 3.3.3.3/24 Security zone: Untrust
Loopback interface		Interface number: 1 IP address: 192.168.1.1	Interface number: 1 IP address: 192.168.2.1
Method of configuring an IPsec policy		ISAKMP + IPsec intelligent uplink selection (based on link quality detection)	Using an IPsec policy template
IPsec proposal	ESP authentication algorithm	SHA2-256	SHA2-256
	ESP encryption algorithm	AES-256-GCM-128	AES-256-GCM-128

 Copyright © Huawei Technologies Co., Ltd.

Item		DeviceA	DeviceB
IKE proposal	Verification method	Pre-shared key	Pre-shared key
	PRF algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	DH group	Group 14	Group 14
	Authentication algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	Encryption algorithm	AES-GCM-256	AES-GCM-256
IKE peer	Pre-shared key	YsHsjx_202206	YsHsjx_202206
	Identity type	IP	IP
	Peer IP address	3.3.3.3	Unspecified

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

- On DeviceA:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure an IPsec intelligent uplink selection profile based on link quality detection and enable the automatic link switchback function.
  d. Configure an ISAKMP IPsec policy and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.
- On DeviceB:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure a template IPsec policy.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure GE0/0/1, GE0/0/2, GE0/0/3, and loopback interfaces on DeviceA.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	trust
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	10.1.1.1/24

3. Click corresponding to GE0/0/2 and set the parameters as follows. Click **OK**.

Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	1.1.1.1/24

4. Click corresponding to GE0/0/3 and set the parameters as follows. Click **OK**.

Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	2.2.2.2/24

5. On the **Network** > **Interface** page, click **Add** to create a local loopback interface. Set the parameters as follows. Click **OK**.

Type	Loopback Interface
Index	1
Virtual System	public
VPN Instance	public

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	192.168.1.1/32

Step 2 Configure security policies on DeviceA to allow the branch and HQ to exchange packets through a specified network segment.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure security policies between the Trust and Untrust zones to allow unencapsulated and decapsulated packets to pass through DeviceA. Click **OK**.

Name	policy1
Source Zone	trust
Source IP Address	10.1.1.0/24
Destination Type	Zone
Destination Zone	untrust
Destination IP Address	10.1.2.0/24
Protocol	any
Action	Permit

Name	policy2
Source Zone	untrust
Source IP Address	10.1.2.0/24
Destination Type	Zone
Destination Zone	trust
Destination IP Address	10.1.1.0/24
Action	Permit

3. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation and continuous link quality detection. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Name	policy3
Source Zone	local
Source IP Address	1.1.1.1/32, 2.2.2.2/32
Destination Type	Zone
Destination Zone	untrust
Destination IP Address	3.3.3.3/32
Action	Permit

Name	policy4
Source Zone	untrust
Source IP Address	3.3.3.3/32
Destination Type	Zone
Destination Zone	local
Destination IP Address	1.1.1.1/32, 2.2.2.2/32
Action	Permit

Name	policy5
Source Zone	local
Source IP Address	192.168.1.1/32
Destination Type	Zone
Destination Zone	untrust
Destination IP Address	192.168.2.1/32
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Name	policy6
Source Zone	untrust
Source IP Address	192.168.2.1/32
Destination Type	Zone
Destination Zone	local
Destination IP Address	192.168.1.1/32
Action	Permit

Step 3 Configure an IPsec intelligent uplink selection profile based on link quality detection on DeviceA.

NOTE

Currently, the IPsec intelligent uplink selection function cannot be configured on the web UI. Click in the upper right corner of the web UI to open the CLI console and configure an IPsec intelligent uplink selection profile through the CLI.

Assume that the next-hop IP address of the route from DeviceA to the Internet through Link 1 is 1.1.1.254, and the next-hop IP address of the route from DeviceA to the Internet through Link 2 is 2.2.2.254.

```
[DeviceA] ipsec smart-link profile profile1
[DeviceA-ipsec-smart-link-profile-profile1] link-switch-mode quality-based
[DeviceA-ipsec-smart-link-profile-profile1] Warning: This operation will change to quality mode and add an acl rule to ipsec group. Continue? [Y/N]:y
[DeviceA-ipsec-smart-link-profile-profile1] link 1 interface ge 0/0/2 local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link 2 interface ge 0/0/3 local 2.2.2.2 nexthop 2.2.2.254 remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection address source 192.168.1.1 destination 192.168.2.1
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection interval 1
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection number 10
[DeviceA-ipsec-smart-link-profile-profile1] auto-switch cycles 3
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-threshold loss 30
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-threshold delay 500
[DeviceA-ipsec-smart-link-profile-profile1] auto-switch preempt enable
```

NOTE

After you run the **link-quality-detection address** command to configure the source and destination addresses of ICMP probe packets, the device automatically adds the following rule to the ACL of the IPsec policy to allow ICMP probe packets to be sent:

rule permit icmp source 192.168.1.1 destination 192.168.2.1

Step 4 Configure an IPsec policy on DeviceA and reference the IPsec intelligent uplink selection profile in the IPsec policy.

NOTE

Currently, the IPsec intelligent uplink selection function cannot be configured on the web UI. Click in the upper right corner of the web UI to open the CLI console and configure an IPsec intelligent uplink selection policy through the CLI.

 Copyright © Huawei Technologies Co., Ltd.

1. Create advanced ACL 3000 to define the data flow to be protected.

```
[DeviceA] acl 3000
[DeviceA-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl-adv-3000] quit
```

2. Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

3. Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

4. Configure an IKE peer.

```
[DeviceA] ike peer a
[DeviceA-ike-peer-a] ike-proposal 10
[DeviceA-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-a] quit
```

5. Create the IPsec policy **map1**.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceA-ipsec-policy-isakmp-map1-10] smart-link profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] route inject dynamic
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

NOTE

The IPsec policy that references an IPsec intelligent uplink selection profile does not need to be applied to an interface. After DeviceA selects a link to establish an IPsec tunnel, it automatically applies the IPsec policy that references an IPsec intelligent uplink selection profile to the local interface for the link.

Step 5 Configure GE0/0/4, GE0/0/5, and loopback interfaces on DeviceB.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/4 and set the parameters as follows. Click **OK**.

Zone	untrust
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	3.3.3.3/24

3. Click corresponding to GE0/0/5 and set the parameters as follows. Click **OK**.

Zone	trust

 Copyright © Huawei Technologies Co., Ltd.

Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	10.1.2.1/24

4. On the **Network** > **Interface** page, click **Add** to create a local loopback interface. Set the parameters as follows. Click **OK**.

Type	Loopback Interface
Index	1
Virtual System	public
VPN Instance	public
IPv4	
IP Address	192.168.2.1/32

Step 6 Configure security policies on DeviceB to allow the branch and HQ to exchange packets through a specified network segment.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure security policies between the Trust and Untrust zones to allow unencapsulated and decapsulated packets to pass through DeviceB. Click **OK**.

Name	policy1
Source Zone	trust
Source IP Address/ Region	10.1.2.0/24
Destination Type	Zone
Destination Zone	untrust
Destination IP Address/Region	10.1.1.0/24
Protocol	any
Action	Permit

Name	policy2
Source Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Source IP Address/ Region	10.1.1.0/24
Destination Type	Zone
Destination Zone	trust
Destination IP Address/Region	10.1.2.0/24
Action	Permit

3. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation and continuous link quality detection. Click **OK**.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

Name	policy3
Source Zone	local
Source IP Address	3.3.3.3/32
Destination Type	Zone
Destination Zone	untrust
Destination IP Address	1.1.1.1/32, 2.2.2.2/32
Action	Permit

Name	policy4
Source Zone	untrust
Source IP Address	1.1.1.1/32, 2.2.2.2/32
Destination Type	Zone
Destination Zone	local
Destination IP Address	3.3.3.3/32
Action	Permit

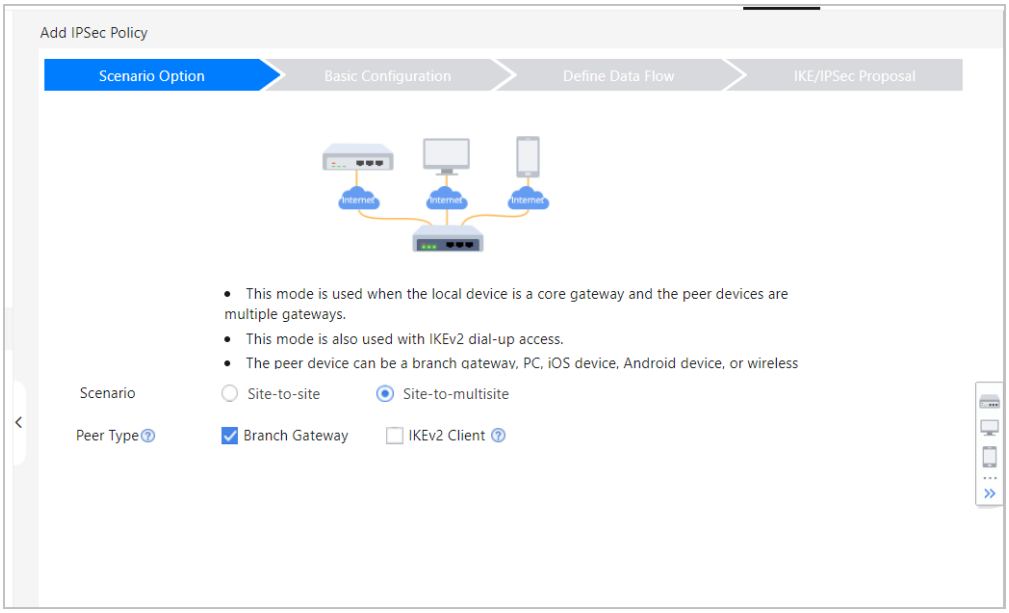
 Copyright © Huawei Technologies Co., Ltd.

Name	policy5
Source Zone	local
Source IP Address	192.168.2.1/32
Destination Type	Zone
Destination Zone	untrust
Destination IP Address	192.168.1.1/32
Action	Permit

Name	policy6
Source Zone	untrust
Source IP Address	192.168.1.1/32
Destination Type	Zone
Destination Zone	local
Destination IP Address	192.168.2.1/32
Action	Permit

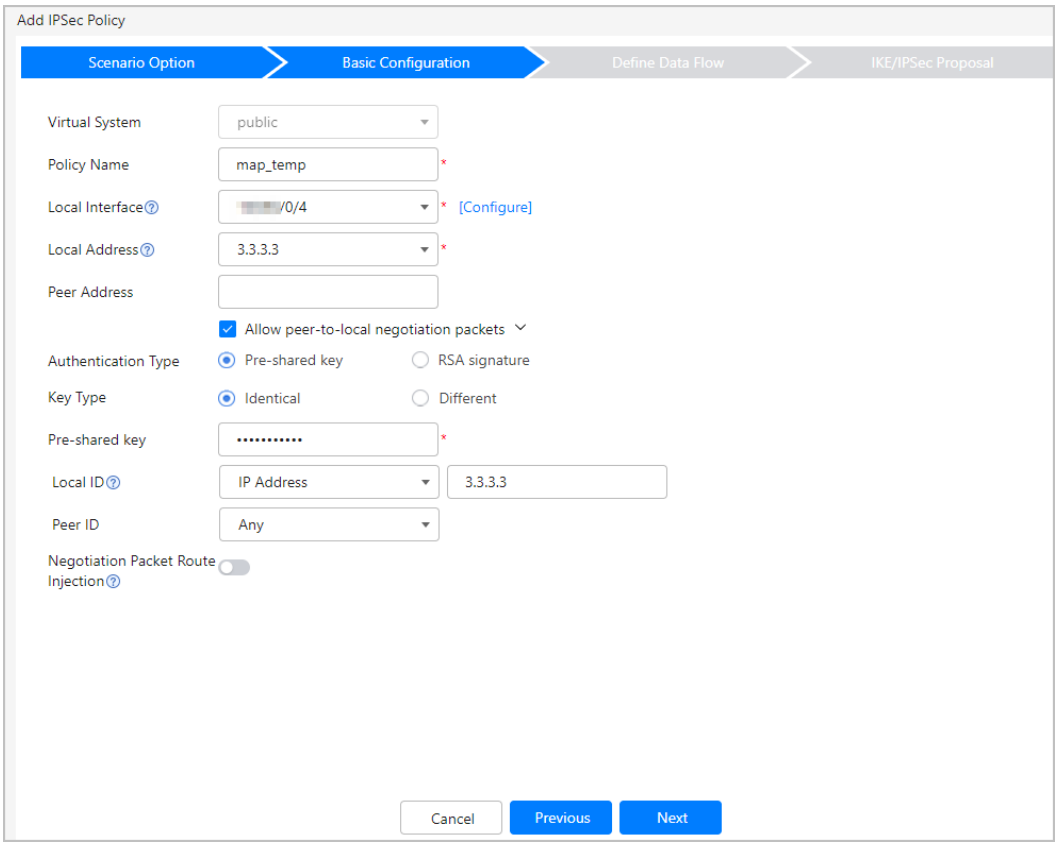
Step 7 Configure an IPsec policy on DeviceB.

1. Choose **Network** > **IPSec** > **IPSec**. Click **Add**.
2. Set **Scenario** to **Site-to-multisite** and **Peer Type** to **Branch Gateway**.



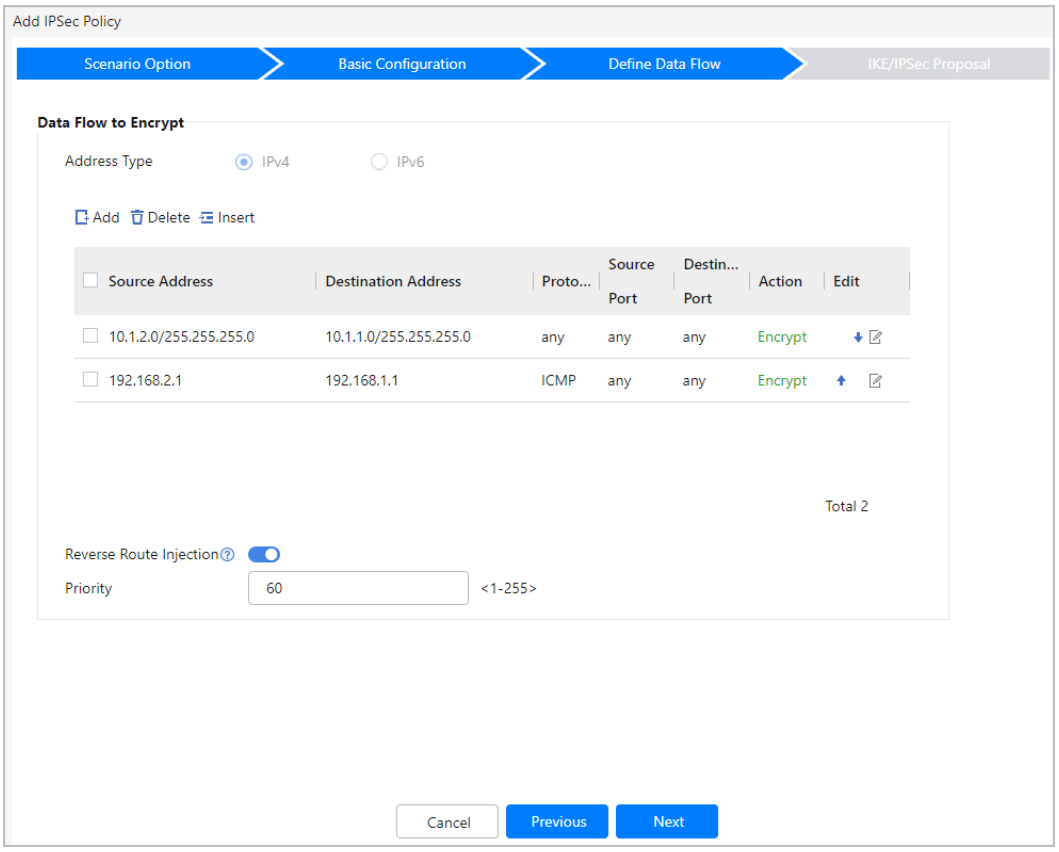
 Copyright © Huawei Technologies Co., Ltd.

3. Configure basic IPsec policy information. To allow multiple gateways to access the network, do not specify detailed information of the peer gateway. Set the pre-shared key to **YsHsjx_202206**. Click **Next**.



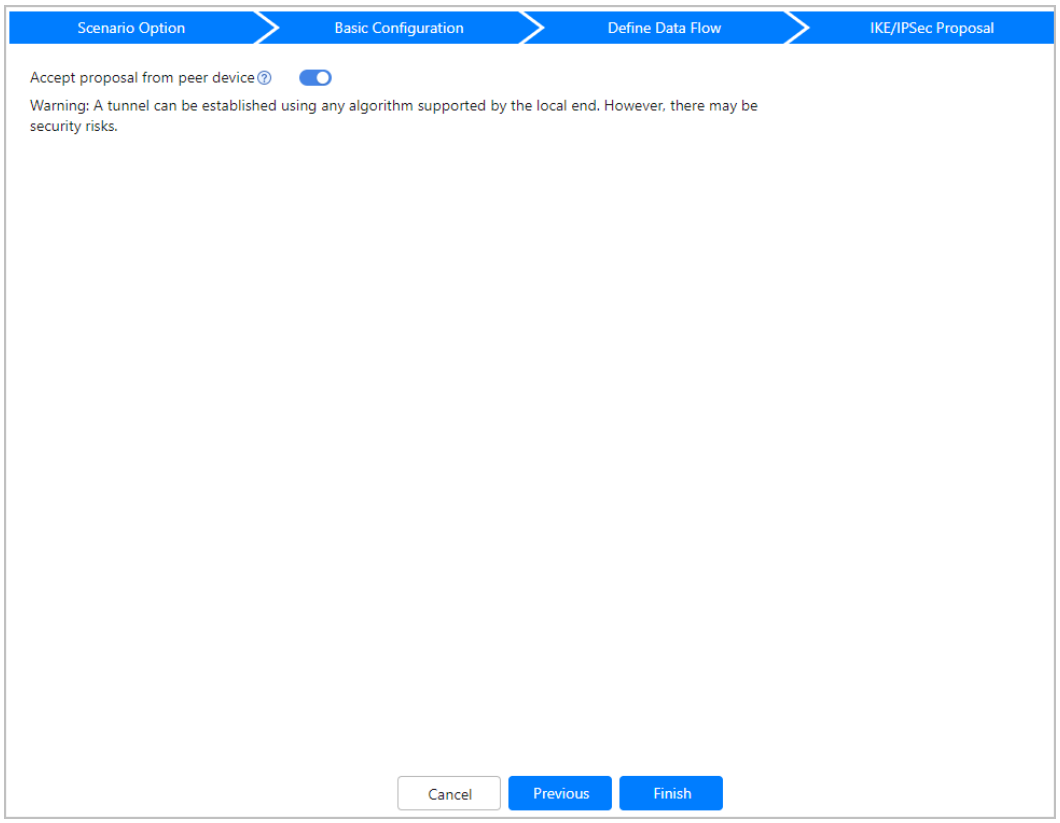
4. In **Data Flow to Encrypt**, click **Add** and add a data flow rule as follows. Enable **Reverse Route Injection** and set **Priority** to 60, indicating that the HQ automatically generates a route to the branch private network. Click **Next**.

 Copyright © Huawei Technologies Co., Ltd.



5. Configure a security proposal. Configure a security proposal according to the following figure. After the configuration is complete, click **Finish**.

 Copyright © Huawei Technologies Co., Ltd.



----End

Verifying the Configuration

1. After the configuration is complete, run the **display ipsec smart-link profile** command on DeviceA. The command output shows that DeviceA at the branch first establishes an IPsec tunnel based on Link 1 (with the local address of 1.1.1.1 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ============================================
 Name                    :profile1
 Detection number        :10
 Detection interval      :1
 Detection source IP     :192.168.1.1
 Detection destination IP  :192.168.2.1
 Cycles                  :3
 Switched times          :0
 Switch mode             :quality-based
 State                   :enable
 IPsec policy alias      :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         0       0          active
 2  2.2.2.2         3.3.3.3         0       0          inactive
 ============================================
```

2. On DeviceA, shut down interfaces on Link 1 and then run the **display ipsec smart-link profile** command. The command output shows that DeviceA automatically establishes an IPsec tunnel based on Link 2 (with the local address of 2.2.2.2 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ============================================
 Name                    :profile1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 Detection number          :10
 Detection interval        :1
 Detection source IP       :192.168.1.1
 Detection destination IP  :192.168.2.1
 Cycles                    :3
 Switched times            :1
 Switch mode               :quality-based
 State                     :enable
 IPsec policy alias        :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         50      0          inactive
 2  2.2.2.2         3.3.3.3         0       0          active
 ==========================================
```

3. After the interfaces of DeviceA recover, run the **display ipsec smart-link profile** command on DeviceA. The command output shows that DeviceA automatically switches traffic back from the IPsec tunnel established based on Link 2 to that established based on Link 1 (with the local address of 1.1.1.1 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ==========================================
 Name                      :profile1
 Detection number          :10
 Detection interval        :1
 Detection source IP       :192.168.1.1
 Detection destination IP  :192.168.2.1
 Cycles                    :3
 Switched times            :2
 Switch mode               :quality-based
 State                     :enable
 IPsec policy alias        :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         100     -1         inactive
 2  2.2.2.2         3.3.3.3         0       0          active
 ==========================================
```

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 4294967294 permit icmp source 192.168.1.1 0 destination 192.168.2.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 10
#
ipsec smart-link profile profile1
 auto-switch preempt enable delay 180
 link 1 interface GE0/0/2 local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
```

 Copyright © Huawei Technologies Co., Ltd.

```
 link 2 interface GE0/0/3 local 2.2.2.2 nexthop 2.2.2.254 remote 3.3.3.3
 link-quality-detection address source 192.168.1.1 destination 192.168.2.1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
 smart-link profile profile1
 route inject dynamic
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 2.2.2.2 255.255.255.0
#
interface loopback 1
 ip address 192.168.1.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
 add interface GE0/0/3
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy5
  source-zone local
  destination-zone untrust
  source-address 192.168.1.1 mask 255.255.255.255
  destination-address 192.168.2.1 mask 255.255.255.255
  action permit
 rule name policy6
  source-zone untrust
  destination-zone local
  source-address 192.168.2.1 mask 255.255.255.255
  destination-address 192.168.1.1 mask 255.255.255.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
#
```

- DeviceB

```
#
sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 6 permit icmp source 192.168.2.1 0 destination 192.168.1.1 0
#
ipsec proposal prop73114145884
  encapsulation-mode auto
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-256-gcm-128
#
ike proposal 1
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike73114145884
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 1
 remote-id-type none
 dpd type periodic
 ike negotiate compatible
#
ipsec policy-template tpl73114145884 1
 security acl 3000
 ike-peer ike73114145884
 proposal prop73114145884
 tunnel local 3.3.3.3
 alias "map_temp 1"
 sa duration traffic-based 83886080
 sa duration time-based 3600
 route inject dynamic preference 60
#
ipsec policy ipsec7311414582 10000 isakmp template tpl73114145884
#
interface GE0/0/4

 ipsec policy map1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/5

 ip address 10.1.2.1 255.255.255.0
#
interface loopback 1
 ip address 192.168.1.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/5
#
firewall zone untrust
 set priority 5
 add interface GE0/0/4
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
rule name policy2
 source-zone untrust
 destination-zone trust
 source-address 10.1.1.0 mask 255.255.255.0
 destination-address 10.1.2.0 mask 255.255.255.0
 action permit
rule name policy3
 source-zone local
 destination-zone untrust
 source-address 3.3.3.3 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 destination-address 2.2.2.2 mask 255.255.255.255
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 1.1.1.1 mask 255.255.255.255
 source-address 2.2.2.2 mask 255.255.255.255
 destination-address 3.3.3.3 mask 255.255.255.255
 action permit
rule name policy5
 source-zone local
 destination-zone untrust
 source-address 192.168.2.1 mask 255.255.255.255
 destination-address 192.168.1.1 mask 255.255.255.255
 action permit
rule name policy6
 source-zone untrust
 destination-zone local
 source-address 192.168.1.1 mask 255.255.255.255
 destination-address 192.168.2.1 mask 255.255.255.255
 action permit
#
```

8.6.2 CLI: Example for Configuring IPsec Intelligent Uplink Selection Based on Link Quality Detection (with Automatic Link Switchback Disabled)

Networking Requirements

As shown in **Figure 8-29**, the HQ and branch are connected to the Internet through DeviceA and DeviceB. DeviceA is connected to the Internet through two links, and DeviceB is connected to the Internet through one link.

The requirements are as follows:

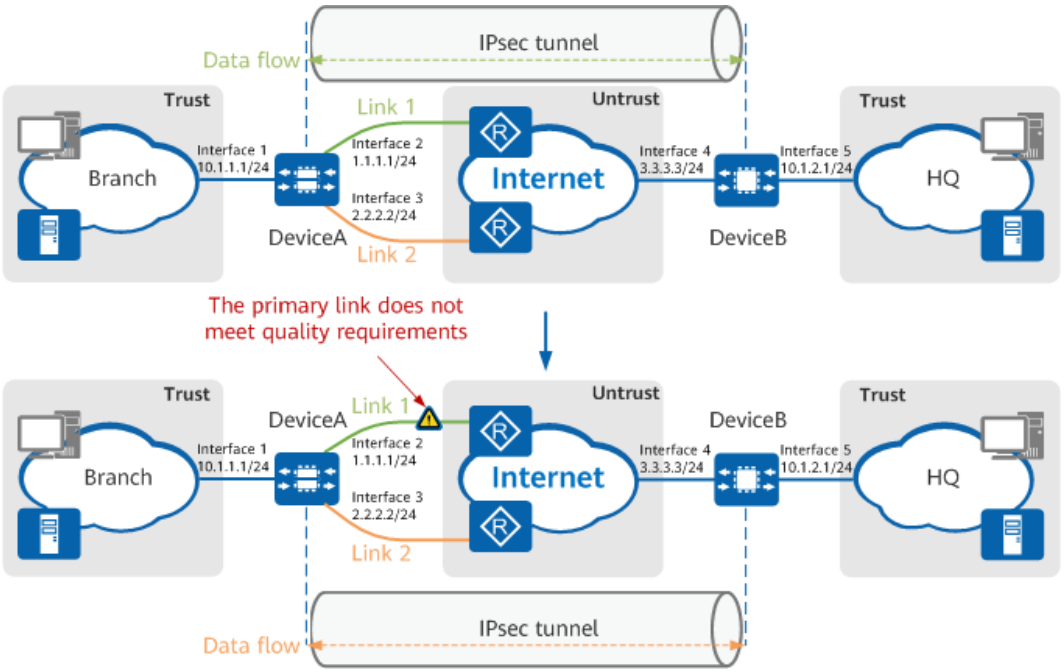
- An IPsec tunnel needs to be established between DeviceA and DeviceB for communication between the HQ and branch.
- DeviceA first establishes an IPsec tunnel with the HQ based on Link 1. If the IPsec tunnel has a high packet loss rate or delay, DeviceA automatically establishes another IPsec tunnel based on Link 2.

Figure 8-29 Network diagram of IPsec intelligent uplink selection

NOTE

In this example, interface 1, interface 2, interface 3, interface 4, and interface 5 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/5, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item		DeviceA	DeviceB
Intranet interface		Interface: GE 0/0/1 IP address: 10.1.1.1/24 Security zone: Trust	Interface: GE 0/0/5 IP address: 10.1.2.1/24 Security zone: Trust
External network interface		• Interface: GE 0/0/2 IP address: 1.1.1.1/24 Security zone: Untrust • Interface: GE 0/0/3 IP address: 2.2.2.2/24 Security zone: Untrust	Interface: GE 0/0/4 IP address: 3.3.3.3/24 Security zone: Untrust
Method of configuring an IPsec policy		ISAKMP + IPsec intelligent uplink selection (based on link quality detection)	Using an IPsec policy template
IPsec proposal	ESP authentication algorithm	SHA2-256	SHA2-256
	ESP encryption algorithm	AES-256-GCM-128	AES-256-GCM-128
IKE proposal	Verification method	Pre-shared key	Pre-shared key

 Copyright © Huawei Technologies Co., Ltd.

Item		DeviceA	DeviceB
	PRF algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	DH group	Group 14	Group 14
	Authentication algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	Encryption algorithm	AES-GCM-256	AES-GCM-256
IKE peer	Pre-shared key	YsHsjx_202206	YsHsjx_202206
	Identity type	IP	IP
	Peer IP address	3.3.3.3	Unspecified

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

- On DeviceA:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure an IPsec intelligent uplink selection profile based on link quality detection.
  d. Configure an ISAKMP IPsec policy and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.
- On DeviceB:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure a template IPsec policy.

Procedure

Step 1 Configure IP addresses for interfaces.

Configure IP addresses for GE 0/0/1, GE 0/0/2, and GE 0/0/3 on DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 2.2.2.2 24
[DeviceA-GE0/0/3] quit
```

Configure IP addresses for GE 0/0/4 and GE 0/0/5 on DeviceB.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/4
[DeviceB-GE0/0/4] undo portswitch
[DeviceB-GE0/0/4] ip address 3.3.3.3 24
[DeviceB-GE0/0/4] quit
[DeviceB] interface ge 0/0/5
[DeviceB-GE0/0/5] undo portswitch
[DeviceB-GE0/0/5] ip address 10.1.2.1 24
[DeviceB-GE0/0/5] quit
```

Step 2 Add interfaces to corresponding security zones.

Add interfaces, GE 0/0/1, GE 0/0/2, and GE 0/0/3 on DeviceA to their corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

Add interfaces, GE 0/0/4 and GE 0/0/5 on DeviceB to their corresponding security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-untrust] add interface ge 0/0/5
[DeviceB-zone-untrust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-trust] add interface ge 0/0/4
[DeviceB-zone-trust] quit
```

Step 3 Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.

Configure security policies on DeviceA.

1. Configure security policies between the Trust and Untrust zones on DeviceA to allow unencapsulated and decapsulated packets to pass through DeviceA.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

2. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] destination-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Configure security policies on DeviceB.

1. Configure security policies between the Trust and Untrust zones to allow unencapsulated and decapsulated packets to pass through DeviceB.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

2. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceB-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] destination-address 3.3.3.3 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 4 Configure an IPsec intelligent uplink selection profile based on link quality detection on DeviceA.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet through Link 1 is 1.1.1.254, and the next-hop IP address of the route from DeviceA to the Internet through Link 2 is 2.2.2.254.

```
[DeviceA] ipsec smart-link profile profile1
[DeviceA-ipsec-smart-link-profile-profile1] link-switch-mode quality-based
[DeviceA-ipsec-smart-link-profile-profile1] link 1 interface ge 0/0/2 local 1.1.1.1 nexthop 1.1.1.254
remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link 2 interface ge 0/0/3 local 2.2.2.2 nexthop 2.2.2.254
remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection interval 1
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection number 10
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection address source 10.1.1.1 destination
10.1.2.1
[DeviceA-ipsec-smart-link-profile-profile1] auto-switch cycles 3
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-threshold loss 30
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-threshold delay 500
```

Step 5 Configure an ISAKMP IPsec policy on DeviceA and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.

Create advanced ACL 3000 to define the data flow to be protected.

```
[DeviceA] acl 3000
[DeviceA-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl-adv-3000] quit
```

Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceA] ike peer a
[DeviceA-ike-peer-a] ike-proposal 10
[DeviceA-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-a] quit
```

Create the IPsec policy **map1**.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceA-ipsec-policy-isakmp-map1-10] smart-link profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] route inject dynamic
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

NOTE

The IPsec policy that references an IPsec intelligent uplink selection profile does not need to be applied to an interface. After DeviceA selects a link to establish an IPsec tunnel, it automatically applies the IPsec policy that references an IPsec intelligent uplink selection profile to the local interface for the link.

Step 6 Configure a template IPsec policy on DeviceB.

Create advanced ACL 3000, define the data flow to be protected, and allow the device to send ICMP packets.

```
[DeviceB] acl 3000
[DeviceB-acl-adv-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-adv-3000] rule 7 permit icmp source 3.3.3.3 0 destination 1.1.1.1 0
[DeviceB-acl-adv-3000] rule 8 permit icmp source 3.3.3.3 0 destination 2.2.2.2 0
[DeviceB-acl-adv-3000] quit
```

Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer b
[DeviceB-ike-peer-b] ike-proposal 10
[DeviceB-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-b] quit
```

Configure an IPsec policy template.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] ipsec policy-template map_temp 1
[DeviceB-ipsec-policy-template-map_temp-1] security acl 3000
[DeviceB-ipsec-policy-template-map_temp-1] proposal tran1
[DeviceB-ipsec-policy-template-map_temp-1] ike-peer b
[DeviceB-ipsec-policy-template-map_temp-1] route inject dynamic preference 65
[DeviceB-ipsec-policy-template-map_temp-1] quit
```

Reference the IPsec policy template **map_temp** in the IPsec policy **map1**.

```
[DeviceB] ipsec policy map1 10 isakmp template map_temp
```

Apply an IPsec policy to GE 0/0/4.

```
[DeviceB] interface ge 0/0/4
[DeviceB-GE0/0/4] ipsec policy map1
[DeviceB-GE0/0/4] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **display ipsec smart-link profile** command on DeviceA. The command output shows that DeviceA at the branch first establishes an IPsec tunnel based on Link 1 (with the local address of 1.1.1.1 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ========================================
 Name                     :profile1
 Detection number         :10
 Detection interval       :1
 Detection source IP      :1.1.1.1
 Detection destination IP  :3.3.3.3
 Cycles                   :3
 Switched times           :0
 Switch mode              :quality-based
 State                    :enable
 IPsec policy alias       :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         0       0          active
 2  2.2.2.2         3.3.3.3         0       0          inactive
 ========================================
```

Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB to check SA establishment. The following example uses the command output on DeviceA, which indicates that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa
IKE SA information :
   Conn-ID      Peer        VPN   Flag(s)   Phase   RemoteType  RemoteID
 -------------------------------------------------------------------------------
   16782417     3.3.3.3:500       RD|ST|A   v2:2    IP          3.3.3.3
   16782416     3.3.3.3:500       RD|ST|A   v2:2    IP          3.3.3.3
   16782415     3.3.3.3:500       RD|ST|A   v2:1    IP          3.3.3.3

 Number of IKE SA : 3
 -------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceB> display ipsec sa brief
Current ipsec sa num:4
Number of SAs:4
   Src address   Dst address     SPI      VPN  Protocol     Algorithm
```

 Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
  1.1.1.1         3.3.3.3     3923280450          ESP       E:AES-256-GCM-128 A:SHA2-256-128
  3.3.3.3         1.1.1.1     787858613           ESP       E:AES-256-GCM-128 A:SHA2-256-128
  1.1.1.1         3.3.3.3     4846992             ESP       E:AES-256-GCM-128 A:SHA2-256-128
  3.3.3.3         1.1.1.1     269647435           ESP       E:AES-256-GCM-128 A:SHA2-256-128
```

2. On DeviceA, shut down interfaces on Link 1 and then run the **display ipsec smart-link profile** command. The command output shows that DeviceA automatically establishes an IPsec tunnel based on Link 2 (with the local address of 2.2.2.2 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ==========================================
 Name                    :profile1
 Detection number        :10
 Detection interval      :1
 Detection source IP     :2.2.2.2
 Detection destination IP  :3.3.3.3
 Cycles                  :3
 Switched times          :0
 Switch mode             :quality-based
 State                   :enable
 IPsec policy alias      :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         100     -1         inactive
 2  2.2.2.2         3.3.3.3         0       0          active
 ==========================================
```

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 10
#
ipsec smart-link profile profile1
 link-quality-detection interval 1
 link-quality-detection number 10
 link-quality-detection address source 10.1.1.1 destination 10.1.2.1
 auto-switch cycles 3
 link-quality-threshold loss 30
 link-quality-threshold delay 500
 link 1 interface GE0/0/2 local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
 link 2 interface GE0/0/3 local 2.2.2.2 nexthop 2.2.2.254 remote 3.3.3.3
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 smart-link profile profile1
 route inject dynamic
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 2.2.2.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
 add interface GE0/0/3
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
```

- DeviceB

```
#
sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 7 permit icmp source 3.3.3.3 0 destination 1.1.1.1 0
 rule 8 permit icmp source 3.3.3.3 0 destination 2.2.2.2 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
ike peer b
 pre-shared-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
#
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/4

 ipsec policy map1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/5

 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/5
#
firewall zone untrust
 set priority 5
 add interface GE0/0/4
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

8.6.3 CLI: Example for Configuring IPsec Intelligent Uplink Selection Based on Link Quality Detection (with Automatic Link Switchback Enabled)

Networking Requirements

As shown in **Figure 8-30**, the HQ and branch are connected to the Internet through DeviceA and DeviceB. DeviceA is connected to the Internet through two links, and DeviceB is connected to the Internet through one link.

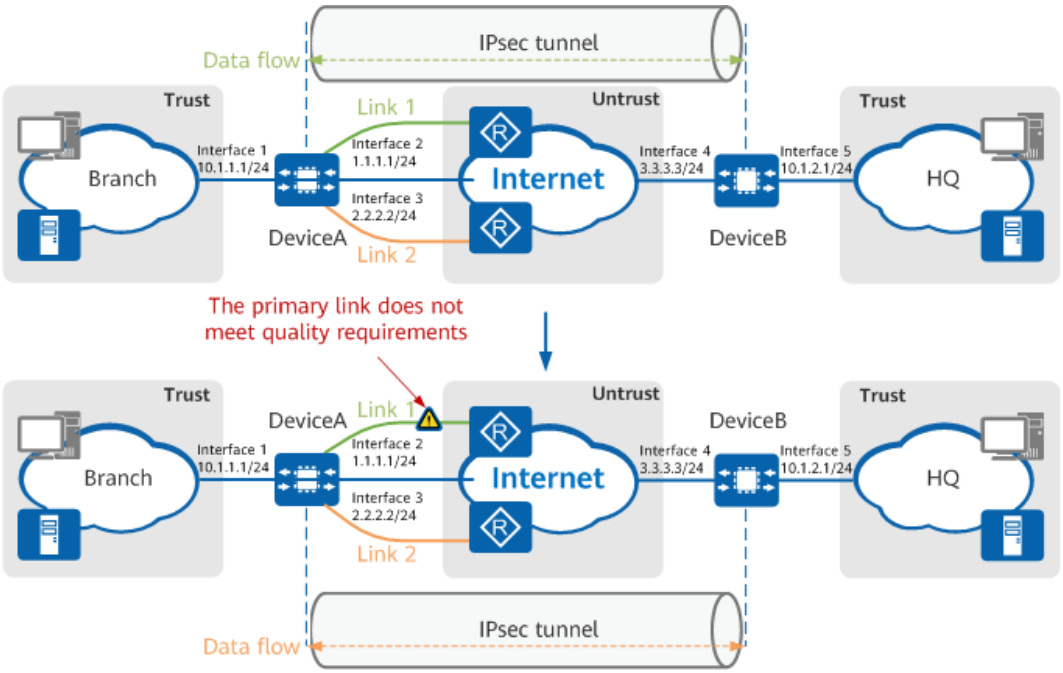
The requirements are as follows:

- An IPsec tunnel needs to be established between DeviceA and DeviceB for communication between the HQ and branch.
- DeviceA first establishes an IPsec tunnel with the HQ based on Link 1. If the IPsec tunnel has a high packet loss rate or delay, DeviceA automatically establishes another IPsec tunnel based on Link 2.
- When automatic link switchback is enabled on DeviceA, after Link 1 recovers, DeviceA automatically switches traffic back from the IPsec tunnel established based on Link 2 to that established based on Link 1.

Figure 8-30 Network diagram of IPsec intelligent uplink selection

NOTE

In this example, interface 1, interface 2, interface 3, interface 4, and interface 5 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/5, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item		DeviceA	DeviceB
Intranet interface		Interface: GE 0/0/1 IP address: 10.1.1.1/24 Security zone: Trust	Interface: GE 0/0/5 IP address: 10.1.2.1/24 Security zone: Trust
External network interface		• Interface: GE 0/0/2 IP address: 1.1.1.1/24 Security zone: Untrust • Interface: GE 0/0/3 IP address: 2.2.2.2/24 Security zone: Untrust	Interface: GE 0/0/4 IP address: 3.3.3.3/24 Security zone: Untrust
Loopback interface		Interface number: 1 IP address: 192.168.1.1	Interface number: 1 IP address: 192.168.2.1
Method of configuring an IPsec policy		ISAKMP + IPsec intelligent uplink selection (based on link quality detection)	Using an IPsec policy template
IPsec proposal	ESP authentication algorithm	SHA2-256	SHA2-256
	ESP encryption algorithm	AES-256-GCM-128	AES-256-GCM-128
IKE proposal	Verification method	Pre-shared key	Pre-shared key
	PRF algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	DH group	Group 14	Group 14
	Authentication algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	Encryption algorithm	AES-GCM-256	AES-GCM-256
IKE peer	Pre-shared key	YsHsjx_202206	YsHsjx_202206
	Identity type	IP	IP
	Peer IP address	3.3.3.3	Unspecified

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

- On DeviceA:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure an IPsec intelligent uplink selection profile based on link quality detection and enable the automatic link switchback function.
  d. Configure an ISAKMP IPsec policy and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.
- On DeviceB:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure a template IPsec policy.

Procedure

Step 1 Configure IP addresses for interfaces.

Configure IP addresses for GE 0/0/1, GE 0/0/2, GE 0/0/3, and the loopback interface on DeviceA.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 2.2.2.2 24
[DeviceA-GE0/0/3] quit
[DeviceA] interface loopback 1
[DeviceA-LoopBack1] ip address 192.168.1.1 32
[DeviceA-LoopBack1] quit
```

Configure IP addresses for GE 0/0/4, GE 0/0/5, and the loopback interface on DeviceB.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/4
[DeviceB-GE0/0/4] undo portswitch
[DeviceB-GE0/0/4] ip address 3.3.3.3 24
[DeviceB-GE0/0/4] quit
[DeviceB] interface ge 0/0/5
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-GE0/0/5] undo portswitch
[DeviceB-GE0/0/5] ip address 10.1.2.1 24
[DeviceB-GE0/0/5] quit
[DeviceB] interface loopback 1
[DeviceB-LoopBack1] ip address 192.168.2.1 32
[DeviceB-LoopBack1] quit
```

Step 2 Add interfaces to corresponding security zones.

Add interfaces, GE 0/0/1, GE 0/0/2, and GE 0/0/3 on DeviceA to their corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

Add interfaces, GE 0/0/4 and GE 0/0/5 on DeviceB to their corresponding security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-untrust] add interface ge 0/0/5
[DeviceB-zone-untrust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-trust] add interface ge 0/0/4
[DeviceB-zone-trust] quit
```

Step 3 Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.

Configure security policies on DeviceA.

1. Configure security policies between the Trust and Untrust zones on DeviceA to allow unencapsulated and decapsulated packets to pass through DeviceA.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

2. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation and continuous link quality detection.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] destination-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] rule name policy5
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 192.168.1.1 32
[DeviceA-policy-security-rule-policy3] destination-address 192.168.2.1 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy6
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 192.168.2.1 32
[DeviceA-policy-security-rule-policy4] destination-address 192.168.1.1 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Configure security policies on DeviceB.

1. Configure security policies between the Trust and Untrust zones to allow unencapsulated and decapsulated packets to pass through DeviceB.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

2. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation and continuous link quality detection.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceB-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] destination-address 3.3.3.3 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
[DeviceB-policy-security] rule name policy5
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 192.168.2.1 32
[DeviceB-policy-security-rule-policy3] destination-address 192.168.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy6
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] source-address 192.168.1.1 32
[DeviceB-policy-security-rule-policy4] destination-address 192.168.2.1 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 4 Configure an IPsec intelligent uplink selection profile based on link quality detection on DeviceA.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet through Link 1 is 1.1.1.254, and the next-hop IP address of the route from DeviceA to the Internet through Link 2 is 2.2.2.254.

```
[DeviceA] ipsec smart-link profile profile1
[DeviceA-ipsec-smart-link-profile-profile1] link-switch-mode quality-based
[DeviceA-ipsec-smart-link-profile-profile1] link 1 interface ge 0/0/2 local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link 2 interface ge 0/0/3 local 2.2.2.2 nexthop 2.2.2.254 remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection address source 192.168.1.1 destination 192.168.2.1
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection interval 1
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-detection number 10
[DeviceA-ipsec-smart-link-profile-profile1] auto-switch cycles 3
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-threshold loss 30
[DeviceA-ipsec-smart-link-profile-profile1] link-quality-threshold delay 500
[DeviceA-ipsec-smart-link-profile-profile1] auto-switch preempt enable
```

Step 5 Configure an ISAKMP IPsec policy on DeviceA and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.

Create advanced ACL 3000 to define the data flow to be protected.

```
[DeviceA] acl 3000
[DeviceA-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl-adv-3000] quit
```

Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceA] ike peer a
[DeviceA-ike-peer-a] ike-proposal 10
[DeviceA-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-a] quit
```

Create the IPsec policy **map1**.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceA-ipsec-policy-isakmp-map1-10] smart-link profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] route inject dynamic
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

NOTE

The IPsec policy that references an IPsec intelligent uplink selection profile does not need to be applied to an interface. After DeviceA selects a link to establish an IPsec tunnel, it automatically applies the IPsec policy that references an IPsec intelligent uplink selection profile to the local interface for the link.

Step 6 Configure a template IPsec policy on DeviceB.

Create advanced ACL 3000, define the data flow to be protected, and allow the device to send ICMP packets.

```
[DeviceB] acl 3000
[DeviceB-acl-adv-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-adv-3000] rule 6 permit icmp source 192.168.2.1 0 destination 192.168.1.1 0
[DeviceB-acl-adv-3000] quit
```

Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer b
[DeviceB-ike-peer-b] ike-proposal 10
[DeviceB-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-b] quit
```

Configure an IPsec policy template.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] ipsec policy-template map_temp 1
[DeviceB-ipsec-policy-template-map_temp-1] security acl 3000
[DeviceB-ipsec-policy-template-map_temp-1] proposal tran1
[DeviceB-ipsec-policy-template-map_temp-1] ike-peer b
[DeviceB-ipsec-policy-template-map_temp-1] route inject dynamic preference 65
[DeviceB-ipsec-policy-template-map_temp-1] quit
```

Reference the IPsec policy template **map_temp** in the IPsec policy **map1**.

```
[DeviceB] ipsec policy map1 10 isakmp template map_temp
```

Apply an IPsec policy to GE 0/0/4.

```
[DeviceB] interface ge 0/0/4
[DeviceB-GE0/0/4] ipsec policy map1
[DeviceB-GE0/0/4] quit
```

----End

Verifying the Configuration

1. After the configuration is complete, run the **display ipsec smart-link profile** command on DeviceA. The command output shows that DeviceA at the branch first establishes an IPsec tunnel based on Link 1 (with the local address of 1.1.1.1 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ========================================
 Name                     :profile1
 Detection number         :10
 Detection interval       :1
 Detection source IP      :1.1.1.1
 Detection destination IP  :3.3.3.3
 Cycles                   :3
 Switched times           :0
 Switch mode              :quality-based
 State                    :enable
 IPsec policy alias       :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         0       0          active
 2  2.2.2.2         3.3.3.3         0       0          inactive
 ========================================
```

Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB to check SA establishment. The following example uses the command output on DeviceA, which indicates that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa
IKE SA information :
   Conn-ID      Peer        VPN   Flag(s)   Phase   RemoteType  RemoteID
 -------------------------------------------------------------------------------
   16782417     3.3.3.3:500       RD|ST|A   v2:2    IP          3.3.3.3
   16782416     3.3.3.3:500       RD|ST|A   v2:2    IP          3.3.3.3
   16782415     3.3.3.3:500       RD|ST|A   v2:1    IP          3.3.3.3

 Number of IKE SA : 3
 -------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceB> display ipsec sa brief
Current ipsec sa num:4
Number of SAs:4
   Src address   Dst address     SPI      VPN  Protocol     Algorithm
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
  1.1.1.1         3.3.3.3     3923280450          ESP       E:AES-256-GCM-128 A:SHA2-256-128
  3.3.3.3         1.1.1.1     787858613           ESP       E:AES-256-GCM-128 A:SHA2-256-128
  1.1.1.1         3.3.3.3     4846992             ESP       E:AES-256-GCM-128 A:SHA2-256-128
  3.3.3.3         1.1.1.1     269647435           ESP       E:AES-256-GCM-128 A:SHA2-256-128
```

2. On DeviceA, shut down interfaces on Link 1 and then run the **display ipsec smart-link profile** command. The command output shows that DeviceA automatically establishes an IPsec tunnel based on Link 2 (with the local address of 2.2.2.2 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ========================================
 Name                    :profile1
 Detection number        :10
 Detection interval      :1
 Detection source IP     :2.2.2.2
 Detection destination IP  :3.3.3.3
 Cycles                  :3
 Switched times          :0
 Switch mode             :quality-based
 State                   :enable
 IPsec policy alias      :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         50      0          inactive
 2  2.2.2.2         3.3.3.3         0       0          active
 ========================================
```

3. After the interfaces of DeviceA recover, run the **display ipsec smart-link profile** command on DeviceA. The command output shows that DeviceA automatically switches traffic back from the IPsec tunnel established based on Link 2 to that established based on Link 1 (with the local address of 1.1.1.1 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ========================================
 Name                    :profile1
 Detection number        :10
 Detection interval      :1
 Detection source IP     :1.1.1.1
 Detection destination IP  :3.3.3.3
 Cycles                  :3
 Switched times          :0
 Switch mode             :quality-based
 State                   :enable
 IPsec policy alias      :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         100     -1         inactive
 2  2.2.2.2         3.3.3.3         0       0          active
 ========================================
```

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 4294967294 permit icmp source 192.168.1.1 0 destination 192.168.2.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 10
#
ipsec smart-link profile pro1
 link-quality-detection interval 1
 link-quality-detection number 10
 link-quality-detection address source 192.168.1.1 destination 192.168.2.1
 auto-switch cycles 3
 link-quality-threshold loss 30
 link-quality-threshold delay 500
 link 1 interface GE0/0/2 local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
 link 2 interface GE0/0/3 local 2.2.2.2 nexthop 2.2.2.254 remote 3.3.3.3
 auto-switch preempt enable
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
 smart-link profile profile1
 route inject dynamic
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 2.2.2.2 255.255.255.0
#
interface loopback 1
 ip address 192.168.1.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
 add interface GE0/0/3
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
rule name policy4
 source-zone untrust
 destination-zone local
 source-address 3.3.3.3 mask 255.255.255.255
 destination-address 1.1.1.1 mask 255.255.255.255
 destination-address 2.2.2.2 mask 255.255.255.255
 action permit
rule name policy5
 source-zone local
 destination-zone untrust
 source-address 192.168.1.1 mask 255.255.255.255
 destination-address 192.168.2.1 mask 255.255.255.255
 action permit
rule name policy6
 source-zone untrust
 destination-zone local
 source-address 192.168.2.1 mask 255.255.255.255
 destination-address 192.168.1.1 mask 255.255.255.255
 action permit
#
```

- DeviceB

```
#
sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 6 permit icmp source 192.168.2.1 0 destination 192.168.1.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%# ike-proposal 10
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
#
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/4

 ipsec policy map1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/5

 ip address 10.1.2.1 255.255.255.0
#
interface loopback 1
 ip address 192.168.1.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/5
#
firewall zone untrust
 set priority 5
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/4
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
 rule name policy5
  source-zone local
  destination-zone untrust
  source-address 192.168.2.1 mask 255.255.255.255
  destination-address 192.168.1.1 mask 255.255.255.255
  action permit
 rule name policy6
  source-zone untrust
  destination-zone local
  source-address 192.168.1.1 mask 255.255.255.255
  destination-address 192.168.2.1 mask 255.255.255.255
  action permit
#
```

8.6.4 CLI: Example for Configuring IPsec Intelligent Uplink Selection Based on Route Status Changes

Networking Requirements

As shown in **Figure 8-31**, the HQ and branch are connected to the Internet through DeviceA and DeviceB. DeviceA is connected to the Internet through two links, and DeviceB is connected to the Internet through one link.

The requirements are as follows:

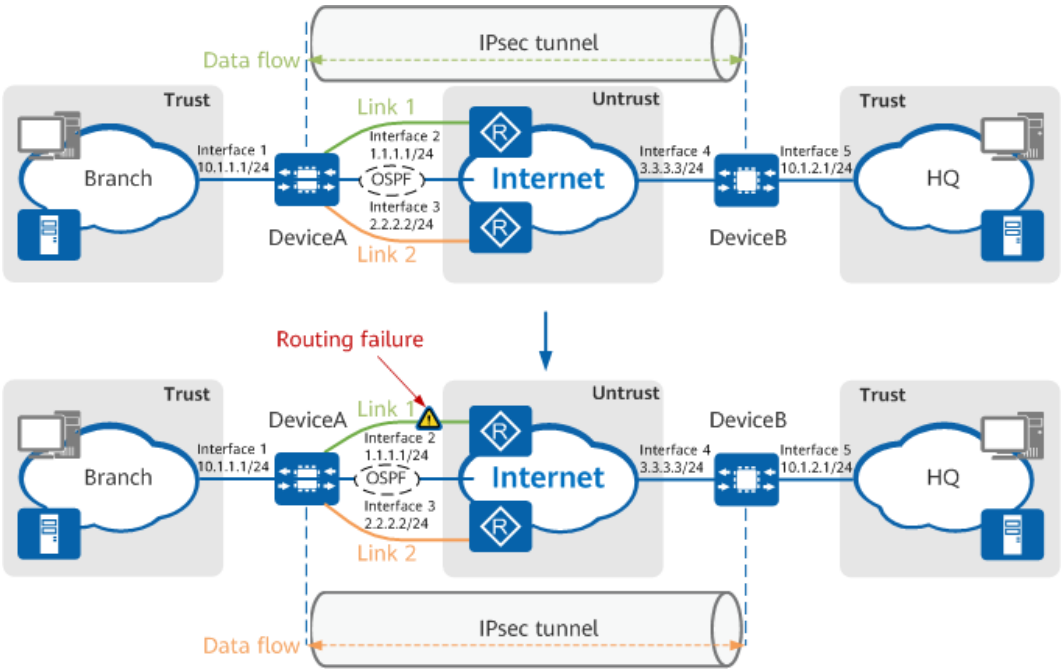
- An IPsec tunnel needs to be established between DeviceA and DeviceB for communication between the HQ and branch.
- DeviceA first establishes an IPsec tunnel with the HQ based on Link 1. If the route for the IPsec tunnel established based on Link 1 is unavailable, DeviceA automatically establishes another IPsec tunnel based on Link 2.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-31 Network diagram of IPsec intelligent uplink selection

NOTE

In this example, interface 1, interface 2, interface 3, interface 4, and interface 5 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, GE 0/0/4, and GE 0/0/5, respectively.



Item		DeviceA	DeviceB
Intranet interface		Interface: GE 0/0/1 IP address: 10.1.1.1/24 Security zone: Trust	Interface: GE 0/0/5 IP address: 10.1.2.1/24 Security zone: Trust
External network interface		• Interface: GE 0/0/2 IP address: 1.1.1.1/24 Security zone: Untrust • Interface: GE 0/0/3 IP address: 2.2.2.2/24 Security zone: Untrust	Interface: GE 0/0/4 IP address: 3.3.3.3/24 Security zone: Untrust
Method of configuring an IPsec policy		ISAKMP + IPsec intelligent uplink selection (based on route status changes)	Using an IPsec policy template
IPsec proposal	ESP authentication algorithm	SHA2-256	SHA2-256

 Copyright © Huawei Technologies Co., Ltd.

Item		DeviceA	DeviceB
	ESP encryption algorithm	AES-256-GCM-128	AES-256-GCM-128
IKE proposal	Verification method	Pre-shared key	Pre-shared key
	PRF algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	DH group	Group 14	Group 14
	Authentication algorithm	HMAC-SHA2-256	HMAC-SHA2-256
	Encryption algorithm	AES-GCM-256	AES-GCM-256
IKE peer	Pre-shared key	YsHsjx_202206	YsHsjx_202206
	Identity type	IP	IP
	Peer IP address	3.3.3.3	Unspecified

Configuration Roadmap

NOTE

The tunnel negotiation parameter settings on DeviceA and DeviceB must be the same.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

- On DeviceA:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.
  c. Configure an IPsec intelligent uplink selection profile based on link status changes.
  d. Configure OSPF routes.
  e. Configure an ISAKMP IPsec policy and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.
- On DeviceB:
  a. Configure IP addresses for interfaces and add interfaces to security zones.
  b. Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.

 Copyright © Huawei Technologies Co., Ltd.

c. Configure a template IPsec policy.

Procedure

Step 1 Configure IP addresses for interfaces.

Configure IP addresses for GE 0/0/1, GE 0/0/2, and GE 0/0/3 on DeviceA.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 2.2.2.2 24
[DeviceA-GE0/0/3] quit
```

Configure IP addresses for GE 0/0/4 and GE 0/0/5 on DeviceB.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/4
[DeviceB-GE0/0/4] undo portswitch
[DeviceB-GE0/0/4] ip address 1.1.1.1 24
[DeviceB-GE0/0/4] quit
[DeviceB] interface ge 0/0/5
[DeviceB-GE0/0/5] undo portswitch
[DeviceB-GE0/0/5] ip address 1.1.1.1 24
[DeviceB-GE0/0/5] quit
```

Step 2 Add interfaces to corresponding security zones.

Add interfaces, GE 0/0/1, GE 0/0/2, and GE 0/0/3 on DeviceA to their corresponding security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

Add interfaces, GE 0/0/4 and GE 0/0/5 on DeviceB to their corresponding security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-untrust] add interface ge 0/0/5
[DeviceB-zone-untrust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-trust] add interface ge 0/0/4
[DeviceB-zone-trust] quit
```

Step 3 Configure security policies to allow the branch and HQ to exchange packets through a specified network segment.

Configure security policies on DeviceA.

1. Configure security policies between the Trust and Untrust zones on DeviceA to allow unencapsulated and decapsulated packets to pass through DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] destination-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone untrust
[DeviceA-policy-security-rule-policy2] destination-zone trust
[DeviceA-policy-security-rule-policy2] source-address 10.1.2.0 24
[DeviceA-policy-security-rule-policy2] destination-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

2. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local
[DeviceA-policy-security-rule-policy3] destination-zone untrust
[DeviceA-policy-security-rule-policy3] source-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy3] source-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy3] destination-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
[DeviceA-policy-security] rule name policy4
[DeviceA-policy-security-rule-policy4] source-zone untrust
[DeviceA-policy-security-rule-policy4] destination-zone local
[DeviceA-policy-security-rule-policy4] source-address 3.3.3.3 32
[DeviceA-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy4] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy4] action permit
[DeviceA-policy-security-rule-policy4] quit
[DeviceA-policy-security] quit
```

Configure security policies on DeviceB.

1. Configure security policies between the Trust and Untrust zones to allow unencapsulated and decapsulated packets to pass through DeviceB.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust
[DeviceB-policy-security-rule-policy1] destination-zone untrust
[DeviceB-policy-security-rule-policy1] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy1] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone untrust
[DeviceB-policy-security-rule-policy2] destination-zone trust
[DeviceB-policy-security-rule-policy2] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-policy2] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

2. Configure security policies between the Local and Untrust zones to allow the devices at the two ends of the IPsec tunnel to communicate for tunnel negotiation.

   NOTE

   The security policies between the Local and Untrust zones ensure that IKE negotiation packets can pass through the device. These policies can use the source and destination addresses as matching criteria and use protocols and ports as additional matching criteria. This example configures source and destination addresses as matching criteria. To use protocols and ports as additional matching criteria, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local
[DeviceB-policy-security-rule-policy3] destination-zone untrust
[DeviceB-policy-security-rule-policy3] source-address 3.3.3.3 32
[DeviceB-policy-security-rule-policy3] destination-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy3] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
[DeviceB-policy-security] rule name policy4
[DeviceB-policy-security-rule-policy4] source-zone untrust
[DeviceB-policy-security-rule-policy4] destination-zone local
[DeviceB-policy-security-rule-policy4] destination-address 1.1.1.1 32
[DeviceB-policy-security-rule-policy4] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-policy4] destination-address 3.3.3.3 32
[DeviceB-policy-security-rule-policy4] action permit
[DeviceB-policy-security-rule-policy4] quit
[DeviceB-policy-security] quit
```

Step 4 Configure an IPsec intelligent uplink selection profile based on link quality detection on DeviceA.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet through Link 1 is 1.1.1.254, and the next-hop IP address of the route from DeviceA to the Internet through Link 2 is 2.2.2.254.

```
[DeviceA] ipsec smart-link profile profile1
[DeviceA-ipsec-smart-link-profile-profile1] link-switch-mode route-based
[DeviceA-ipsec-smart-link-profile-profile1] link 1 interface ge 0/0/2 local 1.1.1.1 nexthop 1.1.1.254
remote 3.3.3.3
[DeviceA-ipsec-smart-link-profile-profile1] link 2 interface ge 0/0/3 local 2.2.2.2 nexthop 2.2.2.254
remote 3.3.3.3
```

Step 5 Configure an ISAKMP IPsec policy on DeviceA and reference the configured IPsec intelligent uplink selection profile in the IPsec policy.

Create advanced ACL 3000 to define the data flow to be protected.

```
[DeviceA] acl 3000
[DeviceA-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl-adv-3000] quit
```

Configure an IPsec proposal.

```
[DeviceA] ipsec proposal tran1
[DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceA-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceA] ike proposal 10
[DeviceA-ike-proposal-10] authentication-method pre-share
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-ike-proposal-10] prf hmac-sha2-256
[DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceA-ike-proposal-10] dh group14
[DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceA-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceA] ike peer a
[DeviceA-ike-peer-a] ike-proposal 10
[DeviceA-ike-peer-a] pre-shared-key YsHsjx_202206
[DeviceA-ike-peer-a] quit
```

Create the IPsec policy **map1**.

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-peer a
[DeviceA-ipsec-policy-isakmp-map1-10] smart-link profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] route inject dynamic
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

NOTE

The IPsec policy that references an IPsec intelligent uplink selection profile does not need to be applied to an interface. After DeviceA selects a link to establish an IPsec tunnel, it automatically applies the IPsec policy that references an IPsec intelligent uplink selection profile to the local interface for the link.

Step 6 Configure a template IPsec policy on DeviceB.

Create advanced ACL 3000, define the data flow to be protected, and allow the device to send ICMP packets.

```
[DeviceB] acl 3000
[DeviceB-acl-adv-3000] rule permit 5 ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-adv-3000] quit
```

Configure an IPsec proposal.

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
[DeviceB-ipsec-proposal-tran1] quit
```

Configure an IKE proposal.

```
[DeviceB] ike proposal 10
[DeviceB-ike-proposal-10] authentication-method pre-share
[DeviceB-ike-proposal-10] prf hmac-sha2-256
[DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
[DeviceB-ike-proposal-10] dh group14
[DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
[DeviceB-ike-proposal-10] quit
```

Configure an IKE peer.

```
[DeviceB] ike peer b
[DeviceB-ike-peer-b] ike-proposal 10
[DeviceB-ike-peer-b] remote-address 1.1.1.1
[DeviceB-ike-peer-b] pre-shared-key YsHsjx_202206
[DeviceB-ike-peer-b] quit
```

Configure an IPsec policy template.

```
[DeviceB] ipsec policy-template map_temp 1
[DeviceB-ipsec-policy-template-map_temp-1] security acl 3000
[DeviceB-ipsec-policy-template-map_temp-1] proposal tran1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-ipsec-policy-template-map_temp-1] ike-peer b
[DeviceB-ipsec-policy-template-map_temp-1] route inject dynamic preference 65
[DeviceB-ipsec-policy-template-map_temp-1] quit
```

Reference the IPsec policy template **map_temp** in the IPsec policy **map1**.

```
[DeviceB] ipsec policy map1 10 isakmp template map_temp
```

Apply an IPsec policy to GE 0/0/4.

```
[DeviceB] interface GE0/0/4
[DeviceB-GE0/0/4] ipsec policy map1
[DeviceB-GE0/0/4] quit
```

Step 7 Configure OSPF routes at the branch.

On DeviceA, configure OSPF routes.

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0.0.0.0
[DeviceA-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 2.2.2.0 0.0.0.255
```

Configure OSPF routes on the two routers connecting DeviceA to the Internet.

For details, see the configuration manual for the corresponding router. When configuring the intermediate routers, ensure that the public network routes between DeviceA and DeviceB are reachable.

----End

Verifying the Configuration

1. After the configuration is complete, run the **display ipsec smart-link profile** command on DeviceA. The command output shows that DeviceA at the branch first establishes an IPsec tunnel based on Link 1 (with the local address of 1.1.1.1 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ============================================
 Name                    :profile1
 Switch mode               :route-based
 State                   :enable
 IPsec policy alias        :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         0       0          active
 2  2.2.2.2         3.3.3.3         0       0          inactive
 ============================================
```

Run the **display ike sa** and **display ipsec sa** commands on DeviceA and DeviceB to check SA establishment. The following example uses the command output on DeviceA, which indicates that IKE SAs and IPsec SAs have been established.

```
<DeviceB> display ike sa
IKE SA information :
   Conn-ID      Peer        VPN   Flag(s)   Phase   RemoteType  RemoteID
 -------------------------------------------------------------------------------
   16782416     3.3.3.3:500       RD|ST|A   v2:2    IP          3.3.3.3
   16782415     3.3.3.3:500       RD|ST|A   v2:1    IP          3.3.3.3

 Number of IKE SA : 2
 -------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
```

 Copyright © Huawei Technologies Co., Ltd.

```
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
<DeviceB> display ipsec sa brief
Current ipsec sa num:2
Number of SAs:2
   Src address   Dst address     SPI      VPN  Protocol     Algorithm
-------------------------------------------------------------------------------
    1.1.1.1       3.3.3.3    3923280450         ESP       E:AES-256-GCM-128 A:SHA2-256-128
    3.3.3.3       1.1.1.1    787858613          ESP       E:AES-256-GCM-128 A:SHA2-256-128
```

2. On DeviceA, shut down interfaces on Link 1 and then run the **display ipsec smart-link profile** command. The command output shows that DeviceA automatically establishes an IPsec tunnel based on Link 2 (with the local address of 2.2.2.2 and remote address of 3.3.3.3).

```
<DeviceA> display ipsec smart-link profile name profile1
 ==========================================
 Name                    :profile1
 Switch mode               :route-based
 State                   :enable
 IPSec policy alias        :map1
 link list:
 ID local-address   remote-address  loss(%) delay(ms)  state
 1  1.1.1.1         3.3.3.3         0       0          inactive
 2  2.2.2.2         3.3.3.3         0       0          active
 ==========================================
```

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 10
#
ipsec smart-link profile pro1
 link-switch-mode route-based
 link 1 interface GE0/0/2 local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
 link 2 interface GE0/0/3 local 2.2.2.2 nexthop 2.2.2.254 remote 3.3.3.3
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer a
 proposal tran1
 smart-link profile profile1
 route inject dynamic
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 2.2.2.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
 add interface GE0/0/3
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 2.2.2.0 0.0.0.255
```

- DeviceB

```
#
sysname DeviceB
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 6 permit icmp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 7 permit icmp source 3.3.3.3 0 destination 1.1.1.1 0
 rule 8 permit icmp source 3.3.3.3 0 destination 2.2.2.2 0
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
```

 Copyright © Huawei Technologies Co., Ltd.

```
 pre-shared-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!7LTnVOK_g:PyTD"{G=@C8]V')EA@JOEw{zK!!!!!2jp5!!!!!!>!!!!
<r(EOYd:m5tpt2O#v#/0aHhgAFBa/0v_d(L[rv&4%+%#
 ike-proposal 10
 remote-address 1.1.1.1
#
ipsec policy-template map_temp 1
 proposal tran1
 ike-peer b
#
ipsec policy map1 10 isakmp template map_temp
#
interface GE0/0/4
 ipsec policy map1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/5
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface interface GE0/0/5
#
firewall zone untrust
 set priority 5
 add interface GE0/0/4
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  action permit
#
```

8.7 Others

8.7.1 Web: Example for Configuring a Base Station to Obtain an IP Address Using the IKEv2 Configuration Payload

Networking Requirements

As shown in **Figure 8-32**, DeviceA is deployed at the egress of network A, and the base station needs to securely communicate with the server on network A.

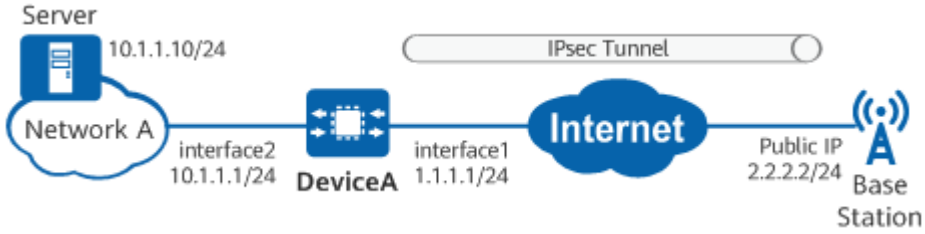
 Copyright © Huawei Technologies Co., Ltd.

DeviceA needs to use IKEv2 to establish an IPsec tunnel with the base station and assign a private IP address of network A to the base station for the base station and network A to communicate.

Figure 8-32 Configuring a base station to obtain an ip address using the IKEv2 configuration payload

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA, respectively.



Configuration Roadmap

1. Complete basic DeviceA configurations.
2. Create a template IPsec policy on DeviceA, because the access is always initiated from the base station to the server on network A.
3. For details about the base station configuration, see the corresponding product documentation.

Procedure

Step 1 Set interface IP addresses and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

3. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

Step 2 Configure security policies to permit IPsec negotiation packets and service packets.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Local-Untrust interzone policy determines whether IKE negotiation packets can pass through the device. The interzone policy can use the source address and destination address as matching conditions and can use the protocol type and port number as additional matching conditions. This example configures source and destination addresses as matching conditions. To use protocols and ports as additional matching conditions, you need to enable the ESP service and UDP port 500. In NAT traversal scenarios, you also need to enable UDP port 4500.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

   In this example, the private subnet assigned to the base station is 10.1.2.0/24.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

3. Repeat the preceding steps to configure the Untrust-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	untrust
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	1.1.1.1/32
Destination Address	2.2.2.2/32
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	2.2.2.2/32
Destination Address	1.1.1.1/32
Action	Permit

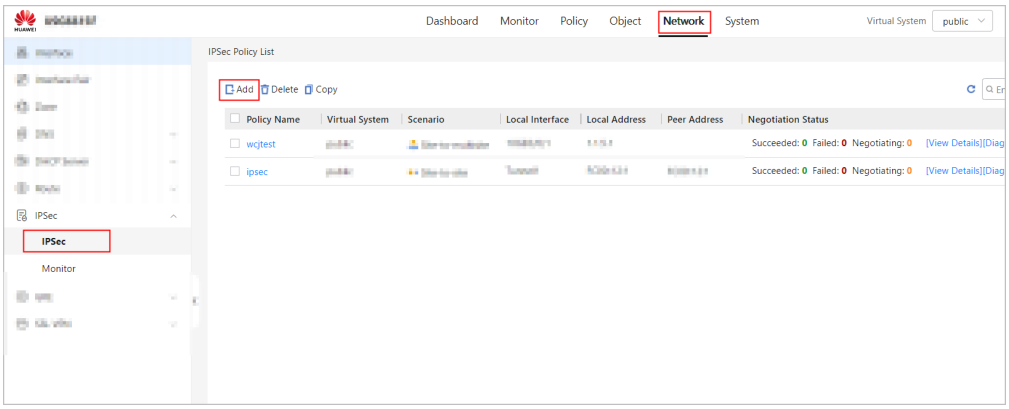
Step 3 Create a static route to the Internet. In this example, the next-hop IP address is 1.1.1.2.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add**.
3. Configure a default route from DeviceA to the Internet as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.2

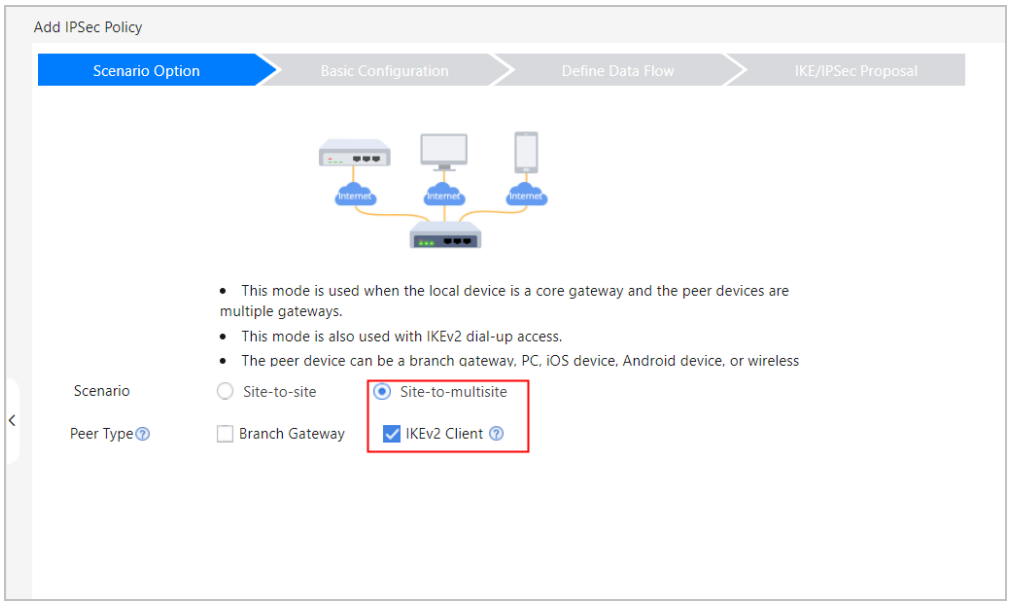
Step 4 Configure an IPsec policy.

1. Choose **Network** > **IPSec** > **IPSec**.

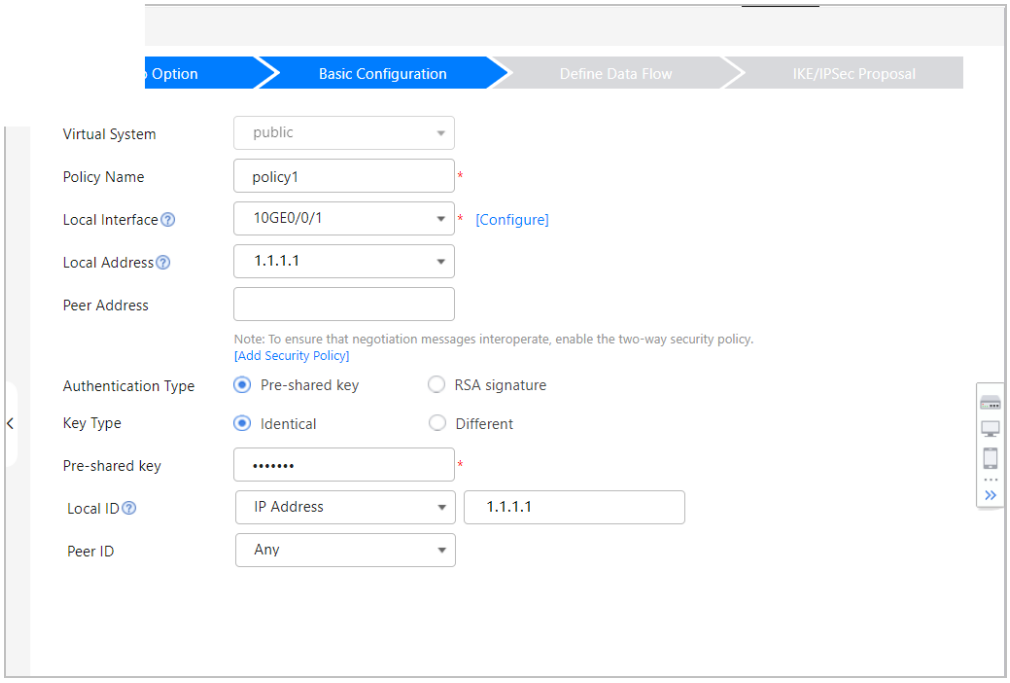


2. Click **Add** to create an IPsec policy as prompted.

 Copyright © Huawei Technologies Co., Ltd.

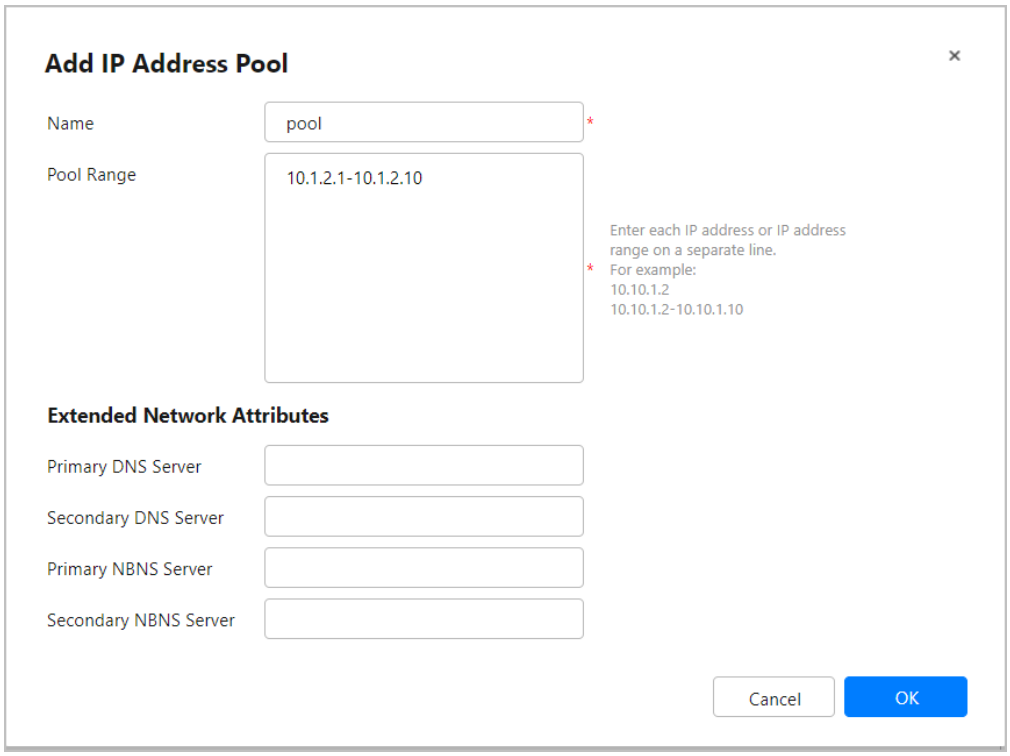


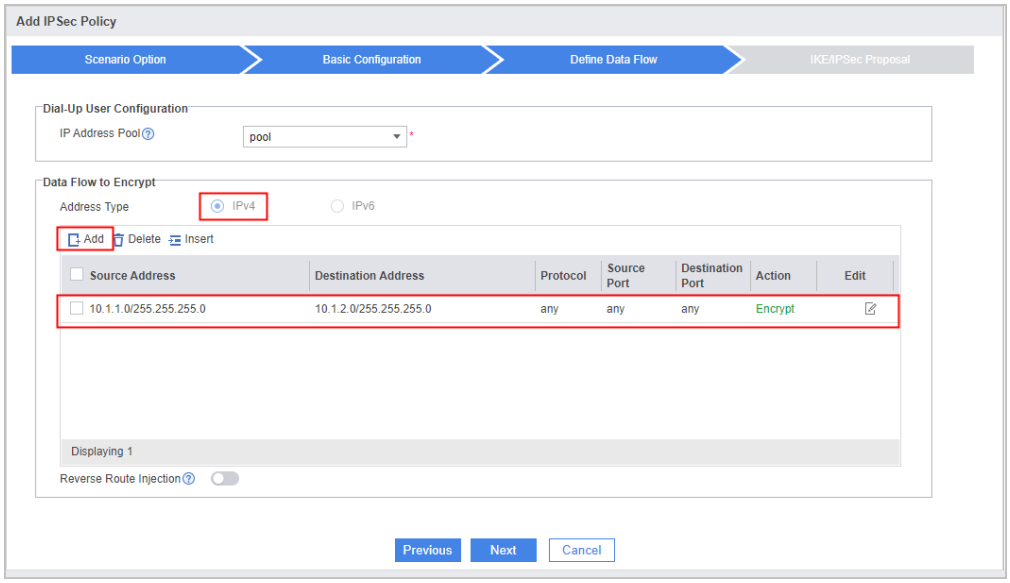
The pre-shared key is YsHsjx_202206.



In the **Dial-up User Configuration** area, click the **IP Address Pool** drop-down list and click **Add IP pool** to create an address pool. The following figure shows the parameter settings.

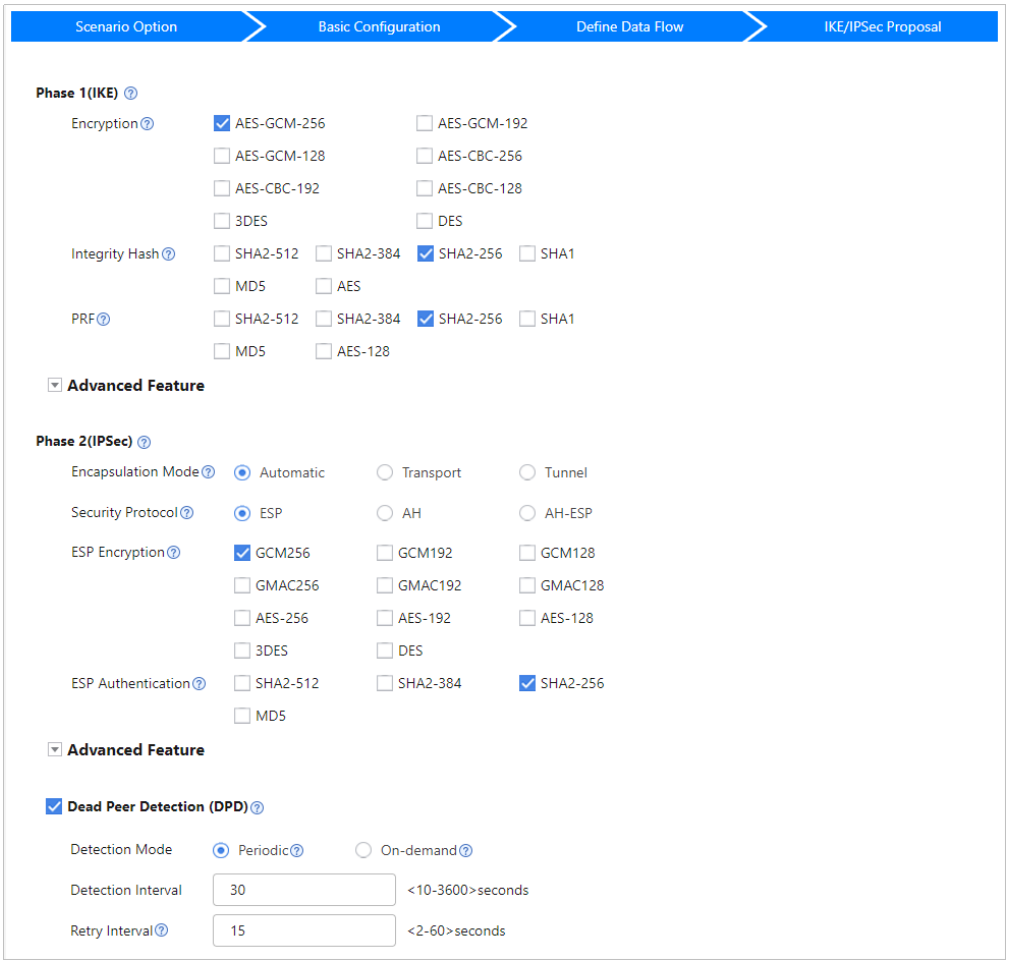
 Copyright © Huawei Technologies Co., Ltd.





In the example, the default parameter settings are used for the IPsec proposal. When modifying the parameter settings, ensure that the security proposals used by the tunnel ends are the same.

 Copyright © Huawei Technologies Co., Ltd.

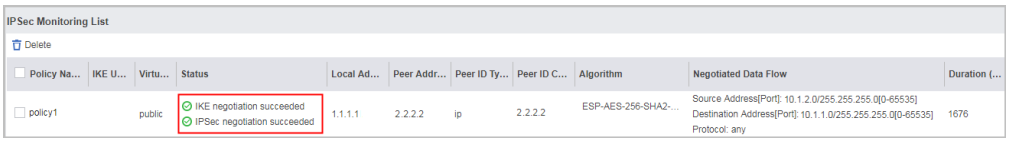


3. Click **Finish**.

----End

Verifying the Configuration

1. On DeviceA, choose **Network** > **IPSec** > **Monitor** to display the IPsec tunnel monitoring information. The following figure shows that the IPsec tunnel is successfully established.



2. The base station has obtained the IP address assigned by DeviceA, the base station and the server on network A can communicate properly, and the service configuration succeeds.

Configuration Scripts

```
#
acl number 3005
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ip pool pool
 section 0 10.1.2.1 10.1.2.10
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
ipsec proposal prop25119505373
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 2
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer ike251195053730
 pre-shared-key %@%@/Ttl*ib{a8;\cWUI"To#2n[\%@%@
 ike-proposal 2
 local-id 1.1.1.1
 ip-pool pool
#
ipsec policy-template tpl251195053730 1
 security acl 3005
 ike-peer ike251195053730
 proposal prop25119505373
 scenario point-to-multi-point ikev2-user-access
#
ipsec policy policy1 10000 isakmp template tpl251195053730
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy policy1
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone trust
 add interface GE0/0/2
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    destination-address 10.1.2.0 mask 255.255.255.0
    action permit
  rule name policy2
    source-zone untrust
    destination-zone trust
    source-address 10.1.2.0 mask 255.255.255.0
    destination-address 10.1.1.0 mask 255.255.255.0
    action permit
  rule name policy3
    source-zone untrust
    destination-zone local
    source-address 2.2.2.2 mask 255.255.255.255
    destination-address 1.1.1.1 mask 255.255.255.255
    action permit
  rule name policy4
    source-zone local
    destination-zone untrust
    source-address 1.1.1.1 mask 255.255.255.255
    destination-address 2.2.2.2 mask 255.255.255.255
    action permit
```

 Copyright © Huawei Technologies Co., Ltd.

9 SSL VPN

9.1 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (User Name + Password Authentication)

9.2 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (User Name + Password Authentication)

9.3 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Anonymous Authentication)

9.4 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Anonymous Authentication)

9.5 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Challenge Authentication)

9.6 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Challenge Authentication)

9.7 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + AD Authorization)

9.8 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + AD Authorization)

9.9 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + Local Authorization)

9.10 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + Local Authorization)

9.11 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + Local Authorization)

9.12 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + Local Authorization)

9.13 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + Local Authorization)

9.14 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + Local Authorization)

 Copyright © Huawei Technologies Co., Ltd.

9.15 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + LDAP Authorization)

9.16 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + LDAP Authorization)

9.17 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + RADIUS Authorization)

9.18 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + RADIUS Authorization)

9.19 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Two-Factor Authentication + Local Authorization)

9.20 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Two-Factor Authentication + Local Authorization)

9.1 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (User Name + Password Authentication)

Networking Requirements

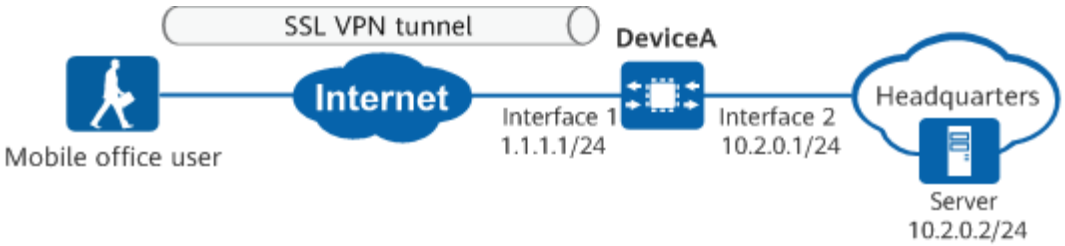
On the enterprise network shown in **Figure 9-1**, the enterprise authenticates employees in each department through local authentication on the device (DeviceA). Authenticated users can access the enterprise intranet.

The enterprise wants mobile office users in a UCL group (group1) to be able to obtain an intranet IP address when they are on the move and can access various resources in the enterprise as if they were on a LAN. To enhance security, local authentication with a user name and password is required.

Figure 9-1 Network diagram for configuring network extension

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address 172.16.1.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name group1
```

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Create an SSL VPN virtual gateway. The default authentication mode for the virtual gateway is user name + password.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example]service address interface ge 0/0/1 port 443
```

Step 6 Configure the network extension function.

Set the keepalive timeout period for the network extension function.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 7 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with the UCL group and resources.

```
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group group1
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

Configure a local access user with the user name **abc** and password **Helloworld@135**, set the access type of this user to **sslvpn**, and bind the user to the UCL group **group1**.

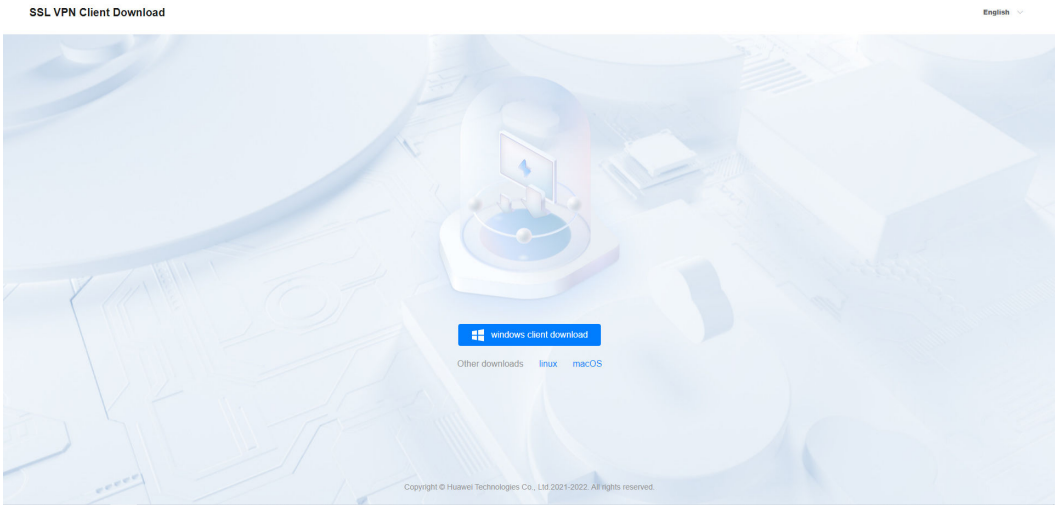
```
[DeviceA] aaa
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] password cipher Helloworld@135
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] ucl-group group1
[DeviceA-aaa-access-user-abc] quit
[DeviceA-aaa] quit
```

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-2 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name group1 index 1
#
aaa
 local-access-user abc
  service-type sslvpn
  ucl-group group1
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 1
 service address interface GE0/0/1 port 443
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
 role staff 0
  group group1
  resource test
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

9.2 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (User Name + Password Authentication)

Networking Requirements

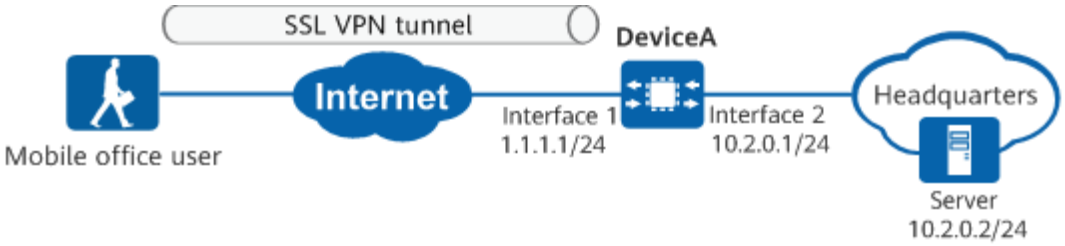
On the enterprise network shown in **Figure 9-3**, the enterprise authenticates employees in each department through local authentication on the device (DeviceA). Authenticated users can access the enterprise intranet.

The enterprise wants mobile office users in a UCL group (group1) to be able to obtain an intranet IP address when they are on the move and can access various intranet resources as if they were on a LAN. To enhance security, local authentication with a user name and password is required.

Figure 9-3 Network diagram for configuring network extension

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Configure an IP address for GE 0/0/2 and add it to a security zone.
   a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

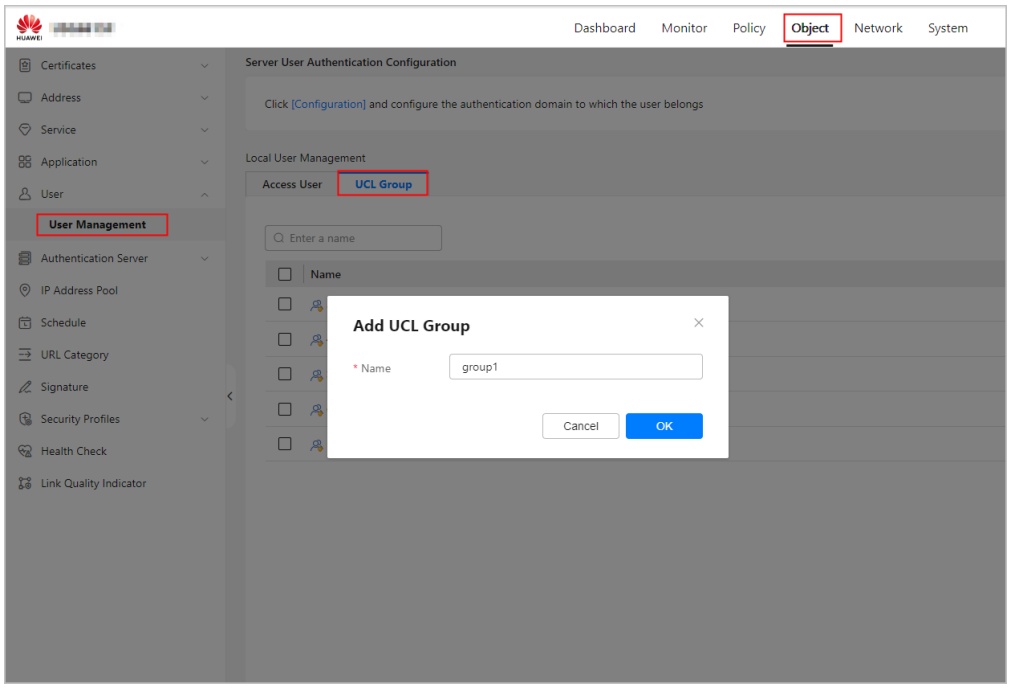
Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.0/24
Action	Permit

5. Click **OK**.

Step 3 Configure a security group, a user, and an address pool.

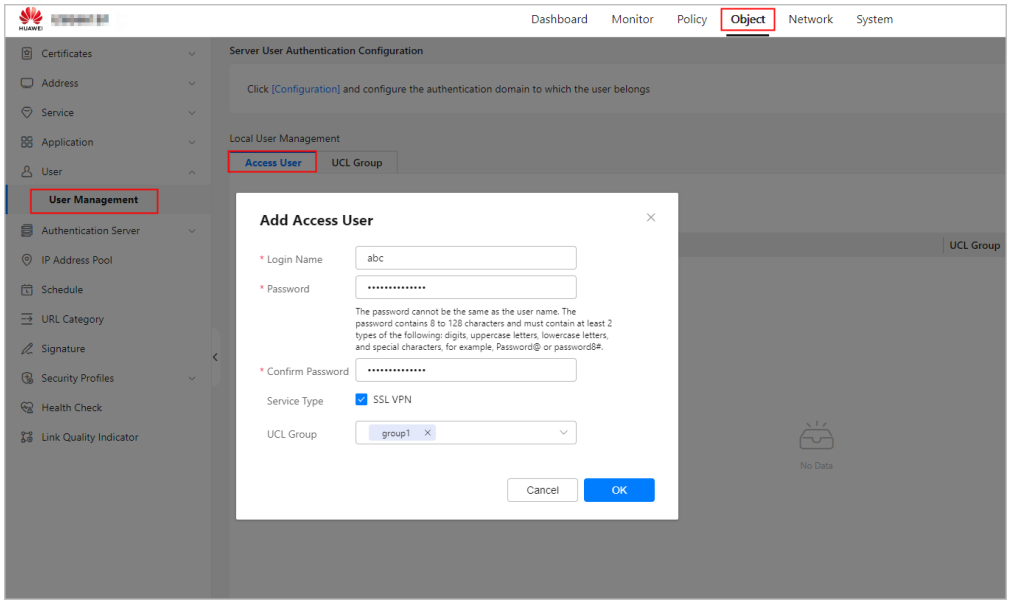
1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.

 Copyright © Huawei Technologies Co., Ltd.



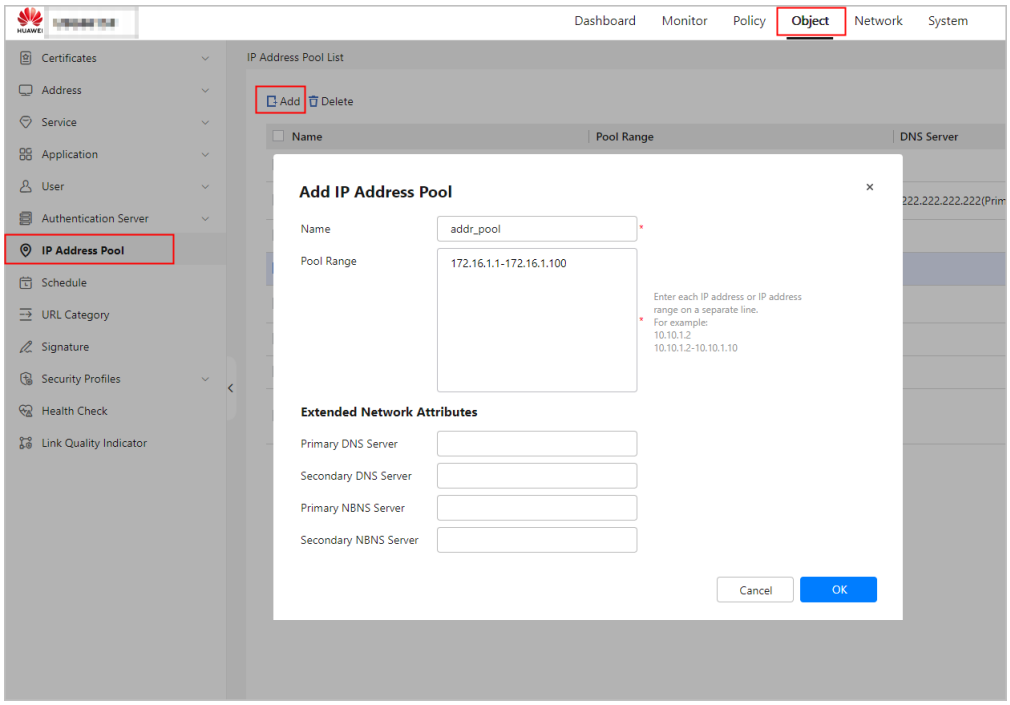
2. Click **OK**.
3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   The user **abc** belongs to the user group **group1** and the password is **Helloworld@135**.



4. Click **OK**.
5. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

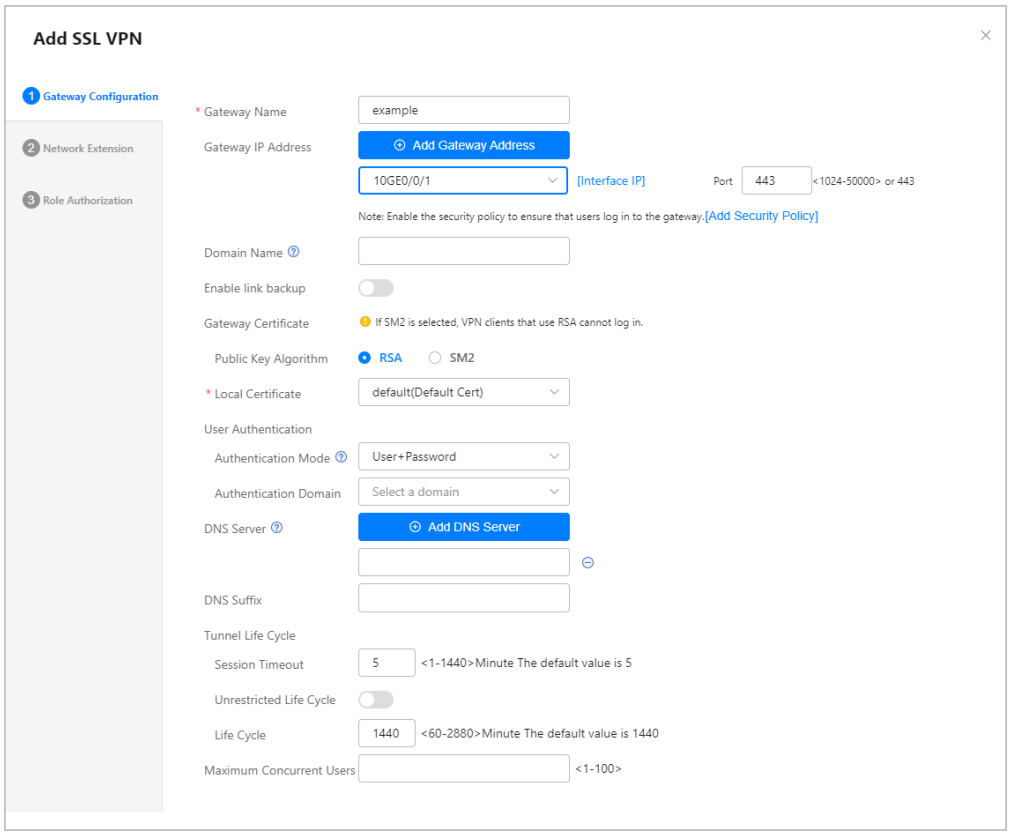
 Copyright © Huawei Technologies Co., Ltd.



6. Click **OK**.

Step 4 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

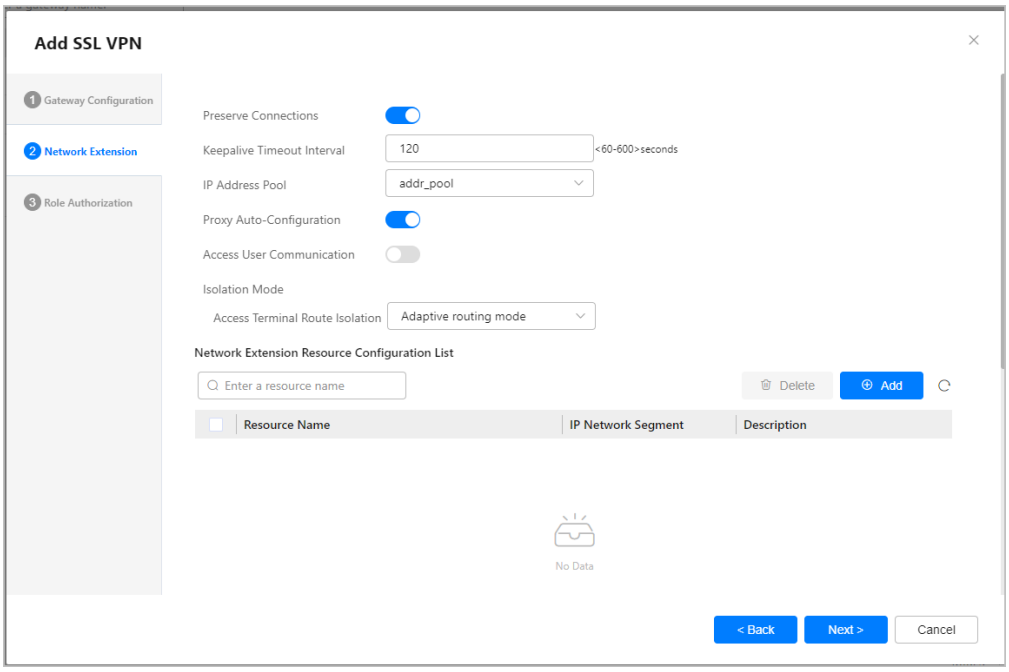


 Copyright © Huawei Technologies Co., Ltd.

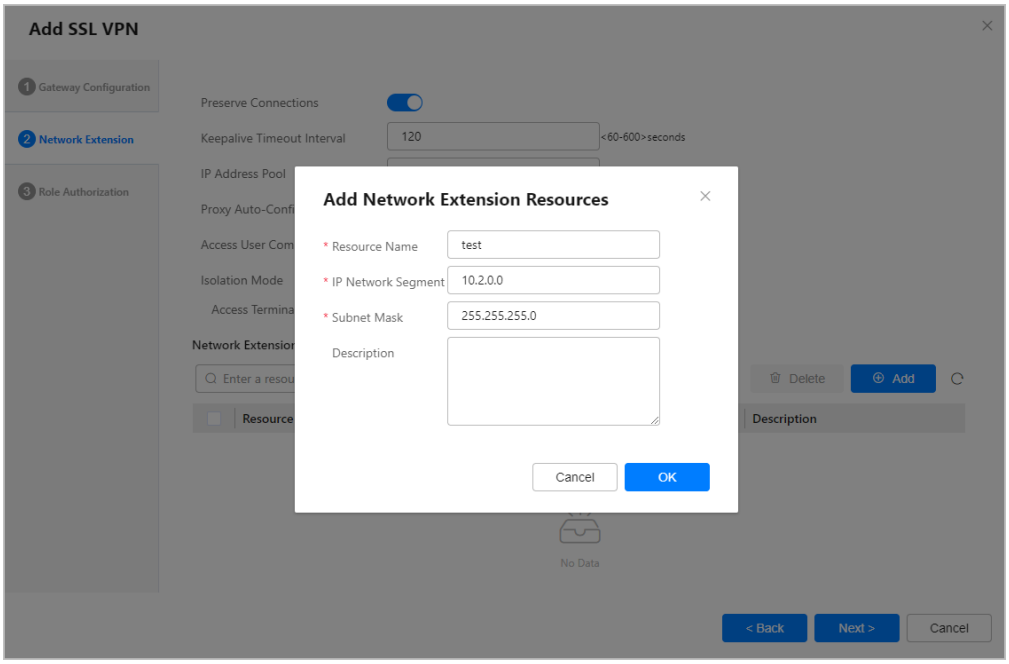
3. Click **Next**.

Step 5 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

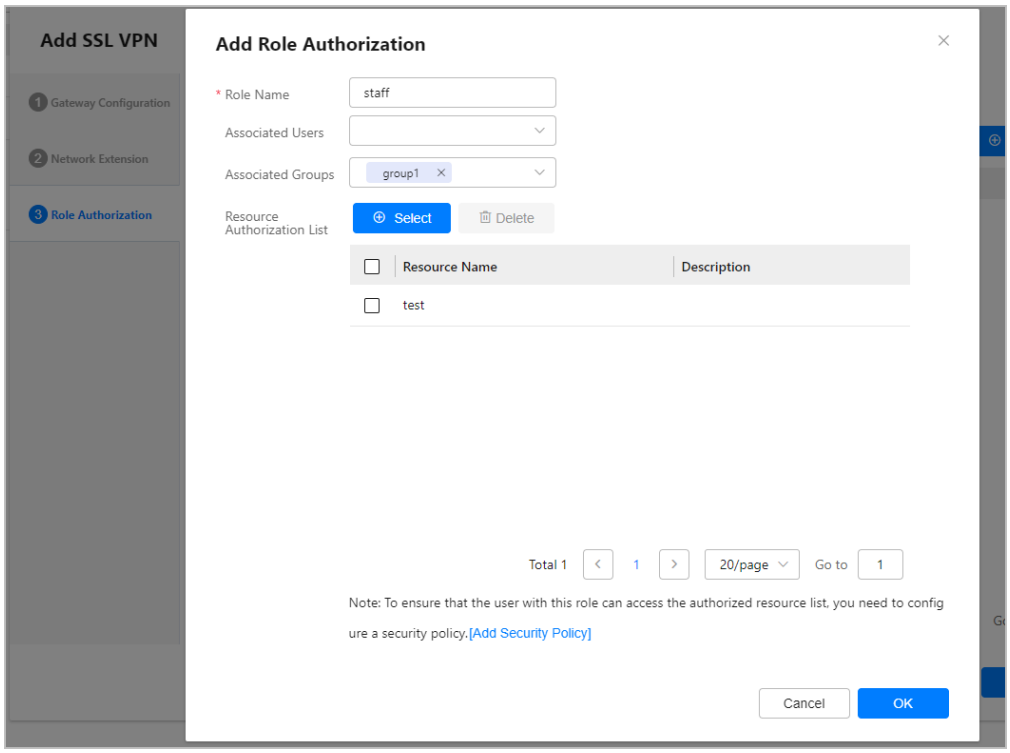


3. Click **Next**.

Step 6 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

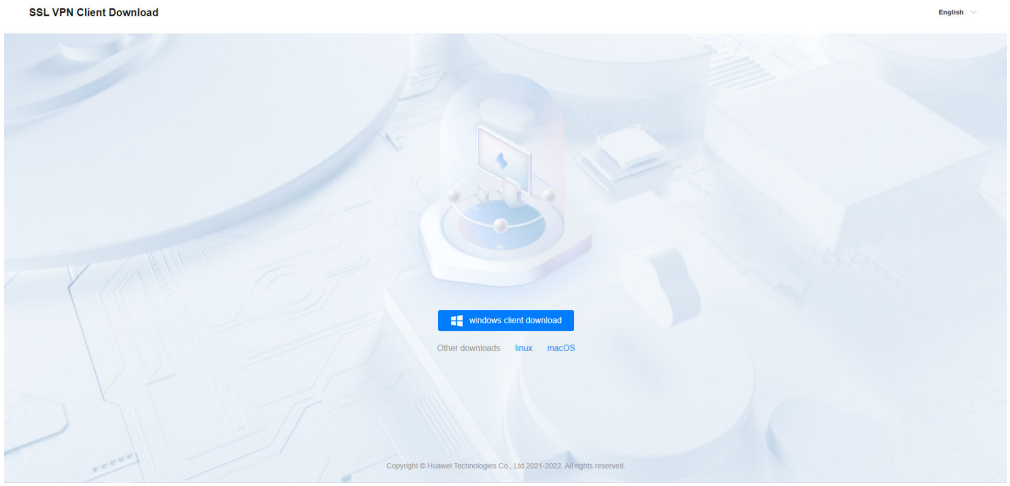
Step 7 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal. As shown in the following figure, download the VPN client installation package based on your operating system and install it. For more information, see **VPN Client Download Description**.

Figure 9-4 Downloading the VPN client installation package from the SSL VPN portal



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name group1 index 1
#
aaa
 local-access-user abc
  service-type sslvpn
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 0
 service address interface GE0/0/1 port 443
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
 role staff 0
  group group1
  resource test
#
return
```

9.3 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Anonymous Authentication)

Networking Requirements

On the enterprise network shown in **Figure 9-5**, the enterprise headquarters has multiple departments, including the research department. The enterprise

 Copyright © Huawei Technologies Co., Ltd.

authenticates employees in each department through local authentication on the device (DeviceA). Authenticated users can access the enterprise intranet.

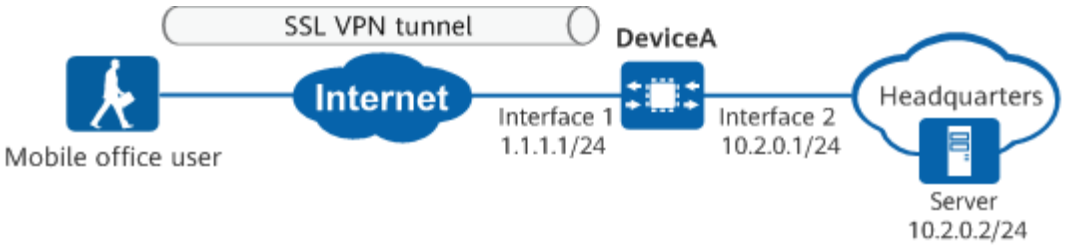
The enterprise wants mobile office users in the research department to be able to obtain an intranet IP address when they are on the move and can access various resources in the enterprise as if they were on a LAN. In addition, to enhance security, certificate authentication (certificate-anonymous authentication) is required to authenticate mobile office users. In this case, users need to install client certificates and do not need to enter passwords.

In this example, the administrator obtains the CA certificate **ca.cer** from a CA. In the client certificate, the CN field value is **user0001**, which is the user name, and the Organizational unit (OU) field value is **research**, which is the group name.

Figure 9-5 Network diagram for configuring network extension

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Apply for the CA certificate and client certificate. For details on how to import a certificate, see "Installing a CA Certificate" and "Installing a Local Certificate" in CLI-based Configuration Guide > Security Protection Configuration > PKI Configuration.

Step 2 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Trust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone trust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 3 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address 172.16.1.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
[DeviceA-policy-security] quit
```

Step 4 Create a UCL group.

```
[DeviceA] ucl-group name research
```

Step 5 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 6 Create an SSL VPN virtual gateway. The default authentication mode for the virtual gateway is user name + password.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example]service address interface ge 0/0/1 port 443
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.255.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the authentication mode for the virtual gateway to certificate-anonymous authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-mode cert-anonymous
```

Configure the client CA certificate of the virtual gateway.

```
[DeviceA-virtual-gateway-example-security] client-ca-certificate ca.cer
```

Set the user filtering field and group filtering field used by the virtual gateway. The user filtering field specifies the field in the client certificate that is used as the user name, and the group filtering field specifies the one that is used as the UCL group name. The two parameters are used for identity authentication and subsequent role authorization.

```
[DeviceA-virtual-gateway-example-security] cert-anonymous cert-field user-filter subject common-name
group-filter subject organization-unit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with the UCL group and resources.

```
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group research
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

Configure a local access user with the user name **abc** , set the access type of this user to **sslvpn**.

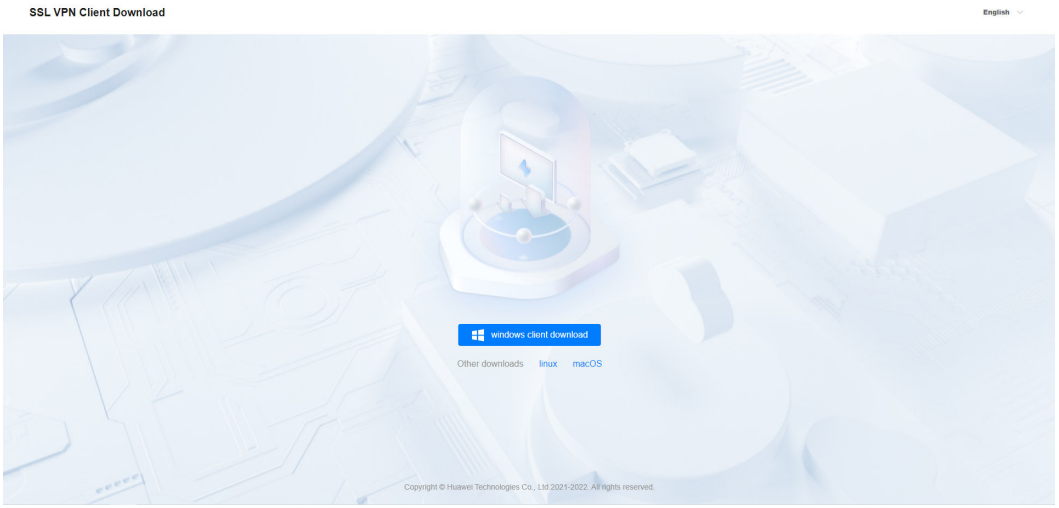
```
[DeviceA] aaa
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] quit
[DeviceA-aaa] quit
```

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-6 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name research index 1
#
aaa
 local-access-user abc
  service-type sslvpn
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.1 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 0
 service address interface GE0/0/1 port 443
 security
  authentication-mode cert-anonymous
  client-ca-certificate ca.cer
  cert-anonymous cert-field user-filter subject common-name group-filter subject organization-unit
 service
  network-extension ip-pool addr_pool
  network-extension proxy-auto-config disable
  network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
 role staff 0
  group research
  resource test
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

9.4 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Anonymous Authentication)

Networking Requirements

On the enterprise network shown in **Figure 9-7**, the enterprise headquarters has multiple departments, including the research department. The enterprise authenticates employees in each department through local authentication on the device (DeviceA). Authenticated users can access the enterprise intranet.

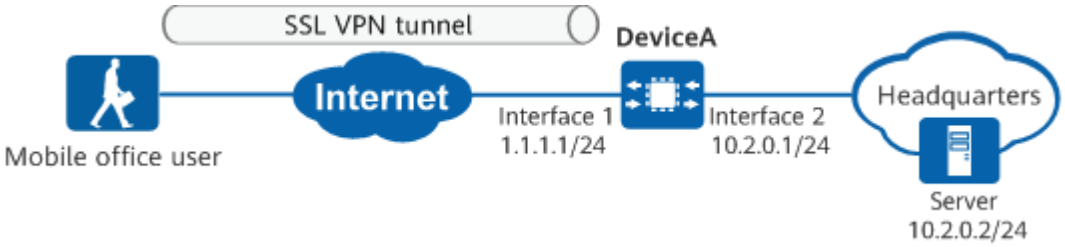
The enterprise wants mobile office users in the research department to be able to obtain an intranet IP address when they are on the move and can access various intranet resources as if they were on a LAN. In addition, to enhance security, certificate authentication (certificate-anonymous authentication) is required to authenticate mobile office users. In this case, users need to install client certificates and do not need to enter passwords.

In this example, the administrator obtains the CA certificate **ca.cer** from a CA. In the client certificate, the common name (CN) field value is **user0001**, which is the user name, and the Organizational unit (OU) field value is **research**, which is the group name.

Figure 9-7 Network diagram for configuring network extension

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Apply for the CA certificate and client certificate. For details on how to import a certificate, see "Installing a CA Certificate" and "Installing a Local Certificate" in CLI Configuration Guide > Security Protection Configuration > PKI Configuration.

Step 2 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Configure an IP address for GE 0/0/2 and add it to a security zone.

a. In **Interface List**, click  in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 3 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

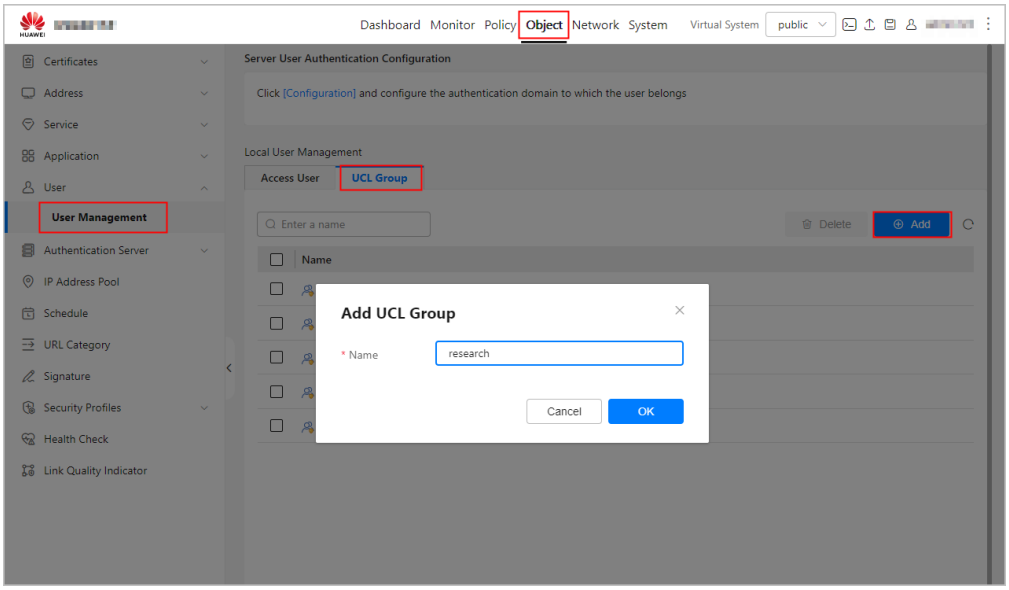
Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.0/24
Action	Permit

5. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

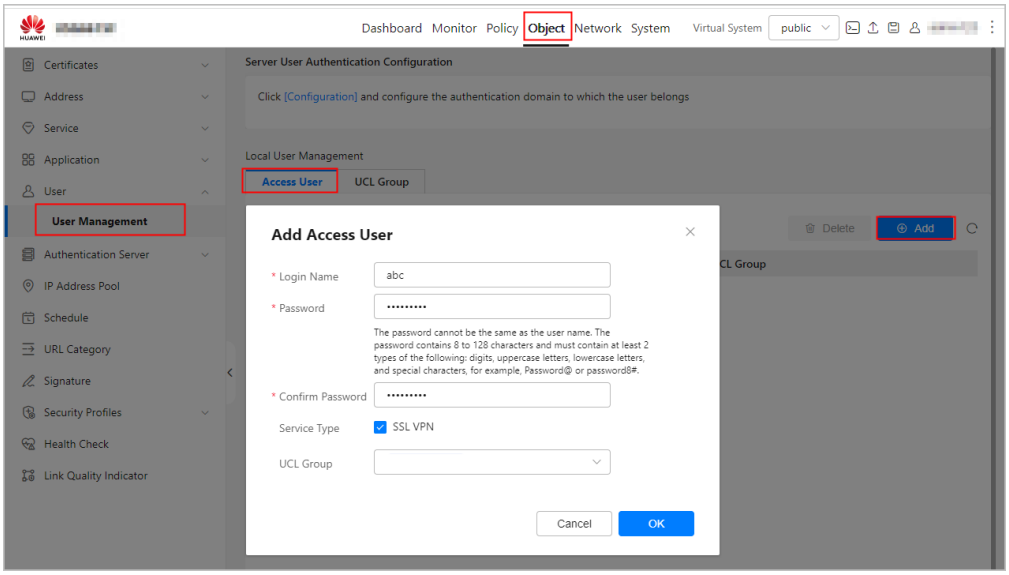
Step 4 Configure a security group and an address pool.

1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.



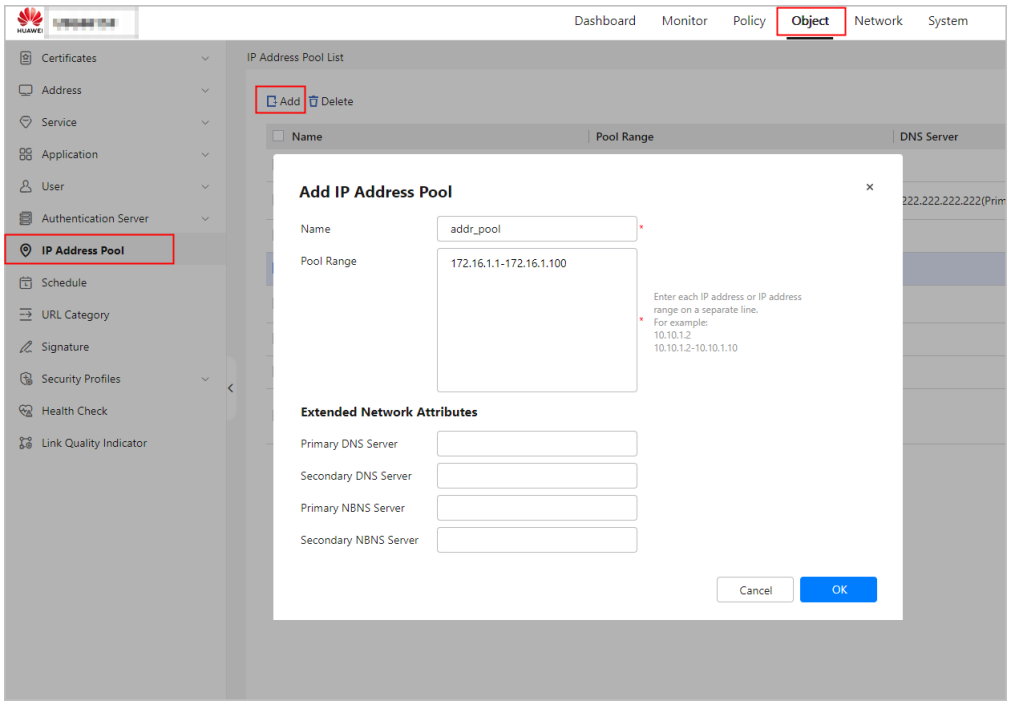
2. Click **OK**.
3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   Create the user **abc** with the password **Helloworld@135**.



4. Click **OK**.
5. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

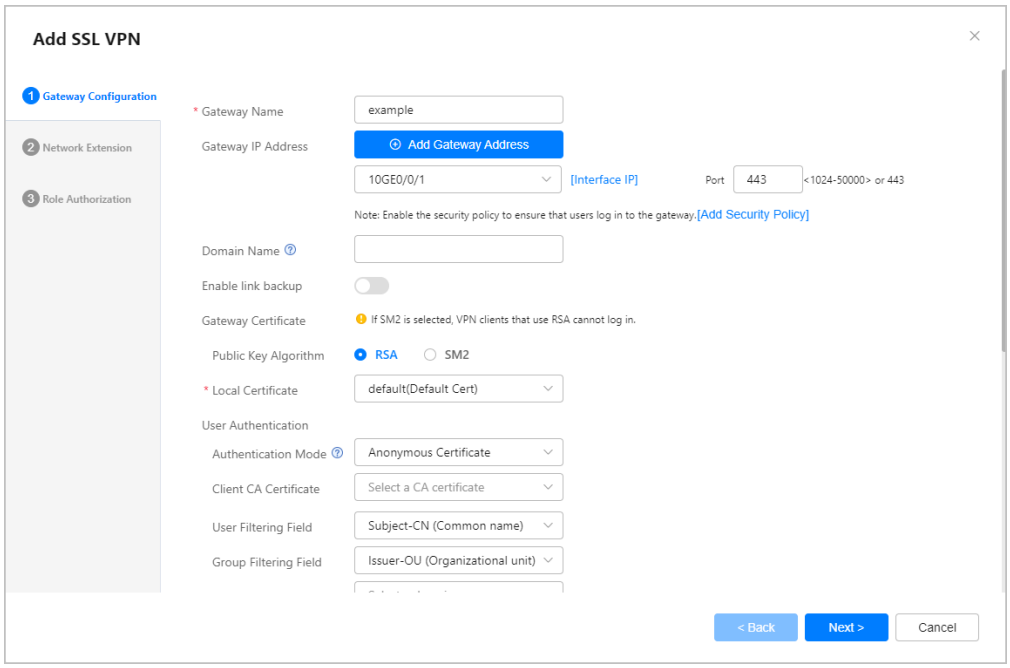
 Copyright © Huawei Technologies Co., Ltd.



6. Click **OK**.

Step 5 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add**, set the authentication mode of the virtual gateway to certificate-anonymous authentication, and set the client CA certificate used by the virtual gateway. You can use the default session timeout interval and life cycle.

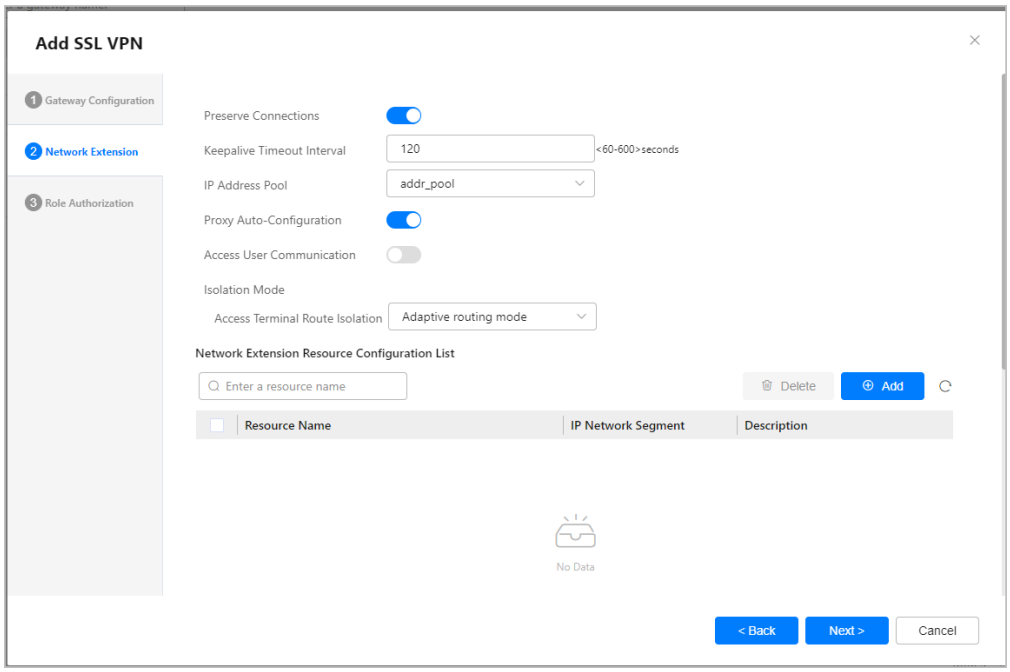


3. Click **Next**.

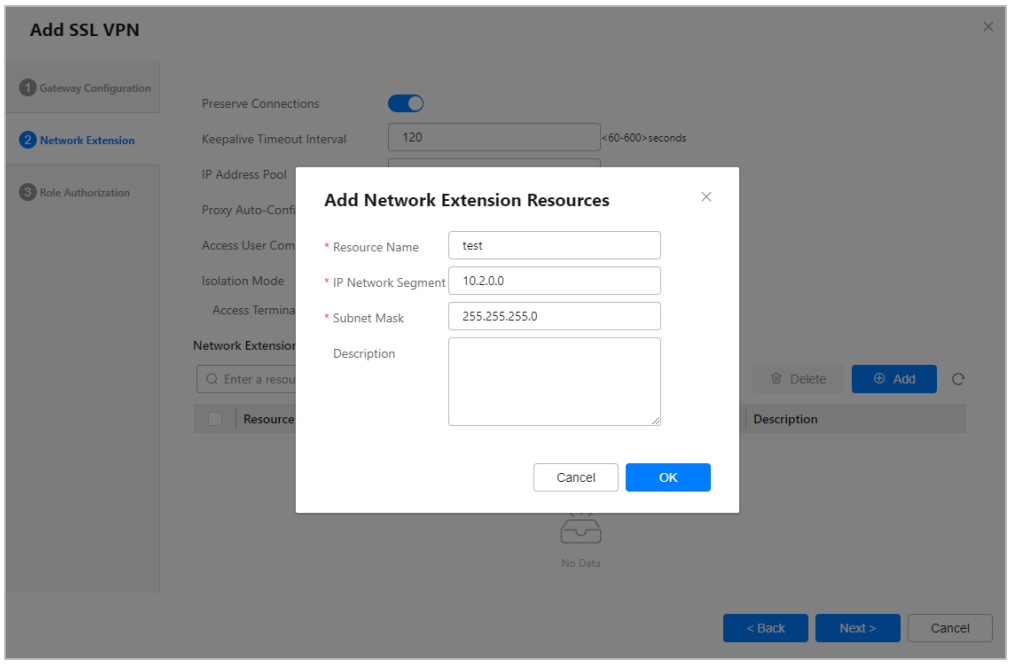
 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

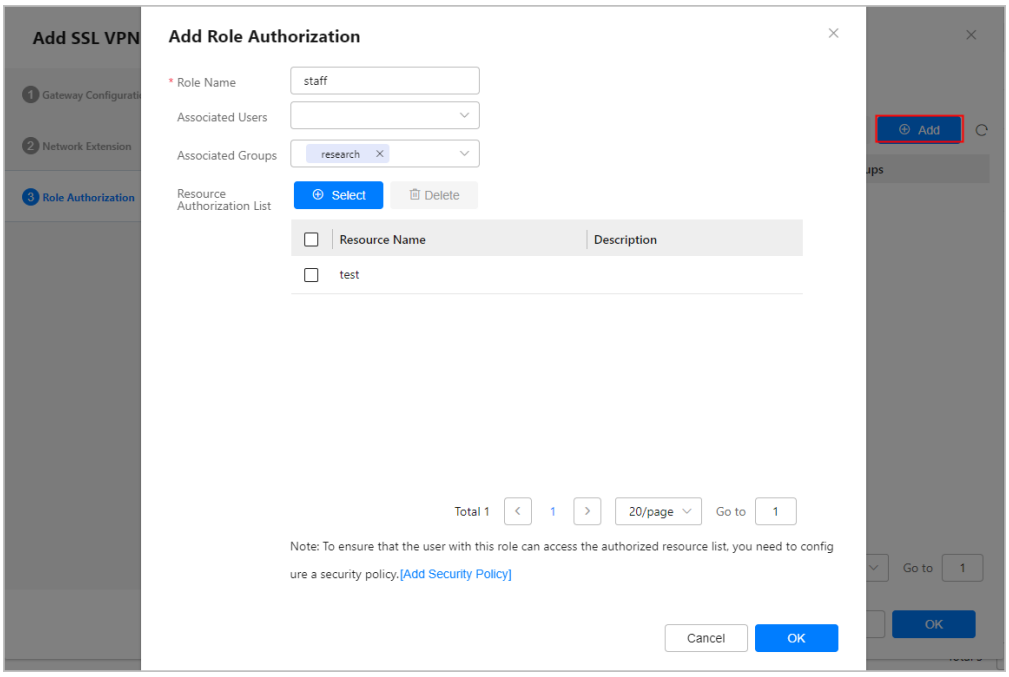


3. Click **Next**.

Step 7 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

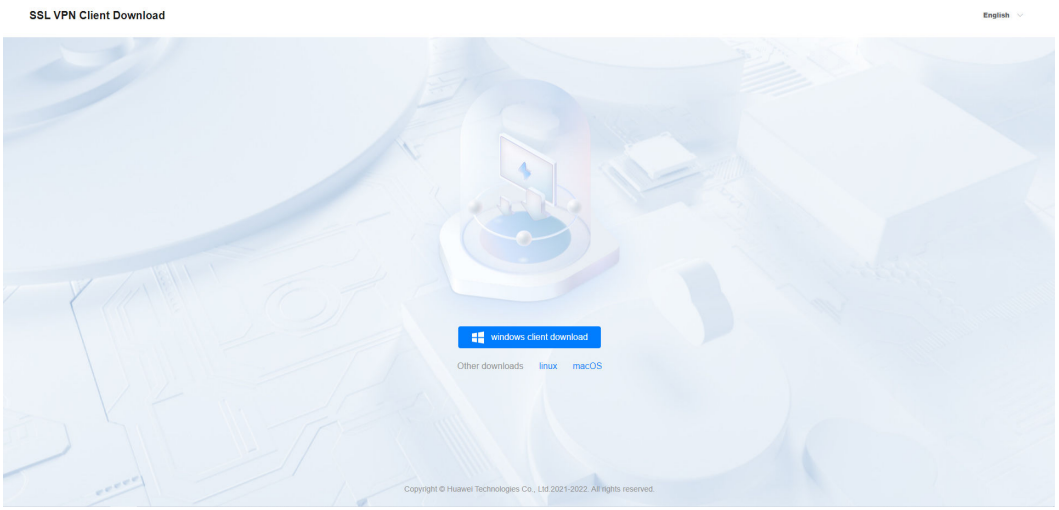
Step 8 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-8 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name research index 1
#
aaa
 local-access-user abc
  service-type sslvpn
#
interface GE0/0/1
 ip address 1.1.1.0 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.0 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 0
 service address interface GE0/0/1 port 443
 security
  authentication-mode cert-anonymous
  client-ca-certificate ca.cer
  cert-anonymous cert-field user-filter subject common-name group-filter issuer organization-unit
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
 role staff 0
  group research
  resource test
#
return
```

9.5 CLI: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Challenge Authentication)

Networking Requirements

On the enterprise network shown in the following figure, the enterprise headquarters has multiple departments, including the research department. The

 Copyright © Huawei Technologies Co., Ltd.

enterprise authenticates employees in each department through local authentication on the device (DeviceA). Authenticated users can access the enterprise intranet.

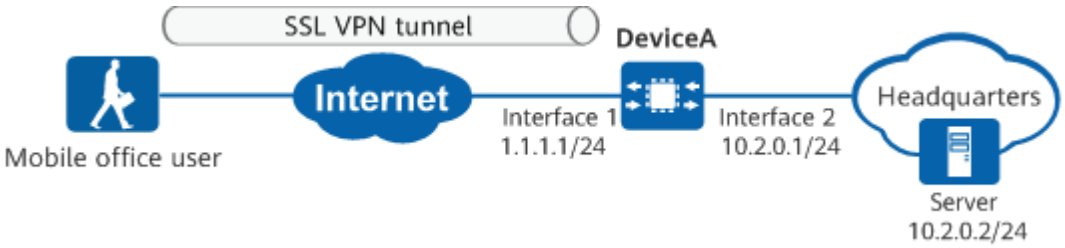
The enterprise wants mobile office users in the research department to be able to obtain an intranet IP address when they are on the move and can access various resources in the enterprise as if they were on a LAN. In addition, to enhance security, certificate authentication and local authentication (certificate-challenge authentication) need to be used together to authenticate mobile office users. In this case, users need to install client certificates and enter passwords.

In this example, the administrator obtains the CA certificate **ca.cer** from a CA. In the client certificate, the CN field value is **abc**, which is the user name, and the Organizational unit (OU) field value is **research**, which is the group name.

Figure 9-9 Network diagram for configuring network extension

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Apply for the CA certificate and client certificate. For details on how to import a certificate, see "Installing a CA Certificate" and "Installing a Local Certificate" in CLI-based Configuration Guide > Security Protection Configuration > PKI Configuration.

Step 2 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 3 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address 172.16.1.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
[DeviceA-policy-security] quit
```

Step 4 Create a UCL group.

```
[DeviceA] ucl-group name research
```

Step 5 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 6 Create an SSL VPN virtual gateway. The default authentication mode for the virtual gateway is user name + password.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example]service address interface ge 0/0/1 port 443
```

Step 7 Configure the network extension function.

Set the keepalive timeout period for the network extension function.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.255.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the authentication mode for the virtual gateway to certificate-challenge authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-mode cert-challenge
```

Configure the client CA certificate of the virtual gateway.

```
[DeviceA-virtual-gateway-example-security] client-ca-certificate ca.cer
```

Set the user filtering field and group filtering field used by the virtual gateway. The user filtering field specifies the field in the client certificate that is used as the user name, and the group filtering field specifies the one that is used as the UCL group name. The two parameters are used for identity authentication and subsequent role authorization.

```
[DeviceA-virtual-gateway-example-security] cert-challenge cert-field user-filter subject common-name group-filter subject organization-unit
[DeviceA-virtual-gateway-example-security] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with the UCL group and resources.

```
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group research
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

Configure a local access user with the user name **abc** and password **Helloworld@135**, set the access type of this user to **sslvpn**.

```
[DeviceA] aaa
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] password cipher Helloworld@135
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] quit
[DeviceA-aaa] quit
```

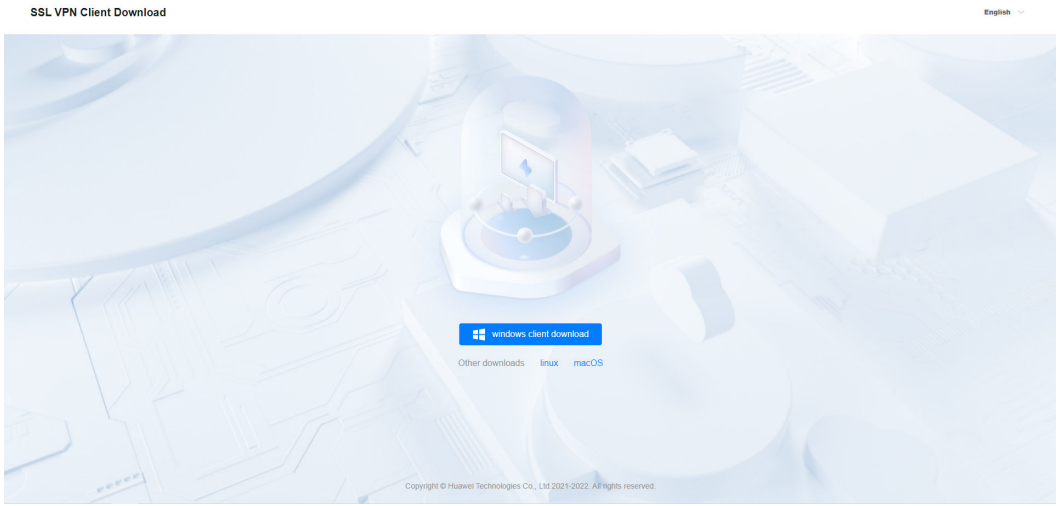
----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-10 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name research index 1
#
aaa
 local-access-user abc
  service-type sslvpn
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 service address interface GE0/0/1 port 443
 security
  authentication-mode cert-challenge
  client-ca-certificate ca.cer
  cert-anonymous cert-field user-filter subject common-name group-filter subject organization-unit
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
 role staff 0
  group research
  resource test
#
return
```

9.6 Web: Example for Configuring Mobile Office Users to Access the Enterprise Intranet Through the SSL VPN Tunnel (Certificate-Challenge Authentication)

Networking Requirements

On the enterprise network shown in **Figure 9-11**, the enterprise headquarters has multiple departments, including the research department. The enterprise authenticates employees in each department through local authentication on the device (DeviceA). Authenticated users can access the enterprise intranet.

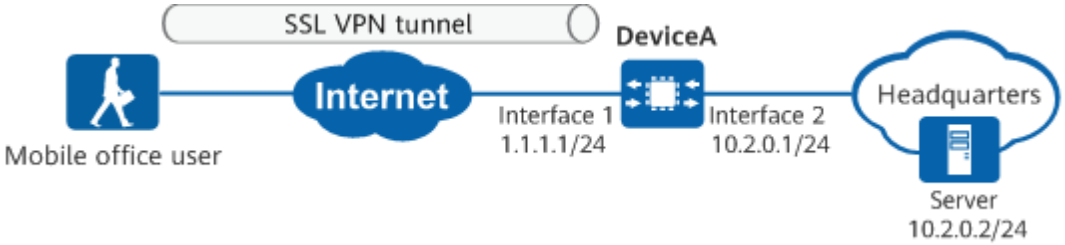
The enterprise wants mobile office users in the research department to be able to obtain an intranet IP address when they are on the move and can access various intranet resources as if they were on a LAN. In addition, to enhance security, certificate authentication and local authentication (certificate-challenge authentication) need to be used together to authenticate mobile office users. In this case, users need to install client certificates and enter passwords.

In this example, the administrator obtains the CA certificate **ca.cer** from a CA. In the client certificate, the common name (CN) field value is **abc**, which is the user name, and the Organizational unit (OU) field value is **research**, which is the group name.

Figure 9-11 Network diagram for configuring network extension

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Apply for the CA certificate and client certificate. For details on how to import a certificate, see "Installing a CA Certificate" and "Installing a Local Certificate" in CLI Configuration Guide > Security Protection Configuration > PKI Configuration.

Step 2 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Configure an IP address for GE 0/0/2 and add it to a security zone.
   a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.

Step 3 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

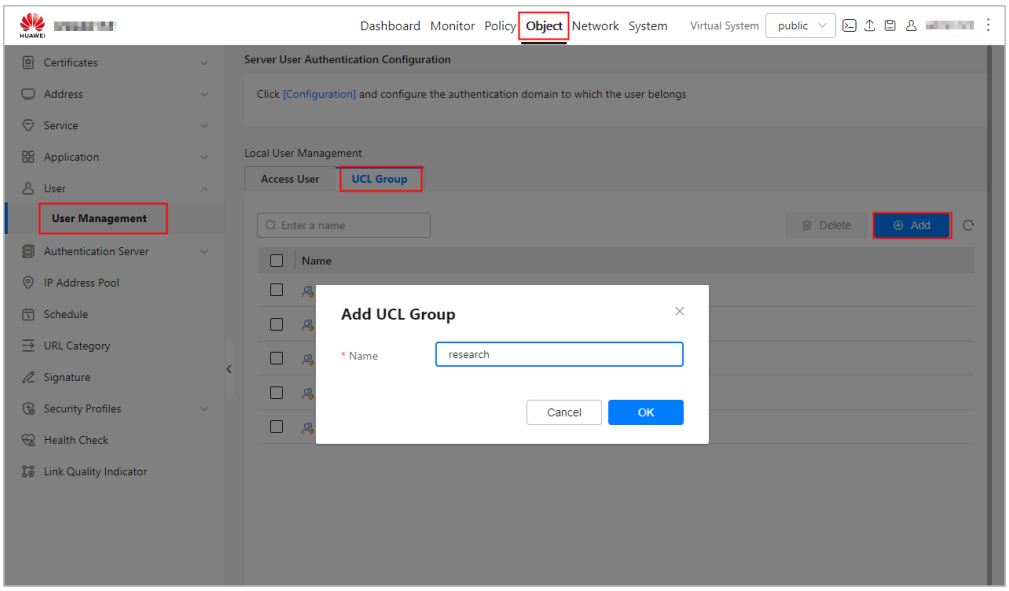
 Copyright © Huawei Technologies Co., Ltd.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.0/24
Action	Permit

5. Click **OK**.

Step 4 Configure a security group, a user, and an address pool.

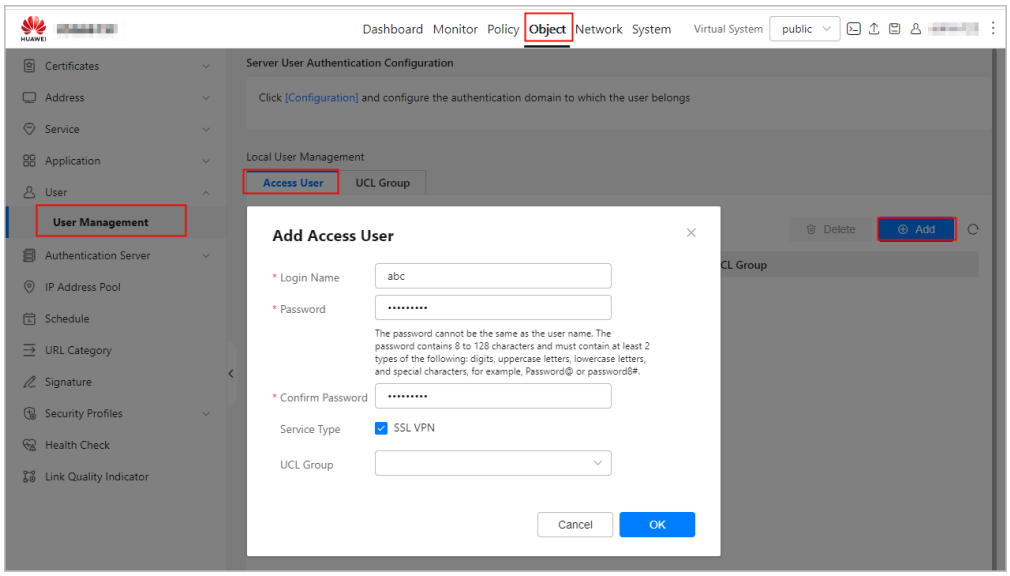
1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.



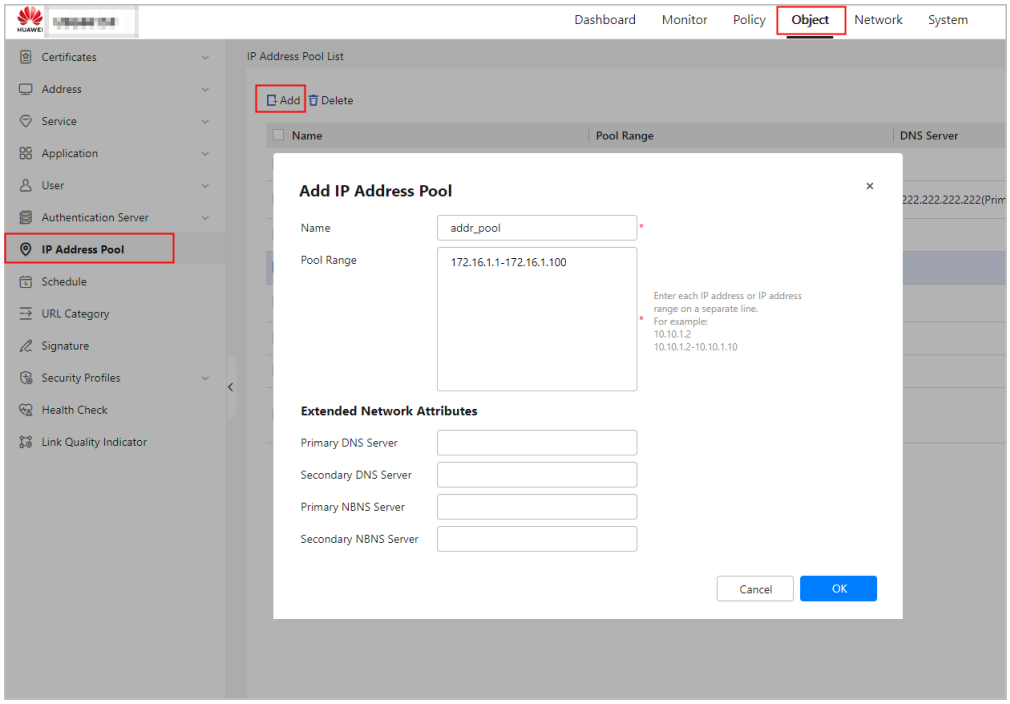
2. Click **OK**.
3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   Create the user **abc** with the password **Helloworld@135**.

 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.
5. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

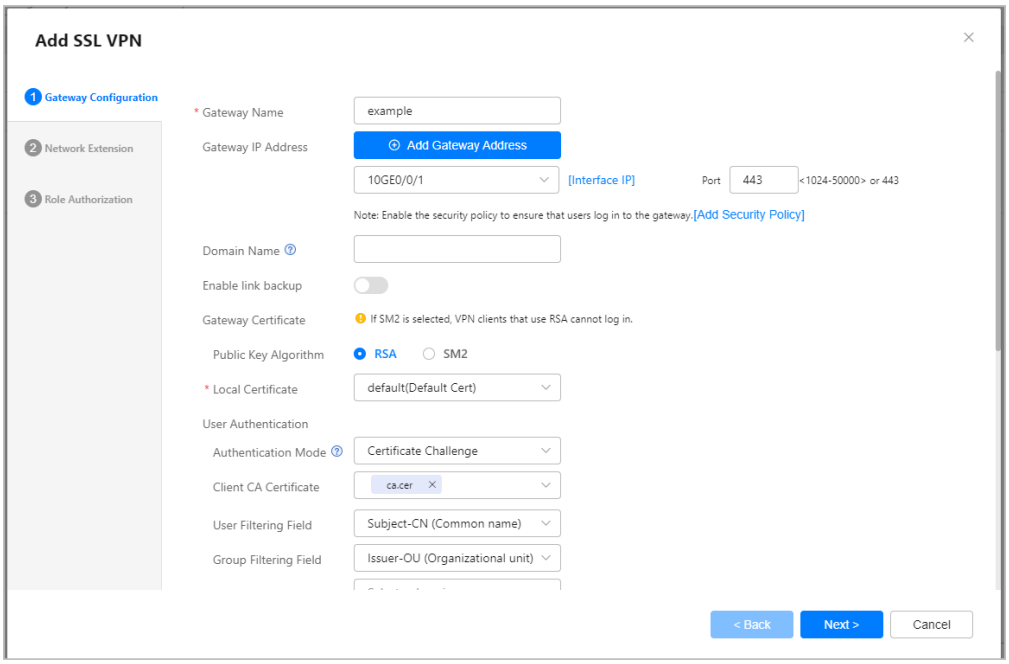


6. Click **OK**.

Step 5 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add**, set the authentication mode of the virtual gateway to certificate-challenge authentication, and set the client CA certificate used by the virtual gateway. You can use the default session timeout interval and life cycle.

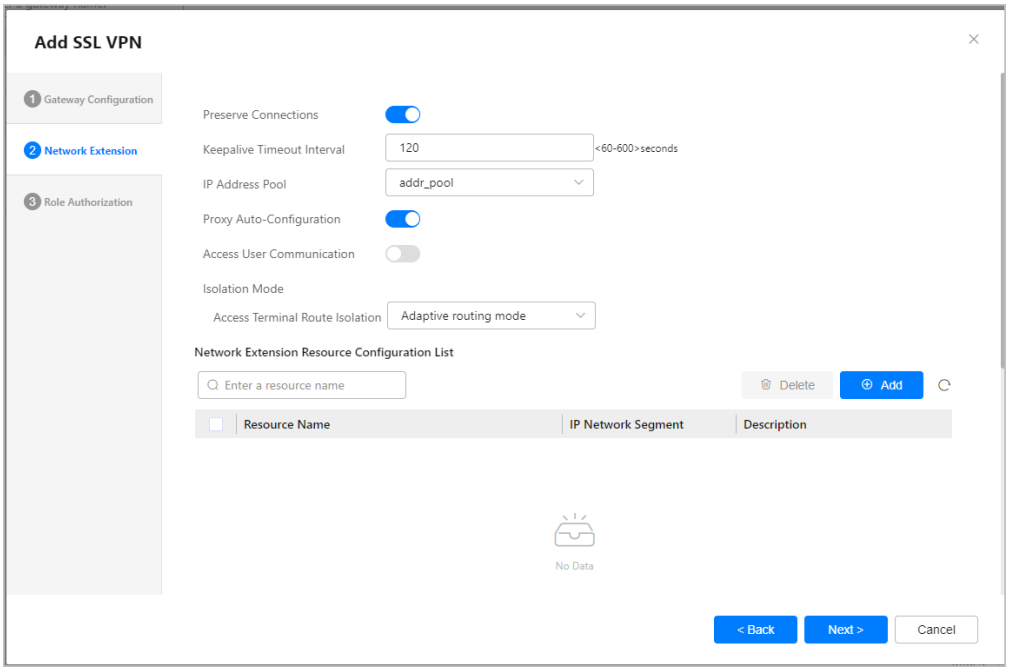
 Copyright © Huawei Technologies Co., Ltd.



3. Click **Next**.

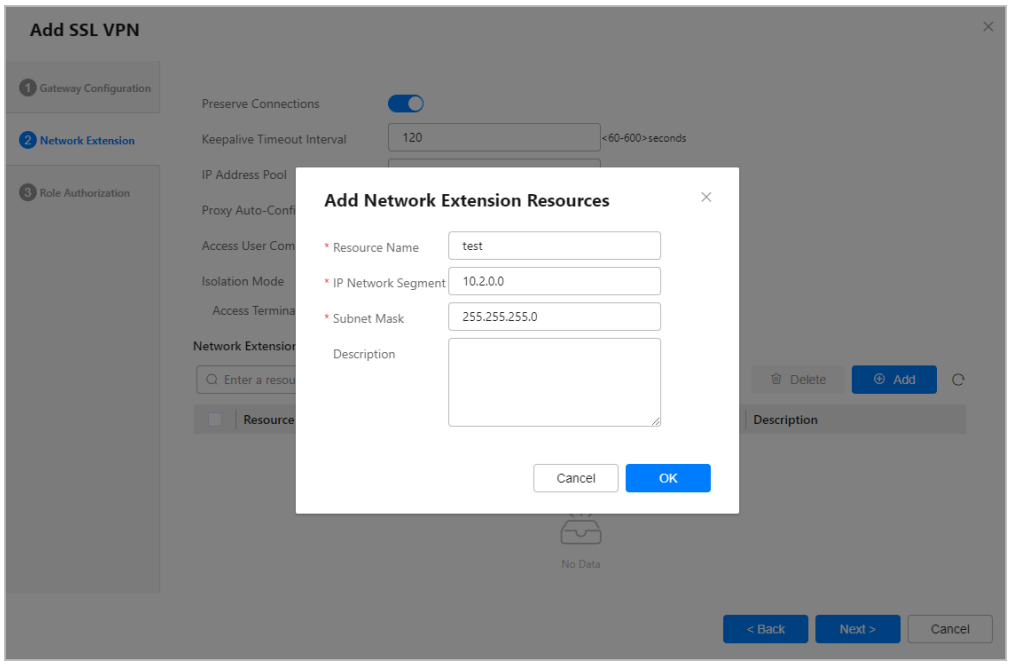
Step 6 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

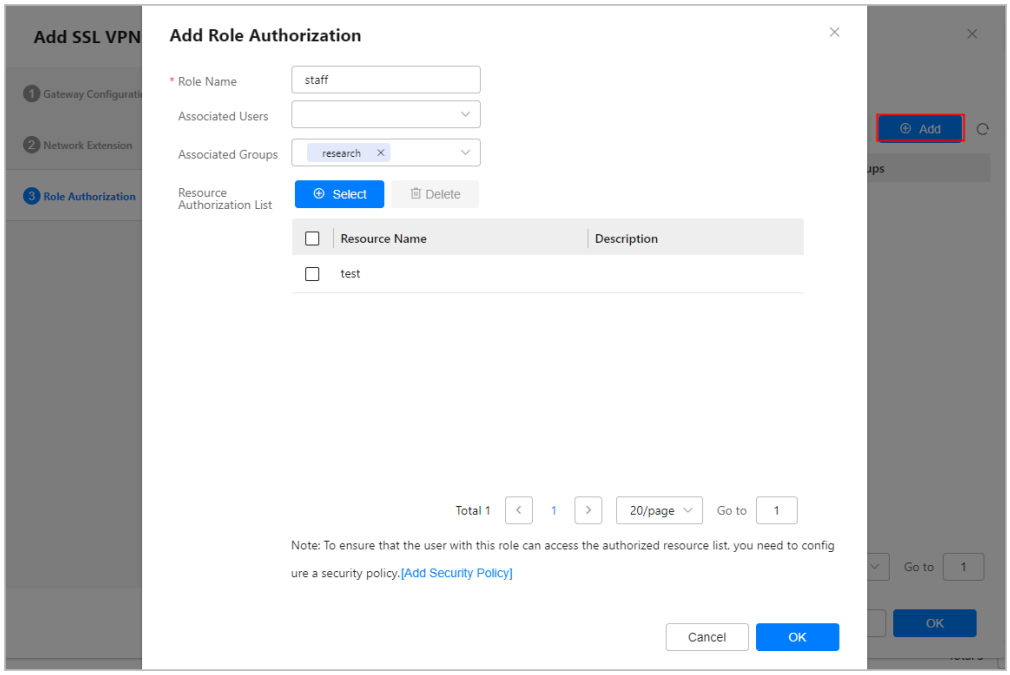
 Copyright © Huawei Technologies Co., Ltd.



3. Click **Next**.

Step 7 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.



2. Click **OK**.

Step 8 Click **OK**. An SSL VPN is created.

----End

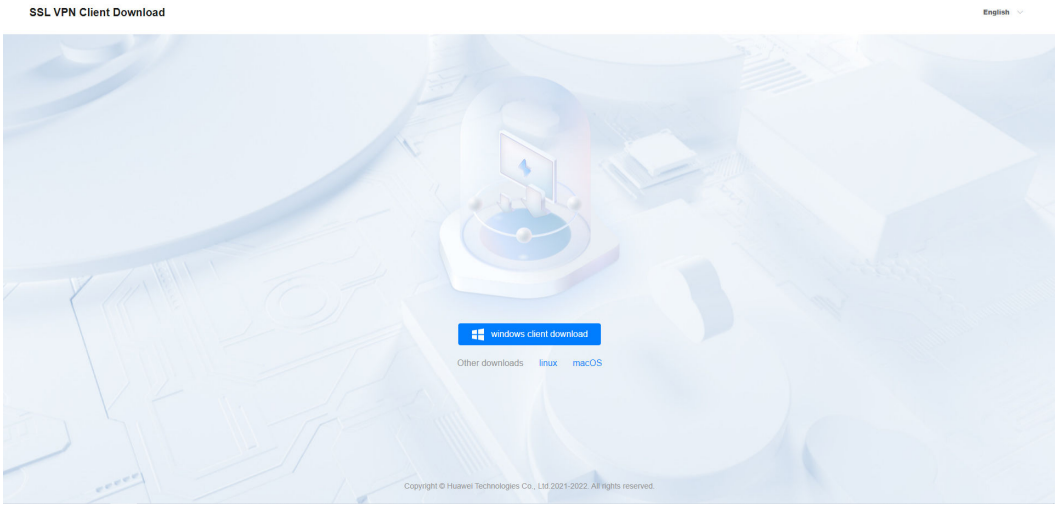
Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install

 Copyright © Huawei Technologies Co., Ltd.

the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

Figure 9-12 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name research index 1
#
aaa
 local-access-user abc
  service-type sslvpn
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-address 10.2.0.0 mask 255.255.255.0
 action permit
#
virtual-gateway example 0
 service address interface GE0/0/1 port 443
 security
  authentication-mode cert-challenge
  client-ca-certificate ca.cer
  cert-anonymous cert-field user-filter subject common-name group-filter issuer organization-unit
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
 role staff 0
  group research
  resource test
#
return
```

9.7 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + AD Authorization)

Networking Requirements

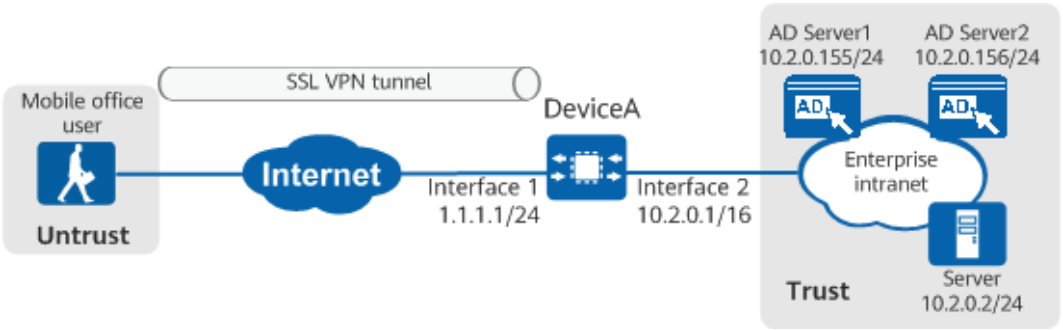
On the enterprise network shown in the following figure, the enterprise authenticates access users through the AD server. Authenticated users can access the enterprise intranet.

The enterprise wants executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, AD authentication with a user name and password is required. In this example, the IP addresses of the primary and secondary AD servers are 10.2.0.155 and 10.2.0.156 respectively.

Figure 9-13 Network diagram for configuring mobile office users to access the headquarters through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

 Copyright © Huawei Technologies Co., Ltd.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface GE0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 16
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.0 24
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 16
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the AD server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.2.0.155 32
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.2.0.156 32
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This example uses server authorization. That is, the device obtains the security group to which a user belongs from the server and searches for the role corresponding to the security group. Therefore, you need to create a security group with the same name as the server on the device. Otherwise, the security group cannot be referenced by the role. The following creates a security group for reference.

The device uses the memberOf attribute value (indicating the group to which a user belongs) of the user on the AD server as the security group name. This attribute value is the same as the name of the security group to be created on the device.

Users are organized by levels on the AD server. If the memberOf attribute of a user has multi-level user group CNs, the device uses only the lowest-level CN value, that is, the first CN value in the attribute, as the security group name. For example, if the memberOf attribute value is **CN=a2,cn=a1,DC=cce,DC=com**, the name of the security group to be created on the device needs to be **a2**.

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Set parameters for communication between the device and AD server. The parameter settings must be the same as those on the AD server.

Configure the AD server template **ad_server**.

```
[DeviceA] ad-server template ad_server
[DeviceA-ad-ad_server] ad-server authentication 10.2.0.155 88 no-ssl
[DeviceA-ad-ad_server] ad-server authentication 10.2.0.156 88 secondary no-ssl
[DeviceA-ad-ad_server] ad-server authentication base-dn dc=cce,dc=com
[DeviceA-ad-ad_server] ad-server authentication manager cn=administrator,cn=users YsHsjx@123
[DeviceA-ad-ad_server] ad-server authentication host-name info-server.cce.com
[DeviceA-ad-ad_server] ad-server authentication host-name info-server2.cce.com secondary
[DeviceA-ad-ad_server] ad-server authentication ldap-port 389  ldap-ssl-port 636
```

Test the connectivity between the device and AD server.

```
[DeviceA-ad-ad_server] test-aaa user_0001 YsHsjx@123 ad-template ad_server
[DeviceA-ad-ad_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

 Copyright © Huawei Technologies Co., Ltd.

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.0.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Configure an authentication domain. Create an authentication scheme and an authorization scheme, set the authentication mode of the authentication scheme to AD authentication, set the authorization mode of the authorization scheme to AD authorization, and apply these schemes to an authentication domain.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme ad
[DeviceA-aaa-authen-ad] authentication-mode ad
[DeviceA-aaa-authen-ad] quit
[DeviceA-aaa] authorization-scheme ad
[DeviceA-aaa-author-ad] authorization-mode ad
[DeviceA-aaa-author-ad] quit
[DeviceA-aaa] domain cce.com
[DeviceA-aaa-domain-cce.com] authentication-scheme ad
[DeviceA-aaa-domain-cce.com] authorization-scheme ad
[DeviceA-aaa-domain-cce.com] ad-server ad_server
[DeviceA-aaa-domain-cce.com] quit
[DeviceA-aaa] quit
```

Set the AAA authentication domain of the virtual gateway to **cce.com**.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain cce.com
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name. For example, if the virtual gateway has been bound to the authentication domain **cce.com**, the user **user_0001** in that authentication domain should enter **user_0001** instead of **user_0001@cce.com** as the user name.

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

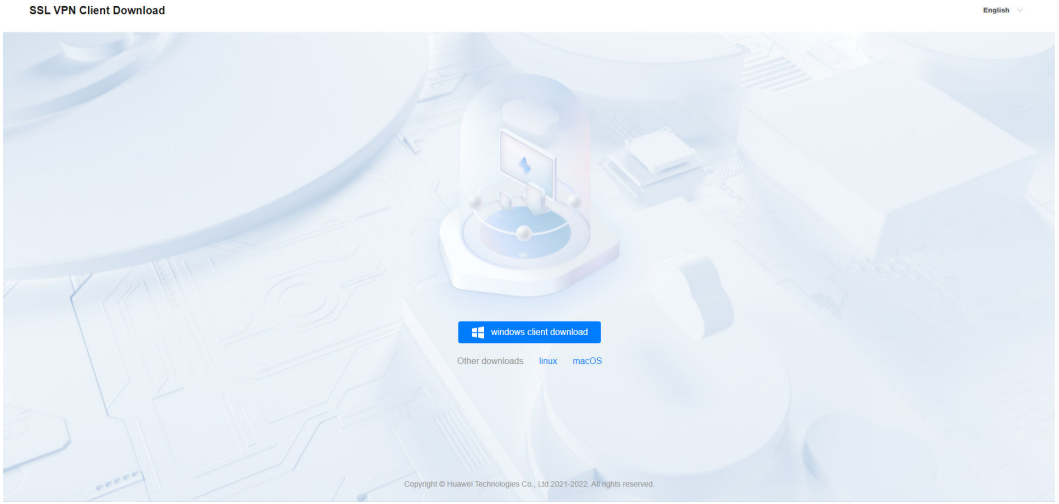
----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-14 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
 authentication-scheme ad
  authentication-mode ad
 authorization-scheme ad
  authorization-mode ad
 domain cce.com
  authentication-scheme ad
  authorization-scheme ad
  accounting-scheme default
  ad-server ad_server



#
ad-server template ad_server
 ad-server authentication base-dn dc=cce,dc=com
 ad-server authentication ldap-port 389 ldap-ssl-port 636
 ad-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW|^it6r))]DA
%1w3lhtdVkOIN<!!!!!2jp5!!!!!!:!!!!(u);AOxJ#E0p-iD71T/0\>bBTc\x@V}/K5Q!!!!!%+%#
 ad-server authentication 10.2.0.155 88 no-ssl
 ad-server authentication host-name info-server.cce.com
 ad-server authentication 10.2.0.156 88 secondary no-ssl
 ad-server authentication host-name info-server2.cce.com secondary
#
interface GE0/0/1
 ip address 1.1.1.0 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
```

```
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
 destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.2.0.155 mask 255.255.255.255
  destination-address 10.2.0.156 mask 255.255.255.255
  action permit
#
virtual-gateway example 1
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain cce.com
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.8 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + AD Authorization)

Networking Requirements

On the enterprise network shown in the following figure, the enterprise authenticates access users through the AD server. Authenticated users can access the enterprise intranet.

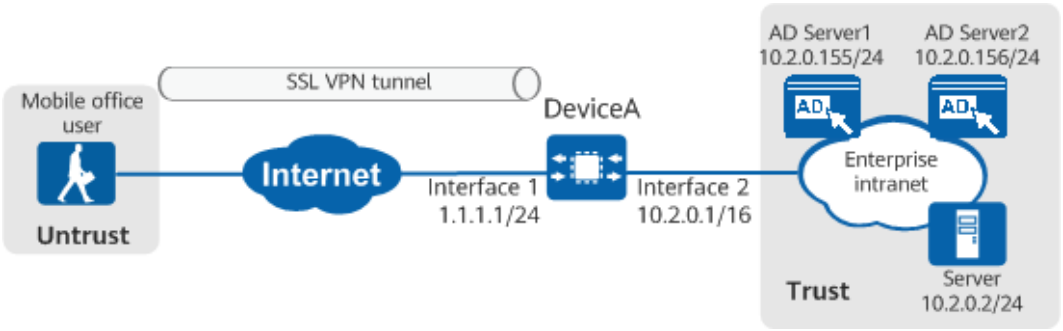
The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, AD authentication with a user name and password is required. In this example, the IP addresses of the primary and secondary AD servers are 10.2.0.155 and 10.2.0.156 respectively.

Figure 9-15 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Configure an IP address for GE 0/0/2 and add it to a security zone.
   a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/16

   b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local

 Copyright © Huawei Technologies Co., Ltd.

Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.1/16
Action	Permit

5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the AD server.

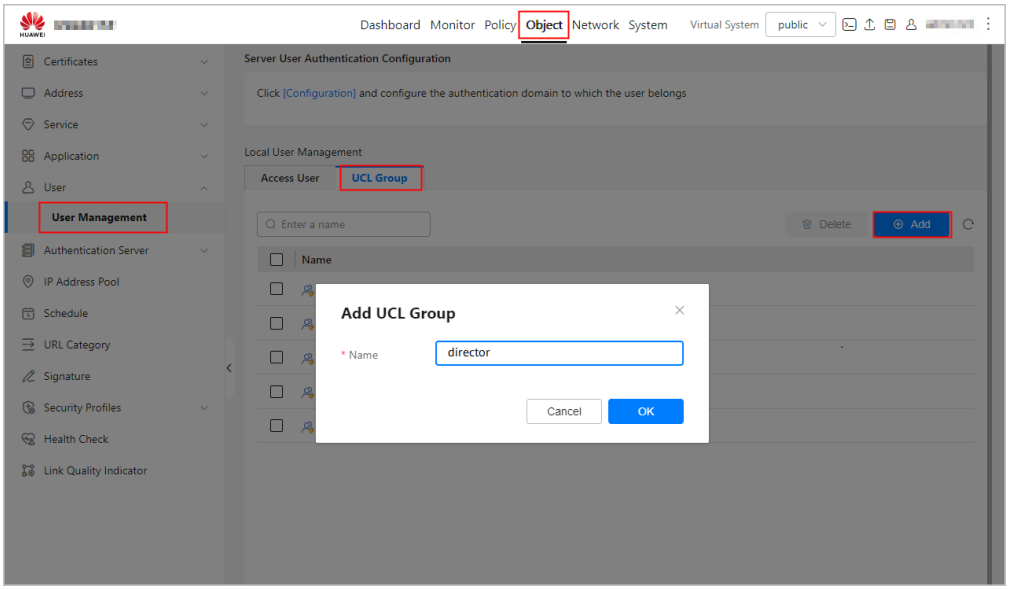
Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.2.0.155/32, 10.2.0.156/32
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

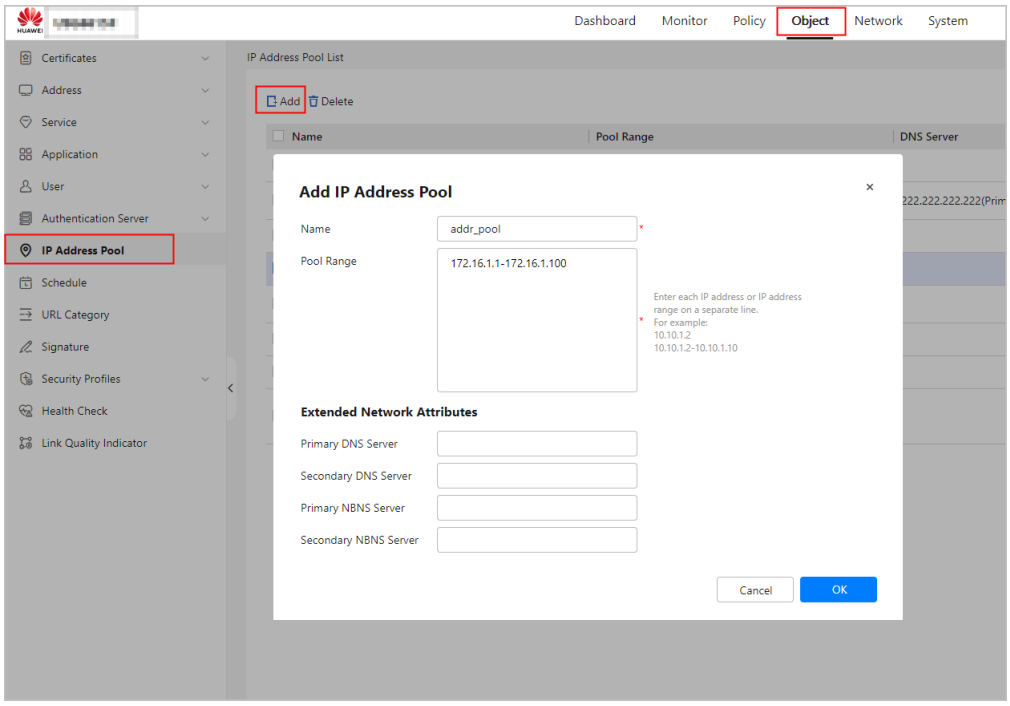
This example uses server authorization. That is, the device obtains the security group to which a user belongs from the server and searches for the role corresponding to the security group. Therefore, you need to create a security group with the same name as the server on the device. Otherwise, the security group cannot be referenced by the role. The following creates a security group for reference.

The device uses the memberOf attribute value (indicating the group to which a user belongs) of the user on the AD server as the security group name. This attribute value is the same as the name of the security group to be created on the device.

Users are organized by levels on the AD server. If the memberOf attribute of a user has multi-level user group CNs, the device uses only the lowest-level CN value, that is, the first CN value in the attribute, as the security group name. For example, if the memberOf attribute value is **CN=a2,cn=a1,DC=cce,DC=com**, the name of the security group to be created on the device needs to be **a2**.

2. Click **OK**.
3. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

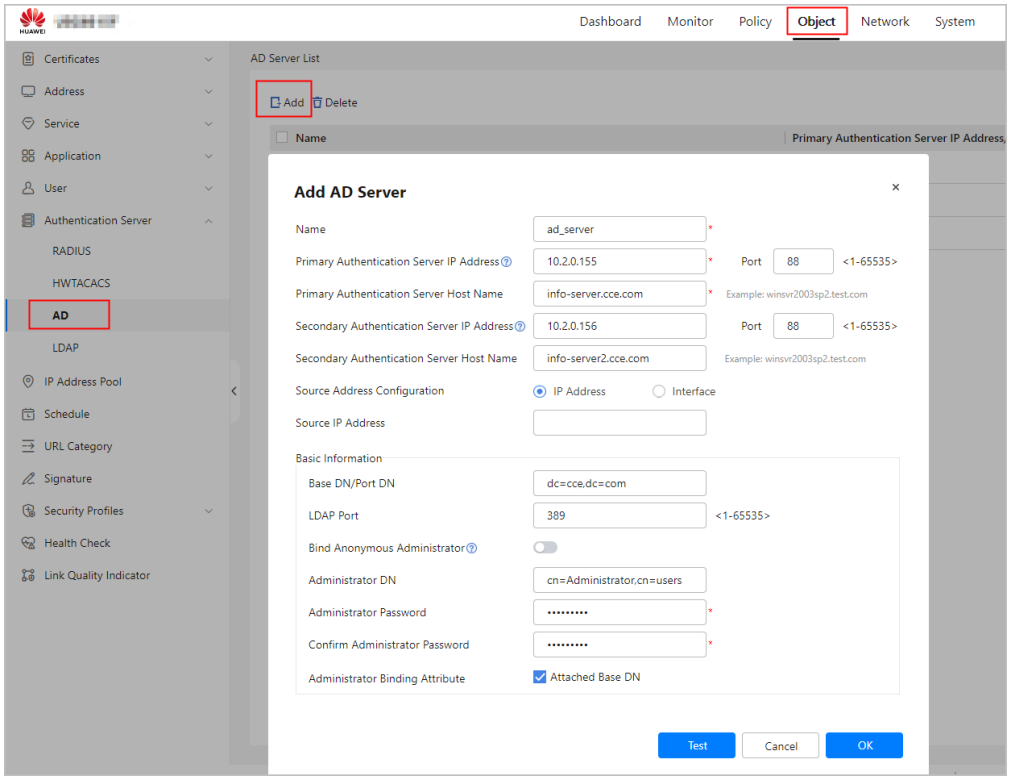
 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **AD**, click **Add**, and set the following parameters to configure the AD server.

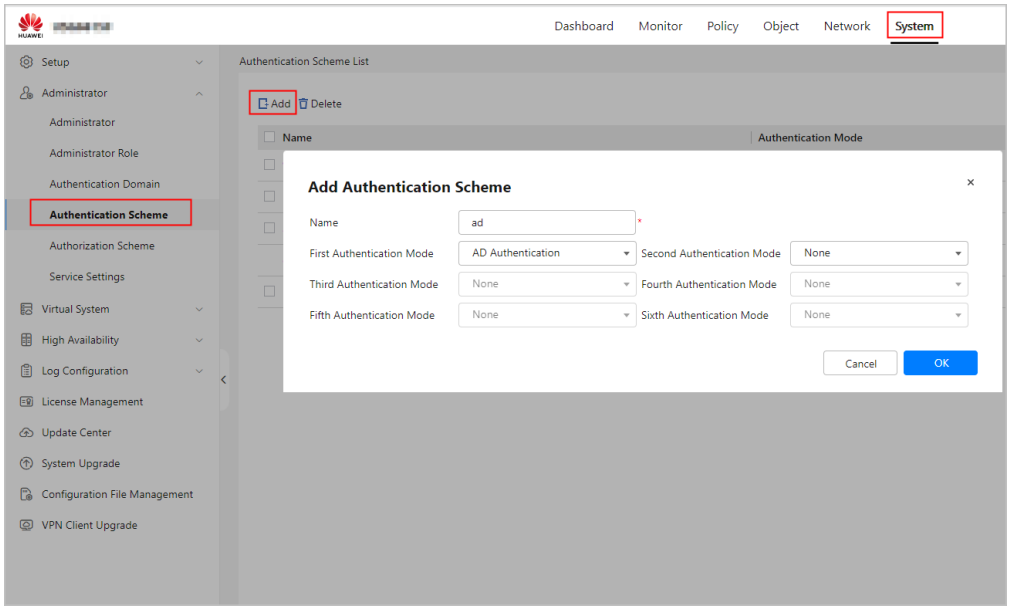


2. Click **OK**.

Step 5 Configure an authentication scheme.

 Copyright © Huawei Technologies Co., Ltd.

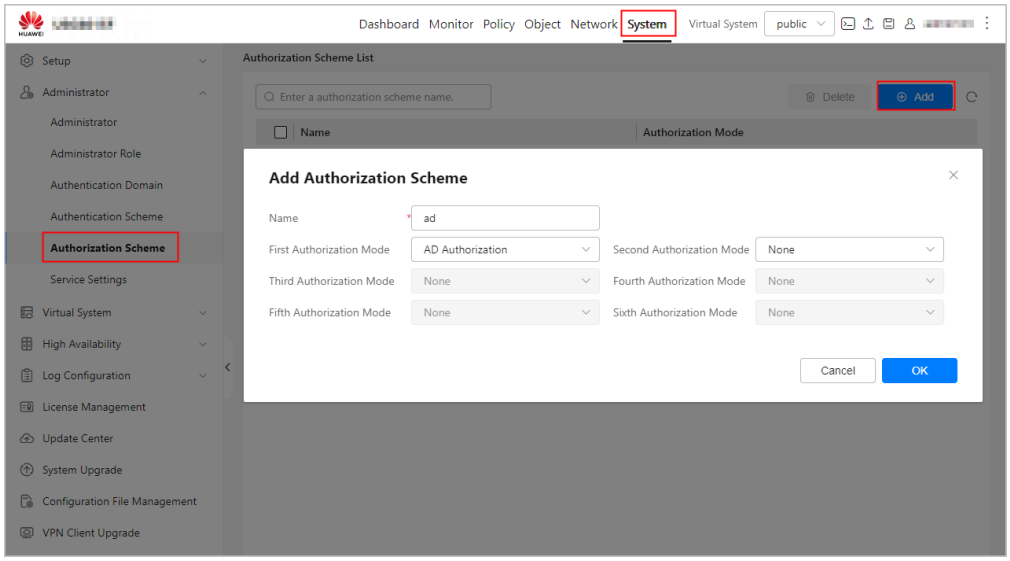
1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.



2. Click **OK**.

Step 6 Configure an authorization scheme.

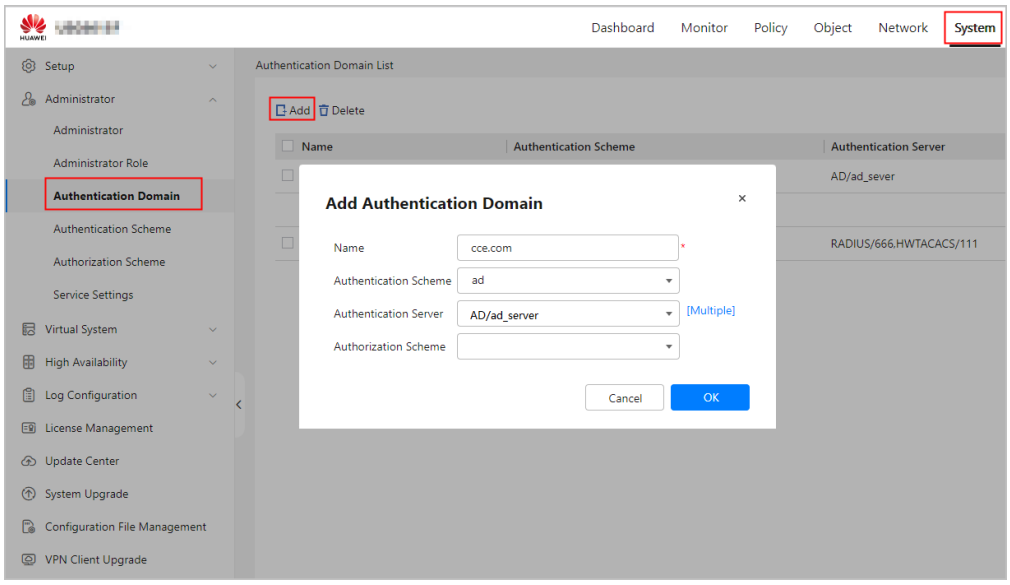
1. Choose **System** > **Administrator** > **Authorization Scheme**, click **Add**, and set the following parameters to configure an authorization scheme.



2. Click **OK**.

Step 7 Configure an authentication domain.

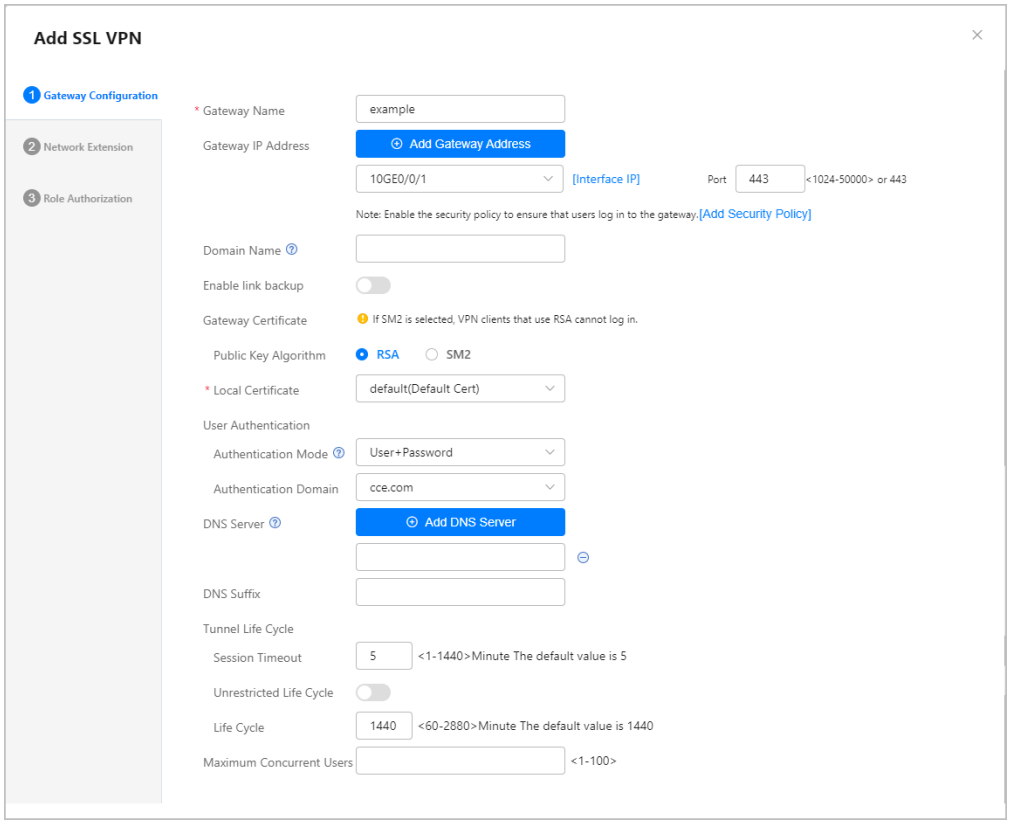
1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.



2. Click **OK**.

Step 8 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

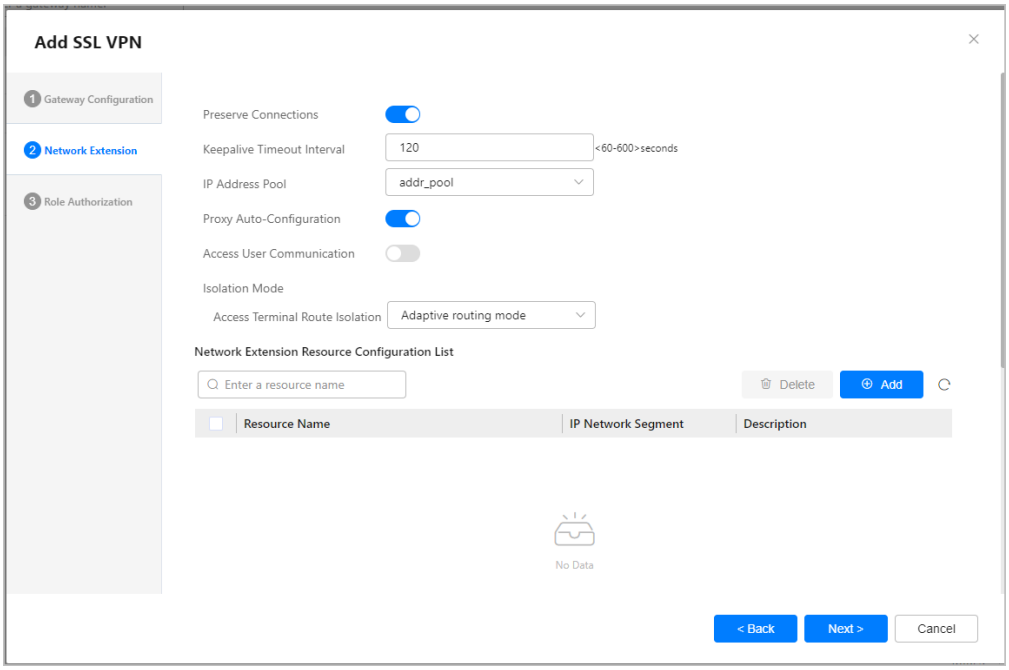


3. Click **Next**.

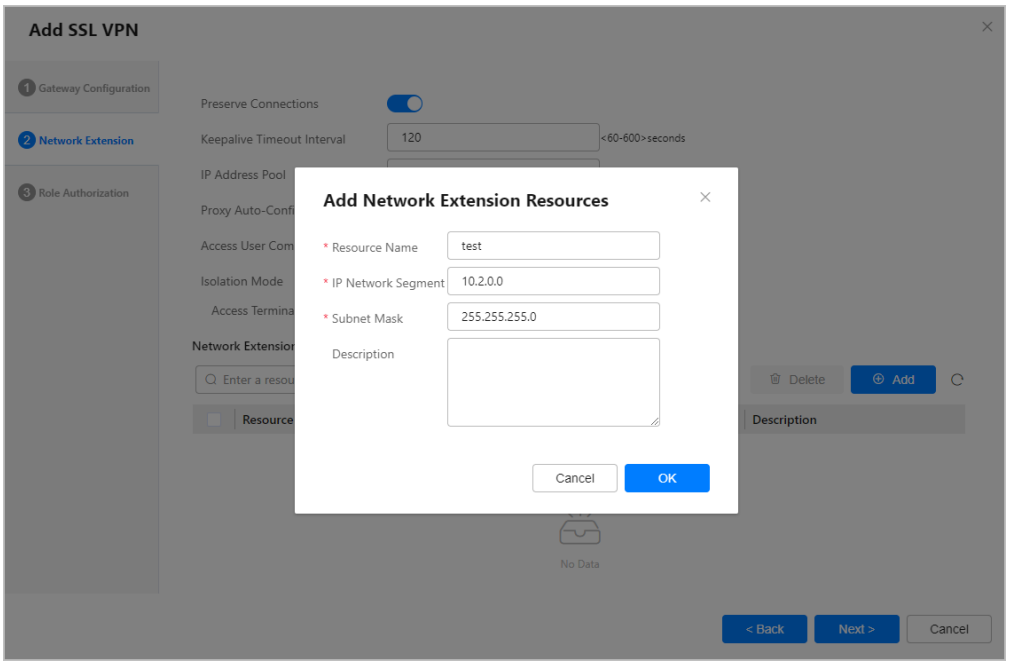
Step 9 Configure the network extension function.

 Copyright © Huawei Technologies Co., Ltd.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

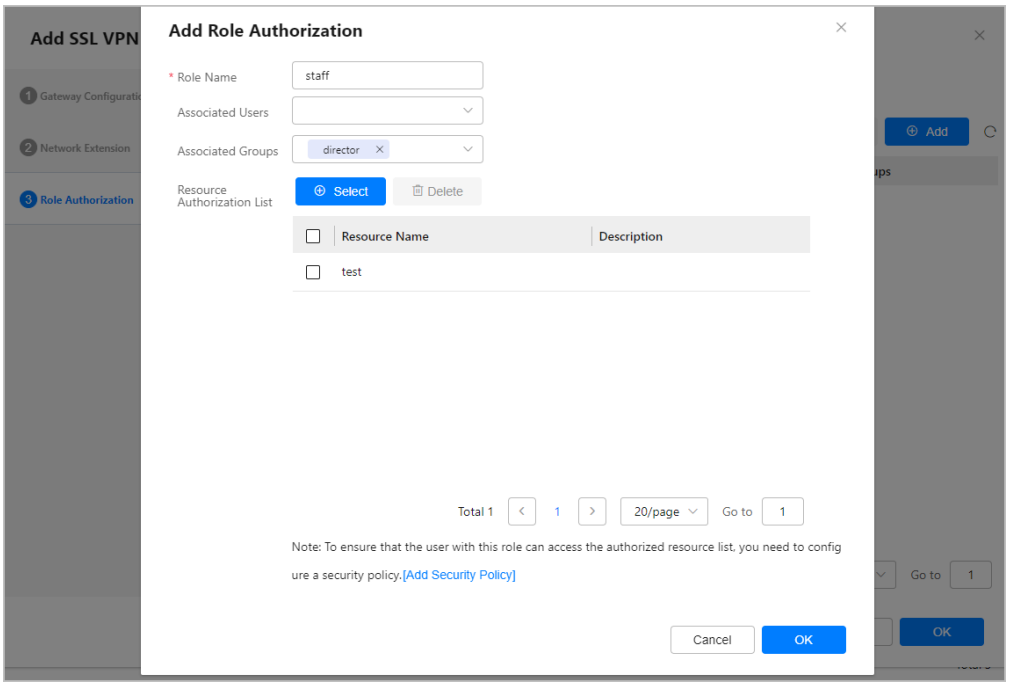


3. Click **Next**.

Step 10 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

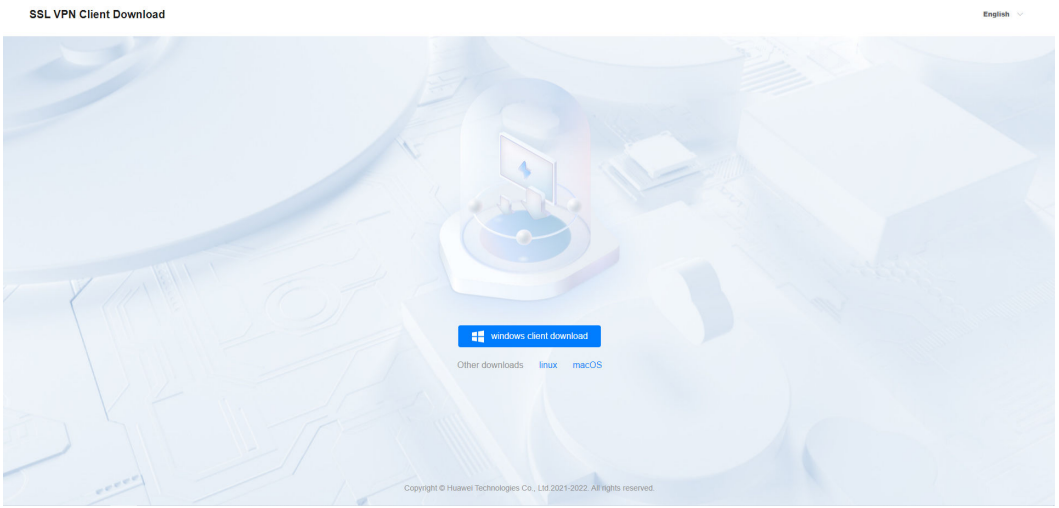
Step 11 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-16 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
 authentication-scheme ad
  authentication-mode ad
 authorization-scheme ad
  authorization-mode ad
 domain cce.com
  authentication-scheme ad
  authorization-scheme ad
  accounting-scheme default
  ad-server ad_server



#
ad-server template ad_server
 ad-server authentication base-dn dc=cce,dc=com
 ad-server authentication ldap-port 389 ldap-ssl-port 636
 ad-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW|^it6r))]DA
%1w3IhtdVkOIN<!!!!!2jp5!!!!!!:!!!!(u);AOxJ#E0p-iD71T/0\>bBTc\x@V}/K5Q!!!!!%+%#
 ad-server authentication 10.2.0.155 88 no-ssl
 ad-server authentication host-name info-server.cce.com
 ad-server authentication 10.2.0.156 88 secondary no-ssl
 ad-server authentication host-name info-server2.cce.com secondary
#
interface GE0/0/1
 ip address 1.1.1.0 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
 destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address  172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.2.0.155 mask 255.255.255.255
  destination-address 10.2.0.156 mask 255.255.255.255
  action permit
#
virtual-gateway example 1
 service address interface GE0/0/1 port 443
 security
```

 Copyright © Huawei Technologies Co., Ltd.

```
 authentication-domain cce.com
service
 network-extension ip-pool addr_pool
 network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
role staff 0
 group director
 resource test
#
return
```

9.9 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + Local Authorization)

Networking Requirements

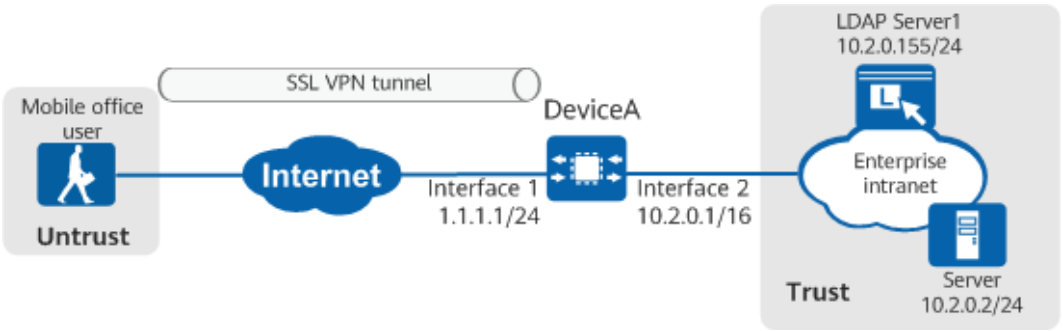
On the enterprise network shown in the following figure, the enterprise authenticates access users through the LDAP server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, LDAP authentication with a user name and password is required. In this example, the IP address of the LDAP server is 10.2.0.155.

Figure 9-17 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface GE0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 16
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 16
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the LDAP server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.2.0.155 32
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Set parameters for communication between the device and LDAP server. The parameter settings must be the same as those on the LDAP server.

NOTE

The device supports AD LDAP, IBM Tivoli LDAP, Sun ONE LDAP, and Open LDAP servers. The following uses the Sun ONE LDAP server as an example.

 Copyright © Huawei Technologies Co., Ltd.

Configure the LDAP server template **ldap_server**.

```
[DeviceA] ldap-server template ldap_server
[DeviceA-ldap-ldap_server] ldap-server server-type sun-one
[DeviceA-ldap-ldap_server] ldap-server authentication 10.2.0.155 389 no-ssl
[DeviceA-ldap-ldap_server] ldap-server authentication base-dn dc=cce,dc=com
[DeviceA-ldap-ldap_server] ldap-server authentication manager cn=administrator,cn=users YsHsjx@123
```

Test the connectivity between the device and LDAP server.

```
[DeviceA-ldap-ldap_server] test-aaa user_0001 YsHsjx@123 ldap-template ldap_server
[DeviceA-ldap-ldap_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.0.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the AAA authentication domain of the virtual gateway to **cce.com**.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain cce.com
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name. For example, if the virtual gateway has been bound to the authentication domain **cce.com**, the user **user_0001** in that authentication domain should enter **user_0001** instead of **user_0001@cce.com** as the user name.

Configure an authentication domain. Create an authentication scheme, set the authentication mode to LDAP authentication, and apply the scheme to an authentication domain.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme ldap
[DeviceA-aaa-authentication-ldap] authentication-mode ldap
[DeviceA-aaa-authentication-ldap] quit
[DeviceA-aaa] domain cce.com
[DeviceA-aaa-domain-cce.com] authentication-scheme ldap
[DeviceA-aaa-domain-cce.com] ldap-server ldap_server
[DeviceA-aaa-domain-cce.com] quit
[DeviceA-aaa] quit
```

Set the local access user name to **abc**, password to **Helloworld@135**, access type to **sslvpn**, and bind the user to the UCL group **director**.

```
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] password cipher Helloworld@135
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] ucl-group director
[DeviceA-aaa-access-user-abc] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

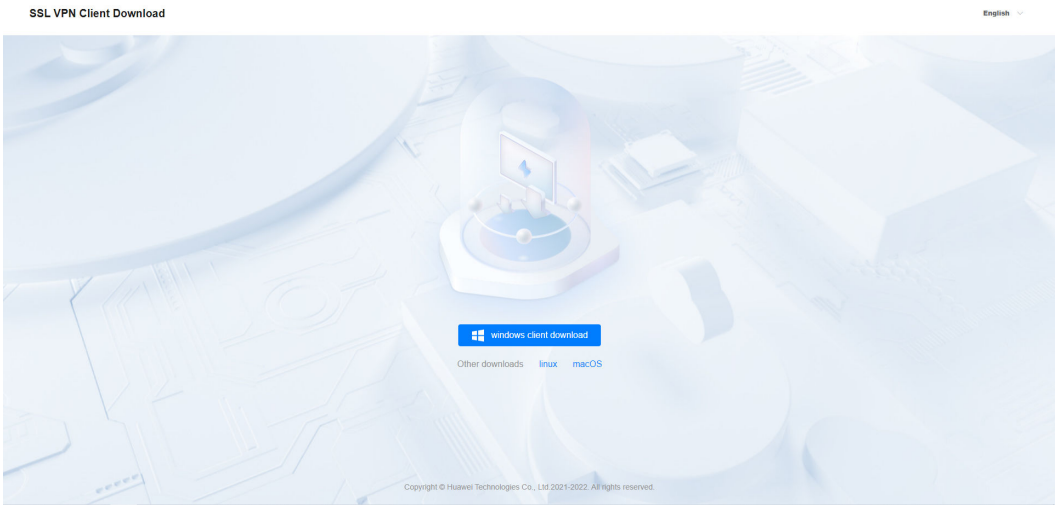
```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-18 Downloading the VPN client installation package from the SSL VPN portal website

2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme ldap
  authentication-mode ldap
  authorization-scheme default
  authorization-mode local
 domain cce.com
  authentication-scheme ldap
  accounting-scheme default
  ldap-server ldap_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
ldap-server template ldap_server
 ldap-server server-type sun-one
 ldap-server authentication base-dn dc=cee,dc=com
 ldap-server authentication 10.2.0.155 389 ssl
 ldap-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!
cZa'*[{[xW[dOX;UfIp4uYisC=ZW(R.t)NE!!!!!2jp5!!!!!!:!!!!Dqsl+`1EBF*rOBF[kt2#%-y-ZG[7_RY`LwU!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.155 mask 255.255.255.255
  action permit
#
virtual-gateway example 1
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain cce.com
 service
  network-extension ip-pool addr_pool
```

 Copyright © Huawei Technologies Co., Ltd.

```
 network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.10 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + Local Authorization)

Networking Requirements

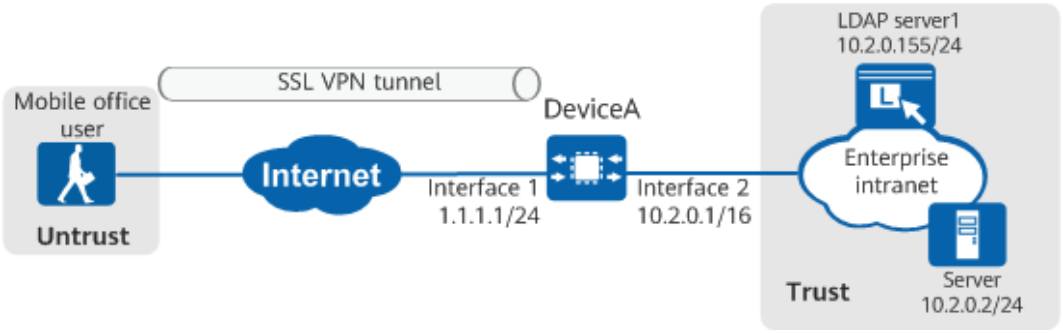
On the enterprise network shown in the following figure, the enterprise authenticates access users through the LDAP server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, LDAP authentication with a user name and password is required. In this example, the IP address of the LDAP server is 10.2.0.155.

Figure 9-19 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Configure an IP address for GE 0/0/2 and add it to a security zone.

a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/16

b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.1/16
Action	Permit

5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the LDAP server.

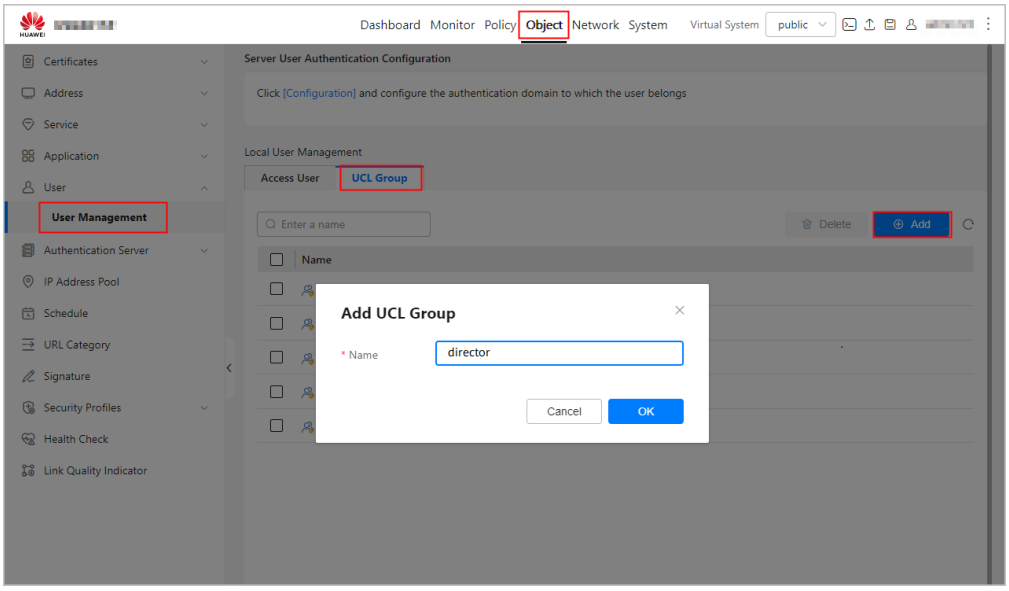
 Copyright © Huawei Technologies Co., Ltd.

Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.2.0.155/32
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

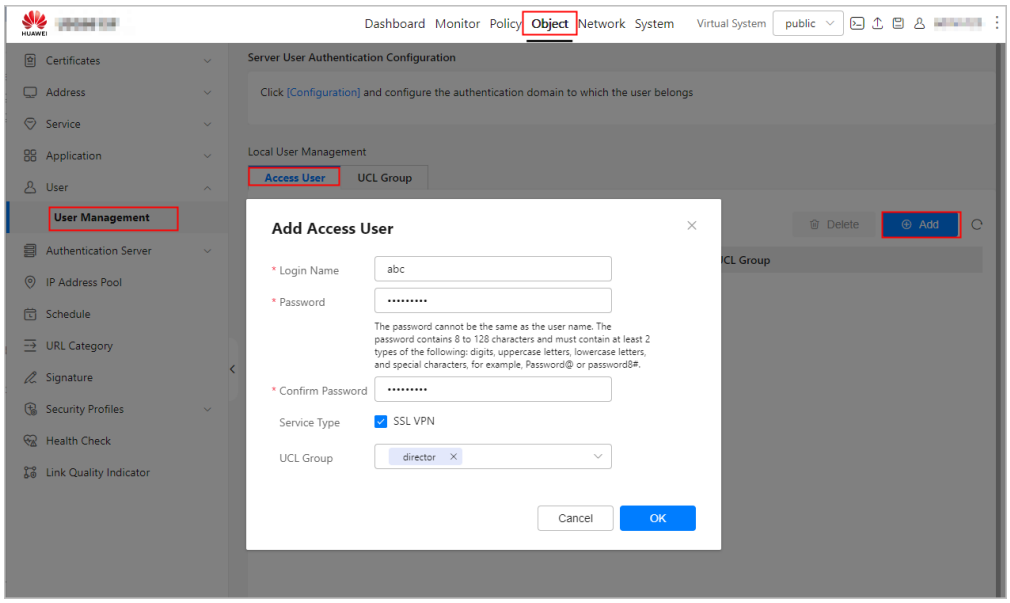
1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.



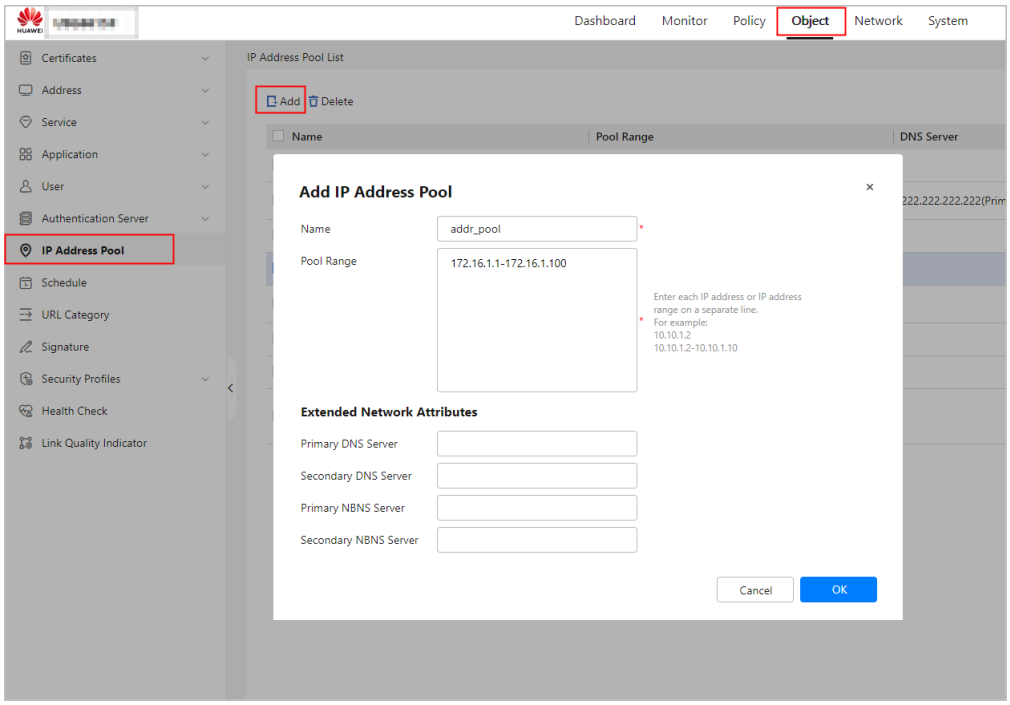
2. Click **OK**.
3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   The user **abc** belongs to the user group **director** and the password is **YsHsjx_202206**.

 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.
5. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

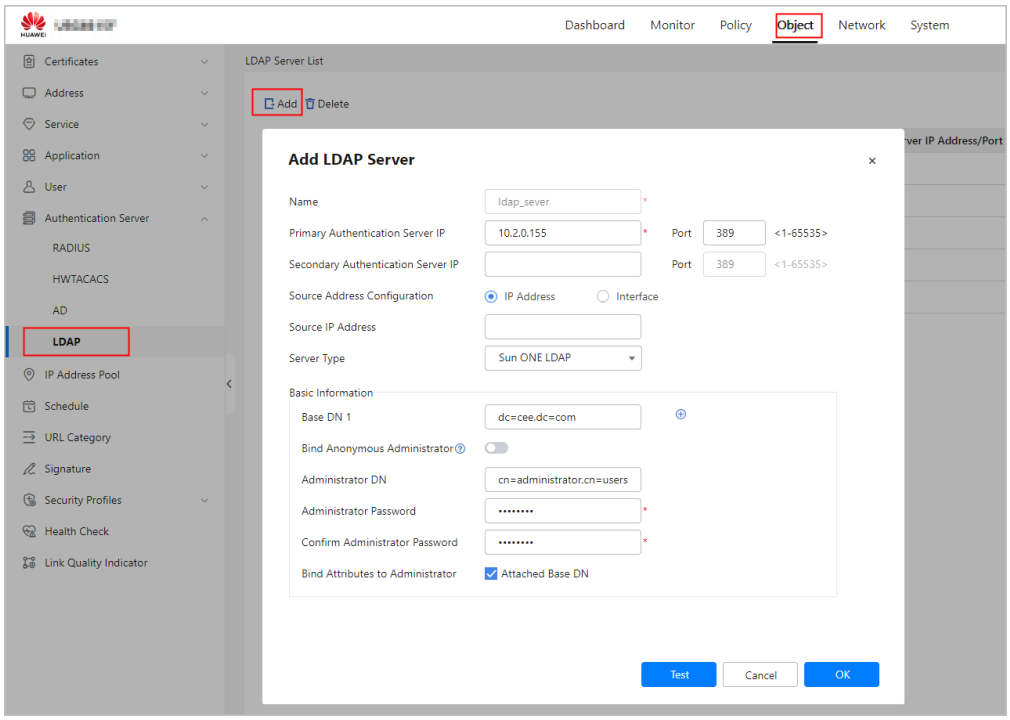


6. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **LDAP**, click **Add**, and set the following parameters to configure the LDAP server.

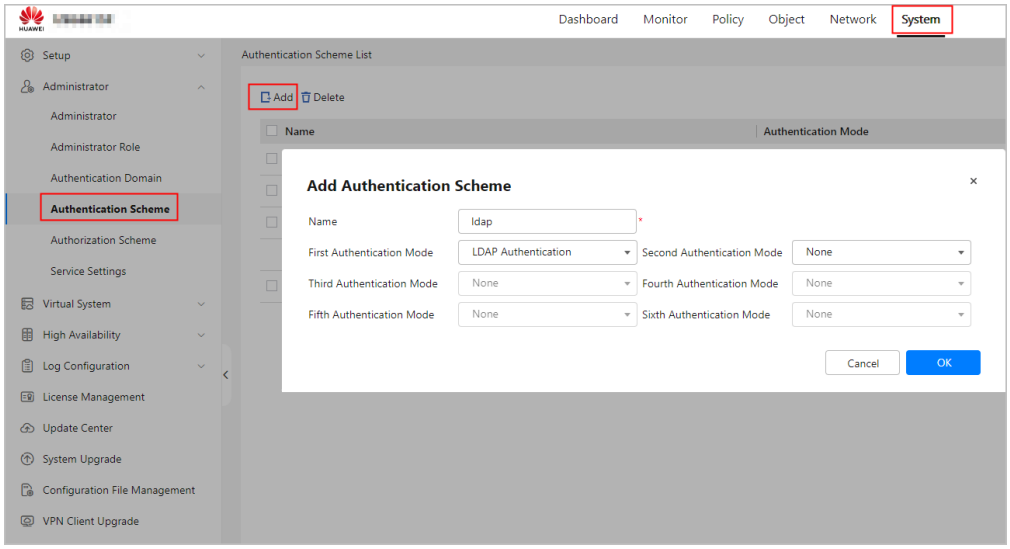
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 5 Configure an authentication scheme.

1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.

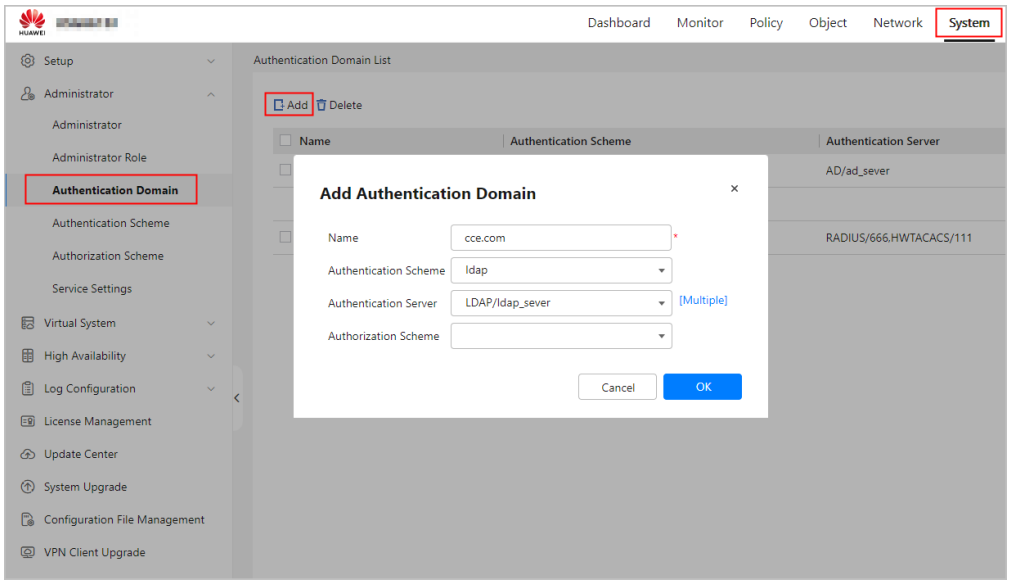


2. Click **OK**.

Step 6 Configure an authentication domain.

1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.

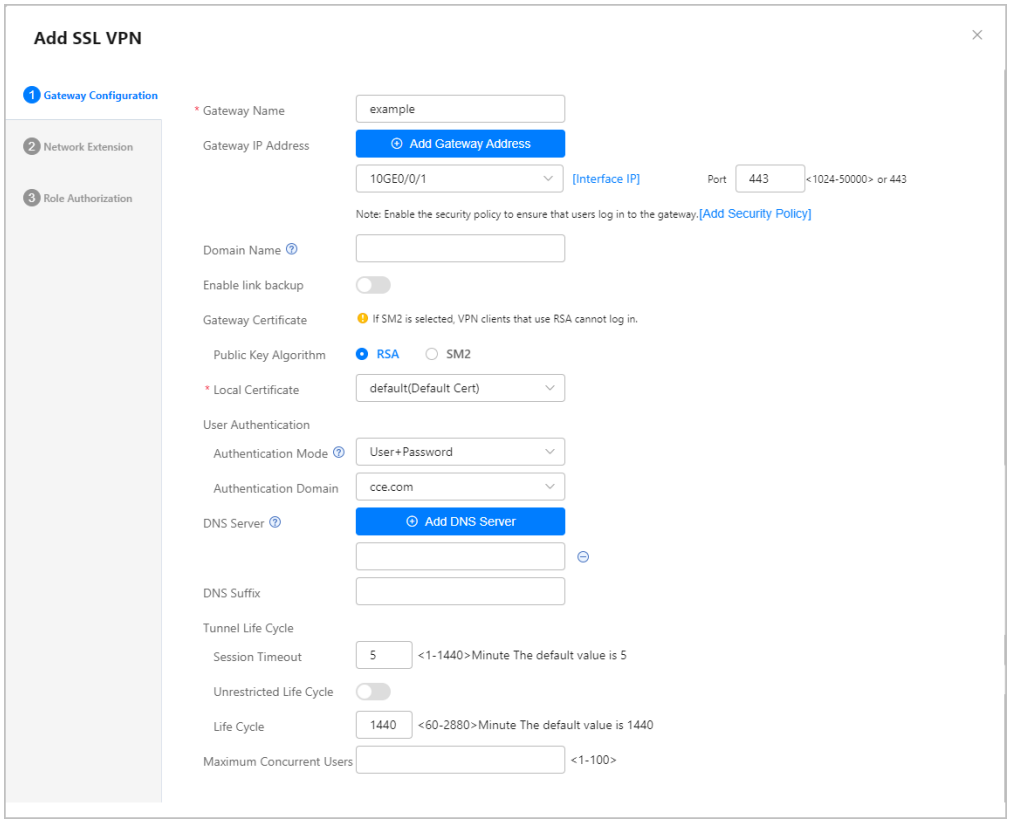
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 7 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

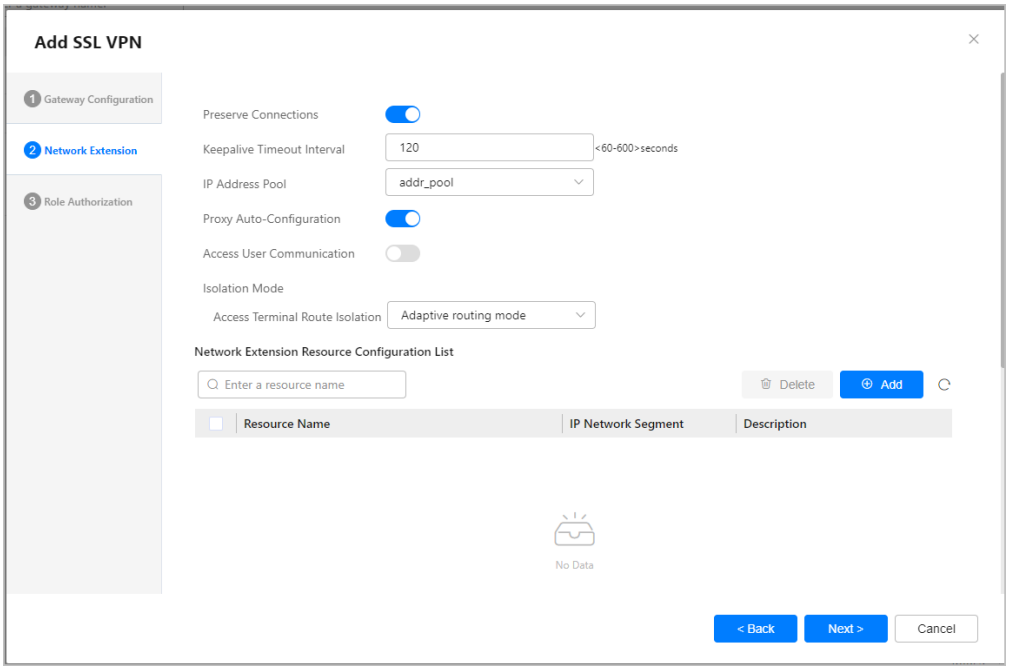


3. Click **Next**.

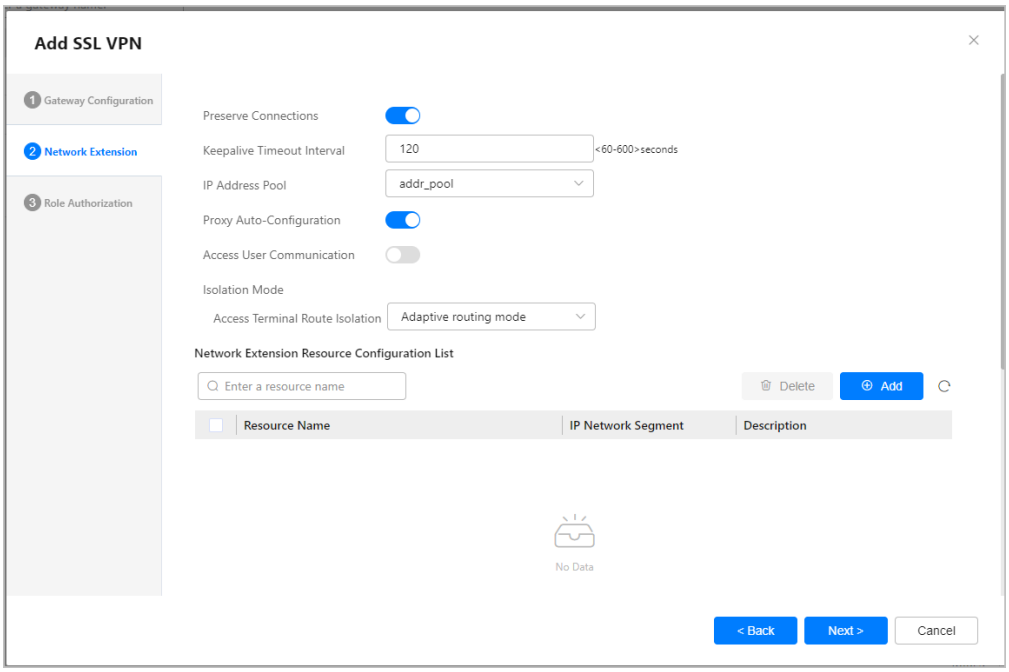
Step 8 Configure the network extension function.

 Copyright © Huawei Technologies Co., Ltd.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

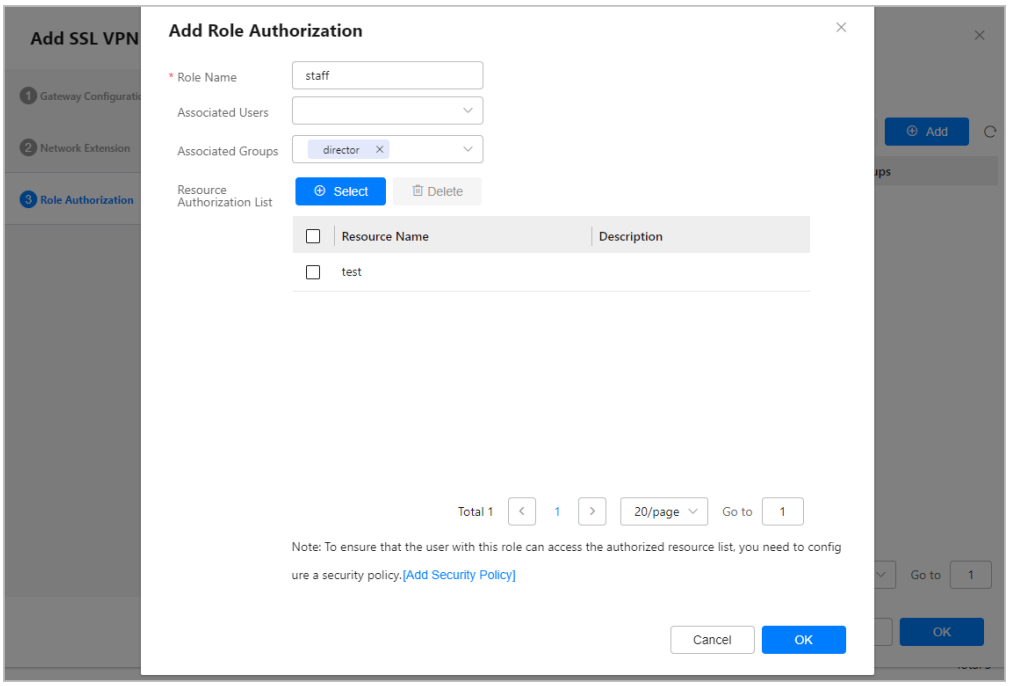


3. Click **Next**.

Step 9 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

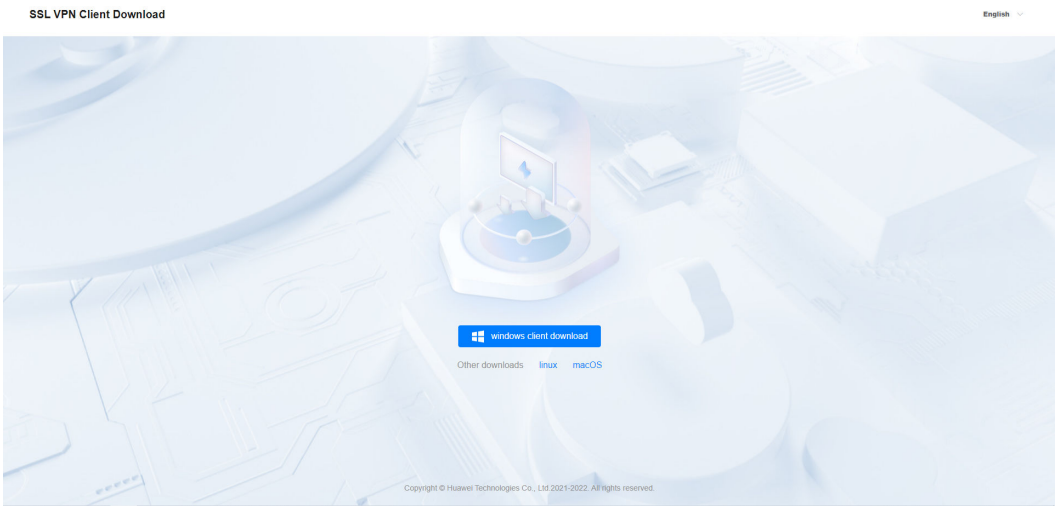
Step 10 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-20 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme ldap
  authentication-mode ldap
  authorization-scheme default
  authorization-mode local
 domain cce.com
  authentication-scheme ldap
  accounting-scheme default
  ldap-server ldap_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
ldap-server template ldap_server
 ldap-server server-type sun-one
 ldap-server authentication base-dn dc=cee,dc=com
 ldap-server authentication 10.2.0.155 389 ssl
 ldap-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!
cZa'*[{[xW[dOX;UfIp4uYisC=ZW(R.t)NE!!!!!2jp5!!!!!!:!!!!Dqsl+`1EBF*rOBF[kt2#%-y-ZG[7_RY`LwU!!!!!%+%#
#
interface 10GE
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface 10GE
#
firewall zone untrust
 set priority 5
 add interface 10GE
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.155 mask 255.255.255.255
  action permit
#
virtual-gateway example 1
 service address interface 10GE port 443
 security
  authentication-domain cce.com
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 role staff 0
  group director
  resource test
#
return
```

9.11 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + Local Authorization)

Networking Requirements

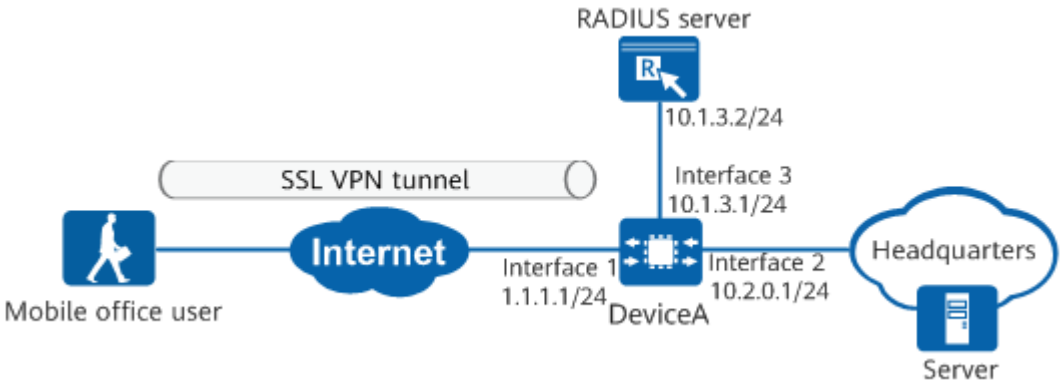
On the enterprise network shown in the following figure, the enterprise authenticates access users through the RADIUS server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, RADIUS authentication with a user name and password is required. In this example, the IP address of the RADIUS server is 10.1.3.2, and IP addresses in the network extension address pool assigned to mobile office users range from 172.16.1.1 to 172.16.1.100.

Figure 9-21 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface GE0/0/1
```

```
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/3.

```
[DeviceA] interface GE0/0/3
[DeviceA-GE0/0/3] ip address 10.1.3.1 24
[DeviceA-GE0/0/3] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 and GE 0/0/3 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] add interface GE0/0/3
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the RADIUS server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.1.3.2 24
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Set parameters for communication between the device and RADIUS server. The parameter settings must be the same as those on the RADIUS server.

Configure the RADIUS server template **radius_server**.

```
[DeviceA] radius-server template radius_server
[DeviceA-radius-radius_server] radius-server authentication 10.1.3.2 1812
[DeviceA-radius-radius_server] radius-server shared-key cipher YsHsjx@123
[DeviceA-radius-radius_server] undo radius-server user-name domain-included
```

Test the connectivity between the device and RADIUS server.

```
[DeviceA-radius-radius_server] test-aaa user_0001 YsHsjx@123 radius-template radius_server
[DeviceA-radius-radius_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.255.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the AAA authentication domain of the virtual gateway to **default**.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain default
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

By default, the authentication domain name of a virtual gateway is extracted from a user name. If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name.

Configure an authentication domain. Create an authentication scheme, set the authentication mode to RADIUS authentication, and apply the scheme to an authentication domain.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme radius
[DeviceA-aaa-authentication-radius] authentication-mode radius
[DeviceA-aaa-authentication-radius] quit
[DeviceA-aaa] domain default
[DeviceA-aaa-domain-default] authentication-scheme radius
[DeviceA-aaa-domain-default] radius-server radius_server
[DeviceA-aaa-domain-default] quit
[DeviceA-aaa] quit
```

Set the local access user name to **abc**, password to **Helloworld@135**, access type to **sslvpn**, and bind the user to the UCL group **director**.

```
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] password cipher Helloworld@135
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] ucl-group director
[DeviceA-aaa-access-user-abc] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

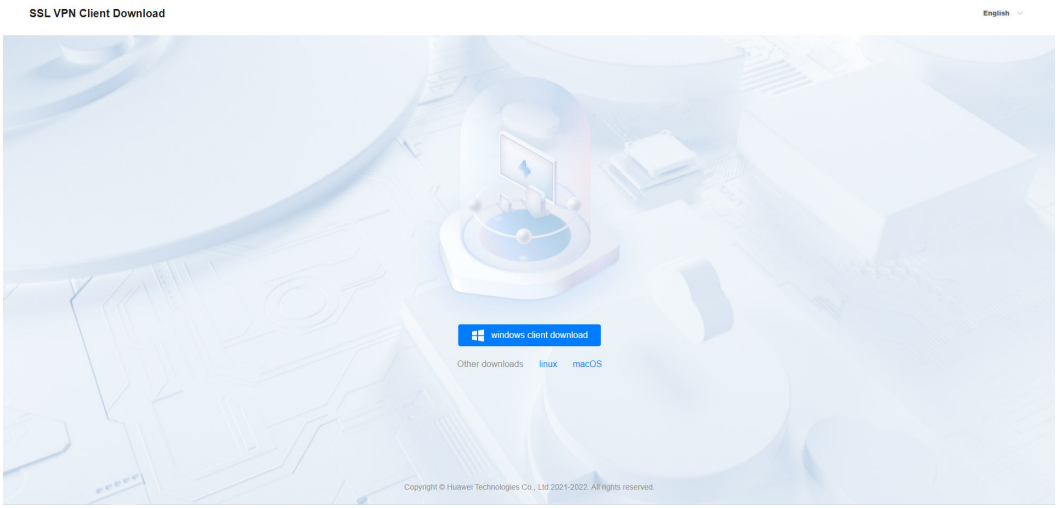
```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-22 Downloading the VPN client installation package from the SSL VPN portal website

2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme radius
  authentication-mode radius
  authorization-scheme default
  authorization-mode local
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server radius_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
radius-server template radius_server
 radius-server shared-key cipher %+%##!!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW&%Ui~]V24G5a|t>k+(m)+Y.0K!!!!!
2jp5!!!!!!:!!!!J=y~T09HG7Q-(u`1p3@X"\>=N~vz&|{~dW!!!!!%+%#
 radius-server authentication 10.1.3.2 1812 weight 80
 undo radius-server user-name domain-included
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 1
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain default
```

 Copyright © Huawei Technologies Co., Ltd.

```
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.12 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + Local Authorization)

Networking Requirements

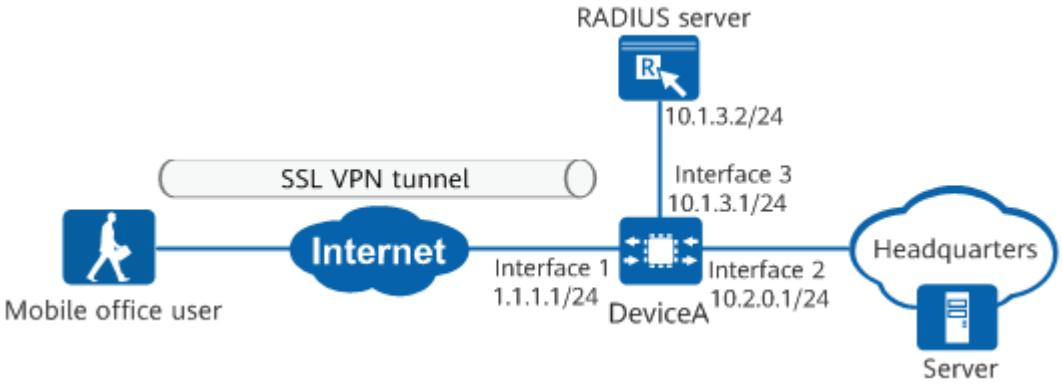
On the enterprise network shown in the following figure, the enterprise authenticates access users through the RADIUS server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, RADIUS authentication with a user name and password is required. In this example, the IP address of the RADIUS server is 10.1.3.2, and IP addresses in the network extension address pool assigned to mobile office users range from 172.16.1.1 to 172.16.1.100.

Figure 9-23 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Configure an IP address for GE 0/0/2 and add it to a security zone.

a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

3. Configure an IP address for GE 0/0/3 and add it to a security zone.

a. In **Interface List**, click in the row of GE 0/0/3 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.1.3.1/24

b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.1 -172.16.1.100
Destination Address	10.2.0.1/24
Action	Permit

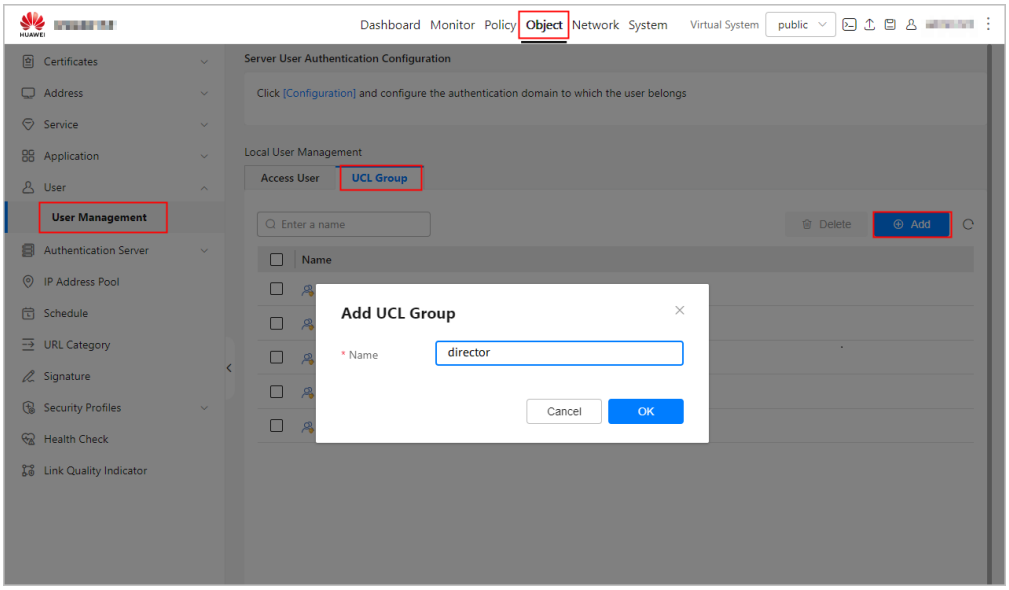
5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the RADIUS server.

Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.1.3.2/24
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.

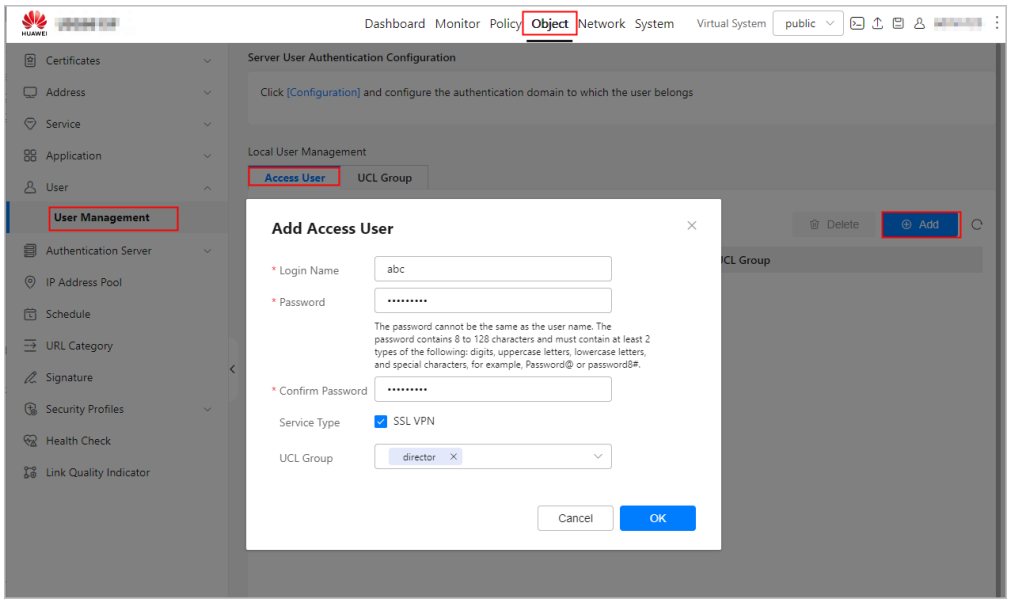


2. Click **OK**.

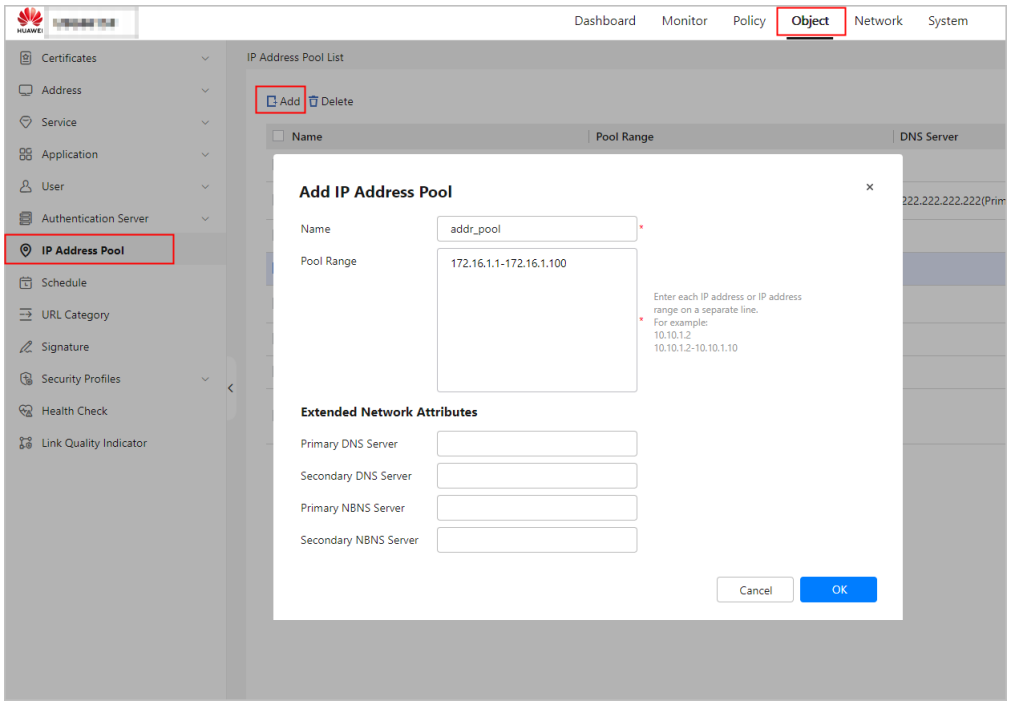
 Copyright © Huawei Technologies Co., Ltd.

3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   The user **abc** belongs to the user group **director** and the password is **YsHsjx_202206**.



4. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

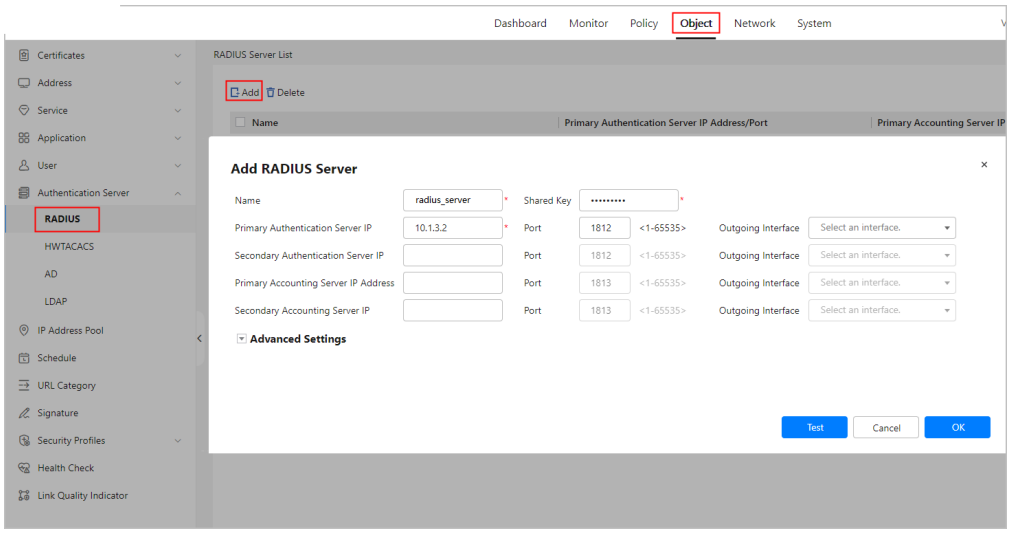


5. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **RADIUS**, click **Add**, and set the following parameters to configure the RADIUS server.

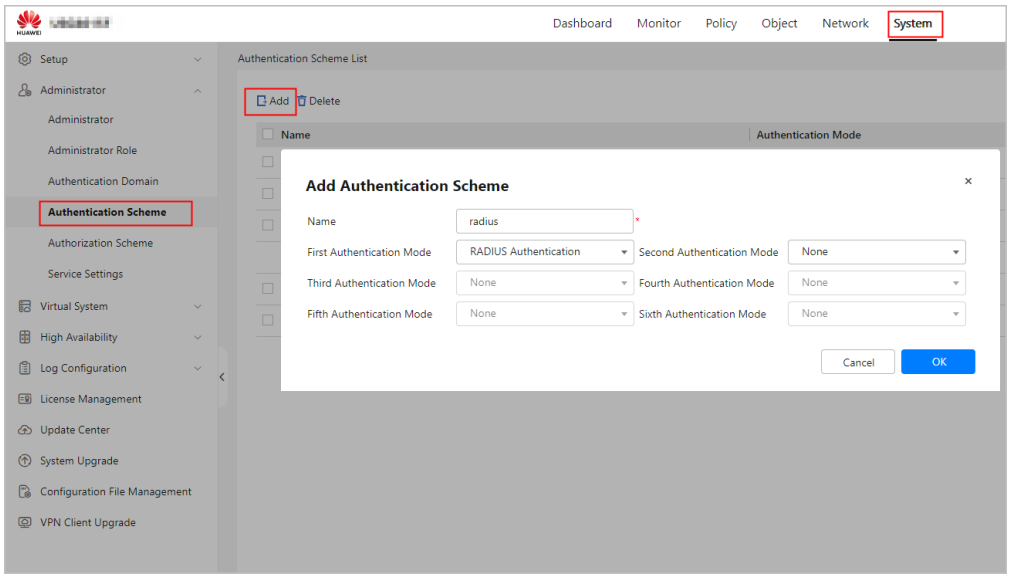
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 5 Configure an authentication scheme.

1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.

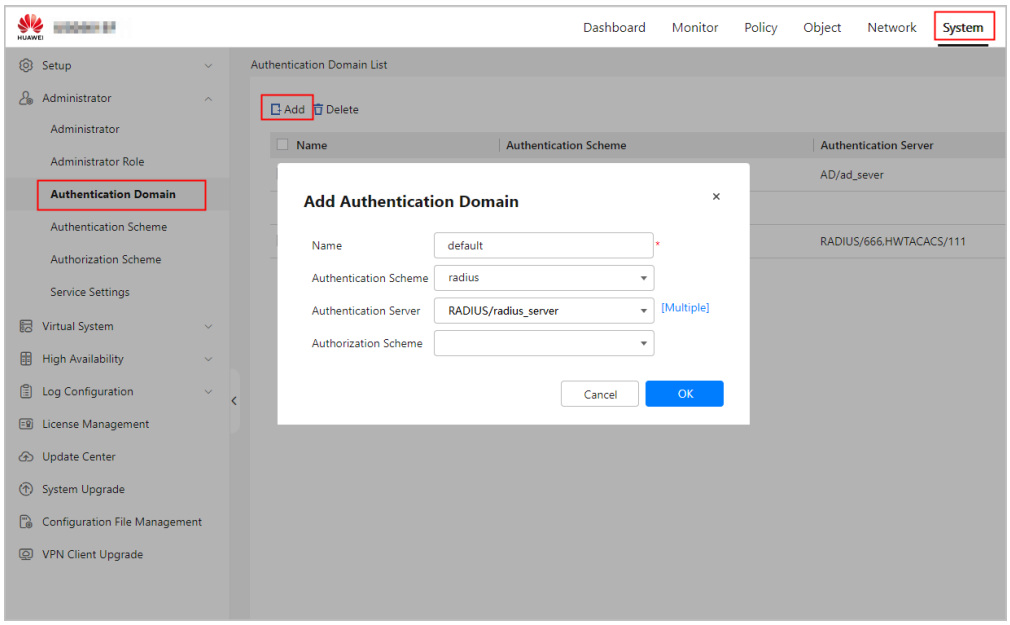


2. Click **OK**.

Step 6 Configure an authentication domain.

1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.

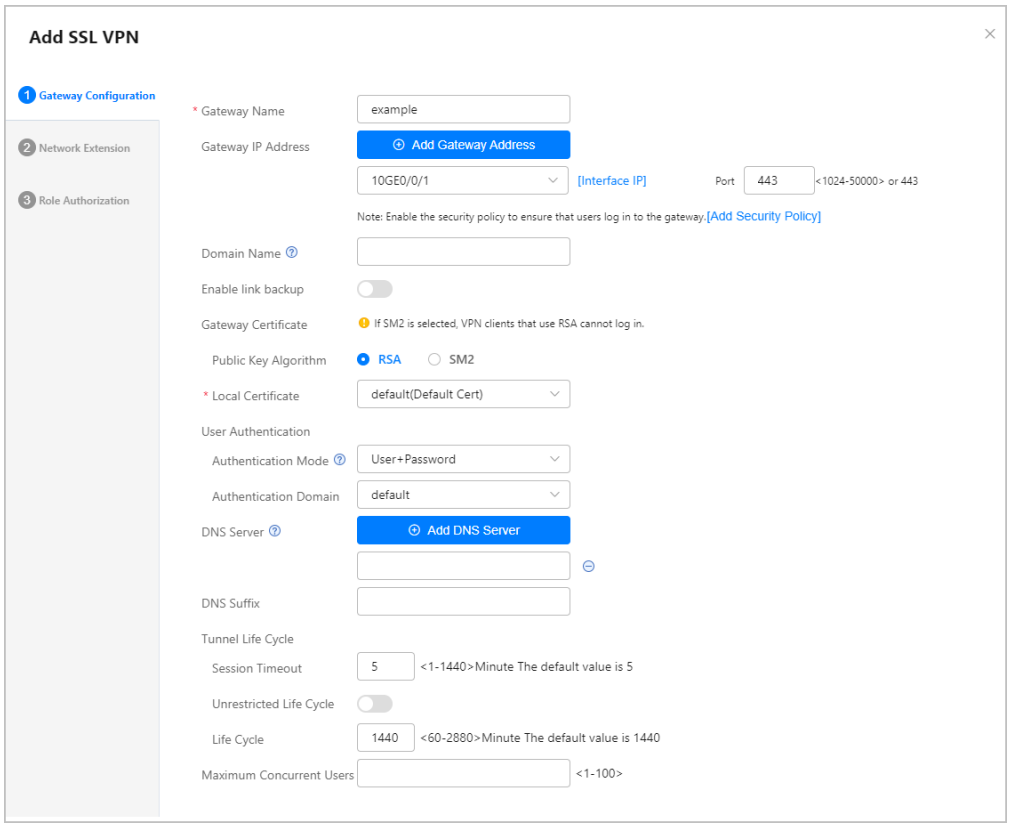
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 7 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

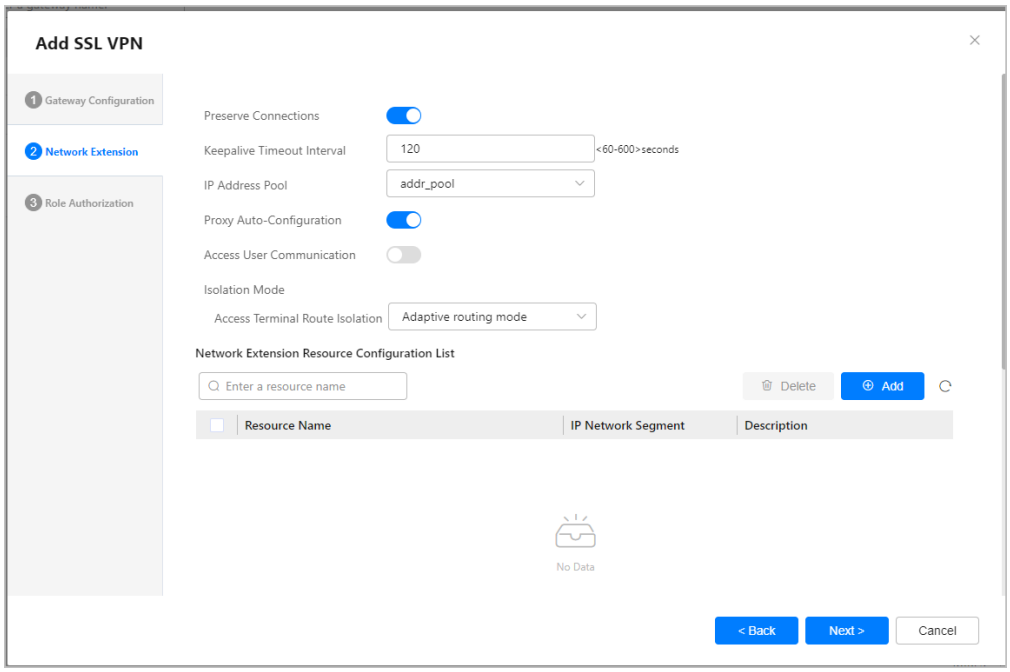


3. Click **Next**.

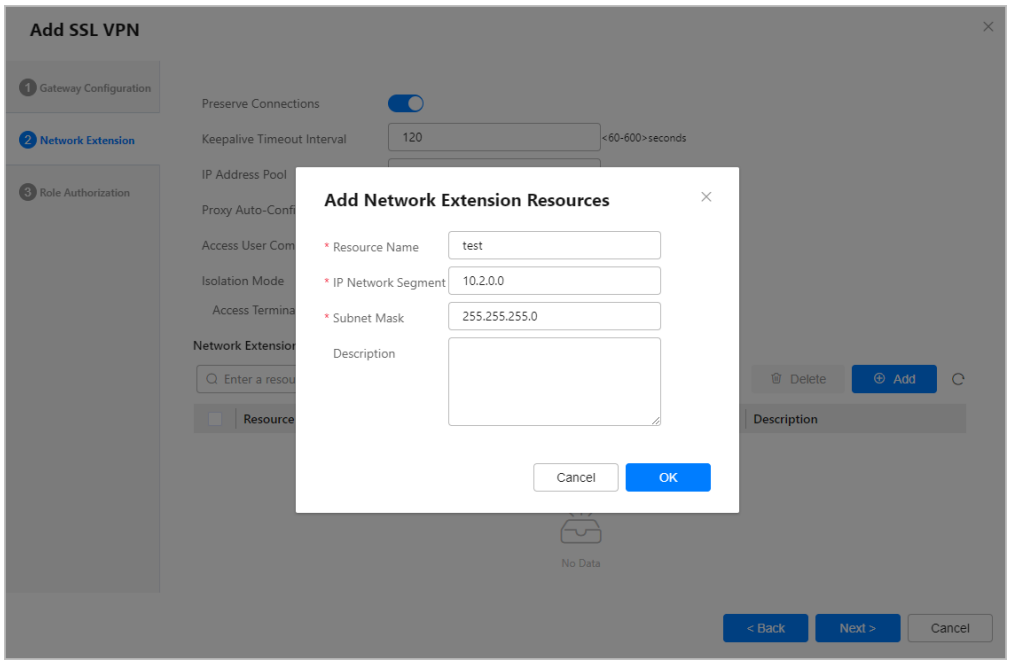
 Copyright © Huawei Technologies Co., Ltd.

Step 8 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

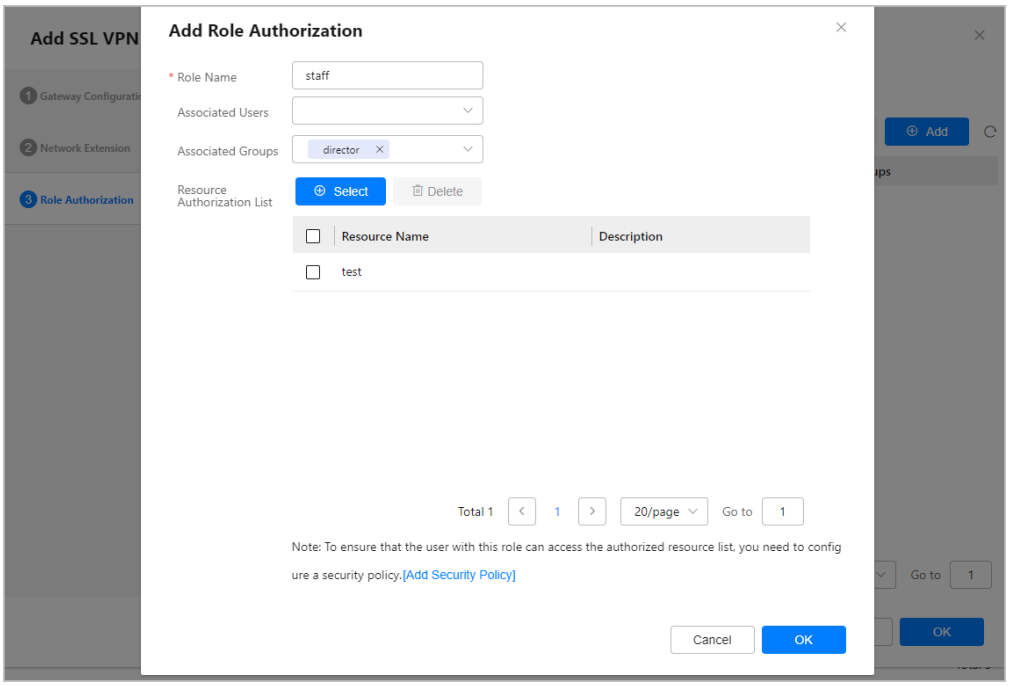


3. Click **Next**.

Step 9 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

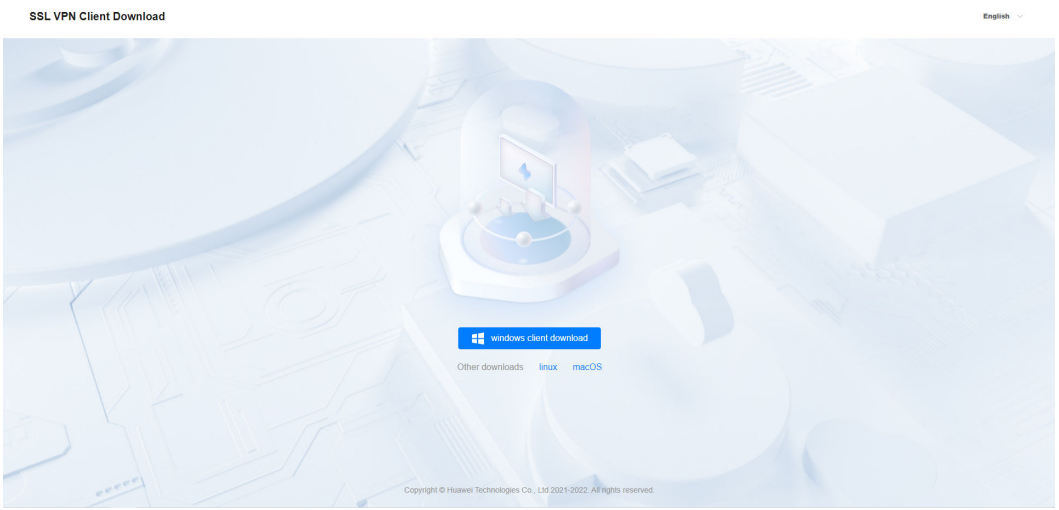
Step 10 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-24 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme radius
  authentication-mode radius
  authorization-scheme default
  authorization-mode local
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server radius_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
radius-server template radius_server
 radius-server shared-key cipher %+%##!!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW&%Ui~]V24G5a|t>k+(m)+Y.0K!!!!!
2jp5!!!!!!:!!!!J=y~T09HG7Q-(u`1p3@X"\>=N~vz&|{~dW!!!!!%+%#
 radius-server authentication 10.1.3.2 1812 weight 80
 undo radius-server user-name domain-included
#
interface 10GE
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE
 ip address 10.2.0.1 255.255.255.0
#
interface 10GE
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface 10GE
 add interface 10GE
#
firewall zone untrust
 set priority 5
 add interface 10GE
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 1
 service address interface 10GE port 443
 security
  authentication-domain default
 service
```

 Copyright © Huawei Technologies Co., Ltd.

```
 network-extension ip-pool addr_pool
 network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
role staff 0
 group director
 resource test
#
return
```

9.13 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + Local Authorization)

Networking Requirements

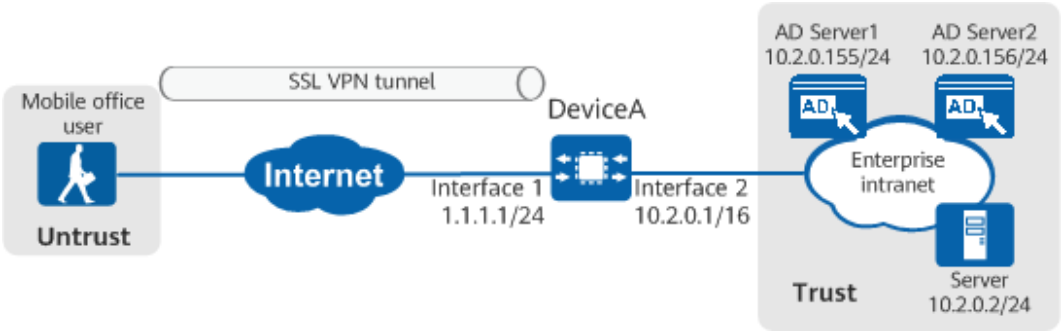
On the enterprise network shown in the following figure, the enterprise authenticates access users through the AD server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, AD authentication with a user name and password is required. In this example, the IP addresses of the primary and secondary AD servers are 10.2.0.155 and 10.2.0.156 respectively.

Figure 9-25 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface GE0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 16
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 16
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the AD server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.2.0.155 32
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.2.0.156 32
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Set parameters for communication between the device and AD server. The parameter settings must be the same as those on the AD server.

Configure the AD server template **ad_server**.

```
[DeviceA] ad-server template ad_server
[DeviceA-ad-ad_server] ad-server authentication 10.2.0.155 88 no-ssl
[DeviceA-ad-ad_server] ad-server authentication 10.2.0.156 88 secondary no-ssl
[DeviceA-ad-ad_server] ad-server authentication base-dn dc=cce,dc=com
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-ad-ad_server] ad-server authentication manager cn=administrator,cn=users YsHsjx@123
[DeviceA-ad-ad_server] ad-server authentication host-name info-server.cce.com
[DeviceA-ad-ad_server] ad-server authentication host-name info-server2.cce.com secondary
[DeviceA-ad-ad_server] ad-server authentication ldap-port 389 ldap-ssl-port 636
```

Test the connectivity between the device and AD server.

```
[DeviceA-ad-ad_server] test-aaa user_0001 YsHsjx@123 ad-template ad_server
[DeviceA-ad-ad_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.0.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the AAA authentication domain of the virtual gateway to **cce.com**.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain cce.com
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name. For example, if the virtual gateway has been bound to the authentication domain **cce.com**, the user **user_0001** in that authentication domain should enter **user_0001** instead of **user_0001@cce.com** as the user name.

Configure an authentication domain. Create an authentication scheme, set the authentication mode to AD authentication, and apply the scheme to an authentication domain.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme ad
[DeviceA-aaa-authentication-ad] authentication-mode ad
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-aaa-authentication-ad] quit
[DeviceA-aaa] domain cce.com
[DeviceA-aaa-domain-cce.com] authentication-scheme ad
[DeviceA-aaa-domain-cce.com] ad-server ad_server
[DeviceA-aaa-domain-cce.com] quit
[DeviceA-aaa] quit
```

Set the local access user name to **abc**, password to **YsHsjx_202206**, access type to **sslvpn**, and bind the user to the UCL group **director**.

```
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] password cipher YsHsjx_202206
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] ucl-group director
[DeviceA-aaa-access-user-abc] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

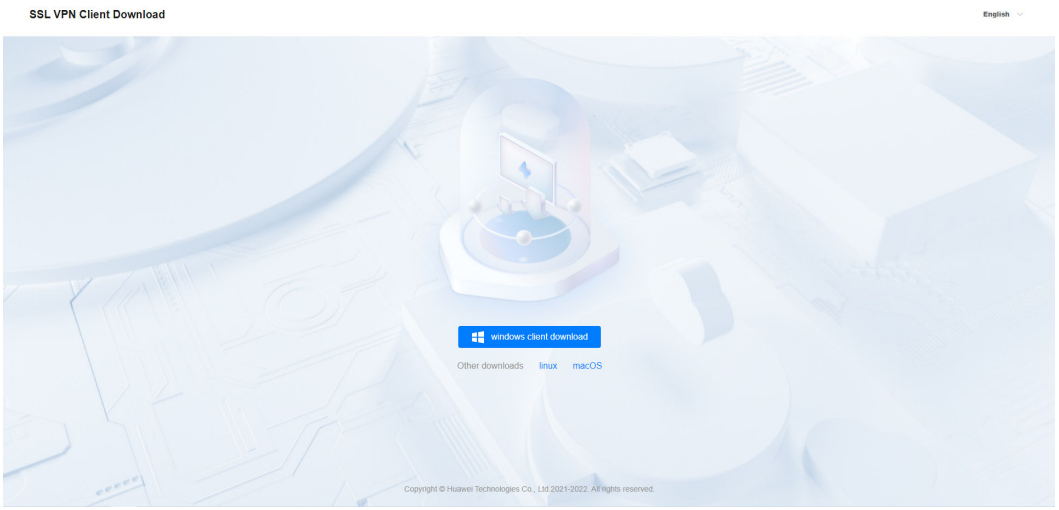
```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-26 Downloading the VPN client installation package from the SSL VPN portal website

2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
```

```
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
 authentication-scheme ad
  authentication-mode ad
 domain cce.com
  authentication-scheme ad
  accounting-scheme default
  ad-server ad_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
ad-server template ad_server
 ad-server authentication base-dn dc=cce,dc=com
 ad-server authentication ldap-port 389 ldap-ssl-port 636
 ad-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW|^it6r))]DA
%1w3IhtdVkOIN<!!!!!2jp5!!!!!!:!!!!(u);AOxJ#E0p-iD71T/0\>bBTc\x@V}/K5Q!!!!!%+%#
 ad-server authentication 10.2.0.155 88 no-ssl
 ad-server authentication host-name info-server.cce.com
 ad-server authentication 10.2.0.156 88 secondary no-ssl
 ad-server authentication host-name info-server2.cce.com secondary
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.155 mask 255.255.255.255
  destination-address 10.2.0.156 mask 255.255.255.255
  action permit
#
virtual-gateway example 1
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain cce.com
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 role staff 0
  group director
  resource test
#
return
```

9.14 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (AD Authentication + Local Authorization)

Networking Requirements

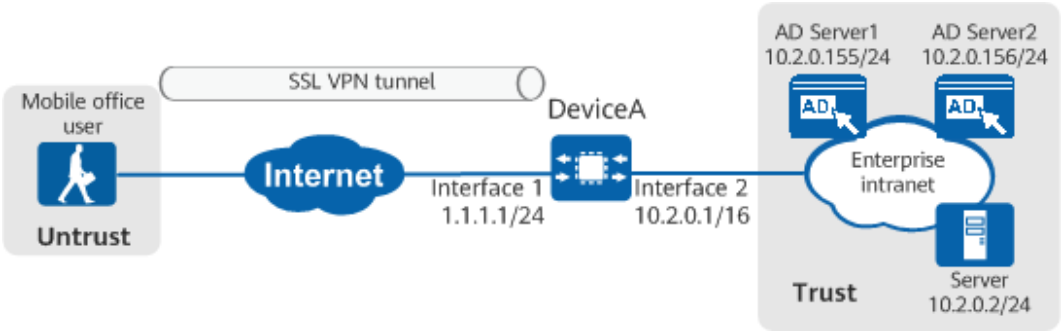
On the enterprise network shown in the following figure, the enterprise authenticates access users through the AD server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, AD authentication with a user name and password is required. In this example, the IP addresses of the primary and secondary AD servers are 10.2.0.155 and 10.2.0.156 respectively.

Figure 9-27 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Configure an IP address for GE 0/0/2 and add it to a security zone.

a. In **Interface List**, click  in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.1/24
Action	Permit

5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the AD server.

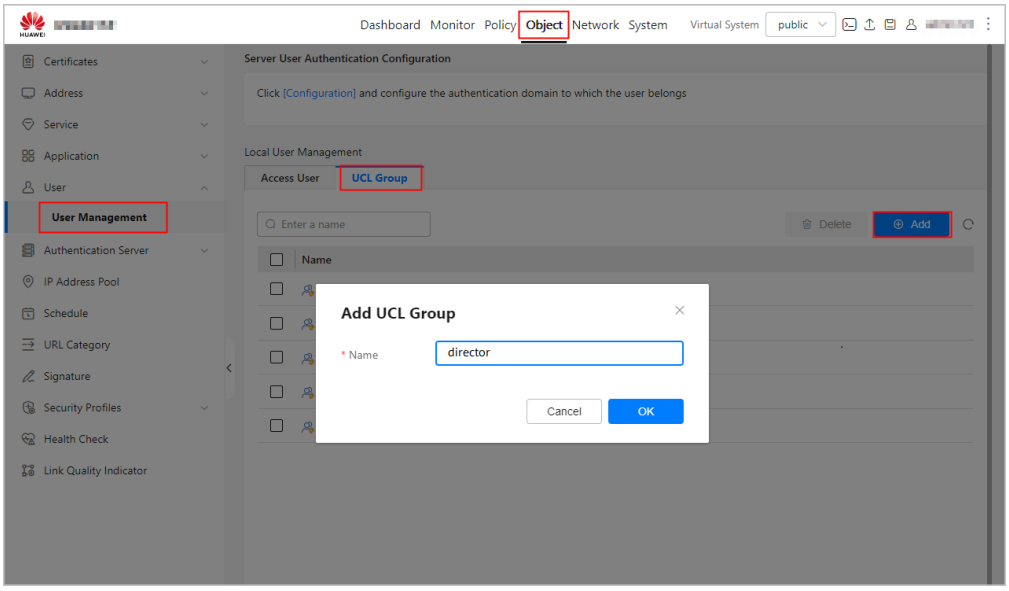
 Copyright © Huawei Technologies Co., Ltd.

Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.2.0.155/32, 10.2.0.156/32
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

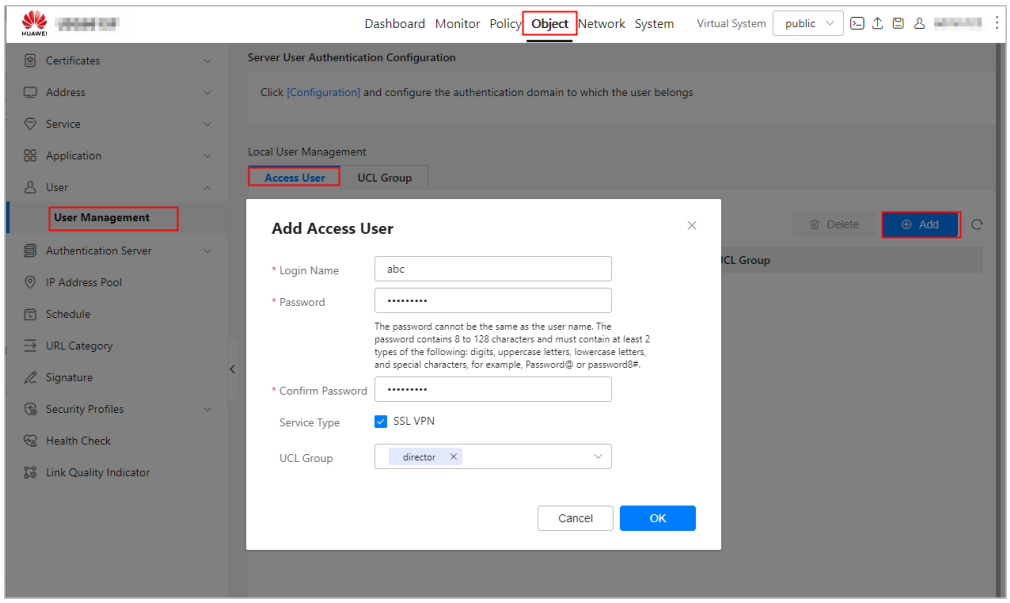
1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.



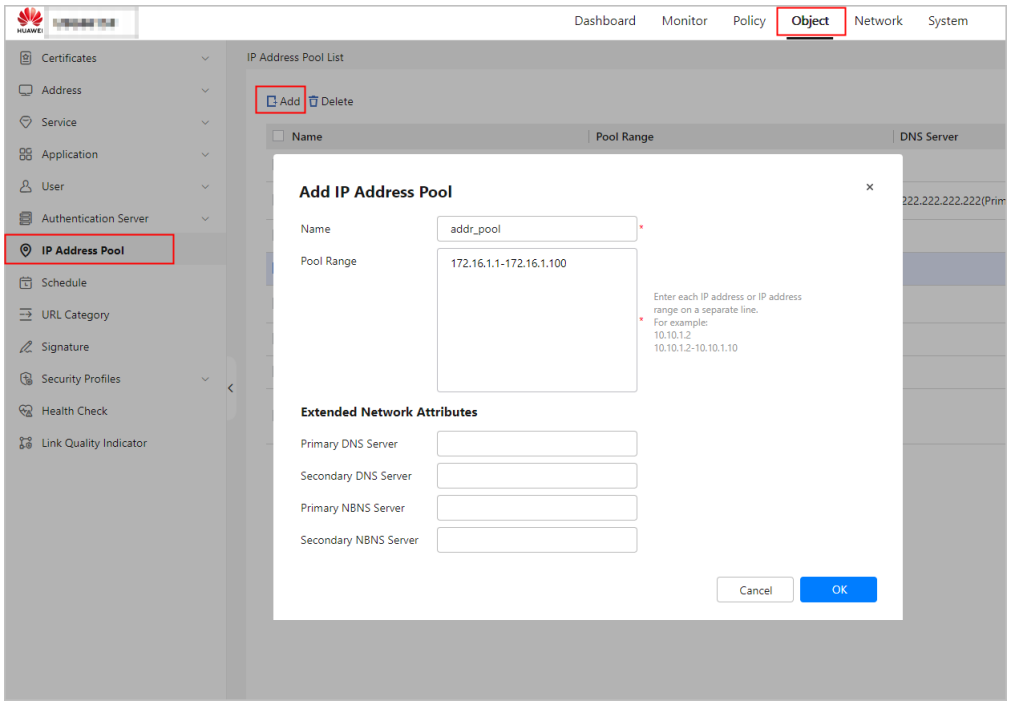
2. Click **OK**.
3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   The user **abc** belongs to the user group **director** and the password is **YsHsjx_202206**.

 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.
5. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

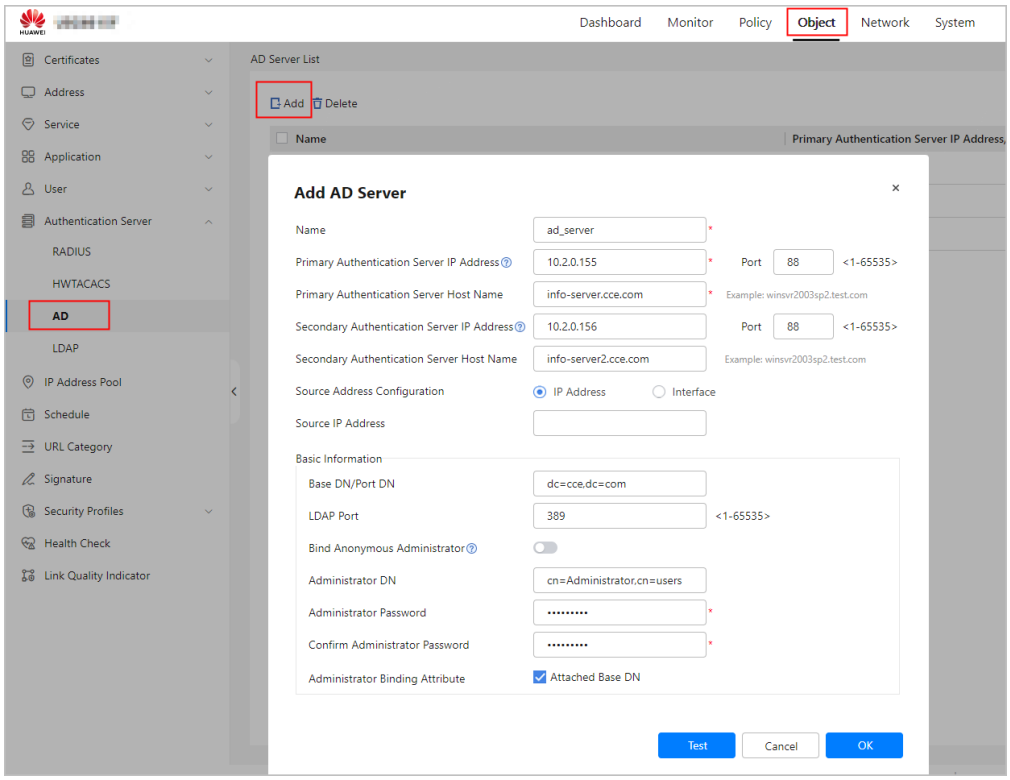


6. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **AD**, click **Add**, and set the following parameters to configure the AD server.

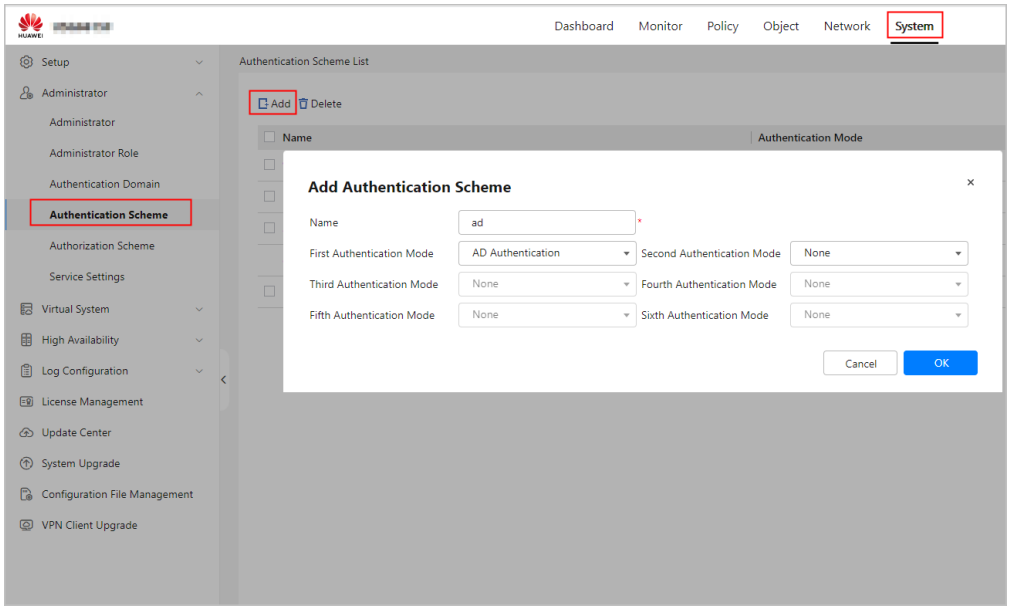
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 5 Configure an authentication scheme.

1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.

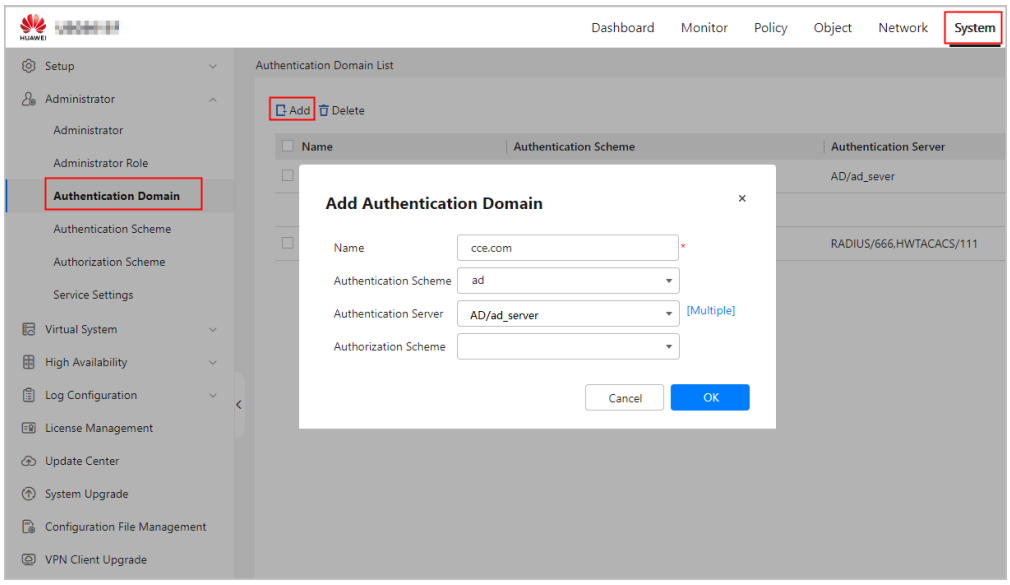


2. Click **OK**.

Step 6 Configure an authentication domain.

1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.

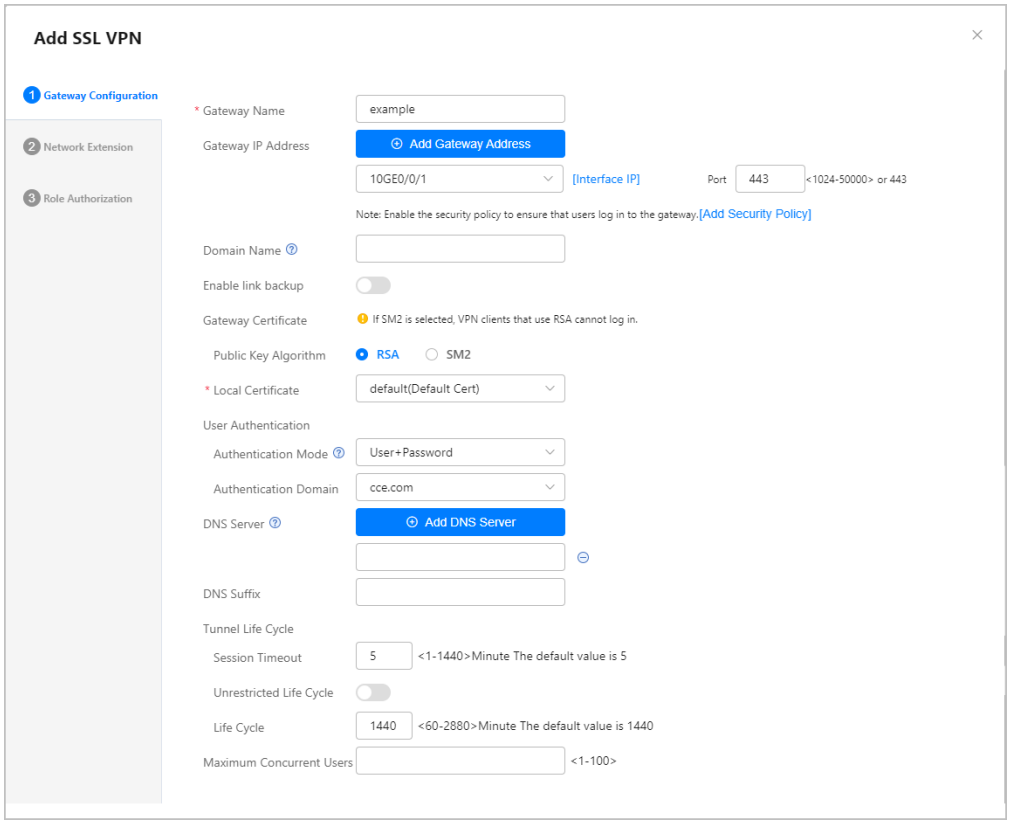
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 7 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

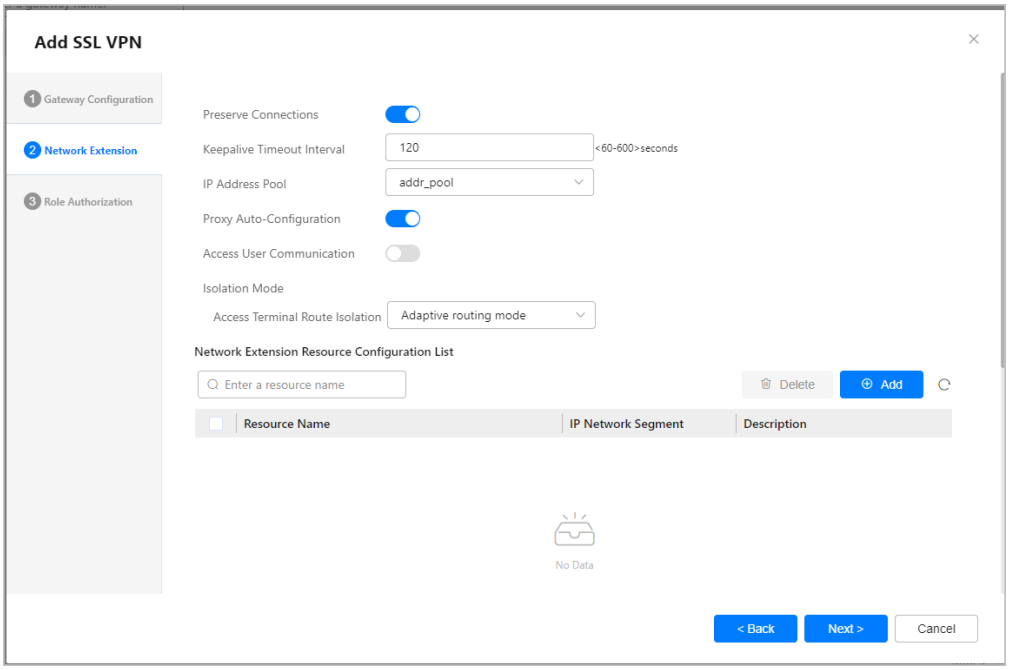


3. Click **Next**.

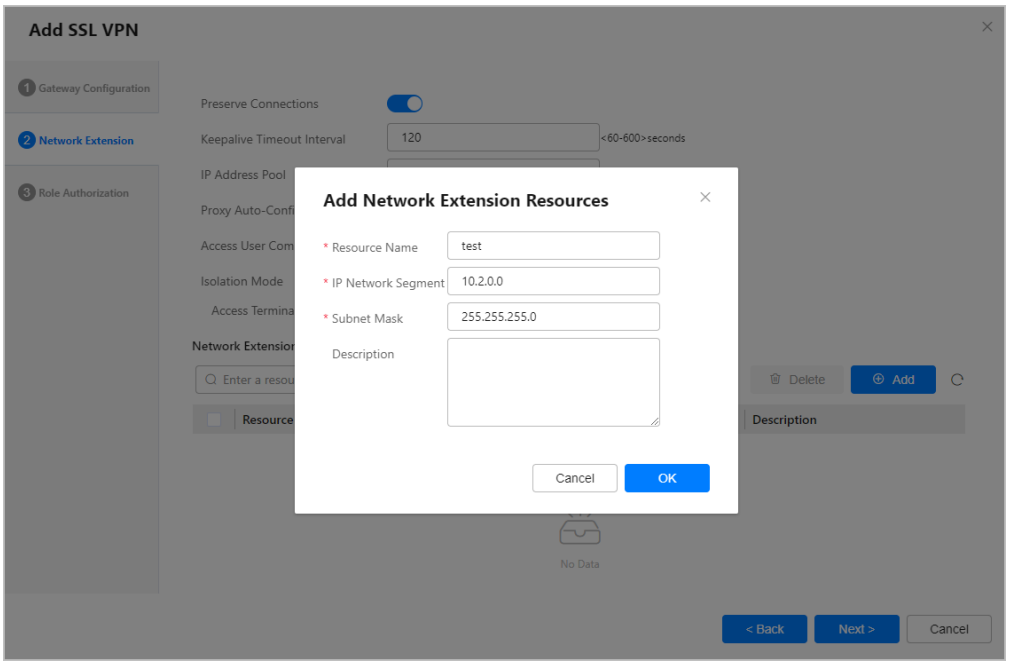
Step 8 Configure the network extension function.

 Copyright © Huawei Technologies Co., Ltd.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

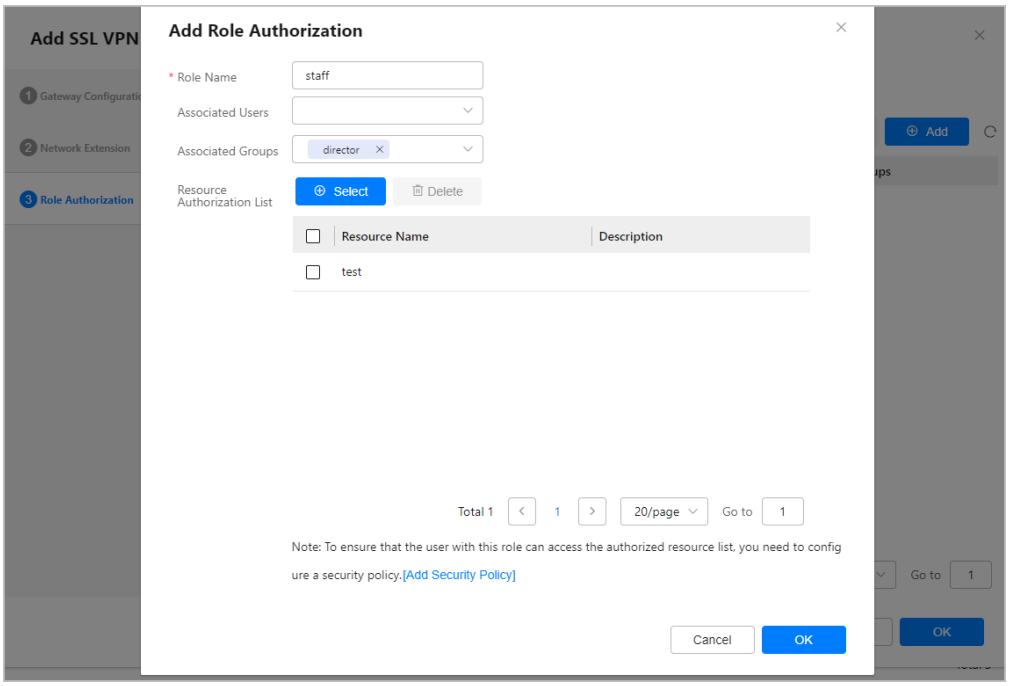


3. Click **Next**.

Step 9 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

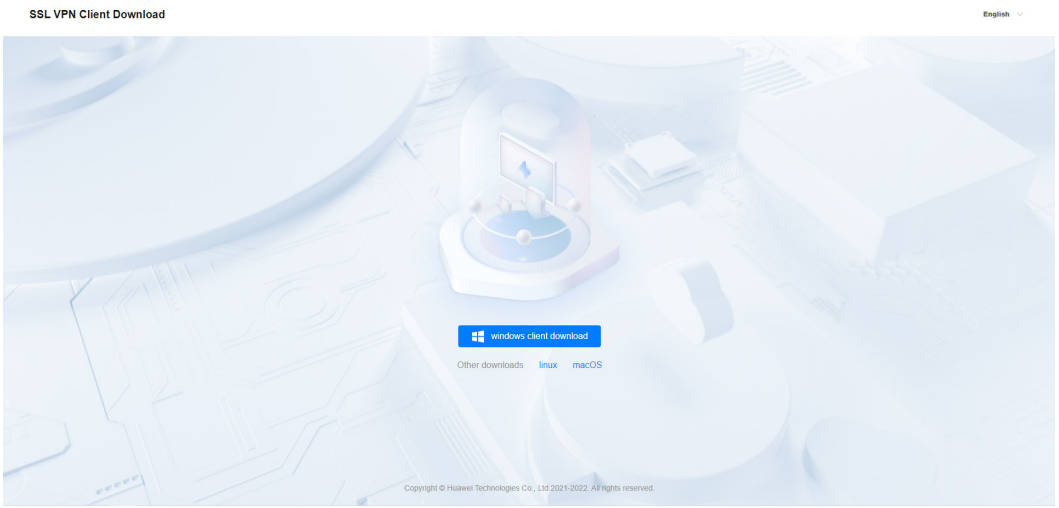
Step 10 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-28 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
 authentication-scheme ad
  authentication-mode ad
 domain cce.com
  authentication-scheme ad
  accounting-scheme default
  ad-server ad_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
ad-server template ad_server
 ad-server authentication base-dn dc=cce,dc=com
 ad-server authentication ldap-port 389 ldap-ssl-port 636
 ad-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW|^it6r))]DA
%1w3IhtdVkOIN<!!!!!2jp5!!!!!!:!!!!(u);AOxJ#E0p-iD71T/0\>bBTc\x@V}/K5Q!!!!!%+%#
 ad-server authentication 10.2.0.155 88 no-ssl
 ad-server authentication host-name info-server.cce.com
 ad-server authentication 10.2.0.156 88 secondary no-ssl
 ad-server authentication host-name info-server2.cce.com secondary
#
interface 10GE
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface 10GE
#
firewall zone untrust
 set priority 5
 add interface 10GE
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.155 mask 255.255.255.255
  destination-address 10.2.0.156 mask 255.255.255.255
  action permit
#
virtual-gateway example 1
 service address interface 10GE port 443
 security
  authentication-domain cce.com
 service
```

 Copyright © Huawei Technologies Co., Ltd.

```
 network-extension ip-pool addr_pool
 network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
role staff 0
 group director
 resource test
#
return
```

9.15 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + LDAP Authorization)

Networking Requirements

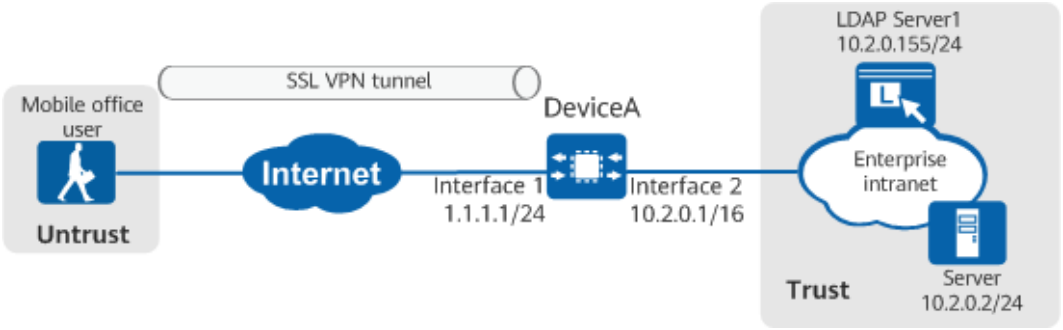
On the enterprise network shown in the following figure, the enterprise authenticates access users through the LDAP server. Authenticated users can access the enterprise intranet.

The enterprise wants executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, LDAP authentication with a user name and password is required. In this example, the IP address of the LDAP server is 10.2.0.155.

Figure 9-29 Network diagram for configuring mobile office users to access the headquarters through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface GE0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 16
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 16
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the LDAP server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.2.0.155 32
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This example uses server authorization. That is, the device obtains the security group to which a user belongs from the server and searches for the role corresponding to the security group. Therefore, you need to create a security group with the same name as the server on the device. Otherwise, the security group cannot be referenced by the role. The following creates a security group for reference.

The attributes used as the names of security groups vary according to servers. The names of security groups created on the device are the same as the corresponding attribute values.

- The UniqueMember attribute value of a user on the Sun ONE LDAP server is used as the security group name.
- The memberOf attribute values of users on the AD LDAP, IBM Tivoli LDAP and Open LDAP servers are used as the security group names.

Users are organized by levels on the LDAP server. If the memberOf attribute of a user has multi-level user group CNs, the device uses only the lowest-level CN value, that is, the first CN value in the attribute, as the security group name. For example, if the memberOf attribute value is **CN=a2,cn=a1,DC=cce,DC=com**, the name of the security group to be created on the device needs to be **a2**.

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Set parameters for communication between the device and LDAP server. The parameter settings must be the same as those on the LDAP server.

NOTE

The device supports AD LDAP, IBM Tivoli LDAP, Sun ONE LDAP, and Open LDAP servers. The following uses the Sun ONE LDAP server as an example.

Configure the LDAP server template **ldap_server**.

```
[DeviceA] ldap-server template ldap_server
[DeviceA-ldap-ldap_server] ldap-server server-type sun-one
[DeviceA-ldap-ldap_server] ldap-server authentication 10.2.0.155 389 no-ssl
[DeviceA-ldap-ldap_server] ldap-server authentication base-dn dc=cce,dc=com
[DeviceA-ldap-ldap_server] ldap-server authentication manager cn=administrator,cn=users YsHsjx@123
[DeviceA-ldap-ldap_server]
```

Test the connectivity between the device and LDAP server.

```
[DeviceA-ldap-ldap_server] test-aaa user_0001 YsHsjx@123 ldap-template ldap_server
[DeviceA-ldap-ldap_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.0.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the AAA authentication domain of the virtual gateway to **cce.com**.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain cce.com
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name. For example, if the virtual gateway has been bound to the authentication domain **cce.com**, the user **user_0001** in that authentication domain should enter **user_0001** instead of **user_0001@cce.com** as the user name.

Configure an authentication domain. Create an authentication scheme and an authorization scheme, set the authentication mode of the authentication scheme to LDAP authentication, set the authorization mode of the authorization scheme to LDAP authorization, and apply these schemes to an authentication domain.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme ldap
[DeviceA-aaa-authentication-ldap] authentication-mode ldap
[DeviceA-aaa-authentication-ldap] quit
[DeviceA-aaa] authorization-scheme ldap
[DeviceA-aaa-author-ldap] authorization-mode ldap
[DeviceA-aaa-author-ldap] quit
[DeviceA-aaa] domain cce.com
[DeviceA-aaa-domain-cce.com] authentication-scheme ldap
[DeviceA-aaa-domain-cce.com] authorization-scheme ldap
[DeviceA-aaa-domain-cce.com] ldap-server ldap_server
[DeviceA-aaa-domain-cce.com] quit
[DeviceA-aaa] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

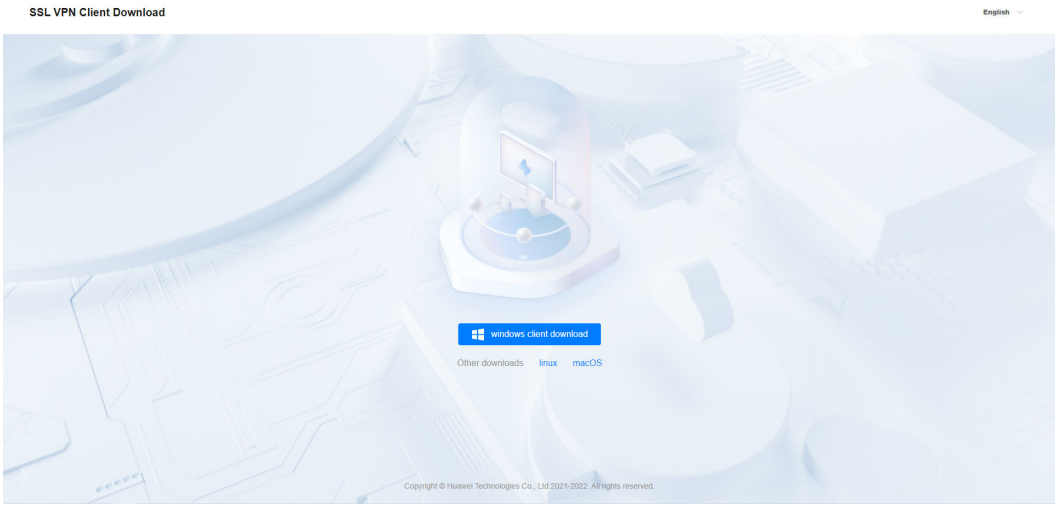
----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-30 Downloading the VPN client installation package from the SSL VPN portal website

2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme ldap
  authentication-mode ldap
  authorization-scheme ldap
  authorization-mode ldap
 domain cce.com
  authentication-scheme ldap
  authorization-scheme ldap
  accounting-scheme default
  ldap-server ldap_server



#
ldap-server template ldap_server
 ldap-server server-type sun-one
 ldap-server authentication base-dn dc=cee,dc=com
 ldap-server authentication 10.2.0.155 389 ssl
 ldap-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!
cZa'*[{[xW[dOX;UfIp4uYisC=ZW(R.t)NE!!!!!2jp5!!!!!!:!!!!DqsI+`1EBF*rOBF[kt2#%-y-ZG[7_RY`LwU!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
```

```
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.155 mask 255.255.255.255
  action permit
#
virtual-gateway example 0
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain cce.com
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.16 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (LDAP Authentication + LDAP Authorization)

Networking Requirements

On the enterprise network shown in the following figure, the enterprise authenticates access users through the LDAP server. Authenticated users can access the enterprise intranet.

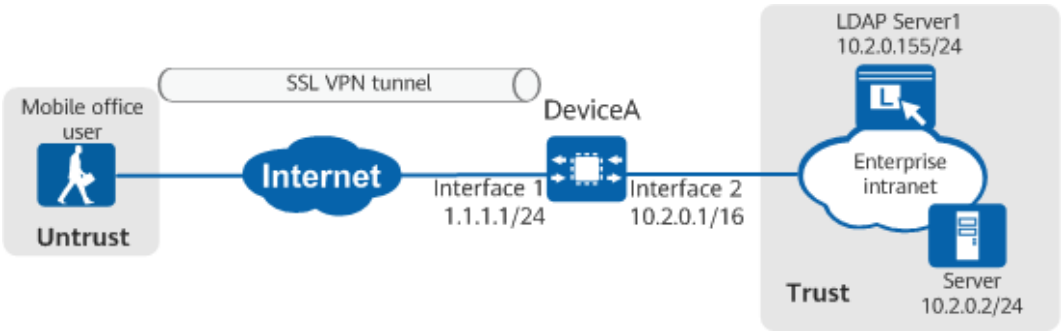
The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, LDAP authentication with a user name and password is required. In this example, the IP address of the LDAP server is 10.2.0.155.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-31 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Configure an IP address for GE 0/0/2 and add it to a security zone.
   a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

 Copyright © Huawei Technologies Co., Ltd.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.1/24
Action	Permit

5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the LDAP server.

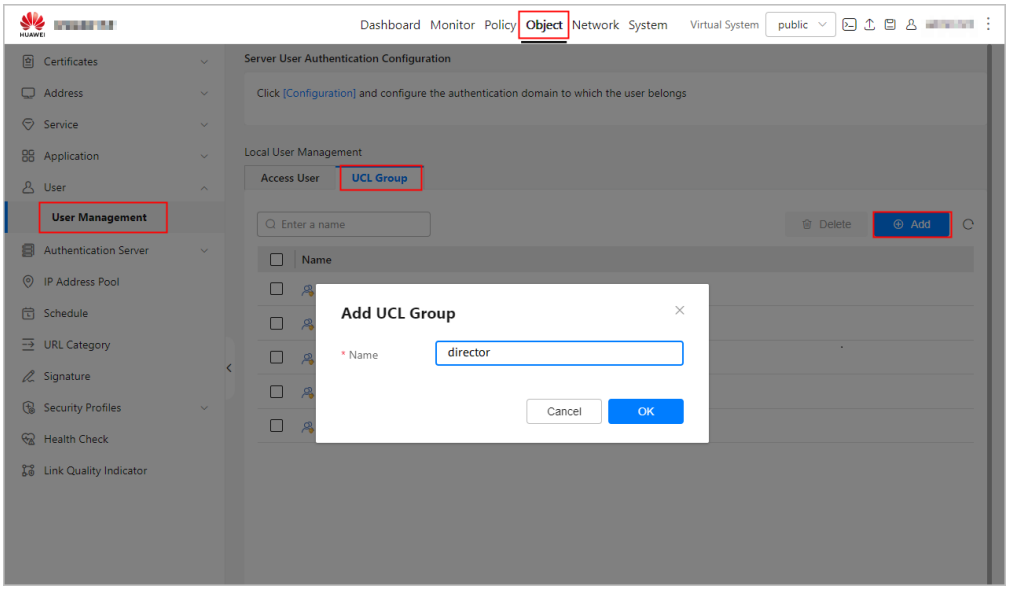
Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.2.0.155/32
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

This example uses server authorization. That is, the device obtains the security group to which a user belongs from the server and searches for the role corresponding to the security group. Therefore, you need to create a security group with the same name as the server on the device. Otherwise, the security group cannot be referenced by the role. The following creates a security group for reference.

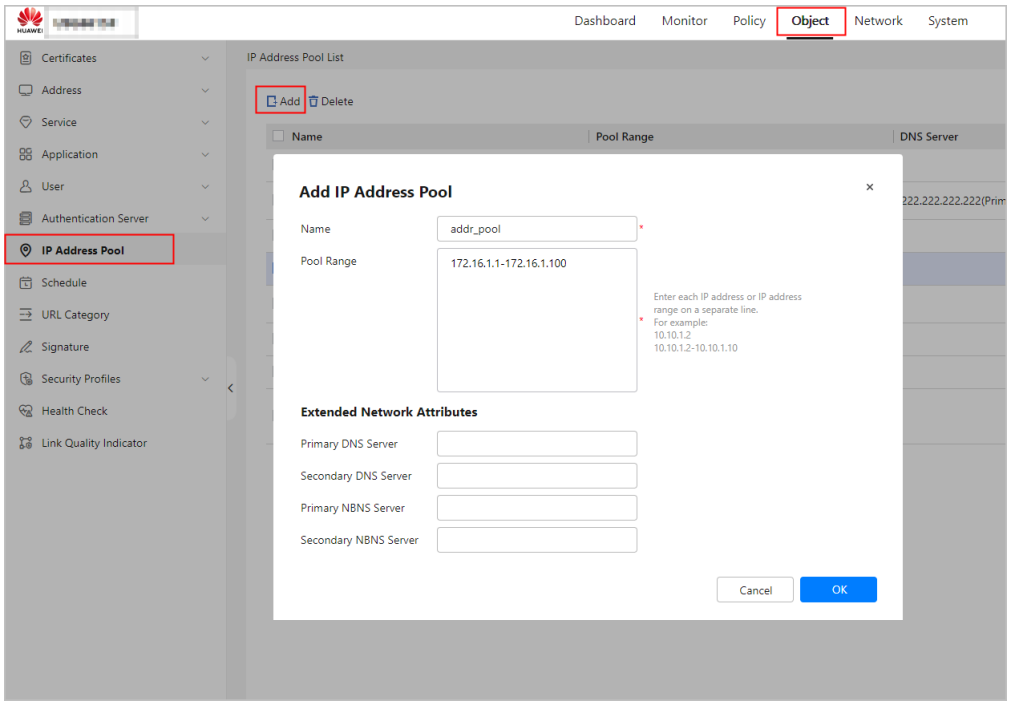
The attributes used as the names of security groups vary according to servers. The names of security groups created on the device are the same as the corresponding attribute values.

- The UniqueMember attribute value of a user on the Sun ONE LDAP server is used as the security group name.
- The memberOf attribute values of users on the AD LDAP, IBM Tivoli LDAP and Open LDAP servers are used as the security group names.

Users are organized by levels on the LDAP server. If the memberOf attribute of a user has multi-level user group CNs, the device uses only the lowest-level CN value, that is, the first CN value in the attribute, as the security group name. For example, if the memberOf attribute value is **CN=a2,cn=a1,DC=cce,DC=com**, the name of the security group to be created on the device needs to be **a2**.

2. Click **OK**.
3. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

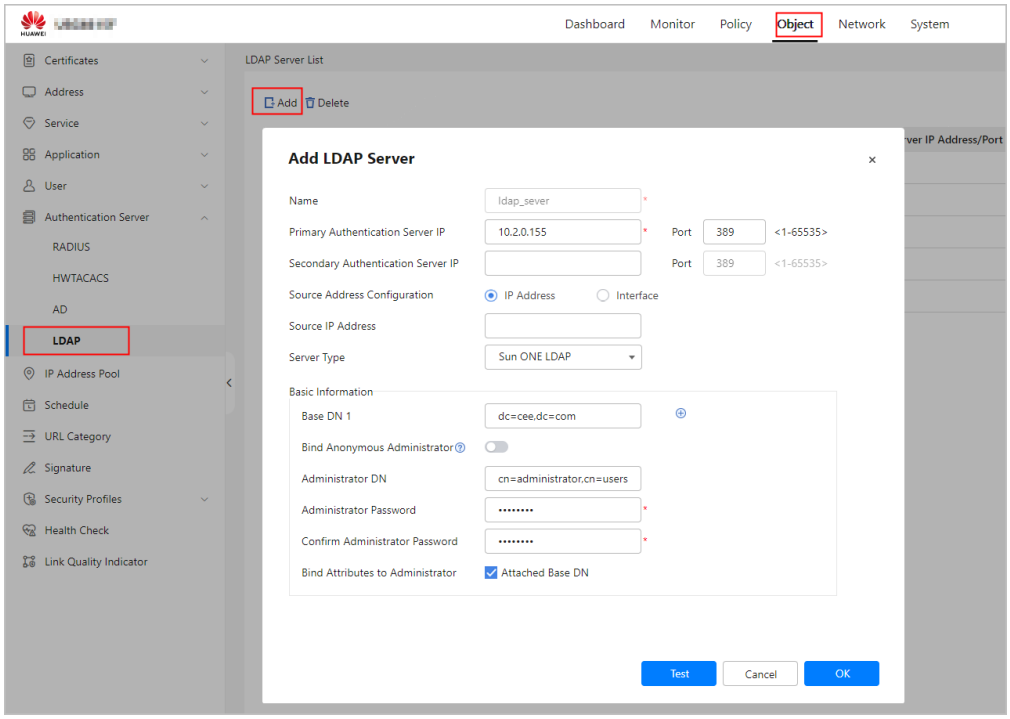
 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **LDAP**, click **Add**, and set the following parameters to configure the LDAP server.

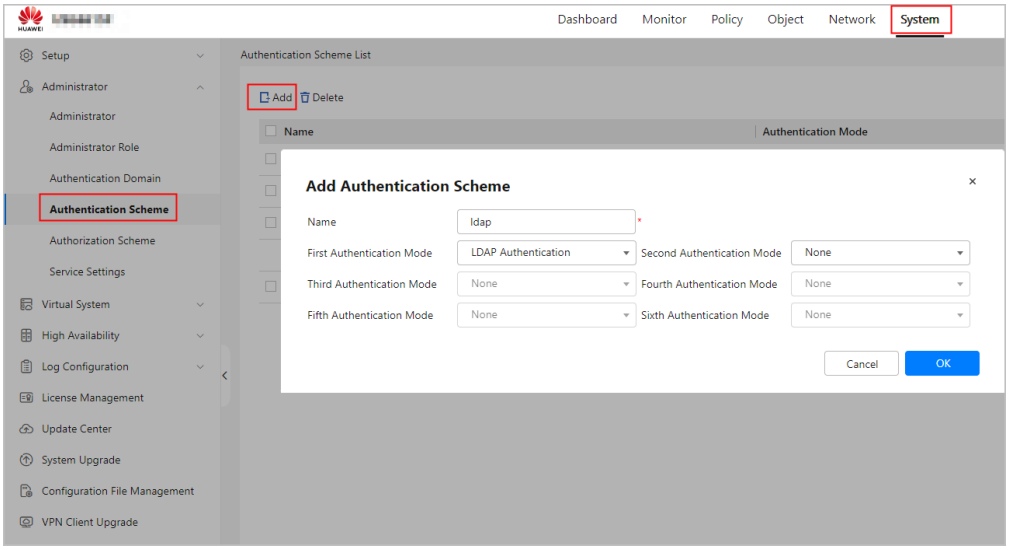


2. Click **OK**.

Step 5 Configure an authentication scheme.

1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.

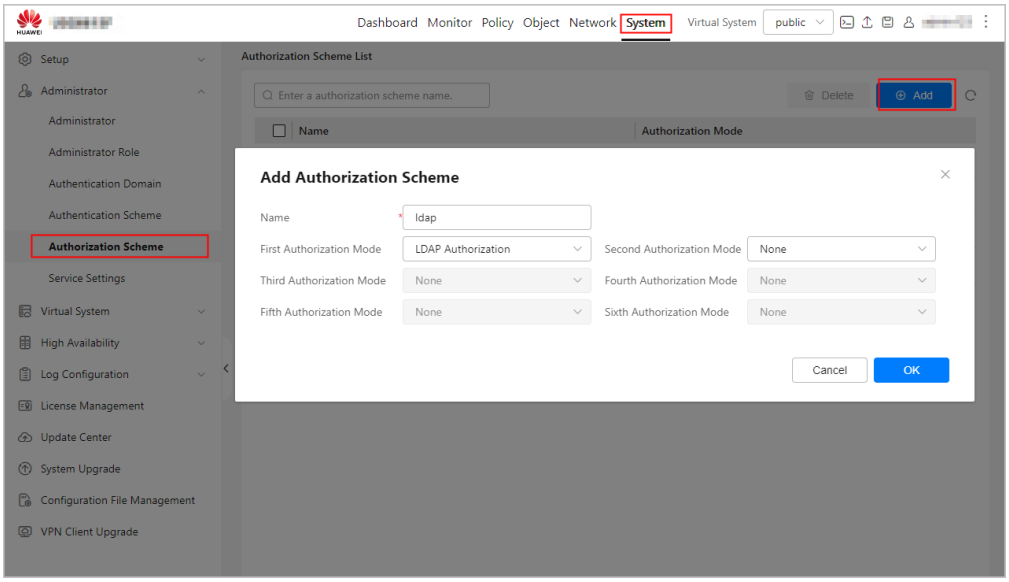
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 6 Configure an authorization scheme.

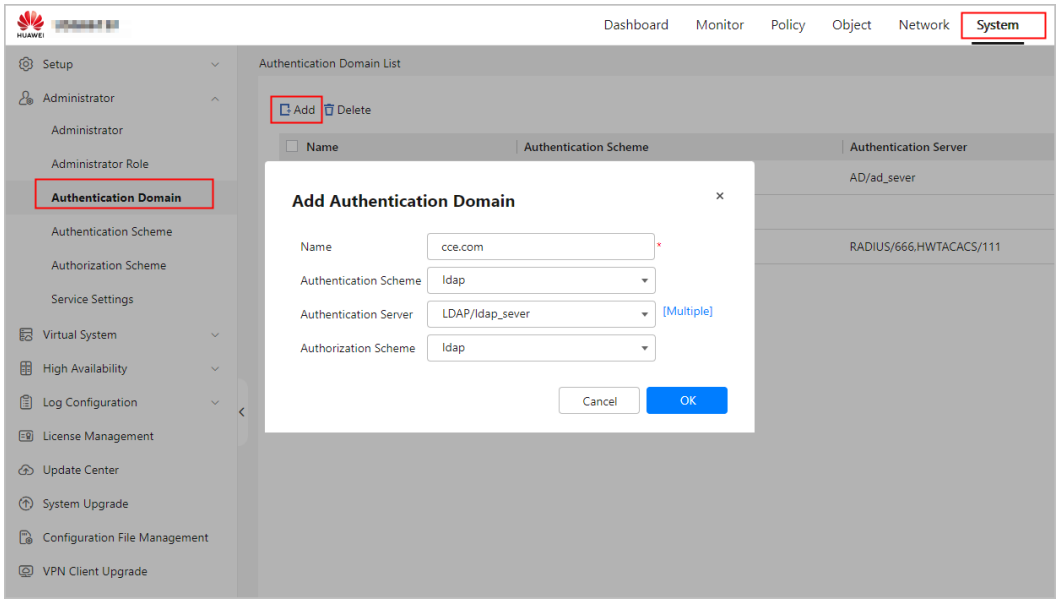
1. Choose **System** > **Administrator** > **Authorization Scheme**, click **Add**, and set the following parameters to configure an authorization scheme.



2. Click **OK**.

Step 7 Configure an authentication domain.

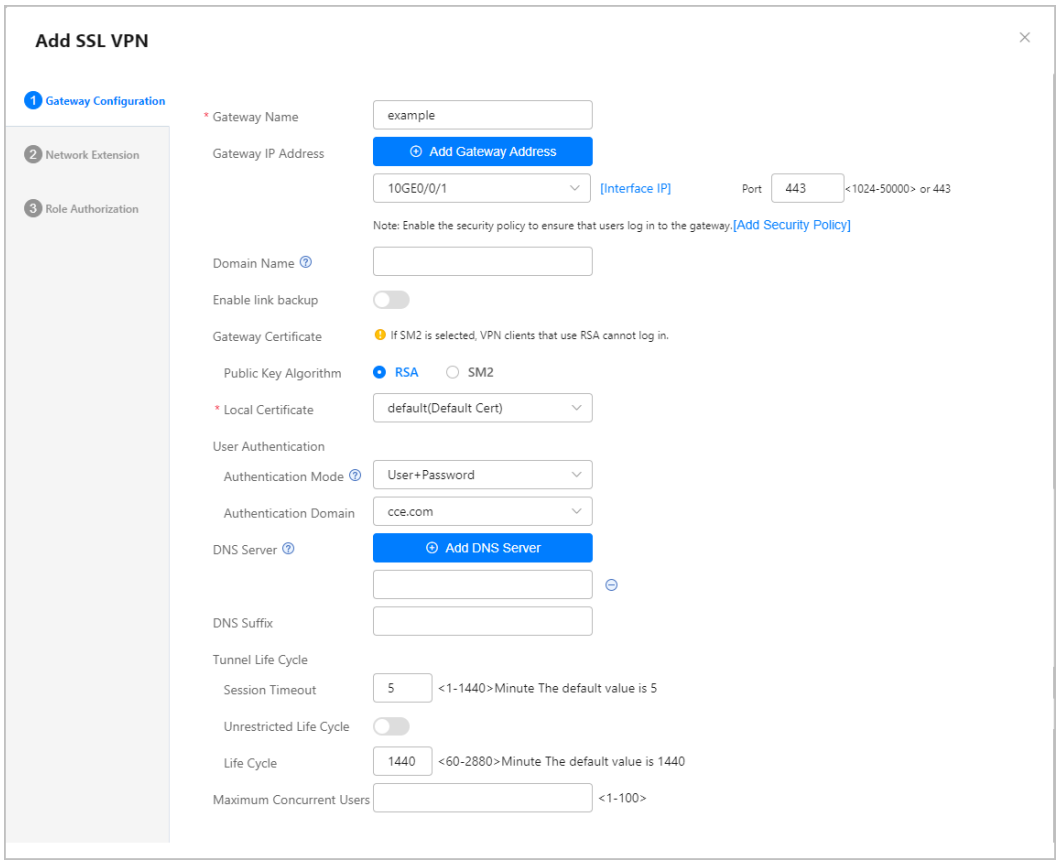
1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.



2. Click **OK**.

Step 8 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

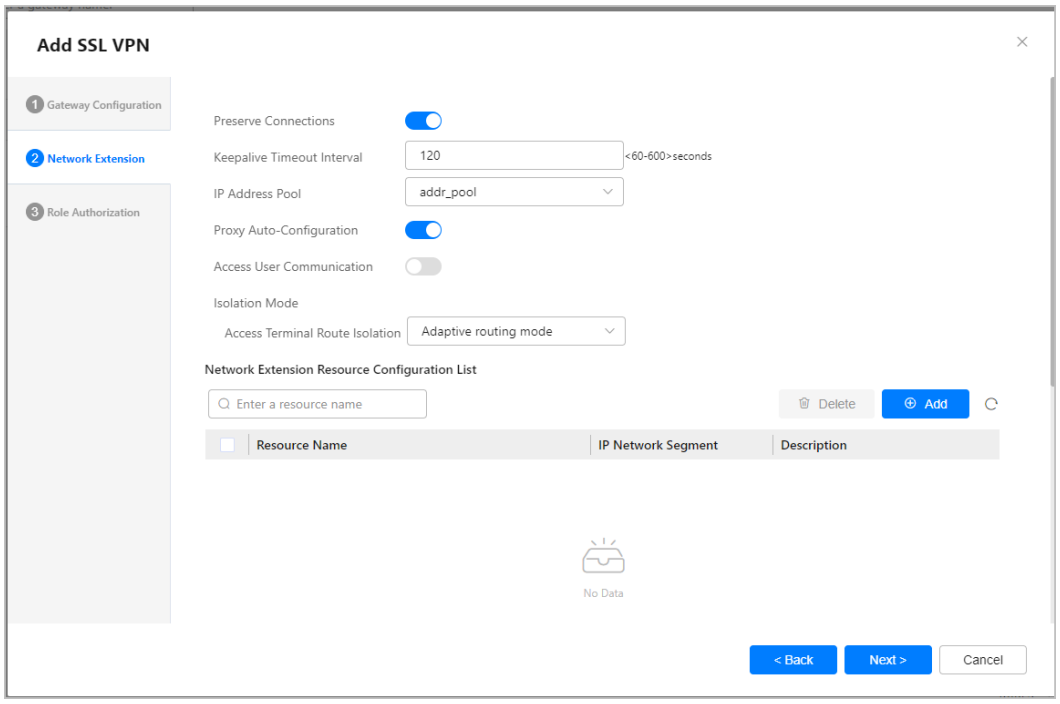


3. Click **Next**.

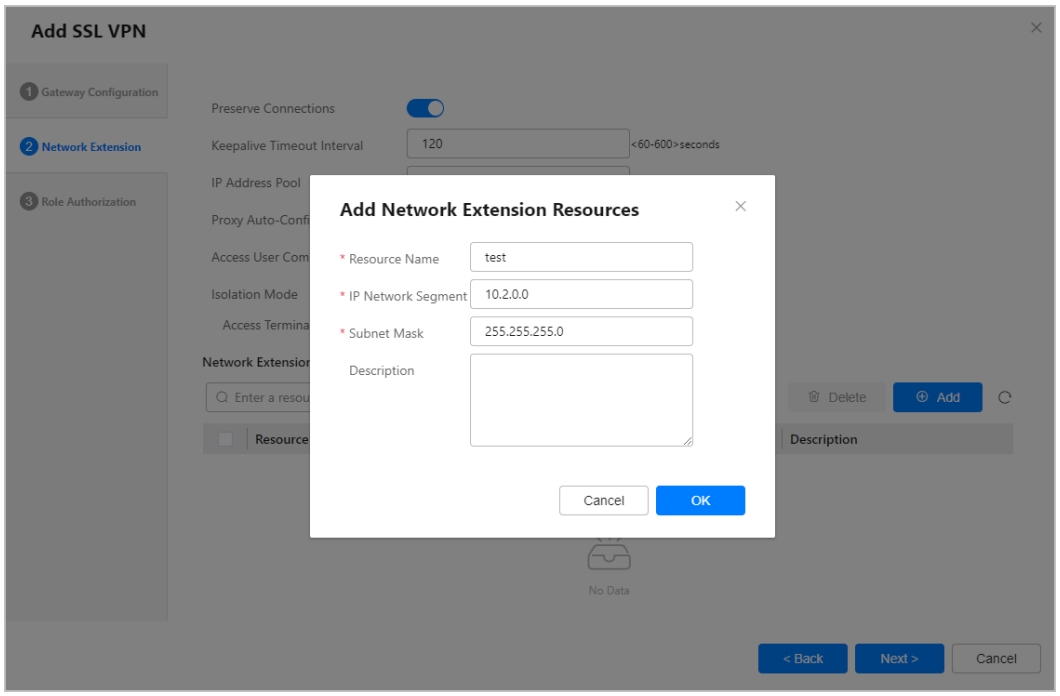
 Copyright © Huawei Technologies Co., Ltd.

Step 9 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

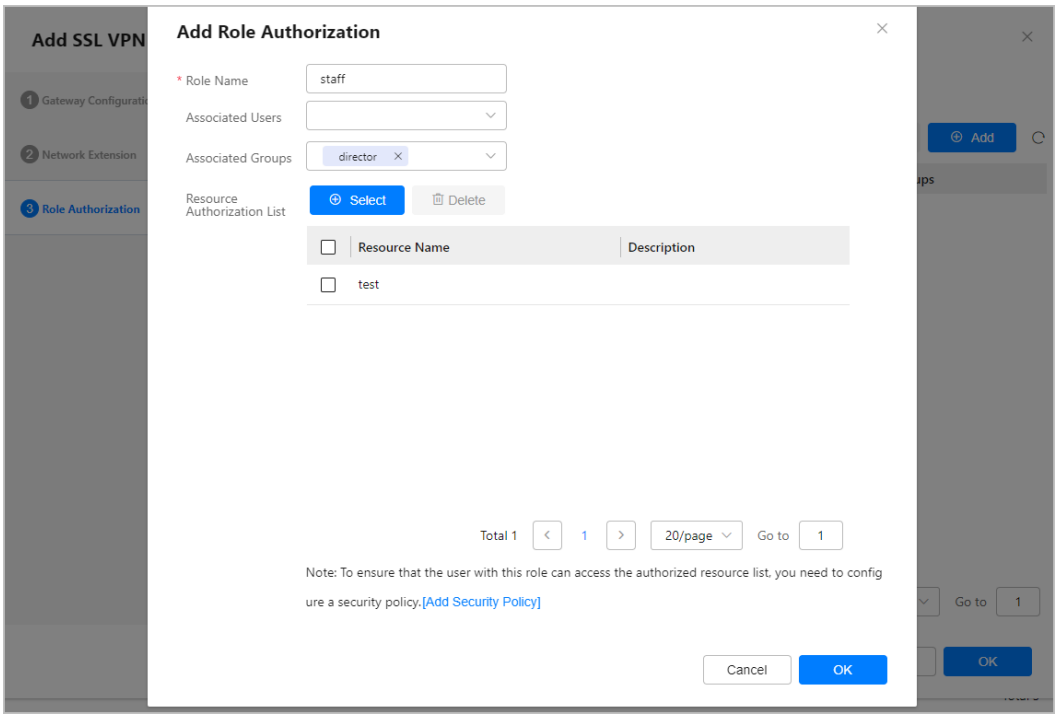


3. Click **Next**.

Step 10 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

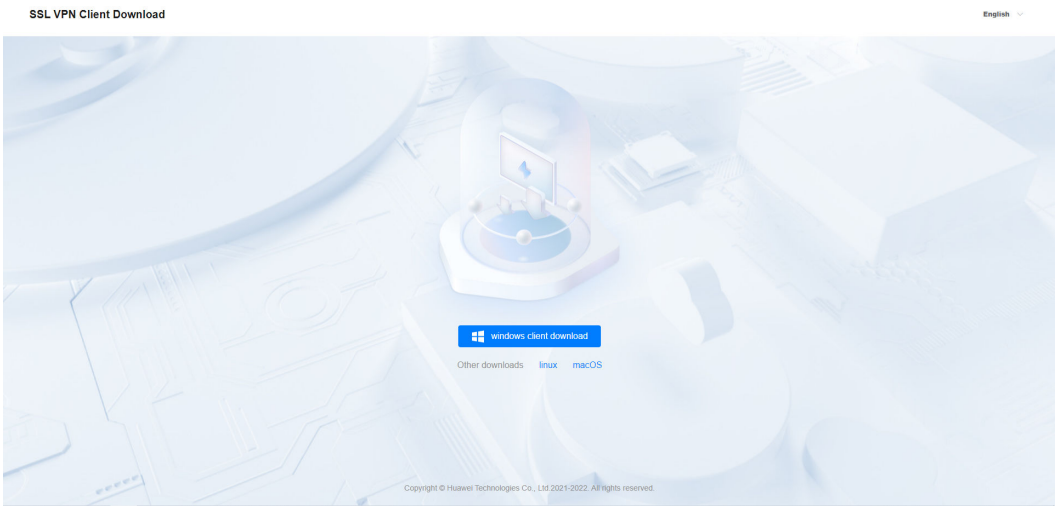
Step 11 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal website. As shown in the following figure, download and install the VPN client installation package required by the user's operating system. For more information, see:**VPN Client Download Description**.

   Figure 9-32 Downloading the VPN client installation package from the SSL VPN portal website



2. Connect to the virtual gateway through the client and access intranet resources.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme ldap
  authentication-mode ldap
  authorization-scheme ldap
  authorization-mode ldap
 domain cce.com
  authentication-scheme ldap
  authorization-scheme ldap
  accounting-scheme default
  ldap-server ldap_server



#
ldap-server template ldap_server
 ldap-server server-type sun-one
 ldap-server authentication base-dn dc=cee,dc=com
 ldap-server authentication 10.2.0.155 389 ssl
 ldap-server authentication manager cn=administrator,cn=users %+%##!!!!!!!!!"!!!!"!!!!*!!!!
cZa'*[{[xW[dOX;UfIp4uYisC=ZW(R.t)NE!!!!!2jp5!!!!!!:!!!!DqsI+`1EBF*rOBF[kt2#%-y-ZG[7_RY`LwU!!!!!%+%#
#
interface 10GE
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE
 ip address 10.2.0.1 255.255.0.0
#
firewall zone trust
 set priority 85
 add interface 10GE
#
firewall zone untrust
 set priority 5
 add interface 10GE
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.0.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  source-address 172.16.1.0 mask 255.255.255.0
  destination-address 10.2.0.155 mask 255.255.255.255
  action permit
#
virtual-gateway example 0
 service address interface 10GE port 443
 security
  authentication-domain cce.com
 service
  network-extension ip-pool addr_pool
```

 Copyright © Huawei Technologies Co., Ltd.

```
 network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.17 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + RADIUS Authorization)

Networking Requirements

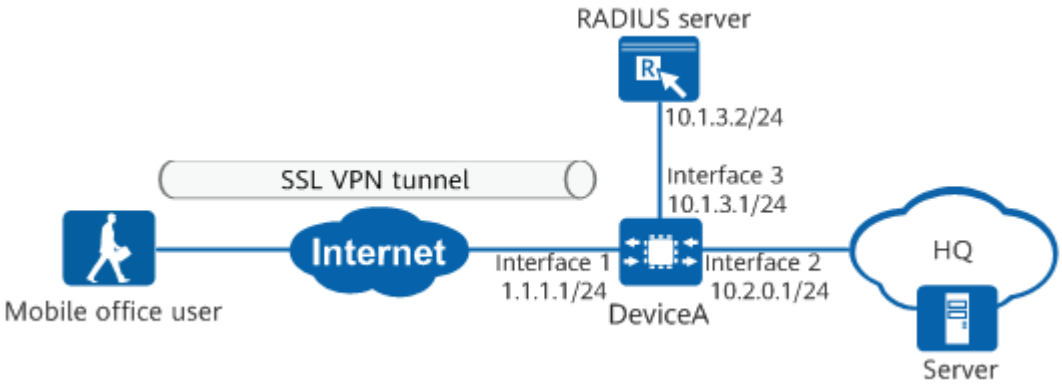
On the enterprise network shown in the following figure, the enterprise authenticates access users through the RADIUS server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, RADIUS authentication with a user name and password is required. In this example, the IP address of the RADIUS server is 10.1.3.2, and IP addresses in the network extension address pool assigned to mobile office users range from 172.16.1.1 to 172.16.1.100.

Figure 9-33 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface GE0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/3.

```
[DeviceA] interface GE
[DeviceA-GE0/0/3] ip address 10.1.3.1 24
[DeviceA-GE0/0/3] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 and GE 0/0/3 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] add interface GE0/0/3
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 32
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the RADIUS server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.1.3.2 24
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This example uses server authorization. That is, the device obtains the security group to which a user belongs from the server and searches for the role corresponding to the security group. Therefore, you need to create a security group with the same name as the server on the device. Otherwise, the security group cannot be referenced by the role. The following creates a security group for reference.

The device uses the Filter-Id attribute value of a user on the RADIUS server as the security group name. The names of security groups created on the device are the same as the corresponding attribute values.

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Set parameters for communication between the device and RADIUS server. The parameter settings must be the same as those on the RADIUS server.

Configure the RADIUS server template **radius_server**.

```
[DeviceA] radius-server template radius_server
[DeviceA-radius-radius_server] radius-server authentication 10.1.3.2 1812
[DeviceA-radius-radius_server] radius-server shared-key cipher Admin@123
[DeviceA-radius-radius_server] quit
```

Test the connectivity between the device and RADIUS server.

```
[DeviceA-radius-radius_server] test-aaa user_0001 Admin@123 radius-template radius_server
[DeviceA-radius-radius_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0
255.255.255.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the AAA authentication domain of the virtual gateway to **default**.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain default
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

By default, the authentication domain name of a virtual gateway is extracted from a user name. If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name.

Configure an authentication domain. Create an authentication scheme and an authorization scheme, set the authentication mode of the authentication scheme to RADIUS authentication, set the authorization mode of the authorization scheme to RADIUS authorization, and apply these schemes to an authentication domain.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme radius
[DeviceA-aaa-authentication-radius] authentication-mode radius
[DeviceA-aaa-authentication-radius] quit
[DeviceA-aaa] domain default
[DeviceA-aaa-domain-default] authentication-scheme radius
[DeviceA-aaa-domain-default] radius-server radius_server
[DeviceA-aaa-domain-default] quit
[DeviceA-aaa] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

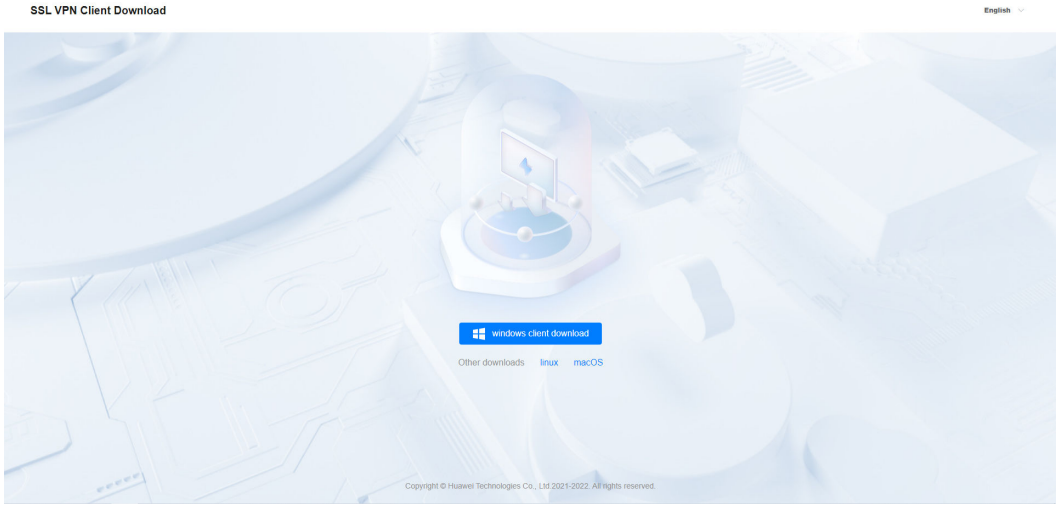
----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal. As shown in the following figure, download the VPN client installation package based on your operating system and install it. For more information, see **VPN Client Download Description**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-34 Downloading the VPN client installation package from the SSL VPN portal



2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme radius
  authentication-mode radius
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server radius_server



#
radius-server template radius_server
 radius-server shared-key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW&%Ui~]V24G5a|t>k+(m)+Y.0K!!!!!
2jp5!!!!!!:!!!!J=y~T09HG7Q-(u'`1p3@X"\>=N~vz&|{~dW!!!!!%+%#
 radius-server authentication 10.1.3.2 1812 weight 80
 undo radius-server user-name domain-included
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone untrust
```

```
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.1 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 0
 service address interface GE0/0/1 port 443
 security
  authentication-domain default
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.18 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Authentication + RADIUS Authorization)

Networking Requirements

On the enterprise network shown in the following figure, the enterprise authenticates access users through the RADIUS server. Authenticated users can access the enterprise intranet.

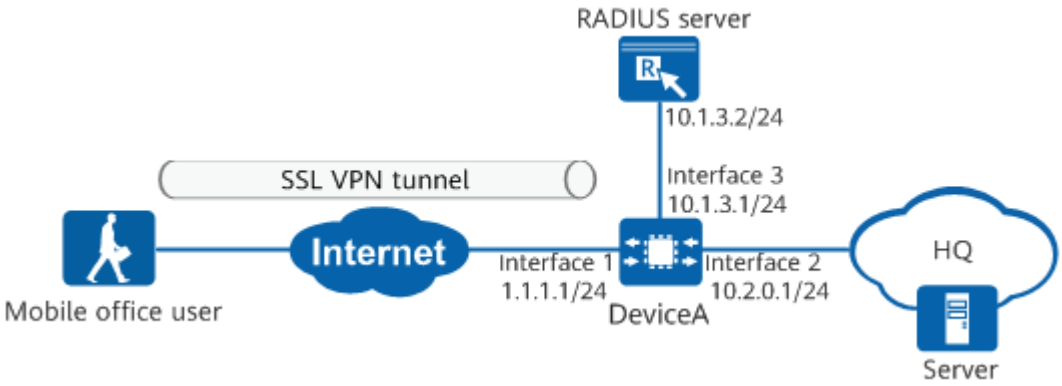
The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. To enhance security, RADIUS authentication with a user name and password is required. In this example, the IP address of the RADIUS server is 10.1.3.2, and IP addresses in the network extension address pool assigned to mobile office users range from 172.16.1.1 to 172.16.1.100.

Figure 9-35 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Configure an IP address for GE 0/0/2 and add it to a security zone.
   a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.
3. Configure an IP address for GE 0/0/3 and add it to a security zone.
   a. In **Interface List**, click in the row of GE 0/0/3 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.1.3.1/24

 Copyright © Huawei Technologies Co., Ltd.

b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust
Destination Zone	trust
Source Address	172.16.1.0/24
Destination Address	10.2.0.1/24
Action	Permit

5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the RADIUS server.

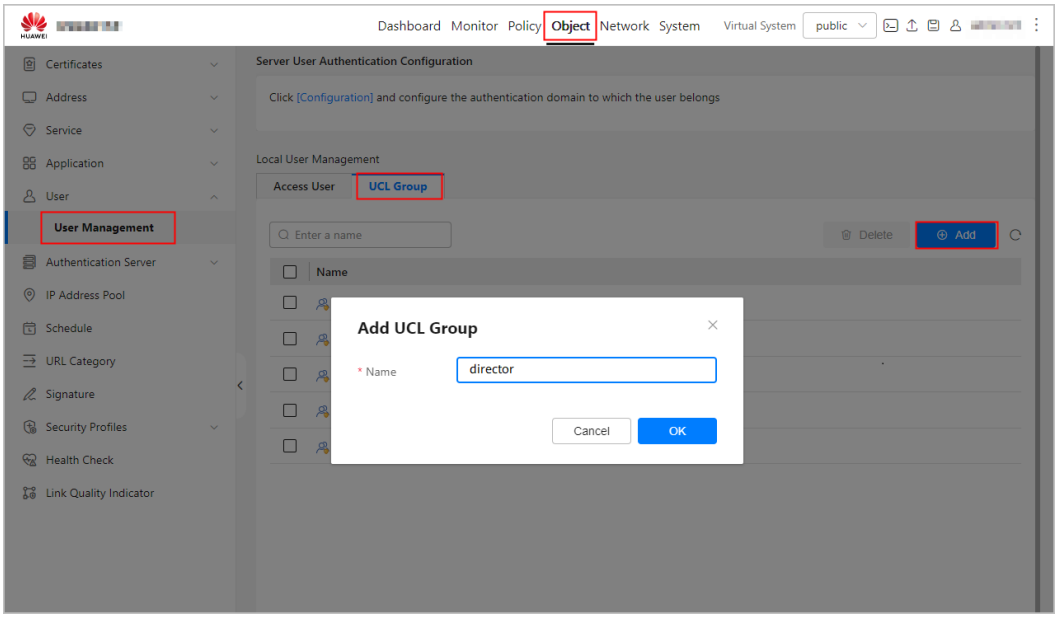
Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.1.3.2/24
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.

 Copyright © Huawei Technologies Co., Ltd.



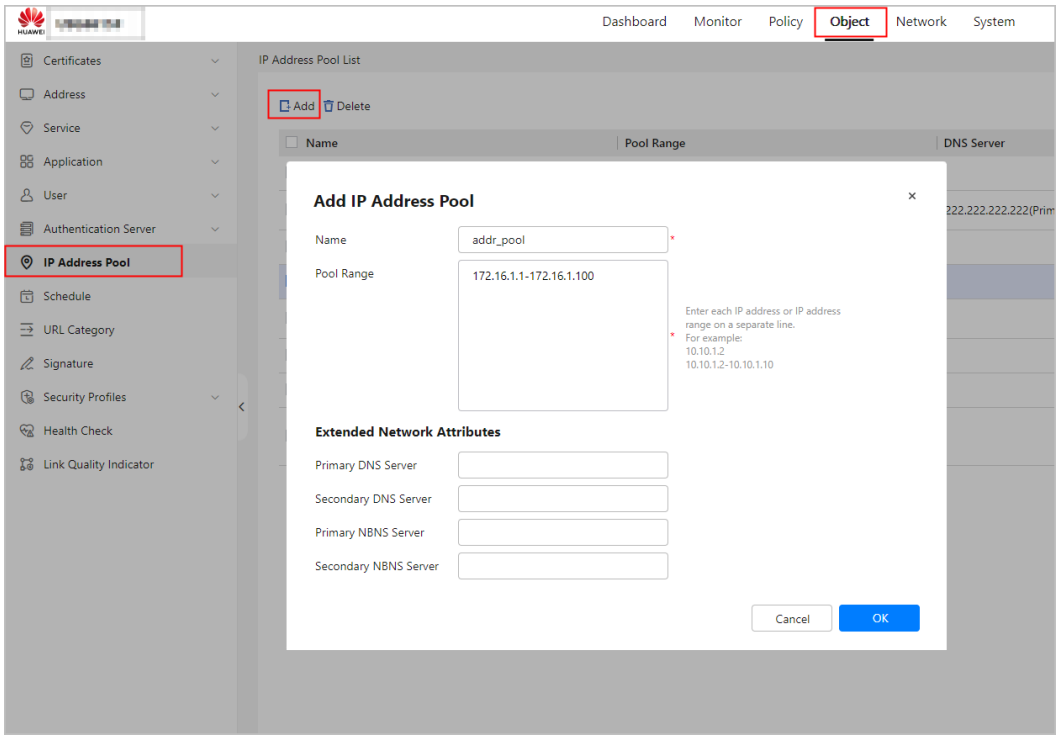
NOTE

This example uses server authorization. That is, the device obtains the security group to which a user belongs from the server and searches for the role corresponding to the security group. Therefore, you need to create a security group with the same name as the server on the device. Otherwise, the security group cannot be referenced by the role. The following creates a security group for reference.

The device uses the Filter-Id attribute value of a user on the RADIUS server as the security group name. The names of security groups created on the device are the same as the corresponding attribute values.

2. Click **OK**.
3. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

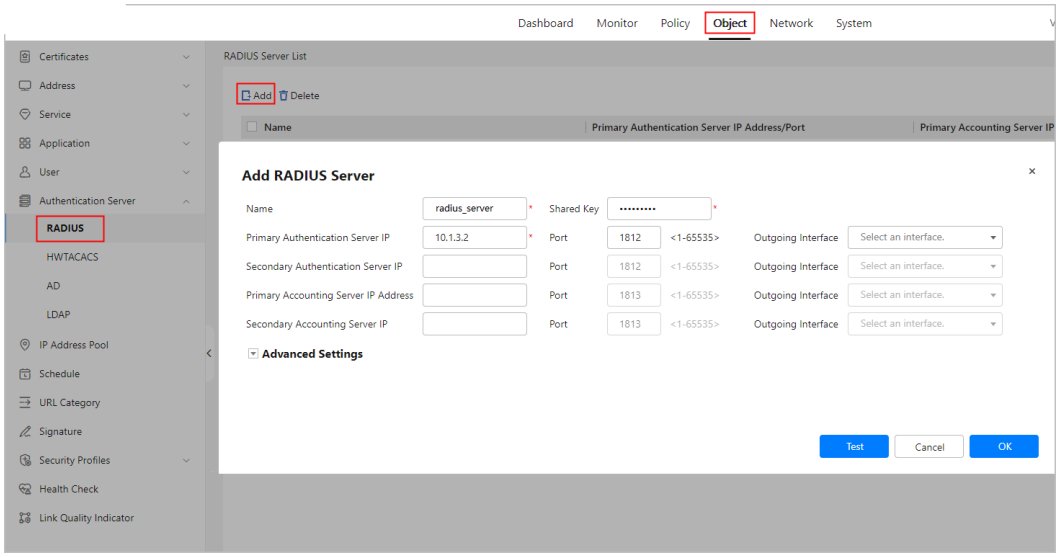
 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **RADIUS**, click **Add**, and set the following parameters to configure the RADIUS server.

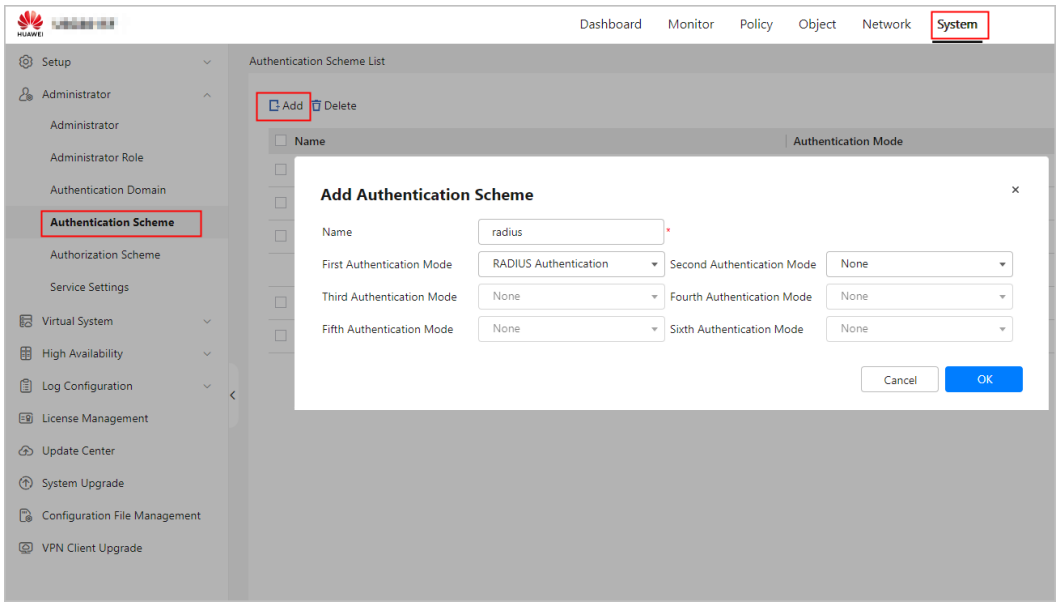


2. Click **OK**.

Step 5 Configure an authentication scheme.

1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.

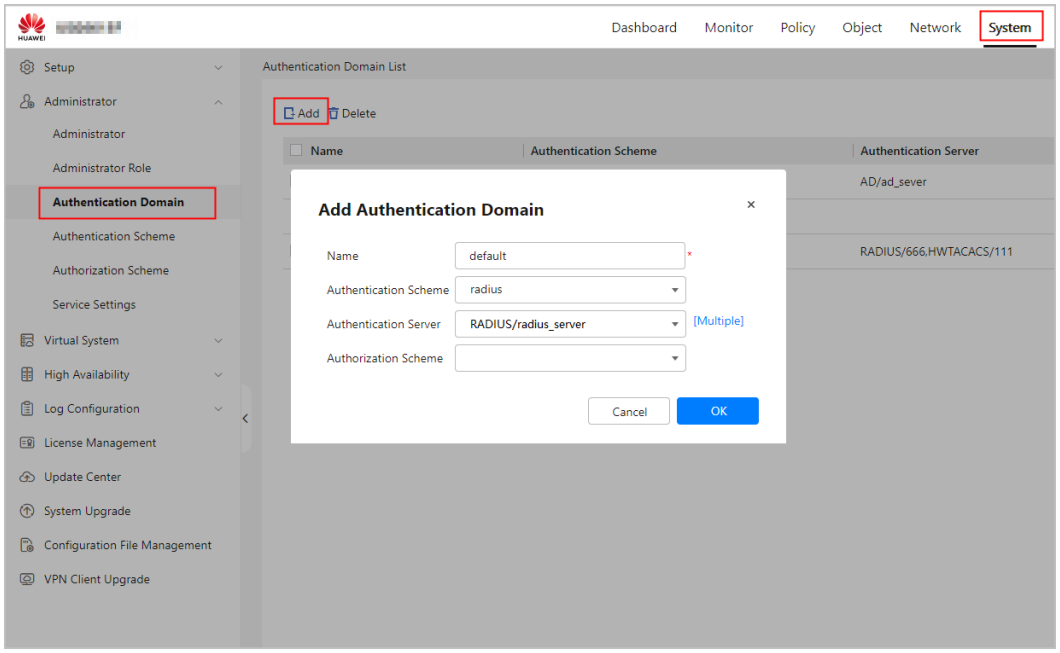
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 6 Configure an authentication domain.

1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.

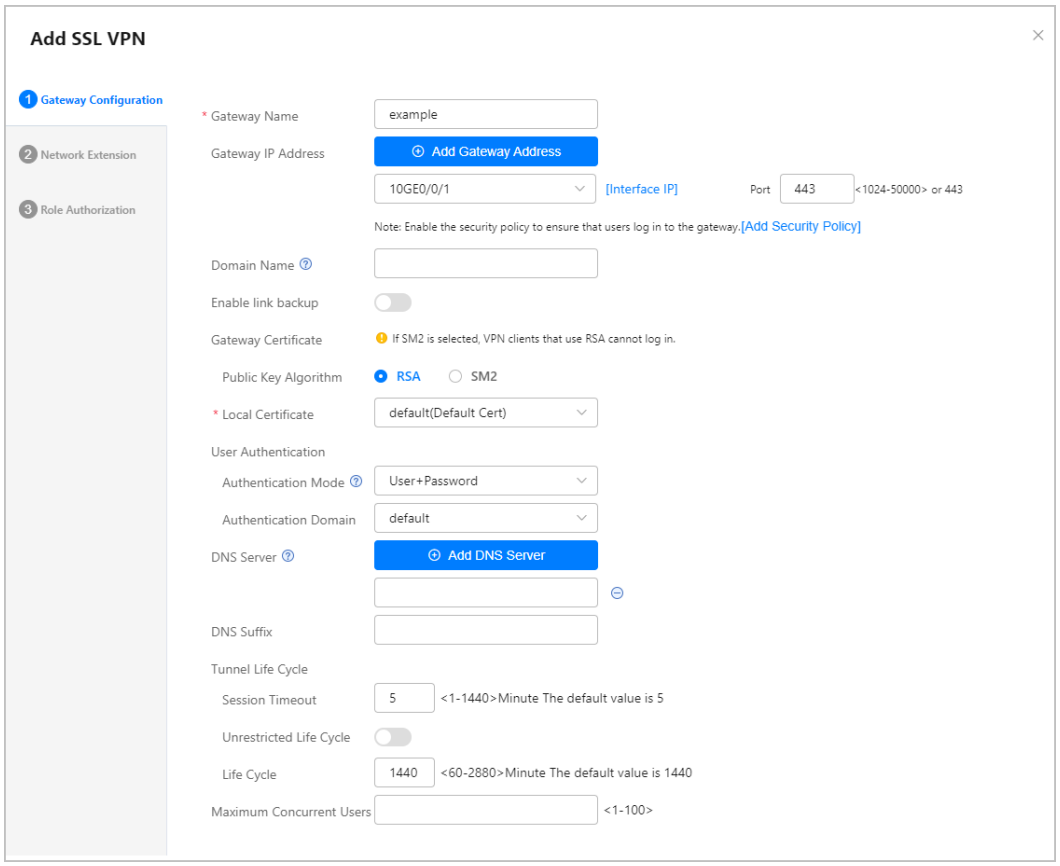


2. Click **OK**.

Step 7 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

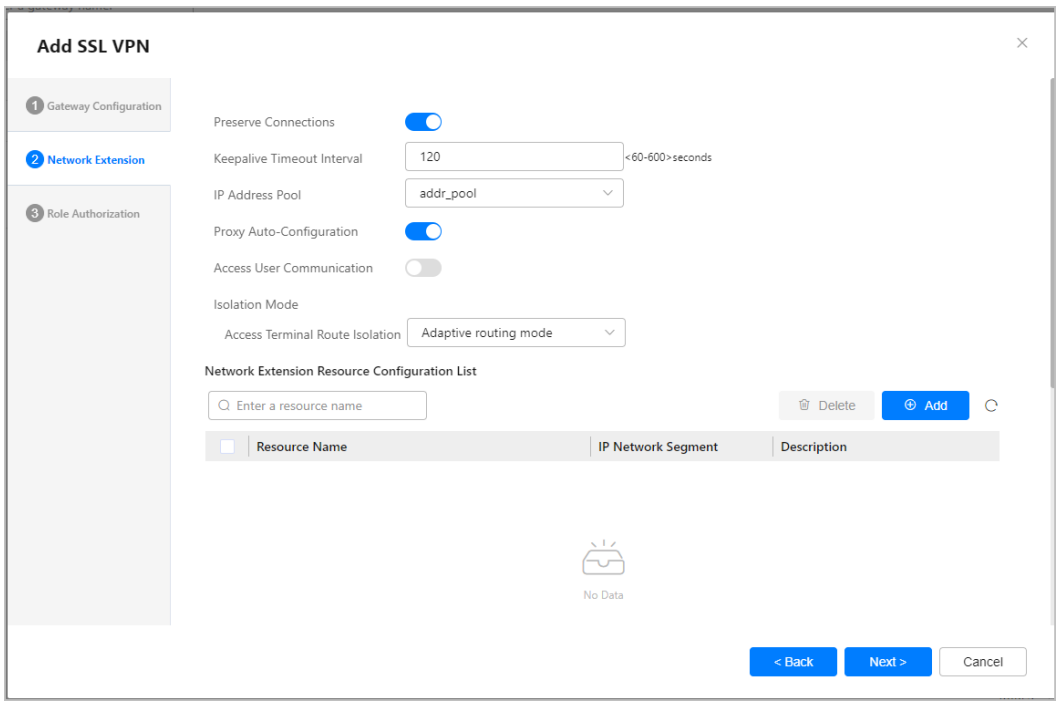
 Copyright © Huawei Technologies Co., Ltd.



3. Click **Next**.

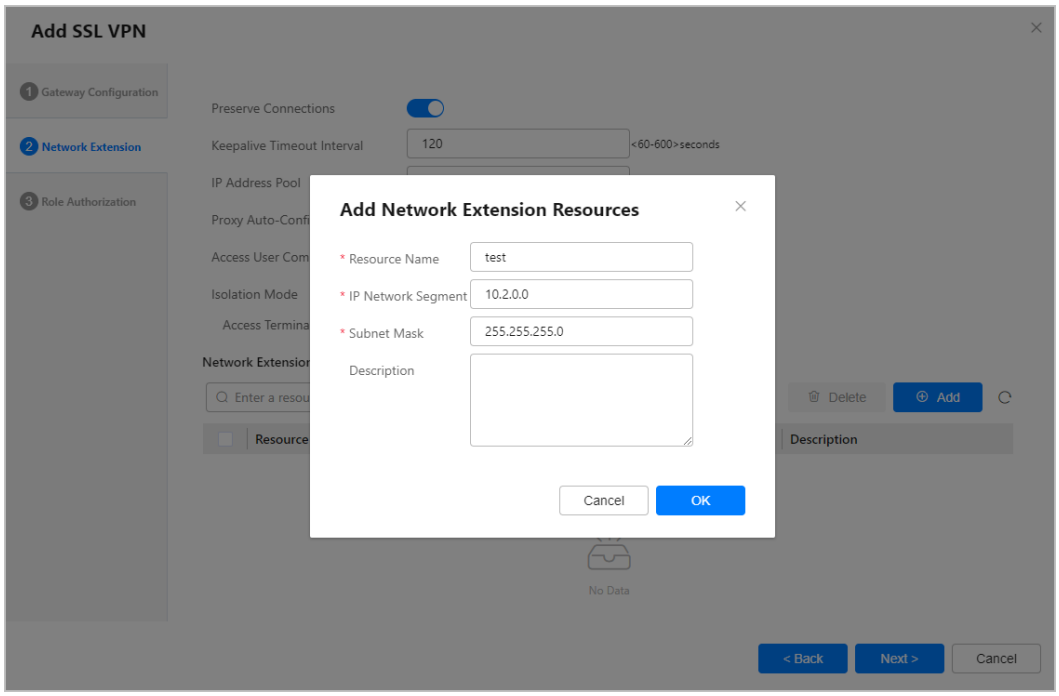
Step 8 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



 Copyright © Huawei Technologies Co., Ltd.

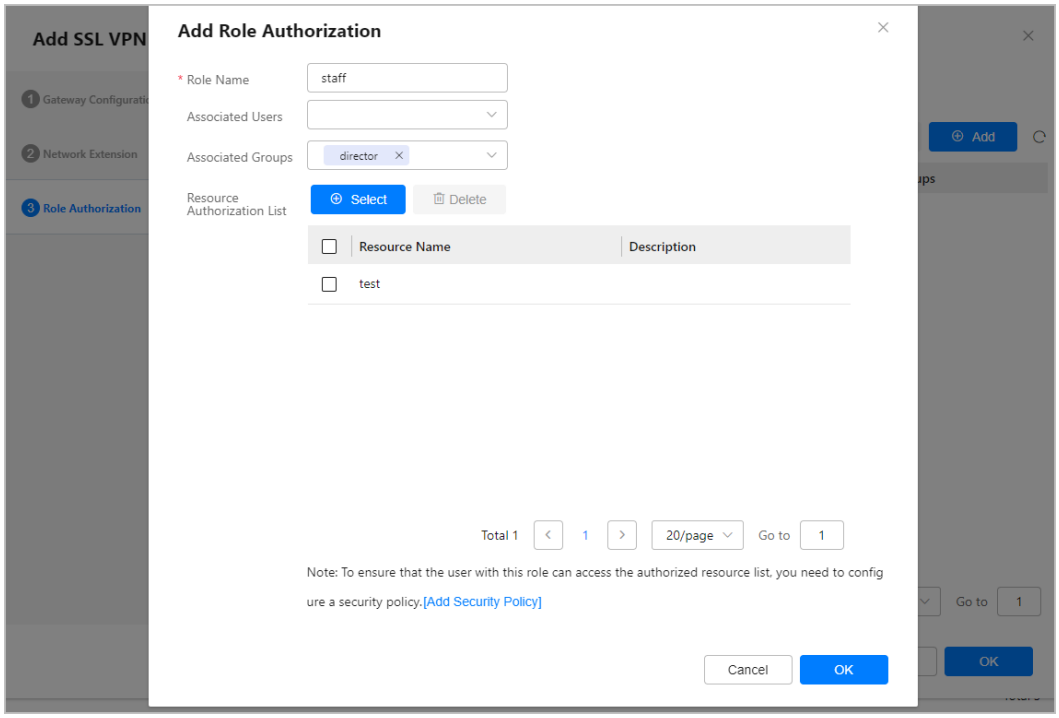
2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.



3. Click **Next**.

Step 9 Configure role authorization for SSL VPN.

1. Configure the role **staff** and associate it with a UCL group and resources.



2. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

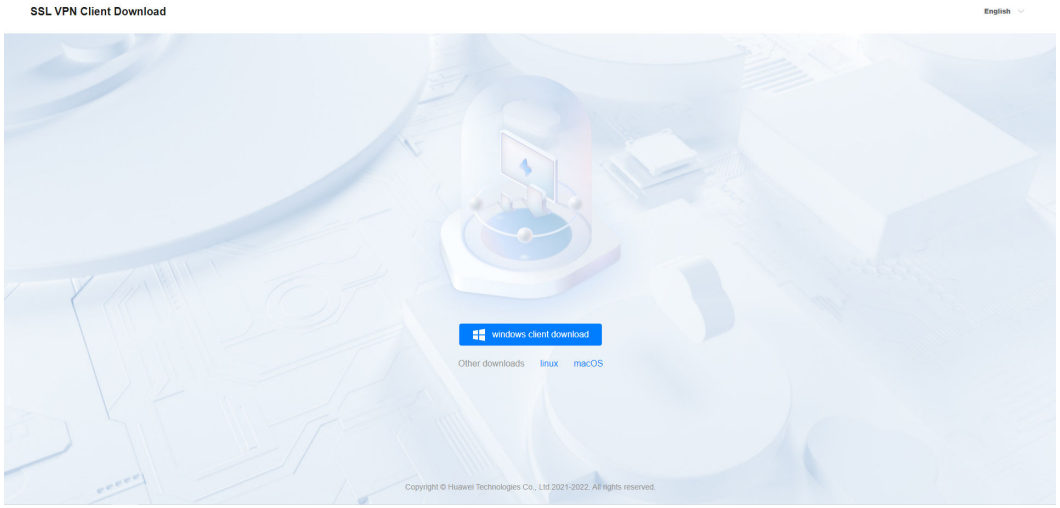
Step 10 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal. As shown in the following figure, download the VPN client installation package based on your operating system and install it. For more information, see **VPN Client Download Description**.

   Figure 9-36 Downloading the VPN client installation package from the SSL VPN portal

2. Connect to the virtual gateway through the client and access intranet resources.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme radius
  authentication-mode radius
  authorization-scheme default
  authorization-mode local
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server radius_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
radius-server template radius_server
 radius-server shared-key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW&%Ui~]V24G5a|t>k+(m)+Y.0K!!!!!
2jp5!!!!!!:!!!!J=y~T09HG7Q-(u`1p3@X"\>=N~vz&|{~dW!!!!!%+%#
 radius-server authentication 10.1.3.2 1812 weight 80
 undo radius-server user-name domain-included
```

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 1
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain default
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

9.19 CLI: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Two-Factor Authentication + Local Authorization)

Networking Requirements

On the enterprise network shown in the following figure, the enterprise authenticates access users through the RADIUS server. Authenticated users can access the enterprise intranet.

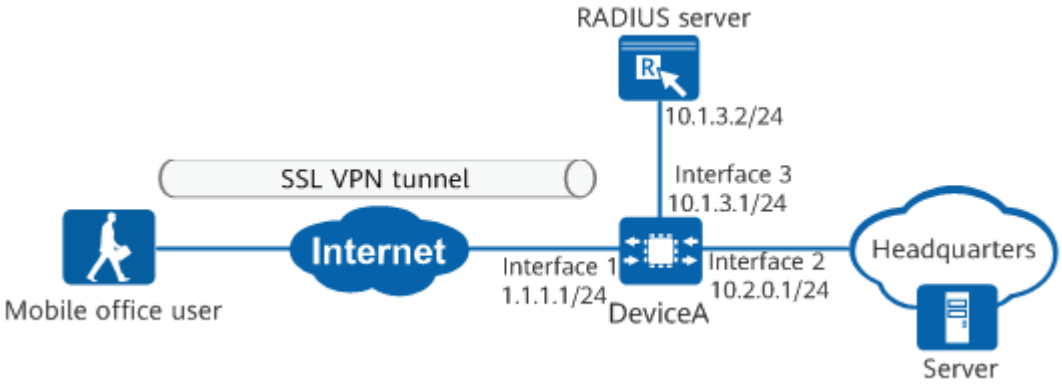
 Copyright © Huawei Technologies Co., Ltd.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. The enterprise has higher security requirements on user authentication. Therefore, RADIUS two-factor authentication needs to be used to authenticate access users. In this example, the IP address of the RADIUS server is 10.1.3.2, and IP addresses in the network extension address pool assigned to mobile office users range from 172.16.1.1 to 172.16.1.100.

Figure 9-37 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface GE0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface GE0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/3.

```
[DeviceA] interface GE0/0/3
[DeviceA-GE0/0/3] ip address 10.1.3.1 24
[DeviceA-GE0/0/3] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface GE0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 and GE 0/0/3 to the Trust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface GE0/0/2
[DeviceA-zone-trust] add interface GE0/0/3
[DeviceA-zone-trust] quit
```

Step 2 Configure SSL VPN security policies.

Configure a security policy to allow users to establish SSL VPN tunnels with the device.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sslvpn_1
[DeviceA-policy-security-rule-policy_sslvpn_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-zone local
[DeviceA-policy-security-rule-policy_sslvpn_1] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-policy_sslvpn_1] action permit
[DeviceA-policy-security-rule-policy_sslvpn_1] quit
```

Configure a security policy to allow users to access intranet resources.

```
[DeviceA-policy-security] rule name policy_sslvpn_2
[DeviceA-policy-security-rule-policy_sslvpn_2] source-zone untrust
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_2] source-address range 172.16.1.1 172.16.1.100
[DeviceA-policy-security-rule-policy_sslvpn_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sslvpn_2] action permit
[DeviceA-policy-security-rule-policy_sslvpn_2] quit
```

Configure a security policy to allow the device to communicate with the RADIUS server.

```
[DeviceA-policy-security] rule name policy_sslvpn_3
[DeviceA-policy-security-rule-policy_sslvpn_3] source-zone local
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-zone trust
[DeviceA-policy-security-rule-policy_sslvpn_3] destination-address 10.1.3.0 24
[DeviceA-policy-security-rule-policy_sslvpn_3] action permit
[DeviceA-policy-security-rule-policy_sslvpn_3] quit
[DeviceA-policy-security] quit
```

Step 3 Create a UCL group.

```
[DeviceA] ucl-group name director
```

Step 4 Configure an IP address pool.

```
[DeviceA] ip pool addr_pool
[DeviceA-ip-pool-addr_pool] section 0 172.16.1.1 172.16.1.100
[DeviceA-ip-pool-addr_pool] quit
```

Step 5 Set parameters for communication between the device and RADIUS server. The parameter settings must be the same as those on the RADIUS server.

Configure the RADIUS server template **radius_server**.

```
[DeviceA] radius-server template radius_server
[DeviceA-radius-radius_server] radius-server authentication 10.1.3.2 1812
[DeviceA-radius-radius_server] radius-server shared-key cipher YsHsjx@123
[DeviceA-radius-radius_server] undo radius-server user-name domain-included
```

Test the connectivity between the device and RADIUS server.

```
[DeviceA-radius-radius_server] test-aaa user_0001 YsHsjx@123 radius-template radius_server
[DeviceA-radius-radius_server] quit
```

Step 6 Configure an SSL VPN virtual gateway.

Create a virtual gateway.

```
[DeviceA] virtual-gateway example 1
[DeviceA-virtual-gateway-example] service address interface GE0/0/1 port 443
```

 Copyright © Huawei Technologies Co., Ltd.

Set the maximum number of concurrent users allowed by the SSL VPN virtual gateway.

```
[DeviceA-virtual-gateway-example] max-online-user 100
```

Step 7 Configure the network extension function.

Set the keepalive timeout period.

```
[DeviceA-virtual-gateway-example] service
[DeviceA-virtual-gateway-example-service] network-extension keep-alive timeout 120
```

Configure a network extension address pool.

```
[DeviceA-virtual-gateway-example-service] network-extension ip-pool addr_pool
```

Set the network extension routing mode to **adapt**.

```
[DeviceA-virtual-gateway-example-service] network-extension mode adapt
```

Configure the resources accessible to network extension users.

```
[DeviceA-virtual-gateway-example-service] network-extension resource test ip-subnet 10.2.0.0 255.255.255.0
[DeviceA-virtual-gateway-example-service] quit
```

Step 8 Configure user authentication.

Set the AAA authentication domain of the virtual gateway to **default**.

```
[DeviceA-virtual-gateway-example] security
[DeviceA-virtual-gateway-example-security] authentication-domain default
[DeviceA-virtual-gateway-example-security] quit
[DeviceA-virtual-gateway-example] quit
```

NOTE

By default, the authentication domain name of a virtual gateway is extracted from a user name. If the virtual gateway is bound to an authentication domain, the user name entered for a login cannot carry authentication domain information. If the user name carries an authentication domain name, the gateway considers the at sign (@) and the string following @ as a part of the user name, but not as an authentication domain name.

Configure an authentication domain. Create an authentication scheme, set the authentication mode to RADIUS authentication, and apply the scheme to an authentication domain.

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme radius
[DeviceA-aaa-authentication-radius] authentication-mode radius
[DeviceA-aaa-authentication-radius] quit
[DeviceA-aaa] domain default
[DeviceA-aaa-domain-default] authentication-scheme radius
[DeviceA-aaa-domain-default] radius-server radius_server
[DeviceA-aaa-domain-default] quit
[DeviceA-aaa] quit
```

Set the local access user name to **abc**, password to **Helloworld@135**, access type to **sslvpn**, and bind the user to the UCL group **director**.

```
[DeviceA-aaa] local-access-user abc
[DeviceA-aaa-access-user-abc] password cipher Helloworld@135
[DeviceA-aaa-access-user-abc] service-type sslvpn
[DeviceA-aaa-access-user-abc] ucl-group director
[DeviceA-aaa-access-user-abc] quit
```

Step 9 Configure role authorization for SSL VPN.

Create the role **staff** and associate it with a UCL group and resources.

 Copyright © Huawei Technologies Co., Ltd.

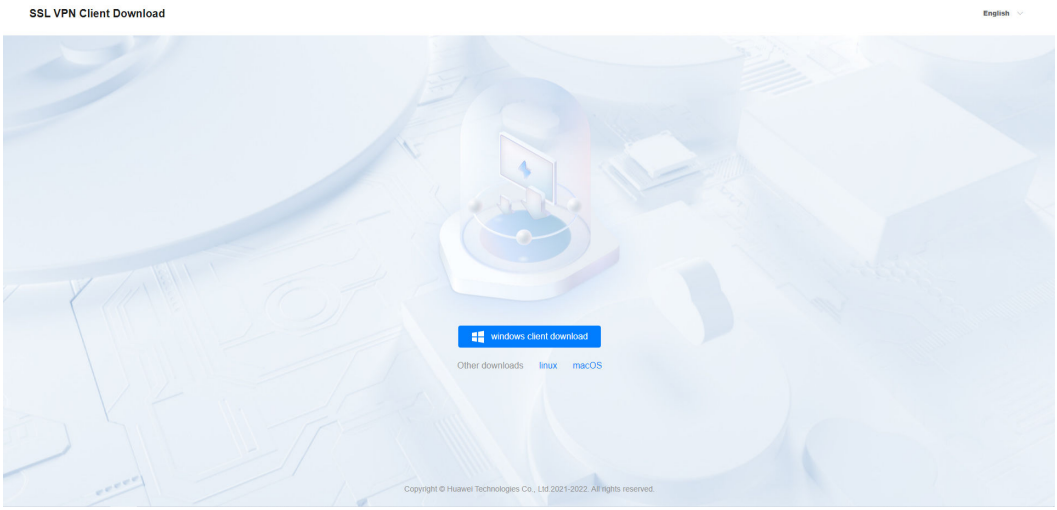
```
[DeviceA] virtual-gateway example
[DeviceA-virtual-gateway-example] role staff
[DeviceA-virtual-gateway-example-role-staff] group director
[DeviceA-virtual-gateway-example-role-staff] resource test
[DeviceA-virtual-gateway-example-role-staff] quit
[DeviceA-virtual-gateway-example] quit
```

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal. As shown in the following figure, download the VPN client installation package based on your operating system and install it. For more information, see **VPN Client Download Description**.

   Figure 9-38 Downloading the VPN client installation package from the SSL VPN portal

2. Enter the user name and password on the client to log in to the virtual gateway. If the user name and password are successfully authenticated, the dynamic verification code page is displayed. Enter the dynamic verification code and click **OK**. The login is successful.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme radius
  authentication-mode radius
  authorization-scheme default
  authorization-mode local
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server radius_server
 local-access-user abc
```

 Copyright © Huawei Technologies Co., Ltd.

```
 service-type sslvpn
 ucl-group director
#
radius-server template radius_server
 radius-server shared-key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW&%Ui~]V24G5a|t>k+(m)+Y.0K!!!!!
2jp5!!!!!!:!!!!J=y~T09HG7Q-(u`1p3@X"\>=N~vz&|{~dW!!!!!%+%#
 radius-server authentication 10.1.3.2 1812 weight 80
 undo radius-server user-name domain-included
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.1.3.0 mask 255.255.255.0
  action permit
#
virtual-gateway example 1
 max-online-user 100
 service address interface GE0/0/1 port 443
 security
  authentication-domain default
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

9.20 Web: Example for Configuring Mobile Office Users to Access the Enterprise HQ through SSL VPN (RADIUS Two-Factor Authentication + Local Authorization)

Networking Requirements

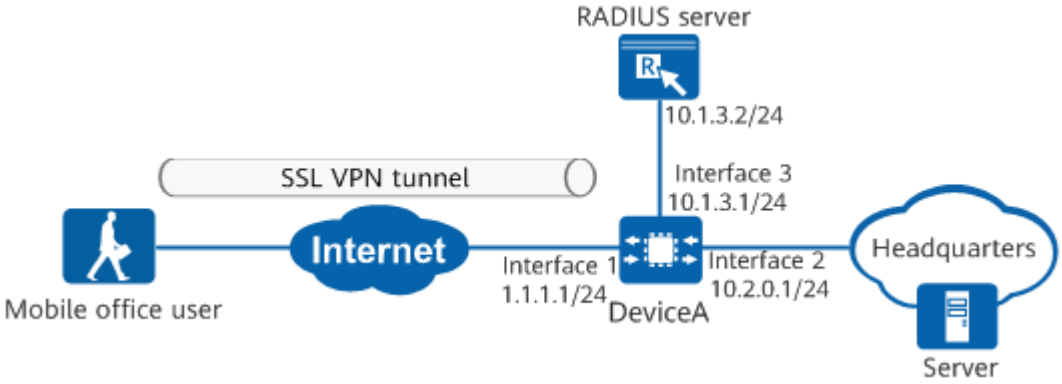
On the enterprise network shown in the following figure, the enterprise authenticates access users through the RADIUS server. Authenticated users can access the enterprise intranet.

The enterprise wants senior executives to be able to obtain an IP address when they are on the move or at home and access various intranet resources as if they were working on the intranet. The enterprise has higher security requirements on user authentication. Therefore, RADIUS two-factor authentication needs to be used to authenticate access users. In this example, the IP address of the RADIUS server is 10.1.3.2, and IP addresses in the network extension address pool assigned to mobile office users range from 172.16.1.1 to 172.16.1.100.

Figure 9-39 Network diagram for configuring mobile office users to access the HQ through SSL VPN

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



Procedure

Step 1 Configure IP addresses for interfaces and add interfaces to security zones.

1. Configure an IP address for GE 0/0/1 and add it to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click in the row of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

IP Address	1.1.1.1/24

c. Click **OK**.

2. Configure an IP address for GE 0/0/2 and add it to a security zone.

a. In **Interface List**, click in the row of GE 0/0/2 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

3. Configure an IP address for GE 0/0/3 and add it to a security zone.

a. In **Interface List**, click in the row of GE 0/0/3 and set the following parameters.

Zone	trust
IPv4	
IP Address	10.1.3.1/24

b. Click **OK**.

Step 2 Configure SSL VPN security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the following parameters to configure a security policy for senior executives. The policy allows users to establish the SSL VPN tunnel with the device.

Name	policy_sslvpn_1
Source Zone	untrust
Destination Zone	local
Destination Address	1.1.1.1/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure another security policy. The policy allows users to access intranet resources.

Name	policy_sslvpn_2
Source Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	trust
Source Address	172.16.1.1-172.16.1.100
Destination Address	10.2.0.1/24
Action	Permit

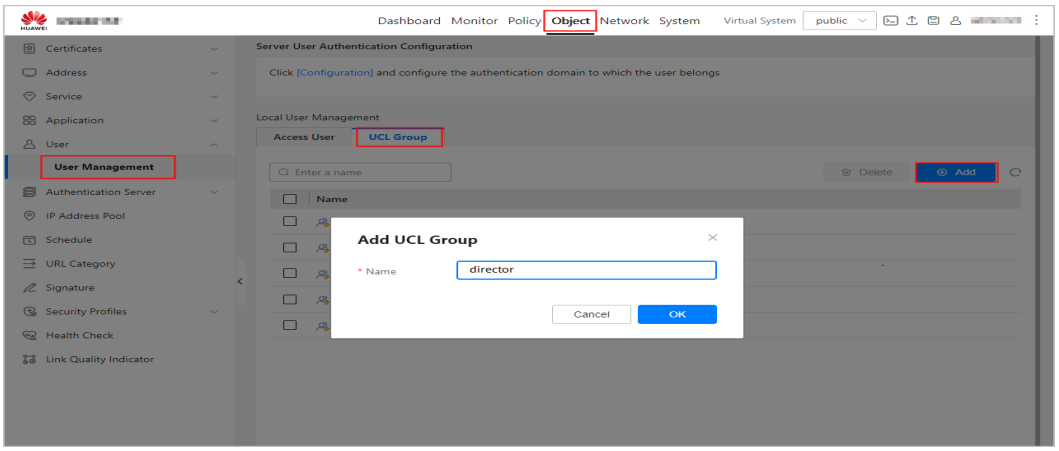
5. Click **OK**.
6. Repeat the preceding steps to configure a security policy to allow the device to communicate with the RADIUS server.

Name	policy_sslvpn_3
Source Zone	local
Destination Zone	trust
Destination Address	10.1.3.2/24
Action	Permit

7. Click **OK**.

Step 3 Configure a security group and an address pool.

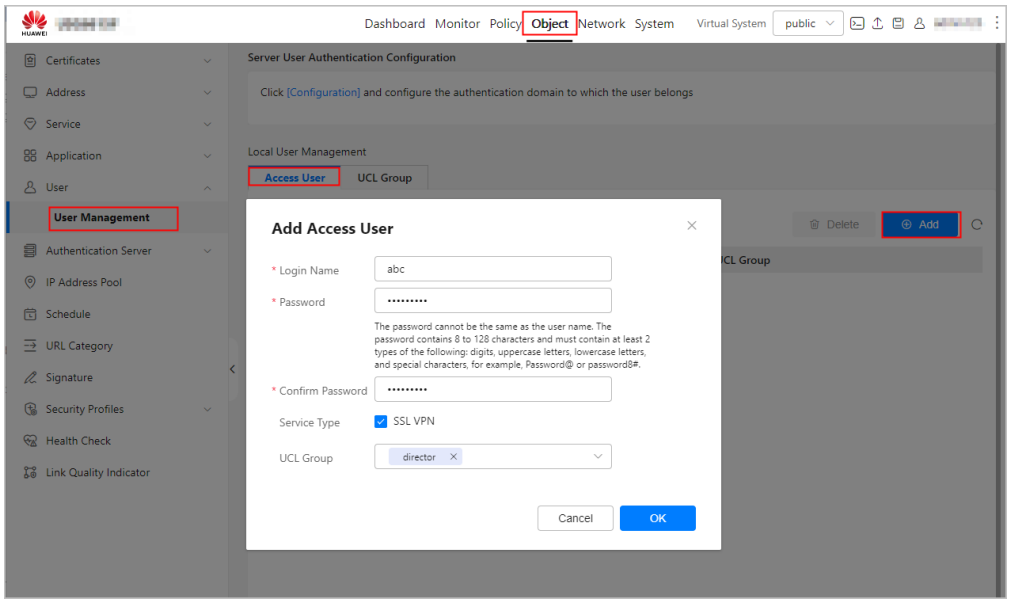
1. Choose **Object** > **User** > **User Management**. On the **UCL Group** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a security group.



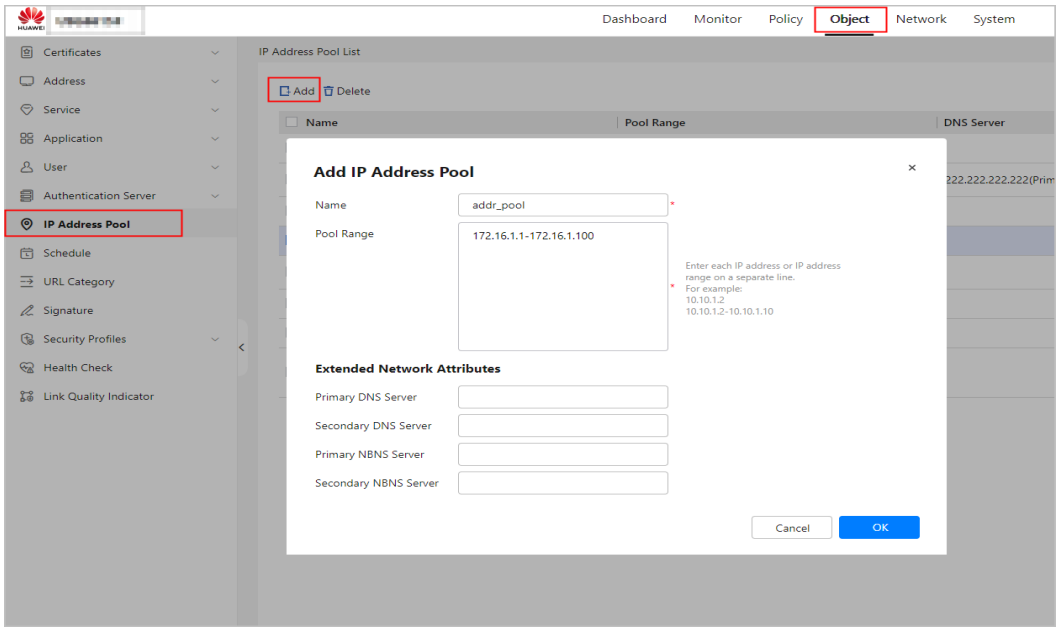
2. Click **OK**.
3. On the **Access User** tab page of **Local User Management**, click **Add**, and set the following parameters to configure a user.

   The user **abc** belongs to the user group **director** and the password is **YsHsjx_202206**.

 Copyright © Huawei Technologies Co., Ltd.



4. Click **OK**.
5. Choose **Object** > **IP Address Pool**, click **Add**, and set the following parameters to configure the address pool **addr_pool**.

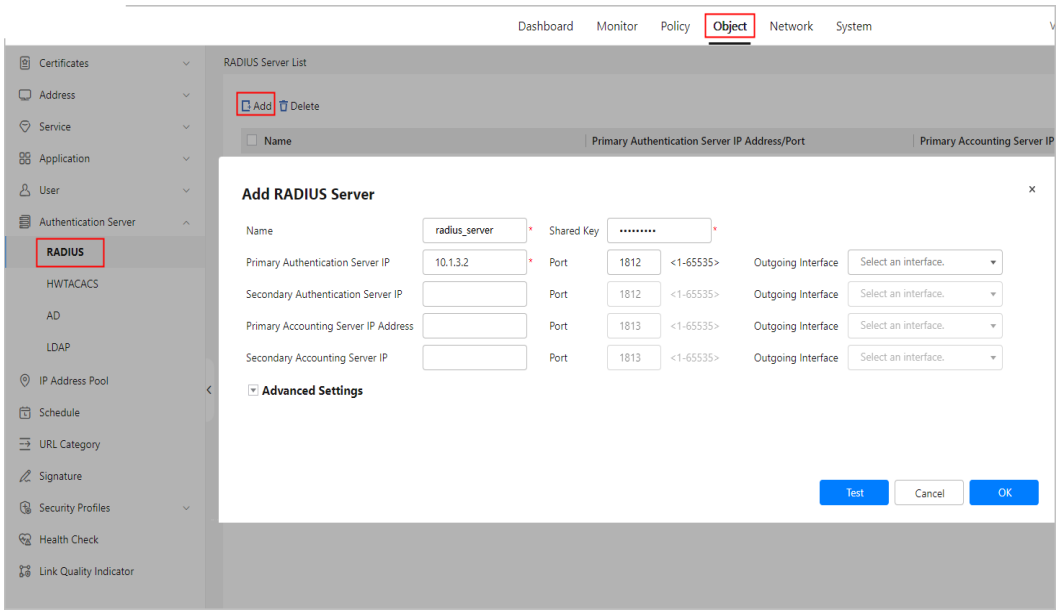


6. Click **OK**.

Step 4 Configure the authentication server.

1. Choose **Object** > **Authentication Server** > **RADIUS**, click **Add**, and set the following parameters to configure the RADIUS server.

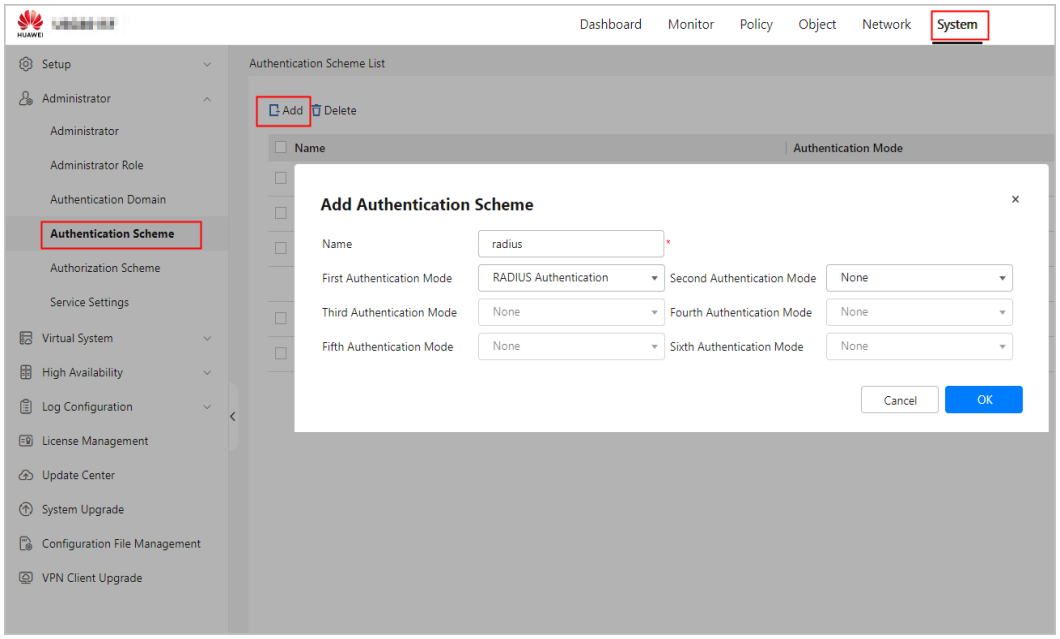
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 5 Configure an authentication scheme.

1. Choose **System** > **Administrator** > **Authentication Scheme**, click **Add**, and set the following parameters to configure an authentication scheme.

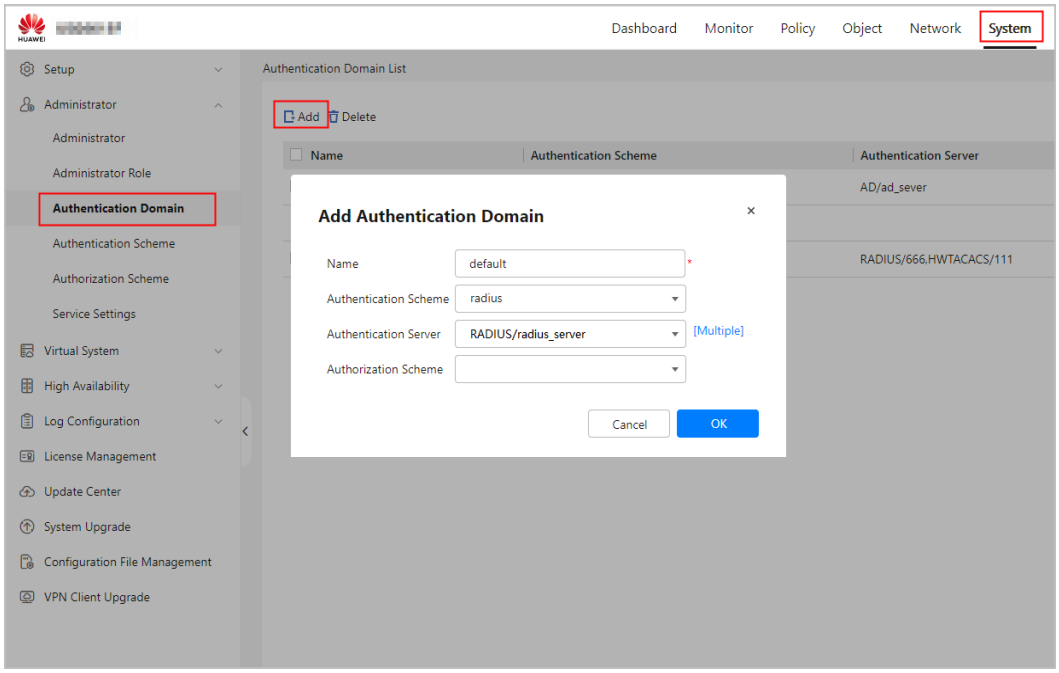


2. Click **OK**.

Step 6 Configure an authentication domain.

1. Choose **System** > **Administrator** > **Authentication Domain**, click **Add**, and set the following parameters to configure an authentication domain.

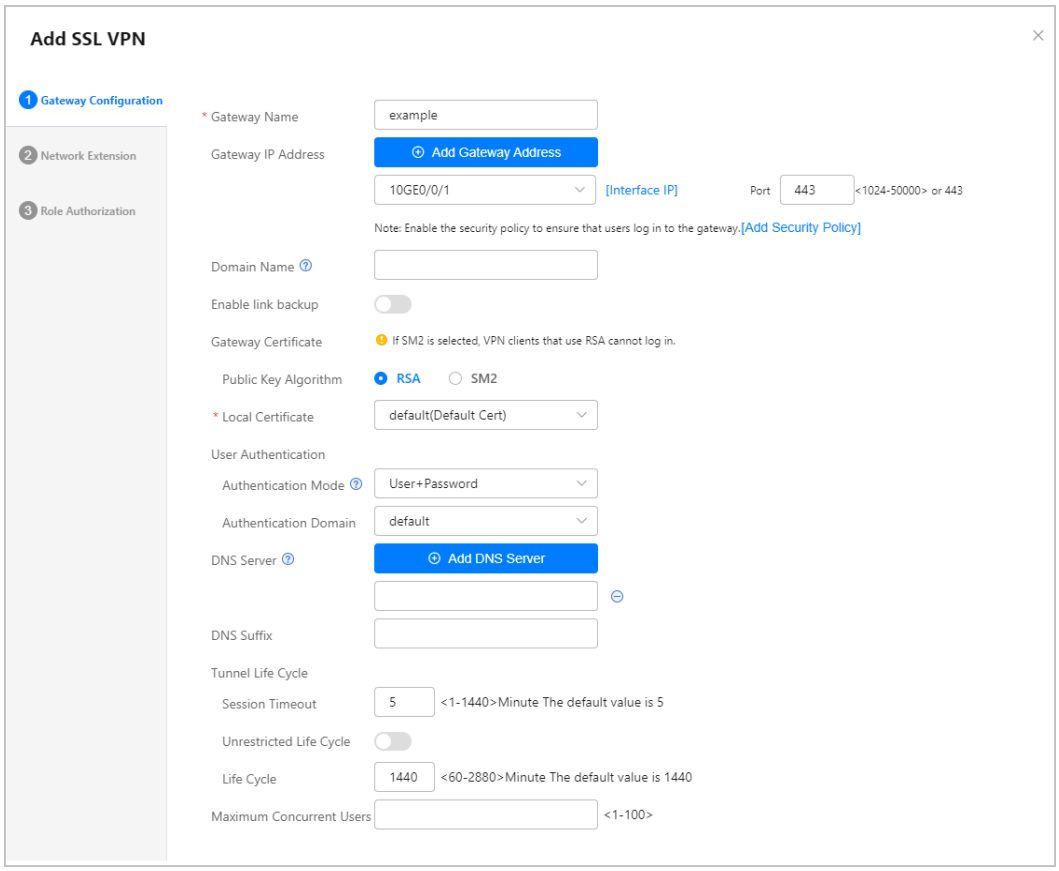
 Copyright © Huawei Technologies Co., Ltd.



2. Click **OK**.

Step 7 Configure an SSL VPN virtual gateway.

1. Choose **Network** > **SSL VPN** > **SSL VPN**.
2. Click **Add** and set the following parameters. You can use the default session timeout interval and life cycle.

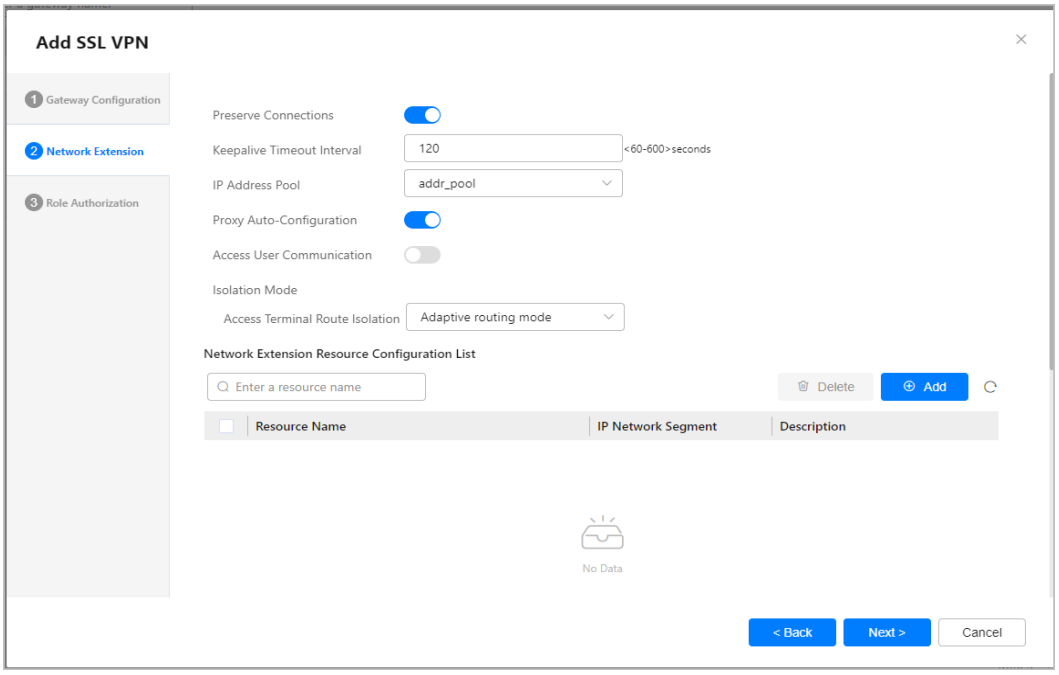


 Copyright © Huawei Technologies Co., Ltd.

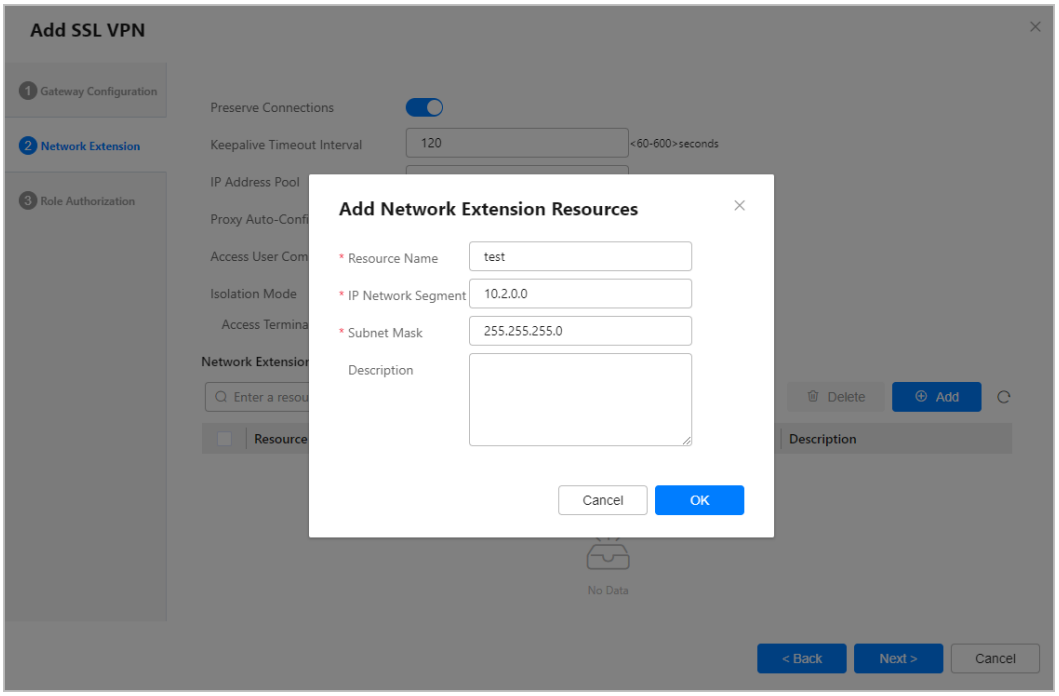
3. Click **Next**.

Step 8 Configure the network extension function.

1. Set the keepalive timeout period, address pool, and routing mode for network extension.



2. In **Network Extension Resource Configuration**, click **Add**, and configure a network extension resource.

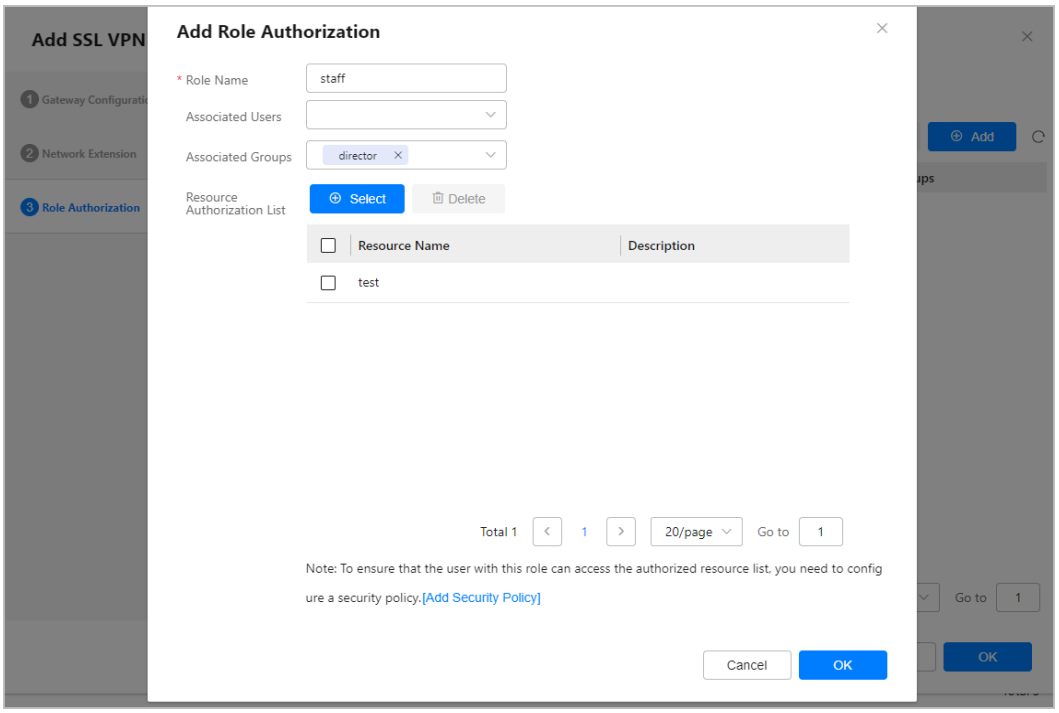


3. Click **Next**.

Step 9 Configure role authorization for SSL VPN.

 Copyright © Huawei Technologies Co., Ltd.

1. Configure the role **staff** and associate it with a UCL group and resources.



2. Click **OK**.

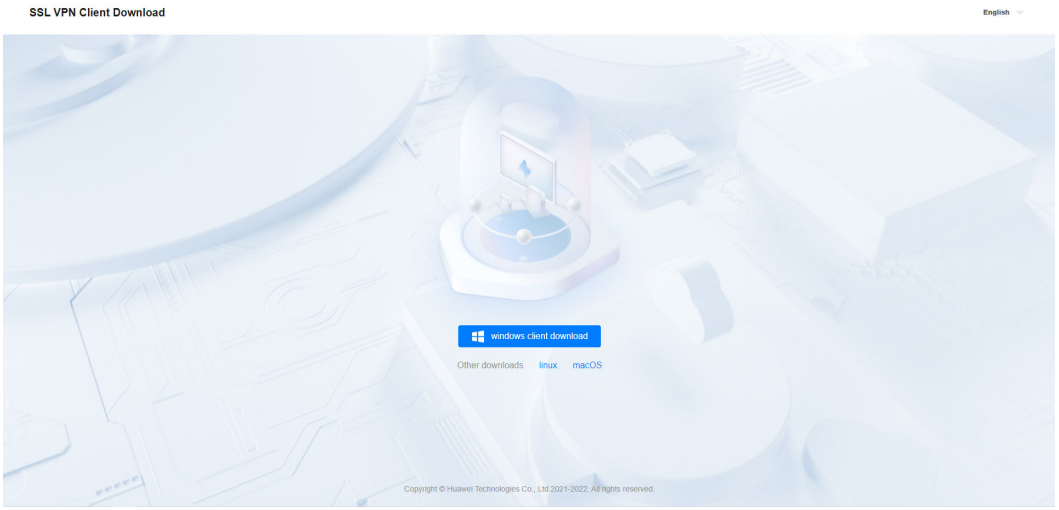
Step 10 Click **OK**. An SSL VPN is created.

----End

Verifying the Configuration

1. Enter **https://1.1.1.1:443** in the address box of the browser to access the SSL VPN portal. As shown in the following figure, download the VPN client installation package based on your operating system and install it. For more information, see **VPN Client Download Description**.

Figure 9-40 Downloading the VPN client installation package from the SSL VPN portal



2. Enter the user name and password on the client to log in to the virtual gateway. If the user name and password are successfully authenticated, the dynamic verification code page is displayed. Enter the dynamic verification code and click **OK**. The login is successful.

Configuration Scripts

```
#
 sysname DeviceA
#
ip pool addr_pool
 section 0 172.16.1.1 172.16.1.100
#
ucl-group name director index 1
#
aaa
  authentication-scheme radius
  authentication-mode radius
  authorization-scheme default
  authorization-mode local
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server radius_server
 local-access-user abc
  service-type sslvpn
  ucl-group director
#
radius-server template radius_server
 radius-server shared-key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!cZa'*[{[xW&%Ui~]V24G5a|t>k+(m)+Y.0K!!!!!
2jp5!!!!!!:!!!!J=y~T09HG7Q-(u`1p3@X"\>=N~vz&|{~dW!!!!!%+%#
 radius-server authentication 10.1.3.2 1812 weight 80
 undo radius-server user-name domain-included
#
interface 10GE
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE
 ip address 10.2.0.1 255.255.255.0
#
interface 10GE
 ip address 10.1.3.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface 10GE
 add interface 10GE
#
firewall zone untrust
 set priority 5
 add interface 10GE
#
security-policy
 rule name policy_sslvpn_1
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_2
  source-zone untrust
  destination-zone trust
  source-address range 172.16.1.1 172.16.1.100
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
 rule name policy_sslvpn_3
  source-zone local
  destination-zone trust
  destination-address 10.1.3.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
  action permit
#
virtual-gateway example 1
 service address interface 10GE port 443
 security
  authentication-domain default
 service
  network-extension ip-pool addr_pool
  network-extension resource test ip-subnet 10.2.0.0 255.255.0.0
 role staff 0
  group director
  resource test
#
return
```

10 Identity Management

10.1 CLI: Example for Configuring RADIUS SSO (In-path Mode)

10.2 CLI: Example for Configuring RADIUS SSO (Off-path Mode)

10.3 CLI: Example for Configuring TSM SSO

10.1 CLI: Example for Configuring RADIUS SSO (In-path Mode)

Networking Requirements

As shown in **Figure 10-1**, an enterprise deploys DeviceA as the egress gateway at the network border to connect the intranet and the Internet. The details are as follows:

- Employees access the network through the NAS device.
- The NAS authenticates employees through the RADIUS server which stores user information.
- Users on the enterprise network include R&D and marketing employees.

The network administrator of the enterprise wants to use the user management mechanism provided by DeviceA to identify intranet IP addresses as users so as to provide reference for performing user-based network behavior control and network permission assignment. The specific requirements are as follows:

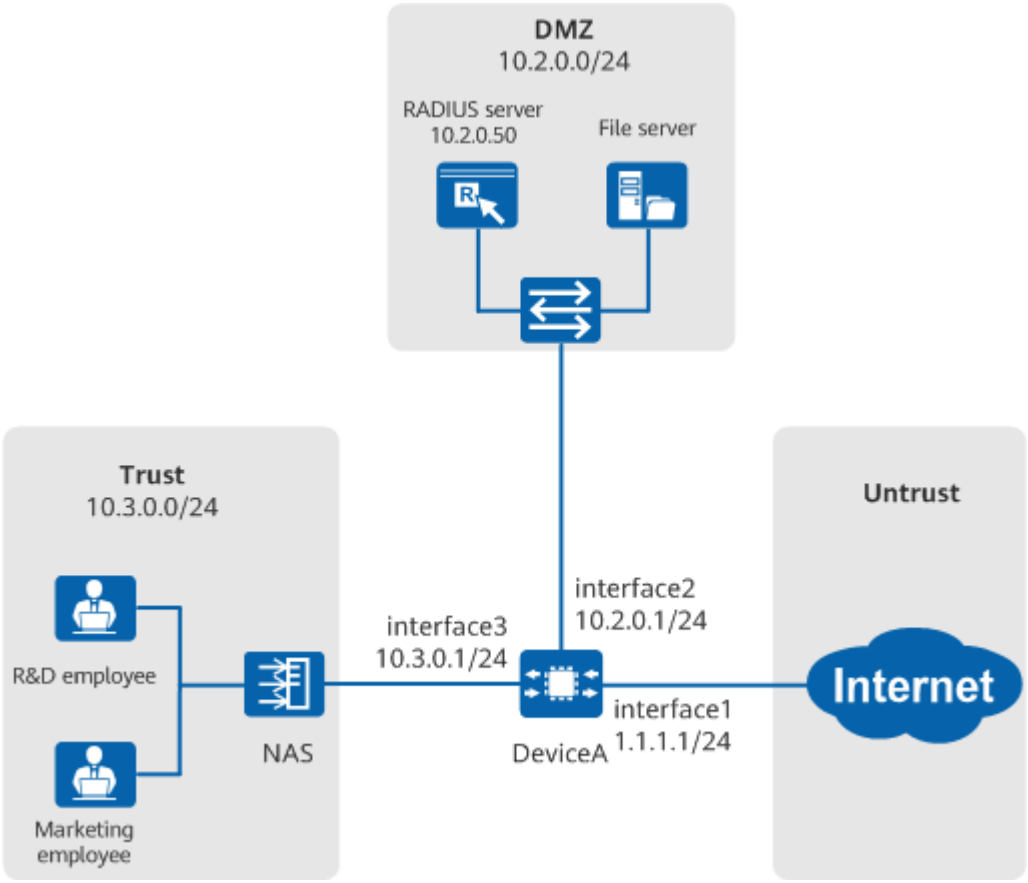
- DeviceA parses sub-attribute 60 in the vendor-specific attribute of RADIUS accounting packets and uses the parsed attribute value as the security group name of the user.
- R&D and marketing employees can access network resources without the need to be authenticated again by DeviceA after passing RADIUS authentication. The identifiers of the R&D and marketing employees are the accounts used in the RADIUS authentication.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-1 Networking diagram of RADIUS SSO

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Item	Data	Description
Security group to which the user belongs	Security group name for R&D employees: research Security group name for marketing employees: marketing	Configure a security group on DeviceA. The security group name must be the same as the attribute value of the security group on the server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
RADIUS SSO	• RADIUS SSO: enabled • Working mode: in-path • Interface for receiving accounting packets: GE0/0/3 • Parsed traffic: 10.2.0.50:1813 (server IP address: accounting port)	Set SSO parameters on DeviceA to parse the RADIUS accounting packets that pass through DeviceA so as to obtain the mappings between users and IP addresses.

Configuration Roadmap

NOTE

This example describes only the configuration of user authentication.

1. Set RADIUS SSO parameters on DeviceA.
2. To prevent users from being continuously re-authenticated due to frequent login and logout on DeviceA, you are advised to set the online user timeout period on DeviceA to be longer than the interval for updating RADIUS accounting packets. In this example, the online user timeout period is set to 480 minutes.
3. Configure a security policy to ensure that the packets exchanged between the NAS device and RADIUS server pass through DeviceA.

Procedure

Step 1 Configure IP addresses for the interfaces on DeviceA and assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Set RADIUS SSO parameters on DeviceA.

```
[DeviceA] identity-management
[DeviceA-identity-management]undo userlog login-out enable
[DeviceA-identity-management]sso-radius
[DeviceA-identity-management-sso-radius] mode in-path
[DeviceA-identity-management-sso-radius] ingress-interface ge 0/0/3
[DeviceA-identity-management-sso-radius] server ip 10.2.0.50 port 1813
[DeviceA-identity-management-sso-radius] security-group attribute-id vendor-specific 60 delimiter ,
[DeviceA-identity-management-sso-radius] online-user aging-time 480
[DeviceA-identity-management-sso-radius] radius-sso enable
[DeviceA-identity-management-sso-radius] quit
[DeviceA-identity-management]quit
```

Step 3 Create security groups on DeviceA.

```
[DeviceA] ucl-group name research
[DeviceA] ucl-group name marketing
```

NOTE

In the example of **Configuring RADIUS SSO Parameters on the Device**, the attribute whose value is used as the security group name is configured in RADIUS accounting packets. DeviceA parses the attribute value as the name of the security group to which the user belongs and searches for a policy based on the security group. Therefore, you need to configure a security group with the same name as the security group attribute value on DeviceA in advance. Otherwise, no policy can reference the security group.

If you do not need to use the RADIUS attribute value as the security group name, create a security group on the local device as required and configure a user with the same name (**local-access-user**) on the serve. In this case, run the **security-group priority-type local-first** command in the system view to enable DeviceA to preferentially search for the security group to which the local user belongs.

Step 4 Configure a security policy.

Configure a security policy for traffic from the Trust zone (where the users and NAS device reside) to the DMZ (where the RADIUS server resides), so that users can be authenticated by the RADIUS SSO server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_radius
[DeviceA-policy-security-rule-policy_sec_radius] source-zone trust
[DeviceA-policy-security-rule-policy_sec_radius] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_radius] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sec_radius] action permit
[DeviceA-policy-security-rule-policy_sec_radius] quit
```

Configure a security policy to allow users to access the Internet.

```
[DeviceA-policy-security] rule name policy_sec_02
[DeviceA-policy-security-rule-policy_sec_02] source-zone trust
[DeviceA-policy-security-rule-policy_sec_02] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_02] user ucl-group research
[DeviceA-policy-security-rule-policy_sec_02] user ucl-group marketing
[DeviceA-policy-security-rule-policy_sec_02] action permit
[DeviceA-policy-security-rule-policy_sec_02] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

- R&D employees can access network resources after they successfully access the NAS device using RADIUS accounts and passwords.
- Marketing employees can access network resources after they successfully access the NAS device using RADIUS accounts and passwords.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display identity-management online-user** command on DeviceA to view information about online users.

```
<DeviceA> display identity-management online-user verbose
Current Total Number: 2
---------------------------------------------------------------------------
Vsys Index: 0
IP Address: 10.3.0.2
User Name : user1
Login Time: 2022-10-27 20:26:05  Online Time 00:07:58  Time-left: 07:52:02
Authentication Mode: RADIUS SSO
Security Group: research
---------------------------------------------------------------------------
Vsys Index: 0
IP Address: 10.3.0.3
User Name : user2
Login Time: 2022-10-27 20:26:05  Online Time 00:08:02  Time-left: 07:51:58
Authentication Mode: RADIUS SSO
Security Group: marketing
---------------------------------------------------------------------------
```

Configuration Scripts

```
#
sysname DeviceA
#
ucl-group name research
ucl-group name marketing
#
identity-management
 undo userlog login-out enable
 sso-radius
  mode in-path
  ingress-interface ge 0/0/3
  server ip 10.2.0.50 port 1813
  security-group attribute-id vendor-specific 60 delimiter ,
  radius-sso enable
  online-user aging-time 480
#
security-policy
 rule name sec_policy_radius
  source-zone trust
  destination-zone dmz
  destination-address 10.2.0.0 255.255.255.0
  action permit
 rule name policy_sec_02
  source-zone trust
  user ucl-group research
  user ucl-group marketing
  destination-zone untrust
  action permit
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone dmz
 add interface GE0/0/2
#
```

 Copyright © Huawei Technologies Co., Ltd.

10.2 CLI: Example for Configuring RADIUS SSO (Off-path Mode)

Networking Requirements

As shown in **Figure 10-2**, an enterprise deploys DeviceA as the egress gateway at the network border to connect the intranet and the Internet. The details are as follows:

- Employees access the network through the NAS device.
- The NAS authenticates employees through the RADIUS server which stores user information.
- Users on the enterprise network include R&D and marketing employees.

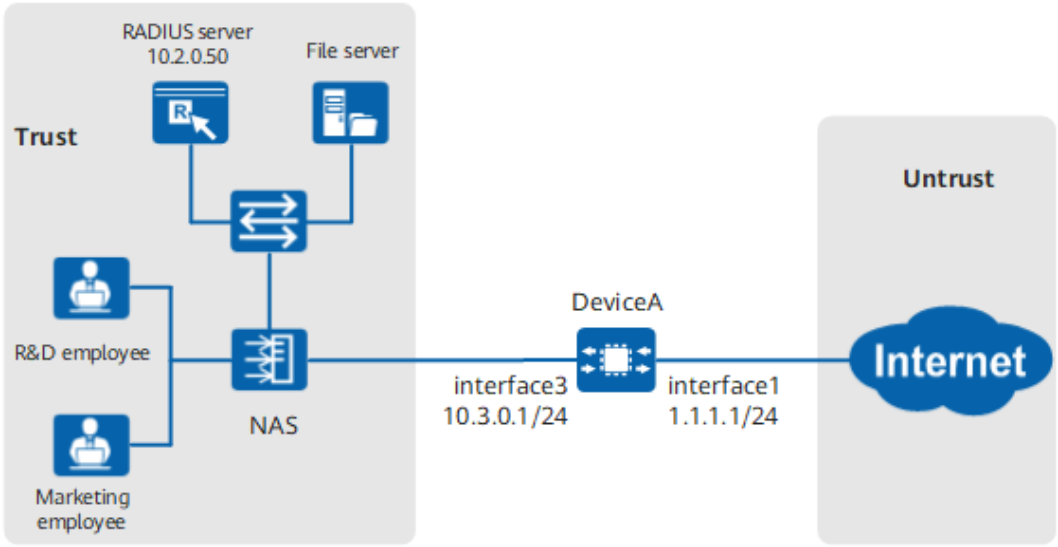
The network administrator of the enterprise wants to use the identity management mechanism provided by DeviceA to identify intranet IP addresses as users so as to provide reference for performing user-based network behavior control and network permission assignment. The specific requirements are as follows:

- DeviceA parses sub-attribute 60 in the vendor-specific attribute of RADIUS accounting packets and uses the parsed attribute value as the security group name of the user.
- R&D and marketing employees can access network resources without the need to be authenticated again by DeviceA after passing RADIUS authentication. The identifiers of the R&D and marketing employees are the accounts used in the RADIUS authentication.

Figure 10-2 Networking diagram of RADIUS SSO

NOTE

In this example, interface1 and interface3 represent GE0/0/1 and GE0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Security group to which the user belongs	Group name: research and marketing	Configure a security group on DeviceA. The security group name must be the same as the attribute value of the security group on the server.
RADIUS SSO	• RADIUS SSO: enabled • Working mode: off-path • Shared key: Test@123 • Interface for receiving accounting packets: GE0/0/3 • Parsed traffic: 10.3.0.1:1813 • RADIUS attribute type: vendor-specific attribute • RADIUS attribute ID: 60	• After SSO parameters are set on DeviceA, DeviceA parses and responds to RADIUS accounting packets sent by the NAS device to obtain the mappings between users and IP addresses. • In addition, DeviceA parses sub-attribute 60 of the vendor-specific attribute and uses the parsed attribute value as the security group name of the user.

Configuration Roadmap

NOTE

This example describes only the configuration of user authentication.

1. Set security groups and RADIUS SSO parameters on DeviceA.
2. To prevent users from being continuously re-authenticated due to frequent login and logout on DeviceA, you are advised to set the online user timeout period on DeviceA to be longer than the interval for updating RADIUS accounting packets. In this example, the online user timeout period is set to 480 minutes.
3. In this deployment mode, the NAS device needs to send an Accounting Start packet to the RADIUS server and DeviceA simultaneously. DeviceA then parses and responds to the packet.

Procedure

Step 1 Configure IP addresses for interfaces and assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Set RADIUS SSO parameters on DeviceA.

```
[DeviceA] identity-management
[DeviceA-identity-management]undo userlog login-out enable
[DeviceA-identity-management]sso-radius
[DeviceA-identity-management-sso-radius] mode out-of-path
[DeviceA-identity-management-sso-radius] shared-key Test@123
[DeviceA-identity-management-sso-radius] ingress-interface ge 0/0/3
[DeviceA-identity-management-sso-radius] server ip 10.3.0.1 port 1813
[DeviceA-identity-management-sso-radius] security-group attribute-id vendor-specific 60 delimiter ,
[DeviceA-identity-management-sso-radius] online-user aging-time 480
[DeviceA-identity-management-sso-radius] radius-sso enable
[DeviceA-identity-management-sso-radius] quit
[DeviceA-identity-management]quit
```

Step 3 Create security groups on DeviceA.

```
[DeviceA] ucl-group name research
[DeviceA] ucl-group name marketing
```

NOTE

In the example of **Configuring RADIUS SSO Parameters on the Device**, the attribute whose value is used as the security group name is configured in RADIUS accounting packets. DeviceA parses the attribute value as the name of the security group to which the user belongs and searches for a policy based on the security group. Therefore, you need to configure a security group with the same name as the security group attribute value on DeviceA in advance. Otherwise, no policy can reference the security group.

If you do not need to use the RADIUS attribute value as the security group name, create a security group on the local device as required and configure a user with the same name (**local-access-user**) on the serve. In this case, run the **security-group priority-type local-first** command in the system view to enable DeviceA to preferentially search for the security group to which the local user belongs.

Step 4 Configure a security policy.

Configure a security policy to allow the NAS device to send RADIUS accounting packets to DeviceA.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_radius
[DeviceA-policy-security-rule-policy_sec_radius] source-zone trust
[DeviceA-policy-security-rule-policy_sec_radius] destination-zone local
[DeviceA-policy-security-rule-policy_sec_radius] destination-address 10.3.0.1 32
[DeviceA-policy-security-rule-policy_sec_radius] action permit
[DeviceA-policy-security-rule-policy_sec_radius] quit
```

Configure a security policy to allow users to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec
[DeviceA-policy-security-rule-policy_sec] source-zone trust
[DeviceA-policy-security-rule-policy_sec] user ucl-group research
[DeviceA-policy-security-rule-policy_sec] user ucl-group marketing
[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec] action permit
[DeviceA-policy-security-rule-policy_sec] quit
[DeviceA-policy-security] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the NAS device to send RADIUS accounting packets to DeviceA. The encryption key configured on the NAS device must be the same as the shared key configured for RADIUS SSO on DeviceA. Otherwise, DeviceA cannot correctly parse the RADIUS accounting packets sent by the NAS device or encrypt the RADIUS Accounting-Response packets to be sent to the NAS device.

----End

Verifying the Configuration

- R&D employees can access network resources after they successfully access the NAS device using RADIUS accounts and passwords.
- Marketing employees can access network resources after they successfully access the NAS device using RADIUS accounts and passwords.
- Run the **display identity-management online-user** command on DeviceA to view information about online users.

```
<DeviceA> display identity-management online-user verbose
Current Total Number: 2
-------------------------------------------------------------------------------
Vsys Index: 0
IP Address: 10.3.0.2
User Name : user1
Login Time: 2022-10-27 20:26:05  Online Time 00:07:58  Time-left: 07:52:02
Authentication Mode: RADIUS SSO
Security Group: research
-------------------------------------------------------------------------------
Vsys Index: 0
IP Address: 10.3.0.3
User Name : user2
Login Time: 2022-10-27 20:26:05  Online Time 00:08:02  Time-left: 07:51:58
Authentication Mode: RADIUS SSO
Security Group: marketing
-------------------------------------------------------------------------------
```

Configuration Scripts

```
#
sysname DeviceA
#
ucl-group name research
ucl-group name marketing
#
identity-management
 undo userlog login-out enable
 sso-radius
  mode out-of-path
  shared-key %^%#o3Z7,b[Ox7Sc#r-f+WDC:D=s%^%#
  ingress-interface ge 0/0/3
  server ip 10.3.0.1 port 1813
  security-group attribute-id vendor-specific 60 delimiter ,
  radius-sso enable
  online-user aging-time 480
#
security-policy
 rule name policy_sec_radius
  source-zone trust
  destination-zone local
  destination-address 10.3.0.1 32
  action permit
 rule name policy_sec
  source-zone trust
  user ucl-group research
  user ucl-group marketing
  destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
```

10.3 CLI: Example for Configuring TSM SSO

Networking Requirements

As shown in **Figure 10-3**, an enterprise deploys DeviceA as the egress gateway at the network border to connect the intranet and the Internet. The details are as follows:

- The TSM identity authentication mechanism has been deployed on the intranet, and the TSM SSO server (iMaster NCE-Campus) stores information about users and security groups.
- Users on the enterprise network include R&D and marketing employees.

The network administrator of the enterprise wants to use the identity management mechanism provided by DeviceA to identify intranet IP addresses as users and security groups so as to provide reference for performing security group-based network behavior control and network permission assignment. The specific requirements are as follows:

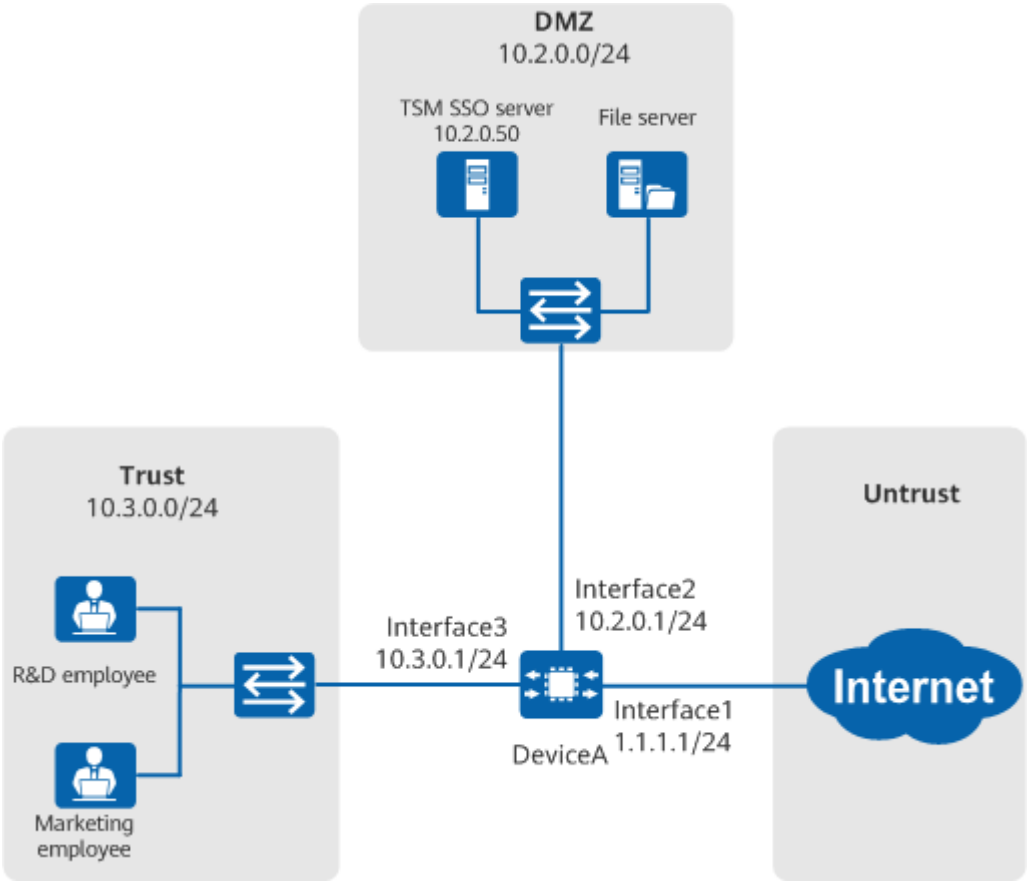
- R&D and marketing employees can access network resources without being authenticated again after their TSM accounts and passwords are authenticated. The identifiers of the R&D and marketing employees are the accounts used in the TSM authentication.
- DeviceA implements policy control based on the organization to which the user belongs, that is, the security group.

Figure 10-3 Networking diagram of TSM SSO

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
TSM SSO server	• TSM SSO server IP address: 10.2.0.50 • Server port number: 8445 • Encryption algorithm: AES-256-GCM • Shared key: Admin2012@123	Configure the TSM SSO server on DeviceA. In other words, set a series of parameters used by DeviceA to communicate with the TSM SSO server. The parameter settings must be the same as those on the TSM SSO server.
Security group to which the user belongs	Security group name for R&D employees: research Security group name for marketing employees: marketing	On DeviceA, create a security group with the same name as that on the TSM SSO server.
TSM SSO	TSM SSO: enabled	Set SSO parameters on DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

This example describes only the configuration of user authentication.

1. Add DeviceA to the TSM SSO server and configure the TSM SSO server on DeviceA so that DeviceA can communicate with the server.
2. Set TSM SSO parameters on DeviceA.
3. Frequent expiration of the online user timeout period during working hours (assuming 8 hours) results in frequent re-authentication on the TSM SSO server. To avoid this, set the online user timeout period to 480 minutes.

Procedure

Step 1 Add DeviceA on the TSM SSO server.

On the TSM SSO server, configure the IP address, device name, port, encryption algorithm, access key, and endpoint IPv4 address list of the online behavior management device. The port, encryption algorithm, and access key must be the same as those configured on DeviceA. For details, see the configuration of online behavior management in the iMaster NCE-Campus product documentation.

NOTE

Protocol version identifier of iMaster NCE-Campus must be set to 100.0 or later.

Step 2 Configure IP addresses for the interfaces on DeviceA and assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 3 Set the TSM SSO server and SSO parameters on DeviceA.

The TSM SSO server parameters set on DeviceA must be the same as those on the TSM SSO server.

```
[DeviceA] identity-management
[DeviceA-identity-management] sso-tsm
[DeviceA-identity-management-sso-tsm] server ip 10.2.0.50 port 8445 shared-key Admin2012@123
[DeviceA-identity-management-sso-tsm] tsm-sso enable
[DeviceA-identity-management-sso-tsm] local-server ip 10.3.0.1 port 8001
[DeviceA-identity-management-sso-tsm] online-user aging-time 480
[DeviceA-identity-management-sso-tsm] quit
[DeviceA-identity-management] quit
```

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> When iMaster NCE-Campus functions as a TSM SSO server, the server port number is fixed to 8445.

Step 4 Create security groups on DeviceA.

```
[DeviceA] ucl-group name research
[DeviceA] ucl-group name marketing
```

> **NOTE**
>
> The configured security group name must be the same as that on the TSM SSO server. Otherwise, DeviceA cannot perform policy control based on the security group after obtaining the security group to which the user belongs from the user login message sent by the TSM SSO server.

Step 5 Configure security policies on DeviceA to ensure normal communication between users, DeviceA, and the TSM SSO server.

1. Configure a security policy for traffic from the Trust zone (where the users reside) to the DMZ (where the TSM SSO server resides), so that users can be authenticated by the TSM SSO server.

   ```
   [DeviceA] security-policy
   [DeviceA-policy-security] rule name sec_policy_tsm
   [DeviceA-policy-security-rule-sec_policy_tsm] source-zone trust
   [DeviceA-policy-security-rule-sec_policy_tsm] source-address 10.3.0.0 24
   [DeviceA-policy-security-rule-sec_policy_tsm] destination-zone dmz
   [DeviceA-policy-security-rule-sec_policy_tsm] destination-address 10.2.0.0 24
   [DeviceA-policy-security-rule-sec_policy_tsm] action permit
   [DeviceA-policy-security-rule-sec_policy_tsm] quit
   ```

2. Configure a security policy for traffic from the DMZ (where the TSM SSO server resides) to the Local zone, so that the TSM SSO server can communicate with DeviceA.

   ```
   [DeviceA-policy-security] rule name local_policy_tsm_01
   [DeviceA-policy-security-rule-local_policy_tsm_01] source-zone local
   [DeviceA-policy-security-rule-local_policy_tsm_01] destination-zone dmz
   [DeviceA-policy-security-rule-local_policy_tsm_01] action permit
   [DeviceA-policy-security-rule-local_policy_tsm_01] quit
   [DeviceA-policy-security] rule name local_policy_tsm_02
   [DeviceA-policy-security-rule-local_policy_tsm_02] source-zone dmz
   [DeviceA-policy-security-rule-local_policy_tsm_02] destination-zone local
   [DeviceA-policy-security-rule-local_policy_tsm_02] action permit
   [DeviceA-policy-security-rule-local_policy_tsm_02] quit
   ```

3. Configure a security policy to allow users to access the Internet.

   ```
   [DeviceA-policy-security] rule name policy_sec_02
   [DeviceA-policy-security-rule-policy_sec_02] source-zone trust
   [DeviceA-policy-security-rule-policy_sec_02] destination-zone untrust
   [DeviceA-policy-security-rule-policy_sec_02] user ucl-group research
   [DeviceA-policy-security-rule-policy_sec_02] user ucl-group marketing
   [DeviceA-policy-security-rule-policy_sec_02] action permit
   [DeviceA-policy-security-rule-policy_sec_02] quit
   [DeviceA-policy-security] quit
   ```

----End

Verifying the Configuration

- R&D employees can access network resources after successful logins based on TSM accounts and passwords.
- Marketing employees can access network resources after successful logins based on TSM accounts and passwords.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display identity-management online-user** command on DeviceA to view information about online users.

```
<DeviceA> display identity-management online-user
verbose
Current Total Number: 2
---------------------------------------------------------------------------

Vsys Index: 0
IP Address: 10.3.0.2
User Name : user1
Login Time: 2022-10-27 20:26:05  Online Time 00:07:58  Time-left: 07:52:02
Authentication Mode: TSM SSO
Security Group: research
---------------------------------------------------------------------------
IP Address: 10.3.0.3
User Name : user2
Login Time: 2022-10-27 20:26:01  Online Time 00:08:02  Time-left: 07:51:58
Authentication Mode: TSM SSO
Security Group: marketing
---------------------------------------------------------------------------
```

Configuration Scripts

```
#
sysname DeviceA
#
ucl-group name research
ucl-group name marketing
#
identity-management
 sso-tsm
  server ip 10.2.0.50 port 8445 shared-key %$%$|5<h@/062'gA|%:9CO.2/JA8%$%$
  tsm-sso enable
  local-server ip 10.3.0.1 port 8001
  online-user aging-time 480
#
security-policy
 rule name sec_policy_tsm
  source-zone trust
  destination-zone dmz
  source-address 10.3.0.0 24
  destination-address 10.2.0.0 255.255.255.0
  action permit
 rule name local_policy_tsm_01
  source-zone local
  destination-zone dmz
  action permit
 rule name local_policy_tsm_02
  source-zone dmz
  destination-zone local
  action permit
 rule name policy_sec_02
  source-zone trust
  user ucl-group research
  user ucl-group marketing
  destination-zone untrust
  action permit
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone dmz
 add interface GE0/0/2
#
```

11 GRE

11.1 Web: Example for Configuring a Static Route-based GRE Tunnel
11.2 Web: Example for Configuring an OSPF-based GRE Tunnel
11.3 CLI: Example for Configuring an IPv4 over IPv4 GRE Tunnel
11.4 CLI: Example for Configuring an IPv6 over IPv4 GRE Tunnel
11.5 Web: Example for Configuring an IPsec over GRE Tunnel
11.6 CLI: Example for Configuring an IPsec over GRE Tunnel

11.1 Web: Example for Configuring a Static Route-based GRE Tunnel

Networking Requirements

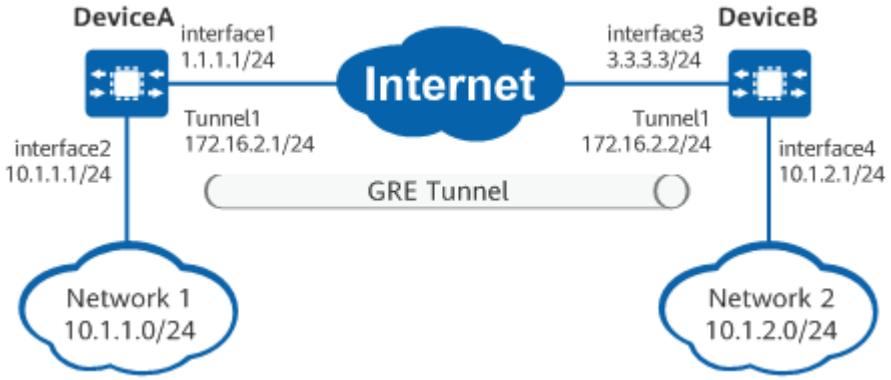
As shown in **Figure 11-1**, DeviceA and DeviceB are connected over the Internet and have reachable public network routes between them. Networks 1 and 2 are private IP networks and have static routes configured. A GRE tunnel needs to be established between DeviceA and DeviceB to enable networks 1 and 2 to exchange static routes over the Internet.

Figure 11-1 Configuring a static route-based GRE tunnel

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA respectively, and interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
DeviceA	Interface configuration	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
		Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	GRE configuration	Interface name: Tunnel1 IP address: 172.16.2.1/24 Source address: 1.1.1.1/24 Destination address: 3.3.3.3/24 Tunnel identification keyword: 123456
DeviceB	Interface configuration	Interface number: GE0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust
		Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	GRE configuration	Interface name: Tunnel1 IP address: 172.16.2.2/24 Source address: 3.3.3.3/24 Destination address: 1.1.1.1/24 Tunnel identification keyword: 123456

Configuration Roadmap

1. Create a tunnel interface on both DeviceA and DeviceB, and set encapsulation parameters such as the source and destination IP addresses of the tunnel on each tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

2. On DeviceA and DeviceB, configure a static route and specify the local tunnel interface as the outbound interface of the route. The route is used to direct traffic to the GRE tunnel.
3. Configure security policies for GRE tunnel setup and traffic forwarding.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

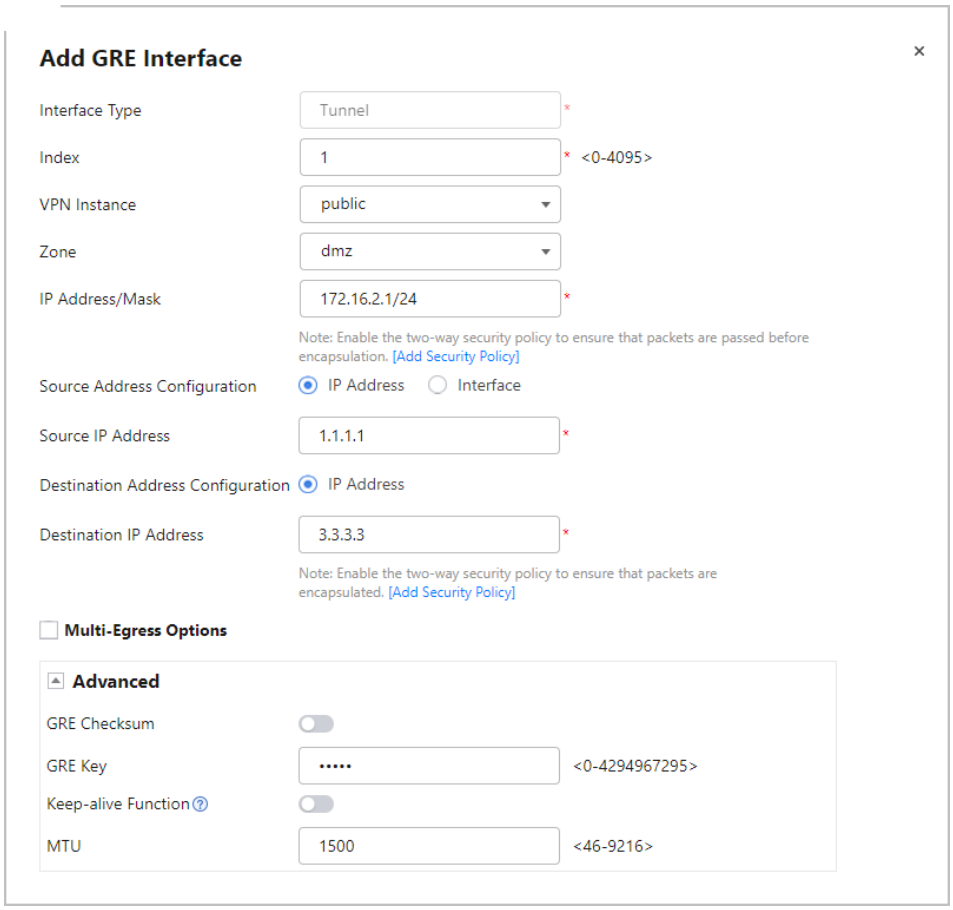
Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

2. Set encapsulation parameters for the tunnel interface.
   a. Choose **Network** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Set GRE tunnel interface parameters. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



3. Configure a static route to direct traffic to be transmitted over the GRE tunnel to the GRE tunnel.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a static route as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.1.2.0/24
Interface	Tunnel1

4. Configure security policies for GRE tunnel setup and traffic forwarding.
   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy as follows to permit original packets. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	dmz

 Copyright © Huawei Technologies Co., Ltd.

Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

c. Repeat the preceding steps to configure a DMZ-to-Trust interzone policy.

Name	policy2
Source Zone	dmz
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

d. Repeat the preceding steps to configure a Local-to-Untrust interzone policy to permit GRE-encapsulated packets.

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	1.1.1.1/32
Destination Address	3.3.3.3/32
Service	gre
Action	Permit

e. Repeat the preceding steps to configure an Untrust-to-Local interzone policy.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	3.3.3.3/32
Destination Address	1.1.1.1/32
Service	gre

 Copyright © Huawei Technologies Co., Ltd.

Action	Permit

Step 2 Configure DeviceB.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

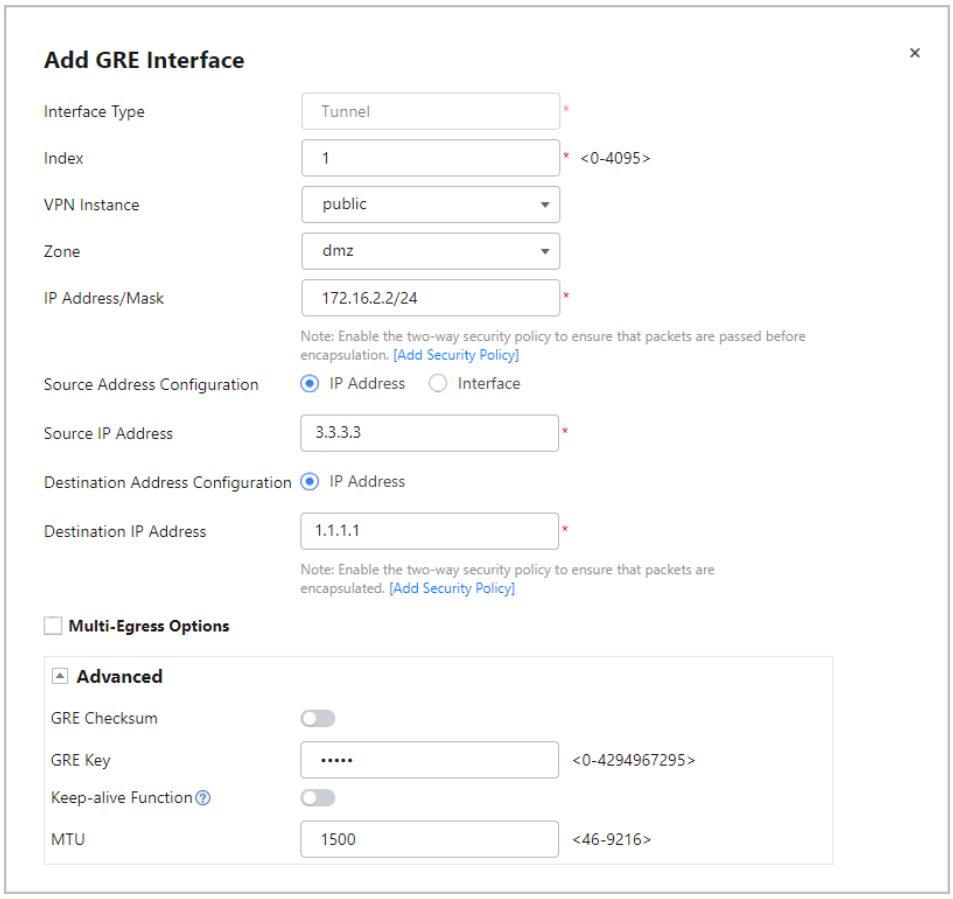
Zone	untrust
IPv4	
IP Address	3.3.3.3/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Set encapsulation parameters for the tunnel interface.
   a. Choose **Network** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Set GRE tunnel interface parameters. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



3. Configure a static route to direct traffic to be transmitted over the GRE tunnel to the GRE tunnel.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a static route as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.1.1.0/24
Interface	Tunnel1

4. Configure security policies for GRE tunnel setup and traffic forwarding.
   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy as follows to permit original packets. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	dmz
Source Address	10.1.2.0/24

 Copyright © Huawei Technologies Co., Ltd.

Destination Address	10.1.1.0/24
Action	Permit

c. Repeat the preceding steps to configure a DMZ-to-Trust interzone policy.

Name	policy2
Source Zone	dmz
Destination Zone	trust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

d. Repeat the preceding steps to configure a Local-to-Untrust interzone policy to permit GRE-encapsulated packets.

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	3.3.3.3/32
Destination Address	1.1.1.1/32
Service	gre
Action	Permit

e. Repeat the preceding steps to configure an Untrust-to-Local interzone policy.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.1.1/32
Destination Address	3.3.3.3/32
Service	gre
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

----End

Verifying the Configuration

1. PCs on networks 1 and 2 can ping each other.
2. A route whose outbound interface is Tunnel1 and destination address is 10.1.2.0/24 can be found on the **Network** > **Route** > **Routing Table** page of DeviceA's web UI.

Configuration Scripts

- DeviceA

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel1
 ip address 172.16.2.1 255.255.255.0
 tunnel-protocol gre
 source 1.1.1.1
 destination 3.3.3.3
 gre key cipher %+%#=F~T>w'>n:QlQ8BI3>67Ir3I*Onzv'\(%+%#
#
ip route-static 10.1.2.0 255.255.255.0 Tunnel1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone dmz
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone dmz
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  service gre
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 3.3.3.3 mask 255.255.255.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-address 1.1.1.1 mask 255.255.255.255
 service gre
 action permit
```

- DeviceB

```
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel1
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 source 3.3.3.3
 destination 1.1.1.1
 gre key cipher %+%#=F~T>w'>n:QlQ8BI3>67Ir3I*Onzv'\(%+%#
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone dmz
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone dmz
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  service gre
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  service gre
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

11.2 Web: Example for Configuring an OSPF-based GRE Tunnel

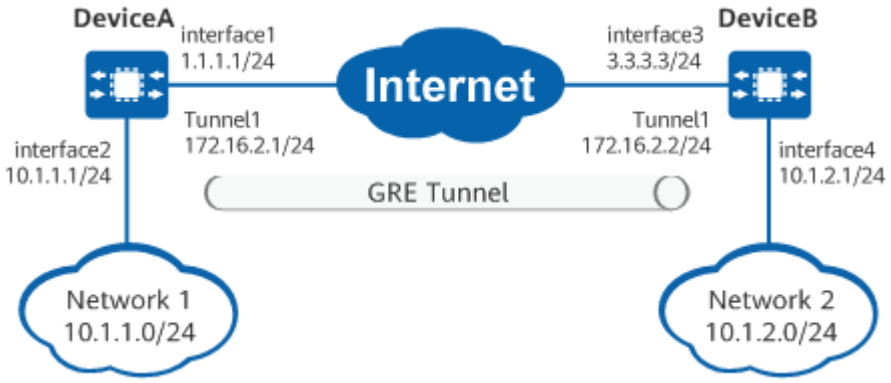
Networking Requirements

As shown in **Figure 11-2**, DeviceA and DeviceB are connected over the Internet and have reachable public network routes between them. Networks 1 and 2 are private IP networks and run OSPF. A GRE tunnel needs to be established between DeviceA and DeviceB to enable networks 1 and 2 to exchange OSPF routing information over the Internet.

Figure 11-2 Configuring an OSPF-based GRE tunnel

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA respectively, and interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB respectively.



Item	Data	Description
DeviceA	Interface configuration	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
		Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	GRE configuration	Interface name: Tunnel1 IP address: 172.16.2.1/24 Source address: 1.1.1.1/24 Destination address: 3.3.3.3/24 Tunnel identification keyword: 123456

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
DeviceB	Interface configuration	Interface number: GE0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust
		Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	GRE configuration	Interface name: Tunnel1 IP address: 172.16.2.2/24 Source address: 3.3.3.3/24 Destination address: 1.1.1.1/24 Tunnel identification keyword: 123456

Configuration Roadmap

1. Create a tunnel interface on both DeviceA and DeviceB, and set encapsulation parameters such as the source and destination IP addresses of the tunnel on each tunnel interface.
2. Start an OSPF process and specify interfaces running OSPF. In this example, network 1 (10.1.1.0/24) and network 172.16.2.0/24 where the tunnel interface resides are advertised to network 2 through the GRE tunnel. The tunnel interfaces establish an OSPF adjacency over the GRE tunnel.
3. Configure security policies for GRE tunnel setup and traffic forwarding.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

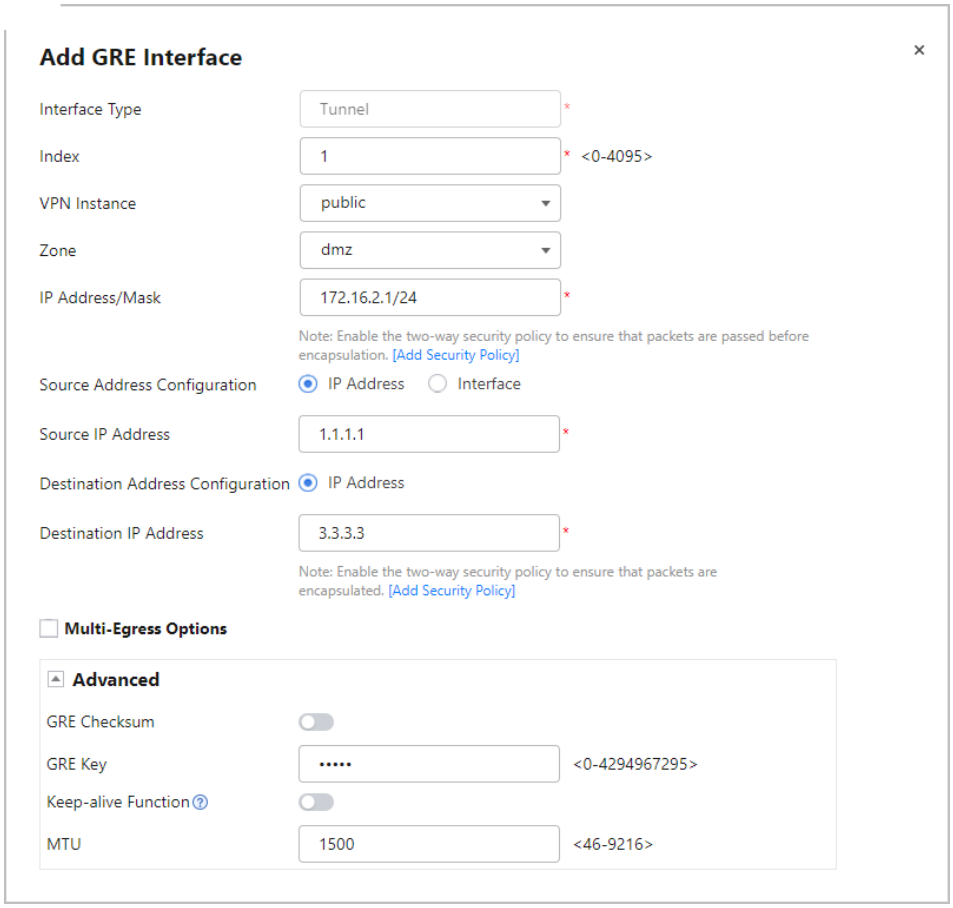
Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

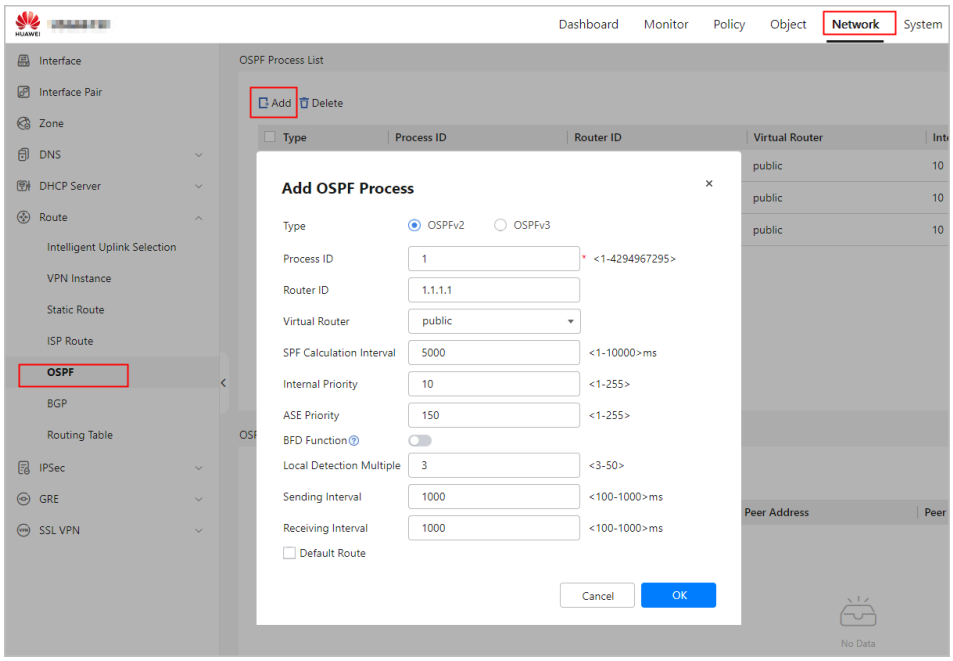
 Copyright © Huawei Technologies Co., Ltd.

2. Set encapsulation parameters for the tunnel interface.
   a. Choose **Network** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Set GRE tunnel interface parameters. Click **OK**.



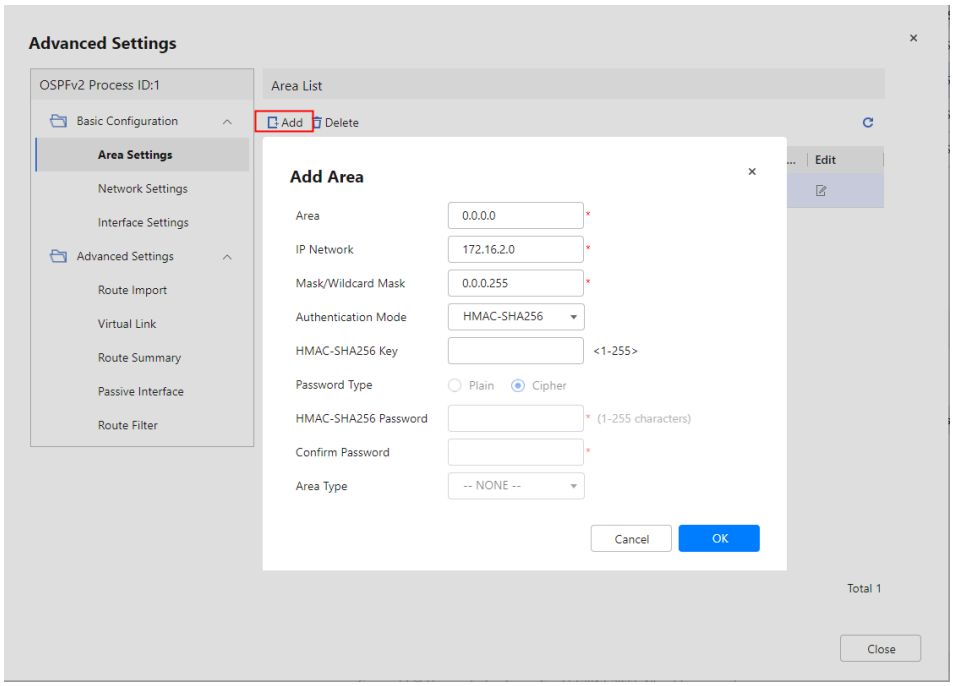
3. Configure OSPF to advertise network 1 (10.1.1.0/24) and network 172.16.2.0/24 where the tunnel interface resides.
   a. Choose **Network** > **Route** > **OSPF**.
   b. Click **Add** in the OSPF process list to create an OSPF process. Click **OK**.
      Set the parameters for the OSPF process as follows:
      - Process ID: 1
      - Router ID: 1.1.1.1

 Copyright © Huawei Technologies Co., Ltd.



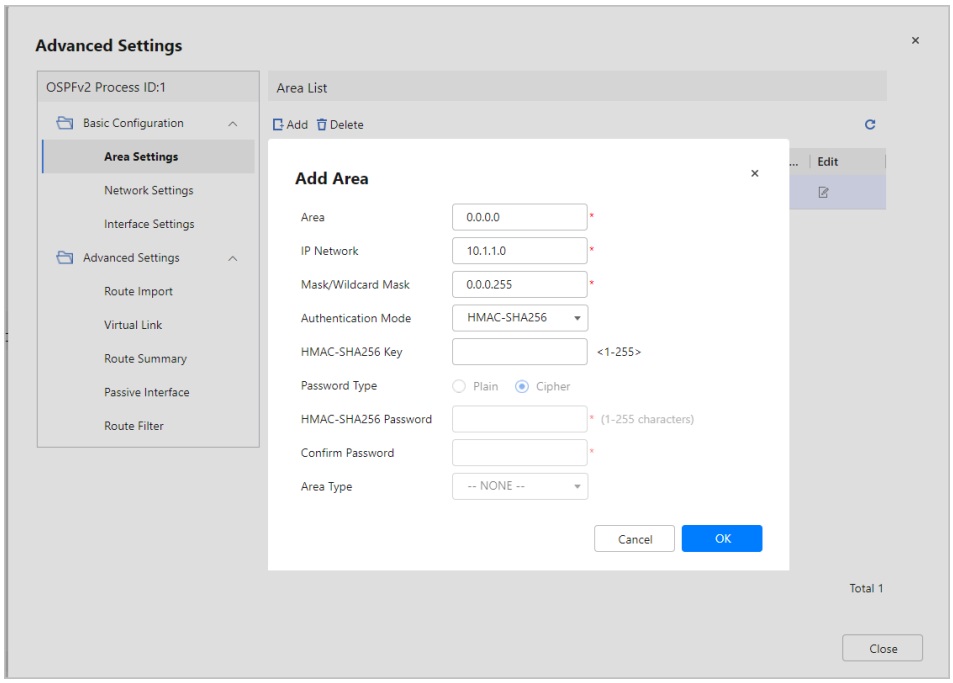
c. Click  of OSPF process 1. Choose **Basic Configuration** > **Area Settings** from the navigation tree.

d. Click **Add** to create an area. Click **OK**.



e. Repeat the preceding steps to create another area.

 Copyright © Huawei Technologies Co., Ltd.



4. Configure security policies for GRE tunnel setup and traffic forwarding.
   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy as follows to permit original packets. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	dmz
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

   c. Repeat the preceding steps to configure a DMZ-to-Trust interzone policy.

Name	policy2
Source Zone	dmz
Destination Zone	trust
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

d. Repeat the preceding steps to configure a Local-to-Untrust interzone policy to permit GRE-encapsulated packets.

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	1.1.1.1/32
Destination Address	3.3.3.3/32
Service	gre, ospf
Action	Permit

e. Repeat the preceding steps to configure an Untrust-to-Local interzone policy.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	3.3.3.3/32
Destination Address	1.1.1.1/32
Service	gre, ospf
Action	Permit

Step 2 Configure DeviceB.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

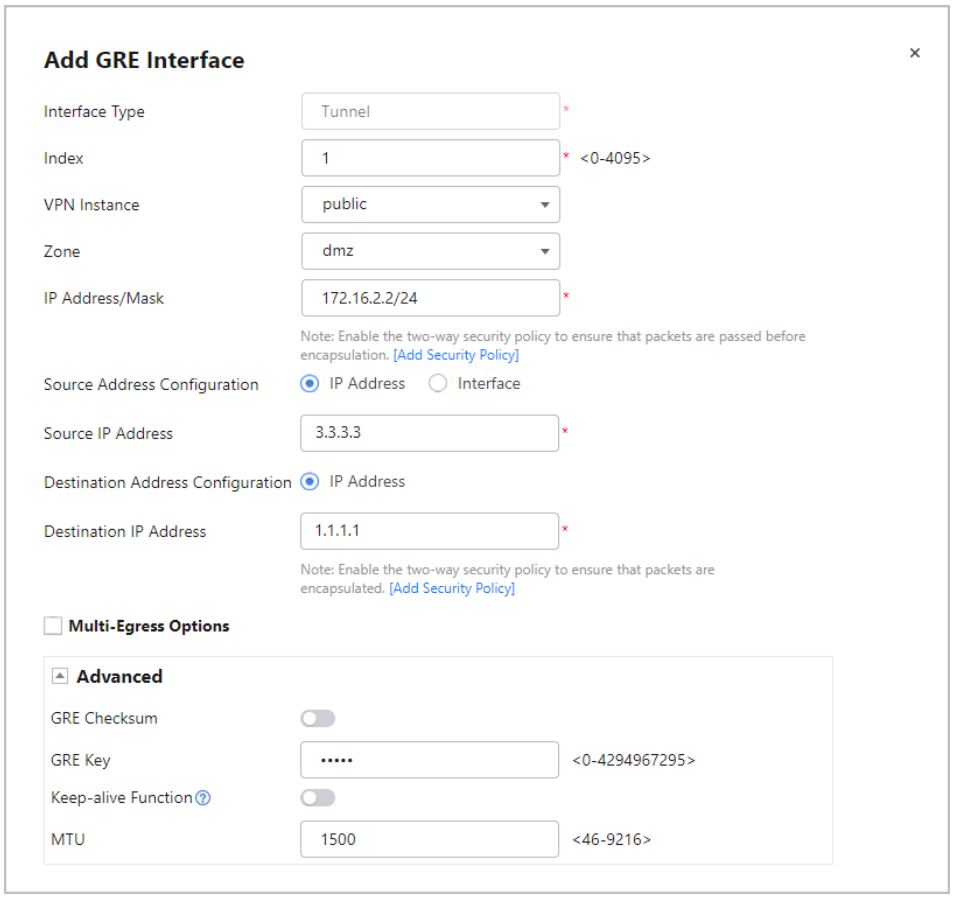
Zone	untrust
IPv4	
IP Address	3.3.3.3/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

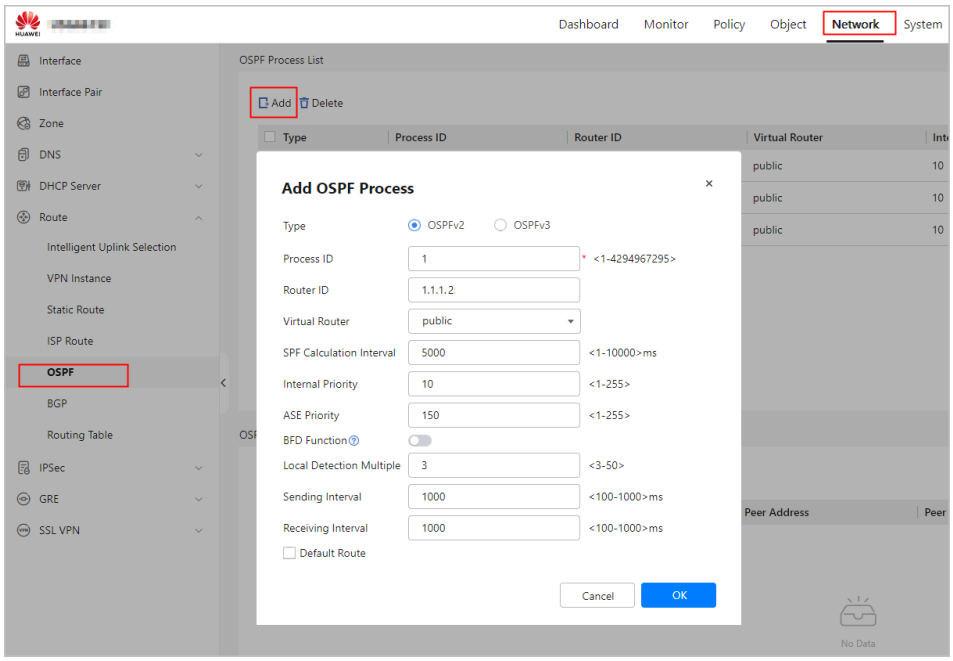
 Copyright © Huawei Technologies Co., Ltd.

2. Set encapsulation parameters for the tunnel interface.
   a. Choose **Network** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Set GRE tunnel interface parameters. Click **OK**.



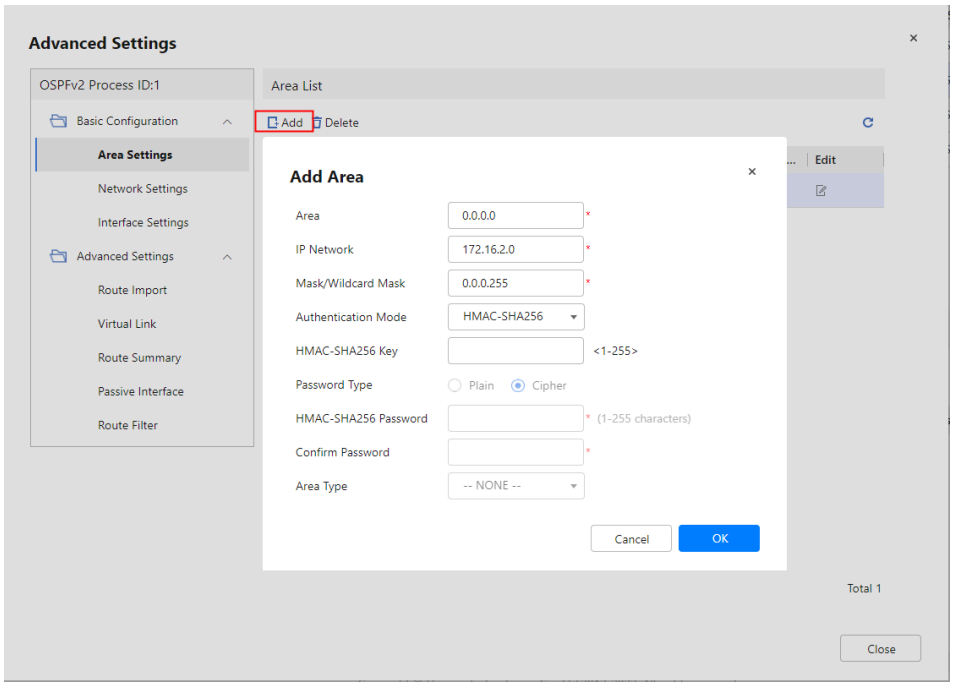
3. Configure OSPF to advertise network 2 (10.1.2.0/24) and network 172.16.2.0/24 where the tunnel interface resides.
   a. Choose **Network** > **Route** > **OSPF**.
   b. Click **Add** in the OSPF process list to create an OSPF process. Click **OK**.
      Set the parameters for the OSPF process as follows:
      - Process ID: 1
      - Router ID: 1.1.1.2

 Copyright © Huawei Technologies Co., Ltd.



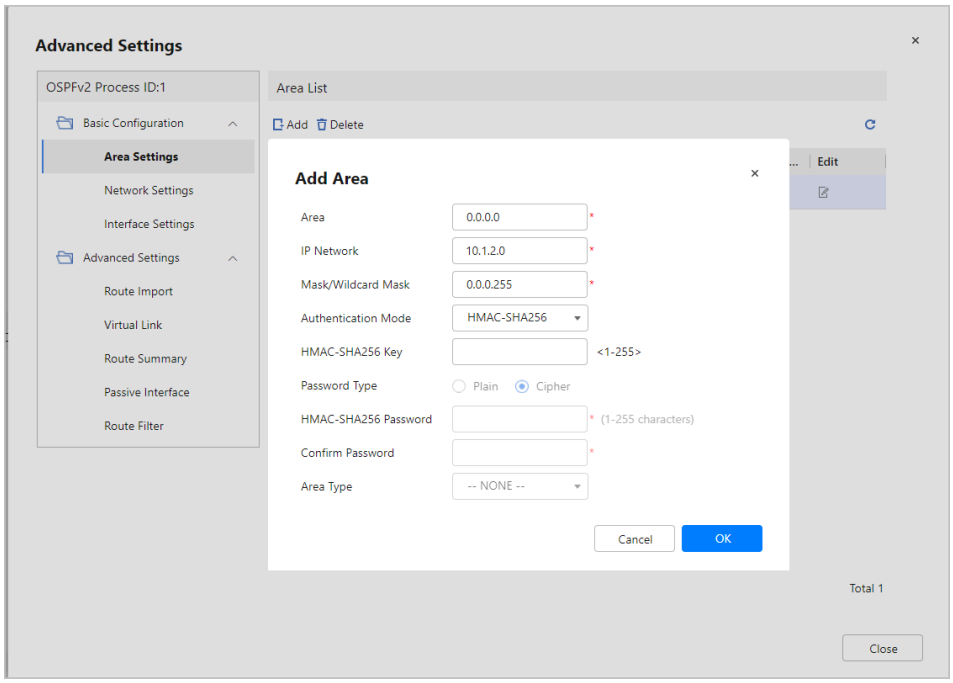
c. Click of OSPF process 1. Choose **Basic Configuration** > **Area Settings** from the navigation tree.

d. Click **Add** to create an area. Click **OK**.



e. Repeat the preceding steps to create another area.

 Copyright © Huawei Technologies Co., Ltd.



4. Configure security policies for GRE tunnel setup and traffic forwarding.
   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy as follows to permit original packets. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	dmz
Source Address	10.1.2.0/24
Destination Address	10.1.1.0/24
Action	Permit

   c. Repeat the preceding steps to configure a DMZ-to-Trust interzone policy.

Name	policy2
Source Zone	dmz
Destination Zone	trust
Source Address	10.1.1.0/24
Destination Address	10.1.2.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

d. Repeat the preceding steps to configure a Local-to-Untrust interzone policy to permit GRE-encapsulated packets.

Name	policy3
Source Zone	local
Destination Zone	untrust
Source Address	3.3.3.3/32
Destination Address	1.1.1.1/32
Service	gre, ospf
Action	Permit

e. Repeat the preceding steps to configure an Untrust-to-Local interzone policy.

Name	policy4
Source Zone	untrust
Destination Zone	local
Source Address	1.1.1.1/32
Destination Address	3.3.3.3/32
Service	gre, ospf
Action	Permit

----End

Verifying the Configuration

1. PCs on networks 1 and 2 can ping each other.
2. A route whose outbound interface is Tunnel1 and destination address is 10.1.2.0/24 can be found on the **Network** > **Route** > **Routing Table** page of DeviceA's web UI.

Configuration Scripts

- DeviceA

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel1
 ip address 172.16.2.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 tunnel-protocol gre
 source 1.1.1.1
 destination 3.3.3.3
 gre key cipher %+%#=F~&KLI;T>w'>n:QlQ8BI3>67Ir3I*Onzv'\&ii(%+%#
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 172.16.2.0 0.0.0.255
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone dmz
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone dmz
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  service gre
  service ospf
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  service gre
  service ospf
  action permit
```

- DeviceB

```
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel1
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 source 3.3.3.3
 destination 1.1.1.1
 gre key cipher %+%#=F~&KLI;T>w'>n:QlQ8BI3>67Ir3I*Onzv'\&ii(%+%#
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
```

 Copyright © Huawei Technologies Co., Ltd.

```
 network 172.16.2.0 0.0.0.255
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone dmz
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name policy2
  source-zone dmz
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  source-address 3.3.3.3 mask 255.255.255.255
  destination-address 1.1.1.1 mask 255.255.255.255
  service gre
  service ospf
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  source-address 1.1.1.1 mask 255.255.255.255
  destination-address 3.3.3.3 mask 255.255.255.255
  service gre
  service ospf
  action permit
```

11.3 CLI: Example for Configuring an IPv4 over IPv4 GRE Tunnel

Networking Requirements

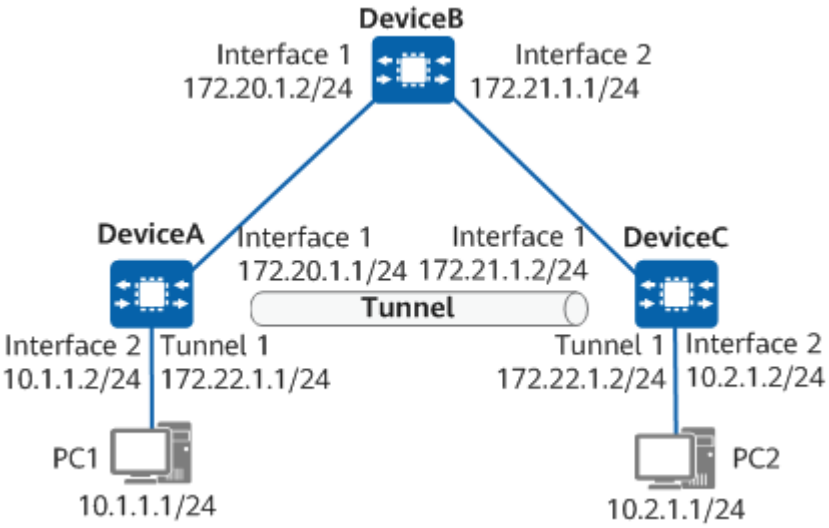
In **Figure 11-3**, DeviceA, DeviceB, and DeviceC belong to the IPv4 backbone network and are running OSPF. A direct link needs to be established between DeviceA and DeviceC to ensure that PC1 and PC2 can communicate with each other. To meet such a requirement, a GRE tunnel needs to be established between DeviceA and DeviceC and static routes need to be configured so that packets between PC1 and PC2 can be forwarded through tunnel interfaces on both ends of the tunnel. DeviceA and DeviceC are the default gateways of PC1 and PC2, respectively.

 Copyright © Huawei Technologies Co., Ltd.

Figure 11-3 Configuring an IPv4 over IPv4 GRE tunnel

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IPv4 dynamic routing protocol for communication between the devices.
2. Create tunnel interfaces on DeviceA and DeviceC and specify the tunnel source and destination addresses. The tunnel source address is the IP address of the interface that sends packets, and the tunnel destination address is the IP address of the interface that receives packets.
3. Configure IP addresses for the tunnel interfaces to generate tunnel routes.
4. Configure a static route between DeviceA and PC1 and between DeviceC and PC2 and specify the local tunnel interface as the outbound interface of the static route so that traffic between PC1 and PC2 can be transmitted through the GRE tunnel.

Procedure

Step 1 Configure IP addresses for interfaces.

Configure an IP address for each interface according to **Figure 11-3**. For detailed configurations, see **Configuration Scripts**.

Step 2 Add interfaces to security zones and configure security policies.

Configure DeviceA.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] security-policy
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security] rule name sec_policy1
[DeviceA-policy-security-rule-sec_policy1] source-zone local
[DeviceA-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceA-policy-security-rule-sec_policy1] action permit
[DeviceA-policy-security-rule-sec_policy1] quit
[DeviceA-policy-security] rule name sec_policy2
[DeviceA-policy-security-rule-sec_policy2] source-zone untrust
[DeviceA-policy-security-rule-sec_policy2] destination-zone local
[DeviceA-policy-security-rule-sec_policy2] action permit
[DeviceA-policy-security-rule-sec_policy2] quit
[DeviceA-policy-security] quit
```

Configure DeviceB.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] add interface ge 0/0/2
[DeviceB-zone-untrust] quit
```

Configure DeviceC.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
[DeviceC] security-policy
[DeviceC-policy-security] rule name sec_policy1
[DeviceC-policy-security-rule-sec_policy1] source-zone local
[DeviceC-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceC-policy-security-rule-sec_policy1] action permit
[DeviceC-policy-security-rule-sec_policy1] quit
[DeviceC-policy-security] rule name sec_policy2
[DeviceC-policy-security-rule-sec_policy2] source-zone untrust
[DeviceC-policy-security-rule-sec_policy2] destination-zone local
[DeviceC-policy-security-rule-sec_policy2] action permit
[DeviceC-policy-security-rule-sec_policy2] quit
[DeviceC-policy-security] quit
```

Step 3 Configure an IGP on the VPN backbone network.

Configure DeviceA.

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 172.20.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

Configure DeviceB.

```
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 172.20.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 172.21.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Configure DeviceC.

```
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 172.21.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

After the configuration is complete, run the **display ip routing-table** command on DeviceA and DeviceC. The command outputs show that DeviceA and DeviceC can learn the OSPF route to the network segment of the remote interface.

 Copyright © Huawei Technologies Co., Ltd.

The following example uses the command output on DeviceA.

```
[DeviceA] display ip routing-table
Proto: Protocol        Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 11       Routes : 11

Destination/Mask    Proto   Pre  Cost       Flags NextHop         Interface

       10.1.1.0/24  Direct  0    0           D  10.1.1.2        GE0/0/2
       10.1.1.2/32  Direct  0    0           D  127.0.0.1       GE0/0/2
     10.1.1.255/32  Direct  0    0           D  127.0.0.1       GE0/0/2
     172.20.1.0/24  Direct  0    0           D  172.20.1.1      GE0/0/1
     172.20.1.1/32  Direct  0    0           D  127.0.0.1       GE0/0/1
   172.20.1.255/32  Direct  0    0           D  127.0.0.1       GE0/0/1
     172.21.1.0/24  OSPF    10   2           D  172.20.1.2      GE0/0/1
      127.0.0.0/8   Direct  0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D  127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
```

Step 4 Configure tunnel interfaces.

Configure DeviceA.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] tunnel-protocol gre
[DeviceA-Tunnel1] ip address 172.22.1.1 255.255.255.0
[DeviceA-Tunnel1] source 172.20.1.1
[DeviceA-Tunnel1] destination 172.21.1.2
[DeviceA-Tunnel1] quit
```

Add DeviceA's tunnel interface to a security zone and configure security policies.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface tunnel 1
[DeviceA-zone-dmz] quit
[DeviceA] security-policy
[DeviceA-policy-security] rule name sec_policy3
[DeviceA-policy-security-rule-sec_policy3] source-zone trust
[DeviceA-policy-security-rule-sec_policy3] destination-zone dmz
[DeviceA-policy-security-rule-sec_policy3] action permit
[DeviceA-policy-security-rule-sec_policy3] quit
[DeviceA-policy-security] rule name sec_policy4
[DeviceA-policy-security-rule-sec_policy4] source-zone dmz
[DeviceA-policy-security-rule-sec_policy4] destination-zone trust
[DeviceA-policy-security-rule-sec_policy4] action permit
[DeviceA-policy-security-rule-sec_policy4] quit
[DeviceA-policy-security] quit
```

Configure DeviceC.

```
[DeviceC] interface tunnel 1
[DeviceC-Tunnel1] tunnel-protocol gre
[DeviceC-Tunnel1] ip address 172.22.1.2 255.255.255.0
[DeviceC-Tunnel1] source 172.21.1.2
[DeviceC-Tunnel1] destination 172.20.1.1
[DeviceC-Tunnel1] quit
```

Add DeviceC's tunnel interface to a security zone and configure security policies.

```
[DeviceC] firewall zone dmz
[DeviceC-zone-dmz] add interface tunnel 1
[DeviceC-zone-dmz] quit
[DeviceC] security-policy
[DeviceC-policy-security] rule name sec_policy3
[DeviceC-policy-security-rule-sec_policy3] source-zone trust
[DeviceC-policy-security-rule-sec_policy3] destination-zone dmz
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-policy-security-rule-sec_policy3] action permit
[DeviceC-policy-security-rule-sec_policy3] quit
[DeviceC-policy-security] rule name sec_policy4
[DeviceC-policy-security-rule-sec_policy4] source-zone dmz
[DeviceC-policy-security-rule-sec_policy4] destination-zone trust
[DeviceC-policy-security-rule-sec_policy4] action permit
[DeviceC-policy-security-rule-sec_policy4] quit
[DeviceC-policy-security] quit
```

After the configuration is complete, the status of tunnel interfaces becomes up and the tunnel interfaces can ping each other successfully after the **service-manage ping permit** command is run on the tunnel interfaces.

Configure DeviceC.

```
[DeviceC] interface tunnel 1
[DeviceC-Tunnel1] service-manage ping permit
[DeviceC-Tunnel1] quit
```

Configure DeviceA. The following example uses the command output on DeviceA.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] service-manage ping permit
[DeviceA-Tunnel1] quit
[DeviceA] ping -a 172.22.1.1 172.22.1.2
  PING 172.22.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.22.1.2: bytes=56 Sequence=1 ttl=255 time=24 ms
    Reply from 172.22.1.2: bytes=56 Sequence=2 ttl=255 time=33 ms
    Reply from 172.22.1.2: bytes=56 Sequence=3 ttl=255 time=48 ms
    Reply from 172.22.1.2: bytes=56 Sequence=4 ttl=255 time=33 ms
    Reply from 172.22.1.2: bytes=56 Sequence=5 ttl=255 time=36 ms
  --- 172.22.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 24/34/48 ms
```

Step 5 Configure static routes.

Configure DeviceA.

```
[DeviceA] ip route-static 10.2.1.0 255.255.255.0 tunnel1
```

Configure DeviceC.

```
[DeviceC] ip route-static 10.1.1.0 255.255.255.0 tunnel1
```

----End

Verifying the Configuration

After the configuration is complete, run the **display ip routing-table** command on DeviceA and DeviceC. The command outputs show the static route with the local tunnel interface as the outbound interface and destined for the network segment of the remote end.

The following example uses the command output on DeviceA.

```
[DeviceA] display ip routing-table
Proto: Protocol        Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 15       Routes : 15
```

 Copyright © Huawei Technologies Co., Ltd.

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.1.0/24  Direct  0    0           D  10.1.1.2        GE0/0/2
      10.1.1.2/32  Direct  0    0           D  127.0.0.1       GE0/0/2
    10.1.1.255/32  Direct  0    0           D  127.0.0.1       GE0/0/2
   10.2.1.0/24  Static  60   0           D  172.22.1.1      Tunnel1
     172.20.1.0/24  Direct  0    0           D  172.20.1.1      GE0/0/1
     172.20.1.1/32  Direct  0    0           D  127.0.0.1       GE0/0/1
   172.20.1.255/32  Direct  0    0           D  127.0.0.1       GE0/0/1
     172.21.1.0/24  OSPF    10   2           D  172.20.1.2      GE0/0/1
     172.22.1.0/24  Direct  0    0           D  172.22.1.1      Tunnel1
     172.22.1.1/32  Direct  0    0           D  127.0.0.1       Tunnel1
   172.22.1.255/32  Direct  0    0           D  127.0.0.1       Tunnel1
      127.0.0.0/8   Direct  0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D  127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
```

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 172.20.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.2 255.255.255.0
#
interface Tunnel1
 ip address 172.22.1.1 255.255.255.0
 tunnel-protocol gre
 source 172.20.1.1
 destination 172.21.1.2
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface tunnel 1
#
security-policy
 rule name sec_policy1
  source-zone local
  destination-zone untrust
  action permit
 rule name sec_policy2
  source-zone untrust
  destination-zone local
  action permit
 rule name sec_policy3
  source-zone trust
  destination-zone dmz
  action permit
 rule name sec_policy4
  source-zone dmz
  destination-zone trust
  action permit
#
ospf 1
 area 0.0.0.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 network 172.20.1.0 0.0.0.255
#
ip route-static 10.2.1.0 255.255.255.0 Tunnel1
#
return
```

- DeviceB

```
#
sysname DeviceB
#
interface GE0/0/1
 ip address 172.20.1.2 255.255.255.0
#
interface GE0/0/2
 ip address 172.21.1.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
ospf 1
 area 0.0.0.0
  network 172.20.1.0 0.0.0.255
  network 172.21.1.0 0.0.0.255
#
return
```

- DeviceC

```
#
sysname DeviceC
#
interface GE0/0/1
 ip address 172.21.1.2 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.1.2 255.255.255.0
#
interface Tunnel1
 ip address 172.22.1.2 255.255.255.0
 tunnel-protocol gre
 source 172.21.1.2
 destination 172.20.1.1
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface tunnel 1
#
security-policy
 rule name sec_policy1
  source-zone local
  destination-zone untrust
  action permit
 rule name sec_policy2
  source-zone untrust
  destination-zone local
  action permit
 rule name sec_policy3
  source-zone trust
  destination-zone dmz
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule name sec_policy4
  source-zone dmz
  destination-zone trust
  action permit
#
ospf 1
 area 0.0.0.0
 network 172.21.1.0 0.0.0.255
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
return
```

11.4 CLI: Example for Configuring an IPv6 over IPv4 GRE Tunnel

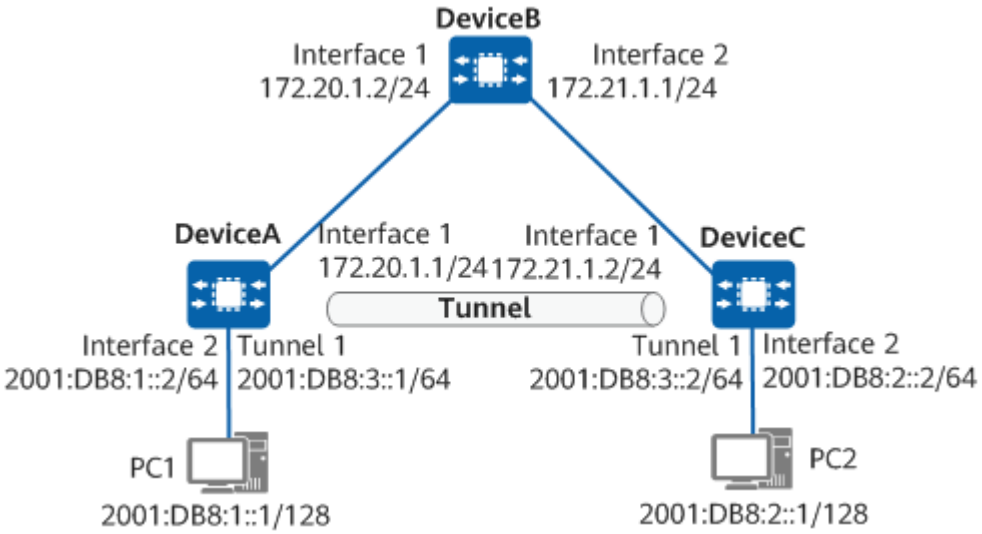
Networking Requirements

In **Figure 11-4**, DeviceA, DeviceB, and DeviceC belong to the IPv4 backbone network and are running OSPF. An IPv6 direct link needs to be established between DeviceA and DeviceC to ensure that PC1 and PC2 can communicate with each other. To meet such a requirement, an IPv6 over IPv4 GRE tunnel needs to be established between DeviceA and DeviceC and IPv6 static routes need to be configured so that packets between PC1 and PC2 can be forwarded through tunnel interfaces on both ends of the tunnel. DeviceA and DeviceC are the default gateways of PC1 and PC2, respectively.

Figure 11-4 Configuring an IPv6 over IPv4 GRE tunnel

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IPv4 dynamic routing protocol for communication between the devices.

 Copyright © Huawei Technologies Co., Ltd.

2. Create tunnel interfaces on DeviceA and DeviceC and specify the tunnel source and destination addresses. The tunnel source address is the IPv4 address of the interface that sends packets, and the tunnel destination address is the IPv4 address of the interface that receives packets.
3. Configure IPv6 addresses for the tunnel interfaces to generate tunnel routes.
4. Configure an IPv6 static route between DeviceA and PC1 and between DeviceC and PC2 and specify the local tunnel interface as the outbound interface of the static route so that IPv6 traffic between PC1 and PC2 can be transmitted through the GRE tunnel.

Procedure

Step 1 Configure IPv4 or IPv6 addresses for interfaces.

Configure an IP address for each interface according to **Figure 11-4**. For detailed configurations, see **Configuration Scripts**.

Step 2 Add interfaces to security zones and configure security policies.

Configure DeviceA.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] security-policy
[DeviceA-policy-security] rule name sec_policy1
[DeviceA-policy-security-rule-sec_policy1] source-zone local
[DeviceA-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceA-policy-security-rule-sec_policy1] action permit
[DeviceA-policy-security-rule-sec_policy1] quit
[DeviceA-policy-security] rule name sec_policy2
[DeviceA-policy-security-rule-sec_policy2] source-zone untrust
[DeviceA-policy-security-rule-sec_policy2] destination-zone local
[DeviceA-policy-security-rule-sec_policy2] action permit
[DeviceA-policy-security-rule-sec_policy2] quit
[DeviceA-policy-security] quit
```

Configure DeviceB.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] add interface ge 0/0/2
[DeviceB-zone-untrust] quit
```

Configure DeviceC.

```
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface ge 0/0/2
[DeviceC-zone-trust] quit
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface ge 0/0/1
[DeviceC-zone-untrust] quit
[DeviceC] security-policy
[DeviceC-policy-security] rule name sec_policy1
[DeviceC-policy-security-rule-sec_policy1] source-zone local
[DeviceC-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceC-policy-security-rule-sec_policy1] action permit
[DeviceC-policy-security-rule-sec_policy1] quit
[DeviceC-policy-security] rule name sec_policy2
[DeviceC-policy-security-rule-sec_policy2] source-zone untrust
[DeviceC-policy-security-rule-sec_policy2] destination-zone local
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceC-policy-security-rule-sec_policy2] action permit
[DeviceC-policy-security-rule-sec_policy2] quit
[DeviceC-policy-security] quit
```

Step 3 Configure an IGP on the IPv4 backbone network.

Configure DeviceA.

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 172.20.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

Configure DeviceB.

```
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 172.20.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 172.21.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Configure DeviceC.

```
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 172.21.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

After the configuration is complete, run the **display ip routing-table** command on DeviceA and DeviceC. The command outputs show that DeviceA and DeviceC can learn the OSPF route to the network segment of the remote interface.

The following example uses the command output on DeviceA.

```
[DeviceA] display ip routing-table
Proto: Protocol         Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      172.20.1.0/24  Direct  0    0           D  172.20.1.1      GE0/0/1
      172.20.1.1/32  Direct  0    0           D  127.0.0.1       GE0/0/1
    172.20.1.255/32  Direct  0    0           D  127.0.0.1       GE0/0/1
      172.21.1.0/24  OSPF    10   2           D  172.20.1.2      GE0/0/1
      127.0.0.0/8    Direct  0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32   Direct  0    0           D  127.0.0.1       InLoopBack0
127.255.255.255/32   Direct  0    0           D  127.0.0.1       InLoopBack0
255.255.255.255/32   Direct  0    0           D  127.0.0.1       InLoopBack0
```

Step 4 Configure tunnel interfaces.

Configure DeviceA.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] tunnel-protocol gre
[DeviceA-Tunnel1] ipv6 enable
[DeviceA-Tunnel1] ipv6 address 2001:DB8:3::1 64
[DeviceA-Tunnel1] source 172.20.1.1
[DeviceA-Tunnel1] destination 172.21.1.2
[DeviceA-Tunnel1] quit
```

Add DeviceA's tunnel interface to a security zone and configure security policies.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface tunnel 1
[DeviceA-zone-dmz] quit
[DeviceA] security-policy
[DeviceA-policy-security] rule name sec_policy3
[DeviceA-policy-security-rule-sec_policy3] source-zone trust
[DeviceA-policy-security-rule-sec_policy3] destination-zone dmz
[DeviceA-policy-security-rule-sec_policy3] action permit
[DeviceA-policy-security-rule-sec_policy3] quit
[DeviceA-policy-security] rule name sec_policy4
[DeviceA-policy-security-rule-sec_policy4] source-zone dmz
[DeviceA-policy-security-rule-sec_policy4] destination-zone trust
[DeviceA-policy-security-rule-sec_policy4] action permit
[DeviceA-policy-security-rule-sec_policy4] quit
[DeviceA-policy-security] quit
```

Configure DeviceC.

```
[DeviceC] interface tunnel 1
[DeviceC-Tunnel1] tunnel-protocol gre
[DeviceC-Tunnel1] ipv6 enable
[DeviceC-Tunnel1] ipv6 address 2001:DB8:3::2 64
[DeviceC-Tunnel1] source 172.21.1.2
[DeviceC-Tunnel1] destination 172.20.1.1
[DeviceC-Tunnel1] quit
```

Add DeviceC's tunnel interface to a security zone and configure security policies.

```
[DeviceC] firewall zone dmz
[DeviceC-zone-dmz] add interface tunnel 1
[DeviceC-zone-dmz] quit
[DeviceC] security-policy
[DeviceC-policy-security] rule name sec_policy3
[DeviceC-policy-security-rule-sec_policy3] source-zone trust
[DeviceC-policy-security-rule-sec_policy3] destination-zone dmz
[DeviceC-policy-security-rule-sec_policy3] action permit
[DeviceC-policy-security-rule-sec_policy3] quit
[DeviceC-policy-security] rule name sec_policy4
[DeviceC-policy-security-rule-sec_policy4] source-zone dmz
[DeviceC-policy-security-rule-sec_policy4] destination-zone trust
[DeviceC-policy-security-rule-sec_policy4] action permit
[DeviceC-policy-security-rule-sec_policy4] quit
[DeviceC-policy-security] quit
```

After the configuration is complete, the IPv6 status of tunnel interfaces becomes Up and the tunnel interfaces can ping each other successfully after the **service-manage ping permit** command is run on the tunnel interfaces.

Configure DeviceC.

```
[DeviceC] interface tunnel 1
[DeviceC-Tunnel1] service-manage ping permit
[DeviceC-Tunnel1] quit
```

Configure DeviceA. The following example uses the command output on DeviceA.

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] service-manage ping permit
[DeviceA-Tunnel1] quit
[DeviceA] ping ipv6 -a 2001:DB8:3::1 2001:DB8:3::2
  PING 2001:DB8:3::2 : 56  data bytes, press CTRL_C to break
    Reply from 2001:DB8:3::2
    bytes=56 Sequence=1 hop limit=64 time=11 ms
    Reply from 2001:DB8:3::2
    bytes=56 Sequence=2 hop limit=64 time=5 ms
    Reply from 2001:DB8:3::2
    bytes=56 Sequence=3 hop limit=64 time=5 ms
    Reply from 2001:DB8:3::2
```

 Copyright © Huawei Technologies Co., Ltd.

```
  bytes=56 Sequence=4 hop limit=64 time=5 ms
  Reply from 2001:DB8:3::2
  bytes=56 Sequence=5 hop limit=64 time=5 ms

 --- 2001:DB8:3::2 ping statistics---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max=5/6/11 ms
```

Step 5 Configure static routes.

Configure DeviceA.

```
[DeviceA] ipv6 route-static 2001:DB8:2:: 64 tunnel1
```

Configure DeviceC.

```
[DeviceC] ipv6 route-static 2001:DB8:1:: 64 tunnel1
```

----End

Verifying the Configuration

After the configuration is complete, run the **display ipv6 routing-table** command on DeviceA and DeviceC. The command outputs show the IPv6 static route with the local tunnel interface as the outbound interface and destined for the network segment of the remote end.

The following example uses the command output on DeviceA.

```
[DeviceA] display ipv6 routing-table
Route Flags: R - relay, D - download to fib, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 8        Routes : 8

Destination  : ::1                          PrefixLength : 128
NextHop      : ::1                          Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : InLoopBack0                  Flags        : D

Destination  : ::FFFF:127.0.0.0             PrefixLength : 104
NextHop      : ::FFFF:127.0.0.1             Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : InLoopBack0                  Flags        : D

Destination  : ::FFFF:127.0.0.1             PrefixLength : 128
NextHop      : ::1                          Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : InLoopBack0                  Flags        : D

Destination  : 2001:DB8:3::                 PrefixLength : 64
NextHop      : 2001:DB8:3::1                Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : Tunnel1                      Flags        : D

Destination  : 2001:DB8:3::1                PrefixLength : 128
NextHop      : ::1                          Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : Tunnel1                      Flags        : D
```

 Copyright © Huawei Technologies Co., Ltd.

```
Destination  : 2001:DB8:1::                 PrefixLength : 64
NextHop      : ::1                         Preference   : 0
Cost         : 0                           Protocol     : Direct
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : GE0/0/2                     Flags        : D

Destination  : 2001:DB8:1::2               PrefixLength : 128
NextHop      : ::1                         Preference   : 0
Cost         : 0                           Protocol     : Direct
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : GE0/0/2                     Flags        : D

Destination  : 2001:DB8:2::                PrefixLength : 64
NextHop      : ::1                         Preference   : 60
Cost         : 0                           Protocol     : Static
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : Tunnel1                     Flags        : D
```

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 172.20.1.1 255.255.255.0
#
interface GE0/0/2
 ipv6 enable
 ipv6 address 2001:DB8:1::2/64
#
interface Tunnel1
 ipv6 enable
 ipv6 address 2001:DB8:3::1/64
 tunnel-protocol gre
 source 172.20.1.1
 destination 172.21.1.2
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface tunnel 1
#
security-policy
 rule name sec_policy1
  source-zone local
  destination-zone untrust
  action permit
 rule name sec_policy2
  source-zone untrust
  destination-zone local
  action permit
 rule name sec_policy3
  source-zone trust
  destination-zone dmz
  action permit
 rule name sec_policy4
  source-zone dmz
  destination-zone trust
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
ospf 1
 area 0.0.0.0
  network 172.20.1.0 0.0.0.255
#
ipv6 route-static 2001:DB8:2:: 64 Tunnel1
#
return
```

- DeviceB

```
#
sysname DeviceB
#
interface GE0/0/1
 ip address 172.20.1.2 255.255.255.0
#
interface GE0/0/2
 ip address 172.21.1.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
ospf 1
 area 0.0.0.0
  network 172.20.1.0 0.0.0.255
  network 172.21.1.0 0.0.0.255
#
return
```

- DeviceC

```
#
sysname DeviceC
#
interface GE0/0/1
 ip address 172.21.1.2 255.255.255.0
#
interface GE0/0/2
 ipv6 enable
 ipv6 address 2001:DB8:2::2/64
#
interface Tunnel1
 ipv6 enable
 ipv6 address 2001:DB8:3::2/64
 tunnel-protocol gre
 source 172.21.1.2
 destination 172.20.1.1
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface tunnel 1
#
security-policy
 rule name sec_policy1
  source-zone local
  destination-zone untrust
  action permit
 rule name sec_policy2
  source-zone untrust
  destination-zone local
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule name sec_policy3
  source-zone trust
  destination-zone dmz
  action permit
 rule name sec_policy4
  source-zone dmz
  destination-zone trust
  action permit
#
ospf 1
 area 0.0.0.0
 network 172.21.1.0 0.0.0.255
#
ipv6 route-static 2001:DB8:1:: 64 Tunnel1
#
return
```

11.5 Web: Example for Configuring an IPsec over GRE Tunnel

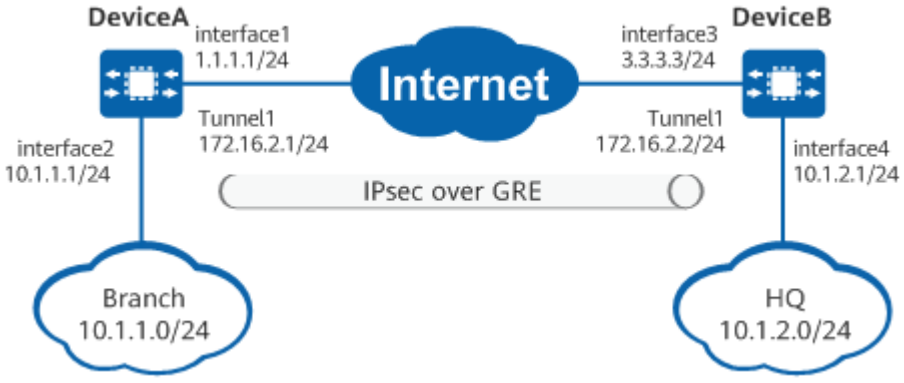
Networking Requirements

The enterprise branch and headquarters originally communicate through a GRE tunnel. As network threats become severe, the enterprise manager intends to enhance network communication security without changing the existing network deployment. Therefore, IPsec protection can be performed on traffic transmitted through the GRE tunnel to form an IPsec over GRE tunnel, as shown in **Figure 11-5**.

Figure 11-5 Configuring an IPsec over GRE tunnel

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 on DeviceA respectively, and interface 3 and interface 4 represent GE0/0/1 and GE0/0/2 on DeviceB respectively.



Item	Data	Description
DeviceA	Interface configuration	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
		Interface number: GE0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	GRE configuration	Interface name: Tunnel1 IP address: 172.16.2.1/24 Source address: 1.1.1.1/24 Destination address: 3.3.3.3/24 Tunnel identification keyword: 123456
	IPsec configuration	Local interface: Tunnel1 Local address: 172.16.2.1 Remote address: 172.16.2.2 Authentication mode: pre-shared key (PSK) authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any remote ID
DeviceB	Interface configuration	Interface number: GE0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust
		Interface number: GE0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	GRE configuration	Interface name: Tunnel1 IP address: 172.16.2.2/24 Source address: 3.3.3.3/24 Destination address: 1.1.1.1/24 Tunnel identification keyword: 123456
	IPsec configuration	Local interface: Tunnel1 Local address: 172.16.2.2 Remote address: 172.16.2.1 Authentication mode: pre-shared key (PSK) authentication PSK: YsHsjx_202206 Local ID type: IP address Remote ID type: any remote ID

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Create a tunnel interface on both DeviceA and DeviceB to establish a GRE tunnel.
2. Configure an IPsec policy on both DeviceA and DeviceB and apply the policy to tunnel interfaces on both ends of the GRE tunnel.

Procedure

Step 1 Configure DeviceA.

1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

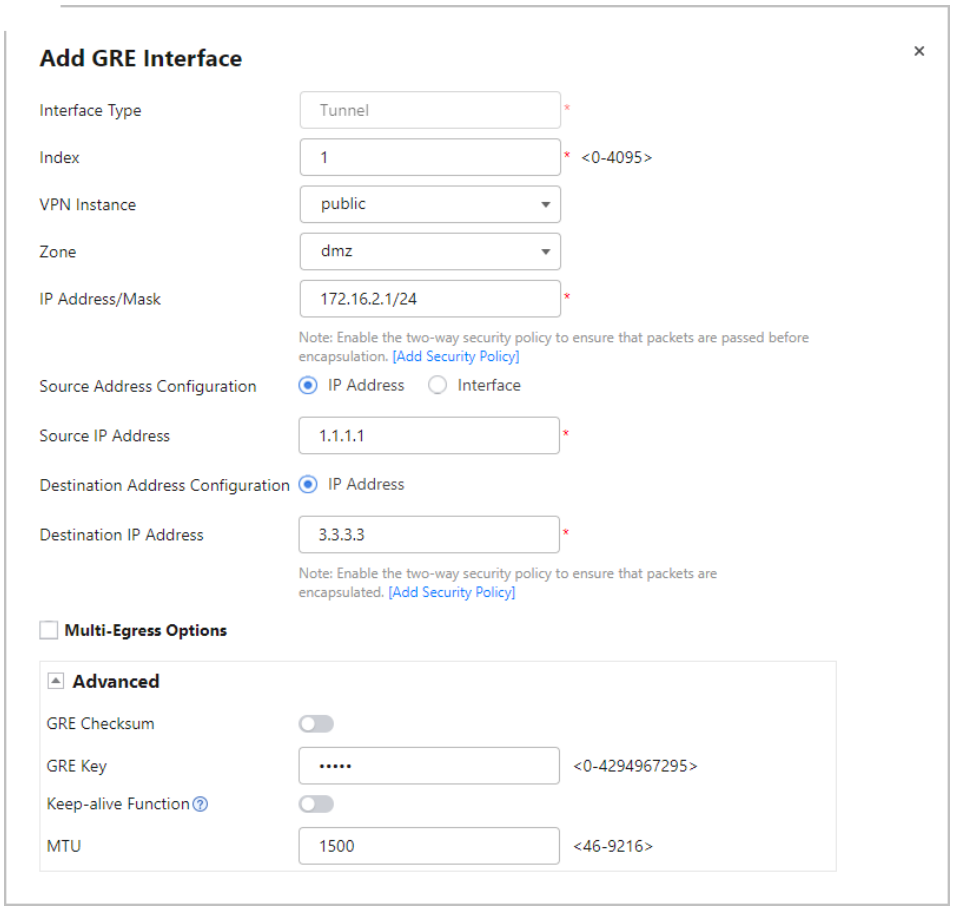
Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.1.1/24

2. Set encapsulation parameters for the tunnel interface.
   a. Choose **Network** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Set GRE tunnel interface parameters. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.



3. Configure security policies to permit original and encapsulated packets.
   a. Choose **Policy** > **Security Policy** > **Security Policy**.
   b. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	dmz
Action	Permit

   c. Repeat the preceding steps to configure the DMZ-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	dmz
Destination Zone	trust
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

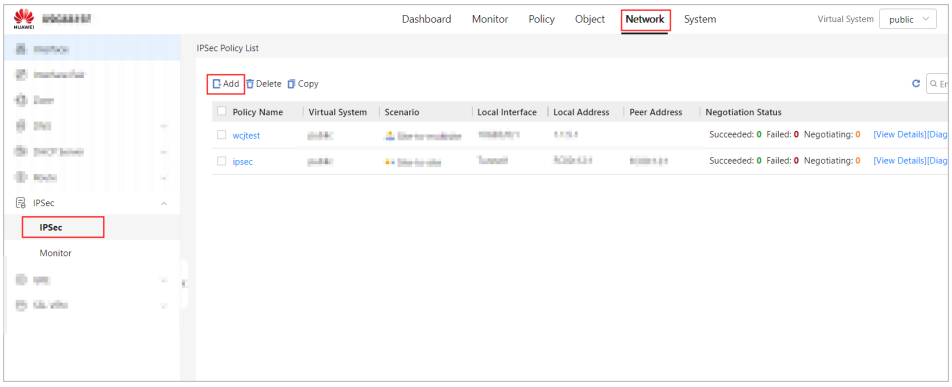
Name	policy3
Source Zone	local
Destination Zone	untrust
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Action	Permit

4. Configure a static route to direct traffic to be transmitted over the GRE tunnel to the GRE tunnel.
   a. Choose **Network** > **Route** > **Static Route**.
   b. In **Static Route List**, click **Add**.
   c. Configure a static route as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.1.2.0/24
Interface	Tunnel1

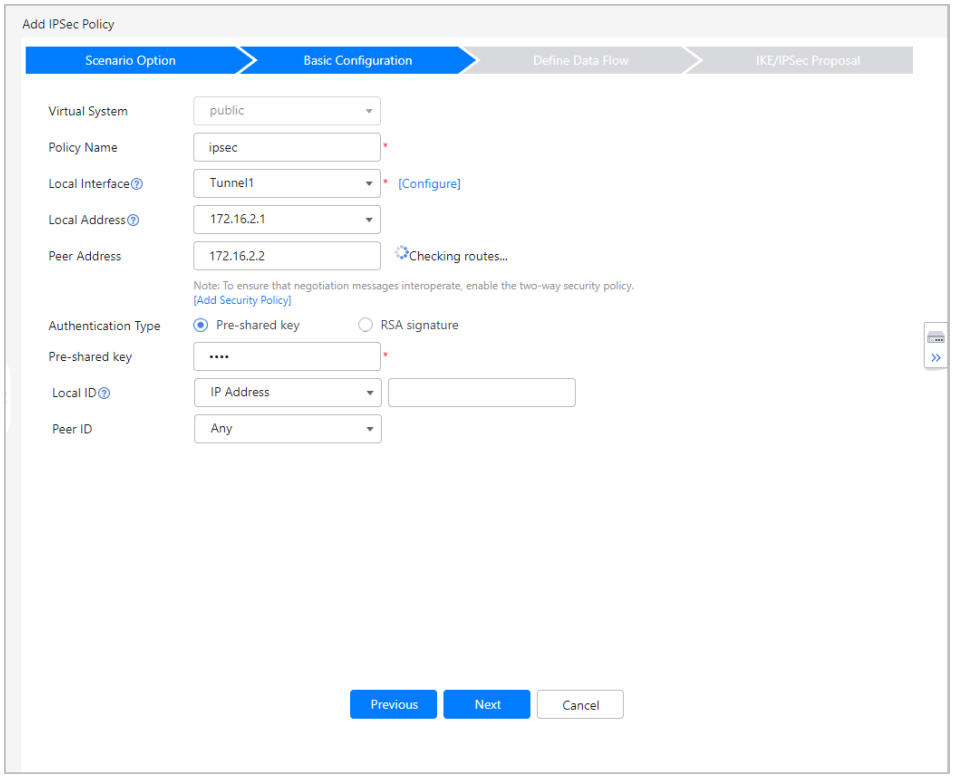
5. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.



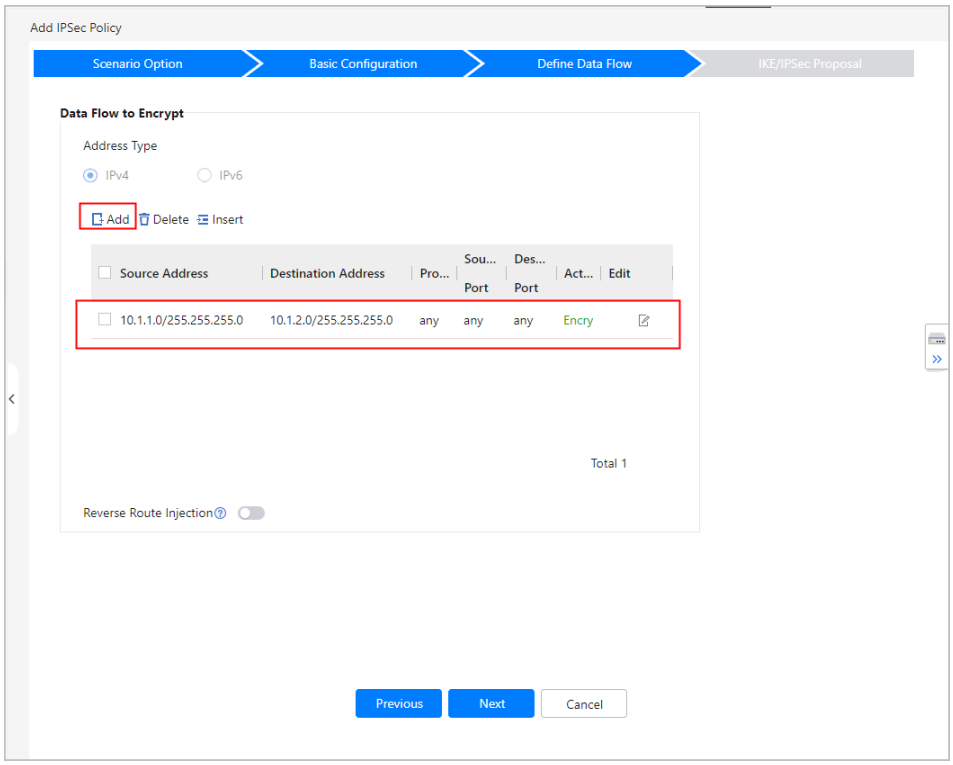
   b. Click **Add** to create an IPsec policy as prompted.

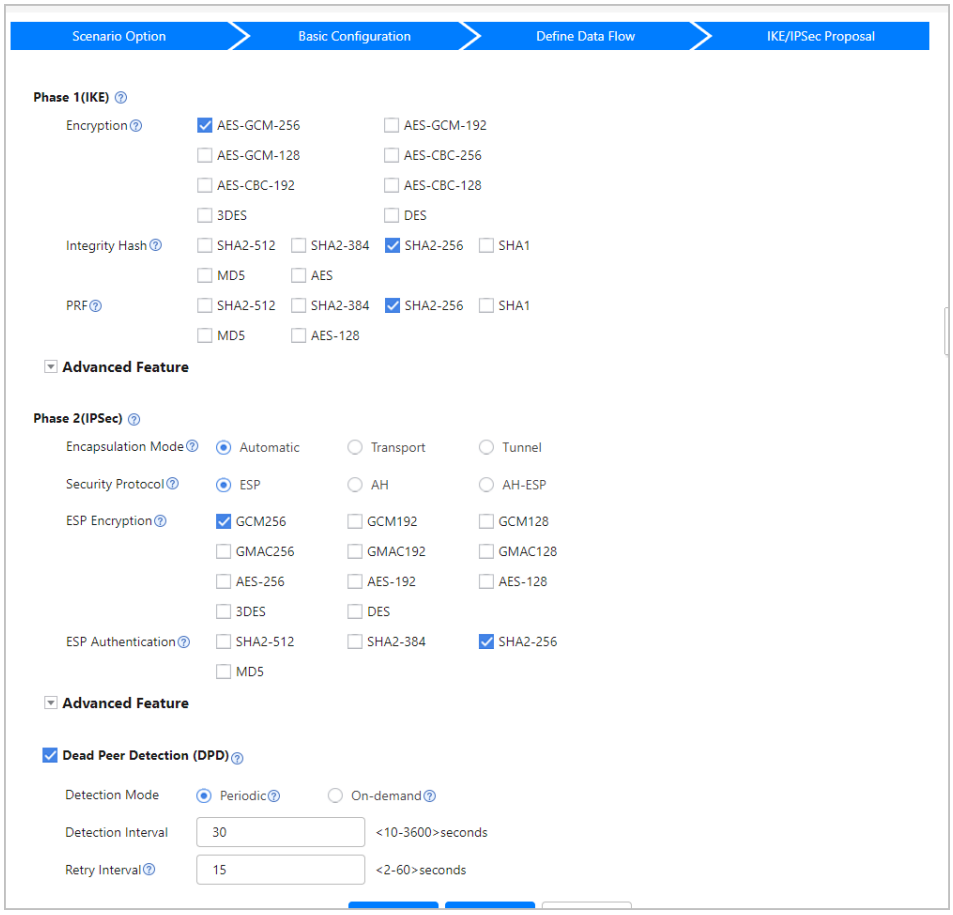
 Copyright © Huawei Technologies Co., Ltd.





 Copyright © Huawei Technologies Co., Ltd.





c. Click **Finish**.

Step 2 Configure DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

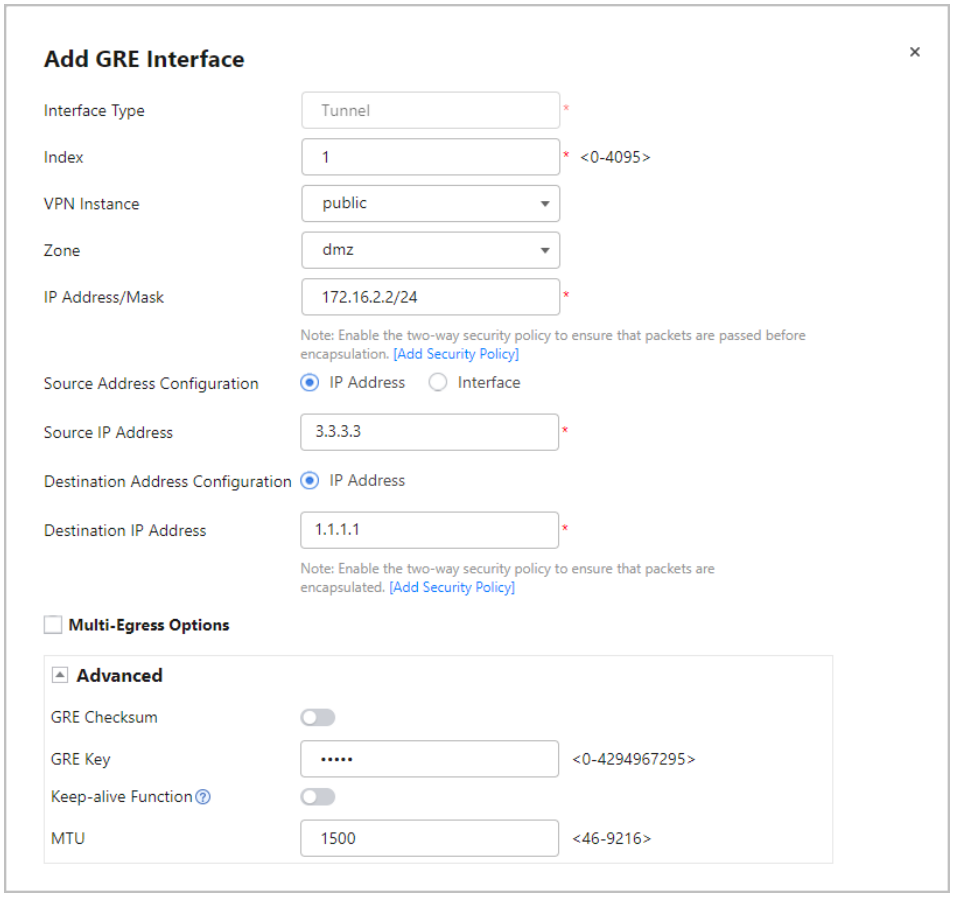
1. Set interface IP addresses and add the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	3.3.3.3/24

   c. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

2. Set encapsulation parameters for the tunnel interface.
   a. Choose **Network** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Set GRE tunnel interface parameters. Click **OK**.



3. Configure security policies.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy as follows to permit original packets. Click **OK**.

Name	policy1
Source Zone	trust
Destination Zone	dmz
Action	Permit

c. Repeat the preceding steps to configure the DMZ-to-Trust, Local-to-Untrust, and Untrust-to-Local interzone policies.

Name	policy2
Source Zone	dmz
Destination Zone	trust
Action	Permit

Name	policy3
Source Zone	local
Destination Zone	untrust
Action	Permit

Name	policy4
Source Zone	untrust
Destination Zone	local
Action	Permit

4. Configure a static route to direct traffic to be transmitted over the GRE tunnel to the GRE tunnel.

a. Choose **Network** > **Route** > **Static Route**.

b. In **Static Route List**, click **Add**.

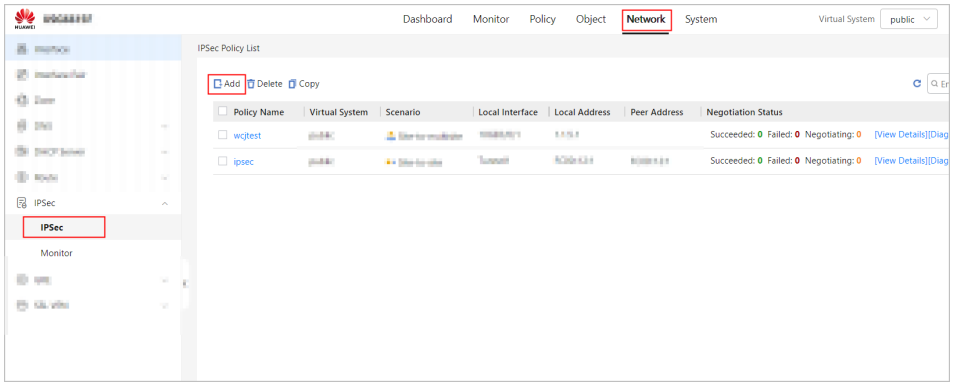
c. Configure a static route as follows. Click **OK**.

Protocol	IPv4
Destination Address/Mask	10.1.1.0/24

 Copyright © Huawei Technologies Co., Ltd.

Interface	Tunnel1

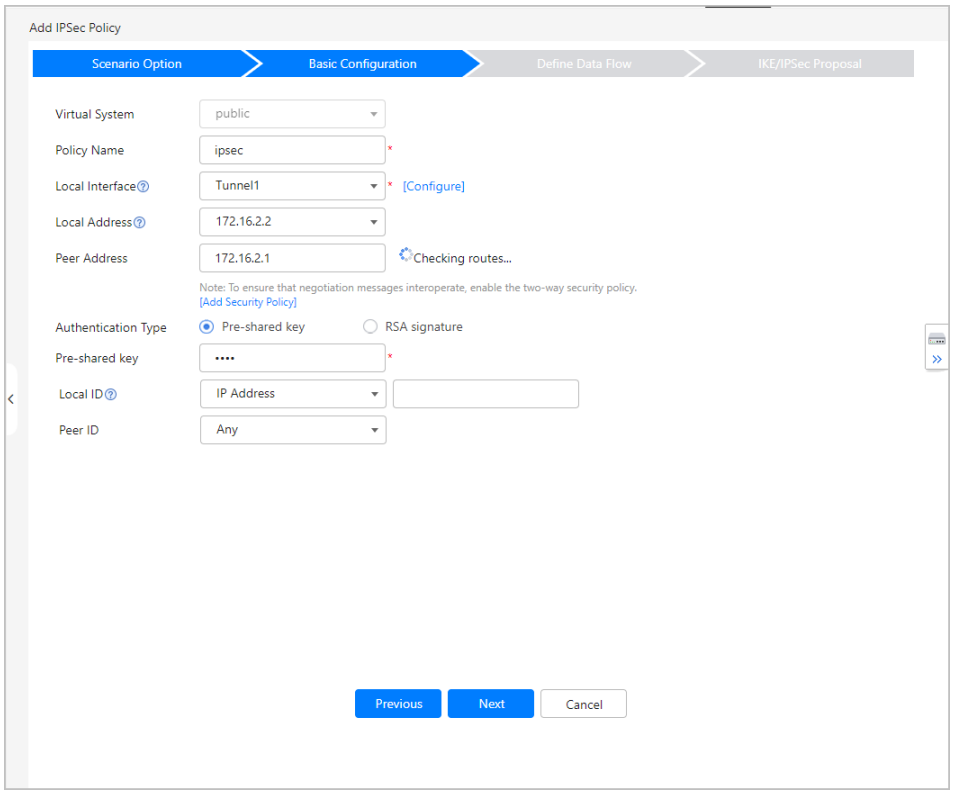
5. Configure an IPsec policy.
   a. Choose **Network** > **IPSec** > **IPSec**.

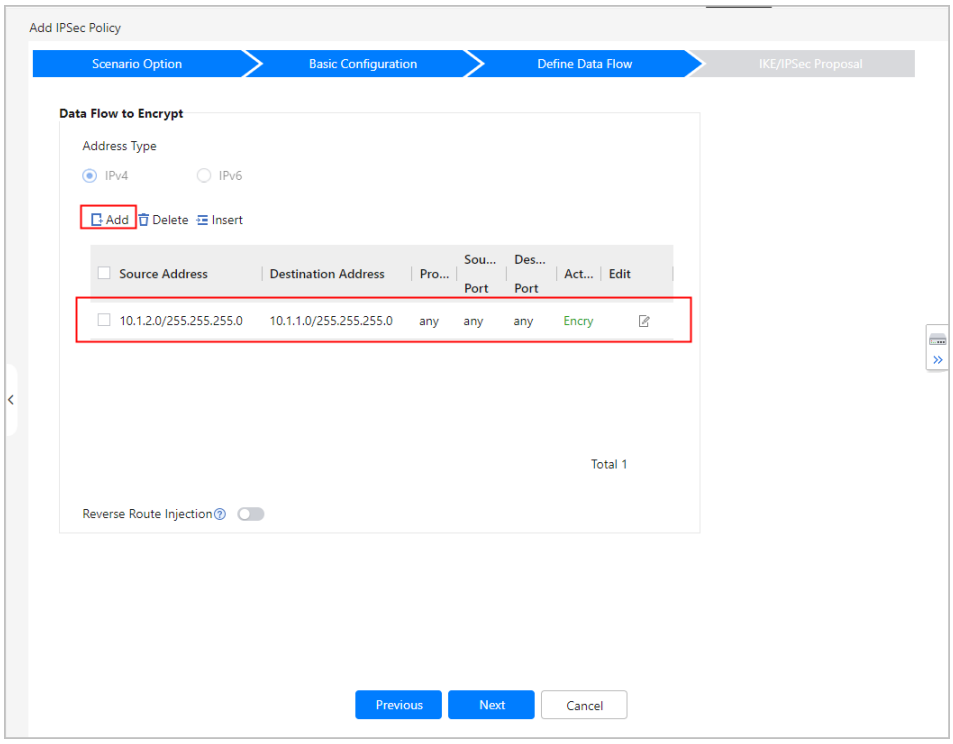


   b. Click **Add** to create an IPsec policy as prompted.

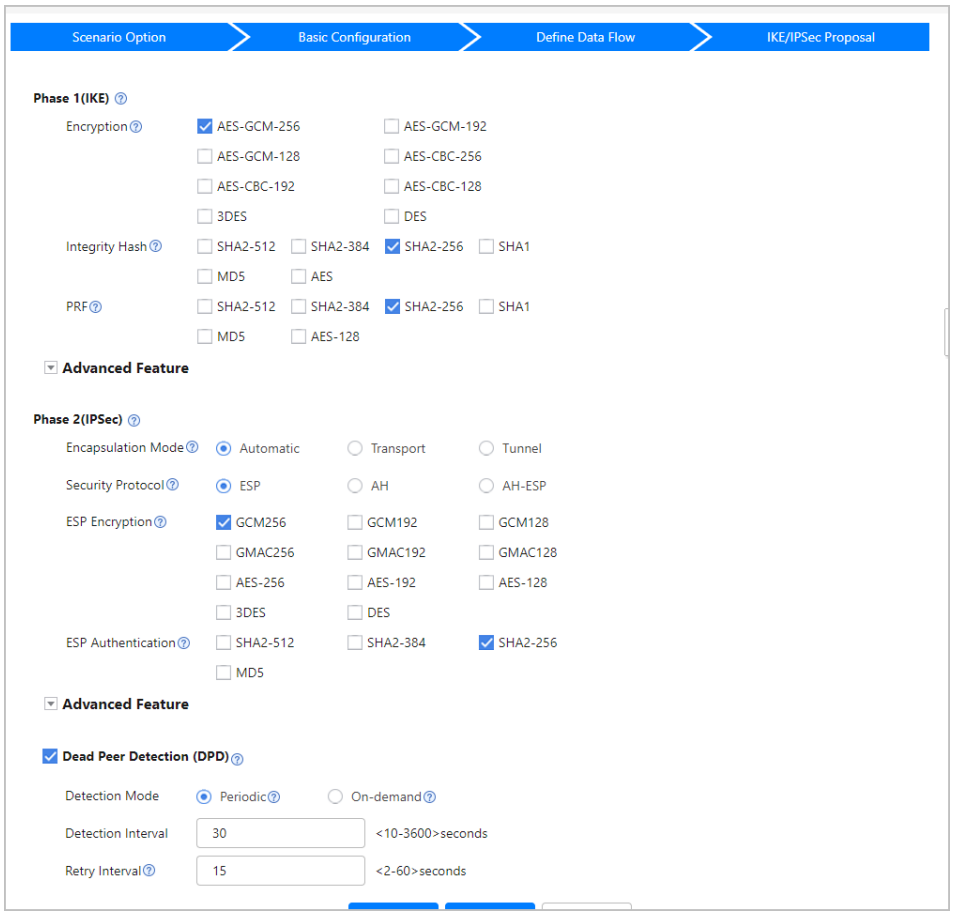


 Copyright © Huawei Technologies Co., Ltd.





 Copyright © Huawei Technologies Co., Ltd.



c. Click **Finish**.

----End

Verifying the Configuration

1. PCs on networks 1 and 2 can ping each other.
2. An IPsec tunnel can be found on the **Network** > **IPSec** > **Monitor** page of DeviceA's or DeviceB's web UI.
3. A route whose outbound interface is Tunnel1 and destination address is 10.1.2.0/24 can be found on the **Network** > **Route** > **Routing Table** page of DeviceA's web Ul.

Configuration Scripts

- DeviceA

```
#
acl 3000
 rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
```

 Copyright © Huawei Technologies Co., Ltd.

```
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer b
 ike-proposal 10
 remote-address 172.16.2.2
 pre-shared-key %+%#eY>XCM5+)9nKwEIT`J+YA0lL31/MGS=gZBF.""`6%+%#
#
ipsec policy ipsec 10 isakmp
 security acl 3000
 proposal tran1
 ike-peer b
 scenario point-to-point
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel1
 ip address 172.16.2.1 255.255.255.0
 tunnel-protocol gre
 source 1.1.1.1
 destination 3.3.3.3
 gre key cipher %+%#=F~T>w'>n:QlQ8BI3>67Ir3I*Onzv'\(%+%#
 ipsec policy ipsec
#
ip route-static 10.1.2.0 255.255.255.0 Tunnel1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone dmz
  action permit
 rule name policy2
  source-zone dmz
  destination-zone trust
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  action permit
```

- DeviceB

```
#
acl 3000
 rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm gcm-128
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 ike-proposal 10
 remote-address 172.16.2.1
 pre-shared-key %+%#eY>XCM5+)9nKwEIT`J+YA0lL31/MGS=gZBF.""`6%+%#
#
ipsec policy ipsec 10 isakmp
 security acl 3000
 proposal tran1
 ike-peer a
 scenario point-to-point
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel1
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 source 3.3.3.3
 destination 1.1.1.1
 gre key cipher %+%#=F~T>w'>n:QlQ8BI3>67Ir3I*Onzv'\(%+%#
 ipsec policy ipsec
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone dmz
  action permit
 rule name policy2
  source-zone dmz
  destination-zone trust
  action permit
 rule name policy3
  source-zone local
  destination-zone untrust
  action permit
 rule name policy4
  source-zone untrust
  destination-zone local
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

11.6 CLI: Example for Configuring an IPsec over GRE Tunnel

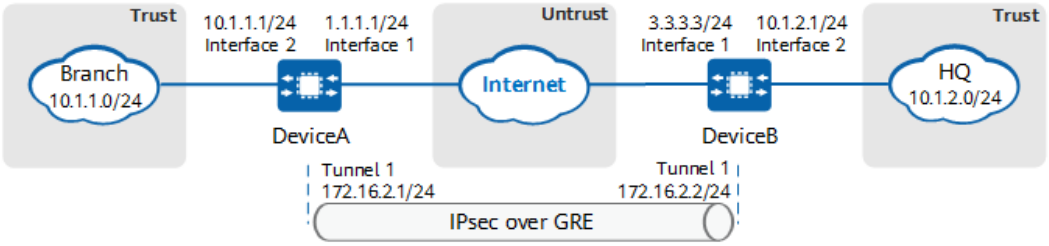
Networking Requirements

In Figure 11-6, the branch and headquarters (HQ) are connected to the Internet through DeviceA and DeviceB, respectively. There are reachable routes between DeviceA and DeviceB. The two devices communicate with each other through a GRE tunnel, and IPsec protection is required for the GRE tunnel to implement secure transmission of data flows in the tunnel.

Figure 11-6 Network diagram of an IPsec over GRE tunnel

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2 respectively.



Item	Data
DeviceA	Interface: GE 0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.1.1/24 Security zone: Trust
	GRE configuration Interface: Tunnel 1 IP address: 172.16.2.1/24 Source address: 1.1.1.1/24 Destination address: 3.3.3.3/24 Tunnel identification keyword: 1024256

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
	IPsec configuration Remote address: 172.16.2.2 Authentication type: pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID type: any remote ID
DeviceB	Interface: GE 0/0/1 IP address: 3.3.3.3/24 Security zone: Untrust
	Interface: GE 0/0/2 IP address: 10.1.2.1/24 Security zone: Trust
	GRE configuration Interface: Tunnel 1 IP address: 172.16.2.2/24 Source address: 3.3.3.3/24 Destination address: 1.1.1.1/24 Tunnel identification keyword: 1024256
	IPsec configuration Remote address: 172.16.2.1 Authentication type: pre-shared key Pre-shared key: YsHsjx_202206 Local ID type: IP address Remote ID type: any remote ID

Configuration Roadmap

NOTE

In this example, IPsec uses default security algorithms.

For security purposes, you are advised not to use the weak security algorithm or weak security protocol of this feature. If you must use such weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm or protocol feature package WEAKEA.

1. Create a tunnel interface on both DeviceA and DeviceB to establish a GRE tunnel.
2. Configure an IPsec policy on DeviceA and DeviceB and apply the policy to both GRE tunnel interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure public and private network interfaces on DeviceA, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Configure the tunnel interface Tunnel 1.

```
[DeviceA] interface Tunnel 1
[DeviceA-Tunnel1] ip address 172.16.2.1 24
[DeviceA-Tunnel1] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Add Tunnel 1 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface tunnel 1
[DeviceA-zone-dmz] quit
```

Step 2 Configure inter-zone security policies on DeviceA to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure a security policy between the Trust zone and DMZ to permit unencapsulated packets.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust dmz
[DeviceA-policy-security-rule-policy1] destination-zone dmz trust
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
```

Configure a security policy between the Local zone and DMZ to permit IPsec encapsulated packets.

```
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone local dmz
[DeviceA-policy-security-rule-policy2] destination-zone dmz local
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
```

Configure a security policy between the Local and Untrust zones to permit GRE encapsulated packets.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security] rule name policy3
[DeviceA-policy-security-rule-policy3] source-zone local untrust
[DeviceA-policy-security-rule-policy3] destination-zone untrust local
[DeviceA-policy-security-rule-policy3] service gre
[DeviceA-policy-security-rule-policy3] action permit
[DeviceA-policy-security-rule-policy3] quit
```

Step 3 Configure a GRE tunnel interface on DeviceA.

```
[DeviceA] interface Tunnel 1
[DeviceA-Tunnel1] tunnel-protocol gre
[DeviceA-Tunnel1] source ge 0/0/1
[DeviceA-Tunnel1] destination 3.3.3.3
[DeviceA-Tunnel1] gre key cipher 1024256
[DeviceA-Tunnel1] keepalive
[DeviceA-Tunnel1] quit
```

Step 4 Configure an ISAKMP IPsec policy on DeviceA.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.1.0/24 to access the network segment 10.1.2.0/24.

   ```
   [DeviceA] acl 3000
   [DeviceA-acl4-advance-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
   [DeviceA-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceA] ipsec proposal tran1
   [DeviceA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceA-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceA-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceA] ike proposal 10
   [DeviceA-ike-proposal-10] authentication-method pre-share
   [DeviceA-ike-proposal-10] prf hmac-sha2-256
   [DeviceA-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceA-ike-proposal-10] dh group14
   [DeviceA-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceA-ike-proposal-10] quit
   ```

4. Configure an IKE peer.

   ```
   [DeviceA] ike peer b
   [DeviceA-ike-peer-b] ike-proposal 10
   [DeviceA-ike-peer-b] remote-address 172.16.2.2
   [DeviceA-ike-peer-b] pre-shared-key YsHsjx_202206
   [DeviceA-ike-peer-b] quit
   ```

5. Configure an IPsec policy.

   ```
   [DeviceA] ipsec policy map1 10 isakmp
   [DeviceA-ipsec-policy-isakmp-map1-10] security acl 3000
   [DeviceA-ipsec-policy-isakmp-map1-10] proposal tran1
   [DeviceA-ipsec-policy-isakmp-map1-10] ike-peer b
   [DeviceA-ipsec-policy-isakmp-map1-10] quit
   ```

6. Apply the IPsec policy to the tunnel interface.

   ```
   [DeviceA] interface tunnel 1
   [DeviceA-Tunnel1] ipsec policy map1
   [DeviceA-Tunnel1] quit
   ```

Step 5 Configure routes on DeviceA to divert traffic destined for the HQ intranet to the GRE tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceA to the Internet is 1.1.1.254.

```
[DeviceA] ip route-static 0.0.0.0 0 1.1.1.254
[DeviceA] ip route-static 10.1.2.0 24 Tunnel1
```

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure public and private network interfaces on DeviceB, and add the interfaces to security zones.

Configure the public network interface GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] undo portswitch
[DeviceB-GE0/0/1] ip address 3.3.3.3 24
[DeviceB-GE0/0/1] quit
```

Configure the private network interface GE 0/0/2.

```
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] undo portswitch
[DeviceB-GE0/0/2] ip address 10.1.2.1 24
[DeviceB-GE0/0/2] quit
```

Configure the tunnel interface Tunnel 1.

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] ip address 172.16.2.2 24
[DeviceB-Tunnel1] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/2
[DeviceB-zone-trust] quit
```

Add Tunnel 1 to the DMZ.

```
[DeviceB] firewall zone dmz
[DeviceB-zone-dmz] add interface tunnel 1
[DeviceB-zone-dmz] quit
```

Step 7 Configure inter-zone security policies on DeviceB to permit tunnel negotiation packets and encrypted data packets transmitted through the tunnel.

Configure a security policy between the Trust zone and DMZ to permit unencapsulated packets.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name policy1
[DeviceB-policy-security-rule-policy1] source-zone trust dmz
[DeviceB-policy-security-rule-policy1] destination-zone dmz trust
[DeviceB-policy-security-rule-policy1] action permit
[DeviceB-policy-security-rule-policy1] quit
```

Configure a security policy between the Local zone and DMZ to permit IPsec encapsulated packets.

```
[DeviceB-policy-security] rule name policy2
[DeviceB-policy-security-rule-policy2] source-zone local dmz
[DeviceB-policy-security-rule-policy2] destination-zone dmz local
[DeviceB-policy-security-rule-policy2] action permit
[DeviceB-policy-security-rule-policy2] quit
```

Configure a security policy between the Local and Untrust zones to permit GRE encapsulated packets.

```
[DeviceB-policy-security] rule name policy3
[DeviceB-policy-security-rule-policy3] source-zone local untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB-policy-security-rule-policy3] destination-zone untrust local
[DeviceB-policy-security-rule-policy3] service gre
[DeviceB-policy-security-rule-policy3] action permit
[DeviceB-policy-security-rule-policy3] quit
```

Step 8 Configure a GRE tunnel interface on DeviceB.

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] tunnel-protocol gre
[DeviceB-Tunnel1] source ge 0/0/1
[DeviceB-Tunnel1] destination 1.1.1.1
[DeviceB-Tunnel1] gre key cipher 1024256
[DeviceB-Tunnel1] keepalive
[DeviceB-Tunnel1] quit
```

Step 9 Configure an ISAKMP IPsec policy on DeviceB.

1. Create the advanced ACL 3000, define the data flow to be protected, and allow devices on the network segment 10.1.2.0/24 to access the network segment 10.1.1.0/24.

   ```
   [DeviceB] acl 3000
   [DeviceB-acl4-advance-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
   [DeviceB-acl4-advance-3000] quit
   ```

2. Configure an IPsec proposal.

   ```
   [DeviceB] ipsec proposal tran1
   [DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
   [DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256-gcm-128
   [DeviceB-ipsec-proposal-tran1] quit
   ```

3. Configure an IKE proposal.

   ```
   [DeviceB] ike proposal 10
   [DeviceB-ike-proposal-10] authentication-method pre-share
   [DeviceB-ike-proposal-10] prf hmac-sha2-256
   [DeviceB-ike-proposal-10] encryption-algorithm aes-gcm-256
   [DeviceB-ike-proposal-10] dh group14
   [DeviceB-ike-proposal-10] integrity-algorithm hmac-sha2-256
   [DeviceB-ike-proposal-10] quit
   ```

4. Configure an IKE peer.

   ```
   [DeviceB] ike peer a
   [DeviceB-ike-peer-a] ike-proposal 10
   [DeviceB-ike-peer-a] remote-address 172.16.2.1
   [DeviceB-ike-peer-a] pre-shared-key YsHsjx_202206
   [DeviceB-ike-peer-a] quit
   ```

5. Configure an IPsec policy.

   ```
   [DeviceB] ipsec policy map1 10 isakmp
   [DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
   [DeviceB-ipsec-policy-isakmp-map1-10] proposal tran1
   [DeviceB-ipsec-policy-isakmp-map1-10] ike-peer a
   [DeviceB-ipsec-policy-isakmp-map1-10] quit
   ```

6. Apply the IPsec policy to the tunnel interface.

   ```
   [DeviceB] interface tunnel 1
   [DeviceB-Tunnel1] ipsec policy map1
   [DeviceB-Tunnel1] quit
   ```

Step 10 Configure routes on DeviceB to divert traffic destined for the branch intranet to the GRE tunnel.

NOTE

Assume that the next-hop IP address of the route from DeviceB to the Internet is 3.3.3.254.

```
[DeviceB] ip route-static 0.0.0.0 0 3.3.3.254
[DeviceB] ip route-static 10.1.1.0 24 Tunnel1
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Run the **display ipsec sa** command to check IPsec SA establishment. The following example uses the command output on DeviceA.

```
[DeviceA] display ipsec sa
ipsec sa information:

===============================
Interface: Tunnel1
===============================

 ----------------------------
 IPSec policy name: "map1"
 Sequence number  : 1
 Acl group        : 3000
 Acl rule         : 5
 Mode             : ISAKMP
 ----------------------------
   Connection ID     : 278
   Encapsulation mode: Tunnel
   Tunnel local      : 172.16.2.1
   Tunnel remote     : 172.16.2.2
   Flow source       : 10.1.1.0/255.255.255.0 0/0
   Flow destination  : 10.1.2.0/255.255.255.0 0/0

   [Outbound ESP SAs]
     SPI: 3907311427 (0xe8e4d743)
     Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-128
     SA remaining key duration (kilobytes/sec): 5242880/2280
     Max sent sequence-number: 10
     UDP encapsulation used for NAT traversal: N
     SA encrypted packets (number/bytes): 9/756

   [Inbound ESP SAs]
     SPI: 3291681250 (0xc43311e2)
     Proposal: ESP-ENCRYPT-AES-256-GCM-128 SHA2-256-1286
     SA remaining key duration (kilobytes/sec): 5242880/2280
     Max received sequence-number: 10
     UDP encapsulation used for NAT traversal: N
     SA decrypted packets (number/bytes): 9/756
     Anti-replay : Enable
     Anti-replay window size: 1024
```

2. Users at the branch can communicate with users at the HQ.
3. Run the **display ip routing-table** command to check the IP routing table.

   The command output displays the route with the destination address being 10.1.2.0/24 and the outbound interface being Tunnel 1.

Configuration Scripts

- DeviceA

```
#
sysname DeviceA
#
acl 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
```

 Copyright © Huawei Technologies Co., Ltd.

```
 prf hmac-sha2-256
#
ike peer b
 ike-proposal 10
 remote-address 172.16.2.2
 pre-shared-key %+%#eY>XCM5+)9nKwEIT`J+YA0lL31/MGS=gZBF.""`6%+%#
#
ipsec policy map1 10 isakmp
 security acl 3000
 proposal tran1
 ike-peer b
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel 1
 ip address 172.16.2.1 255.255.255.0
 tunnel-protocol gre
 source GE0/0/1
 destination 3.3.3.3
 gre key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!]wvQ.geMP<vc*,~@orq0[grV6uxIe71~yD+!!!!!2jp5!!!!!!8!!!!
Kq_mI9bO{4]gFG&,;AMW7s'>1<]{J#!!!!!!!!!!%+%#
 keepalive
 ipsec policy map1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
ip route-static 10.1.2.0 24 Tunnel1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  source-zone dmz
  destination-zone trust
  destination-zone dmz
  action permit
 rule name policy2
  source-zone local
  source-zone dmz
  destination-zone dmz
  destination-zone local
  action permit
 rule name policy3
  source-zone local
  source-zone untrust
  destination-zone untrust
  destination-zone local
  service gre
  action permit
#
return
```

- DeviceB

```
#
sysname DeviceB
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
acl 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer a
 ike-proposal 10
 remote-address 172.16.2.1
 pre-shared-key %+%#eY>XCM5+)9nKwEIT`J+YA0lL31/MGS=gZBF.""`6%+%#
#
ipsec policy map1 10 isakmp
 security acl 3000
 proposal tran1
 ike-peer a
#
interface GE0/0/1
 ip address 3.3.3.3 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel 1
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 source GE0/0/1
 destination 1.1.1.1
 gre key cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!]wvQ.geMP<vc*,~@orq0[grV6uxIe71~yD+!!!!!2jp5!!!!!!8!!!!
Kq_mI9bO{4]gFG&,;AMW7s'>1<]{J#!!!!!!!!!!%+%#
 keepalive
 ipsec policy map1
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.254
ip route-static 10.1.1.0 24 Tunnel1
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Tunnel 1
#
security-policy
 rule name policy1
  source-zone trust
  source-zone dmz
  destination-zone trust
  destination-zone dmz
  action permit
 rule name policy2
  source-zone local
  source-zone dmz
  destination-zone dmz
  destination-zone local
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
 rule name policy3
  source-zone local
  source-zone untrust
  destination-zone untrust
  destination-zone local
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

12 Security Policy

12.1 Web: Example for Configuring Security Policies Based on IP Addresses and Ports

12.2 CLI: Example for Configuring Security Policies Based on IP Addresses and Ports

12.3 Web: Example for Configuring Application-based Security Policies

12.4 CLI: Example for Configuring Application-based Security Policies

12.1 Web: Example for Configuring Security Policies Based on IP Addresses and Ports

Networking Requirements

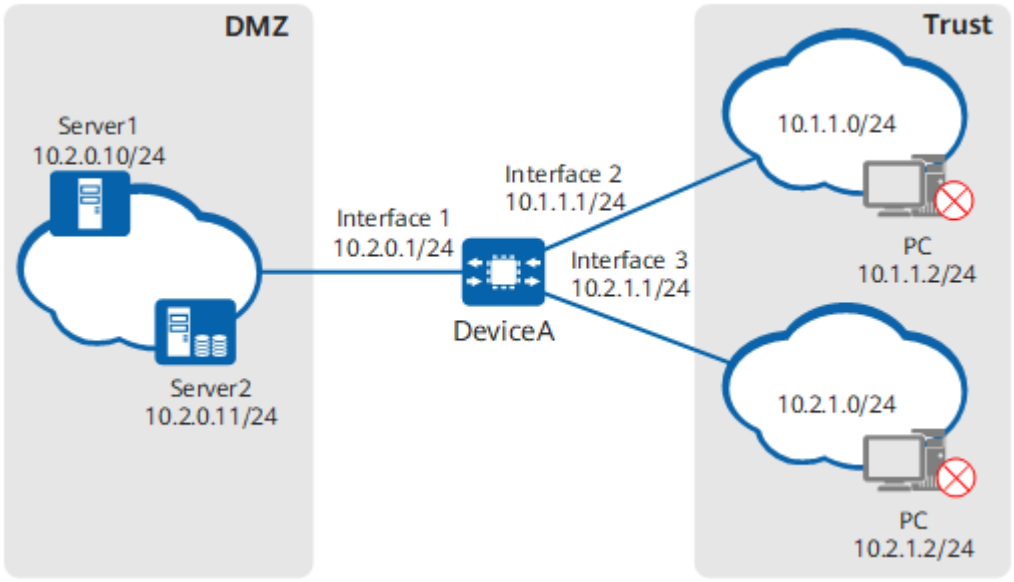
As shown in **Figure 12-1**, an enterprise has two service servers deployed. Server1 provides services through TCP port 8888, and Server2 provides services through UDP port 6666. DeviceA is required to implement access control. The two PCs at 10.1.1.2 and 10.2.1.2 are prohibited from accessing these two servers during working hours (08:00-17:00). Other PCs can access the two servers at any time.

Figure 12-1 Network diagram for configuring security policies based on IP addresses and ports

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Set basic interface parameters for interfaces.

1. Choose **Network** > **Interface**.
2. Click for the GE0/0/1 and set parameters as follows. Keep default values for other parameters.

Zone	dmz
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	10.2.0.1/255.255.255.0

3. Repeat the previous operation and set interface parameters for the other two interfaces.

   Set parameters of GE0/0/2 as follows. Keep default values for other parameters.

Zone	trust
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	10.1.1.1/255.255.255.0

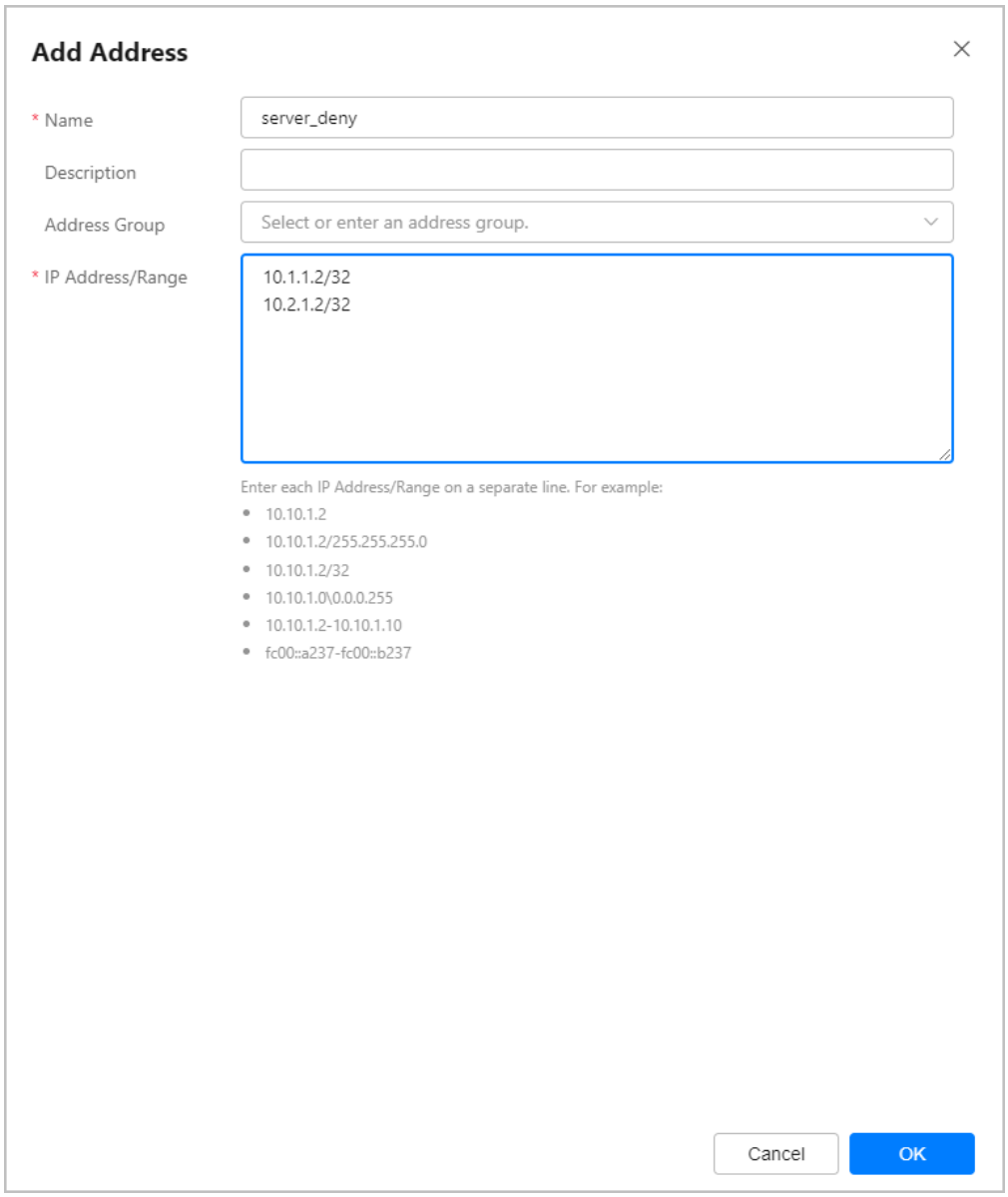
 Copyright © Huawei Technologies Co., Ltd.

Set parameters of GE0/0/3 as follows. Keep default values for other parameters.

Zone	trust
Mode	Routing
IPv4	
Connection Type	Static IP
IP Address	10.2.1.1/255.255.255.0

Step 2 Configure an address object named **server_deny** and add the IP addresses that are not allowed to access the servers to the address object.

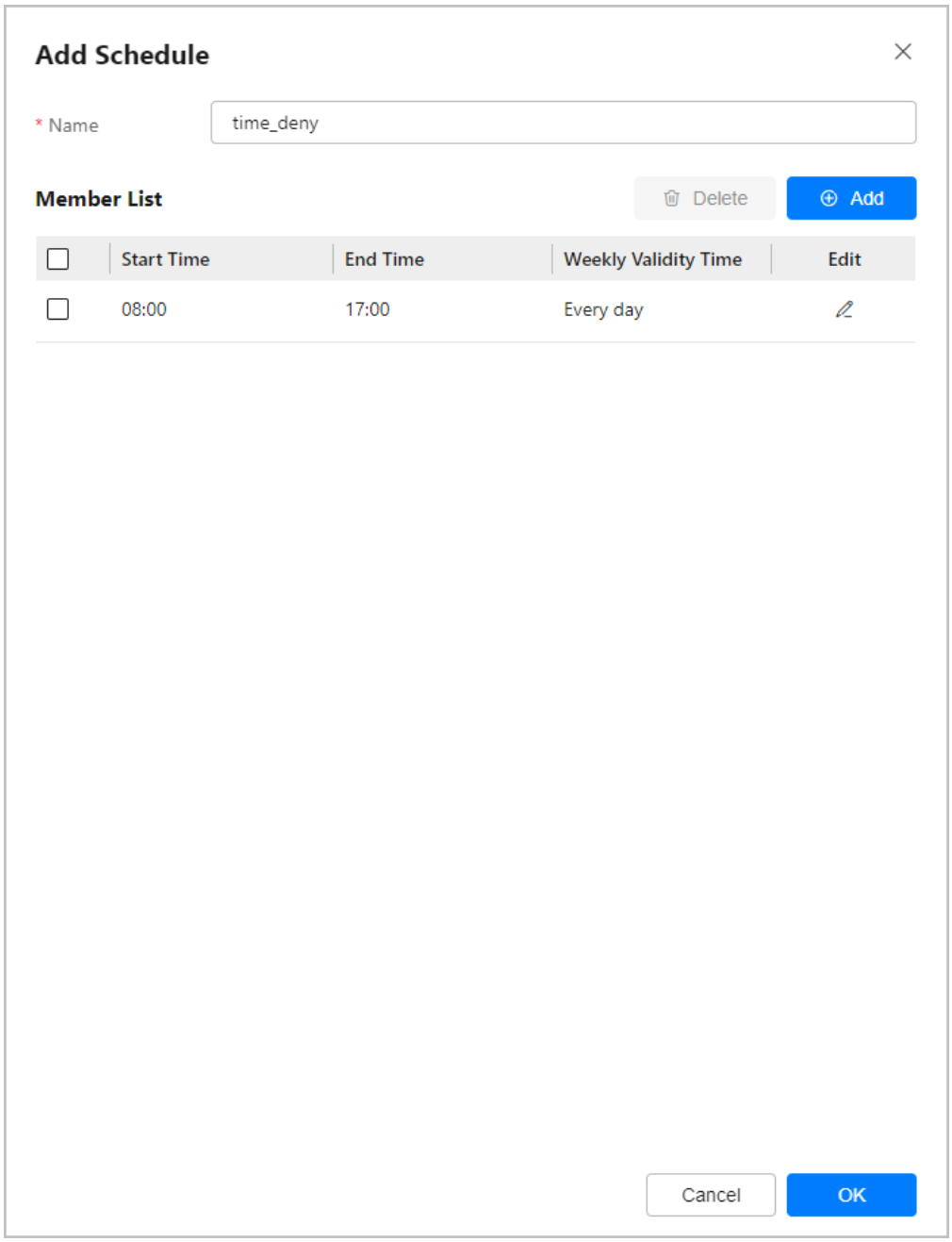
1. Choose **Object** > **Address** > **Address**.
2. Click **Add** to configure an address set and click **OK**.



 Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure a time range named **time_deny** and specify the time during which the specific PCs are not allowed to access the server.

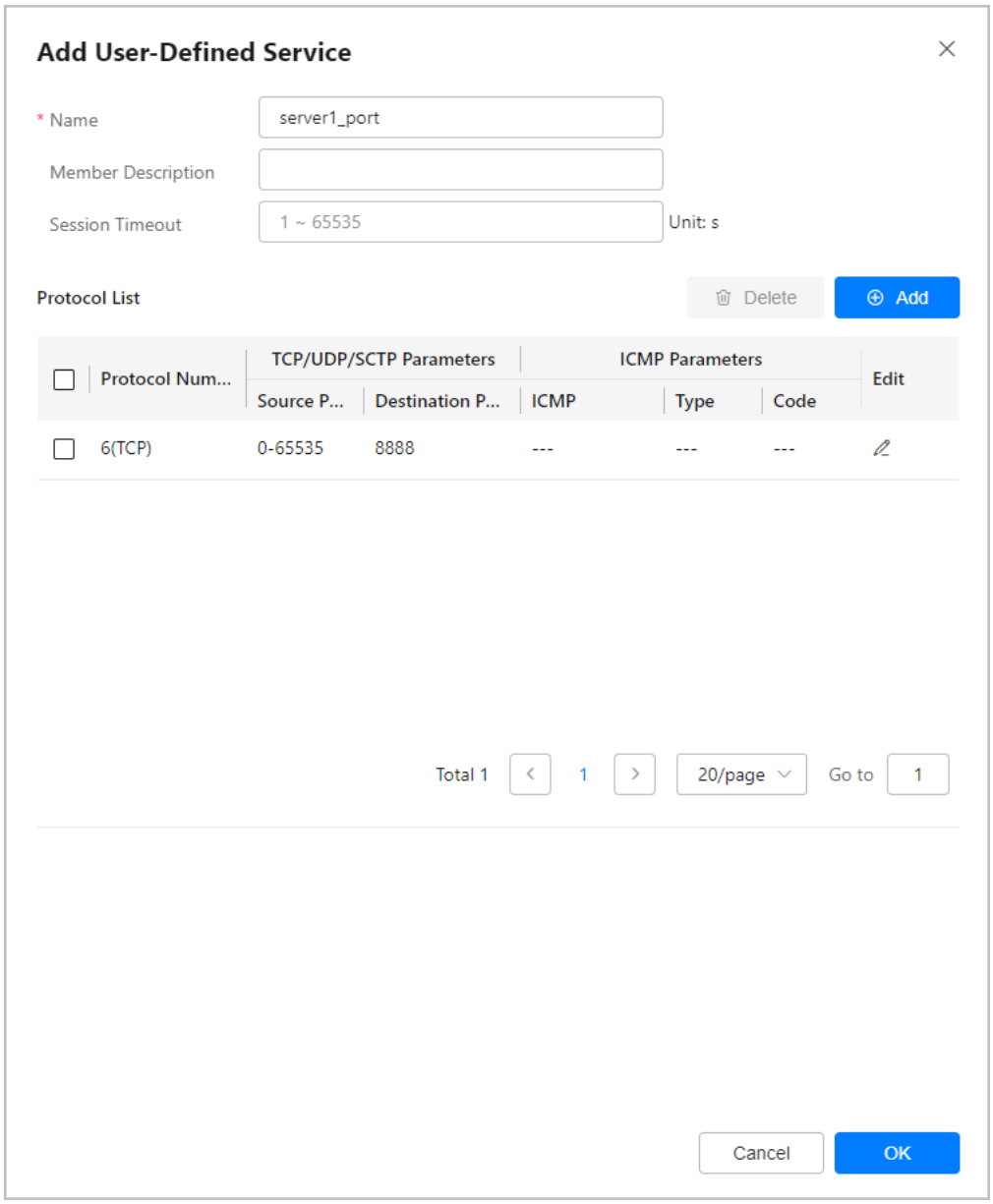
1. Choose **Object** > **Schedule**.
2. Click **Add**, enter the name of a time range.
3. Click **Add** in **Schedule List** to configure a time range.



Step 4 Configure user-defined service sets **server1_port** and **server2_port** for Server1 and Server2, respectively and add the ephemeral ports of the servers to the service sets

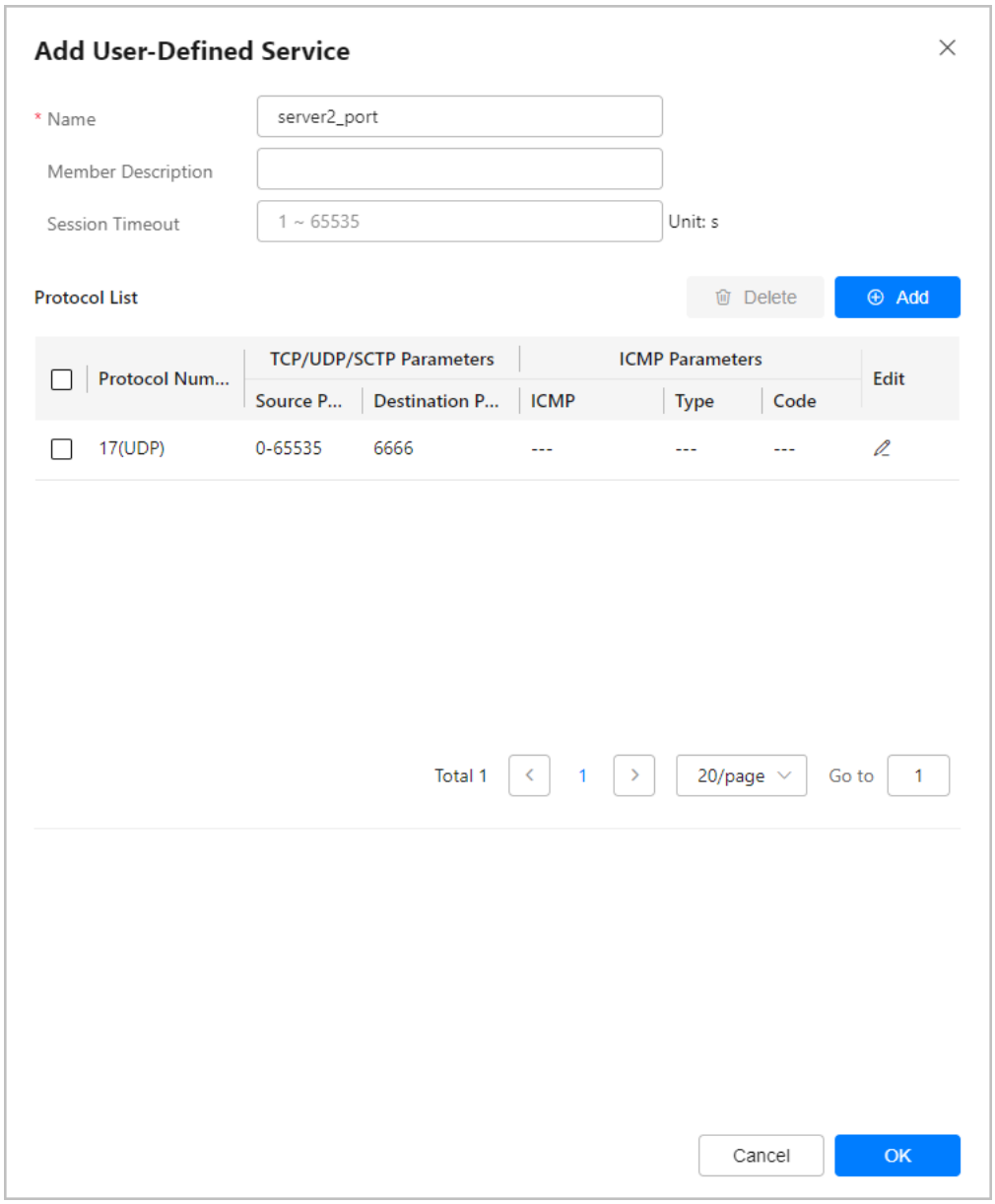
1. Choose **Object** > **Service** > **Service**.
2. Click **Add**, enter a service name, and add the service.

 Copyright © Huawei Technologies Co., Ltd.



3. Repeat previous steps to configure user-defined service set server2_port for Server2.

 Copyright © Huawei Technologies Co., Ltd.

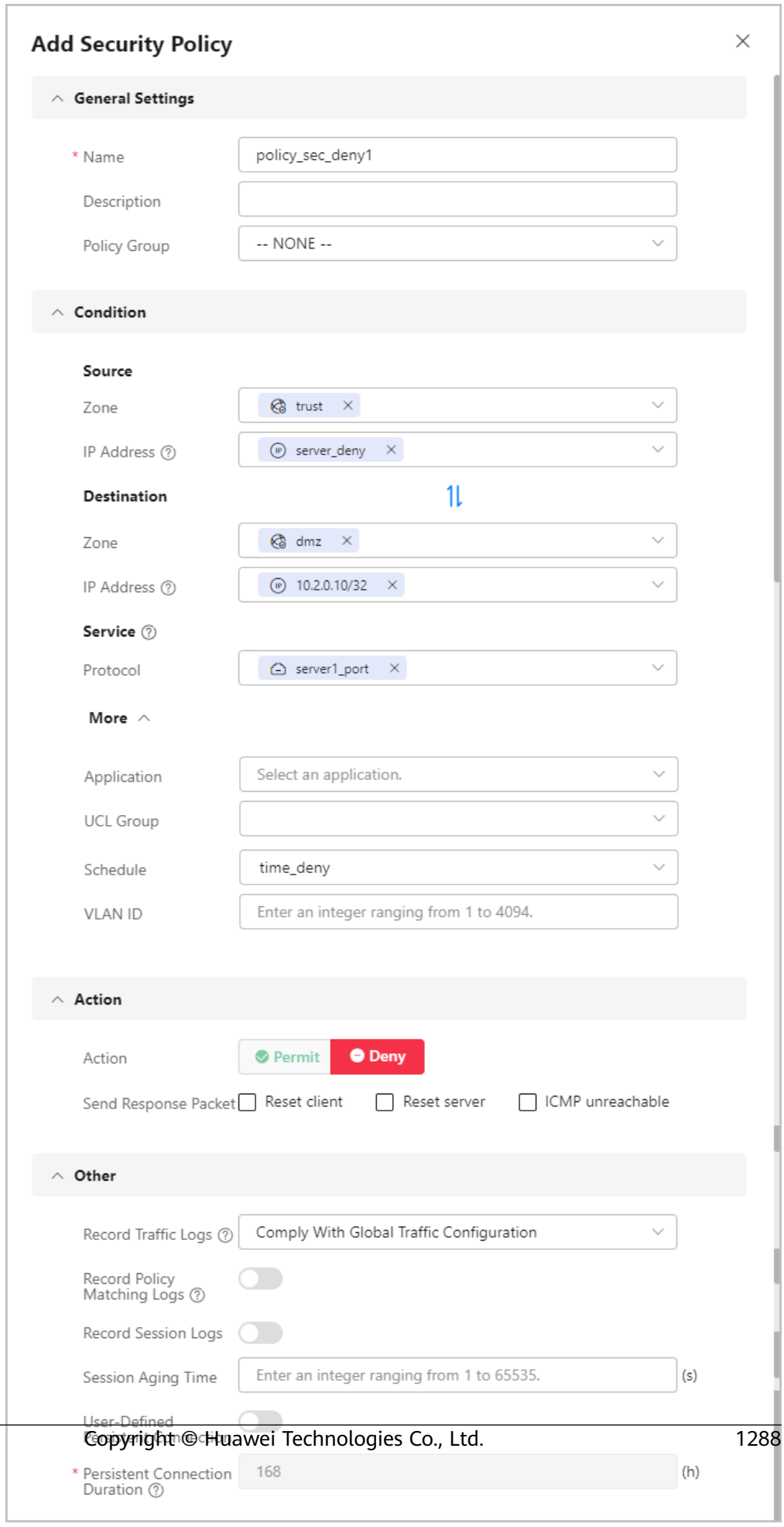


Step 5 Configure security policies and reference the configured address sets, time ranges, and service sets.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** to configure four security policies for the trust-dmz interzone.

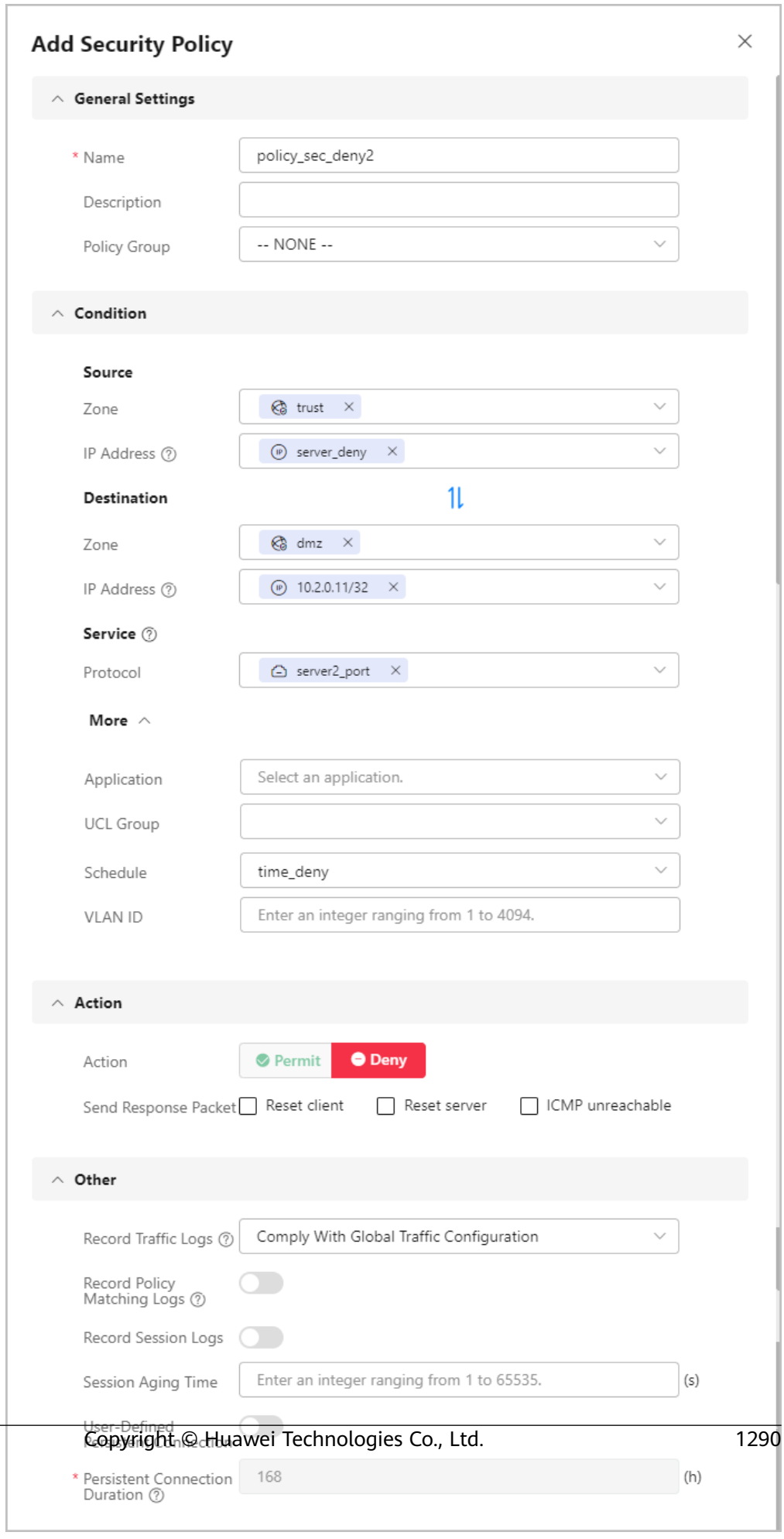
   Security policy that restricts the access of PCs to Server1:

 Copyright © Huawei Technologies Co., Ltd.



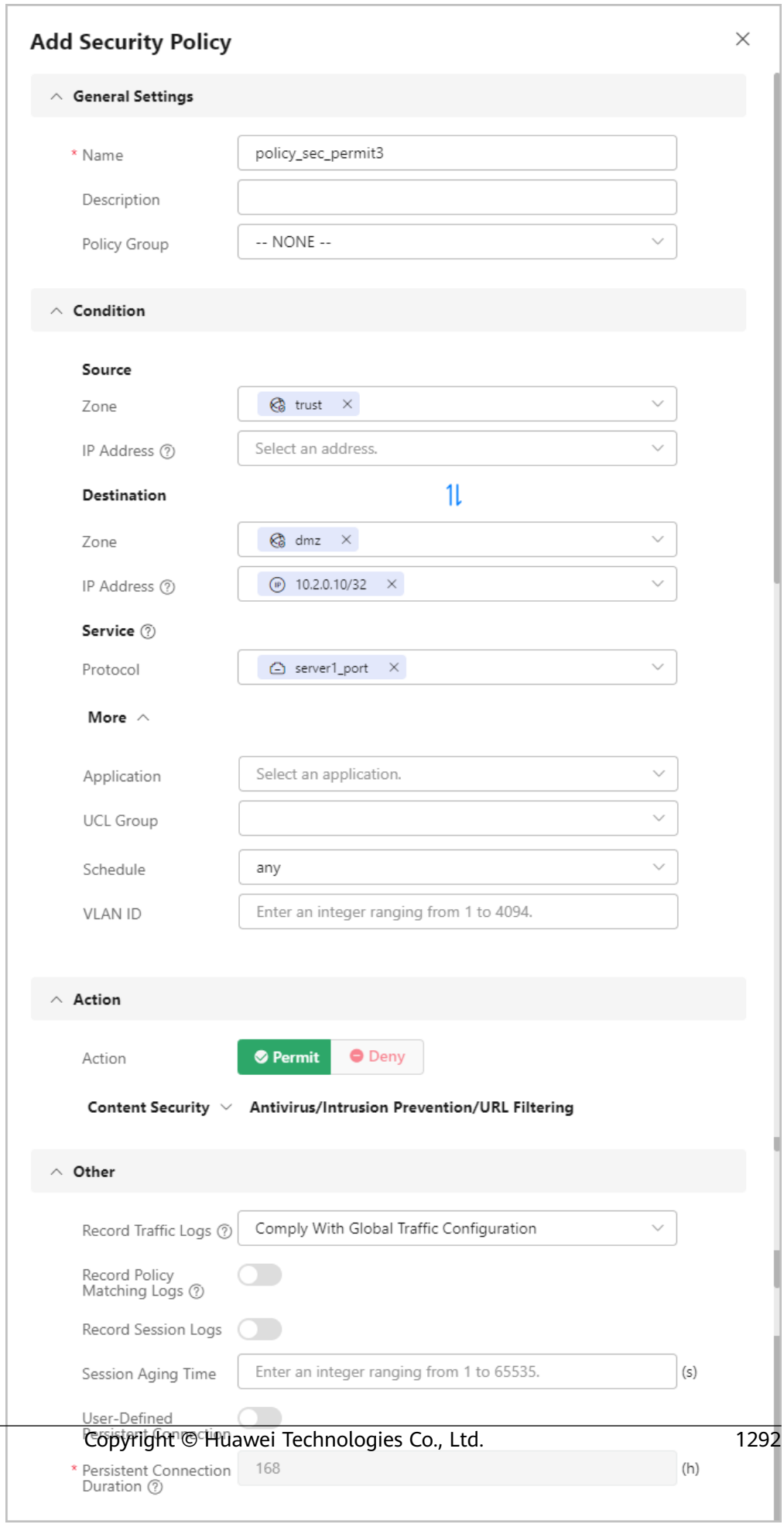
 Copyright © Huawei Technologies Co., Ltd.

Security policy that restricts the access of PCs to Server2:



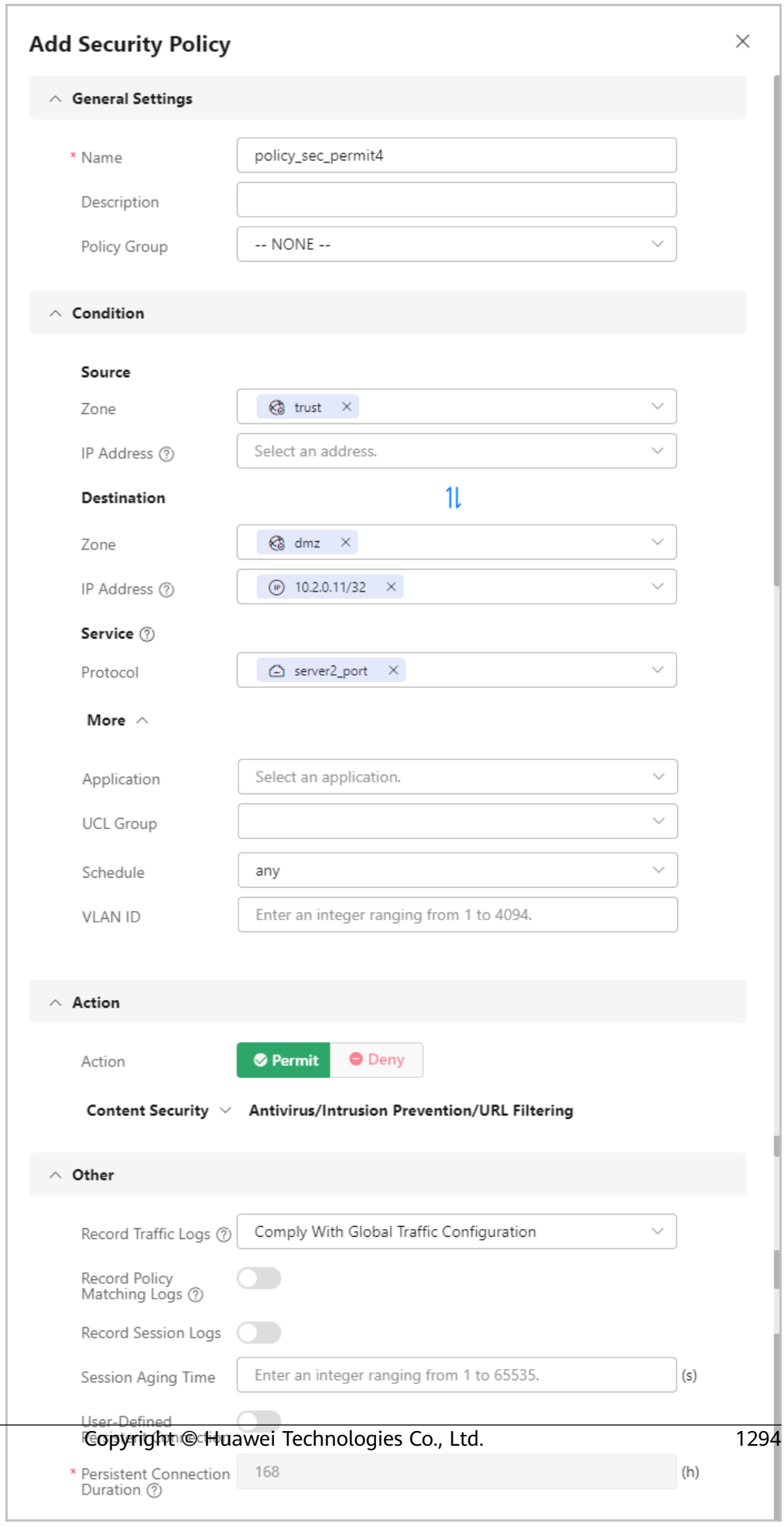
 Copyright © Huawei Technologies Co., Ltd.

Security policy that allows the access of PCs to Server1:



 Copyright © Huawei Technologies Co., Ltd.

Security policy that allows the access of PCs to Server2:



 Copyright © Huawei Technologies Co., Ltd.

----End

Verifying the Security Policy Configuration

During 08:00-17:00, PCs at 10.1.1.2 and 10.2.1.2 cannot access the two servers. These two PCs can access the servers in other time ranges. Other PCs can access these two servers at any time.

Configuration Scripts

```
#
ip address-set server_deny type object
 address 0 10.1.1.2 mask 32
 address 1 10.2.1.2 mask 32
#
ip service-set server1_port type object
 service 0 protocol tcp source-port 0 to 65535 destination-port 8888
#
ip service-set server2_port type object
 service 0 protocol udp source-port 0 to 65535 destination-port 6666
#
time-range time_deny 08:00 to 17:00 daily
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.2.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
security-policy
 rule name policy_sec_deny1
  source-zone trust
  destination-zone dmz
  source-address address-set server_deny
  destination-address 10.2.0.10 mask 255.255.255.255
  service server1_port
  time-range time_deny
  action deny
 rule name policy_sec_deny2
  source-zone trust
  destination-zone dmz
  source-address address-set server_deny
  destination-address 10.2.0.11 mask 255.255.255.255
  service server2_port
  time-range time_deny
  action deny
 rule name policy_sec_permit3
  source-zone trust
  destination-zone dmz
  destination-address 10.2.0.10 mask 255.255.255.255
  service server1_port
  action permit
 rule name policy_sec_permit4
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone dmz
 destination-address 10.2.0.11 mask 255.255.255.255
 service server2_port
 action permit
#
return
```

12.2 CLI: Example for Configuring Security Policies Based on IP Addresses and Ports

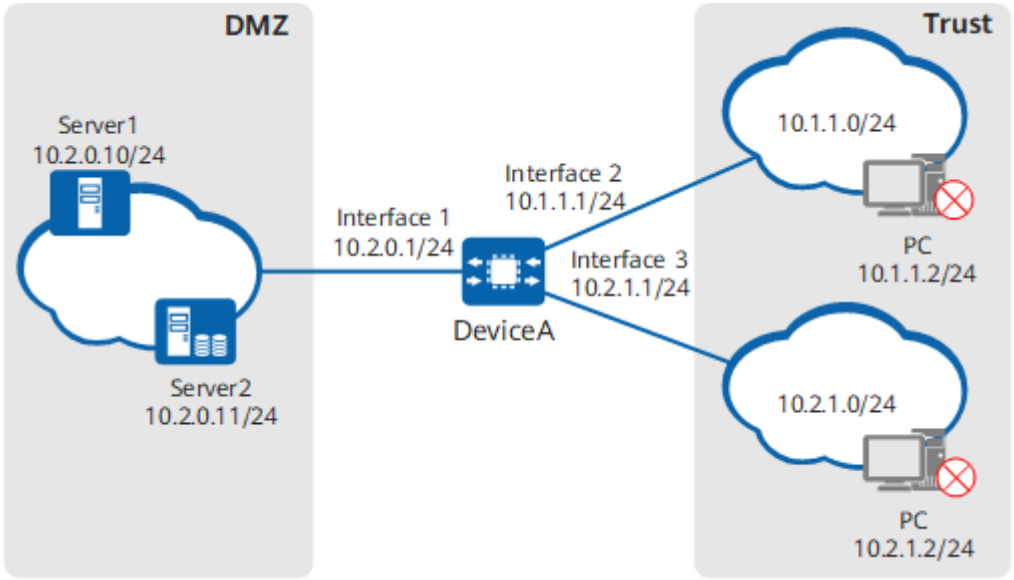
Networking Requirements

As shown in **Figure 12-2**, an enterprise has two service servers deployed. Server1 provides services through TCP port 8888, and Server2 provides services through UDP port 6666. DeviceA is required to implement access control. The two PCs at 10.1.1.2 and 10.2.1.2 are prohibited from accessing these two servers during working hours (08:00-17:00). Other PCs can access the two servers at any time.

Figure 12-2 Network diagram for configuring security policies based on IP addresses and ports

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Procedure

Step 1 Configure an IP address for each interface and assign interfaces to security zones.

Configure an IP address for GE0/0/1 and assign the interface to the DMZ.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.2.0.1 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/1
[DeviceA-zone-dmz] quit
```

Configure an IP address for GE0/0/2 and assign the interface to the Trust zone.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Configure an IP address for GE0/0/3 and assign the interface to the Trust zone.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.2.1.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

Step 2 Configure an address object named **server_deny** and add the IP addresses that are not allowed to access the servers to the address object.

```
[DeviceA] ip address-set server_deny type object
[DeviceA-object-address-set-server_deny] address 10.1.1.2 mask 32
[DeviceA-object-address-set-server_deny] address 10.2.1.2 mask 32
[DeviceA-object-address-set-server_deny] quit
```

Step 3 Configure a time range named **time_deny** and specify the time during which the specific PCs are not allowed to access the server.

```
[DeviceA] time-range time_deny 08:00 to 17:00 daily
```

Step 4 Configure user-defined services **server1_port** and **server2_port** for Server1 and Server2 respectively and add the non-well-known ports of the servers to the services.

```
[DeviceA] ip service-set server1_port type object
[DeviceA-object-service-set-server1_port] service protocol TCP source-port 0 to 65535 destination-port 8888
[DeviceA-object-service-set-server1_port] quit
[DeviceA] ip service-set server2_port type object
[DeviceA-object-service-set-server2_port] service protocol UDP source-port 0 to 65535 destination-port 6666
[DeviceA-object-service-set-server2_port] quit
```

If servers use well-known ports (such as HTTP port 80) to provide services, directly use predefined service sets (such as HTTP and FTP) for security policy configuration.

Step 5 Configure a security policy rule and reference the configured address object, time range, and services.

Configure a security policy that restricts the access of specific PCs to Server1.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_deny1
[DeviceA-policy-security-rule-policy_sec_deny1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_deny1] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_deny1] source-address address-set server_deny


[DeviceA-policy-security-rule-policy_sec_deny1] destination-address 10.2.0.10 32
[DeviceA-policy-security-rule-policy_sec_deny1] service server1_port
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy_sec_deny1] time-range time_deny
[DeviceA-policy-security-rule-policy_sec_deny1] action deny
[DeviceA-policy-security-rule-policy_sec_deny1] quit
```

Configure a security policy that restricts the access of specific PCs to Server2.

```
[DeviceA-policy-security] rule name policy_sec_deny2
[DeviceA-policy-security-rule-policy_sec_deny2] source-zone trust
[DeviceA-policy-security-rule-policy_sec_deny2] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_deny2] source-address address-set server_deny


[DeviceA-policy-security-rule-policy_sec_deny2] destination-address 10.2.0.11 32
[DeviceA-policy-security-rule-policy_sec_deny2] service server2_port
[DeviceA-policy-security-rule-policy_sec_deny2] time-range time_deny
[DeviceA-policy-security-rule-policy_sec_deny2] action deny
[DeviceA-policy-security-rule-policy_sec_deny2] quit
```

Configure a security policy that allows the access of other PCs to Server1.

```
[DeviceA-policy-security] rule name policy_sec_permit3
[DeviceA-policy-security-rule-policy_sec_permit3] source-zone trust
[DeviceA-policy-security-rule-policy_sec_permit3] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_permit3] service server1_port
[DeviceA-policy-security-rule-policy_sec_permit3] action permit
[DeviceA-policy-security-rule-policy_sec_permit3] quit
```

Configure a security policy that allows the access of other PCs to Server2.

```
[DeviceA-policy-security] rule name policy_sec_permit4
[DeviceA-policy-security-rule-policy_sec_permit4] source-zone trust
[DeviceA-policy-security-rule-policy_sec_permit4] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_permit4] service server2_port
[DeviceA-policy-security-rule-policy_sec_permit4] action permit
[DeviceA-policy-security-rule-policy_sec_permit4] quit
[DeviceA-policy-security] quit
```

Security policies are matched based on the configuration sequence. Configure specific policies before configuring general ones.

----End

Verifying the Security Policy Configuration

During 08:00-17:00, PCs at 10.1.1.2 and 10.2.1.2 cannot access the two servers. These two PCs can access the servers in other time ranges. Other PCs can access these two servers at any time.

Configuration Scripts

```
#
sysname DeviceA
#
ip address-set server_deny type object
 address 0 10.1.1.2 mask 32
 address 1 10.2.1.2 mask 32
#
ip service-set server1_port type object
 service 0 protocol tcp source-port 0 to 65535 destination-port 8888
#
ip service-set server2_port type object
 service 0 protocol udp source-port 0 to 65535 destination-port 6666
#
time-range time_deny 08:00 to 17:00 daily
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.2.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
security-policy
 rule name policy_sec_deny1
  source-zone trust
  destination-zone dmz
  source-address address-set server_deny


  destination-address 10.2.0.10 mask 255.255.255.255
  service server1_port
  time-range time_deny
  action deny
 rule name policy_sec_deny2
  source-zone trust
  destination-zone dmz
  source-address address-set server_deny


  destination-address 10.2.0.11 mask 255.255.255.255
  service server2_port
  time-range time_deny
  action deny
 rule name policy_sec_permit3
  source-zone trust
  destination-zone dmz
  service server1_port
  action permit
 rule name policy_sec_permit4
  source-zone trust
  destination-zone dmz
  service server2_port
  action permit
#
return
```

12.3 Web: Example for Configuring Application-based Security Policies

Networking Requirements

As shown in **Figure 12-3**, DeviceA is deployed at the border of an enterprise network as a security gateway. Based on their levels and responsibilities, employees of the enterprise are divided into three types: senior executives, marketing employees, and R&D employees. The three types of users have different permissions to access the Internet, as described in **Table 12-1**.

 Copyright © Huawei Technologies Co., Ltd.

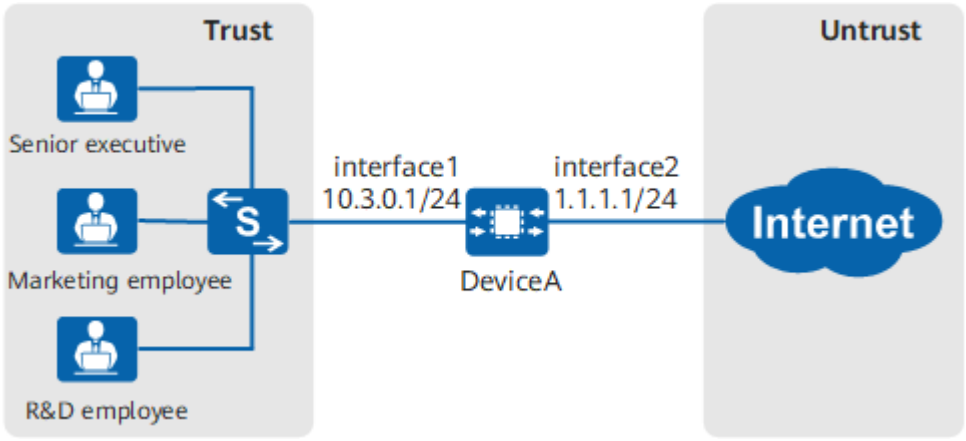
Table 12-1 Relationship between users and permissions

User	IP Address	Permission
Senior executives	10.3.0.2 to 10.3.0.20	Full Internet access permission.
Marketing employees	10.3.0.21 to 10.3.0.120	Can access the Internet but cannot play games or watch online videos.
R&D employees	10.3.0.121 to 10.3.0.220	Can only access the TortoiseSVN application.

Figure 12-3 Network diagram for configuring application-specific security policies

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Set the IP address and security zone of the interface.

1. Choose **Network** > **Interface**.
2. Click of GE0/0/1 and set the parameters as follows:

IP Address	10.3.0.1
Mask	255.255.255.0
Zone	trust

3. Click **OK**.
4. Repeat the previous steps to set the parameters of interface GE0/0/2.

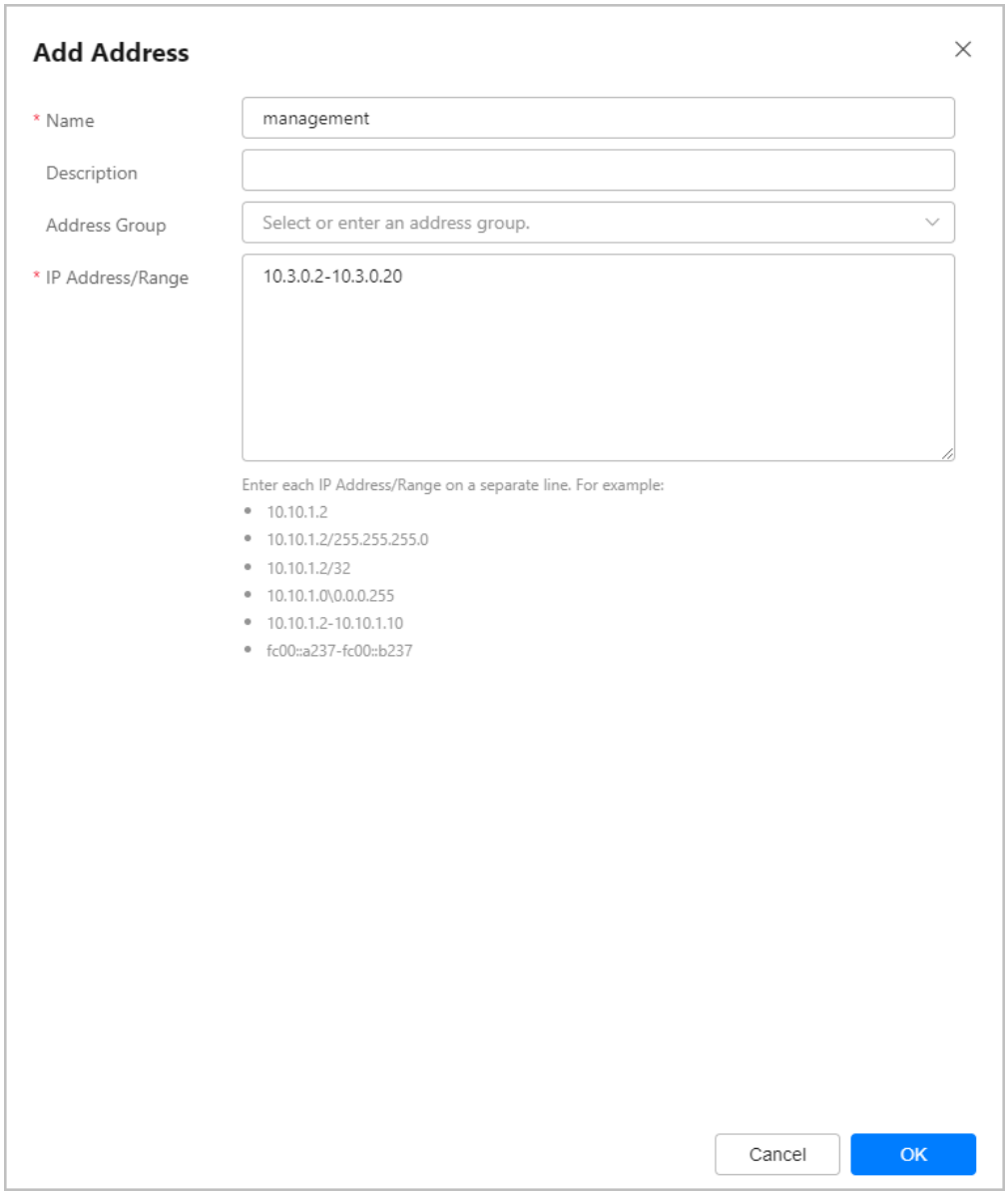
IP Address	1.1.1.1
Mask	255.255.255.0

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust

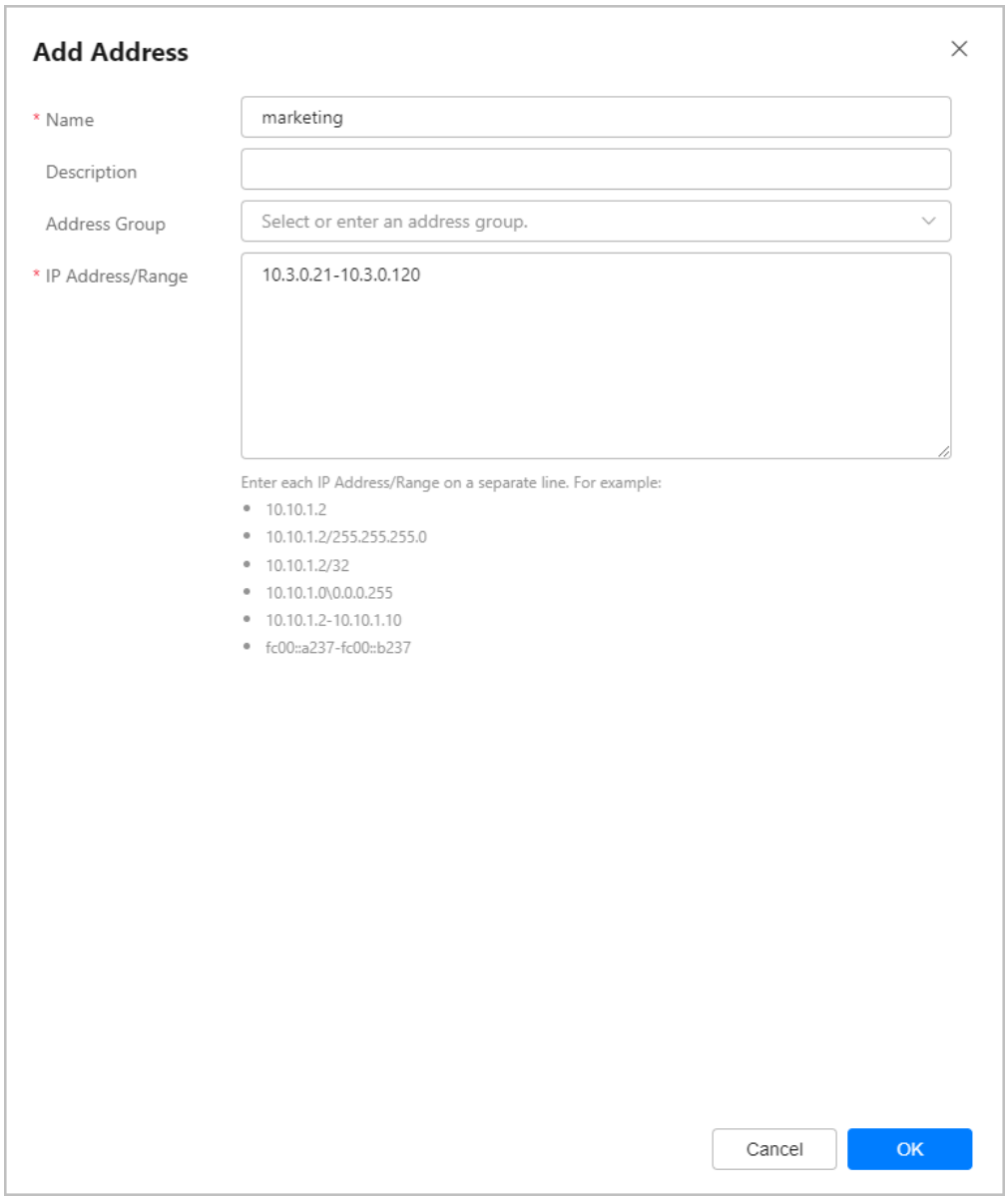
Step 2 Configure address objects for the three types of users.

1. Choose **Object** > **Address** > **Address**.
2. Click **Add** to configure an address object for senior executives.

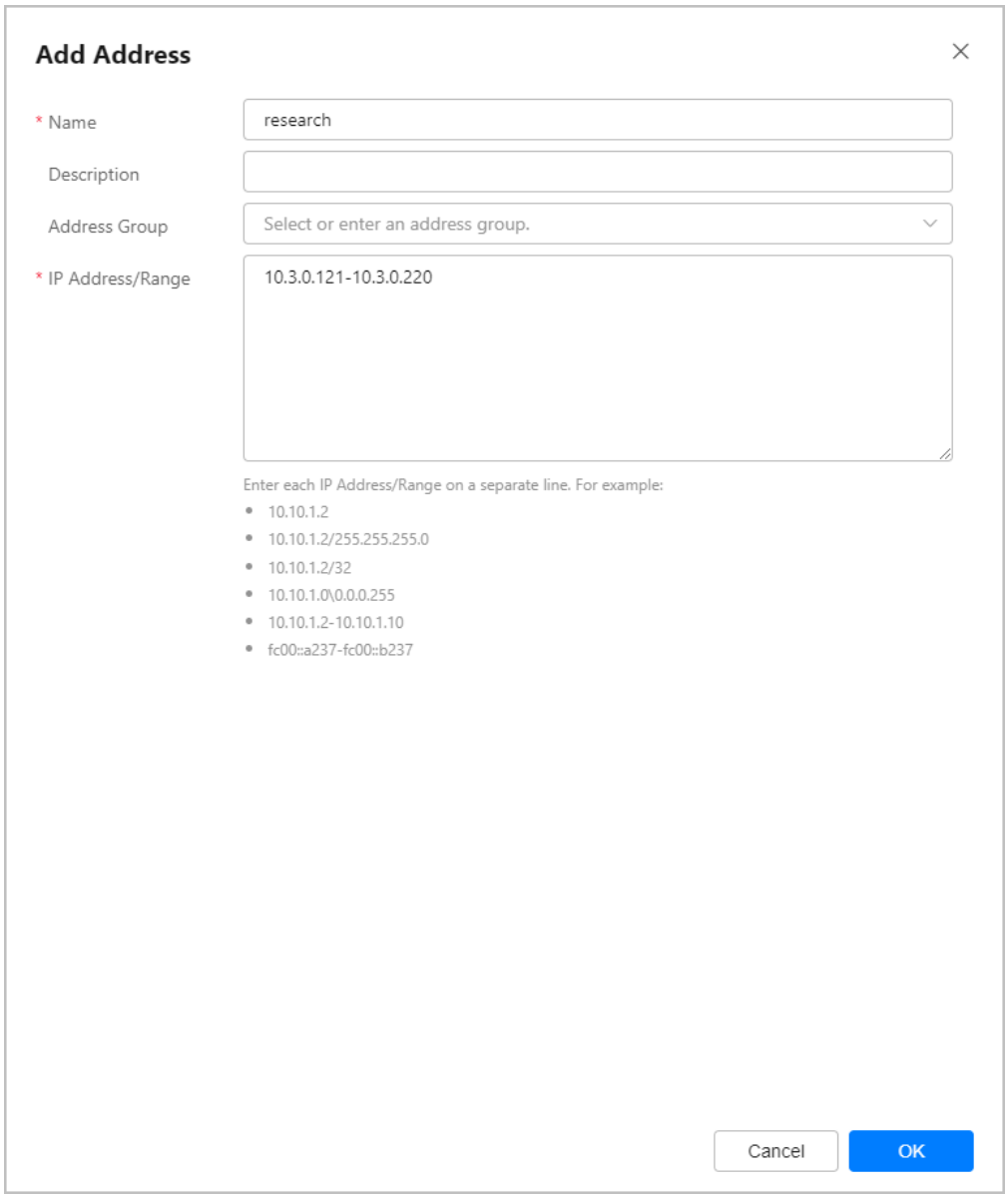


3. Click **OK**.
4. Repeat previous steps to configure address objects for marketing employees and R&D employees.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.



Step 3 Configure security Policies for the three types of users.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, set the parameters of the security policy for senior executives to access the Internet freely.

Name	policy_sec_management
Source Zone	trust
Destination Zone	untrust
Source Address	management
Action	Permit

3. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

4. Repeat the previous steps to configure security policy for marketing employees.

   Configure a security policy to block game and network video traffic.

Name	policy_sec_marketing_1
Source Zone	trust
Destination Zone	untrust
Source Address	marketing
Application	Game, Media_Sharing **NOTE** As there are various types of applications, the loading runs slowly. You are advised to enter the needed application (such as Game) in the **Application** drop-down list box. Wait for a moment and the options in the drop-down list box can be selected.
Action	Deny

   Configure a security policy to allow marketing employees to access the Internet.

Name	policy_sec_marketing_2
Source Zone	trust
Destination Zone	untrust
Source Address	marketing
Application	any
Action	Permit

5. Configure a security policy for R&D employees to access only the TortoiseSVN application.

Name	policy_sec_research
Source Zone	trust
Destination Zone	untrust
Source Address	research
Application	TortoiseSVN
Action	Permit

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Security Policy Configuration

- Use a PC on the network segment of senior executives to verify that the PC can access the Internet without any restriction.
- Use a PC on the network segment of marketing employees to verify that the PC can access other network applications but cannot access online games or watch online videos.
- Use a PC on the network segment of R&D employees to verify that the PC can access only the TortoiseSVN application on the Internet.

Configuration Scripts

```
#
ip address-set management type object
 address 0 range 10.3.0.2 10.3.0.20
#
ip address-set marketing type object
 address 0 range 10.3.0.21 10.3.0.120
#
ip address-set research type object
 address 0 range 10.3.0.121 10.3.0.220
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_management
  source-zone trust
  destination-zone untrust
  source-address address-set management
  action permit
 rule name policy_sec_marketing_1
  source-zone trust
  destination-zone untrust
  source-address address-set marketing
  application category Entertainment sub-category Media_Sharing
  application category Entertainment sub-category Game
  action deny
 rule name policy_sec_marketing_2
  source-zone trust
  destination-zone untrust
  source-address address-set marketing
  action permit
 rule name policy_sec_research
  source-zone trust
  destination-zone untrust
  source-address address-set research
  application app TortoiseSVN
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

12.4 CLI: Example for Configuring Application-based Security Policies

Networking Requirements

As shown in **Figure 12-4**, DeviceA is deployed at the border of an enterprise network as a security gateway. Based on their levels and responsibilities, employees of the enterprise are divided into three types: senior executives, marketing employees, and R&D employees. The three types of users have different permissions to access the Internet, as described in **Table 12-2**.

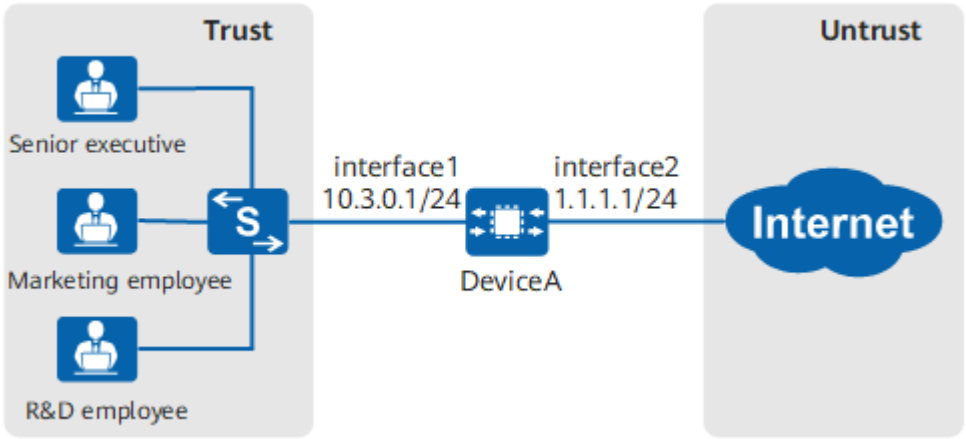
Table 12-2 Relationship between users and permissions

User	IP Address	Permission
Senior executives	10.3.0.2 to 10.3.0.20	Full Internet access permission.
Marketing employees	10.3.0.21 to 10.3.0.120	Can access the Internet but cannot play games or watch online videos.
R&D employees	10.3.0.121 to 10.3.0.220	Can only access the TortoiseSVN application.

Figure 12-4 Network diagram for configuring application-specific security policies

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Configure an IP address for each interface and assign interfaces to security zones.

Configure an IP address for GE0/0/1 and assign the interface to the Trust zone.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.3.0.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Configure an IP address for GE0/0/2 and assign the interface to the Untrust zone.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure address objects for the three types of users.

Configure an address object for senior executives.

```
[DeviceA] ip address-set management type object
[DeviceA-object-address-set-management] address range 10.3.0.2 10.3.0.20
[DeviceA-object-address-set-management] quit
```

Configure an address object for marketing employees.

```
[DeviceA] ip address-set marketing type object
[DeviceA-object-address-set-marketing] address range 10.3.0.21 10.3.0.120
[DeviceA-object-address-set-marketing] quit
```

Configure an address object for R&D employees.

```
[DeviceA] ip address-set research type object
[DeviceA-object-address-set-research] address range 10.3.0.121 10.3.0.220
[DeviceA-object-address-set-research] quit
```

Step 3 Configure a security policy for senior executives to access the Internet freely.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_management
[DeviceA-policy-security-rule-policy_sec_management] source-zone trust
[DeviceA-policy-security-rule-policy_sec_management] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_management] source-address address-set management
[DeviceA-policy-security-rule-policy_sec_management] action permit
[DeviceA-policy-security-rule-policy_sec_management] quit
```

Step 4 Configure a security policy for marketing employees.

Configure a security policy to block game and network video traffic.

```
[DeviceA-policy-security] rule name policy_sec_marketing_1
[DeviceA-policy-security-rule-policy_sec_marketing_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing_1] source-address address-set marketing
[DeviceA-policy-security-rule-policy_sec_marketing_1] application category Entertainment sub-category
Media_Sharing
[DeviceA-policy-security-rule-policy_sec_marketing_1] application category Entertainment sub-category
Game
[DeviceA-policy-security-rule-policy_sec_marketing_1] action deny
[DeviceA-policy-security-rule-policy_sec_marketing_1] quit
```

Configure a security policy to allow marketing employees to access the Internet.

```
[DeviceA-policy-security] rule name policy_sec_marketing_2
[DeviceA-policy-security-rule-policy_sec_marketing_2] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing_2] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing_2] source-address address-set marketing
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy_sec_marketing_2] action permit
[DeviceA-policy-security-rule-policy_sec_marketing_2] quit
```

The previous policy has blocked games and online videos. In this policy, permit all traffic.

Step 5 Configure a security policy for R&D employees to access only the TortoiseSVN application.

```
[DeviceA-policy-security] rule name policy_sec_research
[DeviceA-policy-security-rule-policy_sec_research] source-zone trust
[DeviceA-policy-security-rule-policy_sec_research] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_research] source-address address-set research
[DeviceA-policy-security-rule-policy_sec_research] application app TortoiseSVN
[DeviceA-policy-security-rule-policy_sec_research] action permit
[DeviceA-policy-security-rule-policy_sec_research] quit
```

Other Internet access traffic of R&D employees matches the default security policy and is blocked.

----End

Verifying the Security Policy Configuration

- Use a PC on the network segment of senior executives to verify that the PC can access the Internet without any restriction.
- Use a PC on the network segment of marketing employees to verify that the PC can access other network applications but cannot access online games or watch online videos.
- Use a PC on the network segment of R&D employees to verify that the PC can access only the TortoiseSVN application on the Internet.

Configuration Scripts

```
#
sysname DeviceA
#
ip address-set management type object
 address 0 range 10.3.0.2 10.3.0.20
#
ip address-set marketing type object
 address 0 range 10.3.0.21 10.3.0.120
#
ip address-set research type object
 address 0 range 10.3.0.121 10.3.0.220
#
interface GE 0/0/1
 ip address 10.3.0.1 255.255.255.0
#
interface GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
security-policy
 rule name policy_sec_management
  source-zone trust
  destination-zone untrust
  source-address address-set management
```

 Copyright © Huawei Technologies Co., Ltd.

```
 action permit
 rule name policy_sec_marketing_1
  source-zone trust
  destination-zone untrust
  source-address address-set marketing
  application category Entertainment sub-category Media_Sharing
  application category Entertainment sub-category Game
  action deny
 rule name policy_sec_marketing_2
  source-zone trust
  destination-zone untrust
  source-address address-set marketing
  action permit
 rule name policy_sec_research
  source-zone trust
  destination-zone untrust
  source-address address-set research
  application app TortoiseSVN
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

13 Content Security

13.1 Web: Example for Configuring Antivirus
13.2 Web: Example for Configuring the IPS Function to Protect Intranet Servers
13.3 Web: Example for Configuring the IPS Function to Protect Intranet Users
13.4 CLI: Example for Configuring Intrusion Prevention
13.5 CLI: Example for Configuring Antivirus
13.6 Web: Example for Using URL Categories to Control Website Access
13.7 CLI: Example for Using URL Categories to Control Website Access
13.8 Web: Example for Using the Blacklist and Whitelist to Control Website Access
13.9 CLI: Example for Using the Blacklist and Whitelist to Control Website Access
13.10 CLI: Example for Using URL Categories, Blacklist, and Whitelist to Control Website Access
13.11 Web: Example for Configuring Security Policies for Bypass Detection
13.12 CLI: Example for Configuring Security Policies for Bypass Detection

13.1 Web: Example for Configuring Antivirus

Networking Requirements

In **Figure 13-1**, DeviceA is deployed at the border of an enterprise network as a security gateway.

In the networking:

- Intranet users can download files and emails from the web server and POP3 server.
- The intranet FTP server can receive files uploaded by Internet users.

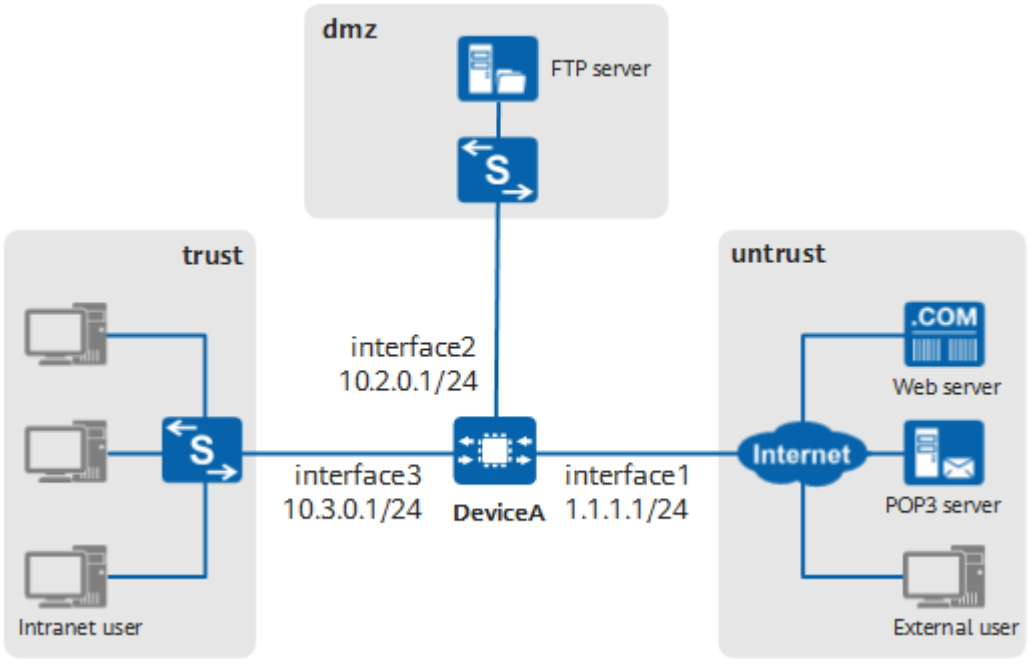
 Copyright © Huawei Technologies Co., Ltd.

To prevent virus files from entering the intranet during both file upload and download and ensure security of intranet users and servers, you need to configure the antivirus function on DeviceA.

Figure 13-1 Antivirus network diagram

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Configuration Roadmap

1. Configure interface IP addresses and assign the interfaces to security zones.
2. Configure the security policy **policy_sec_1** and reference the default antivirus profile **default** in the Trust-to-Untrust interzone to detect and defend against viruses in files and mails downloaded by intranet users from the Internet.
3. Configure the security policy **policy_sec_2** and reference the default antivirus profile **default** in the DMZ-to-Untrust interzone to detect and defend against viruses in files received by the intranet FTP server from the Internet.

Procedure

Step 1 Configure interface IP addresses and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

 Copyright © Huawei Technologies Co., Ltd.

3. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

4. Repeat the preceding steps to set the parameters for GE0/0/3.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

Step 2 Configure a Trust-to-Untrust interzone policy, and reference the default antivirus profile **default**.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**.
3. Reference the default antivirus profile **default** in the security policy and click **OK**.

Name	policy_sec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit
Content Security	
Antivirus	default

Step 3 Configure a DMZ-to-Untrust interzone policy, and reference the default antivirus profile **default**.

Configure the security policy by referring to **Step 2**. Set the parameters as follows.

Name	policy_sec_2
Source Zone	untrust
Destination Zone	dmz
Source Address	10.2.0.0/24
Action	Permit
Content Security	

 Copyright © Huawei Technologies Co., Ltd.

Antivirus	default

Step 4 Click **Save** in the upper right corner of the web page. In the dialog box that is displayed, click **OK**.

----End

Verifying the Configuration

- When an intranet user downloads a virus-infected file using HTTP, the download connection is blocked and the device generates a virus threat log.
- When an intranet user downloads a virus-infected mail using POP3, the device generates a virus threat log.
- When an Internet user uploads a virus-infected file using FTP, the upload connection is blocked and the device generates a virus threat log.
- You can choose **Monitor** > **Logs** > **Threat log** to view threat logs whose threat type is virus. Click to view log details.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone dmz
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  profile av default
  action permit
 rule name policy_sec_2
  source-zone untrust
  destination-zone dmz
  source-address 10.2.0.0 mask 255.255.255.0
  profile av default
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

13.2 Web: Example for Configuring the IPS Function to Protect Intranet Servers

Networking Requirements

In Figure 13-2, DeviceA is deployed at the border of an enterprise network as a security gateway.

In the networking:

- Intranet users can access the FTP server, web server, and mail server on the intranet.
- Internet users can access the web server on the intranet.

The enterprise needs to configure the IPS function on DeviceA to defend against worm, Trojan horse, and botnet attacks launched by Internet users or intranet users against the FTP server, mail server, and web server on the intranet.

Figure 13-2 Configuring the IPS function to protect intranet servers

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

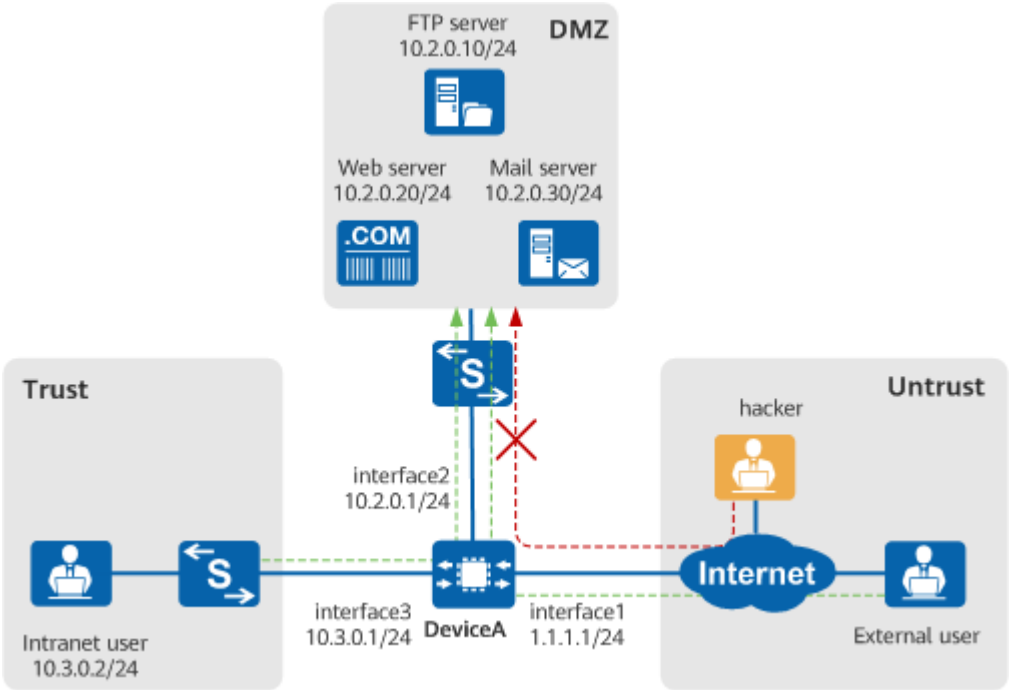


Table 13-1 Data plan for protecting intranet servers

Item	Data
Intranet server	Protect the FTP server, web server, and mail server on the intranet. • FTP server Operating system: Windows Protocol: FTP • Web server Operating system: Linux Protocol: HTTP and SSL • Email server Operating system: Linux Protocol: SMTP, IMAP4, and POP3

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
IPS profile	The most common threats on the enterprise network are worms, Trojan horses, and Botnets, and their severities in signatures are all High. These attacks target servers. Therefore, you can configure signature filters based on the service protocols and operating systems on the servers. ● Profile: Profile_ips_server1 – Signature filter filter_ftp: – Name: filter_ftp – Object: server – Severity: high – Operating system: Windows – Protocol: FTP – Action: alert – Signature filter filter_web: – Name: filter_web – Object: server – Severity: high – Operating system: Unix-like – Protocol: HTTP and SSL – Action: default signature action – Signature filter filter_mail: – Name: filter_mail – Object: server – Severity: high – Operating system: Unix-like – Protocol: SMTP, IMAP4, and POP3 – Action: default signature action ● Profile: Profile_ips_server2 – Signature filter filter_web: – Name: filter_web – Object: server – Severity: high – Operating system: Unix-like – Protocol: HTTP and SSL – Action: default signature action

 Copyright © Huawei Technologies Co., Ltd.

Item	Data
Security policy	Create two security policies to filter the traffic from the Internet and intranet to the intranet server. ● Security policy name: policy_sec_1 – Source security zone: Trust – Destination security zone: DMZ – Source address: 10.3.0.0/24 – Destination address: 10.2.0.0/24 – Service: FTP, HTTP, SSL, SMTP, IMAP4 and POP3 – Action: permit – Content security: Profile_ips_server1 ● Security policy name: policy_sec_2 – Source security zone: Untrust – Destination security zone: DMZ – Destination address: 10.2.0.0/24 – Service: HTTP and SSL – Action: permit – Content security: Profile_ips_server2

Configuration Roadmap

1. Configure interface IP addresses and assign the interfaces to security zones.
2. Configure IPS profiles Profile_ips_server1 and Profile_ips_server2 and configure different signature filters for different servers to meet security requirements.
3. Create security policy policy_sec_1 and policy_sec_2 to reference Profile_ips_server1 and Profile_ips_server2, respectively. This protects the intranet server against attacks from intranet and Internet users.

Procedure

Step 1 Configure interface IP addresses and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

3. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	dmz

 Copyright © Huawei Technologies Co., Ltd.

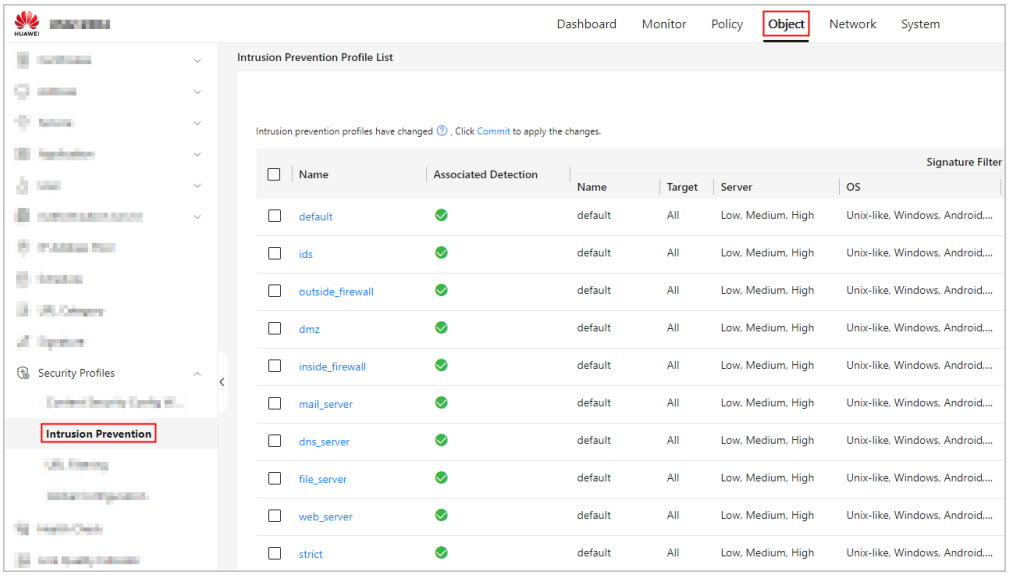
IPv4	
IP Address	10.2.0.1/24

4. Repeat the preceding steps to set the parameters for GE0/0/3.

Zone	trust
IPv4	
IP Address	10.3.0.1/24

Step 2 Create an IPS profile and configure a signature filter.

1. Choose **Object** > **Security Profiles** > **Intrusion Prevention**.

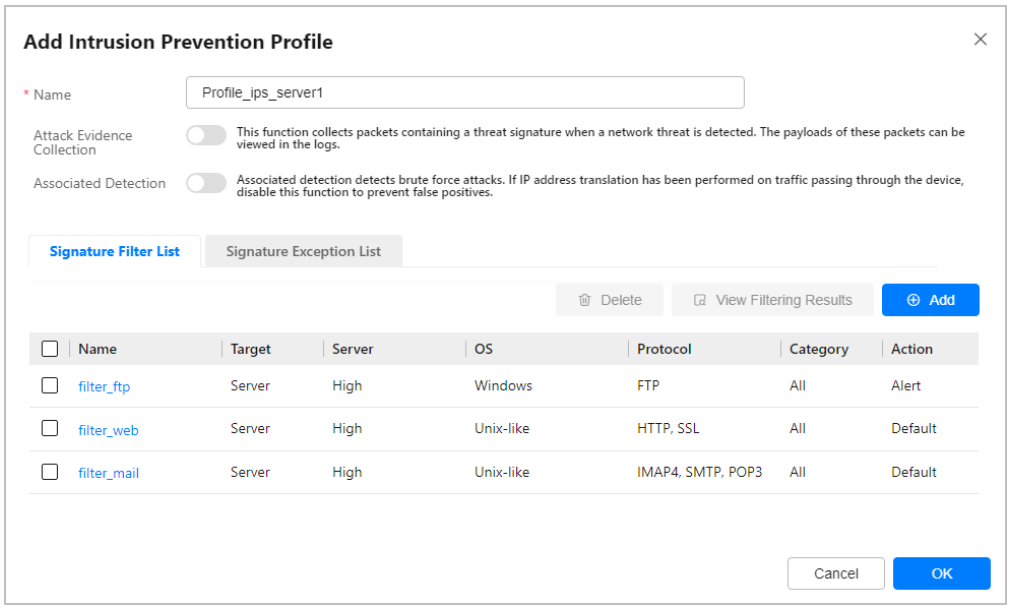


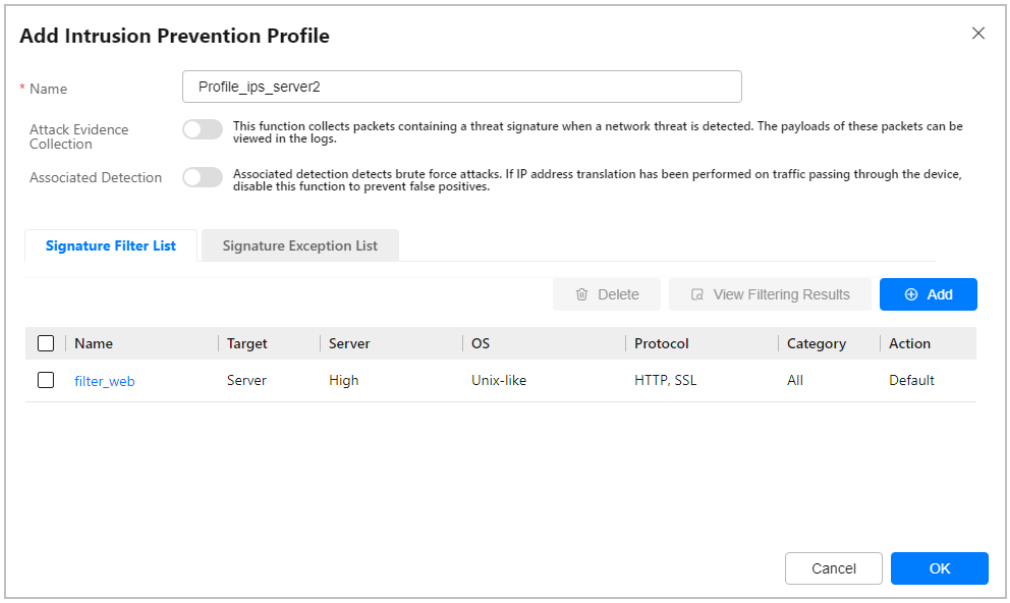
2. In **Intrusion Prevention Profile List**, click **Add** and set parameters as follows for profiles Profile_ips_server1 and Profile_ips_server2, which will be referenced by the Trust-to-DMZ and Untrust-to-DMZ interzone policies respectively. Click **OK**.

NOTE

Based on service requirements, you can set the action of the signature set to alert or use the default action of the signature. You are not advised to set the action to block for all signatures.

 Copyright © Huawei Technologies Co., Ltd.





3. Click **Commit** in the upper right corner of the web page. In the dialog box that is displayed, click **OK**.

Step 3 Configure security policies, and apply the IPS profiles to the security policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the parameters for the Trust-to-DMZ interzone policy. Click **OK**.

Name	policy_sec_1
Source Zone	trust
Destination Zone	dmz
Source Address	10.3.0.0/24

 Copyright © Huawei Technologies Co., Ltd.

Destination Address	10.2.0.0/24
Service	http, ssl, smtp, imap, pop3, ftp
Action	Permit
Content Security	
Intrusion Prevention	Profile_ips_server1

3. Repeat the preceding steps to configure an Untrust-to-DMZ interzone policy.

Name	policy_sec_2
Source Zone	untrust
Destination Zone	dmz
Source Address	any
Destination Address	10.2.0.0/24
Service	http, ssl
Action	Permit
Content Security	
Intrusion Prevention	Profile_ips_server2

Step 4 Click **Save** in the upper right corner of the web page. In the dialog box that is displayed, click **OK**.

----End

Verifying the Configuration

When an attack occurs, the access connection is blocked. Choose **Monitor** > **Logs** > **Threat Logs** to view detected attacks.

After the IPS function is configured, you need to periodically check and adjust the configuration in a timely manner during network running to improve the accuracy of intrusion detection and blocking without affecting services. The threat logs generated when the intranet server is attacked contain a large number of incorrectly reported logs. You can adjust the configuration by identifying and analyzing the incorrectly reported logs. The configuration roadmap is as follows:

 Copyright © Huawei Technologies Co., Ltd.

Procedure	Description	Details
1	Identify suspicious attacks.	Based on threat logs and threat reports, collect statistics from multiple dimensions, such as time, attack source, attack target, and attack type, to identify anomalies. For example, if a large number of attack events occur within a time range, you need to filter out the IP addresses and events that occur within this time range for further analysis.
2	Check whether the log is incorrectly reported and whether services may be affected.	• Determine the attack source or target. For example, if the attack source is an intranet IP address, check whether the access is initiated in normal services. If the request is initiated in a normal service, the request needs to be permitted. If the attack source is an Internet IP address and the access frequency or time is abnormal compared with other IP addresses, you need to further analyze whether the threat event generated by the IP address affects services. • Check whether the attack type is related to the services running on the server corresponding to the attacked IP address. For example, many SQL injection attacks are detected, but no database is running on the attacked server. In this case, the SQL injection attacks are invalid. You can use the following methods to mask signatures as required: – Action permitting: You can set an exception signature to permit the action. The application scope of the exception signature applies only to the current profile. – Signature disabling: Signature disabling applies globally. Once a signature is disabled, it cannot be used by all profiles.

 Copyright © Huawei Technologies Co., Ltd.

Procedure	Description	Details
3	Perform security hardening or upgrade based on threat countermeasures.	The signature details of the device provide countermeasures against common attacks. You can harden or upgrade the device based on the information. The methods for processing attacks of the same type are similar. You can also analyze and process attacks by type. Common attacks are classified into the following types: ● Attacks targeting at operating system and using software vulnerabilities: A large number of threat logs generated by the device are caused this type of attacks. To defend against such attacks, you are advised to check whether the operating system or software of the intranet server or host has been upgraded to a non-vulnerable version. After the upgrade, involved signatures can be disabled to reduce the number of logs. ● Attacks on the database: To defend against such attacks, you need to harden the database security. ● High-risk attacks, such as Trojan horses: If the default action of a signature is alert or permit, you can set the action to block without affecting services.
4	Adjust configurations, including security policies and IPS profiles.	After suspicious attacks are identified, you can modify the configuration to block the attacks that do not affect normal services. For example: ● Some attacks may pose threats only in specific scenarios. In other scenarios, such attacks may not cause harm, and even some special services may have the threat characteristics. In this case, you need to identify whether the blocked threat is an attack in the current network environment. If not, you can configure the signature as an exception signature and set the action to alert. ● In the security-preferred scenario, if some alarms are triggered by abnormal services and the behavior triggering the alarms comply with attack characteristics, you can configure an exception signature and set the action to block. ● You can directly add the source IP address of the intrusion behavior to the blacklist, or add the IP address to the matching condition of the security policy and set the action to block. Exercise caution when modifying the response action if you are not sure whether the blocking will affect normal services.

 Copyright © Huawei Technologies Co., Ltd.

Procedure	Description	Details
5	Monitor the network status and attack events.	Monitor the network status and attack events for a period of time to check whether services are affected. If services are affected, query the configuration logs to check whether the configurations of the affected services are recorded in the logs.
6	Periodically check threat logs and modify configurations.	The configuration of the IPS function cannot be completed at a time. You need to periodically check logs and adjust the configuration. Especially in the case of large-scale attacks, you need to check threat logs and adjust configurations in a timely manner.

The following example describes how to check threat logs and adjust configurations accordingly.

1. Choose **Monitor** > **Logs** > **Threat log**.
2. Determine whether a threat is an attack based on the behavior of the threat source and adjust the configuration.

   Example 1:

   a. Check threat logs. An IP address in the Untrust zone continuously initiates intrusion attacks to multiple IP addresses in the destination security zone.

   b. Check the attack. Enter the time range to be observed and the IP address of the attack source as query conditions to query the attack.

      The query result shows that the attacker continuously launches multiple intrusion attacks within a period of time, indicating that the attack source launches malicious attacks. To block the attacks, you can configure a security policy to block the traffic from the IP address.

 Copyright © Huawei Technologies Co., Ltd.

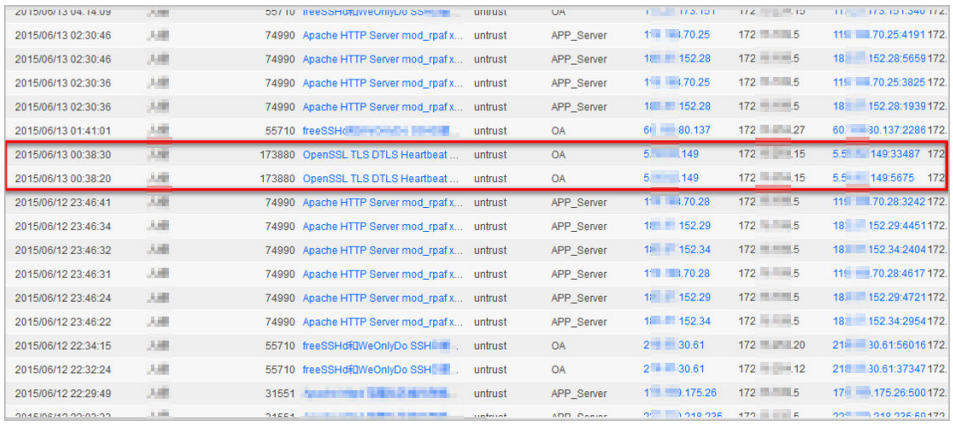


3. Determine whether a threat is an attack based on the threat event information and adjust the configuration.

   Some attacks last for a short period of time, occur only several times, and have a few attack sources. In this case, it is difficult to determine attacks based on the correlation between logs. You need to determine whether a threat is an attack based on the information about the threat event.

   Example 2:

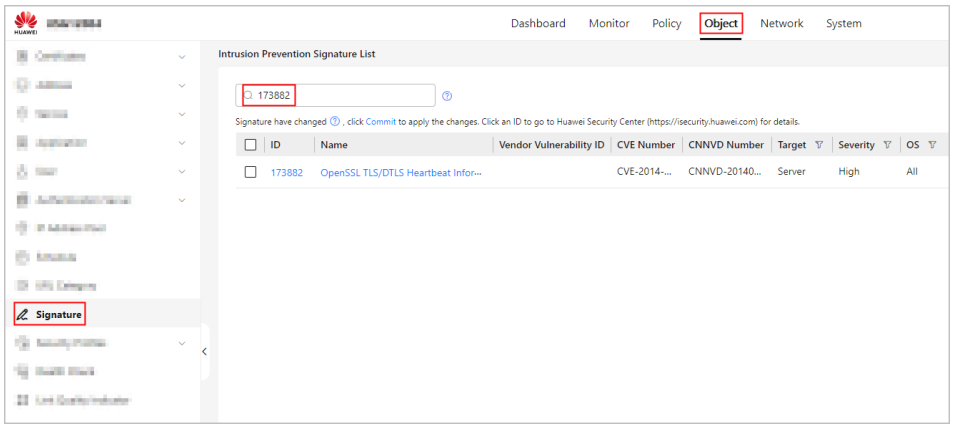
   a. Check threat logs. A few threat logs whose threat type is intrusion are found. The number of attack sources is small. You need to determine whether the threat is an attack based on the threat event information.



   b. Choose **Object** > **Signature** and enter the threat ID recorded in the threat log in the search box. In the search result, click the signature to view its details.

      This is a major OpenSSL vulnerability found at the end of 2014. This vulnerability will cause information leak and affect all software or services that use OpenSSL. It is a high-risk vulnerability with the CVSS score of 10. You need to pay attention to this threat even if it occurs only once. You can block it or perform operations based on the countermeasures in the details.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Scripts

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
profile type ips name Profile_ips_server1
 signature-set name filter_ftp
  action alert
  os windows
  target server
  severity high
  protocol FTP
  category all
 signature-set name filter_web
  os unix-like
  target server
  severity high
  protocol HTTP SSL
  category all
 signature-set name filter_mail
  os unix-like
  target server
  severity high
  protocol IMAP4 SMTP POP3
  category all
#
profile type ips name Profile_ips_server2
 signature-set name filter_web
  os unix-like
  target server
  severity high
  protocol HTTP SSL
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category all
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone dmz
  source-address 10.3.0.0 mask 255.255.255.0
  destination-address 10.2.0.0 mask 255.255.255.0
  service http
  service ftp
  service smtp
  service ssl
  service imap
  service pop3
  profile ips Profile_ips_server1
  action permit
 rule name policy_sec_2
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 mask 255.255.255.0
  service http
  service ssl
  profile ips Profile_ips_server2
  action permit
```

13.3 Web: Example for Configuring the IPS Function to Protect Intranet Users

Networking Requirements

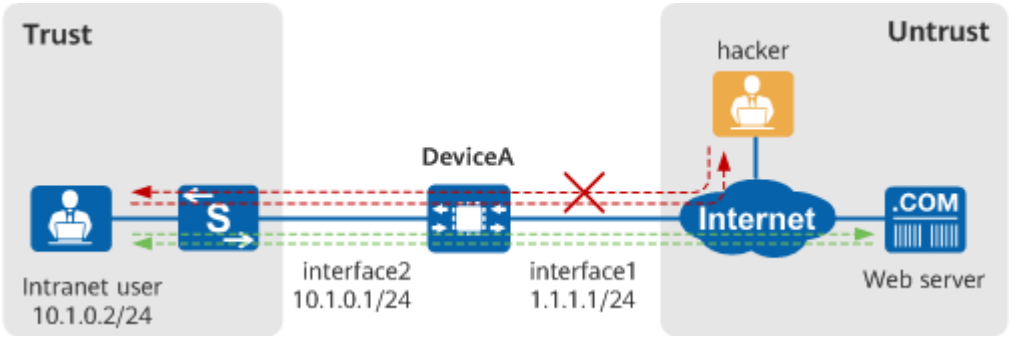
In **Figure 13-3**, DeviceA is deployed at the border of an enterprise network as a security gateway. In this networking, intranet users can access the web server on the Internet.

The enterprise needs to configure the IPS function on DeviceA to protect intranet users from attacks when they access the Internet web server. For example, the web server is infected by malware.

Figure 13-3 Example for configuring the IPS function to protect intranet users

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Table 13-2 Data plan for protecting intranet users

Item	Data
IPS profile	The most common threats on the enterprise network are worms, Trojan horses, and Botnets, and their severities in signatures are all High. The attacks are triggered by the Internet access from intranet users and the targets are intranet users. Therefore, create a signature filter, and set the protocol to HTTP, object to client, and severity to high. • Profile: Profile_ips_pc – Signature filter filter1: – Name: filter1 – Object: client – Severity: high – Protocol: HTTP – Action: default signature action
Security policy	Create a security policy to filter the traffic from the Internet web server to intranet users. • Security policy name: policy_sec_1 – Source security zone: Trust – Destination security zone: Untrust – Source address: 10.1.0.0/24 – Service: HTTP – Action: permit – Content security: Profile_ips_pc

Configuration Roadmap

1. Configure interface IP addresses and assign the interfaces to security zones.
2. Configure IPS profile Profile_ips_pc and configure different a signature filter to meet security requirements.
3. Create security policy policy_sec_1 and reference profile Profile_ips_pc to protect intranet users from Internet attacks.

Procedure

Step 1 Configure interface IP addresses and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click for GE0/0/1 and set the parameters as follows. Click **OK**.

Zone	untrust
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

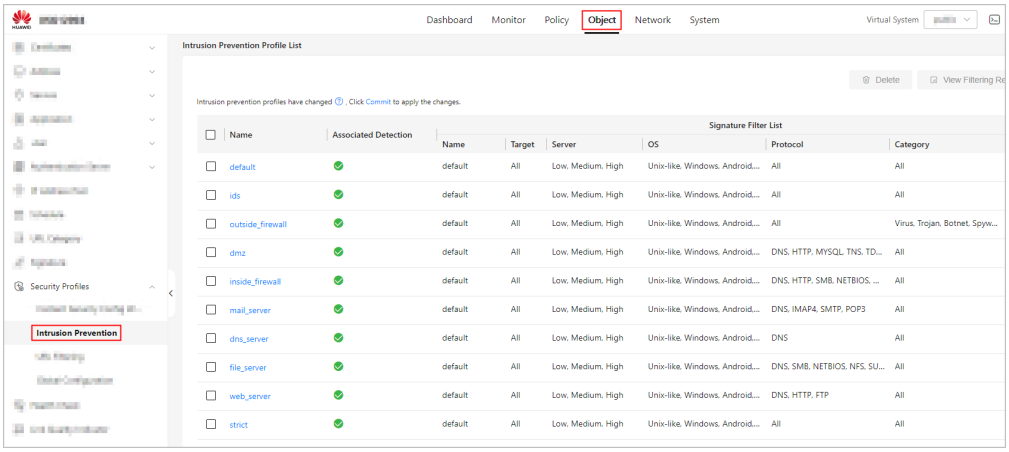
IP Address	1.1.1.1/24

3. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	trust
IPv4	
IP Address	10.1.0.1/24

Step 2 Create an IPS profile and configure a signature filter.

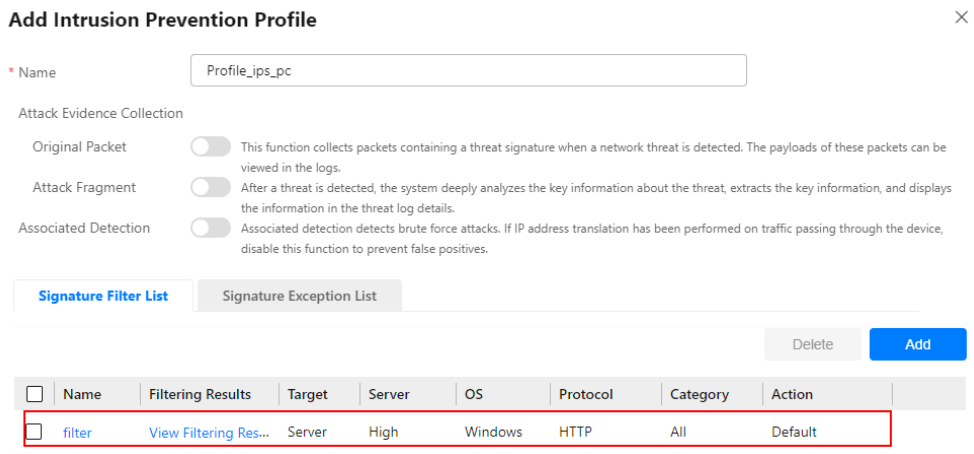
1. Choose **Object** > **Security Profiles** > **Intrusion Prevention**.



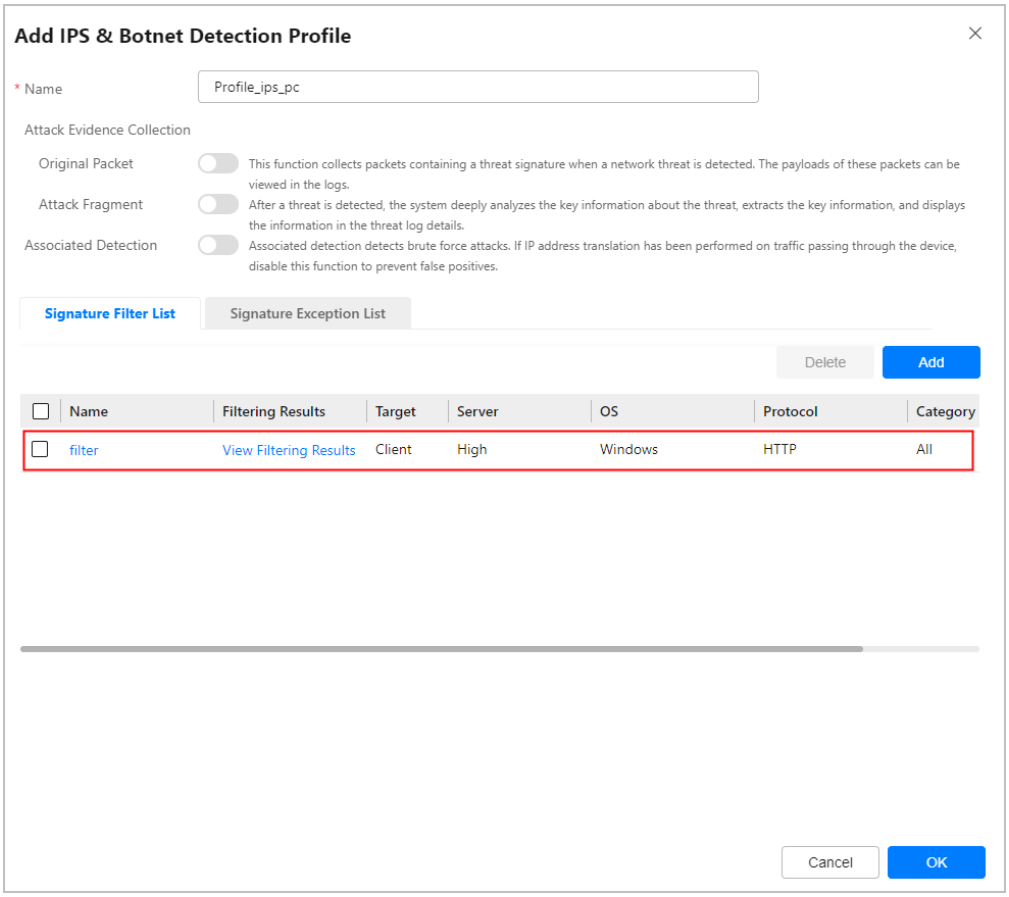
2. In **Intrusion Prevention Profile List**, click **Add** and set parameters as follows for profile Profile_ips_pc, which will be referenced by the Trust-to-Untrust interzone policy. Click **OK**.

NOTE

Based on service requirements, you can set the action of the signature set to alert or use the default action of the signature. You are not advised to set the action to block for all signatures.



 Copyright © Huawei Technologies Co., Ltd.



3. Click **Commit** in the upper right corner of the web page. In the dialog box that is displayed, click **OK**.

Step 3 Configure security policies, and apply the IPS profile to the security policy.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and set the parameters for the Trust-to-Untrust interzone policy. Click **OK**.

Name	policy_sec_1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.0.0/24
Service	http
Action	Permit
Content Security	
Intrusion Prevention	Profile_ips_pc

Step 4 Click **Save** in the upper right corner of the web page. In the dialog box that is displayed, click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

When an attack occurs, the access connection is blocked. Choose **Monitor** > **Logs** > **Threat Logs** to view detected attacks.

After the IPS function is configured, you need to periodically check and adjust the configuration in a timely manner during network running to improve the accuracy of intrusion detection and blocking without affecting services. The threat logs generated when the intranet server is attacked contain a large number of incorrectly reported logs. You can adjust the configuration by identifying and analyzing the incorrectly reported logs. The configuration roadmap is as follows:

Procedure	Description	Details
1	Identify suspicious attacks.	Based on threat logs and threat reports, collect statistics from multiple dimensions, such as time, attack source, attack target, and attack type, to identify anomalies. For example, if a large number of attack events occur within a time range, you need to filter out the IP addresses and events that occur within this time range for further analysis.
2	Check whether the log is incorrectly reported and whether services may be affected.	• Determine the attack source or target. For example, if the attack source is an intranet IP address, check whether the access is initiated in normal services. If the request is initiated in a normal service, the request needs to be permitted. If the attack source is an Internet IP address and the access frequency or time is abnormal compared with other IP addresses, you need to further analyze whether the threat event generated by the IP address affects services. • Check whether the attack type is related to the services running on the server corresponding to the attacked IP address. For example, many SQL injection attacks are detected, but no database is running on the attacked server. In this case, the SQL injection attacks are invalid. You can use the following methods to mask signatures as required: – Action permitting: You can set an exception signature to permit the action. The application scope of the exception signature applies only to the current profile. – Signature disabling: Signature disabling applies globally. Once a signature is disabled, it cannot be used by all profiles.

 Copyright © Huawei Technologies Co., Ltd.

Procedure	Description	Details
3	Perform security hardening or upgrade based on threat countermeasures.	The signature details of the device provide countermeasures against common attacks. You can harden or upgrade the device based on the information. The methods for processing attacks of the same type are similar. You can also analyze and process attacks by type. Common attacks are classified into the following types: ● Attacks targeting at operating system and using software vulnerabilities: A large number of threat logs generated by the device are caused this type of attacks. To defend against such attacks, you are advised to check whether the operating system or software of the intranet server or host has been upgraded to a non-vulnerable version. After the upgrade, involved signatures can be disabled to reduce the number of logs. ● Attacks on the database: To defend against such attacks, you need to harden the database security. ● High-risk attacks, such as Trojan horses: If the default action of a signature is alert or permit, you can set the action to block without affecting services.
4	Adjust configurations, including security policies and IPS profiles.	After suspicious attacks are identified, you can modify the configuration to block the attacks that do not affect normal services. For example: ● Some attacks may pose threats only in specific scenarios. In other scenarios, such attacks may not cause harm, and even some special services may have the threat characteristics. In this case, you need to identify whether the blocked threat is an attack in the current network environment. If not, you can configure the signature as an exception signature and set the action to alert. ● In the security-preferred scenario, if some alarms are triggered by abnormal services and the behavior triggering the alarms comply with attack characteristics, you can configure an exception signature and set the action to block. ● You can directly add the source IP address of the intrusion behavior to the blacklist, or add the IP address to the matching condition of the security policy and set the action to block. Exercise caution when modifying the response action if you are not sure whether the blocking will affect normal services.

 Copyright © Huawei Technologies Co., Ltd.

Procedure	Description	Details
5	Monitor the network status and attack events.	Monitor the network status and attack events for a period of time to check whether services are affected. If services are affected, query the configuration logs to check whether the configurations of the affected services are recorded in the logs.
6	Periodically check threat logs and modify configurations.	The configuration of the IPS function cannot be completed at a time. You need to periodically check logs and adjust the configuration. Especially in the case of large-scale attacks, you need to check threat logs and adjust configurations in a timely manner.

The following example describes how to check threat logs and adjust configurations accordingly.

1. Choose **Monitor** > **Logs** > **Threat log**.
2. Determine whether a threat is an attack based on the behavior of the threat source and adjust the configuration.

   Example 1:

   a. Check threat logs. An IP address in the Untrust zone continuously initiates intrusion attacks to multiple IP addresses in the destination security zone.

   b. Check the attack. Enter the time range to be observed and the IP address of the attack source as query conditions to query the attack.

      The query result shows that the attacker continuously launches multiple intrusion attacks within a period of time, indicating that the attack source launches malicious attacks. To block the attacks, you can configure a security policy to block the traffic from the IP address.

 Copyright © Huawei Technologies Co., Ltd.

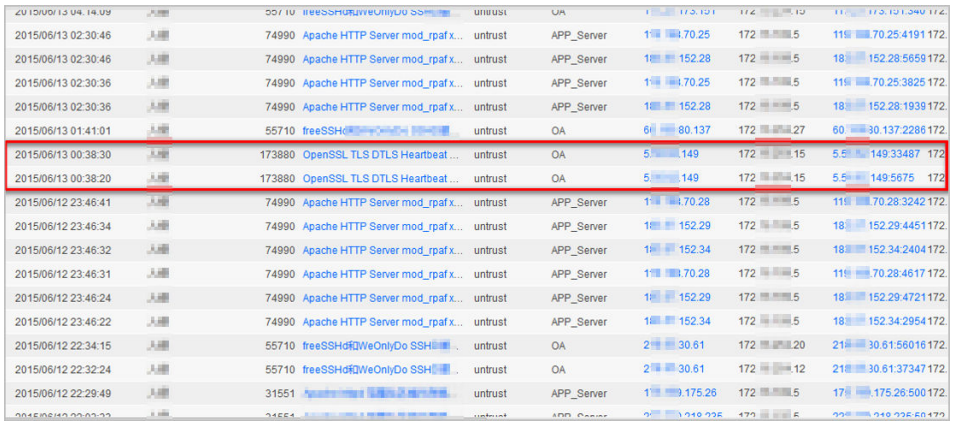


3. Determine whether a threat is an attack based on the threat event information and adjust the configuration.

   Some attacks last for a short period of time, occur only several times, and have a few attack sources. In this case, it is difficult to determine attacks based on the correlation between logs. You need to determine whether a threat is an attack based on the information about the threat event.

   Example 2:

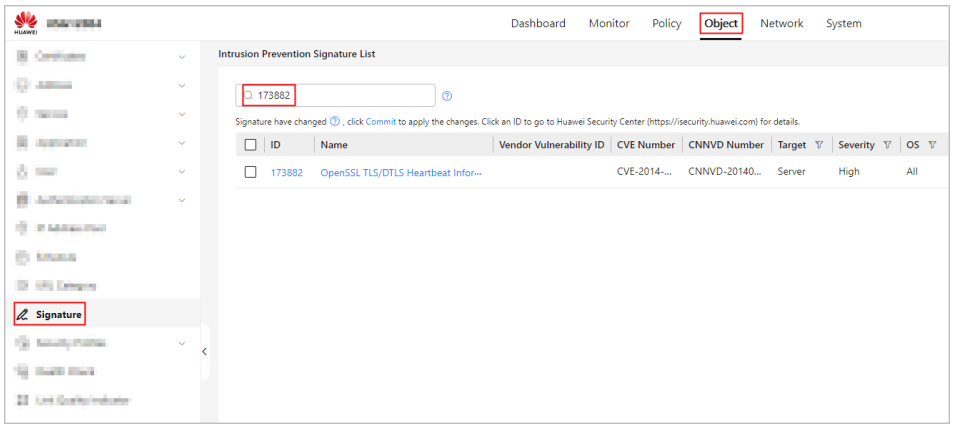
   a. Check threat logs. A few threat logs whose threat type is intrusion are found. The number of attack sources is small. You need to determine whether the threat is an attack based on the threat event information.



   b. Choose **Object** > **Signature** and enter the threat ID recorded in the threat log in the search box. In the search result, click the signature to view its details.

      This is a major OpenSSL vulnerability found at the end of 2014. This vulnerability will cause information leak and affect all software or services that use OpenSSL. It is a high-risk vulnerability with the CVSS score of 10. You need to pay attention to this threat even if it occurs only once. You can block it or perform operations based on the countermeasures in the details.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Scripts

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
profile type ips name Profile_ips_pc
 signature-set name filter1
  os windows
  target client
  severity high
  protocol HTTP
  category all
 #
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.1.0.0 mask 255.255.255.0
  service http
  profile ips Profile_ips_pc
  action permit
```

13.4 CLI: Example for Configuring Intrusion Prevention

Networking Requirements

As shown in **Figure 13-4**, an enterprise deploys **DeviceA** as the security gateway at the network border. In the networking:

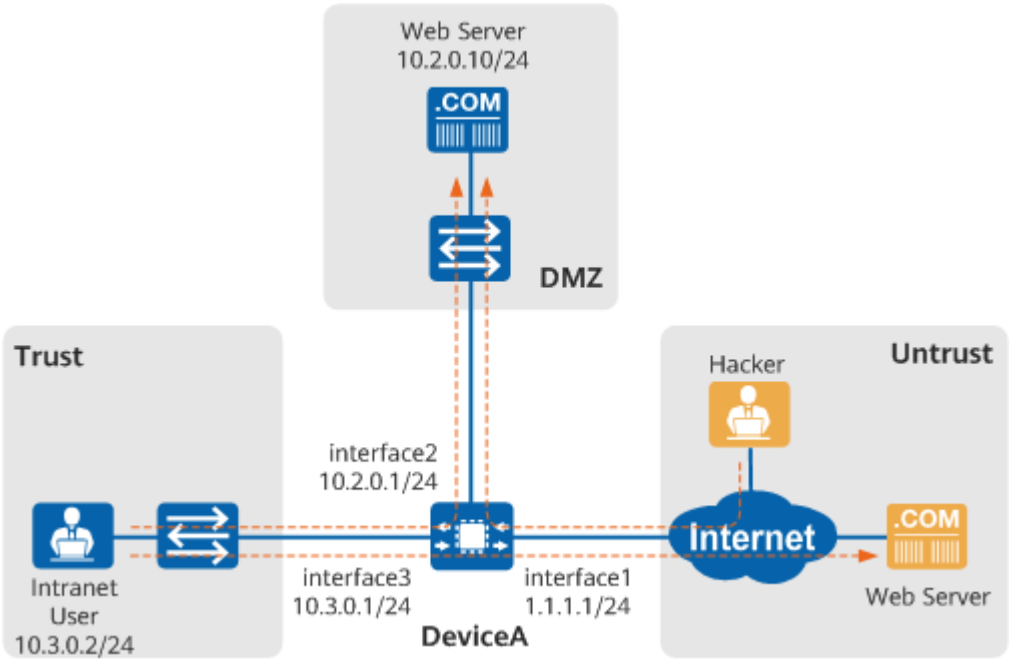
- An intranet user can access the Internet Web server.
- The intranet Web server provides services for both intranet and Internet users.

 Copyright © Huawei Technologies Co., Ltd.

Figure 13-4 Intrusion prevention networking diagram

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



The enterprise wants to enable intrusion prevention on the **DeviceA** to meet the following requirements:

- Protect intranet users.

  Protect intranet users from attacks, such as an attacker launched from a website with malicious code, when the users access the Internet web server.
- Protect the intranet Web server.

  Prevent Internet and intranet users from launching attacks on the intranet Web server.

Configuration Roadmap

The configuration roadmap is as follows:

1. Set the interface IP addresses and add the interfaces to corresponding security zones as required.
2. Create security policy **policy_sec_1** and reference default profile **default** to protect intranet users from Internet attacks.
3. Create security policy **policy_sec_2** and reference default profile **web_server** to protect intranet servers from intranet and Internet attacks.

Procedure

Step 1 Set an IP address for each interface, assign interfaces to security zones, and complete basic parameter settings.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 255.255.255.0
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge0/0/2
[DeviceA-zone-dmz] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy between the Trust and Untrust zones and reference intrusion prevention profile **default**.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_1] profile ips default
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
```

Step 3 Configure security policies for the Trust -> DMZ and Untrust -> DMZ interzones and reference intrusion prevention profile **web_server**.

```
[DeviceA-policy-security] rule name policy_sec_2
[DeviceA-policy-security-rule-policy_sec_2] source-zone trust untrust
[DeviceA-policy-security-rule-policy_sec_2] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sec_2] profile ips web_server
[DeviceA-policy-security-rule-policy_sec_2] action permit
[DeviceA-policy-security-rule-policy_sec_2] quit
[DeviceA-policy-security] quit
```

Step 4 Save the configuration information to upload the configuration file including the above-mentioned configurations automatically for the next startup.

```
[DeviceA] quit
<DeviceA> save
```

----End

Verifying the Configuration

- When an attack event occurs and the access is blocked, you can view the threat log of the IPS module on the device.
- You can run the **display ips statistics** command to view intrusion prevention statistics.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone dmz
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  profile ips default
  action permit
 rule name policy_sec_2
  source-zone trust
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 24
  profile ips web_server
  action permit
```

13.5 CLI: Example for Configuring Antivirus

Networking Requirements

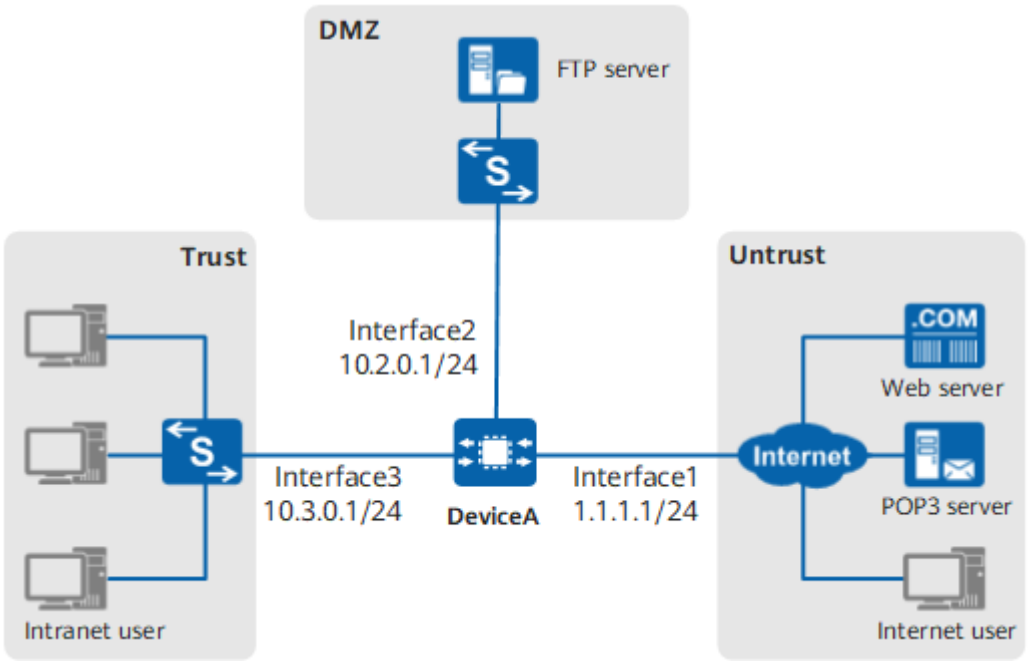
As shown in **Figure 13-5**, DeviceA is deployed at the border of an enterprise network. Intranet users can download files and emails through the web server and POP3 server. The intranet FTP server needs to receive files uploaded by Internet users. The enterprise uses the antivirus function provided by the device to prevent virus files from entering the protected network, ensuring the security of intranet users and servers. Intranet users fail to download important software from the web server. It is found that the software (virus name: EICAR.Test.FILE.1) is blocked because it is identified as a virus by the device. Having confirmed the importance of the software and the trustworthiness of the software source, the administrator temporarily permits the virus file to ensure that users can successfully download the software.

Figure 13-5 Antivirus network diagram

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

1. Configure an IP address for each interface, assign interfaces to security zones, and complete basic parameter settings.
2. Configure antivirus profiles.
   - Configure the antivirus profile **profile_http_pop3**, set matching conditions and response actions for HTTP and POP3, set the file types for detection to all, and configure virus exception with virus name EICAR.Test.FILE.1 in the profile.
   - Configure the antivirus profile **profile_ftp**, set matching conditions and response actions for FTP, and set the file types for detection to all.
3. Configure a security policy for the traffic from the Trust zone to the Untrust zone, and from the Untrust zone to the DMZ, respectively. Then, reference the antivirus profiles in the policies respectively.
   - Configure the security policy **policy_sec_1** for the traffic from the Trust zone to the Untrust zone and reference the antivirus profile **profile_http_pop3** in the policy to detect and defend against viruses in files and mails downloaded by intranet users from the Internet.
   - Configure the security policy **policy_sec_2** for the traffic from the DMZ to the Untrust zone and reference the antivirus profile **profile_ftp** in the policy to detect and defend against viruses in files received by the intranet FTP server from the Internet.

Procedure

Step 1 Configure an IP address for each interface, assign interfaces to security zones, and complete basic parameter settings.

1. Configure an IP address for GE0/0/1, and add the interface to the Untrust zone.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

2. Configure an IP address for GE0/0/2, and add the interface to the DMZ.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

3. Configure an IP address for GE0/0/3, and add the interface to the Trust zone.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

Step 2 Configure antivirus profiles.

1. Configure the antivirus profile for HTTP and POP3 and add virus name EICAR.Test.FILE.1 as an exception in the profile. The antivirus profile applies only to HTTP and POP3. Therefore, disable virus detection for other protocols.

```
[DeviceA] profile type av name profile_http_pop3
[DeviceA-profile-av-profile_http_pop3] http-detect direction download action block
[DeviceA-profile-av-profile_http_pop3] pop3-detect enable
[DeviceA-profile-av-profile_http_pop3] file-type av all
[DeviceA-profile-av-profile_http_pop3] exception av-signature-name EICAR.Test.FILE.1
[DeviceA-profile-av-profile_http_pop3] undo ftp-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smtp-detect enable
[DeviceA-profile-av-profile_http_pop3] undo imap-detect enable
[DeviceA-profile-av-profile_http_pop3] undo nfs-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smb-detect enable
[DeviceA-profile-av-profile_http_pop3] quit
```

2. Configure the antivirus profile for FTP. The antivirus profile applies only to FTP. Therefore, disable virus detection for other protocols.

```
[DeviceA] profile type av name profile_ftp
[DeviceA-profile-av-profile_http_pop3] ftp-detect direction upload action block
[DeviceA-profile-av-profile_http_pop3] file-type av all
[DeviceA-profile-av-profile_http_pop3] undo http-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smtp-detect enable
[DeviceA-profile-av-profile_http_pop3] undo pop3-detect enable
[DeviceA-profile-av-profile_http_pop3] undo imap-detect enable
[DeviceA-profile-av-profile_http_pop3] undo nfs-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smb-detect enable
[DeviceA-profile-av-profile_http_pop3] quit
```

Step 3 Configure security policies.

1. Configure a security policy for the traffic from the Trust zone to the Untrust zone, and reference the default antivirus profile **default**.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] profile av profile_http_pop3
[DeviceA-policy-security-rule-policy_sec_1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

2. Configure a security policy for traffic from the DMZ to the Untrust zone, and reference the default antivirus profile **default**.

```
[DeviceA-policy-security] rule name policy_sec_2
[DeviceA-policy-security-rule-policy_sec_2] source-zone dmz
[DeviceA-policy-security-rule-policy_sec_2] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_2] source-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sec_2] action permit
[DeviceA-policy-security-rule-policy_sec_2] profile av profile_ftp
[DeviceA-policy-security-rule-policy_sec_2] quit
[DeviceA-policy-security] quit
```

Step 4 Commit the configuration in the system view.

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: AV submitted configurations successfully.
Info: Finish committing engine compiling.
```

Step 5 Save the configuration, so it can be automatically loaded during the next startup of the device.

```
[DeviceA] quit
<DeviceA> save
```

----End

Verifying the Configuration

- When an intranet user downloads an infected mail using POP3, the device generates a virus threat log.
- When an Internet user uploads an infected file using FTP, the upload connection is blocked and the device generates a virus threat log.
- Intranet users can download important software infected with virus EICAR.Test.FILE.1.
- To view antivirus statistics, run the **display file-frame statistics** [**slot** *slot-id* **cpu** *cpu-id*] command.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone dmz
 add interface GE0/0/2
#
profile type av name profile_http_pop3
 file-type av all
 http-detect direction download action block
 undo ftp-detect enable
 undo smtp-detect enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
 pop3-detect enable
 undo imap-detect enable
 undo nfs-detect enable
 undo smb-detect enable
 exception av-signature-name EICAR.Test.FILE.1
profile type av name profile_ftp
 file-type av all
 undo http-detect enable
 ftp-detect direction upload action block
 undo smtp-detect enable
 undo pop3-detect enable
 undo imap-detect enable
 undo nfs-detect enable
 undo smb-detect enable
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  profile av profile_http_pop3
  action permit
 rule name policy_sec_2
  source-zone untrust
  destination-zone dmz
  source-address 10.2.0.0 mask 255.255.255.0
  profile av profile_ftp
  action permit
```

13.6 Web: Example for Using URL Categories to Control Website Access

Networking Requirements

As shown in **Figure 13-6**, DeviceA is deployed at the network border as the enterprise's gateway to implement URL filtering on HTTP requests.

The enterprise has the following network access requirements for R&D and marketing employees:

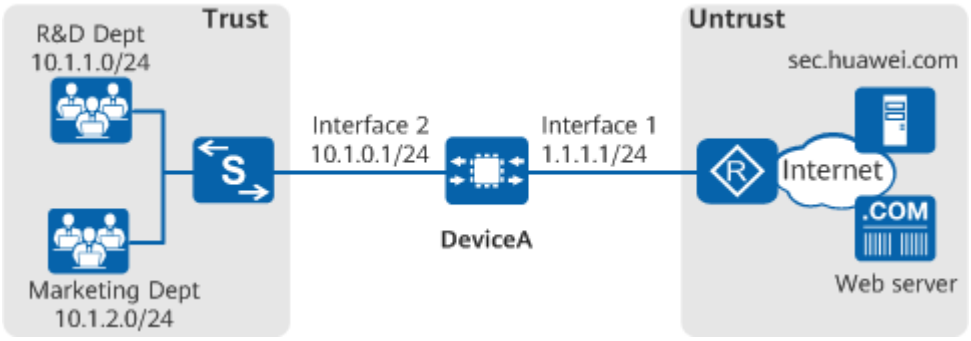
- R&D employees can access only education/science and search engine/portal websites from 09:00 to 17:00, and cannot access other websites.
- Marketing employees can access only education/science, search engine/portal, and social issues websites from 09:00 to 17:00, and cannot access other websites.

Figure 13-6 Network diagram for using URL categories to control website access

NOTE

In this example, interface 1 and interface 2 stand for GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

1. Configure an IP address for each interface and add interfaces to security zones.
2. Configure the remote query server to obtain the mappings between URLs and predefined URL categories. In this example, education/science, search engine/portal, and social issues websites are predefined URL categories, based on which the device filters URLs. To use the remote query function, you need to
   a. activate the license and ensure that the license is within the validity period.
   b. Configure the DNS server so that DeviceA can correctly resolve the domain name sec.huawei.com.
   c. Set the parameters for the remote query server, including the query mode and country name.
   d. Configure a security policy and reference user-defined services to allow DeviceA to access the scheduling center (sec.huawei.com). The user-defined services include:
      - TCP: The destination port number is 443 (for interacting with sec.huawei.com).
      - TCP: The destination port number is 12612 (for interacting with the scheduling server).
      - UDP: The destination port number is 12600 (for interacting with the query server).
3. Configure two URL filtering profiles, **profile_url_research** and **profile_url_marketing**, for the R&D and marketing departments, respectively. Specify control actions for predefined URL categories.
4. Configure a time range.
5. Configure two security policies, and reference the corresponding match criteria, such as the time range and URL filtering profile, in each security policy to control URL access from employees in different departments.

Procedure

Step 1 Configure an IP address for each interface and add interfaces to security zones.

1. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

2. Click corresponding to GE 0/0/2 and set the following parameters. After the configuration is complete, click **OK**.

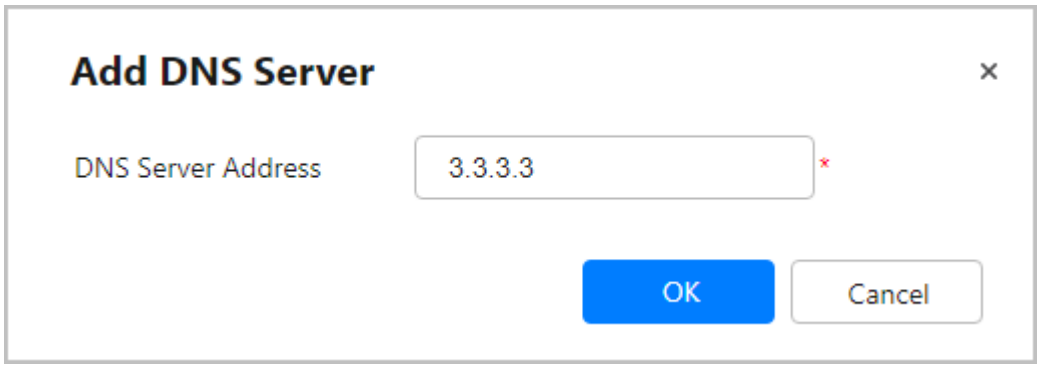
Zone	trust
IPv4	
IP Address	10.1.0.1/24

3. Repeat the preceding steps to configure GE 0/0/1.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

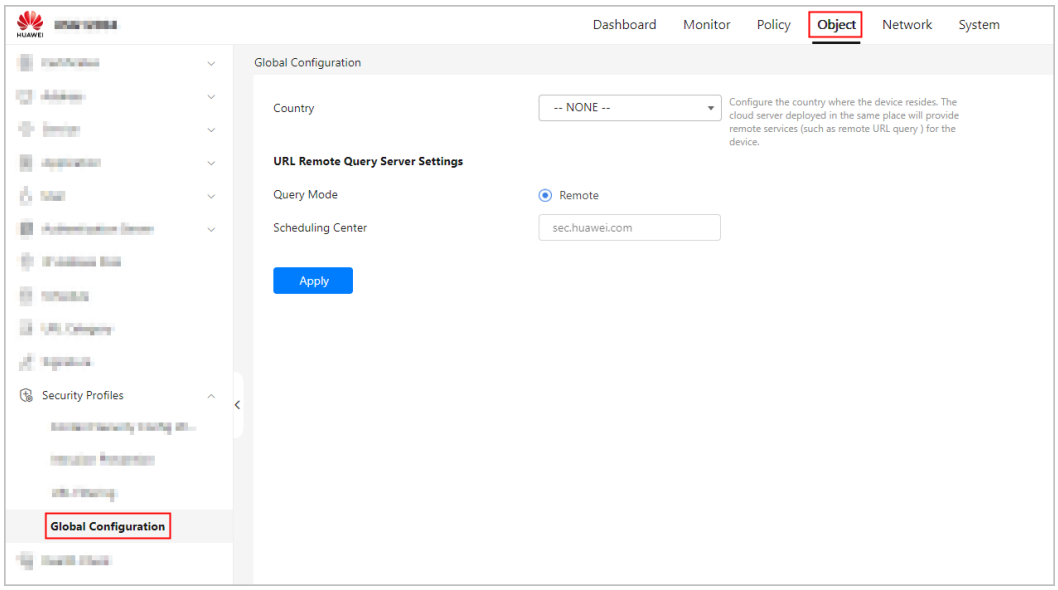
Step 2 Configure the remote query server to obtain the mappings between URLs and predefined URL categories.

1. Activate the remote URL query license and ensure that the license is within the validity period.
2. Configure a DNS server.
   a. Choose **Network** > **DNS** > **DNS** and click **Add**.
   b. Configure a DNS server. After the configuration is complete, click **OK**.
      Assume that the IP address of the DNS server is 3.3.3.3.



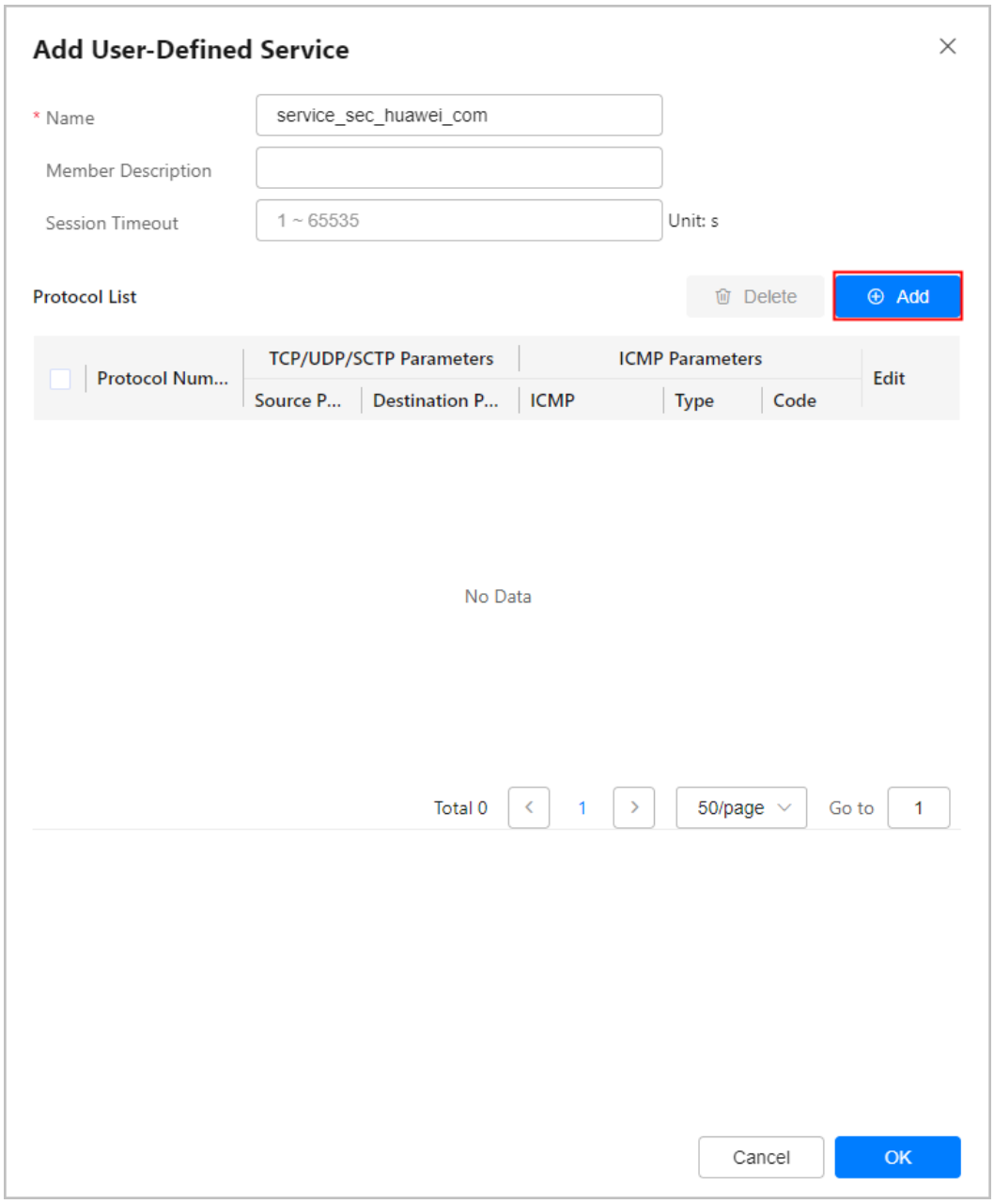
3. Set the parameters for the remote query server, including the query mode, country name, and timeout interval.
   a. Choose **Object** > **Security Profiles** > **Global Configuration**.
   b. Set **Country** to **CHINA** for DeviceA.
   c. Configure the remote URL query server. After the configuration is complete, click **Apply**.

 Copyright © Huawei Technologies Co., Ltd.



4. Configure a user-defined service.
   a. Choose **Object** > **Service** > **Service**.
   b. Click **Add** and enter a user-defined service name **service_sec_huawei_com**.

 Copyright © Huawei Technologies Co., Ltd.



c. In **Protocol List**, click **Add** and set the following parameters. After the configuration is complete, click **OK**.

Protocol	TCP
Protocol Number	6
Source Port	5000-65535
Destination Port	443

d. Repeat the preceding steps to set the following parameters.

Protocol	TCP

 Copyright © Huawei Technologies Co., Ltd.

Protocol Number	6
Source Port	5000-65535
Destination Port	12612

Protocol	UDP
Protocol Number	17
Source Port	5000-65535
Destination Port	12600

e. Click **OK**. The user-defined service is created.

5. Configure a security policy and reference user-defined services to allow DeviceA to access the scheduling center.

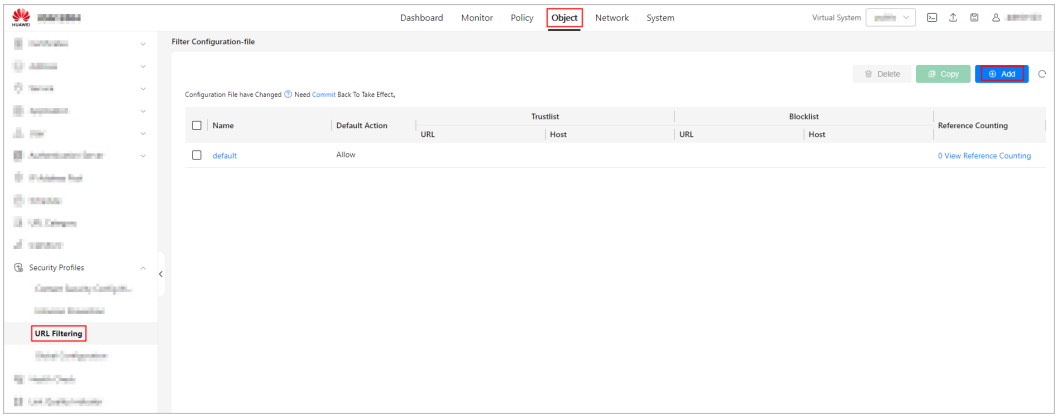
a. Choose **Policy** > **Security Policy** > **Security Policy**.

b. Click **Add Security Policy** and set the following parameters. After the configuration is complete, click **OK**.

Name	policy_sec_huawei_com
Source Zone	local
Destination Zone	untrust
Service	service_sec_huawei_com
Action	Permit

Step 3 Configure a URL filtering profile.

1. Choose **Object** > **Security Profiles** > **URL Filtering**.



2. In **URL Filtering Profile List**, click **Add** and configure URL filtering profile named **profile_url_research**. After the configuration is complete, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Name	profile_url_research
Default Action	Allow
URL Filtering Level	If **User-defined** is selected, the action for predefined categories **Education/Science** and **Search Engines/ Portals** is set to **Allow**, and the action for other predefined categories is set to **Block**. **NOTE** To simplify configuration, you can also perform as follows: After **User-defined** is selected, set the action for all predefined categories to **Block**, and then set the action for the two predefined categories to **Allow**.

3. In **URL Filtering Profile List**, click **Add** and configure URL filtering profile **profile_url_marketing**. After the configuration is complete, click **OK**.

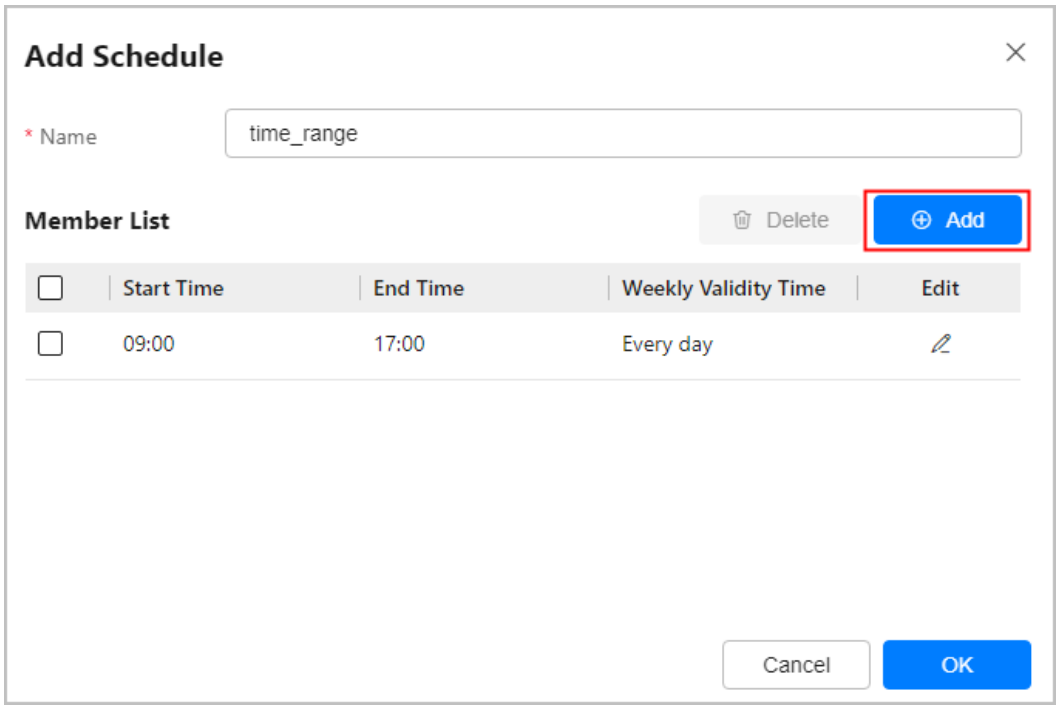
Name	profile_url_marketing
Default Action	Allow
URL Filtering Level	If **User-defined** is selected, the action for predefined categories **Education/Science**, **Search Engines/ Portals**, and **Social Focus** is set to **Allow**, and the action for other predefined categories is set to **Block**. **NOTE** To simplify configuration, you can also perform as follows: After **User-defined** is selected, set the action for all predefined categories to **Block**, and then set the action for the three predefined categories to **Allow**.

4. Click **Commit** on the upper right of the page, and then click **OK** in the dialog box that appears.

Step 4 Configure a time range.

1. Choose **Object** > **Schedule**.
2. Click **Add** and enter a time range name **time_range**.

 Copyright © Huawei Technologies Co., Ltd.



3. In **Member List**, click **Add** and set the following parameters. After the configuration is complete, click **OK**.

Type	Periodic
Start Time	09:00
End Time	17:00
Weekly Validity Time	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday

Step 5 Configure a security policy and apply the URL filtering profile to the security policy.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a URL access control policy for R&D employees. After the configuration is complete, click **OK**.

Name	policy_sec_research
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Schedule	time_range
Action	Permit
Content Security	
URL Filtering	profile_url_research

 Copyright © Huawei Technologies Co., Ltd.

3. Repeat the preceding steps to configure a URL access control policy for marketing employees.

Name	policy_sec_marketing
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.2.0/24
Schedule	time_range
Action	Permit
Content Security	
URL Filtering	profile_url_marketing

Step 6 Click **Save** in the upper right corner and click **OK** in the dialog box that is displayed.

----End

Verifying the Configuration

- The R&D employees can access only websites that belong to the **Education/Science** and **Search Engines/Portals** categories from 09:00 to 17:00 every day, but they cannot access websites that belong to **Social Focus** and forum categories.
- The marketing employees can access only websites that belong to the **Education/Science**, **Search Engines/Portals**, and **Social Focus** categories from 09:00 to 17:00 every day, but they cannot access forum websites.

Configuration Scripts

```
#
 dns resolve
 dns server 3.3.3.3
#
ip service-set service_sec_huawei_com type object
 service 0 protocol tcp source-port 5000 to 65535 destination-port 443
 service 1 protocol tcp source-port 5000 to 65535 destination-port 12612
 service 2 protocol udp source-port 5000 to 65535 destination-port 12600
#
 country CN
#
time-range time_range 09:00 to 17:00 daily
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
  ip address 10.1.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
profile type url-filter name profile_url_research
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 108 action block
 category pre-defined subcategory-id 177 action block
 category pre-defined subcategory-id 251 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
 category pre-defined subcategory-id 189 action block
 category pre-defined subcategory-id 125 action block
 category pre-defined subcategory-id 127 action block
 category pre-defined subcategory-id 128 action block
 category pre-defined subcategory-id 130 action block
 category pre-defined subcategory-id 131 action block
 category pre-defined subcategory-id 132 action block
 category pre-defined subcategory-id 197 action block
 category pre-defined subcategory-id 198 action block
 category pre-defined subcategory-id 199 action block
 category pre-defined subcategory-id 200 action block
 category pre-defined subcategory-id 227 action block
 category pre-defined subcategory-id 228 action block
 category pre-defined subcategory-id 133 action block
 category pre-defined subcategory-id 201 action block
 category pre-defined subcategory-id 202 action block
 category pre-defined subcategory-id 204 action block
 category pre-defined subcategory-id 205 action block
 category pre-defined subcategory-id 134 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 135 action block
 category pre-defined subcategory-id 136 action block
 category pre-defined subcategory-id 137 action block
 category pre-defined subcategory-id 138 action block
 category pre-defined subcategory-id 139 action block
 category pre-defined subcategory-id 140 action block
 category pre-defined subcategory-id 141 action block
 category pre-defined subcategory-id 206 action block
 category pre-defined subcategory-id 207 action block
 category pre-defined subcategory-id 208 action block
 category pre-defined subcategory-id 209 action block
 category pre-defined subcategory-id 210 action block
 category pre-defined subcategory-id 229 action block
 category pre-defined subcategory-id 142 action block
 category pre-defined subcategory-id 143 action block
 category pre-defined subcategory-id 144 action block
 category pre-defined subcategory-id 145 action block
 category pre-defined subcategory-id 146 action block
 category pre-defined subcategory-id 147 action block
 category pre-defined subcategory-id 211 action block
 category pre-defined subcategory-id 212 action block
 category pre-defined subcategory-id 213 action block
 category pre-defined subcategory-id 240 action block
 category pre-defined subcategory-id 253 action block
 category pre-defined subcategory-id 149 action block
 category pre-defined subcategory-id 150 action block
 category pre-defined subcategory-id 214 action block
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
profile type url-filter name profile_url_marketing
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
category pre-defined subcategory-id 164 action block
category pre-defined subcategory-id 165 action block
category pre-defined subcategory-id 103 action block
category pre-defined subcategory-id 166 action block
category pre-defined subcategory-id 167 action block
category pre-defined subcategory-id 168 action block
category pre-defined subcategory-id 104 action block
category pre-defined subcategory-id 169 action block
category pre-defined subcategory-id 170 action block
category pre-defined subcategory-id 106 action block
category pre-defined subcategory-id 108 action block
category pre-defined subcategory-id 177 action block
category pre-defined subcategory-id 251 action block
category pre-defined subcategory-id 109 action block
category pre-defined subcategory-id 110 action block
category pre-defined subcategory-id 111 action block
category pre-defined subcategory-id 112 action block
category pre-defined subcategory-id 114 action block
category pre-defined subcategory-id 115 action block
category pre-defined subcategory-id 117 action block
category pre-defined subcategory-id 178 action block
category pre-defined subcategory-id 179 action block
category pre-defined subcategory-id 180 action block
category pre-defined subcategory-id 181 action block
category pre-defined subcategory-id 248 action block
category pre-defined subcategory-id 118 action block
category pre-defined subcategory-id 119 action block
category pre-defined subcategory-id 122 action block
category pre-defined subcategory-id 182 action block
category pre-defined subcategory-id 183 action block
category pre-defined subcategory-id 184 action block
category pre-defined subcategory-id 123 action block
category pre-defined subcategory-id 124 action block
category pre-defined subcategory-id 186 action block
category pre-defined subcategory-id 187 action block
category pre-defined subcategory-id 188 action block
category pre-defined subcategory-id 189 action block
category pre-defined subcategory-id 125 action block
category pre-defined subcategory-id 127 action block
category pre-defined subcategory-id 128 action block
category pre-defined subcategory-id 130 action block
category pre-defined subcategory-id 131 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 142 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 143 action block
 category pre-defined subcategory-id 144 action block
 category pre-defined subcategory-id 145 action block
 category pre-defined subcategory-id 146 action block
 category pre-defined subcategory-id 147 action block
 category pre-defined subcategory-id 211 action block
 category pre-defined subcategory-id 212 action block
 category pre-defined subcategory-id 213 action block
 category pre-defined subcategory-id 240 action block
 category pre-defined subcategory-id 253 action block
 category pre-defined subcategory-id 149 action block
 category pre-defined subcategory-id 150 action block
 category pre-defined subcategory-id 214 action block
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
#
security-policy
 rule name policy_sec_huawei_com
  source-zone local
  destination-zone untrust
  service service_sec_huawei_com
  action permit
 rule name policy_sec_research
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  time-range time_range
  profile url-filter profile_url_research
  action permit
 rule name policy_sec_marketing
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  time-range time_range
```

 Copyright © Huawei Technologies Co., Ltd.

```
profile url-filter profile_url_marketing
action permit
```

13.7 CLI: Example for Using URL Categories to Control Website Access

Networking Requirements

On the network shown in **Figure 13-7**, DeviceA is deployed as a gateway at the border of an enterprise network. This device is used to implement URL filtering on users' requests for Internet access.

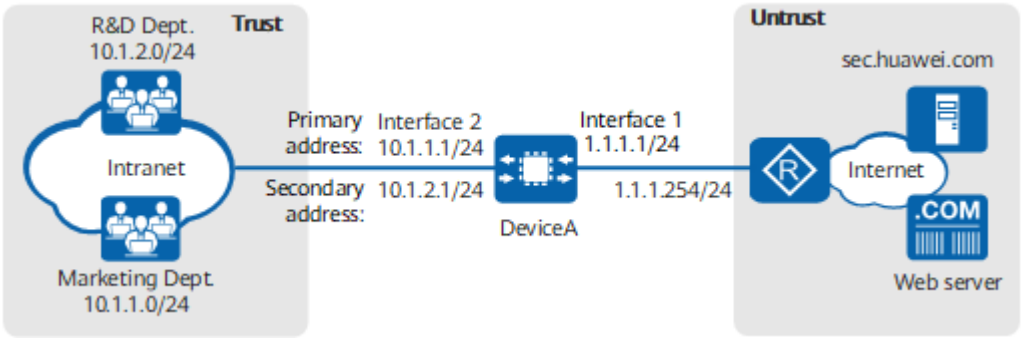
The enterprise has the following network access requirements for R&D and marketing employees:

- R&D employees can access only education/science and search engine/portal websites from 09:00 to 17:00, and cannot access other websites.
- Marketing employees can access only education/science, search engine/portal, and social issues websites from 09:00 to 17:00, and cannot access other websites.

Figure 13-7 Network diagram for using URL categories to control website access

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1, and GE0/0/2, respectively.



Configuration Roadmap

1. Configure an IP address for each interface and add interfaces to security zones.
2. Configure the remote query server to obtain the mappings between URLs and predefined URL categories. In this example, education/science, search engine/portal, and social issues websites are predefined URL categories, based on which the device filters URLs. To use the remote query function, perform the following operations:
   a. Activate the remote URL query license and ensure that the license is within the validity period.
   b. Configure the DNS server so that DeviceA can correctly resolve the domain name isecurity.huawei.com.

 Copyright © Huawei Technologies Co., Ltd.

c. Set the parameters for the remote query server, including the query mode, country name, and timeout interval.

d. Configure a security policy and reference user-defined services to allow DeviceA to access the scheduling center (isecurity.huawei.com). The user-defined services include:

- TCP: destination port number 443 (for interaction with the scheduling center)
- TCP: destination port number 12612 (for interaction with a scheduling server)
- UDP: destination port number 12600 (for interaction with a query server)

3. Configure two URL filtering profiles — **profile_url_research** and **profile_url_marketing** — for the R&D and marketing departments, respectively. Specify control actions for predefined URL categories.
4. Configure a time range.
5. Configure two security policies, and reference the corresponding time range and URL filtering profile in each security policy to control URL access from employees in different departments.

Procedure

Step 1 Configure an IP address for each interface and add interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-GE0/0/2] ip address 10.1.2.1 255.255.255.0 sub
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure the remote query server to obtain the mappings between URLs and predefined URL categories.

1. Activate the remote URL query license and ensure that the license is within the validity period.
2. Configure a DNS server.

```
[DeviceA] dns resolve
[DeviceA] dns server 10.2.0.70
```

3. Set the parameters of the remote query server, including the country name, timeout interval, and timeout action.

```
[DeviceA] country CN
[DeviceA] url-filter query timeout time 3 action allow
```

4. Configure user-defined services.

```
[DeviceA] ip service-set service_sec_huawei_com type object
[DeviceA-object-service-set-service_sec_huawei_com] service protocol TCP source-port 5000 to
65535 destination-port 443
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-object-service-set-service_sec_huawei_com] service protocol TCP source-port 5000 to 65535 destination-port 12612
[DeviceA-object-service-set-service_sec_huawei_com] service protocol UDP source-port 5000 to 65535 destination-port 12600
[DeviceA-object-service-set-service_sec_huawei_com] quit
```

5. Configure a security policy and reference user-defined services to allow DeviceA to access the scheduling center.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_huawei_com
[DeviceA-policy-security-rule-policy_sec_huawei_com] source-zone local
[DeviceA-policy-security-rule-policy_sec_huawei_com] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_huawei_com] service service_sec_huawei_com
[DeviceA-policy-security-rule-policy_sec_huawei_com] action permit
[DeviceA-policy-security-rule-policy_sec_huawei_com] quit
[DeviceA-policy-security] quit
```

Step 3 Configure URL filtering profiles.

NOTE

You can run the **display url-filter category pre-defined** command to query the mappings between the following predefined categories and IDs:

- 17: Education/Science
- 15: Search Engines/Portals
- 5: Social Focus (social issues)

1. Configure a URL filtering profile for the R&D department.

```
[DeviceA] profile type url-filter name profile_url_research
[DeviceA-profile-url-filter-profile_url_research] category pre-defined action block
[DeviceA-profile-url-filter-profile_url_research] category pre-defined category-id 15 action allow
[DeviceA-profile-url-filter-profile_url_research] category pre-defined category-id 17 action allow
[DeviceA-profile-url-filter-profile_url_research] quit
```

2. Configure a URL filtering profile for the marketing department.

```
[DeviceA] profile type url-filter name profile_url_marketing
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined action block
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined category-id 5 action allow
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined category-id 15 action allow
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined category-id 17 action allow
[DeviceA-profile-url-filter-profile_url_marketing] quit
```

Step 4 Configure a time range.

```
[DeviceA] time-range time_range 09:00 to 17:00 daily
```

Step 5 Reference URL filtering profiles in security policies.

1. Configure a security policy for the R&D department.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_research
[DeviceA-policy-security-rule-policy_sec_research] description Security policy of web access protect for research.
[DeviceA-policy-security-rule-policy_sec_research] source-zone trust
[DeviceA-policy-security-rule-policy_sec_research] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_research] source-address 10.1.2.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_research] time-range time_range
[DeviceA-policy-security-rule-policy_sec_research] action permit
[DeviceA-policy-security-rule-policy_sec_research] profile url-filter profile_url_research
[DeviceA-policy-security-rule-policy_sec_research] quit
```

2. Configure a security policy for the marketing department.

```
[DeviceA-policy-security] rule name policy_sec_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] description Security policy of web access protect for marketing.
[DeviceA-policy-security-rule-policy_sec_marketing] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing] source-address 10.1.1.0 mask 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy_sec_marketing] time-range time_range
[DeviceA-policy-security-rule-policy_sec_marketing] action permit
[DeviceA-policy-security-rule-policy_sec_marketing] profile url-filter profile_url_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] quit
[DeviceA-policy-security] quit
```

Step 6 Commit the content security profiles.

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

----End

Verifying the Configuration

- All R&D employees can access only websites that belong to the education/science and search engine/portal categories from 09:00 to 17:00, but they cannot access other websites including websites that belong to the social focus category.

  If an R&D employee attempts to access other websites (including those belonging to the Social Focus category), the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Pre-defined** and **Action** is **Block**.
- All marketing employees can access only websites that belong to the Education/Science, Search Engines/Portals, and Social Focus categories from 09:00 to 17:00, but they cannot access other websites.

  If a marketing employee attempts to access other websites, the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Pre-defined** and **Action** is **Block**.

Configuration Scripts

```
#
sysname DeviceA
#
 dns resolve
 dns server 10.2.0.70
#
ip service-set service_sec_huawei_com type object
 service 0 protocol tcp source-port 5000 to 65535 destination-port 443
 service 1 protocol tcp source-port 5000 to 65535 destination-port 12612
 service 2 protocol udp source-port 5000 to 65535 destination-port 12600
#
 country CN
#
 time-range time_range 09:00 to 17:00
daily
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
  ip address 10.1.1.1 255.255.255.0
  ip address 10.1.2.1 255.255.255.0 sub
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/1
#
profile type url-filter name profile_url_research
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 108 action block
 category pre-defined subcategory-id 177 action block
 category pre-defined subcategory-id 251 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
 category pre-defined subcategory-id 189 action block
 category pre-defined subcategory-id 125 action block
 category pre-defined subcategory-id 127 action block
 category pre-defined subcategory-id 128 action block
 category pre-defined subcategory-id 130 action block
 category pre-defined subcategory-id 131 action block
 category pre-defined subcategory-id 132 action block
 category pre-defined subcategory-id 197 action block
 category pre-defined subcategory-id 198 action block
 category pre-defined subcategory-id 199 action block
 category pre-defined subcategory-id 200 action block
 category pre-defined subcategory-id 227 action block
 category pre-defined subcategory-id 228 action block
 category pre-defined subcategory-id 133 action block
 category pre-defined subcategory-id 201 action block
 category pre-defined subcategory-id 202 action block
 category pre-defined subcategory-id 204 action block
 category pre-defined subcategory-id 205 action block
 category pre-defined subcategory-id 134 action block
 category pre-defined subcategory-id 135 action block
 category pre-defined subcategory-id 136 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 137 action block
 category pre-defined subcategory-id 138 action block
 category pre-defined subcategory-id 139 action block
 category pre-defined subcategory-id 140 action block
 category pre-defined subcategory-id 141 action block
 category pre-defined subcategory-id 206 action block
 category pre-defined subcategory-id 207 action block
 category pre-defined subcategory-id 208 action block
 category pre-defined subcategory-id 209 action block
 category pre-defined subcategory-id 210 action block
 category pre-defined subcategory-id 229 action block
 category pre-defined subcategory-id 142 action block
 category pre-defined subcategory-id 143 action block
 category pre-defined subcategory-id 144 action block
 category pre-defined subcategory-id 145 action block
 category pre-defined subcategory-id 146 action block
 category pre-defined subcategory-id 147 action block
 category pre-defined subcategory-id 211 action block
 category pre-defined subcategory-id 212 action block
 category pre-defined subcategory-id 213 action block
 category pre-defined subcategory-id 240 action block
 category pre-defined subcategory-id 253 action block
 category pre-defined subcategory-id 149 action block
 category pre-defined subcategory-id 150 action block
 category pre-defined subcategory-id 214 action block
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
profile type url-filter name profile_url_marketing
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
category pre-defined subcategory-id 103 action block
category pre-defined subcategory-id 166 action block
category pre-defined subcategory-id 167 action block
category pre-defined subcategory-id 168 action block
category pre-defined subcategory-id 104 action block
category pre-defined subcategory-id 169 action block
category pre-defined subcategory-id 170 action block
category pre-defined subcategory-id 106 action block
category pre-defined subcategory-id 108 action block
category pre-defined subcategory-id 177 action block
category pre-defined subcategory-id 251 action block
category pre-defined subcategory-id 109 action block
category pre-defined subcategory-id 110 action block
category pre-defined subcategory-id 111 action block
category pre-defined subcategory-id 112 action block
category pre-defined subcategory-id 114 action block
category pre-defined subcategory-id 115 action block
category pre-defined subcategory-id 117 action block
category pre-defined subcategory-id 178 action block
category pre-defined subcategory-id 179 action block
category pre-defined subcategory-id 180 action block
category pre-defined subcategory-id 181 action block
category pre-defined subcategory-id 248 action block
category pre-defined subcategory-id 118 action block
category pre-defined subcategory-id 119 action block
category pre-defined subcategory-id 122 action block
category pre-defined subcategory-id 182 action block
category pre-defined subcategory-id 183 action block
category pre-defined subcategory-id 184 action block
category pre-defined subcategory-id 123 action block
category pre-defined subcategory-id 124 action block
category pre-defined subcategory-id 186 action block
category pre-defined subcategory-id 187 action block
category pre-defined subcategory-id 188 action block
category pre-defined subcategory-id 189 action block
category pre-defined subcategory-id 125 action block
category pre-defined subcategory-id 127 action block
category pre-defined subcategory-id 128 action block
category pre-defined subcategory-id 130 action block
category pre-defined subcategory-id 131 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 142 action block
category pre-defined subcategory-id 143 action block
category pre-defined subcategory-id 144 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 145 action block
 category pre-defined subcategory-id 146 action block
 category pre-defined subcategory-id 147 action block
 category pre-defined subcategory-id 211 action block
 category pre-defined subcategory-id 212 action block
 category pre-defined subcategory-id 213 action block
 category pre-defined subcategory-id 240 action block
 category pre-defined subcategory-id 253 action block
 category pre-defined subcategory-id 149 action block
 category pre-defined subcategory-id 150 action block
 category pre-defined subcategory-id 214 action block
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
#
security-policy
 rule name policy_sec_huawei_com
  source-zone local
  destination-zone untrust
  service service_sec_huawei_com
  action permit
 rule name policy_sec_research
  description Security policy of web access protect for research.
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  time-range time_range
  profile url-filter profile_url_research
  action permit
 rule name policy_sec_marketing
  description Security policy of web access protect for marketing.
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  time-range time_range
```

 Copyright © Huawei Technologies Co., Ltd.

```
 profile url-filter profile_url_marketing
  action permit
#
return
```

13.8 Web: Example for Using the Blacklist and Whitelist to Control Website Access

Networking Requirements

As shown in **Figure 13-8**, DeviceA is deployed at the network border as the enterprise's gateway to implement URL filtering on HTTP requests.

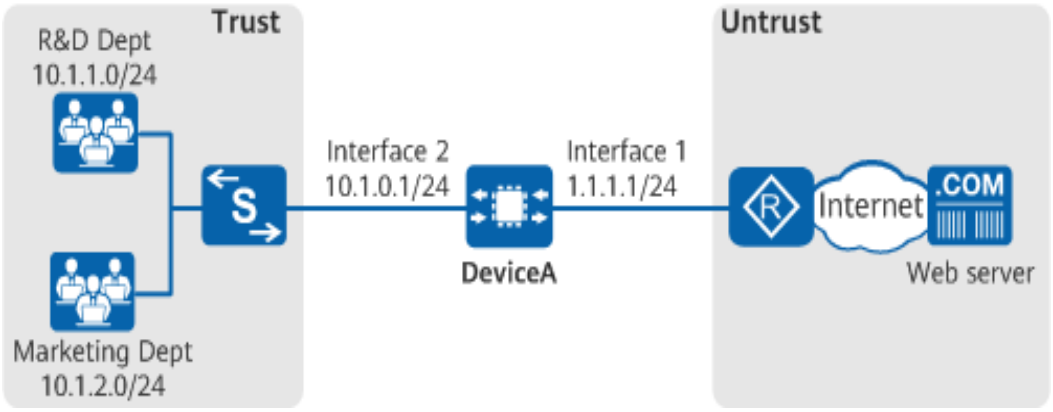
The enterprise has the following network access requirements for R&D and marketing employees:

- A URL whitelist is created for the R&D employees so that they can access only work-related URLs (www.example.com/working) and hosts (www.example.org) from 09:00 to 17:00 every day.
- A URL blacklist is created for the marketing employees so that they can access all URLs except the blacklisted URLs (www.example.net/*) from 09:00 to 17:00 every day.

Figure 13-8 Network diagram for blacklist- and whitelist-based website access control

NOTE

In this example, interface 1 and interface 2 stand for GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

1. Configure an IP address for each interface and add interfaces to security zones.
2. For R&D employees, create a URL filtering profile named **profile_url_research**, add whitelisted URLs (**www.example.com/working**) and hosts (**www.example.org**), and set the action to **Block** for all predefined categories and the default action to **Block** (if the remote query server is unavailable, the device will take the default action to control the access to non-whitelisted URLs).

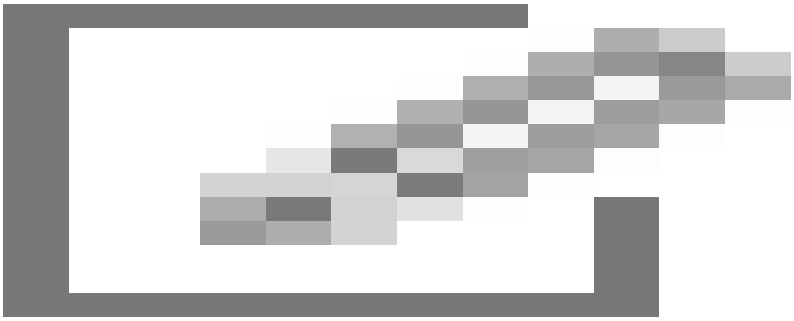
 Copyright © Huawei Technologies Co., Ltd.

3. For marketing employees, create a URL filtering profile named **profile_url_marketing**, add blacklisted URLs (**www.example.net/***), and set the action to **Allow** for all predefined categories and the default action to **Allow** (if the remote query server is unavailable, the device will take the default action to control the access to non-blacklisted URLs).
4. Configure two security policies, and reference the corresponding match criteria, such as the time range and URL filtering profile, in each security policy to control URL access from employees in different departments.

Procedure

Step 1 Configure an IP address for each interface and add interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click



corresponding to GE 0/0/2 and set the following parameters. After the configuration is complete, click **OK**.

Zone	trust
IPv4	
IP Address	10.1.0.1/24

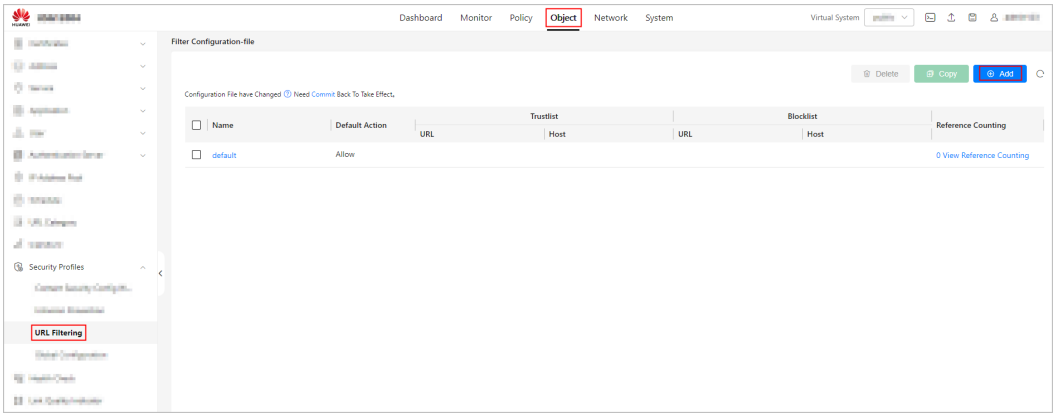
3. Repeat the preceding steps to configure GE 0/0/1.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

Step 2 Configure a URL filtering profile.

1. Choose **Object** > **Security Profiles** > **URL Filtering**.

 Copyright © Huawei Technologies Co., Ltd.



2. In **URL Filtering Profile List**, click **Add** and configure URL filtering profile **profile_url_research**. After the configuration is complete, click **OK**.

Name	profile_url_research
Default Action	Block
Whitelist URL	www.example.com/working
Whitelist Host	www.example.org
URL Filtering Level	If **User-defined** is selected, the action for all predefined categories is set to Block.

3. In **URL Filtering Profile List**, click **Add** and configure URL filtering profile profile_url_marketing as follows: After the configuration is complete, click **OK**.

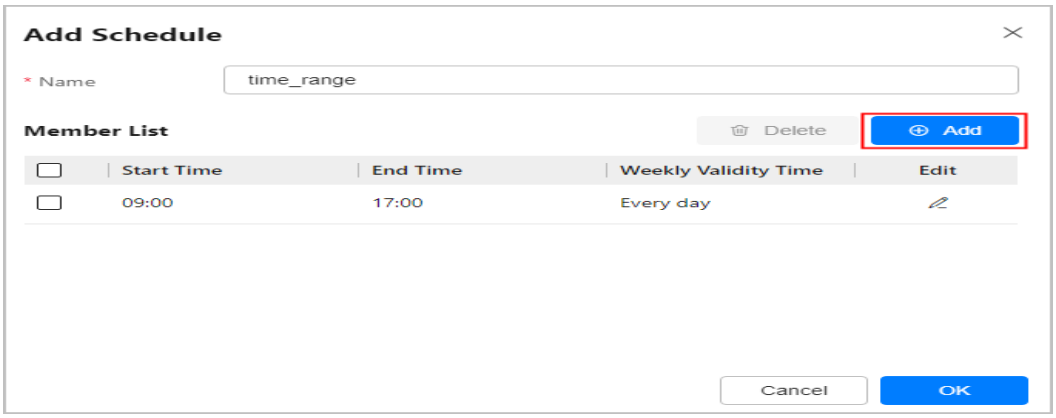
Name	profile_url_marketing
Default Action	Allow
Blacklist URL	www.example.net/*
URL Filtering Level	If **User-defined** is selected, the action for all predefined categories is set to **Allow**.

4. Click **Commit** in the upper right corner, and then click **OK** in the dialog box that appears.

Step 3 Configure a time range.

1. Choose **Object** > **Schedule**.
2. Click **Add** and enter a time range name.**time_range**

 Copyright © Huawei Technologies Co., Ltd.



3. In **Member List**, click **Add** and set the parameters as follows: After the configuration is complete, click **OK**.

Type	Periodic
Start Time	09:00
End Time	17:00
Weekly Validity Time	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday

Step 4 Configure a security policy and apply the URL filtering profile to the security policy.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy** and configure a URL access control policy for R&D employees. After the configuration is complete, click **OK**.

Name	policy_sec_research
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Schedule	time_range
Action	Permit
Content Security	
URL Filtering	profile_url_research

3. Repeat the preceding steps to configure a URL access control policy for marketing employees.

Name	policy_sec_marketing
Source Zone	trust

 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	untrust
Source Address	10.1.2.0/24
Schedule	time_range
Action	Permit
Content Security	
URL Filtering	profile_url_marketing

Step 5 Click **Save** in the upper right corner and click **OK** in the dialog box that is displayed.

----End

Verifying the Configuration

- R&D employees can access only **www.example.com/working** and **www.example.org** from 09:00 to 17:00 every day.

  Sample URLs that R&D employees can access:

  – www.example.com/working/index.htm
  – www.example.com/working/todo
  – www.example.org
  – www.example.org/network

- Marketing employees can access all websites, except **www.example.net/***, from 09:00 to 17:00.

  Sample URLs that marketing employees cannot access:

  – www.example.net
  – www.example.net/index.html
  – www.example.net/game

Configuration Scripts

```
#
 time-range time_range 09:00 to 17:00 daily
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
profile type url-filter name profile_url_research
 add whitelist url www.example.com/working
 add whitelist host www.example.org
 category pre-defined subcategory-id 101 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
category pre-defined subcategory-id 102 action block
category pre-defined subcategory-id 162 action block
category pre-defined subcategory-id 163 action block
category pre-defined subcategory-id 164 action block
category pre-defined subcategory-id 165 action block
category pre-defined subcategory-id 103 action block
category pre-defined subcategory-id 166 action block
category pre-defined subcategory-id 167 action block
category pre-defined subcategory-id 168 action block
category pre-defined subcategory-id 104 action block
category pre-defined subcategory-id 169 action block
category pre-defined subcategory-id 170 action block
category pre-defined subcategory-id 105 action block
category pre-defined subcategory-id 171 action block
category pre-defined subcategory-id 172 action block
category pre-defined subcategory-id 173 action block
category pre-defined subcategory-id 174 action block
category pre-defined subcategory-id 106 action block
category pre-defined subcategory-id 108 action block
category pre-defined subcategory-id 251 action block
category pre-defined subcategory-id 177 action block
category pre-defined subcategory-id 109 action block
category pre-defined subcategory-id 110 action block
category pre-defined subcategory-id 248 action block
category pre-defined subcategory-id 178 action block
category pre-defined subcategory-id 111 action block
category pre-defined subcategory-id 112 action block
category pre-defined subcategory-id 179 action block
category pre-defined subcategory-id 114 action block
category pre-defined subcategory-id 115 action block
category pre-defined subcategory-id 180 action block
category pre-defined subcategory-id 181 action block
category pre-defined subcategory-id 117 action block
category pre-defined subcategory-id 118 action block
category pre-defined subcategory-id 119 action block
category pre-defined subcategory-id 122 action block
category pre-defined subcategory-id 182 action block
category pre-defined subcategory-id 183 action block
category pre-defined subcategory-id 184 action block
category pre-defined subcategory-id 123 action block
category pre-defined subcategory-id 186 action block
category pre-defined subcategory-id 187 action block
category pre-defined subcategory-id 188 action block
category pre-defined subcategory-id 189 action block
category pre-defined subcategory-id 124 action block
category pre-defined subcategory-id 125 action block
category pre-defined subcategory-id 126 action block
category pre-defined subcategory-id 190 action block
category pre-defined subcategory-id 127 action block
category pre-defined subcategory-id 128 action block
category pre-defined subcategory-id 191 action block
category pre-defined subcategory-id 192 action block
category pre-defined subcategory-id 193 action block
category pre-defined subcategory-id 194 action block
category pre-defined subcategory-id 195 action block
category pre-defined subcategory-id 196 action block
category pre-defined subcategory-id 129 action block
category pre-defined subcategory-id 130 action block
category pre-defined subcategory-id 131 action block
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 204 action block
 category pre-defined subcategory-id 205 action block
 category pre-defined subcategory-id 134 action block
 category pre-defined subcategory-id 135 action block
 category pre-defined subcategory-id 136 action block
 category pre-defined subcategory-id 206 action block
 category pre-defined subcategory-id 207 action block
 category pre-defined subcategory-id 208 action block
 category pre-defined subcategory-id 137 action block
 category pre-defined subcategory-id 209 action block
 category pre-defined subcategory-id 210 action block
 category pre-defined subcategory-id 138 action block
 category pre-defined subcategory-id 139 action block
 category pre-defined subcategory-id 229 action block
 category pre-defined subcategory-id 140 action block
 category pre-defined subcategory-id 141 action block
 category pre-defined subcategory-id 142 action block
 category pre-defined subcategory-id 211 action block
 category pre-defined subcategory-id 212 action block
 category pre-defined subcategory-id 143 action block
 category pre-defined subcategory-id 144 action block
 category pre-defined subcategory-id 145 action block
 category pre-defined subcategory-id 240 action block
 category pre-defined subcategory-id 146 action block
 category pre-defined subcategory-id 213 action block
 category pre-defined subcategory-id 147 action block
 category pre-defined subcategory-id 253 action block
 category pre-defined subcategory-id 149 action block
 category pre-defined subcategory-id 150 action block
 category pre-defined subcategory-id 214 action block
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
 default action block
profile type url-filter name profile_url_marketing
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add blacklist url www.example.net/*
#
security-policy
 rule name policy_sec_research
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  time-range time_range
  profile url-filter profile_url_research
  action permit
 rule name policy_sec_marketing
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  time-range time_range
  profile url-filter profile_url_marketing
  action permit
```

13.9 CLI: Example for Using the Blacklist and Whitelist to Control Website Access

Networking Requirements

On the network shown in **Figure 13-9**, DeviceA is deployed as a gateway at the border of an enterprise network. This device is used to implement URL filtering on users' requests for Internet access.

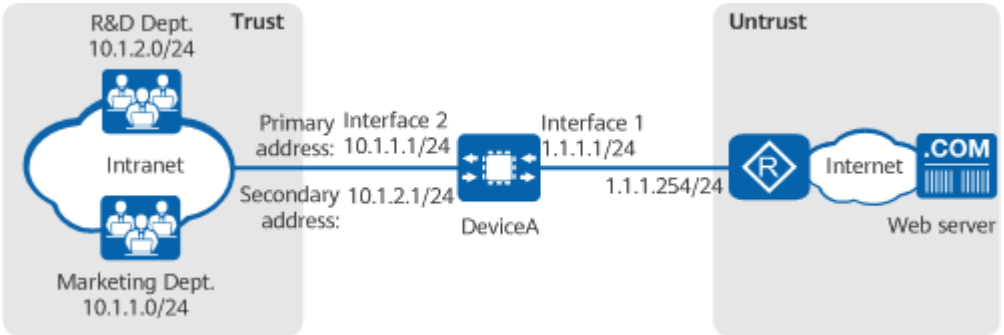
The enterprise has the following network access requirements for R&D and marketing employees:

- A URL whitelist needs to be created for the R&D employees, allowing them to access only work-related URLs (URLs starting with **www.example.com/working**) and URLs with the domain name being **www.example.org**. Access to all other URLs will be denied.
- A URL blacklist needs to be created for the marketing employees, allowing them to access all URLs except those starting with **www.example.net**.

Figure 13-9 Network diagram for using blacklist, and whitelist to control website access

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1, and GE0/0/2, respectively.



Configuration Roadmap

1. Configure an IP address for each interface and add interfaces to security zones.
2. For R&D employees, create a URL filtering profile named **profile_url_research**. Then, add a URL rule (www.example.com/working/*) and host rule (www.example.org) to the whitelist, set the block action for all predefined categories, and set the default action to block. In this case, the device will take the default action if a URL does not match the whitelist or predefined categories, thereby controlling the access to non-whitelisted URLs.
3. For marketing employees, create a URL filtering profile named **profile_url_marketing**. Then, add a URL rule (www.example.net*) to the blacklist, set the allow action for all predefined categories, and set the default action to allow. In this case, the device will take the default action if a URL does not match the blacklist or predefined categories, thereby controlling the access to non-blacklisted URLs.
4. Configure two security policies, and reference the corresponding URL filtering profile in each security policy to control URL access from employees in different departments.

Procedure

Step 1 Configure an IP address for each interface and add interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-GE0/0/2] ip address 10.1.2.1 255.255.255.0 sub
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure URL filtering profiles.

1. Configure a URL filtering profile for the R&D department.

```
[DeviceA] profile type url-filter name profile_url_research
[DeviceA-profile-url-filter-profile_url_research] default action block
[DeviceA-profile-url-filter-profile_url_research] category pre-defined action block
[DeviceA-profile-url-filter-profile_url_research] default action block
[DeviceA-profile-url-filter-profile_url_research] add whitelist url www.example.com/working/*
[DeviceA-profile-url-filter-profile_url_research] add whitelist host www.example.org
[DeviceA-profile-url-filter-profile_url_research] quit
```

2. Configure a URL filtering profile for the marketing department.

```
[DeviceA] profile type url-filter name profile_url_marketing
[DeviceA-profile-url-filter-profile_url_marketing] default action allow
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined action allow
[DeviceA-profile-url-filter-profile_url_marketing] add blacklist url www.example.net*
[DeviceA-profile-url-filter-profile_url_marketing] quit
```

Step 3 Reference the URL filtering profile in the security policy.

1. Configure a security policy for the R&D department.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_research
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy_sec_research] description Security policy of web access protect for research.
[DeviceA-policy-security-rule-policy_sec_research] source-zone trust
[DeviceA-policy-security-rule-policy_sec_research] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_research] source-address 10.1.2.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_research] action permit
[DeviceA-policy-security-rule-policy_sec_research] profile url-filter profile_url_research
[DeviceA-policy-security-rule-policy_sec_research] quit
```

2. Configure a security policy for the marketing department.

```
[DeviceA-policy-security] rule name policy_sec_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] description Security policy of web access protect for marketing.
[DeviceA-policy-security-rule-policy_sec_marketing] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing] source-address 10.1.1.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_marketing] action permit
[DeviceA-policy-security-rule-policy_sec_marketing] profile url-filter profile_url_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] quit
[DeviceA-policy-security] quit
```

Step 4 Commit the content security profiles.

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

----End

Verifying the Configuration

- All R&D employees can access only work-related URLs (URLs starting with **www.example.com/working**) and URLs with the domain name being **www.example.org**, but they cannot access other URLs. Sample URLs that R&D employees can access:
  - www.example.com/working/index.htm
  - www.example.com/working/todo
  - www.example.org
  - www.example.org/network

  If an R&D employee attempts to access other websites, the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Timeout or default action** or **Pre-defined**, and **Action** is **Block**.
- Requests from marketing employees to access URLs starting with **www.example.net** are denied, but they can access other URLs. Sample URLs that marketing employees cannot access:
  - www.example.net
  - www.example.net/index.html
  - www.example.net/game

  If a marketing employee attempts to access URLs starting with **www.example.net**, the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Blacklist** and **Action** is **Block**.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
 ip address 10.1.2.1 255.255.255.0 sub
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
profile type url-filter name profile_url_research
 add whitelist url www.example.com/working/*
 add whitelist host www.example.org
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 108 action block
 category pre-defined subcategory-id 251 action block
 category pre-defined subcategory-id 177 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
 category pre-defined subcategory-id 189 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 125 action block
 category pre-defined subcategory-id 126 action block
 category pre-defined subcategory-id 190 action block
 category pre-defined subcategory-id 127 action block
 category pre-defined subcategory-id 128 action block
 category pre-defined subcategory-id 191 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
category pre-defined subcategory-id 192 action block
category pre-defined subcategory-id 193 action block
category pre-defined subcategory-id 194 action block
category pre-defined subcategory-id 195 action block
category pre-defined subcategory-id 196 action block
category pre-defined subcategory-id 129 action block
category pre-defined subcategory-id 130 action block
category pre-defined subcategory-id 131 action block
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 142 action block
category pre-defined subcategory-id 211 action block
category pre-defined subcategory-id 212 action block
category pre-defined subcategory-id 143 action block
category pre-defined subcategory-id 144 action block
category pre-defined subcategory-id 145 action block
category pre-defined subcategory-id 240 action block
category pre-defined subcategory-id 146 action block
category pre-defined subcategory-id 213 action block
category pre-defined subcategory-id 147 action block
category pre-defined subcategory-id 253 action block
category pre-defined subcategory-id 149 action block
category pre-defined subcategory-id 150 action block
category pre-defined subcategory-id 214 action block
category pre-defined subcategory-id 215 action block
category pre-defined subcategory-id 216 action block
category pre-defined subcategory-id 217 action block
category pre-defined subcategory-id 218 action block
category pre-defined subcategory-id 219 action block
category pre-defined subcategory-id 220 action block
category pre-defined subcategory-id 221 action block
category pre-defined subcategory-id 222 action block
category pre-defined subcategory-id 223 action block
category pre-defined subcategory-id 252 action block
category pre-defined subcategory-id 151 action block
category pre-defined subcategory-id 230 action block
category pre-defined subcategory-id 152 action block
category pre-defined subcategory-id 238 action block
category pre-defined subcategory-id 153 action block
category pre-defined subcategory-id 154 action block
category pre-defined subcategory-id 155 action block
category pre-defined subcategory-id 224 action block
category pre-defined subcategory-id 225 action block
category pre-defined subcategory-id 156 action block
category pre-defined subcategory-id 157 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
 default action block
profile type url-filter name profile_url_marketing
 add blacklist url www.example.net*
#
security-policy
 rule name policy_sec_research
  description Security policy of web access protect for research.
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  profile url-filter profile_url_research
  action permit
 rule name policy_sec_marketing
  description Security policy of web access protect for marketing.
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  profile url-filter profile_url_marketing
  action permit
#
return
```

13.10 CLI: Example for Using URL Categories, Blacklist, and Whitelist to Control Website Access

Networking Requirements

On the network shown in **Figure 13-10**, DeviceA is deployed as a gateway at the border of an enterprise network. This device is used to implement URL filtering on users' requests for Internet access. The enterprise allows employees to access only education/science, search engine/portal, and social networking websites. In addition, the enterprise wants to control the following specific websites:

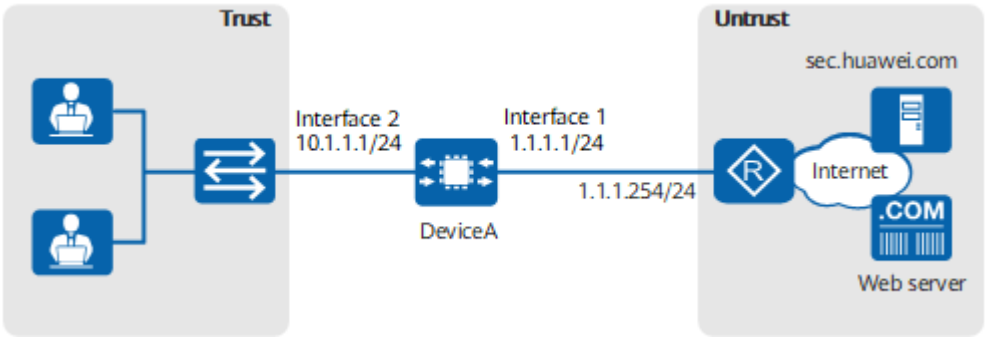
- Allow employees to access internal forum websites **www.example3.com** and **www.example4.com**.
- Deny access to the education/science website **www.example2.com** and social networking website **www.example1.com**.

Figure 13-10 Network diagram for using URL categories, blacklist, and whitelist to control website access

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1, and GE0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

1. Configure an IP address for each interface and add interfaces to security zones.
2. Create a URL filtering profile named **url_profile_01**. Then, add websites **www.example1.com** and **www.example2.com** to the blacklist, and add websites **www.example3.com** and **www.example4.com** to the whitelist. Set the allow action for the predefined URL categories education/science, search engine/portal, and social networking, and set the block action for other websites.
3. Configure a security policy and reference the **url_profile_01** profile to control URL access.

Procedure

Step 1 Configure an IP address for each interface and add interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Step 2 Configure a URL filtering profile.

NOTE

You can run the **display url-filter category pre-defined** command to query the mappings between the following predefined categories and IDs:

- 17: Education/Science
- 15: Search Engines/Portals
- 7: Social Network

```
[DeviceA] profile type url-filter name url_profile_01
[DeviceA-profile-url-filter-url_profile_01] add blacklist url www.example1.com
[DeviceA-profile-url-filter-url_profile_01] add blacklist url www.example2.com
[DeviceA-profile-url-filter-url_profile_01] add whitelist url www.example3.com
[DeviceA-profile-url-filter-url_profile_01] add whitelist url www.example4.com
[DeviceA-profile-url-filter-url_profile_01] category pre-defined action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-profile-url-filter-url_profile_01] category pre-defined category-id 15 action allow
[DeviceA-profile-url-filter-url_profile_01] category pre-defined category-id 17 action allow
[DeviceA-profile-url-filter-url_profile_01] category pre-defined category-id 7 action allow
[DeviceA-profile-url-filter-url_profile_01] quit
```

NOTE

To block non-whitelisted URLs, set the default action to block. If the remote query service is unavailable, DeviceA will take the default action.

To allow non-blacklisted URLs, set the default action to allow. If the remote query service is unavailable, DeviceA will take the default action.

Step 3 Reference the URL filtering profile in the security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_01
[DeviceA-policy-security-rule-policy_sec_01] source-zone trust
[DeviceA-policy-security-rule-policy_sec_01] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_01] source-address 10.1.1.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_01] action permit
[DeviceA-policy-security-rule-policy_sec_01] profile url-filter url_profile_01
[DeviceA-policy-security-rule-policy_sec_01] quit
[DeviceA-policy-security] quit
```

Step 4 Commit the content security profile.

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

----End

Verifying the Configuration

- Enterprise employees can access only URLs that belong to education/science, search engine/portal, and social networking categories.

  If an employee attempts to access other websites, the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Pre-defined** and **Action** is **Block**.

- Employees can access websites **www.example3.com** and **www.example4.com** but not websites **www.example1.com** and **www.example2.com**.

  If an employee attempts to access the website **www.example3.com** or **www.example4.com**, the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Whitelist** and **Action** is **Allow**.

  If an employee attempts to access the website **www.example1.com** or **www.example2.com**, the device generates a URL log (**URL/4/FILTER**), in which **Type** (indicates the filtering type) is **Blacklist** and **Action** is **Block**.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
profile type url-filter name url_profile_01
 add blacklist url www.example1.com
 add blacklist url www.example2.com
 add whitelist url www.example3.com
 add whitelist url www.example4.com
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
 category pre-defined subcategory-id 189 action block
 category pre-defined subcategory-id 125 action block
 category pre-defined subcategory-id 127 action block
 category pre-defined subcategory-id 128 action block
 category pre-defined subcategory-id 130 action block
 category pre-defined subcategory-id 131 action block
 category pre-defined subcategory-id 132 action block
 category pre-defined subcategory-id 197 action block
 category pre-defined subcategory-id 198 action block
 category pre-defined subcategory-id 199 action block
 category pre-defined subcategory-id 200 action block
 category pre-defined subcategory-id 227 action block
 category pre-defined subcategory-id 228 action block
 category pre-defined subcategory-id 133 action block
 category pre-defined subcategory-id 201 action block
 category pre-defined subcategory-id 202 action block
```

 Copyright © Huawei Technologies Co., Ltd.

```
 category pre-defined subcategory-id 204 action block
 category pre-defined subcategory-id 205 action block
 category pre-defined subcategory-id 134 action block
 category pre-defined subcategory-id 135 action block
 category pre-defined subcategory-id 136 action block
 category pre-defined subcategory-id 137 action block
 category pre-defined subcategory-id 138 action block
 category pre-defined subcategory-id 139 action block
 category pre-defined subcategory-id 140 action block
 category pre-defined subcategory-id 141 action block
 category pre-defined subcategory-id 206 action block
 category pre-defined subcategory-id 207 action block
 category pre-defined subcategory-id 208 action block
 category pre-defined subcategory-id 209 action block
 category pre-defined subcategory-id 210 action block
 category pre-defined subcategory-id 229 action block
 category pre-defined subcategory-id 142 action block
 category pre-defined subcategory-id 143 action block
 category pre-defined subcategory-id 144 action block
 category pre-defined subcategory-id 145 action block
 category pre-defined subcategory-id 146 action block
 category pre-defined subcategory-id 147 action block
 category pre-defined subcategory-id 211 action block
 category pre-defined subcategory-id 212 action block
 category pre-defined subcategory-id 213 action block
 category pre-defined subcategory-id 240 action block
 category pre-defined subcategory-id 253 action block
 category pre-defined subcategory-id 149 action block
 category pre-defined subcategory-id 150 action block
 category pre-defined subcategory-id 214 action block
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
#
security-policy
```

 Copyright © Huawei Technologies Co., Ltd.

```
rule name policy_sec_01
 source-zone trust
 destination-zone untrust
 source-address 10.1.1.0 mask 255.255.255.0
 profile url-filter url_profile_01
 action permit
```

13.11 Web: Example for Configuring Security Policies for Bypass Detection

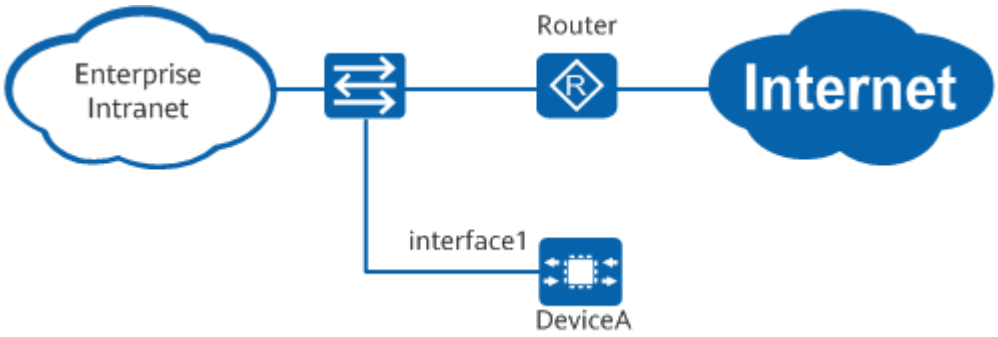
Networking Requirements

As shown in **Figure 13-11**, a router connects an intranet and the Internet. DeviceA functions as a bypass detection device to implement content security checks on the traffic that passes through the router.

NOTE

In this example, interface 1 represents GE0/0/1.

Figure 13-11 Networking diagram of bypass detection



Configuration Roadmap

1. When deviceA functions as a bypass detection device, set detection interface1 to a Layer-2 interface and connect this interface to a switch. The switch mirrors traffic to deviceA for detection.
2. Configure bypass detection on the detection interface so that deviceA only detects traffic.
3. Configure a security policy and reference an applicable security profile to implement content security checks on the traffic.
   - When deviceA has only one interface to receive mirroring traffic or has multiple interfaces to receive mirroring traffic but applies the same security policy to the traffic, you can add the interface or interfaces to any security zone and set the source and destination security zones to **any**.
   - When the deviceA has multiple interfaces to receive mirroring traffic and applies different security policies to the interfaces, you must add the interfaces to different security zones and set the source and destination security zones of each security policy to the security zone where the corresponding interface resides.

 Copyright © Huawei Technologies Co., Ltd.

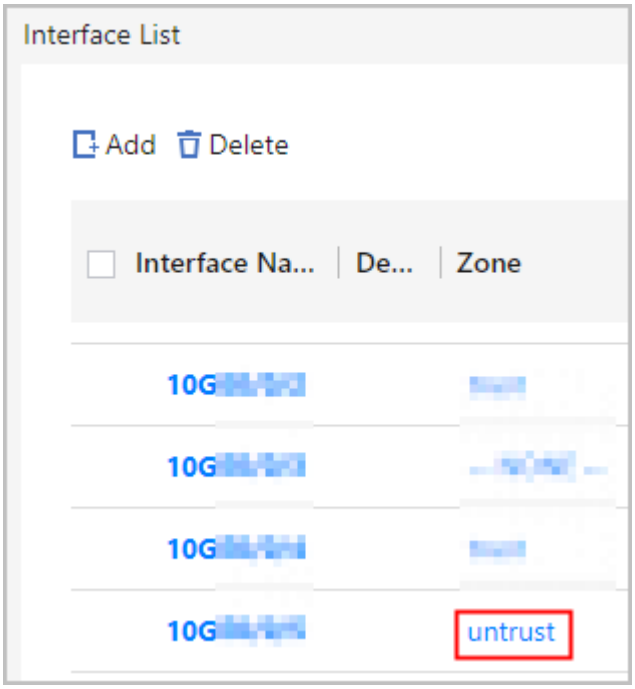
Procedure

Step 1 Configure the interface and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click of GE0/0/1 and set the following parameters:

Mode	Bypass
Connection Type	Trunk
Trunk VLAN ID	10

3. Click **OK**.
4. Set the security zone of GE0/0/1 to the Untrust zone.



5. Click **OK**.

Step 2 Configure a security policy for bypass detection.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**.
3. Set the parameters of the security policy for bypass detection.

Name	policy_sec_bypass_detection
Source Zone	untrust
Destination Zone	untrust
Action	Permit
Content Security	

 Copyright © Huawei Technologies Co., Ltd.

Antivirus	default
Intrusion Prevention	default
Record Policy Matching Log	Enable

NOTE

The antivirus and intrusion prevention profiles are used as examples. You can select other types of profiles as required.

4. Click **OK**.

----End

Configuration Scripts

```
#
vlan batch 1 10
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
 detect-mode tap
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sec_bypass_detection
  policy logging
  source-zone untrust
  destination-zone untrust
  profile av default
  profile ips default
  action permit
```

13.12 CLI: Example for Configuring Security Policies for Bypass Detection

Networking Requirements

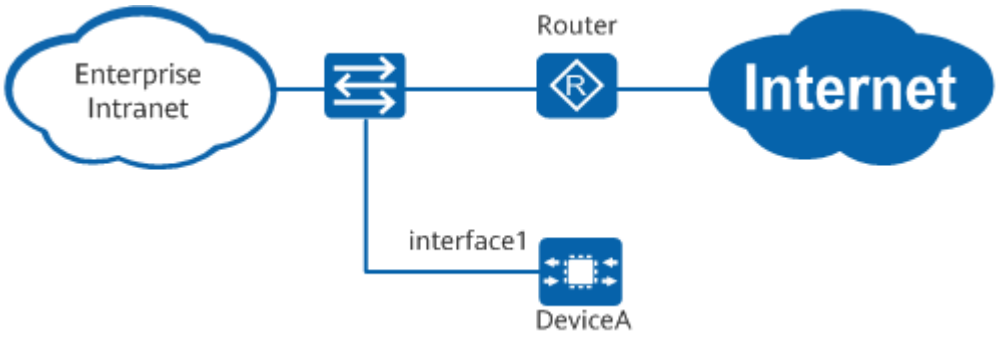
As shown in **Figure 13-12**, a router connects an intranet and the Internet. DeviceA functions as a bypass detection device to implement content security checks on the traffic that passes through the router.

NOTE

In this example, interface 1 represents GE0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

Figure 13-12 Networking diagram of bypass detection



Configuration Roadmap

1. When deviceA functions as a bypass detection device, set detection interface1 to a Layer-2 interface and connect this interface to a switch. The switch mirrors traffic to deviceA for detection.
2. Configure bypass detection on the detection interface so that deviceA only detects traffic.
3. Configure a security policy and reference an applicable security profile to implement content security checks on the traffic.
   - When deviceA has only one interface to receive mirroring traffic or has multiple interfaces to receive mirroring traffic but applies the same security policy to the traffic, you can add the interface or interfaces to any security zone and set the source and destination security zones to **any**.
   - When the deviceA has multiple interfaces to receive mirroring traffic and applies different security policies to the interfaces, you must add the interfaces to different security zones and set the source and destination security zones of each security policy to the security zone where the corresponding interface resides.

Procedure

Step 1 Configure the interface and assign the interfaces to security zones.

NOTE

For the traffic that carries a VLAN tag, you need to run the **port trunk allow-pass vlan** command on the Layer-2 interface and also create the corresponding VLAN on the deviceA.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] portswitch
[DeviceA-GE0/0/1] port link-type trunk
[DeviceA-GE0/0/1] port trunk allow-pass vlan 10
[DeviceA-GE0/0/1] detect-mode tap
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy for bypass detection.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_bypass_detection
[DeviceA-policy-security-rule-policy_sec_bypass_detection] source-zone untrust
[DeviceA-policy-security-rule-policy_sec_bypass_detection] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_bypass_detection] action permit
[DeviceA-policy-security-rule-policy_sec_bypass_detection] profile av default
[DeviceA-policy-security-rule-policy_sec_bypass_detection] profile ips default
[DeviceA-policy-security-rule-policy_sec_bypass_detection] policy logging
```

NOTE

The antivirus and intrusion prevention profiles are used as examples. You can select other types of profiles as required.

----End

Configuration Scripts

```
#
sysname DeviceA
#
vlan batch 1 10
#
interface GE0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
 detect-mode tap
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
security-policy
 rule name policy_sec_bypass_detection
  policy logging
  source-zone untrust
  destination-zone untrust
  profile av default
  profile ips default
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

14 Security Protection

14.1 CLI: Example for Configuring FTP ASPF
14.2 Web: Example for Configuring SIP ALG
14.3 CLI: Example for Configuring SIP ALG
14.4 Web: Examples for DDoS Attack Defense
14.5 CLI: Example for DDoS Attack Defense
14.6 CLI: Examples for Dynamic Traffic Limiting for Defense Against Traffic Attacks
14.7 CLI: Example for Configuring Per-IP New Connection Rate Limiting and New Session Rate Limiting

14.1 CLI: Example for Configuring FTP ASPF

Networking Requirements

DeviceA is deployed at the egress of an enterprise that provides the FTP service.

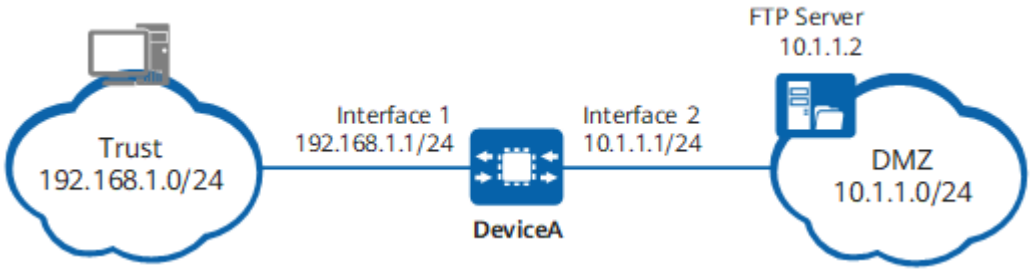
To enable intranet users to access the FTP server, in addition to configuring a security policy to allow the establishment of a control connection between the intranet users and FTP server, you need also to enable ASPF for FTP in the interzone to ensure that a data connection can be successfully established between the intranet users and FTP server.

Figure 14-1 shows the networking diagram.

Figure 14-1 Networking diagram of configuring ASPF

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2 respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
GE0/0/1	IP address: 192.168.1.1 Security zone: Trust	This interface is connected to the PCs of employees and resides on the same network segment as these PCs.
GE0/0/2	IP address: 10.1.1.1 Security zone: DMZ	This interface is connected to the server and resides on the same network segment as the server.
User address range	192.168.1.0/24	The IP addresses of the PCs of all employees are classified into the network segment and deployed in the Trust zone.
FTP server	10.1.1.2/24	FTP server is deployed in the DMZ.

Configuration Roadmap

1. Set an IP address for each interface, assign interfaces to security zones, and complete basic parameter settings.
2. Configure a security policy to allow intranet users to access the FTP server.
3. Configure ASPF to properly forward FTP packets.

Procedure

Step 1 Set the IP addresses of interfaces and assign the interfaces to corresponding security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 192.168.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy to allow intranet users to access the FTP server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_ftp
[DeviceA-policy-security-rule-policy_sec_ftp] source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy_sec_ftp] source-address 192.168.1.0 24
[DeviceA-policy-security-rule-policy_sec_ftp] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_ftp] destination-address 10.1.1.2 32
[DeviceA-policy-security-rule-policy_sec_ftp] service protocol tcp destination-port 21
[DeviceA-policy-security-rule-policy_sec_ftp] action permit
[DeviceA-policy-security-rule-policy_sec_ftp] quit
```

NOTE

To protect the FTP server, you are advised to configure refined matching conditions in the security policy to allow intranet users to access only port 21 on the FTP server. In this example, the FTP server uses the well-known port (TCP 21) to provide FTP services.

Step 3 Run the **detect ftp** command in the interzone to realize the normal forwarding of FTP packets.

```
[DeviceA] firewall interzone trust dmz
[DeviceA-interzone-trust-dmz] detect ftp
[DeviceA-interzone-trust-dmz] quit
```

----End

Verifying the Configuration

- Intranet users successfully access the FTP server.
- Run the **display firewall session table** command on DeviceA to check the session table.

```
<DeviceA> display firewall session table
Current Total Sessions : 2
  ftp  VPN:public --> public 192.168.1.2:2051+->10.1.1.2:21
  ftp-data  VPN:public --> public 10.1.1.2:20-->192.168.1.2:2052
```

Configuration Scripts

The following lists the related scripts of this configuration example.

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
 firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name policy_sec_ftp
  source-zone trust
  destination-zone dmz
  source-address 192.168.1.0 24
  destination-address 10.1.1.2 32
  service protocol tcp destination-port 21
  action permit
#
firewall interzone trust dmz
```

 Copyright © Huawei Technologies Co., Ltd.

```
 detect ftp
#
return
```

14.2 Web: Example for Configuring SIP ALG

Networking Requirements

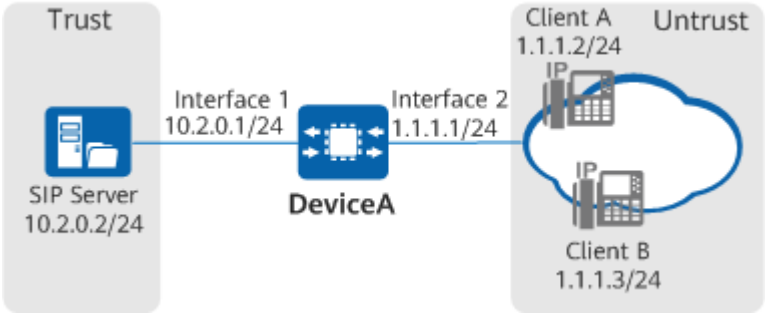
As shown in **Figure 14-2**, a SIP server is deployed on the enterprise intranet. When going online, each SIP client needs to send a register message to the SIP servers. The register messages are carried through SIP.

DeviceA is deployed between the SIP clients and SIP server to implement NAT ALG.

Figure 14-2 Networking diagram for configuring ISP over TLS ALG

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.2.0.1 Security zone: Trust	This interface is connected to the server and resides on the same network segment as the server.
GE0/0/2	IP address: 1.1.1.1 Security zone: Untrust	This interface is connected to the clients and resides on the same network segment as the clients.
SIP server	10.2.0.2/24	Deploy the server in the Trust.

Configuration Roadmap

1. Configure IP addresses for interfaces and assign the interfaces to security zones.

 Copyright © Huawei Technologies Co., Ltd.

2. Configure a security policy for communication between SIP clients and the SIP server.
3. Configure destination NAT so that the intranet SIP server can provide services externally (public address: 1.1.1.10).
4. Configure ALG to properly forward SIP messages.

Procedure

Step 1 Assign IP addresses to interfaces, and add the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click for the GE0/0/1.

   Set parameters of GE0/0/1 as follows. Keep default values for other parameters.

Zone	trust
Mode	Route
IPv4	
Connection Type	Static IP
IP Address	10.2.0.1/255.255.255.0

3. Repeat the previous operation and set interface parameters for GE0/0/2.

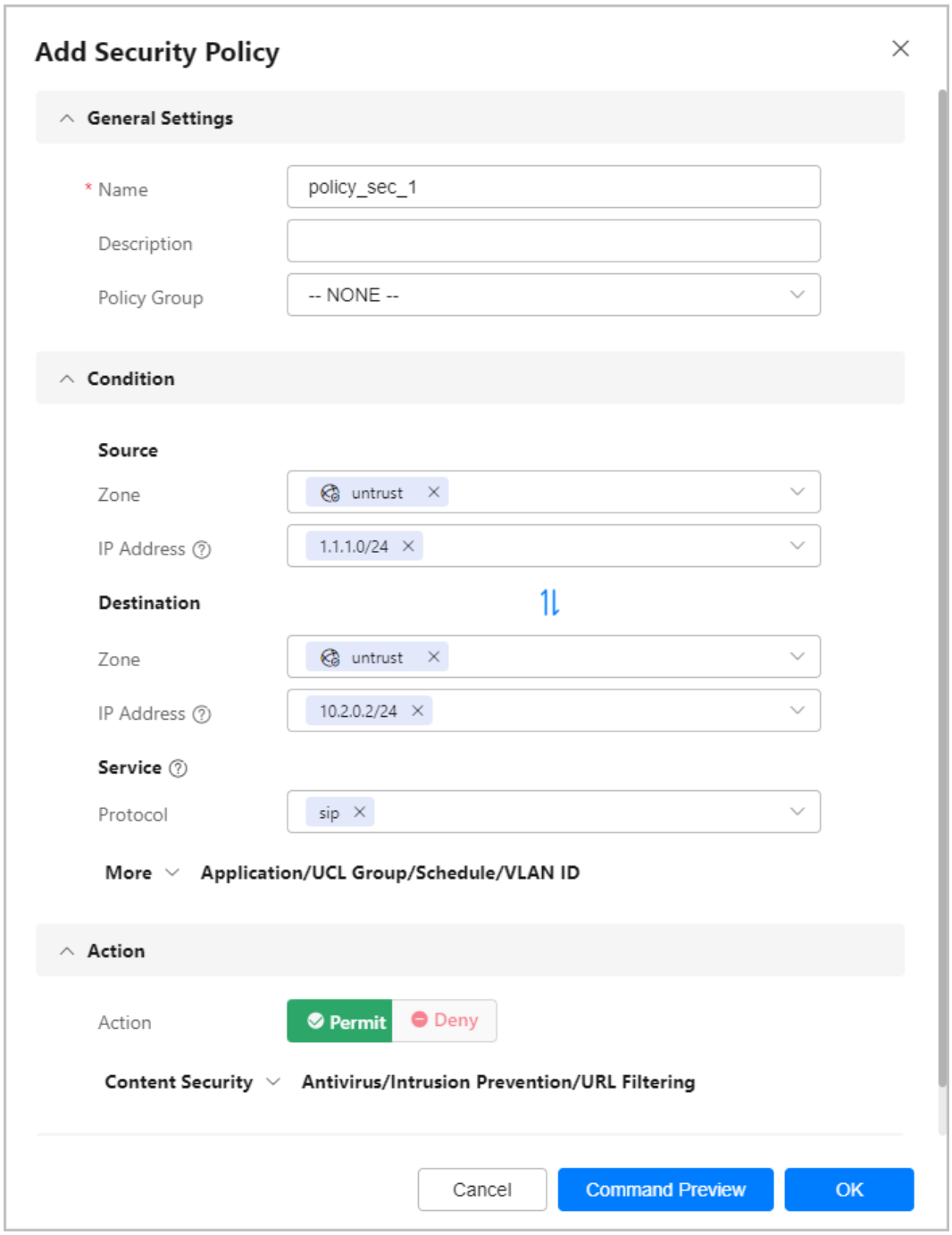
   Set parameters of as follows. Keep default values for other parameters.

Zone	untrust
Mode	Route
IPv4	
Connection Type	Static IP
IP Address	1.1.1.1/255.255.255.0

Step 2 Configure a security policy to allow SIP clients to send messages to the SIP server.

Choose **Policy** > **Security Policy** > **Security Policy**, click **Add Security Policy**.

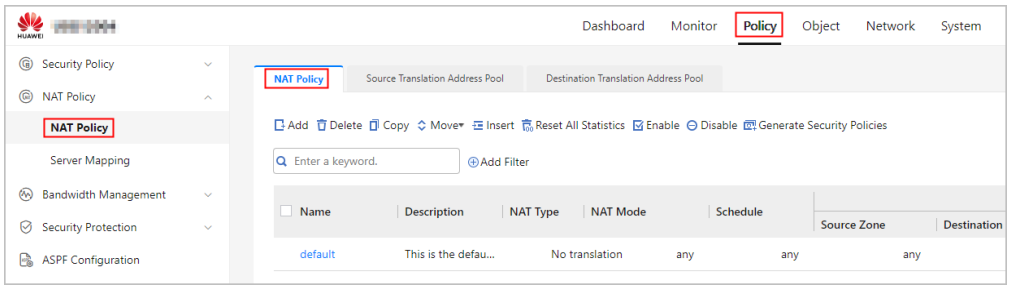
 Copyright © Huawei Technologies Co., Ltd.



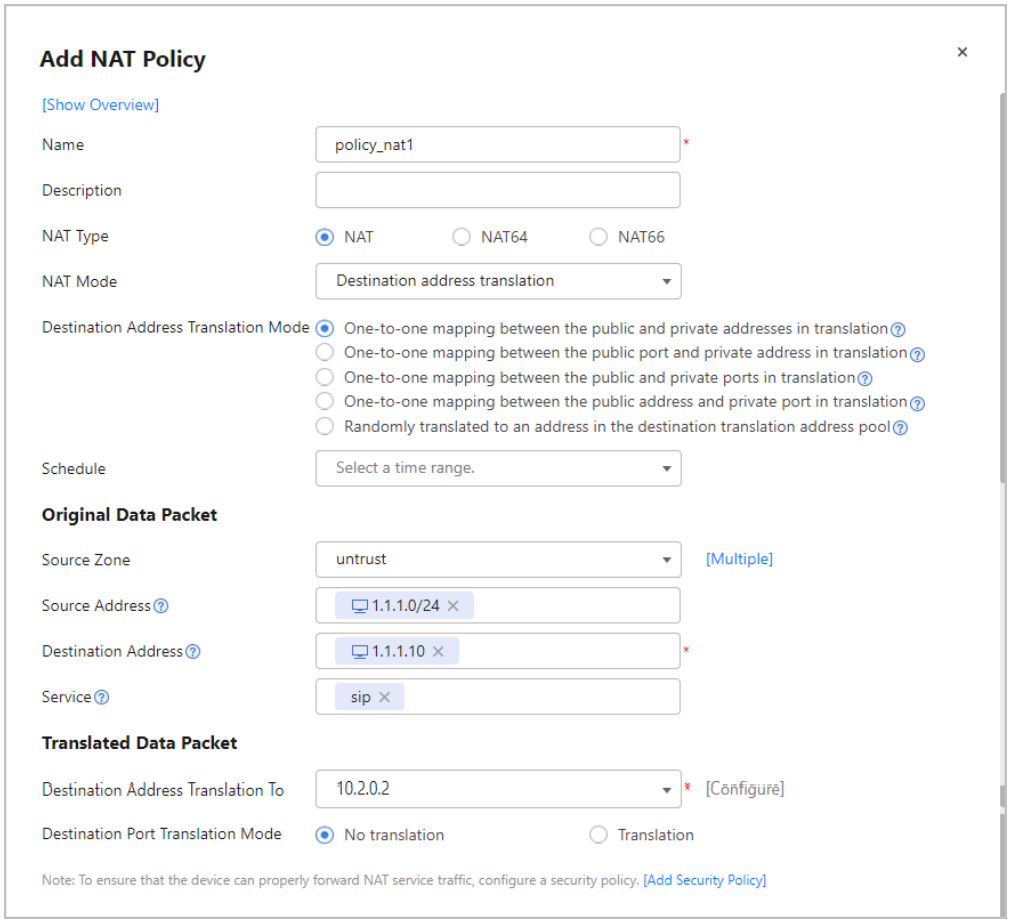
Step 3 Configure destination NAT so that the intranet SIP server can provide services externally.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.

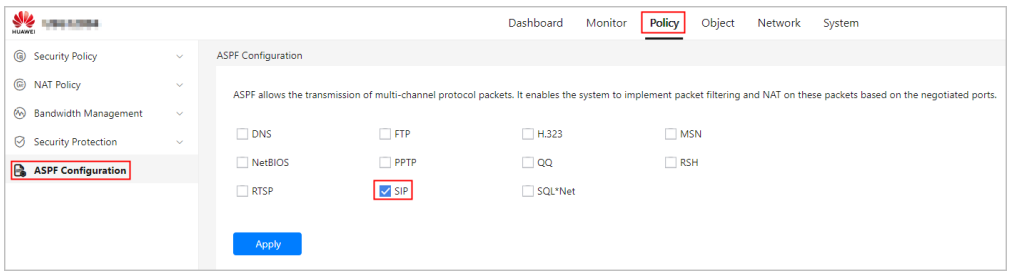


2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.



Step 4 Configure ALG to properly forward SIP messages.

1. Choose **Policy** > **ASPF Configuration**.



2. Select **SIP**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verification

- Client A and Client B register successfully on the server.
- Run the **display firewall session table** command on DeviceA to check the session table.

```
Current Total Sessions : 2
 sip VPN:public --> public 1.1.1.2:2107+ ->1.1.1.10:5060[10.2.0.2:5060]
 sip VPN:public --> public 1.1.1.3:4936+ ->1.1.1.10:5060[10.2.0.2:5060]
```

Configuration Scripts

The following lists the related script of this configuration example.

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall detect sip
#
security-policy
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 10.2.0.2 mask 255.255.255.255
  service sip
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone untrust
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 1.1.1.10 mask 255.255.255.255
  service sip
  action destination-nat static address-to-address address 10.2.0.2
#
return
```

14.3 CLI: Example for Configuring SIP ALG

Networking Requirements

As shown in **Figure 14-3**, a SIP server is deployed on the enterprise intranet. When going online, each SIP client needs to send a register message to the SIP servers. The register messages are carried through SIP.

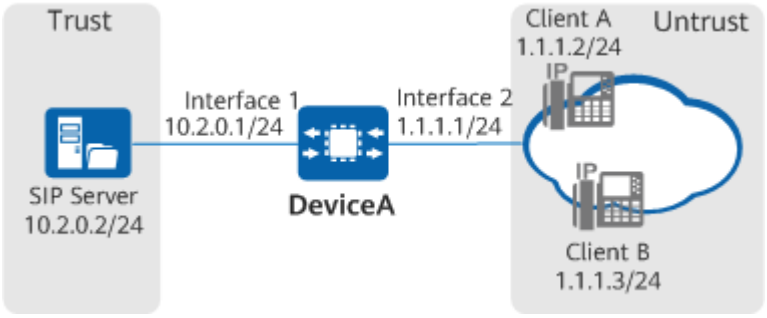
DeviceA is deployed between the SIP clients and SIP server to encrypt SIP messages and implement NAT ALG.

 Copyright © Huawei Technologies Co., Ltd.

Figure 14-3 Networking diagram for configuring SIP over TLS ALG

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.2.0.1 Security zone: Trust	This interface is connected to the server and resides on the same network segment as the server.
GE0/0/2	IP address: 1.1.1.1 Security zone: Untrust	This interface is connected to the clients and resides on the same network segment as the clients.
SIP server	10.2.0.2/24	Deploy the server in the DMZ.

Configuration Roadmap

1. Configure IP addresses for interfaces and assign the interfaces to security zones.
2. Configure a security policy for communication between SIP clients and the SIP server.
3. Configure destination NAT so that the intranet SIP server can provide services externally (public address: 1.1.1.10).
4. Configure ALG to properly forward SIP messages.

Procedure

Step 1 Configure IP addresses for interfaces and assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.2.0.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow SIP clients to send messages to the SIP server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec1
[Device-policy-security-rule-policy_sec1] source-zone untrust
[DeviceA-policy-security-rule-policy_sec1] destination-zone trust
[DeviceA-policy-security-rule-policy_sec1] source-address 1.1.1.0 24
[DeviceA-policy-security-rule-policy_sec1] destination-address 10.2.0.2 32
[DeviceA-policy-security-rule-policy_sec1] service sip
[DeviceA-policy-security-rule-policy_sec1] action permit
[DeviceA-policy-security-rule-policy_sec1] quit
```

Step 3 Configure destination NAT so that the intranet SIP server can provide services externally (public address: 1.1.1.10).

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone trust
[DeviceA-policy-nat-rule-policy_nat1] service sip
[DeviceA-policy-nat-rule-policy_nat1] destination-address 1.1.1.10 32
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static address-to-address address 10.2.0.2
5060
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 4 Configure ALG to properly forward SIP messages.

```
[DeviceA] firewall interzone trust untrust
[DeviceA-interzone-trust-untrust] detect sip
[DeviceA-interzone-trust-untrust] quit
```

----End

Verification

- Client A and Client B register successfully on the server.
- Run the **display firewall session table** command on DeviceA to check the session table.

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 sip VPN:public --> public 1.1.1.2:2107+ ->1.1.1.10:5060[10.2.0.2:5060]
 sip VPN:public --> public 1.1.1.3:4936+ ->1.1.1.10:5060[10.2.0.2:5060]
```

Configuration Scripts

The following lists the related script of this configuration example.

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 85
 add interface GE0/0/1
#
 firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall interzone trust untrust
 detect sip
#
security-policy
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 10.2.0.2 mask 255.255.255.255
  service sip
  action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-zone trust
    destination-address 1.1.1.10 mask 255.255.255.255
    service sip
    action destination-nat static address-to-address address 10.2.0.2 5060
#
return
```

14.4 Web: Examples for DDoS Attack Defense

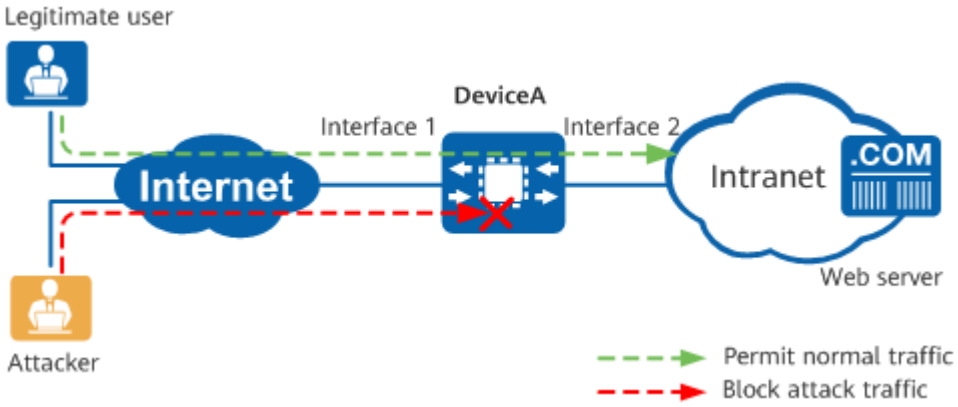
Networking Requirements

In Figure 14-4, a device is deployed at the egress of an enterprise intranet, and a web server, which is vulnerable to SYN flood and HTTP flood attacks, is deployed on the enterprise intranet. To ensure the proper running of the web server, enable the anti-DDoS function on the device to defend against the preceding types of DDoS attacks.

Figure 14-4 Anti-DDoS networking diagram

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



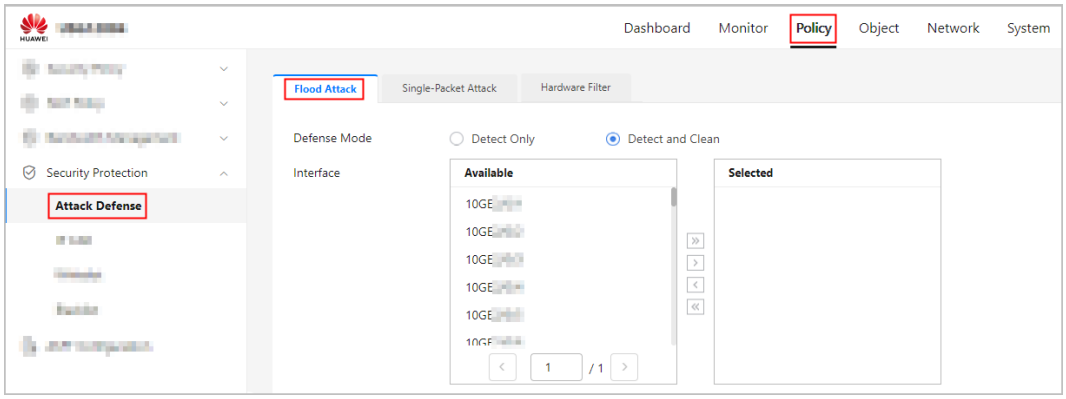
 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Enable the traffic statistics collection function on the interface GE0/0/1 that connects the device to the external network, so that the device can collect statistics on traffic from the external network to the intranet.
2. Enable the threshold learning function on the device so that proper thresholds can be configured for defense against DDoS attacks. To streamline configuration, enable automatic application of threshold learning results.
3. Enable SYN flood and HTTP flood attack defense on the device. Retain the default thresholds for defense against various types of attacks. After threshold learning is complete, the device will automatically apply the threshold learning results.

Procedure

Step 1 Choose **Policy** > **Security Protection** > **Attack Defense** > **Flood Attack**.



Step 2 Double-click GE0/0/1 in **Available** of **Interface** to add GE0/0/1 to the list in **Selected**, so that traffic statistics is enabled on GE0/0/1.

Step 3 Select **Custom** in **Protected Destination IP** and configure the protected IP address to the IP address of the web server, for example, 10.2.1.1/32.

Step 4 Click **Set Learning Parameters** on the **Defense Configuration** tab to configure threshold learning parameters.

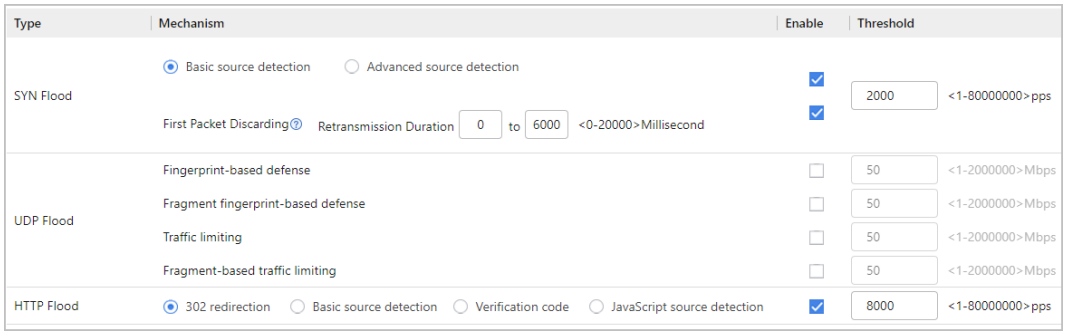
Learning	Enable
Learning Duration	7 day
Learning mode	One-off Learning
Automatic application	Enable
Learning Tolerance	100

Step 5 Select **Enable** next to type of attacks to be defended on the **Defense Configuration** page. Do not change the default threshold for each defense function.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

During threshold learning, **Learning Status** is **Learning**. After the learning process is complete, the device automatically applies the learning result.



Step 6 Click **Apply**.

Step 7 Click **Save** on the upper right of the interface and click **OK** in the dialog box that is displayed.

----End

Verifying the Configuration

After the configuration is complete, the FW logs detected attacks and outputs threat reports. Choose **Monitor** > **Log** > **Threat Log** to view threat logs.

Configuration Scripts

The following lists only the scripts related to this configuration example.

```
#
sysname DeviceA
#
interface GE0/0/1
 anti-ddos flow-statistic enable
#
anti-ddos syn-flood source-detect
anti-ddos first-packet-check syn
anti-ddos http-flood source-detect mode redirect
anti-ddos baseline-learn start
anti-ddos baseline-learn apply
anti-ddos baseline-learn learn-duration 10080
anti-ddos baseline-learn tolerance-value 100
#
anti-ddos ip user-defined enable
anti-ddos ip address 10.2.1.1 32
#
return
```

14.5 CLI: Example for DDoS Attack Defense

Networking Requirements

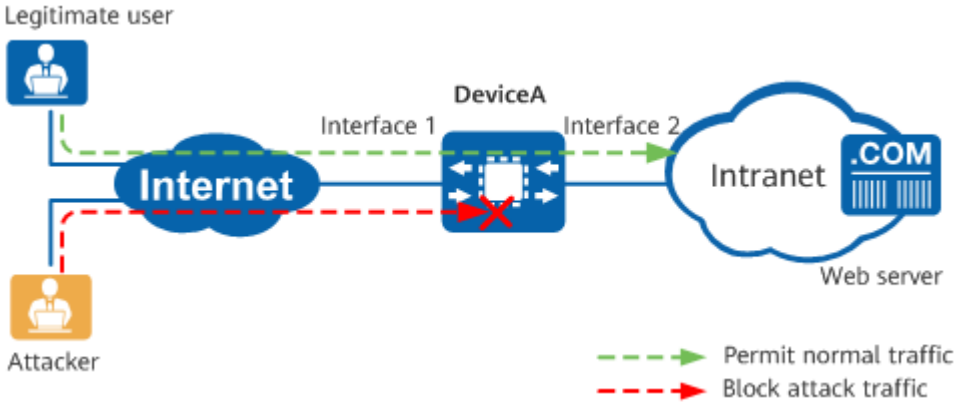
In **Figure 1**, a device is deployed at the egress of an enterprise intranet, and a web server, which is vulnerable to SYN flood and HTTP flood attacks, is deployed on the enterprise intranet. To ensure the proper running of the web server, enable the anti-DDoS function on the device to defend against the preceding DDoS attacks.

 Copyright © Huawei Technologies Co., Ltd.

Figure 14-5 Network diagram of DDoS attack mitigation

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Configuration Roadmap

1. Enable the traffic statistics collection function on GE 0/0/1 connecting the device to the extranet (that is, bind this function to GE 0/0/1) to collect statistics on the traffic from the extranet to the intranet.
2. Enable the threshold learning function on the device so that proper thresholds can be configured for defense against DDoS attacks. For the convenience of configuration, enable the automatic application function.
3. Enable SYN flood and HTTP flood attack defense on the device. Retain the default thresholds for defense against various types of attacks. After threshold learning is complete, the device will automatically apply the threshold learning results.

Procedure

Step 1 Configure attack defense parameters.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] anti-ddos flow-statistic enable
[DeviceA-GE0/0/1] quit
[DeviceA] ddos-mode detect-clean
[DeviceA] anti-ddos ip user-defined enable
[DeviceA] anti-ddos ip address 10.2.1.1 32    //IP address of the web server
```

Step 2 Configure the threshold learning function.

```
[DeviceA] anti-ddos baseline-learn start
[DeviceA] anti-ddos baseline-learn learn-duration 10080
[DeviceA] anti-ddos baseline-learn tolerance-value 100
[DeviceA] anti-ddos baseline-learn apply
```

Step 3 Enable the attack defense function.

```
[DeviceA] anti-ddos syn-flood source-detect
[DeviceA] anti-ddos first-packet-check syn
[DeviceA] anti-ddos http-flood source-detect mode redirect
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

For details, see Maintaining Attack Defense.

Configuration Scripts

The following lists only the scripts related to this configuration example.

```
#
 sysname DeviceA
#
interface GE0/0/1
 anti-ddos flow-statistic enable
#
 anti-ddos syn-flood source-detect
 anti-ddos first-packet-check syn
 anti-ddos http-flood source-detect mode redirect
 anti-ddos baseline-learn tolerance-value 100
 anti-ddos baseline-learn learn-duration 10080
 anti-ddos baseline-learn start
 anti-ddos baseline-learn apply
#
anti-ddos ip user-defined enable
anti-ddos ip address 10.2.1.1 32
#
return
```

14.6 CLI: Examples for Dynamic Traffic Limiting for Defense Against Traffic Attacks

Networking Requirements

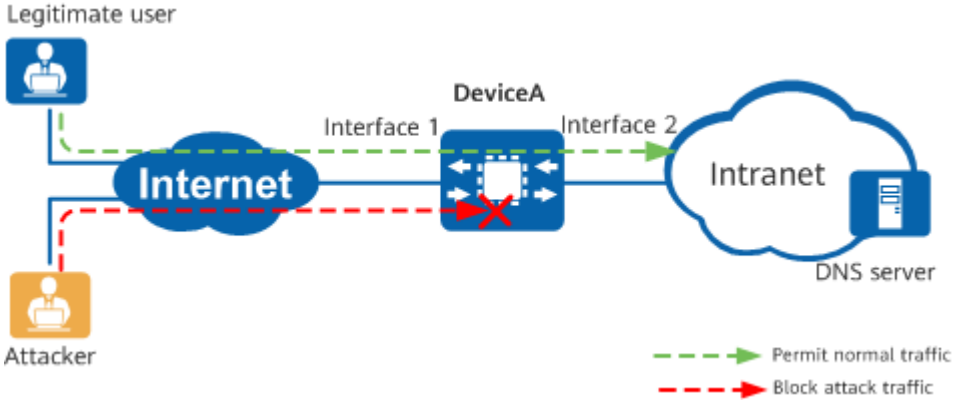
In **Figure 1**, a device is deployed at the egress of an enterprise intranet, and a DNS server is deployed on the enterprise intranet. Frequent traffic attacks are detected on the DNS server, and sessions can be established for attack traffic. Despite there being only a small amount of attack traffic, each flow is transmitted at a high rate.

To ensure normal operation of the DNS server and reduce any adverse impact on services, enable dynamic traffic limiting against traffic attacks.

Figure 14-6 Network diagram of dynamic traffic limiting against traffic attacks

NOTE

In this example, interface 1 and interface 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

As this example assumes that you have completed basic network configurations, only the configuration of dynamic traffic limiting against traffic attacks is described.

1. Enable dynamic traffic limiting against traffic attacks.
2. Configure the CAR for triggering traffic limiting.
3. Configure dynamic traffic limiting against session-based traffic attacks.
4. **Optional:**

   Configure the aging time for automatically delivered dynamic rules.

   You are advised to use the default aging time (30 minutes). If the attack traffic lasts longer than 30 minutes, set the dynamic rule aging time to a larger value than the attack traffic duration.

Procedure

Step 1 Enable dynamic traffic limiting against traffic attacks.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
<DeviceA> system-view
[DeviceA] anti-ddos auto-defend traffic-policy enable
```

Step 2 Configure the CAR for triggering the defense against traffic attacks to 50 Mbit/s.

You can observe the rate of normal service traffic for a certain period of time, and then configure the CAR based on your site requirements.

```
[DeviceA] anti-ddos auto-defend car 50000
```

Step 3 Enable dynamic traffic limiting against session-based traffic attacks and configure the alarm threshold and maximum threshold for the rate of session packets.

You can observe the maximum rate of normal service traffic for a certain period of time during peak hours. You are advised to set the maximum threshold for triggering dynamic traffic limiting to 2 to 3 times the maximum traffic rate.

You are advised to retain the default values of the alarm threshold and maximum threshold, which are 100000 pps and 200000 pps, respectively. Typically, the default values can meet most application scenarios.

```
[DeviceA] anti-ddos auto-defend base-session enable
[DeviceA] anti-ddos auto-defend base-session alert-rate 100000 max-rate 200000
```

Step 4 **Optional:** Configure the aging time for automatically delivered dynamic rules.

In most situations, you are advised to use the default aging time (30 minutes). Attack traffic may last a long period of time, in which case dynamic rules may age out before the attack traffic ends. To prevent this, configure a longer aging time for dynamic rules.

```
[DeviceA] anti-ddos auto-defend rule aging-time 30
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

If traffic attacks occur and the attack traffic rate reaches the pre-configured maximum threshold:

- Run the **display anti-ddos auto-defend car-information** command in the diagnostic view to view the automatically delivered dynamic rules.
- The following dynamic traffic limiting entry can be found in the logs: **FWD/4/DDOSCARBEGIN**.

Configuration Scripts

The following lists only the scripts related to this configuration example.

```
#
 sysname DeviceA
#
anti-ddos auto-defend traffic-policy enable
anti-ddos auto-defend car 50000
anti-ddos auto-defend base-session enable
anti-ddos auto-defend base-session alert-rate 100000 max-rate 200000
#
return
```

14.7 CLI: Example for Configuring Per-IP New Connection Rate Limiting and New Session Rate Limiting

Networking Requirements

DeviceA serves as the security gateway at the border of an enterprise network. The intranet (LAN) PCs access the Internet (WAN) through the public IP addresses in the address pool. The enterprise applies to the carrier for two public IP addresses (1.1.1.10 and 1.1.1.11) for address translation. **Figure 14-7** shows the networking diagram.

If malicious attackers continuously initiate a large number of new connections to the Internet using intranet PCs, a large number of performance resources of DeviceA are consumed, which may cause service faults. Therefore, you need to configure new connection rate limiting based on the source IP address on the LAN interface of DeviceA. In addition, the public IP address may be used by malicious attackers from external networks. These malicious attackers continuously initiate a large number of new connections to the public IP address, occupying a large number of DeviceA's performance resources and causing other service exceptions. Therefore, you also need to configure new connection rate limiting based on the destination IP address on the WAN interface of DeviceA.

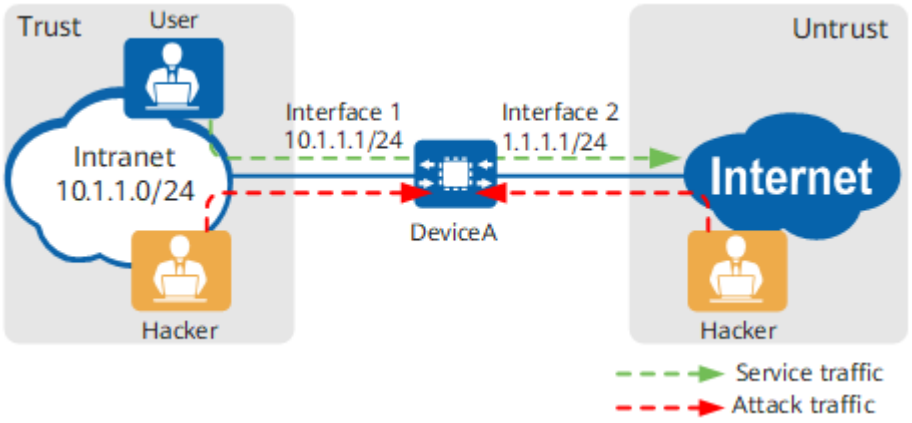
To ensure that the device can process packets of existing sessions when the CPU usage is high, you need to enable new session rate limiting. When the CPU usage reaches a certain threshold, the device limits the new session rate to ensure normal services.

 Copyright © Huawei Technologies Co., Ltd.

Figure 14-7 Networking diagram of LAN and WAN protection

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: Trust	Configure 10.1.1.1 as the default gateway for intranet PCs.
GE0/0/2	IP address: 1.1.1.1/24 Security zone: Untrust	-
Post-NAT public addresses	1.1.1.10-1.1.1.11	As the number of private addresses is greater than public addresses, one-to-one mapping is impossible. Port translation must be enabled to allow the reuse of public addresses. A black-hole route must be configured for the public address pool.
New connection rate for an IP address	Source IP address: 500 connections per second Destination IP address: 1000 connections per second Processing mode: alarming	-
New session rate	Triggering threshold: 90% Recovery threshold: 70%	-

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Assign IP addresses to interfaces, add the interfaces to security zones, and configure network connectivity.
2. Configure a security policy to allow a specific intranet segment to access the Internet.
3. Configure a NAT address pool and enable port translation.
4. Configure a source NAT policy for translating source addresses between private and public address realms when hosts on the specific intranet segment access the Internet.
5. Configure routes on DeviceA and carrier network devices to ensure that private network traffic can be normally forwarded to the Internet and the traffic returned from the Internet can be forwarded to DeviceA. Set the parameters according to the actual network environment. This example does not describe the configuration.
6. Configure the default gateway on each PC in the intranet, so that the PCs send traffic to DeviceA when they access the Internet. Set the parameters according to the actual network environment. This example does not describe the configuration.
7. On DeviceA, configure per-IP new connection rate limiting for LAN and WAN protection.
8. On DeviceA, configure new session rate limiting to ensure normal service forwarding.

Procedure

Step 1 Assign IP addresses to interfaces, add the interfaces to security zones, and configure network connectivity.

Assign an IP address to GE0/0/1.

```
<DeviceA> system-view
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Assign an IP address to GE0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow a specific intranet segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool and enable port translation.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.11
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a source NAT policy for translating source addresses between private and public address realms when hosts on the specific intranet segment access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure per-IP new connection rate limiting for LAN and WAN protection.

This function on DeviceA limits the rate of new connections for an IP address in the inbound direction of an interface. In the LAN protection scenario, the source IP addresses of malicious attacks are fixed, and the destination IP addresses are random and numerous. Therefore, you need to configure new connection rate limiting based on source IP addresses on the interface connecting to the Intranet. In WAN protection scenarios, the destination IP addresses of attack packets are the addresses in the address pool. Therefore, you need to configure new connection rate limiting based on destination IP addresses on the interface connecting to the Internet.

NOTE

During initial configuration, you are advised to set the protection mode to the **alert** mode, adjust the threshold based on the reported logs and the peak value of the new connection rate in the IP monitoring entries, and then change the protection mode to the **drop** mode.

```
[DeviceA] firewall defend ipcar source session-rate-limit 500
[DeviceA] firewall defend ipcar destination session-rate-limit 1000
[DeviceA] firewall defend ipcar source mode alert
[DeviceA] firewall defend ipcar destination mode alert
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] firewall defend ipcar source session-rate-limit enable
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] firewall defend ipcar destination session-rate-limit enable
[DeviceA-GE0/0/2] quit
```

The configuration of the maximum new connection rate is for reference only and must be determined based on the actual network environment. In most cases, you are advised to set the maximum new connection rate per IP address to 500 for LAN protection and the maximum new connection rate per IP address to 1000 for WAN protection.

Step 6 On DeviceA, configure new session rate limiting to ensure normal service forwarding.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall session create-rate-control enable
[DeviceA] firewall session create-rate-control cpu-usage 90 70
```

Step 7 After the device runs for a period of time, run the **display logbuffer module DEFEND_IPCAR** command to check whether alarm logs exist, and run the **display firewall defend ipcar table all** command to view the new connection rate for each IP address in IP monitoring entries and determine whether the maximum new connection rate is set properly. If not, adjust the maximum new connection rate to a proper value and then check logs and IP monitoring entries.

```
<DeviceA> display logbuffer module DEFEND_IPCAR
Logging buffer configuration and contents : enabled
Allowed max buffer size : 2048
Actual buffer size : 1024
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 1

Jul  6 2018 18:26:45 sysname %%01DEFEND_IPCAR/4/SESS_RATE(l): The session creation rate exceeded the threshold. (vsys=public, IP address=10.1.1.1, type=source, peak rate=520, session rate threshold=500)
```

Step 8 After the maximum new connection rate is adjusted to a proper value, change the defense action to **drop** for LAN and WAN protection.

```
[DeviceA] firewall defend ipcar source mode drop
[DeviceA] firewall defend ipcar destination mode drop
```

----End

Verifying the Configuration

- Run the **display firewall defend ipcar table all** command to check whether the IP monitoring table exists.
- Run the **display logbuffer module DEFEND_IPCAR** command to check whether alarm logs exist.

```
<DeviceA> display logbuffer module DEFEND_IPCAR
Logging buffer configuration and contents : enabled
Allowed max buffer size : 2048
Actual buffer size : 1024
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 1

Jul  6 2018 18:26:45 sysname %%01DEFEND_IPCAR/4/SESS_RATE(l): The session creation rate exceeded the threshold. (vsys=public, IP address=10.1.1.1, type=source, peak rate=520, session rate threshold=500)
```

Configuration Scripts

The following lists only the scripts of this configuration example.

```
#
 sysname DeviceA
#
 firewall defend ipcar destination session-rate-limit 1000
 firewall defend ipcar source session-rate-limit 500
 firewall defend ipcar destination mode drop
 firewall defend ipcar source mode drop
 firewall session create-rate-control enable
 firewall session create-rate-control cpu-usage 90 70
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 firewall defend ipcar source session-rate-limit enable
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
 firewall defend ipcar destination session-rate-limit enable
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.11
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15 NAT

15.1 Source NAT
15.2 Policy-based Destination NAT
15.3 NAT Server
15.4 Bidirectional NAT (Source NAT+Destination NAT)
15.5 Bidirectional NAT (Source NAT+NAT Server)
15.6 NAT in Hot Standby Scenarios

15.1 Source NAT

15.1.1 Web: Example for Configuring NAT No-PAT for Intranet Users to Access the Internet

Networking Requirements

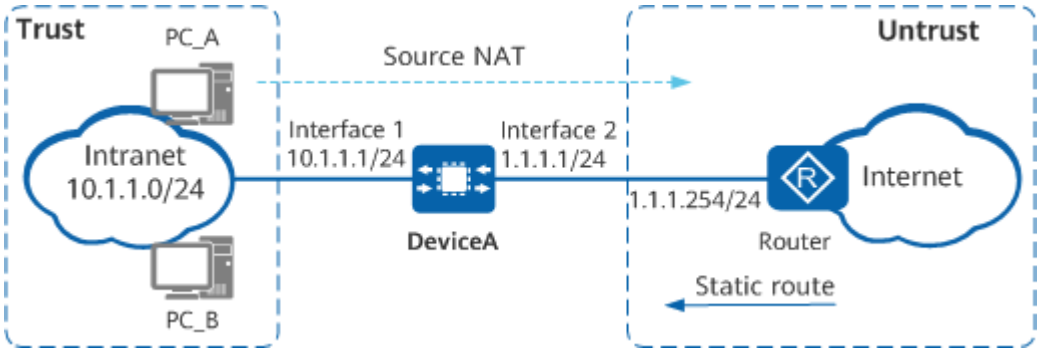
An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. As only a small number of users require access to the Internet, NAT No-PAT can be configured on DeviceA to perform one-to-one translation between private and public addresses. The enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the Internet service provider (ISP) for address translation. **Figure 15-1** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-1 Network diagram of NAT No-PAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item		Data	Description
GE0/0/1		IP address: 10.1.1.1/24 Security zone: trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2		IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet		10.1.1.0/24	-
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	Configure NAT No-PAT on DeviceA as a small number of users require access to the Internet.
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

 Copyright © Huawei Technologies Co., Ltd.

2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool and disable port translation.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.
7. Configure a static route on the ISP router, enabling it to forward traffic returned by the Internet to DeviceA.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	trust
IPv4	
IP Address	10.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   b. Click **OK**.

Step 2 Configure a security policy to allow users on a specific network to access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	trust
Destination Zone	untrust

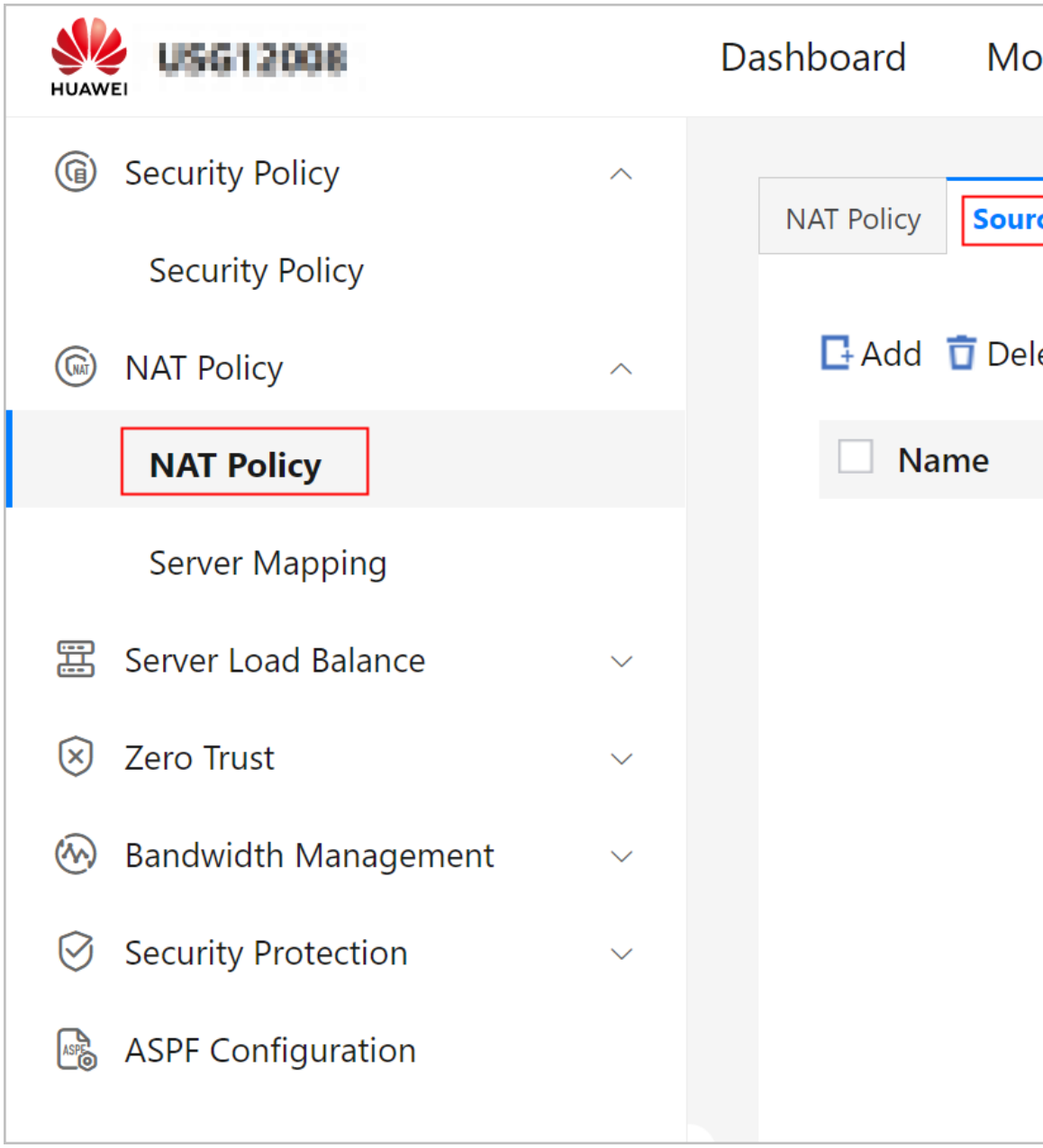
 Copyright © Huawei Technologies Co., Ltd.

Source Address	10.1.1.0/24
Action	Permit

3. Click **OK**.

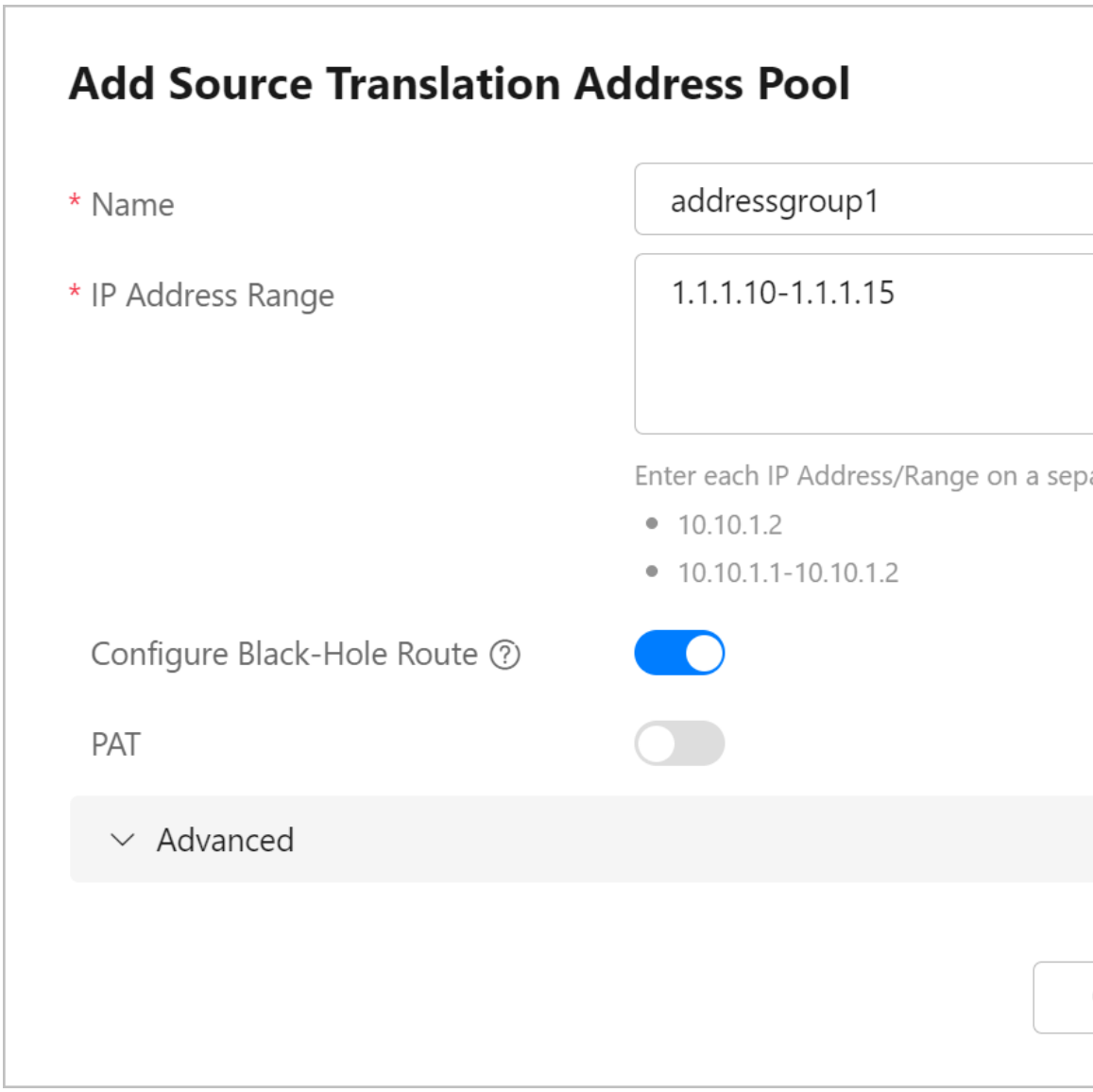
Step 3 Configure a NAT address pool and a NAT policy.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.



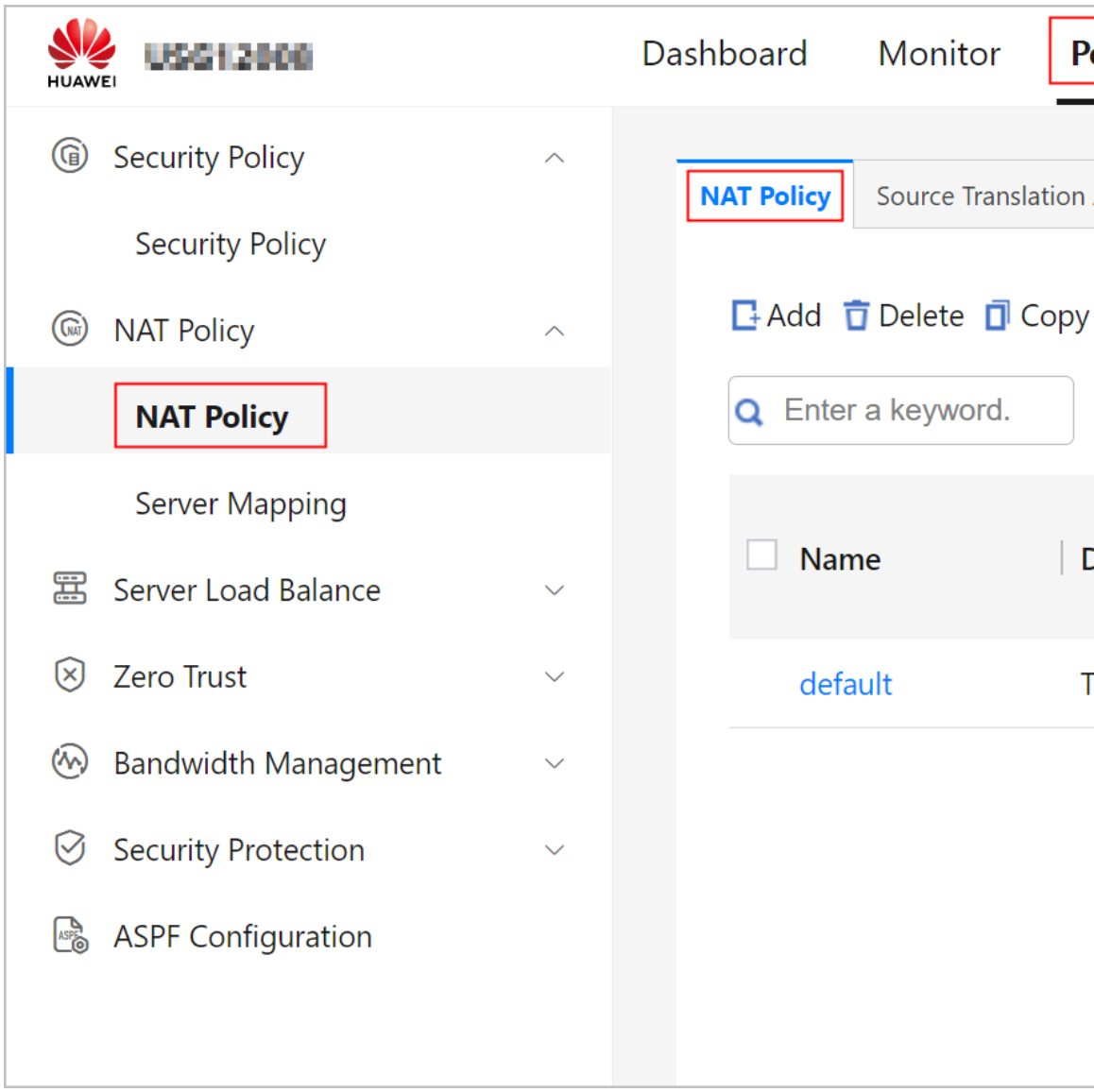
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



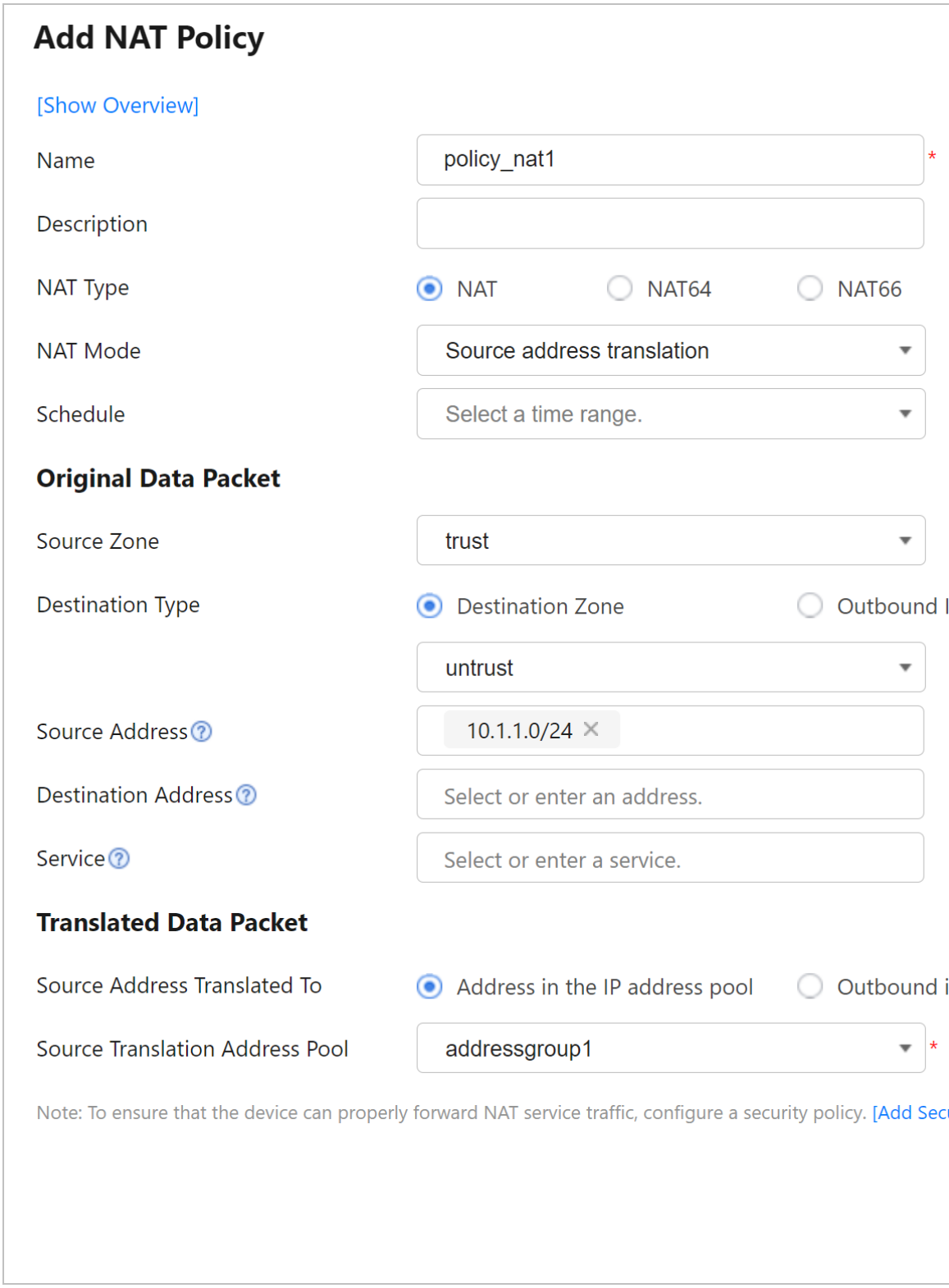
3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.



5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



6. Click **OK**.

Step 4 Configure a default route on the DeviceA, so that traffic from the private network can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.

 Copyright © Huawei Technologies Co., Ltd.

2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 5 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 6 On the ISP router, configure a static route to addresses in the NAT address pool (1.1.1.10 to 1.1.1.15), with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic returned by the Internet to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. When intranet PCs access the Internet, choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode no-pat global
 route enable
 section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
  action source-nat address-group addressgroup1
#
return
```

15.1.2 CLI: Example for Configuring NAT No-PAT for Intranet Users to Access the Internet

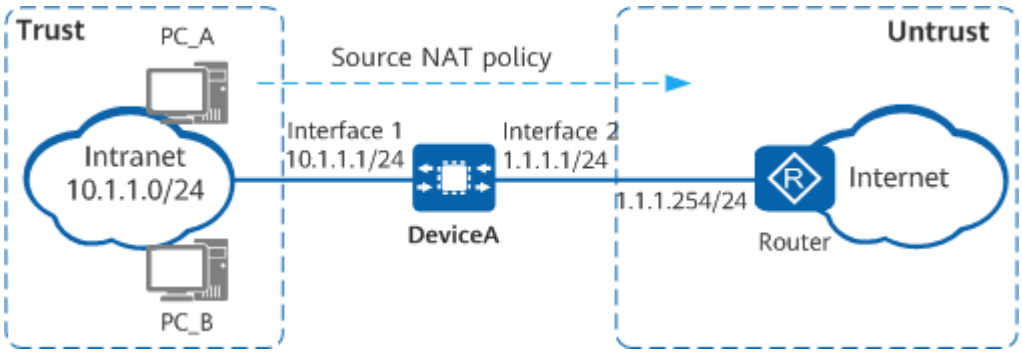
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. As only a small number of users require access to the Internet, NAT No-PAT can be configured on DeviceA to perform one-to-one translation between private and public addresses. The enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the Internet service provider (ISP) for address translation. **Figure 15-2** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-2 Network diagram of NAT No-PAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet	10.1.1.0/24	-

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	Configure NAT No-PAT on DeviceA as a small number of users require access to the Internet.
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool and disable port translation.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool and disable port translation.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode no-pat global
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 6 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 7 If the addresses in the NAT address pool and the IP address of GE0/0/2 are on different network segments, configure a static route to the addresses in the NAT address pool on the ISP router, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic returned by the Internet to DeviceA.

The post-NAT public addresses are not assigned to any interfaces. As a result, the ISP router is unable to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the addresses in the address pool on the ISP router.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Run the **display nat-policy rule name** *rule-name* command on DeviceA to check the number of times traffic matches the source NAT policy.
3. Run the **display firewall session table** command on DeviceA to check for the session entries with source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is an IP address in

 Copyright © Huawei Technologies Co., Ltd.

the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.1.1.3:2474[1.1.1.10:2474]-->3.3.3.3:80
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode no-pat global
 route enable
 section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

15.1.3 Web: Example for Configuring NAPT for Intranet Users to Access the Internet

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the ISP for address translation. If a large number of users on the intranet access the Internet, you need to configure NAPT to enable both address and port translation; however, port conflicts may occur during NAT translation. To avoid this, set the maximum number of private

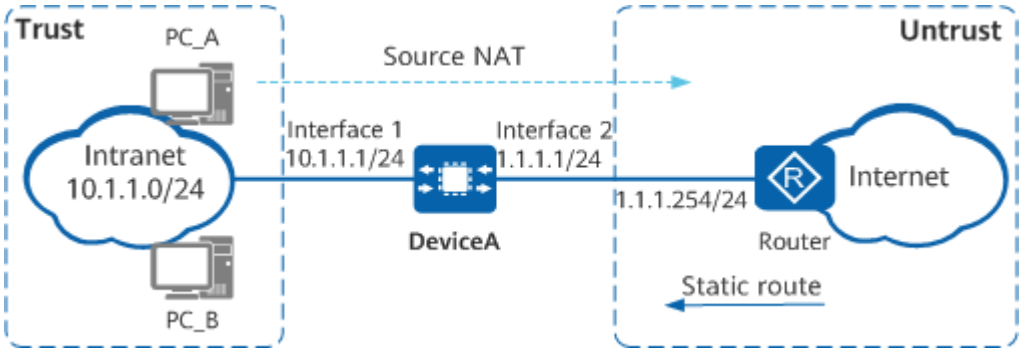
 Copyright © Huawei Technologies Co., Ltd.

addresses that can correspond to a public address. **Figure 15-3** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-3 Network diagram of NAPT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item		Data	Description
GE0/0/1		IP address: 10.1.1.1/24 Security zone: trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2		IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet		10.1.1.0/24	-
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	As private addresses far outnumber public addresses, one-to-one mapping cannot be implemented. To translate all private addresses into public addresses, enable port translation.
(Optional configuration) Maximum number of private addresses corresponding to a single public address		256	-
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool and enable port translation so that public addresses can be reused. Set the maximum number of private addresses to be translated into one public address to 256.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.
7. Configure a static route on the ISP router, enabling it to forward traffic returned by the Internet to DeviceA.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	trust
IPv4	
IP Address	10.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.

 Copyright © Huawei Technologies Co., Ltd.

a. In **Interface List**, click of GE 0/0/2 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

b. Click **OK**.

Step 2 Configure a security policy to allow users on a specific network to access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

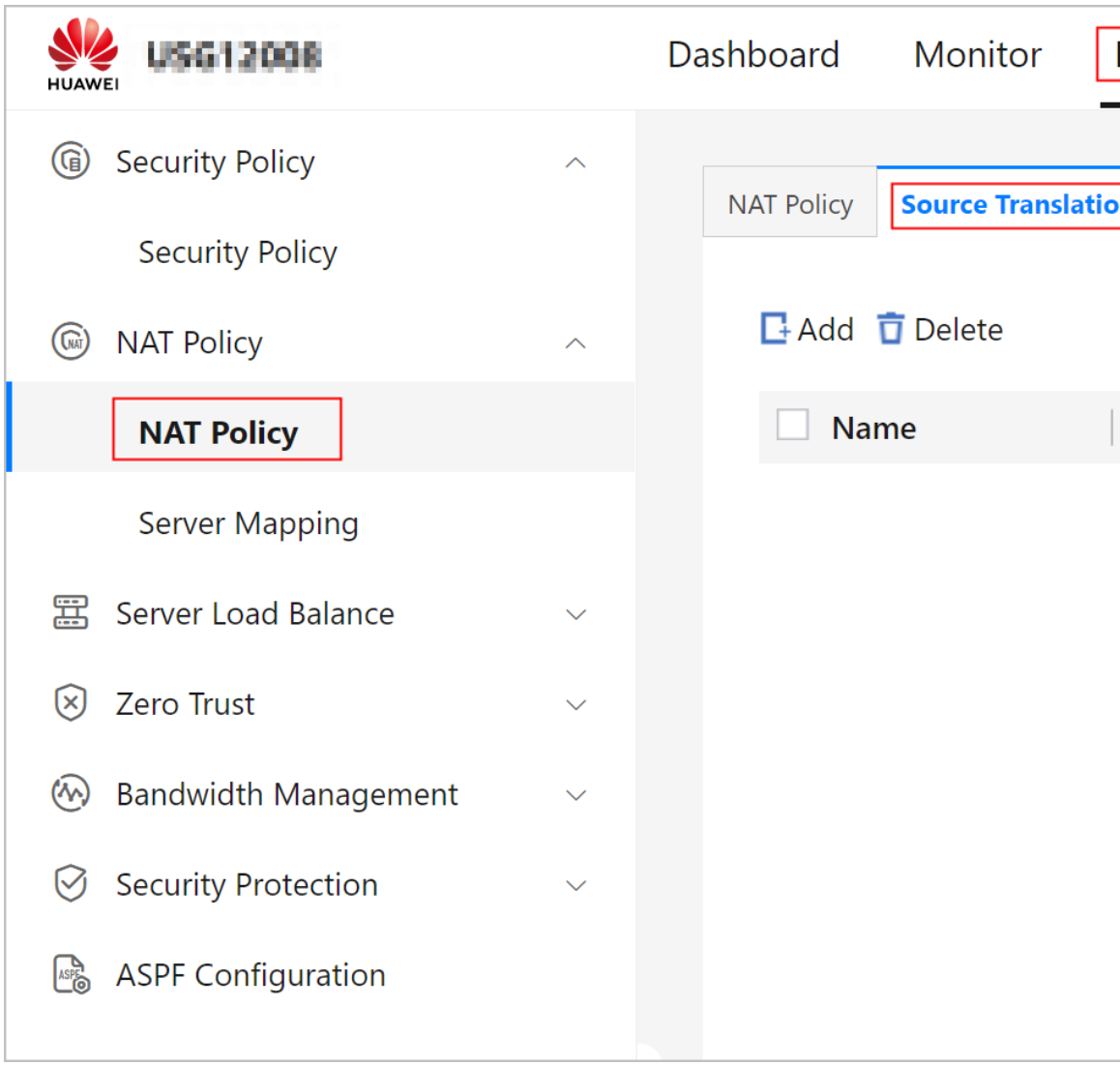
Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure a NAT address pool and a NAT policy.

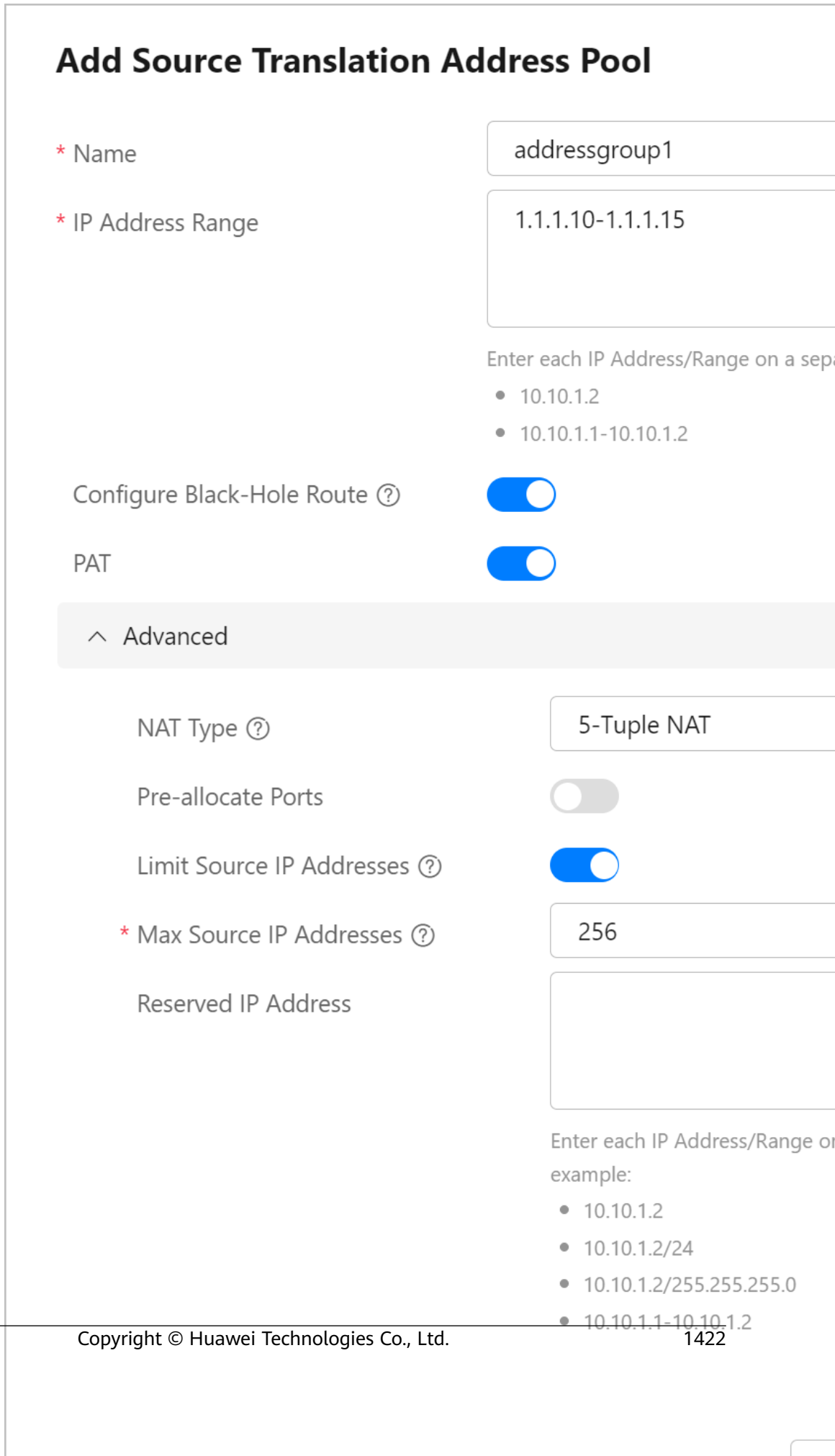
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

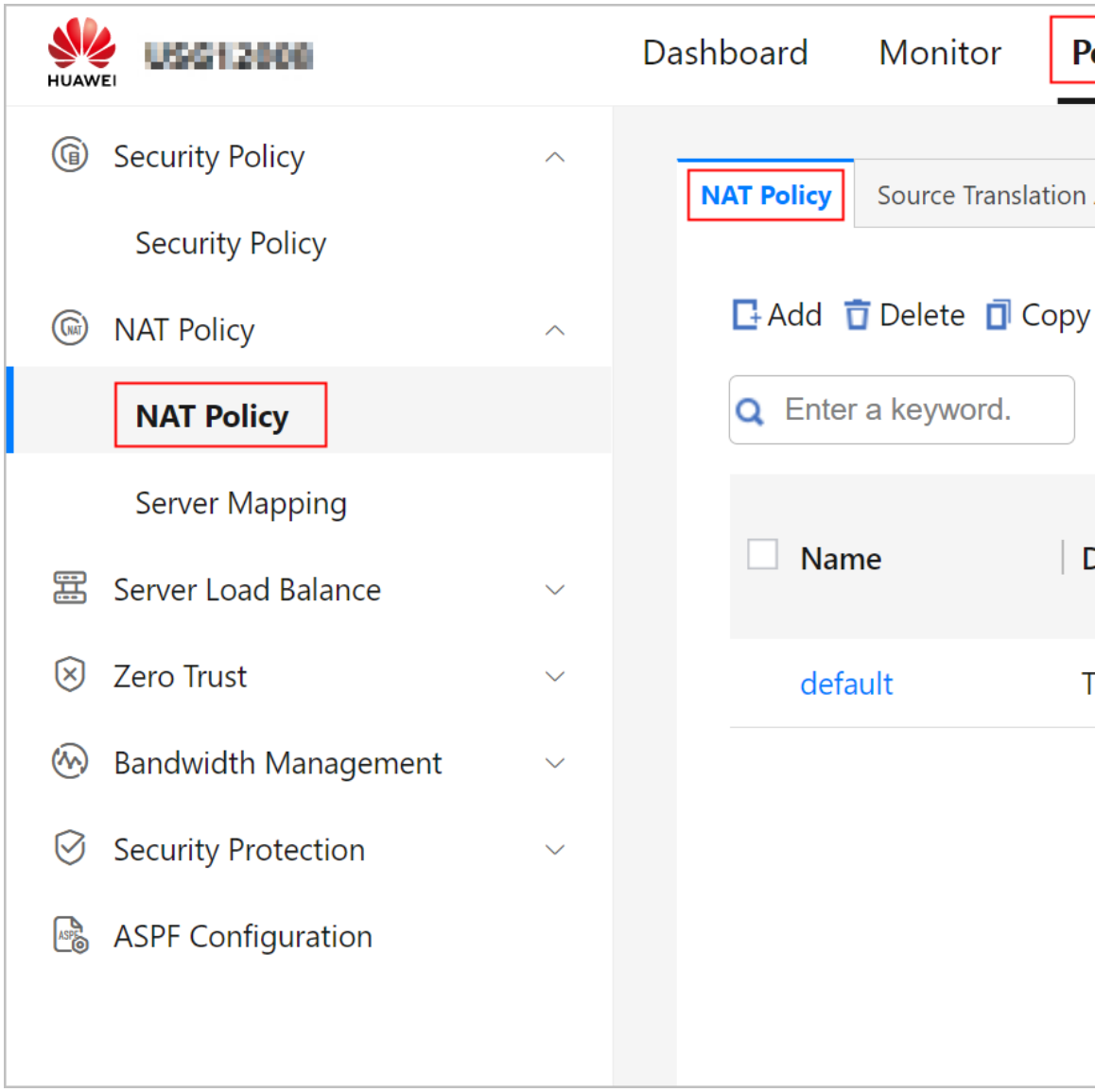
Limit Source IP Addresses is optional. When a large number of intranet users access the Internet, you can set the number of private IP addresses corresponding to a single public IP address to prevent port conflicts during NAT.

For USG6700F series, before configuring **Limit Source IP Addresses** , set the hash mode of service CPU traffic distribution to source IP address mode.

```
<DeviceA> system-view
[DeviceA] firewall hash-mode source-only
[DeviceA] quit
<DeviceA> reboot
```

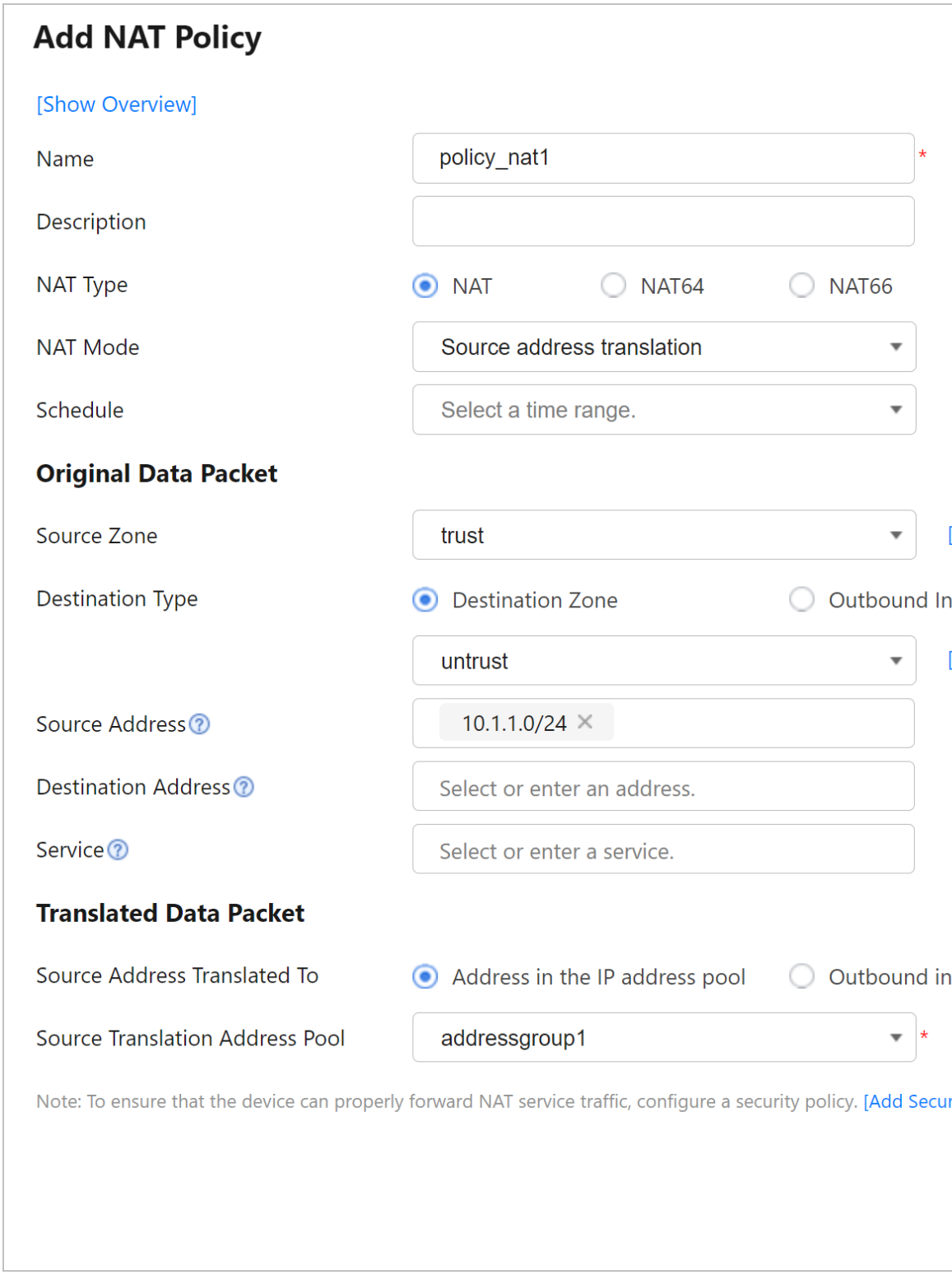
The modified hash mode takes effect only after the device is restarted. In addition, ensure that the configuration file is saved before you restart the device.

3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



6. Click **OK**.

Step 4 Configure a default route on the DeviceA, so that traffic from the private network can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.

 Copyright © Huawei Technologies Co., Ltd.

2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 5 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 6 On the router, configure a static route destined for the network segment of the address pool (1.1.1.10 to 1.1.1.15) and set the next-hop address of the static route to 1.1.1.1 so that Internet traffic destined for the intranet server can be forwarded by the DeviceA.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. When intranet PCs access the Internet, choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.
3. Verify that DeviceA can send a log and alarm when the number of private IP addresses that have been translated into the same public IP address reaches the threshold.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.15
 srcip-car-num 256
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 24
  action source-nat address-group addressgroup1
#
return
```

15.1.4 CLI: Example for Configuring NAPT for Intranet Users to Access the Internet

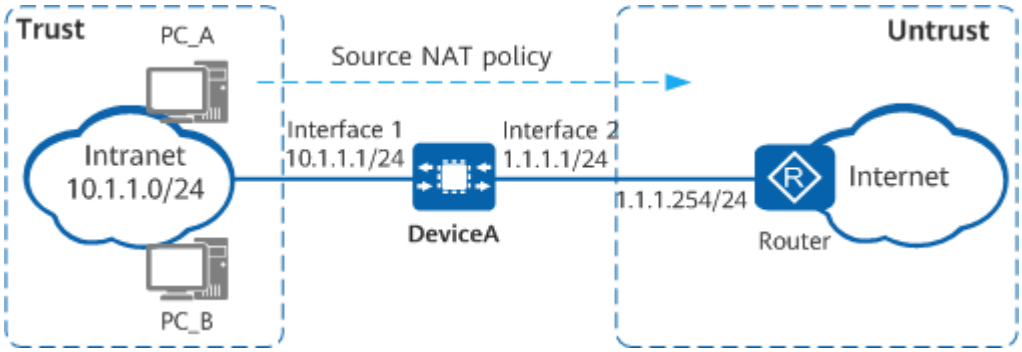
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the ISP for address translation. If a large number of users on the intranet access the Internet, you need to configure NAPT to enable both address and port translation; however, port conflicts may occur during NAT translation. To avoid this, set the maximum number of private addresses that can correspond to a public address. **Figure 15-4** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-4 Network diagram of NAPT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.1.1.1.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
GE0/0/2		IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet		10.1.1.0/24	-
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	As private addresses far outnumber public addresses, one-to-one mapping cannot be implemented. To translate all private addresses into public addresses, use port translation.
(Optional) Maximum number of private addresses corresponding to a single public address		256	-
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool and enable port translation so that public addresses can be reused. Set the maximum number of private addresses to be translated into one public address to 256.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

 Copyright © Huawei Technologies Co., Ltd.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool, enable port translation, and set the maximum number of private addresses to be translated into one public address to 256.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-addressgroup1] srcip-car-num 256
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

NOTE

The **srcip-car-num** command can be configured only when the hash mode is source IP address–based.

You can run the **firewall hash-mode** command to configure the hash mode. When the **realtime** parameter is specified in this command, the new hash mode takes effect immediately.

When the hash mode is modified and the modification takes effect immediately, NAT, IPsec, and service forwarding are interrupted for a short period of time. Services will be restored after session entries are re-established.

Step 4 Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 6 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 7 If the addresses in the NAT address pool and the IP address of GE 0/0/2 are on different network segments, configure a static route to the addresses in the NAT address pool on the ISP router, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic returned by the Internet to DeviceA.

The post-NAT public addresses are not assigned to any interfaces. As a result, the ISP router is unable to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the addresses in the address pool on the ISP router.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Check for the session entries with the source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.1.1.3:2474[1.1.1.10:3761]-->3.3.3.3:80
```

3. Verify that DeviceA can send a log and alarm when the number of private IP addresses that have been translated into the same public IP address reaches the threshold.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.15
 srcip-car-num 256
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    action source-nat address-group addressgroup1
#
return
```

15.1.5 Web: Example for Configuring Easy IP for Intranet Users to Access the Internet

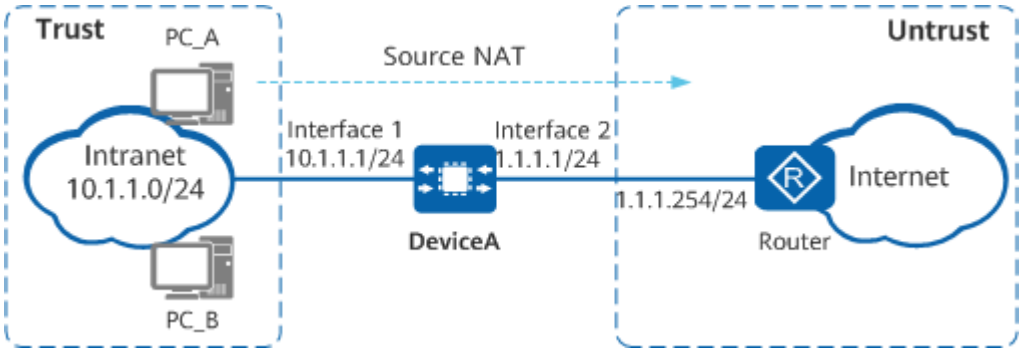
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border and obtained only one public IP address from an ISP. This public IP address is assigned to the WAN interface of DeviceA so that it can communicate with the ISP router, which is an access gateway on the ISP network. To allow intranet users on the 10.1.1.0/24 network segment to access the Internet, you need to configure a source NAT policy in Easy IP mode on DeviceA. This policy allows DeviceA to translate private IP addresses of intranet users into the public IP address of the outbound interface (the WAN interface of DeviceA) of user packets. **Figure 15-5** shows the network diagram of source NAT in Easy IP mode.

Figure 15-5 Networking diagram of NAT in Easy IP mode

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet	10.1.1.0/24	-
Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
4. Configure a source NAT policy in Easy IP mode on DeviceA, enabling it to translate source private IP addresses of the packets sent from intranet users to the Internet into the public IP address of the outbound interface.

   NOTE

   Only the **easy-ip** parameter needs to be specified in a source NAT policy. DeviceA will automatically discover the outbound interface address based on routing information.
5. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	trust
IPv4	
IP Address	10.1.1.1/24

 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.

a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

b. Click **OK**.

Step 2 Configure a security policy to allow users on a specific network to access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure a default route on the DeviceA, so that traffic from the private network can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

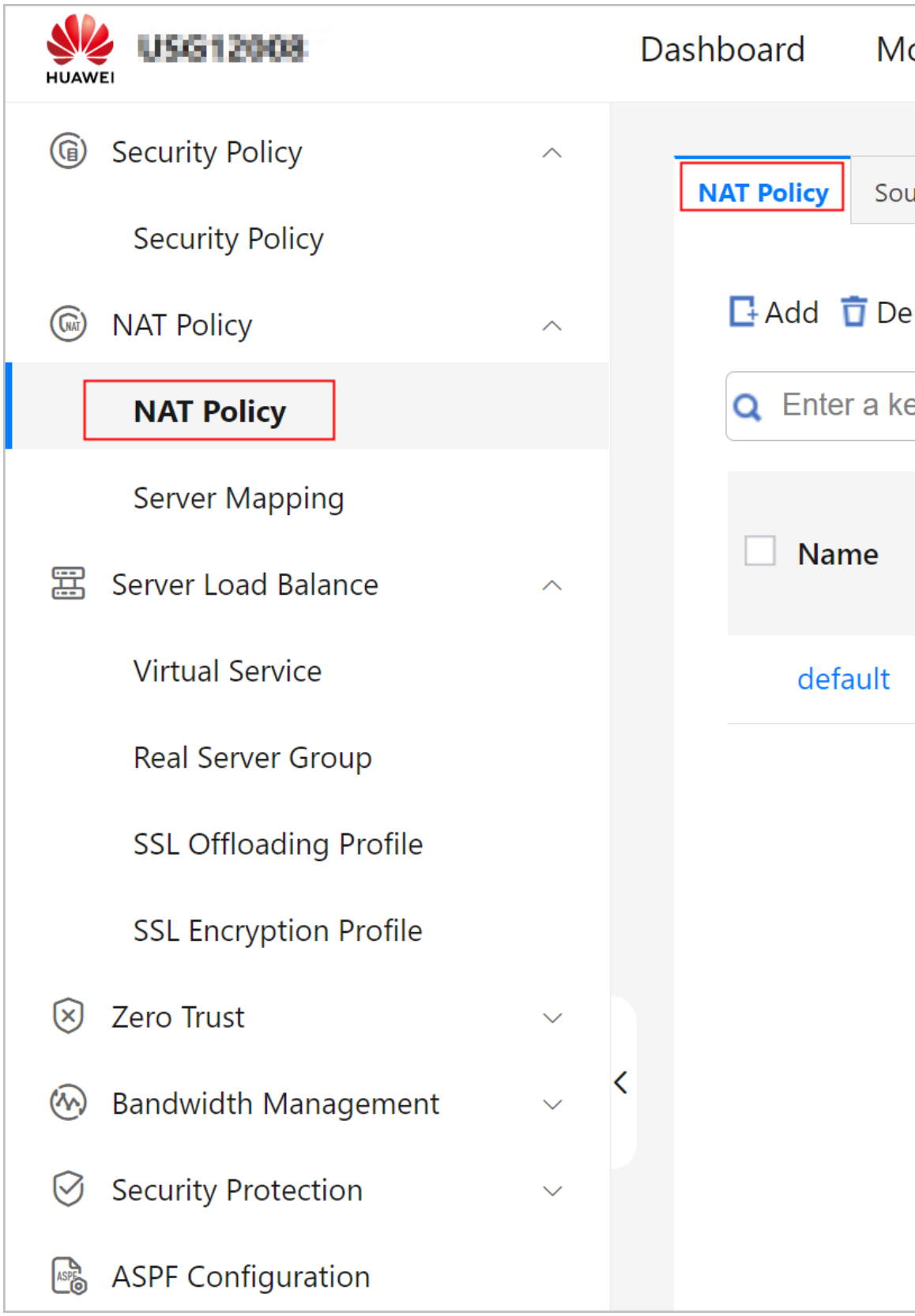
Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 4 Configure a NAT policy working in outbound interface address mode so that intranet users can use the DeviceA's public IP address to access the Internet.

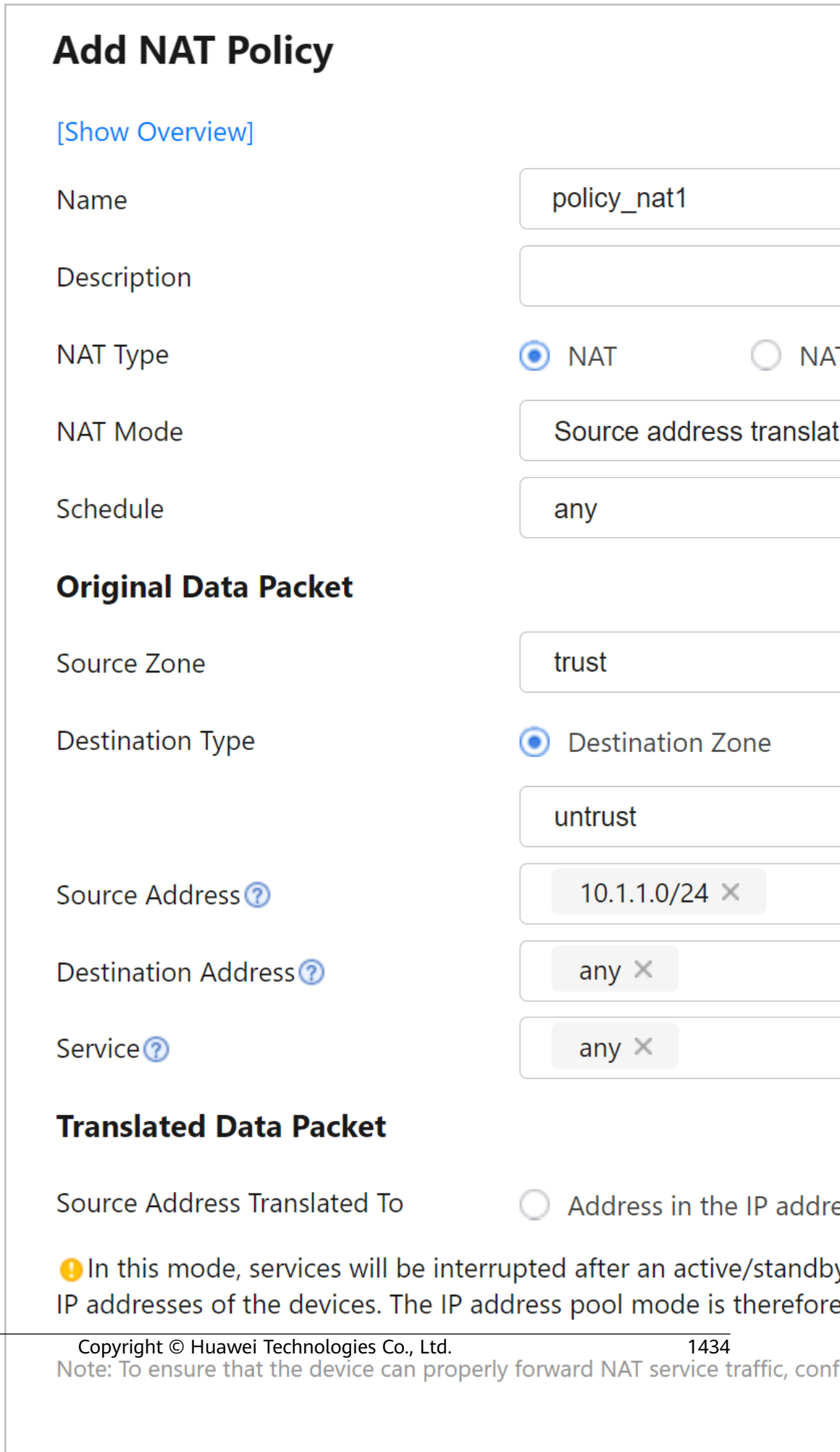
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.



2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

3. Click **OK**.

Step 5 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. When intranet PCs access the Internet, choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat easy-ip
#
return
```

15.1.6 CLI: Example for Configuring Easy IP for Intranet Users to Access the Internet

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. This public IP address is assigned to the WAN interface of DeviceA so that it can communicate with the ISP router, which is an access gateway on the ISP network. To allow intranet users on the 10.1.1.0/24 network segment to access the Internet,

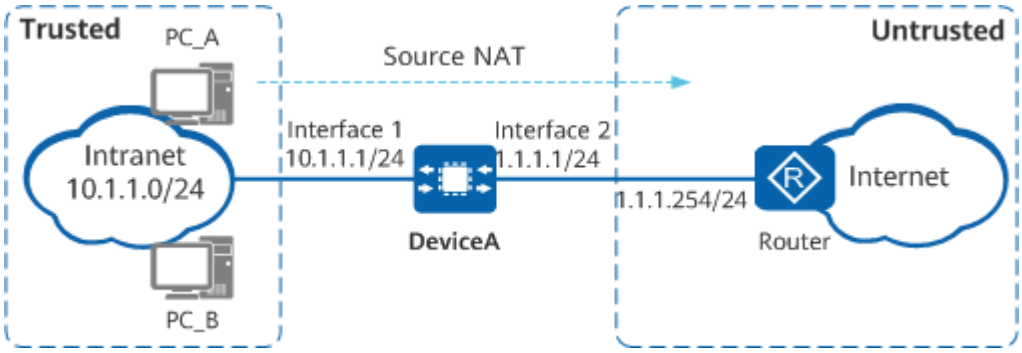
 Copyright © Huawei Technologies Co., Ltd.

you need to configure a source NAT policy in Easy IP mode on DeviceA. This policy allows DeviceA to translate private IP addresses of intranet users into the public IP address of the outbound interface (the WAN interface of DeviceA) of user packets. **Figure 15-6** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-6 Network diagram of Easy IP

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet	10.1.1.0/24	-
Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.

 Copyright © Huawei Technologies Co., Ltd.

4. Configure a source NAT policy in Easy IP mode on DeviceA, enabling it to translate source private IP addresses of the packets sent from intranet users to the Internet into the public IP address of the outbound interface.

   NOTE

   Only the **easy-ip** parameter needs to be specified in a source NAT policy. DeviceA will automatically discover the outbound interface address based on routing information.

5. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 4 Configure a NAT policy in Easy IP mode.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat easy-ip
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Run the **display nat-policy rule name** *rule-name* command on DeviceA to check the number of times traffic matches the source NAT policy.
3. Check for the session entries with the source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is the public IP address of the WAN interface, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.1.1.3:2474[1.1.1.1:3761]-->3.3.3.3:80
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 mask 255.255.255.0
    action source-nat easy-ip
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.1.7 CLI: Example for Configuring Smart NAT for Intranet Users to Access the Internet

Networking Requirements

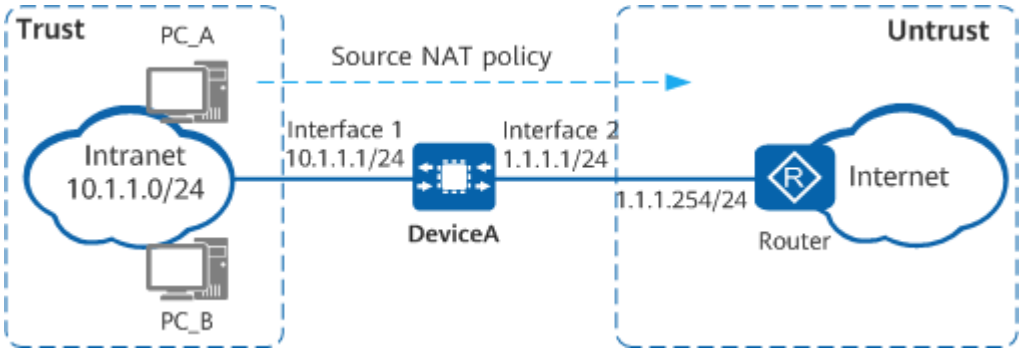
An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the ISP for address translation. **Figure 15-7** shows the network diagram, in which the router is the access gateway provided by the ISP.

In most cases, only a small number of intranet users access the Internet simultaneously, and therefore NAT No-PAT translation can be used for these users. In addition, a public IP address is reserved for NAPT in case the public IP addresses used in No-PAT are insufficient.

Figure 15-7 Network diagram of smart NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet	10.1.1.0/24	-
Post-NAT public addresses	1.1.1.10 to 1.1.1.14	Public IP address in NAT No-PAT
	1.1.1.15	Public IP address in NAPT

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool, reserve a public IP address for NAPT, and enable No-PAT for other public IP addresses.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.
7. Configure a static route on the ISP router, enabling it to forward traffic returned by the Internet to DeviceA.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode no-pat global
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.14
[DeviceA-address-group-addressgroup1] smart-nopat 1.1.1.15
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 6 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 7 On the ISP router, configure a static route to addresses in the NAT address pool (1.1.1.10 to 1.1.1.15), with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic returned by the Internet to DeviceA.

Contact the ISP network administrator to perform this step.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Run the **display nat-policy rule name** *rule-name* command on DeviceA to check the number of times traffic matches the source NAT policy.
3. Run the **display firewall session table** command on DeviceA to check for the session entries with the source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 3
 http  VPN:public --> public  10.1.1.3:2474[1.1.1.10:2474]-->3.3.3.3:80
 http  VPN:public --> public  10.1.1.4:2478[1.1.1.11:2478]-->3.3.3.2:80
 http  VPN:public --> public  10.1.1.5:2472[1.1.1.12:2472]-->3.3.3.5:80
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode no-pat global
 smart-nopat 1.1.1.15
 route enable
 section 0 1.1.1.10 1.1.1.14
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.1.8 Web: Example for Configuring Triplet NAT for Intranet Users to Access the Internet

Networking Requirements

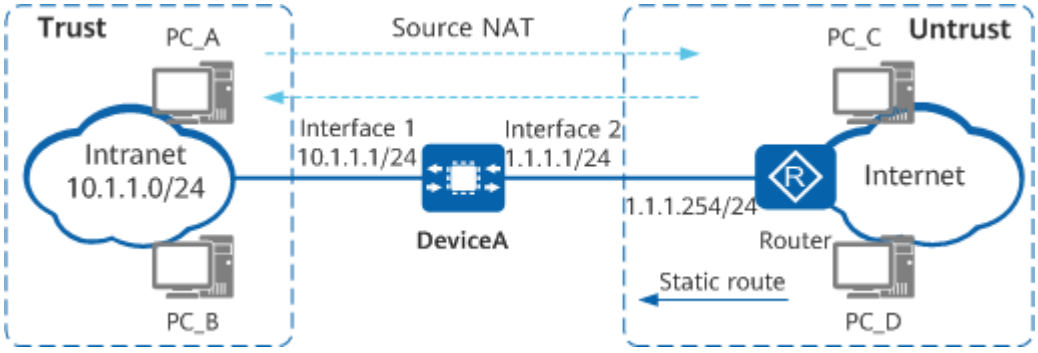
An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the ISP for address translation. **Figure 15-8** shows the network diagram, in which the router is the access gateway provided by the ISP.

In addition, P2P services, such as file sharing, audio communication, and video transmission, are required between users on the intranet and hosts on the Internet, regardless of which side initiates the service. In this case, configure 3-tuple NAT to meet the service requirements.

Figure 15-8 Network diagram of 3-tuple NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE 0/0/1	IP address: 10.1.1.1/24 Security zone: trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet	10.1.1.0/24	-
Post-NAT public addresses	1.1.1.10 to 1.1.1.15	Public IP addresses for Triplet NAT.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.
7. Configure a static route on the ISP router, enabling it to forward traffic returned by the Internet to DeviceA.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click ofGE 0/0/1 and set the parameters as follows:

Zone	trust
IPv4	
IP Address	10.1.1.1/24

 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.

a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

b. Click **OK**.

Step 2 Configure a security policy to allow users on a specific network to access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Action	Permit

3. Click **OK**.

Step 3 For USG6700F series, set the hash mode of service CPU traffic distribution to source IP address mode.

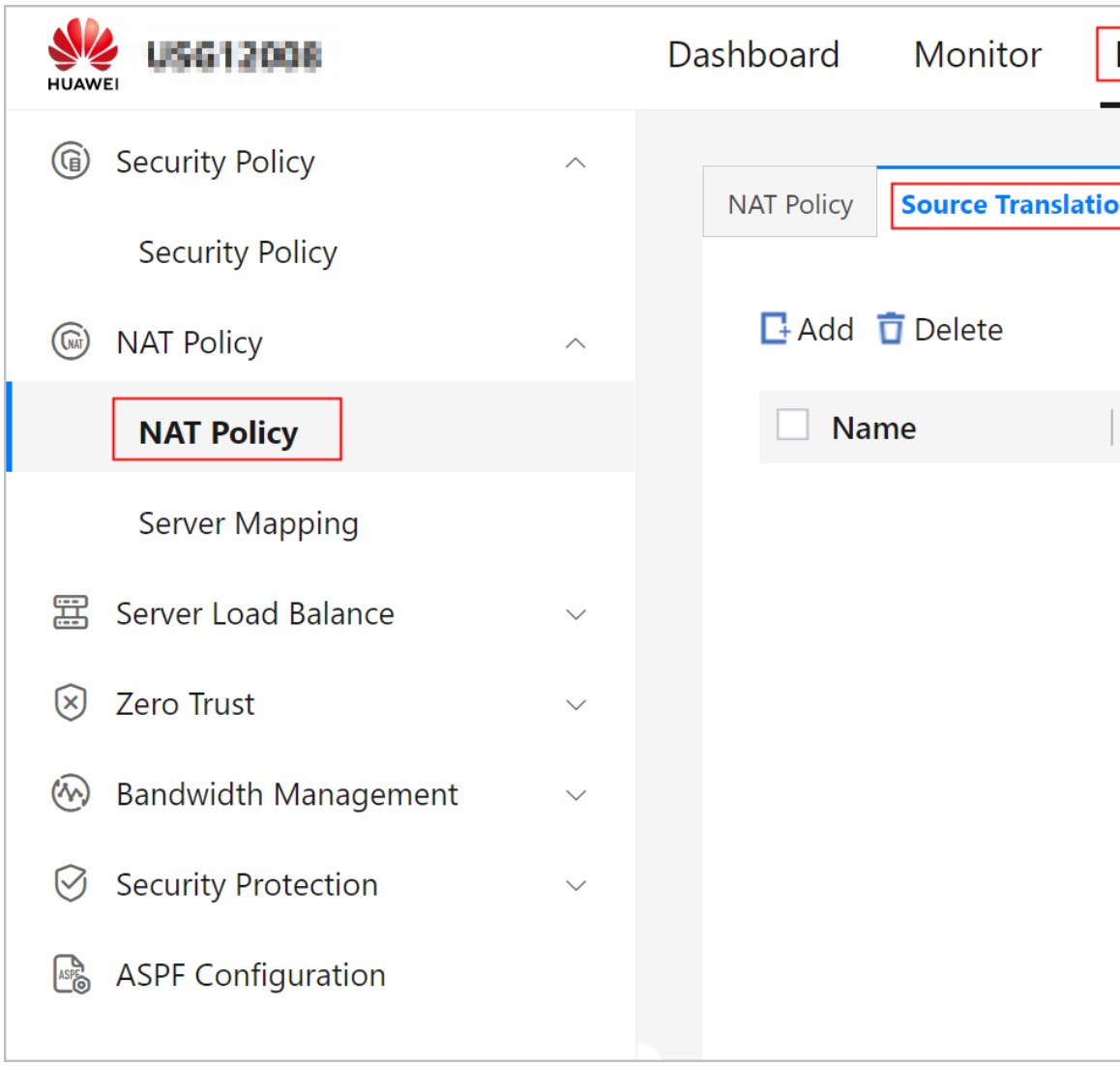
```
<DeviceA> system-view
[DeviceA] firewall hash-mode source-only
[DeviceA] quit
<DeviceA> reboot
```

The modified hash mode takes effect only after the device is restarted. In addition, ensure that the configuration file is saved before you restart the device.

Step 4 Configure a NAT address pool and a NAT policy.

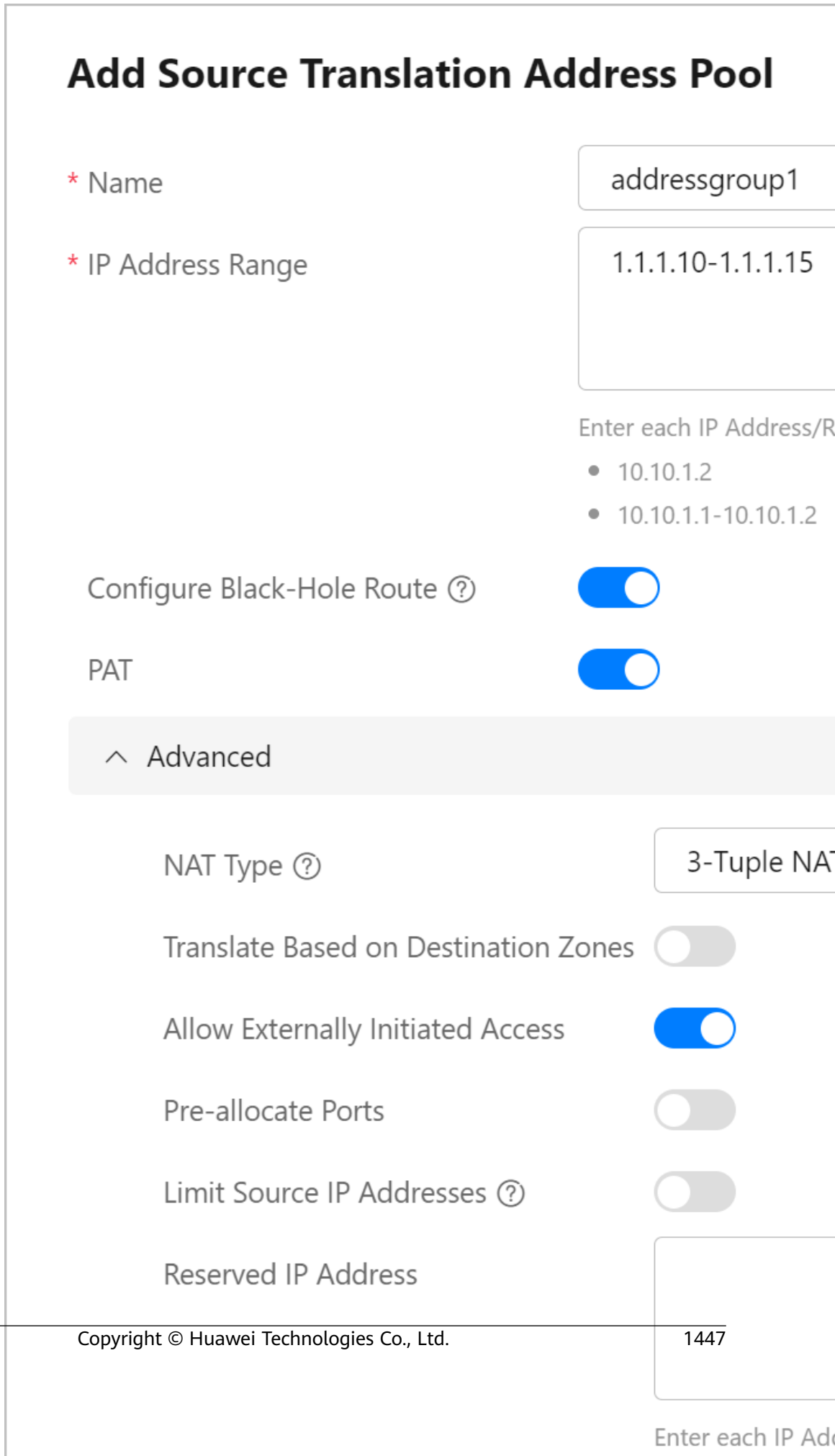
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



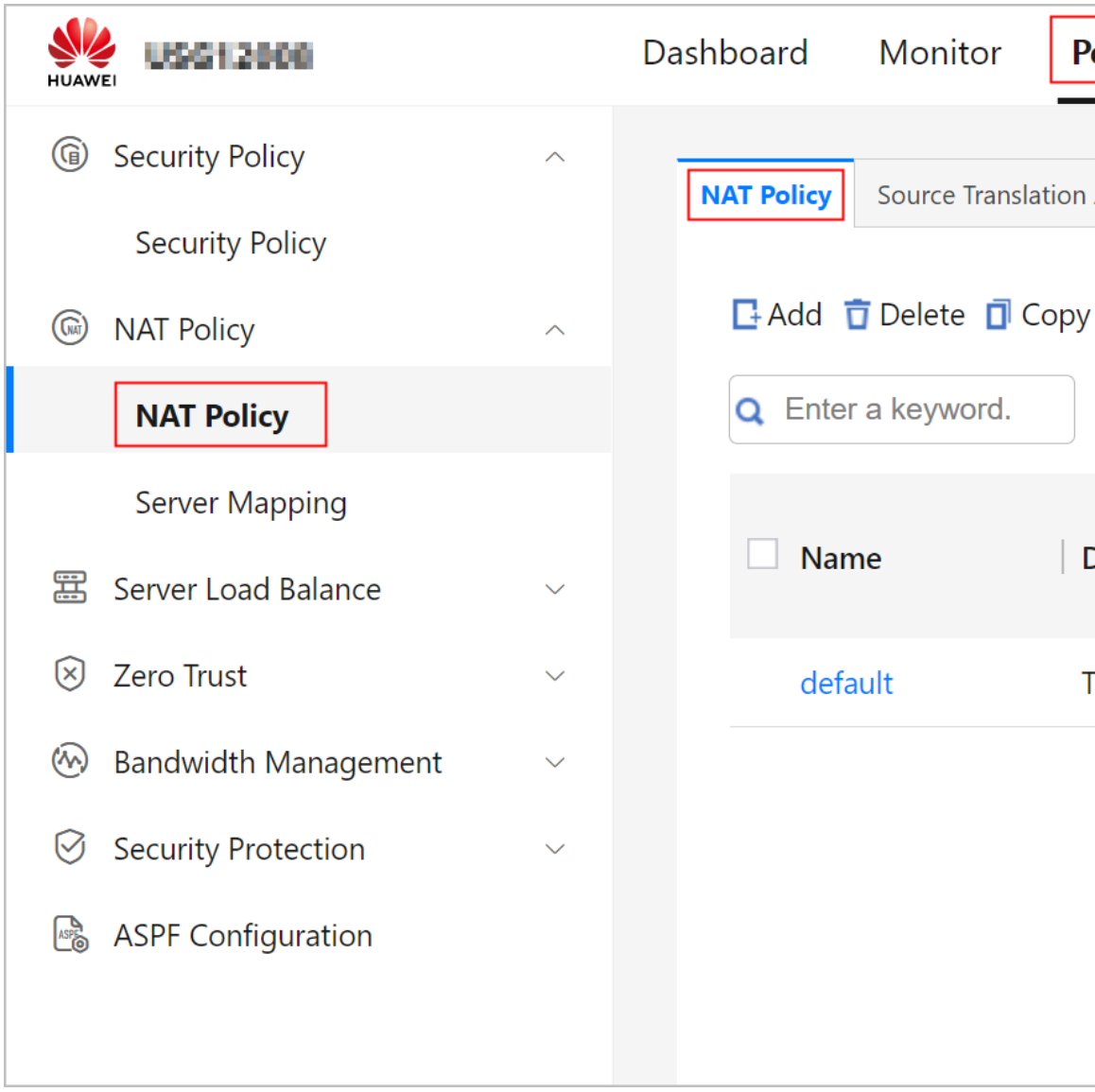
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



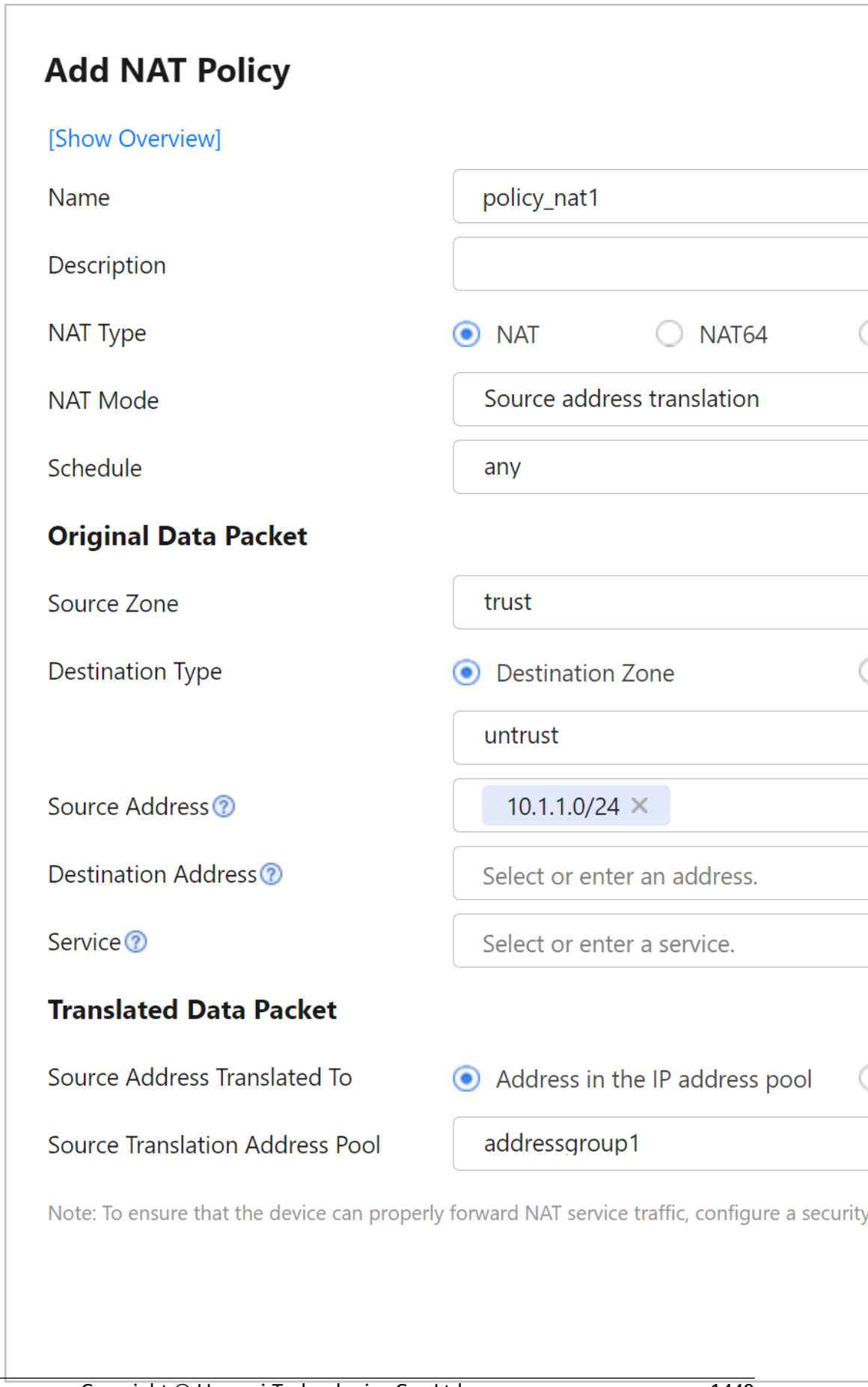
 Copyright © Huawei Technologies Co., Ltd.

3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

6. Click **OK**.

Step 5 Configure a default route on the device, so that traffic from the private network can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 6 **Optional:** Enable endpoint-independent filtering function. By default, the function is enabled. If the function is disabled, configure a security policy for traffic from the public network to the private network.

```
[DeviceA] firewall endpoint-independent filter enable
```

Step 7 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 8 On the router, configure a static route destined for the network segment of the address pool (1.1.1.10 to 1.1.1.15) and set the next-hop address of the static route to 1.1.1.1 so that Internet traffic destined for the intranet server can be forwarded by the DeviceA.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Verify that Internet hosts can access intranet PCs.
3. When intranet PCs access the Internet, choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 5
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode full-cone global
 route enable
 section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

15.1.9 CLI: Example for Configuring 3-Tuple NAT for Intranet Users to Access the Internet

Networking Requirements

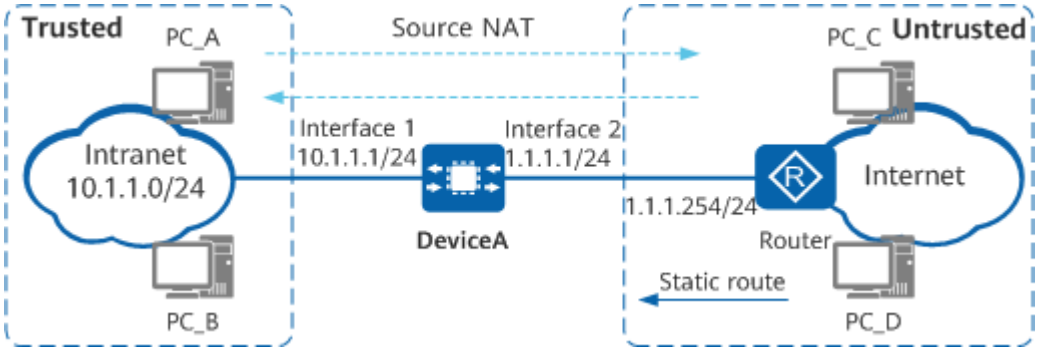
An enterprise has deployed DeviceA as a security gateway at the intranet border. A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from the ISP for address translation. **Figure 15-9** shows the network diagram, in which the router is the access gateway provided by the ISP.

In addition, P2P services, such as file sharing, audio communication, and video transmission, are required between users on the intranet and hosts on the Internet, regardless of which side initiates the service. In this case, configure 3-tuple NAT to meet the service requirements.

Figure 15-9 Network diagram of 3-tuple NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
GE0/0/1		IP address: 10.1.1.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.1.1.1.
GE0/0/2		IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
Private network segment allowed to access the Internet		10.1.1.0/24	-
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	Public IP addresses for full-cone NAT
Routes	Default route on DeviceA	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA, enabling it to forward traffic from the intranet to the ISP router.
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
5. Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.
6. Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA.
7. Configure a static route on the ISP router, enabling it to forward traffic returned by the Internet to DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool and enable port translation.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode full-cone global
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-addressgroup1] quit
```

NOTE

The **mode full-cone** command can be configured only when the hash mode is source IP address–based.

You can run the **firewall hash-mode** command to configure the hash mode. When the **realtime** parameter is specified in this command, the new hash mode takes effect immediately.

When the hash mode is modified and the modification takes effect immediately, NAT, IPsec, and service forwarding are interrupted for a short period of time. Services will be restored after session entries are re-established.

Step 4 Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a default route on DeviceA, enabling it to forward traffic sent from intranet users to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 6 **Optional:** Enable the endpoint-independent filtering function. By default, the endpoint-independent filtering function is enabled. If this function is disabled, configure a security policy to permit traffic sent from the Internet to the intranet.

```
[DeviceA] firewall endpoint-independent filter enable
```

Step 7 Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to DeviceA. The detailed configuration process is not provided here.

Step 8 On the ISP router, configure a static route to addresses in the NAT address pool (1.1.1.10 to 1.1.1.15), with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic returned by the Internet to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Run the **display nat-policy rule name** *rule-name* command on DeviceA to check the number of times traffic matches the source NAT policy.
3. Run the **display firewall session table** command on DeviceA to check for the session entries with the source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.1.1.3:2474[1.1.1.10:2474]-->3.3.3.3:80
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode full-cone global
 route enable
 section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

15.1.10 Web: Example for Configuring NAPT for Users on a Dual-Egress Intranet to Access the Internet

Networking Requirements

In **Figure 15-10**, an enterprise has deployed DeviceA as a security gateway at the intranet border and purchased broadband services from ISP1 and ISP2 to allow intranet users to access the Internet.

The specific requirements are as follows:

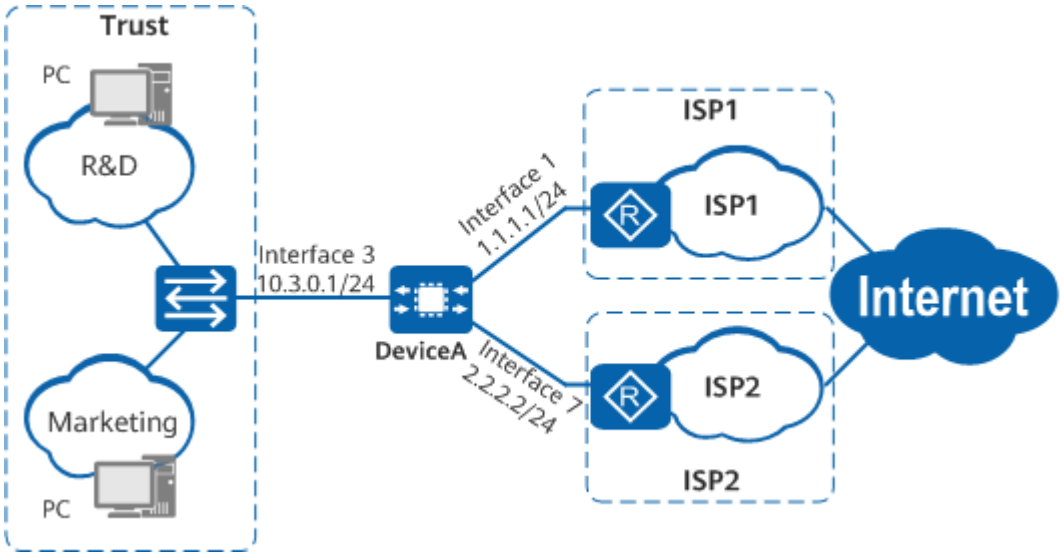
- PCs of the R&D and marketing departments can access the Internet through the networks of ISP1 and ISP2. Traffic sent from intranet PCs to a specific destination on the Internet must be forwarded by the corresponding ISP.
- If the link to one ISP network fails, traffic is immediately switched to the link connected to the other ISP network.

Figure 15-10 Dual uplinks for access to two ISP networks

NOTE

In this example, interfaces 1, 3, and 7 representGE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



The following information is only for reference. The desired service information can be obtained from your ISP.

Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: ISP1 Default gateway address: 1.1.1.254	Public IP address and gateway address assigned by ISP1
GE0/0/3	IP address: 10.3.0.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.3.0.1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: ISP2 Default gateway address: 2.2.2.254	Public IP address and gateway address assigned by ISP2
DNS server addresses	9.9.9.9	Provided by ISP1
	11.11.11.11	Provided by ISP2
NAT address pool	1.1.1.10-1.1.1.12	Provided by ISP1
	2.2.2.10-2.2.2.12	Provided by ISP2

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones. Set the default gateway address to 1.1.1.254 for GE 0/0/1 and 2.2.2.254 for GE0/0/7.
2. Configure static routes to ISP networks.
3. Configure a security policy to allow intranet PCs to access the Internet.

 Copyright © Huawei Technologies Co., Ltd.

4. Configure a source NAT policy for source address translation.
5. Configure routes on ISP devices to enable them to forward traffic returned by the Internet to DeviceA. This step is performed by ISPs, and the configuration details are not provided.
6. Plan IP addresses for intranet PCs, and set the gateway address to 10.3.0.1 and DNS server addresses to 9.9.9.9 and 11.11.11.11 on each intranet PC. This step is performed by the enterprise network administrator, and the configuration details are not provided.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE0/0/3 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE0/0/3 and set the parameters as follows:

Zone	trust
IPv4	
IP Address	10.3.0.1/24

   c. Click **OK**.
2. Set the IP address of GE0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** to create security zone **isp1** based on the following parameter values.

Zone Name	isp1
Priority	10

   c. Click **OK**.
   d. Choose **Network** > **Interface**.
   e. In **Interface List**, click on the line of GE0/0/1 and set the following parameters.

Zone	isp1
IPv4	
IP Address	1.1.1.1/24
Default Gateway	1.1.1.254

   f. Click **OK**.
3. Set the IP address of GE0/0/7 and assign the interface to a security zone.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **Network** > **Zone**.

b. Click **Add** to create security zone **isp2** based on the following parameter values.

Zone Name	isp2
Priority	20

c. Click **OK**.

d. Choose **Network** > **Interface**.

e. In **Interface List**, click on the line of GE0/0/7 and set the following parameters.

Zone	isp2
IPv4	
IP Address	2.2.2.2/24
Default Gateway	2.2.2.254

f. Click **OK**.

Step 2 Configure a security policy to allow a specific intranet segment to access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	trust
Destination Zone	isp1
Source Address	10.3.0.0/24
Action	Permit

3. Click **OK**.
4. Repeat the preceding steps to configure security policy **policy2**.

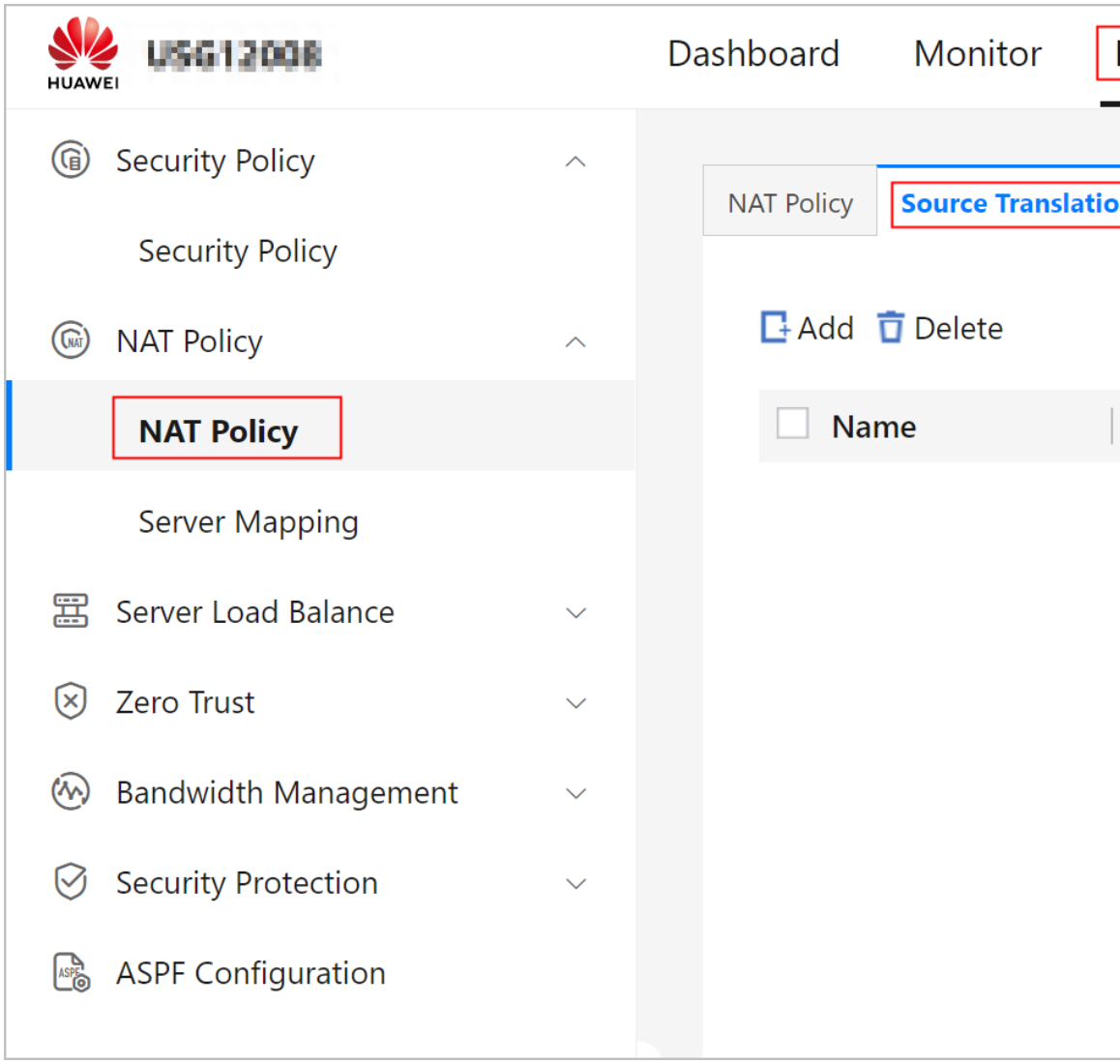
Name	policy2
Source Zone	trust
Destination Zone	isp2
Source Address	10.3.0.0/24
Action	Permit

 Copyright © Huawei Technologies Co., Ltd.

5. Click **OK**.

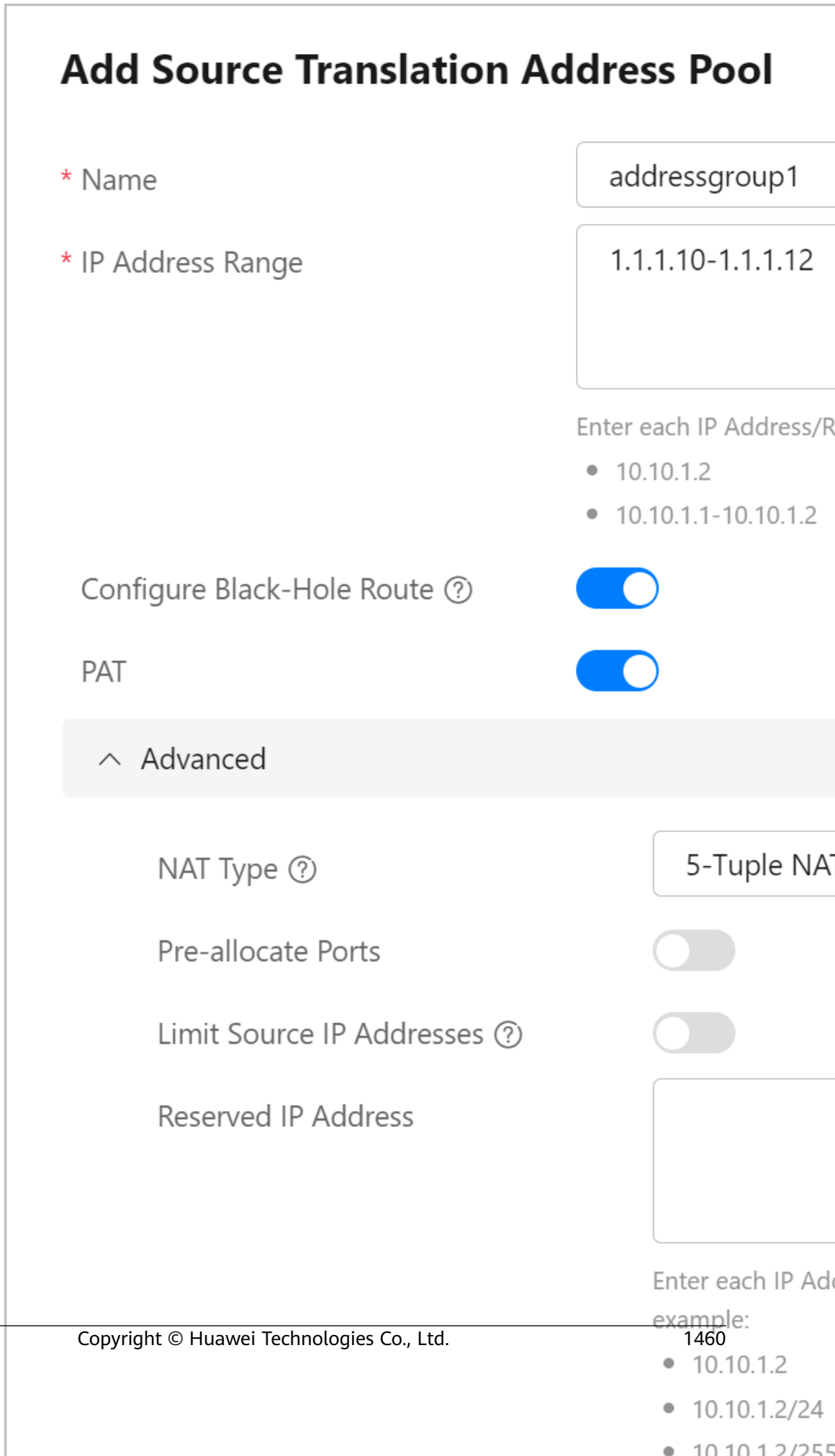
Step 3 Configure a NAT address pool.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.



2. In **Source Translation Address Pool List**, click **Add** and configure the NAT address pool provided by ISP1 based on the following parameter values.

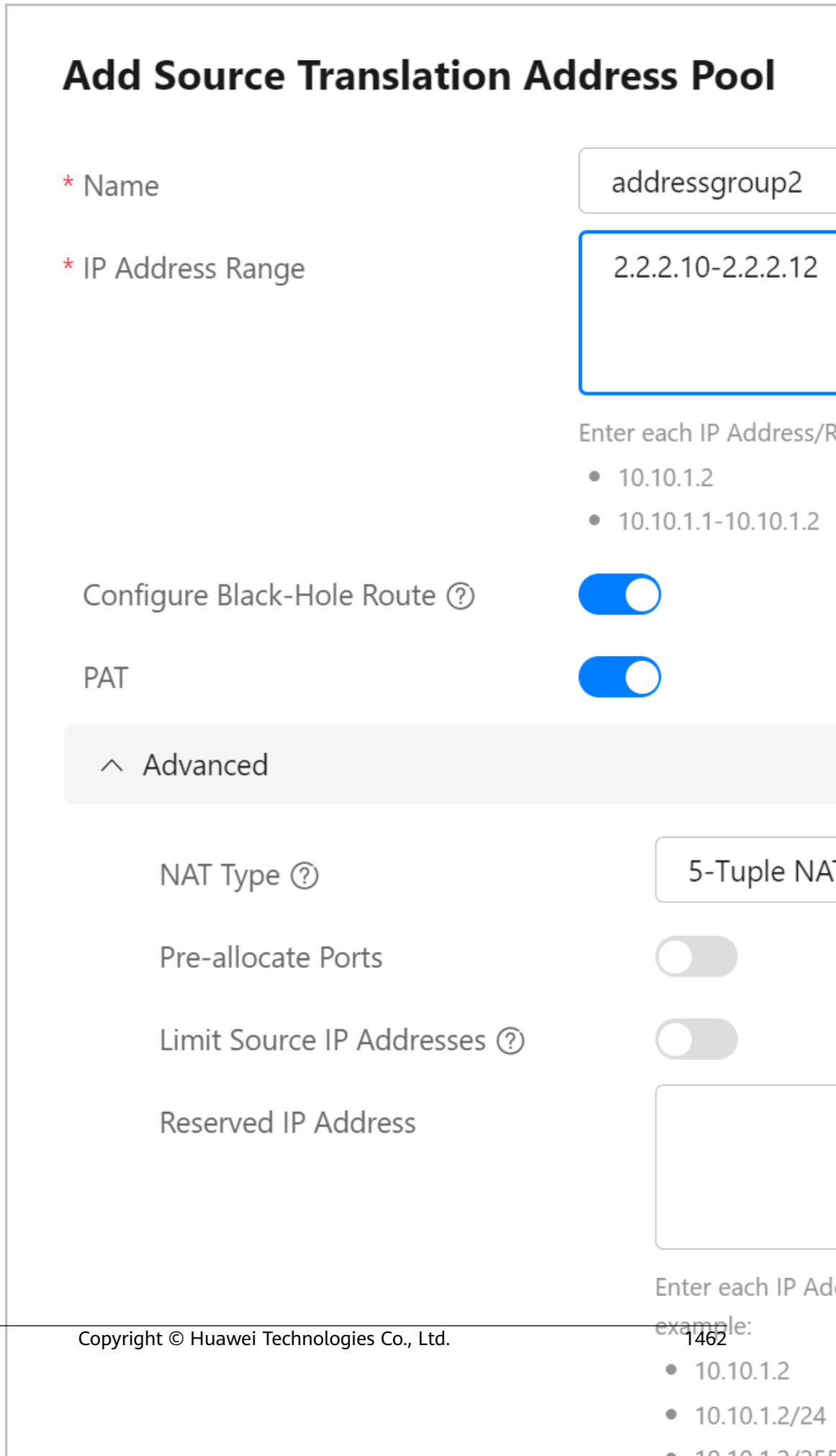
 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

3. Click **OK**.
4. In **Source Translation Address Pool List**, click **Add** and configure the NAT address pool provided by ISP2 based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.

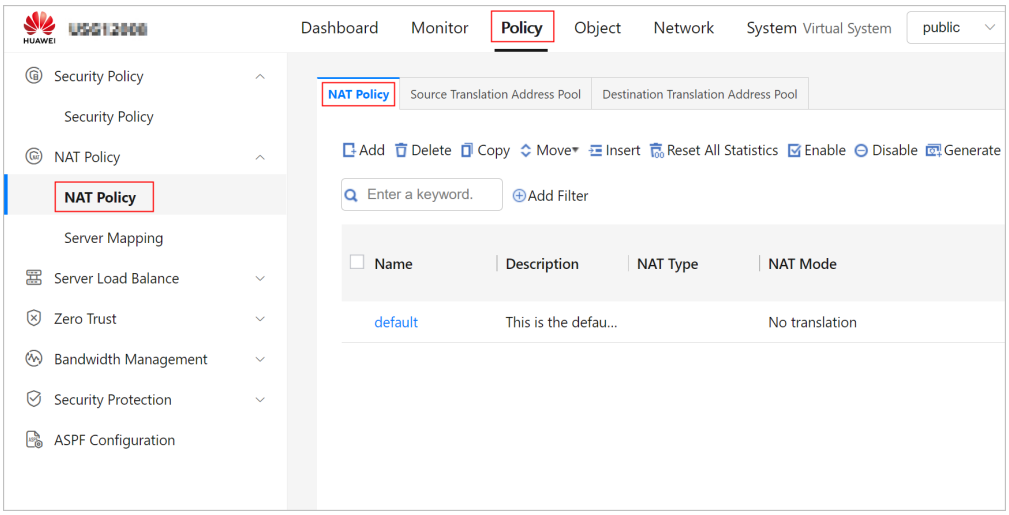


 Copyright © Huawei Technologies Co., Ltd.

5. Click **OK**.

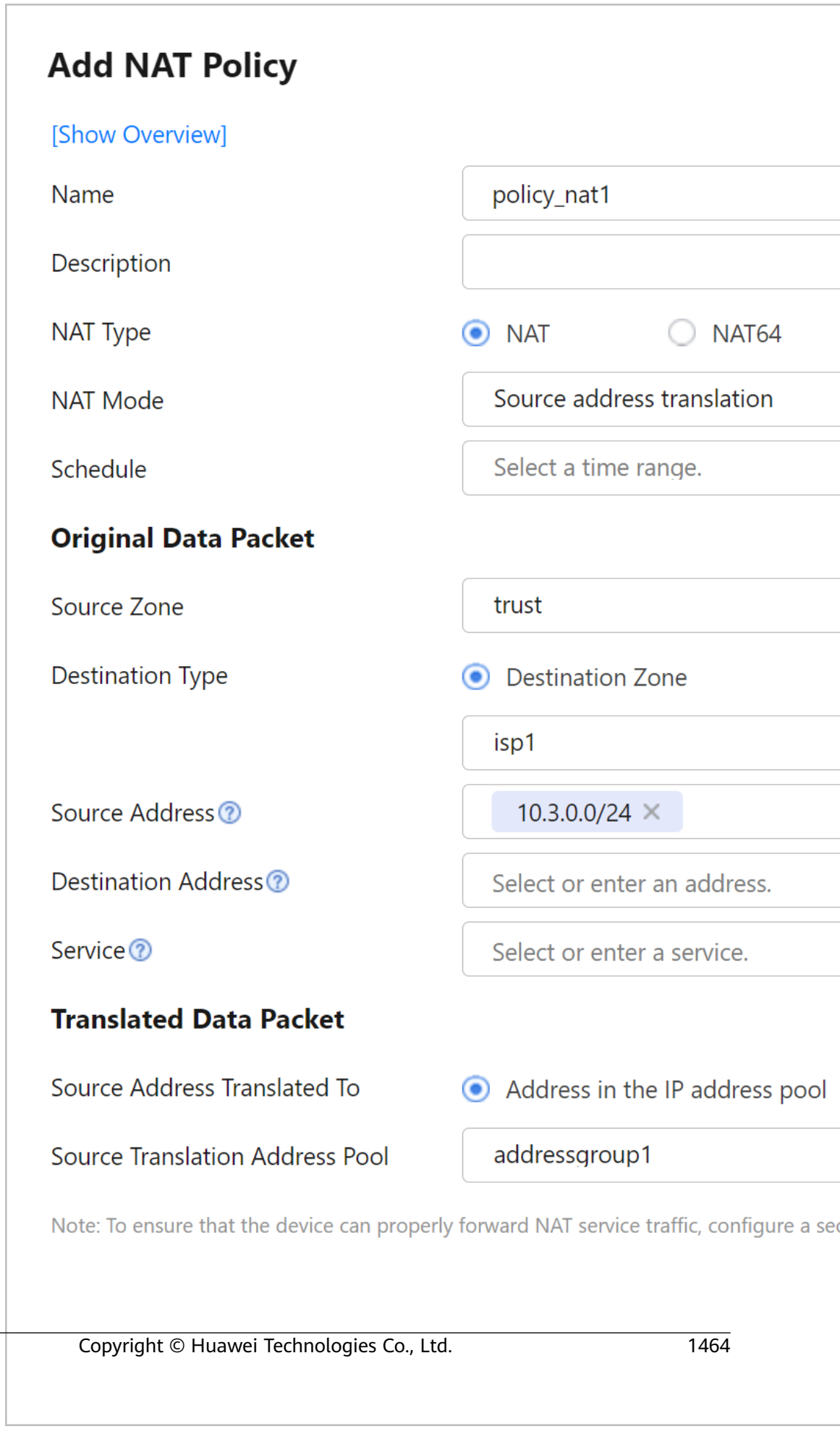
Step 4 Configure a source NAT policy for translating source addresses between private and public address realms when hosts on the specific intranet segment access the Internet.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values, so that intranet users can access the Internet through ISP1 network.

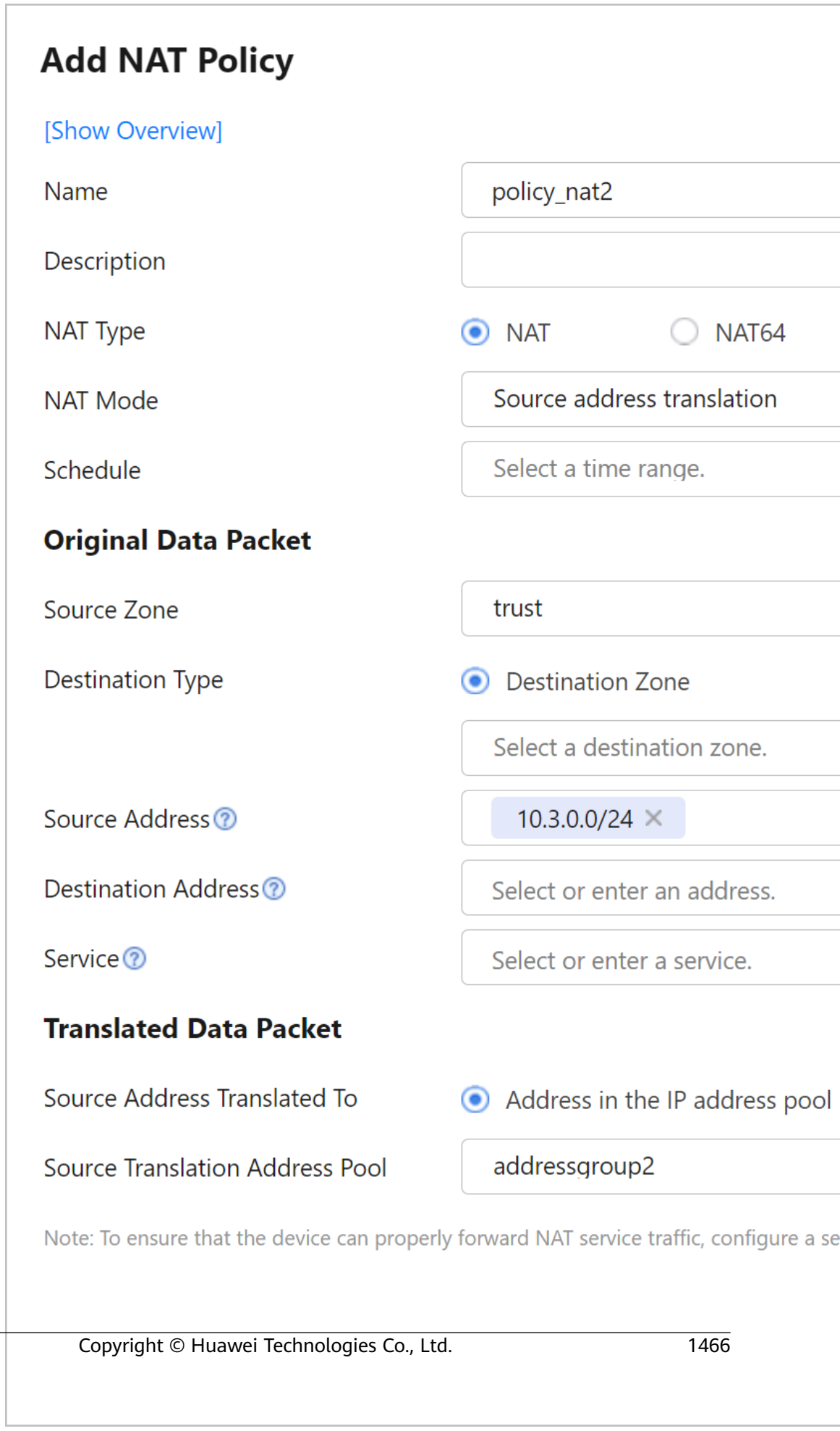
 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

3. Click **OK**.
4. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values, so that intranet users can access the Internet through ISP2 network.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

5. Click **OK**.

Step 5 Configure static routes.

NOTE

In the example, the packets destined for 1.1.2.0/24 and 1.1.3.0/24 are forwarded over ISP1 network, and the packets destined for 2.2.3.0/24 and 2.2.4.0/24 are forwarded over ISP2 network. In actual service configurations, you may need more static routes. Obtain the desired ISP network segment information from your local ISP.

To improve configuration efficiency, you can also use ISP link selection to import ISP routes file and configure ISP routes in batches. For details, see "Route - Intelligent Uplink Selection - Configuring ISP Link Selection" in *Web Configuration Guide-Network*.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a static route through which packets destined for 1.1.2.0/24 are forwarded through ISP1 network.

Protocol	IPv4
Destination Address/Mask	1.1.2.0/255.255.255.0
Next Hop	1.1.1.254

3. Click **OK**.
4. Repeat the preceding steps to configure other static routes. The configuration is omitted.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. When intranet PCs access the Internet, choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.

Configuration Scripts

Configuration script for the device:

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone name isp1 id 4
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 10
 add interface GE0/0/1
#
firewall zone name isp2 id 5
 set priority 20
 add interface GE0/0/7
#
 ip route-static 1.1.2.0 255.255.255.0 1.1.1.254
 ip route-static 1.1.3.0 255.255.255.0 1.1.1.254
 ip route-static 2.2.3.0 255.255.255.0 2.2.2.254
 ip route-static 2.2.4.0 255.255.255.0 2.2.2.254
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.12
#
nat address-group addressgroup2 1
 mode pat
 route enable
 section 0 2.2.2.10 2.2.2.12
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone isp1
    source-address 10.3.0.0 24
    action permit
  rule name policy2
    source-zone trust
    destination-zone isp2
    source-address 10.3.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone isp1
    source-address 10.3.0.0 24
    action source-nat address-group addressgroup1
  rule name policy_nat2
    source-zone trust
    destination-zone isp2
    source-address 10.3.0.0 24
    action source-nat address-group addressgroup2
#
return
```

15.1.11 CLI: Example for Configuring NAPT for Users on a Dual-Egress Intranet to Access the Internet

Networking Requirements

In **Figure 15-11**, an enterprise has deployed DeviceA as a security gateway at the intranet border and purchased broadband services from ISP1 and ISP2 to allow intranet users to access the Internet.

The specific requirements are as follows:

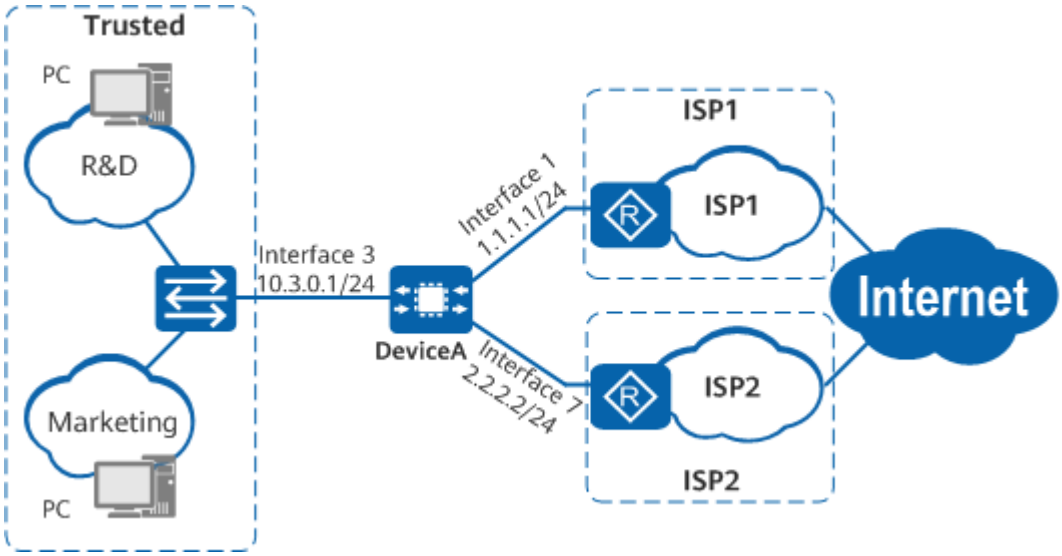
- PCs of the R&D and marketing departments can access the Internet through the networks of ISP1 and ISP2. Traffic sent from intranet PCs to a specific destination on the Internet must be forwarded by the corresponding ISP.
- If the link to one ISP network fails, traffic is immediately switched to the link connected to the other ISP network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-11 Dual uplinks for access to two ISP networks

NOTE

In this example, interfaces 1, 3, and 7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.



The following information is only for reference. The desired service information can be obtained from your ISP.

Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: ISP1 Default gateway address: 1.1.1.254	Public IP address and gateway address assigned by ISP1
GE0/0/3	IP address: 10.3.0.1/24 Security zone: Trust	Set the default gateway address on each intranet host to 10.3.0.1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: ISP2 Default gateway address: 2.2.2.254	Public IP address and gateway address assigned by ISP2
DNS server addresses	9.9.9.9	Provided by ISP1
	11.11.11.11	Provided by ISP2
NAT address pool	1.1.1.10-1.1.1.12	Provided by ISP1
	2.2.2.10-2.2.2.12	Provided by ISP2

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones. Set the default gateway address to 1.1.1.254 for GE 0/0/1 and 2.2.2.254 for GE 0/0/7.
2. Configure static routes to ISP networks.
3. Configure a security policy to allow intranet PCs to access the Internet.
4. Configure a source NAT policy for source address translation.
5. Configure routes on ISP devices to enable them to forward traffic returned by the Internet to DeviceA. This step is performed by ISPs, and the configuration details are not provided.
6. Plan IP addresses for intranet PCs, and set the gateway address to 10.3.0.1 and DNS server addresses to 9.9.9.9 and 11.11.11.11 on each intranet PC. This step is performed by the enterprise network administrator, and the configuration details are not provided.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/3.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
```

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/3 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

Add GE 0/0/1 to the **isp1** zone.

```
[DeviceA] firewall zone name isp1
[DeviceA-zone-isp1] set priority 10
[DeviceA-zone-isp1] add interface ge 0/0/1
[DeviceA-zone-isp1] quit
```

Add GE 0/0/7 to the **isp2** zone.

```
[DeviceA] firewall zone name isp2
[DeviceA-zone-isp2] set priority 20
[DeviceA-zone-isp2] add interface ge 0/0/7
[DeviceA-zone-isp2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone isp1
[DeviceA-policy-security-rule-policy1] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] rule name policy2
[DeviceA-policy-security-rule-policy2] source-zone trust
[DeviceA-policy-security-rule-policy2] destination-zone isp2
[DeviceA-policy-security-rule-policy2] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy2] action permit
[DeviceA-policy-security-rule-policy2] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.12
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
[DeviceA] nat address-group addressgroup2
[DeviceA-address-group-addressgroup2] mode pat
[DeviceA-address-group-addressgroup2] section 0 2.2.2.10 2.2.2.12
[DeviceA-address-group-addressgroup2] route enable
[DeviceA-address-group-addressgroup2] quit
```

Step 4 Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone isp1
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.3.0.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] rule name policy_nat2
[DeviceA-policy-nat-rule-policy_nat2] source-zone trust
[DeviceA-policy-nat-rule-policy_nat2] destination-zone isp2
[DeviceA-policy-nat-rule-policy_nat2] source-address 10.3.0.0 24
[DeviceA-policy-nat-rule-policy_nat2] action source-nat address-group addressgroup2
[DeviceA-policy-nat-rule-policy_nat2] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure static routes.

NOTE

In this example, the packets destined for 1.1.2.0/24 and 1.1.3.0/24 are forwarded over the ISP1 network, and those destined for 2.2.3.0/24 and 2.2.4.0/24 over the ISP2 network. Four static routes are configured in this example. In actual service configurations, you may require more static routes. The desired ISP network segment information can be obtained from your ISP.

To improve configuration efficiency, you can also use ISP link selection to quickly import ISP routes. For details, see "Intelligent Uplink Selection Configuration" in CLI Configuration Guide > Traffic Management Configuration.

```
[DeviceA] ip route-static 1.1.2.0 24 1.1.1.254
[DeviceA] ip route-static 1.1.3.0 24 1.1.1.254
[DeviceA] ip route-static 2.2.3.0 24 2.2.2.254
[DeviceA] ip route-static 2.2.4.0 24 2.2.2.254
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Verify that intranet users can access servers on the Internet over two links.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 http  VPN:public --> public  10.3.0.3:2474[1.1.1.10:3761]-->9.9.9.9:80
 http  VPN:public --> public  10.3.0.9:2479[2.2.2.10:3527]-->11.11.11.11:80
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone name isp1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name isp2 id 5
 set priority 20
 add interface GE0/0/7
#
 ip route-static 1.1.2.0 255.255.255.0 1.1.1.254
 ip route-static 1.1.3.0 255.255.255.0 1.1.1.254
 ip route-static 2.2.3.0 255.255.255.0 2.2.2.254
 ip route-static 2.2.4.0 255.255.255.0 2.2.2.254
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.12
#
nat address-group addressgroup2 1
 mode pat
 route enable
 section 0 2.2.2.10 2.2.2.12
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone isp1
    source-address 10.3.0.0 24
    action permit
  rule name policy2
    source-zone trust
    destination-zone isp2
    source-address 10.3.0.0 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-zone isp1
  source-address 10.3.0.0 24
  action source-nat address-group addressgroup1
 rule name policy_nat2
  source-zone trust
  destination-zone isp2
  source-address 10.3.0.0 24
  action source-nat address-group addressgroup2
#
return
```

15.1.12 Web: Example for Configuring NAPT for Users on a Layer-2 Intranet to Access the Internet

Networking Requirements

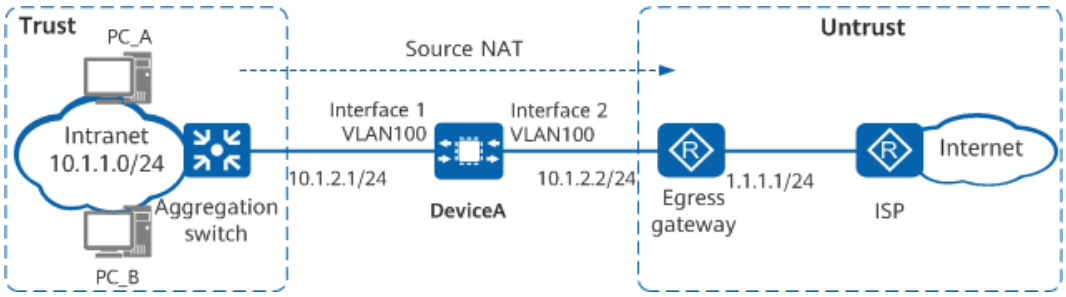
On the network shown in **Figure 15-12**, DeviceA is deployed in transparent mode to ensure the existing network topology remains unchanged. Its uplink and downlink interfaces work in Layer 2 mode.

A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on the egress gateway, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) for address translation.

Figure 15-12 Network diagram of NAT on a device working in transparent mode

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE 0/0/1	VLAN: 100 Security zone: Trust	-
GE 0/0/2	VLAN: 100 Security zone: Untrust	-
Private network segment allowed to access the Internet	10.1.1.0/24	-

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	As private addresses outnumber public addresses, one-to-one mapping cannot be implemented. To translate all private addresses into public addresses, enable port translation.
Routes	Blackhole route on the aggregation switch	Destination address: 1.1.1.10 to 1.1.1.15 Outbound interface: NULL 0	Configure blackhole routes to prevent routing loops that may occur between the aggregation switch and egress gateway when users on the Internet access the post-NAT public addresses.
	Static route on the egress gateway	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 10.1.2.1	-
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Switch interfaces to the Layer 2 mode and add them to a VLAN and security zones.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool and enable port translation.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

Procedure

Step 1 Add the interfaces to security zones, and configure network connectivity

1. Assign GE 0/0/1 to a security zone.
   a. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	trust
Mode	Switching
Connection Type	Access
Access VLAN ID	100

c. Click **OK**.

2. Assign GE 0/0/2 to a security zone.

a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	untrust
Mode	Switching
Connection Type	Access
Access VLAN ID	100

b. Click **OK**.

Step 2 Configure a security policy to allow a specific intranet segment to access the Internet.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

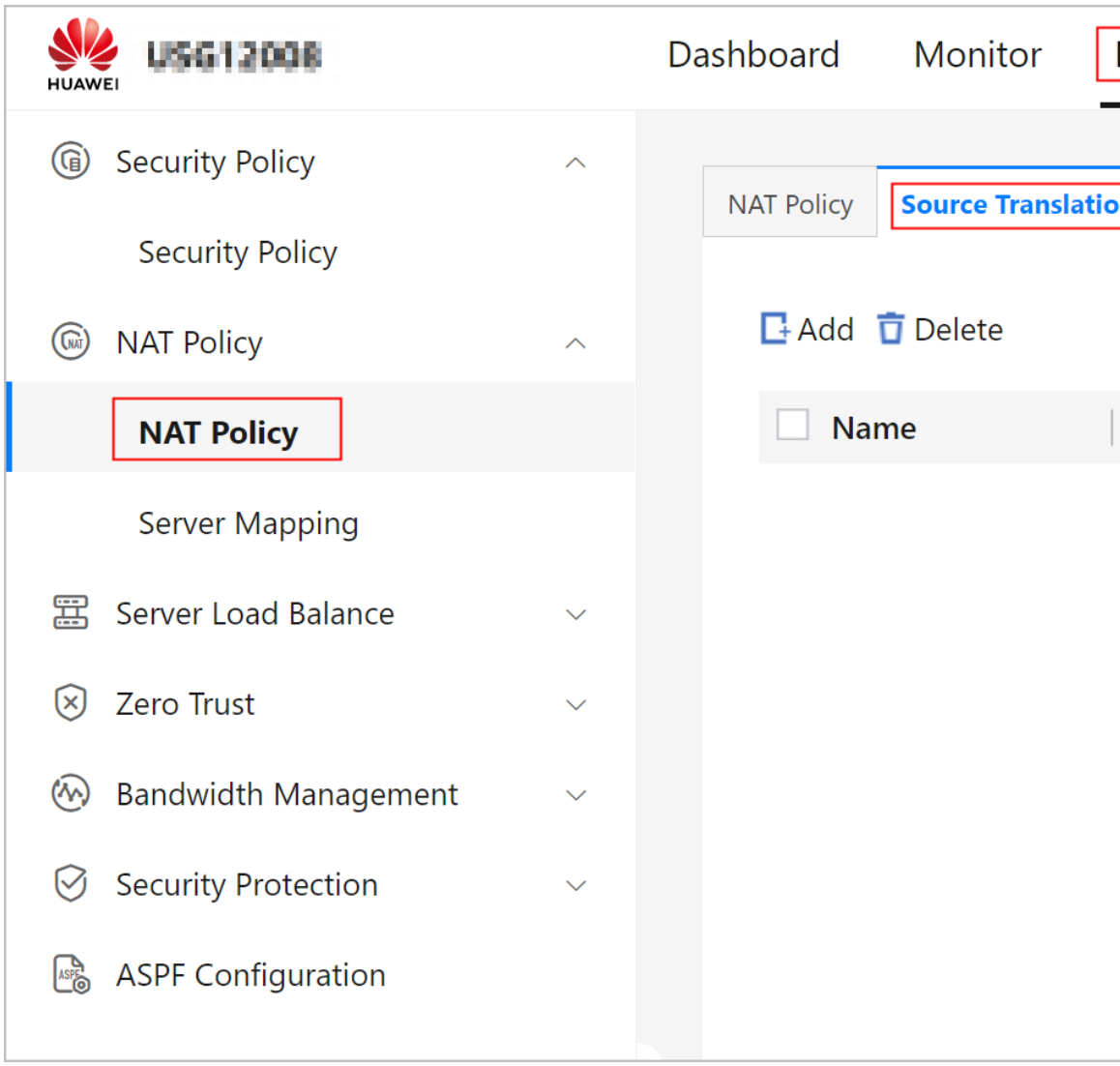
Name	policy1
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure a NAT address pool and a NAT policy.

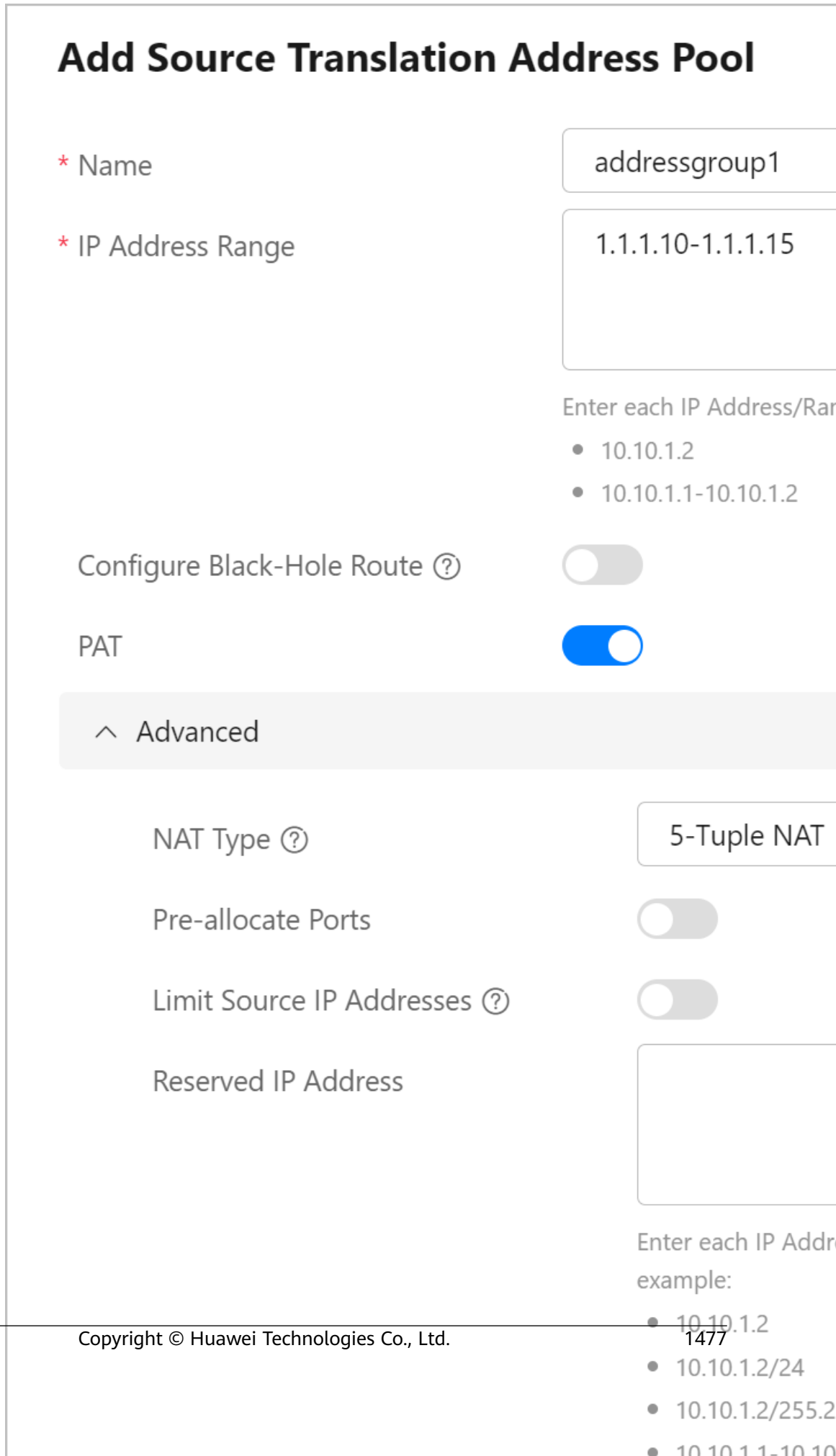
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



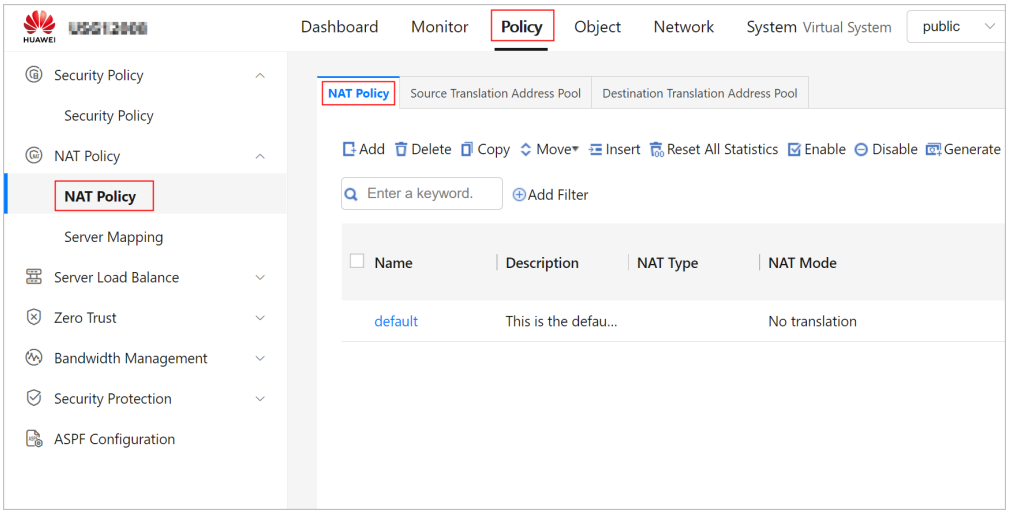
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



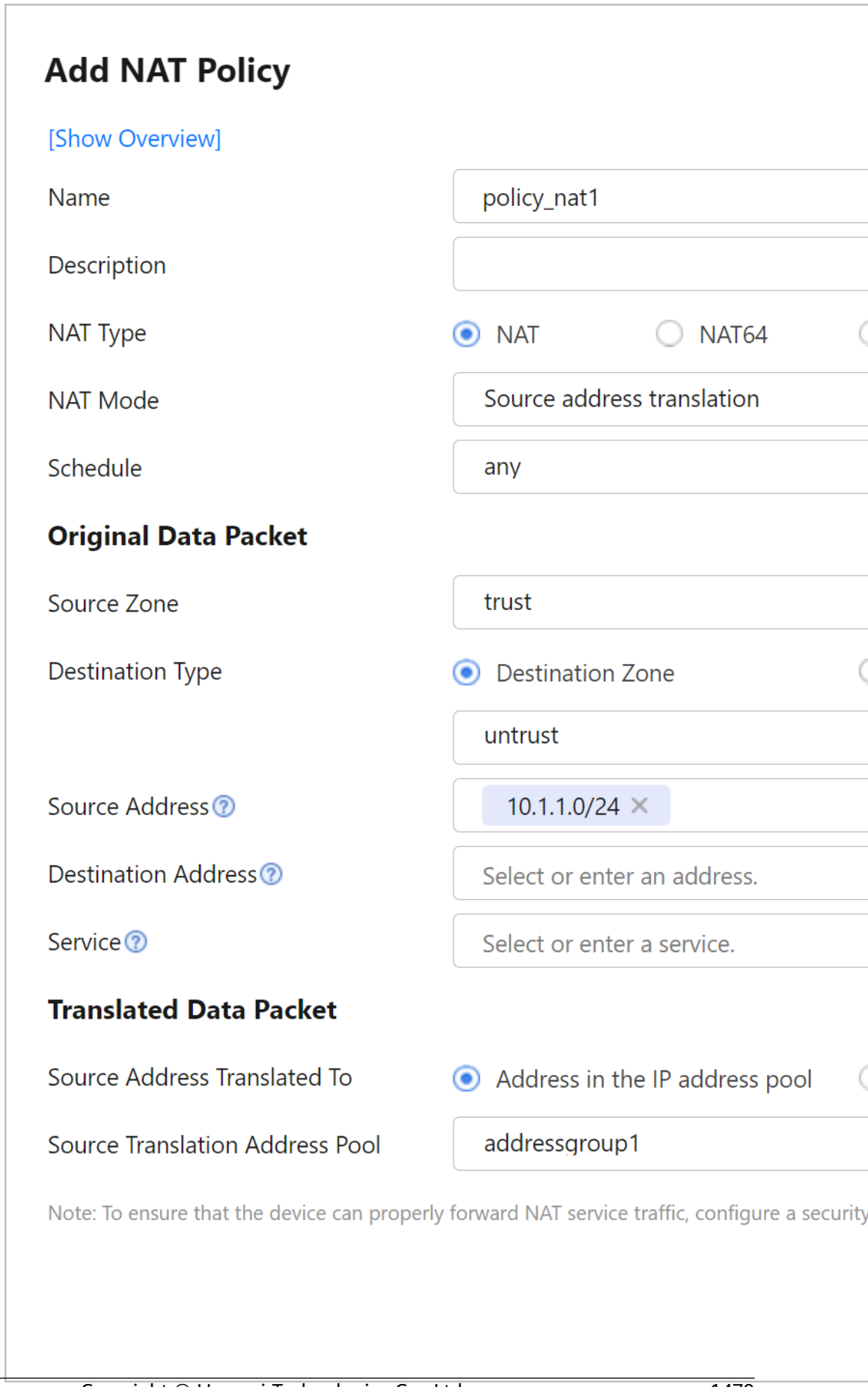
 Copyright © Huawei Technologies Co., Ltd.

3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

6. Click **OK**.

Step 4 Configure black-hole routes to the NAT address pool (1.1.1.10 to 1.1.1.15) on the aggregation switch. The following part uses a Huawei switch to illustrate the configuration:

```
<switch> system-view
[switch] ip route-static 1.1.1.10 32 NULL0
[switch] ip route-static 1.1.1.11 32 NULL0
[switch] ip route-static 1.1.1.12 32 NULL0
[switch] ip route-static 1.1.1.13 32 NULL0
[switch] ip route-static 1.1.1.14 32 NULL0
[switch] ip route-static 1.1.1.15 32 NULL0
```

Step 5 Configure static routes to the NAT address pool (1.1.1.10 to 1.1.1.15) on the egress gateway, with the next hop being 10.1.2.1. The following part uses a Huawei switch to illustrate the configuration:

```
<router> system-view
[router] ip route-static 1.1.1.10 32 10.1.2.1
[router] ip route-static 1.1.1.11 32 10.1.2.1
[router] ip route-static 1.1.1.12 32 10.1.2.1
[router] ip route-static 1.1.1.13 32 10.1.2.1
[router] ip route-static 1.1.1.14 32 10.1.2.1
[router] ip route-static 1.1.1.15 32 10.1.2.1
```

Step 6 Configure static routes to the NAT address pool (1.1.1.10 to 1.1.1.15) on the ISP router, with the next hop being 1.1.1.1, so that traffic returned from the Internet can be forwarded to the enterprise egress gateway.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. When intranet PCs access the Internet, choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
vlan batch 100
#
interface GE 0/0/1
 portswitch
 port link-type access
 port default vlan 100
#
interface GE 0/0/2
 portswitch
 port link-type access
 port default vlan 100
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
nat address-group addressgroup1 0
 mode pat
 section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

15.1.13 CLI: Example for Configuring NAPT for Users on a Layer 2 Intranet to Access the Internet

Networking Requirements

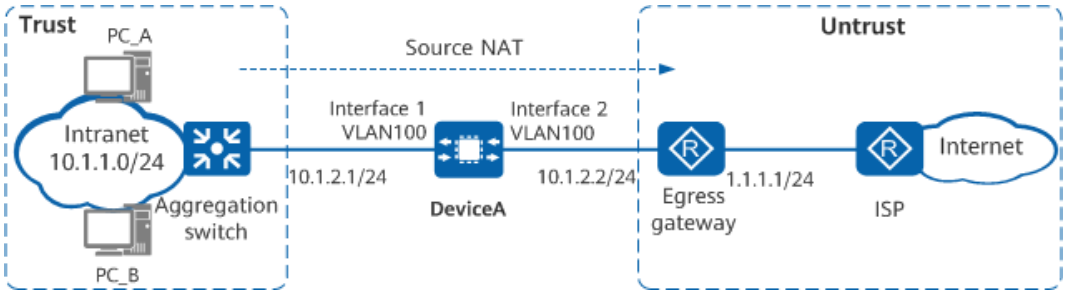
On the network shown in **Figure 15-13**, DeviceA is deployed in transparent mode to ensure the existing network topology remains unchanged. Its uplink and downlink interfaces work in Layer 2 mode.

A source NAT policy needs to be configured on DeviceA so that intranet users on the 10.1.1.0/24 network segment can access the Internet. In addition to the public IP address of the WAN interface on the egress gateway, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) for address translation.

Figure 15-13 Network diagram of NAT on a device working in transparent mode

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	VLAN: 100 Security zone: Trust	-
GE0/0/2	VLAN: 100 Security zone: Untrust	-

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
Private network segment allowed to access the Internet		10.1.1.0/24	-
Post-NAT public addresses		1.1.1.10 to 1.1.1.15	As private addresses outnumber public addresses, one-to-one mapping cannot be implemented. To translate all private addresses into public addresses, enable port translation.
Routes	Blackhole route on the aggregation switch	Destination address: 1.1.1.10 to 1.1.1.15 Outbound interface: NULL 0	Configure blackhole routes to prevent routing loops that may occur between the aggregation switch and egress gateway when users on the Internet access the post-NAT public addresses.
	Static route on the egress gateway	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 10.1.2.1	-
	Static route on the ISP router	Destination address: 1.1.1.10 to 1.1.1.15 Next-hop address: 1.1.1.1	The post-NAT public addresses are not assigned to interfaces, which results in the ISP router not being able to use a routing protocol to discover routes to these public addresses. Therefore, contact the ISP network administrator to configure a static route to the network segment in the address pool on the router.

Configuration Roadmap

1. Switch interfaces to the Layer 2 mode and add them to a VLAN and security zones.
2. Configure a security policy to allow intranet users on a specified network segment to access the Internet.
3. Configure a NAT address pool and enable port translation.
4. Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

Procedure

Step 1 Add interfaces to security zones.

Create a VLAN.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan 100
[DeviceA-vlan100] quit
```

Add GE 0/0/1 to VLAN 100.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] portswitch
[DeviceA-GE0/0/1] port link-type access
[DeviceA-GE0/0/1] port default vlan 100
[DeviceA-GE0/0/1] quit
```

Add GE 0/0/2 to VLAN 100.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] portswitch
[DeviceA-GE0/0/2] port link-type access
[DeviceA-GE0/0/2] port default vlan 100
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 10.1.1.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool and enable port translation.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.1.1.0 24
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure blackhole routes to the NAT address pool (1.1.1.10 to 1.1.1.15) on the aggregation switch. The following provides the configuration on a Huawei switch.

```
<switch> system-view
[switch] ip route-static 1.1.1.10 32 NULL0
[switch] ip route-static 1.1.1.11 32 NULL0
```

 Copyright © Huawei Technologies Co., Ltd.

```
[switch] ip route-static 1.1.1.12 32 NULL0
[switch] ip route-static 1.1.1.13 32 NULL0
[switch] ip route-static 1.1.1.14 32 NULL0
[switch] ip route-static 1.1.1.15 32 NULL0
```

Step 6 Configure static routes to the NAT address pool (1.1.1.10 to 1.1.1.15) on the egress gateway, with the next hop set to 10.1.2.1. The following provides the configuration on a Huawei switch.

```
<router> system-view
[router] ip route-static 1.1.1.10 32 10.1.2.1
[router] ip route-static 1.1.1.11 32 10.1.2.1
[router] ip route-static 1.1.1.12 32 10.1.2.1
[router] ip route-static 1.1.1.13 32 10.1.2.1
[router] ip route-static 1.1.1.14 32 10.1.2.1
[router] ip route-static 1.1.1.15 32 10.1.2.1
```

Step 7 Configure static routes to the NAT address pool (1.1.1.10 to 1.1.1.15) on the ISP router, with the next hop set to 1.1.1.1, so that traffic returned from the Internet can be forwarded to the enterprise egress gateway.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the Internet.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the source addresses being the private addresses of intranet PCs. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.1.1.3:2474[1.1.1.10:3761]-->3.3.3.3:80
```

Configuration Scripts

```
#
 sysname DeviceA
#
vlan batch 100
#
interface GE0/0/1
 portswitch
 port link-type access
 port default vlan 100
#
interface GE0/0/2
 portswitch
 port link-type access
 port default vlan 100
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
nat address-group addressgroup1 0
 mode pat
```

 Copyright © Huawei Technologies Co., Ltd.

```
 route enable
 section 0 1.1.1.10 1.1.1.15
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

15.2 Policy-based Destination NAT

15.2.1 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-one Mappings Between Public and Private IP Addresses)

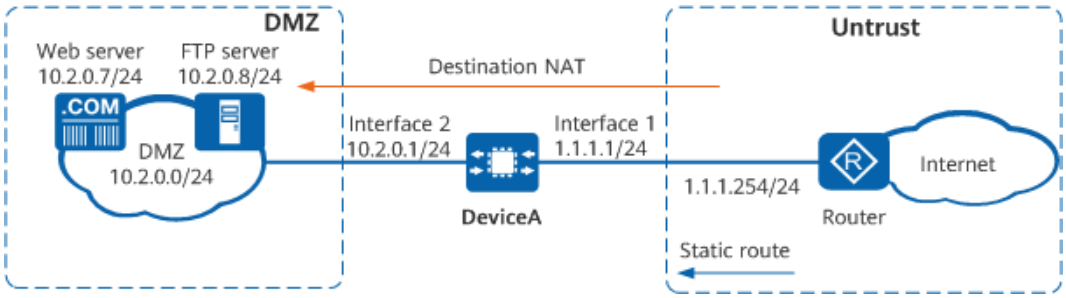
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by intranet servers to provide services to Internet users. **Figure 15-14** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-14 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Destination NAT	Destination address pool: 10.2.0.7 to 10.2.0.8	When an Internet user accesses an intranet server, DeviceA can forward traffic to intranet servers if the destination NAT function is enabled. Public and destination addresses in the address pool are in one-to-one mappings in sequence; that is, DeviceA translates destination address 1.1.10.10 into 10.2.0.7 and destination address 1.1.10.11 into 10.2.0.8.
Default route	Destination address: 0.0.0.0 Next hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA so that it can forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow Internet users to access intranet servers.
3. Configure the destination NAT function to enable DeviceA to forward traffic sent from Internet users to intranet servers.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure static routes to the public addresses of intranet servers on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

 Copyright © Huawei Technologies Co., Ltd.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.

a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

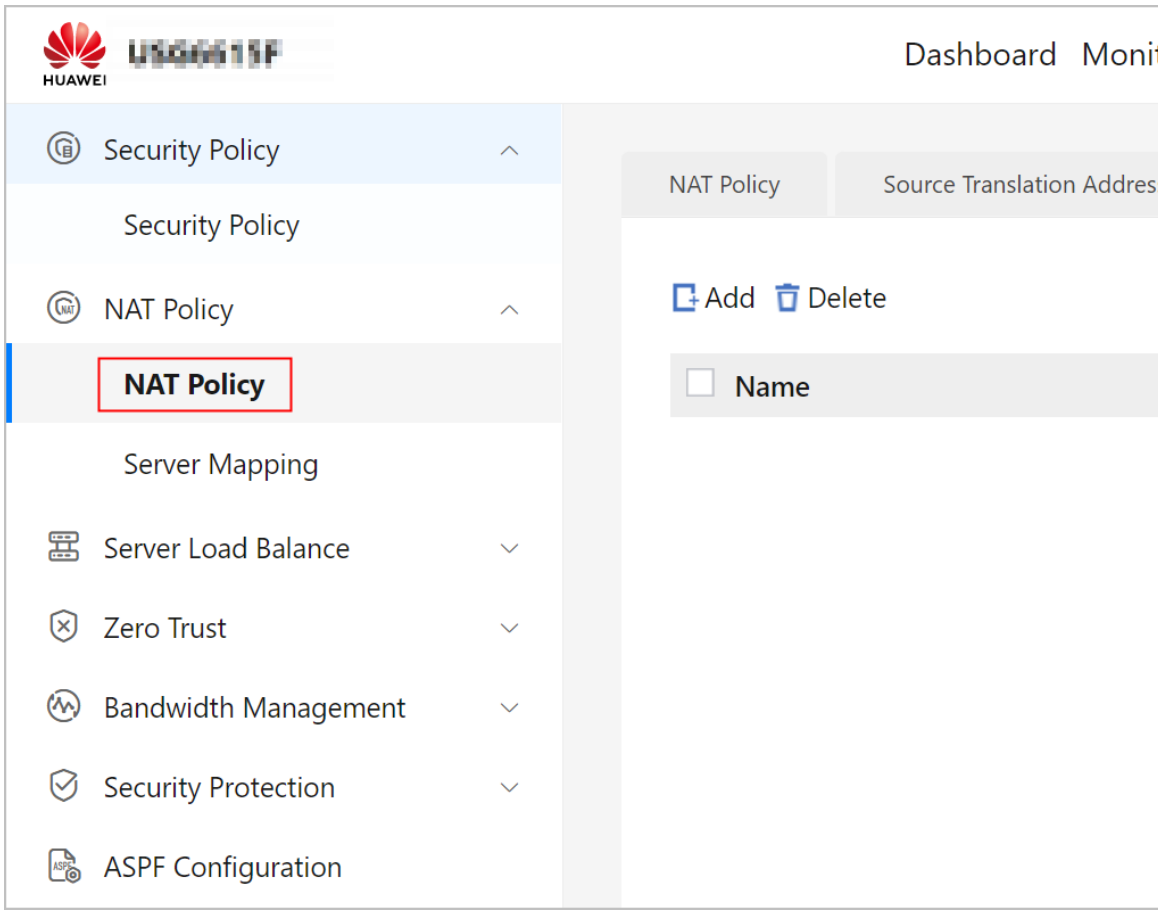
Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT address pools and NAT policies.

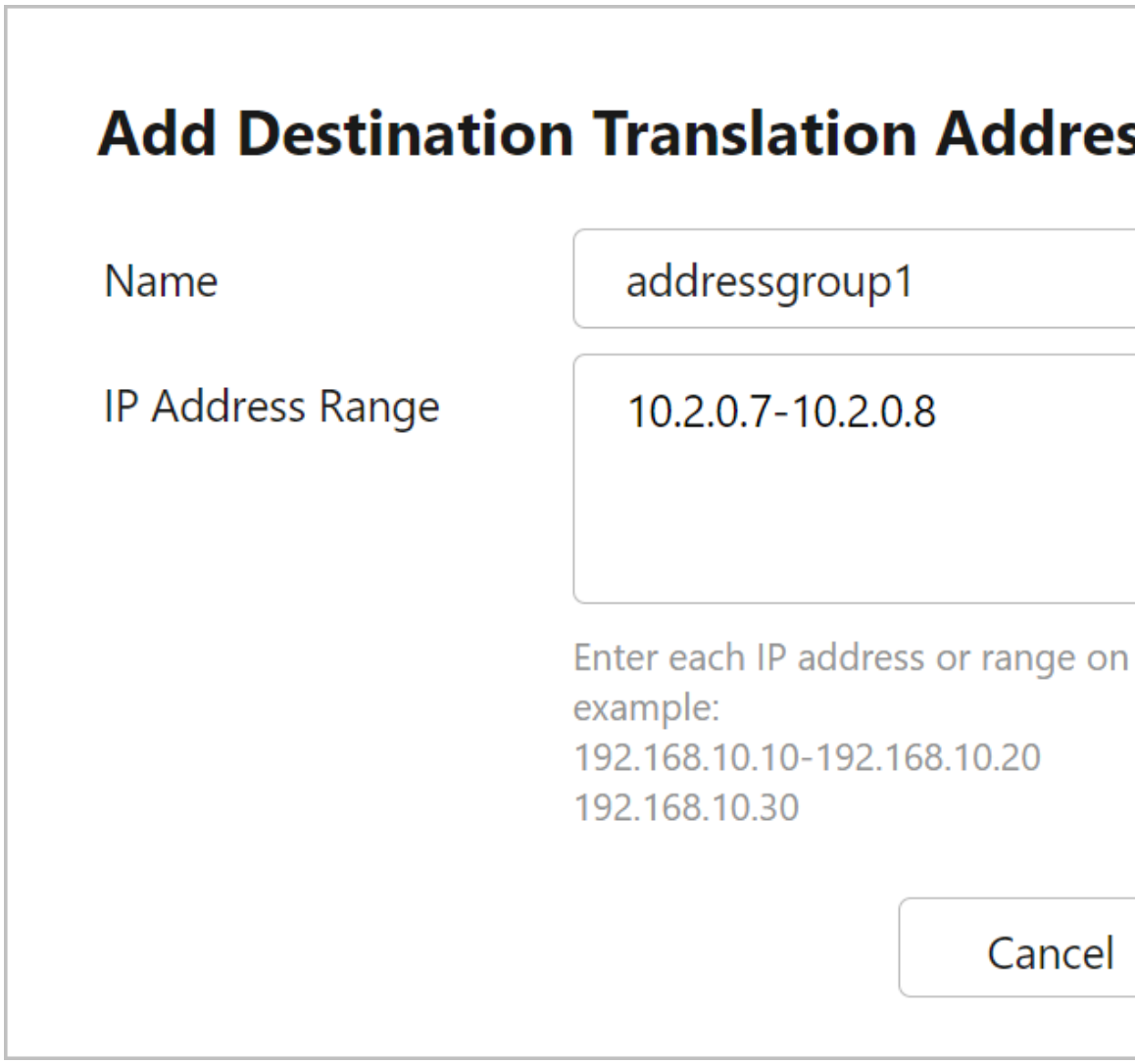
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Destination Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.

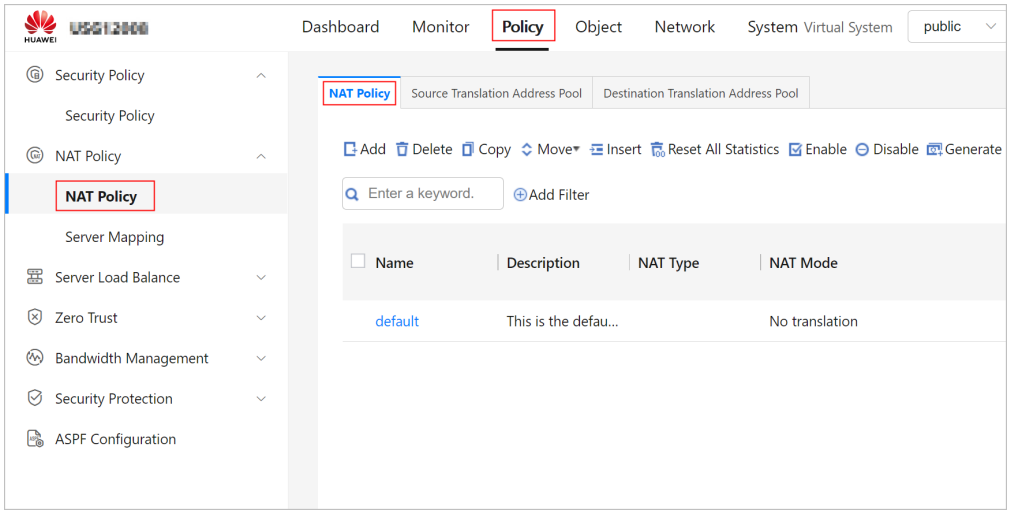


2. In **Destination Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

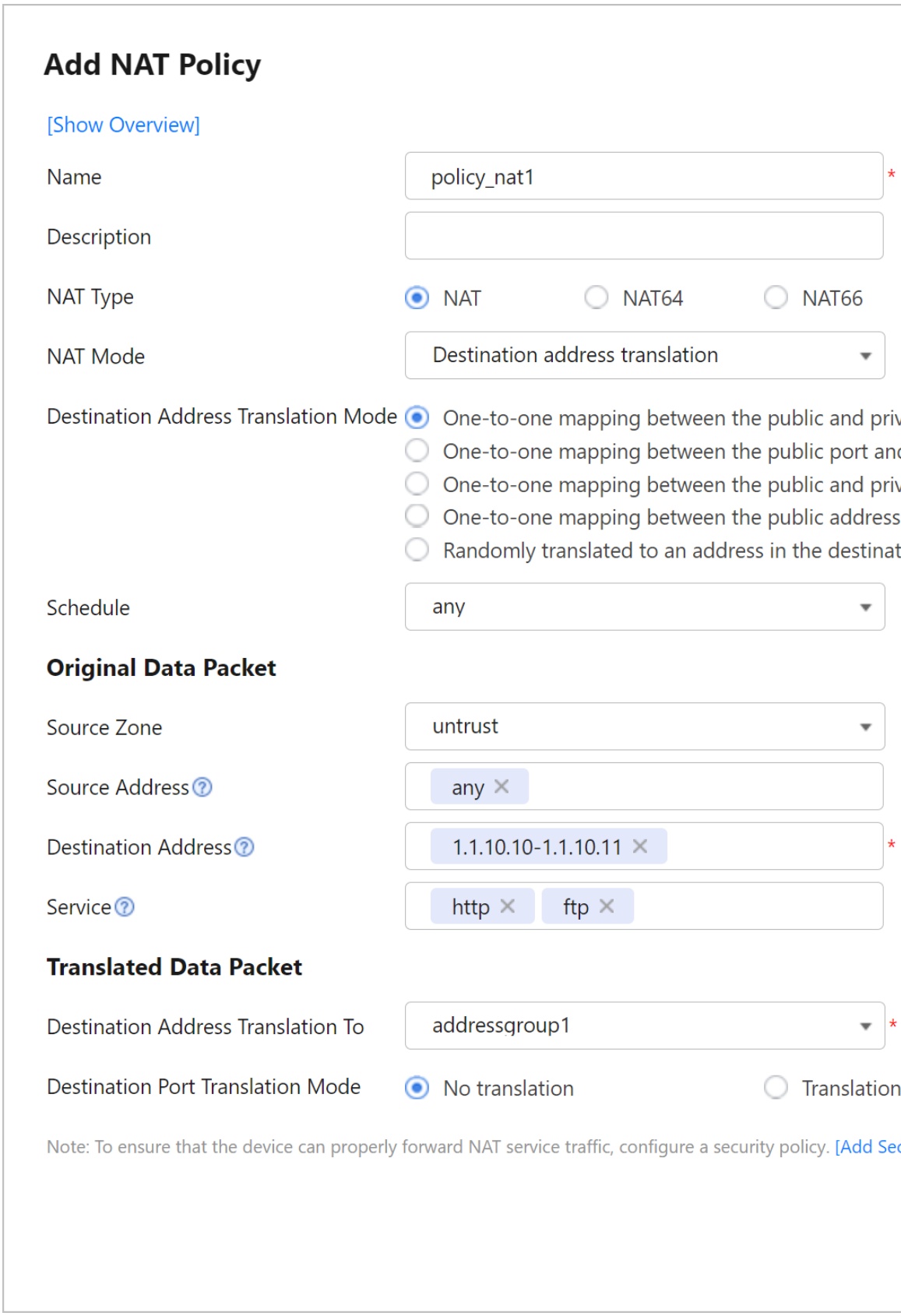


3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

In this example, port translation is not performed. A NAT policy can be configured to translate only one port. If the post-NAT ports of different servers are different, you need to configure a NAT policy for each server. Batch configuration is not supported.

6. Click **OK**.

Step 4 Configure a black-hole route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a black-hole route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	1.1.10.10/255.255.255.0
Outbound Interface	NULL0

3. Repeat the preceding steps to configure the black-hole route as follows.

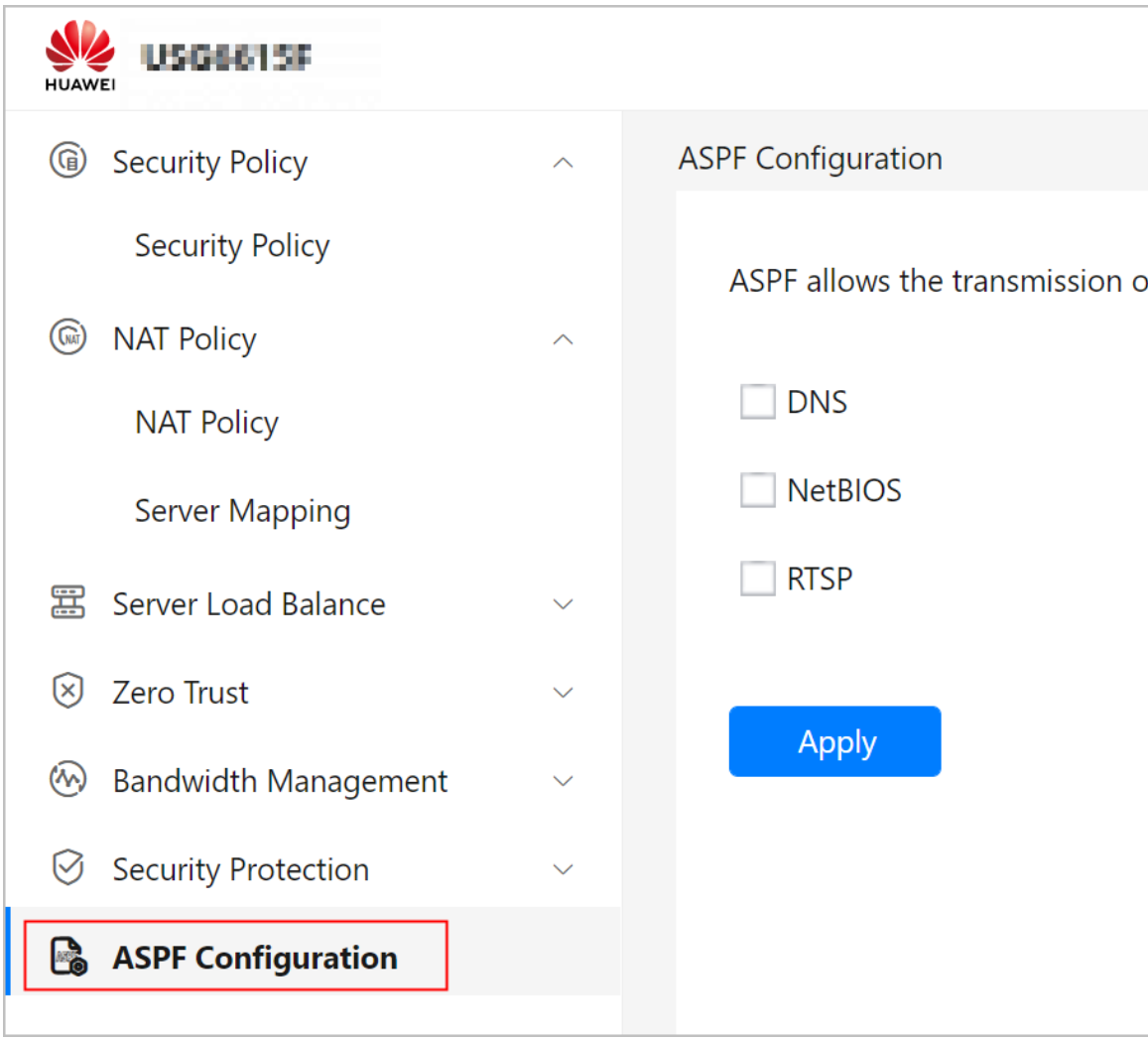
Protocol	IPv4
Destination Address/Mask	1.1.10.11/255.255.255.0
Outbound Interface	NULL0

4. Click **OK**.

Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.



2. Select **FTP**.

Step 6 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 7 Configure a static route to public address (1.1.10.10 and 1.1.10.11) with the next hop being 1.1.1.1 on the router so that traffic destined for the server can be sent to the DeviceA.

Contact your ISP administrator to perform this step.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 1.1.10.11 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1 0
 section 10.2.0.7 10.2.0.8
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address range 1.1.10.10 1.1.10.11
    service http
    service ftp
    action destination-nat static address-to-address address-group addressgroup1
#
return
```

15.2.2 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mappings Between Public and Private Addresses)

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users.

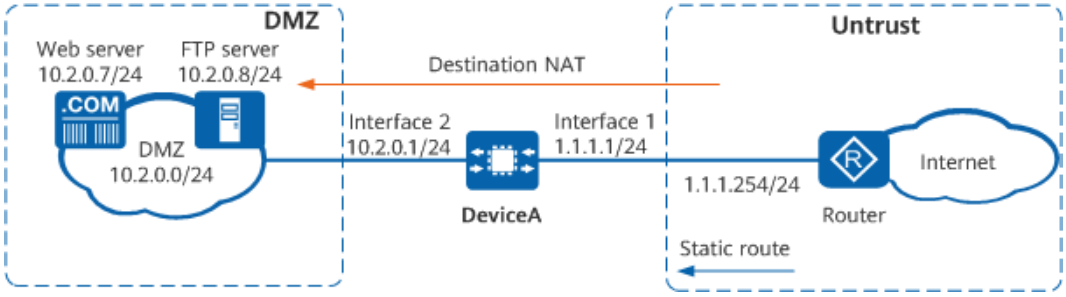
 Copyright © Huawei Technologies Co., Ltd.

In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by intranet servers to provide services to Internet users. **Figure 15-15** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-15 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Destination NAT	Destination address pool: 10.2.0.7 to 10.2.0.8	When an Internet user accesses an intranet server, DeviceA can forward traffic to intranet servers if the destination NAT function is enabled. Public and destination addresses in the address pool are in one-to-one mappings in sequence; that is, DeviceA translates destination address 1.1.10.10 into 10.2.0.7 and destination address 1.1.10.11 into 10.2.0.8.
Default route	Destination address: 0.0.0.0 Next hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA so that it can forward traffic from intranet servers to the ISP router.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure the destination NAT function to enable DeviceA to forward traffic sent from Internet users to intranet servers.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure static routes to the public addresses of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.7 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-nat-rule-policy_nat1] destination-address range 1.1.10.10 1.1.10.11
[DeviceA-policy-nat-rule-policy_nat1] service http
[DeviceA-policy-nat-rule-policy_nat1] service ftp
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static address-to-address address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure blackhole routes to the public addresses of intranet servers to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
[DeviceA] ip route-static 1.1.10.11 255.255.255.255 NULL0
```

Step 6 Enable the NAT application level gateway (ALG) function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 7 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 8 On the ISP router, configure static routes to the public addresses (1.1.10.10 and 1.1.10.11) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet servers to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  1.2.1.3:2474-->1.1.10.10:2080[10.2.0.7:2080]
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall interzone dmz untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 1.1.10.11 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1 0
 section 10.2.0.7 10.2.0.8
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address range 1.1.10.10 1.1.10.11
    service http
    service ftp
    action destination-nat static address-to-address address-group addressgroup1
#
return
```

15.2.3 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mapping Between the Public and Private Ports)

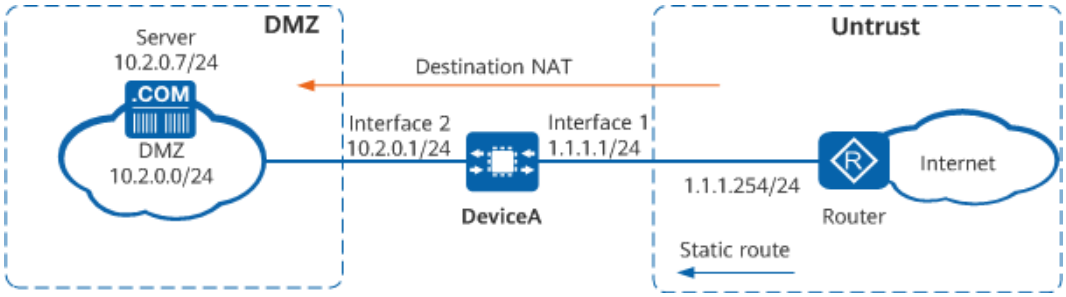
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that an intranet server can provide different services through different ports to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by the intranet server to provide services to Internet users. **Figure 15-16** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-16 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	The intranet server uses 10.2.0.1 as the default gateway address.
Destination NAT	Destination address before translation: 1.1.10.10 Destination address after translation: 10.2.0.7 Ports before translation: 2000 and 2001 Port number after translation: 80 and 81	With the destination NAT function enabled, DeviceA can forward traffic destined for 1.1.10.10 to the intranet server.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from the intranet server to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure the destination NAT function to enable DeviceA to forward traffic originated from Internet users and destined for 1.1.10.10 to the intranet server.
4. Configure a default route on DeviceA to enable it to forward traffic from the intranet server to the ISP router.
5. Configure a static route to the public address of the intranet server on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click  of GE 0/0/1 and set the parameters as follows:

Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.

a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

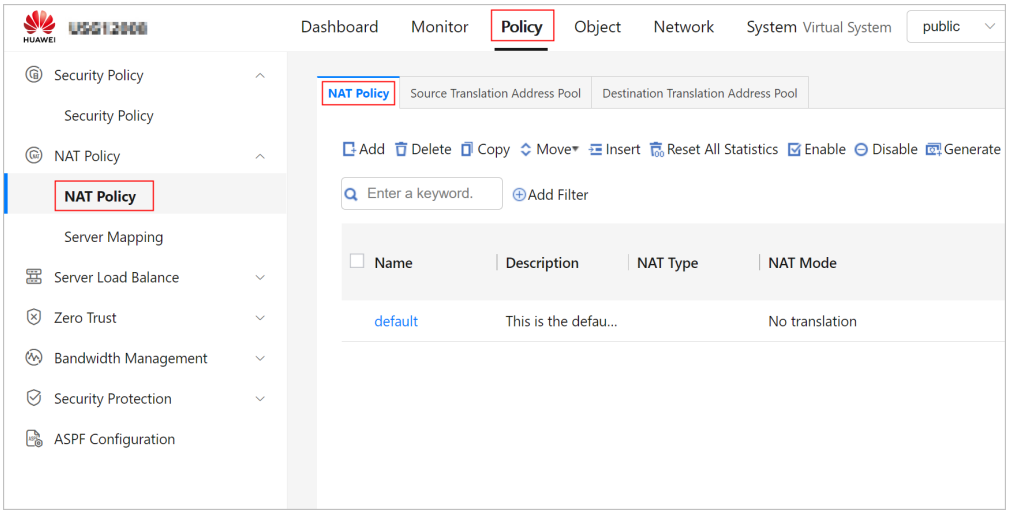
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT policies.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.



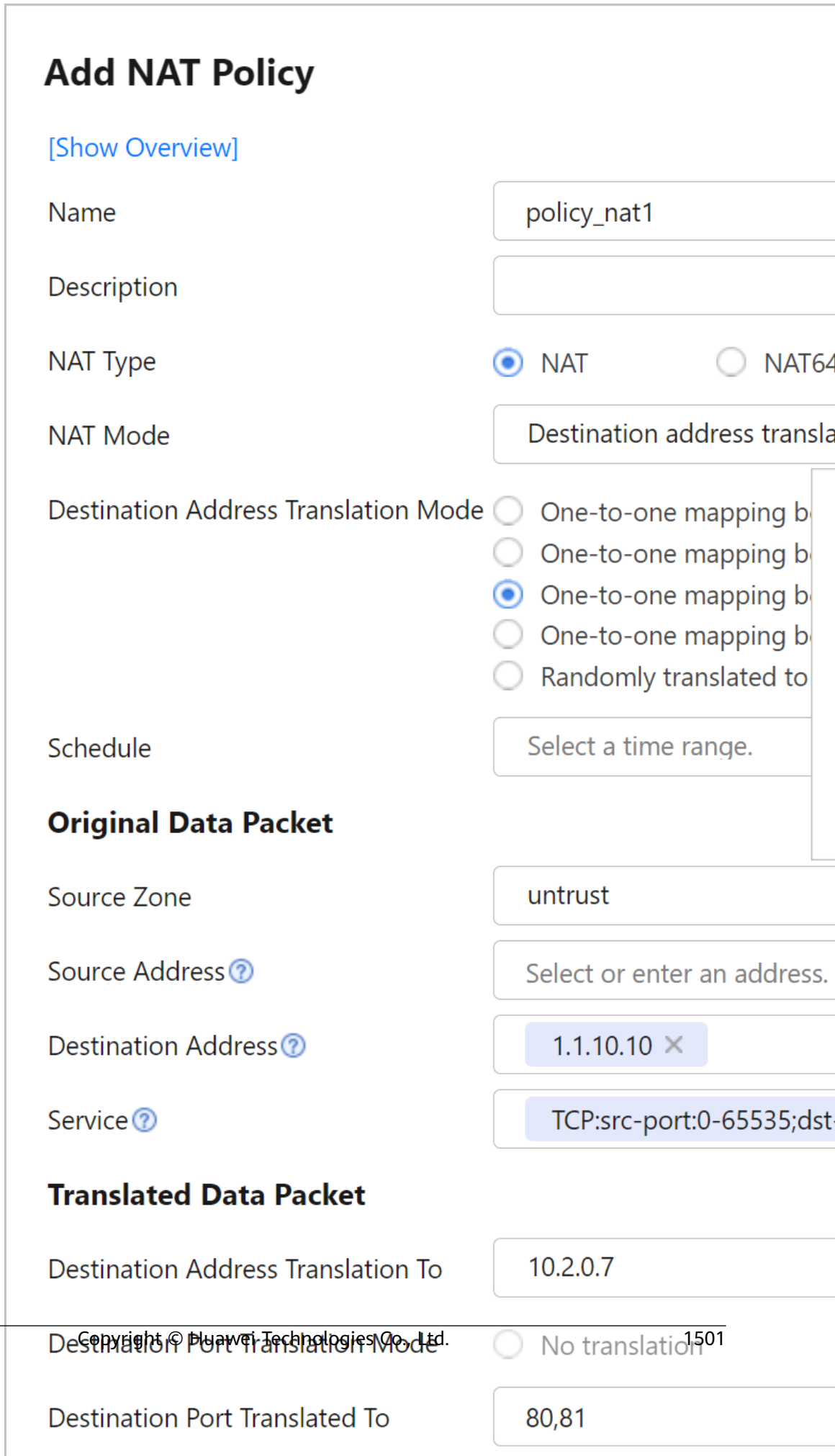
 Copyright © Huawei Technologies Co., Ltd.

2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

   NOTE

   For one-to-one mapping between public and private ports, only one value can be configured for both **Destination Address** and **Destination Address Translation To**. If multiple servers provide external services, configure a NAT policy for each server.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

When configuring **Service**, right-click the input box in the column where **Service** resides and choose **Add** > **Add Protocol or Protocol Number** from the shortcut menu.

3. Click **OK**.

Step 4 Configure a black-hole route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a black-hole route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	1.1.10.10/255.255.255.0
Outbound Interface	NULL0

3. Click **OK**.

Step 5 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 6 Configure a static route to public address (1.1.10.10) with the next hop being 1.1.1.1 on the router so that traffic destined for the server can be sent to the DeviceA.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address 1.1.10.10 32
    service protocol tcp destination-port 2000 to 2001
    action destination-nat static port-to-port address 10.2.0.7 80 to 81
#
return
```

15.2.4 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mappings Between Public and Private Ports)

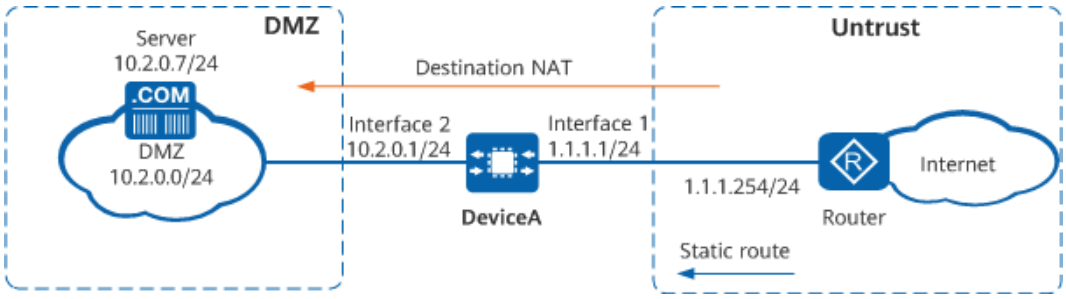
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that an intranet server can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by the intranet server to provide services to Internet users. **Figure 15-17** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-17 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	The intranet server uses 10.2.0.1 as the default gateway address.
Destination NAT	Destination address pool: 10.2.0.7	With the destination NAT function enabled, DeviceA can forward traffic destined for 1.1.10.10 to the intranet server.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from the intranet server to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure the destination NAT function to enable DeviceA to forward traffic originated from Internet users and destined for 1.1.10.10 to the intranet server.
4. Configure a default route on DeviceA to enable it to forward traffic from the intranet server to the ISP router.
5. Configure a static route to the public address of the intranet server on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/2 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.7 10.2.0.7
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy_nat1] service protocol tcp destination-port 2000 to 2001
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static port-to-port address-group
addressgroup1 80 to 81
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a blackhole route to the public address of the intranet server to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
```

Step 6 Configure a default route on DeviceA to enable it to forward traffic from the intranet server to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 7 On the ISP router, configure a static route to the public address (1.1.10.10) of the intranet server, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that an Internet user can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entry with the destination address as the public address of the intranet server. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

 Copyright © Huawei Technologies Co., Ltd.

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 tcp  VPN:public --> public  1.2.1.3:2474-->1.1.10.10:2000[10.2.0.7:80]
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1 0
 section 10.2.0.7 10.2.0.7
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address 1.1.10.10 32
    service protocol tcp destination-port 2000 to 2001
    action destination-nat static port-to-port address-group addressgroup1 80 to 81
#
return
```

15.2.5 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-one Mappings Between Public Ports and Private IP Addresses)

Networking Requirements

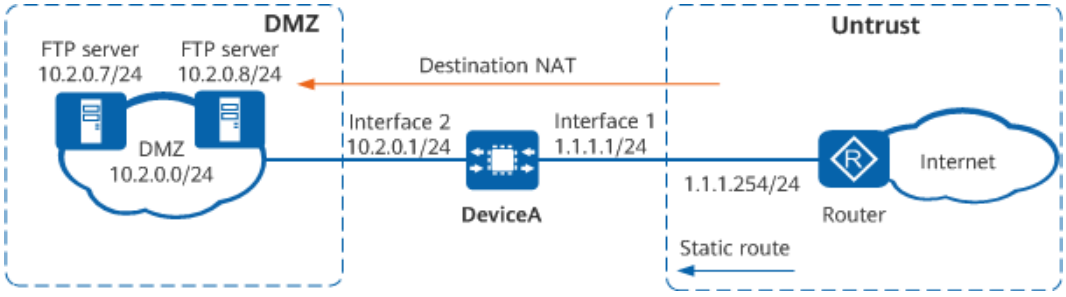
An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the two FTP servers on the enterprise's private network can provide services through different ports (3000 and 3001) of the same public IP address to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by intranet servers to provide services to Internet users. **Figure 15-18** shows the network diagram, in which the router is the access gateway provided by the ISP.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-18 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Destination NAT	Destination address pool: 10.2.0.7 to 10.2.0.8	With the destination NAT function enabled, DeviceA can forward traffic destined for 1.1.10.10 to intranet servers.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure the destination NAT function to enable DeviceA to forward traffic originated from Internet users and destined for 1.1.10.10 to intranet servers.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure static routes to the public address of intranet servers on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

 Copyright © Huawei Technologies Co., Ltd.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

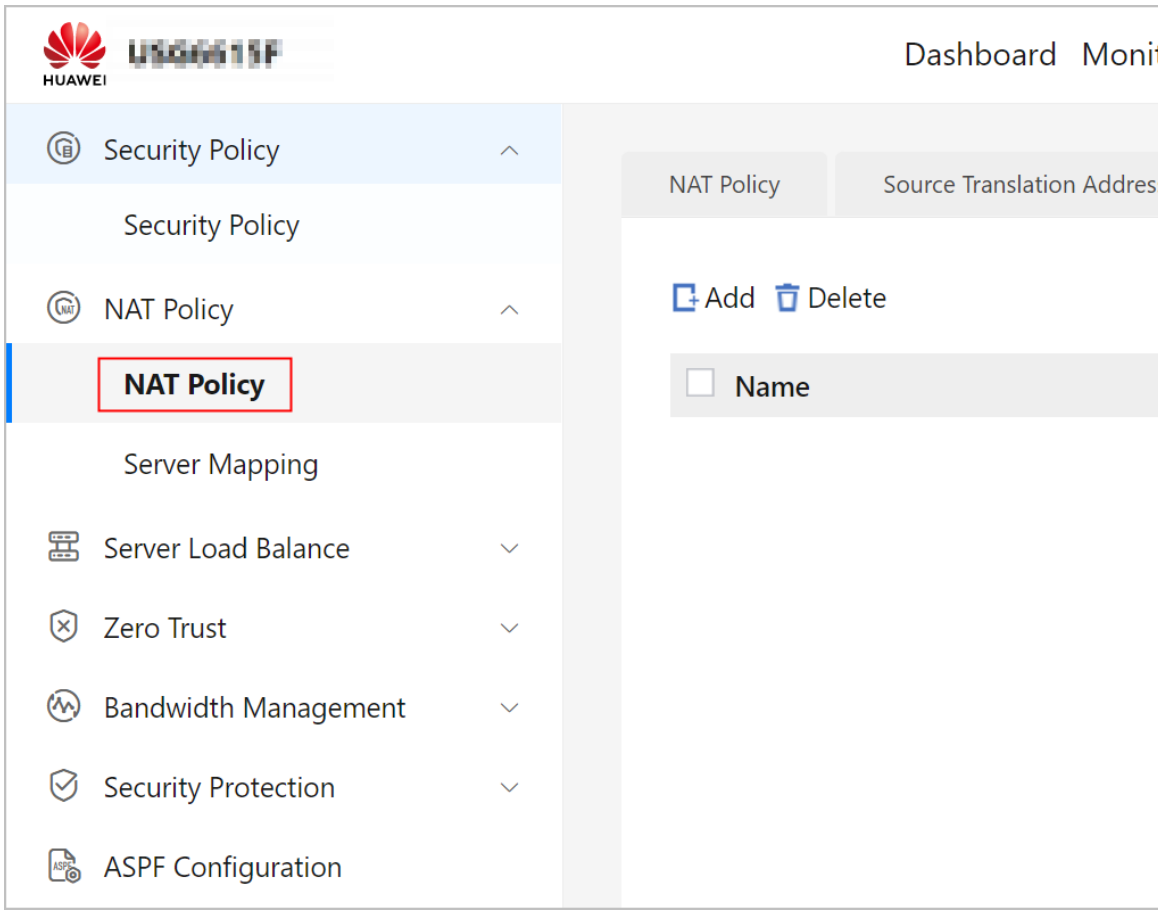
Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT address pools and NAT policies.

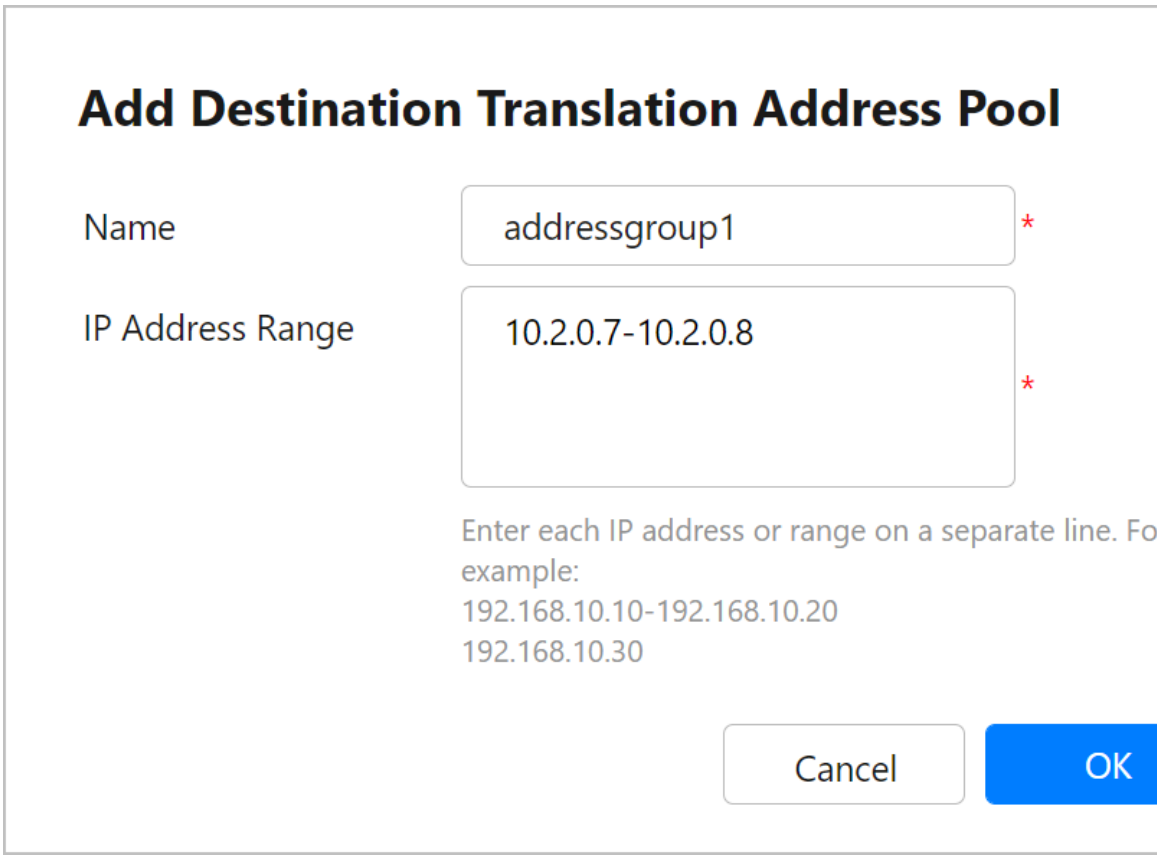
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Destination Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.

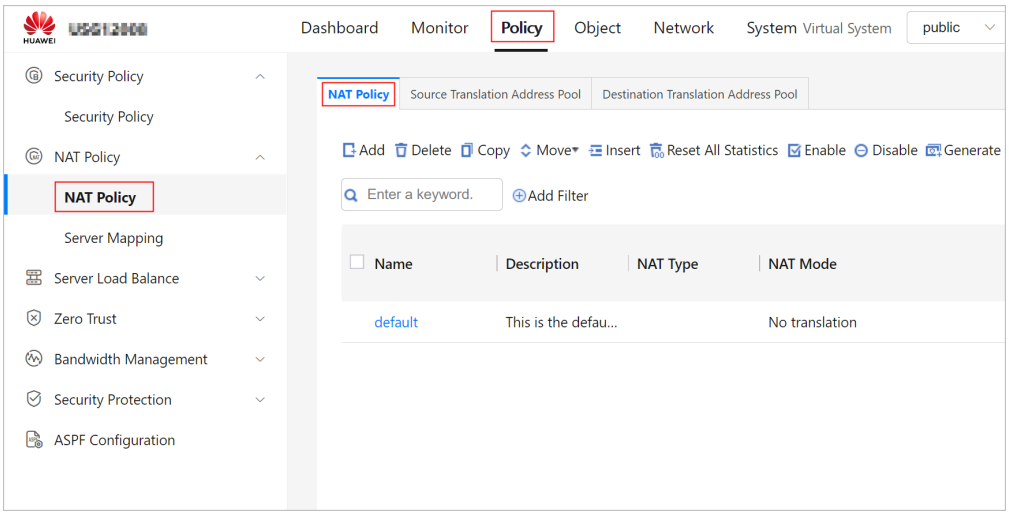


2. In **Destination Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy**.

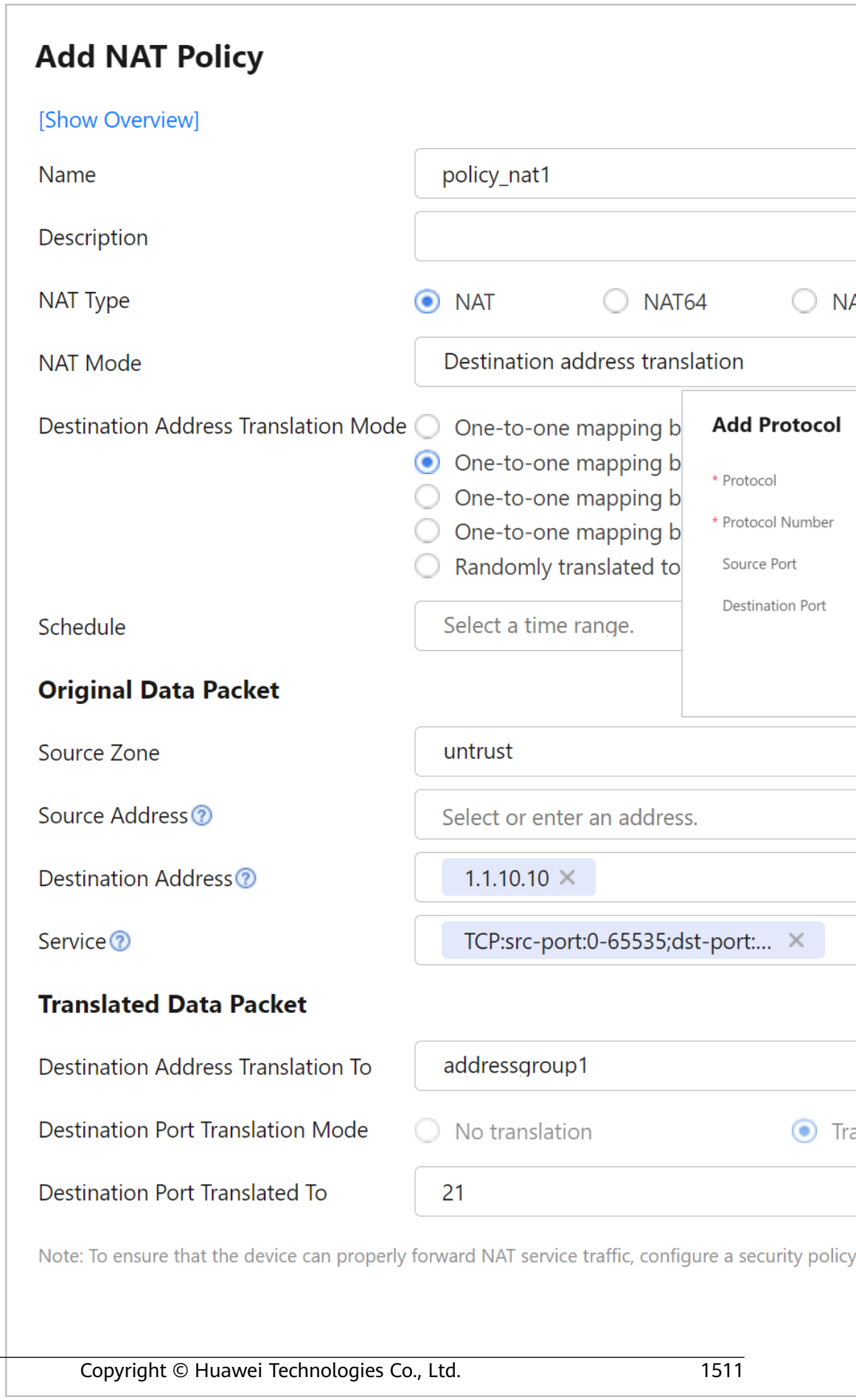


5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

NOTE

For one-to-one mapping between public ports and private IP addresses, only one value can be configured for both **Destination Address** and **Destination Port Translated To**.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

When configuring **Service**, right-click the input box in the column where **Service** resides and choose **Add** > **Add Protocol or Protocol Number** from the shortcut menu.

6. Click **OK**.

Step 4 Configure a black-hole route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

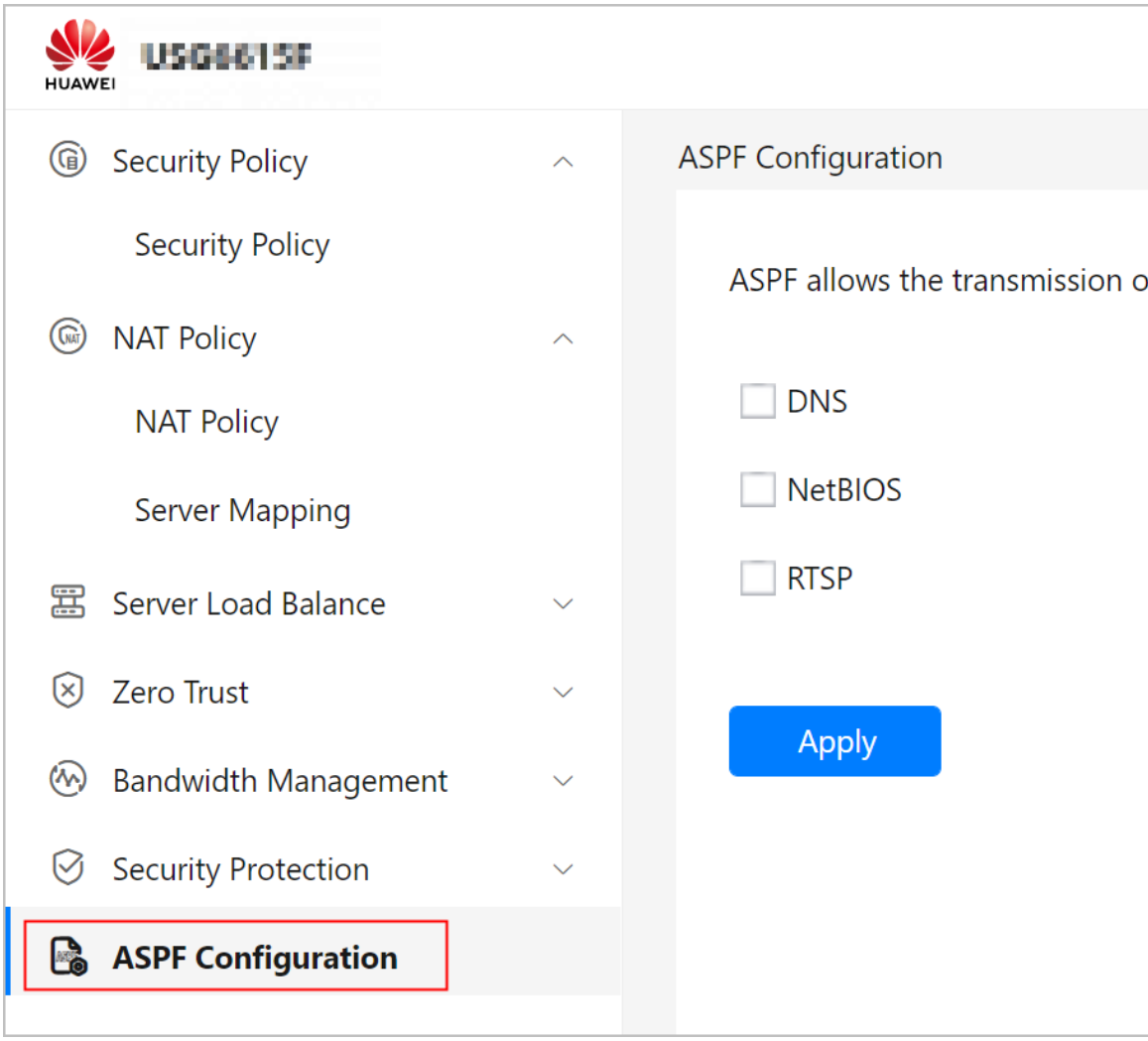
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a black-hole route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	1.1.10.10/255.255.255.0
Outbound Interface	NULL0

3. Click **OK**.

Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.



 Copyright © Huawei Technologies Co., Ltd.

2. Select **FTP**.

Step 6 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 7 On the router, configure a static route, in which the destination address is 1.1.10.10 and the next-hop address is 1.1.1.1. The router directs traffic destined for 1.1.10.10 to the DeviceA based on the static route so that the DeviceA can forward the traffic to the intranet server.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1 0
 section 10.2.0.7 10.2.0.8
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address 1.1.10.10 32
    service protocol tcp destination-port  3000 to 3001
    action destination-nat static port-to-address address-group addressgroup1 21
#
return
```

15.2.6 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-one Mappings Between Public Ports and Private Addresses)

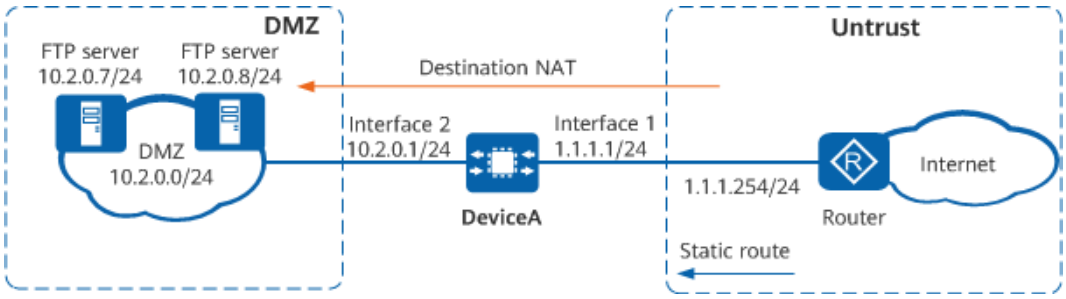
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by intranet servers to provide services to Internet users. **Figure 15-19** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-19 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Destination NAT	Destination address pool: 10.2.0.7 to 10.2.0.8	With the destination NAT function enabled, DeviceA can forward traffic destined for 1.1.10.10 to intranet servers.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure the destination NAT function to enable DeviceA to forward traffic originated from Internet users and destined for 1.1.10.10 to intranet servers.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure static routes to the public address of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure a security policy so that Internet users can access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.7 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy_nat1] service protocol tcp destination-port 3000 to 3001
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static port-to-address address-group addressgroup1 21
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a blackhole route to the public address of intranet servers to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 7 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 8 On the ISP router, configure a static route to the public address (1.1.10.10) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet servers to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entry with the destination address as the public address of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 tcp  VPN:public --> public  1.2.1.3:2474-->1.1.10.10:3000[10.2.0.7:21]
```

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1 0
 section 10.2.0.7 10.2.0.8
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address 1.1.10.10 32
    service protocol tcp destination-port  3000 to 3001
    action destination-nat static port-to-address address-group addressgroup1 21
#
return
```

15.2.7 Web: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mapping Between the Public Address and Private Port)

Networking Requirements

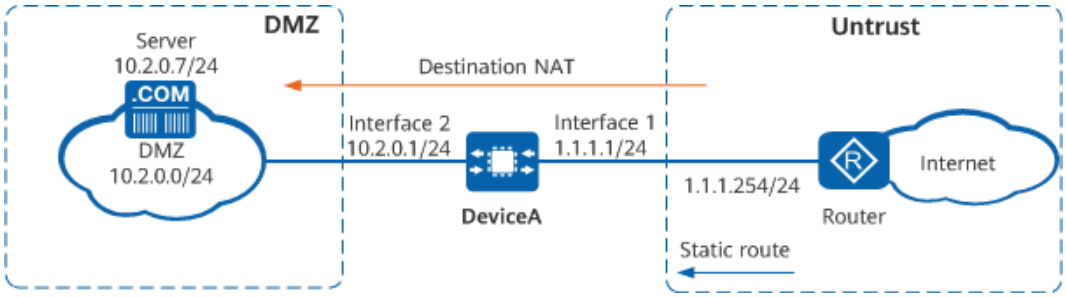
An enterprise has deployed DeviceA as a security gateway at the intranet border. An intranet server provides different services through different ports (80 and 81) and advertises different public IP addresses to the Internet users for different services. Destination NAT needs to be configured on DeviceA so that an intranet server can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by the intranet server to provide different services to Internet users. **Figure 15-20** shows the network diagram, in which the router is the access gateway provided by the ISP.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-20 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	The intranet server uses 10.2.0.1 as the default gateway address.
Destination NAT	Destination address pool: 10.2.0.7	With the destination NAT function enabled, DeviceA can forward traffic to the intranet server.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from the intranet server to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure the destination NAT function to enable DeviceA to forward traffic sent from Internet users to the intranet server.
4. Configure a default route on DeviceA to enable it to forward traffic from the intranet server to the ISP router.
5. Configure static routes to the public addresses of the intranet server on the ISP router.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

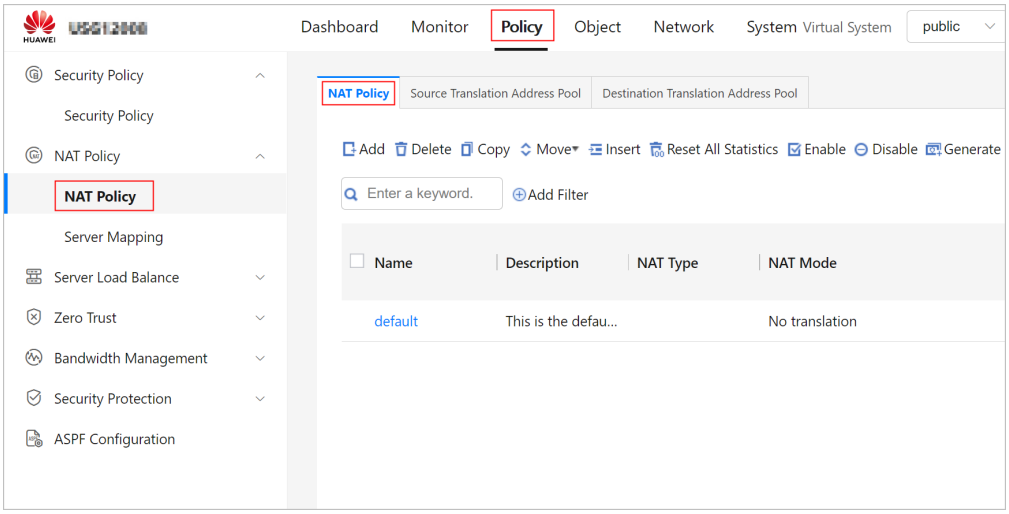
Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT policies.

1. Choose **Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.

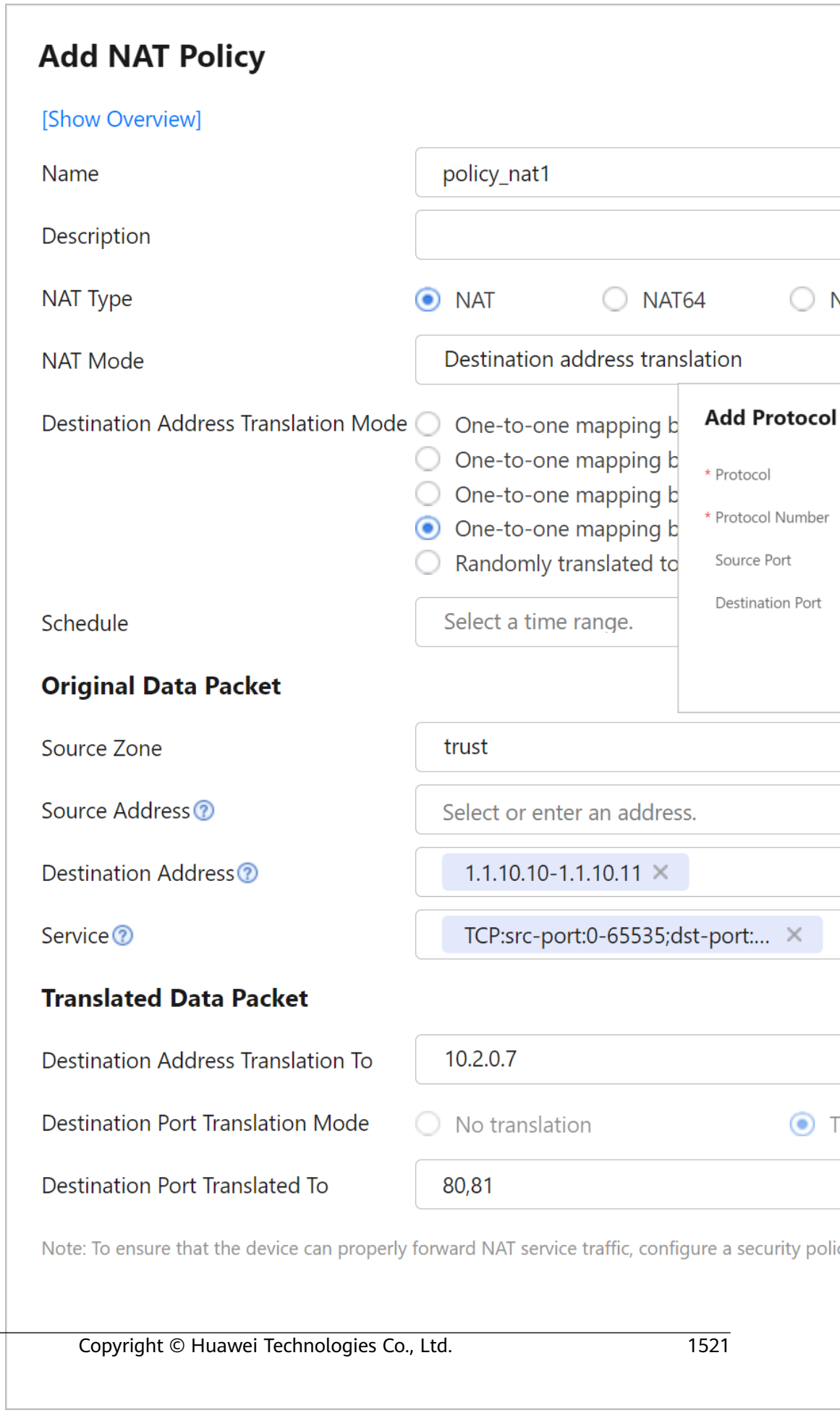


2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

   NOTE

   For one-to-one mapping between public IP addresses and private port numbers, only one value can be configured for both **Service** and **Destination Address Translation To**. If multiple servers are involved, configure a NAT policy for each server.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

When configuring **Service**, right-click the input box in the column where **Service** resides and choose **Add** > **Add Protocol or Protocol Number** from the shortcut menu.

3. Click **OK**.

Step 4 Configure a black-hole route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a black-hole route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	1.1.10.10/255.255.255.0
Outbound Interface	NULL0

3. Repeat the preceding steps to configure the black-hole route as follows.

Protocol	IPv4
Destination Address/Mask	1.1.10.11/255.255.255.0
Outbound Interface	NULL0

4. Click **OK**.

Step 5 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 6 Configure a static route to public address (1.1.10.10 and 1.1.10.11) with the next hop being 1.1.1.1 on the router so that traffic destined for the server can be sent to the DeviceA.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.

 Copyright © Huawei Technologies Co., Ltd.

2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 1.1.10.11 255.255.255.255 NULL0
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address range 1.1.10.10 1.1.10.11
    service protocol tcp destination-port 2000
    action destination-nat static address-to-port address 10.2.0.7 80 to 81
#
return
```

15.2.8 CLI: Example for Configuring Destination NAT for Internet Users to Access Intranet Servers (One-to-One Mappings Between Public Addresses and Private Ports)

Networking Requirements

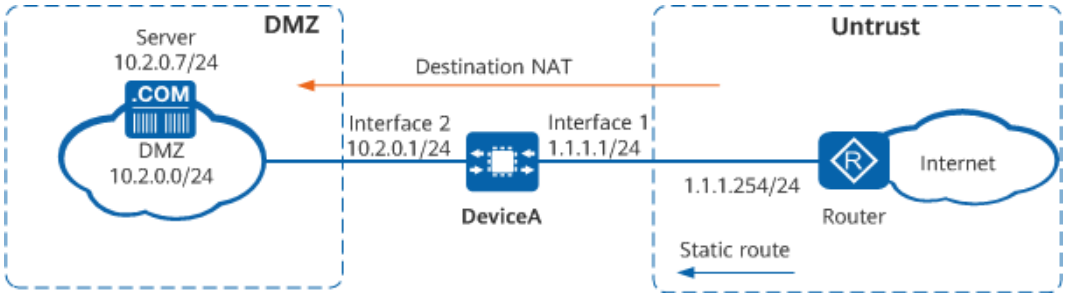
An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that an intranet server can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by the intranet server to provide different services to Internet users. **Figure 15-21** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-21 Network diagram of destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	The intranet server uses 10.2.0.1 as the default gateway address.
Destination NAT	Destination address pool: 10.2.0.7	With the destination NAT function enabled, DeviceA can forward traffic to the intranet server.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from the intranet server to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure the destination NAT function to enable DeviceA to forward traffic sent from Internet users to the intranet server.
4. Configure a default route on DeviceA to enable it to forward traffic from the intranet server to the ISP router.
5. Configure static routes to the public addresses of the intranet server on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.7 10.2.0.7
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-address range 1.1.10.10 1.1.10.11
[DeviceA-policy-nat-rule-policy_nat1] service protocol tcp destination-port 2000
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static address-to-port address-group addressgroup1 80 to 81
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure blackhole routes to the public addresses of the intranet server to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
[DeviceA] ip route-static 1.1.10.11 255.255.255.255 NULL0
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 7 Configure a default route on DeviceA to enable it to forward traffic from the intranet server to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 8 On the ISP router, configure static routes to the public addresses (1.1.10.10 and 1.1.10.11) of the intranet server, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet server to DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of the intranet server. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 tcp  VPN:public --> public  1.2.1.3:2474-->1.1.10.10:2000[10.2.0.7:80]
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 1.1.10.11 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1 0
 section 10.2.0.7 10.2.0.7
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-address range 1.1.10.10 1.1.10.11
    service protocol tcp destination-port 2000
    action destination-nat static address-to-port address-group addressgroup1 80 to 81
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.2.9 CLI: Example for Configuring Destination NAT for Mobile Phone Users to Access Wireless Networks (Translating Public Addresses Randomly Into Addresses in a Destination Address Pool)

Networking Requirements

Mobile phone users access the Internet by logging in to a Wireless Application Protocol (WAP) gateway. If the gateway address used by mobile phones for Internet access is not the IP address of the WAP gateway, rules need to be configured to translate the destination IP address of Internet access requests into the IP address of the WAP gateway.

In **Figure 15-22**, the default gateway address of a mobile phone is 1.1.1.1, but that the gateway address provided by the carrier is 2.2.2.2. In this case, destination NAT needs to be configured on DeviceA so that the destination gateway address of packets sent from the mobile phone can be translated into 2.2.2.2.

Figure 15-22 Network diagram of destination NAT for mobile phone users

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 10.1.1.1/24 Security zone: Trust	-
GE0/0/2	IP address: 172.16.1.1/24 Security zone: Untrust	-
Destination NAT	Destination address pool: 2.2.2.2	-
Security policy	Source zone: Trust Destination zone: Untrust Destination address: 2.2.2.2	This security policy permits the traffic destined for the carrier's gateway address to pass through DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure the destination NAT function to enable DeviceA to translate destination addresses.
3. Configure a security policy to permit the traffic sent from mobile phone users to pass through DeviceA.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 10.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 172.16.1.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Step 2 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 2.2.2.2 2.2.2.2
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 3 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone trust
[DeviceA-policy-nat-rule-policy_nat1] destination-address 1.1.1.1 32
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 4 Configure a blackhole route to the pre-NAT destination address of packets to prevent routing loops.

```
[DeviceA] ip route-static 1.1.1.1 255.255.255.255 NULL0
```

Step 5 Configure a security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy1] destination-address 2.2.2.2 32
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

1. Verify that mobile phone users can access the Internet to confirm that destination NAT has been configured successfully.
2. Run the **display firewall session table verbose** command to check for the session entry with the destination address as 1.1.1.1.

```
<DeviceA> display firewall session table verbose
Current Total Sessions : 1
 http  VPN:public --> public  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust TTL: 00:00:45  Left: 00:00:45
 Interface: GE0/0/2 NextHop: 2.2.2.254 MAC: xxxx-xxxx-xxxx
 <--packets: 25 bytes: 2,600 --> packets: 25 bytes: 2,600
 10.1.1.100:4194-->1.1.1.1:2048[2.2.2.2:2048] PolicyName: policy1
```

   According to the command output, DeviceA successfully translates the gateway address in the packets sent from mobile phone users (1.1.1.1) into the carrier's gateway address (2.2.2.2), which is enclosed in square brackets ([ ]).

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 1.1.1.1 255.255.255.255 NULL0
#
destination-nat address-group addressgroup1
 section 2.2.2.2 2.2.2.2
#
security-policy
  rule name policy1
    source-zone trust
    destination-zone untrust
    destination-address 2.2.2.2 32
    action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
  destination-address 1.1.1.1 32
  action destination-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.2.10 Web: Example for Configuring NAT Policy for Internet Users to Access Servers on an Intranet with Two Egresses

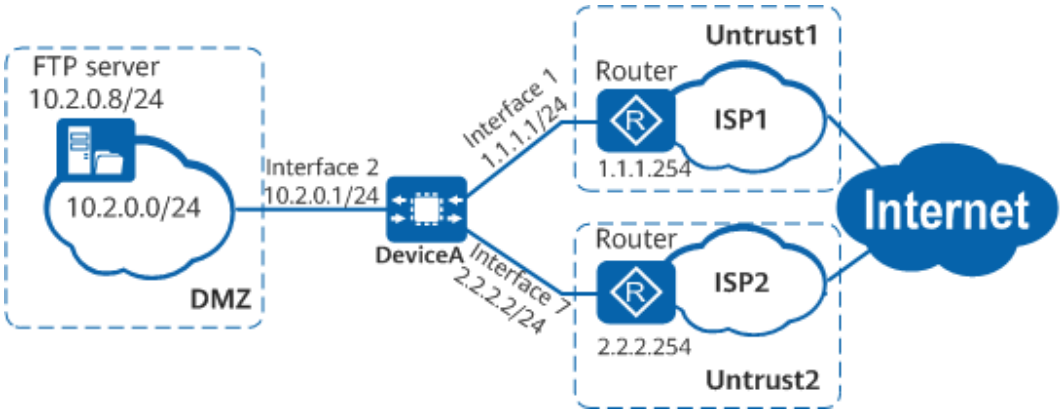
Networking Requirements

In **Figure 15-23**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. A NAT policy needs to be configured on DeviceA so that the intranet FTP server can provide services to Internet users, configure a NAT policy on DeviceA. In addition to the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 2.2.20.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. **Figure 15-23** shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-23 Network diagram of a NAT policy on an intranet with two egresses

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE0/0/2, and GE0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
NAT policy	Policy rule name: policy1 Source zone: Untrust1 Public address: 1.1.10.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 1.1.10.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.
	Policy rule name: policy2 Source zone: Untrust2 Public address: 2.2.20.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 2.2.20.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure a NAT policy.
4. On GE0/0/1 and GE0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.
5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set an IP address for GE0/0/2 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE0/0/2 and set the following parameters.

Security Zone	dmz
IPv4	
IP Address	10.2.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

2. Set an IP address for GE0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** and create security zone **untrust1** based on the following parameter values.

Name	untrust1
Priority	10

   c. Click **OK**.
   d. Choose **Network** > **Interface**.
   e. In **Interface List**, click on the line of GE0/0/1 and set the following parameters.

Security Zone	untrust1
IPv4	
IP Address	1.1.1.1/24

   f. Click **OK**.
3. Set an IP address for GE0/0/7 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** and create security zone **untrust2** based on the following parameter values.

Name	untrust2
Priority	20

   c. Click **OK**.
   d. Choose **Network** > **Interface**.
   e. In **Interface List**, click on the line of GE0/0/7 and set the following parameters.

Security Zone	untrust2
IPv4	
IP Address	2.2.2.2/24

   f. Click **OK**.

Step 2 Configure a security policy to allow Internet users to access the intranet server.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add** and choose **Add Security Policy**. Set the following parameters to configure a security policy.

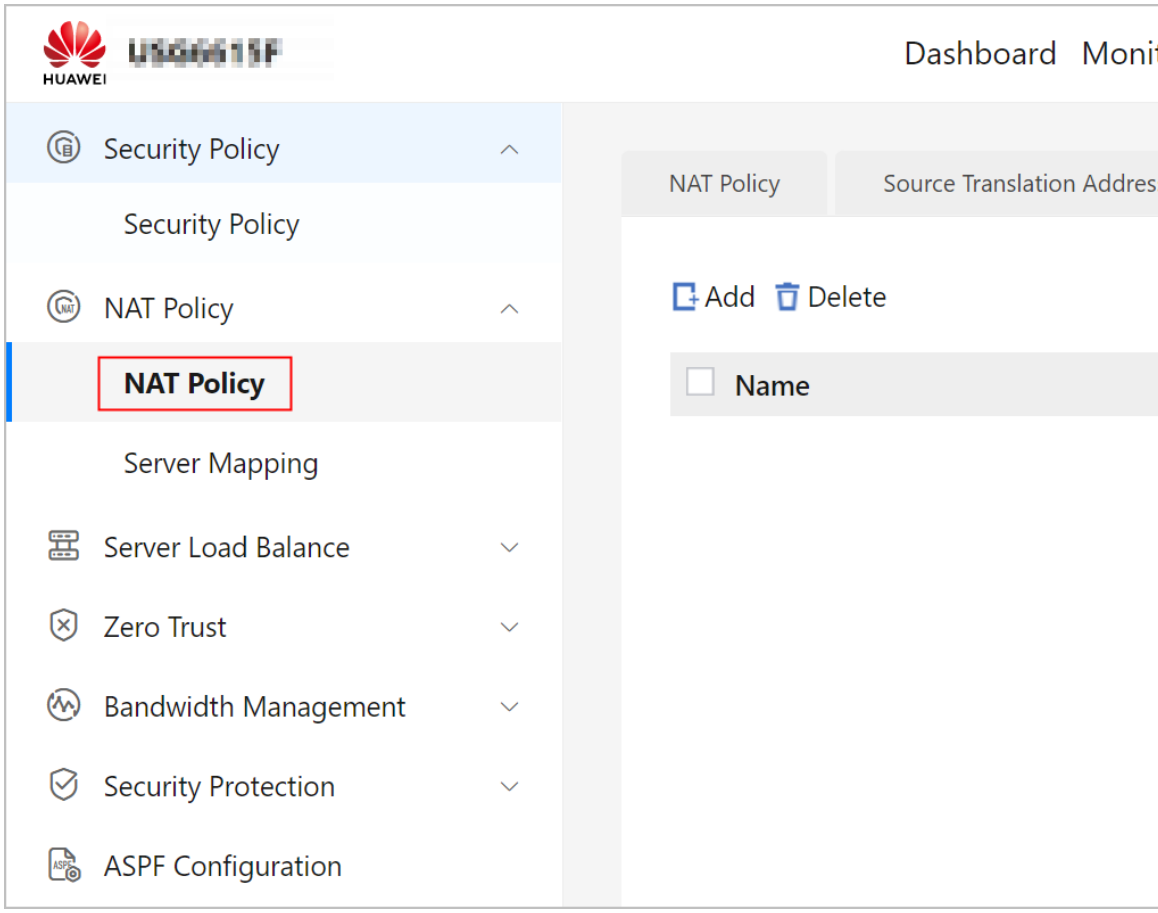
 Copyright © Huawei Technologies Co., Ltd.

Name	policy1
Source Zone	untrust1, untrust2
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

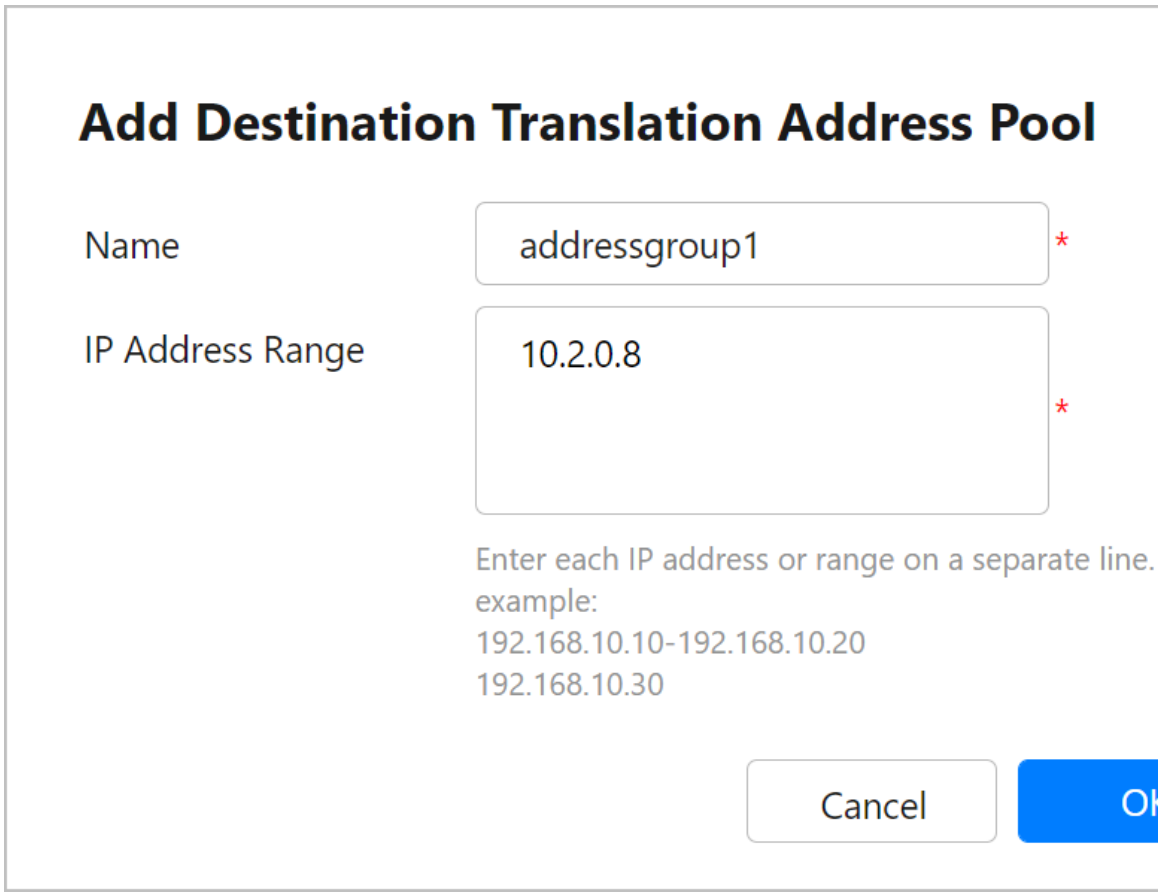
Step 3 Configure a NAT address pool and NAT policy.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Destination Translation Address Pool**.

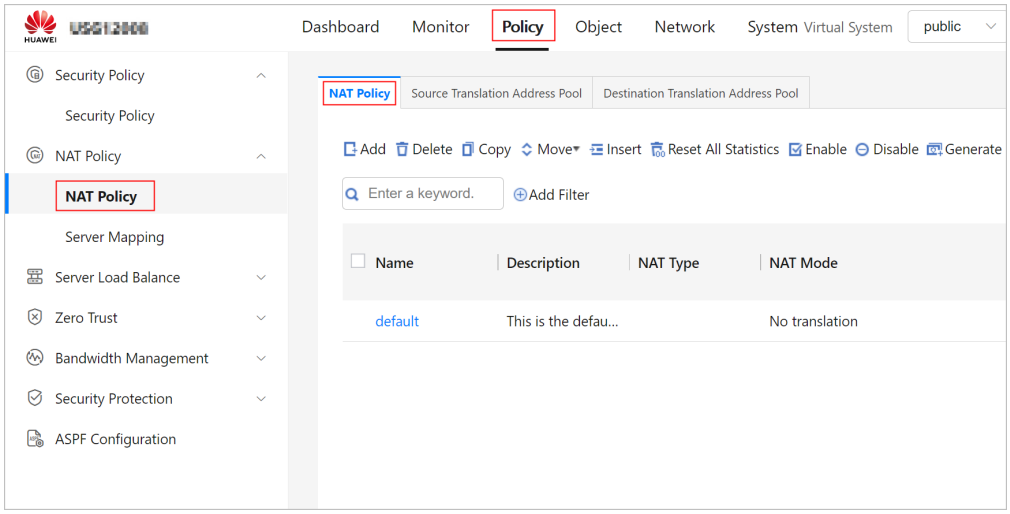


2. In **Destination Translation Address Pool List**, click **Add** and set the following parameters to configure a NAT address pool.

 Copyright © Huawei Technologies Co., Ltd.

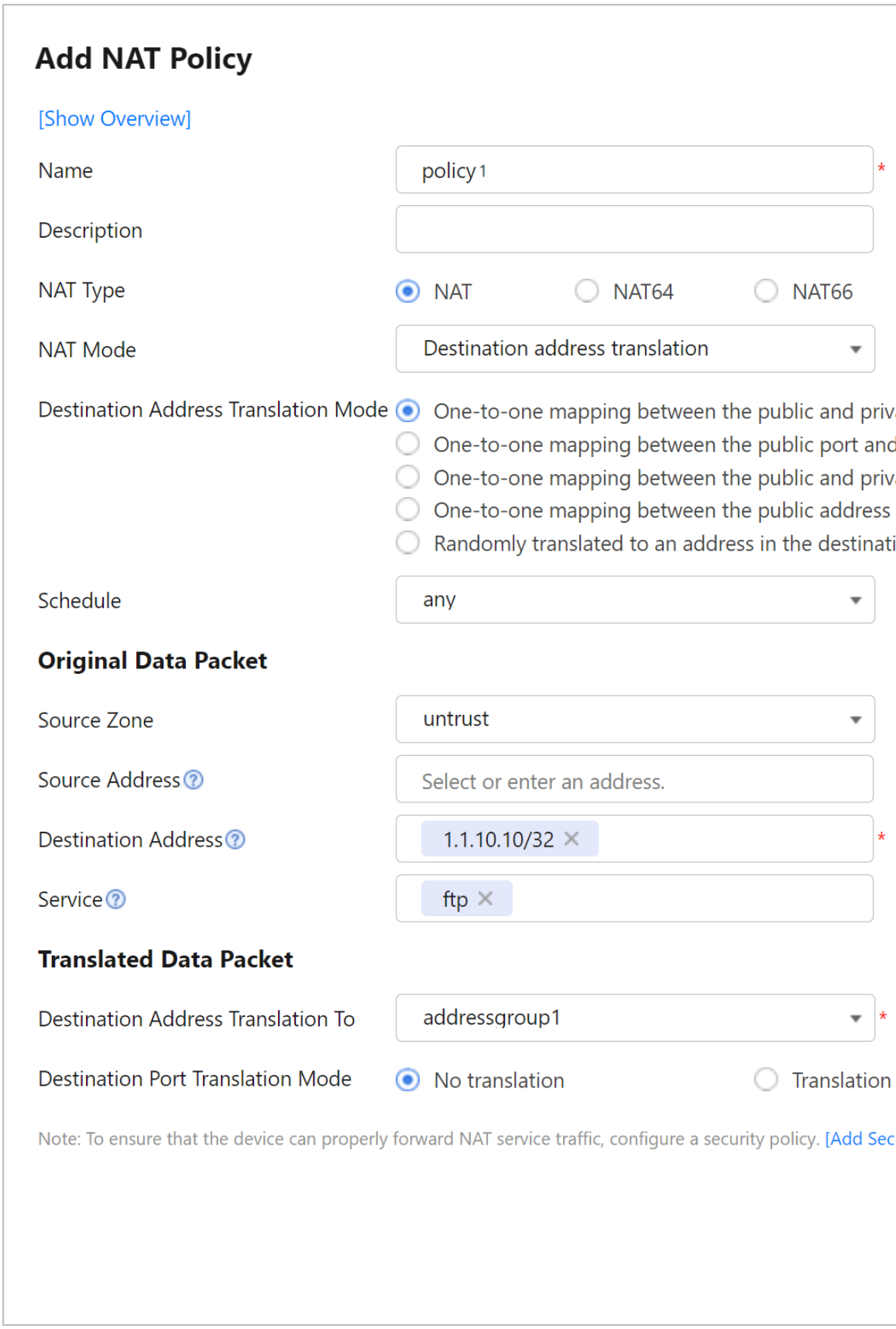


3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and set the following parameters to configure a NAT policy.

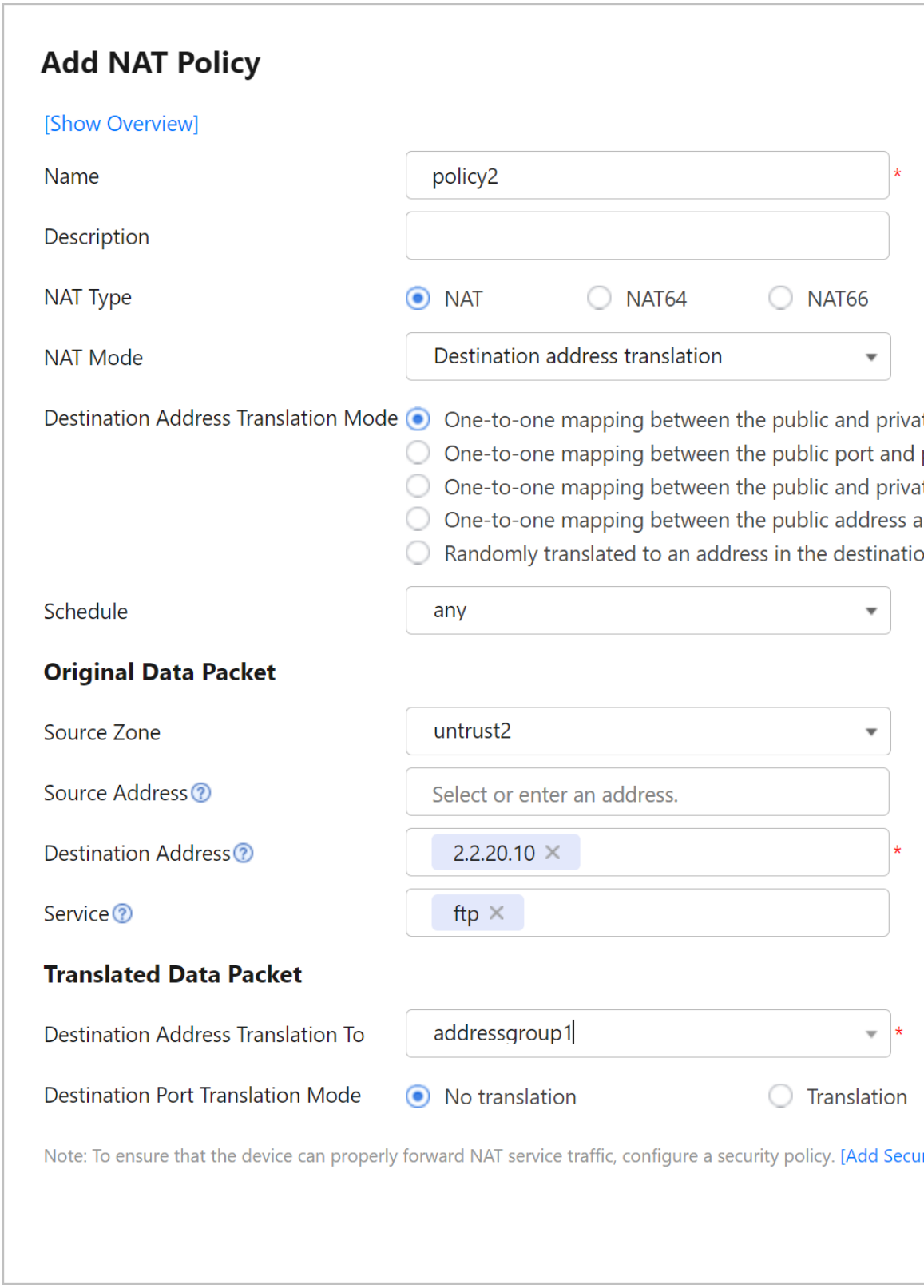
 Copyright © Huawei Technologies Co., Ltd.



6. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

7. Repeat the preceding substeps to configure policy2.



8. Click **OK**.

Step 4 Configure a blackhole route to prevent route loops.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Network** > **Router** > **Static Route**.
2. In **Static Route List**, click **Add** and set the following parameters.

Protocol Type	IPv4
Destination IP Address/ Mask	1.1.10.10/255.255.255.0
Out Interface	NULL0

3. Repeat the preceding substeps to configure the default route based on the following parameter values.

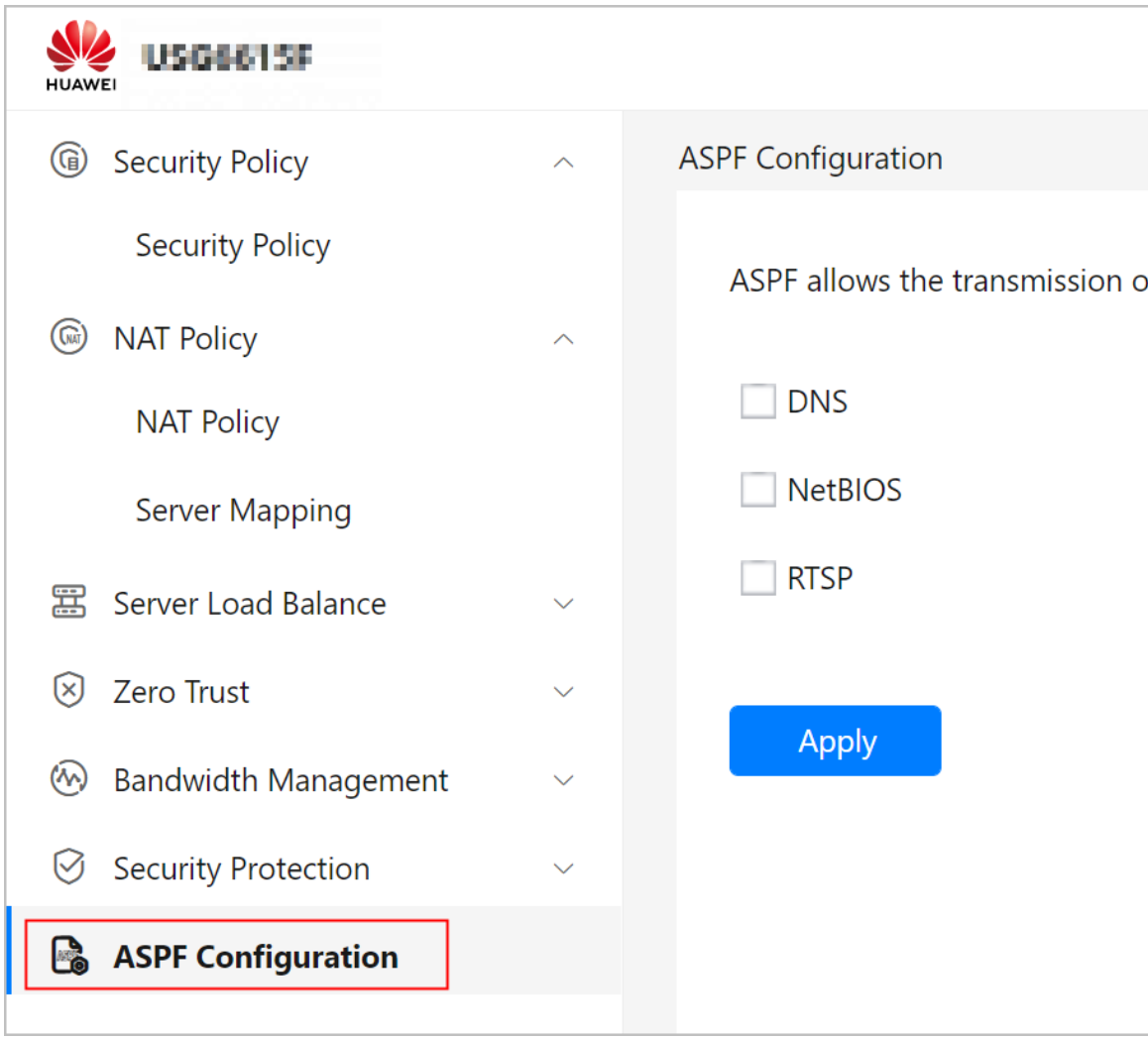
Protocol Type	IPv4
Destination IP Address/ Mask	2.2.20.10/255.255.255.0
Out Interface	NULL0

4. Click **OK**.

Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.

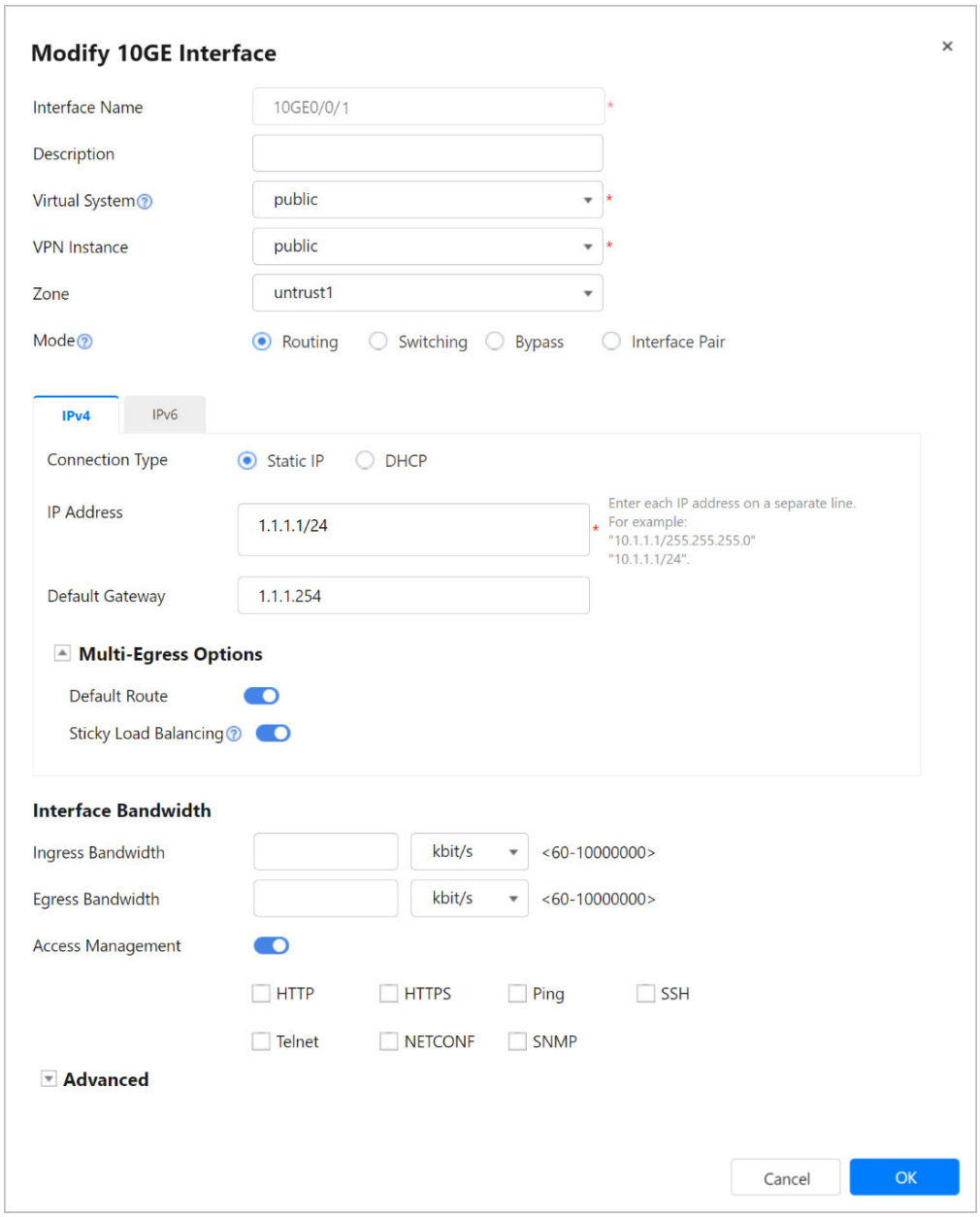


2. Select **FTP**.

Step 6 Configure sticky load balancing and the default gateway.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click on the line of GE 0/0/1 and set the following parameters.

 Copyright © Huawei Technologies Co., Ltd.



3. Repeat the preceding step to configure GE0/0/7.

Step 7 On the routers, configure static routes to the public address of the intranet server so that traffic to the server can be sent to the DeviceA.

Contact the ISP's network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 2.2.20.10 255.255.255.255 NULL0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
firewall interzone dmz untrust2
 detect ftp
#
destination-nat address-group addressgroup1
 section 10.2.0.8 10.2.0.8
#
nat-policy
 rule name policy1
  source-zone untrust1
  destination-address 1.1.10.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
 rule name policy2
  source-zone untrust2
  destination-address 2.2.20.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.2.11 Example for Configuring a NAT Policy for Internet Users to Access a Server on an Intranet with Two Egresses in Different Security Zones

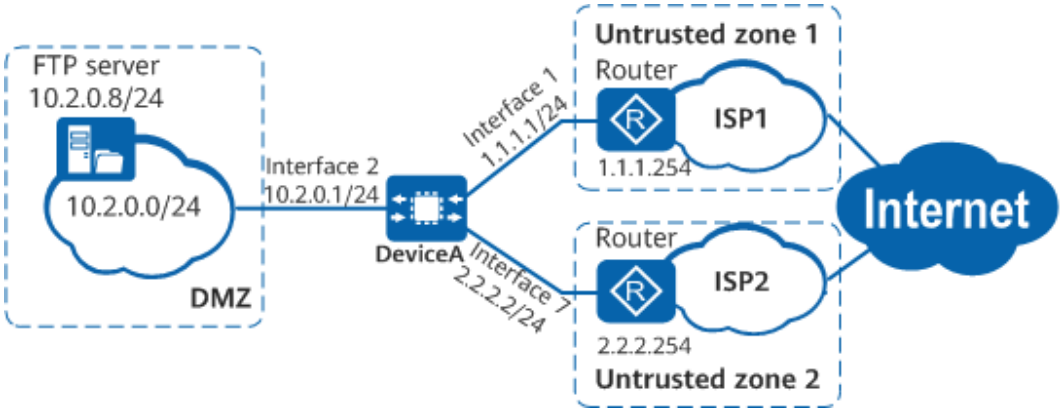
Networking Requirements

In **Figure 15-24**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. A NAT policy needs to be configured on DeviceA so that the intranet FTP server can provide services to Internet users, configure a NAT policy on DeviceA. In addition to the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 2.2.20.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. **Figure 15-24** shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-24 Network diagram of a NAT policy on an intranet with two egresses in different security zones

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
NAT policy	Policy rule name: policy1 Source zone: Untrust1 Public address: 1.1.10.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 1.1.10.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.
	Policy rule name: policy2 Source zone: Untrust2 Public address: 2.2.20.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 2.2.20.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure a NAT policy.
4. On GE 0/0/1 and GE 0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.
5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE 0/0/1 to the Untrust1 zone.

```
[DeviceA] firewall zone name untrust1
[DeviceA-zone-untrust1] set priority 10
[DeviceA-zone-untrust1] add interface ge 0/0/1
[DeviceA-zone-untrust1] quit
```

Add GE 0/0/7 to the Untrust2 zone.

```
[DeviceA] firewall zone name untrust2
[DeviceA-zone-untrust2] set priority 20
[DeviceA-zone-untrust2] add interface ge 0/0/7
[DeviceA-zone-untrust2] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust1
[DeviceA-policy-security-rule-policy1] source-zone untrust2
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.8 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] source-zone untrust1
[DeviceA-policy-nat-rule-policy1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy1] service ftp
[DeviceA-policy-nat-rule-policy1] action destination-nat static address-to-address address-group
addressgroup1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] rule name policy2
[DeviceA-policy-nat-rule-policy2] source-zone untrust2
[DeviceA-policy-nat-rule-policy2] destination-address 2.2.20.10 32
[DeviceA-policy-nat-rule-policy2] service ftp
[DeviceA-policy-nat-rule-policy2] action destination-nat static address-to-address address-group
addressgroup1
[DeviceA-policy-nat-rule-policy2] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure blackhole routes to the public addresses of the intranet server to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
[DeviceA] ip route-static 2.2.20.10 255.255.255.255 NULL0
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust1
[DeviceA-interzone-dmz-untrust1] detect ftp
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-interzone-dmz-untrust1] quit
[DeviceA] firewall interzone dmz untrust2
[DeviceA-interzone-dmz-untrust2] detect ftp
[DeviceA-interzone-dmz-untrust2] quit
```

Step 7 Enable the sticky load balancing function and configure the default gateway address.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] redirect-reverse next-hop 1.1.1.254
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] redirect-reverse next-hop 2.2.2.254
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Step 8 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of the intranet server. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 tcp  VPN:public --> public  1.1.1.9:2474-->1.1.10.10:2080[10.2.0.8:3721]
 tcp  VPN:public --> public  2.2.2.25:2025-->2.2.20.10:3658[10.2.0.8:3318]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 2.2.20.10 255.255.255.255 NULL0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
firewall interzone dmz untrust2
 detect ftp
#
destination-nat address-group addressgroup1
 section 10.2.0.8 10.2.0.8
#
nat-policy
 rule name policy1
  source-zone untrust1
  destination-address 1.1.10.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
 rule name policy2
  source-zone untrust2
  destination-address 2.2.20.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.2.12 CLI: Example for Configuring a NAT Policy for Internet Users to Access a Server on an Intranet with Two Egresses in the Same Security Zone

Networking Requirements

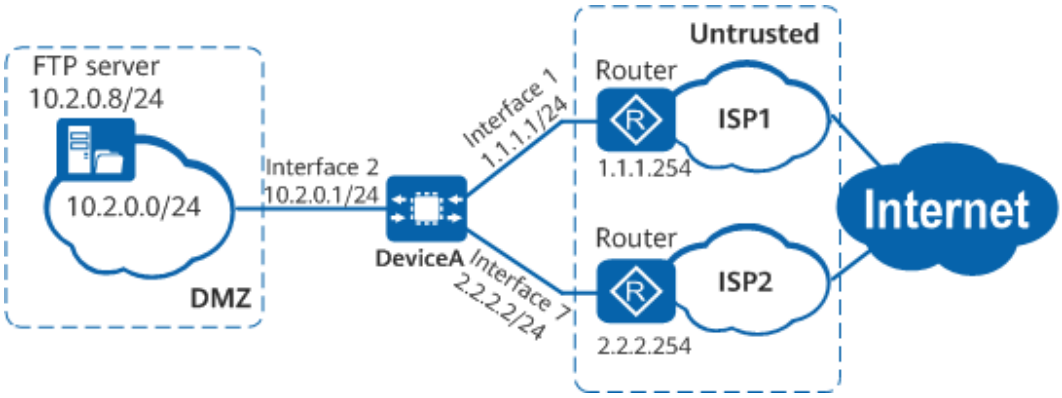
In **Figure 15-25**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. To enable the intranet FTP server to provide services to Internet users, configure a NAT policy on DeviceA. In addition to the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 2.2.20.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. **Figure 15-25** shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-25 Network diagram of a NAT policy on an intranet with two egresses in the same security zone

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-
NAT policy	Policy rule name: policy1 Source zone: Untrust Public address: 1.1.10.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 1.1.10.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.
	Policy rule name: policy2 Source zone: Untrust Public address: 2.2.20.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 2.2.20.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure a NAT policy.
4. On GE 0/0/1 and GE 0/0/7, enable the sticky load balancing function and configure the default gateway address.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.

5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/7 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/7
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.8 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy1] source-zone untrust
[DeviceA-policy-nat-rule-policy1] service ftp
[DeviceA-policy-nat-rule-policy1] action destination-nat static address-to-address address-group addressgroup1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] rule name policy_nat2
[DeviceA-policy-nat-rule-policy2] destination-address 2.2.20.10 32
[DeviceA-policy-nat-rule-policy2] source-zone untrust
[DeviceA-policy-nat-rule-policy2] service ftp
[DeviceA-policy-nat-rule-policy2] action destination-nat static address-to-address address-group addressgroup1
[DeviceA-policy-nat-rule-policy2] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure blackhole routes to the public addresses of the intranet server to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
[DeviceA] ip route-static 2.2.20.10 255.255.255.255 NULL0
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 7 Enable the sticky load balancing function and configure the default gateway address.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] redirect-reverse next-hop 1.1.1.254
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] redirect-reverse next-hop 2.2.2.254
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Step 8 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of the intranet server. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 tcp  VPN:public --> public  1.1.1.9:2474-->1.1.10.10:2080[10.2.0.8:3721]
 tcp  VPN:public --> public  2.2.2.25:2025-->2.2.20.10:3658[10.2.0.8:3318]
```

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 2.2.20.10 255.255.255.255 NULL0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
 #
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/7
#
firewall interzone dmz untrust
 detect ftp
#
destination-nat address-group addressgroup1
 section 10.2.0.8 10.2.0.8
#
nat-policy
 rule name policy1
  source-zone untrust
  destination-address 1.1.10.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
 rule name policy2
  source-zone untrust
  destination-address 2.2.20.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.2.13 Web: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP Address of a Server on a Dual-Egress Intranet (Sticky Load Balancing)

Networking Requirements

In **Figure 15-26**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. In addition

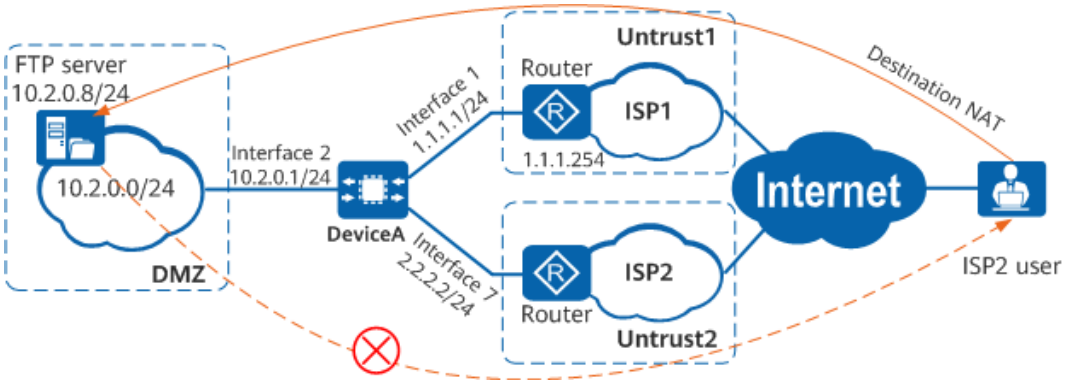
 Copyright © Huawei Technologies Co., Ltd.

to the public addresses of WAN interfaces on DeviceA, only one public IP address (1.1.10.10) is obtained from ISP1 for the intranet FTP server to provide services for Internet users. Users on both the ISP1 and ISP2 networks use this public IP address to access the FTP server.

Figure 15-26 Network diagram of a NAT policy on a dual-egress intranet, with the sticky load balancing function enabled

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-
NAT policy	Policy name: policy1 Source zones: Untrust1 and Untrust2 Public address: 1.1.10.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 1.1.10.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.

Configuration Roadmap

1. Configure a NAT policy to enable Internet users to access the intranet FTP server using a public IP address.
2. On GE 0/0/1, enable the sticky load balancing function and configure the default gateway address.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set an IP address for GE0/0/2 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE0/0/2 and set the following parameters.

Security Zone	dmz
IPv4	
IP Address	10.2.0.1/24

   c. Click **OK**.
2. Set an IP address forGE0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** and create security zone **untrust1** based on the following parameter values.

Name	untrust1
Priority	10

   c. Click **OK**.
   d. Choose **Network** > **Interface**.
   e. In **Interface List**, click on the line of GE0/0/1 and set the following parameters.

Security Zone	untrust1
IPv4	
IP Address	1.1.1.1/24

   f. Click **OK**.
3. Set an IP address for GE0/0/7 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** and create security zone **untrust2** based on the following parameter values.

Name	untrust2

 Copyright © Huawei Technologies Co., Ltd.

Priority	20

c. Click **OK**.

d. Choose **Network** > **Interface**.

e. In **Interface List**, click on the line of GE0/0/7 and set the following parameters.

Security Zone	untrust2
IPv4	
IP Address	2.2.2.2/24

f. Click **OK**.

Step 2 Configure a security policy to allow Internet users to access the intranet server.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add** and choose **Add Security Policy**. Set the following parameters to configure a security policy.

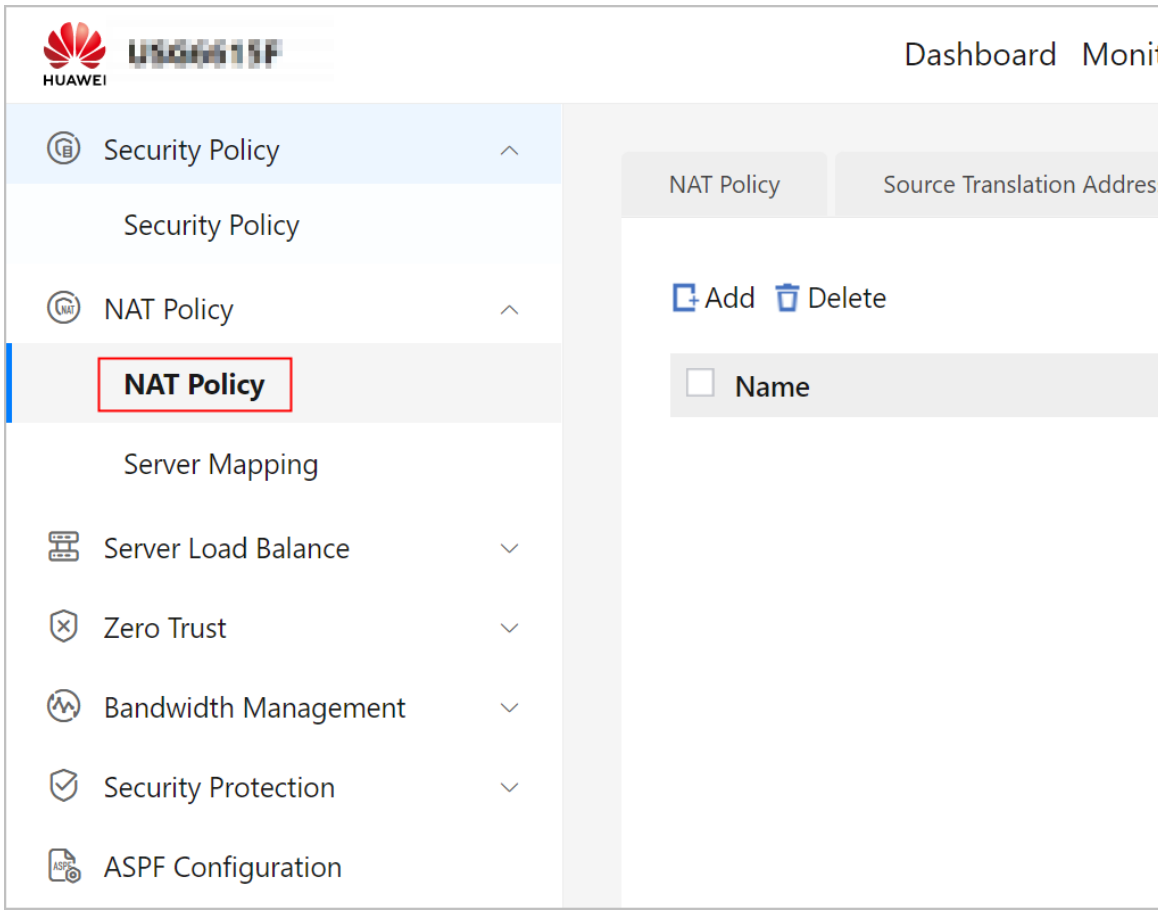
Name	policy1
Source Zone	untrust1, untrust2
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure a NAT address pool and NAT policy.

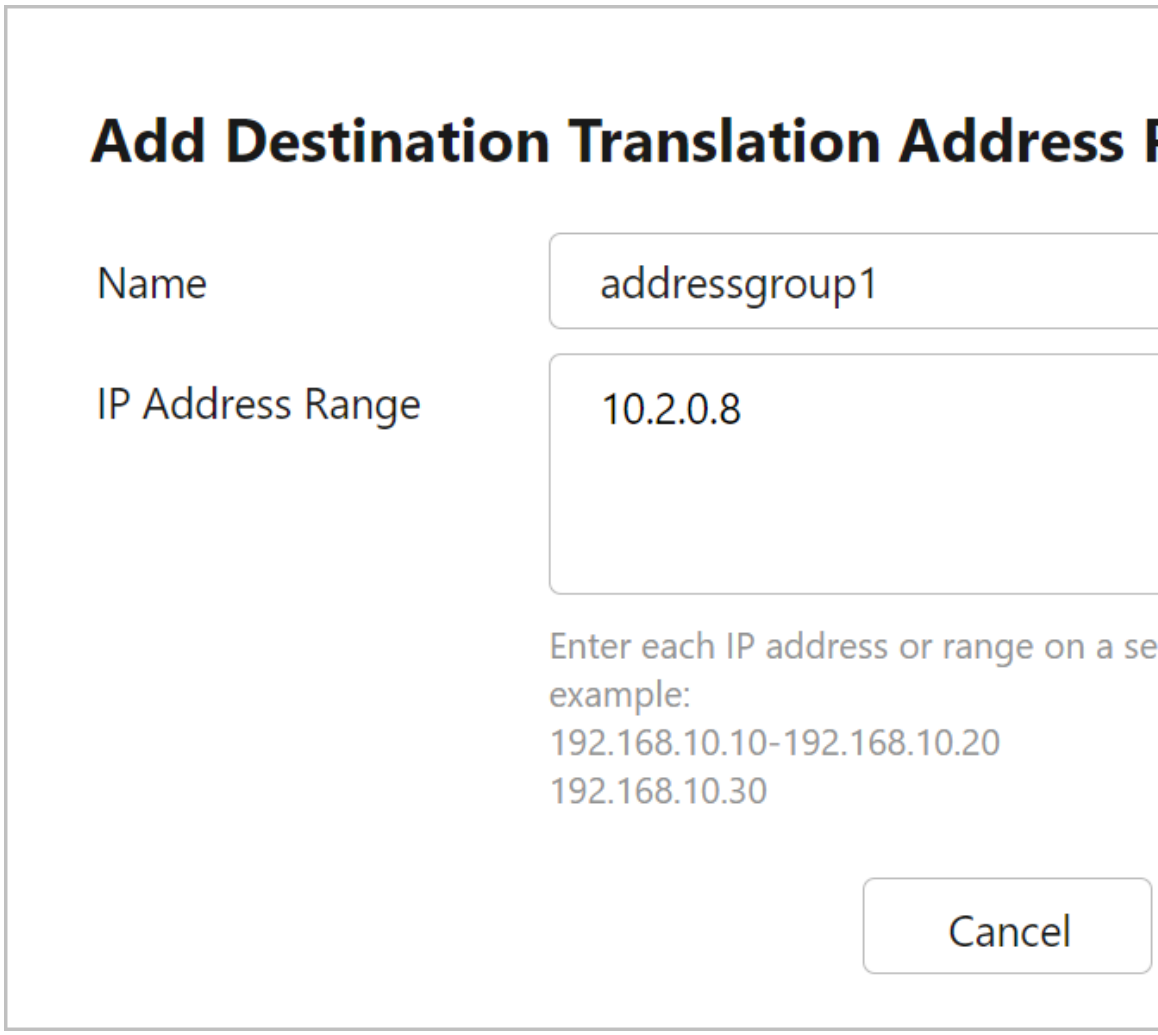
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Destination Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.

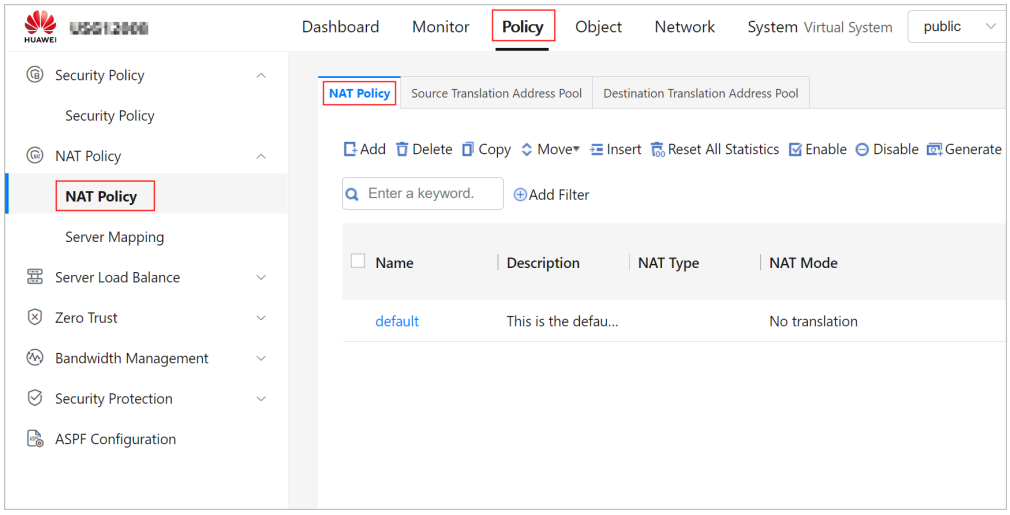


2. In **Destination Translation Address Pool List**, click **Add** and set the following parameters to configure a NAT address pool.

 Copyright © Huawei Technologies Co., Ltd.

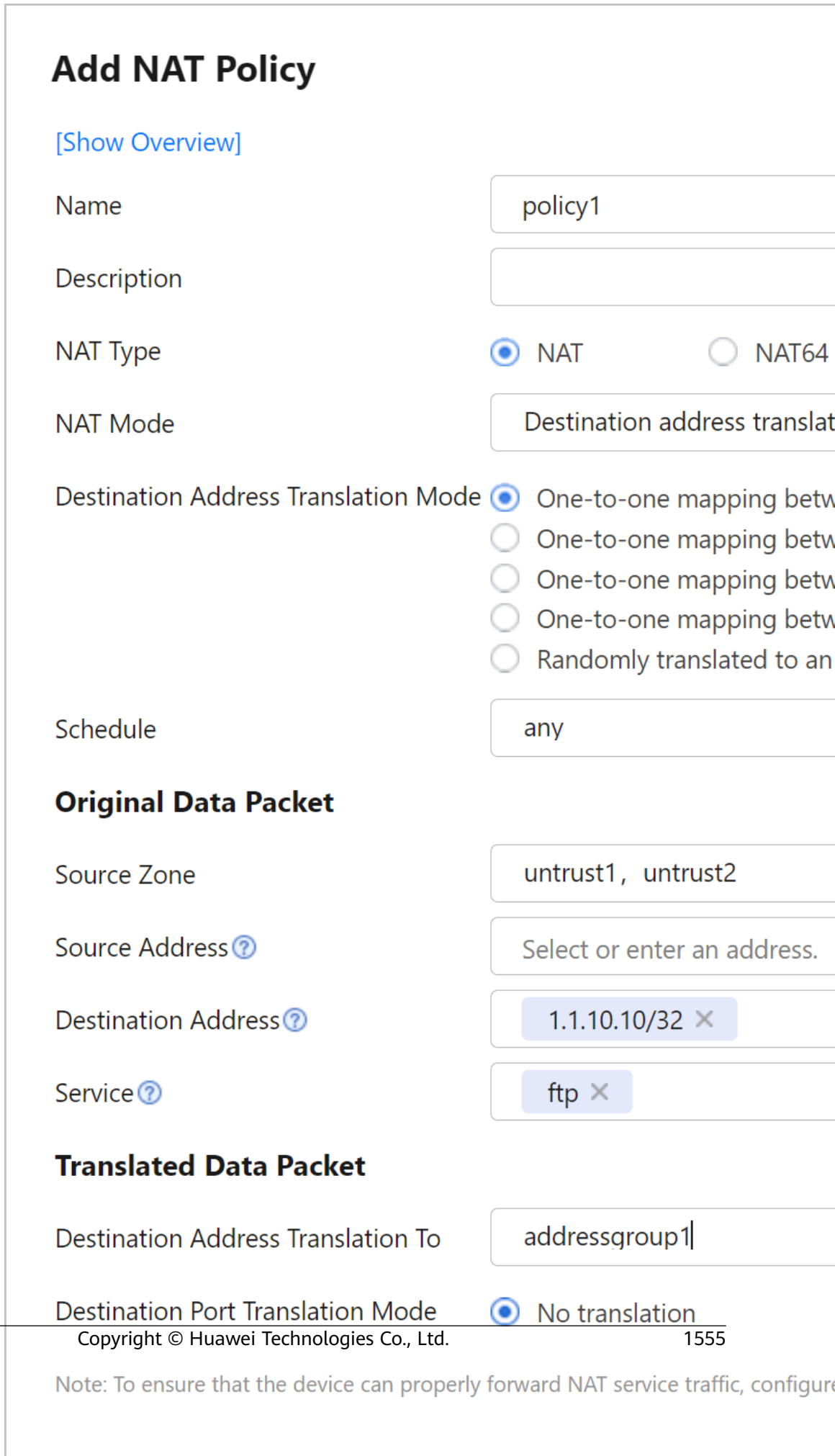


3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and set the following parameters to configure a NAT policy.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

6. Click **OK**.

Step 4 Configure a blackhole route to prevent route loops.

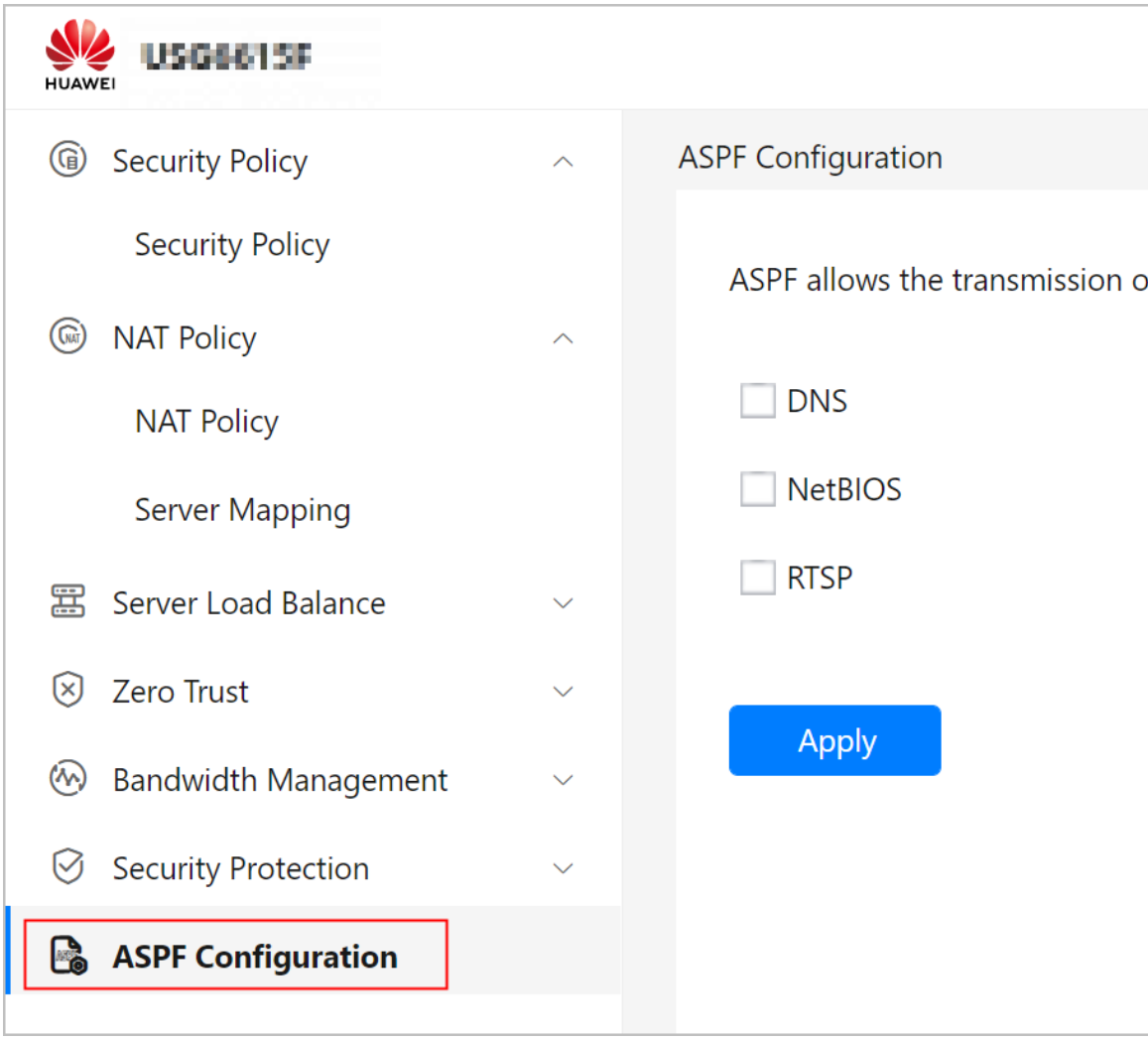
1. Choose **Network** > **Router** > **Static Route**.
2. In **Static Route List**, click **Add** and set the following parameters.

Protocol Type	IPv4
Destination IP Address/ Mask	1.1.10.10/255.255.255.0
Outbound Interface	NULL0

3. Click **OK**.

Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

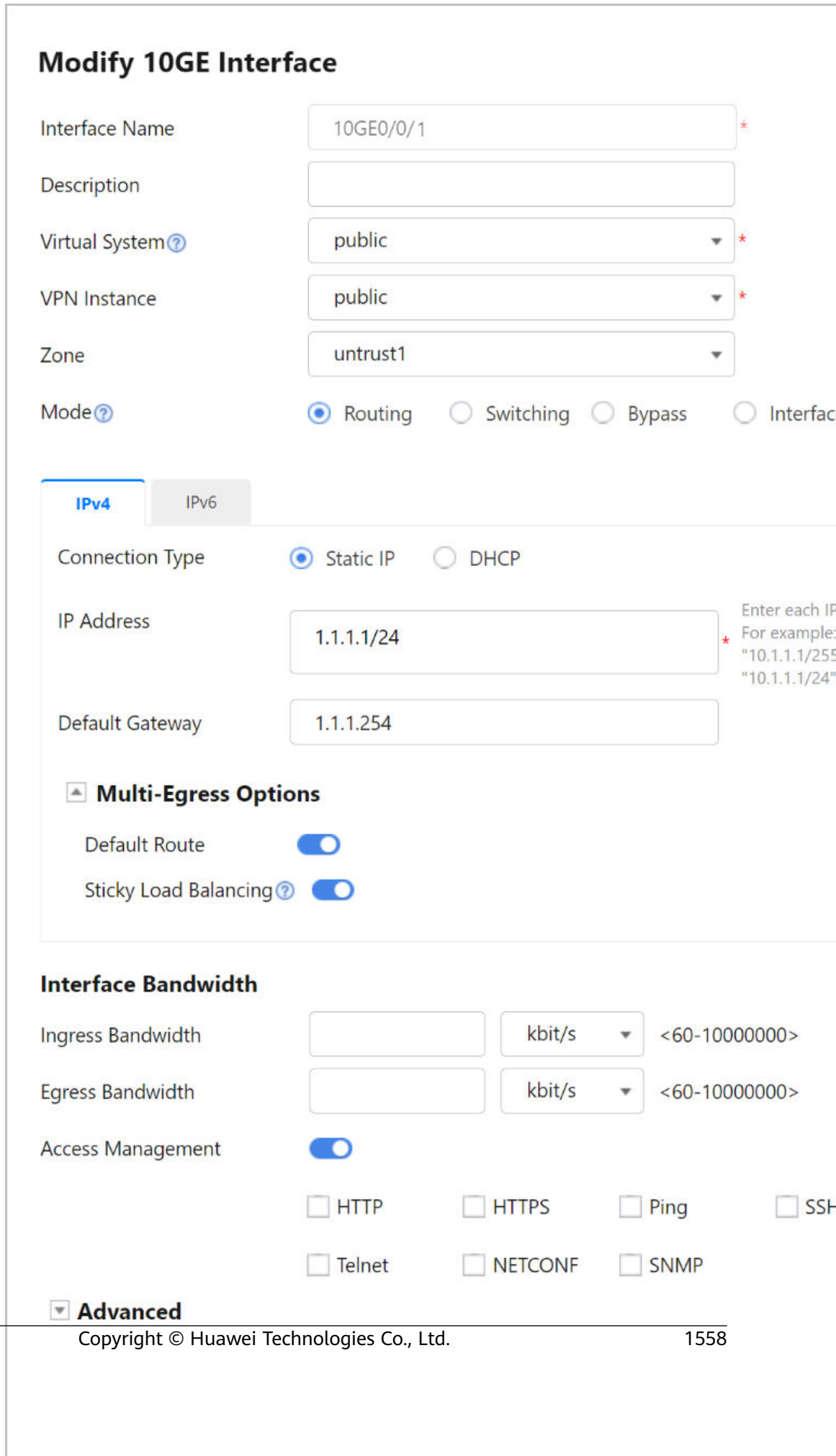


2. Select **FTP**.

Step 6 Configure sticky load balancing and the default gateway.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click on the line of GE0/0/1 and set the following parameters.



 Copyright © Huawei Technologies Co., Ltd.

In this example, the company applies only for the public IP address of the server from ISP1. Therefore, traffic to the server is sent to GE 0/0/1. Configure sticky load balancing only on this interface.

3. Set the default gateway address of GE0/0/7 to 2.2.2.254.

Step 7 On the routers, configure static routes to the public address of the intranet server so that traffic to the server can be sent to the DeviceA.

Contact the ISP's network administrator to perform this step.

----End

Configuration Scripts

```
#
 sysname DeviceA
#
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
destination-nat address-group addressgroup1
 section 10.2.0.8 10.2.0.8
#
nat-policy
 rule name policy1
  source-zone untrust1
  source-zone untrust2
  destination-address 1.1.10.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.2.14 CLI: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP Address of a Server on a Dual-Egress Intranet (Sticky Load Balancing)

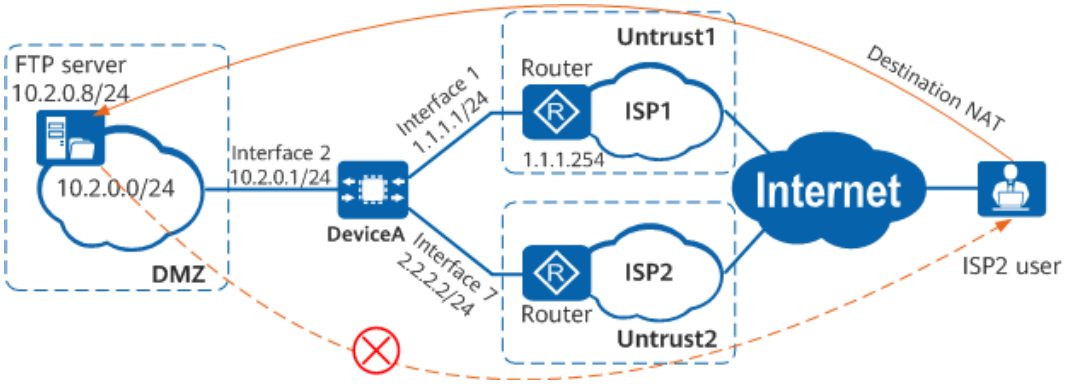
Networking Requirements

In Figure 15-27, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. In addition to the public addresses of WAN interfaces on DeviceA, only one public IP address (1.1.10.10) is obtained from ISP1 for the intranet FTP server to provide services for Internet users. Users on both the ISP1 and ISP2 networks use this public IP address to access the FTP server.

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.

Figure 15-27 Network diagram of a NAT policy on a dual-egress intranet, with the sticky load balancing function enabled



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-
NAT policy	Policy name: policy1 Source zones: Untrust1 and Untrust2 Public address: 1.1.10.10 Destination address pool: 10.2.0.8	This NAT policy rule enables DeviceA to translate the destination address 1.1.10.10 of packets into 10.2.0.8, so that these packets can be forwarded to the intranet FTP server.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure a NAT policy to enable Internet users to access the intranet FTP server using a public IP address.
2. On GE 0/0/1 and GE 0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE 0/0/1 to the Untrust1 zone.

```
[DeviceA] firewall zone name untrust1
[DeviceA-zone-untrust1] set priority 10
[DeviceA-zone-untrust1] add interface ge 0/0/1
[DeviceA-zone-untrust1] quit
```

Add GE 0/0/7 to the Untrust2 zone.

```
[DeviceA] firewall zone name untrust2
[DeviceA-zone-untrust2] set priority 20
[DeviceA-zone-untrust2] add interface ge 0/0/7
[DeviceA-zone-untrust2] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy1] source-zone untrust2
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup1
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.8 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 4 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy1] source-zone untrust1
[DeviceA-policy-nat-rule-policy1] source-zone untrust2
[DeviceA-policy-nat-rule-policy1] service ftp
[DeviceA-policy-nat-rule-policy1] action destination-nat static address-to-address address-group
addressgroup1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure a blackhole route to the public address of the intranet server to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust1
[DeviceA-interzone-dmz-untrust1] detect ftp
[DeviceA-interzone-dmz-untrust1] quit
```

Step 7 Enable the sticky load balancing function and configure the default gateway address.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] redirect-reverse next-hop 1.1.1.254
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] redirect-reverse next-hop 2.2.2.254
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Step 8 Configure a static route to the public address of the intranet server on the ISP1 router, so that it can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entry with the destination address as the public address of the intranet server. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 tcp  VPN:public --> public  1.1.1.9:2474-->1.1.10.10:2080[10.2.0.8:3721]
```

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

```
#
 sysname DeviceA
#
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
destination-nat address-group addressgroup1
 section 10.2.0.8 10.2.0.8
#
nat-policy
 rule name policy1
  source-zone untrust1
  source-zone untrust2
  destination-address 1.1.10.10 32
  service ftp
  action destination-nat static address-to-address address-group addressgroup1
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.3 NAT Server

 Copyright © Huawei Technologies Co., Ltd.

15.3.1 Web: Example for Configuring NAT Server for Internet Users to Access Intranet Servers

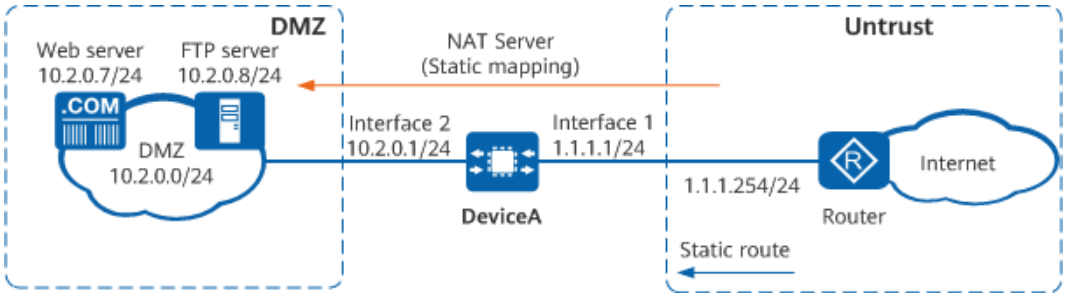
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. NAT Server needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.1.10) from the ISP, which is used by intranet servers to provide services to Internet users. **Figure 15-28** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-28 Network diagram of NAT Server

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: untrust	1.1.1.1/24 is a public address provided by the ISP.
10GE 1/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
NAT Server	Name: policy_web Public IP address: 1.1.1.10 Private IP address: 10.2.0.7 Public port: 8080 Private port: 80	When Internet users send traffic to 1.1.1.10 through port 8080, DeviceA can forward the traffic to the web server based on this mapping entry. The web server has the private address 10.2.0.7 and private port number 80.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic to 1.1.1.10 through port 21, DeviceA can forward the traffic to the FTP server based on this mapping entry. The FTP server has the private address 10.2.0.8 and private port number 21.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA so that it can forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure NAT Server to implement address translation for the intranet web and FTP server.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

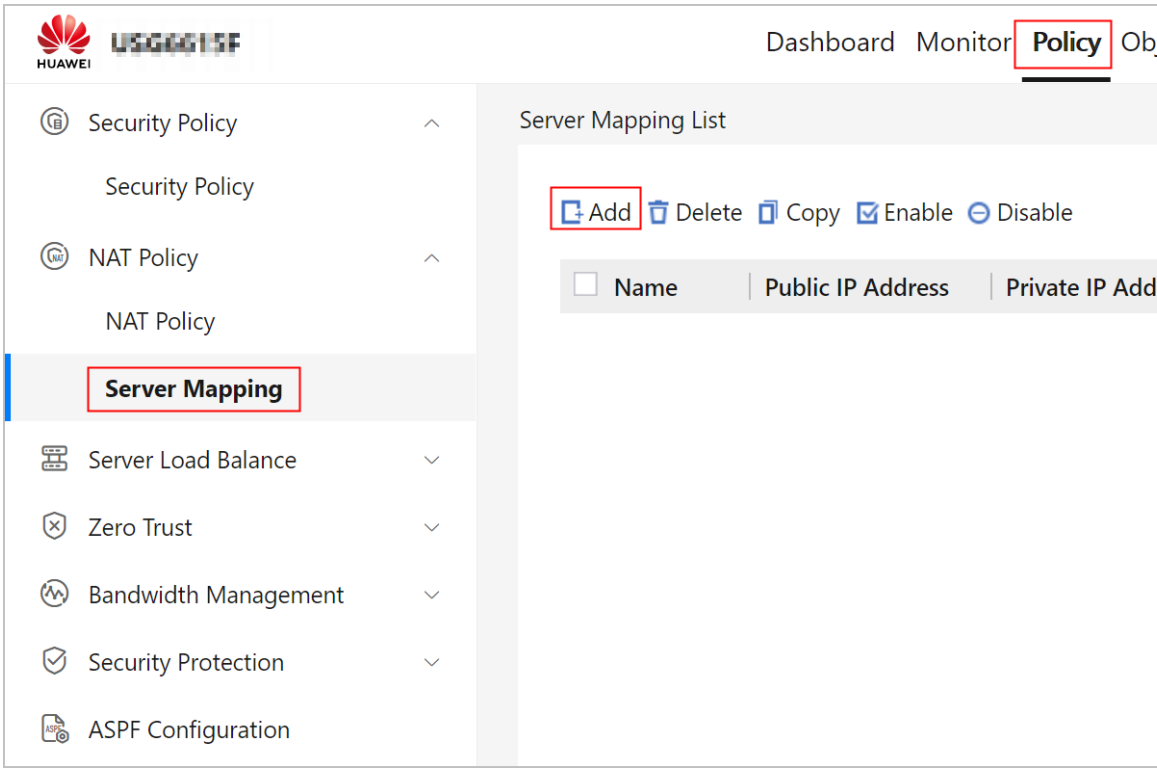
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

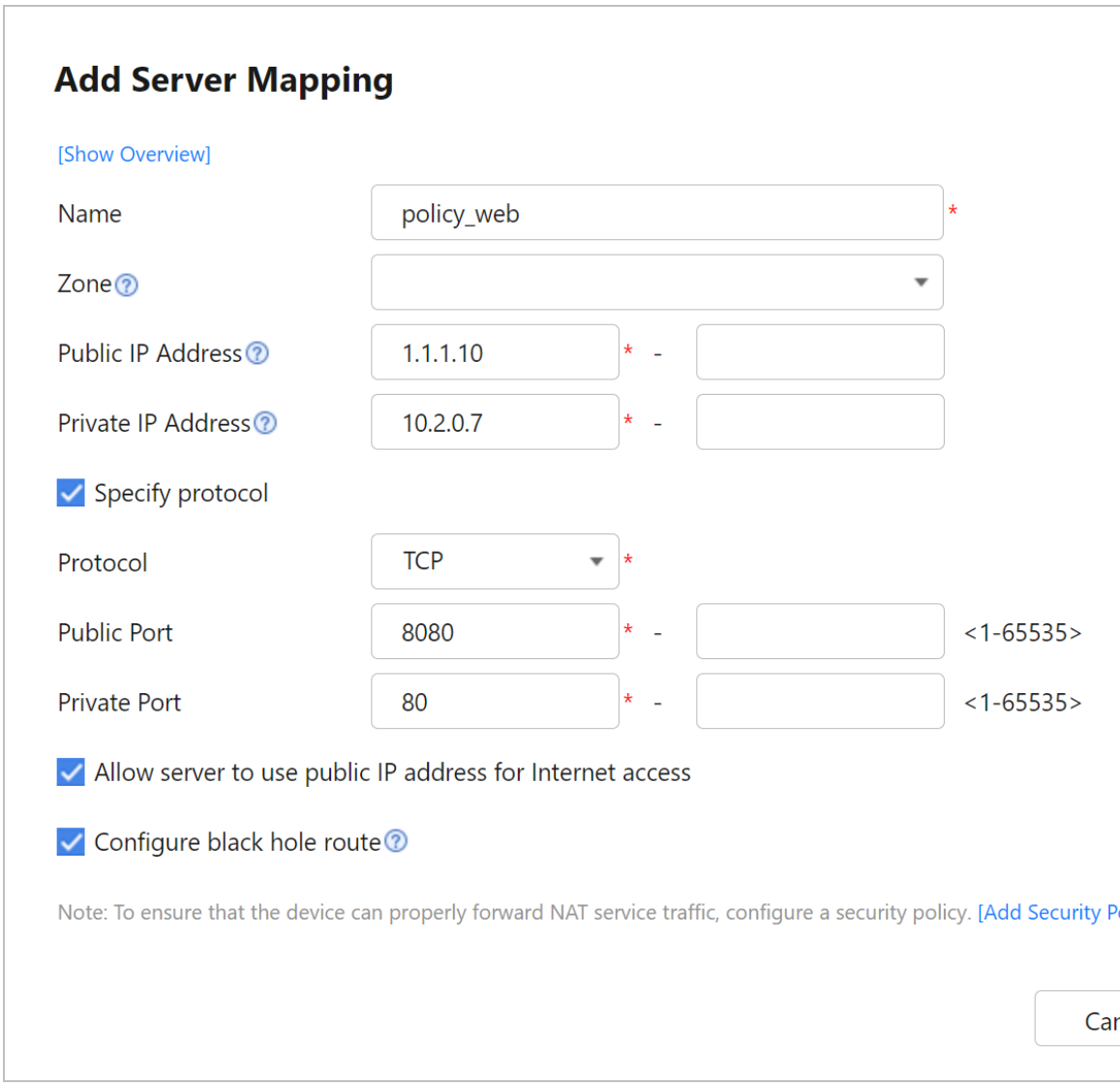
Step 3 Configure two server mapping entries, one for the web server and the other for the FTP server.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.



2. Click **Add** and set the following parameters for a server mapping policy named **policy_web** used for directing traffic to the web server.

 Copyright © Huawei Technologies Co., Ltd.

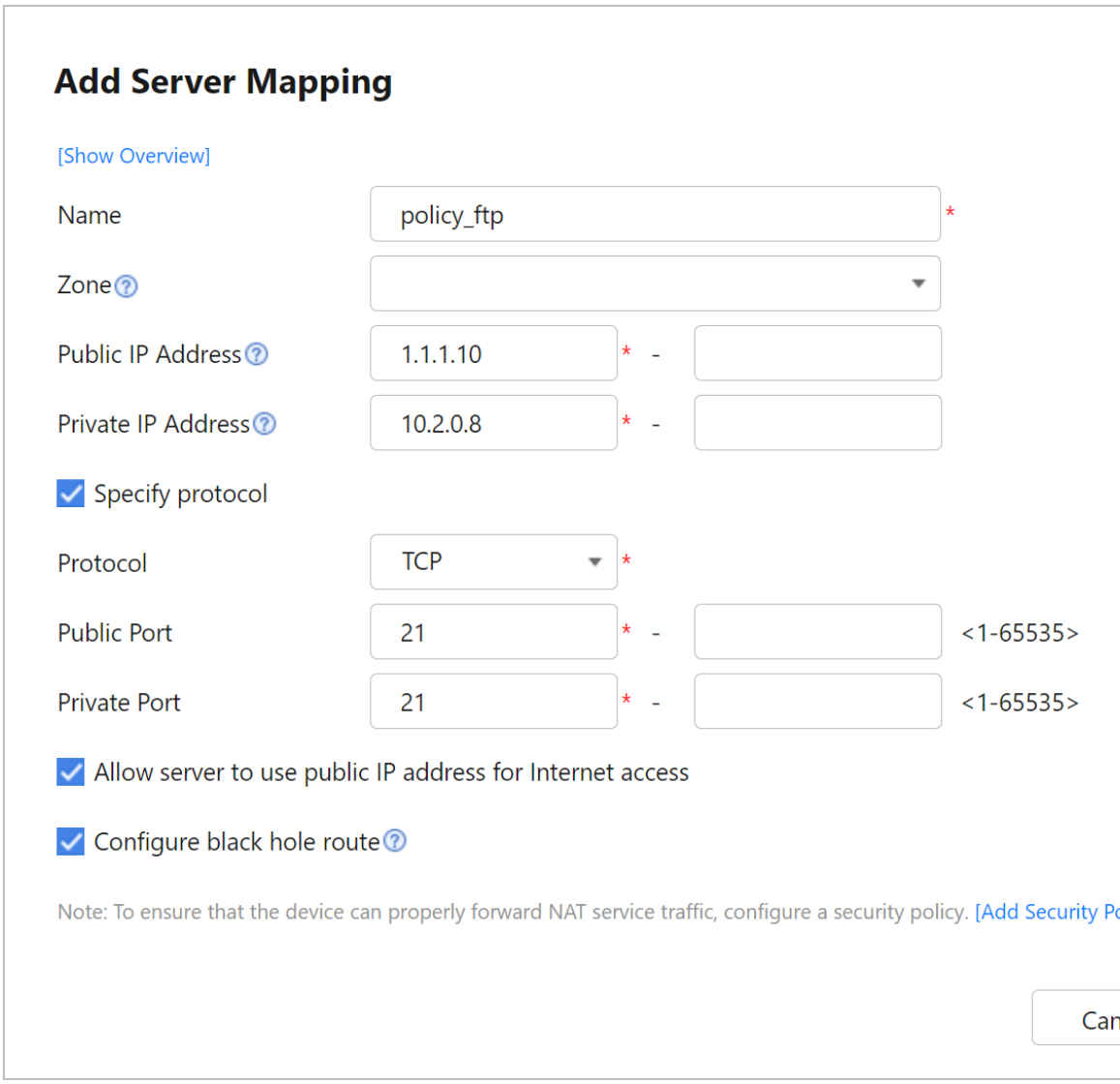


NOTE

If the global address configured in NAT Server and the WAN interface address are on different network segments, a blackhole route is required. If they are on the same network segment, a blackhole route is recommended. If the global address of NAT Server is consistent with the WAN interface address, no routing loop occurs and no black-hole route is required.

3. Click **OK**.
4. Repeat the preceding substeps and set the following parameters for another server mapping policy named **policy_ftp** used for directing traffic to the FTP server.

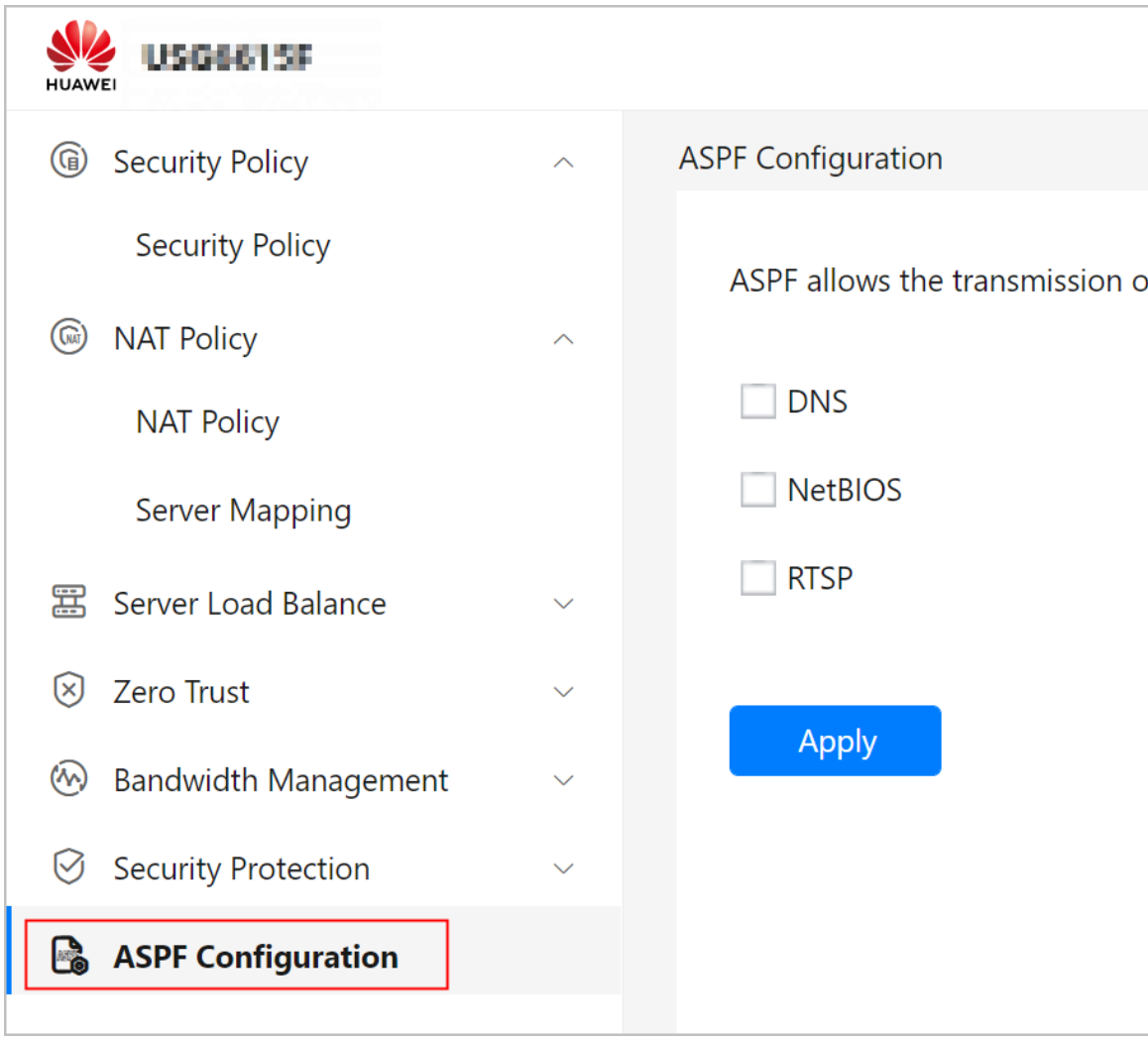
 Copyright © Huawei Technologies Co., Ltd.



Step 4 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.



2. Select **FTP**.

Step 5 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 6 On the router, configure a static route, in which the destination address is 1.1.1.10 and the next-hop address is 1.1.1.1. The router directs traffic destined for 1.1.1.10 to the DeviceA can forward the traffic to the intranet server.

 Copyright © Huawei Technologies Co., Ltd.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.3.2 CLI: Example for Configuring NAT Server for Internet Users to Access Intranet Servers

Networking Requirements

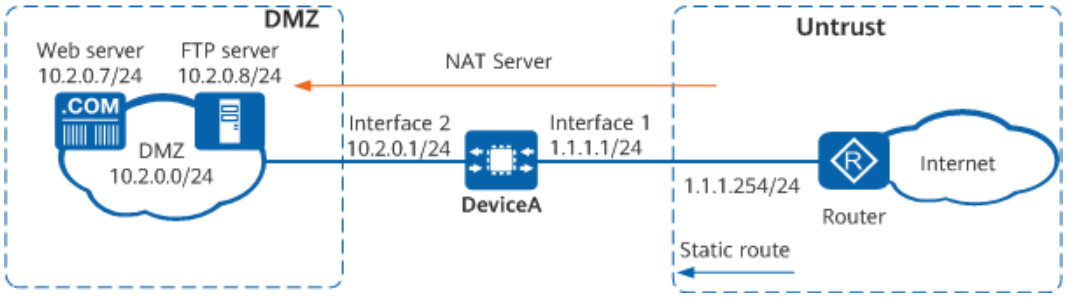
An enterprise has deployed DeviceA as a security gateway at the intranet border. NAT Server needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.1.10) from the ISP, which is used by intranet servers to provide services to Internet users. **Figure 15-29** shows the network diagram, in which the router is the access gateway provided by the ISP.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-29 Network diagram of NAT Server

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
NAT Server	Name: policy_web Public IP address: 1.1.1.10 Private IP address: 10.2.0.7 Public port: 8080 Private port: 80	When Internet users send traffic to 1.1.1.10 through port 8080, DeviceA can forward the traffic to the web server based on this mapping entry. The web server has the private address 10.2.0.7 and private port number 80.
	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic to 1.1.1.10 through port 21, DeviceA can forward the traffic to the FTP server based on this mapping entry. The FTP server has the private address 10.2.0.8 and private port number 21.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA so that it can forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

 Copyright © Huawei Technologies Co., Ltd.

2. Configure a security policy so that Internet users can access intranet servers.
3. Configure NAT Server to implement address translation for the intranet web and FTP servers.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure NAT Server.

```
[DeviceA] nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
[DeviceA] nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
```

Step 4 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 5 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

 Copyright © Huawei Technologies Co., Ltd.

Step 6 On the ISP router, configure a static route to the public address (1.1.1.10) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination address as the public address of intranet servers. If such an entry is found and the post-NAT IP address is the private IP address of an intranet server, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 tcp  VPN:public --> public  1.2.1.3:2474-->1.1.1.10:8080[10.2.0.7:80]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.3.3 Web: Example for Configuring NAT Server for Internet Users to Access Servers on an Intranet with Two Egresses in Different Security Zones

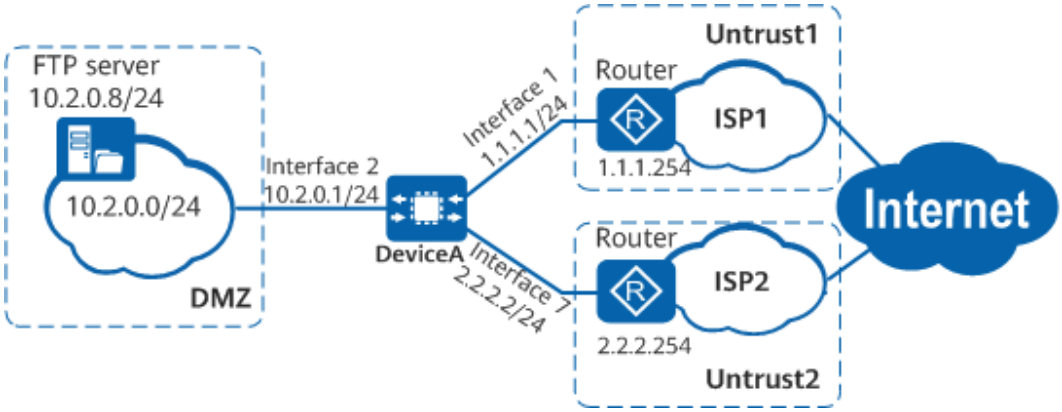
Networking Requirements

In **Figure 15-30**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. NAT Server needs to be configured with the **zone** parameter specified on DeviceA so that the intranet FTP server can provide services to Internet users. In addition to the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.1.10 and 2.2.2.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. **Figure 15-30** shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-30 Network diagram of NAT Server on an intranet with two egresses in different security zones

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
NAT Server	Name: policy_ftp1 Zone: Untrust1 Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 1.1.1.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.
	Name: policy_ftp2 Zone: Untrust2 Public IP address: 2.2.2.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 2.2.2.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure NAT Server.
4. On GE0/0/1 and GE0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.
5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE0/0/2 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE0/0/2 and set the parameters as follows:

 Copyright © Huawei Technologies Co., Ltd.

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

c. Click **OK**.

2. Set the IP address of GE0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** and create security zone **untrust1** based on the following parameter values.

Zone Name	untrust1
Priority	10

   c. Click **OK**.
   d. Choose **Network** > **Interface**.
   e. In **Interface List**, click on the line of GE0/0/1 and set the following parameters.

Zone	untrust1
IPv4	
IP Address	1.1.1.1/24

   f. Click **OK**.
3. Set the IP address of GE0/0/7 and assign the interface to a security zone.
   a. Choose **Network** > **Zone**.
   b. Click **Add** and create security zone **untrust2** based on the following parameter values.

Zone Name	untrust2
Priority	20

   c. Click **OK**.
   d. Choose **Network** > **Interface**.
   e. In **Interface List**, click on the line of GE0/0/7 and set the following parameters.

Zone	untrust2
IPv4	
IP Address	2.2.2.2/24

 Copyright © Huawei Technologies Co., Ltd.

f. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

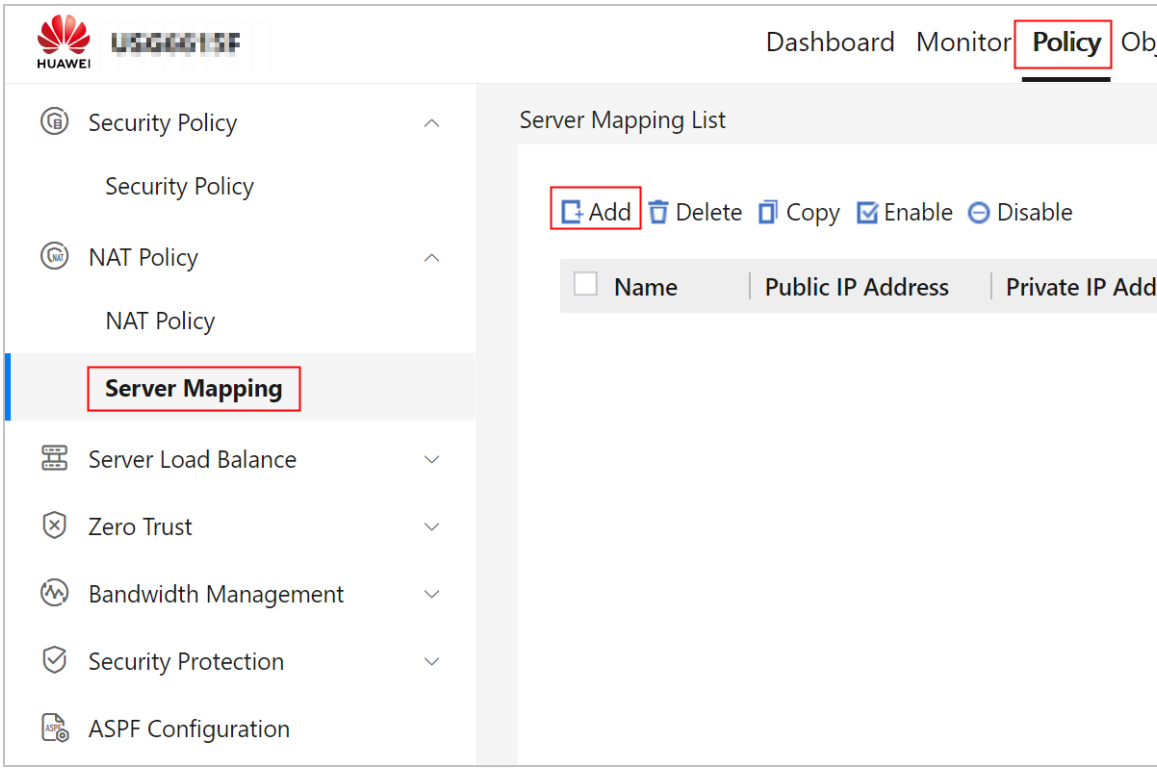
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	untrust1 and untrust2
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

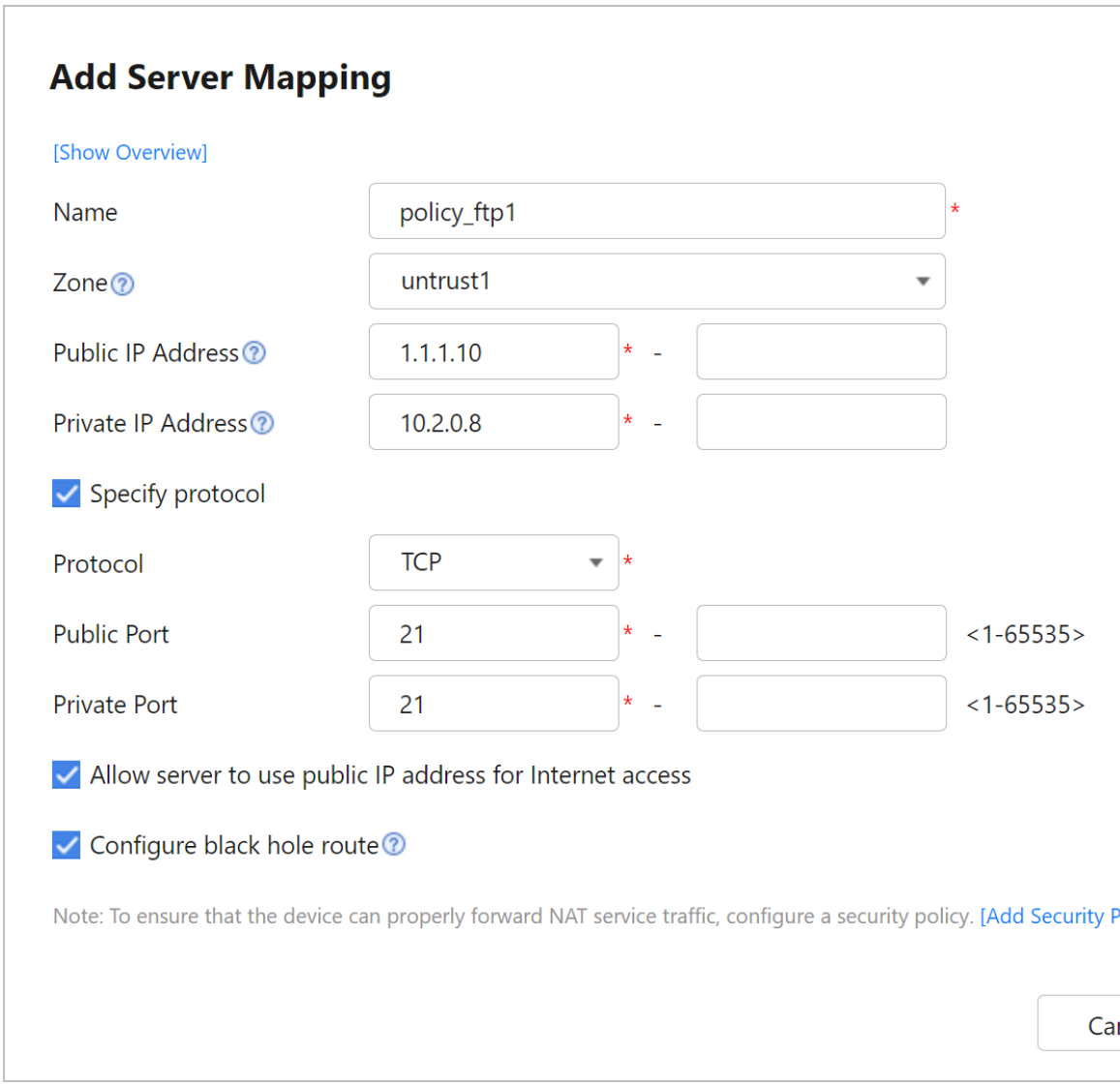
Step 3 Configure NAT Server.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.



2. Click **Add** and configure a server mapping between the untrust1 zone and the intranet FTP server.

 Copyright © Huawei Technologies Co., Ltd.

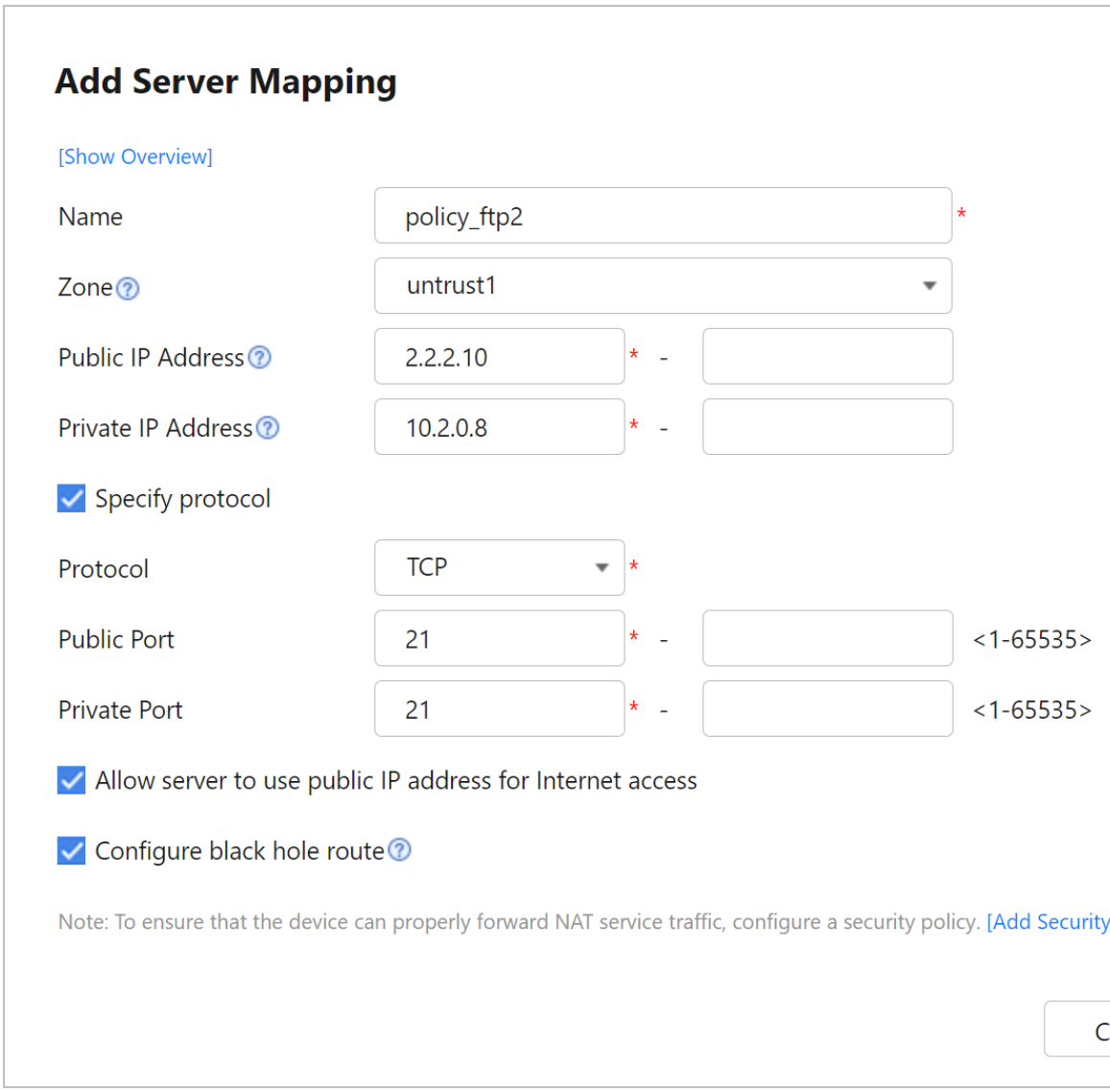


NOTE

By specifying different security zones, a private IP address of a server can advertise multiple public IP addresses. In this scenario, you can select **Allow server to use public IP address for Internet access**.

3. Click **OK**.
4. Repeat the preceding steps to configure a server mapping between the untrust2 zone and the intranet FTP server.

 Copyright © Huawei Technologies Co., Ltd.

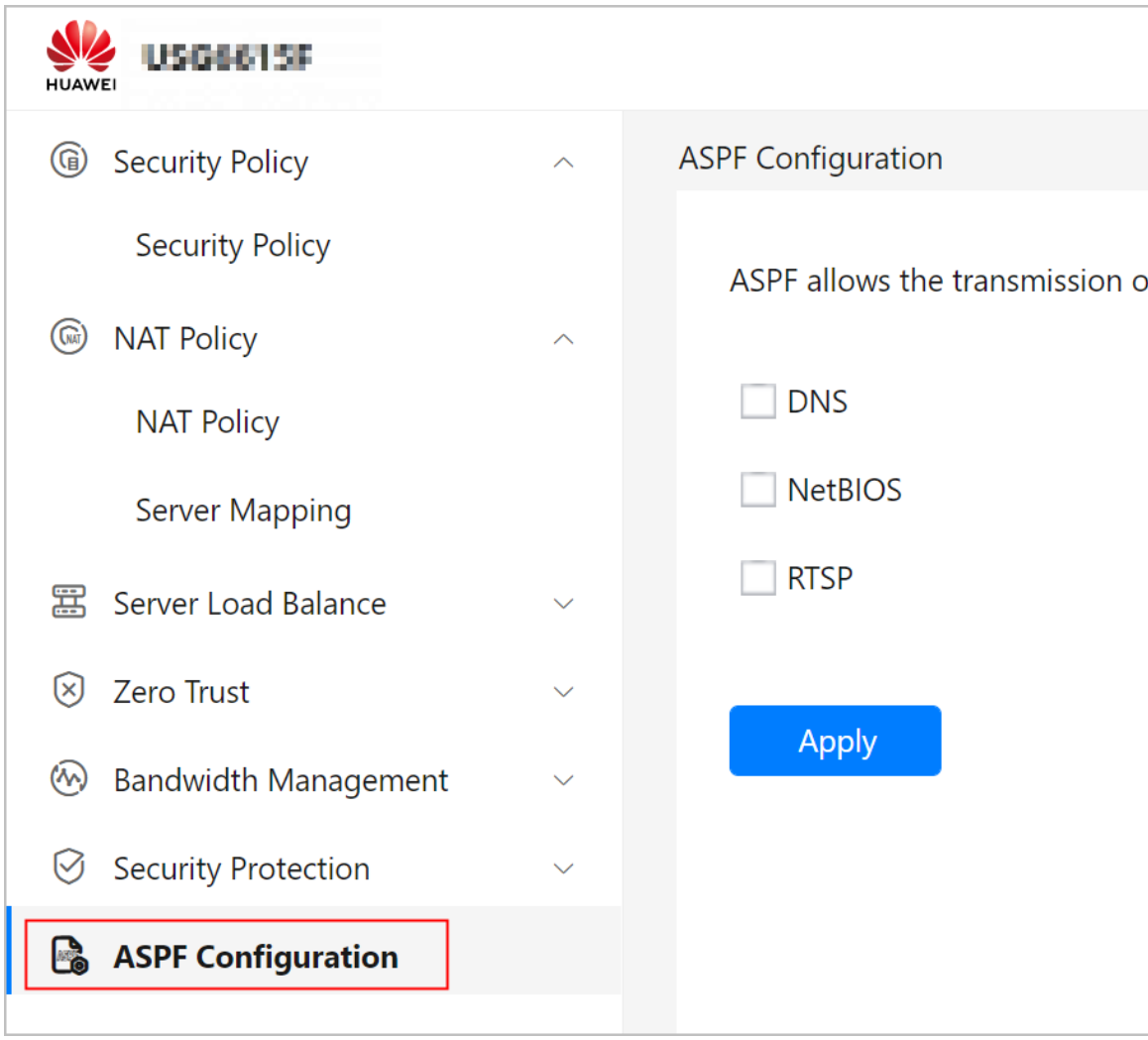


5. Click **OK**.

Step 4 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.

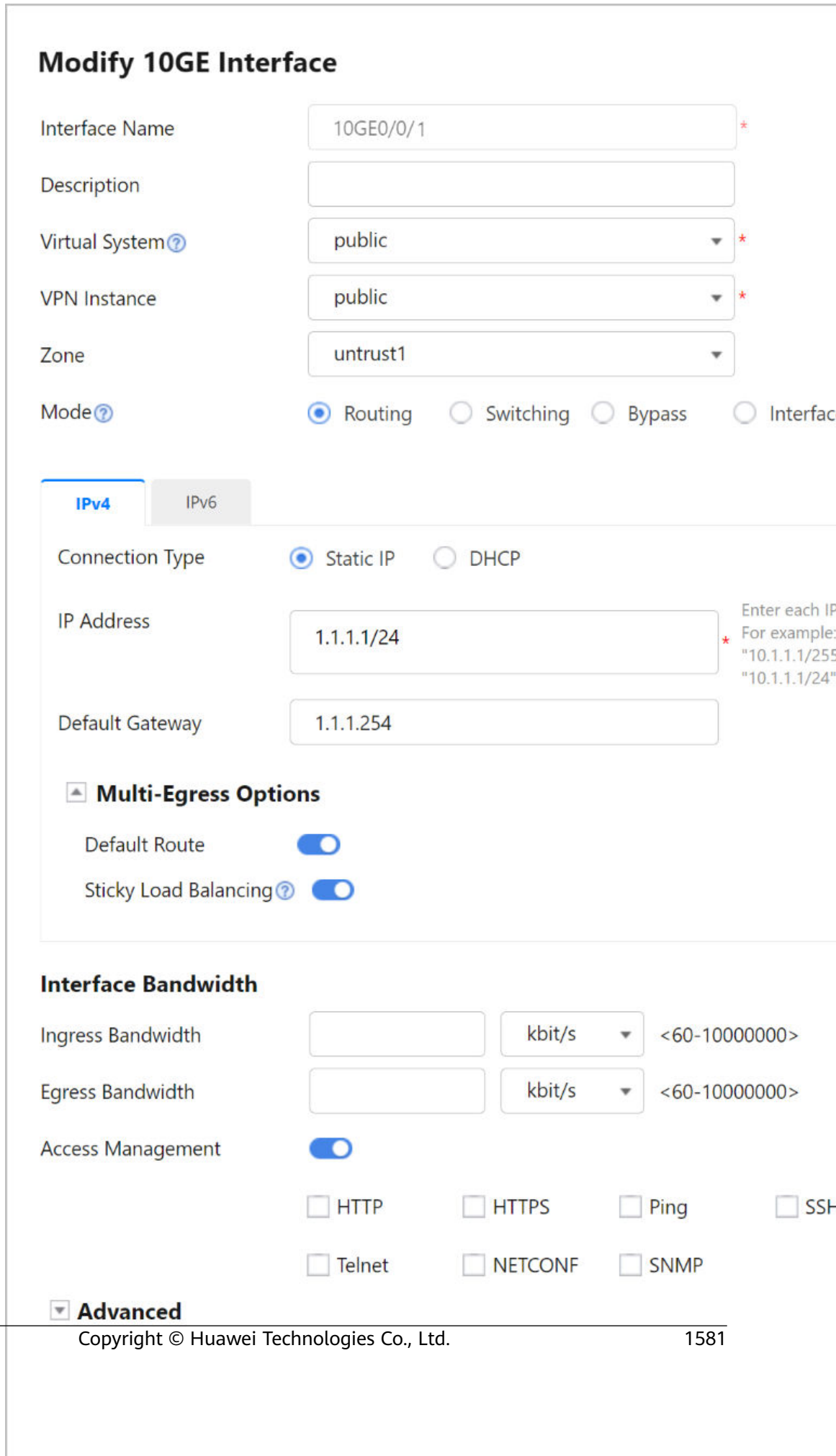


2. Select **FTP**.

Step 5 Configure the sticky load balancing function and default gateway.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click of GE0/0/1 and set the parameters as follows:

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

3. Repeat the preceding steps to configure GE0/0/7.

Step 6 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_ftp1 zone untrust1 protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
 nat server policy_ftp2 zone untrust2 protocol tcp global 2.2.2.10 ftp inside 10.2.0.8 ftp route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
firewall interzone dmz untrust2
 detect ftp
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.3.4 CLI: Example for Configuring NAT Server for Internet Users to Access a Server on an Intranet with Two Egresses in Different Security Zones

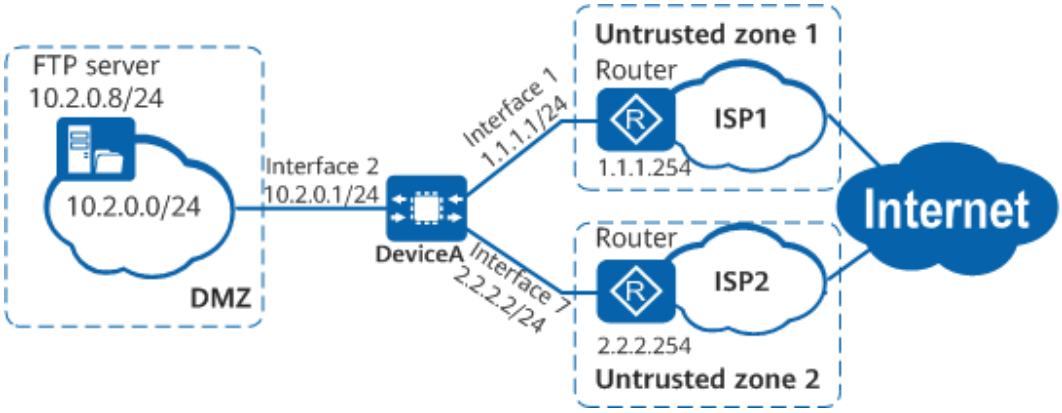
Networking Requirements

In **Figure 15-31**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. NAT Server needs to be configured with the **zone** parameter specified on DeviceA so that the intranet FTP server can provide services to Internet users. In addition to the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.1.10 and 2.2.2.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. **Figure 15-31** shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-31 Network diagram of NAT Server on an intranet with two egresses in different security zones

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
NAT Server	Name: policy_ftp1 Security zone: Untrust1 Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 1.1.1.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.
	Name: policy_ftp2 Security zone: Untrust2 Public IP address: 2.2.2.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 2.2.2.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure NAT Server.
4. On GE 0/0/1 and GE 0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.
5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE 0/0/1 to the Untrust1 zone.

```
[DeviceA] firewall zone name untrust1
[DeviceA-zone-untrust1] set priority 10
[DeviceA-zone-untrust1] add interface ge 0/0/1
[DeviceA-zone-untrust1] quit
```

Add GE 0/0/7 to the Untrust2 zone.

```
[DeviceA] firewall zone name untrust2
[DeviceA-zone-untrust2] set priority 20
[DeviceA-zone-untrust2] add interface ge 0/0/7
[DeviceA-zone-untrust2] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust1
[DeviceA-policy-security-rule-policy1] source-zone untrust2
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure NAT Server.

```
[DeviceA] nat server policy_ftp1 zone untrust1 protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
[DeviceA] nat server policy_ftp2 zone untrust2 protocol tcp global 2.2.2.10 ftp inside 10.2.0.8 ftp route
```

Step 4 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust1
[DeviceA-interzone-dmz-untrust1] detect ftp
[DeviceA-interzone-dmz-untrust1] quit
[DeviceA] firewall interzone dmz untrust2
[DeviceA-interzone-dmz-untrust2] detect ftp
[DeviceA-interzone-dmz-untrust2] quit
```

Step 5 Enable the sticky load balancing function and configure the default gateway address.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] redirect-reverse next-hop 1.1.1.254
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] redirect-reverse next-hop 2.2.2.254
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Step 6 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Verify that Internet users can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of the intranet server. If such an entry is found and the post-NAT IP address is the private IP address of the intranet server, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 tcp  VPN:public --> public  1.1.1.35:2474-->1.1.1.10:21[10.2.0.8:21]
 tcp  VPN:public --> public  2.2.2.22:2025-->2.2.2.10:21[10.2.0.8:21]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_ftp1 zone untrust1 protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
 nat server policy_ftp2 zone untrust2 protocol tcp global 2.2.2.10 ftp inside 10.2.0.8 ftp route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
firewall interzone dmz untrust2
 detect ftp
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.3.5 Web: Example for Configuring NAT Server for Internet Users to Access Servers on an Intranet with Two Egresses in the Same Security Zone

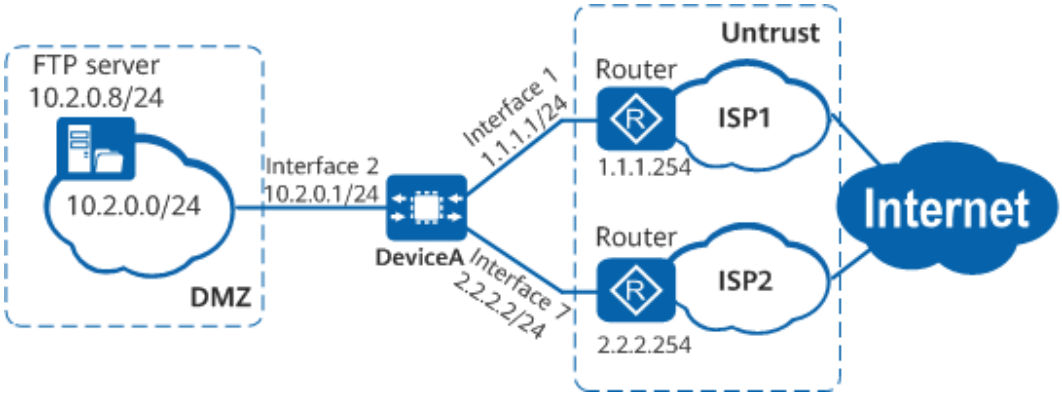
Networking Requirements

In Figure 15-32, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. NAT Server needs to be configured without the **Allow server to use public IP address for Internet access** parameter specified on DeviceA so that the intranet FTP server can provide services to Internet users. In addition to the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.1.10 and 2.2.2.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. Figure 15-32 shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-32 Network diagram of NAT Server on an intranet with two egresses in the same security zone

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust	2.2.2.2/24 is a public address provided by ISP1.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
NAT Server	Name: policy_ftp1 Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 1.1.1.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.
	Name: policy_ftp2 Public IP address: 2.2.2.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 2.2.2.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure NAT Server.
4. On GE0/0/1 and GE0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.
5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE0/0/2 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	

IP Address	10.2.0.1/24

c. Click **OK**.

2. Set the IP address of GE0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE 0/0/1 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.

3. Set the IP address of GE0/0/7 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE0/0/7 and set the following parameters.

Zone	untrust
IPv4	
IP Address	2.2.2.2/24

   c. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

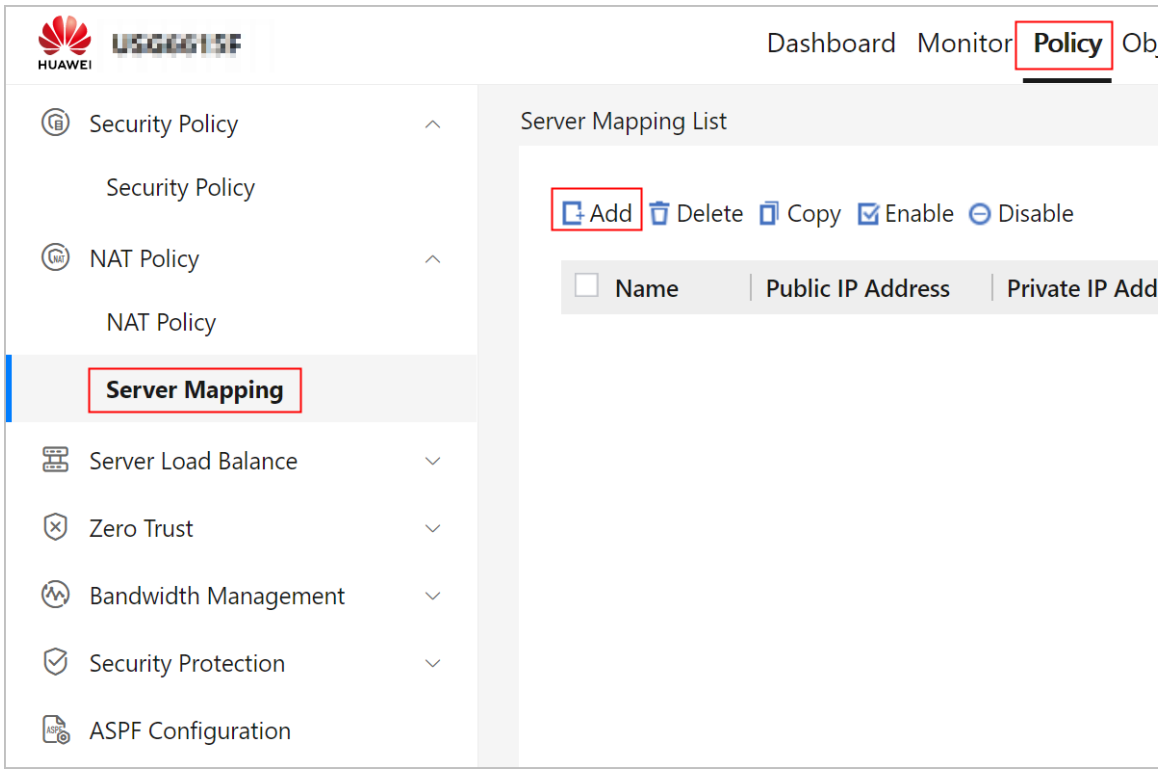
Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT Server.

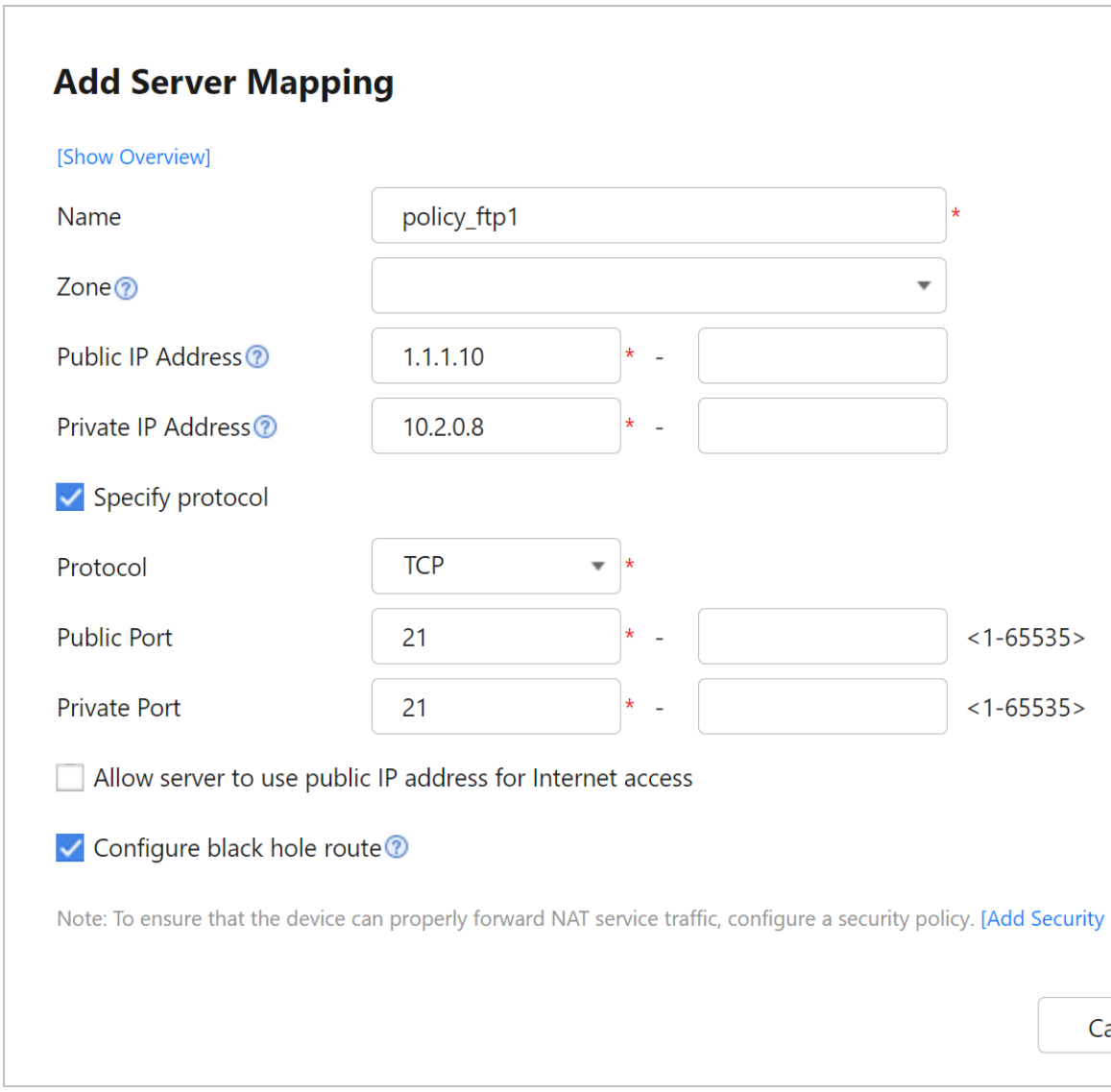
1. Choose **Policy** > **NAT Policy** > **Server Mapping**.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **Add** and configure a server mapping based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.

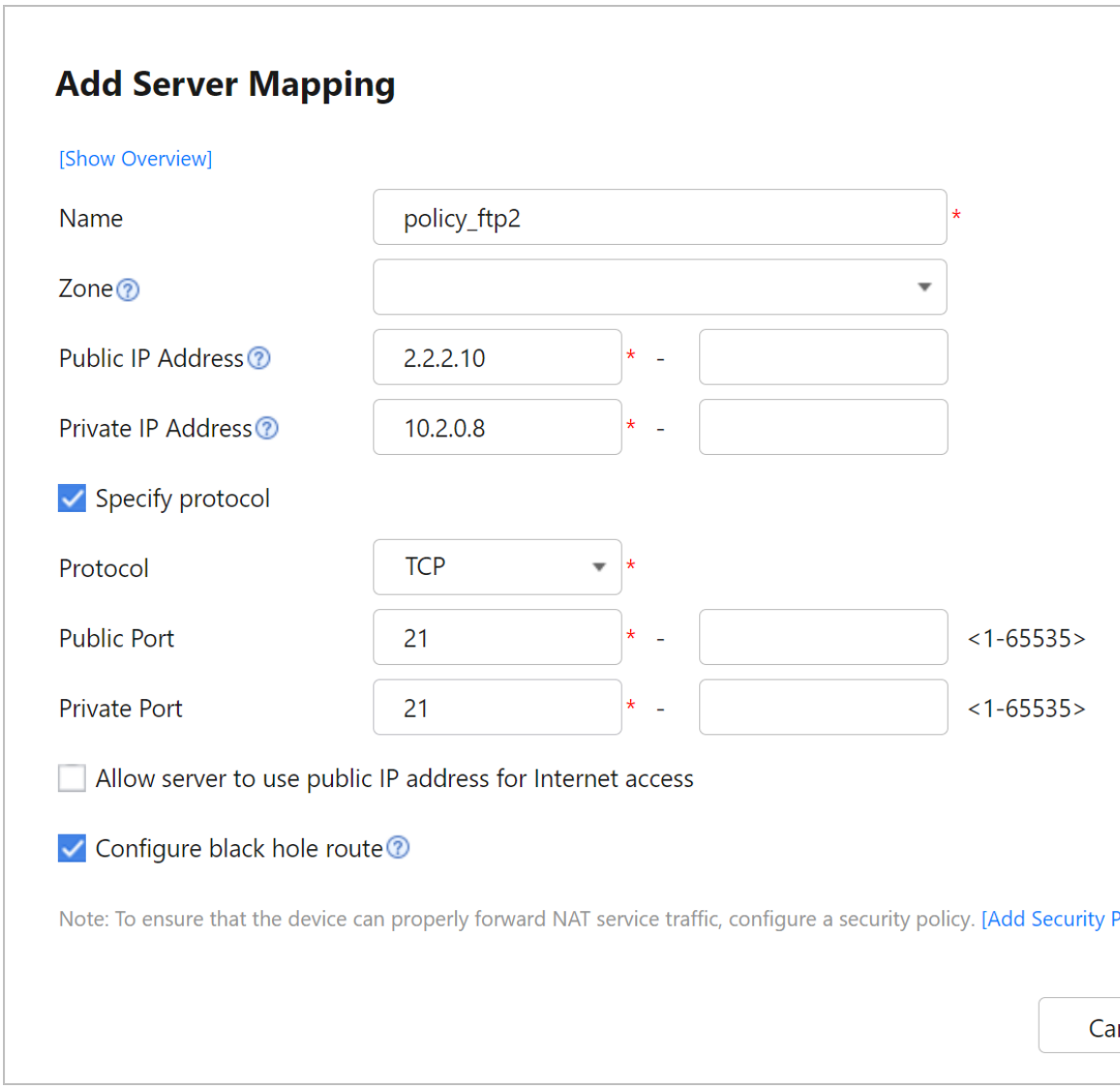


NOTE

In this example, different ISP links belong to the same security zone. In this case, do not select **Allow server to use public IP address for Internet access**.

3. Click **OK**.
4. Repeat the preceding steps to configure another server mapping.

 Copyright © Huawei Technologies Co., Ltd.

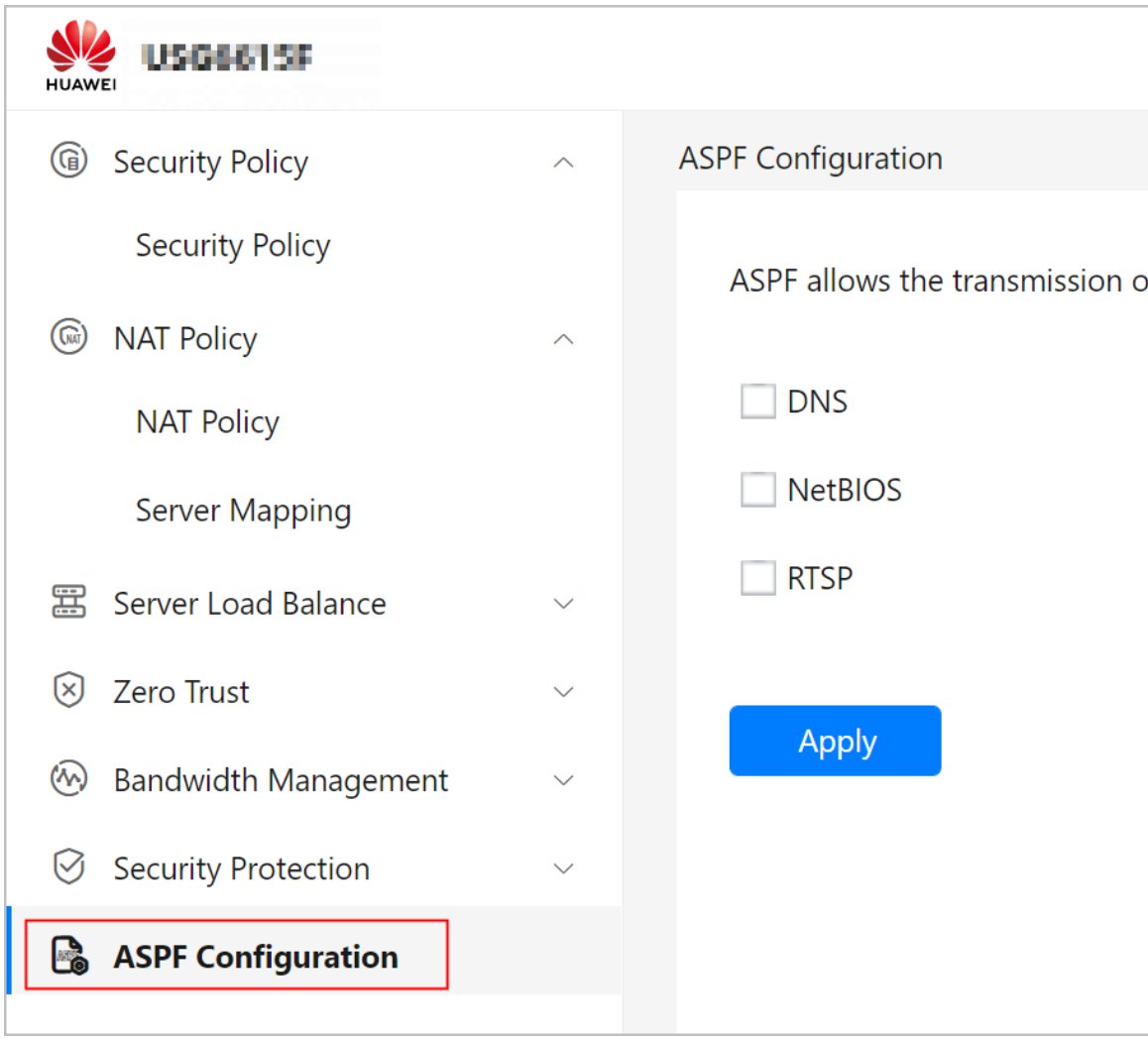


5. Click **OK**.

Step 4 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.

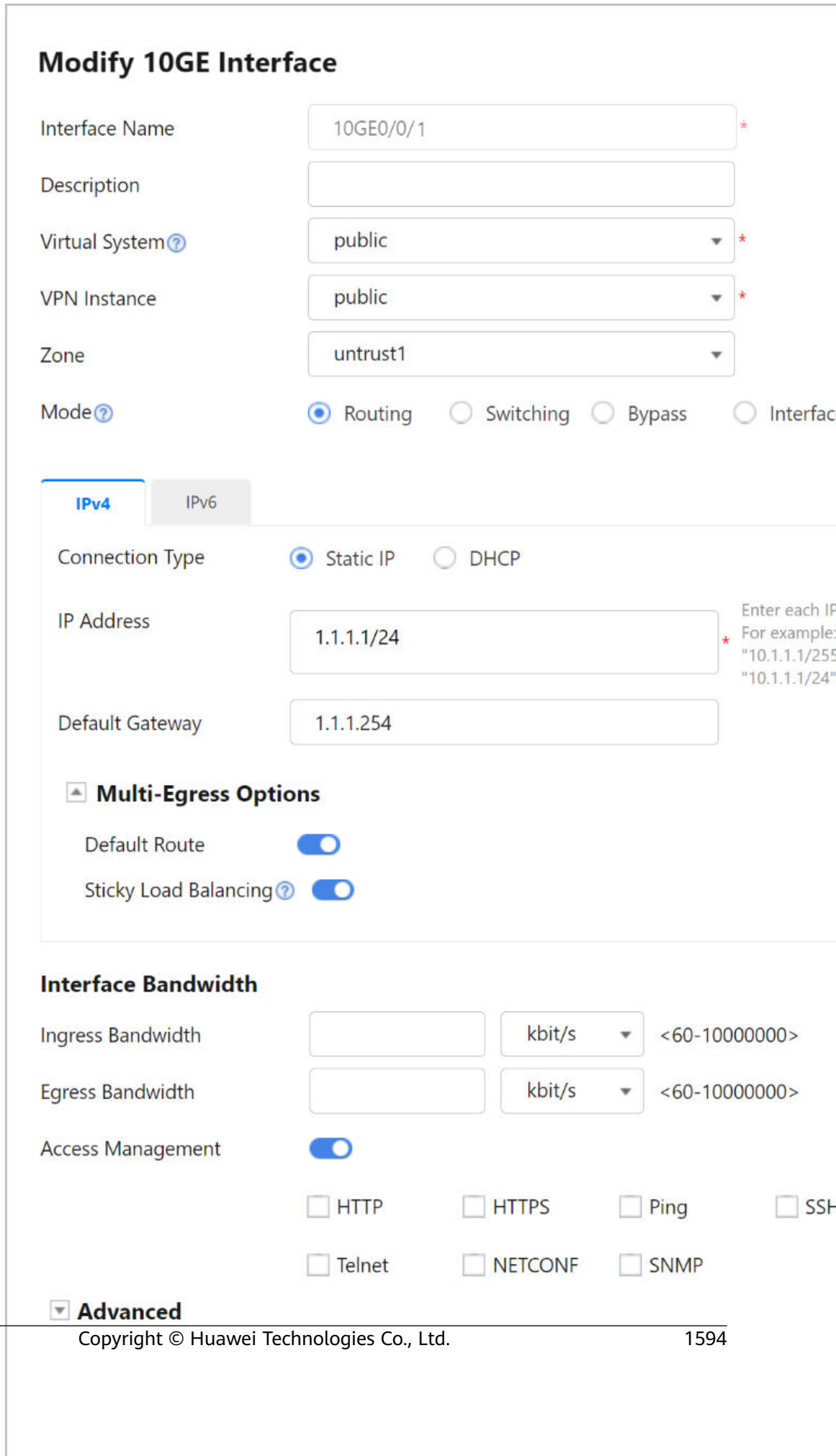


2. Select **FTP**.

Step 5 Configure the sticky load balancing function and default gateway.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click of GE0/0/1 and set the parameters as follows:

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

3. Repeat the preceding steps to configure GE0/0/7.

Step 6 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_ftp1 protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse route
 nat server policy_ftp2 protocol tcp global 2.2.2.10 ftp inside 10.2.0.8 ftp no-reverse route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
 #
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/7
#
firewall interzone dmz untrust
 detect ftp
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.3.6 CLI: Example for Configuring NAT Server for Internet Users to Access a Server on an Intranet with Two Egresses in the Same Security Zone

Networking Requirements

In **Figure 15-33**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. NAT Server needs to be configured with the **no-reverse** parameter specified on DeviceA so that the intranet FTP server can provide services to Internet users. In addition to

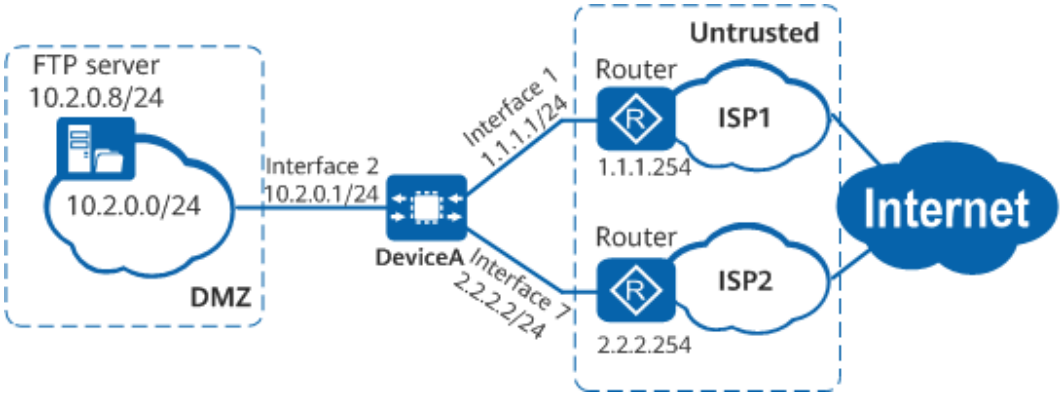
 Copyright © Huawei Technologies Co., Ltd.

the public addresses of WAN interfaces on DeviceA, the enterprise has obtained public IP addresses 1.1.1.10 and 2.2.2.10 from ISP1 and ISP2, respectively, which are used by the intranet FTP server to provide services to Internet users. **Figure 15-33** shows the network diagram, in which the routers are access gateways provided by ISP1 and ISP2.

Figure 15-33 Network diagram of NAT Server on an intranet with two egresses in the same security zone

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-
NAT Server	Name: policy_ftp1 Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 1.1.1.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.
	Name: policy_ftp2 Public IP address: 2.2.2.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 2.2.2.10, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access the intranet server.
3. Configure NAT Server.
4. On GE 0/0/1 and GE 0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.
5. Configure static routes to the public addresses of the intranet server on ISP routers.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/7 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/7
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure NAT Server.

```
[DeviceA] nat server policy_ftp1 protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse route
[DeviceA] nat server policy_ftp2 protocol tcp global 2.2.2.10 ftp inside 10.2.0.8 ftp no-reverse route
```

Step 4 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 5 Enable the sticky load balancing function and configure the default gateway address.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] redirect-reverse next-hop 1.1.1.254
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] redirect-reverse next-hop 2.2.2.254
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Step 6 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of the intranet server. If such an entry is found and the post-NAT IP address is the private IP address of the intranet server, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 tcp  VPN:public --> public  1.1.1.35:2474-->1.1.1.10:21[10.2.0.8:21]
 tcp  VPN:public --> public  2.2.2.22:2025-->2.2.2.10:21[10.2.0.8:21]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_ftp1 protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse route
 nat server policy_ftp2 protocol tcp global 2.2.2.10 ftp inside 10.2.0.8 ftp no-reverse route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
 #
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/7
#
firewall interzone dmz untrust
 detect ftp
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.3.7 Web: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP address of a Server on a Dual-Egress Intranet (Sticky Load Balancing)

Networking Requirements

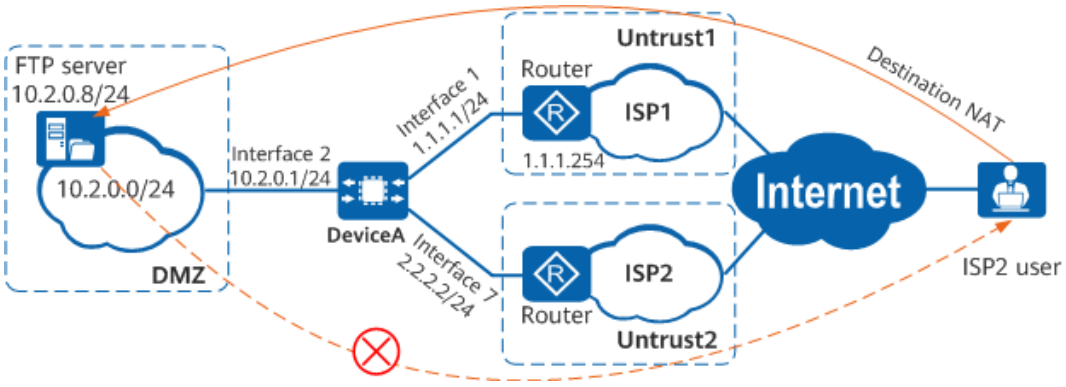
In **Figure 15-34**, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. In addition to the public addresses of WAN interfaces on DeviceA, only one public IP address (1.1.1.10) is obtained from ISP1 for the intranet FTP server to provide services for Internet users. Users on both the ISP1 and ISP2 networks use this public IP address to access the FTP server.

Figure 15-34 Network diagram of NAT Server on a dual-egress intranet, with the sticky load balancing function enabled

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-
NAT Server	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 1.1.1.10 through port 21, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.

Configuration Roadmap

1. Configure NAT Server to enable Internet users to access the intranet FTP server using a public IP address.
2. On GE0/0/1, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE0/0/2 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

b. In **Interface List**, click of GE0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

c. Click **OK**.

2. Set the IP address of GE0/0/1 and assign the interface to a security zone.

a. Choose **Network** > **Zone**.

b. Click **Add** and create security zone **untrust1** based on the following parameter values.

Zone Name	untrust1
Priority	10

c. Click **OK**.

d. Choose **Network** > **Interface**.

e. In **Interface List**, click on the line of GE0/0/1 and set the following parameters.

Zone	untrust1
IPv4	
IP Address	1.1.1.1/24

f. Click **OK**.

3. Set the IP address of GE0/0/7 and assign the interface to a security zone.

a. Choose **Network** > **Zone**.

b. Click **Add** and create security zone **untrust2** based on the following parameter values.

Zone Name	untrust2
Priority	20

c. Click **OK**.

d. Choose **Network** > **Interface**.

e. In **Interface List**, click on the line of GE0/0/7 and set the following parameters.

Zone	untrust2
IPv4	

 Copyright © Huawei Technologies Co., Ltd.

IP Address	2.2.2.2/24

f. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

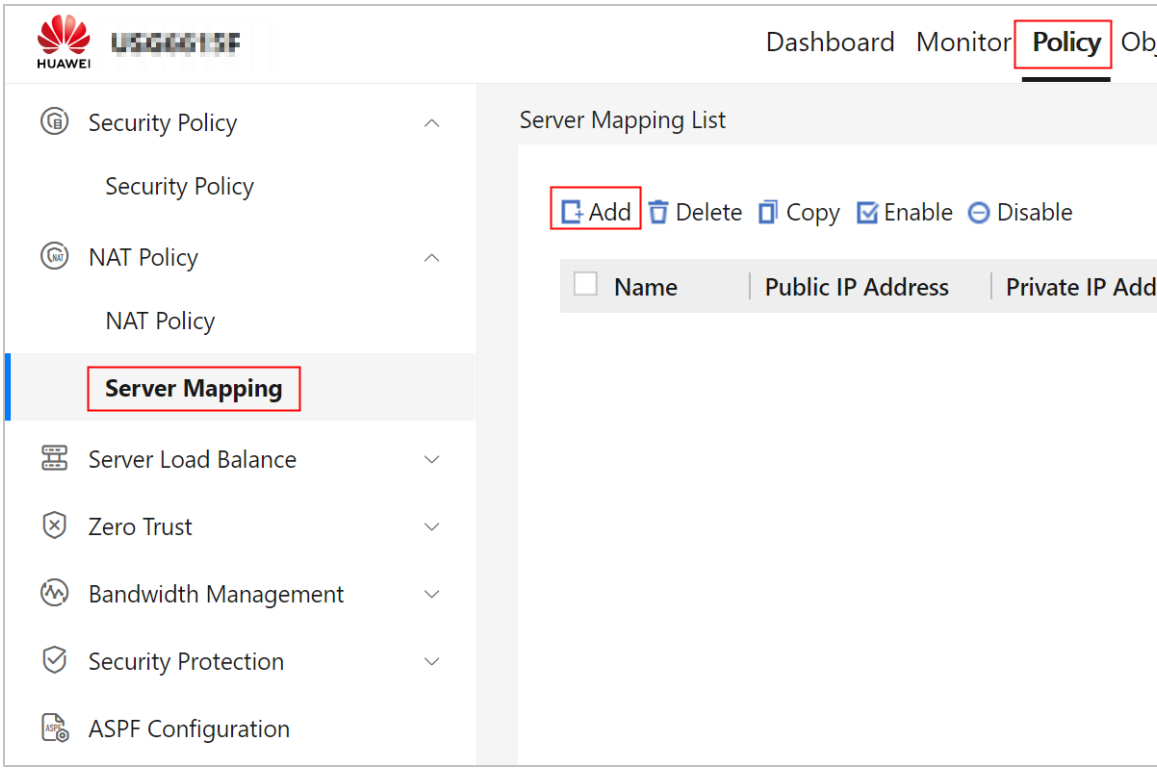
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	untrust1 and untrust2
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

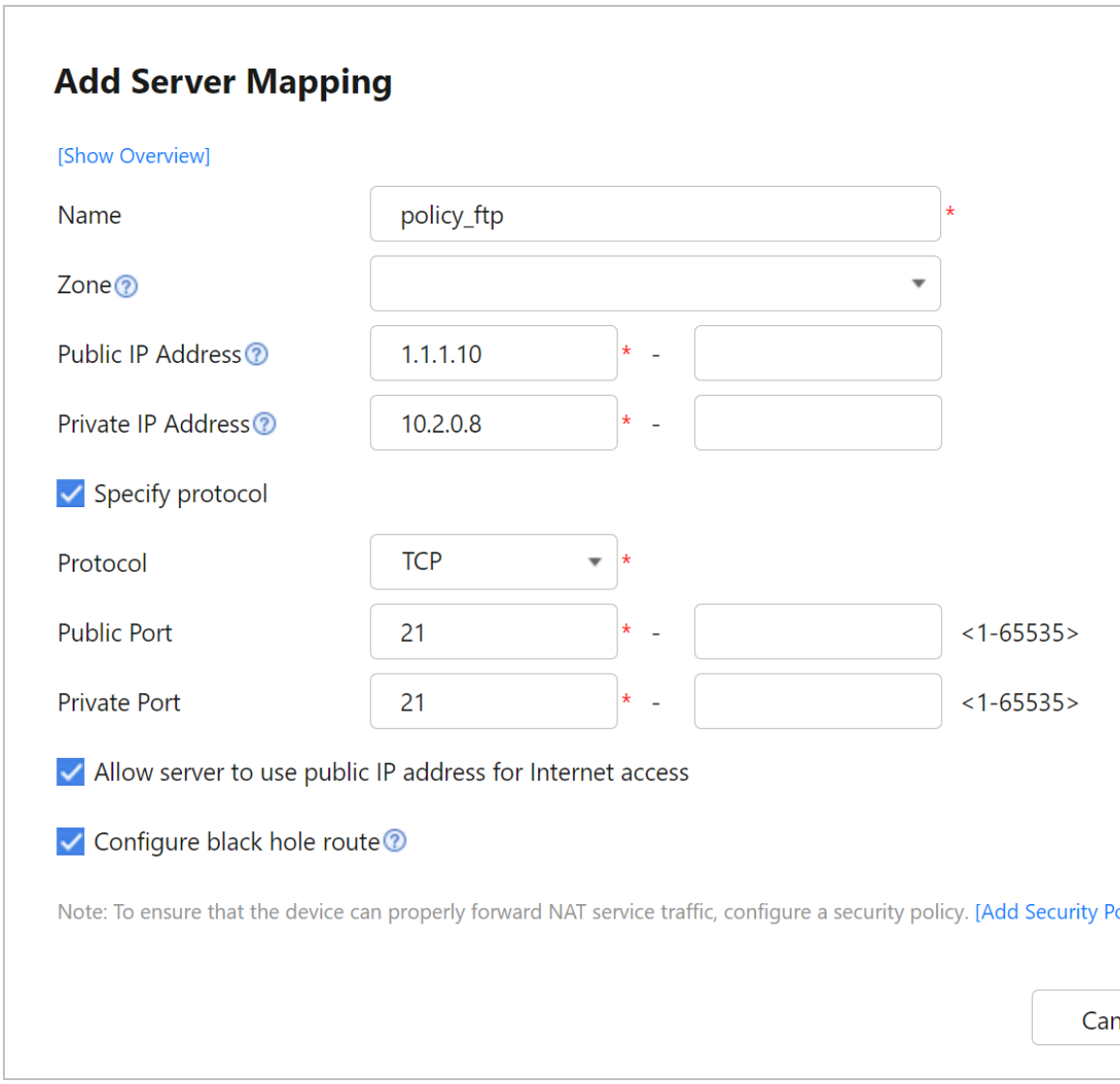
Step 3 Configure NAT Server.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.



2. Click **Add** and configure a server mapping based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.

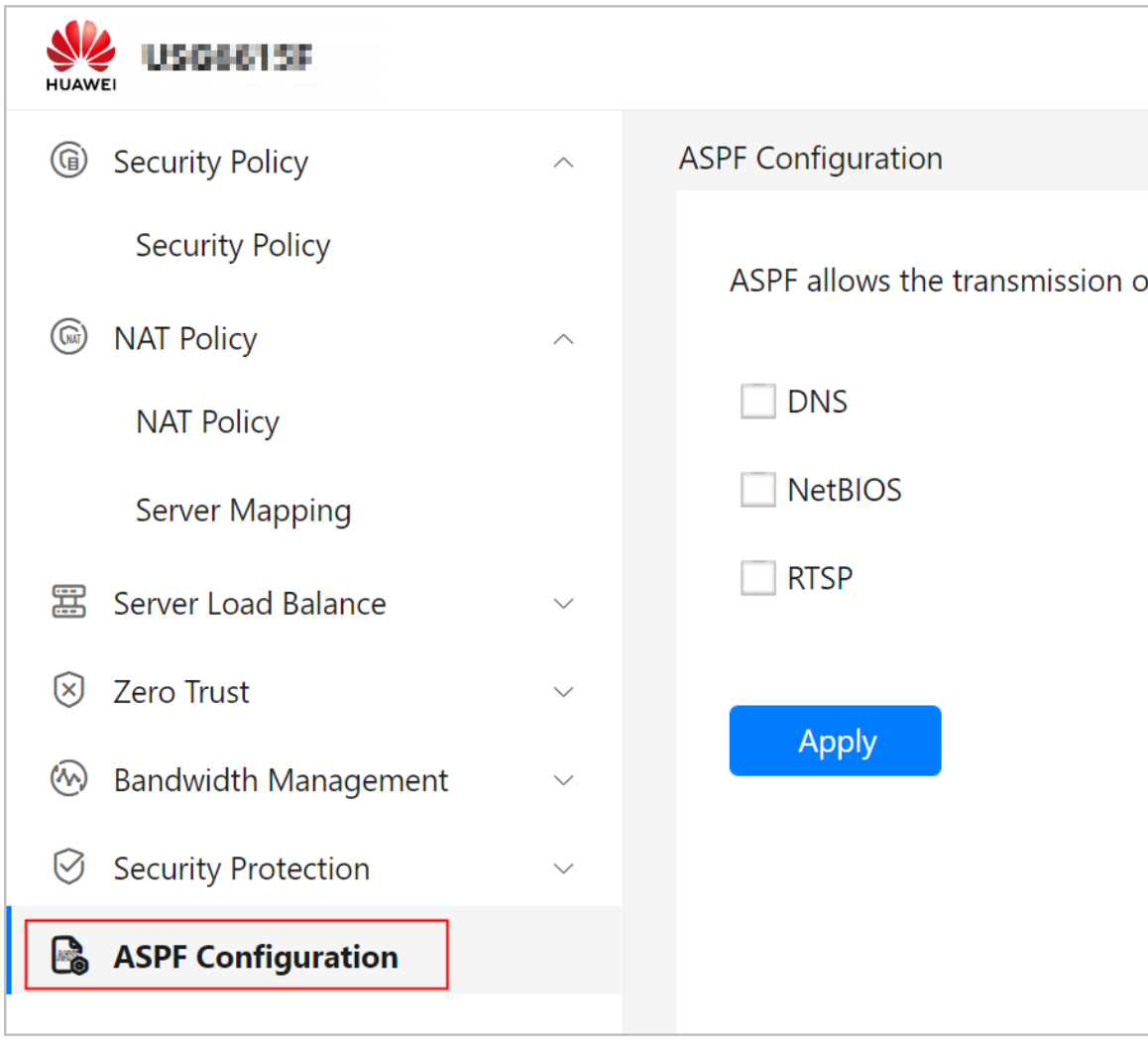


3. Click **OK**.

Step 4 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.

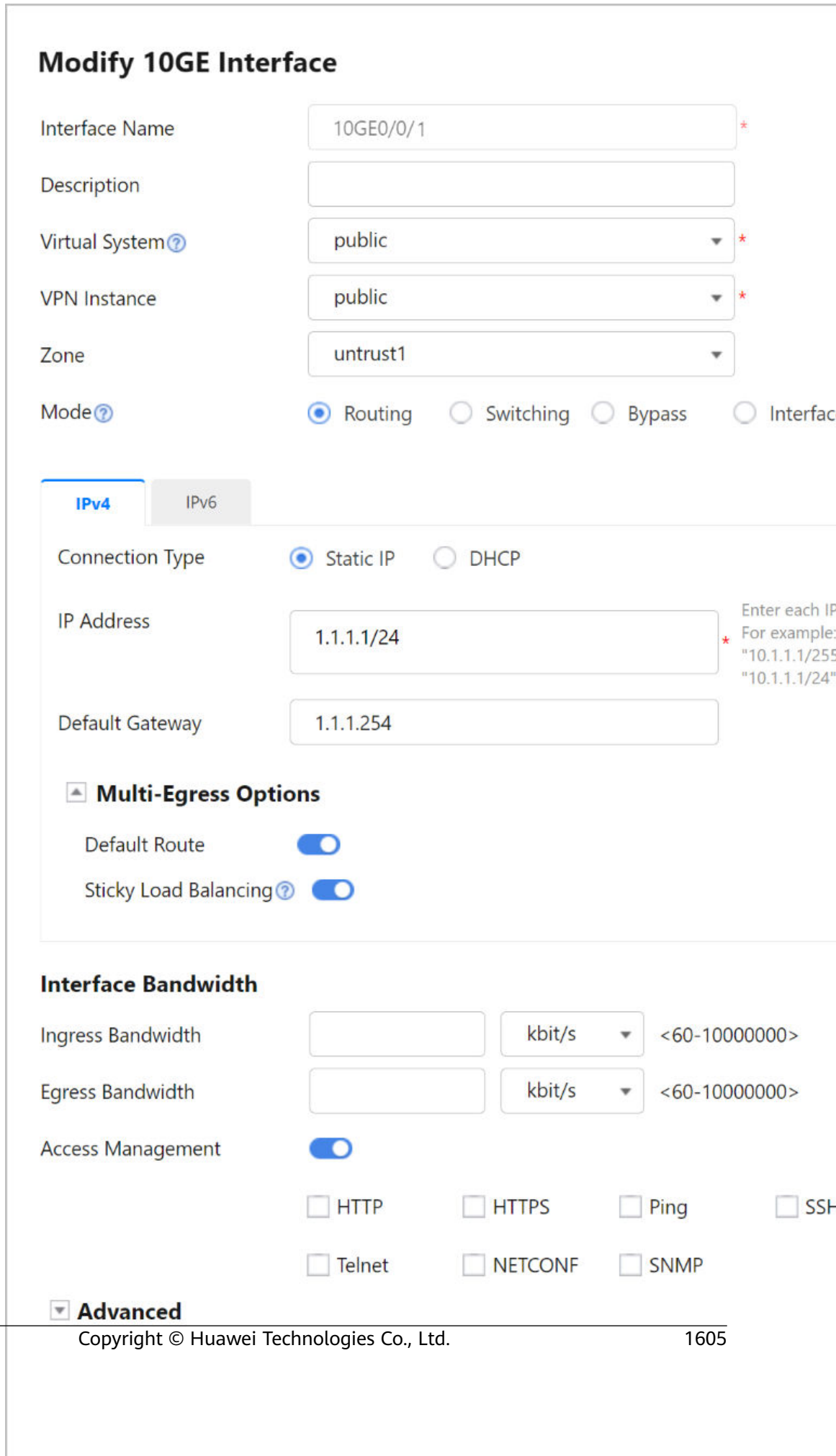


2. Select **FTP**.

Step 5 Configure the sticky load balancing function and default gateway.

1. Choose **Network** > **Interface**.
2. In **Interface List**, click of GE0/0/1 and set the parameters as follows:

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

In this example, the company applies only for the public IP address of the server from ISP1. Therefore, traffic to the server is sent to GE 0/0/1. Configure sticky load balancing only on this interface.

1. Set the default gateway address of GE0/0/7 to 2.2.2.254.

Step 6 Configure static routes to the public addresses of the intranet server on ISP routers, so that they can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrators to perform this step.

----End

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 gateway 2.2.2.254
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.3.8 CLI: Example for Configuring Internet Users of Different ISPs to Access the Same Public IP Address of a Server on a Dual-Egress Intranet (Sticky Load Balancing)

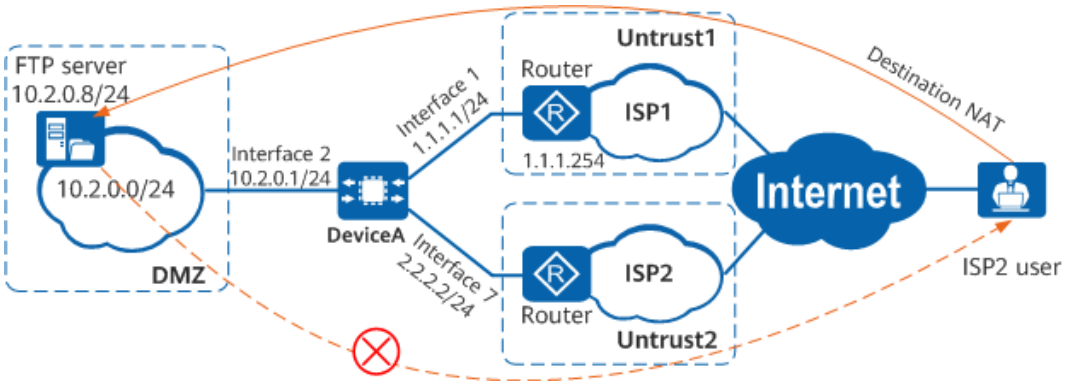
Networking Requirements

In Figure 15-35, an enterprise has deployed DeviceA at the network border as a security gateway that connects to the Internet over two ISP networks. In addition to the public addresses of WAN interfaces on DeviceA, only one public IP address (1.1.1.10) is obtained from ISP1 for the intranet FTP server to provide services for Internet users. Users on both the ISP1 and ISP2 networks use this public IP address to access the FTP server.

Figure 15-35 Network diagram of NAT Server on a dual-egress intranet, with the sticky load balancing function enabled

NOTE

In this example, interfaces 1, 2, and 7 represent GE 0/0/1, GE 0/0/2, and GE 0/0/7, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust1	1.1.1.1/24 is a public address provided by ISP1.
GE0/0/7	IP address: 2.2.2.2/24 Security zone: Untrust2	2.2.2.2/24 is a public address provided by ISP2.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	-
NAT Server	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic destined for 1.1.1.10 through port 21, DeviceA can forward the traffic to the intranet FTP server based on this mapping entry.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure NAT Server to enable Internet users to access the intranet FTP server using a public IP address.
2. On GE 0/0/1 and GE 0/0/7, enable the sticky load balancing function and configure the default gateway address.

   NOTE

   Determine the inbound interfaces of traffic that may have different forward and return paths based on the configured routing information before enabling the sticky load balancing function on them.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE 0/0/7.

```
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 2.2.2.2 24
[DeviceA-GE0/0/7] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE 0/0/1 to the Untrust1 zone.

```
[DeviceA] firewall zone name untrust1
[DeviceA-zone-untrust1] set priority 10
[DeviceA-zone-untrust1] add interface ge 0/0/1
[DeviceA-zone-untrust1] quit
```

Add GE 0/0/7 to the Untrust2 zone.

```
[DeviceA] firewall zone name untrust2
[DeviceA-zone-untrust2] set priority 20
[DeviceA-zone-untrust2] add interface ge 0/0/7
[DeviceA-zone-untrust2] quit
```

Step 2 Configure a security policy so that Internet users can access the intranet server.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust1
[DeviceA-policy-security-rule-policy1] source-zone untrust2
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure NAT Server.

```
[DeviceA] nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse route
```

Step 4 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust1
[DeviceA-interzone-dmz-untrust1] detect ftp
[DeviceA-interzone-dmz-untrust1] quit
```

Step 5 Enable the sticky load balancing function and configure the default gateway address.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] redirect-reverse next-hop 1.1.1.254
[DeviceA-GE0/0/1] gateway 1.1.1.254
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] redirect-reverse next-hop 2.2.2.254
[DeviceA-GE0/0/7] gateway 2.2.2.254
[DeviceA-GE0/0/7] quit
```

Step 6 Configure static routes to the public addresses of the intranet server on the ISP1 router, so that it can forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access the intranet server.
2. Run the **display firewall session table** command on DeviceA to check for the session entry with the destination address as the public address of the intranet server. If such an entry is found and the post-NAT IP address is the private IP address of the intranet server, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 1
 tcp  VPN:public --> public  1.1.1.35:2474-->1.1.1.10:21[10.2.0.8:21]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 redirect-reverse next-hop 1.1.1.254
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 2.2.2.2 255.255.255.0
 redirect-reverse next-hop 2.2.2.254
 gateway 2.2.2.254
#
firewall zone dmz
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set priority 50
 add interface GE0/0/2
#
firewall zone name untrust1 id 4
 set priority 10
 add interface GE0/0/1
#
firewall zone name untrust2 id 5
 set priority 20
 add interface GE0/0/7
#
firewall interzone dmz untrust1
 detect ftp
#
security-policy
  rule name policy1
    source-zone untrust1
    source-zone untrust2
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
return
```

15.4 Bidirectional NAT (Source NAT+Destination NAT)

15.4.1 Web: Example for Configuring Bidirectional NAT (Source NAT + Static Destination NAT) for Internet Users to Access Intranet Servers

Networking Requirements

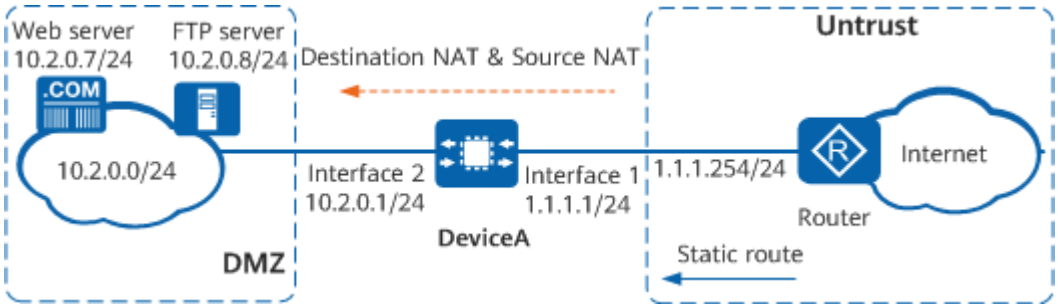
An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by the intranet servers to provide services to Internet users. A source NAT policy is also required to enable intranet servers to send response packets to DeviceA, removing the need to configure return routes for intranet servers. **Figure 15-36** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-36 Network diagram of bidirectional NAT (source NAT + static destination NAT) allowing Internet users to access intranet servers

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
10GE 1/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Source NAT address pool	10.2.0.10 to 10.2.0.15	The source and destination NAT address pools are on the same network segment.
Destination NAT address pool	10.2.0.7 to 10.2.0.8	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA so that it can forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure a destination NAT policy to translate the destination addresses of packets sent from Internet users to intranet servers into addresses in the destination NAT address pool.
4. Configure a source NAT policy to translate the source addresses of packets sent from Internet users to intranet servers into addresses in the source NAT address pool.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure static routes to the public addresses of intranet servers on the ISP router.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

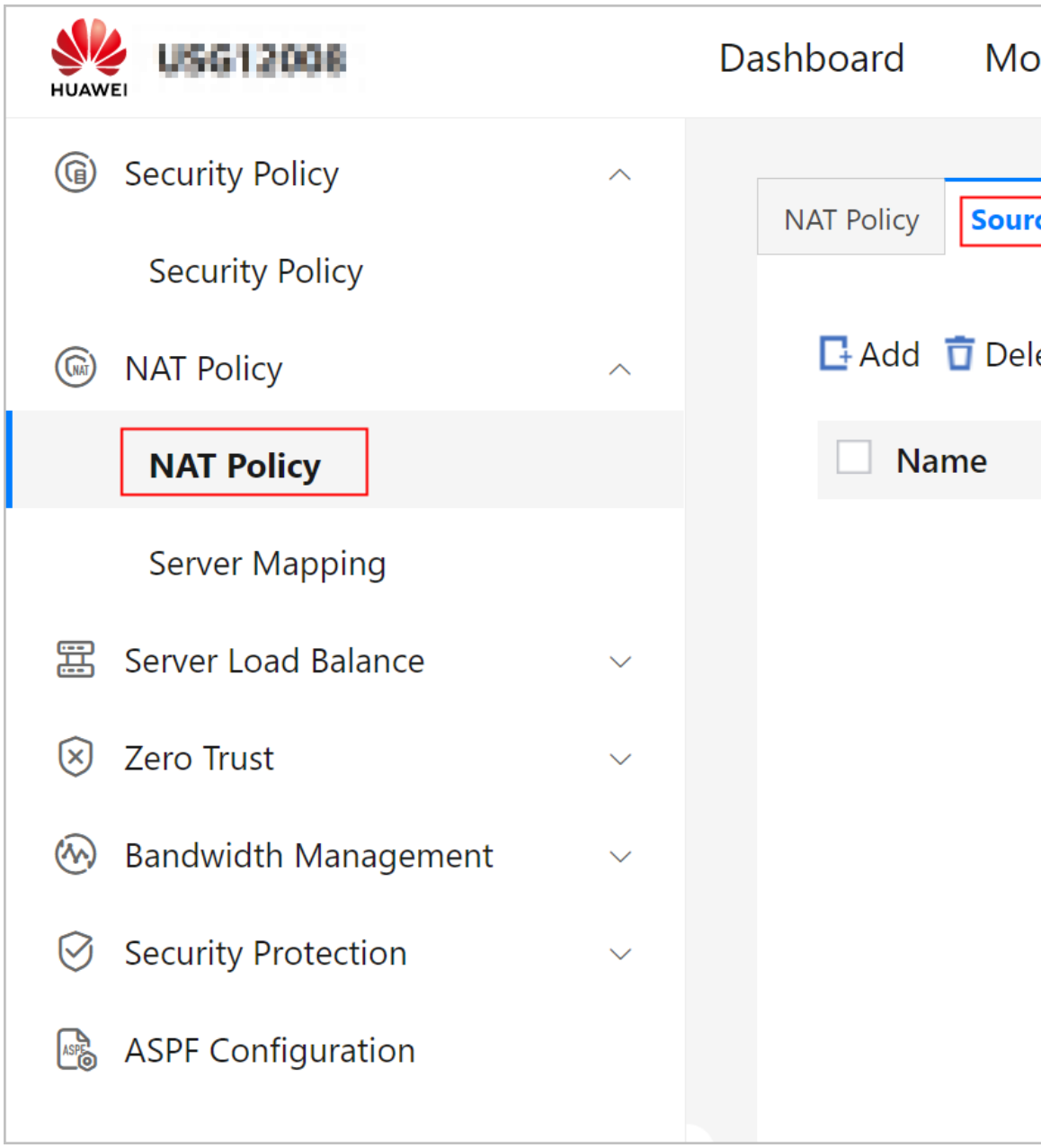
Name	policy1
Source Zone	untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT address pools and NAT policies.

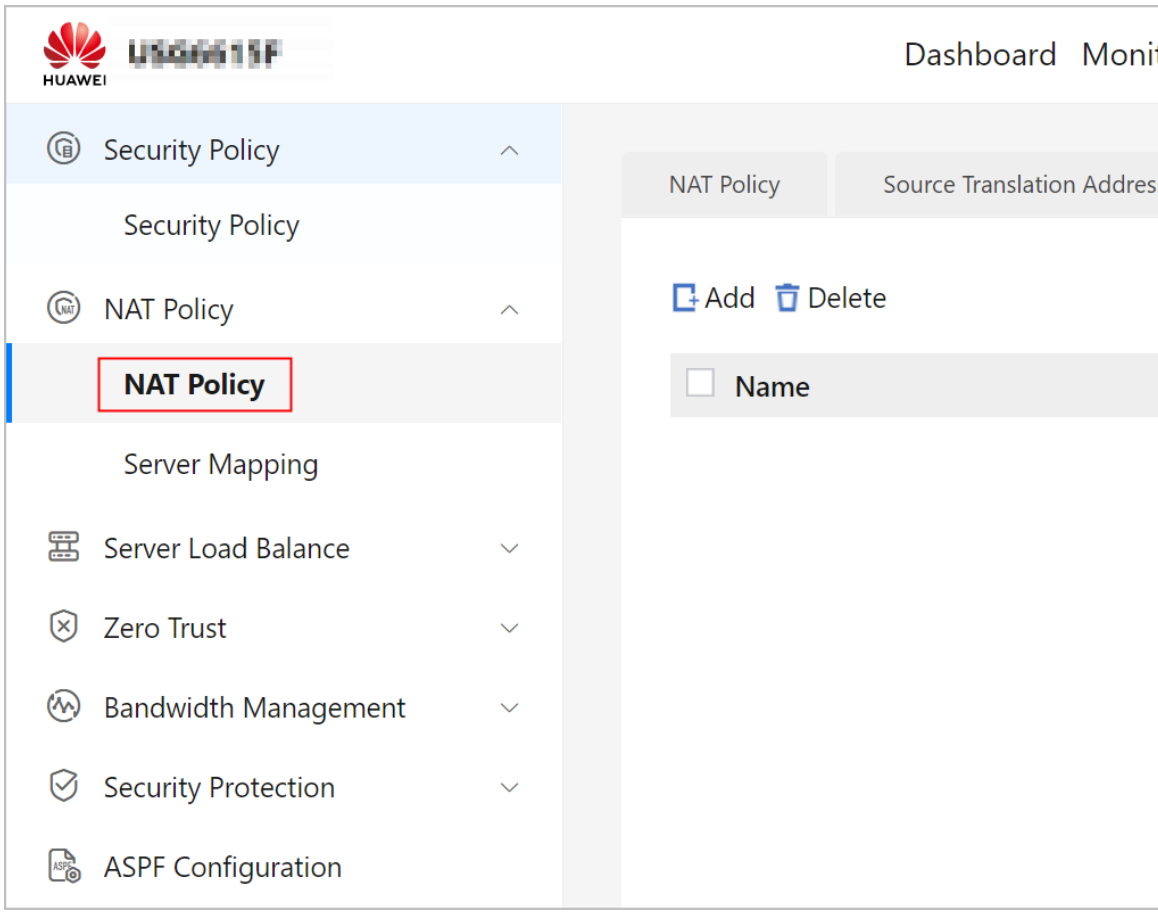
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



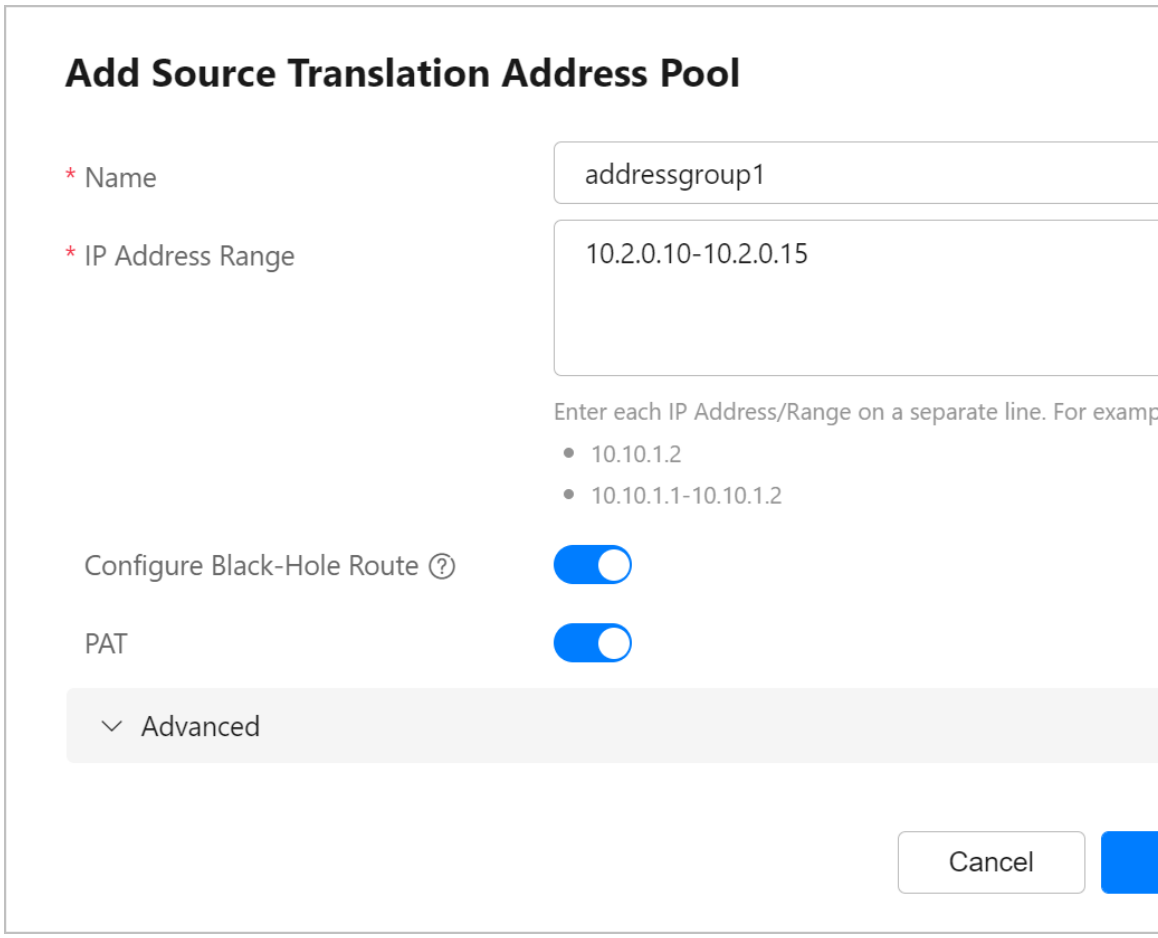
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.
3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Destination Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.

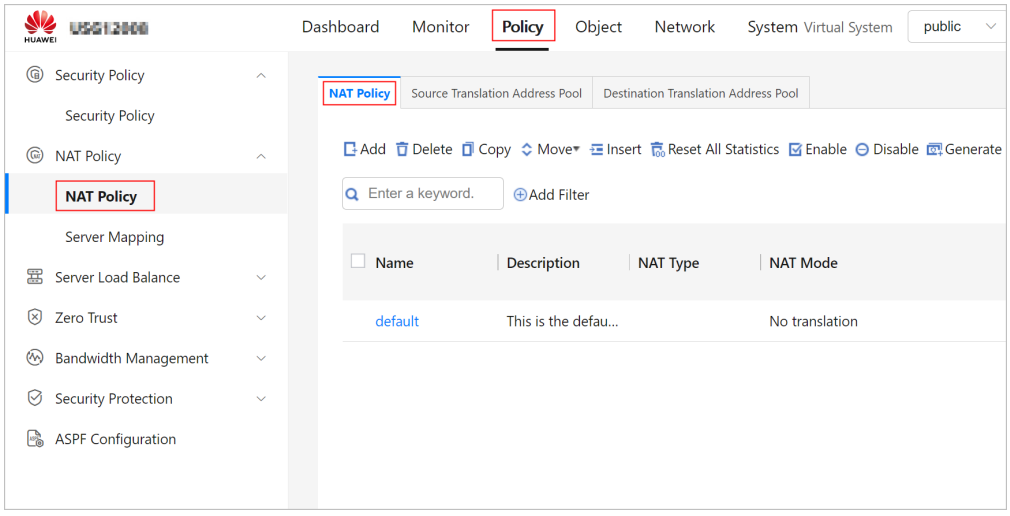


5. In **Destination Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.



6. Click **OK**.
7. Choose **Policy** > **NAT Policy** > **NAT Policy**.



8. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

Add NAT Policy

[Show Overview]

Name: policy_nat1 *

Description:

NAT Type: (•) NAT ( ) NAT64 ( ) NAT66

NAT Mode: Source and destination address translation

Destination Address Translation Mode:
(•) One-to-one mapping between the public and pri
( ) One-to-one mapping between the public port an
( ) One-to-one mapping between the public and pri
( ) One-to-one mapping between the public addres
( ) Randomly translated to an address in the destina

Schedule: any

Original Data Packet

Source Zone: untrust

Source Address: any ×

Destination Address: 1.1.10.10-1.1.10.11 × *

Service: http × ftp ×

Translated Data Packet

Source Address Translated To: (•) Address in the IP address pool ( ) Outbound

Source Translation Address Pool: addressgroup1 *

Destination Address Translation To: addressgroup2 *

Destination Port Translation Mode: (•) No translation ( ) Translation

Note: To ensure that the device can properly forward NAT service traffic, configure a security policy. [Add Se

 Copyright © Huawei Technologies Co., Ltd.

9. Click **OK**.

Step 4 Configure a black-hole route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

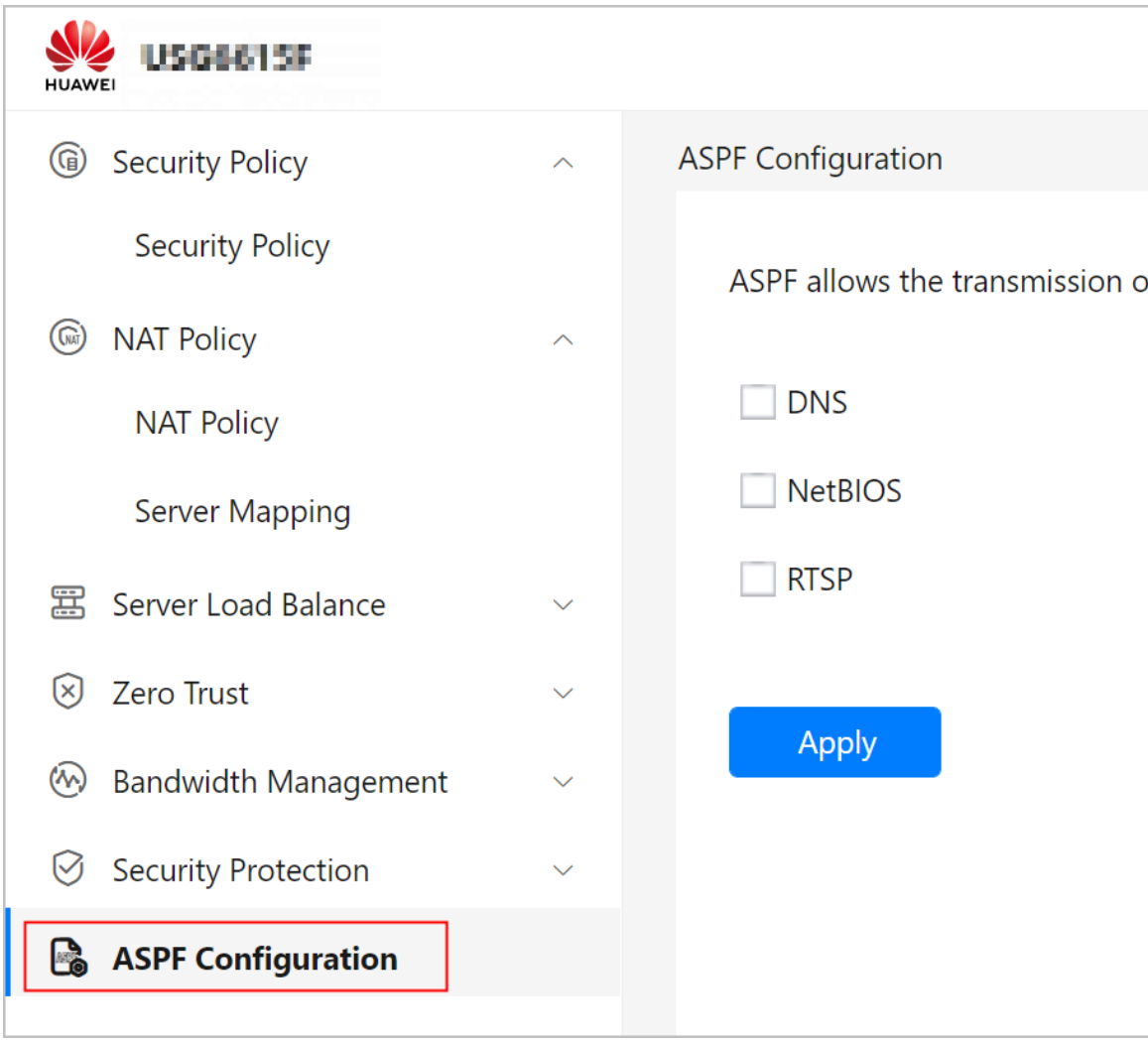
1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a black-hole route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	1.1.10.10/255.255.255.0
Outbound Interface	NULL0

3. Click **OK**.

Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.



2. Select **FTP**.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure a default route on the DeviceA so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 7 Configure a static route to public address (1.1.10.10 and 1.1.10.11) with the next hop being 1.1.1.1 on the router so that traffic destined for the server can be sent to the DeviceA.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 1.1.10.11 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 10.2.0.10 10.2.0.15
#
destination-nat address-group addressgroup2 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 section 10.2.0.7 10.2.0.8
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat
    source-zone untrust
    destination-address range 1.1.10.10 1.1.10.11
    service http
    service ftp
    action source-nat address-group addressgroup1
    action destination-nat static address-to-address address-group addressgroup2
#
return
```

15.4.2 CLI: Example for Configuring Bidirectional NAT (Source NAT + Static Destination NAT) for Internet Users to Access Intranet Servers

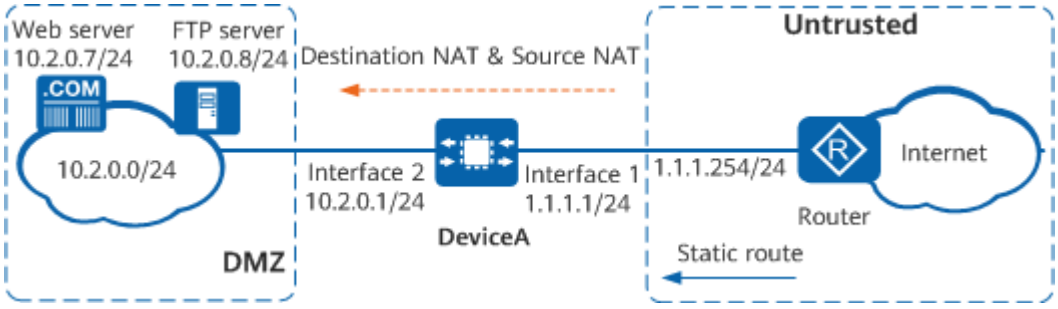
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by the intranet servers to provide services to Internet users. A source NAT policy is also required to enable intranet servers to send response packets to DeviceA, removing the need to configure return routes for intranet servers. **Figure 15-37** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-37 Network diagram of bidirectional NAT (source NAT + static destination NAT) allowing Internet users to access intranet servers

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Source NAT address pool	10.2.0.10 to 10.2.0.15	-
Destination NAT address pool	10.2.0.7 to 10.2.0.8	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA so that it can forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure a destination NAT policy to translate the destination addresses of packets sent from Internet users to intranet servers into addresses in the destination NAT address pool.
4. Configure a source NAT policy to translate the source addresses of packets sent from Internet users to intranet servers into addresses in the source NAT address pool.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure static routes to the public addresses of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a source NAT address pool.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 10.2.0.10 10.2.0.15
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup2
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.7 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

Step 5 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-address range 1.1.10.10 1.1.10.11
[DeviceA-policy-nat-rule-policy_nat1] service http
[DeviceA-policy-nat-rule-policy_nat1] service ftp
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static address-to-address address-group
addressgroup2
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 6 Configure blackhole routes to the public addresses of intranet servers to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
[DeviceA] ip route-static 1.1.10.11 255.255.255.255 NULL0
```

Step 7 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 8 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

 Copyright © Huawei Technologies Co., Ltd.

Step 9 On the ISP router, configure static routes to the public addresses (1.1.10.10 and 1.1.10.11) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet servers to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 http  VPN:public --> public  1.1.1.9:2474[10.2.0.11:2674]-->1.1.10.10:8080[10.2.0.7:80]
 tcp  VPN:public --> public  1.1.1.25:3685[10.2.0.12:3625]-->1.1.10.11:9748[10.2.0.8:8542]
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
 ip route-static 1.1.10.11 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 10.2.0.10 10.2.0.15
#
destination-nat address-group addressgroup2 0
 section 10.2.0.7 10.2.0.8
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone untrust
 destination-address range 1.1.10.10 1.1.10.11
 service http
 service ftp
 action source-nat address-group addressgroup1
 action destination-nat static address-to-address address-group addressgroup2
#
return
```

15.4.3 Web: Example for Configuring Intranet Users to Access the Public Addresses of Intranet Servers (Source NAT+Static Destination NAT)

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the two FTP servers on the enterprise's private network can provide services to Internet usersA. PC D in the same network segment and security zone as the two servers also requires access the intranet servers using a public address; therefore, source NAT also needs to be configured on DeviceA.

In addition to the public address of the WAN interface on DeviceA, the enterprise has obtained the following public addresses from the ISP:

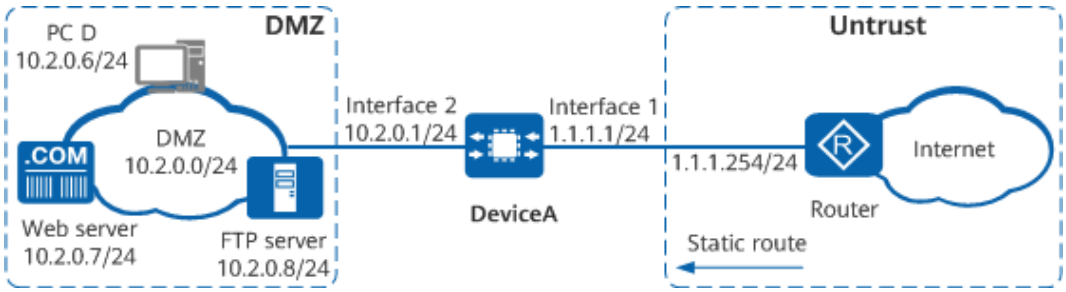
- 1.1.10.10: used by intranet servers to provide services
- 1.1.10.11: used as the post-NAT address of PC D's private address

Figure 15-38 shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-38 Network diagram of source NAT and static destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Source NAT address pool	1.1.10.11	-
Destination NAT address pool	10.2.0.7 to 10.2.0.8	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users to access intranet servers.
3. Configure a source NAT policy to allow PC D to access intranet servers using a public address.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

 Copyright © Huawei Technologies Co., Ltd.

b. Click **OK**.

Step 2 Configure a security policy for traffic between intranet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

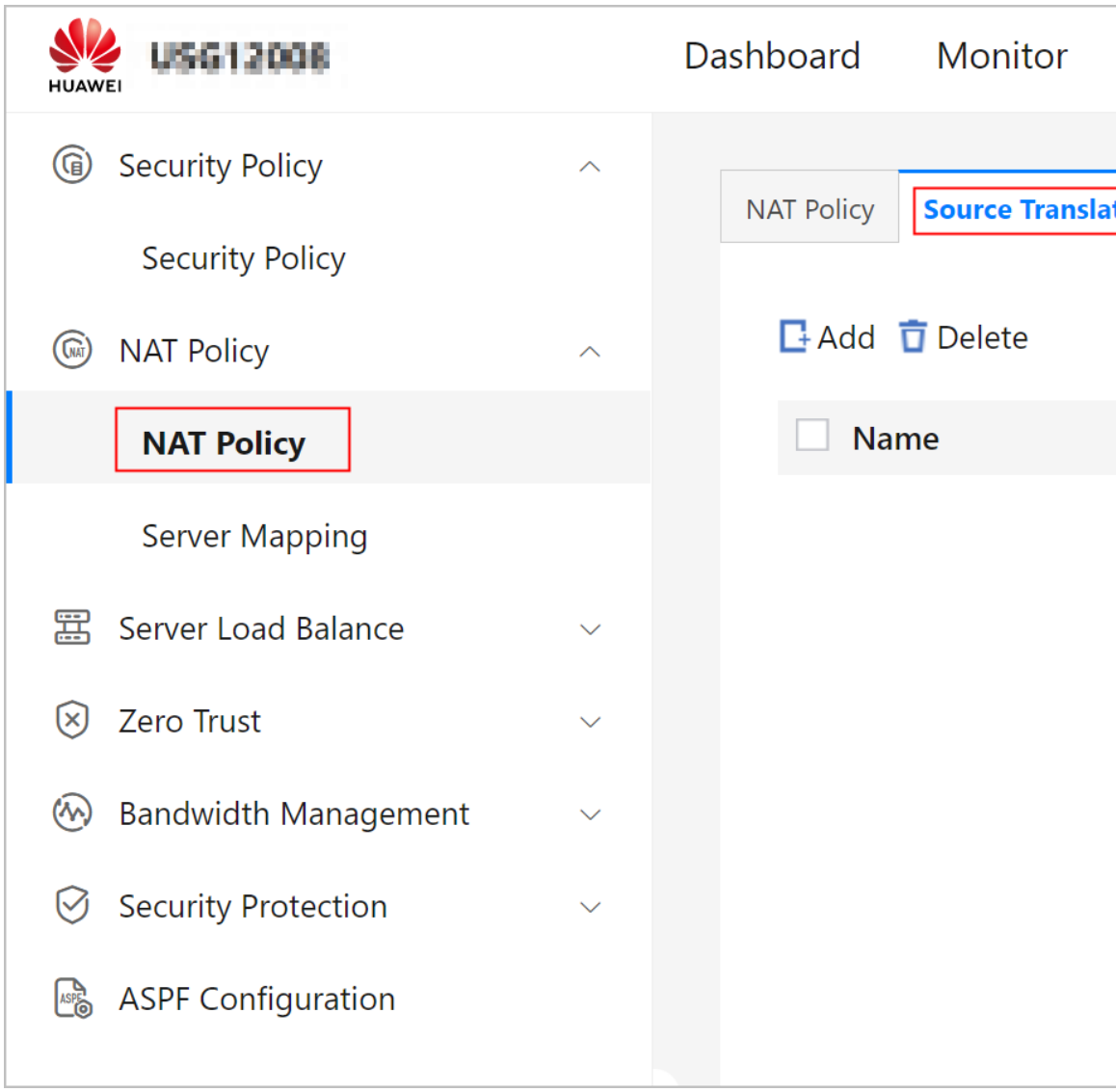
Name	policy1
Source Zone	dmz
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure NAT address pools and NAT policies.

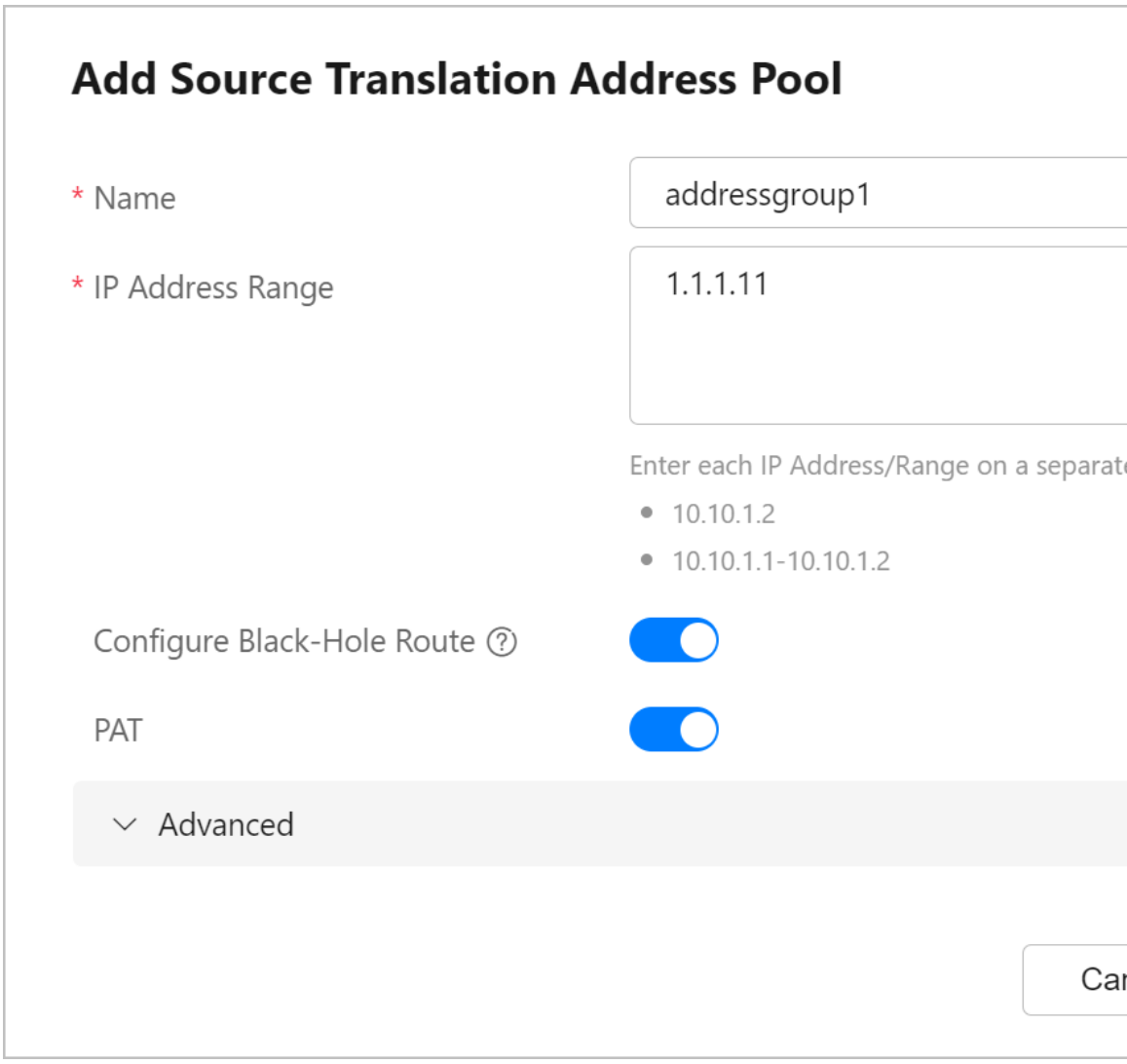
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



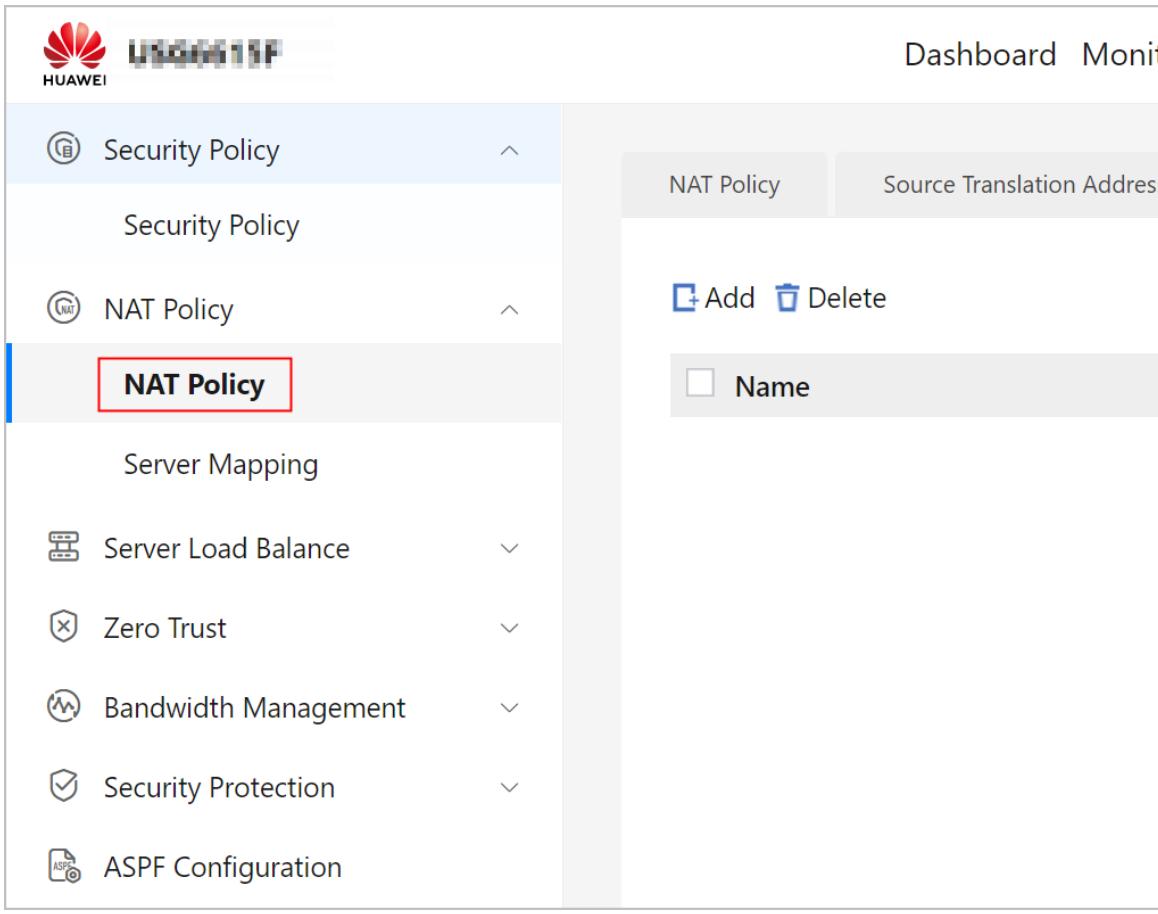
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

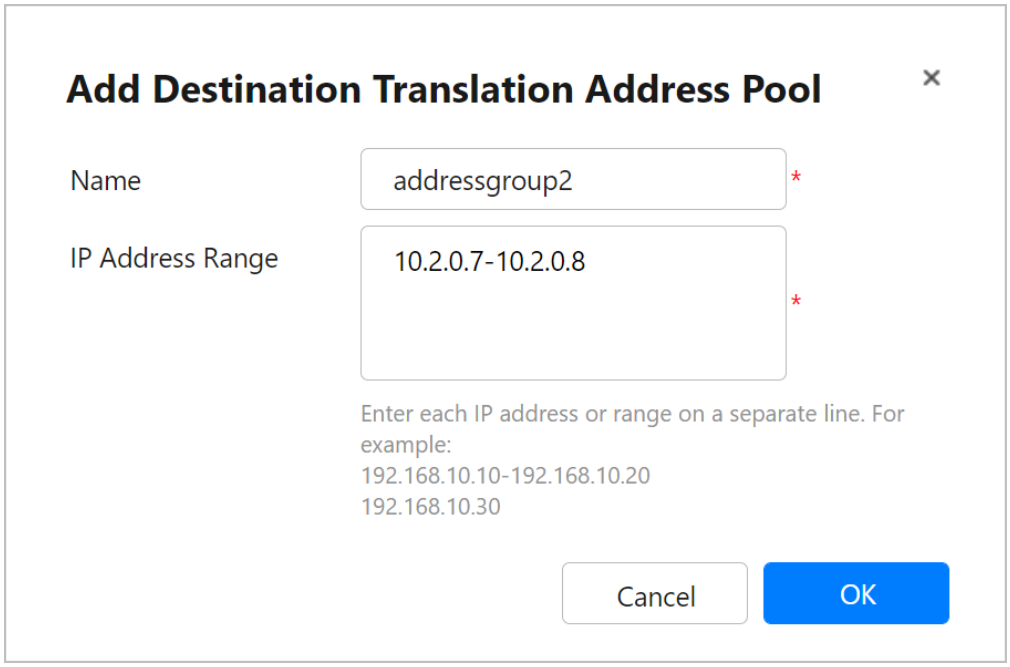


3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Destination Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.

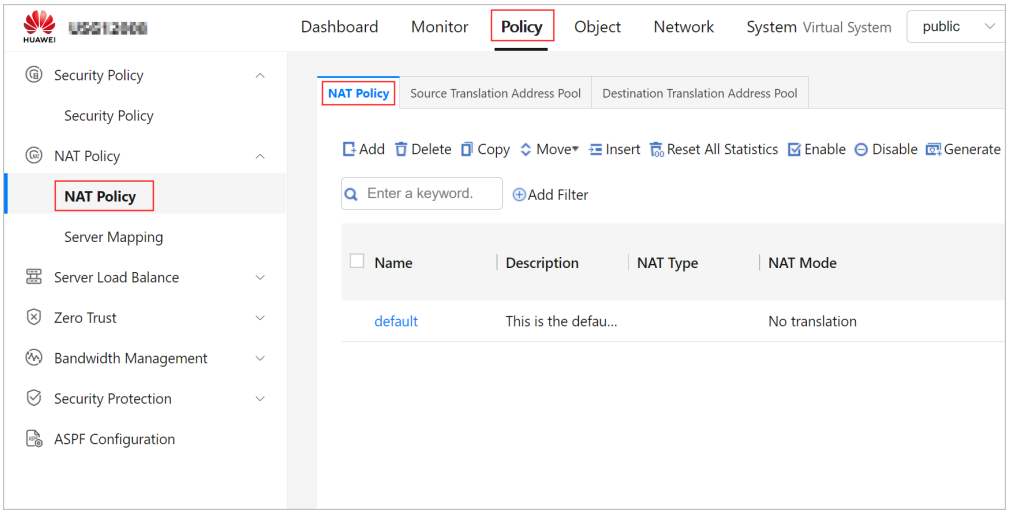


5. In **Destination Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.



6. Click **OK**.
7. Choose **Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.



8. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

Add NAT Policy

[Show Overview]

Name: policy_nat1 *

Description:

NAT Type: (•) NAT ( ) NAT64 ( ) NAT66

NAT Mode: Source and destination address translation

Destination Address Translation Mode:
( ) One-to-one mapping between the public and pr
(•) One-to-one mapping between the public port ar
( ) One-to-one mapping between the public and pr
( ) One-to-one mapping between the public addres
( ) Randomly translated to an address in the destina

Schedule: any

Original Data Packet

Source Zone: dmz

Source Address: 10.2.0.6/24 ×

Destination Address: 1.1.10.10/32 × *

Service: TCP:src-port:0-65535;dst-port:... × *

Translated Data Packet

Source Address Translated To: (•) Address in the IP address pool ( ) Outbound

Source Translation Address Pool: addressgroup1 *

Destination Address Translation To: addressgroup2 *

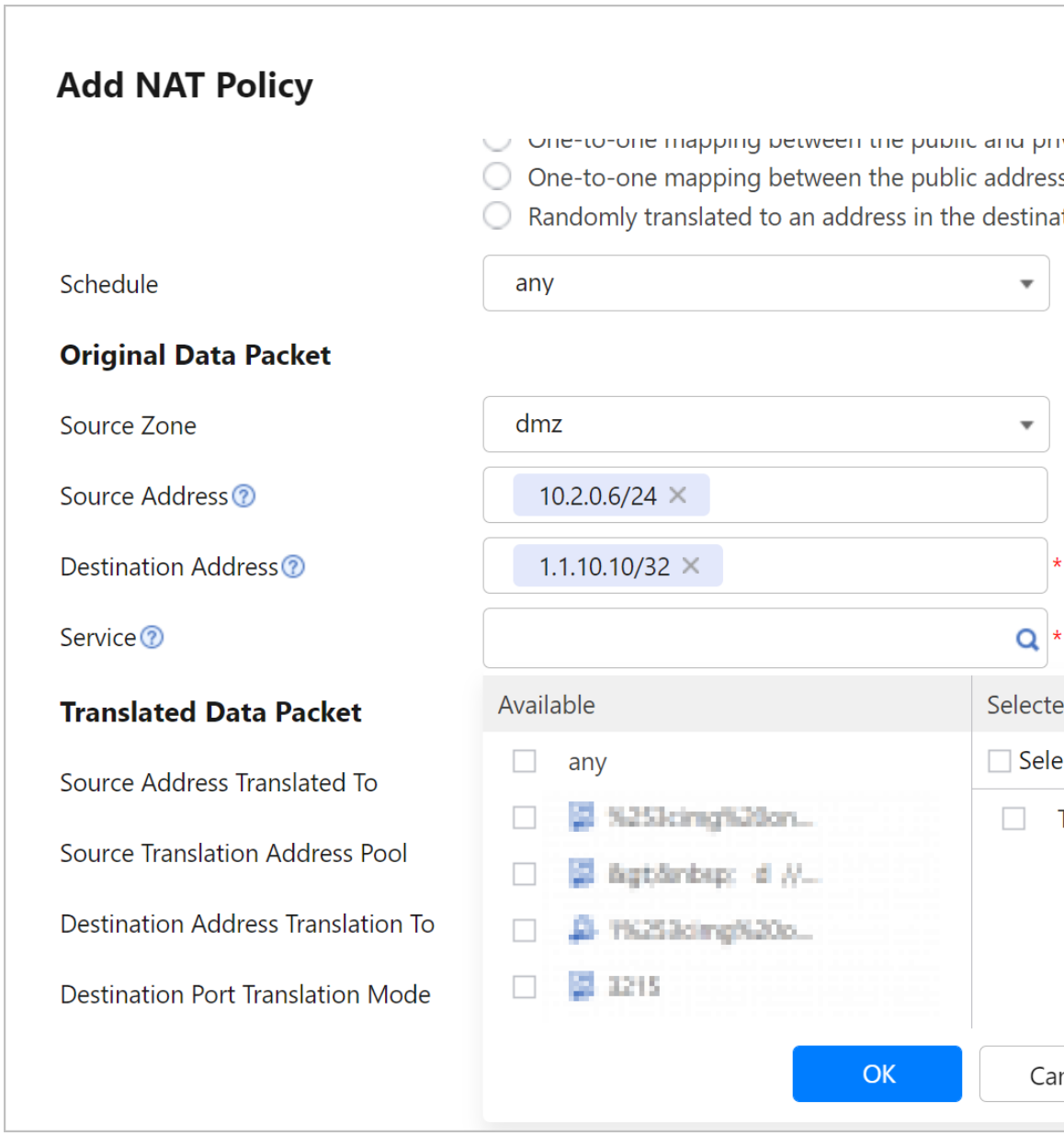
Destination Port Translation Mode: ( ) No translation (•) Translatio

Destination Port Translated To: Enter an integer ranging from 1 to 65535. *

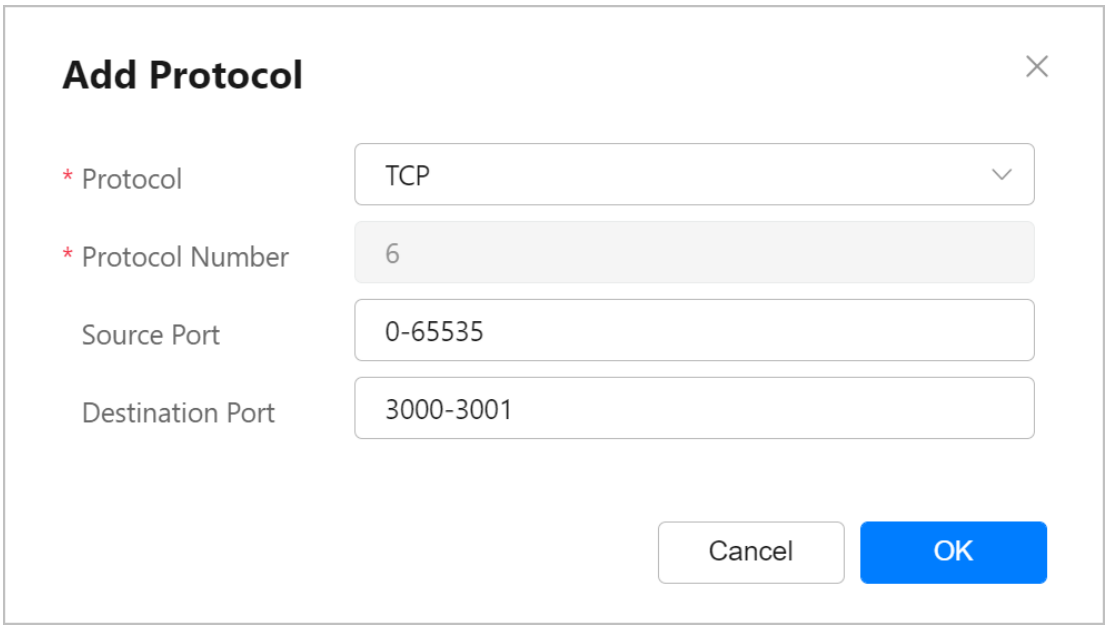
Note: To ensure that the device can properly forward NAT service traffic, configure a security policy. [Add Se

 Copyright © Huawei Technologies Co., Ltd.

9. When configuring **Service**, right-click the input box in the column where **Service** resides and choose **Add** > **Add Protocol or Protocol Number** from the shortcut menu.



10. Set a protocol number as follows:



11. Click **OK**.

Step 4 Configure a black-hole route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a black-hole route based on the following parameter values.

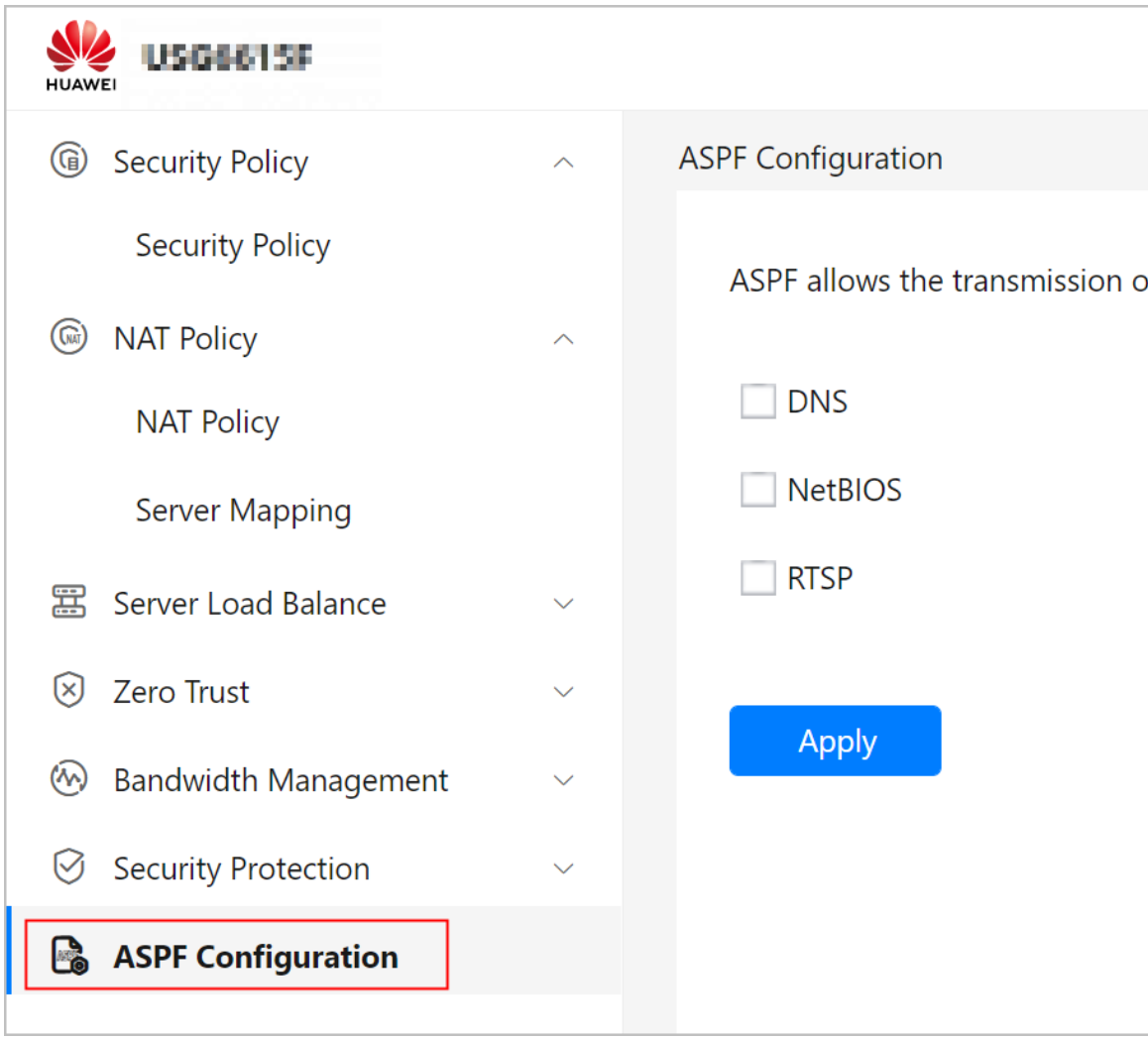
Protocol	IPv4
Destination Address/Mask	1.1.10.10/255.255.255.0
Next Hop	NULL0

3. Click **OK**.

Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.



2. Select **FTP**.

Step 6 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 7 Configure a static route to public address (1.1.10.10) with the next hop being 1.1.1.1 on the router so that traffic destined for the server can be sent to the DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet users can access intranet servers.
2. When intranet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
 detect ftp
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.10.11 1.1.10.11
#
destination-nat address-group addressgroup2 0
 section 10.2.0.7 10.2.0.8
#
security-policy
  rule name policy1
    source-zone dmz
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone dmz
    source-address 10.2.0.6 24
    destination-address 1.1.10.10 32
    service protocol tcp destination-port  3000 to 3001
    action source-nat address-group addressgroup1
    action destination-nat static port-to-address address-group addressgroup2 21
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.4.4 CLI: Example for Configuring Intranet Users to Access Intranet Servers Using Public Addresses (Source NAT + Static Destination NAT)

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. PC D in the same network segment and security zone as the two servers also requires access the intranet servers using a public address; therefore, source NAT also needs to be configured on DeviceA.

In addition to the public address of the WAN interface on DeviceA, the enterprise has obtained the following public addresses from the ISP:

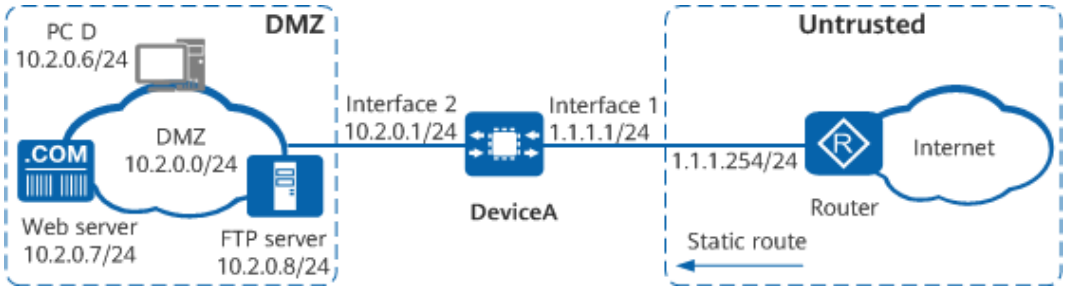
- 1.1.10.10: used by intranet servers to provide services
- 1.1.10.11: used as the post-NAT address of PC D's private address

Figure 15-39 shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-39 Network diagram of source NAT and static destination NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Source NAT address pool	1.1.10.11	-
Destination NAT address pool	10.2.0.7 to 10.2.0.8	-

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow intranet users to access intranet servers.
3. Configure a source NAT policy to allow PC D to access intranet servers using a public address.
4. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
5. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy to allow intranet users to access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone dmz
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a source NAT address pool.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 1.1.10.11 1.1.10.11
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup2
[DeviceA-dnat-address-group-addressgroup2] section 10.2.0.7 10.2.0.8
[DeviceA-dnat-address-group-addressgroup2] quit
```

Step 5 Configure a source NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone dmz
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.2.0.6 24
[DeviceA-policy-nat-rule-policy_nat1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy_nat1] service protocol tcp destination-port 3000 to 3001
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat static port-to-address address-group addressgroup2 21
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 6 Configure a blackhole route to the public address of intranet servers to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
```

Step 7 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] detect ftp
[DeviceA-zone-dmz] quit
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 8 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 9 On the ISP router, configure a static route to the public address (1.1.10.10) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet servers to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that PC D can access intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
```

 Copyright © Huawei Technologies Co., Ltd.

```
tcp  VPN:public --> public  10.2.0.6:2474[1.1.10.11:2674]-->1.1.10.10:3000[10.2.0.7:21]
tcp  VPN:public --> public  10.2.0.6:3685[1.1.10.11:3625]-->1.1.10.10:3001[10.2.0.8:21]
```

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
 detect ftp
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.10.11 1.1.10.11
#
destination-nat address-group addressgroup2 0
 section 10.2.0.7 10.2.0.8
#
security-policy
 rule name policy1
  source-zone dmz
  destination-zone dmz
  destination-address 10.2.0.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone dmz
  source-address 10.2.0.6 mask 255.255.255.0
  destination-address 1.1.10.10 mask 255.255.255.255
  service protocol tcp destination-port 3000 to 3001
  action source-nat address-group addressgroup1
  action destination-nat static port-to-address address-group addressgroup2 21
#
return
```

15.4.5 CLI: Example for Configuring Bidirectional NAT (Source NAT + Dynamic Destination NAT) for Internet Users to Access Intranet Servers

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Dynamic destination NAT needs to be configured on DeviceA to prevent a large number of Internet users from accessing a specific server. In addition to the public

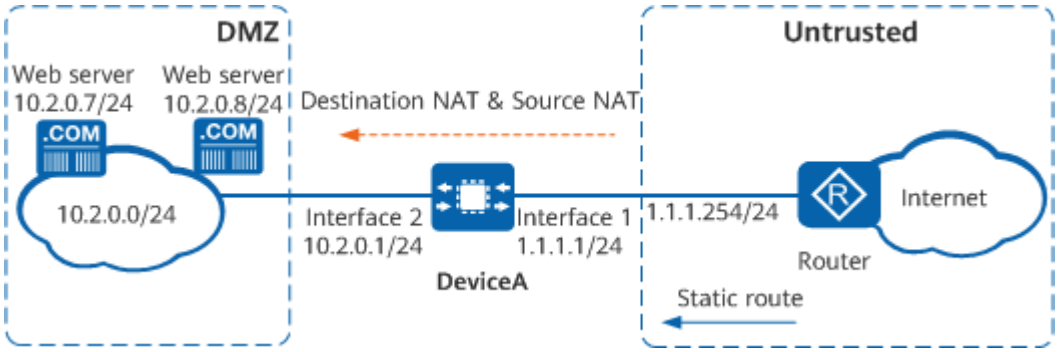
 Copyright © Huawei Technologies Co., Ltd.

IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by intranet servers to provide services to Internet users. A source NAT policy is required so that intranet servers can send response packets to DeviceA, removing the need to configure return routes for intranet servers. **Figure 15-40** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-40 Network diagram of bidirectional NAT (source NAT + dynamic destination NAT) allowing Internet users to access intranet servers

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
Source NAT address pool	10.10.10.10 to 10.10.10.15	-
Destination NAT address pool	10.2.0.7 to 10.2.0.8	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure a destination NAT policy to translate the destination addresses of packets sent from Internet users to intranet servers into addresses in the destination NAT address pool.
4. Configure a source NAT policy to translate the source addresses of packets sent from Internet users to intranet servers into addresses in the source NAT address pool.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a source NAT address pool.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 10.10.10.10 10.10.10.15
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a destination NAT address pool.

```
[DeviceA] destination-nat address-group addressgroup2
[DeviceA-dnat-address-group-addressgroup1] section 10.2.0.7 10.2.0.8
[DeviceA-dnat-address-group-addressgroup1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-address 1.1.10.10 32
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] action destination-nat address-group addressgroup2
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 6 Configure a blackhole route to the public address of intranet servers to prevent routing loops.

```
[DeviceA] ip route-static 1.1.10.10 255.255.255.255 NULL0
```

Step 7 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 8 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 9 On the ISP router, configure a static route to the public address (1.1.10.10) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet servers to DeviceA.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 http  VPN:public --> public  1.1.1.9:2474[10.10.10.11:2674]-->1.1.10.10:8080[10.2.0.7:80]
 http  VPN:public --> public  1.1.1.25:3685[10.10.10.12:3625]-->1.1.10.10:9748[10.2.0.8:8542]
```

Configuration Scripts

```
#
 sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.10.10 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 10.10.10.10 10.10.10.15
#
destination-nat address-group addressgroup2 0
 section 10.2.0.7 10.2.0.8
#
security-policy
 rule name policy1
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone untrust
  destination-address 1.1.10.10 32
  action source-nat address-group addressgroup1
  action destination-nat address-group addressgroup2
#
return
```

15.5 Bidirectional NAT (Source NAT+NAT Server)

15.5.1 Web: Example for Configuring NAPT and NAT Server for Internet Users to Access Intranet Servers

Networking Requirements

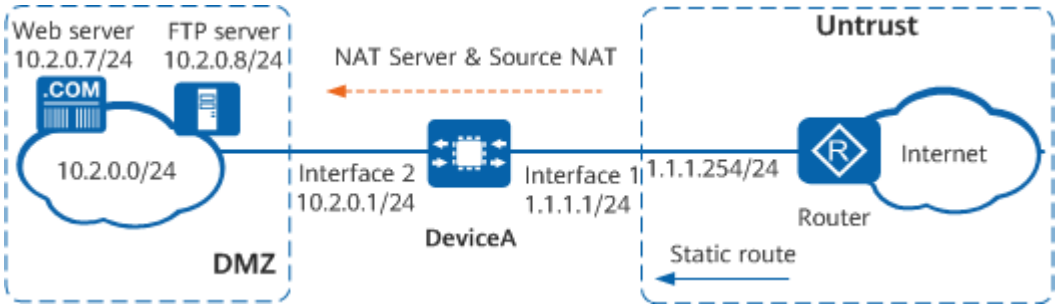
An enterprise has deployed DeviceA as a security gateway at the intranet border. NAT Server needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.1.10) from the ISP, which is used by the intranet servers to provide services to Internet users. A source NAT policy is also required to enable intranet servers to send response packets to DeviceA, removing the need to configure return routes for intranet servers. **Figure 15-41** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-41 Network diagram of NAT Server and source NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
NAT Server	Name: policy_web Public IP address: 1.1.1.10 Private IP address: 10.2.0.7 Public port: 8080 Private port: 80	When Internet users send traffic to 1.1.1.10 through port 8080, DeviceA can forward it to the web server based on this mapping entry. The web server has the private address 10.2.0.7 and private port number 80.
	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic to 1.1.1.10 through port 21, DeviceA can forward it to the FTP server based on this mapping entry. The FTP server has the private address 10.2.0.8 and private port number 21.
NAT address pool	10.2.0.10-10.2.0.15	The addresses in the NAT address pool and the private IP address of the intranet server are in the same network segment.
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure NAT Server by specifying two static mapping entries, that is, one for the web server and one for the FTP server.
4. Configure a source NAT policy to translate the source addresses of packets sent from Internet users to intranet servers into addresses in the NAT address pool.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2and assign the interface to a security zone.
   a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

   b. Click **OK**.

Step 2 Configure a security policy for traffic between Internet users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy1
Source Zone	untrust

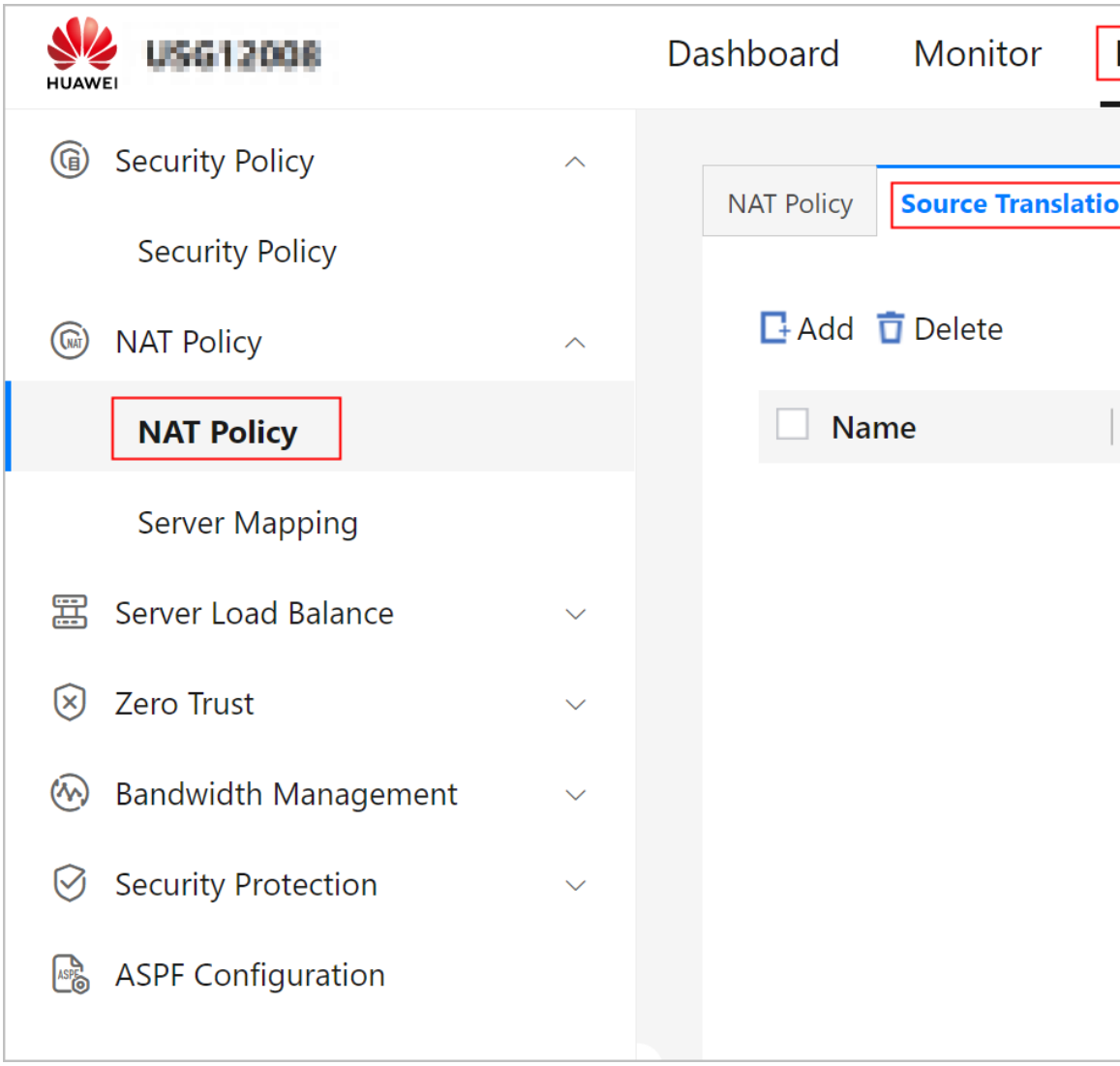
 Copyright © Huawei Technologies Co., Ltd.

Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

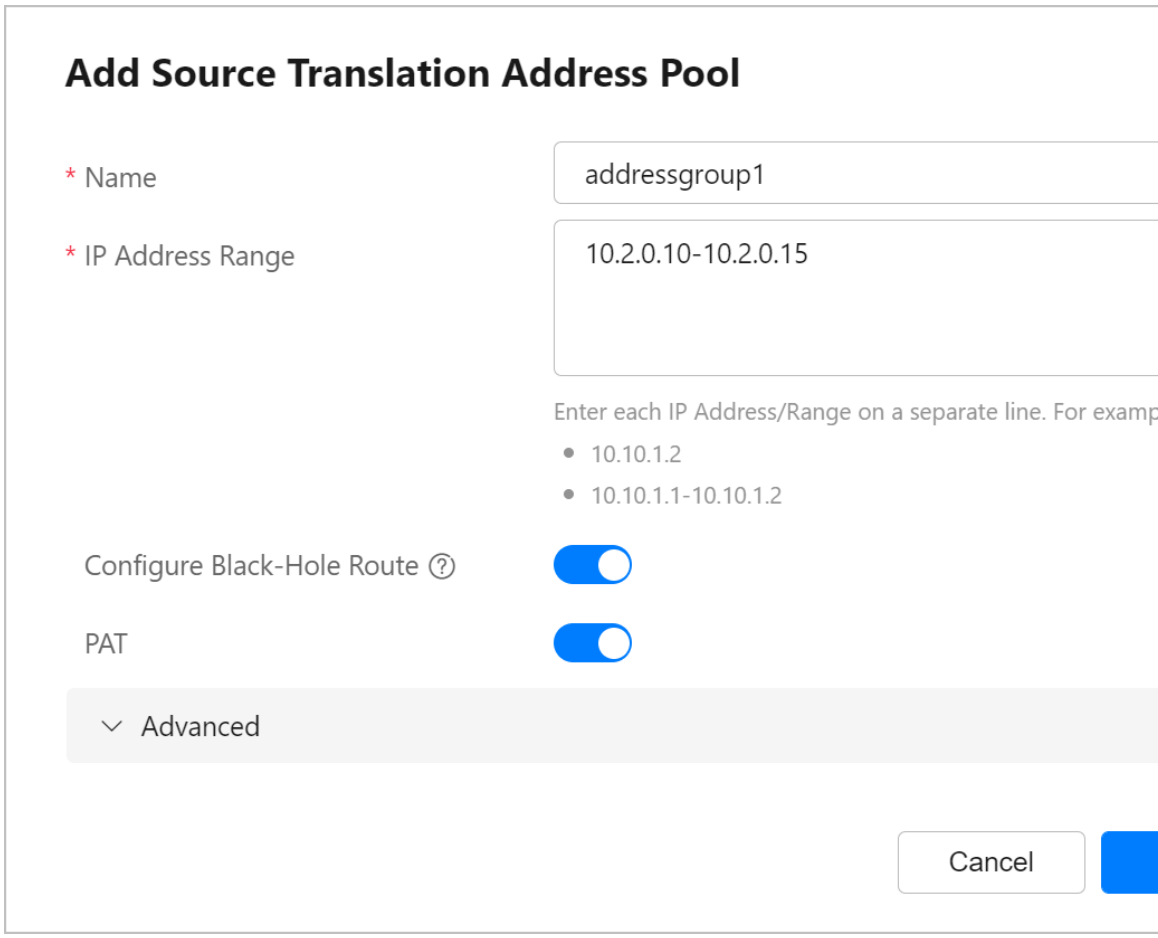
Step 3 Configure a NAT address pool and a NAT policy.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

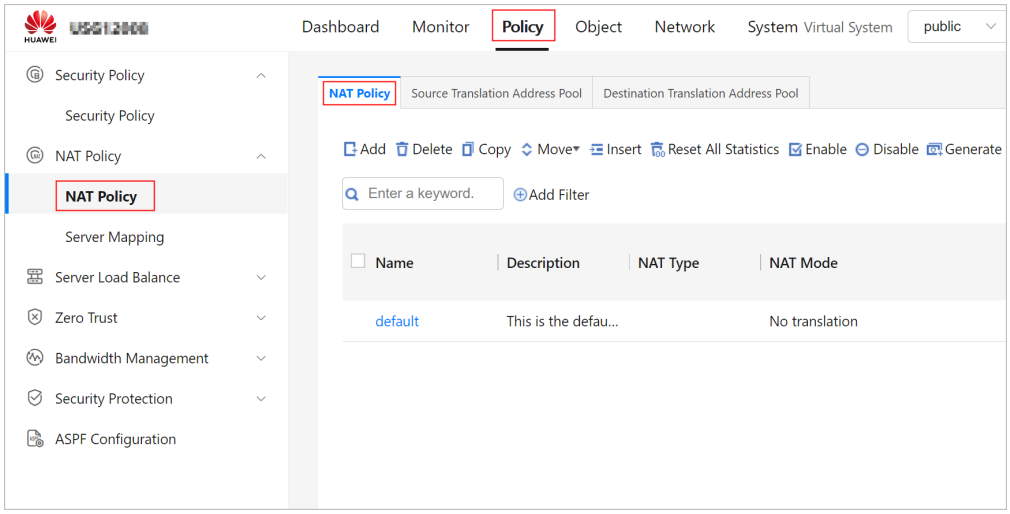


2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy**.

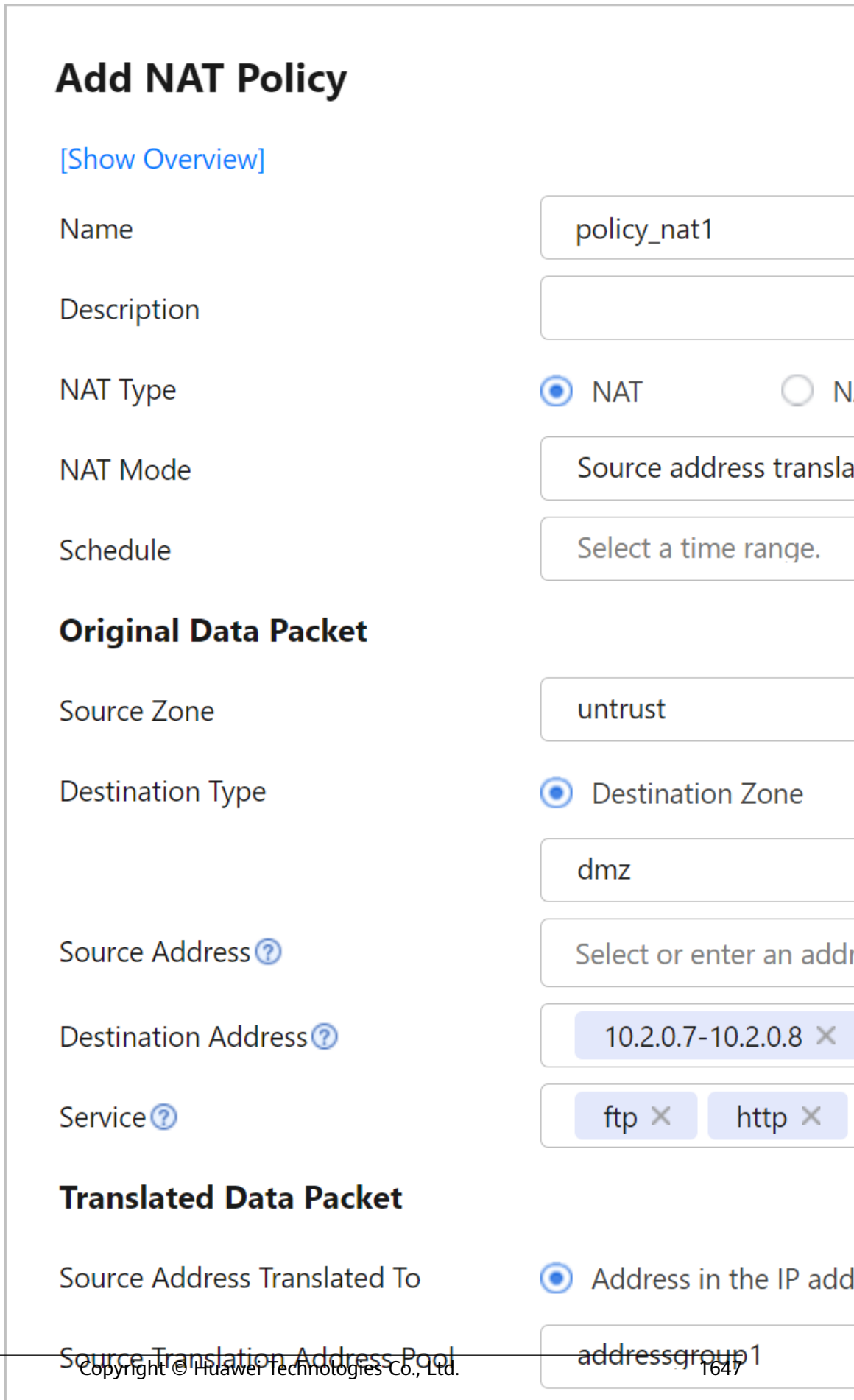


5. In **Source NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

NOTE

The destination address is the private IP address of the intranet server. Because NAT Server is processed before source NAT, the destination address has been translated into the private IP address of the intranet server when source NAT is performed.

 Copyright © Huawei Technologies Co., Ltd.

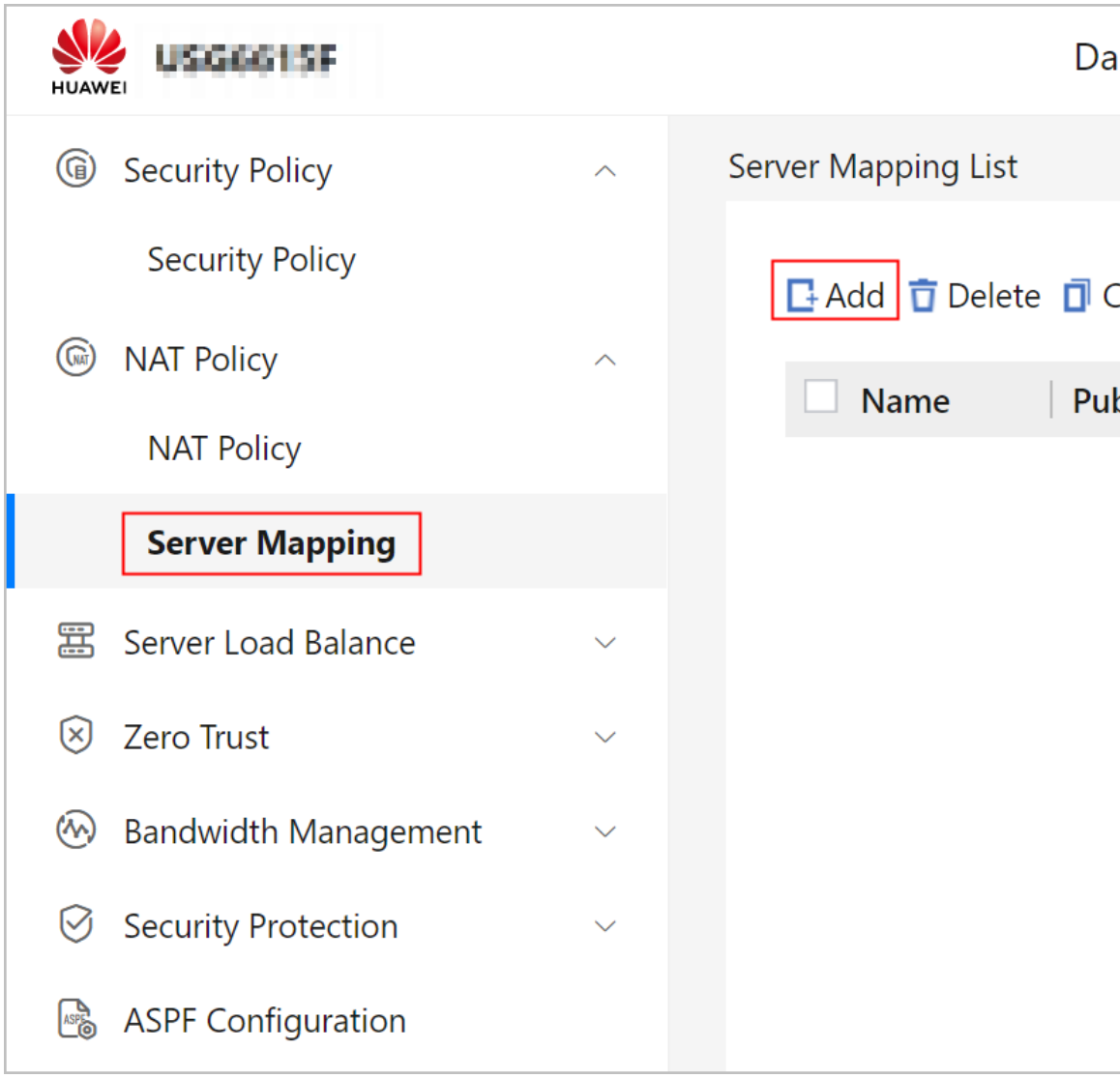


 Copyright © Huawei Technologies Co., Ltd.

6. Click **OK**.

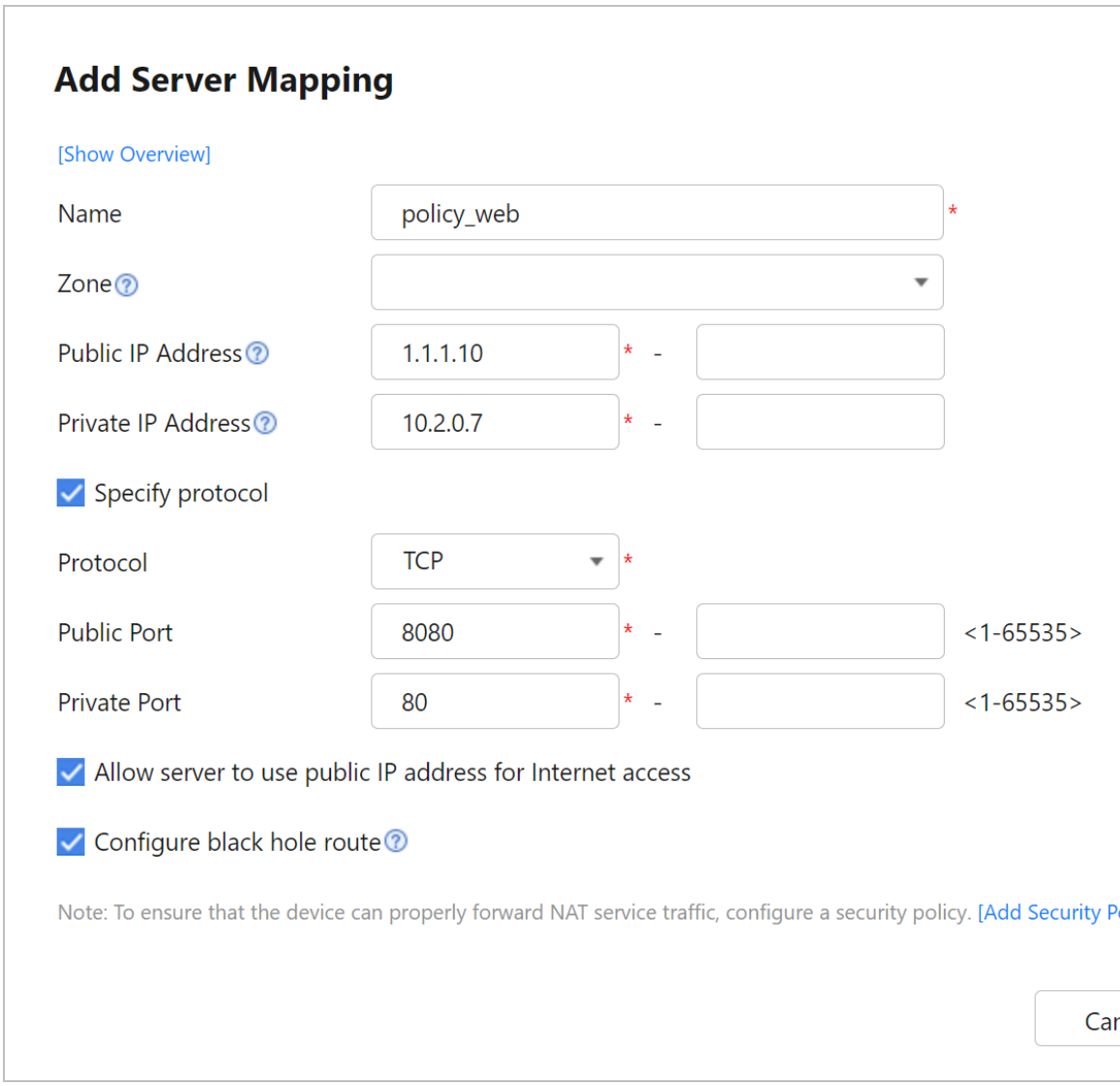
Step 4 Configure NAT Server. Configure two server mapping entries, one for the web server and the other for the FTP server.

1. Choose **Policy** > **NAT Policy** > **Server Mapping**.



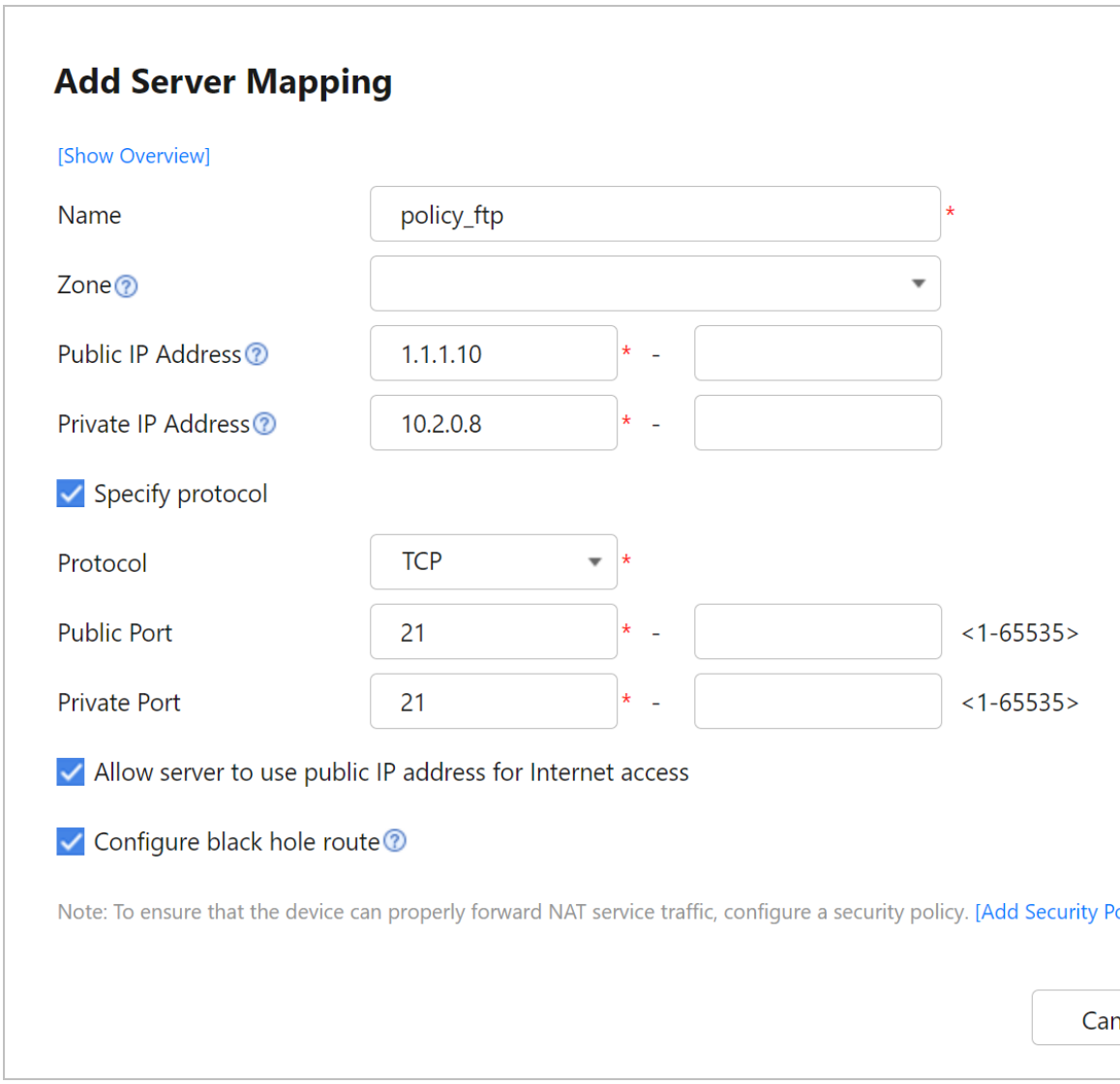
2. Click **Add** and set the following parameters for a server mapping policy named **policy_web** used for directing traffic to the web server.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **OK**.
4. Repeat the preceding substeps and set the following parameters for another server mapping policy named **policy_ftp** used for directing traffic to the FTP server.

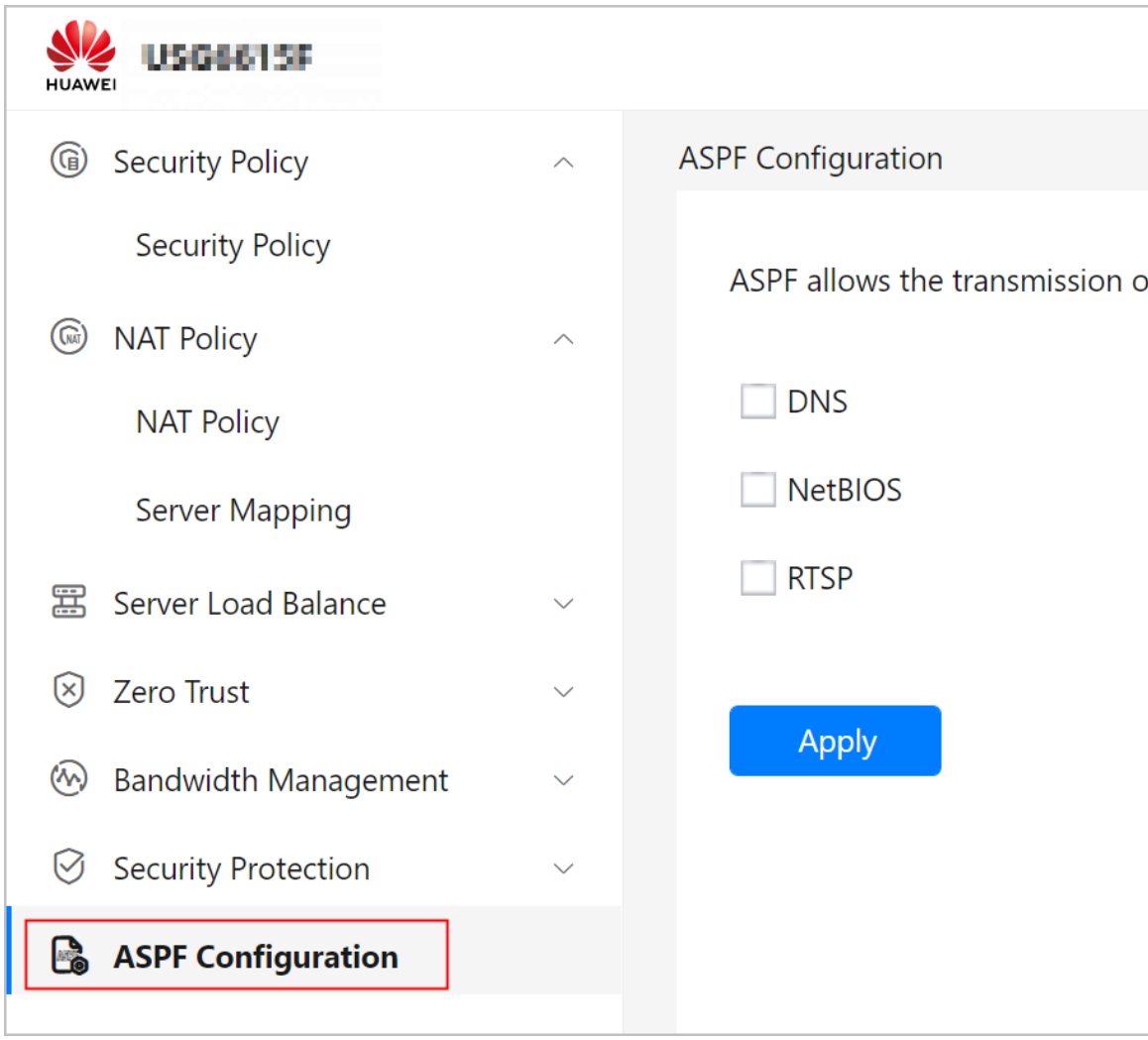
 Copyright © Huawei Technologies Co., Ltd.



Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.



2. Select **FTP**.

Step 6 Configure a default route on the DevceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 7 On the router, configure a static route, in which the destination address is 1.1.1.10 and the next-hop address is 1.1.1.1. The router directs traffic destined for 1.1.1.10 to the DeviceA based on the static route so that the DeviceA can forward the traffic to the intranet server.

 Copyright © Huawei Technologies Co., Ltd.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. When Internet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.1.10 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 10.2.0.10 10.2.0.15
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-zone dmz
    destination-address range 10.2.0.7 10.2.0.8
    service http
    service ftp
    action source-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.5.2 CLI: Example for Configuring NAPT and NAT Server for Internet Users to Access Intranet Servers

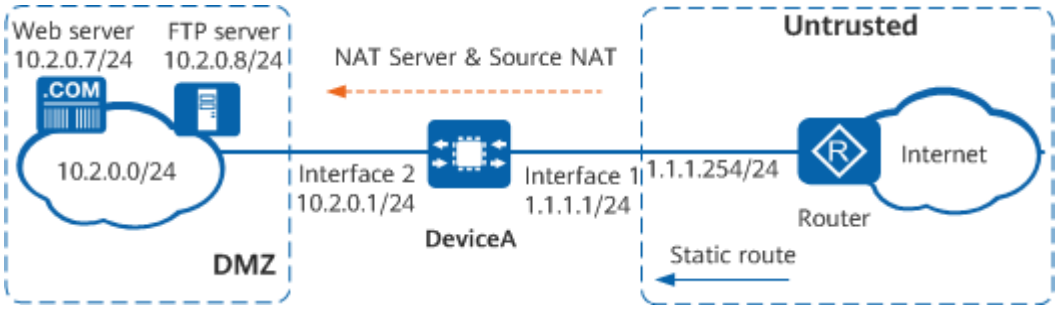
Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. NAT Server needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.1.10) from the ISP, which is used by the intranet servers to provide services to Internet users. To hide the addresses of Internet users, source NAT is required to translate the source addresses of packets sent from them. **Figure 15-42** shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-42 Network diagram of NAT Server and source NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
NAT Server	Name: policy_web Public IP address: 1.1.1.10 Private IP address: 10.2.0.7 Public port: 8080 Private port: 80	When Internet users send traffic to 1.1.1.10 through port 8080, DeviceA can forward it to the web server based on this mapping entry. The web server has the private address 10.2.0.7 and private port number 80.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic to 1.1.1.10 through port 21, DeviceA can forward it to the FTP server based on this mapping entry. The FTP server has the private address 10.2.0.8 and private port number 21.
NAT address pool	10.2.0.10 to 10.2.0.15	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy so that Internet users can access intranet servers.
3. Configure NAT Server by specifying two static mapping entries, that is, one for the web server and one for the FTP server.
4. Configure a source NAT policy to translate the source addresses of packets sent from Internet users to intranet servers into addresses in the NAT address pool.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy so that Internet users can access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool and enable port translation.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 10.2.0.10 10.2.0.15
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a source NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat1] destination-zone dmz
[DeviceA-policy-nat-rule-policy_nat1] destination-address range 10.2.0.7 10.2.0.8
[DeviceA-policy-nat-rule-policy_nat1] service http
[DeviceA-policy-nat-rule-policy_nat1] service ftp
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure NAT Server by specifying two static mapping entries, that is, one for the web server and one for the FTP server.

```
[DeviceA] nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
[DeviceA] nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 7 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

Step 8 On the ISP router, configure a static route to the public address (1.1.1.10) of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet server to DeviceA.

Contact the ISP network administrator to perform this step.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. Verify that Internet users can access intranet servers.
2. Run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 tcp  VPN:public --> public  1.1.1.9:2474[10.2.0.11:2674]-->1.1.1.10:8080[10.2.0.7:80]
 tcp  VPN:public --> public  1.1.1.25:3685[10.2.0.12:3625]-->1.1.1.10:21[10.2.0.8:21]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
 ip route-static 1.1.1.10 255.255.255.255 NULL0
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 10.2.0.10 10.2.0.15
#
security-policy
  rule name policy1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone untrust
    destination-zone dmz
    destination-address range 10.2.0.7 10.2.0.8
    service http
    service ftp
    action source-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.5.3 Web: Example for Configuring Intranet Users to Access the Public Addresses of Intranet Servers

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. NAT Server needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. PC D in the same network segment and security zone as the two servers also requires access the intranet servers using a public address; therefore, source NAT also needs to be configured on DeviceA.

In addition to the public address of the WAN interface on DeviceA, the enterprise has obtained the following public addresses from the ISP:

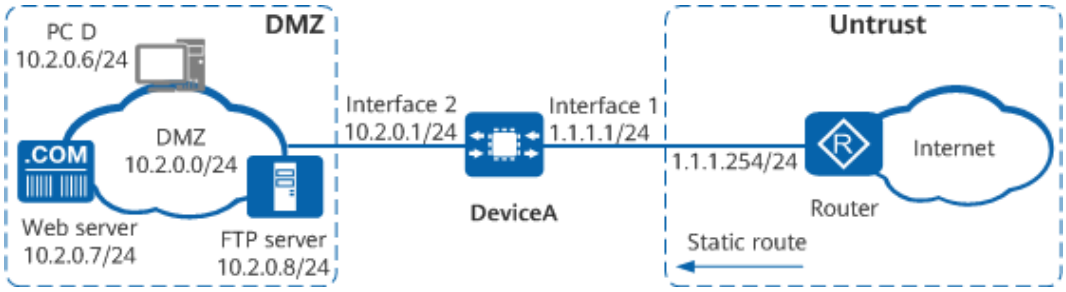
- 1.1.1.10: used by intranet servers to provide services
- 1.1.1.11: used as the post-NAT address of PC D's private address

Figure 15-43 illustrates the networking for a source NAT policy in outbound interface mode. The router is an access gateway on the ISP network.

Figure 15-43 Network diagram of NAT Server and source NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
NAT Server	Name: policy_web Public IP address: 1.1.1.10 Private IP address: 10.2.0.7 Public port: 8080 Private port: 80	When Internet users send traffic to 1.1.1.10 through port 8080, DeviceA can forward it to the web server based on this mapping entry. The web server has the private address 10.2.0.7 and private port number 80.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic to 1.1.1.10 through port 21, DeviceA can forward it to the FTP server based on this mapping entry. The FTP server has the private address 10.2.0.8 and private port number 21.
Source NAT policy	Name: policy_nat1 Private address that can access the Internet: 10.2.0.6 Address in a NAT address pool: 1.1.1.11	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow both intranet and Internet users to access intranet servers.
3. Configure NAT Server by specifying two static mapping entries, that is, one for the web server and one for the FTP server.
4. Configure a source NAT policy to allow PC D to access intranet servers using a public address.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the parameters as follows:

Zone	untrust

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	1.1.1.1/24

c. Click **OK**.

2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.

a. In **Interface List**, click of GE 0/0/2 and set the parameters as follows:

Zone	dmz
IPv4	
IP Address	10.2.0.1/24

b. Click **OK**.

Step 2 Configure a security policy for traffic between users and intranet servers.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

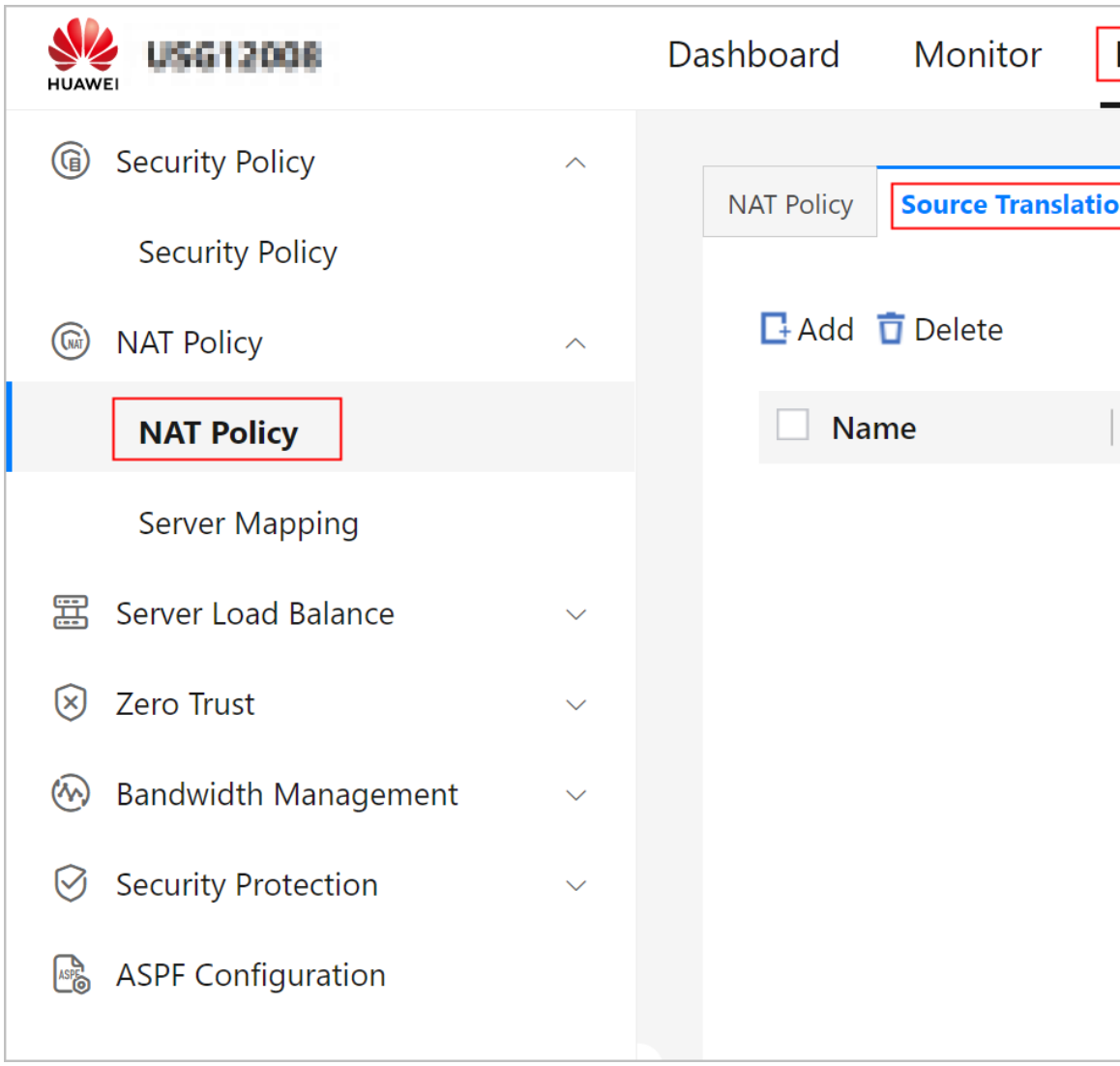
Name	policy1
Source Zone	dmz,untrust
Destination Zone	dmz
Destination Address	10.2.0.0/24
Action	Permit

3. Click **OK**.

Step 3 Configure a NAT address pool and a NAT policy.

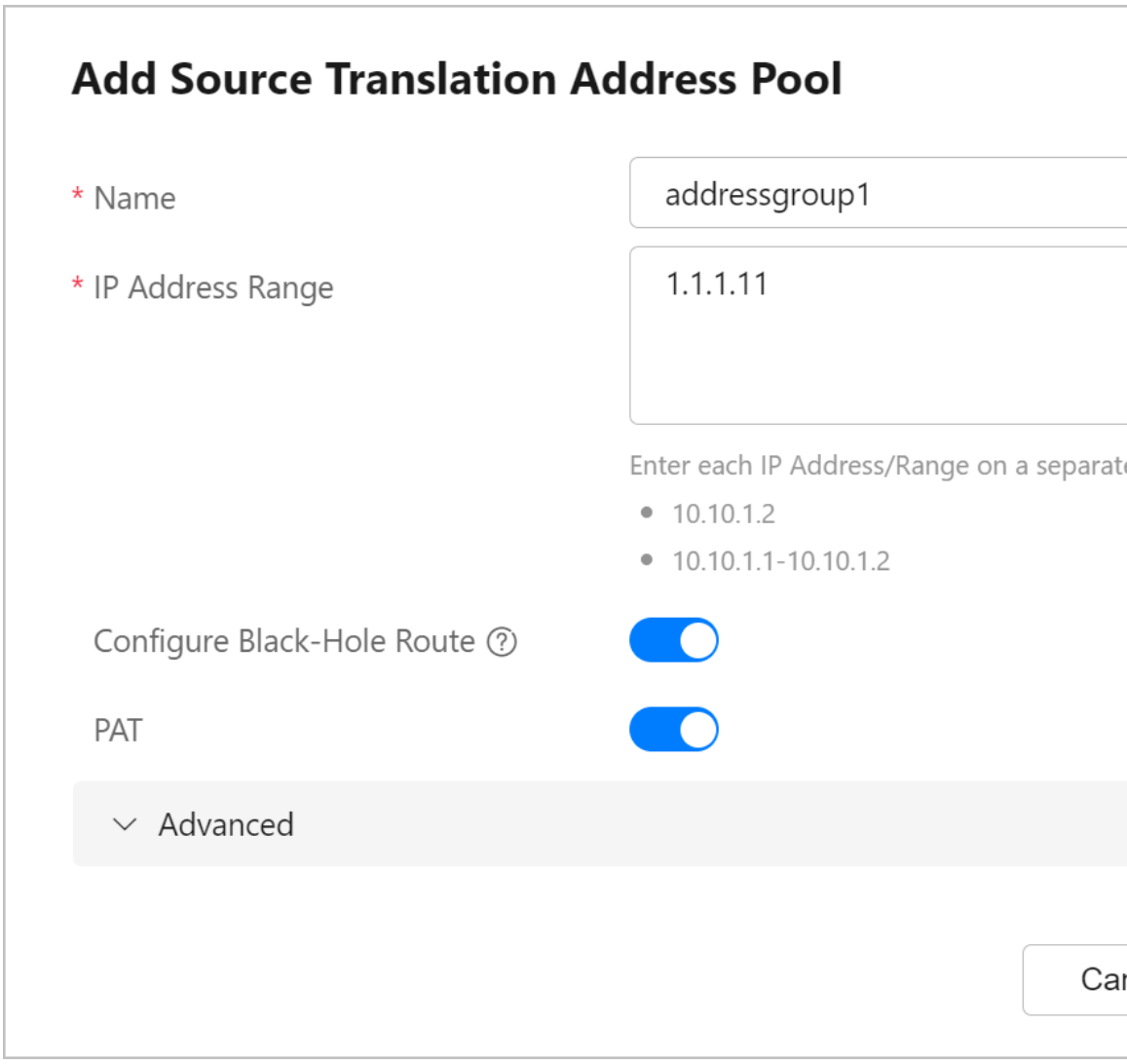
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



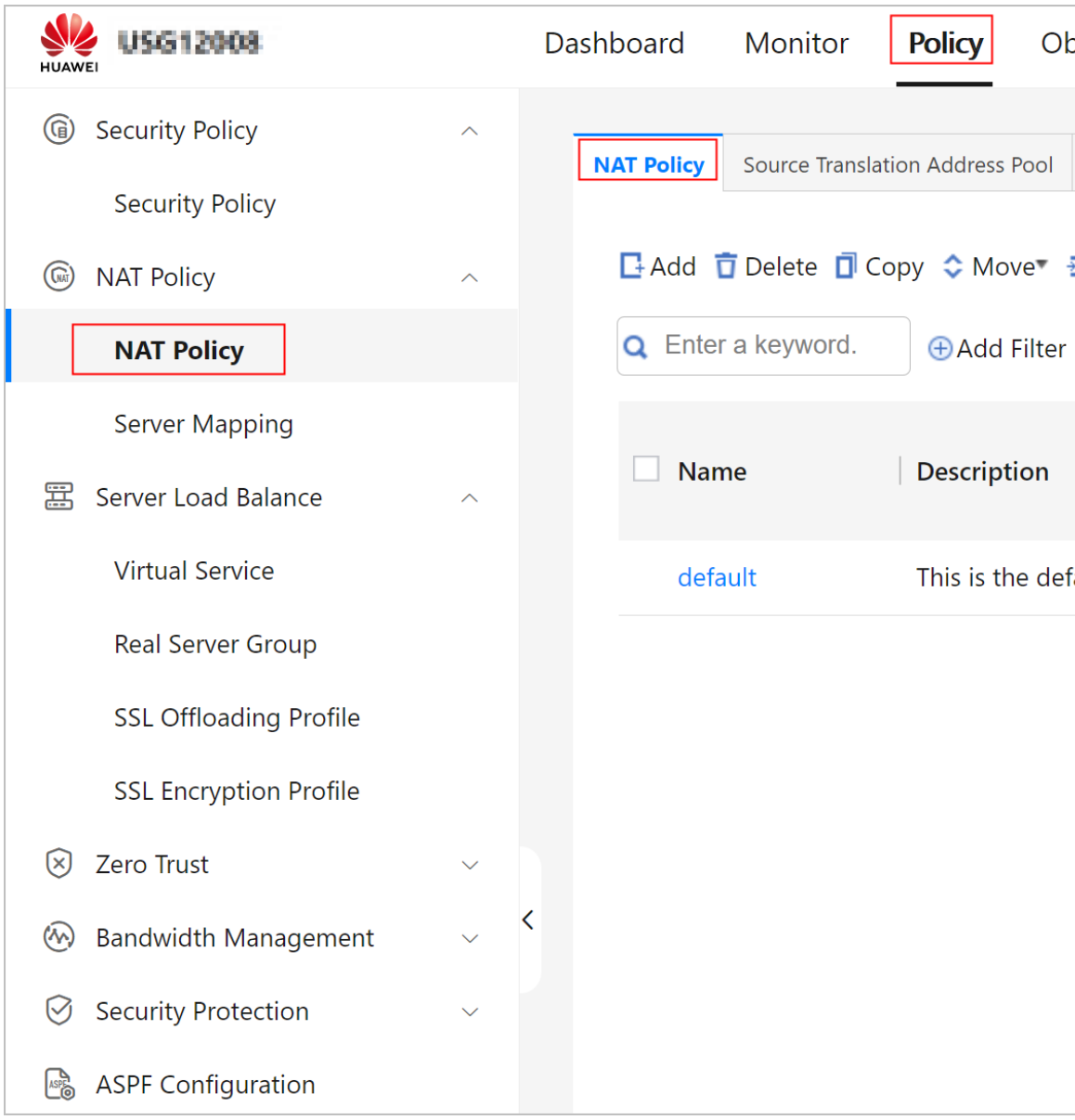
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.



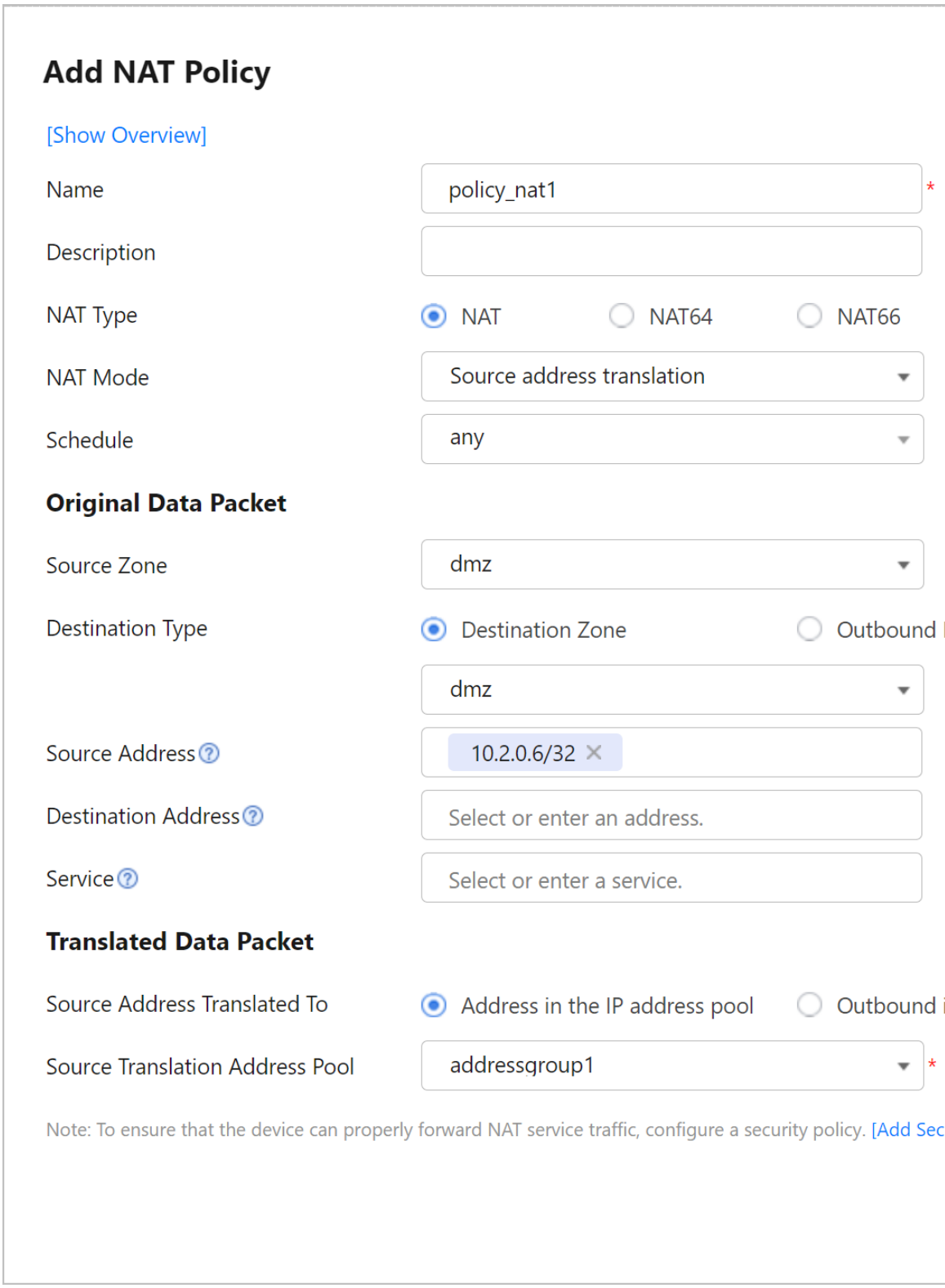
3. Click **OK**.
4. Choose **Policy** > **NAT Policy** > **NAT Policy**.

 Copyright © Huawei Technologies Co., Ltd.



5. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

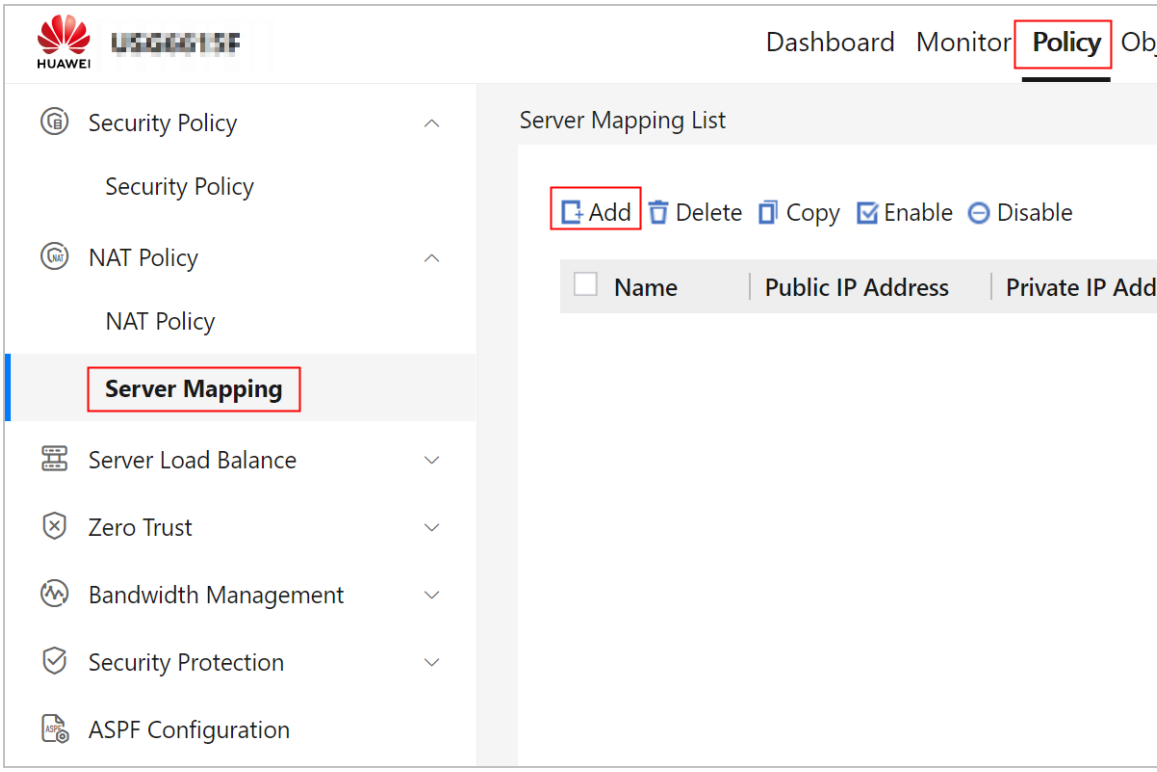


6. Click **OK**.

Step 4 Configure NAT Server. Configure two server mapping entries, one for the web server and the other for the FTP server.

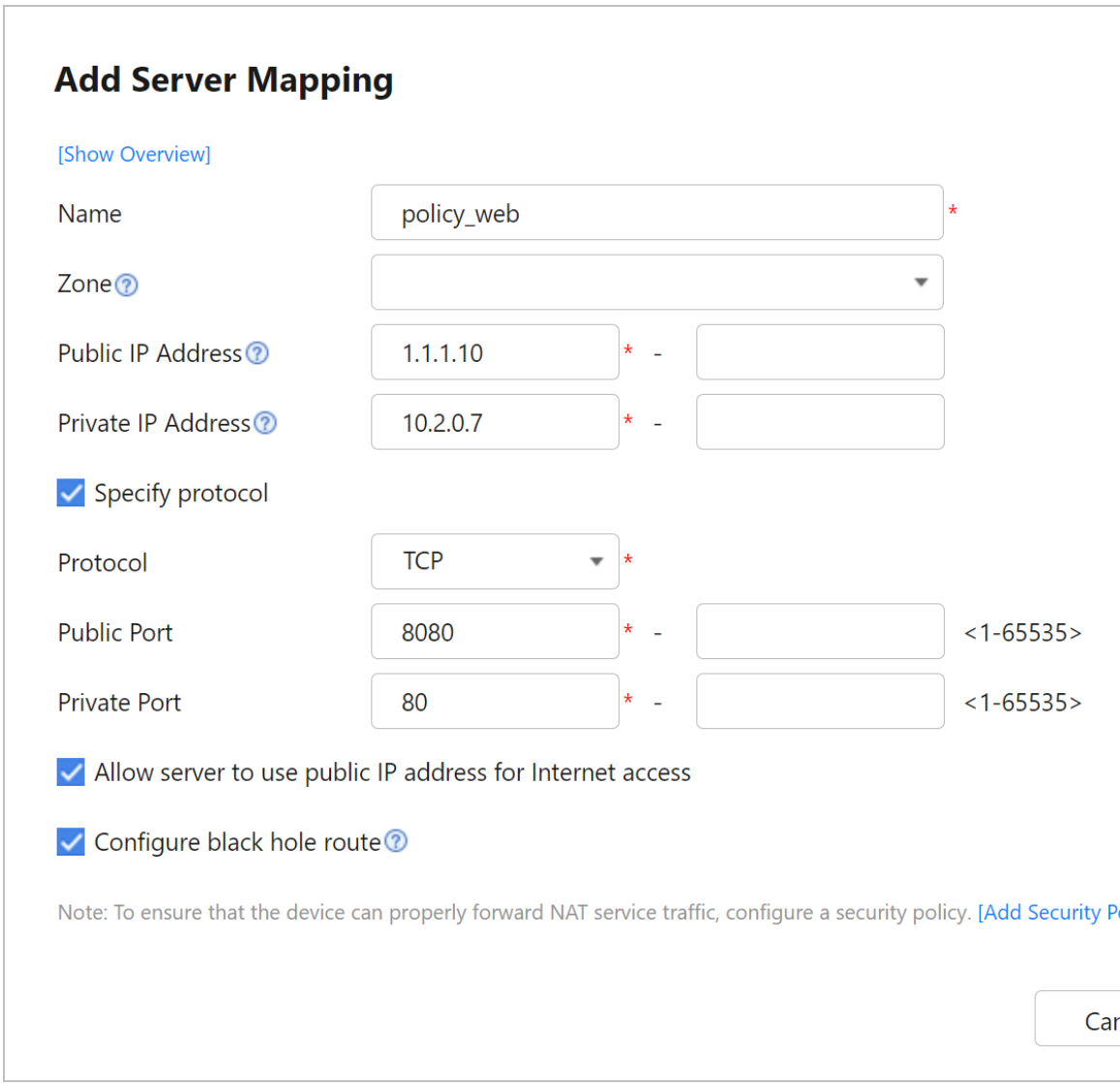
1. Choose **Policy** > **NAT Policy** > **Server Mapping**.

 Copyright © Huawei Technologies Co., Ltd.



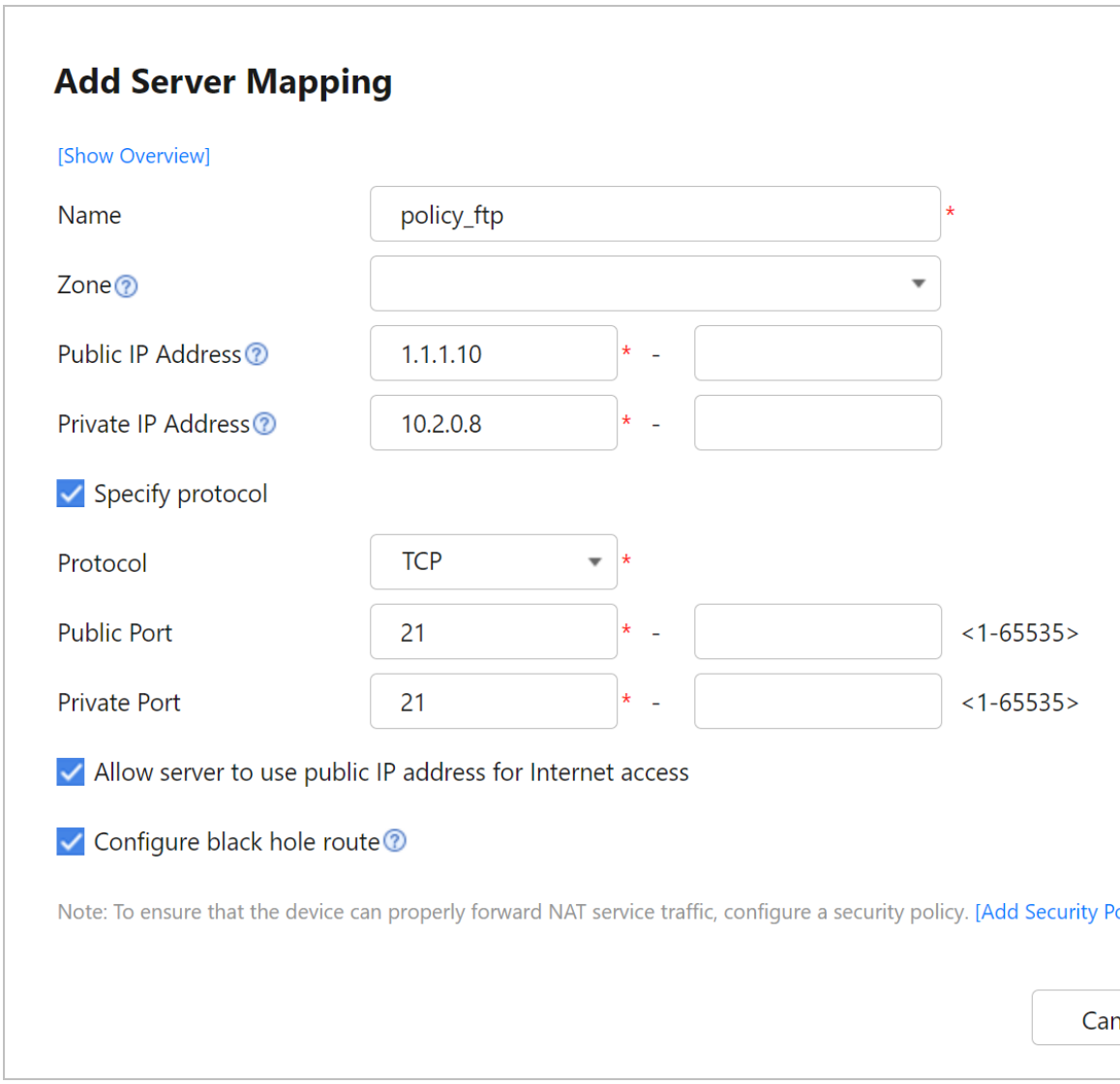
2. Click **Add** and set the following parameters for a server mapping policy named **policy_web** used for directing traffic to the web server.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **OK**.
4. Repeat the preceding substeps and set the following parameters for another server mapping policy named **policy_ftp** used for directing traffic to the FTP server.

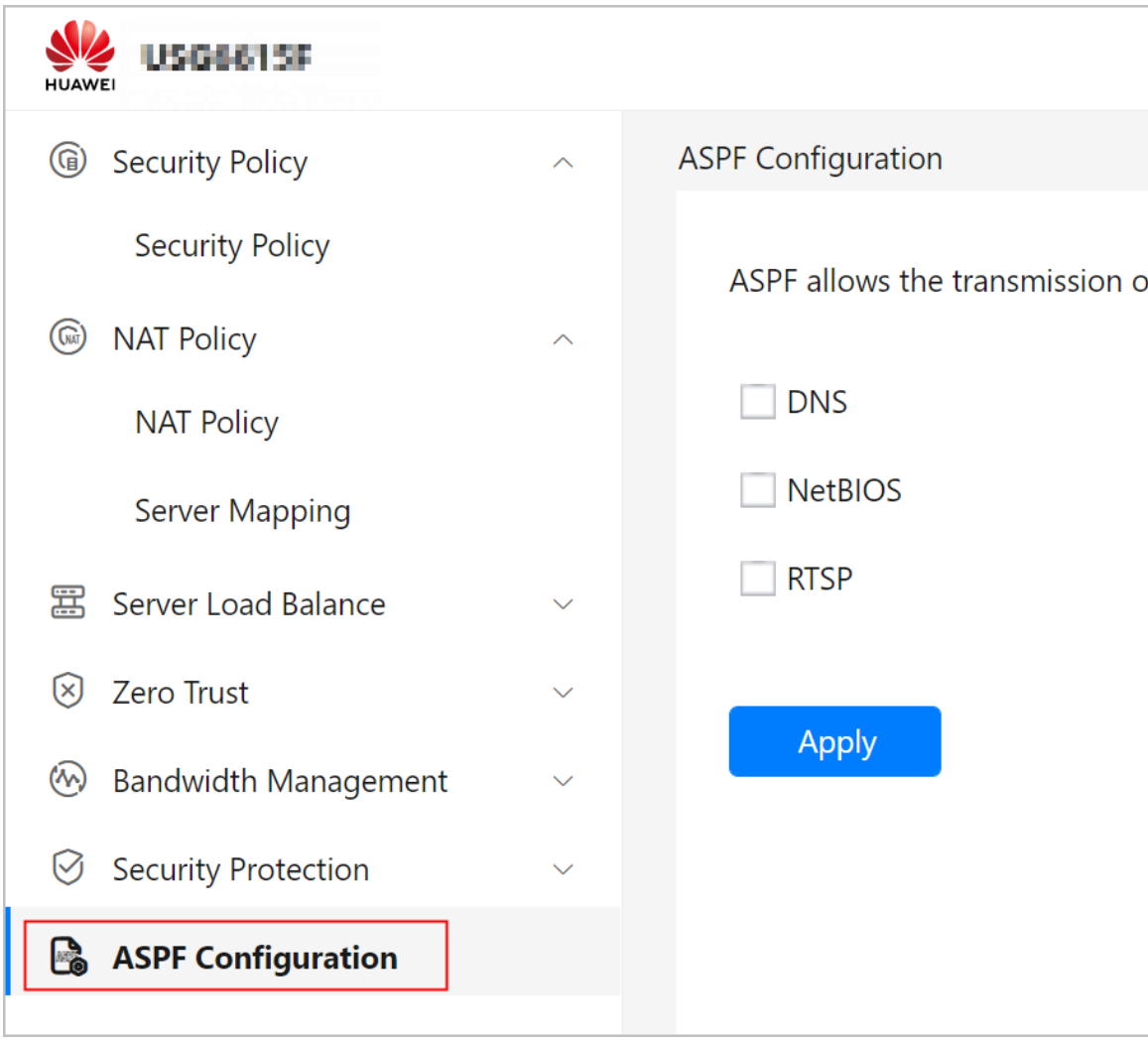
 Copyright © Huawei Technologies Co., Ltd.



Step 5 Enable NAT ALG for FTP.

1. Choose **Policy** > **ASPF Configuration**.

 Copyright © Huawei Technologies Co., Ltd.



2. Select **FTP**.

Step 6 Configure a default route on the DeviceA, so that traffic from intranet servers can be forwarded to the ISP router.

1. Choose **Network** > **Route** > **Static Route**.
2. In **Static Route List**, click **Add** and configure a default route based on the following parameter values.

Protocol	IPv4
Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.254

3. Click **OK**.

Step 7 On the router, configure a static route, in which the destination address is 1.1.1.10 and the next-hop address is 1.1.1.1. The router directs traffic destined for 1.1.1.10 to the DeivceA based on the static route so that the DeviceA can forward the traffic to the intranet server.

 Copyright © Huawei Technologies Co., Ltd.

Contact your ISP administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet users can access intranet servers.
2. When intranet users access intranet servers, choose **Monitor** > **Session Table** to verify that the sessions whose destination addresses are the public IP addresses of the intranet servers are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE 0/0/2
 detect ftp
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.1.11 1.1.1.11
#
security-policy
  rule name policy1
    source-zone dmz
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone dmz
    destination-zone dmz
    source-address 10.2.0.6 32
    action source-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

15.5.4 CLI: Example for Configuring Intranet Users to Access Intranet Servers Using Public Addresses

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. NAT Server needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. PC D in the same network segment and security zone as the two intranet servers also requires access to these servers using a public address; therefore, source NAT also needs to be configured on DeviceA.

In addition to the public address of the WAN interface on DeviceA, the enterprise has obtained the following public addresses from the ISP:

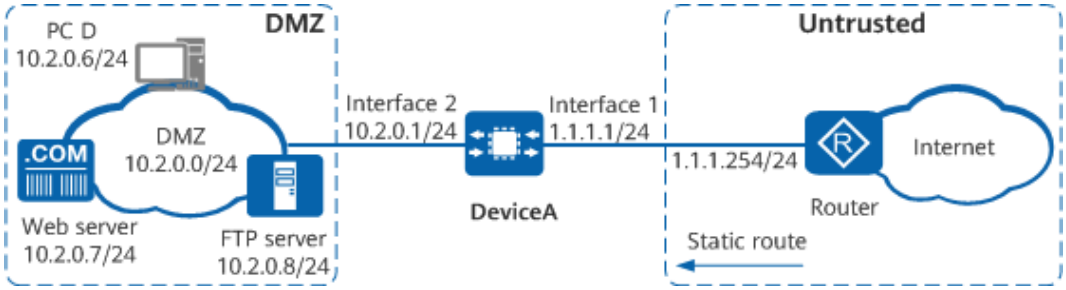
- 1.1.1.10: used by intranet servers to provide services
- 1.1.1.11: used as the post-NAT address of PC D's private address

Figure 15-44 shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 15-44 Network diagram of NAT Server and source NAT

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item	Data	Description
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	1.1.1.1/24 is a public address provided by the ISP.
GE0/0/2	IP address: 10.2.0.1/24 Security zone: DMZ	Intranet servers use 10.2.0.1 as the default gateway address.
NAT Server	Name: policy_web Public IP address: 1.1.1.10 Private IP address: 10.2.0.7 Public port: 8080 Private port: 80	When Internet users send traffic to 1.1.1.10 through port 8080, DeviceA can forward the traffic to the web server based on this mapping entry. The web server has the private address 10.2.0.7 and private port number 80.

 Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
	Name: policy_ftp Public IP address: 1.1.1.10 Private IP address: 10.2.0.8 Public port: 21 Private port: 21	When Internet users send traffic to 1.1.1.10 through port 21, DeviceA can forward the traffic to the FTP server based on this mapping entry. The FTP server has the private address 10.2.0.8 and private port number 21.
Source NAT policy	Name: policy_nat1 Private address that can access the Internet: 10.2.0.6 Address in a NAT address pool: 1.1.1.11	-
Default route	Destination address: 0.0.0.0 Next-hop address: 1.1.1.254	Configure a default route to the Internet on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

Configuration Roadmap

1. Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure a security policy to allow both intranet and Internet users to access intranet servers.
3. Configure NAT Server by specifying two static mapping entries, that is, one for the web server and one for the FTP server.
4. Configure a source NAT policy to allow PC D to access intranet servers using a public address.
5. Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.
6. Configure a static route to the public address of intranet servers on the ISP router.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.

Configure an IP address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the DMZ zone.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Step 2 Configure a security policy to allow both intranet and Internet users to access intranet servers.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone dmz untrust
[DeviceA-policy-security-rule-policy1] destination-zone dmz
[DeviceA-policy-security-rule-policy1] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT address pool.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 0 1.1.1.11 1.1.1.11
[DeviceA-address-group-addressgroup1] route enable
[DeviceA-address-group-addressgroup1] quit
```

Step 4 Configure a source NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat1
[DeviceA-policy-nat-rule-policy_nat1] source-zone dmz
[DeviceA-policy-nat-rule-policy_nat1] destination-zone dmz
[DeviceA-policy-nat-rule-policy_nat1] source-address 10.2.0.6 32
[DeviceA-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat1] quit
[DeviceA-policy-nat] quit
```

Step 5 Configure NAT Server by specifying two static mapping entries, that is, one for the web server and one for the FTP server.

```
[DeviceA] nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
[DeviceA] nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
```

Step 6 Enable the NAT ALG function for FTP.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] detect ftp
[DeviceA-zone-dmz] quit
[DeviceA] firewall interzone dmz untrust
[DeviceA-interzone-dmz-untrust] detect ftp
[DeviceA-interzone-dmz-untrust] quit
```

Step 7 Configure a default route on DeviceA to enable it to forward traffic from intranet servers to the ISP router.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

Step 8 On the ISP router, configure a static route to the public address of intranet servers, with the next-hop address set to 1.1.1.1. The ISP router can then forward traffic destined for the intranet servers to DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Contact the ISP network administrator to perform this step.

----End

Verifying the Configuration

1. Verify that intranet users can access intranet servers.
2. When intranet users access intranet servers, run the **display firewall session table** command on DeviceA to check for the session entries with the destination addresses being the public addresses of intranet servers. If such an entry is found and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy has been configured successfully. In the command output, the post-NAT IP address and port number are enclosed in square brackets ([ ]).

```
<DeviceA> display firewall session table
Current Total Sessions : 2
 tcp  VPN:public --> public  10.2.0.6:2474[1.1.1.11:2674]-->1.1.1.10:8080[10.2.0.7:80]
 tcp  VPN:public --> public  10.2.0.6:3685[1.1.1.11:3625]-->1.1.1.10:21[10.2.0.8:21]
```

Configuration Scripts

```
#
 sysname DeviceA
#
 nat server policy_web protocol tcp global 1.1.1.10 8080 inside 10.2.0.7 www route
 nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp route
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
 detect ftp
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 1.1.1.11 1.1.1.11
#
security-policy
  rule name policy1
    source-zone dmz
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0 24
    action permit
#
nat-policy
  rule name policy_nat1
    source-zone dmz
    destination-zone dmz
    source-address 10.2.0.6 32
```

 Copyright © Huawei Technologies Co., Ltd.

```
  action source-nat address-group addressgroup1
#
return
```

15.6 NAT in Hot Standby Scenarios

15.6.1 Web: Example for Configuring Source NAT in Load Balancing Scenarios (Active and Standby Devices Share One Address Pool)

Networking Requirements

On the network shown in **Figure 15-45**, the service interfaces of two devices work at Layer 3 and are directly connected to routers. The devices and directly connected routers run OSPF. Uplink interfaces of egress routers connect to the same ISP network.

The devices are required to work in load balancing mode. In normal cases, DeviceA forwards traffic from Dept. A, and DeviceB forwards traffic from Dept. B. If either device fails, the other device forwards all traffic to ensure service continuity.

NOTE

In this load balancing networking, devices connect to routers in both upstream and downstream directions. On live networks, you must determine whether OSPF is required based on the upstream and downstream devices and interfaces. The Source NAT configuration remains unchanged.

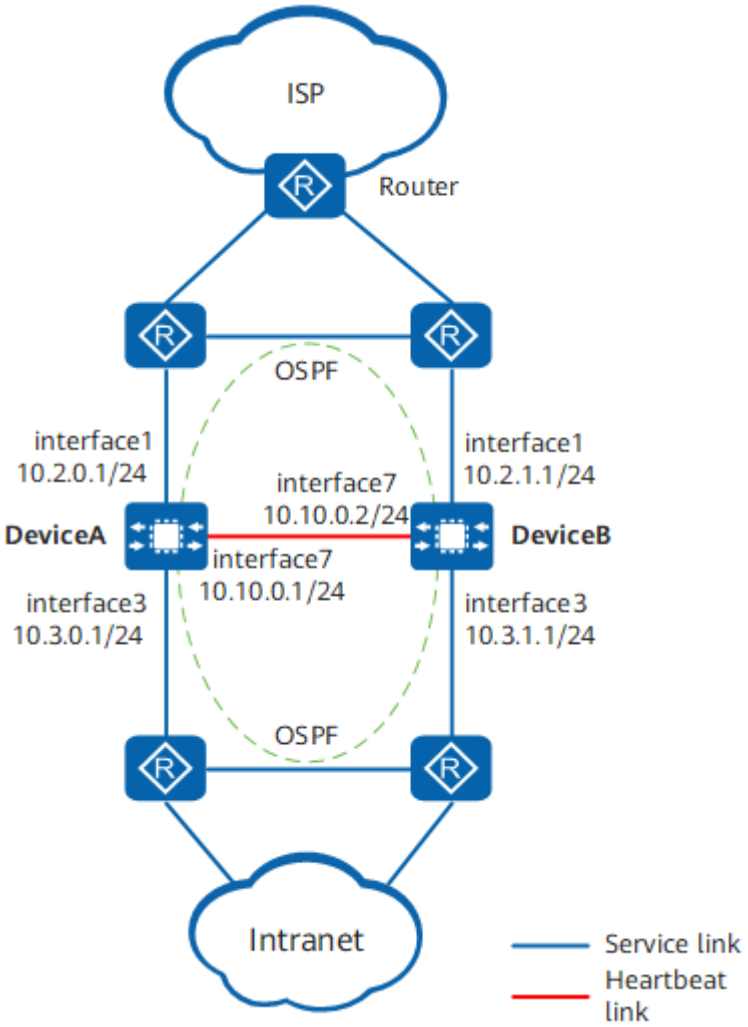
This example does not apply when uplink interfaces connect to different ISP networks.

Figure 15-45 Network diagram for configuring source NAT in a load balancing scenario

NOTE

In this example, interfaces 1, 3, and 7 represent GE 0/0/1, GE 0/0/3, and GE 0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	DeviceA	DeviceB
GE0/0/1	IP address: 10.2.0.1/24 Security zone: Untrust	IP address: 10.2.1.1/24 Security zone: Untrust
GE0/0/3	IP address: 10.3.0.1/24 Security zone: Trust	IP address: 10.3.1.1/24 Security zone: Trust
GE0/0/7	IP address: 10.10.0.1/24 Security zone: DMZ	IP address: 10.10.0.2/24 Security zone: DMZ
OSPF	Process ID: 10 Area ID: 0 Network segment for the area: 10.2.0.0/24, 10.3.0.0/24	Process ID: 10 Area ID: 0 Network segment for the area: 10.2.1.0/24, 10.3.1.0/24

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. On DeviceA and DeviceB, configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure OSPF on DeviceA and DeviceB.
3. Configure hot standby on DeviceA and DeviceB. To be specific, configure interface monitoring, specify heartbeat interfaces, and enable quick session backup.
4. If DeviceA and DeviceB share one NAT address pool and work properly, they may translate the source IP addresses and source ports of the packets sent from different hosts into the same pair of public IP address and port. To prevent port conflicts, you must specify different port ranges for the active and standby devices.
5. Configure a security policy on DeviceA to allow OSPF packet exchange between devices and Internet access from the intranet. The security policy configured on DeviceA is automatically backed up to DeviceB.
6. Configure a NAT address pool on DeviceA. The NAT address pool configured on DeviceA is automatically backed up to DeviceB.
7. Configure a Source NAT policy on DeviceA to implement source address translation for Internet access from the intranet. The Source NAT policy configured on DeviceA is automatically backed up to DeviceB.
8. Configure the downstream devices, so that traffic from department A is forwarded through DeviceA, and traffic from department B is forwarded through DeviceB.
9. On the upstream router, configure an interface address and a static route destined for the ISP, and configure OSPF so that the device and router can learn routes from each other. On the downstream router, configure an interface address and configure OSPF so that the device and router can learn routes from each other.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Set interface IP addresses on DeviceA and assign the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click of GE0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	10.2.0.1/24

   c. Click **OK**.
   d. Repeat the preceding steps to configure GE0/0/3.

Zone	trust

 Copyright © Huawei Technologies Co., Ltd.

IPv4	
IP Address	10.3.0.1/24

e. Repeat the preceding steps to configure GE0/0/7.

Zone	dmz
IPv4	
IP Address	10.10.0.1/24

2. Set interface IP addresses on DeviceB and assign the interfaces to security zones.
   a. Choose **Network** > **Interface**.
   b. Click of GE0/0/1 and set the parameters as follows:

Zone	untrust
IPv4	
IP Address	10.2.1.1/24

   c. Click **OK**.
   d. Repeat the preceding steps to configure GE0/0/3.

Zone	trust
IPv4	
IP Address	10.3.1.1/24

   e. Repeat the preceding steps to configure GE0/0/7.

Zone	dmz
IPv4	
IP Address	10.10.0.2/24

Step 2 Configure OSPF.

1. Configure OSPF on DeviceA.
   a. Choose **Network** > **Route** > **OSPF**.
   b. Click **Add** in the OSPF list.
   c. Create an OSPF process and set the parameters as follows:
      - Process ID: 10
      - Router ID: 1.1.1.1

 Copyright © Huawei Technologies Co., Ltd.

d. Click of OSPF process 10. In the navigation tree, choose **Basic Configuration** > **Area Settings**.

e. Click **Add** to create an area.

f. Set area parameters as follows:

Area	0.0.0.0
IP Network	10.2.0.0
Mask/Wildcard Mask	255.255.255.0

Area	0.0.0.0
IP Network	10.3.0.0
Mask/Wildcard Mask	255.255.255.0

g. Import an OPR route into OSPF and import the NAT address pool route to the upstream router.

Choose **Advanced Setting** > **Route Import** and click **Add**.

Set **Route Type** to **OP-ROUTE**.

2. Configure OSPF on DeviceB.

a. Choose **Network** > **Route** > **OSPF**.

b. Click **Add** in the OSPF list.

c. Create an OSPF process and set the parameters as follows:

- Process ID: 10
- Router ID: 1.1.1.2

d. Click of OSPF process 10. In the navigation tree, choose **Basic Configuration** > **Area Settings**.

e. Click **Add** to create an area.

f. Set area parameters as follows:

Area	0.0.0.0
IP Network	10.2.1.0
Mask/Wildcard Mask	255.255.255.0

Area	0.0.0.0

 Copyright © Huawei Technologies Co., Ltd.

IP Network	10.3.1.0
Mask/Wildcard Mask	255.255.255.0

g. Import an OPR route into OSPF and import the NAT address pool route to the upstream router.

Choose **Advanced Setting** > **Route Import** and click **Add**.

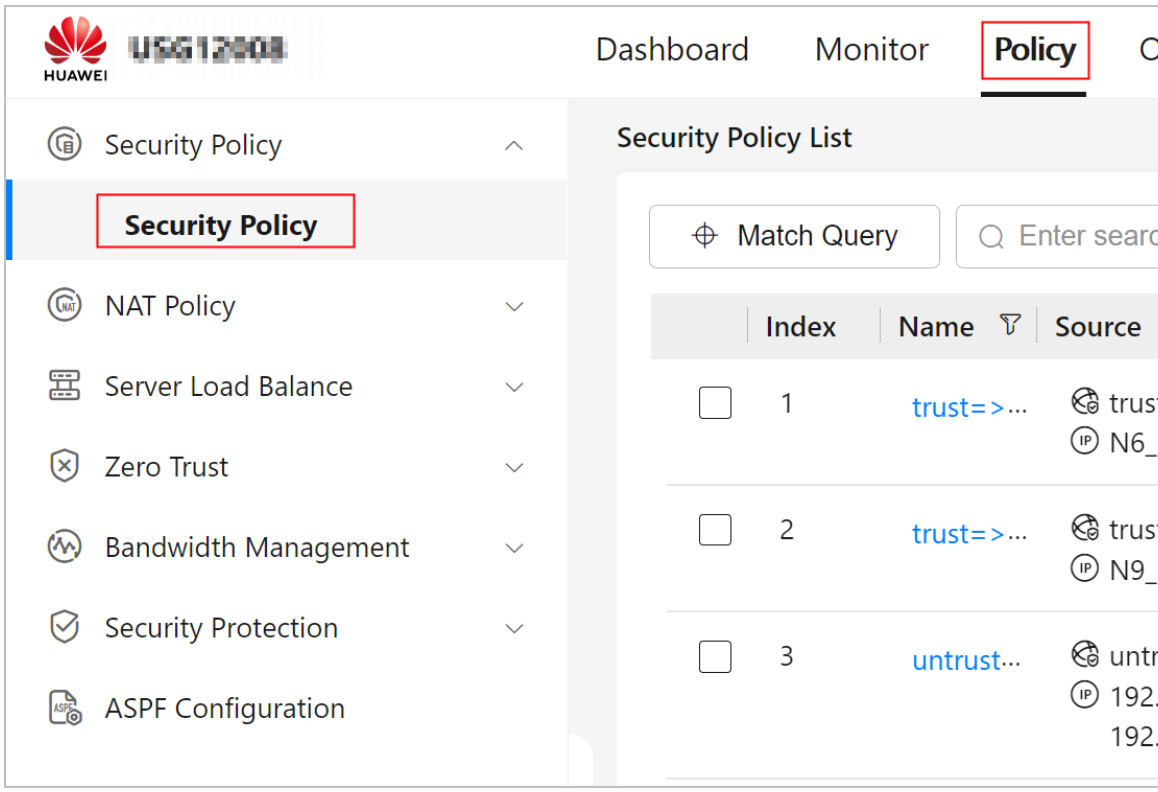
Set **Route Type** to **OP-ROUTE**.

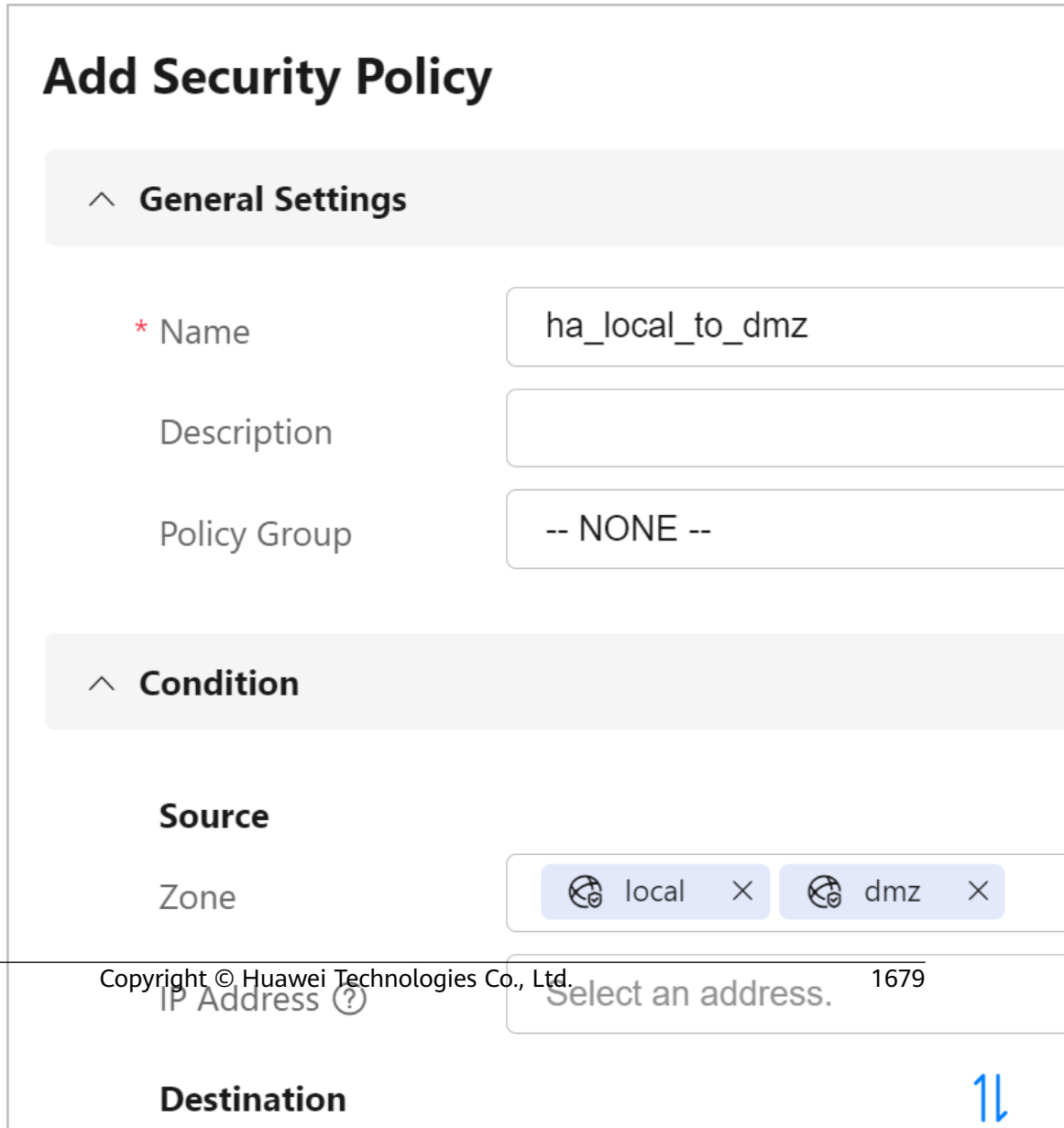
Step 3 Configure a security policy to allow HRP packets to be exchanged between heartbeat interfaces.

The configurations on DeviceA are the same as those on DeviceB. The following uses DeviceA as an example.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, configure a security policy and set the parameters as follows, and then click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

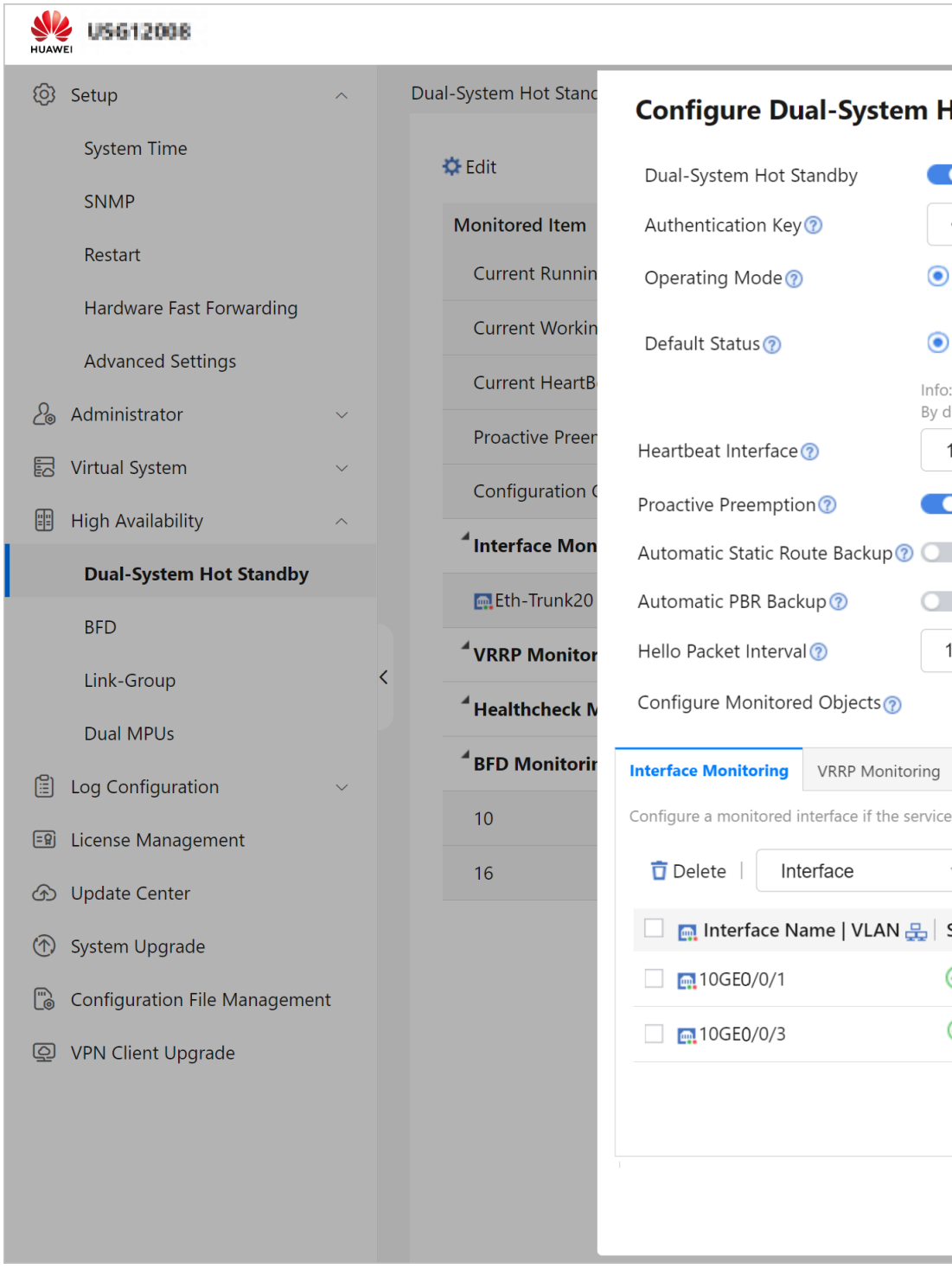




 Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure hot standby.

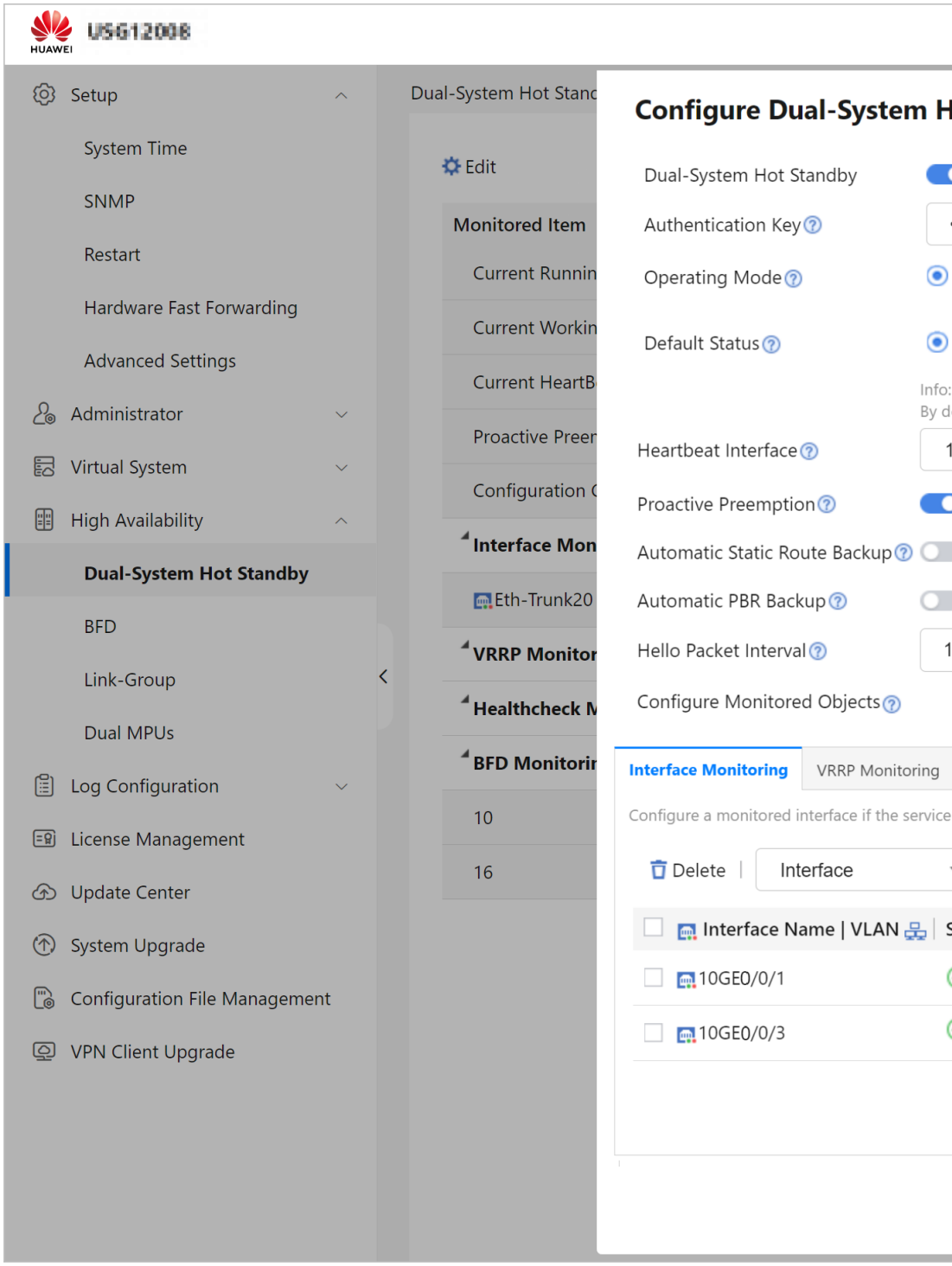
1. Configure hot standby on DeviceA.
   a. Choose **System** > **High Availability** > **Dual-System Hot Standby**.
   b. Click **Edit**.
   c. Select the **Enable** check box and configure hot standby as follows:



   d. Click **OK**.
2. Configure hot standby on DeviceB.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **System** > **High Availability** > **Dual-System Hot Standby**.
b. Click **Edit**.
c. Select the **Enable** check box and configure hot standby as follows:



d. Click **OK**.

Step 5 Configure NAT address pool port allocation in the load balancing scenario.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In the hot standby load balancing scenario, If NAPT is configured, the devices may have conflicting public ports. To prevent such conflicts, configure respective NAT resources (including public IP addresses and ports) for the devices. You can run the **hrp nat resource primary-group** command on the active device. The standby device will automatically generate the **hrp nat resource secondary-group** command (if you run the **hrp nat resource secondary-group** command on the active device, the standby device will automatically generate the **hrp nat resource primary-group** command).

```
HRP_M[Device_A] hrp nat resource primary-group
```

Step 6 Configure a security policy on DeviceA to allow OSPF packet exchange between devices and Internet access from the intranet.

The security policy configured on DeviceA is automatically backed up to DeviceB.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add** and select **Add Security**.

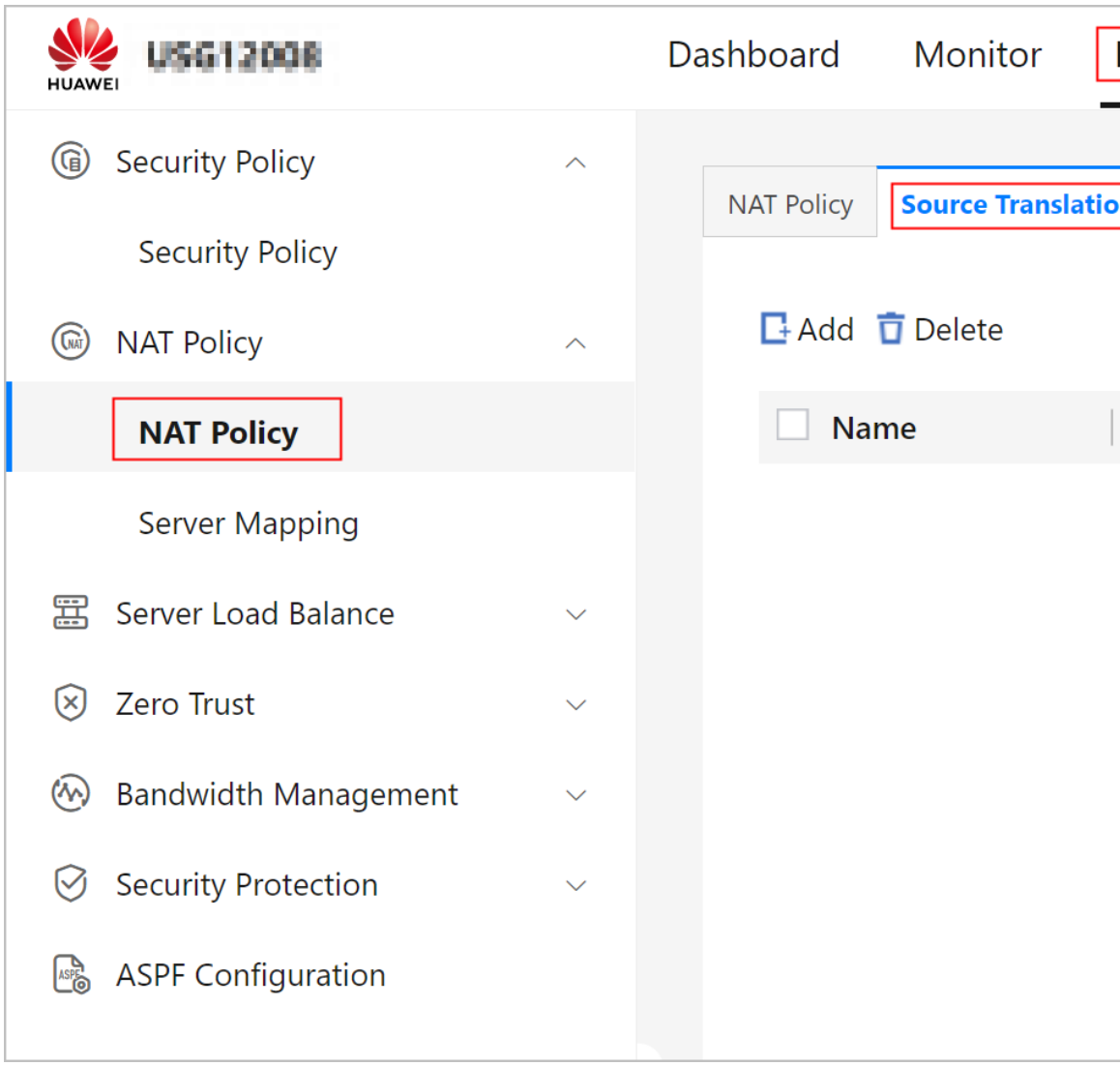
Name	policy1
Source Zone	local,trust,untrust
Destination Zone	local,trust,untrust
Action	Permit

Step 7 Configure a NAT address pool and permit port conversion to reuse public network addresses.

The NAT address pool configured on DeviceA is automatically backed up to DeviceB.

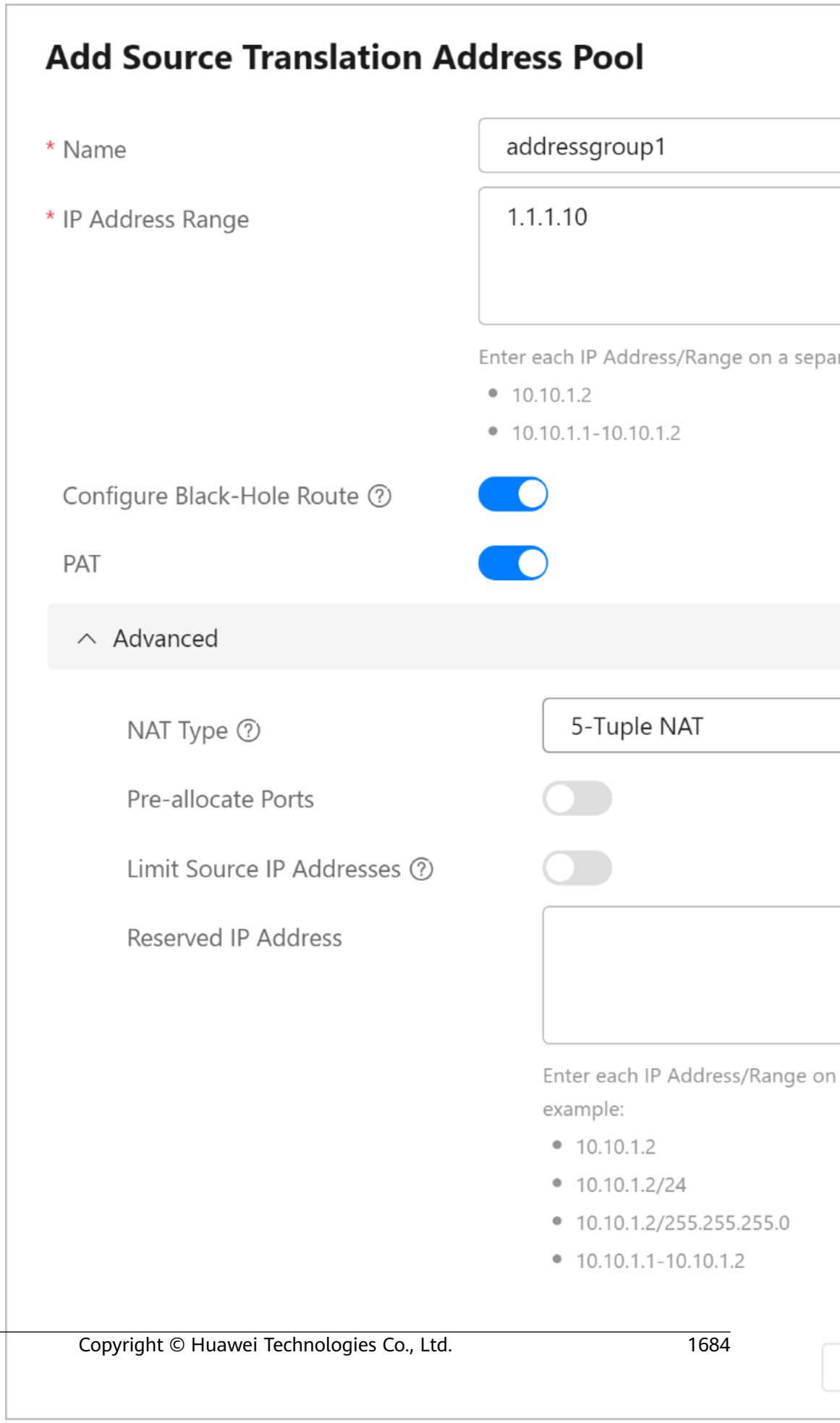
1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.

 Copyright © Huawei Technologies Co., Ltd.



2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.

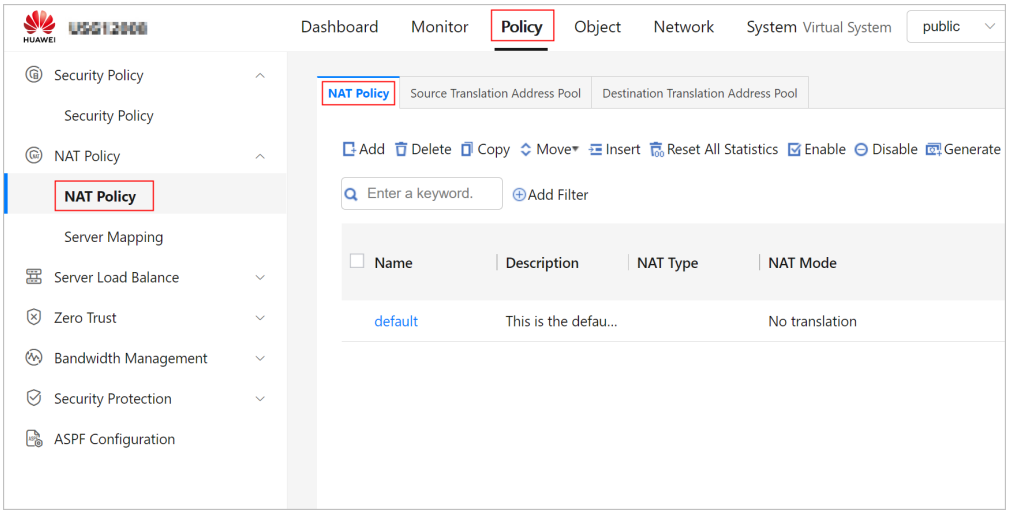


 Copyright © Huawei Technologies Co., Ltd.

Step 8 Configure a NAT policy to allow intranet users to access the Internet by using post-NAT public IP addresses.

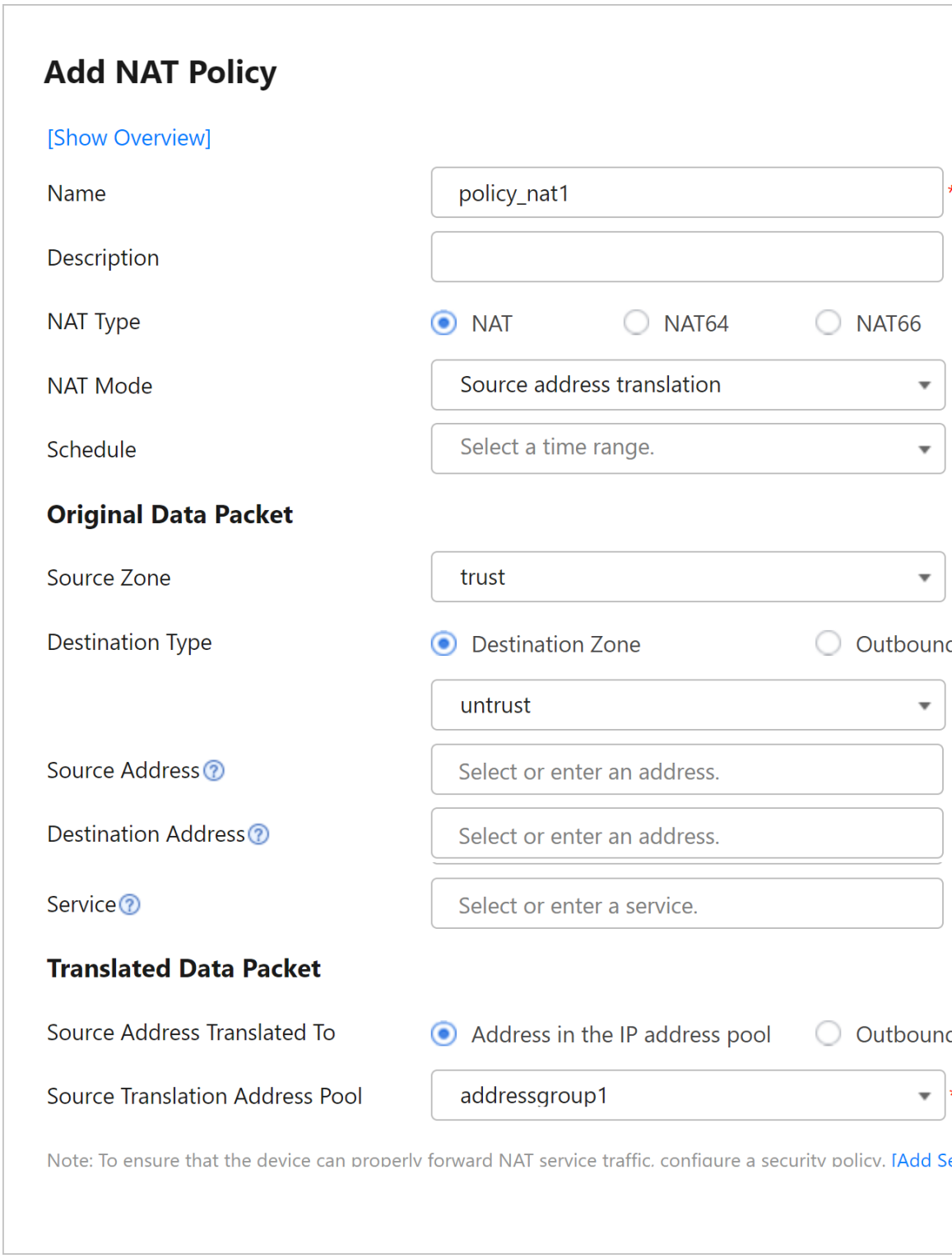
The NAT policy configured on DeviceA is automatically backed up to DeviceB.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



2. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



Step 9 Configure the downstream devices, so that traffic from department A is forwarded through DeviceA, and traffic from department B is forwarded through DeviceB.

Step 10 On the upstream router, configure an interface address and a static route destined for the ISP, and configure OSPF so that the device and router can learn routes

 Copyright © Huawei Technologies Co., Ltd.

from each other. On the downstream router, configure an interface address and configure OSPF so that the device and router can learn routes from each other.

----End

Configuration Verification

1. On DeviceA and DeviceB, choose **System** > **High Availability** > **Dual-System Hot Standby** to view hot standby status. If the following information is displayed, HRP is successfully configured. **Current Running Mode** is **Load Balancing** for both DeviceA and DeviceB; **Current Working Role** is **Active** for both DeviceA and DeviceB. In this case, both devices forward traffic.
2. Verify that intranet PCs can access the Internet.
3. Choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet users are displayed.
4. The services are still available even if an interface fault occurs on DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
 sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.2
 hrp mirror session enable
 hrp authentication-key %@%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%@%#
#
hrp nat resource primary-group
#
hrp track interface GE0/0/1
hrp track interface GE0/0/3
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10 route-id 1.1.1.1
 import-route op-route
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
 nat address-group addressgroup1
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy1
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
```

DeviceB

```
#
 sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.1
 hrp mirror session enable
 hrp authentication-key %@%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%@%#
#
hrp nat resource secondary-group
#
hrp track interface GE0/0/1
hrp track interface GE0/0/3
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10 route-id 1.1.1.2
 import-route op-route
 area 0.0.0.0
  network 10.2.1.0.0.0.255
  network 10.3.1.0 0.0.0.255
#
 nat address-group addressgroup1
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy1
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
destination-zone untrust action source-nat address-group addressgroup1 # return	destination-zone untrust action source-nat address-group addressgroup1 # return

15.6.2 CLI: Example for Configuring Source NAT in a Load Balancing Scenario (Active and Standby Devices Share One Address Pool)

Networking Requirements

On the network shown in **Figure 15-46**, the service interfaces of two devices work at Layer 3 and are directly connected to routers. The devices and directly connected routers run OSPF. Uplink interfaces of egress routers connect to the same ISP network.

The devices are required to work in load balancing mode. In normal cases, DeviceA forwards traffic from department A, and DeviceB forwards traffic from department B. If one device fails, the other device forwards all traffic to ensure service continuity. If one device fails, the other device forwards all traffic to ensure service continuity.

NOTE

In this load balancing networking, devices connect to routers in both upstream and downstream directions. On live networks, you need to determine whether OSPF is required based on the upstream and downstream devices and interfaces. The source NAT configuration is the same.

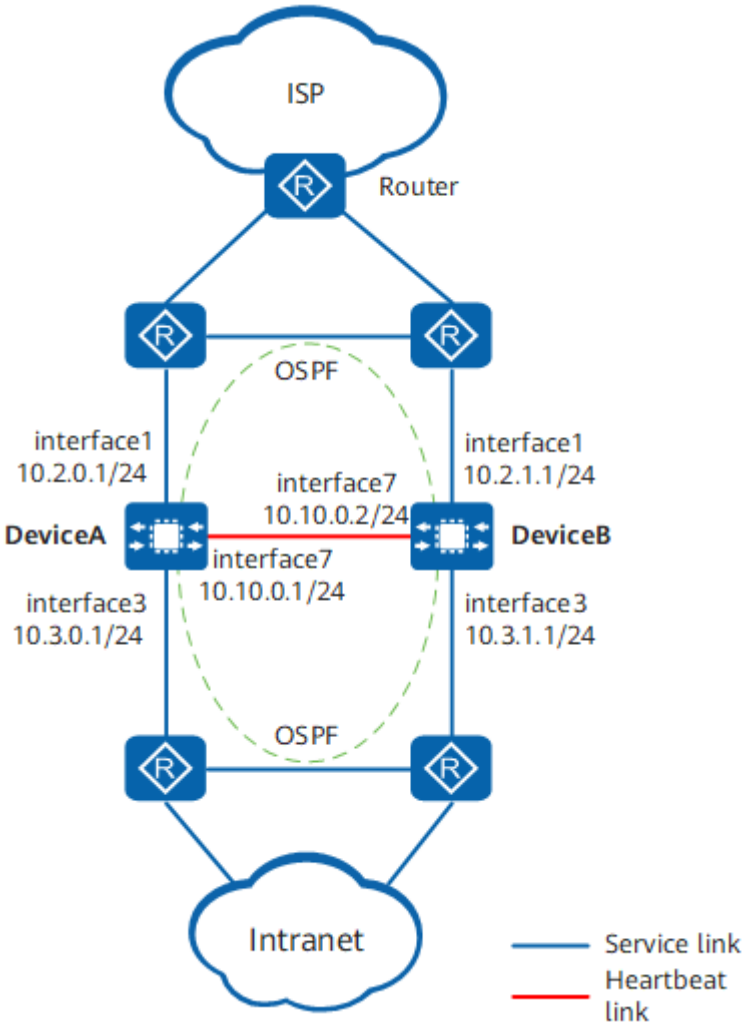
This example does not apply when uplink interfaces of egress routers connect to different ISP networks.

Figure 15-46 Networking diagram for configuring source NAT in a load balancing scenario.

NOTE

In this example, interfaces 1, 3, and 7 represent GE0/0/1, GE0/0/3 and GE0/0/7, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	DeviceA	DeviceB
GE0/0/1	IP address: 10.2.0.1/24 Security zone: Untrust	IP address: 10.2.1.1/24 Security zone: Untrust
GE0/0/3	IP address: 10.3.0.1/24 Security zone: Trust	IP address: 10.3.1.1/24 Security zone: Trust
GE0/0/7	IP address: 10.10.0.1/24 Security zone: DMZ	IP address: 10.10.0.2/24 Security zone: DMZ
OSPF	Process ID: 10 Area ID: 0 Network segment for the area: 10.2.0.0/24, 10.3.0.0/24, and 1.1.1.10/32	Process ID: 10 Area ID: 0 Network segment for the area: 10.2.1.0/24, 10.3.1.0/24, and 1.1.1.10/32

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. On DeviceA and DeviceB, configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure OSPF on DeviceA and DeviceB.
3. If DeviceA and DeviceB share one NAT address pool and work properly, they may translate the source IP addresses and source port numbers of the packets sent from different hosts into the same pair of public IP address and port number. To prevent port conflicts, specify different port ranges for the active and standby devices.
4. Configure hot standby on DeviceA and DeviceB. To be specific, configure interface monitoring, specify heartbeat interfaces, and enable quick session backup.
5. Configure a security policy on DeviceA to allow OSPF packet exchange between devices and Internet access from the intranet. The security policy configured on DeviceA is automatically backed up to DeviceB.
6. Configure a NAT address pool on DeviceA. The NAT address pool configured on DeviceA is automatically backed up to DeviceB.
7. Configure a source NAT policy on DeviceA to implement source address translation for Internet access from the intranet. The source NAT policy configured on DeviceA is automatically backed up to DeviceB.
8. Configure the downstream devices, so that traffic from department A is forwarded through DeviceA and traffic from department B is forwarded through DeviceB.
9. On the upstream router, configure an interface address and a static route destined for the ISP, and configure OSPF so that the device and router can learn routes from each other. On the downstream router, configure an interface address and configure OSPF so that the device and router can learn routes from each other. The detailed configurations are not provided here.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones.

1. Configure interfaces on DeviceA.

   # Configure interface IP addresses.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 10.2.0.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/7
[DeviceA-GE0/0/7] ip address 10.10.0.1 24
[DeviceA-GE0/0/7] quit
```

   # Add interfaces to security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/7
[DeviceA-zone-dmz] quit
```

2. Configure interfaces on DeviceB.

   # Configure interface IP addresses.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ip address 10.2.1.1 24
[DeviceB-GE0/0/1] quit
[DeviceB] interface ge 0/0/3
[DeviceB-GE0/0/3] ip address 10.3.1.1 24
[DeviceB-GE0/0/3] quit
[DeviceB] interface ge 0/0/7
[DeviceB-GE0/0/7] ip address 10.10.0.2 24
[DeviceB-GE0/0/7] quit
```

   # Assign interfaces to security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/3
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] quit
[DeviceB] firewall zone dmz
[DeviceB-zone-dmz] add interface ge 0/0/7
[DeviceB-zone-dmz] quit
```

Step 2 Configure OSPF on DeviceA and DeviceB.

Configure OSPF on DeviceA.

```
[DeviceA] ospf 10
[DeviceA-ospf-10] import-route op-route
[DeviceA-ospf-10] area 0
[DeviceA-ospf-10-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceA-ospf-10-area-0.0.0.0] network 10.3.0.0 0.0.0.255
[DeviceA-ospf-10-area-0.0.0.0] quit
[DeviceA-ospf-10] quit
```

Configure OSPF on DeviceB.

```
[DeviceB] ospf 10
[DeviceB-ospf-10] import-route op-route
[DeviceB-ospf-10] area 0
[DeviceB-ospf-10-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[DeviceB-ospf-10-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[DeviceB-ospf-10-area-0.0.0.0] quit
[DeviceB-ospf-10] quit
```

Step 3 Allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

Configure DeviceA.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name ha_local_to_dmz
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-security-rule-ha_local_to_dmz] source-zone local dmz
[DeviceA-policy-security-rule-ha_local_to_dmz] destination-zone local dmz
[DeviceA-policy-security-rule-ha_local_to_dmz] service protocol udp destination-port 18514
[DeviceA-policy-security-rule-ha_local_to_dmz] action permit
[DeviceA-policy-security-rule-ha_local_to_dmz] quit
[DeviceA-policy-security] quit
```

Configure DeviceB.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ha_local_to_dmz
[DeviceB-policy-security-rule-ha_local_to_dmz] source-zone local dmz
[DeviceB-policy-security-rule-ha_local_to_dmz] destination-zone local dmz
[DeviceB-policy-security-rule-ha_local_to_dmz] service protocol udp destination-port 18514
[DeviceB-policy-security-rule-ha_local_to_dmz] action permit
[DeviceB-policy-security-rule-ha_local_to_dmz] quit
[DeviceB-policy-security] quit
```

Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.

   # Configure interface monitoring.

   ```
   [DeviceA] hrp track interface ge 0/0/1
   [DeviceA] hrp track interface ge 0/0/3
   ```

   # Specify a heartbeat interface and configure the authentication key.

   ```
   [DeviceA] hrp interface ge 0/0/7 remote 10.10.0.2
   [DeviceA] hrp authentication-key YsH_2022
   ```

   # Enable quick session backup.

   ```
   [DeviceA] hrp mirror session enable
   ```

   NOTE

   When the devices work in load-balancing mode, the forward and return packets may pass through different devices. To ensure service continuity, enable quick session backup to ensure that the session information on one device is synchronized to the other device.

   # Enable hot standby.

   ```
   [DeviceA] hrp enable
   ```

2. Configure hot standby on DeviceB.

   # Configure interface monitoring.

   ```
   [DeviceB] hrp track interface ge 0/0/1
   [DeviceB] hrp track interface ge 0/0/3
   ```

   # Specify a heartbeat interface and configure the authentication key.

   ```
   [DeviceB] hrp interface ge 0/0/7 remote 10.10.0.1
   [DeviceB] hrp authentication-key YsH_2022
   ```

   # Enable quick session backup.

   ```
   [DeviceB] hrp mirror session enable
   ```

   # Enable hot standby.

   ```
   [DeviceB] hrp enable
   ```

Step 5 Configure NAT address pool port allocation in the load balancing scenario.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In the hot standby load balancing scenario, if NAPT is configured and the two devices share the same NAT address pool, the devices may have conflicting public port numbers. To prevent such conflicts, configure respective NAT resources (including public IP addresses and ports) for the devices. You can run the **hrp nat resource primary-group** command on the active device. The standby device will automatically generate the **hrp nat resource secondary-group** command (if you run the **hrp nat resource secondary-group** command on the active device, the standby device will automatically generate the **hrp nat resource primary-group** command).

```
[DeviceA] hrp nat resource primary-group
```

Step 6 Configure a security policy on DeviceA to allow OSPF packet exchange between devices and Internet access from the intranet.

The security policy configured on DeviceA will be automatically backed up to DeviceA.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec_1
HRP_M[DeviceA-policy-security-rule-policy_sec_1] source-zone local trust untrust
HRP_M[DeviceA-policy-security-rule-policy_sec_1] destination-zone local trust untrust
HRP_M[DeviceA-policy-security-rule-policy_sec_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec_1] quit
HRP_M[DeviceA-policy-security] quit
```

Step 7 Configure a NAT address pool and permit port translation to reuse public network addresses.

The NAT address pool configured on DeviceA will be automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.10
HRP_M[DeviceA-address-group-addressgroup1] mode pat
HRP_M[DeviceA-address-group-addressgroup1] route enable
HRP_M[DeviceA-address-group-addressgroup1] quit
```

Step 8 Configure a source NAT policy to allow intranet users to access the Internet by using post-NAT public IP addresses.

The NAT policy configured on DeviceA will be automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat_1
HRP_M[DeviceA-policy-rule-nat-policy_nat_1] source-zone trust
HRP_M[DeviceA-policy-rule-nat-policy_nat_1] destination-zone untrust
HRP_M[DeviceA-policy-rule-nat-policy_nat_1] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-rule-nat-policy_nat_1] quit
HRP_M[DeviceA-policy-nat] quit
```

Step 9 Configure downstream devices, so that traffic from department A is forwarded through DeviceA, and traffic from department B is forwarded through DeviceB.

Step 10 On the upstream router, configure an interface address and a static route destined for the ISP, and configure OSPF so that the device and router can learn routes from each other. On the downstream router, configure an interface address and configure OSPF so that the device and router can learn routes from each other. The detailed configurations are not provided here.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

1. If intranet PCs can access the Internet, the security policies are successfully configured.
2. Run the **display nat-policy rule name** *rule-name* command on DeviceA and DeviceB respectively to check the number of times traffic matches the source NAT policy.
3. Run the **display firewall session table** command on DeviceA and DeviceB respectively to search for an entry whose source address is the private address of an intranet PC. If the entry exists and the post-NAT IP address exists in the NAT address pool, the NAT policy is successfully configured. Information in the brackets ([]) is the post-NAT or IP address.

```
HRP_M<Device> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.3.2.55:2474[1.1.1.10:3761]-->3.3.3.3:80
```

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
 sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.2
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
hrp nat resource primary-group
#
hrp track interface GE0/0/1
hrp track interface GE0/0/3
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10 router-id 1.1.1.1
 import-route op-route
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
 nat address-group addressgroup1
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec_1
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  action permit
#
nat-policy
```

DeviceB

```
#
 sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/7 remote 10.10.0.1
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
hrp nat resource secondary-group
#
hrp track interface GE0/0/1
hrp track interface GE0/0/3
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10 router-id 1.1.1.2
 import-route op-route
 area 0.0.0.0
  network 10.2.1.0.0.0.255
  network 10.3.1.0 0.0.0.255
#
 nat address-group addressgroup1
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.10
#
security-policy
 rule name ha_local_to_dmz
  source-zone local dmz
  destination-zone local dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec_1
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  action permit
#
nat-policy
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
rule name policy_nat_1 source-zone trust destination-zone untrust action source-nat address-group addressgroup1 # return	rule name policy_nat_1 source-zone trust destination-zone untrust action source-nat address-group addressgroup1 # return

15.6.3 CLI: Example for Configuring Source NAT in a Load Balancing Scenario (Active and Standby Devices Use Different Address Pools)

Networking Requirements

On the network shown in **Figure 15-47**, the service interfaces of two devices work at Layer 3 and are directly connected to switches. The devices connect to Layer 2 switches in both upstream and downstream directions.

The devices are required to work in load balancing mode. In normal cases, DeviceA forwards traffic from department A (IP address range: 10.3.0.51 to 10.3.0.100), and DeviceB forwards traffic from department B (IP address range: 10.3.0.101 to 10.3.0.150). If one device fails, the other device forwards all traffic to ensure service continuity.

To enable private network users to access the Internet, you need to configure a source NAT policy on DeviceA and DeviceB.

The address pool including address 1.1.1.4 is created on DeviceA to provide a post-NAT public address for PCs from department A (IP address range: 10.3.0.51 to 10.3.0.100). The address pool including address 1.1.2.4 is created on DeviceB to provide a post-NAT public address for PCs from department. B (IP address range: 10.3.0.101 to 10.3.0.150).

NOTE

In this load balancing networking, devices connect to switches in both upstream and downstream directions. On live networks, you need to determine whether VRRP groups are required based on the upstream and downstream devices and interfaces. The source NAT configuration is the same.

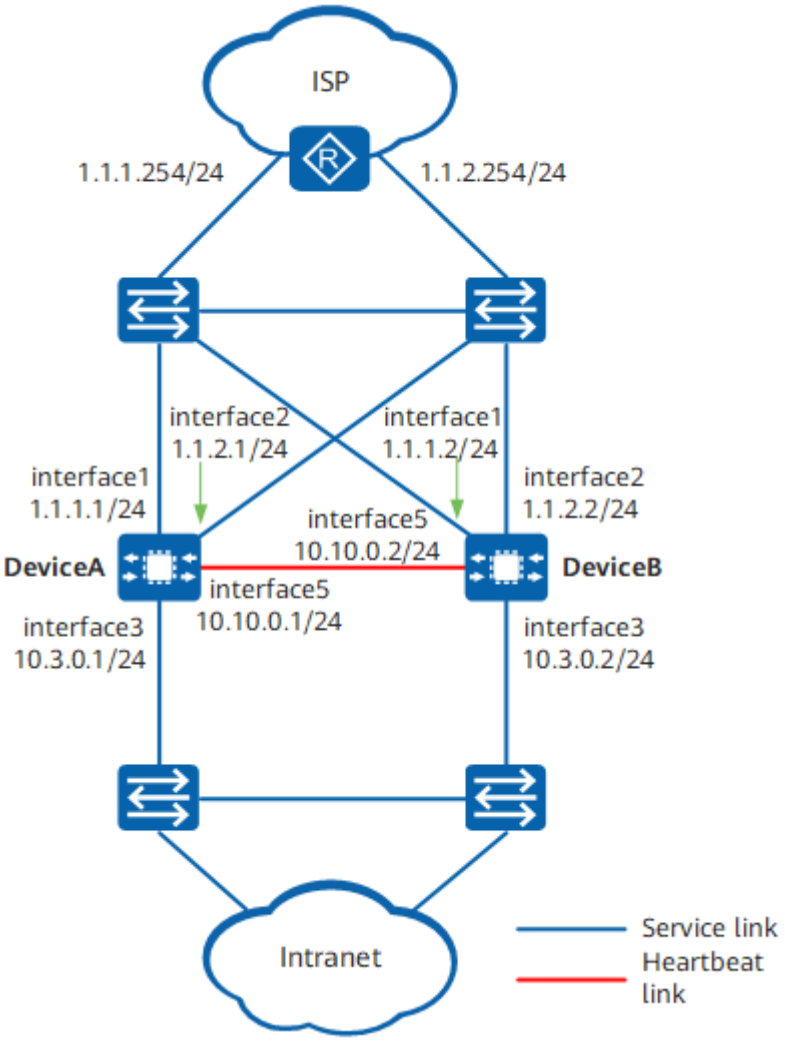
This example does not apply when uplink interfaces connect to different ISP networks.

Figure 15-47 Networking diagram for configuring source NAT in a load balancing scenario.

NOTE

In this example, interfaces 1, 2, 3, and 5 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/5, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Item	DeviceA	DeviceB
GE0/0/1	IP address: 1.1.1.1/24 Security zone: Untrust	IP address: 1.1.1.2/24 Security zone: Untrust
GE0/0/2	IP address: 1.1.2.1/24 Security zone: Untrust	IP address: 1.1.2.2/24 Security zone: Untrust
GE0/0/3	IP address: 10.3.0.1/24 Security zone: Trust	IP address: 10.3.0.2/24 Security zone: Trust
GE0/0/5	IP address: 10.10.0.1/24 Security zone: DMZ	IP address: 10.10.0.2/24 Security zone: DMZ

 Copyright © Huawei Technologies Co., Ltd.

Item	DeviceA	DeviceB
VRRP Groups	On GE0/0/1, configure VRRP group 1 (active). On GE0/0/2, configure VRRP group 2 (standby). On GE0/0/3, configure VRRP groups 3 (active) and VRRP group 4 (standby). Virtual address of VRRP group 1: 1.1.1.3/24 Virtual address of VRRP group 2: 1.1.2.3/24 Virtual address of VRRP group 3: 10.3.0.3/24 Virtual address of VRRP group 4: 10.3.0.4/24	On GE0/0/1, configure VRRP group 1 (standby). On GE0/0/2, configure VRRP group 2 (active). On GE0/0/3, configure VRRP groups 3 (standby) and VRRP group 4 (active). Virtual address of VRRP group 1: 1.1.1.3/24 Virtual address of VRRP group 2: 1.1.2.3/24 Virtual address of VRRP group 3: 10.3.0.3/24 Virtual address of VRRP group 4: 10.3.0.4/24

Configuration Roadmap

1. On DeviceA and DeviceB, configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
2. Configure two default routes on DeviceA. Set the next hop of one default route to 1.1.1.254. Set the next hop of the other default route to 1.1.2.254 and set a higher preference. Configure two default routes on DeviceB. Set the next hop of one default route to 1.1.2.254. Set the next hop of the other default route to 1.1.1.254 and set a higher preference.
3. Configure hot standby on DeviceA and DeviceB. To be specific, configure VRRP groups, specify heartbeat interfaces, and enable quick session backup.
4. Configure a security policy on DeviceA to allow intranet users on a specified network segment to access the Internet. The security policy configured on DeviceA will be automatically backed up to DeviceB.
5. Configure two NAT address pools (**addressgroup1** and **addressgroup2**) on DeviceA. The NAT address pools configured on DeviceA will be automatically backed up to DeviceB.
6. Configure a source NAT policy on DeviceA to translate the source addresses of users in department A (10.3.0.51-10.3.0.100) into addresses in the address pool **addressgroup1** and translate the source addresses of users in department B (10.3.0.101-10.3.0.150) into addresses in the address pool **addressgroup2** when the users access the Internet. The source NAT policy configured on DeviceA will be automatically backed up to DeviceB.
7. Configure default routes on intranet PCs to set the next hop of department A to the virtual IP address 10.3.0.3 of VRRP group 3 and the next hop of department B to the virtual IP address 10.3.0.4 of VRRP group 4.
8. Configure two static routes on the router. For one static route, set the destination address to an address in the address pool **addressgroup1** and the next hop to the virtual IP address 1.1.2.3 of VRRP group 2. For the other static

 Copyright © Huawei Technologies Co., Ltd.

route, set the destination address to an address in the address pool **addressgroup2** and the next hop to the virtual IP address 1.1.1.3 of VRRP group 1. If one link fails, traffic can travel along the other link.

Procedure

Step 1 Configure IP addresses for interfaces and add them to security zones.

1. Configure interfaces on DeviceA.

   # Configure interface IP addresses.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 1.1.2.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] interface ge 0/0/5
[DeviceA-GE0/0/5] ip address 10.10.0.1 24
[DeviceA-GE0/0/5] quit
```

   # Add interfaces to security zones.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/5
[DeviceA-zone-dmz] quit
```

2. Configure interfaces on DeviceB.

   # Configure interface IP addresses.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] ip address 1.1.1.2 24
[DeviceB-GE0/0/1] quit
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] ip address 1.1.2.2 24
[DeviceB-GE0/0/2] quit
[DeviceB] interface ge 0/0/3
[DeviceB-GE0/0/3] ip address 10.3.0.2 24
[DeviceB-GE0/0/3] quit
[DeviceB] interface ge 0/0/5
[DeviceB-GE0/0/5] ip address 10.10.0.2 24
[DeviceB-GE0/0/5] quit
```

   # Add interfaces to security zones.

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface ge 0/0/3
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface ge 0/0/1
[DeviceB-zone-untrust] add interface ge 0/0/2
[DeviceB-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceB] firewall zone dmz
[DeviceB-zone-dmz] add interface ge 0/0/5
[DeviceB-zone-dmz] quit
```

Step 2 Configure two default routes on DeviceA. Set the next hop of one default route to 1.1.1.254. Set the next hop of the other default route to 1.1.2.254 and set a higher preference. Configure two default routes on DeviceB. Set the next hop of one default route to 1.1.2.254. Set the next hop of the other default route to 1.1.1.254 and set a higher preference.

Configure default routes on DeviceA.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.2.254 preference 50
```

Configure default routes on DeviceB.

```
[DeviceB] ip route-static 0.0.0.0 0.0.0.0 1.1.2.254
[DeviceB] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254 preference 50
```

Step 3 Allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

HRP packets are controlled by the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled, meaning that HRP packets are controlled by security policies. As such, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, the function of the **firewall packet-filter basic-protocol enable** command is enabled.

Configure DeviceA.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name ha_local_to_dmz
[DeviceA-policy-security-rule-ha_local_to_dmz] source-zone local dmz
[DeviceA-policy-security-rule-ha_local_to_dmz] destination-zone local dmz
[DeviceA-policy-security-rule-ha_local_to_dmz] service protocol udp destination-port 18514
[DeviceA-policy-security-rule-ha_local_to_dmz] action permit
[DeviceA-policy-security-rule-ha_local_to_dmz] quit
[DeviceA-policy-security] quit
```

Configure DeviceB.

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ha_local_to_dmz
[DeviceB-policy-security-rule-ha_local_to_dmz] source-zone local dmz
[DeviceB-policy-security-rule-ha_local_to_dmz] destination-zone local dmz
[DeviceB-policy-security-rule-ha_local_to_dmz] service protocol udp destination-port 18514
[DeviceB-policy-security-rule-ha_local_to_dmz] action permit
[DeviceB-policy-security-rule-ha_local_to_dmz] quit
[DeviceB-policy-security] quit
```

Step 4 Configure hot standby.

1. Configure hot standby on DeviceA.

   # Configure VRRP groups.

   ```
   [Device_A] interface ge 0/0/1
   [DeviceA-GE0/0/1] vrrp vrid 1 virtual-ip 1.1.1.3 active
   [DeviceA-GE0/0/1] quit
   [DeviceA] interface ge 0/0/2
   [DeviceA-GE0/0/2] vrrp vrid 2 virtual-ip 1.1.2.3 standby
   [DeviceA-GE0/0/2] quit
   [DeviceA] interface ge 0/0/3
   [DeviceA-GE0/0/3] vrrp vrid 3 virtual-ip 10.3.0.3 active
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/3] vrrp vrid 4 virtual-ip 10.3.0.4 standby
[DeviceA-GE0/0/3] quit
```

Specify a heartbeat interface and configure the authentication key.

```
[DeviceA] hrp interface ge 0/0/5 remote 10.10.0.2
[DeviceA] hrp authentication-key YsH_2022
```

Enable quick session backup.

```
[DeviceA] hrp mirror session enable
```

NOTE

When the devices work in load-balancing mode, the forward and return packets may pass through different devices. To ensure service continuity, enable quick session backup to ensure that the session information on one device is synchronized to the other device.

Enable hot standby.

```
[DeviceA] hrp enable
```

2. Configure hot standby on DeviceB.

Configure VRRP groups.

```
[DeviceB] interface ge 0/0/1
[DeviceB-GE0/0/1] vrrp vrid 1 virtual-ip 1.1.1.3 standby
[DeviceB-GE0/0/1] quit
[DeviceB] interface ge 0/0/2
[DeviceB-GE0/0/2] vrrp vrid 2 virtual-ip 1.1.2.3 active
[DeviceB-GE0/0/2] quit
[DeviceB] interface ge 0/0/3
[DeviceB-GE0/0/3] vrrp vrid 3 virtual-ip 10.3.0.3 standby
[DeviceB-GE0/0/3] vrrp vrid 4 virtual-ip 10.3.0.4 active
[DeviceB-GE0/0/3] quit
```

Specify a heartbeat interface and configure the authentication key.

```
[DeviceB] hrp interface ge 0/0/5  remote 10.10.0.1
[DeviceB] hrp authentication-key YsH_2022
```

Enable quick session backup.

```
[DeviceB] hrp mirror session enable
```

Enable hot standby.

```
[DeviceB] hrp enable
```

Step 5 Configure a security policy on DeviceA to allow intranet users to access the Internet.

Security policies configured on DeviceA will be automatically backed up to DeviceB.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec_1
HRP_M[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
HRP_M[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.2.0 24
HRP_M[DeviceA-policy-security-rule-policy_sec_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec_1] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure NAT address pools and permit port translation to reuse public network addresses.

 Copyright © Huawei Technologies Co., Ltd.

Create address pools **addressgroup1** (1.1.1.4-1.1.1.4) and **addressgroup2** (1.1.2.4-1.1.2.4) on DeviceA. The NAT address pools configured on DeviceA are automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-nat-address-group-addressgroup1] section 0 1.1.1.4 1.1.1.4
HRP_M[DeviceA-nat-address-group-addressgroup1] mode pat
HRP_M[DeviceA-nat-address-group-addressgroup1] quit
HRP_M[DeviceA] nat address-group addressgroup2
HRP_M[DeviceA-nat-address-group-addressgroup2] section 1 1.1.2.4 1.1.2.4
HRP_M[DeviceA-nat-address-group-addressgroup2] mode pat
HRP_M[DeviceA-nat-address-group-addressgroup2] quit
```

Step 7 Configure NAT policies to allow intranet users to access the Internet by using post-NAT public IP addresses.

Configure a source NAT policy on DeviceA to translate the source addresses of users in department A (10.3.0.51-10.3.0.100) into addresses in the address pool **addressgroup1** and translate the source addresses of users in department B (10.3.0.101-10.3.0.150) into addresses in the address pool **addressgroup2** when the users access the Internet. The source NAT policy configured on DeviceA will be automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat_1
HRP_M[DeviceA-policy-nat-policy_nat_1] source-address range 10.3.0.51 10.3.0.100
HRP_M[DeviceA-policy-nat-policy_nat_1] source-zone trust
HRP_M[DeviceA-policy-nat-policy_nat_1] destination-zone untrust
HRP_M[DeviceA-policy-nat-policy_nat_1] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-policy_nat_1] quit
HRP_M[DeviceA-policy-nat] rule name policy_nat_2
HRP_M[DeviceA-policy-nat-policy_nat_2] source-address range 10.3.0.101 10.3.0.150
HRP_M[DeviceA-policy-nat-policy_nat_2] source-zone trust
HRP_M[DeviceA-policy-nat-policy_nat_2] destination-zone untrust
HRP_M[DeviceA-policy-nat-policy_nat_2] action source-nat address-group addressgroup2
HRP_M[DeviceA-policy-nat-policy_nat_2] quit
HRP_M[DeviceA-policy-nat] quit
```

Step 8 Configure default routes for intranet PCs, so that traffic from department A is forwarded through DeviceA and traffic from department B is forwarded through DeviceB when both devices work properly.

Configure default routes on intranet PCs to set the next hop of department A to the virtual IP address 10.3.0.3 of VRRP group 3 and the next hop of department B to the virtual IP address 10.3.0.4 of VRRP group 4.

Step 9 Configure two static routes on the router. For one static route, set the destination address to an address in the address pool addressgroup1 and the next hop to the virtual IP address 1.1.2.3 of VRRP group 2. For the other static route, set the destination address to an address in the address pool addressgroup2 and the next hop to the virtual IP address 1.1.1.3 of VRRP group 1. If one link fails, traffic can travel along the other link.

You need to contact the ISP network administrator to configure these static routes.

----End

Verifying the Configuration

1. If intranet PCs can access the Internet, the security policies are successfully configured.

 Copyright © Huawei Technologies Co., Ltd.

2. Run the **display nat-policy rule name** *rule-name* command on DeviceA and DeviceB respectively to check the number of times traffic matches the source NAT policy.
3. Run the **display firewall session table** command on DeviceA and DeviceB respectively to search for an entry whose source address is the private address of an intranet PC. If the entry exists and the post-NAT IP address exists in the NAT address pool, the NAT policy is successfully configured. Information in the brackets ([]) is the post-NAT or IP address.

```
HRP_M<DeviceA> display firewall session table
Current Total Sessions : 1
 http  VPN:public --> public  10.3.0.55:2474[1.1.1.4:3761]-->3.3.3.3:80
```

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
 sysname DeviceA
#
 hrp enable
 hrp interface GE0/0/5 remote 10.10.0.2
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 active
#
interface GE0/0/2
 ip address 1.1.2.1 255.255.255.0
 vrrp vrid 2 virtual-ip 1.1.2.3 standby
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 active
 vrrp vrid 4 virtual-ip 10.3.0.4 standby
#
interface GE0/0/5
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/5
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
ip route-static 0.0.0.0 0.0.0.0 1.1.2.254 preference
50
#
nat address-group addressgroup1
 section 0 1.1.1.4 1.1.1.4
nat address-group addressgroup2
 section 1 1.1.2.4 1.1.2.4
#
security-policy
 rule name ha_local_to_dmz
  source-zone dmz
  source-zone local
  destination-zone dmz
  destination-zone local
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec_1
  source-zone trust
  source-address 10.3.2.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name policy_nat_1
```

DeviceB

```
#
 sysname DeviceB
#
 hrp enable
 hrp interface GE0/0/5 remote 10.10.0.1
 hrp mirror session enable
 hrp authentication-key %+%##!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 1.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.1.1.3 standby
#
interface GE0/0/2
 ip address 1.1.2.2 255.255.255.0
 vrrp vrid 2 virtual-ip 1.1.2.3 active
#
interface GE0/0/3
 ip address 10.3.0.2 255.255.255.0
 vrrp vrid 3 virtual-ip 10.3.0.3 standby
 vrrp vrid 4 virtual-ip 10.3.0.4 active
#
interface GE0/0/5
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/5
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254 preference
50
ip route-static 0.0.0.0 0.0.0.0 1.1.2.254
#
nat address-group addressgroup1
 section 0 1.1.1.4 1.1.1.4
nat address-group addressgroup2
 section 1 1.1.2.4 1.1.2.4
#
security-policy
 rule name ha_local_to_dmz
  source-zone dmz
  source-zone local
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
 rule name policy_sec_1
  source-zone trust
  source-address 10.3.2.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name policy_nat_1
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
source-zone trust destination-zone untrust source-address range 10.3.0.51 10.3.0.100 action source-nat address-group addressgroup1 rule name policy_nat_2 source-zone trust destination-zone untrust source-address range 10.3.0.101 10.3.0.150 action source-nat address-group addressgroup2 # return	source-zone trust destination-zone untrust source-address range 10.3.0.51 10.3.0.100 action source-nat address-group addressgroup1 rule name policy_nat_2 source-zone trust destination-zone untrust source-address range 10.3.0.101 10.3.0.150 action source-nat address-group addressgroup2 # return

 Copyright © Huawei Technologies Co., Ltd.

16 CGN

16.1 Web: Example for a Private IPv4 User Traversing the Carrier Network to Access the IPv4 Internet

16.2 CLI: Example for Configuring NAT444

16.3 CLI: Example for Configuring Static Mappings

16.4 CLI: Example for Applying Port Pre-Allocation and Incremental Allocation to a NAT444 Scenario

16.5 Web: Example for Enabling an IPv6 User to Access an IPv4 Server

16.6 CLI: Example for Enabling an IPv6 User to Access an IPv4 Server

16.7 CLI: Example for Enabling an IPv4 User to Access an IPv6 Server

16.8 CLI: Example for Applying Port Pre-Allocation and Incremental Allocation to a NAT64 Scenario

16.9 CLI: Example for Configuring an IPv6 User in a Virtual System to Access an IPv4 Server

16.10 CLI: Example for Configuring an IPv4 User in a Virtual System to Access an IPv6 Server

16.11 CLI: Example for Configuring a Public IPv4 Network User to Access a Private IPv6 Network Server (Access from the Public System to a Virtual System)

16.12 CLI: Example for Configuring a Private IPv6 Network User to Access a Public IPv4 Network Server (Access from a Virtual System to the Public System)

16.13 CLI: Example for Configuring an IPv6 User on a Private Network to Access an IPv4 Server on Another Private Network (Access Between Virtual Systems)

16.1 Web: Example for a Private IPv4 User Traversing the Carrier Network to Access the IPv4 Internet

Networking Requirements

Carrier A has insufficient public IPv4 addresses, and therefore its internal MAN uses private IPv4 addresses. To enable IPv4 users connected to the MAN to access

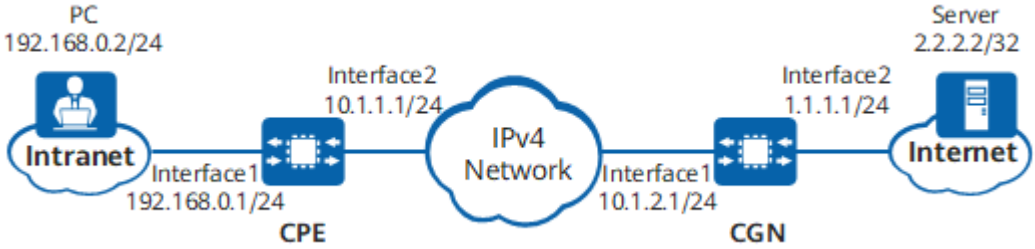
 Copyright © Huawei Technologies Co., Ltd.

the IPv4 Internet, NAT needs to be performed on the CPE and CGN devices separately, as shown in **Figure 16-1**.

Figure 16-1 NAT444 networking diagram

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item		Data
CPE	GE 0/0/1	Security zone: Trust
	GE 0/0/2	Security zone: Untrust
	NAT	Translation mode: Easy IP Outbound interface: GE 0/0/2
CGN	GE 0/0/1	Security zone: Trust
	GE 0/0/2	Security zone: Untrust
	NAT	Translation mode: NAPT Address pool: 1.1.1.11-1.1.1.20

Configuration Roadmap

1. Complete basic configurations on the CPE, including setting interface IP addresses and adding the interfaces to security zones.
2. Configure a NAT policy on the CPE to translate users' private address to carrier's private address.
3. Complete basic configurations on the CGN device, including setting interface IP addresses and adding the interfaces to security zones.
4. Configure a NAT policy on the CGN device to translate carrier's private addresses to public addresses so that private network users can access the Internet.

Procedure

- Configure the CPE.
  a. Configure interface addresses and add the interfaces to security zones.
     i. Choose **Network** > **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

ii. In **Interface List**, click of GE 0/0/2 and set the following parameters.

Zone	untrust
IPv4	
IP Address	10.1.1.1/24

iii. In **Interface List**, click on the line of GE 0/0/1 and set the following parameters.

Zone	trust
IPv4	
IP Address	192.168.0.1/24

iv. Click **OK**.

b. Configure a security policy.

i. Choose **Policy** > **Security Policy** > **Security Policy**.

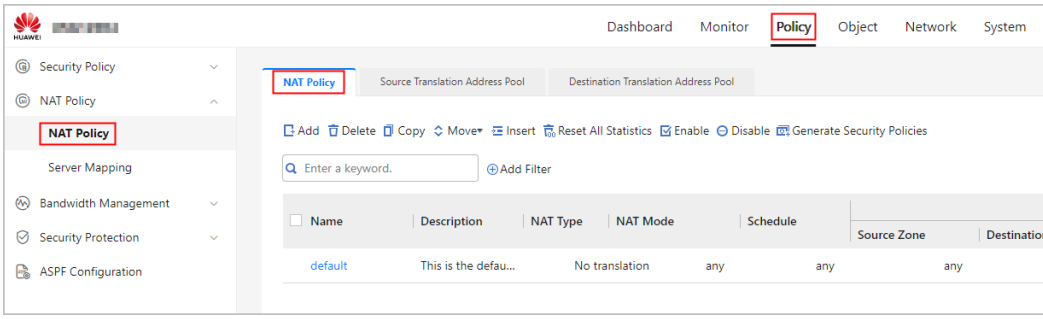
ii. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	security_policy
Source Zone	trust
Destination Zone	untrust
Source Address	192.168.0.0/24
Action	Permit

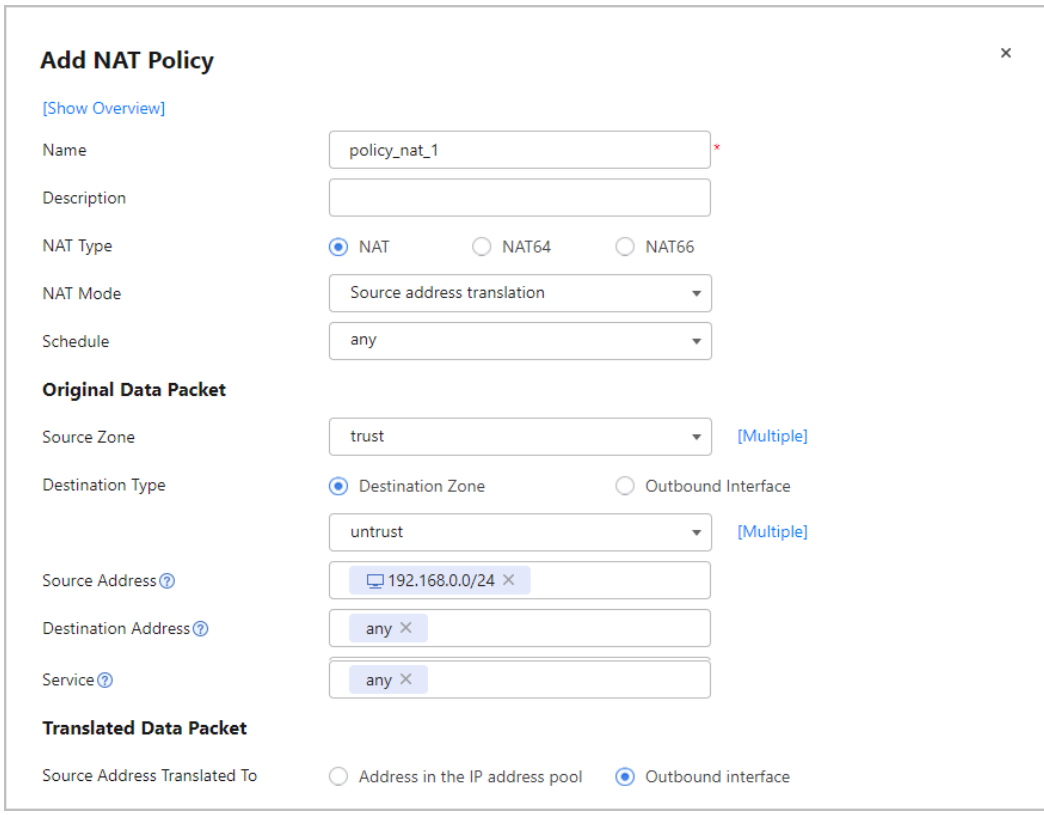
iii. Click **OK**.

c. Configure an outbound source NAT policy to translate users' private addresses to the address on the CPE.

i. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



ii. In **NAT Policy List**, click **Add** and configure a NAT address pool based on the following parameter values.



iii. Click **OK**.

d. Configure a default route. In this example, the next-hop address of the CPE to the carrier MAN is 10.1.1.2.

Choose **Network** > **Route** > **Static Route**, click **Add**, and set the parameters as follows:

Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	10.1.1.2

- Configure the CGN.
  a. Configure interface addresses and add the interfaces to security zones.
     i. Choose **Network** > **Interface**.
     ii. In **Interface List**, click on the line of GE 0/0/2 and set the following parameters.

Zone	untrust
IPv4	
IP Address	1.1.1.1/24

     iii. In **Interface List**, click on the line of GE 0/0/1 and set the following parameters.

 Copyright © Huawei Technologies Co., Ltd.

Zone	trust
IPv4	
IP Address	10.1.2.1/24

iv. Click **OK**.

b. Configure a security policy.

i. Choose **Policy** > **Security Policy** > **Security Policy**.

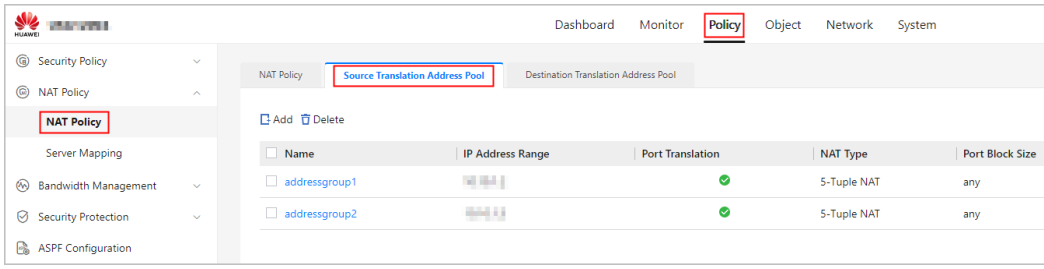
ii. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	security_policy
Source Zone	trust
Destination Zone	untrust
Source Address	10.1.1.0/24 This source IP address is the NAT-translated IP address segment of the outbound interface on the CPE side.
Action	Permit

iii. Click **OK**.

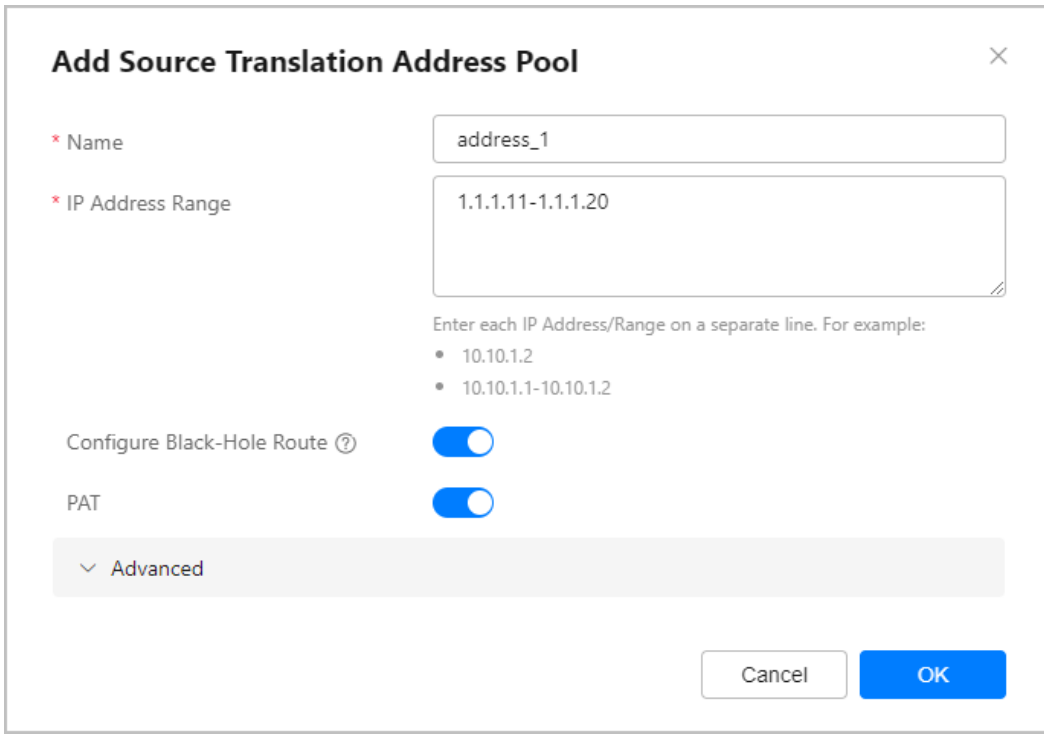
c. Configure a source NAT policy to translate carrier's private addresses to public addresses, enabling private network users to access the Internet.

i. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.



ii. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.

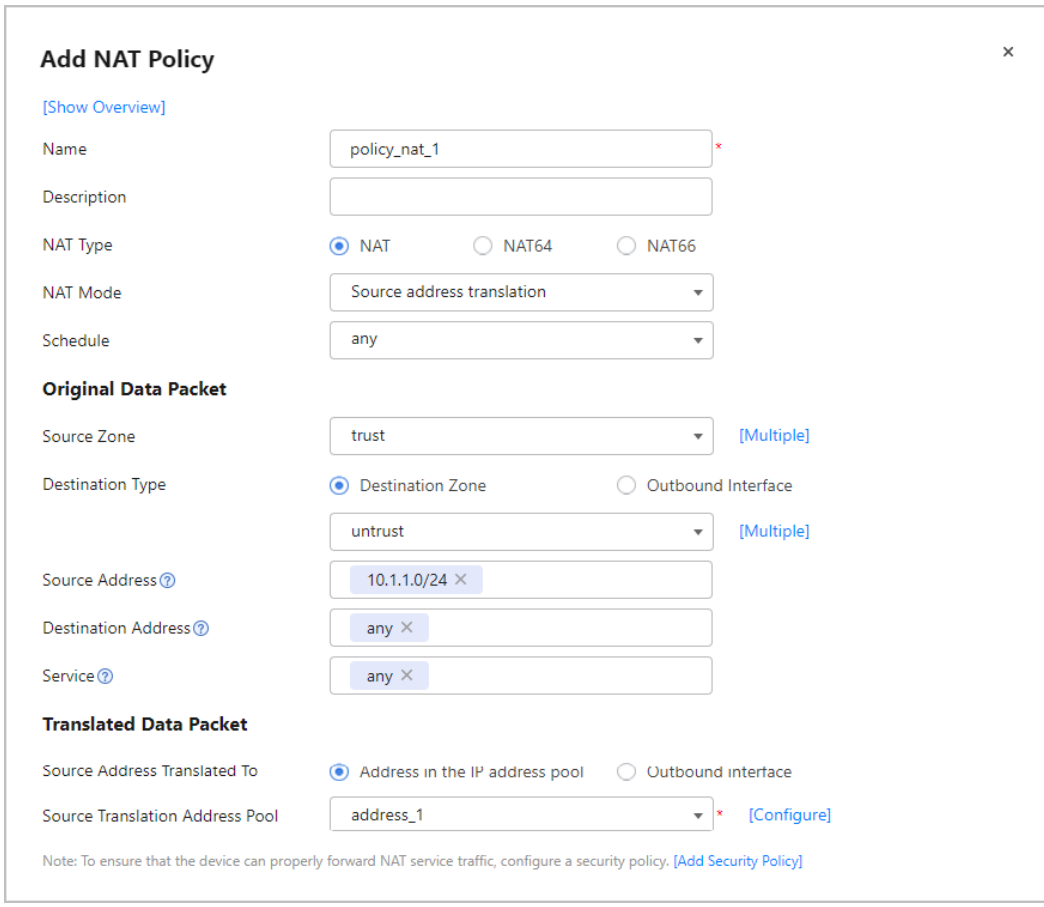


iii. Click **OK**.

iv. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.

v. In **NAT Policy List**, click **Add** and configure a NAT policy based on the following parameter values.

 Copyright © Huawei Technologies Co., Ltd.



vi. Click **OK**.

d. Configure route.

In this example, the next hop address of the CGN to the Internet is 1.1.1.2.

Choose **Network** > **Route** > **Static Route**, click **Add**, and set the parameters as follows:

Destination Address/Mask	0.0.0.0/0.0.0.0
Next Hop	1.1.1.2

In this example, the next hop address of the CGN to the CPE is 10.1.2.2.

Choose **Network** > **Route** > **Static Route**, click **Add**, and set the parameters as follows:

Destination Address/Mask	10.1.1.1/255.255.255.255
Next Hop	10.1.2.2

 Copyright © Huawei Technologies Co., Ltd.

- Configure the server.
  - Set the IP address of the server to 2.2.2.2/32.
  - The route to addresses in the address pool of the CGN must be configured on the server.
- Configure the PC.

  Configure the PC address and specify a gateway. The configuration methods of PC addresses and routes vary with the PC operating systems. Therefore, the configuration methods are not described here.

----End

Verifying the Configuration

1. Verify that intranet PCs can access the server.
2. View the session table on the CPE side.

   Choose **Monitor** > **Session Table** to verify that the sessions whose source addresses are the private IP addresses of the intranet PCs are displayed.
3. View the session table on the CGN side.

   Choose **Monitor** > **Session Table** to verify that the session whose source address is 10.1.1.1 is displayed.

Configuration Scripts

- CPE

```
#
 sysname CPE
#
interface GE 0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GE 0/0/1
 ip address 192.168.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.0.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.0.0 24
    action source-nat easy-ip
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

- CGN device

```
#
 sysname CGN
#
interface GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/1
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
 ip route-static 10.1.1.1 255.255.255.255 10.1.2.2
#
nat address-group address_1
 mode pat
 route enable
 section 0 1.1.1.11 1.1.1.20
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group address_1
#
return
```

16.2 CLI: Example for Configuring NAT444

Networking Requirements

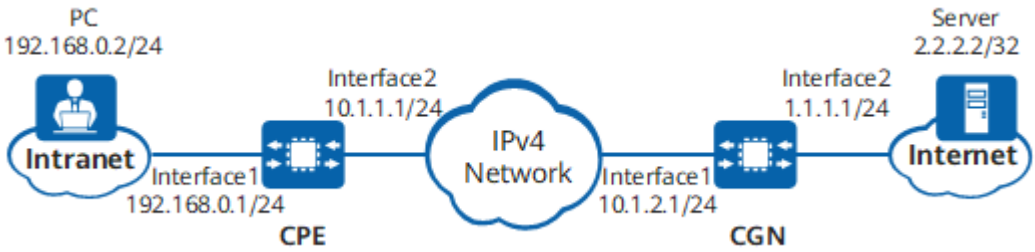
Carrier A has insufficient public IPv4 addresses, and therefore its internal MAN uses private IPv4 addresses. To enable IPv4 users connected to the MAN to access the IPv4 Internet, NAT needs to be performed on the CPE and CGN devices separately, as shown in **Figure 16-2**.

Figure 16-2 NAT444 networking diagram

NOTE

In this example, interfaces 1 and 2 represent GE0/0/1 and GE0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

1. Complete basic configurations on the CPE, including setting interface IP addresses and adding the interfaces to security zones.
2. Configure a NAT policy on the CPE to translate users' private address to carrier's private address.
3. Complete basic configurations on the CGN device, including setting interface IP addresses and adding the interfaces to security zones.
4. Configure a NAT policy on the CGN device to translate carrier's private addresses to public addresses so that private network users can access the Internet.

Procedure

- Configure the CPE.
  a. Configure interface addresses and add the interfaces to security zones.

     # Configure an IP address for GE0/0/2.

     ```
     <HUAWEI> system-view
     [HUAWEI] sysname CPE
     [CPE] interface ge 0/0/2
     [CPE-GE0/0/2] ip address 10.1.1.1 255.255.255.0
     [CPE-GE0/0/2] quit
     [CPE] firewall zone untrust
     [CPE-zone-untrust] add interface ge 0/0/2
     [CPE-zone-untrust] quit
     ```

     # Configure an IP address for GE0/0/1.

     ```
     [CPE] interface ge 0/0/1
     [CPE-GE0/0/1] ip address 192.168.0.1 255.255.255.0
     [CPE-GE0/0/1] quit
     [CPE] firewall zone trust
     [CPE-zone-trust] add interface ge 0/0/1
     [CPE-zone-trust] quit
     ```

  b. Configure a security policy.

     ```
     [CPE] security-policy
     [CPE-policy-security] rule name policy_sec_1
     [CPE-policy-security-rule-policy_sec_1] source-zone trust
     [CPE-policy-security-rule-policy_sec_1] destination-zone untrust
     [CPE-policy-security-rule-policy_sec_1] source-address 192.168.0.0 24
     [CPE-policy-security-rule-policy_sec_1] action permit
     [CPE-policy-security-rule-policy_sec_1] quit
     [CPE-policy-security] quit
     ```

  c. Configure an outbound source NAT policy to translate users' private addresses to the GE0/0/2 address on the CPE.

     ```
     [CPE] nat-policy
     [CPE-policy-nat] rule name policy_nat_1
     ```

 Copyright © Huawei Technologies Co., Ltd.

```
[CPE-policy-nat-rule-policy_nat_1] source-zone trust
[CPE-policy-nat-rule-policy_nat_1] destination-zone untrust
[CPE-policy-nat-rule-policy_nat_1] source-address 192.168.0.0 24
[CPE-policy-nat-rule-policy_nat_1] action source-nat easy-ip
[CPE-policy-nat-rule-policy_nat_1] quit
[CPE-policy-nat] quit
```

d. Configure a default route. In this example, the next hop address in the route from the CPE to the carrier MAN is 10.1.1.2.

```
[CPE] ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
```

- Configure the CGN device.

a. Configure interface addresses and add the interfaces to security zones.

Configure an IP address for GE0/0/2.

```
<HUAWEI> system-view
[HUAWEI] sysname CGN
[CGN] interface ge 0/0/2
[CGN-GE0/0/2] ip address 1.1.1.1 255.255.255.0
[CGN-GE0/0/2] quit
[CGN] firewall zone untrust
[CGN-zone-untrust] add interface ge 0/0/2
[CGN-zone-untrust] quit
```

Configure an IP address for GE0/0/1.

```
[CGN] interface ge 0/0/1
[CGN-GE0/0/1] ip address 10.1.2.1 255.255.255.0
[CGN-GE0/0/1] quit
[CGN] firewall zone trust
[CGN-zone-trust] add interface ge 0/0/1
[CGN-zone-trust] quit
```

b. Configure a security policy.

```
[CGN] security-policy
[CGN-policy-security] rule name policy_sec_1
[CGN-policy-security-rule-policy_sec_1] source-zone trust
[CGN-policy-security-rule-policy_sec_1] destination-zone untrust
[CGN-policy-security-rule-policy_sec_1] source-address 10.1.1.0 24
[CGN-policy-security-rule-policy_sec_1] action permit
[CGN-policy-security-rule-policy_sec_1] quit
[CGN-policy-security] quit
```

c. Configure a source NAT policy to translate carrier's private addresses to public addresses, enabling private network users to access the Internet.

Configure an address pool. Enable port translation for reuse of public addresses.

```
[CGN] nat address-group address_1
[CGN-address-group-address_1] mode pat
[CGN-address-group-address_1] route enable
[CGN-address-group-address_1] section 0 1.1.1.11 1.1.1.20
[CGN-address-group-address_1] quit
```

Configure a NAT policy.

```
[CGN] nat-policy
[CGN-policy-nat] rule name policy_nat_1
[CGN-policy-nat-rule-policy_nat_1] source-zone trust
[CGN-policy-nat-rule-policy_nat_1] destination-zone untrust
[CGN-policy-nat-rule-policy_nat_1] source-address 10.1.1.0 24
[CGN-policy-nat-rule-policy_nat_1] action source-nat address-group address_1
[CGN-policy-nat-rule-policy_nat_1] quit
[CGN-policy-nat] quit
```

d. Configure a default route.

 Copyright © Huawei Technologies Co., Ltd.

In this example, the next hop address in the route from the CGN device to the Internet is 1.1.1.2.

```
[CGN] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

In this example, the next hop address in the route from the CGN device to the CPE is 10.1.2.2.

```
[CGN] ip route-static 10.1.1.1 255.255.255.255 10.1.2.2
```

- Configure the server.
  - Set the IP address of the server to 2.2.2.2/32.
  - On the server, configure routes to addresses in the address pool of the CGN device.
- Configure the PC.

  Configure an IP address for the PC and specify a gateway. The configuration methods of PC addresses and routes vary according to the PC operating systems.

----End

Verifying the Configuration

1. Check whether an intranet PC can access the Server properly.
2. Run the **display nat-policy rule name** *rule-name* command on the CPE and CGN to check the number of times that the source NAT policy is matched. If the number is greater than or equal to 1, there are data flows matching the NAT policy.
3. Run the **display firewall session table** command on the CPE to check the NAT translation entry with the source address being the private address of the intranet PC. If the entry exists and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy is configured successfully. The content contained in square brackets ([]) indicates the post-NAT IP address and port number.

   ```
   <DeviceA> display firewall session table
   Current Total Sessions : 1
    http  VPN:public --> public  192.168.0.2:2474[10.1.1.1:2474]-->2.2.2.2:80
   ```
4. Run the **display firewall session table** command on the CGN to check the NAT translation entry with the source address being the private address of the intranet PC. If the entry exists and the post-NAT IP address is an IP address in the NAT address pool, the NAT policy is configured successfully. The content contained in square brackets ([]) indicates the post-NAT IP address and port number.

   ```
   <DeviceA> display firewall session table
   Current Total Sessions : 1
    http  VPN:public --> public  10.1.1.1:2581[1.1.1.11:2581]-->2.2.2.2:80
   ```

Configuration Scripts

- CPE

  ```
  #
   sysname CPE
  #
  interface GE0/0/2
   ip address 10.1.1.1 255.255.255.0
  #
  interface GE0/0/1
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 192.168.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.0.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.0.0 24
    action source-nat easy-ip
#
return
```

- CGN device

```
#
 sysname CGN
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
 ip route-static 10.1.1.1 255.255.255.255 10.1.2.2
#
nat address-group address_1
 mode pat
 route enable
 section 0 1.1.1.11 1.1.1.20
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group address_1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

16.3 CLI: Example for Configuring Static Mappings

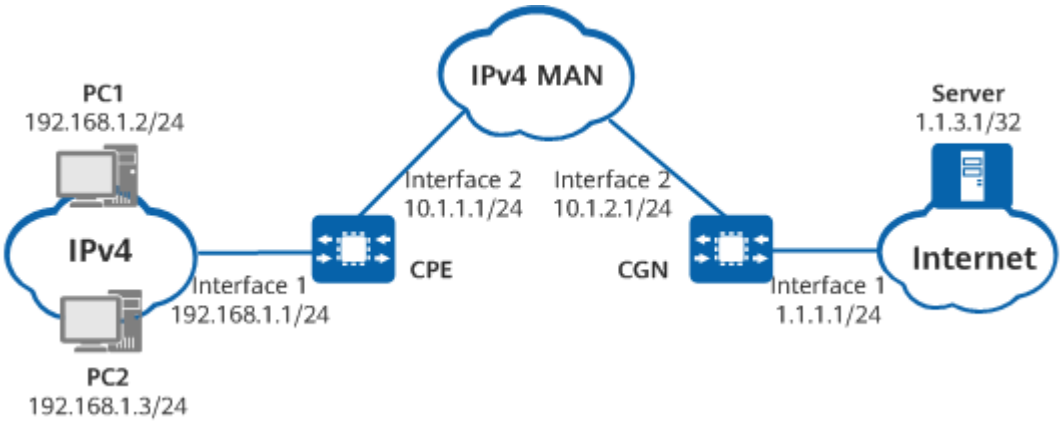
Networking Requirements

In this example, the NMS on carrier A's network fails to deliver commands to a CGN device due to an NMS fault. As such, static mappings among public addresses, private addresses, and port ranges can be configured on the CGN device using commands to implement address translation, enabling users on private networks to access the public network. **Figure 16-3** shows the network planning.

Figure 16-3 Networking diagram for configuring static mappings

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Item		Data	Remarks
CPE	GE 0/0/1	Private IPv4 address: 192.168.1.1/24 Security zone: Trust	Interface connected to users on the IPv4 private network.
	GE 0/0/2	Private IPv4 address assigned by the carrier: 10.1.1.1/24 Security zone: Untrust	Interface connected to the MAN of the carrier. Assume that the next-hop address from the CPE to the MAN is 10.1.1.2.
	Address pool	Post-NAT address: address of GE 0/0/2	Users' private IPv4 addresses are translated into the private IPv4 addresses assigned by the carrier.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Remarks
CGN	GE 0/0/1	Public IPv4 address: 1.1.1.1/24 Security zone: Untrust	Interface connected to the IPv4 Internet. Assume that the next-hop address from the CGN device to the Internet is 1.1.1.2/24.
	GE 0/0/2	Private IPv4 address assigned by the carrier: 10.1.2.1/24 Security zone: Trust	Interface connected to the MAN of the carrier. Assume that the next-hop address from the CGN device to the MAN is 10.1.2.2.
	Static mapping 1	Private address pool: 10.1.1.1 to 10.1.1.10 Public address pool: 1.1.2.6 to 1.1.2.10 Available ports: 2048 to 4095 Number of ports in a port range: 256 Static mapping mode: 5-tuple NAT	Used to translate the carrier's private IPv4 addresses into public IPv4 addresses.
	Static mapping 2	Private address pool: 10.1.1.11 to 10.1.1.20 Public address pool: 1.1.2.11 to 1.1.2.15 Available ports: 2048 to 4095 Number of ports in a port range: 256 Static mapping mode: 5-tuple NAT	Used to translate the carrier's private IPv4 addresses into public IPv4 addresses.
PC1		Private IPv4 address: 192.168.1.2/24	–
PC2		Private IPv4 address: 192.168.1.3/24	–
Server on the Internet		Public IPv4 address: 1.1.3.1/32	–

Procedure

- Configure the CPE.
  a. Configure IP addresses for interfaces and add them to security zones.

     # Configure an IP address for GE 0/0/1 and add it to the Trust zone.

     ```
     <HUAWEI> system-view
     [HUAWEI] sysname CPE
     ```

 Copyright © Huawei Technologies Co., Ltd.

```
[CPE] interface ge 0/0/1
[CPE-GE0/0/1] ip address 192.168.1.1 255.255.255.0
[CPE-GE0/0/1] quit
[CPE] firewall zone trust
[CPE-zone-trust] add interface ge 0/0/1
[CPE-zone-trust] quit
```

Configure an IP address for GE 0/0/2 and add it to the Untrust zone.

```
[CPE] interface ge 0/0/2
[CPE-GE0/0/2] ip address 10.1.1.1 255.255.255.0
[CPE-GE0/0/2] quit
[CPE] firewall zone untrust
[CPE-zone-untrust] add interface ge 0/0/2
[CPE-zone-untrust] quit
```

b. Configure a security policy.

```
[CPE] security-policy
[CPE-policy-security] rule name policy_sec_1
[CPE-policy-security-rule-policy_sec_1] source-zone trust
[CPE-policy-security-rule-policy_sec_1] destination-zone untrust
[CPE-policy-security-rule-policy_sec_1] source-address 192.168.1.0 24
[CPE-policy-security-rule-policy_sec_1] action permit
[CPE-policy-security-rule-policy_sec_1] quit
[CPE-policy-security] quit
```

c. Configure a source NAT policy to translate users' private addresses into the address of the outbound interface GE 0/0/2 on the CPE.

```
[CPE] nat-policy
[CPE-policy-nat] rule name policy_nat_1
[CPE-policy-nat-rule-policy_nat_1] source-zone trust
[CPE-policy-nat-rule-policy_nat_1] destination-zone untrust
[CPE-policy-nat-rule-policy_nat_1] source-address 192.168.1.0 24
[CPE-policy-nat-rule-policy_nat_1] action source-nat easy-ip
[CPE-policy-nat-rule-policy_nat_1] quit
[CPE-policy-nat] quit
```

d. Configure a static IPv4 route.

Configure a static IPv4 route to the CGN device, with the next-hop address set to 10.1.1.2.

```
[CPE] ip route-static 10.1.2.0 255.255.255.0 10.1.1.2
```

- Configure the CGN device.
  a. Configure the hash mode for selecting the CPU to be based only on source IP addresses.

```
<HUAWEI> system-view
[HUAWEI] sysname CGN
[CGN] firewall hash-mode source-only
```

NOTE

The new hash mode takes effect only after the device is restarted.

Source IP address-based hash mode needs to be configured only on USG6700F series.

b. Configure IP addresses for interfaces and add them to security zones.

Configure an IP address for GE 0/0/1 and add it to the Untrust zone.

```
[CGN] interface ge 0/0/1
[CGN-GE0/0/1] ip address 1.1.1.1 255.255.255.0
[CGN-GE0/0/1] quit
[CGN] firewall zone untrust
[CGN-zone-untrust] add interface ge 0/0/1
[CGN-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure an IP address for GE 0/0/2 and add it to the Trust zone.

```
[CGN] interface ge 0/0/2
[CGN-GE0/0/2] ip address 10.1.2.1 255.255.255.0
[CGN-GE0/0/2] quit
[CGN] firewall zone trust
[CGN-zone-trust] add interface ge 0/0/2
[CGN-zone-trust] quit
```

Configure a security policy.

```
[CGN] security-policy
[CGN-policy-security] rule name policy_sec_1
[CGN-policy-security-rule-policy_sec_1] source-zone trust
[CGN-policy-security-rule-policy_sec_1] destination-zone untrust
[CGN-policy-security-rule-policy_sec_1] source-address 10.1.1.0 24
[CGN-policy-security-rule-policy_sec_1] action permit
[CGN-policy-security-rule-policy_sec_1] quit
[CGN-policy-security] quit
```

c. Configure static mappings to translate the carrier's private IPv4 addresses into public IPv4 addresses.

Enter the static mapping view.

```
[CGN] nat static-mapping
```

NOTE

The **nat static-mapping** command supports configuration only when the hash-based mode is source-only hash mode.

The **firewall hash-mode** command configures the hash-based mode to select a CPU that processes service packets. With the **realtime** parameter configured, the changed hash-based mode takes effect without restarting the device.

After the hash-based mode is changed and takes effect immediately, NAT, IPsec, and forwarding services are temporarily interrupted. After the sessions of these services are reestablished, the services are automatically restored.

Configure private address pools.

```
[CGN-nat-static] inside-ipv4-pool 1
[CGN-nat-static-inside-ipv4-pool-1] section 1 10.1.1.1 10.1.1.10
[CGN-nat-static-inside-ipv4-pool-1] quit
[CGN-nat-static] inside-ipv4-pool 2
[CGN-nat-static-inside-ipv4-pool-2] section 2 10.1.1.11 10.1.1.20
[CGN-nat-static-inside-ipv4-pool-2] quit
```

Configure public address pools.

```
[CGN-nat-static] global-pool 1
[CGN-nat-static-global-pool-1] section 1 1.1.2.6 1.1.2.10
[CGN-nat-static-global-pool-1] route enable
[CGN-nat-static-global-pool-1] quit
[CGN-nat-static] global-pool 2
[CGN-nat-static-global-pool-2] section 2 1.1.2.11 1.1.2.15
[CGN-nat-static-global-pool-2] route enable
[CGN-nat-static-global-pool-2] quit
```

Configure static mappings.

```
[CGN-nat-static] static-mapping 1 inside-ipv4-pool 1 global-pool 1 port-range 2048 4095 port-block-size 256 ip-first
[CGN-nat-static] static-mapping 2 inside-ipv4-pool 2 global-pool 2 port-range 2048 4095 port-block-size 256 ip-first
[CGN-nat-static] quit
```

Apply static mappings to the NAT policy.

 Copyright © Huawei Technologies Co., Ltd.

```
[CGN] nat-policy
[CGN-policy-nat] rule name policy_nat_1
[CGN-policy-nat-rule-policy_nat_1] source-address range 10.1.1.1 10.1.1.10
[CGN-policy-nat-rule-policy_nat_1] source-zone trust
[CGN-policy-nat-rule-policy_nat_1] destination-zone untrust
[CGN-policy-nat-rule-policy_nat_1] action source-nat static-mapping 1
[CGN-policy-nat-rule-policy_nat_1] quit
[CGN-policy-nat] rule name policy_nat_2
[CGN-policy-nat-rule-policy_nat_2] source-address range 10.1.1.11 10.1.1.20
[CGN-policy-nat-rule-policy_nat_2] source-zone trust
[CGN-policy-nat-rule-policy_nat_2] destination-zone untrust
[CGN-policy-nat-rule-policy_nat_2] action source-nat static-mapping 2
[CGN-policy-nat-rule-policy_nat_2] quit
[CGN-policy-nat] quit
```

d. Configure static IPv4 routes.

Configure a static IPv4 route to the CPE, with the next-hop address set to 10.1.2.2.

```
[CGN] ip route-static 10.1.1.0 255.255.255.0 10.1.2.2
```

Configure a static IPv4 route to the server on the Internet, with the next-hop address set to 1.1.1.2.

```
[CGN] ip route-static 1.1.3.1 255.255.255.255 1.1.1.2
```

- Configure the server on the Internet.

  The server on the Internet is typically configured by the carrier. This section describes only the following key points for the server configuration:

  Configure IP address 1.1.3.1/32 for the server, and ensure that the server has reachable routes to the addresses in the address pools on the CGN device.
- Configure PC1 and PC2 on the internal network.

  Configure the gateway address to 192.168.1.1 for PC1 and PC2.

----End

Verifying the Configuration

1. After completing the preceding configurations, you can ping the IP address of the server on the Internet from PC1.

```
C:\Documents and Settings\Administrator>ping 1.1.3.1

Pinging 1.1.3.1 with 32 bytes of data:

Reply from 1.1.3.1: bytes=32 time=9ms TTL=253
Reply from 1.1.3.1: bytes=32 time<1ms TTL=253
Reply from 1.1.3.1: bytes=32 time<1ms TTL=253
Reply from 1.1.3.1: bytes=32 time<1ms TTL=253

Ping statistics for 1.1.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms
```

2. Run the **display cpe-user information cpe-ipv4 10.1.1.1** command in any view on the CGN device to check details of the CPE using 10.1.1.1.

```
[CGN] display cpe-user information cpe-ipv4 10.1.1.1 slot 0 cpu 0
 This operation will take a few minutes. Press 'Ctrl+C' to
break ...
 UserTbl item(s) on slot 0 cpu 0
 ------------------------------------------------------------------------
 Scene: NAT444  DstZone: untrust  CPEIP:
10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 TTL: 40   LeftTime: 37 Increase Count: 0  VPN:
public
 StaticMapping ID: 1 PublicIP: 1.1.2.6  StartPort:
2048
 PortNumber: 256  PortTotal: 256  Used Port Number:
0
```

As shown in the preceding command output, the CPE address 10.1.1.1 is translated into the public address 1.1.2.6 through the static mapping. The start port number is 2048, which is the same as that in the configuration.

3. Run the **display nat static-mapping 1 inside-ipv4 10.1.1.1** command in any view on the CGN device to check the static mapping configuration.

```
[CGN] display nat static-mapping 1 inside-ipv4 10.1.1.1
slot: 0  cpu: 0  static-mapping id: 1
mapping: 10.1.1.1 -> 1.1.2.6 [ 2048 2303 ]
```

As shown in the preceding command output, the CPE address 10.1.1.1 is translated into the public address 1.1.2.6 through the static mapping, and the port range is from 2048 to 2303 (total of 256 ports).

4. Ping the IP address of the server on the Internet from PC2. Run the **display cpe-user information cpe-ipv4 10.1.1.1** and **display nat static-mapping 1 inside-ipv4 10.1.1.1** commands in any view on the CGN to check details of the CPE using 10.1.1.1 and to check the static mapping configuration, respectively. The post-NAT address (1.1.2.6) and the port range (2048 to 2303) are the same as those in the preceding command outputs.

Configuration Scripts

- CPE

```
#
 sysname CPE
#
interface GE0/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 10.1.2.0 255.255.255.0 10.1.1.2
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.1.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.1.0 24
    action source-nat easy-ip
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

- CGN

```
#
 sysname CGN
#
 firewall hash-mode source-only
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 10.1.1.0 255.255.255.0 10.1.2.2
 ip route-static 1 1.3.1.255.255.255.255 1.1.1.2
#
nat static-mapping
 inside-ipv4-pool 1
  section 1 10.1.1.1 10.1.1.10
 global-pool 1
  section 1 1.1.2.6 1.1.2.10
  route enable
 static-mapping 1 inside-ipv4-pool 1 global-pool 1 port-range 2048 4095 port-block-size 256 ip-first
 inside-ipv4-pool 2
  section 2 10.1.1.11 10.1.1.20
 global-pool 2
  section 2 1.1.2.11 1.1.2.15
  route enable
 static-mapping 2 inside-ipv4-pool 2 global-pool 2 port-range 2048 4095 port-block-size 256 ip-first
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-address range 10.1.1.1 10.1.1.10
    source-zone trust
    destination-zone untrust
    action source-nat static-mapping 1
  rule name policy_nat_2
    source-address range 10.1.1.11 10.1.1.20
    source-zone trust
    destination-zone untrust
    action source-nat static-mapping 2
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

16.4 CLI: Example for Applying Port Pre-Allocation and Incremental Allocation to a NAT444 Scenario

Networking Requirements

To adapt to network development, carrier A needs to plan the network segment to:

- Save public address resources.
- Properly allocate ports.
- Facilitate user address obtaining.

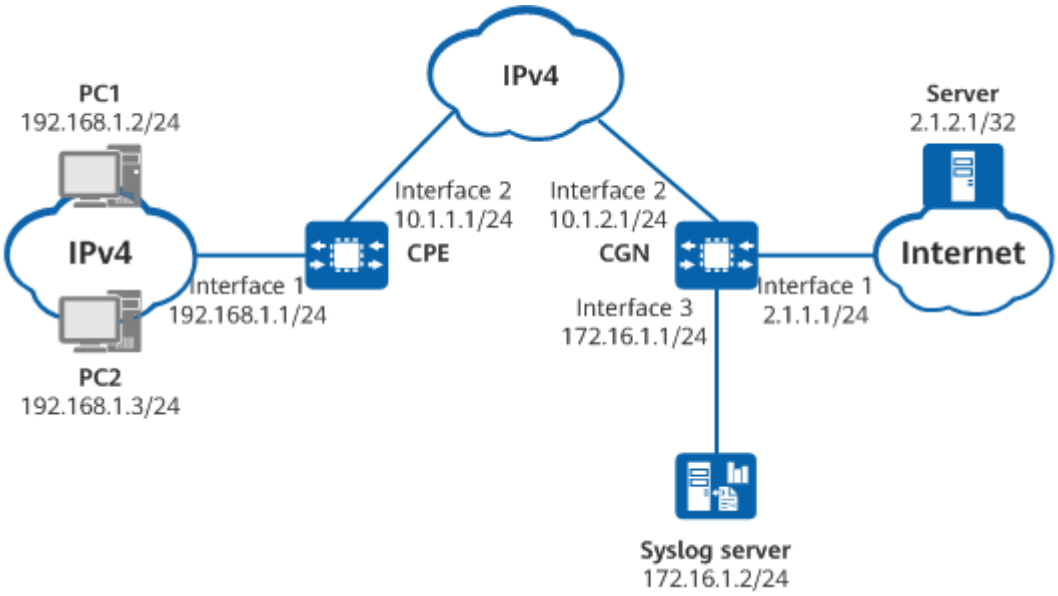
The carrier uses the network plan shown in **Figure 16-4** to meet the preceding requirements. Its network plan is as follows:

- To save public IPv4 addresses, allocate private addresses to IPv4 users, and configure 2-level NAT on the CPE and CGN device to enable users on the private IPv4 network to access the IPv4 Internet.
- To properly allocate ports, configure a NAT policy on the CGN device to provide the port pre-allocation and incremental allocation functions, enabling service traffic from the CPE to use the pre-allocated or incrementally allocated ports.
- To obtain user address information, configure the syslog server to interwork with the CGN device. The CGN device generates logs upon port allocation and release, and sends the logs to the syslog server that parses the logs to obtain source addresses and port ranges to obtain user address information.

Figure 16-4 Network diagram of applying port pre-allocation and incremental allocation in a NAT444 scenario

NOTE

In this example, interfaces 1, 2, and 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Remarks
CPE	GE 0/0/1	Private IPv4 address: 192.168.1.1/24 Security zone: Trust	Interface connected to users on the private IPv4 network.
	GE 0/0/2	Private IPv4 address assigned by the carrier: 10.1.1.1/24 Security zone: Untrust	Interface connected to the MAN of the carrier. Assume that the next-hop address from the CPE to the MAN is 10.1.1.2.
	Address pool	Post-NAT address: address of GE 0/0/2	Users' private IPv4 addresses are translated into the private IPv4 addresses assigned by the carrier.
CGN	GE 0/0/1	Public IPv4 address: 2.1.1.1/24 Security zone: Untrust	Interface connected to the IPv4 Internet. Assume that the next-hop address from the CGN device to the Internet is 2.1.1.2/24.
	GE 0/0/2	Private IPv4 address assigned by the carrier: 10.1.2.1/24 Security zone: Trust	Interface connected to the MAN of the carrier. Assume that the next-hop address from the CGN device to the MAN is 10.1.2.2.
	GE 0/0/3	IP address: 172.16.1.1/24 Security zone: DMZ	Interface connected to a syslog server.
	Address pool	Address pool: 1.1.2.1 to 1.1.2.5	Used to translate the carrier's private IPv4 addresses into public IPv4 addresses.
PC1		Private IPv4 address: 192.168.1.2/24	–
PC2		Private IPv4 address: 192.168.1.3/24	–
Internet server		Public IPv4 address: 2.1.2.1/32	–
Syslog server		IPv4 address: 172.16.1.2/24	Parses log packets to obtain user (CPE) address information.

Procedure

- Configure the CPE.
  a. Configure IP addresses for interfaces and add them to security zones.

     # Configure an IP address for GE 0/0/1 and add it to the Trust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
[HUAWEI] sysname CPE
[CPE] interface ge 0/0/1
[CPE-GE0/0/1] ip address 192.168.1.1 255.255.255.0
[CPE-GE0/0/1] quit
[CPE] firewall zone trust
[CPE-zone-trust] add interface ge 0/0/1
[CPE-zone-trust] quit
```

Configure an IP address for GE 0/0/2 and add it to the Untrust zone.

```
[CPE] interface ge 0/0/2
[CPE-GE0/0/2] ip address 10.1.1.1 255.255.255.0
[CPE-GE0/0/2] quit
[CPE] firewall zone untrust
[CPE-zone-untrust] add interface ge 0/0/2
[CPE-zone-untrust] quit
```

b. Configure a security policy.

```
[CPE] security-policy
[CPE-policy-security] rule name policy_sec_1
[CPE-policy-security-rule-policy_sec_1] source-zone trust
[CPE-policy-security-rule-policy_sec_1] destination-zone untrust
[CPE-policy-security-rule-policy_sec_1] source-address 192.168.1.0 24
[CPE-policy-security-rule-policy_sec_1] action permit
[CPE-policy-security-rule-policy_sec_1] quit
[CPE-policy-security] quit
```

c. Configure a NAT policy to translate users' private IPv4 addresses into the CPE's private IPv4 address assigned by the carrier.

```
[CPE] nat-policy
[CPE-policy-nat] rule name policy_nat_1
[CPE-policy-nat-rule-policy_nat_1] source-zone trust
[CPE-policy-nat-rule-policy_nat_1] destination-zone untrust
[CPE-policy-nat-rule-policy_nat_1] source-address 192.168.1.0 24
[CPE-policy-nat-rule-policy_nat_1] action source-nat easy-ip
[CPE-policy-nat-rule-policy_nat_1] quit
[CPE-policy-nat] quit
```

d. Configure a static IPv4 route.

Configure a static IPv4 route to the CGN device, with the next-hop address set to 10.1.1.2.

```
[CPE] ip route-static 10.1.2.0 255.255.255.0 10.1.1.2
```

- Configure the CGN device.

a. Configure the hash mode for selecting the CPU to be based only on source IP addresses.

```
<HUAWEI> system-view
[HUAWEI] sysname CGN
[CGN] firewall hash-mode source-only
```

NOTE

The **port-block-size** command supports configuration only when the hash-based mode is source-only hash mode.

The **firewall hash-mode** command configures the hash-based mode to select a CPU that processes service packets. With the **realtime** parameter configured, the changed hash-based mode takes effect without restarting the device.

After the hash-based mode is changed and takes effect immediately, NAT, IPsec, and forwarding services are temporarily interrupted. After the sessions of these services are reestablished, the services are automatically restored.

b. Configure IP addresses for interfaces and add them to security zones.

Configure an IP address for GE 0/0/1 and add it to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[CGN] interface ge 0/0/1
[CGN-GE0/0/1] ip address 2.1.1.1 255.255.255.0
[CGN-GE0/0/1] quit
[CGN] firewall zone untrust
[CGN-zone-untrust] add interface ge 0/0/1
[CGN-zone-untrust] quit
```

Configure an IP address for GE 0/0/2 and add it to the Trust zone.

```
[CGN] interface ge 0/0/2
[CGN-GE0/0/2] ip address 10.1.2.1 255.255.255.0
[CGN-GE0/0/2] quit
[CGN] firewall zone trust
[CGN-zone-trust] add interface ge 0/0/2
[CGN-zone-trust] quit
```

Configure an IP address for GE 0/0/3 and add it to the DMZ.

```
[CGN] interface ge 0/0/3
[CGN-GE0/0/3] ip address 172.16.1.1 255.255.255.0
[CGN-GE0/0/3] quit
[CGN] firewall zone dmz
[CGN-zone-dmz] add interface ge 0/0/3
[CGN-zone-dmz] quit
```

Configure a security policy.

```
[CGN] security-policy
[CGN-policy-security] rule name policy_sec_1
[CGN-policy-security-rule-policy_sec_1] source-zone trust
[CGN-policy-security-rule-policy_sec_1] destination-zone untrust
[CGN-policy-security-rule-policy_sec_1] source-address 10.1.1.0 24
[CGN-policy-security-rule-policy_sec_1] action permit
[CGN-policy-security-rule-policy_sec_1] quit
[CGN-policy-security] rule name policy_sec_2
[CGN-policy-security-rule-policy_sec_2] source-zone local
[CGN-policy-security-rule-policy_sec_2] destination-zone dmz
[CGN-policy-security-rule-policy_sec_2] destination-address 172.16.1.0 24
[CGN-policy-security-rule-policy_sec_2] action permit
[CGN-policy-security-rule-policy_sec_2] quit
[CGN-policy-security] quit
```

c. Configure a NAT policy to translate CPE's private IPv4 address assigned by the carrier into public IPv4 addresses.

Configure a NAT address pool. Set the size of the pre-allocated port block to 256.

```
[CGN] nat address-group addressgroup1
[CGN-address-group-addressgroup1] route enable
[CGN-address-group-addressgroup1] section 1 1.1.2.1 1.1.2.5
[CGN-address-group-addressgroup1] port-block-size 256
[CGN-address-group-addressgroup1] quit
```

Configure a NAT policy.

```
[CGN] nat-policy
[CGN-policy-nat] rule name policy_nat_1
[CGN-policy-nat-rule-policy_nat_1] source-zone trust
[CGN-policy-nat-rule-policy_nat_1] destination-zone untrust
[CGN-policy-nat-rule-policy_nat_1] source-address 10.1.1.0 24
[CGN-policy-nat-rule-policy_nat_1] action source-nat address-group addressgroup1
[CGN-policy-nat-rule-policy_nat_1] quit
[CGN-policy-nat] quit
```

d. Configure interoperation between the CGN device and the syslog server.

Enable the function of sending syslogs upon port allocation and release.

 Copyright © Huawei Technologies Co., Ltd.

```
[CGN] nat port-block assigning syslog enable
[CGN] nat port-block freeing syslog enable
```

Configure the syslog server.

```
[CGN] nat port-block syslog host 172.16.1.2 source CGN 172.16.1.1 514
```

e. Configure a static IPv4 route.

Configure a static IPv4 route to the CPE, with the next-hop address set to 10.1.2.2.

```
[CGN] ip route-static 10.1.1.0 255.255.255.0 10.1.2.2
```

Configure a static IPv4 route to the server on the Internet, with the next-hop address set to 2.1.1.2.

```
[CGN] ip route-static 2.1.2.1 255.255.255.255 2.1.1.2
```

- Configure the server on the Internet.

  The server on the Internet is typically configured by the carrier. This section describes only the following key points for the server configuration:

  – Configure IP address 2.1.3.1/32 for the server.
  – Ensure that the server has reachable routes to the addresses in the address pools on the CGN device.

- Configure PC1 and PC2 on the internal network.

  Configure the gateway address to 192.168.1.1 for PC1 and PC2.

- Configure the syslog server.

  The configuration varies according to the model of the syslog server. For details, see the product documentation of the syslog server.

----End

Verifying the Configuration

1. After completing the preceding configurations, you can ping the IP address of the server on the Internet from PC1.

```
C:\Documents and Settings\Administrator>ping 2.1.2.1

Pinging 2.1.2.1 with 32 bytes of data:

Reply from 2.1.2.1: bytes=32 time=9ms TTL=253
Reply from 2.1.2.1: bytes=32 time<1ms TTL=253
Reply from 2.1.2.1: bytes=32 time<1ms TTL=253
Reply from 2.1.2.1: bytes=32 time<1ms TTL=253

Ping statistics for 2.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms
```

2. Run the **display cpe-user information cpe-ipv4 10.1.1.1** command in any view on the CGN device to check details of the CPE user using 10.1.1.1.

```
[CGN] display cpe-user information cpe-ipv4 10.1.1.1 slot 0 cpu 0
 This operation will take a few minutes. Press 'Ctrl+C' to break ...
 UserTbl item(s) on slot 0 cpu 0
 ------------------------------------------------------------------------
 Scene: NAT444  DstZone: untrust CPEIP: 10.1.1.1
 TTL: 40   LeftTime: 34 Increase Count: 0  VPN: public
 PoolID: addressgroup1  SectionID: 1  PublicIP: 1.1.2.2  StartPort: 2048
 PortNumber: 256  PortTotal: 256  Used Port Number: 0
```

 Copyright © Huawei Technologies Co., Ltd.

As shown in the command output, the source addresses of service flows sent from the CPE at 10.1.1.1 are translated into 1.1.2.2, and the port range is from 2048 to 2303 (total of 256 ports).

3. Ping the IP address of the server on the Internet from PC2. Run the **display cpe-user information cpe-ipv4 10.1.1.1** command in any view on the CGN device to check details of the CPE user using 10.1.1.1. The command output shows that the post-NAT address and port range remain the same as those in step 2.
4. The syslog server receives a log during port pre-allocation or incremental allocation. The following example shows a syslog in France Telecom format displayed on the syslog server. To change the syslog format, run the **nat port-block syslog descriptive format** command in the system view.

```
NAT444userbased - %%01SEC/6/BIND(l): An initial portrange is assigned, in nat444 scene. privateip='10.1.1.1' srcvrfid='0' publicip='1.1.2.2' publicportrange='2048~2303' time='2012-05-02 18:24:09'.
```

This log is generated upon the initial port re-allocation, and contains the IP address of the CPE, post-NAT public IP address, port range, and timestamp, which are used for user address obtaining.

Configuration Scripts

- CPE

```
#
 sysname CPE
#
interface GE0/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 10.1.2.0 255.255.255.0 10.1.1.2
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.1.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 192.168.1.0 24
    action source-nat easy-ip
#
return
```

- CGN

```
#
 sysname CGN
#
 firewall hash-mode source-only
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/1
 ip address 2.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GE0/0/3
 ip address 172.16.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
 ip route-static 10.1.1.0 255.255.255.0 10.1.2.2
 ip route-static 2.1.2.1 255.255.255.255 2.1.1.2
#
 nat port-block assigning syslog enable
 nat port-block freeing syslog enable
 nat port-block syslog host 172.16.1.2 source CGN 172.16.1.1 514
#
 nat address-group addressgroup1
   port-block-size 256
   route enable
   section 1 1.1.2.1 1.1.2.5
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
  rule name policy_sec_2
    source-zone local
    destination-zone dmz
    source-address destination-address 172.16.1.0 24
    action permit
#
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action source-nat address-group addressgroup1
#
return
```

16.5 Web: Example for Enabling an IPv6 User to Access an IPv4 Server

Networking Requirements

On the network shown in **Figure 16-5**, DeviceA supports the IPv4/IPv6 dual stack and is connected to an IPv6 network and an IPv4 network. The IPv6 network has a large number of PCs using unfixed IP addresses. These PCs need to access the server on the IPv4 network through the domain name example.huawei.com.

 Copyright © Huawei Technologies Co., Ltd.

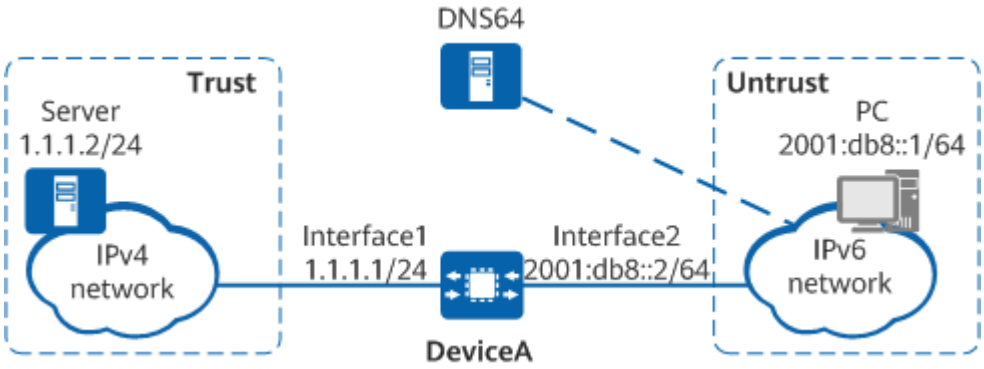
NOTE

When both NAT64 and DNS64 are deployed, configure the same NAT64 prefix and prefix length on the DNS64 and NAT64 devices.

Figure 16-5 Network diagram of dynamic NAT64

NOTE

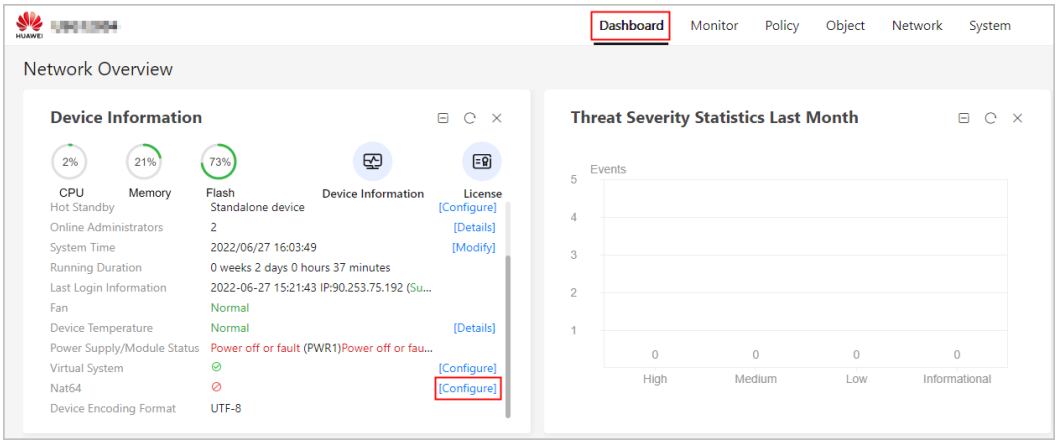
In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

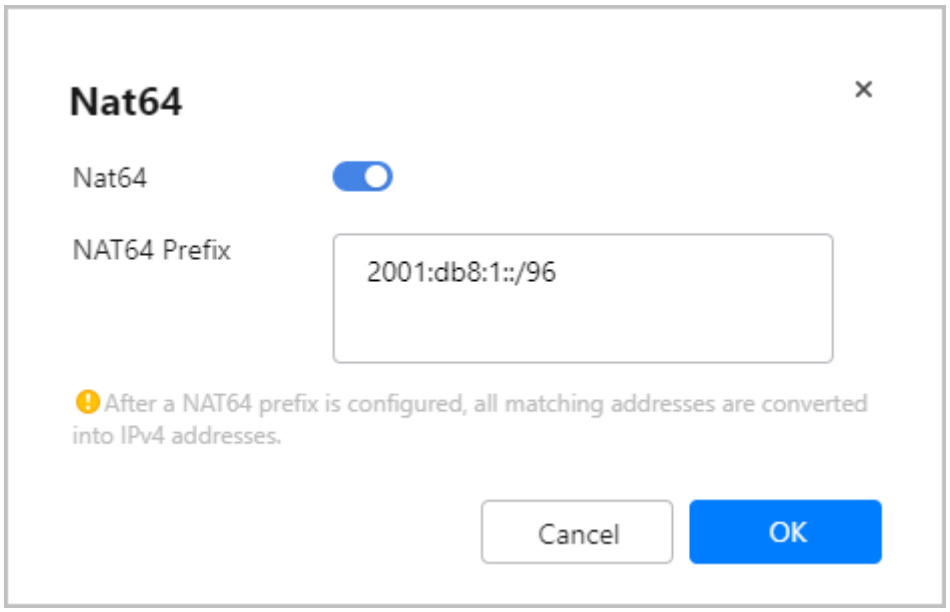
Step 1 Enable NAT64.

1. Choose **Dashboard** > **Device Information**.



2. Click **Configure** on the line of **Nat64** and enable NAT64 function.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

In this example, the NAT64 prefix is 2001:db8:1::/96. If no NAT64 prefix is configured, the well-known prefix is used by default.

3. Click **OK**.

Step 2 Set IP addresses for interfaces and assign the interfaces to security zones.

1. Set the IP address of GE 0/0/1 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click of GE 0/0/1 and set the following parameters.

Zone	trust
IPv4	
IP Address	1.1.1.1/24

   c. Click **OK**.
2. Set the IP address of GE 0/0/2 and assign the interface to a security zone.
   a. Choose **Network** > **Interface**.
   b. In **Interface List**, click on the line of GE 0/0/2 and set the following parameters.

Zone	untrust
IPv6	
IP Address	2001:db8::2/64

   c. Click **OK**.

Step 3 Configure a security policy for traffic between Internet users and intranet servers.

 Copyright © Huawei Technologies Co., Ltd.

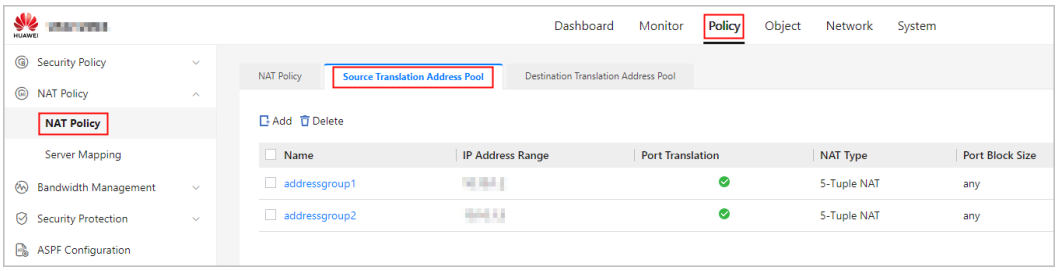
1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add**, select **Add Security Policy**, and configure a security policy based on the following parameter values.

Name	policy_sec_1
Source Zone	untrust
Destination Zone	trust
Source Address	2001:db8::/64
Action	Permit

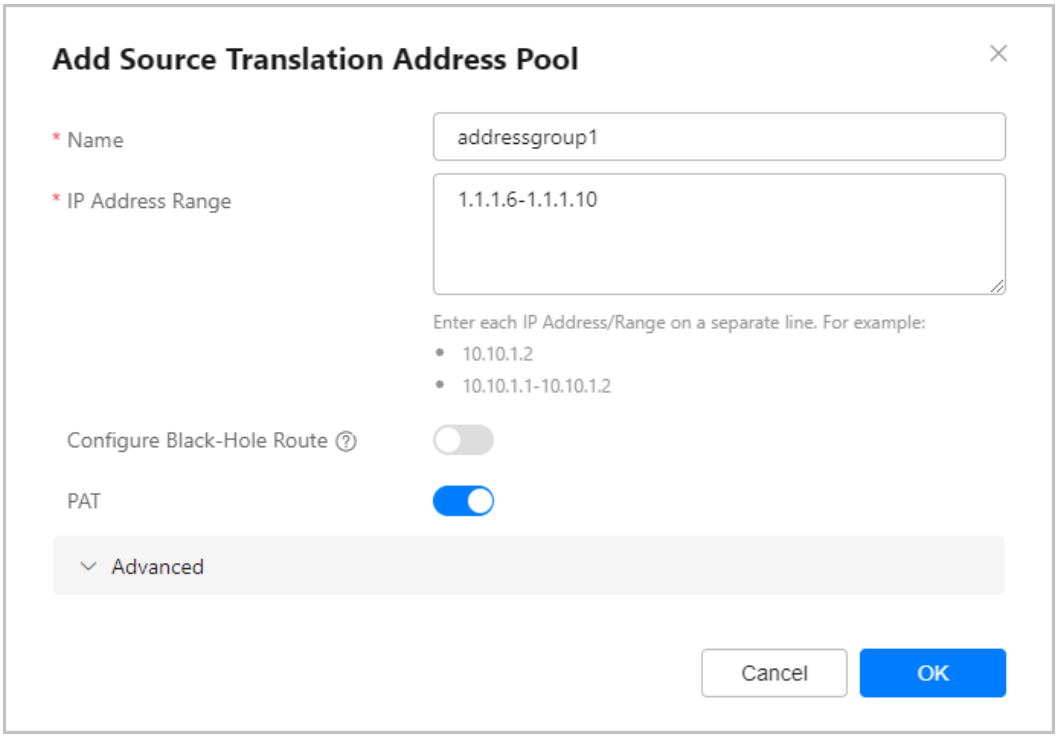
3. Click **OK**.

Step 4 Configure a NAT address pool and a NAT64 policy.

1. Choose **Policy** > **NAT Policy** > **NAT Policy** > **Source Translation Address Pool**.



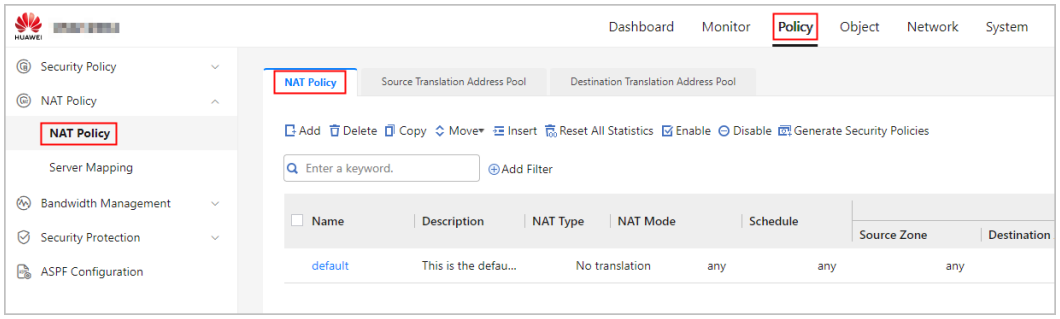
2. In **Source Translation Address Pool List**, click **Add** and configure a NAT address pool based on the following parameter values.



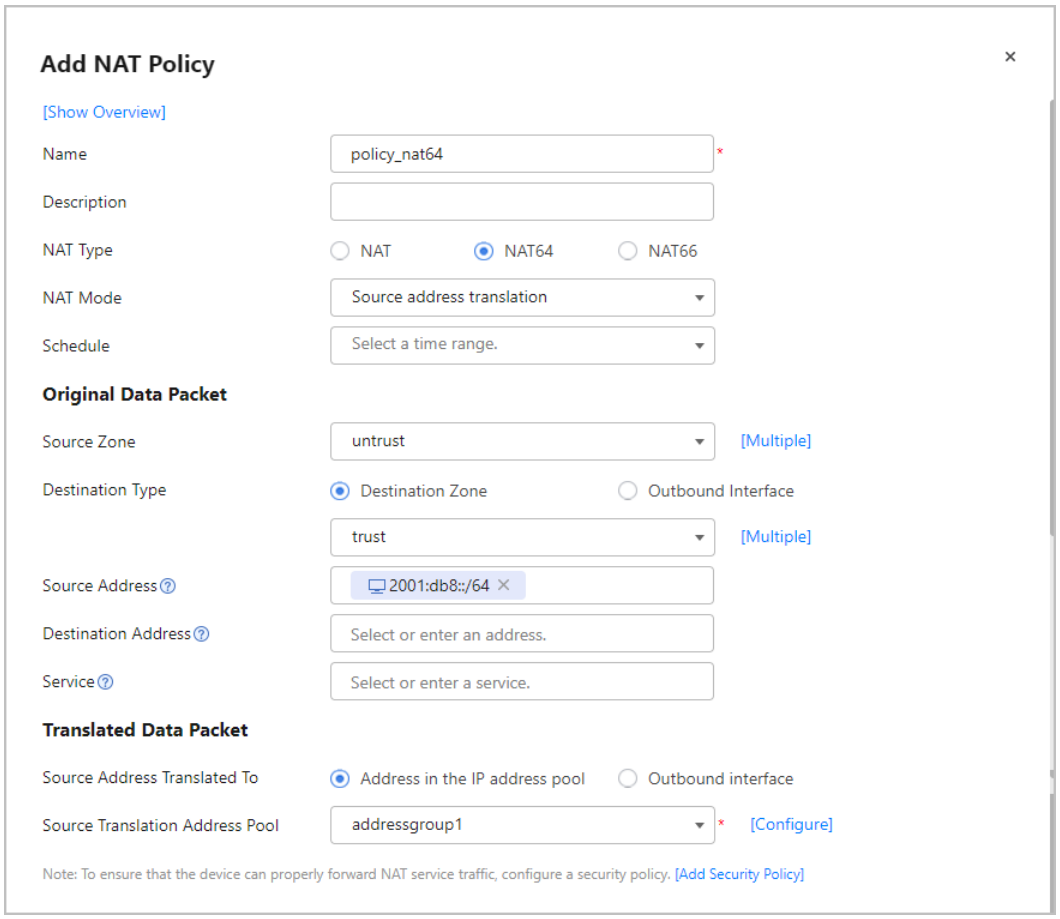
3. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

4. Choose **Policy** > **NAT Policy** > **NAT Policy** > **NAT Policy**.



5. In **NAT Policy List**, click **Add** and configure a NAT64 policy based on the following parameter values.



6. Click **OK**.

Step 5 Configure the DNS64 server.

Set the IPv6 prefix of the DNS64 server to 2001:db8:1::/96, which is the same as the NAT64 prefix of DeviceA.

Configure routes from the DNS64 server to the PC and the IPv4 server.

Step 6 On the PC, configure an IPv6 address, a route, and a DNS server. (The method of configuring an IPv6 address and a route for the PC varies according to the PC operating system. The detailed configuration procedure is not provided here.)

Set the PC IPv6 address to 2001:db8::1/64, which is on the same subnet as GE 0/0/2 of DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Configure a static route from the PC to DeviceA, with the destination address set to 2001:db8:1::/96 and the next hop address set to 2001:db8::2.

Configure the DNS64 server IPv6 address on the PC.

Step 7 Configure the IPv4 server address. (The method of configuring the IPv4 server address varies according to the server operating system. The detailed configuration procedure is not provided here.)

Set the IPv4 server address to 1.1.1.2/24, which is on the same subnet as GE 0/0/1 of DeviceA.

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping example.huawei.com** command on the PC.

```
c:\ ping example.huawei.com
Pinging 2001:db8:1::0101:102 with 32 bytes of data:

Reply from 2001:db8:1::0101:102: time=23ms
Reply from 2001:db8:1::0101:102: time=6ms
Reply from 2001:db8:1::0101:102: time=12ms
Reply from 2001:db8:1::0101:102: time=33ms

Ping statistics for 2001:db8:1::0101:102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 33ms, Average = 18ms
```

2. Choose **Monitor** > **Session Table** to verify that the NAT64 session tables are displayed.

Configuration Scripts

```
#
 sysname DeviceA
#
nat64 enable
#
interface GE 0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE 0/0/2
 ipv6 enable
 ipv6 address 2001:db8::2/64
#
nat address-group addressgroup1
 mode pat
 section 1 1.1.1.6 1.1.1.10
#
firewall zone trust
 set priority 85
 add interface GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE 0/0/2
#
 nat64 prefix 2001:db8:1:: 96
#
security-policy
  rule name policy_sec_1
    source-zone untrust
    destination-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
   source-address 2001:db8:: 64
   action permit
#
nat-policy
 rule name policy_nat64
   source-zone untrust
   destination-zone trust
   nat-type nat64
   source-address 2001:db8:: 64
   action source-nat address-group addressgroup1
#
return
```

16.6 CLI: Example for Enabling an IPv6 User to Access an IPv4 Server

Networking Requirements

On the network shown in **Figure 16-6**, DeviceA supports the IPv4/IPv6 dual stack and is connected to an IPv6 network and an IPv4 network. The IPv6 network has a large number of PCs using unfixed IP addresses. These PCs need to access the server on the IPv4 network through the domain name example.huawei.com.

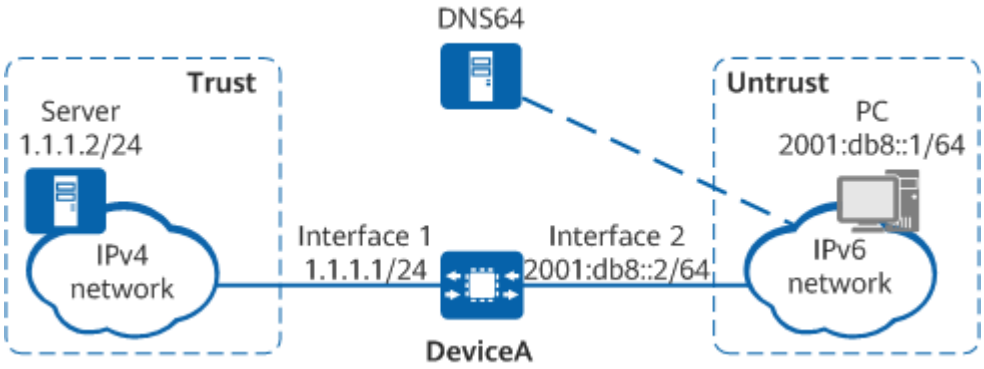
NOTE

When both NAT64 and DNS64 are deployed, configure the same NAT64 prefix and prefix length on the DNS64 and NAT64 devices.

Figure 16-6 Network diagram of dynamic NAT64

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure DeviceA.

Configure an IPv4 address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure an IPv6 address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:db8::2 64
```

Enable NAT64 on GE 0/0/2.

```
[DeviceA-GE0/0/2] nat64 enable
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Configure a security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone trust
[DeviceA-policy-security-rule-policy_sec_1] source-address 2001:db8:: 64
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
[DeviceA-policy-security] quit
```

Set the NAT64 prefix to 2001:db8:1::/96.

```
[DeviceA] nat64 prefix 2001:db8:1:: 96
```

NOTE

In this example, the NAT64 prefix is 2001:db8:1::/96. If no NAT64 prefix is configured, the well-known prefix is used by default.

Configure an IPv4 NAT address pool named **addressgroup1**, with the address range from 1.1.1.6 to 1.1.1.10. The addresses in this NAT address pool will be used as post-NAT64 addresses.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] mode pat
[DeviceA-address-group-addressgroup1] section 1 1.1.1.6 1.1.1.10
[DeviceA-address-group-addressgroup1] quit
```

Configure dynamic NAT64 mapping.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat64
[DeviceA-policy-nat-rule-policy_nat64] nat-type nat64
[DeviceA-policy-nat-rule-policy_nat64] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat64] destination-zone trust
[DeviceA-policy-nat-rule-policy_nat64] source-address 2001:db8:: 64
[DeviceA-policy-nat-rule-policy_nat64] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat64] quit
[DeviceA-policy-nat] quit
```

Step 2 Configure the DNS64 server.

Set the IPv6 prefix of the DNS64 server to 2001:db8:1::/96, which is the same as the NAT64 prefix of DeviceA.

 Copyright © Huawei Technologies Co., Ltd.

Configure routes from the DNS64 server to the PC and the IPv4 server.

Step 3 On the PC, configure an IPv6 address, a route, and a DNS server. (The method of configuring an IPv6 address and a route for the PC varies according to the PC operating system. The detailed configuration procedure is not provided here.)

Set the PC IPv6 address to 2001:db8::1/64, which is on the same subnet as GE 0/0/2 of DeviceA.

Configure a static route from the PC to DeviceA, with the destination address set to 2001:db8:1::/96 and the next hop address set to 2001:db8::2.

Configure the DNS64 server IPv6 address on the PC.

Step 4 Configure the IPv4 server address. (The method of configuring the IPv4 server address varies according to the server operating system. The detailed configuration procedure is not provided here.)

Set the IPv4 server address to 1.1.1.2/24, which is on the same subnet as GE 0/0/1 of DeviceA.

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping example.huawei.com** command on the PC.

```
c:\ ping example.huawei.com
Pinging 2001:db8:1::0101:102 with 32 bytes of data:

Reply from 2001:db8:1::0101:102: time=23ms
Reply from 2001:db8:1::0101:102: time=6ms
Reply from 2001:db8:1::0101:102: time=12ms
Reply from 2001:db8:1::0101:102: time=33ms

Ping statistics for 2001:db8:1::0101:102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 33ms, Average = 18ms
```

2. The PC pings the IPv4 server address successfully.
3. On DeviceA, run the **display firewall ipv6 session table** command in any view to check the NAT64 session table.

```
<DeviceA> display firewall ipv6 session table
NAT64: icmp6 VPN: public --> public  2001:db8::1.44152[1.1.1.10:10296] -->
2001:db8:1::0101:102.2048[1.1.1.2:2048]
```

   You can obtain the mappings between IPv6 and IPv4 addresses according to the NAT64 session table.

Configuration Scripts

```
#
 sysname DeviceA
#

interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ipv6 enable
 nat64 enable
 ipv6 address 2001:db8::2/64
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
nat address-group addressgroup1
 mode pat
 section 1 1.1.1.6 1.1.1.10
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 nat64 prefix 2001:db8:1:: 96
#
security-policy
  rule name policy_sec_1
    source-zone untrust
    destination-zone trust
    source-address 2001:db8:: 64
    action permit
#
nat-policy
  rule name policy_nat64
    source-zone untrust
    destination-zone trust
    nat-type nat64
    source-address 2001:db8:: 64
    action source-nat address-group addressgroup1
#
return
```

16.7 CLI: Example for Enabling an IPv4 User to Access an IPv6 Server

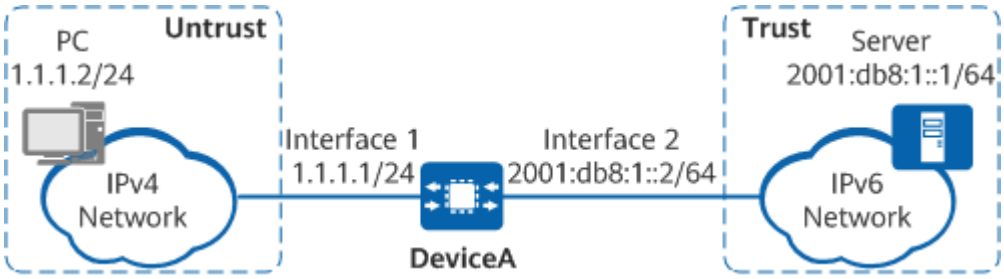
Networking Requirements

On the network shown in **Figure 16-7**, the device supports the IPv4/IPv6 dual stack and is connected to an IPv6 network and an IPv4 network. The PC on the IPv4 network needs to access the server on the IPv6 network through IPv4 address 1.1.1.10.

Figure 16-7 Networking diagram for configuring static NAT64

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure DeviceA.

Configure an IPv4 address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IPv6 address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:db8:1::2 64
```

Enable NAT64 on GE 0/0/2.

```
[DeviceA-GE0/0/2] nat64 enable
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Add GE 0/0/2 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] quit
```

Configure a NAT64 prefix. The source address of the packets from the PC to the server on the IPv6 network is the combination of the prefix and the IPv4 address of the PC.

```
[DeviceA] nat64 prefix 2001:db8:2:: 96
```

NOTE

In this example, the NAT64 prefix is 2001:db8:2::/96. If no NAT64 prefix is configured, the well-known prefix is used by default.

Configure a static NAT64 mapping to translate IPv6 address 2001:db8:1::1 (of the server) into IPv4 address 1.1.1.10.

```
[DeviceA] nat64 static 2001:db8:1::1 1.1.1.10 route
```

Configure a security policy.

NOTE

An IPv6 security policy is required for NAT64 static mapping.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-address 2001:db8:1::1 64
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
```

Step 2 Configure an IPv4 address for the PC. (The method of configuring the IPv4 address and route varies depending on the operating system of the PC and is omitted here.)

 Copyright © Huawei Technologies Co., Ltd.

Set the PC IPv4 address to 1.1.1.2/24, which is on the same subnet as GE0/0/1 of DeviceA.

Step 3 Set the server IPv6 address and route. (The method of configuring the IPv6 address and route varies depending on the operating system of the server. The setting method is omitted here.)

Set the server IPv6 address to 2001:db8:1::1/64, which is on the same subnet as GE0/0/2 of DeviceA.

Set a static route from the server to DeviceA. The destination address is 2001:db8:2::/96, and the next-hop address is 2001:db8:1::2.

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping 1.1.1.10** command on the PC.

```
C:\> ping 1.1.1.10
Pinging 1.1.1.10 with 32 bytes of data:

Reply from 1.1.1.10: time=69ms
Reply from 1.1.1.10: time=34ms
Reply from 1.1.1.10: time=17ms
Reply from 1.1.1.10: time=18ms

Ping statistics for 1.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 69ms, Average = 34ms
```

2. The IPv4 address of the server can be pinged through from the PC.
3. In any view of DeviceA, run the **display firewall ipv6 session table** command to verify information about the NAT64 session table.

```
<DeviceA> display firewall ipv6 session table
 Current total IPv6 sessions: 1
NAT64: icmp6 VPN: public --> public  2001:db8:2::101:102.44006[1.1.1.2:44006] -->
2001:db8:1::1.2048[1.1.1.10:2048]
```

   According to the NAT64 session table information, you can obtain the mapping of IPv6 addresses and IPv4 addresses.

Configuration Scripts

```
#
 sysname DeviceA
#

interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ipv6 enable
 nat64 enable
 ipv6 address 2001:db8:1::2/64
#
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
 nat64 prefix 2001:db8:2:: 96
 nat64 static 2001:db8:1::1 1.1.1.10 route
#
security-policy
 rule name policy_sec_1
  source-zone untrust
  destination-zone trust
  destination-address 2001:db8:1::1 64
  action permit
#
return
```

16.8 CLI: Example for Applying Port Pre-Allocation and Incremental Allocation to a NAT64 Scenario

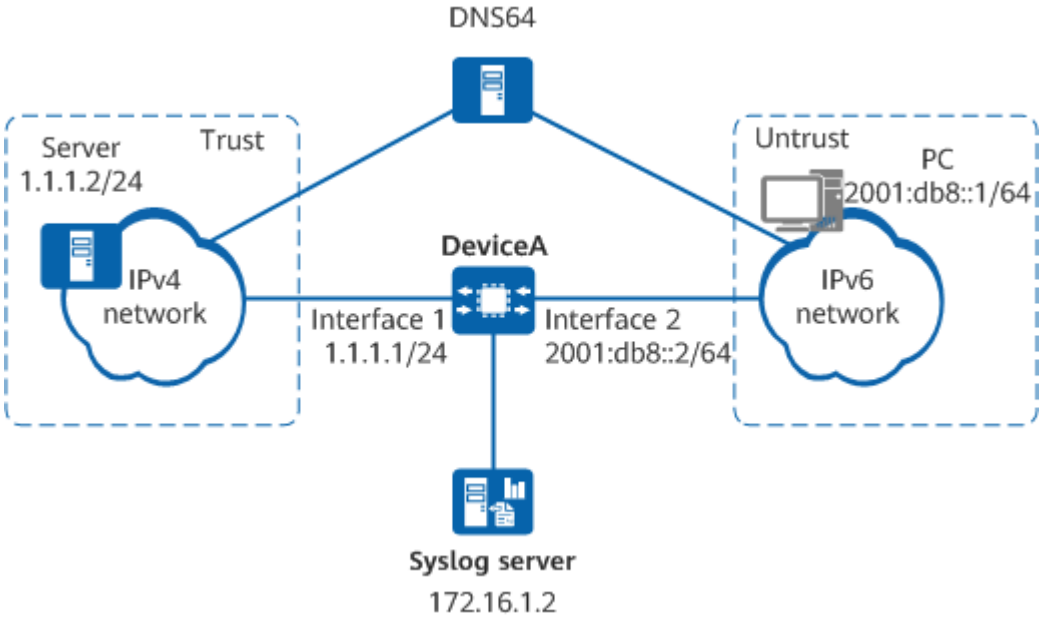
Networking Requirements

A carrier provides NAT64 for single-stack IPv6 users to access IPv4 servers. On the network shown in **Figure 16-8**, the PC on an IPv6 network needs to access the server on an IPv4 network through the domain name **example.huawei.com**, ports need to be properly allocated, and user addresses need to be obtained.

Figure 16-8 Network diagram of applying port pre-allocation and incremental allocation in a NAT64 scenario

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



Procedure

Step 1 Configure DeviceA.

Configure an IPv4 address for GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IPv6 address for GE 0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:db8::2 64
```

Enable NAT64 on GE 0/0/2.

```
[DeviceA-GE0/0/2] nat64 enable
[DeviceA-GE0/0/2] quit
```

Add GE 0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE 0/0/2 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Configure a security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone trust
[DeviceA-policy-security-rule-policy_sec_1] source-address 2001:db8:: 64
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
[DeviceA-policy-security] quit
```

Set the NAT64 prefix to 2001:db8:2::/96.

```
[DeviceA] nat64 prefix 2001:db8:2:: 96
```

NOTE

In this example, the NAT64 prefix is 2001:db8:2::/96. If the NAT64 prefix is not specified, the well-known prefix is used by default.

Configure an IPv4 NAT address pool named **addressgroup1**, with the address range from 1.1.1.6 to 1.1.1.10. Addresses in this NAT address pool will be used as post-NAT64 addresses.

```
[DeviceA] nat address-group addressgroup1
[DeviceA-address-group-addressgroup1] port-block-size 256
[DeviceA-address-group-addressgroup1] section 1 1.1.1.6 1.1.1.10
[DeviceA-address-group-addressgroup1] quit
```

NOTE

The **port-block-size** command supports configuration only when the hash-based mode is source-only hash mode.

The **firewall hash-mode** command configures the hash-based mode to select a CPU that processes service packets. With the **realtime** parameter configured, the changed hash-based mode takes effect without restarting the device.

After the hash-based mode is changed and takes effect immediately, NAT, IPsec, and forwarding services are temporarily interrupted. After the sessions of these services are reestablished, the services are automatically restored.

Configure dynamic NAT64.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy_nat64
[DeviceA-policy-nat-rule-policy_nat64] nat-type nat64
[DeviceA-policy-nat-rule-policy_nat64] source-zone untrust
[DeviceA-policy-nat-rule-policy_nat64] destination-zone trust
[DeviceA-policy-nat-rule-policy_nat64] source-address 2001:db8:: 64
[DeviceA-policy-nat-rule-policy_nat64] action source-nat address-group addressgroup1
[DeviceA-policy-nat-rule-policy_nat64] quit
[DeviceA-policy-nat] quit
```

Step 2 Configure the DNS64 server.

Set the IPv6 prefix of the DNS64 server to 2001:db8:2::/96, which is the same as the NAT64 prefix of DeviceA.

Configure routes from the DNS64 server to the PC and the IPv4 server.

Step 3 Configure interoperation between DeviceA and the syslog server.

```
[DeviceA] nat port-block assigning syslog enable
[DeviceA] nat port-block syslog host 172.16.1.2 source CGN 172.16.1.1 514
```

Step 4 On the PC, configure an IPv6 address, route, and DNS server. (The method of configuring an IPv6 address and route for the PC varies according to the PC operating system; the detailed configuration procedures are not provided here.)

Set the PC IPv6 address to 2001:db8::1/24, which is on the same subnet as GE 0/0/2 of DeviceA.

Configure a static route from the PC to DeviceA, with the destination address set to 2001:db8:2::/96 and the next hop address set to 2001:db8::2.

Configure the DNS64 server IPv6 address on the PC.

Step 5 Configure the IPv4 server address. (The configuration method varies according to the server operating system, and is not provided here.)

Set the IPv4 server address to 1.1.1.2/24, which is on the same subnet as GE 0/0/1 of DeviceA.

Step 6 Configure the syslog server.

The configuration varies according to the model of the syslog server. For details, see the product documentation of the syslog server.

----End

Verifying the Configuration

1. After completing the configuration, run the **ping example.huawei.com** command on the PC.

```
c:\ ping example.huawei.com
Pinging 2001:db8:2::0101:102 with 32 bytes of data:

Reply from 2001:db8:2::0101:102: time=23ms
Reply from 2001:db8:2::0101:102: time=6ms
Reply from 2001:db8:2::0101:102: time=12ms
Reply from 2001:db8:2::0101:102: time=33ms

Ping statistics for 2001:db8:2::0101:102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 33ms, Average = 18ms
```

2. The PC pings the IPv4 address of the server successfully.

 Copyright © Huawei Technologies Co., Ltd.

3. On DeviceA, run the **display cpe-user information cpe-ipv6 2001:db8::1** command in any view to check details of NAT64 users.

```
[DeviceA] display cpe-user information cpe-ipv6 2001:db8::1
Scene: NAT64 DstZone: untrust CPEIP: 2001:db8::1
TTL: 40 LeftTime: 1 Increase Count: 0 VPN: public
PoolID: 7 SectionID: 1 PublicIP: 1.1.1.10 StartPort: 2048
PortNumber: 256 PortTotal: 256 Used Port Number: 0
```

   As shown in the command output, the source addresses of service flows sent from 2001:db8::1 are translated into 1.1.1.10, and the port range is from 2048 to 2303 (total of 256 ports).

4. The syslog server receives a log during port pre-allocation or incremental allocation. The following example shows a syslog in France Telecom format displayed on the syslog server upon the initial port re-allocation. To change the syslog format, run the **nat port-block syslog descriptive format** command in the system view.

```
 NAT64userbased - %%01SEC/6/BIND(l): An initial portrange is assigned, in nat64 scene.
privateip='2001:db8::1 ' srcvrfid='0' publicip='1.1.1.10' publicportrange='2048~2303' time='2012-05-02
18:24:09'.
```

   This log displays the user's IP address, post-NAT public IP address, port range, and timestamp, which can be used for user address obtaining.

Configuration Scripts

```
#
 sysname DeviceA
#

interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ipv6 enable
 nat64 enable
 ipv6 address 2001:db8::2/64
#
 nat address-group addressgroup1
   port-block-size 256
   section 1 1.1.1.6 1.1.1.10
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 nat64 prefix 2001:db8:2:: 96
#
 nat port-block assigning syslog enable
 nat port-block syslog host 172.16.1.2 source  CGN 172.16.1.1 514
#
security-policy
  rule name policy_sec_1
    source-zone untrust
    destination-zone trust
    source-address 2001:db8:: 64
    action permit
#
nat-policy
  rule name policy_nat64
    source-zone untrust
    destination-zone trust
    nat-type nat64
```

 Copyright © Huawei Technologies Co., Ltd.

```
    source-address 2001:db8:: 64
    action source-nat address-group addressgroup1
#
return
```

16.9 CLI: Example for Configuring an IPv6 User in a Virtual System to Access an IPv4 Server

Networking Requirements

As shown in **Figure 16-9**, the virtual system **vsysa** supports the IPv6/IPv4 dual stack and is connected to an IPv6 network and an IPv4 network. The PC on the IPv6 network can access the server on the IPv4 network using URL example.huawei.com.

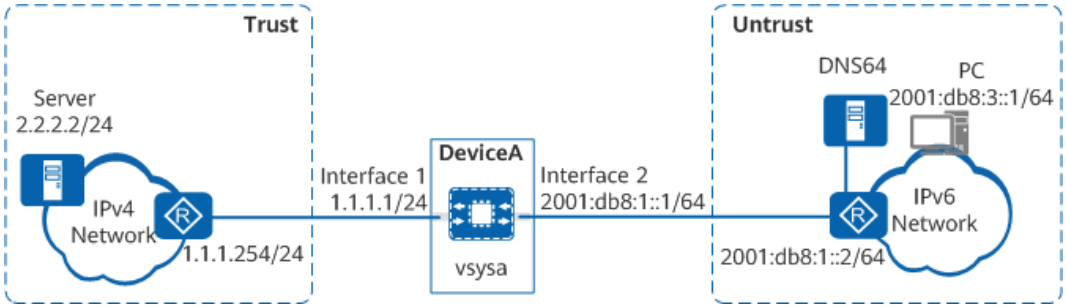
NOTE

When both NAT64 and DNS64 are deployed, configure the same NAT64 prefix and prefix length on the DNS64 and NAT64 devices.

Figure 16-9 Networking diagram for configuring dynamic NAT64 in a virtual system

NOTE

In this example, interfaces 1 and 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Create virtual system vsysa, and assigns interfaces and global ip addresses to vsysa.

Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vsys enable
```

Create a virtual system and assign interfaces and global IP addresses to the virtual system. Global IP addresses will be used in the NAT address pool.

```
[DeviceA] vsys name vsysa
[DeviceA-vsys-vsysa] assign interface ge 0/0/1
[DeviceA-vsys-vsysa] assign interface ge 0/0/2
[DeviceA-vsys-vsysa] assign global-ip 1.1.1.6 1.1.1.10 exclusive
[DeviceA-vsys-vsysa] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure IP addresses, routes, and security policies for vsysa.

Set interface IP addresses.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:db8:1::1 64
[DeviceA-GE0/0/2] quit
```

Access the configuration view of the virtual system.

```
[DeviceA] switch vsys vsysa
```

Assign interfaces to security zones.

```
<DeviceA-vsysa> system-view
[DeviceA-vsysa] firewall zone trust
[DeviceA-vsysa-zone-trust] add interface ge 0/0/1
[DeviceA-vsysa-zone-trust] quit
[DeviceA-vsysa] firewall zone untrust
[DeviceA-vsysa-zone-untrust] add interface ge 0/0/2
[DeviceA-vsysa-zone-untrust] quit
```

Configure a security policy.

```
[DeviceA-vsysa] security-policy
[DeviceA-vsysa-policy-security] rule name policy_sec_1
[DeviceA-vsysa-policy-security-rule-policy_sec_1] source-zone untrust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] destination-zone trust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] source-address 2001:db8:3:: 64
[DeviceA-vsysa-policy-security-rule-policy_sec_1] action permit
[DeviceA-vsysa-policy-security-rule-policy_sec_1] quit
[DeviceA-vsysa-policy-security] quit
```

Configure a static route to the IPv4 and IPv6 network.

```
[DeviceA-vsysa] ip route-static 2.2.2.0 24 1.1.1.254
[DeviceA-vsysa] ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
```

Step 3 Configure NAT64.

Enable the NAT64 function to connect to the IPv6 network interface.

```
[DeviceA-vsysa] interface ge 0/0/2
[DeviceA-vsysa-GE0/0/2] nat64 enable
[DeviceA-vsysa-GE0/0/2] quit
```

Set the NAT64 prefix to 2001:db8:2::/96.

```
[DeviceA-vsysa] nat64 prefix 2001:db8:2:: 96
```

NOTE

In the example, the NAT64 prefix is 2001:db8:2::/96. If no prefix is configured, the well-known prefix is used by default.

Configure IPv4 NAT address pool addressgroup1 whose addresses range from 1.1.1.6 through 1.1.1.10. The addresses in this NAT address pool are the IPv4 addresses of resulting packets.

```
[DeviceA-vsysa] nat address-group addressgroup1
[DeviceA-vsysa-address-group-addressgroup1] mode pat
[DeviceA-vsysa-address-group-addressgroup1] section 1 1.1.1.6 1.1.1.10
[DeviceA-vsysa-address-group-addressgroup1] quit
```

Configure a dynamic NAT64 mapping.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-vsysa] nat-policy
[DeviceA-vsysa-policy-nat] rule name policy_nat64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] nat-type nat64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] source-zone untrust
[DeviceA-vsysa-policy-nat-rule-policy_nat64] destination-zone trust
[DeviceA-vsysa-policy-nat-rule-policy_nat64] source-address 2001:db8:3:: 64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] action source-nat address-group addressgroup1
[DeviceA-vsysa-policy-nat-rule-policy_nat64] quit
[DeviceA-vsysa-policy-nat] quit
```

Step 4 Configure the DNS64 device.

Set the IPv6 prefix of the DNS64 device to 2001:db8:2::/96, which is the same as the NAT64 prefix of DeviceA.

Configure a route from the DNS64 device to the PC.

Step 5 Configure the IPv6 address, route and DNS server for the PC. (The method of setting the IPv6 address, route, and DNS server varies depending on the operating system of the PC. The setting method is omitted here.)

Set the PC IPv6 address to 2001:db8:3::1/64.

Configure a route from the PC to 2001:db8:2::/96 and set the next hop to the address of the egress router on the IPv6 network.

Set the DNS server of the PC as the IPv6 address of the DNS64 device.

Step 6 Configure the IPv4 address and route for the server. (The method of setting the IPv4 address varies depending on the operating system of the server. The setting method is omitted here.)

Set the server IPv4 address to 2.2.2.2/24.

Configure a route from the server to 1.1.1.6-1.1.1.10 and set the next hop to the address of the egress router on the IPv4 network.

----End

Verifying the Configuration

1. Access example.huawei.com from the PC. The access succeeds.
2. Check the NAT64 session table information.

```
<DeviceA> display firewall ipv6 session table verbose vsys vsysa
 Current Total IPv6 Sessions : 1
 NAT64: icmpv6  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust TTL: 00:00:45  Left: 00:00:45
 Interface: GE0/0/1 NextHop: 1.1.1.254 MAC: xxxx-xxxx-xxxx
 <--packets: 25 bytes: 2,600 --> packets: 25 bytes: 2,600
 2001:db8:3::1.44019[1.1.1.7:2051] --> 2001:db8:2::202:202.2048[2.2.2.2:2048] PolicyName:
policy_sec_1
```

Configuration Scripts

- Public system:

```
#
 sysname DeviceA
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/1
 assign interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 assign global-ip 1.1.1.6 1.1.1.10 exclusive
#
interface GE0/0/1
 ip binding vpn-instance vsysa
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip binding vpn-instance vsysa
 ipv6 enable
 ipv6 address 2001:db8:1::1/64
#
return
```

- vsysa

```
#
switch vsys vsysa
#
interface GE0/0/2
 nat64 enable
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
nat address-group addressgroup1
 mode pat
 section 1 1.1.1.6 1.1.1.10
#
 nat64 prefix 2001:db8:2:: 96
#
 ip route-static 2.2.2.0 24 1.1.1.254
 ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
#
security-policy
  rule name policy_sec_1
    source-zone untrust
    destination-zone trust
    source-address 2001:db8:3:: 64
    action permit
#
nat-policy
  rule name policy_nat64
    source-zone untrust
    destination-zone trust
    nat-type nat64
    source-address 2001:db8:3:: 64
    action source-nat address-group addressgroup1
#
return
```

16.10 CLI: Example for Configuring an IPv4 User in a Virtual System to Access an IPv6 Server

Networking Requirements

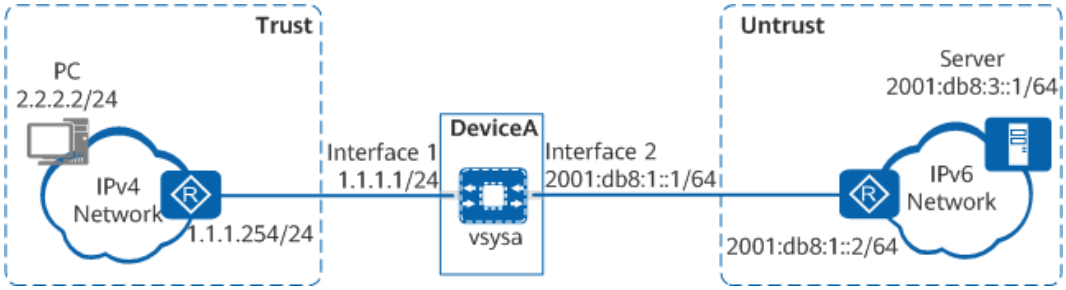
As shown in **Figure 16-10**, the virtual system **vsysa** supports the IPv6/IPv4 dual stack and is connected to an IPv6 network and an IPv4 network. The PC on the IPv4 network can access the server on the IPv6 network with IPv4 address 1.1.1.10.

 Copyright © Huawei Technologies Co., Ltd.

Figure 16-10 Networking diagram for configuring static NAT64 in a virtual system

NOTE

In this example, interfaces 1 and 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Create virtual system vsysa, and assigns interfaces and global ip addresses to vsysa.

Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vsys enable
```

Create a virtual system and assign interfaces and global IP addresses to the virtual system. Public IP addresses will be used for static NAT64 mapping.

```
[DeviceA] vsys name vsysa
[DeviceA-vsys-vsysa] assign interface ge 0/0/1
[DeviceA-vsys-vsysa] assign interface ge 0/0/2
[DeviceA-vsys-vsysa] assign global-ip 1.1.1.10 1.1.1.10 exclusive
[DeviceA-vsys-vsysa] quit
```

Step 2 Configure IP addresses, routes, and security policies for vsysa.

Set interface IP addresses.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ipv6 enable
[DeviceA-GE0/0/2] ipv6 address 2001:db8:1::1 64
[DeviceA-GE0/0/2] quit
```

Access the configuration view of the virtual system.

```
[DeviceA] switch vsys vsysa
```

Assign interfaces to security zones.

```
<DeviceA-vsysa> system-view
[DeviceA-vsysa] firewall zone trust
[DeviceA-vsysa-zone-trust] add interface ge 0/0/1
[DeviceA-vsysa-zone-trust] quit
[DeviceA-vsysa] firewall zone untrust
[DeviceA-vsysa-zone-untrust] add interface ge 0/0/2
[DeviceA-vsysa-zone-untrust] quit
```

Configure a security policy.

```
[DeviceA-vsysa] security-policy
[DeviceA-vsysa-policy-security] rule name policy_sec_1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-vsysa-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] destination-address 2001:db8:3::1 64
[DeviceA-vsysa-policy-security-rule-policy_sec_1] action permit
[DeviceA-vsysa-policy-security-rule-policy_sec_1] quit
[DeviceA-vsysa-policy-security] quit
```

Configure a static route to the IPv4 and IPv6 network.

```
[DeviceA-vsysa] ip route-static 2.2.2.0 24 1.1.1.254
[DeviceA-vsysa] ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
```

Step 3 Configure NAT64.

Enable the NAT64 function to connect to the IPv6 network interface.

```
[DeviceA-vsysa] interface ge 0/0/2
[DeviceA-vsysa-GE0/0/2] nat64 enable
[DeviceA-vsysa-GE0/0/2] quit
```

Configure a NAT64 prefix. The source address of the packets from the PC to the server on the IPv6 network is the combination of the prefix and the IPv4 address of the PC.

```
[DeviceA-vsysa] nat64 prefix 2001:db8:2:: 96
```

NOTE

In the example, the NAT64 prefix is 2001:db8:2::/96. If no prefix is configured, the well-known prefix is used by default.

Configure a static NAT64 mapping to translate IPv6 address 2001:db8:3::1 (of the server) into IPv4 address 1.1.1.10.

```
[DeviceA-vsysa] nat64 static 2001:db8:3::1 1.1.1.10 route
```

Step 4 Configure the IPv4 address and route for the PC. (The method of configuring the IPv4 address and route varies depending on the operating system of the PC and is omitted here.)

Set the PC IPv4 address to 2.2.2.2/24.

Configure a route from the PC to 1.1.1.10 and set the next hop to the address of the egress router on the IPv4 network.

Step 5 Set IPv6 address and route for the server. (The method of configuring the IPv6 address and route varies depending on the operating system of the server. The setting method is omitted here.)

Set the server IPv6 address to 2001:db8:3::1/64.

Configure a route from the server to 2001:db8:2::/96 and set the next hop to the address of the egress router on the IPv6 network.

----End

Verifying the Configuration

1. After the configuration is complete, run the **ping 1.1.1.10** command on the PC.
2. Check the NAT64 session table information.

```
<DeviceA> display firewall ipv6 session table verbose vsys vsysa
 Current Total IPv6 Sessions : 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
 NAT64: icmpv6  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust TTL: 00:00:45  Left: 00:00:45
 Interface: GE0/0/2 NextHop: 2001:db8:1::2 MAC: xxxx-xxxx-xxxx
 <--packets: 50 bytes: 5,200 --> packets: 50 bytes: 5,200
 2001:db8:2::202:202.44026[2.2.2.2:44026] --> 2001:db8:3::1.2048[1.1.1.10:2048] PolicyName:
policy_sec_1
```

Configuration Scripts

- Public system:

```
#
 sysname DeviceA
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/1
 assign interface GE0/0/2
 assign global-ip 1.1.1.10 1.1.1.10 exclusive
#
interface GE0/0/1
 ip binding vpn-instance vsysa
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip binding vpn-instance vsysa
 ipv6 enable
 ipv6 address 2001:db8:1::1/64
#
return
```

- vsysa

```
#
switch vsys vsysa
#
interface GE0/0/2
 nat64 enable
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 nat64 prefix 2001:db8:2:: 96
 nat64 static 2001:db8:3::1 1.1.1.10 route
#
 ip route-static 2.2.2.0 24 1.1.1.254
 ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    destination-address 2001:db8:3:: 64
    action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

16.11 CLI: Example for Configuring a Public IPv4 Network User to Access a Private IPv6 Network Server (Access from the Public System to a Virtual System)

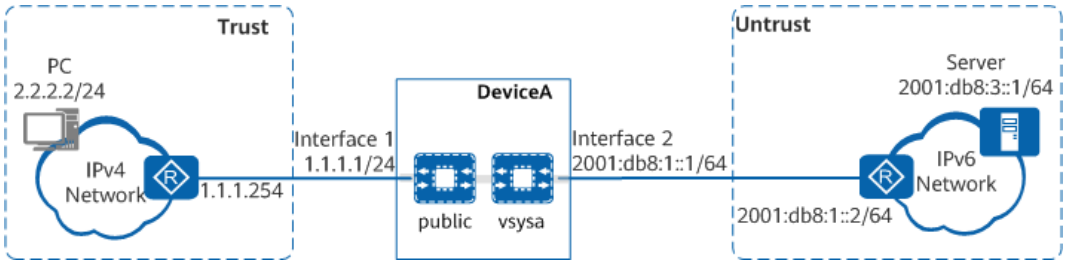
Networking Requirements

As shown in **Figure 16-11**, a virtual system supports IPv4/IPv6 dual stack and connects to IPv6 and IPv4 networks. It is required that a PC on the public IPv4 network be able to directly access a server on the private IPv6 network across the public system and virtual system. The address of the IPv6 network server mapped to the IPv4 network is **1.1.1.10**.

Figure 16-11 Networking diagram for configuring static NAT64 in a virtual system

NOTE

In this example, interfaces 1 and 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Create virtual system **vsysa** and assign an interface to it.

Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vsys enable
```

Create a virtual system and assign an interface and a public address to it. The public address is used in the NAT address pool.

```
[DeviceA] vsys name vsysa
[DeviceA-vsys-vsysa] assign interface ge 0/0/2
[DeviceA-vsys-vsysa] assign global-ip 1.1.1.10 1.1.1.10 exclusive
[DeviceA-vsys-vsysa] quit
```

Step 2 Configure IP addresses and routes on the public system.

On the public system, set IP addresses for the interfaces and assign the interfaces to security zones. The IP address of Virtual-if0 can be any value as long as it is not in conflict with the IP address on any other interface.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface Virtual-if 0
[DeviceA-virtual-if0] ip address 172.16.0.1 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-virtual-if0] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface Virtual-if 0
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Configure the traffic diversion table for diverting traffic to **vsysa**.

```
[DeviceA] firewall import-flow public 1.1.1.10 1.1.1.10 vpn-instance vsysa
Warning: The destination of this IP range should be in this vsys network, otherwise it may cause flow loop!
Please select [Y/N]:Y
```

Configure a route to the IPv4 network.

```
[DeviceA] ip route-static 2.2.2.0 24 1.1.1.254
```

Step 3 Configure IP addresses, routes, and security policies on the virtual system.

Access the virtual system configuration view.

```
[DeviceA] switch vsys vsysa
```

Set an IP address for an interface and assign the interface to a security zone.

NOTE

The IP address of Virtual-if1 can be any value as long as it is not in conflict with the IP address on any other interface.

The IDs of Virtual-if interfaces are randomly assigned from available IDs in the system. Therefore, in the actual configuration, the interface may not be Virtual-if1.

```
<DeviceA-vsysa> system-view
[DeviceA-vsysa] interface ge 0/0/2
[DeviceA-vsysa-GE0/0/2] ipv6 enable
[DeviceA-vsysa-GE0/0/2] ipv6 address 2001:db8:1::1 64
[DeviceA-vsysa-GE0/0/2] quit
[DeviceA-vsysa] interface Virtual-if 1
[DeviceA-vsysa-Virtual-if1] ip address 172.16.1.1 24
[DeviceA-vsysa-Virtual-if1] quit
[DeviceA-vsysa] firewall zone trust
[DeviceA-vsysa-zone-trust] add interface Virtual-if 1
[DeviceA-vsysa-zone-trust] quit
[DeviceA-vsysa] firewall zone untrust
[DeviceA-vsysa-zone-untrust] add interface ge 0/0/2
[DeviceA-vsysa-zone-untrust] quit
```

Configure a security policy.

```
[DeviceA-vsysa] security-policy
[DeviceA-vsysa-policy-security] rule name policy_sec_1
[DeviceA-vsysa-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] destination-address 2001:db8:3::1 64
[DeviceA-vsysa-policy-security-rule-policy_sec_1] action permit
[DeviceA-vsysa-policy-security-rule-policy_sec_1] quit
[DeviceA-vsysa-policy-security] quit
```

Configure a static route to the IPv6 network.

```
[DeviceA-vsysa] ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
```

Step 4 Configure NAT64.

Enable the NAT64 function on the IPv6 network interface.

```
[DeviceA-vsysa] interface ge 0/0/2
[DeviceA-vsysa-GE0/0/2] nat64 enable
[DeviceA-vsysa-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a NAT64 prefix. The source address used to transmit the packet for the PC to access the server over the IPv6 network is composed of the NAT64 prefix and the PC's IPv4 address.

```
[DeviceA-vsysa] nat64 prefix 2001:db8:2:: 96
```

NOTE

In this example, the NAT64 prefix is **2001:db8:2::/96**. If the prefix is left unconfigured, a well-known prefix is used by default.

Configure a static NAT64 mapping to translate the server's IPv6 address 2001:db8:3::1 into IPv4 address **1.1.1.10**.

```
[DeviceA-vsysa] nat64 static 2001:db8:3::1 1.1.1.10 route
```

Step 5 Configure the IPv4 address and route of the PC. (The method of setting the IPv4 address is determined by the operating system of the PC. The setting method is not described here.)

Set the IPv4 address of the PC to **2.2.2.2/24**.

Configure a route from the PC to **1.1.1.10**. The next hop of the route is the address of the IPv4 network egress router.

Step 6 Configure the IPv6 address and route of the server. (The configuration methods of IPv6 addresses and routes vary with the operating systems of the servers. The configuration methods are not described here.)

Set the IPv6 address of the server to **2001:db8:3::1/64**.

Configure a route from the server to the network segment **2001:db8:2::/96** and set the next hop to the address of the IPv6 network egress router.

----End

Verifying the Configuration

1. After the configurations are complete, run the **ping 1.1.1.10** command on the PC.
2. Check NAT64 session table information.

```
<DeviceA> display firewall ipv6 session table verbose vsys vsysa
 Current Total IPv6 Sessions : 1
 NAT64: icmpv6  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: trust --> untrust TTL: 00:00:45  Left: 00:00:45
 Interface: GE0/0/2 NextHop: 2001:db8:1::2 MAC: xxxx-xxxx-xxxx
 <--packets: 50 bytes: 5,200 --> packets: 50 bytes: 5,200
 2001:db8:2::202:202.44026[2.2.2.2:44026] --> 2001:db8:3::1.2048[1.1.1.10:2048] PolicyName:
policy_sec_1
```

Configuration Scripts

- Public system:

```
#
 sysname DeviceA
#
vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/2
 assign global-ip 1.1.1.10 1.1.1.10 exclusive
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Virtual-if 0
 ip address 172.16.0.1 24
#
firewall zone trust
 set priority 85
 add interface Virtual-if 0
 add interface GE0/0/1
#
 firewall import-flow public 1.1.1.10 1.1.1.10 vpn-instance vsysa
#
 ip route-static 2.2.2.0 24 1.1.1.254
#
return
```

- vsysa

```
#
switch vsys vsysa
#
interface GE0/0/2
 ipv6 enable
 ipv6 address 2001:db8:1::1 64
 nat64 enable
#
interface Virtual-if 1
 ip address 172.16.1.1 24
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall zone trust
 set priority 85
 add interface virtual-if 1
#
 nat64 prefix 2001:db8:2:: 96
 nat64 static 2001:db8:3::1 1.1.1.10 route
#
security-policy
  rule name policy_sec_1
    source-zone untrust
    destination-zone untrust
    destination-address 2001:db8:3::1 64
    action permit
#
 ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
#
return
```

16.12 CLI: Example for Configuring a Private IPv6 Network User to Access a Public IPv4 Network Server (Access from a Virtual System to the Public System)

Networking Requirements

As shown in **Figure 16-12**, virtual system **vsysa** supports IPv4/IPv6 dual stack and connects to IPv6 and IPv4 networks. It is required that a PC on the private IPv6 network be able to access a server on the public IPv4 network through domain name example.huawei.com and across the public system and virtual system.

 Copyright © Huawei Technologies Co., Ltd.

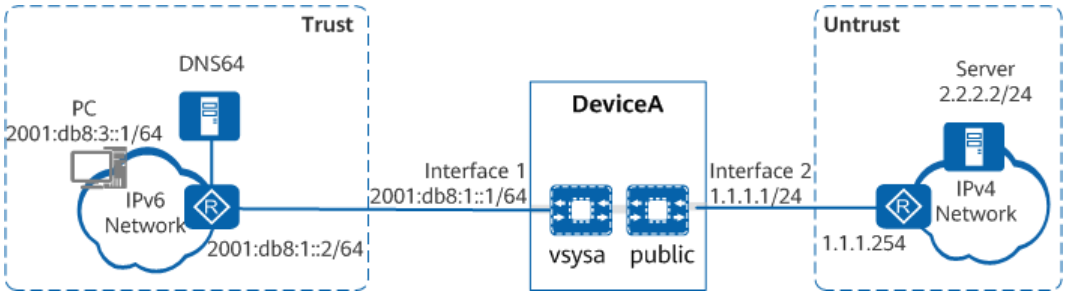
NOTE

Usually, the NAT64 is deployed with the DNS64. The DNS64 performs domain name translation. The prefix and length configured for the DNS64 are the same as those of the NAT64 device.

Figure 16-12 Networking diagram for configuring dynamic NAT64 in a virtual system

NOTE

In this example, interfaces 1 and 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Create virtual system **vsysa** and assign an interface and a public address to it.

Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vsys enable
```

Create a virtual system and assign an interface and a public address to it. The public address is used in the NAT address pool.

```
[DeviceA] vsys name vsysa
[DeviceA-vsys-vsysa] assign interface ge 0/0/1
[DeviceA-vsys-vsysa] assign global-ip 1.1.1.6 1.1.1.10 exclusive
[DeviceA-vsys-vsysa] quit
```

Step 2 Configure IP addresses, routes, and security policies on the public system.

On the public system, set IP addresses for the interfaces and assign the interfaces to security zones. The IP address of Virtual-if0 can be any value as long as it is not in conflict with the IP address on any other interface.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] interface Virtual-if 0
[DeviceA-virtual-if0] ip address 172.16.0.1 24
[DeviceA-virtual-if0] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface Virtual-if 0
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/2
[DeviceA-zone-untrust] quit
```

Configure a static route to the IPv4 network.

```
[DeviceA] ip route-static 2.2.2.0 24 1.1.1.254
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] destination-address 2.2.2.2 24
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure IP addresses and routes on the virtual system.

Access the virtual system configuration view.

```
[DeviceA] switch vsys vsysa
```

Set an IP address for an interface and assign the interface to a security zone.

NOTE

The IP address of Virtual-if1 can be any value as long as it is not in conflict with the IP address on any other interface.

The IDs of Virtual-if interfaces are randomly assigned from available IDs in the system. Therefore, in the actual configuration, the interface may not be Virtual-if 1.

```
<DeviceA-vsysa> system-view
[DeviceA-vsysa] interface ge 0/0/1
[DeviceA-vsysa-GE0/0/1] ipv6 enable
[DeviceA-vsysa-GE0/0/1] ipv6 address 2001:db8:1::1 64
[DeviceA-vsysa-GE0/0/1] quit
[DeviceA-vsysa] interface Virtual-if 1
[DeviceA-vsysa-Virtual-if1] ip address 172.16.1.1 24
[DeviceA-vsysa-Virtual-if1] quit
[DeviceA-vsysa] firewall zone trust
[DeviceA-vsysa-zone-trust] add interface ge 0/0/1
[DeviceA-vsysa-zone-trust] add interface Virtual-if 1
[DeviceA-vsysa-zone-trust] quit
```

#Configure a static route to the public system.

```
[DeviceA-vsysa] ip route-static 2.2.2.2 32 public
```

Configure a static route to the IPv6 network.

```
[DeviceA-vsysa] ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
```

Step 4 Configure NAT64.

Enable the NAT64 function on the IPv6 network interface.

```
[DeviceA-vsysa] interface ge 0/0/1
[DeviceA-vsysa-GE0/0/1] nat64 enable
[DeviceA-vsysa-GE0/0/1] quit
```

Set the NAT64 prefix to 2001:db8:2::/96.

```
[DeviceA-vsysa] nat64 prefix 2001:db8:2:: 96
```

NOTE

In this example, the NAT64 prefix is **2001:db8:2::/96**. If the prefix is left unconfigured, a well-known prefix is used by default.

Configure IPv4 NAT address pool **addressgroup1** and set the address range to **1.1.1.6 to 1.1.1.10**. Use the addresses in the NAT address pool as the IPv4 addresses after the NAT64 processing.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-vsysa] nat address-group addressgroup1
[DeviceA-vsysa-address-group-addressgroup1] mode pat
[DeviceA-vsysa-address-group-addressgroup1] section 1 1.1.1.6 1.1.1.10
[DeviceA-vsysa-address-group-addressgroup1] quit
```

Configure dynamic NAT64 mapping.

```
[DeviceA-vsysa] nat-policy
[DeviceA-vsysa-policy-nat] rule name policy_nat64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] nat-type nat64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] source-zone trust
[DeviceA-vsysa-policy-nat-rule-policy_nat64] destination-zone trust
[DeviceA-vsysa-policy-nat-rule-policy_nat64] source-address 2001:db8:3:: 64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] action source-nat address-group addressgroup1
[DeviceA-vsysa-policy-nat-rule-policy_nat64] quit
[DeviceA-vsysa-policy-nat] quit
```

Step 5 Configure the DNS64 device.

Set the IPv6 prefix of the DNS64 device to the NAT64 prefix of the DeviceA, namely, **2001:db8:2::/96**.

Configure a route from the DNS64 device to the PC to ensure reachability.

Step 6 Configure the IPv6 address, route, and DNS of the PC. (The configuration methods of IPv6 addresses and routes vary with the operating systems of the PCs. The configuration methods are not described here.)

Set the IPv6 address of the PC to **2001:db8:3::1/64**.

Configure a route from the PC to the network segment 2001:db8:2::/96 and set the next hop to the address of the IPv6 network egress router.

Set the DNS address of the PC to the IPv6 address of the DNS64 device.

Step 7 Configure the IPv4 address and route of the server. (The method of setting the IPv4 address is determined by the operating system of the server. The setting method is not described here.)

Set the IPv4 address of the server to **2.2.2.2/24**.

Configure a route from the server to the address range **1.1.1.6 to 1.1.1.10**. The next hop of the route is the address of the IPv4 network egress router.

----End

Verifying the Configuration

1. Access example.huawei.com from the PC. The access succeeds.
2. Check NAT64 session table information.

```
<DeviceA> display firewall ipv6 session table verbose vsys vsysa
 Current Total IPv6 Sessions : 1
 NAT64: icmpv6  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust TTL: 00:00:45  Left: 00:00:45
 Interface: GE0/0/1 NextHop: 1.1.1.254 MAC: xxxx-xxxx-xxxx
 <--packets: 25 bytes: 2,600 --> packets: 25 bytes: 2,600
 2001:db8:3::1.44019[1.1.1.7:2051] --> 2001:db8:2::202:202.2048[2.2.2.2:2048] PolicyName:
policy_sec_1
```

Configuration Scripts

- Public system

 Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname DeviceA
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/1
 assign global-ip 1.1.1.6 1.1.1.10 exclusive
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface  Virtual-if 0
 ip address 172.16.0.1 24
#
firewall zone trust
 set priority 85
 add interface Virtual-if 0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
 ip route-static 2.2.2.0 24 1.1.1.254
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    destination-address 2.2.2.2 24
    action permit
#
return
```

- vsysa

```
#
switch vsys vsysa
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:db8:1::1/64
 nat64 enable

#
interface Virtual-if 1
 ip address 172.16.1.1 24
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
 add interface Virtual-if 1
#
nat address-group addressgroup1
 mode pat
 section 1 1.1.1.6 1.1.1.10
#
 nat64 prefix 2001:db8:2:: 96
#
 ip route-static 2.2.2.2 32 public
 ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
#
nat-policy
  rule name policy_nat64
    source-zone untrust
    destination-zone trust
    nat-type nat64
    source-address 2001:db8:3:: 64
    action source-nat address-group addressgroup1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

16.13 CLI: Example for Configuring an IPv6 User on a Private Network to Access an IPv4 Server on Another Private Network (Access Between Virtual Systems)

Networking Requirements

As shown in **Figure 16-13**, the virtual system **vsysa** supports the IPv6/IPv4 dual stack and is connected to an IPv6 network and an IPv4 network. It is required that a PC on the private IPv6 network be able to access a server on the public IPv4 network through domain name **example.huawei.com** and across multiple virtual systems.

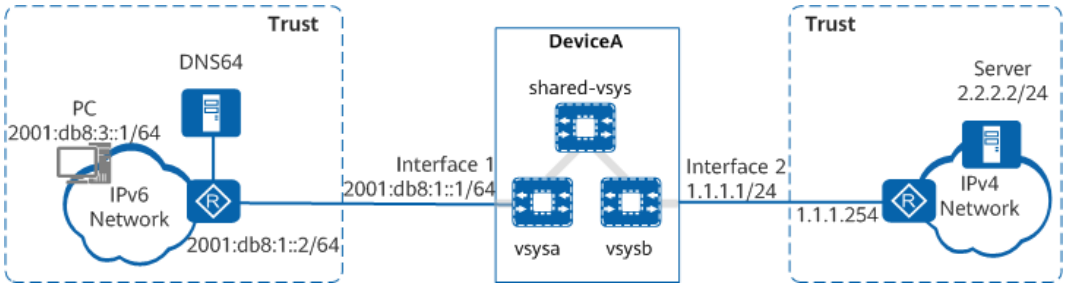
NOTE

Usually, the NAT64 is deployed with the DNS64. The DNS64 performs domain name translation. The prefix and length configured for the DNS64 are the same as those of the NAT64 device.

Figure 16-13 Networking diagram for configuring dynamic NAT64 in virtual systems

NOTE

In this example, interfaces 1 and 2 represent GE0/0/1 and GE0/0/2, respectively.



Procedure

Step 1 Create virtual system **vsysa** and assign an interface and a public address to it.

Enable the virtual system function.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vsys enable
```

Create a virtual system and assign an interface and a public address to it. The public address is used in the NAT address pool.

```
[DeviceA] vsys name vsysa
[DeviceA-vsys-vsysa] assign interface ge 0/0/1
[DeviceA-vsys-vsysa] assign global-ip 1.1.1.6 1.1.1.10 exclusive
[DeviceA-vsys-vsysa] quit
```

Step 2 Create virtual system **vsysb** and assign an interface and a public address to it.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] vsys name vsysb
[DeviceA-vsys-vsysb] assign interface ge 0/0/2
[DeviceA-vsys-vsysb] quit
```

Step 3 Create virtual system **shared_vsys**.

```
[DeviceA] vsys name shared_vsys
[DeviceA-vsys-shared_vsys] quit
```

Step 4 Configure virtual systems to communicate in extended mode.

```
[DeviceA] firewall forward cross-vsys extended
```

Configure a static route to **shared_vsys**.

```
[DeviceA] ip route-static 2.2.2.2 32 vpn-instance shared_vsys
```

Configure a static route to **vsysb**.

```
[DeviceA] ip route-static 2.2.2.2 32 vpn-instance vsysb
```

Step 5 Configure IP addresses, routes, and security policies.

Access the configuration view of virtual system **vsysa**.

```
[DeviceA] switch vsys vsysa
```

Set an IP address for an interface and assign the interface to a security zone. The IP address of Virtual-if1 can be any value as long as it is not in conflict with the IP address on any other interface.

```
<DeviceA-vsysa> system-view
[DeviceA-vsysa] interface ge 0/0/1
[DeviceA-vsysa-GE0/0/1] ipv6 enable
[DeviceA-vsysa-GE0/0/1] ipv6 address 2001:db8:1::1 64
[DeviceA-vsysa-GE0/0/1] quit
[DeviceA-vsysa] interface  Virtual-if 1
[DeviceA-Virtual-if1] ip address 172.16.1.1 24
[DeviceA-Virtual-if1] quit
[DeviceA-vsysa] firewall zone trust
[DeviceA-vsysa-zone-trust] add interface ge 0/0/1
[DeviceA-vsysa-zone-trust] quit
[DeviceA-vsysa] firewall zone untrust
[DeviceA-vsysa-zone-untrust] add interface Virtual-if 1
[DeviceA-vsysa-zone-untrust] quit
```

Configure a static route to the IPv6 network.

```
[DeviceA-vsysa] ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
```

Configure a security policy.

```
[DeviceA-vsysa] security-policy
[DeviceA-vsysa-policy-security] rule name policy_sec_1
[DeviceA-vsysa-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-vsysa-policy-security-rule-policy_sec_1] source-address 2001:db8:3:: 64
[DeviceA-vsysa-policy-security-rule-policy_sec_1] action permit
[DeviceA-vsysa-policy-security-rule-policy_sec_1] quit
[DeviceA-vsysa-policy-security] quit
[DeviceA-vsysa] quit
<DeviceA-vsysb> quit
```

Access the configuration view of virtual system **shared_vsys**.

```
[DeviceA] switch vsys shared_vsys
<DeviceA-shared_vsys> system-view
```

Set an IP address for an interface and assign the interface to a security zone. The IP address of Virtual-if2 can be any value as long as it does not conflict with the IP address on any other interface.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-shared_vsys] interface  Virtual-if 2
[DeviceA-Virtual-if2] ip address 172.16.2.1 24
[DeviceA-Virtual-if2] quit
[DeviceA-shared_vsys] firewall zone untrust
[DeviceA-shared_vsys-zone-untrust] add interface Virtual-if 2
[DeviceA-shared_vsys-zone-untrust] quit
[DeviceA-shared_vsys] quit
<DeviceA-vsysb> quit
```

Access the configuration view of virtual system **vsysb**.

```
[DeviceA] switch vsys vsysb
<DeviceA-shared_vsys> system-view
```

Set an IP address for an interface and assign the interface to a security zone. The IP address of Virtual-if3 can be set to any address different from the IP addresses of all the other interfaces.

```
[DeviceA-vsysb] interface Virtual-if 3
[DeviceA-Virtual-if3] ip address 172.16.3.1 24
[DeviceA-Virtual-if3] quit
[DeviceA-vsysb] interface ge 0/0/2
[DeviceA-vsysb-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-vsysb-GE0/0/2] quit
[DeviceA-vsysb] firewall zone trust
[DeviceA-vsysb-zone-trust] add interface ge 0/0/2
[DeviceA-vsysb-zone-trust] quit
[DeviceA-vsysb] firewall zone untrust
[DeviceA-vsysb-zone-untrust] add interface Virtual-if 3
[DeviceA-vsysb-zone-untrust] quit
```

Configure a static route to the IPv4 network.

```
[DeviceA-vsysb] ip route-static 2.2.2.0 24 1.1.1.254
```

Configure a security policy.

```
[DeviceA-vsysb] security-policy
[DeviceA-vsysb-policy-security] rule name policy_sec_3
[DeviceA-vsysb-policy-security-rule-policy_sec_3] source-zone untrust
[DeviceA-vsysb-policy-security-rule-policy_sec_3] destination-zone trust
[DeviceA-vsysb-policy-security-rule-policy_sec_3] destination-address 2.2.2.2 24
[DeviceA-vsysb-policy-security-rule-policy_sec_3] action permit
[DeviceA-vsysb-policy-security-rule-policy_sec_3] quit
[DeviceA-vsysb-policy-security] quit
[DeviceA-vsysb] quit
<DeviceA-vsysb> quit
```

Step 6 Configure NAT64.

Enable the NAT64 function on the IPv6 network interface.

```
[DeviceA] switch vsys vsysa
<DeviceA-shared_vsys> system-view
[DeviceA-vsysa] interface ge 0/0/1
[DeviceA-vsysa-GE0/0/1] nat64 enable
[DeviceA-vsysa-GE0/0/1] quit
```

Set the NAT64 prefix to 2001:db8:2::/96.

```
[DeviceA-vsysa] nat64 prefix 2001:db8:2:: 96
```

NOTE

In this example, the NAT64 prefix is **2001:db8:2::/96**. If the prefix is left unconfigured, a well-known prefix is used by default.

Configure IPv4 NAT address pool **addressgroup1** and set the address range to **1.1.1.6 to 1.1.1.10**. Use the addresses in the NAT address pool as the IPv4 addresses after the NAT64 processing.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-vsysa] nat address-group addressgroup1
[DeviceA-vsysa-address-group-addressgroup1] mode pat
[DeviceA-vsysa-address-group-addressgroup1] section 1 1.1.1.6 1.1.1.10
[DeviceA-vsysa-address-group-addressgroup1] quit
```

Configure dynamic NAT64 mapping.

```
[DeviceA-vsysa] nat-policy
[DeviceA-vsysa-policy-nat] rule name policy_nat64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] nat-type nat64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] source-zone trust
[DeviceA-vsysa-policy-nat-rule-policy_nat64] destination-zone trust
[DeviceA-vsysa-policy-nat-rule-policy_nat64] source-address 2001:db8:3:: 64
[DeviceA-vsysa-policy-nat-rule-policy_nat64] action source-nat address-group addressgroup1
[DeviceA-vsysa-policy-nat-rule-policy_nat64] quit
[DeviceA-vsysa-policy-nat] quit
[DeviceA-vsysb] quit
<DeviceA-vsysb> quit
```

Step 7 Configure the DNS64 device.

Set the IPv6 prefix of the DNS64 device to the NAT64 prefix of the DeviceA, namely, **2001:db8:2::/96**.

Configure a route from the DNS64 to the PC to ensure reachability.

Step 8 Configure the IPv6 address, route, and DNS of the PC. (The configuration methods of IPv6 addresses and routes vary with the operating systems of the PCs. The configuration methods are not described here.)

Set the IPv6 address of the PC to **2001:db8:3::1/64**.

Configure a route from the PC to the network segment 2001:db8:2::/96 and set the next hop to the address of the IPv6 network egress router.

Set the DNS address of the PC to the IPv6 address of the DNS64 device.

Step 9 Configure the IPv4 address and route of the server. (The method of setting the IPv4 address is determined by the operating system of the server. The setting method is not described here.)

Set the IPv4 address of the server to **2.2.2.2/24**.

Configure a route from the server to the address range **1.1.1.6 to 1.1.1.10**. The next hop of the route is the address of the IPv4 network egress router.

----End

Verifying the Configuration

1. Access **example.huawei.com** from the PC. The access succeeds.
2. Check NAT64 session table information.

```
<DeviceA> display firewall ipv6 session table verbose vsys vsysa
 Current Total IPv6 Sessions : 1
 NAT64: icmpv6  VPN: vsysa --> vsysa  ID: xxxxxxxxxxxxxxxxxxxxxx
 Zone: untrust --> trust TTL: 00:00:45  Left: 00:00:45
 Interface: GE0/0/1 NextHop: 1.1.1.254 MAC: xxxx-xxxx-xxxx
 <--packets: 25 bytes: 2,600 --> packets: 25 bytes: 2,600
 2001:db8:3::1.44019[1.1.1.7:2051] --> 2001:db8:2::202:202.2048[2.2.2.2:2048] PolicyName:
policy_sec_1
```

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

- Public system

```
#
 sysname DeviceA
#
 vsys enable
#
vsys name vsysa 1
 assign interface GE0/0/1
 assign global-ip 1.1.1.6 1.1.1.10 exclusive
vsys name vsysb 2
 assign interface GE0/0/2
vsys name shared_vsys
#
 firewall forward cross-vsys extended
#
return
```

- vsysa

```
#
switch vsys vsysa
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2001:db8:1::1 64
 nat64 enable
#
interface  Virtual-if 1
 ip address 172.16.1.1 24
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 85
 add interface Virtual-if 1
#
nat address-group addressgroup1
 mode pat
 section 1 1.1.1.6 1.1.1.10
#
 nat64 prefix 2001:db8:2:: 96
#
 ip route-static 2.2.2.2 32 vpn-instance shared_vsys
 ipv6 route-static 2001:db8:3:: 64 2001:db8:1::2
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 2001:db8:3:: 64
    action permit
#
nat-policy
  rule name policy_nat64
    source-zone trust
    destination-zone trust
    nat-type nat64
    source-address 2001:db8:3:: 64
    action source-nat address-group addressgroup1
#
return
```

- shared_vsys

```
#
switch vsys shared_vsys
#
interface  Virtual-if 2
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip address 172.16.2.1 24
firewall zone untrust
 set priority 85
 add interface Virtual-if 2
#
ip route-static 2.2.2.2 32 vpn-instance vsysb
#
return
```

- vsysb

```
#
switch vsys vsysb
#
interface  Virtual-if 3
 ip address 172.16.3.1 24
interface GE0/0/2
 ip address 1.1.1.1 24
firewall zone trust
 set priority 85
 add interface GE0/0/2
#
firewall zone untrust
 set priority 15
 add interface Virtual-if 2
#
ip route-static 2.2.2.0 24 1.1.1.254
#
security-policy
 rule name policy_sec_3
 source-zone untrust
 destination-zone trust
 destination-address 2.2.2.2 24
 action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

17 Traffic Management

17.1 Web: Example for Configuring Maximum Bandwidth and Guaranteed Bandwidth

17.2 CLI: Example for Configuring Maximum Bandwidth and Guaranteed Bandwidth

17.3 Web: Example for Configuring the Connection Limit

17.4 CLI: Example for Configuring the Connection Limit

17.5 CLI: Example for Configuring Bandwidth Control Based on Public IP Addresses

17.1 Web: Example for Configuring Maximum Bandwidth and Guaranteed Bandwidth

Networking Requirements

As shown in **Figure 17-1**, an enterprise purchases 100 Mbit/s bandwidth from an ISP. On office networks, email and ERP traffic is key service traffic, and P2P and online video traffic is non-key service traffic. However, P2P and online video traffic exhausts the limited bandwidth resources on the enterprise network, and key service traffic, such as email and ERP traffic, is not properly forwarded. As a result, emails fail to be sent, and web pages fail to be displayed, which greatly affects the daily operation of the enterprise.

To prevent the preceding symptoms, the enterprise requires to enable the bandwidth management function on the device to meet the following requirements:

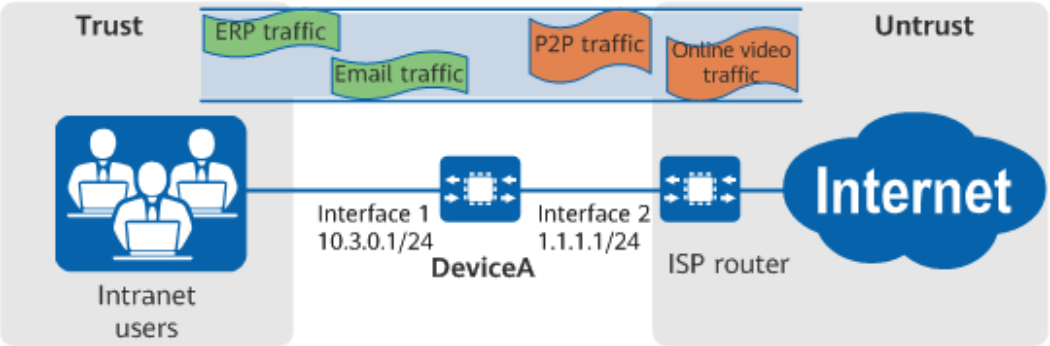
- Restrict P2P and online video traffic within 30 Mbit/s at any time.
- Assign a minimum of 60 Mbit/s bandwidth for applications, such as email and ERP.

 Copyright © Huawei Technologies Co., Ltd.

Figure 17-1 Networking diagram for configuring the maximum and guaranteed bandwidth for bandwidth management on enterprise networks

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.



Configuration Roadmap

1. Set interface IP addresses and assign the interfaces to security zones.
2. Configure a bandwidth policy for P2P and online video applications and reference the bandwidth profile in which the overall maximum bandwidth is 30 Mbit/s.
3. Configure a bandwidth policy for email and ERP applications and reference the bandwidth profile in which the overall guaranteed bandwidth is 60 Mbit/s.
4. Configure a security policy to allow intranet users to access the Internet.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/1 and set the parameters as follows.

Zone	trust
IPv4	
IP Address	10.3.0.1/255.255.255.0

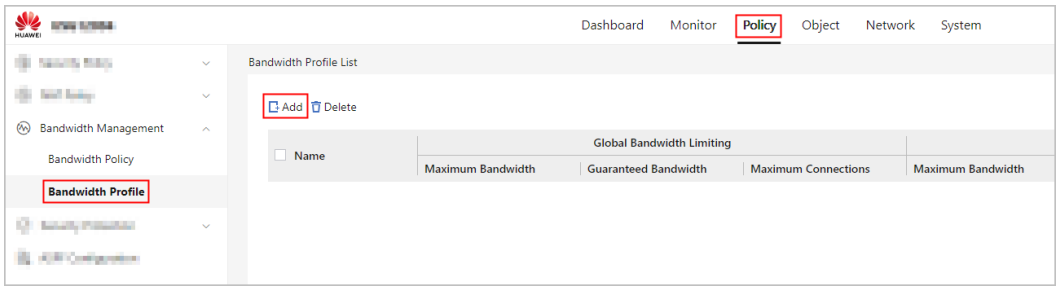
3. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	untrust
IPv4	
IP Address	1.1.1.1/255.255.255.0

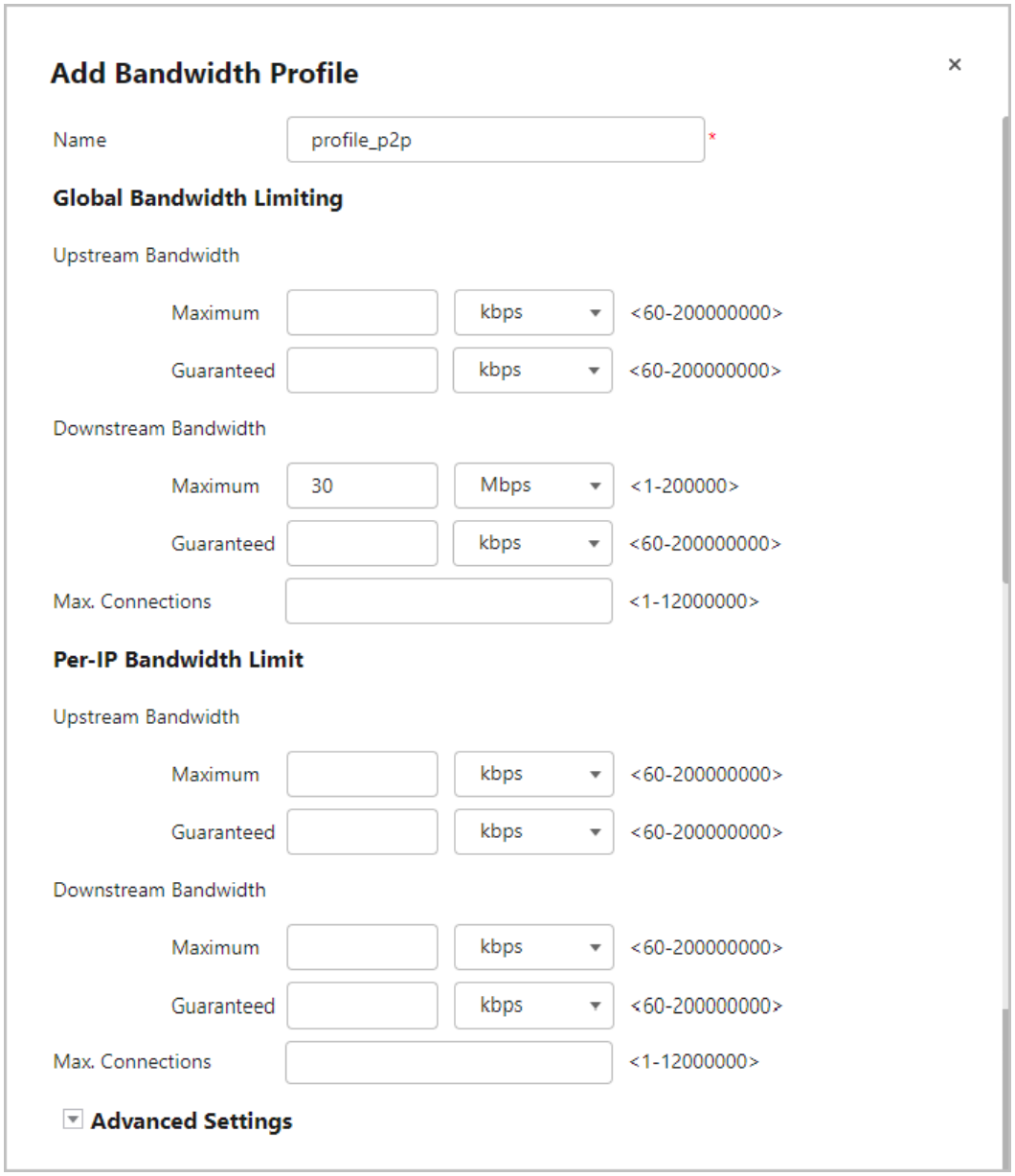
Step 2 Configure a bandwidth profile for P2P and online video services and for email and ERP services respectively.

1. Choose **Policy** > **Bandwidth Management** > **Bandwidth Profile**. In **Bandwidth Profile List**, click **Add**

 Copyright © Huawei Technologies Co., Ltd.

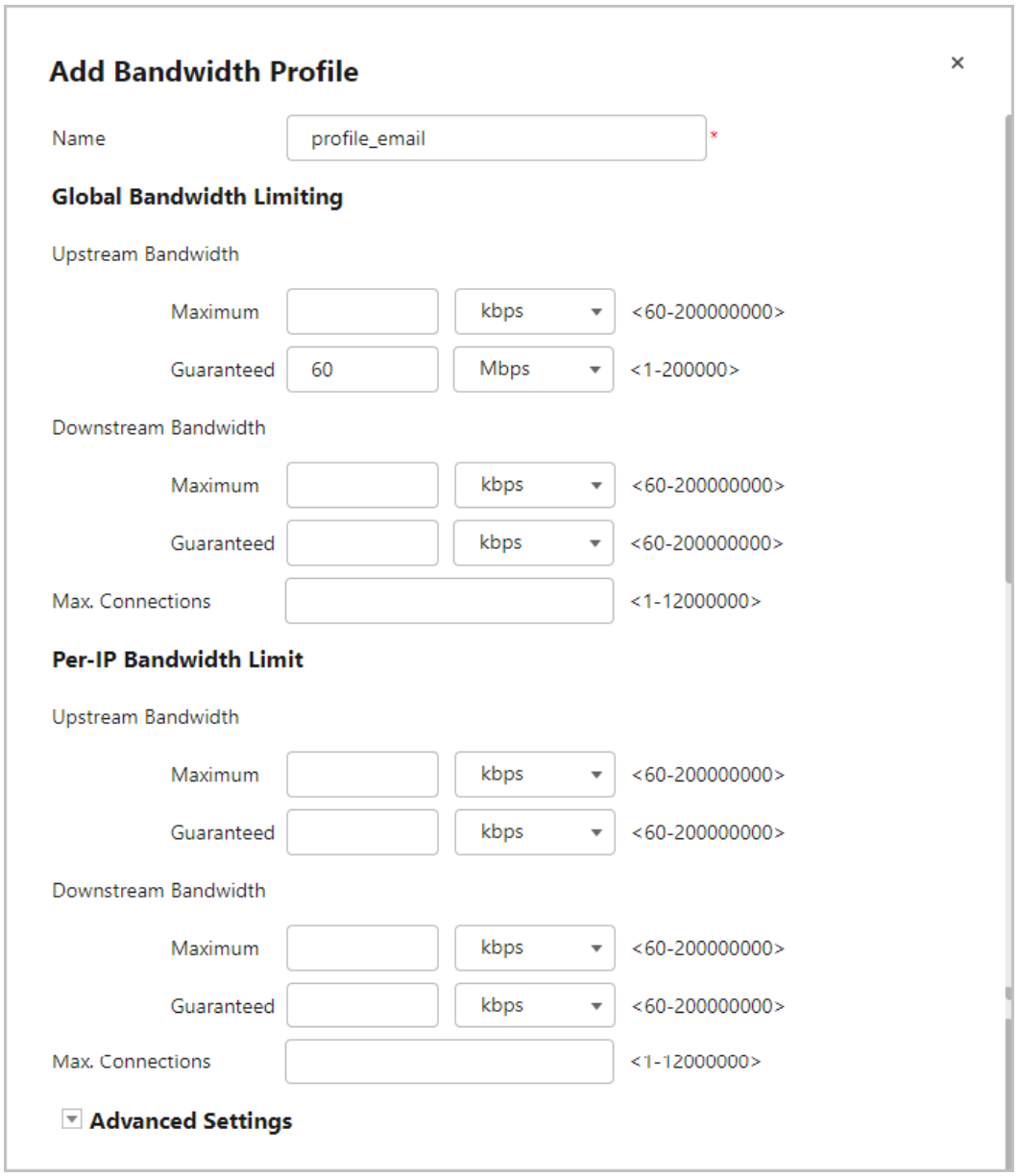


2. Configure a bandwidth profile for P2P and online video services. Set the maximum width to 30 Mbit/s.



3. Configure a bandwidth profile for email and ERP services. Set the guaranteed width to 60 Mbit/s.

 Copyright © Huawei Technologies Co., Ltd.



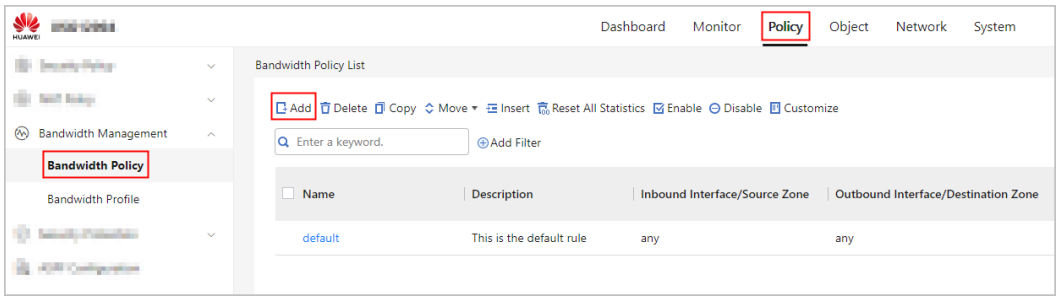
Step 3 Configure a bandwidth policy for P2P and online video services and for email and ERP services respectively.

NOTE

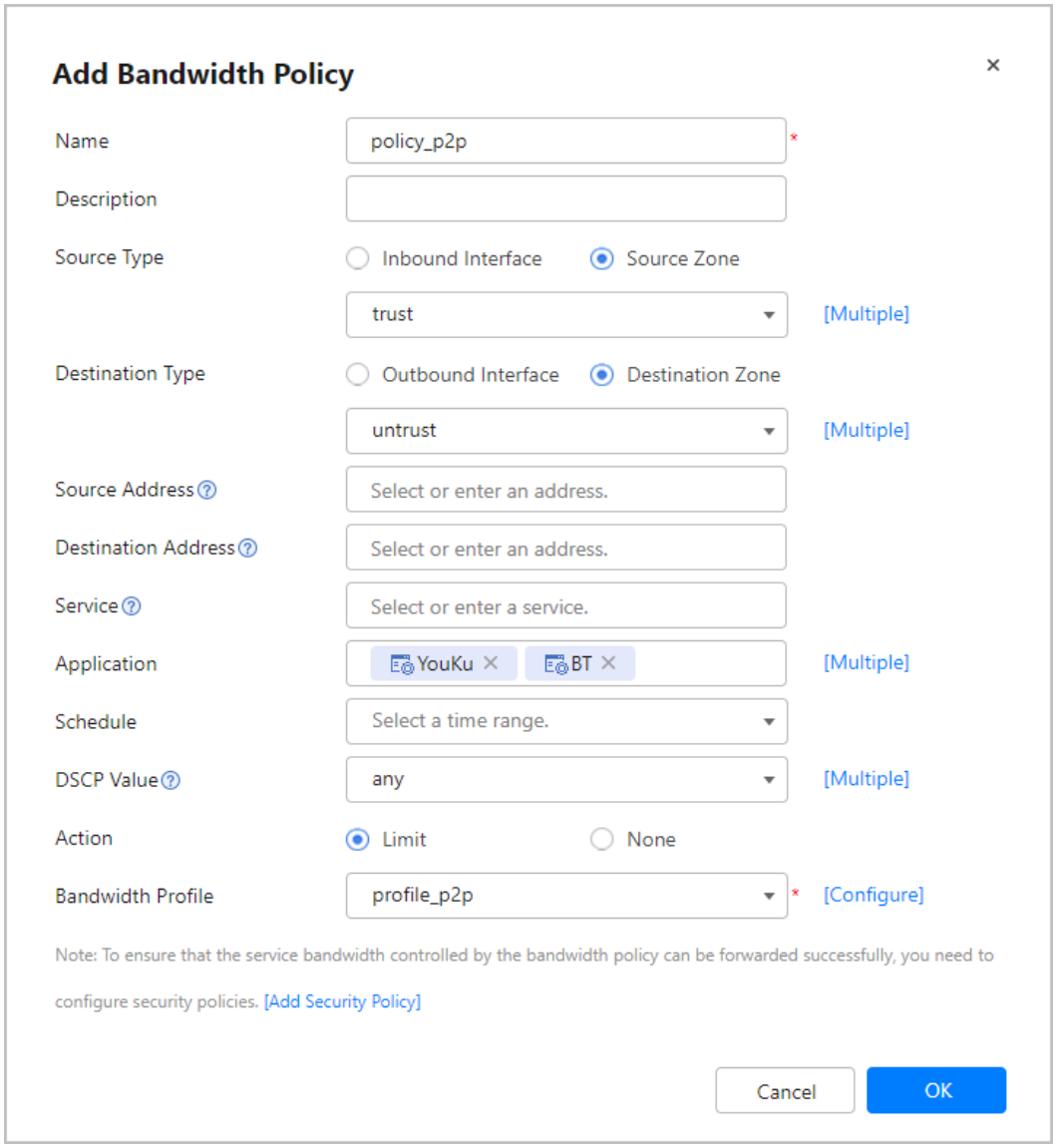
- The following example describes the bandwidth management configuration for BitTorrent (BT) and Youku services. Specify the application based on the site requirements.
- The following example describes the bandwidth management configuration for Outlook Web Access and LotusNotes. Specify the application based on the site requirements.

1. Choose **Policy** > **Bandwidth Management** > **Bandwidth Policy**. In **Bandwidth Policy List**, click **Add**

 Copyright © Huawei Technologies Co., Ltd.

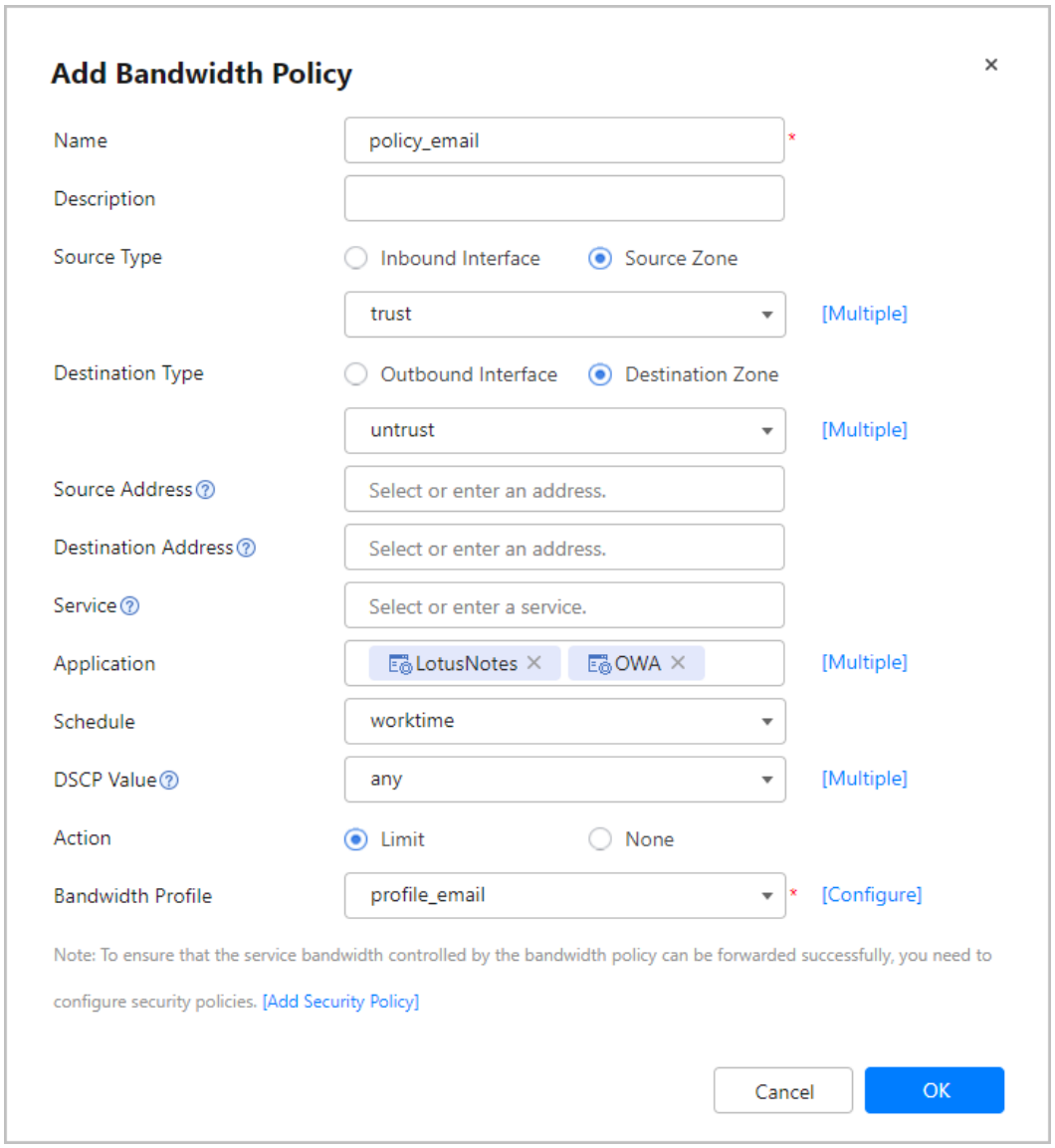


2. Configure a traffic policy for P2P and online video services.



3. Configure a bandwidth policy for email and ERP services.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure a security policy to allow intranet users to access the Internet. In actual configuration, you are advised to configure refined security policies based on networking requirements.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Action	Permit

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

- When a large amount of P2P and online video traffic exists, check whether key service traffic, such as email and ERP traffic, is properly forwarded.
- Run the **display bandwidth-policy statistic bandwidth** command on DeviceA to view bandwidth policy statistics. In the command output, **Rcv-Rate** and **Pass-Rate** indicate the number of received packets per second before and after rate limiting, respectively.

```
<DeviceA> display bandwidth-policy statistic bandwidth whole upstream rule policy_p2p
Bandwidth Statistic:
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Drop Packets), DB(Drop Bytes)
------------------------------------------------------------------------------
Rule        Profile       PP     PB    DP     DB     Rcv-Rate    Pass-Rate
------------------------------------------------------------------------------
policy_p2p    profile_p2p   3141  34480  63321   815088   259704   30056
------------------------------------------------------------------------------
```

Configuration Scripts

This section provides only the script related to the example.

```
#
sysname DeviceA
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
security-policy
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
bandwidth-policy
 profile name profile_p2p
  bandwidth maximum-bandwidth whole downstream 30000
 profile name profile_email
  bandwidth guaranteed-bandwidth whole upstream 60000
 rule name policy_p2p
  source-zone trust
  destination-zone untrust
  application app BT
  application app YouKu
  action qos profile profile_p2p
 rule name policy_email
  source-zone trust
  destination-zone untrust
  application app LotusNotes
  application app OWA
  time-range work_time
  action qos profile profile_email
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

17.2 CLI: Example for Configuring Maximum Bandwidth and Guaranteed Bandwidth

Networking Requirements

As shown in **Figure 17-2**, an enterprise purchases 100 Mbit/s bandwidth from an ISP. On office networks, email and ERP traffic is key service traffic, and P2P and online video traffic is non-key service traffic. However, P2P and online video traffic exhausts the limited bandwidth resources on the enterprise network, and key service traffic, such as email and ERP traffic, is not properly forwarded. As a result, emails fail to be sent, and web pages fail to be displayed, which greatly affects the daily operation of the enterprise.

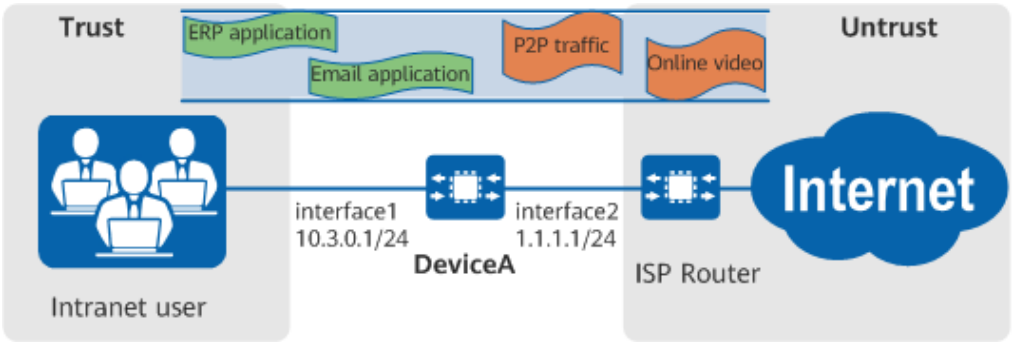
To prevent the preceding symptoms, the enterprise requires to enable the bandwidth management function on the device to meet the following requirements:

- Restrict P2P and online video traffic within 30 Mbit/s at any time.
- Assign a minimum of 60 Mbit/s bandwidth for applications, such as email and ERP.

Figure 17-2 Networking diagram for configuring the maximum and guaranteed bandwidth for bandwidth management on enterprise networks

NOTE

In this example, interface1 and interface2 represent GE0/0/1 and GE0/0/2, respectively.



Configuration Roadmap

1. Set interface IP addresses and assign the interfaces to security zones.
2. Configure a bandwidth policy for P2P and online video applications and reference the bandwidth profile in which the overall maximum bandwidth is 30 Mbit/s.
3. Configure a bandwidth policy for email and ERP applications and reference the bandwidth profile in which the overall guaranteed bandwidth is 60 Mbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Set an IP address for interface GE0/0/2 and add the interface to the Untrust zone.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge0/0/2
[DeviceA-zone-untrust] quit
```

2. Set an IP address for interface GE0/0/1 and add the interface to the Trust zone.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.3.0.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

3. Configure a security policy to allow intranet users to access the Internet. In actual configuration, you are advised to configure refined security policies based on networking requirements.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec
[DeviceA-policy-security-rule-policy_sec] source-zone trust
[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec] action permit
[DeviceA-policy-security-rule-policy_sec] quit
```

Step 2 Configure a schedule.

```
[DeviceA] time-range work_time 09:00 to 18:00 working-day
```

Step 3 Configure a bandwidth profile for P2P and online video services.

```
[DeviceA] bandwidth-policy
[DeviceA-policy-bandwidth] profile name profile_p2p
[DeviceA-policy-bandwidth-profile-profile_p2p] bandwidth maximum-bandwidth whole upstream 30000
[DeviceA-policy-bandwidth-profile-profile_p2p] bandwidth maximum-bandwidth whole downstream
30000
[DeviceA-policy-bandwidth-profile-profile_p2p] quit
```

Step 4 Configure a bandwidth policy for P2P and online video services.

NOTE

The following example describes the bandwidth management configuration for BitTorrent (BT) and Youku services. You can specify other P2P services as required.

```
[DeviceA-policy-bandwidth] rule name policy_p2p
[DeviceA-policy-bandwidth-rule-policy_p2p] source-zone trust
[DeviceA-policy-bandwidth-rule-policy_p2p] destination-zone untrust
[DeviceA-policy-bandwidth-rule-policy_p2p] application app BT
[DeviceA-policy-bandwidth-rule-policy_p2p] application app YouKu
[DeviceA-policy-bandwidth-rule-policy_p2p] action qos profile profile_p2p
[DeviceA-policy-bandwidth-rule-policy_p2p] quit
```

Step 5 Configure a bandwidth profile for email and ERP services.

```
[DeviceA-policy-bandwidth] profile name profile_email
[DeviceA-policy-bandwidth-profile-profile_email] bandwidth guaranteed-bandwidth whole upstream
60000
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-bandwidth-profile-profile_email] bandwidth guaranteed-bandwidth whole downstream
60000
[DeviceA-policy-bandwidth-profile-profile_email] quit
```

Step 6 Configure a bandwidth policy for email and ERP services.

NOTE

The following example describes the bandwidth management configuration for Outlook Web Access and LotusNotes. You can specify other P2P services as required.

```
[DeviceA-policy-bandwidth] rule name policy_email
[DeviceA-policy-bandwidth-rule-policy_email] source-zone trust
[DeviceA-policy-bandwidth-rule-policy_email] destination-zone untrust
[DeviceA-policy-bandwidth-rule-policy_email] application app LotusNotes
[DeviceA-policy-bandwidth-rule-policy_email] application app OWA
[DeviceA-policy-bandwidth-rule-policy_email] time-range work_time
[DeviceA-policy-bandwidth-rule-policy_email] action qos profile profile_email
[DeviceA-policy-bandwidth-rule-policy_email] quit
```

----End

Verifying the Configuration

- When a large amount of P2P and online video traffic exists, check whether key service traffic, such as email and ERP traffic, is properly forwarded.
- Run the **display bandwidth-policy statistic bandwidth** command on DeviceA to view bandwidth policy statistics. In the command output, **Rcv-Rate** and **Pass-Rate** indicate the number of received packets per second before and after rate limiting, respectively.

```
<DeviceA> display bandwidth-policy statistic bandwidth whole upstream rule policy_p2p
Bandwidth Statistic:
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Drop Packets), DB(Drop Bytes)
------------------------------------------------------------------------------
Rule       Profile      PP    PB    DP    DB    Rcv-Rate   Pass-Rate
------------------------------------------------------------------------------
policy_p2p   profile_p2p   3141  34480  63321   815088   259704   30056
------------------------------------------------------------------------------
```

Configuration Scripts

This section provides only the script related to the example.

```
#
sysname DeviceA
#
 time-range work_time 09:00 to 18:00 working-day
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
security-policy
 rule name policy_sec
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone untrust
 action permit
#
bandwidth-policy
 profile name profile_p2p
  bandwidth maximum-bandwidth whole upstream 30000
  bandwidth maximum-bandwidth whole downstream 30000
 profile name profile_email
  bandwidth guaranteed-bandwidth whole upstream 60000
  bandwidth guaranteed-bandwidth whole downstream 60000
 rule name policy_p2p
  source-zone trust
  destination-zone untrust
  application app BT
  application app YouKu
  action qos profile profile_p2p
 rule name policy_email
  source-zone trust
  destination-zone untrust
  application app LotusNotes
  application app OWA
  time-range work_time
  action qos profile profile_email
```

17.3 Web: Example for Configuring the Connection Limit

Networking Requirements

As shown in **Figure 17-3**, an enterprise purchases 100 Mbit/s bandwidth from an ISP. On office networks, email and ERP traffic is key service traffic, and P2P and online video traffic is non-key service traffic. However, P2P and online video traffic exhausts the limited bandwidth resources on the enterprise network, and key service traffic, such as email and ERP traffic, is not properly forwarded. As a result, emails fail to be sent, and web pages fail to be displayed, which greatly affects the daily operation of the enterprise.

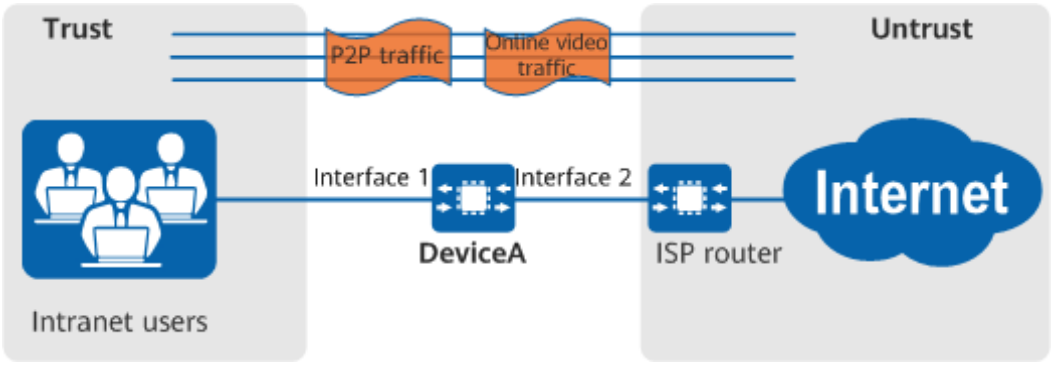
To solve the preceding problems, the enterprise administrator wants to use the bandwidth management function provided by the device. The enterprise administrator can set the maximum number of connections to 10000 to control P2P and online video traffic.

Figure 17-3 Networking diagram for configuring the maximum and guaranteed bandwidth for bandwidth management on enterprise networks

NOTE

In this example, interface 1 and interface 2 represent GE0/0/1 and GE0/0/2, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

1. Set interface IP addresses and assign the interfaces to security zones.
2. Configure a bandwidth policy for P2P and online video applications and a bandwidth profile in which the overall maximum number of connections is 10000.
3. Configure a security policy to allow intranet users to access the Internet.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click corresponding to GE0/0/1 and set the parameters as follows.

Zone	trust
IPv4	
IP Address	10.3.0.1/255.255.255.0

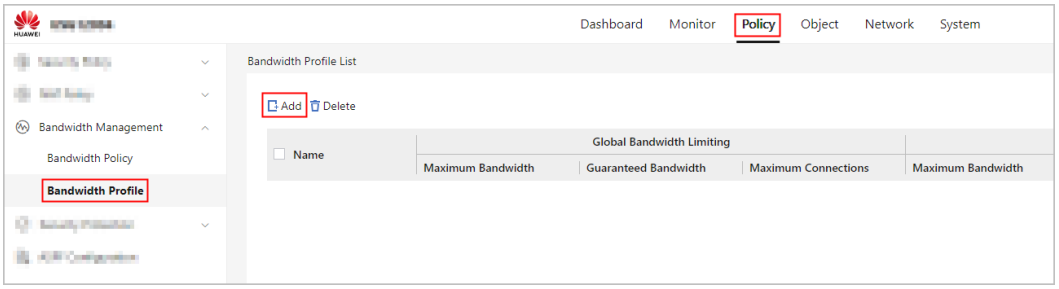
3. Repeat the preceding steps to set the parameters for GE0/0/2.

Zone	untrust
IPv4	
IP Address	1.1.1.1/255.255.255.0

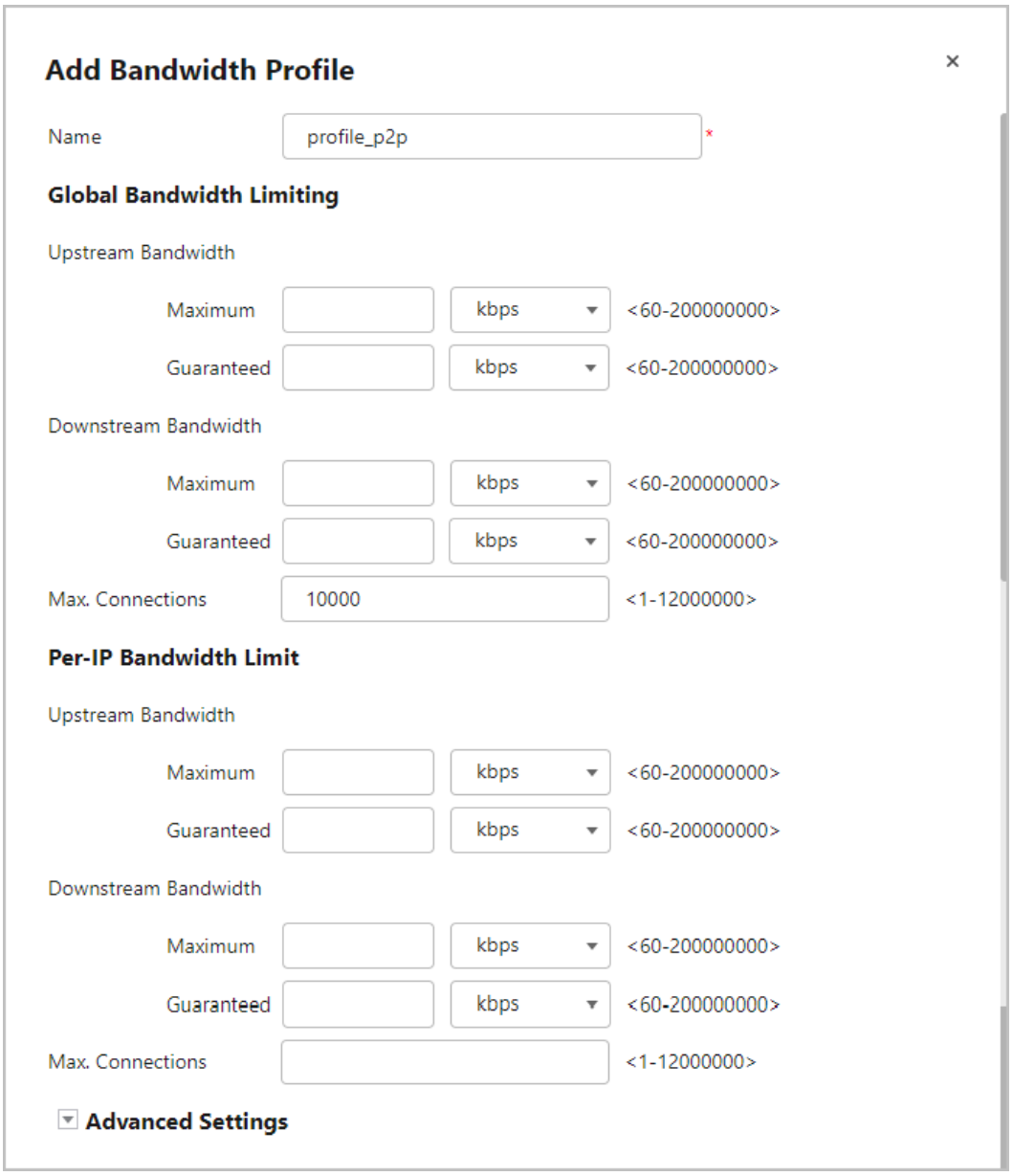
Step 2 Configure a bandwidth profile for P2P and online video services.

1. Choose **Policy** > **Bandwidth Management** > **Bandwidth Profile**. In **Bandwidth Profile List**, click **Add**

 Copyright © Huawei Technologies Co., Ltd.



2. Configure a traffic profile for P2P and online video services and set the overall maximum number of connections to 10000.



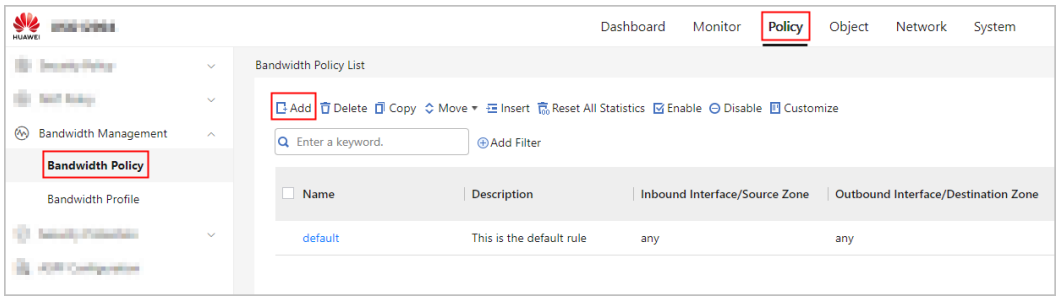
Step 3 Configure a traffic policy for P2P and online video services.

NOTE

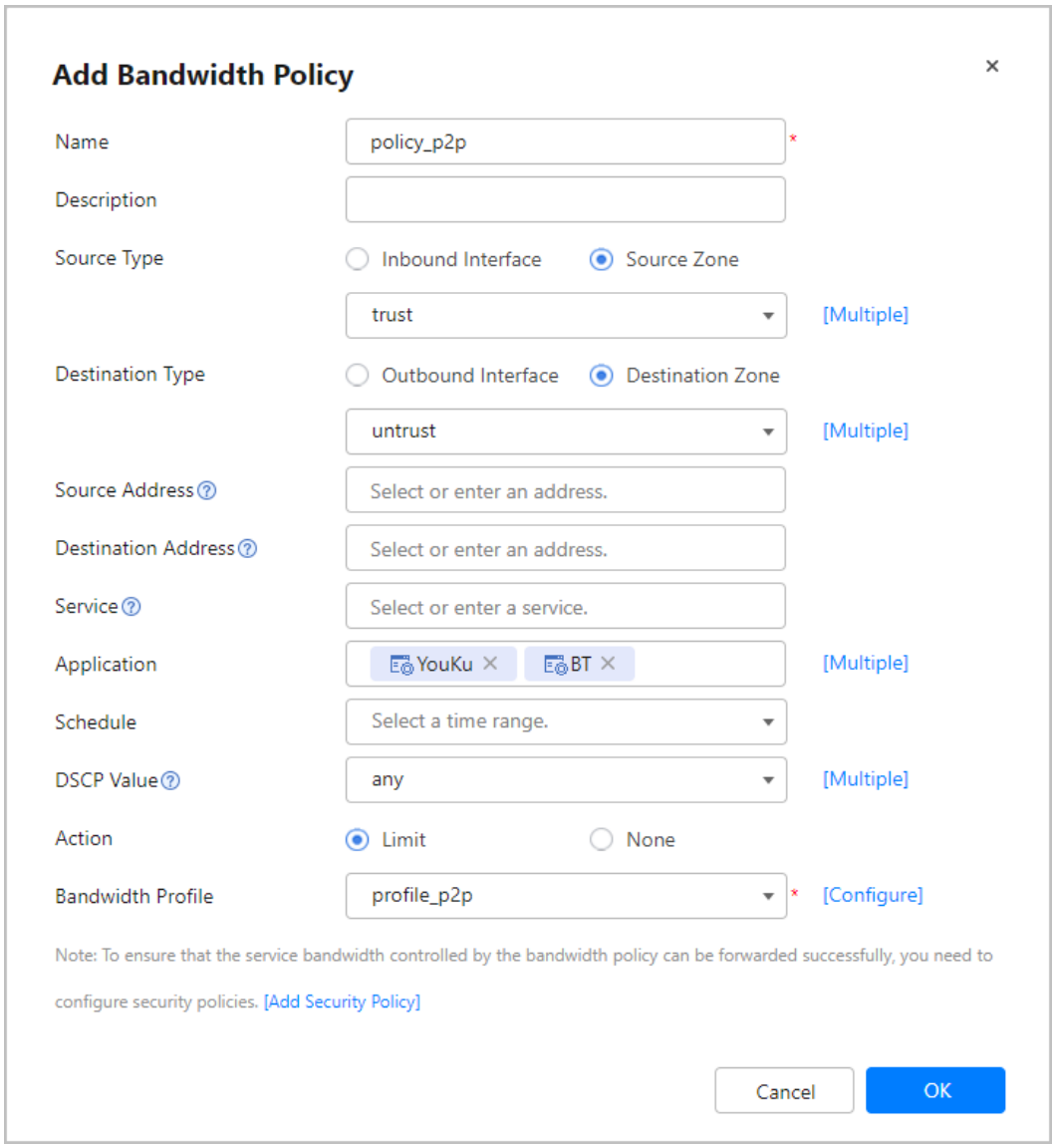
- The following example describes the bandwidth management configuration for BitTorrent (BT) and Youku services.

 Copyright © Huawei Technologies Co., Ltd.

1. Choose **Policy** > **Bandwidth Management** > **Bandwidth Policy**. In **Bandwidth Policy List**, click **Add**



2. Configure a traffic policy for P2P and online video services.



Step 4 Configure a security policy to allow intranet users to access the Internet. In actual configuration, you are advised to configure refined security policies based on networking requirements.

1. Choose **Policy** > **Security Policy** > **Security Policy**.

 Copyright © Huawei Technologies Co., Ltd.

2. In **Security Policy List**, click **Add Security Policy** and configure a security policy based on the following parameter values.

Name	policy_sec
Source Zone	trust
Destination Zone	untrust
Action	Permit

----End

Verifying the Configuration

When a large amount of P2P and online video traffic exists, run the **display bandwidth-policy statistic connection** command on DeviceA to view statistics about the connection limit. In the command output, **CC** indicates the number of current connections.

```
<DeviceA> display bandwidth-policy statistic connection-limit whole both all
Statistic:  Total current items: 1
Codes: CC(Current Connection), RC(Rejective Connection)
------------------------------------------------------------------------------
 Policy        Profile     CC         RC
------------------------------------------------------------------------------
policy_p2p     profile_p2p     10000      5435
------------------------------------------------------------------------------
```

Configuration Scripts

This section provides only the script related to the example.

```
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
security-policy
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
bandwidth-policy
 profile name profile_p2p
  bandwidth connection-limit whole both 10000
 rule name policy_p2p
  source-zone trust
  destination-zone untrust
  application app BT
  application app YouKu
  action qos profile profile_p2p
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

17.4 CLI: Example for Configuring the Connection Limit

Networking Requirements

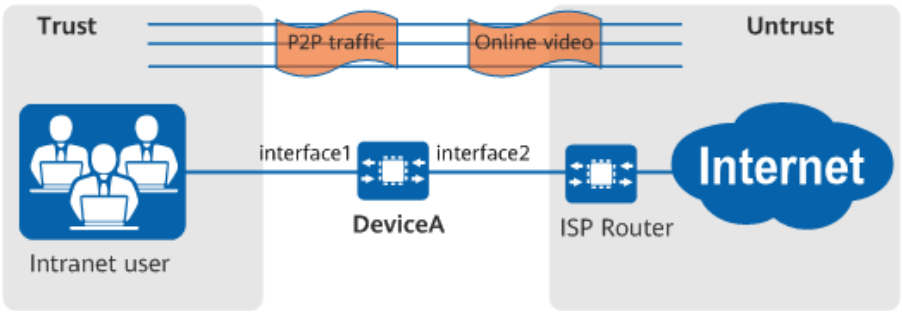
As shown in **Figure 17-4**, an enterprise purchases 100 Mbit/s bandwidth from an ISP. On office networks, email and ERP traffic is key service traffic, and P2P and online video traffic is non-key service traffic. However, P2P and online video traffic exhausts the limited bandwidth resources on the enterprise network, and key service traffic, such as email and ERP traffic, is not properly forwarded. As a result, emails fail to be sent, and web pages fail to be displayed, which greatly affects the daily operation of the enterprise.

To solve the preceding problems, the enterprise administrator wants to use the bandwidth management function provided by the device. The enterprise administrator can set the maximum number of connections to 10000 to control P2P and online video traffic.

Figure 17-4 Networking diagram for configuring the maximum connection limit for bandwidth management on enterprise networks

NOTE

In this example, interface1 and interface2 represent GE0/0/1 and GE0/0/2, respectively.



Configuration Roadmap

1. Set interface IP addresses and assign the interfaces to security zones.
2. Configure a bandwidth policy for P2P and online video applications and a bandwidth profile in which the overall maximum number of connections is 10000.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Set an IP address for interface GE0/0/2 and add the interface to the Untrust zone.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 1.1.1.1 24
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceAzone-untrust] add interface ge 0/0/2
[DeviceAzone-untrust] quit
```

2. Set an IP address for interface GE0/0/1 and add the interface to the Trust zone.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 10.3.0.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

3. Configure a security policy to allow intranet users to access the Internet. In actual configuration, you are advised to configure refined security policies based on networking requirements.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec
[DeviceA-policy-security-rule-policy_sec] source-zone trust
[DeviceA-policy-security-rule-policy_sec] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec] action permit
[DeviceA-policy-security-rule-policy_sec] quit
[DeviceA-policy-security] quit
```

Step 2 Configure a schedule.

```
[DeviceA] time-range work_time 09:00 to 18:00 working-day
```

Step 3 Configure a bandwidth profile for P2P and online video services.

```
[DeviceA] bandwidth-policy
[DeviceA-policy-bandwidth] profile name profile_p2p
[DeviceA-policy-bandwidth-profile-profile_p2p] bandwidth connection-limit whole both 10000
[DeviceA-policy-bandwidth-profile-profile_p2p] quit
```

Step 4 Configure a bandwidth policy for P2P and online video services.

NOTE

The following example describes the bandwidth management configuration for BitTorrent (BT) and Youku services. You can specify other P2P services as required.

```
[DeviceA-policy-bandwidth] rule name policy_p2p
[DeviceA-policy-bandwidth-rule-policy_p2p] source-zone trust
[DeviceA-policy-bandwidth-rule-policy_p2p] destination-zone untrust
[DeviceA-policy-bandwidth-rule-policy_p2p] application app BT
[DeviceA-policy-bandwidth-rule-policy_p2p] application app YouKu
[DeviceA-policy-bandwidth-rule-policy_p2p] action qos profile profile_p2p
[DeviceA-policy-bandwidth-rule-policy_p2p] quit
[DeviceA-policy-bandwidth] quit
```

----End

Verifying the Configuration

When a large amount of P2P and online video traffic exists, run the **display bandwidth-policy statistic connection** command on DeviceA to view statistics about the connection limit. In the command output, **CC** indicates the number of current connections.

```
<DeviceA> display bandwidth-policy statistic connection-limit whole both all
Statistic:  Total current items: 1
Codes: CC(Current Connection), RC(Rejective Connection)
------------------------------------------------------------------------------
 Policy       Profile     CC        RC
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
policy_p2p  profile_p2p   10000     5435
------------------------------------------------------------------------------
```

Configuration Scripts

This section provides only the script related to the example.

```
#
sysname DeviceA
#
time-range work_time 09:00 to 18:00 working-day
#
interface GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/1
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
security-policy
 rule name policy_sec
  source-zone trust
  destination-zone untrust
  action permit
#
bandwidth-policy
 profile name profile_p2p
  bandwidth connection-limit whole both 10000
 rule name policy_p2p
  source-zone trust
  destination-zone untrust
  application app BT
  application app YouKu
  action qos profile profile_p2p
#
return
```

17.5 CLI: Example for Configuring Bandwidth Control Based on Public IP Addresses

Networking Requirements

As shown in **Figure 17-5**, employees access the Internet through Source NAT. The enterprise applies for four IP addresses (1.1.1.2 to 1.1.1.5) as the post-NAT public IP addresses. The enterprise deploys multiple Web servers which provide Web access services through NAT Server for users on the Internet. The public IP address of the servers is **1.1.1.6**. In peak hours, when Internet users access the web servers, the web pages and pictures fail to be displayed completely. On the other hand, when the web servers suffer from burst access, the Internet access experience of enterprise employees is also compromised.

The enterprise administrator wants to use bandwidth management provided by DeviceA to limit the total bandwidth of Internet access users and the total bandwidth provided by web servers for external users. That is, bandwidth

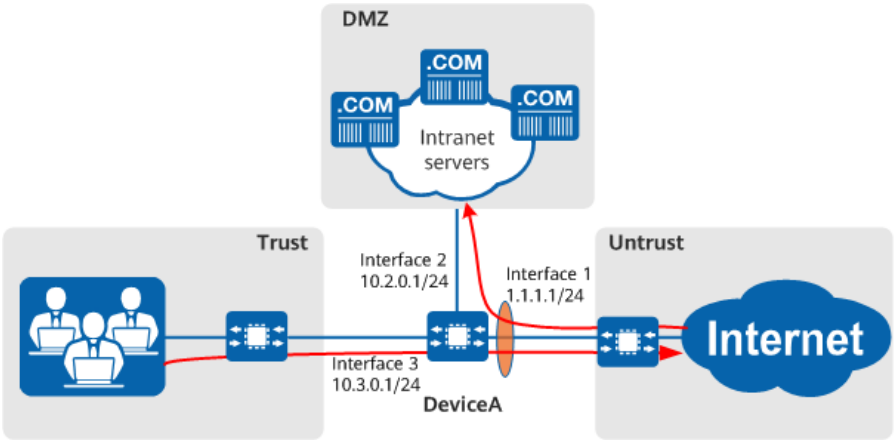
 Copyright © Huawei Technologies Co., Ltd.

management is implemented based on public IP addresses after Source NAT or before NAT Server, instead of bandwidth usage for each user or server. 60 Mbit/s downstream bandwidth (Untrust to Trust) is assigned for intranet users to access the Internet and 40 Mbit/s downstream bandwidth (DMZ to Untrust) is assigned for Internet users to access Web servers.

Figure 17-5 Bandwidth management on public IP addresses with Source NAT or NAT Server enabled

NOTE

In this example, interface1, interface2, and interface3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Configuration Roadmap

1. Set interface IP addresses and assign the interfaces to security zones.
2. Configure a bandwidth policy for intranet users to access the Internet and reference the bandwidth profile in which the overall maximum downstream bandwidth is 60 Mbit/s.
3. Configure a bandwidth policy for intranet web servers and reference the bandwidth profile in which the overall maximum downstream bandwidth is 40 Mbit/s.

Procedure

Step 1 Set interface IP addresses and assign the interfaces to security zones.

1. Set an IP address for interface GE0/0/1 and add the interface to the Untrust zone.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

2. Set an IP address for interface GE0/0/3 and add the interface to the Trust zone.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-GE0/0/3] ip address 10.3.0.1 24
[DeviceA-GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
```

3. Set an IP address for interface GE0/0/2 and add the interface to the DMZ.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 10.2.0.1 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

4. Configure security policies to allow intranet users to access the Internet and allow Internet users to access intranet servers. In actual configuration, you are advised to configure refined security policies based on networking requirements.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec1
[DeviceA-policy-security-rule-policy_sec1] source-zone trust
[DeviceA-policy-security-rule-policy_sec1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec1] action permit
[DeviceA-policy-security-rule-policy_sec1] quit
[DeviceA-policy-security] rule name policy_sec2
[DeviceA-policy-security-rule-policy_sec2] source-zone untrust
[DeviceA-policy-security-rule-policy_sec2] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec2] action permit
[DeviceA-policy-security-rule-policy_sec2] quit
```

Step 2 Configure a bandwidth profile for employees to access the Internet.

```
[DeviceA] bandwidth-policy
[DeviceA-policy-bandwidth] profile name profile_surf
[DeviceA-policy-bandwidth-profile-profile_surf] bandwidth maximum-bandwidth whole upstream 60000
[DeviceA-policy-bandwidth-profile-profile_surf] bandwidth maximum-bandwidth whole downstream
60000
[DeviceA-policy-bandwidth-profile-profile_surf] quit
```

Step 3 Enable the public IP address matching function for Internet access users.

```
[DeviceA-policy-bandwidth] public-ip source match enable
```

Step 4 Configure a bandwidth policy for employees to access the Internet.

```
[DeviceA-policy-bandwidth] rule name policy_surf
[DeviceA-policy-bandwidth-rule-policy_surf] source-zone trust
[DeviceA-policy-bandwidth-rule-policy_surf] destination-zone untrust
[DeviceA-policy-bandwidth-rule-policy_surf] source-address range 1.1.1.2 1.1.1.5
[DeviceA-policy-bandwidth-rule-policy_surf] action qos profile profile_surf
[DeviceA-policy-bandwidth-rule-policy_surf] quit
```

Step 5 Configure a bandwidth profile for intranet web servers.

```
[DeviceA-policy-bandwidth] profile name profile_websvr
[DeviceA-policy-bandwidth-profile-profile_websvr] bandwidth maximum-bandwidth whole upstream
40000
[DeviceA-policy-bandwidth-profile-profile_websvr] bandwidth maximum-bandwidth whole downstream
40000
[DeviceA-policy-bandwidth-profile-profile_websvr] quit
```

Step 6 Enable the public IP address matching function for Internet access users.

```
[DeviceA-policy-bandwidth] public-ip destination match enable
```

Step 7 Configure a bandwidth policy for intranet web servers.

```
[DeviceA-policy-bandwidth] rule name policy_websvr
[DeviceA-policy-bandwidth-rule-policy_websvr] source-zone untrust
[DeviceA-policy-bandwidth-rule-policy_websvr] destination-zone dmz
[DeviceA-policy-bandwidth-rule-policy_websvr] destination-address 1.1.1.6 32
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-policy-bandwidth-rule-policy_websvr] action qos profile profile_websvr
[DeviceA-policy-bandwidth-rule-policy_websvr] quit
```

----End

Verifying the Configuration

Run the **display bandwidth-policy statistic bandwidth** command on DeviceA to view bandwidth policy statistics. In the command output, **Rcv-Rate** and **Pass-Rate** indicate the number of received packets per second before and after rate limiting, respectively.

```
<DeviceA> display bandwidth-policy statistic bandwidth whole upstream rule policy_websvr
Bandwidth Statistic:
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Drop Packets), DB(Drop Bytes)
------------------------------------------------------------------------------
Policy          Profile       PP     PB    DP     DB     Rcv-Rate    Pass-Rate
------------------------------------------------------------------------------
policy_websvr  profile_websvr 3141  34480  63321   815088   2592704   38905
------------------------------------------------------------------------------
```

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  action permit
 rule name policy_sec2
  source-zone untrust
  destination-zone dmz
  action permit
#
bandwidth-policy
 public-ip destination match enable
 public-ip source match enable
 profile name profile_surf
  bandwidth maximum-bandwidth whole upstream 60000
  bandwidth maximum-bandwidth whole downstream 60000
 profile name profile_websvr
  bandwidth maximum-bandwidth whole upstream 40000
  bandwidth maximum-bandwidth whole downstream 40000
 rule name policy_surf
  source-zone trust
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone untrust
 source-address range 1.1.1.2 1.1.1.5
 action qos profile profile_surf
rule name policy_websvr
 source-zone untrust
 destination-zone dmz
 destination-address 1.1.1.6 255.255.255.255
 action qos profile profile_websvr
```

 Copyright © Huawei Technologies Co., Ltd.

18 SLB

18.1 CLI: Example for Configuring FTP SLB

18.1 CLI: Example for Configuring FTP SLB

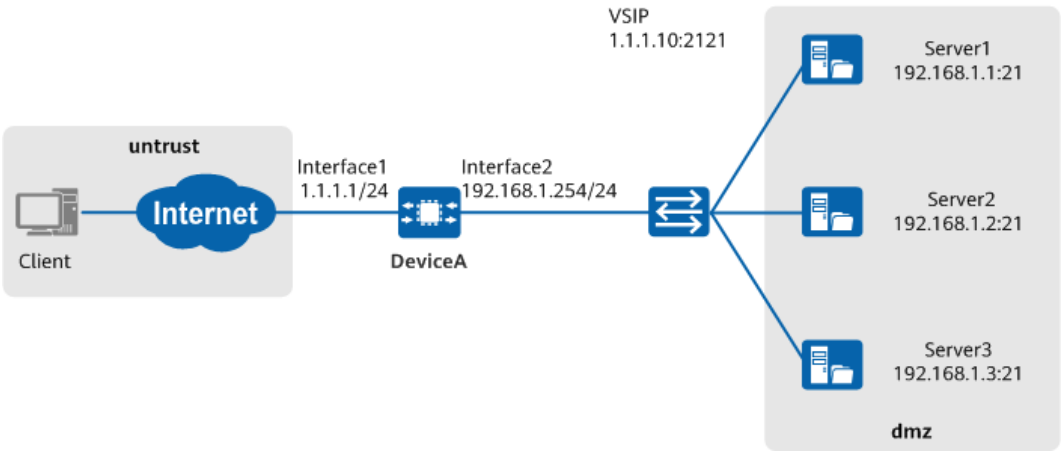
Networking Requirements

As shown in **Figure 18-1**, an enterprise has three servers: Server1, Server2, and Server3. The hardware performance of the servers decreases in sequence. This means the performance of Server1 is twice that of Server2, whose performance is twice that of Server3. SLB is configured to allow the three servers to provide services as a whole. The carried services match the server hardware performance. In addition, the health check function is configured to monitor the work of the servers. In addition, IPS and antivirus detection is performed on the traffic destined for the virtual service. The PC at 1.1.1.11 initiates attacks and its access needs to be blocked.

NOTE

In this example, interface1 and interface2 represent GE0/0/1 and GE0/0/2, respectively.

Figure 18-1 Networking diagram for configuring SLB



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Set the load balancing algorithm to **weight-least-connection** for performance-based SLB. As Server1 performs twice as good as Server2, which performs twice as good as Server3, the weight ratio of the servers is 4:2:1.
2. Configure health check on the load balancing device to monitor the reachability of the three servers. In this example, the health check protocol type is set to ICMP.
3. Configure the sticky session function on the load balancing device because a client may need to establish multiple connections to a server for one task. In this case, the connection request packets from the client can be allocated to the same server.
4. Configure a security policy.

Procedure

Step 1 Set IP addresses for interfaces and assign the interfaces to security zones.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 1.1.1.1 24
[DeviceA-GE0/0/1] quit
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 192.168.1.254 24
[DeviceA-GE0/0/2] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
```

Step 2 Create a real server group and add real servers to it.

```
[DeviceA] slb
[DeviceA-slb] group 0 Rserver
[DeviceA-slb-group-Rserver] metric weight-least-connection
[DeviceA-slb-group-Rserver] rserver 0 rip 192.168.1.1 port 21 status health-check weight 4 description server1
[DeviceA-slb-group-Rserver] rserver 1 rip 192.168.1.2 port 21 status health-check weight 2 description server2
[DeviceA-slb-group-Rserver] rserver 2 rip 192.168.1.3 port 21 status health-check weight 1 description server3
```

Select the load balancing algorithm **weight-least-connection**, configure real servers Server1, Server2, and Server3, and set the weights of the servers to 4, 2, and 1, respectively.

Step 3 Configure the health check function.

```
[DeviceA-slb-group-Rserver] health-check type icmp tx-interval 5 times 3
[DeviceA-slb-group-Rserver] quit
```

Step 4 Configure sticky session.

```
[DeviceA] slb
[DeviceA-slb]session persistence 0 sourceip
```

Step 5 Configure a virtual server and associate it with a real server group.

```
[DeviceA-slb] security-policy enable
[DeviceA-slb] vserver 0 vs-1.1.1.10
[DeviceA-slb-vserver-vs-1.1.1.10] vserver type l4
[DeviceA-slb-vserver-vs-1.1.1.10] protocol tcp
[DeviceA-slb-vserver-vs-1.1.1.10] vip 0 1.1.1.10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA-slb-vserver-vs-1.1.1.10] vport 2121
[DeviceA-slb-vserver-vs-1.1.1.10] group Rserver
[DeviceA-slb-vserver-vs-1.1.1.10] persistence sourceip
[DeviceA-slb-vserver-vs-1.1.1.10] quit
```

Step 6 Enable the security policy function for SLB traffic.

```
[DeviceA-slb] security-policy enable
[DeviceA-slb] quit
```

Step 7 Configure a security policy.

Implement security management and control on traffic based on virtual services and reference intrusion prevention and antivirus profiles in security policies.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec0
[DeviceA-policy-security-rule-policy_sec0] source-address 1.1.1.11 32
[DeviceA-policy-security-rule-policy_sec0] vserver vs-1.1.1.10
[DeviceA-policy-security-rule-policy_sec0] action deny
[DeviceA-policy-security-rule-policy_sec0] quit
[DeviceA-policy-security] rule name policy_sec1
[DeviceA-policy-security-rule-policy_sec1] source-address 1.1.1.0 24
[DeviceA-policy-security-rule-policy_sec1] vserver vs-1.1.1.10
[DeviceA-policy-security-rule-policy_sec1] action permit
[DeviceA-policy-security-rule-policy_sec1] profile ips default
[DeviceA-policy-security-rule-policy_sec1] profile av default
[DeviceA-policy-security-rule-policy_sec1] quit
[DeviceA-policy-security] quit
```

----End

Verifying the Configuration

1. Check the static server mapping table on the device. If the table contains the associated entry, SLB is configured successfully.

```
[DeviceA] display firewall server-map static
 Current Total Server-map : 1
 Type: SLB,  ANY -> 1.1.1.10:2121[vs-1.1.1.10/0],  Zone:---,  protocol:tcp
 Vpn: public -> public
```

2. Send numerous requests to the servers. After some time, view the running status of the virtual servers and real servers on the device. The total and concurrent session ratios of the three servers are approximately 4:2:1.

```
[DeviceA] display slb vserver name vs-1.1.1.10 verbose
Virtual Server Information(Total 1)
------------------------------------------------------------------------------
  Virtual Server Name      : vs-1.1.1.10
  Virtual Server ID        : 0
  Virtual Server IP        : 1.1.1.10
  Protocol                 : tcp
  Source-nat Type          : NA
  Virtual Server Port      : 2121
  Http X-forward Enable    : Disable
  Virtual Server Max-conn  : --
  Group Name               : Rserver
  Group ID                 : 0
  Persistence Name/ID(Type): sourceip/0(source-ip)
  Tunnel Mode              : Disable
  Auth-Enable              : Disable
  Virtual Server Statistics
   Current Connection      :112
   Total connection        :300
   Total Flow              :3247856_B
------------------------------------------------
[DeviceA] display slb group name Rserver verbose
Group Information(Total 1)
```

 Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
------------------------------
  Group Name               : Rserver
  Group ID                 : 0
  Metric                   : weight-least-connection
  Health Check Type        : icmp
  Real Server Number       : 3
    RserverID  IP-Address      Weight  Max-connection  Status        Ratio        TotalSession
CurSession
    0          192.168.1.1     4       -               Active        57.03%           1525
65
    1          192.168.1.2     2       -               Active        28.42%           760
32
    2          192.168.1.3     1       -               Active        14.55%           389
15
------------------------------------------------------------------------------
------------------------------
```

Configuring Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 192.168.1.254 255.255.255.0
#
firewall zone untrust
 add interface GE0/0/1
#
firewall zone dmz
 add interface GE0/0/2
#
security-policy
 rule name policy_sec0
  source-address 1.1.1.11  32
  vserver vs-1.1.1.10
  action deny
 rule name policy_sec1
  source-address 1.1.1.0  24
  vserver vs-1.1.1.10
  action permit
  profile ips default
  profile av default
#
healthcheck enable
slb
 group 0 Rserver
  metric weight-least-connection
  health-check type icmp
  rserver 0 rip 192.168.1.1 port 21 status health-check weight 4 description server1
  rserver 1 rip 192.168.1.2 port 21 status health-check weight 2 description server2
  rserver 2 rip 192.168.1.3 port 21 status health-check description server3
 session persistence 0 sourceip
 security-policy enable
 vserver 0 vs-1.1.1.10
  vserver type l4
  vip 0 1.1.1.10
  protocol tcp
  vport 2121
  persistence sourceip
  group Rserver
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

19 QoS

19.1 Packet Filtering Configuration

19.2 Traffic Statistics Collection Configuration

19.3 Priority Mapping Configuration

19.1 Packet Filtering Configuration

19.1.1 CLI: Example for Configuring MQC-based Packet Filtering

Networking Requirements

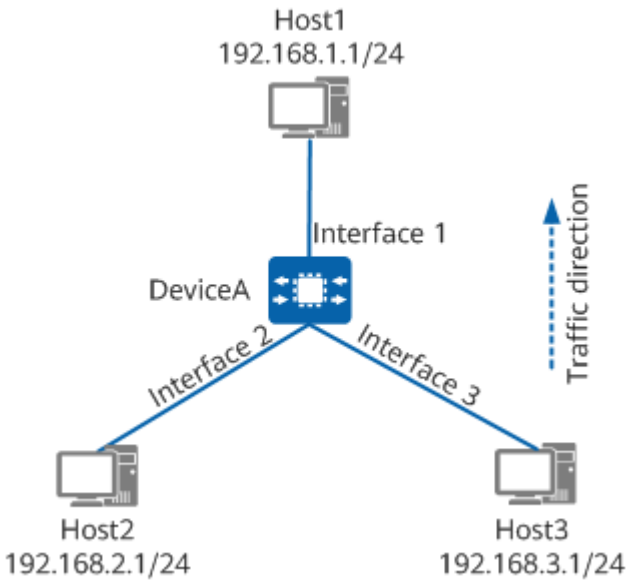
In **Figure 19-1**, Host1, Host2, and Host3 communicate with each other through DeviceA. For specific reasons, Host1 is allowed to receive traffic from Host2 through DeviceA but is not allowed to receive traffic from Host3.

Figure 19-1 Network diagram of packet filtering

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE 0/0/1, GE 0/0/2, and GE 0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Procedure

Step 1 Configure an ACL rule.

On DeviceA, create ACL 3001 to match the traffic with source IP address 192.168.3.1 and destination IP address 192.168.1.1 (traffic from Host3 to Host1).

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] acl 3001
[DeviceA-acl4-advance-3001] rule permit ip destination 192.168.1.1 24 source 192.168.3.1 24
[DeviceA-acl4-advance-3001] quit
```

Step 2 Configure a security policy.

Add interfaces to corresponding security zones and configure a security policy.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/2
[DeviceA-zone-trust] add interface ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] security-policy
[DeviceA-policy-security] rule name sec_policy1
[DeviceA-policy-security-rule-sec_policy1] source-zone trust
[DeviceA-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceA-policy-security-rule-sec_policy1] action permit
[DeviceA-policy-security-rule-sec_policy1] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a traffic classifier.

On DeviceA, create traffic classifier **c1** and reference ACL 3001 in the traffic classifier.

```
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match acl 3001
[DeviceA-classifier-c1] quit
```

Step 4 Configure a traffic behavior.

 Copyright © Huawei Technologies Co., Ltd.

On DeviceA, create traffic behavior **b1** and define the deny action in the traffic behavior.

```
[DeviceA] traffic behavior b1
[DeviceA-behavior-b1] deny
[DeviceA-behavior-b1] quit
```

Step 5 Configure a traffic policy and apply it to the outbound direction of GE 0/0/1.

On DeviceA, create traffic policy **p1**, in which traffic classifier **c1** is associated with traffic behavior **b1**.

```
[DeviceA] traffic policy p1
[DeviceA-trafficpolicy-p1] classifier c1 behavior b1
[DeviceA-trafficpolicy-p1] quit
```

Apply traffic policy **p1** to the outbound direction of GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] traffic-policy p1 outbound
[DeviceA-GE0/0/1] quit
[DeviceA] quit
```

----End

Verifying the Configuration

Check the ACL configuration.

```
<DeviceA> display acl 3001
Advanced ACL 3001, 1 rule
ACL's step is 5
 rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 (0 times matched)
```

Check the traffic classifier configuration.

```
<DeviceA> display traffic classifier c1
  Traffic Classifier Information:
    Classifier: c1
      Type: OR
      Rule(s):
        if-match acl 3001
```

Check the traffic policy configuration.

```
<DeviceA> display traffic policy p1
  Traffic Policy Information:
    Policy: p1
      Classifier: c1
        Type: OR
      Behavior: b1
        Deny
```

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
acl number 3001
 rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
traffic classifier c1 type or
 if-match acl 3001
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
traffic behavior b1
 deny
#
traffic policy p1
 classifier c1 behavior b1 precedence 5
#
interface GE0/0/1
 traffic-policy p1 outbound
#
firewall zone trust
 add interface GE0/0/2
 add interface GE0/0/3
#
firewall zone untrust
 add interface GE0/0/1
#
security-policy
 rule name sec_policy1
  source-zone trust
  destination-zone untrust
  action permit
#
return
```

19.2 Traffic Statistics Collection Configuration

19.2.1 CLI: Example for Configuring MQC-based Traffic Statistics Collection

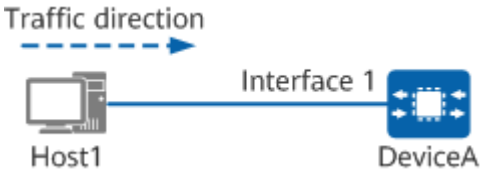
Networking Requirements

In Figure 19-2, Host1 sends packets with the 802.1p value of 6 to DeviceA. Statistics on service packets need to be collected to properly allocate bandwidth resources.

Figure 19-2 Network diagram of traffic statistics collection

NOTE

In this example, interface 1 represents GE 0/0/1.



Procedure

Step 1 Add the interface to a security zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Step 2 Configure an ACL rule.

 Copyright © Huawei Technologies Co., Ltd.

On DeviceA, create Layer 2 ACL 4000 to match packets with the 802.1p value of 6.

```
[DeviceA] acl 4000
[DeviceA-acl-L2-4000] rule permit 8021p 6
[DeviceA-acl-L2-4000] quit
```

Step 3 Configure a traffic classifier.

On DeviceA, create traffic classifier **c1** and match ACL 4000.

```
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match acl 4000
[DeviceA-classifier-c1] quit
```

Step 4 Configure a traffic behavior.

On DeviceA, create traffic behavior **b1** and define the traffic statistics collection action in the traffic behavior.

```
[DeviceA] traffic behavior b1
[DeviceA-behavior-b1] statistics enable
[DeviceA-behavior-b1] quit
```

Step 5 Configure a traffic policy and apply it to the interface.

On DeviceA, create traffic policy **p1**, in which traffic classifier **c1** is associated with traffic behavior **b1**.

```
[DeviceA] traffic policy p1
[DeviceA-trafficpolicy-p1] classifier c1 behavior b1
[DeviceA-trafficpolicy-p1] quit
```

Apply traffic policy **p1** to the inbound direction of GE 0/0/1.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] traffic-policy p1 inbound
[DeviceA-GE0/0/1] quit
[DeviceA] quit
```

----End

Verifying the Configuration

Check the ACL configuration.

```
<DeviceA> display acl 4000
L2 ACL 4000, 1 rule
ACL's step is 5
 rule 5 permit 8021p 6 (0 times matched)
```

Check the traffic classifier configuration.

```
<DeviceA> display traffic classifier c1
  Traffic Classifier Information:
    Classifier: c1
      Type: OR
      Rule(s):
        if-match acl 4000
```

Check the traffic policy configuration.

```
<DeviceA> display traffic policy p1
  Traffic Policy Information:
    Policy: p1
      Classifier: c1
        Type: OR
```

 Copyright © Huawei Technologies Co., Ltd.

```
    Behavior: b1
      Statistics: enable
```

Check traffic statistics.

```
<DeviceA> display traffic-policy statistics interface ge 0/0/1 inbound
Traffic policy: p1, inbound
-------------------------------------------------------------------------------
 Slot: 0
 Item              Packets              Bytes          pps          bps
 -------------------------------------------------------------------------------
 Matched             212185           22067448         1600      1379215
  Passed             212185           22067448         1600      1379215
  Dropped                 0                  0            0            0
   Filter                 0                  0            0            0
   CAR                    0                  0            0            0
 -------------------------------------------------------------------------------
```

You can view the statistics on service packets on GE 0/0/1.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
vlan batch 100
#
acl number 4000
 rule 5 permit 8021p 6
#
traffic classifier c1 type or
 if-match acl 4000
#
traffic behavior b1
 statistics enable
#
traffic policy p1
 classifier c1 behavior b1 precedence 5
#
interface GE0/0/1
 traffic-policy p1 inbound
#
firewall zone trust
 add interface GE0/0/1
#
return
```

19.3 Priority Mapping Configuration

19.3.1 CLI: Example for Configuring Priority Mapping

Networking Requirements

In **Figure 19-3**, Host1 and Host2 are connected to DeviceB and DeviceC through DeviceD, and then access the network through DeviceA.

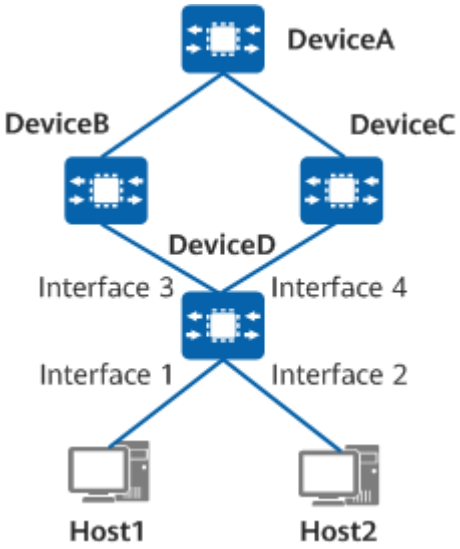
The 802.1p values of packets sent from Host1 and Host2 are both 0. To ensure normal running of low-latency services on Host1, the customer wants to configure the CoS of Host1 to be higher than that of Host2, offering differentiated services for Host1 and Host2.

 Copyright © Huawei Technologies Co., Ltd.

Figure 19-3 Network diagram of priority mapping

NOTE

In this example, interface 1, interface 2, interface 3, and interface 4 represent GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4, respectively.



Procedure

Step 1 Create VLANs and configure interfaces so that DeviceD can communicate with Host1, Host2, DeviceB, and DeviceC.

Create VLAN 100 and VLAN 200.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] vlan batch 100 200
```

Set the link type of GE 0/0/3 and GE 0/0/4 on DeviceD to trunk, and add GE 0/0/1 to VLAN 100, GE 0/0/2 to VLAN 200, and GE 0/0/3 and GE 0/0/4 to both VLAN 100 and VLAN 200.

```
[DeviceD] interface ge 0/0/1
[DeviceD-GE0/0/1] portswitch
[DeviceD-GE0/0/1] port default vlan 100
[DeviceD-GE0/0/1] quit
[DeviceD] interface ge 0/0/2
[DeviceD-GE0/0/2] portswitch
[DeviceD-GE0/0/2] port default vlan 200
[DeviceD-GE0/0/2] quit
[DeviceD] interface ge 0/0/3
[DeviceD-GE0/0/3] portswitch
[DeviceD-GE0/0/3] port link-type trunk
[DeviceD-GE0/0/3] port trunk allow-pass vlan 100 200
[DeviceD-GE0/0/3] quit
[DeviceD] interface ge 0/0/4
[DeviceD-GE0/0/4] portswitch
[DeviceD-GE0/0/4] port link-type trunk
[DeviceD-GE0/0/4] port trunk allow-pass vlan 100 200
[DeviceD-GE0/0/4] quit
```

Step 2 Add the interfaces to security zones and configure a security policy.

```
[DeviceD] firewall zone trust
[DeviceD-zone-trust] add interface ge 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceD-zone-trust] add interface ge 0/0/2
[DeviceD-zone-trust] quit
[DeviceD] firewall zone untrust
[DeviceD-zone-untrust] add interface ge 0/0/3
[DeviceD-zone-untrust] add interface ge 0/0/4
[DeviceD-zone-untrust] quit
[DeviceD] security-policy
[DeviceD-policy-security] rule name sec_policy1
[DeviceD-policy-security-rule-sec_policy1] source-zone trust
[DeviceD-policy-security-rule-sec_policy1] destination-zone untrust
[DeviceD-policy-security-rule-sec_policy1] action permit
[DeviceD-policy-security-rule-sec_policy1] quit
[DeviceD-policy-security] quit
```

Step 3 Configure interfaces to trust outer 802.1p values in packets.

Configure GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4 to trust outer 802.1p values in packets.

```
[DeviceD] interface ge 0/0/1
[DeviceD-GE0/0/1] trust 8021p outer
[DeviceD-GE0/0/1] quit
[DeviceD] interface ge 0/0/2
[DeviceD-GE0/0/2] trust 8021p outer
[DeviceD-GE0/0/2] quit
[DeviceD] interface ge 0/0/3
[DeviceD-GE0/0/3] trust 8021p outer
[DeviceD-GE0/0/3] quit
[DeviceD] interface ge 0/0/4
[DeviceD-GE0/0/4] trust 8021p outer
[DeviceD-GE0/0/4] quit
```

Step 4 Create DiffServ domains, configure priority mapping in the DiffServ domains, and bind the DiffServ domains to interfaces.

Create DiffServ domains **ds1** and **ds2** on DeviceD and map the 802.1p values of packets sent from Host1 and Host2 to different internal priorities.

```
[DeviceD] diffserv domain ds1
[DeviceD-dsdomain-ds1] 8021p-inbound 0 phb af4 green
[DeviceD-dsdomain-ds1] quit
[DeviceD] diffserv domain ds2
[DeviceD-dsdomain-ds2] 8021p-inbound 0 phb af2 green
[DeviceD-dsdomain-ds2] quit
```

Bind DiffServ domains **ds1** and **ds2** to GE 0/0/1 and GE 0/0/2, respectively.

```
[DeviceD] interface ge 0/0/1
[DeviceD-GE0/0/1] trust upstream ds1
[DeviceD-GE0/0/1] quit
[DeviceD] interface ge 0/0/2
[DeviceD-GE0/0/2] trust upstream ds2
[DeviceD-GE0/0/2] quit
```

----End

Verifying the Configuration

Display queue statistics on the outbound interface. If there are packet statistics in queue 2 corresponding to the internal priority AF2, and in queue 4 corresponding to the internal priority AF4, priority mapping is configured successfully.

```
[DeviceD] display qos queue statistics interface ge 0/0/3
 Queue  CIR/PIR          Passed     Pass Rate          Dropped     Drop Rate  Drop Time
        (% or kbps)   (Packets/Bytes)    (pps/bps)   (Packets/Bytes)   (pps/
```

 Copyright © Huawei Technologies Co., Ltd.

```
bps)
------------------------------------------------------------------------------
  0      -             0          0             0          0       -
         -             0          0             0          0
------------------------------------------------------------------------------
  1      -             0          0             0          0       -
         -             0          0             0          0
------------------------------------------------------------------------------
  2      -      11295086      17516             0          0       -
         -     114688668   14573986             0          0
------------------------------------------------------------------------------
  3      -             0          0             0          0       -
         -             0          0             0          0
------------------------------------------------------------------------------
  4      -      11511125      19563             0          0       -
         -     112653485   15352321             0          0
------------------------------------------------------------------------------
  5      -             0          0             0          0       -
         -             0          0             0          0
------------------------------------------------------------------------------
  6      -             0          0             0          0       -
         -             0          0             0          0
------------------------------------------------------------------------------
  7      -             0          0             0          0       -
         -             0          0             0          0
------------------------------------------------------------------------------
```

Configuration Scripts

DeviceD

```
#
sysname DeviceD
#
vlan batch 100 200
#
diffserv domain ds1
 8021p-inbound 0 phb af4 green
#
diffserv domain ds2
 8021p-inbound 0 phb af2 green
#
interface GE0/0/1
 portswitch
 port default vlan 100
 trust upstream ds1
 trust 8021p outer
#
interface GE0/0/2
 portswitch
 port default vlan 200
 trust upstream ds2
 trust 8021p outer
#
interface GE0/0/3
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 100 200
 trust 8021p outer
#
interface GE0/0/4
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 100 200
 trust 8021p outer
#
firewall zone trust
 add interface GE0/0/1
 add interface GE0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
firewall zone untrust
 add interface GE0/0/3
 add interface GE0/0/4
#
security-policy
 rule name sec_policy1
  source-zone trust
  destination-zone untrust
  action permit
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

20 System Management and Monitoring

20.1 Web: Example for Configuring a Device to Connect to eSight Using SNMPv3

20.2 CLI: Example for Configuring a Device to Connect to eSight Using SNMPv3

20.3 Web: Example for Configuring Devices to Connect to iMaster NCE-Campus

20.4 CLI: Example for Sending IPv4 Session Logs to the SecoManager

20.5 CLI: Example for Sending User Session Logs to the SecoManager

20.6 CLI: Example for Sending Intrusion Prevention Logs to the SecoManager

20.7 CLI: Example for Sending Virus Event Logs to the SecoManager

20.8 CLI: Example for Sending Syslogs in Default or MTN Format to a Third-Party Log Host

20.9 CLI: Example for Outputting Customized Syslog Session Logs to a Third-Party Log Host

20.10 CLI: Example for Outputting Customized NetFlow Session Logs to a Third-Party Log Host

20.11 CLI: Example for Sending Service Logs to a Third-Party Log Host

20.12 CLI: Example for Outputting Packet Loss Logs to a Third-Party Log Host

20.13 CLI: Example for Sending IPv4 Session Logs to the SecoManager in Hot Standby Deployment of Loading Balancing Mode

20.1 Web: Example for Configuring a Device to Connect to eSight Using SNMPv3

Networking Requirements

As shown in **Figure 20-1**, DeviceA is deployed at the network border of an enterprise as the security gateway and eSight is deployed to centrally manage

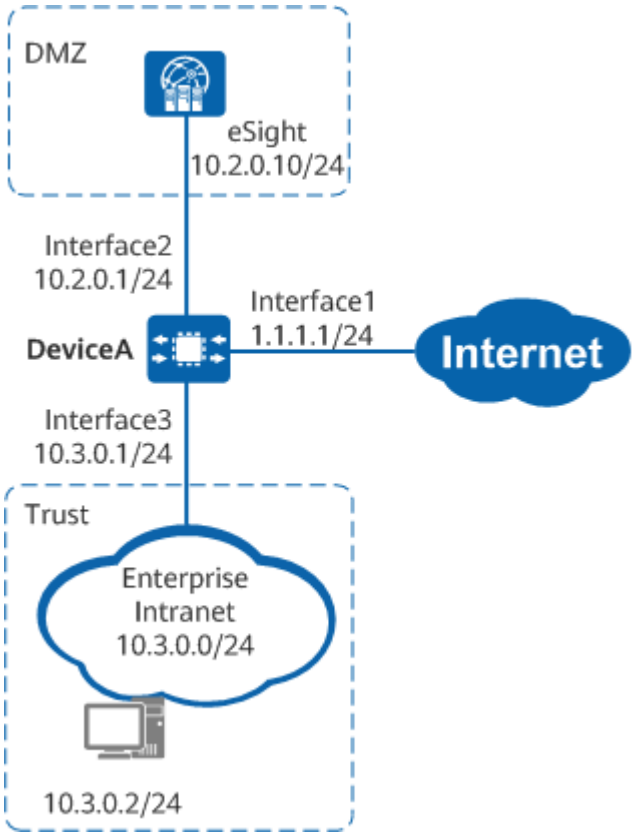
 Copyright © Huawei Technologies Co., Ltd.

network devices. eSight needs to monitor and manage DeviceA and receive alarms from DeviceA.

Figure 20-1 Managing DeviceA using eSight

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Data Planning

Item		Data	Description
DeviceA	Interface	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust	Interface connecting to the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
		Interface number: GE0/0/2 IP address: 10.2.0.1/24 Security zone: DMZ	Interface communicating with the eSight server.
		Interface number: GE0/0/3 IP address: 10.3.0.1/24 Security zone: Trust	Interface connecting to the enterprise intranet.
	SNMP parameters	User name: V3user SNMP version: V3 Authentication protocol: HMAC-SHA2-256 Authentication password: YsHsjx_202206 Encryption protocol: AES256 Encryption password: YsHsjx_202206	The SNMP parameters of DeviceA and eSight must be the same.
eSight	IP address	10.2.0.10/24	Deployed in the DMZ in centralized mode.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
	SNMP parameters	User name: V3user Parameter type: v3 Authentication protocol: HMAC-SHA2-256 Authentication password: YsHsjx_202206 Privacy protocol: AES256 Encryption password: YsHsjx_202206	The SNMP parameters of eSight and DeviceA must be the same.

Configuration Roadmap

1. Enable communication between DeviceA and eSight. Specifically, configure IP addresses for interfaces on DeviceA, add the interfaces to security zones, and configure the interface access management function to permit SNMP packets.

   If the interface access management function is not used, you need to configure related security policies. Before disabling the interface access management function, configure security policies for the remote management protocol to ensure that DeviceA can be remotely managed.
2. Enable eSight to manage DeviceA and receive alarms from DeviceA. Specifically, set SNMP parameters and enable the trap function on DeviceA, and set the same SNMP parameters on eSight and add DeviceA to eSight. To enable DeviceA to send alarms to eSight, you need to configure related security policies.

NOTE

This example focuses on the configurations of the interconnection between DeviceA and eSight. Configure routes to ensure that devices are routable. For other configurations on eSight, see related manuals.

Ensure that the system time and time zone of Device A are the same as those of eSight.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set IP addresses for interfaces, and assign the interfaces to security zones.

1. Choose **Network** > **Interface**.
2. Click of GE0/0/1 and set the following parameters.

IP Address	1.1.1.1
Mask	255.255.255.0
Zone	untrust

3. Click **OK**.
4. Repeat the previous steps to set the parameters of interface GE0/0/2.

IP Address	10.2.0.1
Mask	255.255.255.0
Zone	dmz
Access Management	SNMP

5. Repeat the previous steps to set the parameters of interface GE0/0/3.

IP Address	10.3.0.1
Mask	255.255.255.0
Zone	trust

Step 2 Configure security Policies.

1. Choose **Policy** > **Security Policy** > **Security Policy**.
2. Click **Add Security Policy**, set the parameters as follows for the security policy of the Trust->Untrust.

Name	trust_untrust_outbound
Source Zone	trust
Destination Zone	untrust
Source Address	10.3.0.0/24
Action	Permit

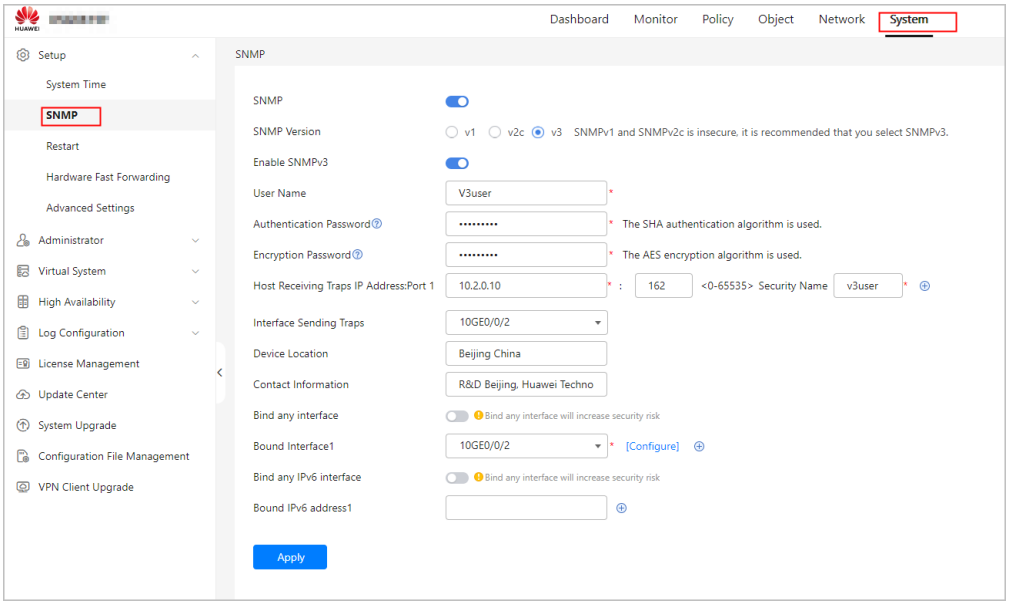
3. Click **OK**.
4. Repeat the previous steps to set the parameters as follows for the security policy of the Local->DMZ interzone to ensure that deviceA can send alarms to the eSight.

 Copyright © Huawei Technologies Co., Ltd.

Name	local_dmz_outbound
Source Zone	local
Destination Zone	dmz
Source Address	10.2.0.1/24
Action	Permit

Step 3 Set the SNMP parameters and enable the deviceA to send alarms to the eSight.

1. Choose **System** > **Setup** > > **SNMP**.
2. Set the parameters as follows.



3. Click **Apply**.

Step 4 Configure eSight.

1. Create an SNMP template.
   a. Choose **Resource** > **Common** > **Add Resource** > **Protocol Template** > **SNMP Template**.
   b. On the **SNMP Template** tab page, click **Create** and create an SNMP template based on the following parameter settings.

Template Name	snmpv3_template
Parameter Type	V3
Authentication protocol	HMAC-SHA2-256
Authentication password	YsHsjx_202206
Privacy protocol	AES_256

 Copyright © Huawei Technologies Co., Ltd.

Encryption password	YsHsjx_202206
User name	V3user
Port(1-65535)	161
Timeout period (1-60s)	3
Retries (1-20)	3

NOTE

The user name, authentication protocol password, and privacy protocol password on eSight must be the same as the corresponding parameter settings on DeviceA.

2. Add DeviceA to eSight.
   a. Choose **Resource** > **Common** > **Add Resource** > **Add Resource**.
   b. Set **Discovery Protocol** to **SNMP**.
   c. Set **IP address** to **10.2.0.1**, which is used by DeviceA to interconnect with eSight.
   d. Click **Select template** in **SNMP** and select the protocol template **snmpv3_template** created in **Create an SNMP template** to add the device.
   e. Click **OK**.

----End

Verifying the Configuration

Check whether the eSight can receive alarms.

1. Log in to the deviceA from the web UI. Choose **Network** > **Interface** and deselect **Enable** of ge 0/0/4.
2. On eSight, choose **Fault** > **Current Alarms**, where you can view the alarm information.

Configuration Scripts

```
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
 service-manage enable
 service-manage snmp permit
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
security-policy
 rule name trust_untrust_outbound
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name local_dmz_outbound
  source-zone local
  destination-zone dmz
  source-address 10.2.0.1 mask 255.255.255.0
  action
permit
                                                #
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF000077D0
 snmp-agent sys-info version v3
snmp-agent target-host trap address udp-domain 10.2.0.10 params securityname %
 $%$Lch*5Z>Q0:BIj9Nv<&^W(>5,%$%$ v3  privacy  private-netmanager
 snmp-agent usm-user v3 V3user authentication-mode sha2-256 cipher %+%#]lck/kEvSA'=g^
 WsIwEI~rf&=qHpDEhhB\3Dmt1(%+%#
 snmp-agent usm-user v3 V3user privacy-mode aes256 cipher %+%#Ow4n$dQvbD:^-A
 snmp-agent trap enable
#
 snmp-agent protocol source-interface GE0/0/2
 snmp-agent trap source GE0/0/2
#
return
```

20.2 CLI: Example for Configuring a Device to Connect to eSight Using SNMPv3

Networking Requirements

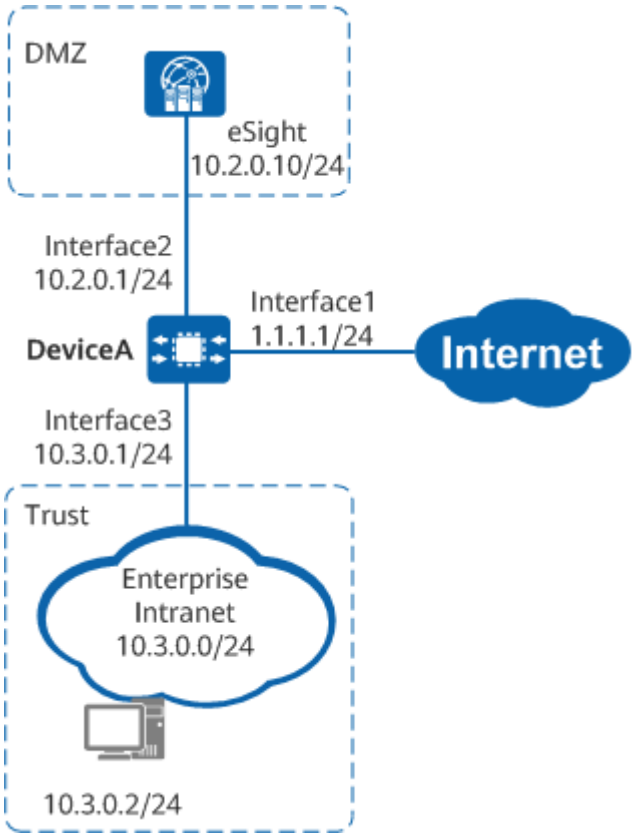
As shown in **Figure 20-2**, DeviceA is deployed at the network border of an enterprise as the security gateway and eSight is deployed to centrally manage network devices. eSight needs to monitor and manage DeviceA and receive alarms from DeviceA.

Figure 20-2 Managing DeviceA using eSight

NOTE

In this example, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Data Planning

Item		Data	Description
DeviceA	Interface	Interface number: GE0/0/1 IP address: 1.1.1.1/24 Security zone: Untrust	Interface connecting to the Internet. In this example, the next-hop address of the interface to the Internet is 1.1.1.2.
		Interface number: GE0/0/2 IP address: 10.2.0.1/24 Security zone: DMZ	Interface communicating with the eSight server.
		Interface number: GE0/0/3 IP address: 10.3.0.1/24 Security zone: Trust	Interface connecting to the enterprise intranet.

 Copyright © Huawei Technologies Co., Ltd.

Item		Data	Description
	SNMP parameters	User name: V3user SNMP version: V3 Authentication protocol: HMAC-SHA2-256 Authentication password: YsHsjx_202206 Encryption protocol: AES128 Encryption password: YsHsjx_202206	The SNMP parameters of DeviceA and eSight must be the same.
eSight	IP address	10.2.0.10/24	Deployed in the DMZ in centralized mode.
	SNMP parameters	User name: V3user Parameter type: v3 Authentication protocol: HMAC-SHA2-256 Authentication password: YsHsjx_202206 Privacy protocol: AES128 Encryption password: YsHsjx_202206	The SNMP parameters of eSight and DeviceA must be the same.

Configuration Roadmap

1. Enable communication between DeviceA and eSight. Specifically, configure IP addresses for interfaces on DeviceA, add the interfaces to security zones, and configure the interface access management function to permit SNMP packets.

   If the interface access management function is not used, you need to configure related security policies. Before disabling the interface access management function, configure security policies for the remote management protocol to ensure that DeviceA can be remotely managed.
2. Enable eSight to manage DeviceA and receive alarms from DeviceA. Specifically, set SNMP parameters and enable the trap function on DeviceA, and set the same SNMP parameters on eSight and add DeviceA to eSight. To enable DeviceA to send alarms to eSight, you need to configure related security policies.

NOTE

This example focuses on the configurations of the interconnection between DeviceA and eSight. Configure routes to ensure that devices are routable. For other configurations on eSight, see related manuals.

Ensure that the system time and time zone of Device A are the same as those of eSight.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure DeviceA.
  a. Configure IP addresses for interfaces, add the interfaces to security zones, and configure the interface access management function to permit SNMP packets.

     # Configure an IP address for GE0/0/1.

     ```
     <HUAWEI> system-view
     [HUAWEI] sysname DeviceA
     [DeviceA] interface ge 0/0/1
     [DeviceA-GE0/0/1] ip address 1.1.1.1 24
     [DeviceA-GE0/0/1] quit
     ```

     # Configure an IP address for GE0/0/2 and configure the interface access management function.

     ```
     [DeviceA] interface ge 0/0/2
     [DeviceA-GE0/0/2] ip address 10.2.0.1 24
     [DeviceA-GE0/0/2] service-manage enable
     [DeviceA-GE0/0/2] service-manage snmp permit
     [DeviceA-GE0/0/2] quit
     ```

     # Configure an IP address for GE0/0/3.

     ```
     [DeviceA] interface ge 0/0/3
     [DeviceA-GE0/0/3] ip address 10.3.0.1 24
     [DeviceA-GE0/0/3] quit
     ```

     # Add GE0/0/1 to the Untrust zone.

     ```
     [DeviceA] firewall zone untrust
     [DeviceA-zone-untrust] add interface ge 0/0/1
     [DeviceA-zone-untrust] quit
     ```

     # Add GE0/0/2 to the DMZ.

     ```
     [DeviceA] firewall zone dmz
     [DeviceA-zone-dmz] add interface ge 0/0/2
     [DeviceA-zone-dmz] quit
     ```

     # Add GE0/0/3 to the Trust zone.

     ```
     [DeviceA] firewall zone trust
     [DeviceA-zone-trust] add interface ge 0/0/3
     [DeviceA-zone-trust] quit
     ```

  b. Configure security policies.

     # Configure a Trust-Untrust interzone security policy.

     ```
     [DeviceA] security-policy
     [DeviceA-policy-security] rule name trust_untrust_outbound
     [DeviceA-policy-security-trust_untrust_outbound] source-zone trust
     [DeviceA-policy-security-trust_untrust_outbound] destination-zone untrust
     [DeviceA-policy-security-trust_untrust_outbound] source-address 10.3.0.0 mask 255.255.255.0
     [DeviceA-policy-security-trust_untrust_outbound] action permit
     [DeviceA-policy-security-trust_untrust_outbound] quit
     ```

     # Configure a Local-DMZ interzone security policy.

     ```
     [DeviceA-policy-security] rule name local_dmz
     [DeviceA-policy-security-local_dmz] source-zone local
     [DeviceA-policy-security-local_dmz] destination-zone dmz
     [DeviceA-policy-security-local_dmz] source-address 10.2.0.1 mask 255.255.255.0
     [DeviceA-policy-security-local_dmz] action permit
     [DeviceA-policy-security-local_dmz] quit
     [DeviceA-policy-security] quit
     ```

 Copyright © Huawei Technologies Co., Ltd.

c. Configure a route.

Configure a default route and set the next hop to that of the route destined for the Internet.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

d. Set SNMP parameters on DeviceA and configure DeviceA to send its alarms to eSight.

```
[DeviceA] snmp-agent sys-info version v3
[DeviceA] snmp-agent mib-view include iso iso
[DeviceA] snmp-agent group v3 v3group privacy
[DeviceA] snmp-agent usm-user v3 V3user authentication-mode sha2-256
Please configure the authentication password (8-255)
Enter Password:
Confirm Password:
[DeviceA] snmp-agent usm-user v3 V3user privacy-mode aes128
Please configure the privacy password (8-255)
Enter Password:
Confirm Password:
[DeviceA] snmp-agent usm-user v3 V3user group v3group
[DeviceA] snmp-agent group v3 v3group privacy write-view iso notify-view iso
[DeviceA] snmp-agent target-host trap address udp-domain 10.2.0.10 params securityname V3user v3 privacy private-netmanager
[DeviceA] snmp-agent trap enable
```

NOTE

This section uses the **snmp-agent mib-view include iso iso** command as an example to describe how to view all alarms under the iso object. Configure the OID object or object name as required.

e. Specify the source interface used by SNMP to receive and respond to requests from an NMS.

```
[DeviceA] snmp-agent protocol source-interface ge 0/0/2
[DeviceA] snmp-agent trap source ge 0/0/2
```

- Configure eSight.
  a. Create an SNMP template.
     i. Choose **Resource** > **Common** > **Add Resource** > **Protocol Template** > **SNMP Template**.
     ii. On the **SNMP Template** tab page, click **Create** and create an SNMP template based on the following parameter settings.

Template Name	snmpv3_template
Parameter Type	V3
Authentication protocol	HMAC-SHA2-256
Authentication password	YsHsjx_202206
Privacy protocol	AES_128
Encryption password	YsHsjx_202206
User name	V3user
Port	161

 Copyright © Huawei Technologies Co., Ltd.

Timeout period (s)	3
Retries	3

NOTE

The user name, authentication protocol password, and proprietary protocol password on eSight must be the same as the corresponding parameter settings on DeviceA.

b. Add DeviceA to eSight.

i. Choose **Resource** > **Common** > **Add Resource** > **Add Resource**.

ii. Set **Discovery Protocol** to **SNMP**.

iii. Set **IP address** to **10.2.0.1**, which is used by DeviceA to interconnect with eSight.

iv. Click **Select template** in **SNMP** and select the protocol template **snmpv3_template** created in **a** to add the device.

v. Click **OK**.

----End

Verifying the Configuration

Check whether eSight can receive alarms.

1. Set the status of the interface whose physical link is Up to Down.

```
[DeviceA] interface ge 0/0/4
[DeviceA-GE0/0/4] shutdown
```

2. On eSight, choose **Fault** > **Current Alarms**, where you can view the alarm information.

Configuration Scripts

```
#
sysname DeviceA
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GE0/0/2
 ip address 10.2.0.1 255.255.255.0
 service-manage snmp permit
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
firewall zone trust
 set priority 85
```

 Copyright © Huawei Technologies Co., Ltd.

```
 add interface GE0/0/3
#
security-policy
 rule name trust_untrust_outbound
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  action permit
 rule name local_dmz
  source-zone local
  destination-zone dmz
  source-address 10.2.0.1 mask 255.255.255.0
  action permit
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF000077D0
 snmp-agent sys-info version v3
 snmp-agent mib-view include iso iso
 snmp-agent group v3 v3group privacy
 snmp-agent group v3 v3group privacy write-view iso notify-view iso
snmp-agent target-host trap  address udp-domain 10.2.0.10 params securityname %
 $%$Lch*5Z>Q0:BIj9Nv<&^W(>5,%$%$ v3  privacy  private-netmanager
 snmp-agent usm-user v3 V3user authentication-mode sha2-256 cipher %+%#]lck/kEvSA'=g^
 WsIwEI~rf&=qHpDEhhB\3Dmt1(%+%#
 snmp-agent usm-user v3 V3user privacy-mode aes128 cipher %+%#Ow4n$dQvbD:^-Asnmp
 -agent usm-user v3 V3user privacy-mode aes128 cipher %+%#Ow4n$dQvbD:^-A
 snmp-agent usm-user v3 V3user group v3group
 snmp-agent trap enable
#
 snmp-agent protocol source-interface GE0/0/2
 snmp-agent trap source GE0/0/2
#
return
```

20.3 Web: Example for Configuring Devices to Connect to iMaster NCE-Campus

Networking Requirements

As shown in **Figure 20-3**, the service interfaces of DeviceA and DeviceB work at Layer 3 and are directly connected to Layer 2 switches in both upstream and downstream directions. The upstream switch is connected to the ISP network, and the IP addresses that the ISP assigns to the enterprise are from 1.1.1.1 to 1.1.1.5. Two devices are required to form a hot standby system in mirroring mode and connect to iMaster NCE-Campus. After the devices are managed by iMaster NCE-Campus, service configurations are delivered by iMaster NCE-Campus.

NOTE

The USG6510F-DPL, USG6585F-B, and USG6530F-DPL cannot interconnect with iMaster NCE-Campus.

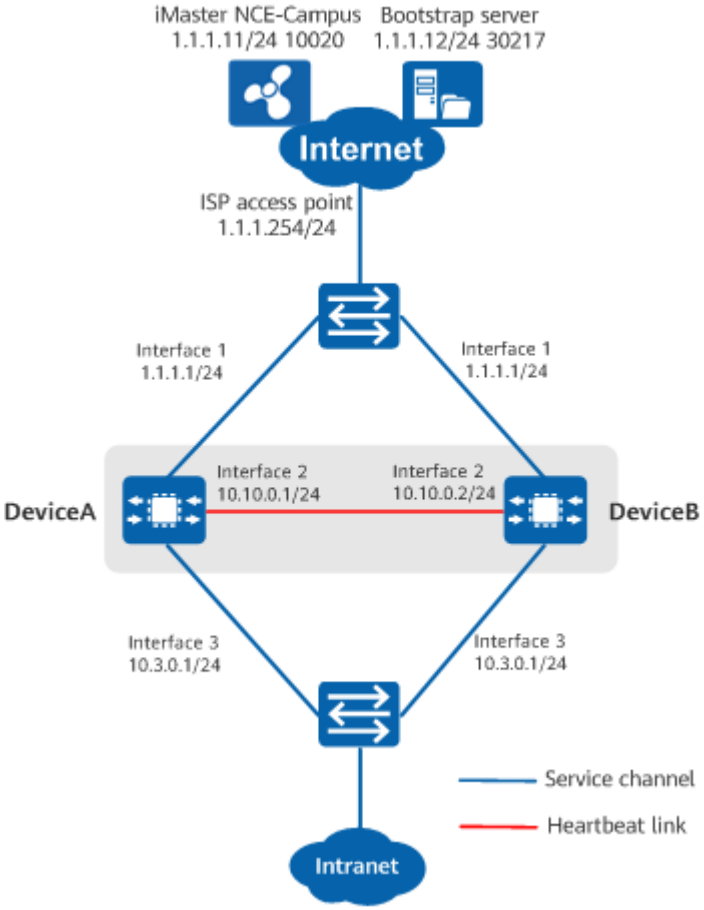
 Copyright © Huawei Technologies Co., Ltd.

Figure 20-3 Configuring devices to connect to iMaster NCE-Campus

NOTE

In this figure, interface 1, interface 2, and interface 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

On iMaster NCE-Campus, you need to add devices to sites and deploy the BootStrap server. For details, see iMaster NCE-Campus Product Documentation.



Procedure

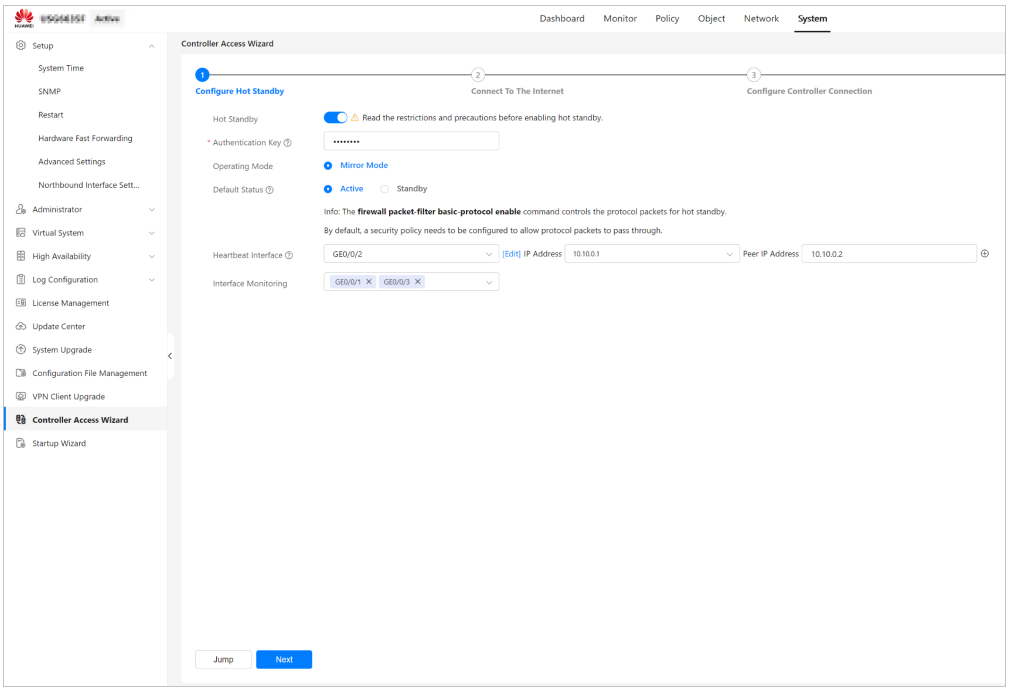
Step 1 Configure hot standby.

NOTE

The wizard needs to be executed on DeviceA and DeviceB separately.

1. Choose **System** > **Controller Access Wizard**. The wizard page of DeviceA is displayed.
2. Set the parameters as shown in the following figure. The authentication key for the packets transmitted between the heartbeat interfaces of the active and standby devices is used. The authentication keys of the two devices must be the same.

 Copyright © Huawei Technologies Co., Ltd.



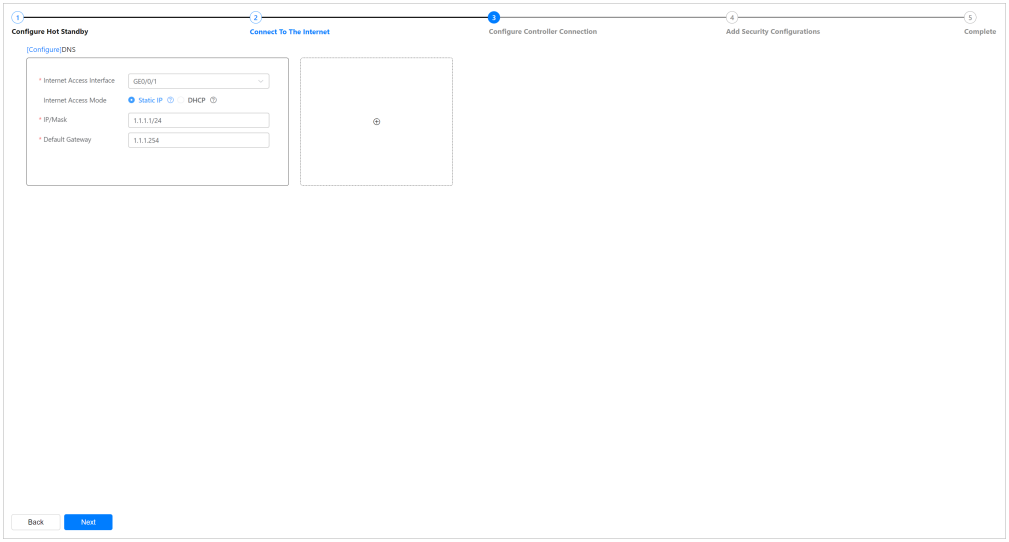
3. Click **Next**.

Step 2 Connect devices to the Internet.

1. Click **Configure** to configure the DNS server.
2. Set the Internet access parameters as shown in the following figure.

NOTE

This page varies depending on the device model. The following uses the static IP address of the wired network port as an example to describe how to access the Internet.

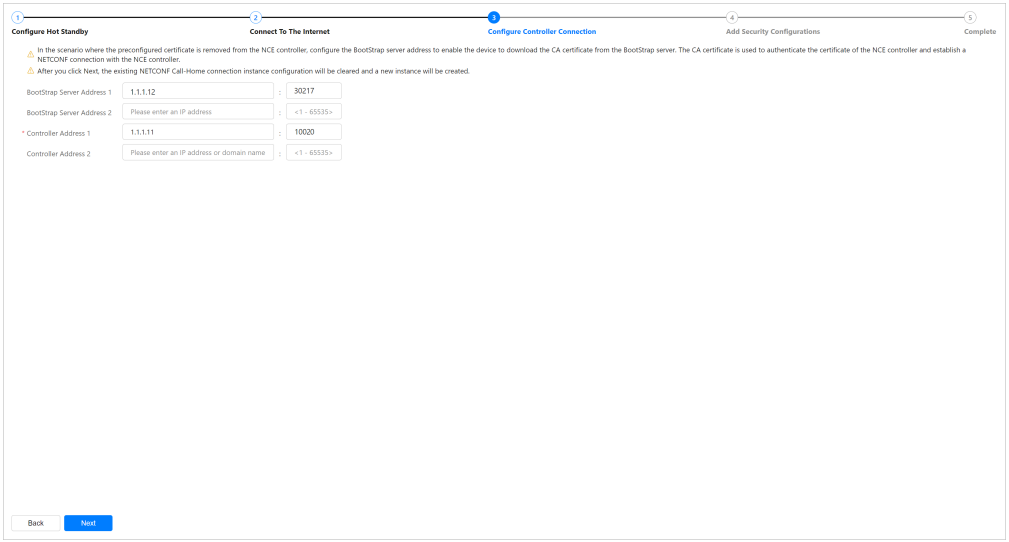


3. Click **Next**.

Step 3 Set parameters for connecting to the controller.

1. Set the parameters as shown in the following figure.

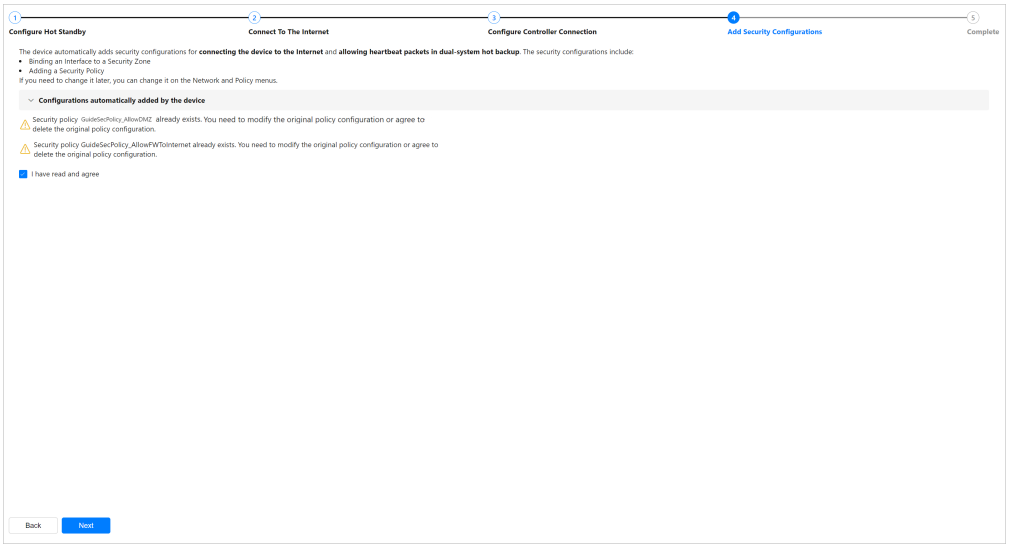
 Copyright © Huawei Technologies Co., Ltd.



2. Click **Next**.

Step 4 Add the security configuration.

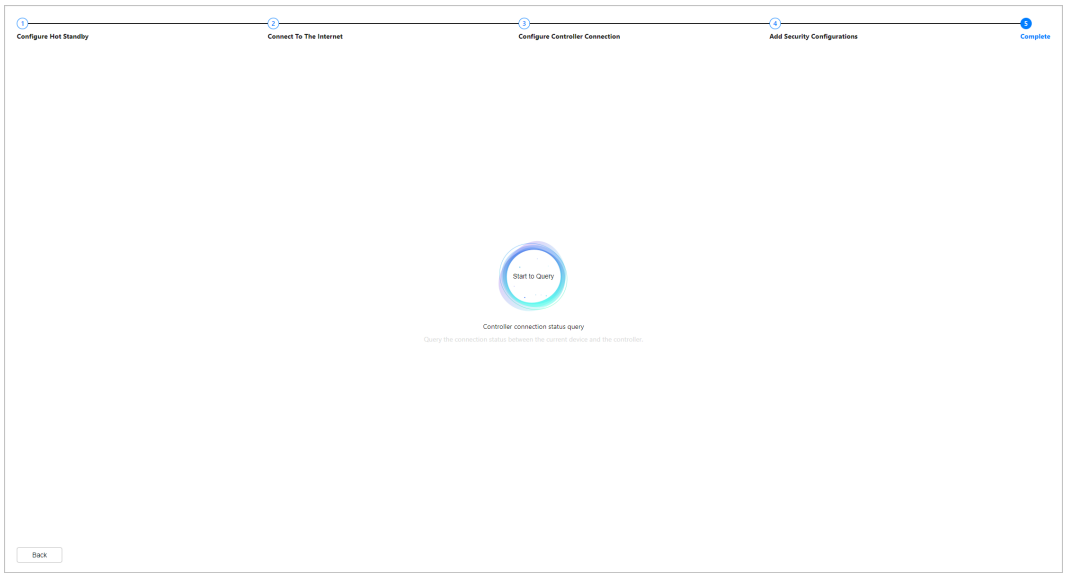
1. As shown in the following figure, the device automatically adds the security configuration for connecting devices to the Internet and permitting hot standby heartbeat packets, including binding interfaces to security zones and adding security policies. To modify the configuration, choose **Network** and **Policy**.



2. Click **Next**.

Step 5 Click **Start to Query** to query the controller connection status.

 Copyright © Huawei Technologies Co., Ltd.



Step 6 Repeat the preceding steps to execute the wizard on DeviceB.

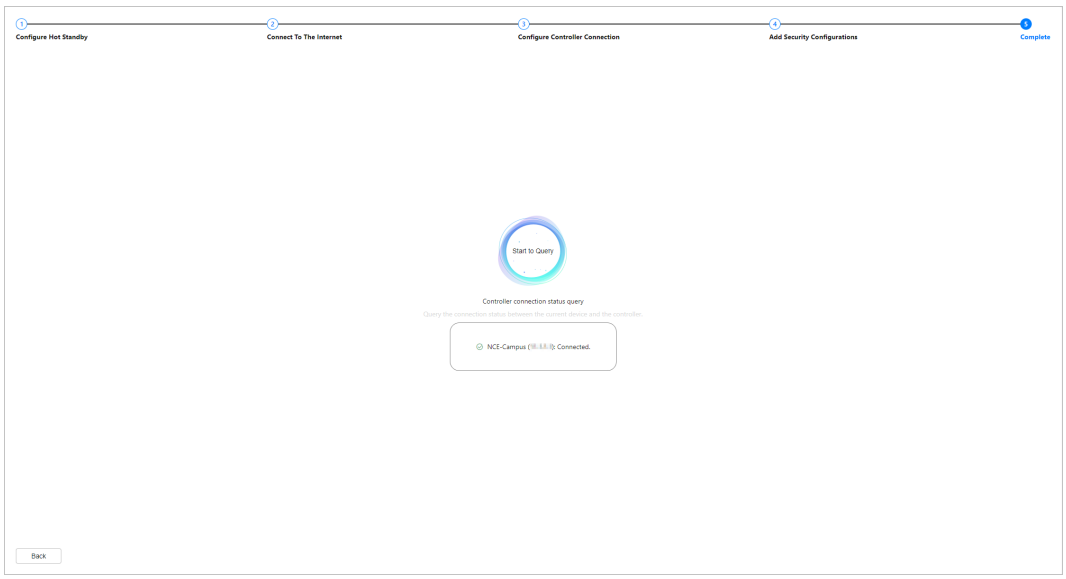
The key configuration points of DeviceB are as follows:

- The device role is standby in the hot standby system.
- The heartbeat interface IP address and the peer interface IP address are different from those on DeviceA, and are 10.10.0.2 and 10.10.0.1, respectively.
- Other configuration items are the same as those of DeviceA. Note that the service interface IP address of the standby device is also the same as that of the active device in mirroring mode.

----End

Verifying the Configuration

Query the controller connection status after the configuration is complete. If the configuration is successful, the following page is displayed.



 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
dns resolve
dns server 3.3.3.3
#
hrp enable
hrp mirror config enable
undo hrp auto-sync config
hrp standby route inject
hrp device active
hrp interface GE0/0/2 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.10.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name GuideSecPolicy_AllowFWToInternet
  source-zone local
  source-zone dmz
  destination-zone untrust
  action permit
 rule name GuideSecPolicy_AllowDMZ
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  action permit
#
ssl policy policyForNCECampus
 pki-domain default
#
ztp certificate-remote 1.1.1.12 port 30217 ssl-
policy policyForNCECampus
#
snetconf server enable
ssh user huawei
ssh user huawei authentication-type x509v3-rsa
ssh user huawei assign pki default
```

DeviceB

```
#
sysname DeviceB
#
dns resolve
dns server 3.3.3.3
#
hrp enable
hrp mirror config enable
undo hrp auto-sync config   //Disable
configuration synchronization. The controller
delivers configurations to both the active and
standby devices.
hrp standby route inject   //Generate a route from
the standby device to the active device through
the heartbeat interface so that the standby device
can be managed by the controller.
hrp device standby
hrp interface GE0/0/2 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%
#
interface GE0/0/1
 ip address 1.1.1.1 255.255.255.0
 gateway 1.1.1.254
#
interface GE0/0/2
 ip address 10.10.0.2 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name GuideSecPolicy_AllowFWToInternet
  source-zone local
  source-zone dmz
  destination-zone untrust
  action permit
 rule name GuideSecPolicy_AllowDMZ
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  action permit
#
ssl policy policyForNCECampus
 pki-domain default
#
ztp certificate-remote 1.1.1.12 port 30217 ssl-
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
ssh user huawei service-type snetconf ssh server assign pki default ssh authorization-type default root # ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr ssh server key-exchange dh_group_exchange_sha256 ssh server dh-exchange min-len 3072 ssh server publickey x509v3-rsa2048-sha256 # ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr ssh client key-exchange dh_group_exchange_sha256 ssh client publickey x509v3-ssh-rsa rsa_sha2_256 rsa_sha2_512 # netconf protocol inbound ssh port 830 callhome cis endpoint NCE-Campus peer-ip 1.1.1.11 port 10020 work-mode yang	policy policyForNCECampus # snetconf server enable ssh user huawei ssh user huawei authentication-type x509v3-rsa ssh user huawei assign pki default ssh user huawei service-type snetconf ssh server assign pki default ssh authorization-type default root # ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr ssh server key-exchange dh_group_exchange_sha256 ssh server dh-exchange min-len 3072 ssh server publickey x509v3-rsa2048-sha256 # ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr ssh client key-exchange dh_group_exchange_sha256 ssh client publickey x509v3-ssh-rsa rsa_sha2_256 rsa_sha2_512 # netconf protocol inbound ssh port 830 callhome cis endpoint NCE-Campus peer-ip 1.1.1.11 port 10020 work-mode yang

20.4 CLI: Example for Sending IPv4 Session Logs to the SecoManager

Networking Requirements

As shown in **Figure 20-4**, DeviceA is deployed at the border of a network as a gateway. A NAT policy in PAT mode is configured on DeviceA to perform the address and port translation for packets that access external networks from the internal network.

The administrator wants to check IPv4 PAT session logs on the SecoManager to understand the creation of sessions by packet in a timely manner and, when necessary, perform NAT source tracing.

 Copyright © Huawei Technologies Co., Ltd.

Figure 20-4 Networking diagram of checking IPv4 session logs on the SecoManager

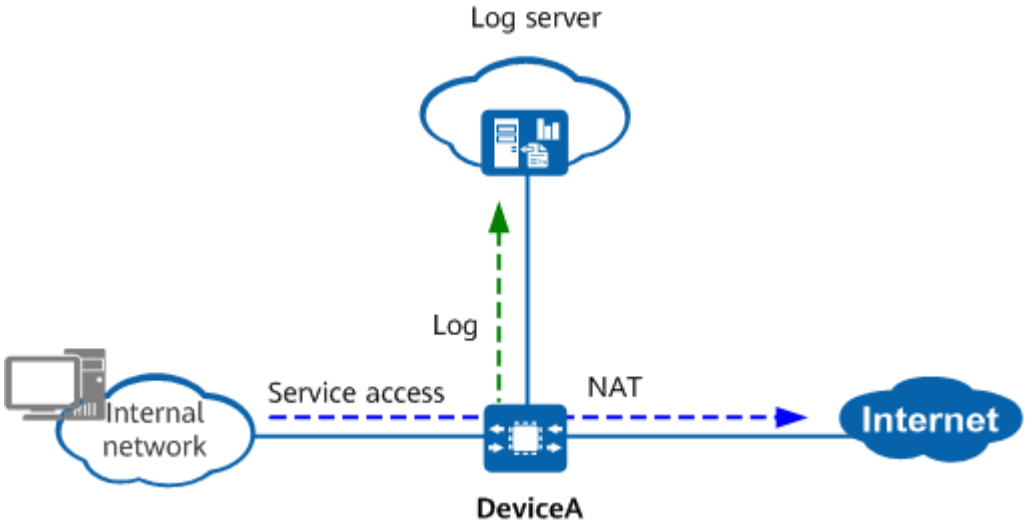


Table 20-1 Data planning

Data Planning on DeviceA		Data Planning on the SecoManager	
Interface and IP Address	**Security Policy**	**IP Address**	**Collection Mode**
Interface connecting to the SecoManager: GE0/0/1 Associated security zone: DMZ IP address: 172.16.81.1/16	Security policy for service traffic: • Source security zone: Trust • Destination security zone: Untrust • Source IP address: 192.168.0.0/24 • Action: Permit • Session logging function: enabled NAT policy for service traffic: • Source security zone: Trust • Destination security zone: Untrust • Source IP address: 192.168.0.0/24 • Action: NAT • NAT address pool: addr1	172.16.110.168	Collector rule set: Firewall_Session Port: 9002

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

To meet the preceding requirements, the administrator needs to consider the following key configuration points:

- Configure a NAT policy in PAT mode on DeviceA, and set interconnection parameters to output logs to the SecoManager.
- Configure log access on the SecoManager and associate the collector with the log source.

Procedure

Step 1 Configure DeviceA.

1. Check whether the time zone and time of the device are the same as those of the SecoManager collector. In the case of inconsistency, run the following commands to adjust the time zone or time of the device.

   # Adjust the time zone of the device to keep consistency with that of the SecoManager collector. Assume that the SecoManager collector is in the Beijing time zone. The time of the collector is 8 hours earlier than the default Universal Time Coordinated (UTC) on the device. Therefore, use the **add 08:00:00** parameter. If the SecoManager collector is in a time zone where the time is later than UTC, use the **minus** parameter.

   ```
   <HUAWEI> clock timezone BJ add 08:00:00
   ```

   # Adjust the time of the device to keep consistency with that of the SecoManager collector. Assume that the current time of the SecoManager collector is 00:00:00 on August 1, 2020.

   ```
   <HUAWEI> clock datetime 0:0:0 2020-08-01
   ```

   After the preceding configuration, run the **display clock** command to view configuration results.

   ```
   <HUAWEI> display clock
   2020-08-01 16:26:51.835 +08:00
   2020-08-01 16:26:51+08:00
   Saturday
   Time Zone(Beijing) : UTC+08:00
   ```

2. If the SecoManager manages the device through automatic discovery, SNMP parameters must be configured on the device. However, if the SecoManager manages the device through manual adding, skip this step.

   Configure SNMP parameters on the device, so that it can be automatically discovered by the SecoManager. As SNMPv3 is more secure than SNMPv1 or SNMPv2c, you are advised to use SNMPv3. In addition, you are advised to use SHA2-256 as the authentication protocol and AES128 as the encryption protocol.

   ```
   <HUAWEI> system-view
   [HUAWEI] sysname DeviceA
   [DeviceA] snmp-agent sys-info version v3
   [DeviceA] snmp-agent group v3 group privacy
   [DeviceA] snmp-agent usm-user v3 admin group group
   [DeviceA] snmp-agent usm-user v3 admin authentication-mode sha2-256
   Please configure the authentication password (8-255)
   Enter Password:
   Confirm Password:
   [DeviceA] snmp-agent usm-user v3 admin privacy-mode aes128
   Please configure the privacy password (8-255)
   Enter Password:
   Confirm Password:
   ```

 Copyright © Huawei Technologies Co., Ltd.

3. Configure an IP address for an interface and add the interface to a security zone. The following uses the interface connecting the device to the SecoManager as an example.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 172.16.81.1 16
[DeviceA-GE0/0/1] service-manage enable
[DeviceA-GE0/0/1] service-manage snmp permit
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/1
[DeviceA-zone-dmz] quit
```

NOTE

The device is managed in automatic discovery mode in this example. Therefore, you need to run the **service-manage enable** and **service-manage snmp permit** commands on the interface to enable the SNMP access permission. You do not need to configure the access permission in manual adding mode.

If the device and the SecoManager belong to different networks, you need to configure a route to the SecoManager on the device.

4. Configure a security policy for service traffic.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

NOTE

Session log packets are not controlled by security policies. Therefore, you do not need to configure a security policy for session logs. You only need to configure the preceding security policy.

5. Configure the NAT policy.

   # Configure the NAT address pool and use the PAT mode (also the default mode). If the **mode no-pat** command is used to specify the No-PAT mode, the device will generate No-PAT session logs.

```
[DeviceA] nat address-group addr1
[DeviceA-address-group-addr1] mode pat
[DeviceA-address-group-addr1] section 0 192.168.5.100 192.168.5.120
[DeviceA-address-group-addr1] quit
```

   # Configure the NAT policy and reference the NAT address pool.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] source-zone trust
[DeviceA-policy-nat-rule-policy1] destination-zone untrust
[DeviceA-policy-nat-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-nat-rule-policy1] action source-nat address-group addr1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] quit
```

6. Set the IP address of the log server to 172.16.110.168 and port to 9002.

```
[DeviceA] firewall log host 1 172.16.110.168 9002
```

7. Set the source IP address and port for the device to send session logs.

```
[DeviceA] firewall log source 172.16.81.1 6666
```

8. Configure the log encryption password.

```
firewall log password YsHsjx_202206
```

 Copyright © Huawei Technologies Co., Ltd.

9. **Optional:**

   Set the output format of session logs to binary.

   ```
   [DeviceA] firewall log session log-type binary
   ```

   NOTE

   The default output format of session logs is binary.

10. Configure the session log type according to actual requirements.

    NOTICE

    If the device outputs session aging logs, session creation logs, and periodic session logs at the same time, the number of logs received by the SecoManager increases sharply, consuming the storage space. Therefore, perform this configuration with caution.

    # To enable the device to output logs when sessions are created, run the following command:

    ```
    [DeviceA] firewall log session new-session enable
    ```

    # To enable the device to output logs periodically, run the following command. Assume that session logs are output every 120 minutes.

    ```
    [DeviceA] firewall log session periodic enable
    [DeviceA] firewall log session periodic time-interval 120
    ```

    # When the address pool is in No-PAT mode, run the following command to output information about the dynamic server mapping table generated by NAT No-PAT.

    ```
    [DeviceA] firewall log nat-nopat enable
    ```

11. Enable the session logging function.

    # Enable the session logging function in the security policy for service traffic.

    ```
    [DeviceA] security-policy
    [DeviceA-policy-security] rule name policy1
    [DeviceA-policy-security-rule-policy1] session logging
    [DeviceA-policy-security-rule-policy1] quit
    [DeviceA-policy-security] quit
    ```

Step 2 Configure the SecoManager.

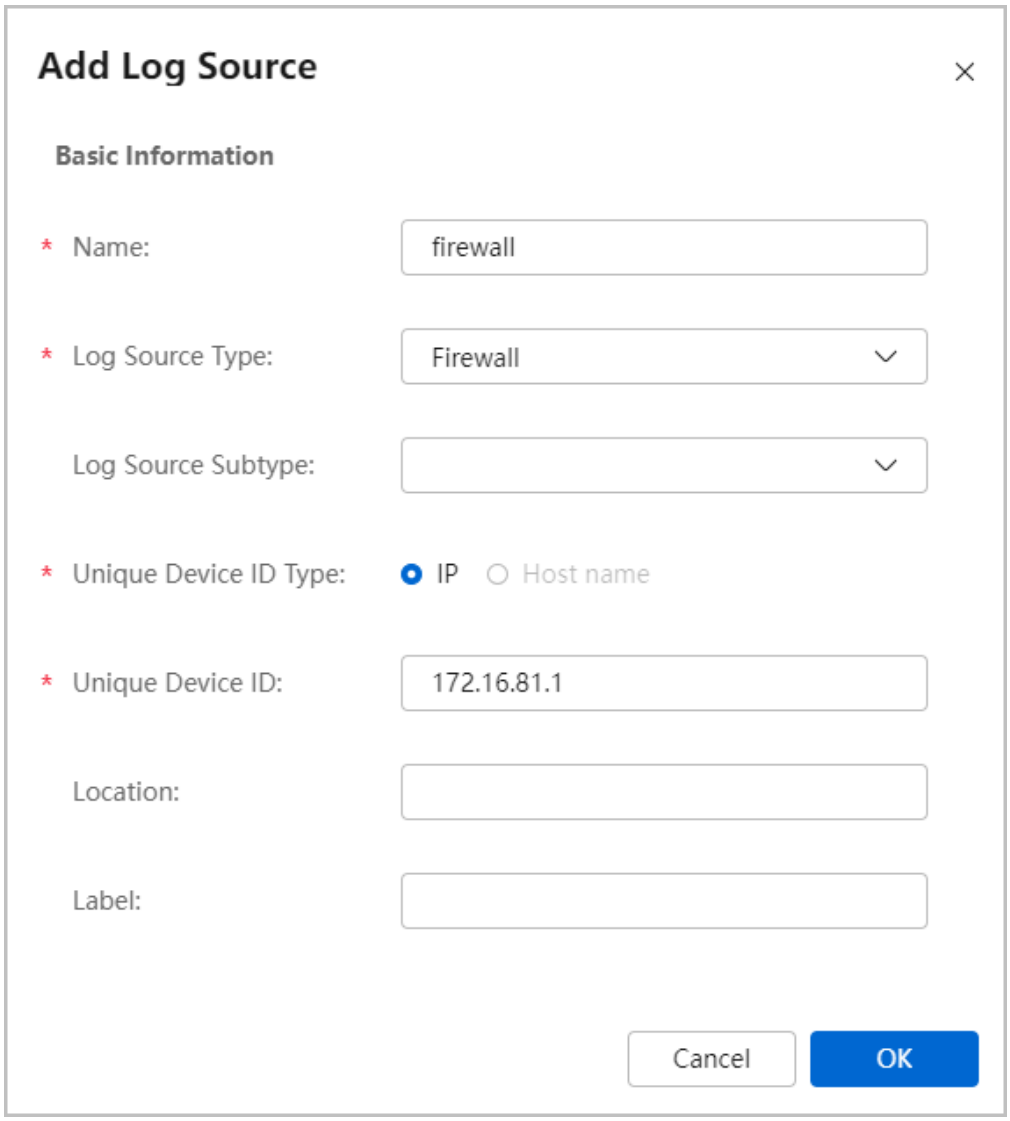
NOTE

The SecoManager GUI is for reference only. The GUI may vary depending on the version.

1. **Optional:** Open the **Device Log Management** app, choose **Log Access** > **Log Source Management**, and click **Add**.

   Devices managed by the SecoManager are automatically synchronized to the **Log Source Management** page as log sources. You need to perform this step only when a device is not managed.

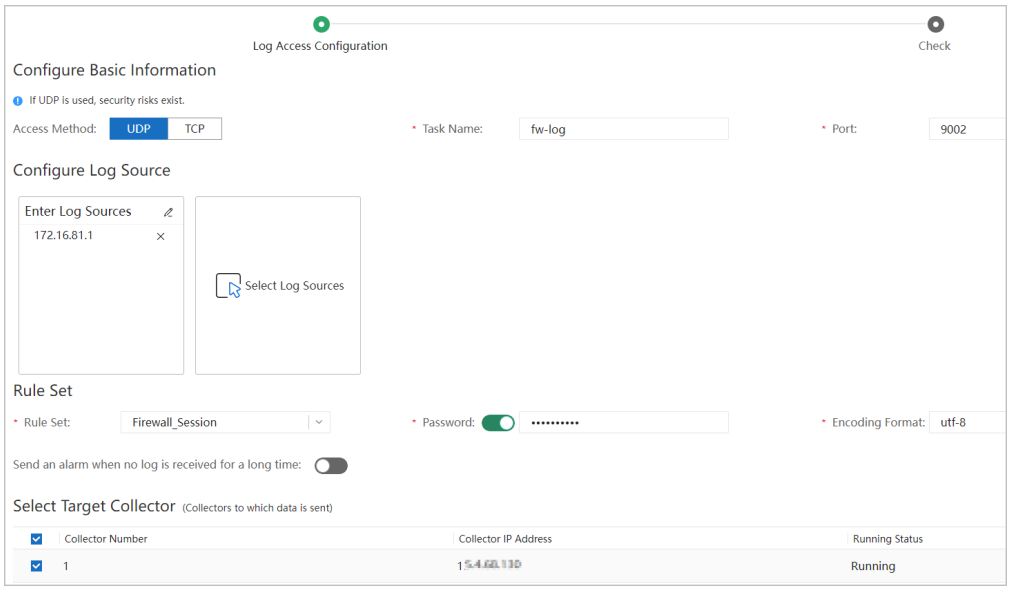
 Copyright © Huawei Technologies Co., Ltd.



2. Open the **Device Log Management** app, choose **Log Access** > **Log Access Management**, and click **Create New Task**.
3. Set basic task parameters and click **Next**.

   The password must be the same as that configured using the **firewall log password** command on the device.

 Copyright © Huawei Technologies Co., Ltd.



4. Verify that the configurations are correct and click **Commit**.
5. The new task is displayed in the log access task list and is in **Running** state.

----End

Verifying the Configuration

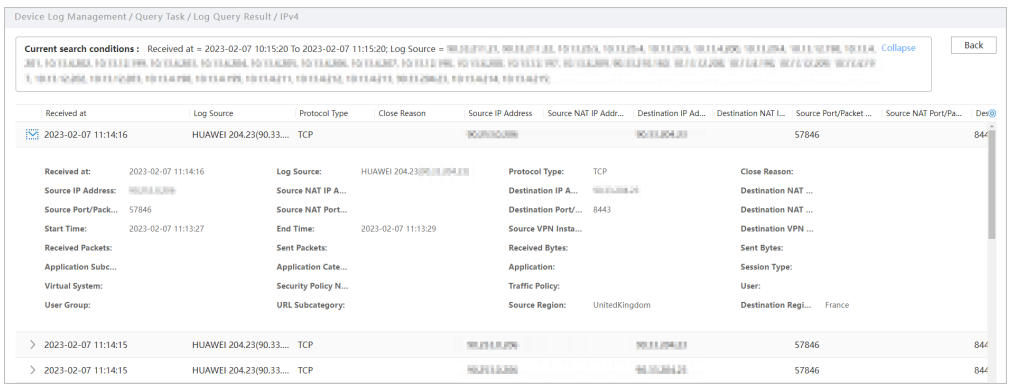
After the configurations are complete, when users on internal networks access external networks, corresponding sessions are generated on the device. After the sessions age, the device sends the session logs to the SecoManager. Then you can view the IPv4 session logs on the SecoManager.

1. Open the **Device Log Management** app, and choose **Session Analysis** > **IPv4 Session Log**.
2. Set parameters for querying logs and click **Query**.

   The following figure shows detailed information about log query results. The log information here is for reference only. Log information varies depending on actual network environments.

   NOTE

   To view session creation logs, select **The duration of the session should have intersection with the query time range** from the **Session Query Type** drop-down list box.



By checking the log information above, the administrator can learn about the

creation of sessions by packet in time. They can also learn about the information (such as the IP address) before NAT is performed on packets and perform, when necessary, the NAT source tracing.

Configuration Scripts

```
#
sysname DeviceA
#
firewall log source 172.16.81.1 6666
firewall log host 1 172.16.110.168 9002
firewall log password $1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!ab48y=Ic*xEUR4pVhR2"9-~,$
firewall log session periodic enable
firewall log session periodic time-interval 120
firewall log session new-session enable
firewall log nat-nopat enable
#
interface GE0/0/1
 ip address 172.16.81.1 255.255.0.0
 service-manage snmp permit
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
snmp-agent
#
snmp-agent sys-info version v3
snmp-agent group v3 group privacy
#
snmp-agent usm-user v3 admin
snmp-agent usm-user v3 admin group group
snmp-agent usm-user v3 admin authentication-mode sha2-256 cipher %^%#ZgL-L2HsZ<5P]s
+:6d)LcBG5)~mdl=te
snmp-agent usm-user v3 admin privacy-mode aes128 cipher %^%#i!rs46cpF"_)d#.cJ,'1>wE_>wE
#
nat address-group addr1 0
 mode pat
 section 0 192.168.5.100 192.168.5.120
#
security-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  session logging
  action permit
#
nat-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  action source-nat address-group addr1
#
return
```

20.5 CLI: Example for Sending User Session Logs to the SecoManager

Networking Requirements

As shown in **Figure 20-5**, DeviceA is deployed at the egress of the home broadband network to connect to the internal network. It is required that the

 Copyright © Huawei Technologies Co., Ltd.

session logs of Internet access recorded on DeviceA contain user names. DeviceA sends the logs to the log host so that the administrator can view and analyze session information.

Figure 20-5 Networking diagram of sending session logs to the log host.

NOTE

In this example, interfaces 1, 2, and 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

The networking diagram uses the home broadband network as an example. The wireless network also requires user source tracing based on session logs. The configuration procedures are the same, but the fields for source tracing may be different. This example applies to the configurations of two networking modes.

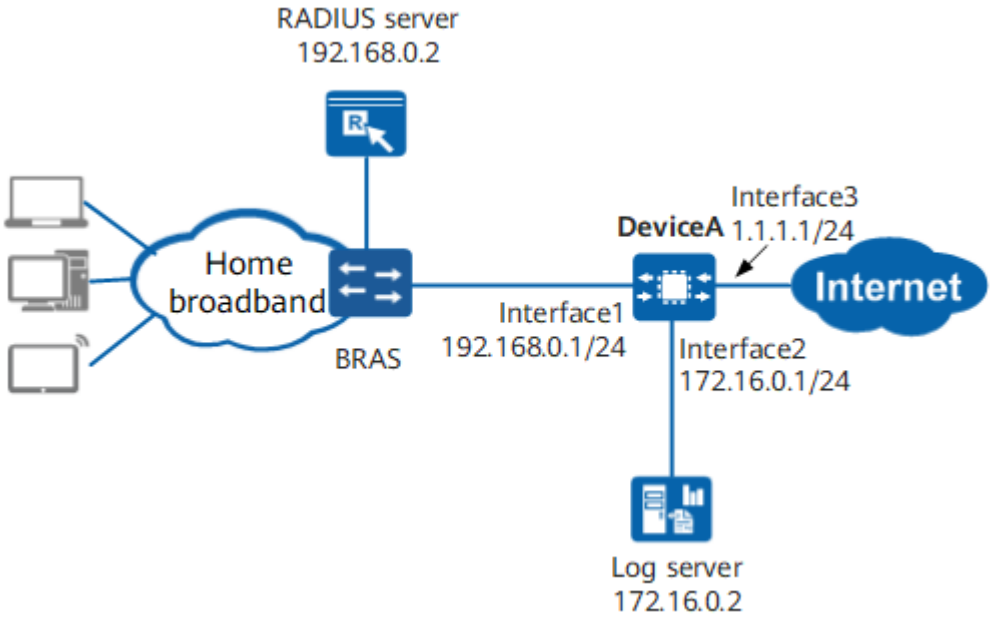


Table 20-2 Data planning

Item	Data	Description
RADIUS SSO	• RADIUS SSO: enabled • Working mode: off-path • Shared key: Test@123 • Interface for receiving accounting packets: GE0/0/1 • Parsed traffic: 192.168.0.1:1813	Configure SSO parameters on DeviceA so that DeviceA can parse RADIUS accounting packets.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

NOTE

- This example describes only the configurations related to the output of session logs. The system time must be set correctly during the initial configuration. Changing the system time during device running will result in incorrect timestamps in historical logs. The time zone of the log server must be the same as that of the device.
- In this mode, a BRAS needs to send an Accounting Start packet to the RADIUS server and the device simultaneously. The device then parses and responds to the Accounting Start packet.

Home broadband users need to be authenticated by the RADIUS server. After parsing accounting packets between the gateway (BRAS in the figure) and RADIUS server, DeviceA obtains the mapping between user IP addresses and user names and sends session logs containing user names to the log server.

1. Configure security zones and security policies.
2. Configure RADIUS SSO to enable users to go online and the device to parse the fields for user source tracing.
3. Configure the log hosts.

Procedure

Step 1 Configure interfaces on DeviceA and add the interfaces to security zones.

Configure an IP address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] ip address 192.168.0.1 24
[DeviceA-GE0/0/1] quit
```

Set an IP address for GE0/0/2 and configure interface access management.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] ip address 172.16.0.1 24
[DeviceA-GE0/0/2] quit
```

NOTE

If the device and SecoManager belong to different networks, you need to configure a route to SecoManager on the device.

Configure an IP address for GE0/0/3.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] ip address 1.1.1.1 24
[DeviceA-GE0/0/3] quit
```

Add GE0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE0/0/2 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE0/0/3 to the Untrust zone.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge0/0/3
[DeviceA-zone-untrust] quit
```

Step 2 Configure a security policy and enable the session logging function. This function takes effect only when the action in the security policy is set to **permit**.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name trust_untrust
[DeviceA-policy-security-rule-trust_untrust] source-zone trust
[DeviceA-policy-security-rule-trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-trust_untrust] source-address 192.168.0.1 24
[DeviceA-policy-security-rule-trust_untrust] action permit
[DeviceA-policy-security-rule-trust_untrust] session logging
[DeviceA-policy-security-rule-trust_untrust] quit
```

NOTE

Session log packets are not subject to security policies. Therefore, you do not need to configure a security policy for session logs. Instead, you need to configure only the preceding security policy.

Step 3 Configure RADIUS SSO.

```
[DeviceA] identity-management
[DeviceA-identity-management]sso-radius
[DeviceA-identity-management-sso-radius] mode out-of-path
[DeviceA-identity-management-sso-radius] shared-key Test@123
[DeviceA-identity-management-sso-radius] ingress-interface ge 0/0/1
[DeviceA-identity-management-sso-radius] server ip 192.168.0.1 port 1813
[DeviceA-identity-management-sso-radius] radius-sso enable
```

Step 4 Customize the RADIUS attributes as fields for source tracing in session logs. Perform this step based on the site requirements. (The following attribute IDs are for reference only.)

```
[DeviceA-identity-management-sso-radius] user-name attribute-id 31
```

Step 5 Configure the device to parse the IPv6 address prefix in RADIUS accounting packets so that IPv6 users can go online.

```
[DeviceA-identity-management-sso-radius] ipv6prefix 32
[DeviceA-identity-management-sso-radius] quit
[DeviceA-identity-management]quit
```

Step 6 Configure the log hosts.

```
[DeviceA] firewall log host 1 172.16.0.2 9002
[DeviceA] firewall log session log-type binary
```

Step 7 Configure the source IP address and source port for sending logs.

```
[DeviceA] firewall log source 172.16.0.1 6000
```

Step 8 Configure the content extension function for session logs in binary format.

The **user** parameter is optional. This parameter indicates that the user field in session logs is stored based on the actual length instead of a fixed length, saving storage space.

```
[DeviceA] firewall log session log-type binary content smart-append user
```

Step 9 Configure the BRAS to send RADIUS accounting packets to the device. The encryption key configured on the BRAS must be the same as the shared key configured for RADIUS SSO on the device. Otherwise, the device cannot correctly parse the RADIUS accounting packets sent by the BRAS or encrypt the RADIUS Accounting-Response packets sent to the BRAS.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

- Run the **display identity-management online-user** command on DeviceA to view user source tracing information.

```
<DeviceA> display identity-management online-user verbose
Current Total Number: 1
---------------------------------------------------------------------------
Vsys Index: 0
IP Address: 10.1.1.1
User Name : test
Login Time: 2022-04-18 23:48:33  Online Time 00:01:14  Time-left: 00:10:00
Authentication Mode: RADIUS SSO Authentication
Security Group: -
```

- View IPv4 session logs on SecoManager. Specifically, open the **Device Log Management** app, choose **Session Analysis** > **IPv4 Session Log**, and click the **IPv4 Session** tab. The queried session logs contain the user names.

Configuration Scripts

```
#
sysname DeviceA
#
identity-management
 sso-radius
  mode out-of-path
  shared-key Test@123 %^%#o3Z7,b[Ox7Sc#r-f+WDC:D=s%^%#
  ingress-interface GE0/0/1
  server ip 192.168.0.1 port 1813
  radius-sso enable
  user-name attribute-id 31
  ipv6prefix 32
#
 firewall log host 1 172.16.0.2 9002
 firewall log session log-type binary
 firewall log source 172.16.0.1 6000
 firewall log session log-type binary content smart-append user
#
interface GE0/0/1
 ip address 192.168.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name trust_untrust
  session logging
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 24
  action permit
#
```

 Copyright © Huawei Technologies Co., Ltd.

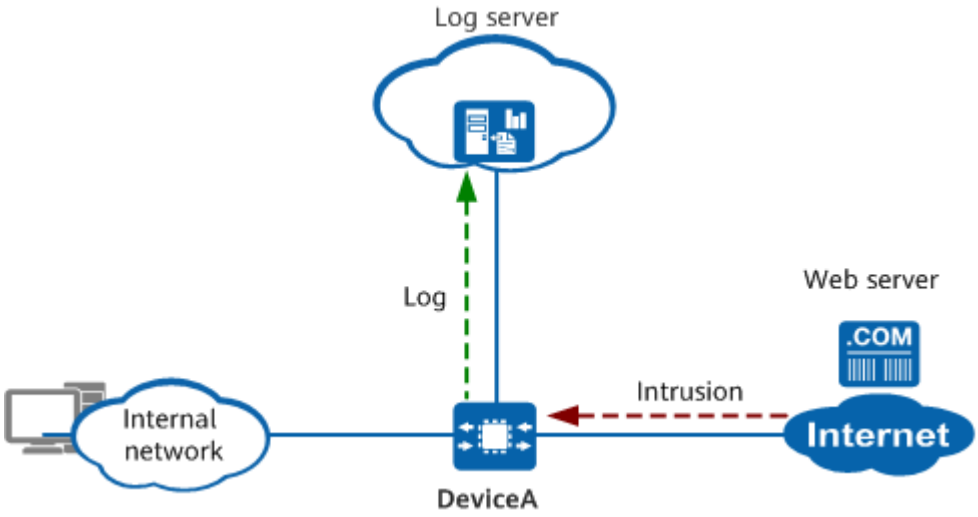
20.6 CLI: Example for Sending Intrusion Prevention Logs to the SecoManager

Networking Requirements

As shown in **Figure 20-6**, DeviceA is deployed at the border of a network as a gateway. The intrusion prevention function is configured on DeviceA to protect users on the internal network against attacks from malicious web servers.

The network administrator wants to check intrusion prevention logs on the SecoManager to learn the attacks from malicious web servers on external networks and thereby make timely policy adjustment or implement proactive attack defense.

Figure 20-6 Networking diagram of checking intrusion prevention logs on the SecoManager



 Copyright © Huawei Technologies Co., Ltd.

Table 20-3 Data planning

Data Planning on DeviceA		Data Planning on the SecoManager	
Interface and IP Address	**Security Policy**	**IP Address**	**Collection Mode**
Interface connecting to the SecoManager: GE0/0/1 Associated security zone: DMZ IP address: 172.16.81.1/16	Security policy for service traffic: • Source security zone: Trust • Destination security zone: Untrust • Source IP address: 192.168.0.0/24 • Action: Permit • Intrusion prevention profile: default	172.16.110.168	• When logs in syslog format are collected: – Collector rule set: Firewall_Syslog – Port number: 514 • When logs in dataflow format are collected: – Collector rule set: Firewall_Dataflow – Port number: 9903

Configuration Roadmap

To meet the preceding requirements, the administrator needs to consider the following key configuration points:

- Configure the intrusion prevention function on DeviceA, and set interconnection parameters to output logs to the SecoManager.
- Configure log access on the SecoManager and associate the collector with the log source.

NOTE

This example describes configurations related to logs. For details about how to configure the SecoManager to manage devices, see the SecoManager product documentation. If the SecoManager does not manage devices, you need to manually add log sources on it.

Procedure

Step 1 Configure DeviceA.

1. Check whether the time zone and time of the device are the same as those of the SecoManager collector. In the case of inconsistency, run the following commands to adjust the time zone or time of the device.

   # Adjust the time zone of the device to keep consistency with that of the SecoManager collector. Assume that the SecoManager collector is in the Beijing time zone. The time of the collector is 8 hours earlier than the default Universal Time Coordinated (UTC) on the device. Therefore, use the **add**

 Copyright © Huawei Technologies Co., Ltd.

08:00:00 parameter. If the SecoManager collector is in a time zone where the time is later than UTC, use the **minus** parameter.

```
<HUAWEI> clock timezone BJ add 08:00:00
```

Adjust the time of the device to keep consistency with that of the SecoManager collector. Assume that the current time of the SecoManager collector is 00:00:00 on August 1, 2020.

```
<HUAWEI> clock datetime 0:0:0 2020-08-01
```

After the preceding configuration, run the **display clock** command to view configuration results.

```
<HUAWEI> display clock
2020-08-01 16:26:51.835 +08:00
2020-08-01 16:26:51+08:00
Saturday
Time Zone(Beijing) : UTC+08:00
```

2. Configure an IP address for an interface and add the interface to a security zone. The following uses the interface connecting the device to the SecoManager as an example. In addition, if the device and the SecoManager belong to different networks, you need to configure a route to the SecoManager on the device.

```
[DeviceA] interface ge 0/0/1
[DeviceA] undo portswitch
[DeviceA-GE0/0/1] ip address 172.16.81.1 16
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/1
[DeviceA-zone-dmz] quit
```

3. Configure a security policy that allows the device to send logs to the SecoManager.

```
[DeviceA]security-policy
[DeviceA-policy-security]rule name log_policy
[DeviceA-policy-security-rule-log_policy] source-zone local
[DeviceA-policy-security-rule-log_policy] destination-zone dmz
[DeviceA-policy-security-rule-log_policy] destination-address 172.16.110.168 16
[DeviceA-policy-security-rule-log_policy] action permit
[DeviceA-policy-security-rule-log_policy] quit
[DeviceA-policy-security] quit
```

4. Configure a security policy for service traffic.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

5. Configure the log server.

   Set the format of service logs to be output based on the site requirements.

   – Output service logs in syslog format.

     # Enable the information center function. This step is optional. By default, the information center function is enabled on the device. If the information center function is disabled, run the following command to enable it.

     ```
     [DeviceA] info-center enable
     ```

     # Add intrusion prevention logs to the information channel where the log server resides. This step is optional. By default, the severity level of logs output by the information channel where the log server resides is

 Copyright © Huawei Technologies Co., Ltd.

informational (level 6). The severity level of intrusion prevention logs is higher than informational. Therefore, intrusion prevention logs can be output by default.

```
[DeviceA] info-center source IPS channel loghost
```

Set the IP address of the log server to 172.16.110.168.

```
[DeviceA] info-center loghost 172.16.110.168
```

Configure the function of sending logs in syslog format.

```
[DeviceA] firewall log service log-type syslog
```

This step is optional. By default, service logs in syslog format are sent.

– Output service logs in dataflow format.

Set the IP address of the log server to 172.16.110.168.

```
[DeviceA] firewall log host 1 172.16.110.168 9002
```

When sending service logs in dataflow format to the SecoManager, the device uses fixed port 9903, which is irrelevant to the port number configured on the log server. If port 9903 is used, the device cannot send session logs in dataflow and binary formats at the same time. Therefore, set the port number to 9002.

Configure the source IP address and port to be used to send service logs.

```
[DeviceA] firewall log source 172.16.81.1 6666
```

Configure the log encryption password.

```
[DeviceA] firewall log password YsHsjx_202206
```

Configure the function of sending logs in dataflow format.

```
[DeviceA] dataflow enable
```

Configure the function of sending intrusion prevention logs.

```
[DeviceA] dataflow type ips enable
```

6. Reference the intrusion prevention profile in the security policy for service traffic. The default profile is used here. You can select another profile according to the actual conditions.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] profile ips default
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

7. Enable the logging function of the intrusion prevention module.

```
[DeviceA] engine log ips enable
```

This step is optional. By default, the logging function of the intrusion prevention module is enabled. If this function is disabled, enable it.

Step 2 Configure log access on the SecoManager.

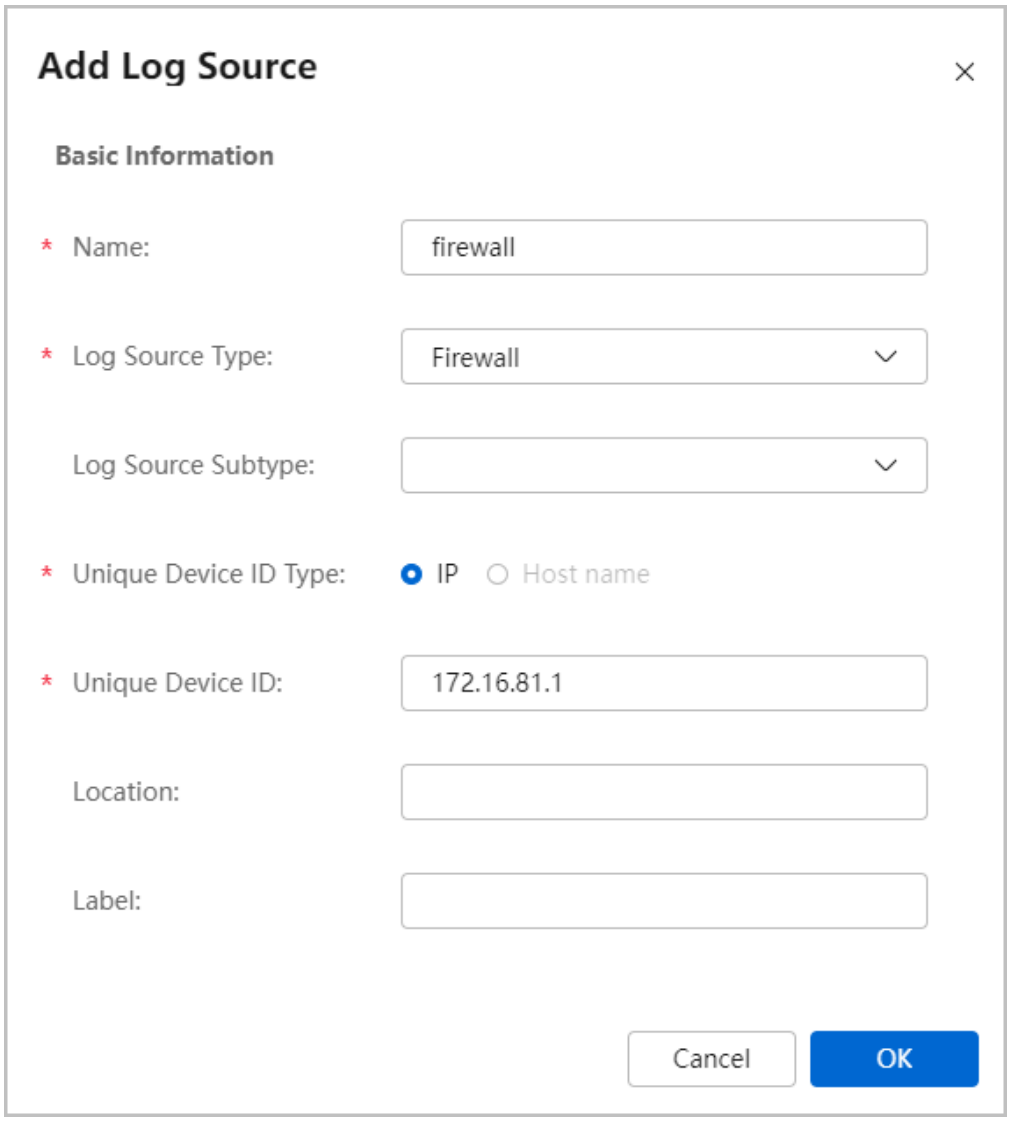
NOTE

The SecoManager GUI is for reference only. The GUI may vary depending on the version.

1. **Optional:** Open the **Device Log Management** app, choose **Log Access** > **Log Source Management**, and click **Add**.

Devices managed by the SecoManager are automatically synchronized to the **Log Source Management** page as log sources. You need to perform this step only when a device is not managed.

 Copyright © Huawei Technologies Co., Ltd.

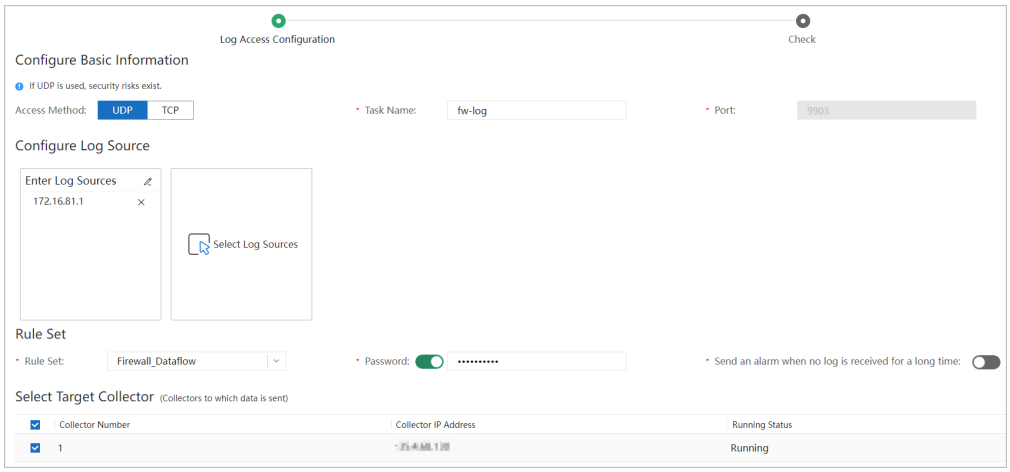


2. Open the **Device Log Management** app, choose **Log Access** > **Log Access Management**, and click **Create New Task**.
3. Set basic task parameters and click **Next**.

   The password must be the same as that configured using the **firewall log password** command on the device.

   The following example describes the collection of logs in dataflow format. If logs in syslog format are collected, set **Rule Set** to **Firewall_Syslog** and **Port** to **514**.

 Copyright © Huawei Technologies Co., Ltd.



4. Verify that the configurations are correct and click **Commit**.
5. In the dialog box that is displayed, click **OK**. The new task is displayed in the log access task list and is in **Running** state.

----End

Verifying the Configuration

After the preceding configurations are completed, if a user on an internal network accesses a malicious web server on an external network, the device performs prevention and sends a log to the SecoManager. Then the intrusion prevention log can be queried on the SecoManager.

1. Open the **Device Log Management** app and choose **Network Security Analysis** > **Threat Log**.
2. Set parameters for querying logs, filter logs whose threat type is intrusion, and click **Query**.

Configuration Scripts

This example provides only the configuration script regarding the interworking between the device and SecoManager.

```
#
sysname DeviceA
# Output service logs in syslog format.
info-center source ips channel 2
info-center loghost 172.16.110.168
# Output service logs in dataflow format.
firewall log host 1 172.16.110.168 9002
firewall log source 172.16.81.1 6666
firewall log password $1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!ab48y=Ic*xEUR4pVhR2"9-~,$
dataflow enable
dataflow type ips enable
#
interface GE0/0/1
 ip address 172.16.81.1 255.255.0.0
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
security-policy
 rule name log-policy
  source-zone local
```

 Copyright © Huawei Technologies Co., Ltd.

```
 destination-zone dmz
 destination-address 172.16.0.0 mask 255.255.0.0
 action permit
rule name policy1
 source-zone trust
 destination-zone untrust
 source-address 192.168.0.0 mask 255.255.255.0
 profile ips default
 action permit
#
return
```

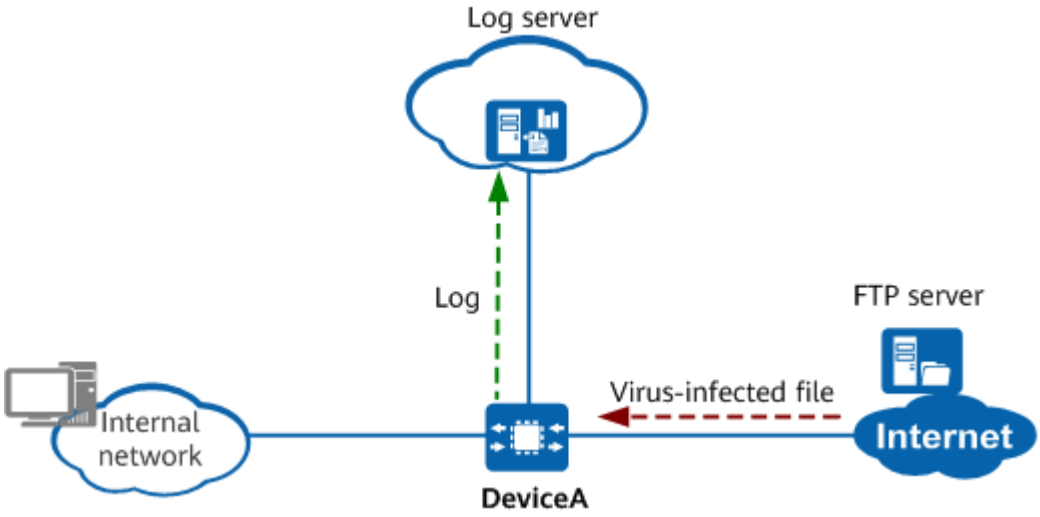
20.7 CLI: Example for Sending Virus Event Logs to the SecoManager

Networking Requirements

As shown in **Figure 20-7**, DeviceA is deployed at the border of a network as a gateway. The administrator configures the antivirus function on DeviceA. When a user on the internal network downloads a virus-infected file from the FTP server, DeviceA blocks the file and thereby ensures the security of the internal network.

The administrator wants to check virus event logs on the SecoManager to learn about the blocking of virus-infected files by DeviceA and frequent virus events and thereby grasp the network security status in time.

Figure 20-7 Networking diagram of checking virus event logs on the SecoManager



 Copyright © Huawei Technologies Co., Ltd.

Table 20-4 Data planning

Data Planning on DeviceA		Data Planning on the SecoManager	
Interface and IP Address	**Security Policy**	**IP Address**	**Collection Mode**
Interface connecting to the SecoManager: GE0/0/1 Associated security zone: DMZ IP address: 172.16.81.1/16	Security policy for service traffic: • Source security zone: Trust • Destination security zone: Untrust • Source IP address: 192.168.0.0/24 • Action: Permit • Antivirus profile: default	172.16.110.168	• When logs in syslog format are collected: – Collector rule set: Firewall_Syslog – Port number: 514 • When logs in dataflow format are collected: – Collector rule set: Firewall_Dataflow – Port number: 9903

Configuration Roadmap

To meet the preceding requirements, the administrator needs to consider the following key configuration points:

- Configure the antivirus function on DeviceA, and set interconnection parameters to output logs to the SecoManager.
- Configure log access on the SecoManager and associate the collector with the log source.

NOTE

This example describes configurations related to logs. For details about how to configure the SecoManager to manage devices, see the SecoManager product documentation. If the SecoManager does not manage devices, you need to manually add log sources on it.

Procedure

Step 1 Configure DeviceA.

1. Check whether the time zone and time of the device are the same as those of the SecoManager collector. In the case of inconsistency, run the following commands to adjust the time zone or time of the device.

   # Adjust the time zone of the device to keep consistency with that of the SecoManager collector. Assume that the SecoManager collector is in the Beijing time zone. The time of the collector is 8 hours earlier than the default Universal Time Coordinated (UTC) on the device. Therefore, use the **add 08:00:00** parameter. If the SecoManager collector is in a time zone where the time is later than UTC, use the **minus** parameter.

   ```
   <HUAWEI> clock timezone BJ add 08:00:00
   ```

 Copyright © Huawei Technologies Co., Ltd.

Adjust the time of the device to keep consistency with that of the SecoManager collector. Assume that the current time of the SecoManager collector is 00:00:00 on August 1, 2020.

```
<HUAWEI> clock datetime 0:0:0 2020-08-01
```

After the preceding configuration, run the **display clock** command to view configuration results.

```
<HUAWEI> display clock
2020-08-01 16:26:51.835 +08:00
2020-08-01 16:26:51+08:00
Saturday
Time Zone(Beijing) : UTC+08:00
```

2. Configure an IP address for an interface and add the interface to a security zone. The following uses the interface connecting the device to the SecoManager as an example. In addition, if the device and the SecoManager belong to different networks, you need to configure a route to the SecoManager on the device.

```
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 172.16.81.1 16
[DeviceA-GE0/0/1] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/1
[DeviceA-zone-dmz] quit
```

3. Configure a security policy that allows the device to send logs to the SecoManager.

```
[DeviceA]security-policy
[DeviceA-policy-security]rule name log_policy
[DeviceA-policy-security-rule-log_policy] source-zone local
[DeviceA-policy-security-rule-log_policy] destination-zone dmz
[DeviceA-policy-security-rule-log_policy] destination-address 172.16.110.168 16
[DeviceA-policy-security-rule-log_policy] action permit
[DeviceA-policy-security-rule-log_policy] quit
[DeviceA-policy-security] quit
```

4. Configure a security policy for service traffic.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy1
[DeviceA-policy-security-rule-policy1] source-zone trust
[DeviceA-policy-security-rule-policy1] destination-zone untrust
[DeviceA-policy-security-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-policy1] action permit
[DeviceA-policy-security-rule-policy1] quit
[DeviceA-policy-security] quit
```

5. Configure the log server.

   Set the format of service logs to be output based on the site requirements.

   – Output service logs in syslog format.

     # Enable the information center function. This step is optional. By default, the information center function is enabled on the device. If the information center function is disabled, run the following command to enable it.

     ```
     [DeviceA] info-center enable
     ```

     # Add virus event logs to the information channel where the log server resides. This step is optional. By default, the severity level of logs output by the information channel where the log server resides is informational (level 6). The severity level of virus event logs is higher than informational. Therefore, virus event logs can be output by default.

     ```
     [DeviceA] info-center source AV channel loghost
     ```

 Copyright © Huawei Technologies Co., Ltd.

Set the IP address of the log server to 172.16.110.168.

```
[DeviceA] info-center loghost 172.16.110.168
```

Configure the function of sending logs in syslog format.

```
[DeviceA] firewall log service log-type syslog
```

This step is optional. By default, service logs in syslog format are sent.

- Output service logs in dataflow format.

  # Set the IP address of the log server to 172.16.110.168.

  ```
  [DeviceA] firewall log host 1 172.16.110.168 9002
  ```

  When sending service logs in dataflow format to the SecoManager, the device uses fixed port 9903, which is irrelevant to the port number configured on the log server. If port 9903 is used, the device cannot send session logs in dataflow and binary formats at the same time. Therefore, set the port number to 9002.

  # Configure the source IP address and port to be used to send service logs.

  ```
  [DeviceA] firewall log source 172.16.81.1 6666
  ```

  # Configure the log encryption password.

  ```
  [DeviceA] firewall log password YsHsjx_202206
  ```

  # Configure the function of sending logs in dataflow format.

  ```
  [DeviceA] dataflow enable
  ```

  # Configure the function of sending virus event logs.

  ```
  [DeviceA] dataflow type av enable
  ```

6. Configure the antivirus function. Ensure that the virus signature database is successfully loaded, and you are advised to update the virus signature database to the latest version.

   # Reference the antivirus profile in the security policy for service traffic. The default profile is used here. You can select another profile according to the actual conditions.

   ```
   [DeviceA] security-policy
   [DeviceA-policy-security] rule name policy1
   [DeviceA-policy-security-rule-policy1] profile av default
   [DeviceA-policy-security-rule-policy1] quit
   [DeviceA-policy-security] quit
   ```

7. Enable the logging function of the antivirus module.

   ```
   [DeviceA] engine log av enable
   ```

   This step is optional. By default, the logging function of the antivirus module is enabled. If this function is disabled, enable it.

Step 2 Configure log access on the SecoManager.

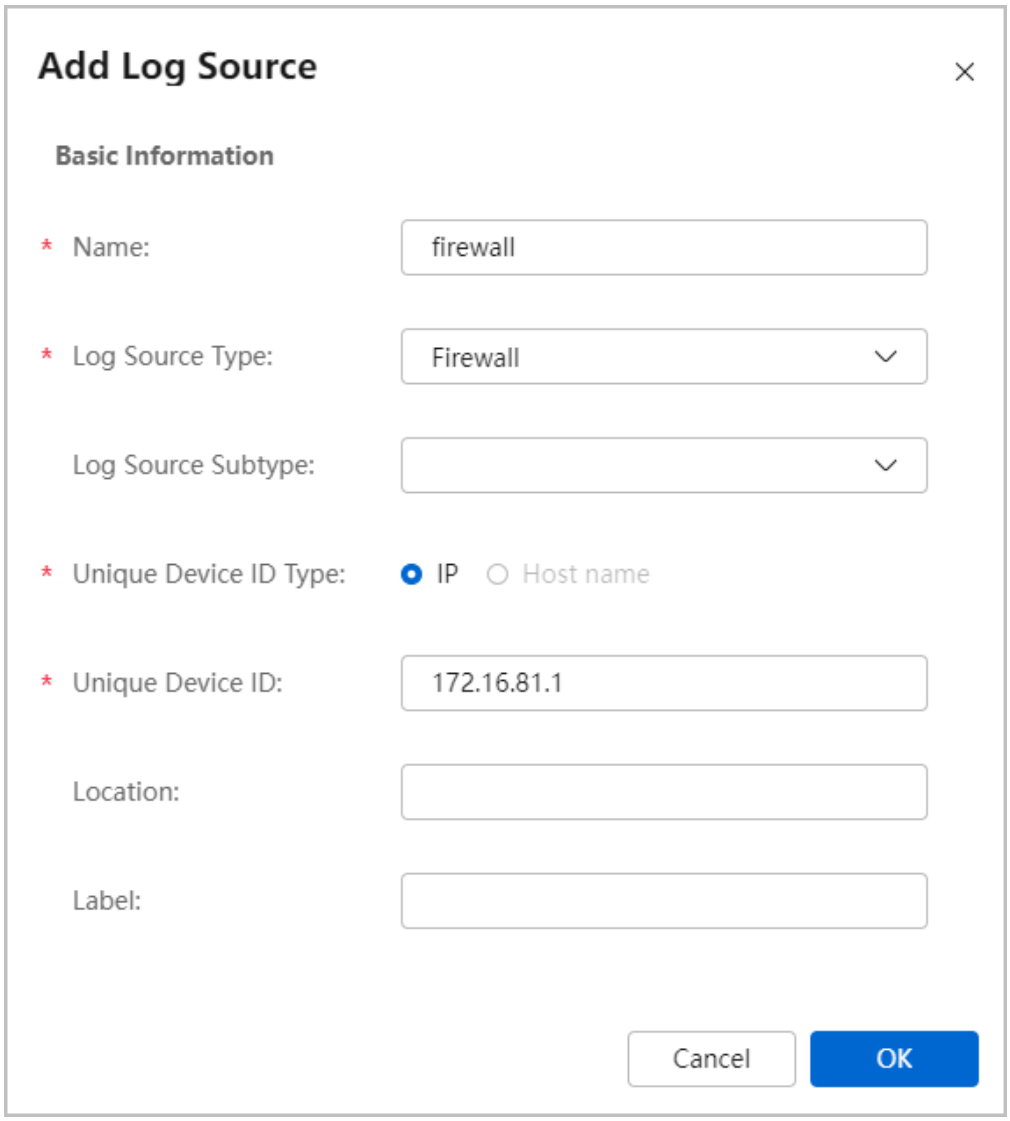
NOTE

The SecoManager GUI is for reference only. The GUI may vary depending on the version.

1. **Optional:** Open the **Device Log Management** app, choose **Log Access** > **Log Source Management**, and click **Add**.

   Devices managed by the SecoManager are automatically synchronized to the **Log Source Management** page as log sources. You need to perform this step only when a device is not managed.

 Copyright © Huawei Technologies Co., Ltd.

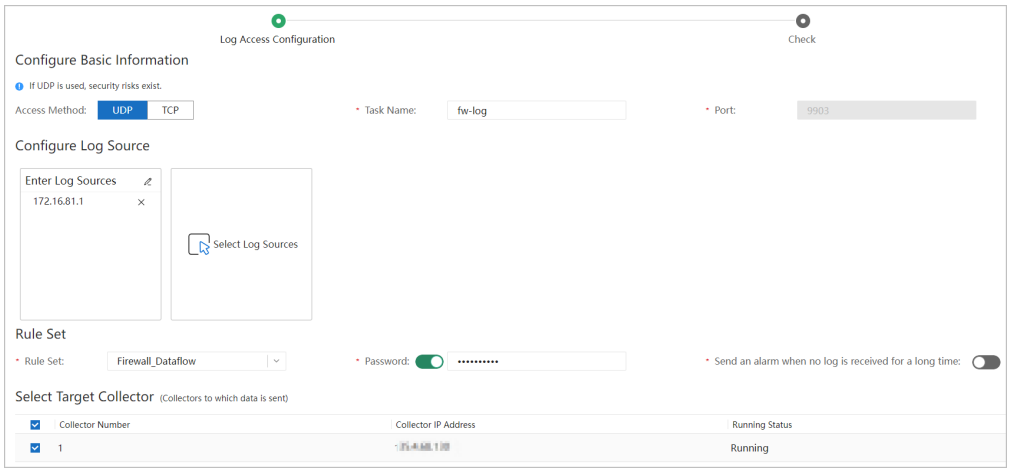


2. Open the **Device Log Management** app, choose **Log Access** > **Log Access Management**, and click **Create New Task**.
3. Set basic task parameters and click **Next**.

   The password must be the same as that configured using the **firewall log password** command on the device.

   The following example describes the collection of logs in dataflow format. If logs in syslog format are collected, set **Rule Set** to **Firewall_Syslog** and **Port** to **514**.

 Copyright © Huawei Technologies Co., Ltd.



4. Verify that the configurations are correct and click **Commit**.
5. In the dialog box that is displayed, click **OK**. The new task is displayed in the log access task list and is in **Running** state.

----End

Verifying the Configuration

After the preceding configurations are complete, when a user on an internal network downloads a virus-infected file (for example, the EICAR file is used to simulate the virus-infected file) from an FTP server on an external network, the device blocks the file and sends a log to the SecoManager. Then you can check the virus event log on the SecoManager.

1. Open the **Device Log Management** app and choose **Network Security Analysis** > **Threat Log**.
2. Set parameters for querying logs, filter logs whose threat type is virus, and click **Query**.

Configuration Scripts

This example provides only the configuration script regarding the interworking between the device and SecoManager.

```
#
sysname DeviceA
# Output service logs in syslog format.
info-center source av channel 2
info-center loghost 172.16.110.168
# Output service logs in dataflow format.
firewall log host 1 172.16.110.168 9002
firewall log source 172.16.81.1 6666
firewall log password $1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!ab48y=Ic*xEUR4pVhR2"9-~,$
dataflow enable
dataflow type av enable
#
interface GE0/0/1
 ip address 172.16.81.1 255.255.0.0
#
firewall zone dmz
 set priority 50
 add interface GE0/0/1
#
security-policy
 rule name log-policy
```

 Copyright © Huawei Technologies Co., Ltd.

```
 source-zone local
 destination-zone dmz
 destination-address 172.16.110.168 16
 action permit
 rule name policy1
 source-zone trust
 destination-zone untrust
 source-address 192.168.0.0 mask 255.255.255.0
 profile av default
 action permit
#
return
```

20.8 CLI: Example for Sending Syslogs in Default or MTN Format to a Third-Party Log Host

Networking Requirements

As shown in **Figure 20-8**, DeviceA is deployed on the network border. The network environment is as follows:

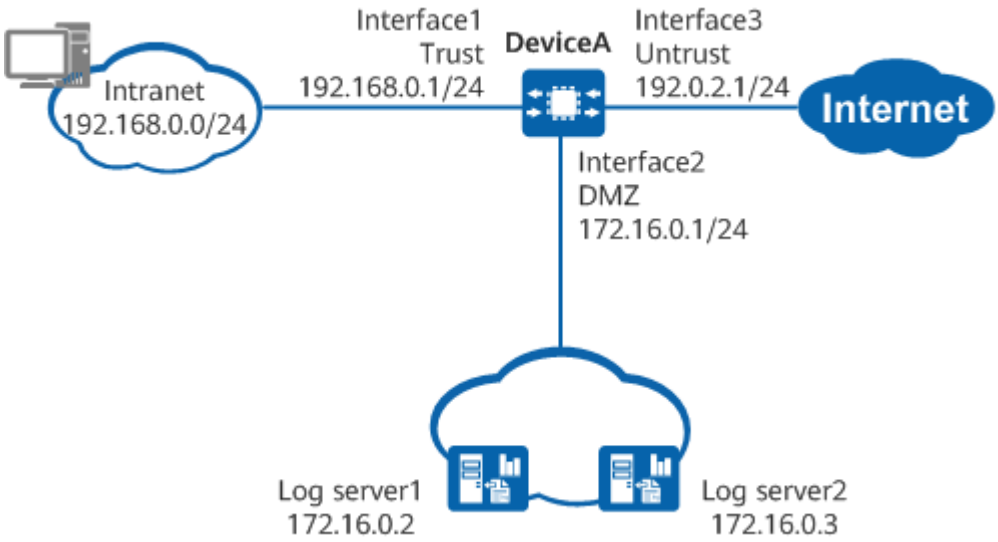
- The intranet is the Trust zone, while the Internet is the Untrust zone. Users on the intranet access the Internet using the NAT function provided by DeviceA.
- The DMZ has two third-party log servers.

DeviceA is required to send session information generated when intranet users access the Internet to the log servers. The log concurrent function is required, so that each log can be sent to both log servers.

Figure 20-8 Networking for sending syslog session logs to log servers

NOTE

In this example, interfaces 1, 2, and 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Configuration Roadmap

NOTE

This example provides only the DeviceA configuration. For the configurations of the third-party log servers, see the product documentation of the third-party log servers.

The system time must be set correctly during the initial configuration. Changing the system time during device running will result in incorrect timestamps in historical logs. The time zone of the log server must be the same as that of DeviceA.

1. Set the IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies.
3. Configure a NAT policy.
4. Configure routes.
5. Configure log servers.
6. Enable the session logging function in a security policy.
7. Configure the log output format and the source IP address and source port, and enable the log concurrent function.

Procedure

Step 1 Set the IP addresses for interfaces and add the interfaces to security zones.

Configure an IP address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 192.168.0.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 172.16.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE0/0/3.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 192.0.2.1 24
[DeviceA-GE0/0/3] quit
```

Add GE0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE0/0/2 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE0/0/3 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/3
[DeviceA-zone-untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure a Trust-Untrust interzone security policy and enable the session logging function. This function takes effect only when the policy action is set to **permit**.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name trust_untrust
[DeviceA-policy-security-rule-trust_untrust] source-zone trust
[DeviceA-policy-security-rule-trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-trust_untrust] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-trust_untrust] action permit
[DeviceA-policy-security-rule-trust_untrust] session logging
[DeviceA-policy-security-rule-trust_untrust] quit
[DeviceA-policy-security] quit
```

NOTE

Session log packets are not subject to security policies. Therefore, you do not need to configure a security policy for session logs. Instead, you need to configure only the preceding security policies.

Step 3 Configure a NAT policy.

Configure NAT address pool 1 and set the mode to PAT. In this example, the public address ranges from 192.0.2.10 to 192.0.2.15.

```
[DeviceA] nat address-group add1
[DeviceA-address-group-add1] mode pat
[DeviceA-address-group-add1] section 0 192.0.2.10 192.0.2.15
[DeviceA-address-group-add1] route enable
[DeviceA-address-group-add1] quit
```

Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] source-zone trust
[DeviceA-policy-nat-rule-policy1] destination-zone untrust
[DeviceA-policy-nat-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-nat-rule-policy1] action source-nat address-group add1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] quit
```

Step 4 Configure a default route. In this example, the next hop of DeviceA to the Internet is 192.0.2.2.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 192.0.2.2
```

Step 5 Configure log servers.

```
[DeviceA] firewall log host 1 172.16.0.2 514
[DeviceA] firewall log host 2 172.16.0.3 514
```

Step 6 Set the session log output format to syslog.

```
[DeviceA] firewall log session log-type syslog
```

Step 7 **Optional:** Set the content format of output syslog session logs to MTN.

```
[DeviceA] firewall log syslog content format mtn
```

NOTE

By default, the content format of syslog session logs is set to default. To configure session logs in the default format, you do not need to run the preceding command.

Session logs output in MTN format can only be parsed by third-party log servers. IPv6 logs cannot be output in MTN format.

Step 8 Enable the log concurrent function and set the source IP address and port number for sending logs.

```
[DeviceA] firewall log session multi-host-mode concurrent
[DeviceA] firewall log source 172.16.0.1 6000
```

 Copyright © Huawei Technologies Co., Ltd.

Step 9 Configure a third-party log server and view logs on it.

----End

Verifying the Configuration

Logs can be viewed on the third-party log server.

Configuration Scripts

```
#
sysname DeviceA
#
firewall log source 172.16.0.1 6000
firewall log host 1 172.16.0.2 514
firewall log host 2 172.16.0.3 514
firewall log session multi-host-mode concurrent
firewall log session log-type syslog
#
nat address-group add1 0
 mode pat
 route enable
 section 0 192.0.2.10 192.0.2.15
#
interface GE0/0/1
 ip address 192.168.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 192.0.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  session logging
  action permit
#
nat-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  action source-nat address-group add1
#
 ip route-static 0.0.0.0 0.0.0.0 192.0.2.2
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

20.9 CLI: Example for Outputting Customized Syslog Session Logs to a Third-Party Log Host

Networking Requirements

As shown in **Figure 20-9**, DeviceA is deployed on the network border. The network environment is as follows:

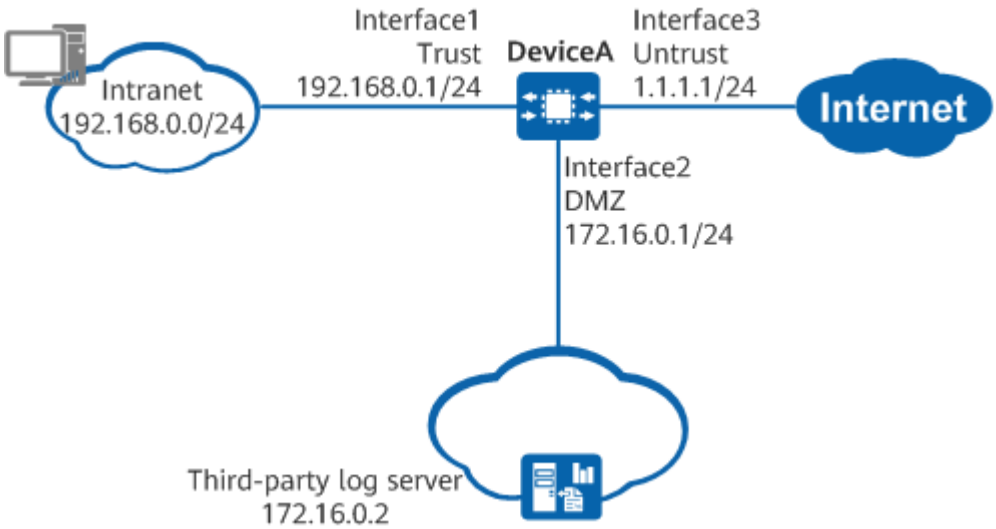
- The intranet is the Trust zone, while the Internet is the Untrust zone. Users on the intranet access the Internet using the NAT function provided by DeviceA.
- A third-party log server is deployed in the DMZ.

DeviceA is required to send session information generated when intranet users access the Internet to the third-party log server in the customized syslog format. The administrator can view and analyze session information on the third-party log server.

Figure 20-9 Networking for sending syslog session logs to log servers

NOTE

In this example, interfaces 1, 2, and 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Configuration Roadmap

NOTE

This example provides only the DeviceA configuration. For the third-party log server configuration, see the third-party log server product document.

The system time must be set correctly during the initial configuration. Changing the system time during device running will result in incorrect timestamps in historical logs. The time zone of the log server must be the same as that of DeviceA.

1. Set the IP addresses for interfaces and add the interfaces to security zones.

 Copyright © Huawei Technologies Co., Ltd.

2. Configure security policies.
3. Configure a NAT policy.
4. Configure routes.
5. Configure log servers.
6. Enable the session logging function in a security policy.
7. Set the output format of syslog session logs.

Procedure

Step 1 Set the IP addresses for interfaces and add the interfaces to security zones.

Configure an IP address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 192.168.0.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 172.16.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE0/0/3.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 1.1.1.1 24
[DeviceA-GE0/0/3] quit
```

Add GE0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE0/0/2 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE0/0/3 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge0/0/3
[DeviceA-zone-untrust] quit
```

Step 2 Configure a Trust-Untrust interzone security policy and enable the session logging function. This function takes effect only when the policy action is set to **permit**.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name trust_untrust
[DeviceA-policy-security-rule-trust_untrust] source-zone trust
[DeviceA-policy-security-rule-trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-trust_untrust] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-trust_untrust] action permit
[DeviceA-policy-security-rule-trust_untrust] session logging
[DeviceA-policy-security-rule-trust_untrust] quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Session log packets are not subject to security policies. Therefore, you do not need to configure a security policy for session logs. Instead, you need to configure only the preceding security policies.

Step 3 Configure a NAT policy.

Configure NAT address pool 1 and set the mode to PAT. In this example, the public address ranges from 1.1.1.10 to 1.1.1.15.

```
[DeviceA] nat address-group add1
[DeviceA-address-group-add1] mode pat
[DeviceA-address-group-add1] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-add1] route enable
[DeviceA-address-group-add1] quit
```

Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] source-zone trust
[DeviceA-policy-nat-rule-policy1] destination-zone untrust
[DeviceA-policy-nat-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-nat-rule-policy1] action source-nat address-group add1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] quit
```

Step 4 Configure a default route. In this example, the next hop of DeviceA to the Internet is 1.1.1.2.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

Step 5 Configure the log server.

```
[DeviceA] firewall log host 1 172.16.0.2 514
```

Step 6 Configure the source IP address and source port for sending logs.

```
[DeviceA] firewall log source 172.16.0.1 6666
```

Step 7 Set the session log output format to syslog.

```
[DeviceA] firewall log session log-type syslog
```

Step 8 Customize the output syslog content.

You can customize the syslog output format in either expression mode or list mode. These two modes are mutually exclusive. That is, you can select only one mode for a syslog template. The specific configurations are as follows:

- Customizing syslog session logs in expression mode
  a. Configure a template for syslog session logs and access the template view.
     ```
     [DeviceA] session-log template test type syslog
     ```
  b. Configure a content expression for session logs.
     ```
     [DeviceA-syslog-template-test] expression message "$logtype ipver=$ipversion pro:$protocol source=$srcip:$srcport
      destination=$dstip:$dstport"
     [DeviceA-syslog-template-test] quit
     ```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If IPv4 and IPv6 session logs share the same expression, run the preceding command once.
- If IPv4 and IPv6 session logs use different expressions, run the preceding command twice. Set the IPv6 session log expression to **expression message ipv6 "$logtype ipver=$ipversion pro:$protocol source=$srcip:$srcport destination=$dstip:$dstport"**.

c. Set the content format of syslog session logs to the template format.
[DeviceA] **firewall log syslog content format template test**

- Customizing syslog session logs in list mode

a. Configure a template for syslog session logs and access the template view.
[DeviceA] **session-log template test type syslog**

b. Configure field delimiters in syslog session logs.
[DeviceA-syslog-template-test] **separate semicolon**

The default field delimiters are commas (,).

c. Configure the fields contained in syslog session logs and their sequences.
[DeviceA-syslog-template-test] **expression ip-version source-ip destination-ip source-port source-nat-ip source-nat-port protocol**

d. Create prefixes for the fields in syslog session logs.
[DeviceA-syslog-template-test] **ip-version prefix-characters ipversion=**
[DeviceA-syslog-template-test] **protocol prefix-characters Protocol=**
[DeviceA-syslog-template-test] **source-ip prefix-characters Source_IP**
[DeviceA-syslog-template-test] **quit**

e. Set the content format of syslog session logs to the template format.
[DeviceA] **firewall log syslog content format template test**

Step 9 Configure a third-party log server.

----End

Verifying the Configuration

Logs can be viewed on the third-party log server.

Configuration Scripts

The following script uses customizing syslog session logs in list mode as an example.

```
#
sysname DeviceA
#
firewall log source 172.16.0.1 6666
firewall log host 1 172.16.0.2 514
firewall log session log-type syslog
firewall log syslog content format template test
#
nat address-group add1 0
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.15
#
interface GE0/0/1
 ip address 192.168.0.1 255.255.255.0
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/2
 ip address 172.16.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  session logging
  action permit
#
nat-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 24
  action source-nat address-group add1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
session-log template test type syslog
separate semicolon
expression ip-version source-ip destination-ip source-port source-nat-ip source-nat-port protocol
ip-version prefix-characters ipversion=
protocol prefix-characters Protocol=
source-ip prefix-characters Source_IP
#
return
```

20.10 CLI: Example for Outputting Customized NetFlow Session Logs to a Third-Party Log Host

Networking Requirements

As shown in **Figure 20-10**, DeviceA is deployed on the network border. The network environment is as follows:

- The intranet is the Trust zone, while the Internet is the Untrust zone. Users on the intranet access the Internet using the NAT function provided by DeviceA.
- A third-party log server is deployed in the DMZ.

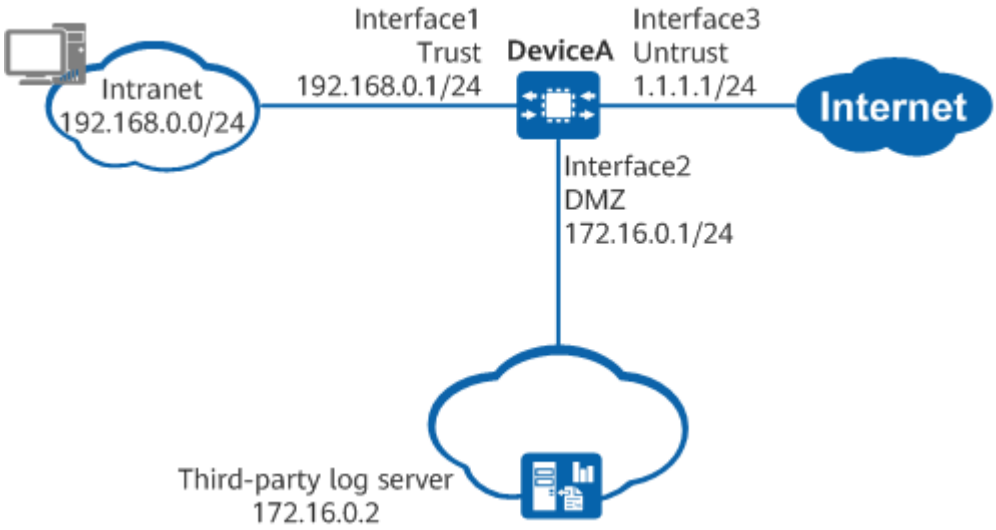
DeviceA is required to send session information generated when intranet users access the Internet to the third-party log server in the customized NetFlow IPv4 format. The administrator can view and analyze session information on the third-party log server.

 Copyright © Huawei Technologies Co., Ltd.

Figure 20-10 Networking for sending NetFlow session logs to a log server

NOTE

In this example, interfaces 1, 2, and 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.



Configuration Roadmap

NOTE

This example provides only the DeviceA configuration. For the third-party log server configuration, see the third-party log server product document.

The system time must be set correctly during the initial configuration. Changing the system time during device running will result in incorrect timestamps in historical logs. The time zone of the log server must be the same as that of DeviceA.

1. Set the IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies.
3. Configure a NAT policy.
4. Configure routes.
5. Enable the session logging function in a security policy.
6. Configure a log server.
7. Customize the output format of NetFlow session logs.

Procedure

Step 1 Set the IP addresses for interfaces and add the interfaces to security zones.

Configure an IP address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 192.168.0.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE0/0/2.

 Copyright © Huawei Technologies Co., Ltd.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 172.16.0.1 24
[DeviceA-GE0/0/2] quit
```

Configure an IP address for GE0/0/3.

```
[DeviceA] interface ge0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 1.1.1.1 24
[DeviceA-GE0/0/3] quit
```

Add GE0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE0/0/2 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE0/0/3 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge0/0/3
[DeviceA-zone-untrust] quit
```

Step 2 Configure a Trust-Untrust interzone security policy and enable the session logging function. This function takes effect only when the policy action is set to **permit**.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name trust_untrust
[DeviceA-policy-security-rule-trust_untrust] source-zone trust
[DeviceA-policy-security-rule-trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-trust_untrust] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-trust_untrust] action permit
[DeviceA-policy-security-rule-trust_untrust] session logging
[DeviceA-policy-security-rule-trust_untrust] quit
[DeviceA-policy-security] quit
```

NOTE

Session log packets are not subject to security policies. Therefore, you do not need to configure a security policy for session logs. Instead, you need to configure only the preceding security policies.

Step 3 Configure a NAT policy.

Configure NAT address pool 1 and set the mode to PAT. In this example, the public address ranges from 1.1.1.10 to 1.1.1.15.

```
[DeviceA] nat address-group add1
[DeviceA-address-group-add1] mode pat
[DeviceA-address-group-add1] section 0 1.1.1.10 1.1.1.15
[DeviceA-address-group-add1] route enable
[DeviceA-address-group-add1] quit
```

Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] source-zone trust
[DeviceA-policy-nat-rule-policy1] destination-zone untrust
[DeviceA-policy-nat-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-nat-rule-policy1] action source-nat address-group add1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure a default route. In this example, the next hop of DeviceA to the Internet is 1.1.1.2.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

Step 5 Configure the log server.

```
[DeviceA] firewall log host 1 172.16.0.2 9996
```

Step 6 Set the source IP address and port for the device to send session logs.

```
[DeviceA] firewall log source 172.16.0.1 6666
```

Step 7 Set the session log output format to NetFlow.

```
[DeviceA] firewall log session log-type netflow
```

Step 8 Customize the output format of NetFlow session logs.

1. Configure a template for NetFlow session logs and access the template view.
   ```
   [DeviceA] session-log template name1 type netflow
   ```
2. Customize IPv4 NetFlow session logs.
   ```
   [DeviceA-netflow-template-name1] template id 655 ipv4 content protocol source-ip source-port source-nat-ip source-nat-port
   ```
   To customize IPv6 NAT64 NetFlow session logs, run the following command:
   ```
   [DeviceA-netflow-template-name1] template id 656 ipv6 content protocol source-ip source-port source-nat-ip source-nat-port
   ```
   By default, NetFlow session logs contain the log header, template, and flow information. To configure a NetFlow session log that does not contain template data, run the following command:
   ```
   [DeviceA-netflow-template-name1] template exclude
   [DeviceA-netflow-template-name1] quit
   ```
   NOTE

   After this command is run, the NetFlow session log does not contain template data. Whether the template data is required shall be negotiated with the third-party log server.
3. Set the NetFlow session log content format to the template format.
   ```
   [DeviceA] firewall log session log-type netflow template name1
   ```

Step 9 Configure a third-party log server.

----End

Verifying the Configuration

Logs can be viewed on the third-party log server.

Configuration Scripts

The following script uses the IPv4 NetFlow session log as an example.

```
#
sysname DeviceA
#
firewall log source 172.16.0.1 6666
firewall log host 1 172.16.0.2 9996
firewall log session log-type netflow template name1
#
nat address-group add1 0
 mode pat
 route enable
 section 0 1.1.1.10 1.1.1.15
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
interface GE0/0/1
 ip address 192.168.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
firewall zone untrust
 set priority 5
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  session logging
  action permit
#
nat-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  action source-nat address-group add1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
session-log template name1 type netflow
template id 655 ipv4 content protocol source-ip source-port source-nat-ip source-nat-port
#
return
```

20.11 CLI: Example for Sending Service Logs to a Third-Party Log Host

Networking Requirements

As shown in **Figure 20-11**, DeviceA connects to four third-party log servers.

DeviceA is required to send service logs to the third-party log servers to meet the following requirements:

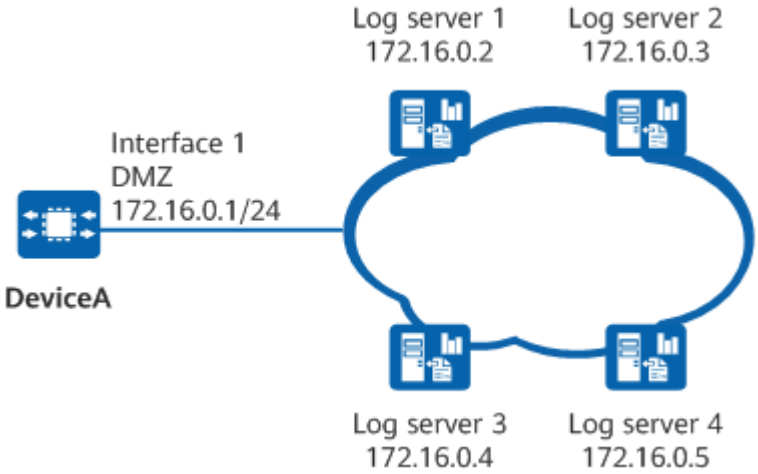
- DeviceA sends all logs that are generated by the POLICY module with the severity being Informational to log server 1. Log server 3 functions as the backup of log server 1.
- DeviceA sends all service logs to log server 2. Log server 4 functions as the backup of log server 2.

 Copyright © Huawei Technologies Co., Ltd.

Figure 20-11 Networking for sending service logs to log servers

NOTE

In this example, interface 1 represents GE0/0/2.



Configuration Roadmap

NOTE

This example provides only the DeviceA configuration. For the third-party log server configuration, see the third-party log server product document.

The system time must be set correctly during the initial configuration. Changing the system time during device running will result in incorrect timestamps in historical logs. The time zone of the log server must be the same as that of DeviceA.

1. Set the IP addresses for interfaces and add the interfaces to security zones.
2. Configure a security policy.
3. Enable the information center.
4. Name the information channel.
5. Specify the modules from which logs are output.
6. Configure log servers.

Procedure

Step 1 Set the IP addresses for interfaces and add the interfaces to security zones.

Configure an IP address for GE0/0/2.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 172.16.0.1 24
[DeviceA-GE0/0/2] quit
```

Add GE0/0/2 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure a Local-DMZ interzone security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name local_dmz
[DeviceA-policy-security-rule-local_dmz] source-zone local
[DeviceA-policy-security-rule-local_dmz] destination-zone dmz
[DeviceA-policy-security-rule-local_dmz] destination-address 172.16.0.2 32
[DeviceA-policy-security-rule-local_dmz] destination-address 172.16.0.3 32
[DeviceA-policy-security-rule-local_dmz] destination-address 172.16.0.4 32
[DeviceA-policy-security-rule-local_dmz] destination-address 172.16.0.5 32
[DeviceA-policy-security-rule-local_dmz] action permit
[DeviceA-policy-security-rule-local_dmz] quit
[DeviceA-policy-security] quit
```

Step 3 Enable the information center.

```
[DeviceA] info-center enable
```

Step 4 Name the information channel.

```
[DeviceA] info-center channel 6 name loghost1
```

Step 5 Specify the modules from which logs are output.

```
[DeviceA] info-center source policy channel loghost log level informational
```

NOTE

- By default, the device sends logs of level 6 or lower (level 0 to level 6). If the logs are of a higher level, you need to adjust the log level by setting the **level** *severitylog* parameter, so that the logs can be sent.
- Before configuring output rules for modules using the **info-center source Policy channel loghost log level Informational** command, run the **display info-center channel loghost** command to view information about the current channel. Then run the **undo info-center source** command to delete information about unnecessary modules from the information channel.

Step 6 Configure log servers.

Configure log server 1 as the master log server and log server 3 as the backup log server to receive logs generated by the POLICY module and NAT module. Use log recording tool **Local2**.

```
[DeviceA] info-center loghost 172.16.0.2 channel loghost facility local2
[DeviceA] info-center loghost 172.16.0.4 channel loghost facility local2
```

Configure log server 2 as the master log server and log server 4 as the backup log server. Use log recording tool **Local4**.

```
[DeviceA] info-center loghost 172.16.0.3 channel loghost1 facility local4
[DeviceA] info-center loghost 172.16.0.5 channel loghost1 facility local4
```

Step 7 Enable the function of sending service logs in syslog format. This step is optional. By default, service logs in syslog format are sent.

```
[DeviceA] firewall log service log-type syslog
```

Step 8 Enable the service functions of each module.

For details about how to configure intrusion prevention, attack event, and antivirus, see the configuration description of each service module.

Step 9 Configure a third-party log server.

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

Logs can be viewed on the third-party log server.

Configuration Scripts

```
#
sysname DeviceA
#
info-center channel 6 name loghost1
info-center source policy channel 2
info-center loghost 172.16.0.2 facility local2
info-center loghost 172.16.0.4 facility local2
info-center loghost 172.16.0.3 channel 6 facility local4
info-center loghost 172.16.0.5 channel 6 facility local4
#
interface GE0/0/2
 ip address 172.16.0.1 255.255.255.0
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name local_dmz
  source-zone local
  destination-zone dmz
  destination-address 172.16.0.2 mask 255.255.255.255
  destination-address 172.16.0.3 mask 255.255.255.255
  destination-address 172.16.0.4 mask 255.255.255.255
  destination-address 172.16.0.5 mask 255.255.255.255
  action permit
#
return
```

20.12 CLI: Example for Outputting Packet Loss Logs to a Third-Party Log Host

Networking Requirements

As shown in **Figure 20-12**, DeviceA is deployed on the network border. The network environment is as follows:

- The intranet is the Trust zone, while the Internet is the Untrust zone. Users on the intranet access the Internet using the NAT function provided by DeviceA.
- The DMZ has two third-party log servers.

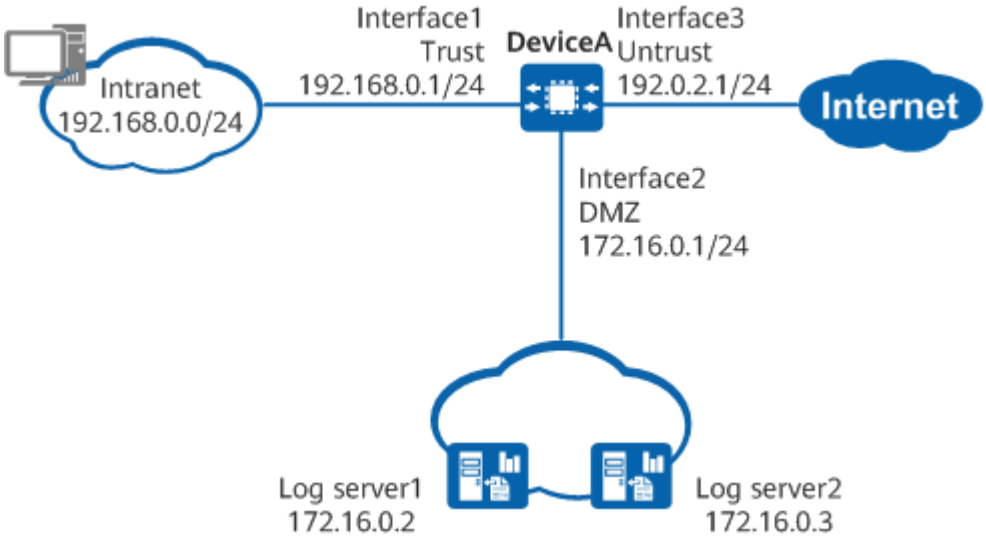
DeviceA is required to send packet loss information as syslogs to the third-party servers. The administrator can view and analyze packet loss information on the third-party servers. The log concurrent function is required, so that each log can be sent to both third-party servers.

Figure 20-12 Networking for sending packet discard logs to third-party log hosts

NOTE

In this example, interfaces 1, 2, and 3 represent GE0/0/1, GE0/0/2, and GE0/0/3, respectively.

 Copyright © Huawei Technologies Co., Ltd.



Configuration Roadmap

NOTE

This example provides only the DeviceA configuration. For the third-party log server configuration, see the third-party log server product document.

The system time must be set correctly during the initial configuration. Changing the system time during device running will result in incorrect timestamps in historical logs. The time zone of the log server must be the same as that of DeviceA.

1. Set the IP addresses for interfaces and add the interfaces to security zones.
2. Configure security policies.
3. Configure a NAT policy.
4. Configure routes.
5. Set the format of packet discard logs to syslog.
6. Configure the log hosts.
7. Enable the function of sending packet discard logs.
8. Enable the log concurrent function and configure the source IP address and source port.

Procedure

Step 1 Set the IP addresses for interfaces and add the interfaces to security zones.

Configure an IP address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface ge 0/0/1
[DeviceA-GE0/0/1] undo portswitch
[DeviceA-GE0/0/1] ip address 192.168.0.1 24
[DeviceA-GE0/0/1] quit
```

Configure an IP address for GE0/0/2.

```
[DeviceA] interface ge 0/0/2
[DeviceA-GE0/0/2] undo portswitch
[DeviceA-GE0/0/2] ip address 172.16.0.1 24
[DeviceA-GE0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Configure an IP address for GE 0/0/3.

```
[DeviceA] interface ge 0/0/3
[DeviceA-GE0/0/3] undo portswitch
[DeviceA-GE0/0/3] ip address 192.0.2.1 24
[DeviceA-GE0/0/3] quit
```

Add GE0/0/1 to the Trust zone.

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface ge 0/0/1
[DeviceA-zone-trust] quit
```

Add GE0/0/2 to the DMZ.

```
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface ge 0/0/2
[DeviceA-zone-dmz] quit
```

Add GE0/0/3 to the Untrust zone.

```
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface ge 0/0/3
[DeviceA-zone-untrust] quit
```

Step 2 Configure a Trust-Untrust interzone security policy.

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name trust_untrust
[DeviceA-policy-security-rule-trust_untrust] source-zone trust
[DeviceA-policy-security-rule-trust_untrust] destination-zone untrust
[DeviceA-policy-security-rule-trust_untrust] source-address 192.168.0.0 24
[DeviceA-policy-security-rule-trust_untrust] action permit
[DeviceA-policy-security-rule-trust_untrust] quit
[DeviceA-policy-security] quit
```

Step 3 Configure a NAT policy.

Configure NAT address pool 1 and set the mode to PAT. In this example, the public IP address ranges from 192.0.2.10 to 192.0.2.15.

```
[DeviceA] nat address-group add1
[DeviceA-address-group-add1] mode pat
[DeviceA-address-group-add1] section 0 192.0.2.10 192.0.2.15
[DeviceA-address-group-add1] route enable
[DeviceA-address-group-add1] quit
```

Configure a NAT policy.

```
[DeviceA] nat-policy
[DeviceA-policy-nat] rule name policy1
[DeviceA-policy-nat-rule-policy1] source-zone trust
[DeviceA-policy-nat-rule-policy1] destination-zone untrust
[DeviceA-policy-nat-rule-policy1] source-address 192.168.0.0 24
[DeviceA-policy-nat-rule-policy1] action source-nat address-group add1
[DeviceA-policy-nat-rule-policy1] quit
[DeviceA-policy-nat] quit
```

Step 4 Configure a default route. In this example, the next-hop IP address of the device connected to the Internet is 192.0.2.2.

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 192.0.2.2
```

Step 5 Set the format of packet discard logs to syslog.

```
[DeviceA] firewall log session log-type syslog
```

Step 6 Configure the log hosts.

```
[DeviceA] firewall log host 1 172.16.0.2 514
[DeviceA] firewall log host 2 172.16.0.3 514
```

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Enable the function of sending packet discard logs.

```
[DeviceA] firewall log packet-discard enable
[DeviceA] firewall log packet-discard default-packet-filter
[DeviceA] firewall log packet-discard packet-filter
[DeviceA] firewall log packet-discard session-miss
[DeviceA] firewall log packet-discard others
```

NOTE

- If **session-miss** is specified, the device sends a log when a packet does not match any session entry.
- If **packet-filter** is specified, the device sends a log when a packet is discarded because it matches a security policy.
- If **default-packet-filter** is specified, the device sends a log when a packet is discarded because it matches the default security policy.
- If **others** is specified, the device sends a log when a packet is discarded due to other factors.

  IPv6 packet discard logs do not support the **others** parameter.

Step 8 Enable the log concurrent function and configure the source IP address and source port.

```
[DeviceA] firewall log session multi-host-mode concurrent
[DeviceA] firewall log source 172.16.0.1 6000
```

Step 9 Configure a third-party log host and view logs on it.

----End

Verifying the Configuration

Logs can be viewed on the third-party log host.

Configuration Scripts

```
#
sysname DeviceA
#
firewall log source 172.16.0.1 6000
firewall log host 1 172.16.0.2 514
firewall log host 2 172.16.0.3 514
firewall log session multi-host-mode concurrent
firewall log session log-type syslog
firewall log packet-discard enable
firewall log packet-discard packet-filter
firewall log packet-discard default-packet-filter
#
nat address-group add1 0
 mode pat
 route enable
 section 0 192.0.2.1 192.0.2.2
#
interface GE0/0/1
 ip address 192.168.0.1 255.255.255.0
#
interface GE0/0/2
 ip address 172.16.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 192.0.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/1
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
firewall zone untrust
 set priority 5
 add interface GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface GE0/0/2
#
security-policy
 rule name trust_untrust
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address 192.168.0.0 mask 255.255.255.0
  action source-nat address-group add1
#
 ip route-static 0.0.0.0 0.0.0.0 203.0.113.2
#
return
```

20.13 CLI: Example for Sending IPv4 Session Logs to the SecoManager in Hot Standby Deployment of Loading Balancing Mode

Networking Requirements

On the network shown in **Figure 20-13**, the service interfaces of two devices work at Layer 3 and are directly connected to routers. The devices and directly connected routers run OSPF. The upstream interfaces are connected to the same ISP network.

The devices are required to work in load balancing mode. In normal cases, DeviceA forwards traffic from Dept.A, and DeviceB forwards traffic from Dept.B. If either device fails, the other device forwards all traffic to ensure service continuity.

The administrator wants to check IPv4 PAT session logs on the SecoManager to understand the creation of sessions by packets in a timely manner and, when necessary, perform NAT source tracing.

NOTE

In this load balancing networking, devices connect to routers in both upstream and downstream directions. On live networks, you must determine whether OSPF is required based on the upstream and downstream devices and interfaces. The source NAT configuration remains unchanged.

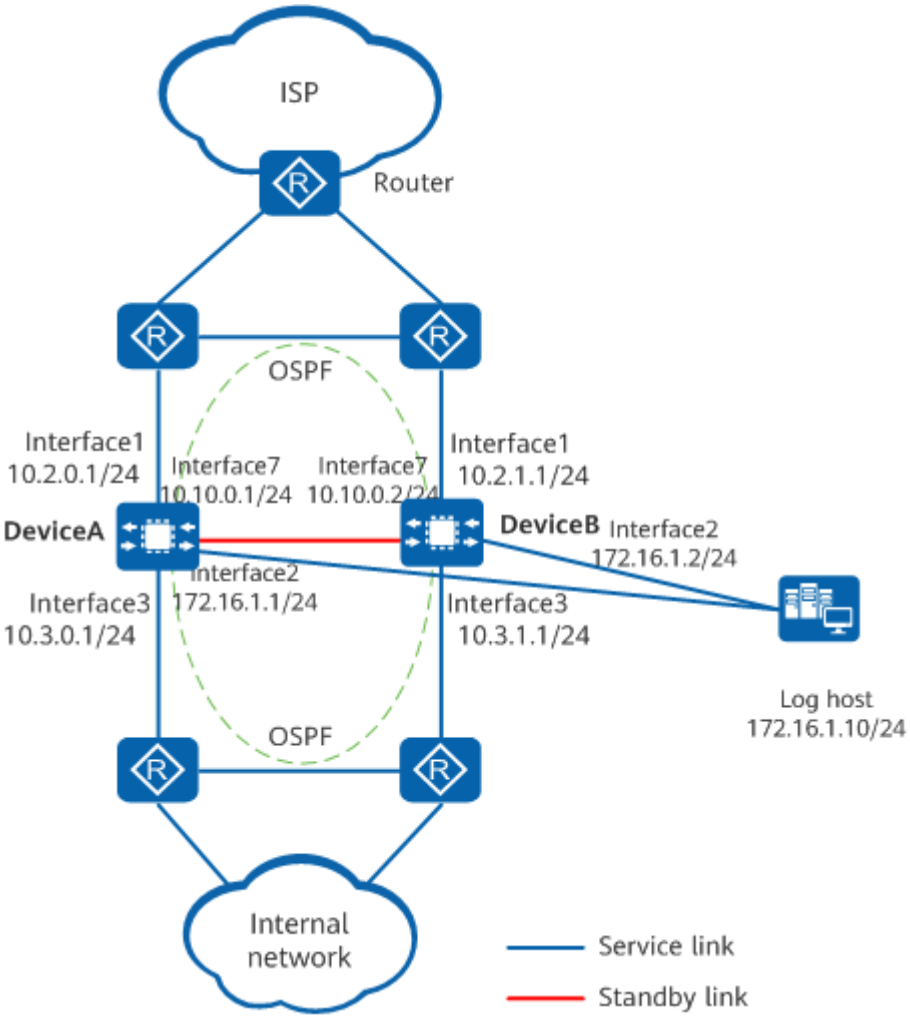
This example does not apply when upstream interfaces connect to different ISP networks.

 Copyright © Huawei Technologies Co., Ltd.

Figure 20-13 Network diagram for configuring source NAT in a load balancing scenario.

NOTE

In this example, interfaces 1, 2, 3, and 7 represent GE0/0/1, GE0/0/2, GE0/0/3, and GE0/0/7, respectively.



Item	DeviceA	DeviceB
Interface	GE0/0/1 IP address: 10.2.0.1/24 Security zone: Untrust GE0/0/3 IP address: 10.3.0.1/24 Security zone: Trust GE0/0/7 IP address: 10.10.0.1/24 Security zone: DMZ	GE0/0/1 IP address: 10.2.1.1/24 Security zone: Untrust GE0/0/3 IP address: 10.3.1.1/24 Security zone: Trust GE0/0/7 IP address: 10.10.0.2/24 Security zone: DMZ

Item	DeviceA	DeviceB
OSPF	Process ID: 10 Area ID: 0 Network segments for the area: 10.2.0.0/24, 10.3.0.0/24, and 1.1.1.10/32	Process ID: 10 Area ID: 0 Network segments for the area: 10.2.1.0/24, 10.3.1.0/24, and 1.1.1.10/32

Configuration Roadmap

1. Assign IP addresses to interfaces, add the interfaces to security zones, and configure network connectivity on DeviceA and DeviceB.
2. Configure OSPF on DeviceA and DeviceB.
3. Configure hot standby on DeviceA and DeviceB. To be specific, configure interface monitoring, specify heartbeat interfaces, and enable quick session backup.
4. Configure a security policy on DeviceA to allow OSPF packet exchange between devices and Internet access from the intranet. The security policy configured on DeviceA is automatically backed up to DeviceB.
5. Configure a NAT address pool on DeviceA. The NAT address pool configured on DeviceA is automatically backed up to DeviceB.
6. Configure a Source NAT policy on DeviceA to implement source address translation for Internet access from the intranet. The Source NAT policy configured on DeviceA is automatically backed up to DeviceB.
7. Configure the downstream devices, so that traffic from department A is forwarded through DeviceA, and traffic from department B is forwarded through DeviceB.
8. On the upstream router, configure an interface address and a static route destined for the ISP, and configure OSPF so that the device and router can learn routes from each other. On the downstream router, configure an interface address and configure OSPF so that the device and router can learn routes from each other. For detailed configurations, see the router product documentation. The configurations are omitted here.
9. Configure log hosts and enable log recording on the two devices.

Procedure

Step 1 Complete basic network configurations.

DeviceA	DeviceB
# Set IP addresses for the interfaces on DeviceA and DeviceB.	

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
<HUAWEI> **system-view** [HUAWEI] **sysname DeviceA** [DeviceA] **interface ge 0/0/1** [DeviceA-GE0/0/1] **undo portswitch** [DeviceA-GE0/0/1] **ip address 10.2.0.1 24** [DeviceA-GE0/0/1] **quit** [DeviceA] **interface ge 0/0/3** [DeviceA-GE0/0/3] **undo portswitch** [DeviceA-GE0/0/3] **ip address 10.3.0.1 24** [DeviceA-GE0/0/3] **quit** [DeviceA] **interface ge 0/0/7** [DeviceA-GE0/0/7] **undo portswitch** [DeviceA-GE0/0/7] **ip address 10.10.0.1 24** [DeviceA-GE0/0/7] **quit**	<HUAWEI> **system-view** [HUAWEI] **sysname DeviceB** [DeviceB] **interface ge 0/0/1** [DeviceB-GE0/0/1] **ip address 10.2.1.1 24** [DeviceB-GE0/0/1] **quit** [DeviceB] **interface ge 0/0/3** [DeviceB-GE0/0/3] **ip address 10.3.1.1 24** [DeviceB-GE0/0/3] **quit** [DeviceB] **interface ge 0/0/7** [DeviceB-GE0/0/7] **ip address 10.10.0.2 24** [DeviceB-GE0/0/7] **quit**
# Assign the interfaces to security zones on DeviceA and DeviceB.	
[DeviceA] **firewall zone untrust** [DeviceA-zone-untrust] **add interface ge 0/0/1** [DeviceA-zone-untrust] **quit** [DeviceA] **firewall zone trust** [DeviceA-zone-trust] **add interface ge 0/0/3** [DeviceA-zone-trust] **quit** [DeviceA] **firewall zone dmz** [DeviceA-zone-dmz] **add interface ge 0/0/7** [DeviceA-zone-dmz] **quit**	[DeviceB] **firewall zone untrust** [DeviceB-zone-untrust] **add interface ge 0/0/1** [DeviceB-zone-untrust] **quit** [DeviceB] **firewall zone trust** [DeviceB-zone-trust] **add interface ge 0/0/3** [DeviceB-zone-trust] **quit** [DeviceB] **firewall zone dmz** [DeviceB-zone-dmz] **add interface ge 0/0/7** [DeviceB-zone-dmz] **quit**
# Configure OSPF to ensure IP connectivity on DeviceA and DeviceB.	
[DeviceA] **ospf 10** [DeviceA-ospf-10] **area 0** [DeviceA-ospf-10-area-0.0.0.0] **network 10.2.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **network 10.3.0.0 0.0.0.255** [DeviceA-ospf-10-area-0.0.0.0] **quit** [DeviceA-ospf-10] **quit**	[DeviceB] **ospf 10** [DeviceB-ospf-10] **area 0** [DeviceB-ospf-10-area-0.0.0.0] **network 10.2.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **network 10.3.1.0 0.0.0.255** [DeviceB-ospf-10-area-0.0.0.0] **quit** [DeviceB-ospf-10] **quit**

Step 2 Allow HRP packets to be exchanged between heartbeat interfaces.

NOTE

Controlling function of security policies for HRP packets are configured using the **firewall packet-filter basic-protocol enable** command. By default, the function of the **firewall packet-filter basic-protocol enable** command is enabled. That is, HRP packets are controlled by security policies. In this case, a security policy must be configured between the security zone where the heartbeat interface resides and the local zone to allow HRP packets to pass. In this example, enabling the function of the **firewall packet-filter basic-protocol enable** command is used as an example.

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
[DeviceA] **security-policy** [DeviceA-policy-security] **rule name ha_local_to_dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceA-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceA-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceA-policy-security-rule-ha_local_to_dmz] **quit** [DeviceA-policy-security] **quit**	[DeviceB] **security-policy** [DeviceB-policy-security] **rule name ha_local_to_dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **source-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **destination-zone local dmz** [DeviceB-policy-security-rule-ha_local_to_dmz] **service protocol udp destination-port 18514** [DeviceB-policy-security-rule-ha_local_to_dmz] **action permit** [DeviceB-policy-security-rule-ha_local_to_dmz] **quit** [DeviceB-policy-security] **quit**

Step 3 Configure hot standby.

DeviceA	DeviceB
# Monitor upstream and downstream service interfaces on DeviceA and DeviceB.	
[DeviceA] **hrp track interface ge 0/0/1** [DeviceA] **hrp track interface ge 0/0/3**	[DeviceB] **hrp track interface ge 0/0/1** [DeviceB] **hrp track interface ge 0/0/3**
# Configure quick session backup on DeviceA and DeviceB in case of inconsistent forward and return packet paths.	
[DeviceA] **hrp mirror session enable**	[DeviceB] **hrp mirror session enable**
# Specify the heartbeat interface, configure the authentication key, and enable hot standby on DeviceA and DeviceB.	
[DeviceA] **hrp interface ge 0/0/7 remote 10.10.0.2** [DeviceA] **hrp authentication-key YsHsjx_202206@123** [DeviceA] **hrp enable**	[DeviceB] **hrp interface ge 0/0/7 remote 10.10.0.1** [DeviceB] **hrp authentication-key YsHsjx_202206@123** [DeviceB] **hrp enable**

Step 4 Configure NAT address pool port allocation in the load balancing scenario.

NOTE

In the hot standby load balancing scenario, If NAPT is configured, the devices may have conflicting public ports. To prevent such conflicts, configure respective NAT resources (including public IP addresses and ports) for the devices. You can run the **hrp nat resource primary-group** command on the active device. The standby device will automatically generate the **hrp nat resource secondary-group** command (if you run the **hrp nat resource secondary-group** command on the active device, the standby device will automatically generate the **hrp nat resource primary-group** command).

HRP_S[DeviceA] **hrp nat resource primary-group**

Step 5 Configure a security policy on DeviceA to allow OSPF packet exchange between devices and Internet access from the intranet.

The security policy configured on DeviceA is automatically backed up to DeviceB.

HRP_M[DeviceA] **security-policy**
HRP_M[DeviceA-policy-security] **rule name policy_sec_1**

 Copyright © Huawei Technologies Co., Ltd.

```
HRP_M[DeviceA-policy-security-rule-policy_sec_1] source-zone local trust untrust
HRP_M[DeviceA-policy-security-rule-policy_sec_1] destination-zone local trust untrust
HRP_M[DeviceA-policy-security-rule-policy_sec_1] action permit
HRP_M[DeviceA-policy-security-rule-policy_sec_1] quit
HRP_M[DeviceA-policy-security] quit
```

Step 6 Configure a NAT address pool and permit port conversion to reuse public network addresses.

The NAT address pool configured on DeviceA is automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat address-group addressgroup1
HRP_M[DeviceA-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15
HRP_M[DeviceA-address-group-addressgroup1] mode pat
HRP_M[DeviceA-address-group-addressgroup1] route enable
HRP_M[DeviceA-address-group-addressgroup1] quit
```

Step 7 Configure a NAT policy to allow intranet users to access the Internet by using post-NAT public IP addresses.

The NAT policy configured on DeviceA is automatically backed up to DeviceB.

```
HRP_M[DeviceA] nat-policy
HRP_M[DeviceA-policy-nat] rule name policy_nat_1
HRP_M[DeviceA-policy-nat-policy_nat_1] source-zone trust
HRP_M[DeviceA-policy-nat-policy_nat_1] destination-zone untrust
HRP_M[DeviceA-policy-nat-policy_nat_1] action source-nat address-group addressgroup1
HRP_M[DeviceA-policy-nat-policy_nat_1] quit
HRP_M[DeviceA-policy-nat] quit
```

Step 8 Configure the downstream devices, so that traffic from department A is forwarded through DeviceA, and traffic from department B is forwarded through DeviceB.

Step 9 On the upstream router, configure an interface address and a static route destined for the ISP, and configure OSPF so that the device and router can learn routes from each other. On the downstream router, configure an interface address and configure OSPF so that the device and router can learn routes from each other. For detailed configurations, see the router product documentation. The configurations are omitted here.

Step 10 Configure a log host on DeviceA.

```
HRP_M[DeviceA] firewall log host 1 172.16.1.10 9002
```

Step 11 Configure the source IP address and port used by the device to send session logs on DeviceA.

```
HRP_M[DeviceA] firewall log source 172.16.1.1 6666
```

Step 12 Configure the source IP address and port used by the device to send session logs on DeviceB.

```
HRP_S[DeviceB] firewall log source 172.16.1.2 6666
```

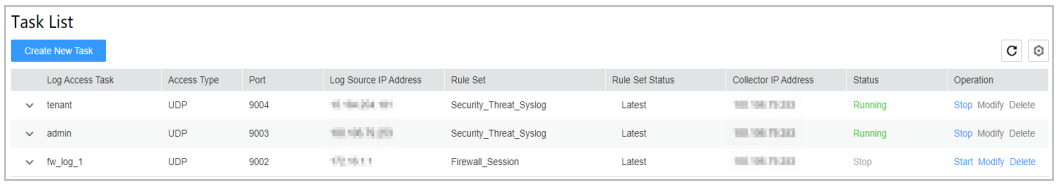
Step 13 Enable the session logging function in the security policy for service traffic on DeviceA.

```
HRP_M[DeviceA] security-policy
HRP_M[DeviceA-policy-security] rule name policy_sec_1
HRP_M[DeviceA-policy-security-rule-policy_sec_1] session logging
HRP_M[DeviceA-policy-security-rule-policy_sec_1] quit
HRP_M[DeviceA-policy-security] quit
```

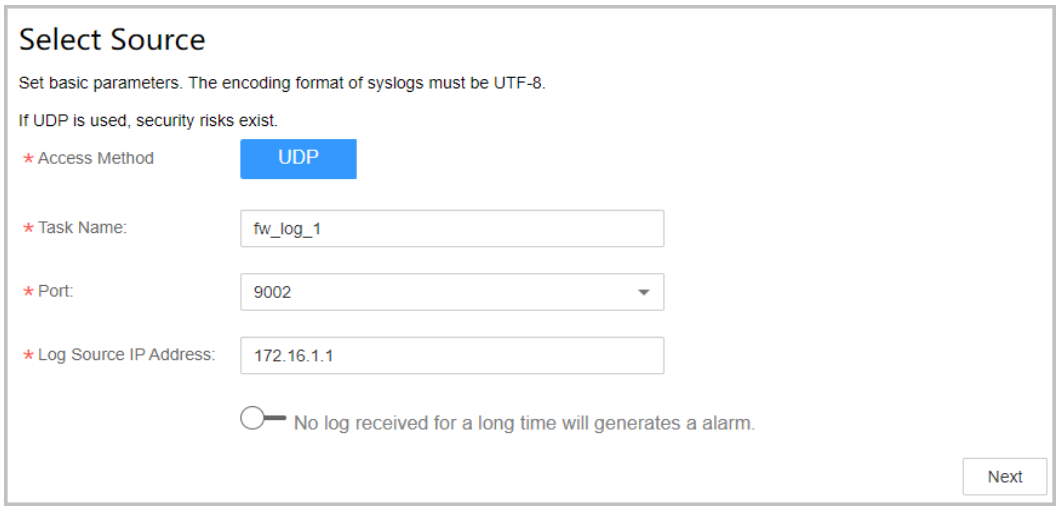
Step 14 Configure the SecoManager.

1. Open the **Device Log Management** app, choose **Log Access** > **Log Access Management**, and click **Create New Task**.

 Copyright © Huawei Technologies Co., Ltd.



2. Set basic task parameters, add DeviceA to the log source, and click **Next**.

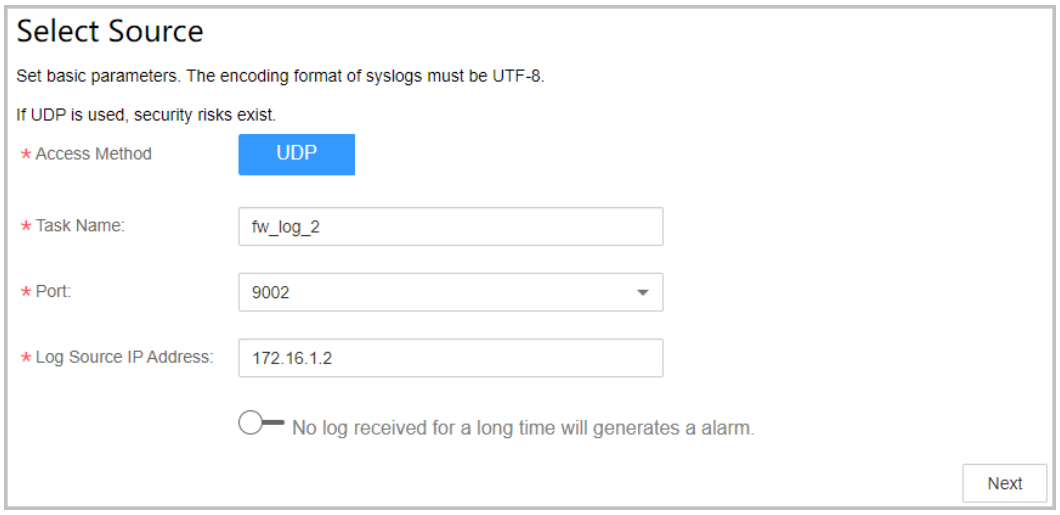


3. Configure a rule set, select a collector, and click **Next**.



4. Verify that the configurations are correct and click **Commit**.
5. Repeat the preceding steps to add DeviceB to the log source.

 Copyright © Huawei Technologies Co., Ltd.



----End

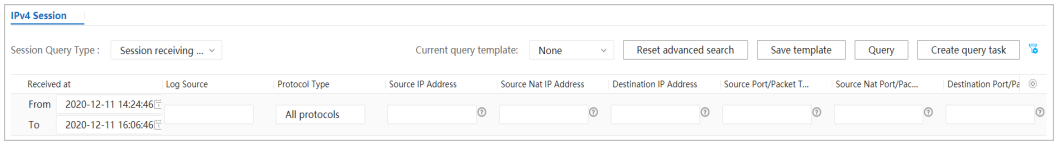
Verifying the Configuration

After the configurations are complete, when users on internal networks access external networks, corresponding sessions are generated on the device. After the sessions age, the device sends the session logs to the SecoManager. Then you can view the IPv4 session logs on the SecoManager.

1. Open the **Device Log Management** app, choose **Session Analysis** > **IPv4 Session Log**, and click the **IPv4 Session** tab.
2. Click in the upper right corner of the list and set query parameters.

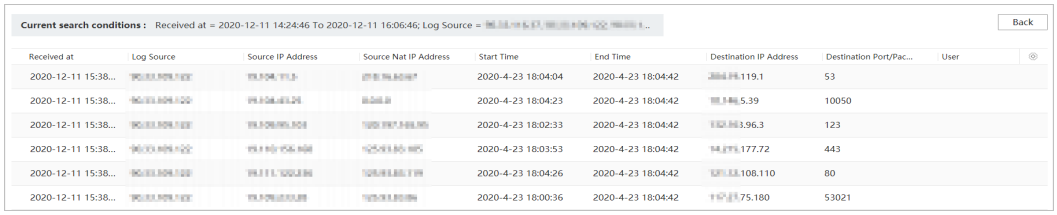
   NOTE

   To view session creation logs, select **The duration of the session should have intersection with the query time range** from the **Session Query Type** drop-down list box.



3. Click **Query**.

   The query results are displayed, as shown in the following figure. The log information here is for reference only. Log information varies depending on actual network environments.



   By checking the log information above, the administrator can know about the creation of sessions by packets in time. The administrator can also learn the information (such as the IP address) before NAT is performed on packets and perform, when necessary, the NAT source tracing.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Scripts

DeviceA

```
#
sysname DeviceA
#
firewall log source 172.16.1.1 6666
firewall log host 1 172.16.1.10 9002
#
hrp enable
hrp mirror session enable
hrp interface GE0/0/7 remote 10.10.0.2
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
J6+;U#>V\!_e1NY[iGLXjT
%k=rKkg,Z)CI0!!!!!!!!!!!!!!!:!!!!
Ec&0;Y9kF~"+*IM>Io(Sm{&9' 5y$6'L:2@-!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
nat address-group addressgroup1 0
mode pat
route enable
section 0 1.1.1.10 1.1.1.15
#
security-policy
 rule name policy_sec_1
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  session logging
  action permit
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
```

DeviceB

```
#
sysname DeviceB
#
firewall log source 172.16.1.2 6666
firewall log host 1 172.16.1.10 9002
#
hrp enable
hrp mirror session enable
hrp interface GE0/0/7 remote 10.10.0.1
hrp track interface GE0/0/1
hrp track interface GE0/0/3
hrp authentication-key %+%##!!!!!!!!!!"!!!!"!!!!*!!!!
\FR0@B|5m51t2(SLB$(Yzq_KUB|
V43Td3,.!!!!!!!!!!!!!!!:!!!!>$P4S-0S{KqT>VWoG2!K9t\i4
t;1e+vR$$U!!!!!%+%#
#
interface GE0/0/1
 ip address 10.2.1.1 255.255.255.0
#
interface GE0/0/3
 ip address 10.3.1.1 255.255.255.0
#
interface GE0/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GE0/0/3
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface GE0/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.1.0.0.0.255
  network 10.3.1.0 0.0.0.255
#
nat address-group addressgroup1 0
mode pat
route enable
section 0 1.1.1.10 1.1.1.15
#
security-policy
 rule name policy_sec_1
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  session logging
  action permit
 rule name ha_local_to_dmz
  source-zone local
  source-zone dmz
  destination-zone local
  destination-zone dmz
  service protocol udp destination-port 18514
  action permit
```

 Copyright © Huawei Technologies Co., Ltd.

DeviceA	DeviceB
# nat-policy rule name policy_nat_1 source-zone trust destination-zone untrust action source-nat address-group addressgroup1 # return	# nat-policy rule name policy_nat_1 source-zone trust destination-zone untrust action source-nat address-group addressgroup1 # return

 Copyright © Huawei Technologies Co., Ltd.