DO NOT REPRINT
© FORTINET

Visit on Brave-Dumps.com

FORTINET CERTIFIED SOLUTION SPECIALIST Network Security

FORTINET CERTIFIED SOLUTION SPECIALIST Secure Access Service Edge

SD-WAN Architect

Lab Guide

FortiOS 7.4

FORTINET Training Institute

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET

11/20/2024

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

TABLE OF CONTENTS

Network Topology 6
Lab 1: Basic DIA Setup 7
Exercise 1: Configuring a Basic DIA Setup 8
Configure a Zone and Members for DIA 8
Configure a Performance SLA 10
Configure Rules 14
Configure a Static Route and Firewall Policy 19
Exercise 2: Monitoring DIA Traffic 24
Generate Internet Traffic From branch1_client 24
Review SD-WAN Member Health and Routes 24
Monitor DIA Traffic Distribution 27
Bring Down port1 29
Monitor SD-WAN Events and Traffic Logs 29
Bring Up port1 32
Lab 2: Centralized Management 33
Exercise 1: Configuring SD-WAN on FortiManager 35
Add branch1_fgt and branch2_fgt to FortiManager 35
Import SD-WAN Settings Into the SD-WAN Template 38
Configure the SD-WAN Template 40
Review and Create Metadata Variables 45
Configure the Device Settings and Policy Package 49
Install the Device Settings and Policy Package 55
Verify Installed Settings and Logging 56
Exercise 2: Monitoring DIA Traffic on FortiManager 60
Generate Internet Traffic and Trigger an Interface Failure 60
Monitor DIA Traffic Distribution 60
View Traffic Logs 66
Exercise 3: Configuring the Overlay With the SD-WAN Overlay Template 68
Add dc1_fgt to FortiManager 69
Configure the Overlay Tunnels With the SD-WAN Overlay Template 70
Review, Adjust, and Install the Overlay Configuration 76
Monitor the Status of the Overlay Tunnels 83
Lab 3: Zero-Touch Provisioning of SD-WAN Branches 88

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Configuring Firewall Policies and SD-WAN Rules **89**
Configure Firewall Policies 89
Configure an SD-WAN Rule for the Overlays 93
Verify the Overlays as SD-WAN Members 94
Exercise 2: Onboarding a New Branch With ZTP **97**
Create Device Blueprints 97
Declare New Devices 100
Deploy New Branch Devices 113
Exercise 3: Monitoring SD-WAN With FortiManager **117**
Review the VPN Tunnel Status 117
Review the SD-WAN Status on the SD-WAN Monitor Page 119
Lab 4: Members, Zones, and Performance SLAs **127**
Exercise 1: Using Ping to Actively Monitor the Overlays **129**
Configure an Active Performance SLA (Ping) 129
Verify the Health of the Overlays 131
Exercise 2: Testing an Active Performance SLA **134**
Monitor a Performance SLA on the FortiGate CLI 134
Test the Performance SLA 135
Exercise 3: Monitoring SD-WAN With FortiAnalyzer **140**
Confirm Log Forwarding on the FortiGate Devices 140
Analyze Traffic Logs 141
Analyze Event Logs 146
Discover the Secure SD-WAN Monitor Page 148
Discover the SD-WAN Summary Page 149
Lab 5: Routing and Sessions **152**
Exercise 1: Testing the Behavior of a Policy Route **153**
Configure a Policy Route and Check the Impact on SD-WAN Rules 153
Exercise 2: Monitoring the Reevaluation of Sessions **162**
Monitor the Session Reevaluation When the Link Performance Degrades 162
Lab 6: Rules **173**
Exercise 1: Configuring and Testing Rule Strategies **174**
Configure and Test a Best Quality Rule 174
Configure and Test a Lowest Cost (SLA) Rule 180
Configure and Test a Lowest Cost (SLA) and Load Balancing Rule 185
Lab 7: SD-WAN Overlay Design and Best Practices **192**
Exercise 1: Reviewing the Overlay and BGP Configurations **193**
Review the Overlay Configuration 193
Review the BGP Configuration 202
Fine-Tune IPsec and BGP 212
Lab 8: SD-WAN Dual Hub Deployment **220**

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

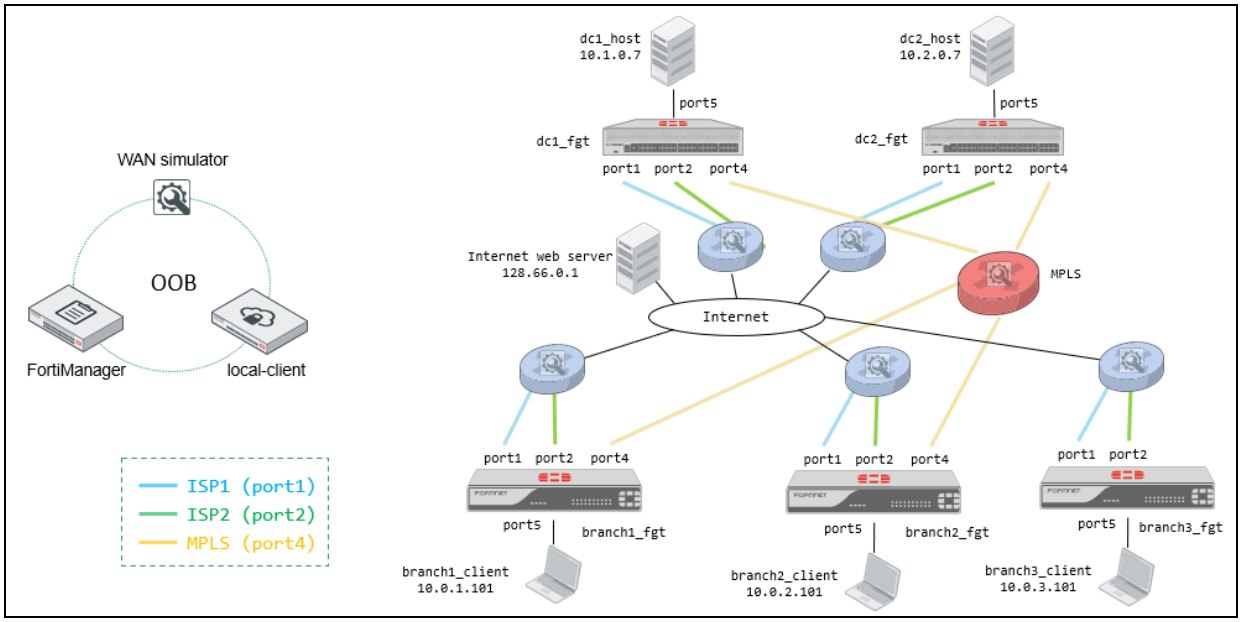
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Updating the SD-WAN Overlay Template for a Dual Hub Topology **222**
Add dc2_fgt to FortiManager 222
Update the SD-WAN Overlay Template for a Dual Hub Topology 223
Review, Adjust, and Install the Configurations 227
Review the Device Status and Topology 238
Exercise 2: Refining the Dual Hub Configuration **240**
Review the Configuration on the Branches 240
Lab 9: ADVPN **251**
Exercise 1: Configuring ADVPN **252**
Configure Basic ADVPN 252
Prevent Cross Overlay Shortcuts 254
Exercise 2: Monitoring ADVPN Tunnels **256**
Monitor ADVPN Tunnels 256
Check VPN Log Messages 266
Configure an Idle Timeout for ADVPN 268
Lab 10: SD-WAN Troubleshooting **272**
Exercise 1: Troubleshooting Spoke-to-Spoke Traffic (Single Hub) **275**
Configuration 275
Problem Description 275
Objective 276
Solution Requirements 276
Tips for Troubleshooting 276
Solution 278
Exercise 2: Troubleshooting DIA Traffic **279**
Configuration 280
Problem Description 280
Objective 281
Solution Requirements 281
Tips for Troubleshooting 281
Solution 283
Exercise 3: Troubleshooting Rules **284**
Configuration 285
Problem Description 285
Objective 286
Solution Requirements 286
Tips for Troubleshooting 286
Solution 288

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Network Topology



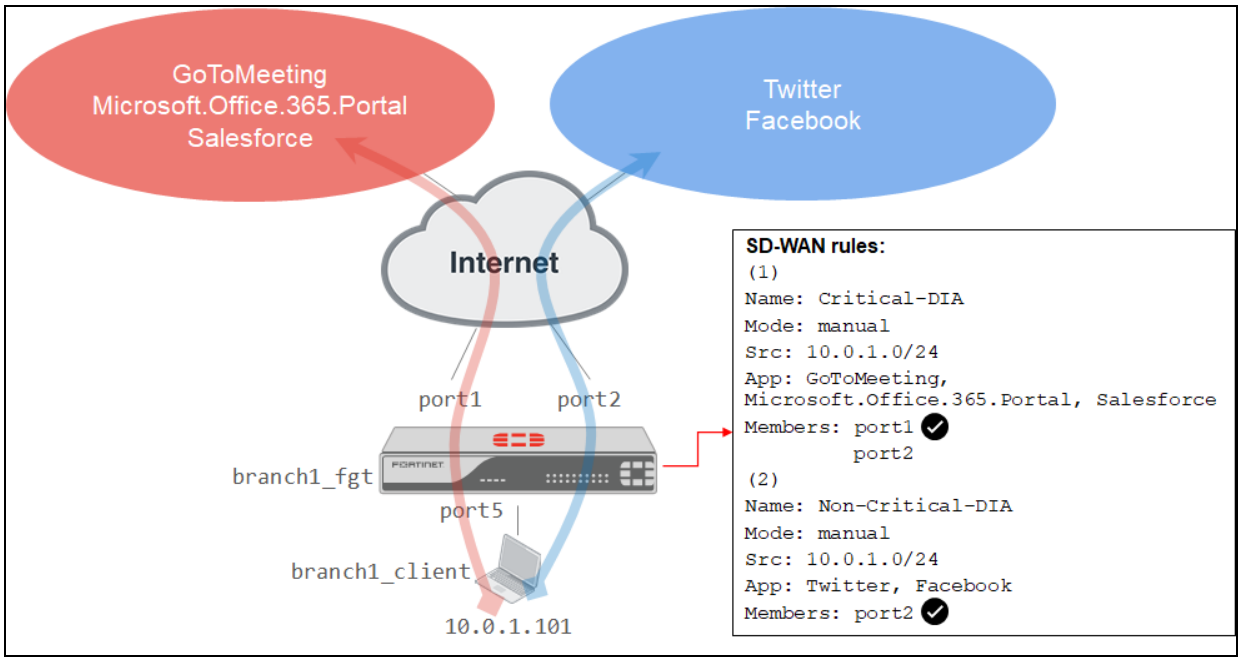
Device	port1	port2	port4	port5
branch1_fgt	192.2.0.1	192.2.0.9	172.16.0.1	10.0.1.254
branch2_fgt	203.0.113.1	203.0.113.9	172.16.0.9	10.0.2.254
branch3_fgt	100.64.33.1	100.64.33.9	—	10.0.3.1
dc1_fgt	100.64.1.1	100.64.1.9	172.16.1.5	10.1.0.1
dc2_fgt	100.64.1.3	100.64.1.11	172.16.1.1	10.2.0.1

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 1: Basic DIA Setup

In this lab, you will configure the following basic SD-WAN direct internet access (DIA) setup on branch1_fgt:



After that, you will generate internet traffic on branch1_client and monitor the traffic distribution and events on the FortiGate GUI.

Objectives

- Configure a basic SD-WAN DIA setup
- Configure route and firewall policies for SD-WAN
- Verify SD-WAN traffic distribution and events

Time to Complete

Estimated: 50 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Configuring a Basic DIA Setup

In this exercise, you will configure a basic DIA setup using the FortiGate GUI. You will create a zone for port1 and port2 on branch1_fgt, and then configure SD-WAN rules to steer traffic for critical and non-critical internet applications.

Configure a Zone and Members for DIA

You will configure the underlay zone, and then add port1 and port2 as members.

To create an SD-WAN zone

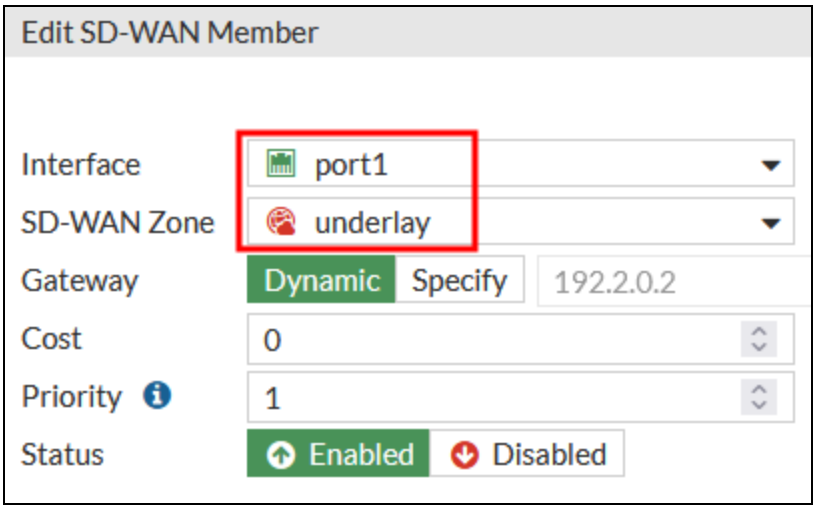
1. Access the branch1_fgt GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Network** > **SD-WAN**, and then click the **SD-WAN Zones** tab.
3. Click **Create New** > **SD-WAN Zone** to add an SD-WAN zone.
4. In the **Name** field, type `underlay`.

5. Click **OK** to save the settings.
6. Click **Create New** > **SD-WAN Member** to add an SD-WAN member, and then configure the following settings:

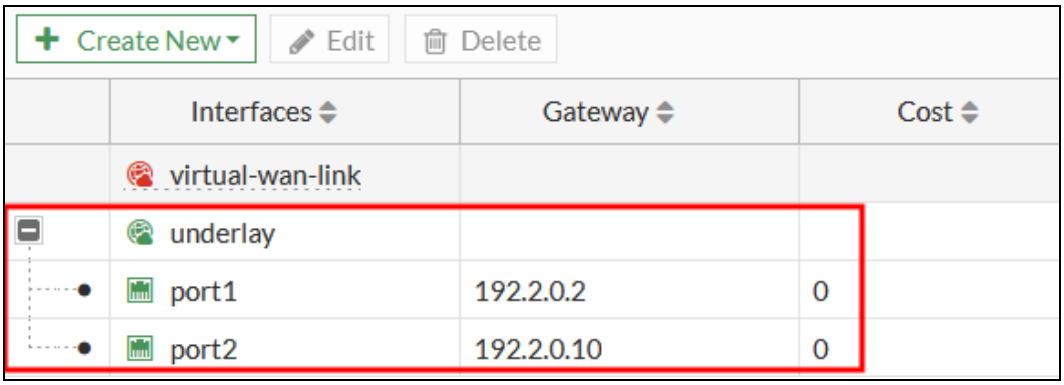
Field	Value
Interface	port1
SD-WAN Zone	underlay

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



7. Click **OK** to save the settings.
8. Repeat the previous steps to add port2 as an SD-WAN member and assign it to the same zone (**underlay**).
9. On the **SD-WAN Zones** tab, expand the **underlay** zone.
   Your page should look similar to the following example:



port1 and **port2** are members of the **underlay** zone.

Stop and think!

You didn't configure the gateway for each member. Yet, FortiGate is displaying them correctly. Why?

When you added port1 and port2 as SD-WAN members, you selected **Dynamic** for the **Gateway** setting. This instructs FortiGate to automatically retrieve the member gateway address. Because port1 and port2 are both configured as DHCP interfaces, FortiGate uses the gateway assigned over DHCP.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Configure a Performance SLA

You will configure a performance SLA for monitoring the health of port1 and port2 and review the routing table.

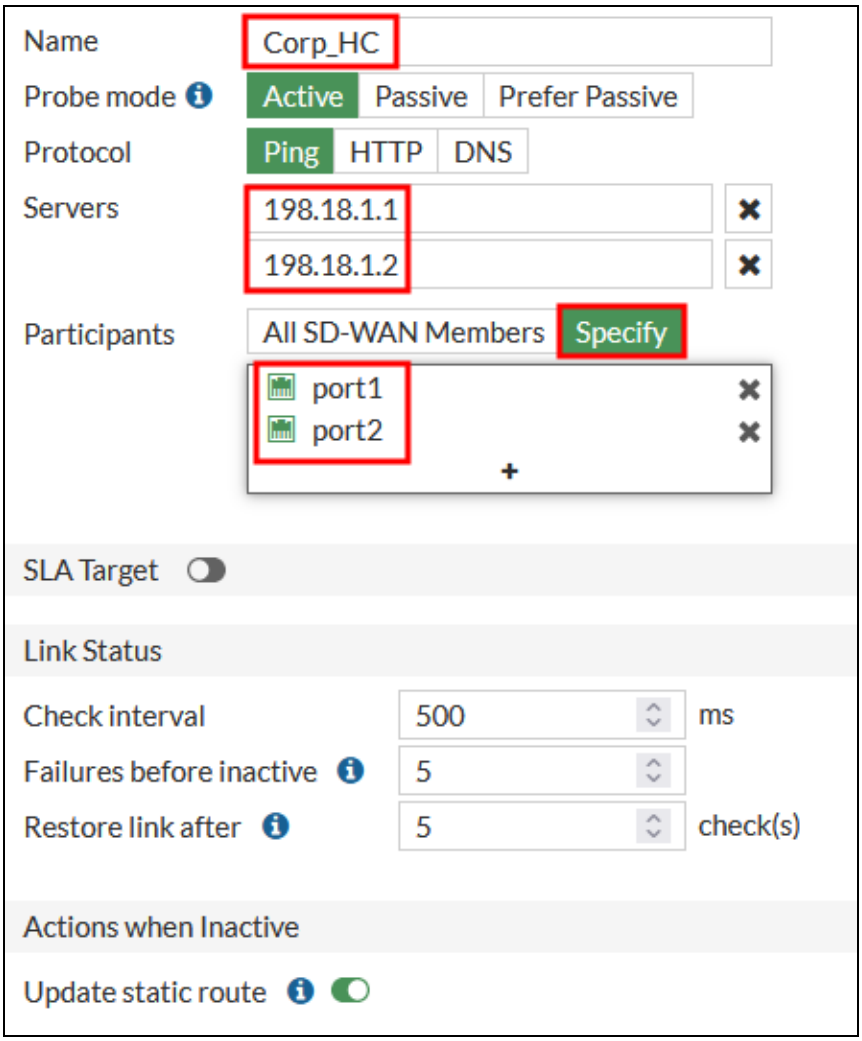
To configure a performance SLA

1. Continuing on the branch1_fgt GUI, click **Network** > **SD-WAN**, and then click the **Performance SLAs** tab.
2. Click **Create New** to add a performance SLA.
3. Configure the following settings:

Field	Value
Name	Corp_HC
Servers	`198.18.1.1` Click **+**, and then type `198.18.1.2`.
Participants	Select **Specify**, and then select **port1** and **port2**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



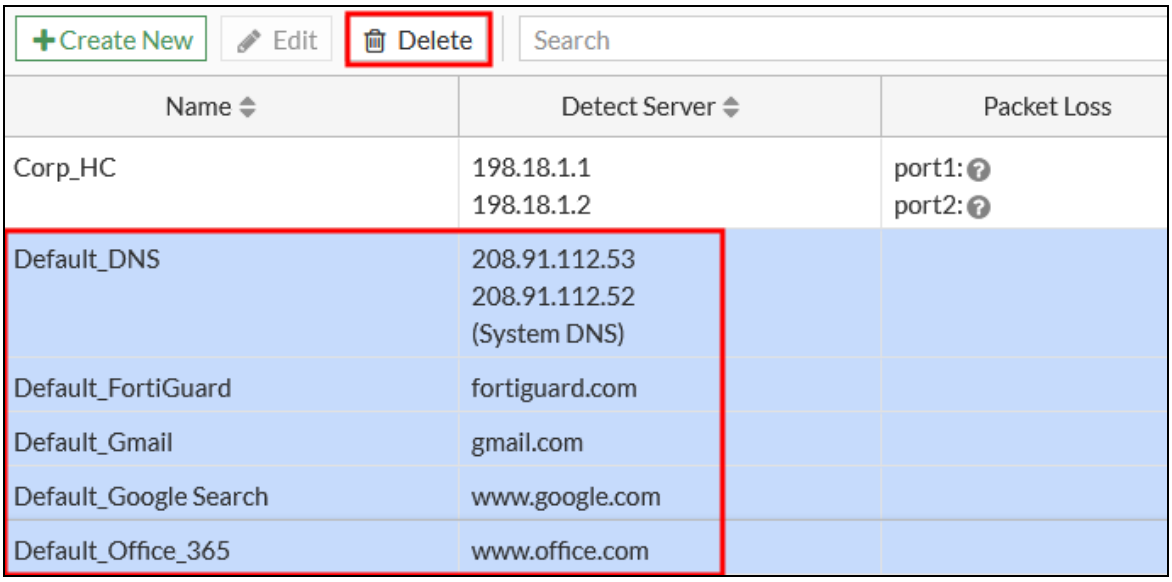
4. Click **OK** to save the settings.
5. Click **Network** > **SD-WAN**, and then click the **Performance SLAs** tab to refresh the page.
   The page should show that port1 and port2 are alive (green up arrow).

Name	Detect Server	Packet Loss	Latency	Jitter
Corp_HC	198.18.1.1 198.18.1.2	port1: 0.00% port2: 0.00%	port1: 0.68ms port2: 0.57ms	port1: 0.08ms port2: 0.06ms

6. Press `Shift`, select all lines that reference preconfigured default SLA targets, and then click **Delete**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



By default, FortiGate has some predefined performance SLAs that you can select and adjust according to your requirements.

In these lab exercises, you will use only manually defined SLA targets, therefore, for a simplified view, you are removing the predefined SLA detect servers.

7. Click **OK** to confirm the deletion of the selected elements.

To check the routing table

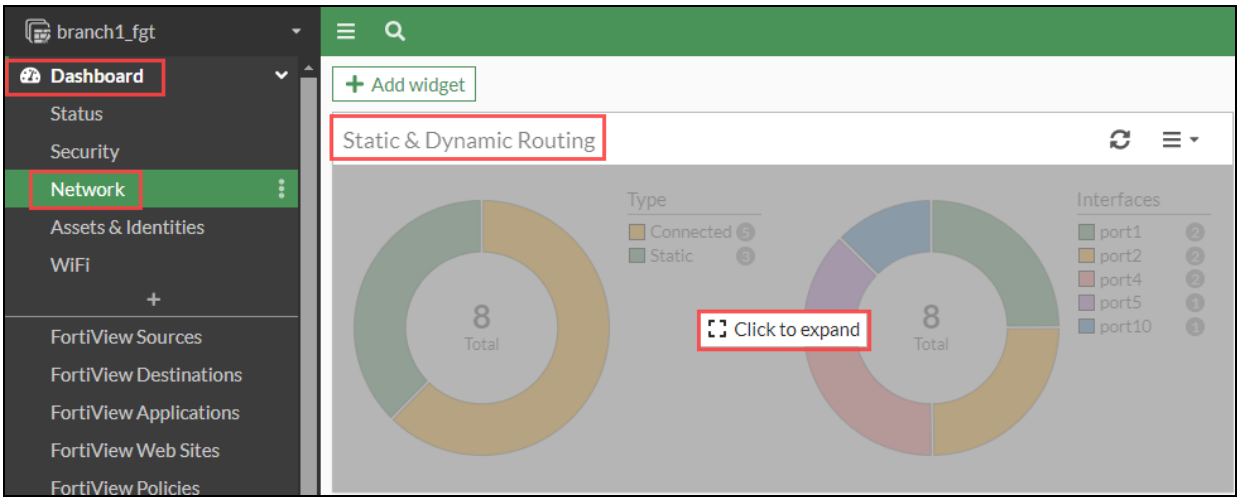
1. Click **Network** > **Static Routes** to review the static route configuration.
   Your page should look similar to the following example:

Destination	Gateway IP	Interface	Status
172.16.0.0/16	172.16.0.2	port4	Enabled

2. Click **Dashboard** > **Network**, and then click the **Static & Dynamic Routing** widget to expand it.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



Your page should look similar to the following example:

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	192.2.0.2	port1	5	Static
0.0.0.0/0	192.2.0.10	port2	5	Static
10.0.1.0/24	0.0.0.0	port5	0	Connected
172.16.0.0/16	172.16.0.2	port4	10	Static
172.16.0.0/29	0.0.0.0	port4	0	Connected
192.2.0.0/29	0.0.0.0	port1	0	Connected
192.2.0.8/29	0.0.0.0	port2	0	Connected
192.168.0.0/24	0.0.0.0	port10	0	Connected

Stop and think!

Only one static route was preconfigured for you on this FortiGate, but the **Static & Dynamic Routing** widget displays three static routes. Why?

The port1 and port2 interfaces are both configured as DHCP clients. They dynamically retrieve their IP addresses and default gateways from the DHCP server. With such settings, by default, FortiGate automatically adds a default static route to the gateway IP address with a distance of 5.

The default distance for manually configured static routes is 10.

3. Open an SSH session to branch1_fgt, and then log in to the FortiGate CLI with the following credentials:
   - Username: `admin`
   - Password: `password`
4. Enter the following command:
   ```
   get router info kernel | grep proto=18
   ```
   Your output should display the following lines:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
type=1 proto=18 prio=0 192.2.0.1/255.255.255.255/0->198.18.1.1/32 pref=0.0.0.0 gwy=192.2.0.2 dev=3(port1)
type=1 proto=18 prio=0 192.2.0.9/255.255.255.255/0->198.18.1.1/32 pref=0.0.0.0 gwy=192.2.0.10 dev=4(port2)
type=1 proto=18 prio=0 192.2.0.1/255.255.255.255/0->198.18.1.2/32 pref=0.0.0.0 gwy=192.2.0.2 dev=3(port1)
type=1 proto=18 prio=0 192.2.0.9/255.255.255.255/0->198.18.1.2/32 pref=0.0.0.0 gwy=192.2.0.10 dev=4(port2)
```

To route the health check probes, FortiOS installs special kernel routes using the gateway information of the SD-WAN members. These routes are not displayed in the routing table, but you can use the `get router info kernel` CLI command to see them. These kernel routes are flagged as `proto=18`.

Those routes are useful for interfaces with manually defined IP addresses, when there is no associated default route defined.

Configure Rules

You will configure two SD-WAN rules. One rule will be used to steer the traffic of critical applications. The other rule will be used to steer the traffic of non-critical applications. Both rules will use manual mode.

By default, application detection for SD-WAN rules is not visible on the GUI. Before you can configure SD-WAN rules to steer traffic per application, you must enable GUI visibility with CLI commands.

To enable GUI visibility for application detection

1. Continuing on the branch1_fgt SSH session, enter the following commands to enable the visibility of application detection for SD-WAN rules:

```
config system global
   set gui-app-detection-sdwan enable
end
```

To view the application field on the GUI, you must refresh the browser page. Alternatively, you can log out of the GUI, and then log in again.

To configure rules

1. Return to the branch1_fgt GUI, and then refresh the browser page.
2. Click **Network** > **SD-WAN**, and then click the **SD-WAN Rules** tab.
3. Click **Create New** to add a rule.
4. Configure the following settings:

Field	Value
Name	Critical-DIA
Source Address	LAN-net
Application	Select **Salesforce** and **Microsoft.Portal**.
Interface selection strategy	Select **Manual**.
Interface preference	Select **port1**, and then select **port2**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

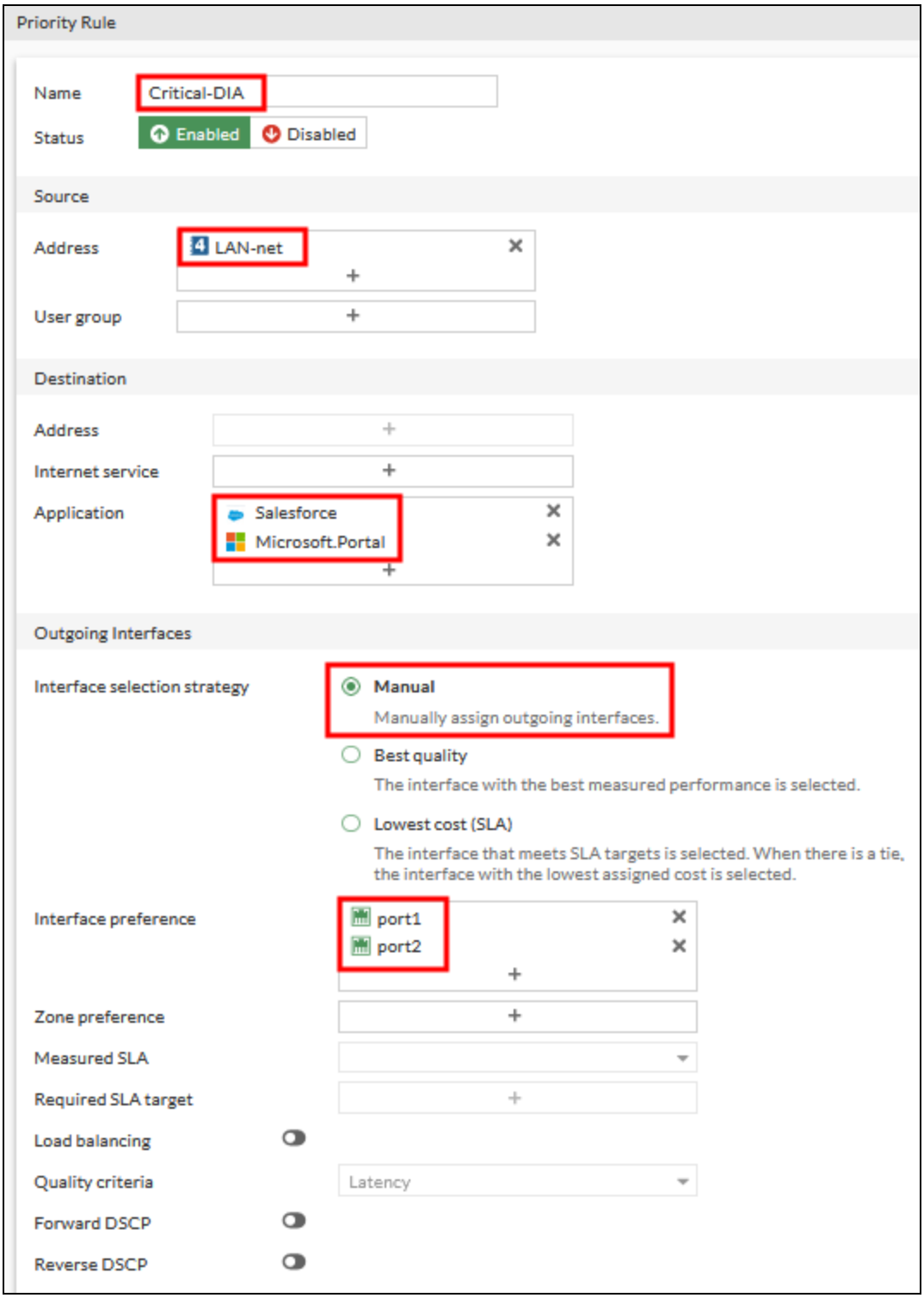
The **LAN-net** firewall address object was preconfigured.

The order in which you define the interface is important. It determines the interface preference. When an SD-WAN rule selects an interface to steer the traffic, it refers to the interface order to determine the preferred interface.

Your page should look similar to the following example. Note that you may not be able to view the application icons at this stage.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

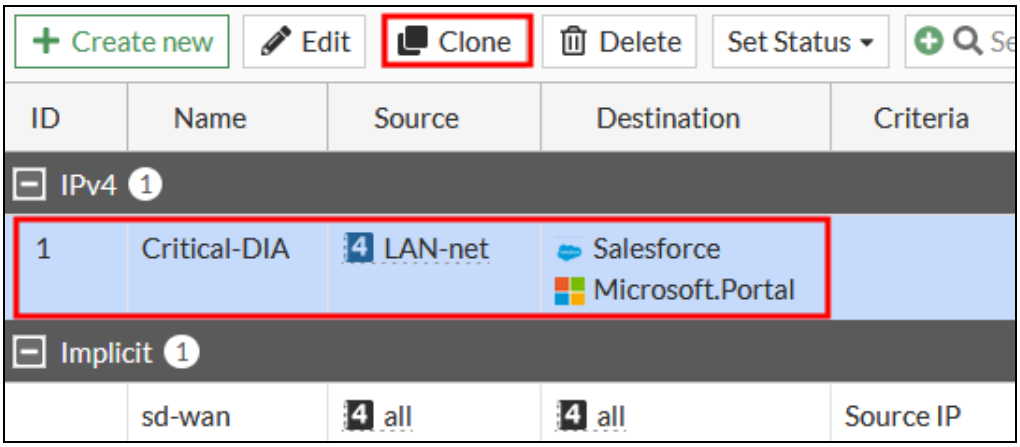
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



5. Click **OK** to save the settings.
6. Select the SD-WAN rule that you created, and then click **Clone**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

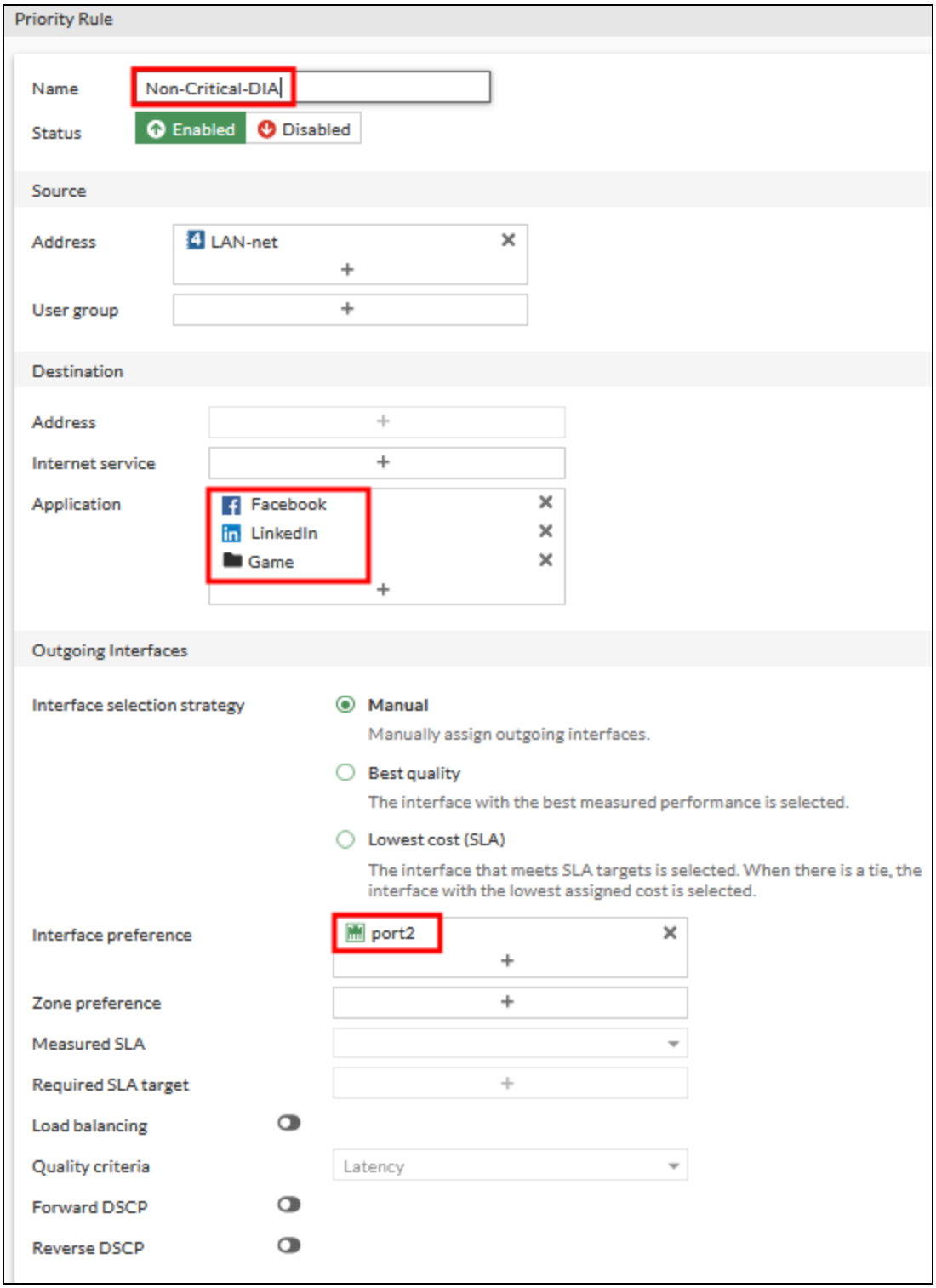


7. Adjust the cloned rule to configure a rule for non-critical traffic using the following settings:

Field	Value
Name	Non-Critical-DIA
Source Address	LAN-net
Application	Remove the application selected for the previous rule. Select **Apps**, and then select **Facebook** and **LinkedIn**. Select **Category**, and then select **Game**.
Interface selection strategy	Select **Manual**.
Interface preference	Keep only **port2**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



8. Click **OK** to save the settings.
9. Click **Network** > **SD-WAN**, and then click the **SD-WAN Rules** tab to refresh the page.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

ID	Name	Source	Destination	Criteria	Members
IPv4 2					
1	Critical-DIA	LAN-net	Salesforce Microsoft.Portal		port1 port2
2	Non-Critical-DIA	LAN-net	Facebook LinkedIn Game		port2
Implicit 1					
	sd-wan	all	all	Source IP	any

port1 is the preferred member for rule ID 1, and **port2** is the preferred member for rule ID 2.

Configure a Static Route and Firewall Policy

You will configure a static route and firewall policy for routing and allowing SD-WAN traffic. Both objects will reference the underlay zone.

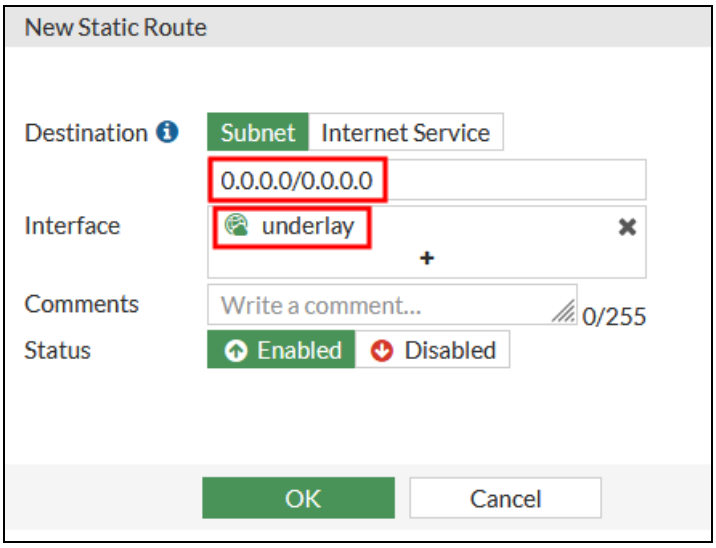
Note that this exercise is for demonstration purpose only. FortiGate already defined a static route with the same destination, gateway, and interfaces.

To configure a static route

1. Continuing on the branch1_fgt GUI, click **Network** > **Static Routes**.
2. Click **Create New** to add a static route.
3. In the **Interface** field, select **underlay**.
4. Keep **0.0.0.0/0.0.0.0** as the destination subnet to create a default route.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

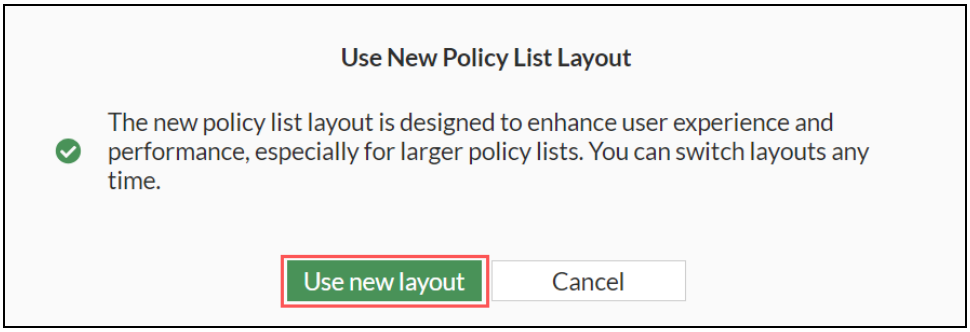
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



5. Click **OK** to save the settings.

To configure a firewall policy

1. Click **Policy & Objects** > **Firewall Policy**.
2. If prompted, click **Use new layout**.



3. Click **Create New** to add a firewall policy.
4. Configure the following settings:

Field	Value
Name	DIA
Incoming interface	port5
Outgoing interface	underlay
Source	LAN-net
Destination	all
Schedule	always

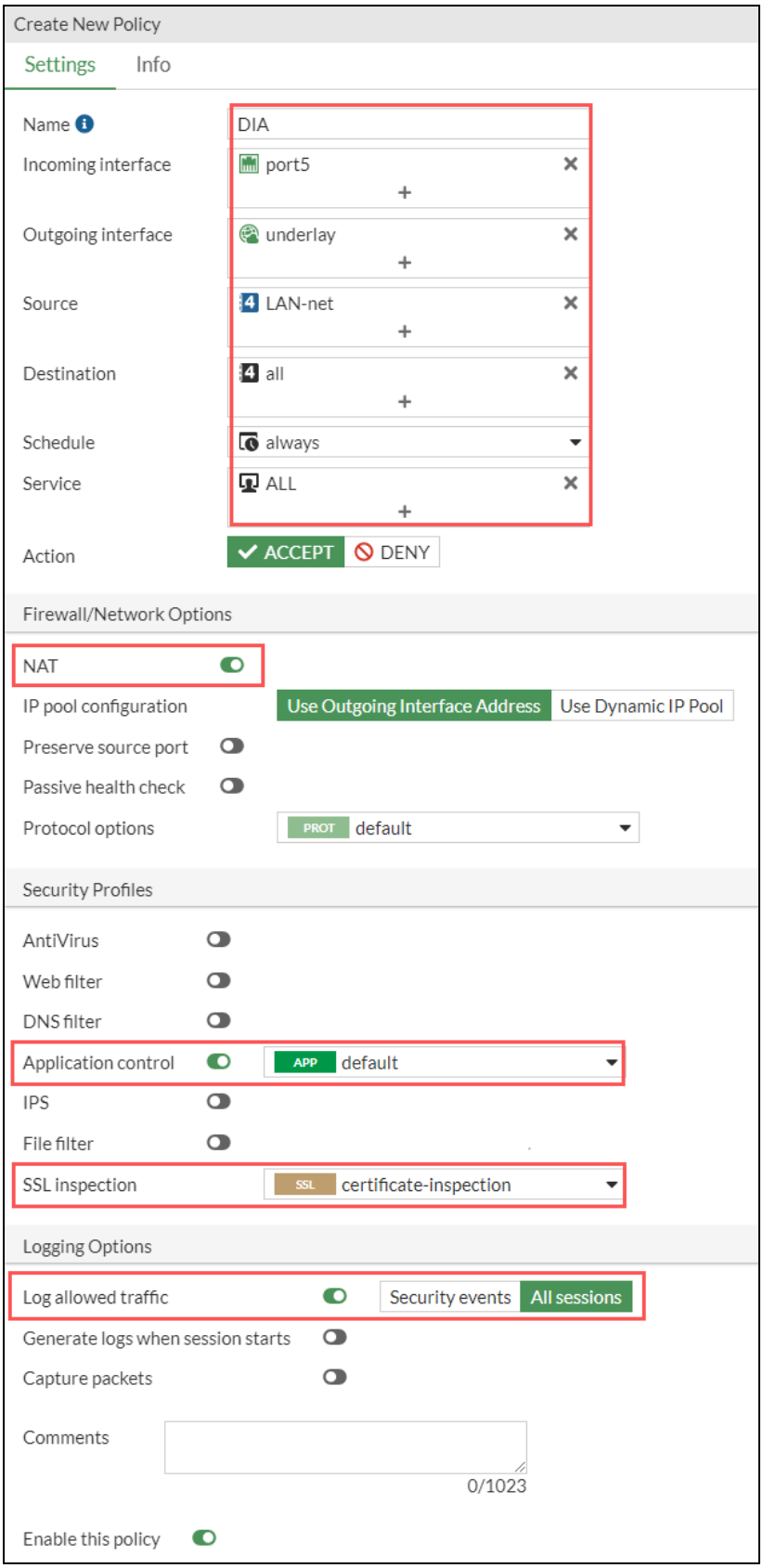
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Service	ALL
NAT	Enabled
Application control	Enable this setting, and then select **default**.
SSL inspection	Select **certificate-inspection**.
Log allowed traffic	Enable this setting, and then select **All sessions**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

5. Click **OK** to save the settings.

   Your page should look similar to the following example:

	Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles
port5 → underlay 1										
	DIA (1)	LAN-net	all	always	ALL	ACCEPT		NAT	Standard	SSL certificate-inspection APP default

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Monitoring DIA Traffic

In this exercise, you will generate internet traffic from branch1_client. Next, you will monitor DIA traffic distribution and logs using the SD-WAN tools available on the FortiGate GUI.

Generate Internet Traffic From branch1_client

You will generate internet traffic from branch1_client using a traffic generator tool.

To generate internet traffic from branch1_client

1. Open an SSH session to branch1_client.
2. Log in with the following credentials:
   - Username: `root`
   - Password: `password`
3. Enter the following command:
   `wget http://128.66.0.1/files/linix.iso`
4. Wait for the file download to complete, and then enter the following commands:
   `cd /fortipoc/traffic/`
   `./trafficgenerator.sh`
   Your output shows a turning progress bar. It should look similar to the following example:

```
root@branch1-client-cli:/# cd /fortipoc/traffic
root@branch1-client-cli:/fortipoc/traffic# ./trafficgenerator.sh
 [-]
```

branch1_client is generating various types of internet traffic.

Review SD-WAN Member Health and Routes

You will use the SD-WAN dashboard widget on the FortiGate GUI to review the SD-WAN member health. Next, you will review the static routes associated with SD-WAN members.

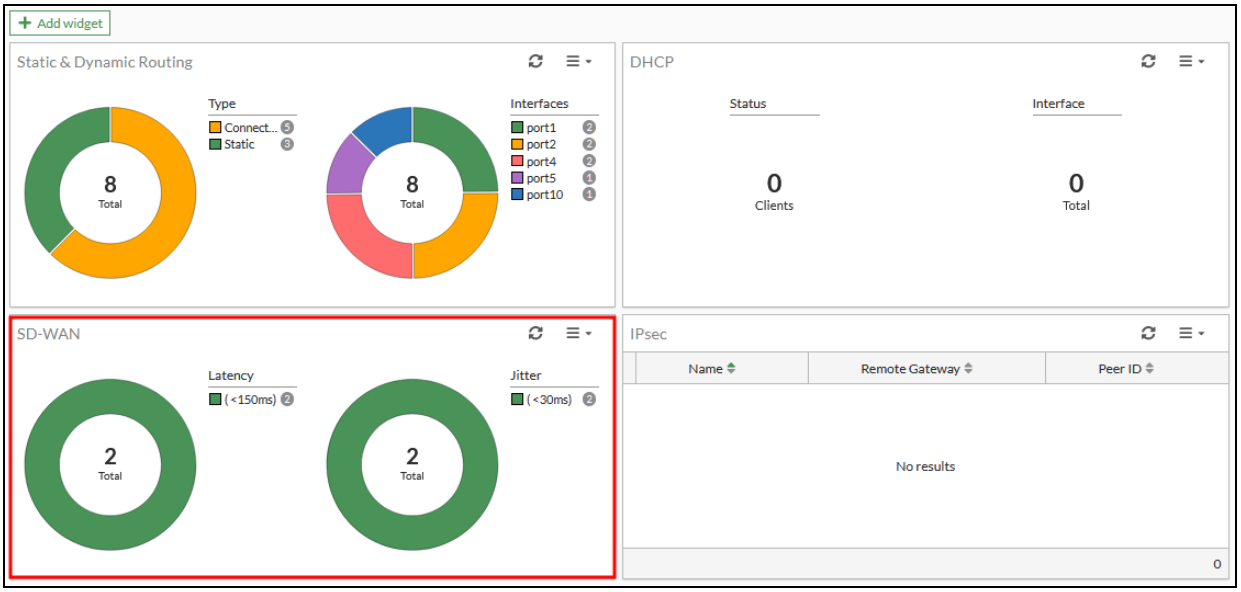
To review SD-WAN member health

1. Access the branch1_fgt GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Dashboard** > **Network**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

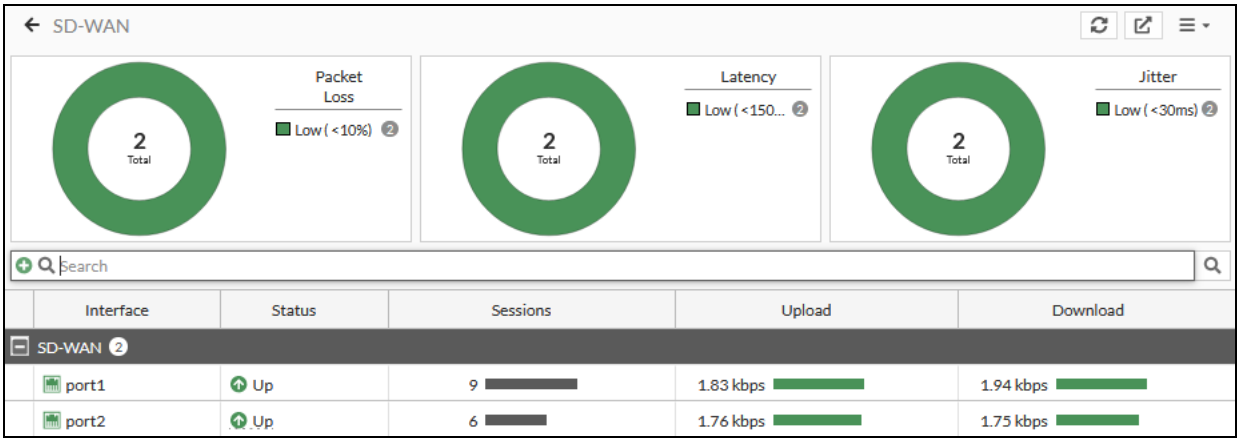
Your page should look similar to the following example:



Note that the number of images, and the level of details, that you see will differ according to your screen display size and resolution.

3. Click the **SD-WAN** widget to expand and view the details.

   Your page should look similar to the following example:



4. Hover over the graphs to view details.
5. If the packet loss, latency, or jitter values are *not* low for one member, tell your instructor.

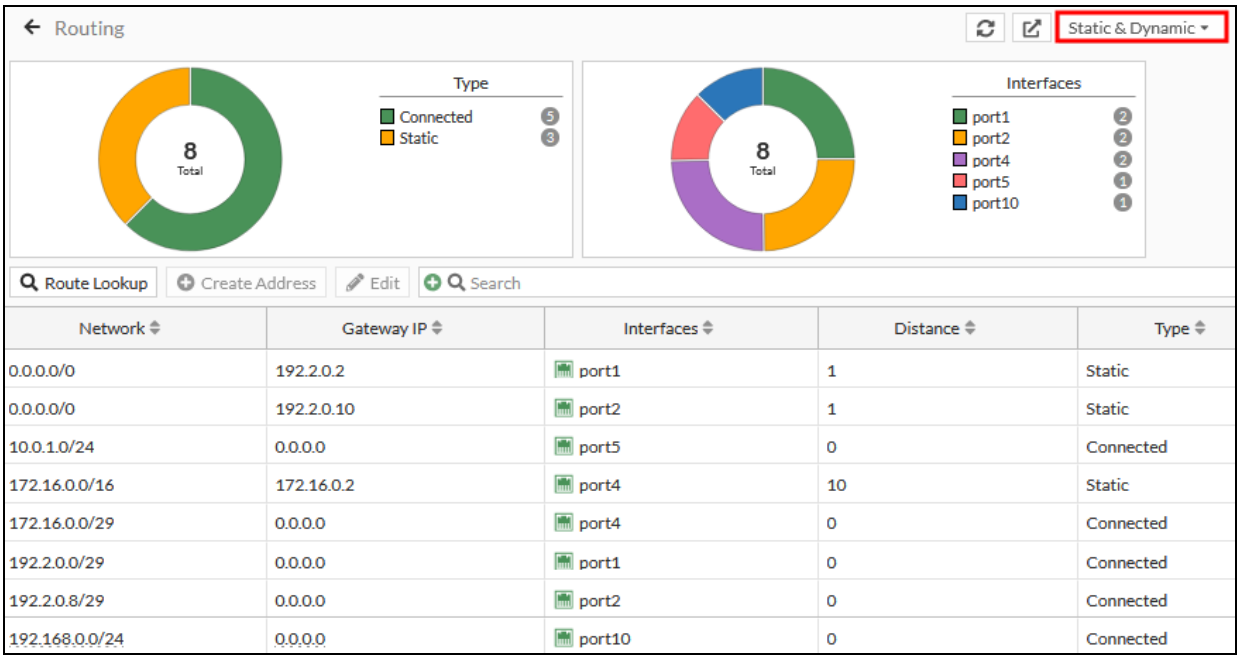
To review the static routes associated with SD-WAN members

1. Click the back arrow to return to the **Network** dashboard, and then click the **Static & Dynamic Routing** widget to expand it and display the device routing table.

   Your output should look similar to the following example:

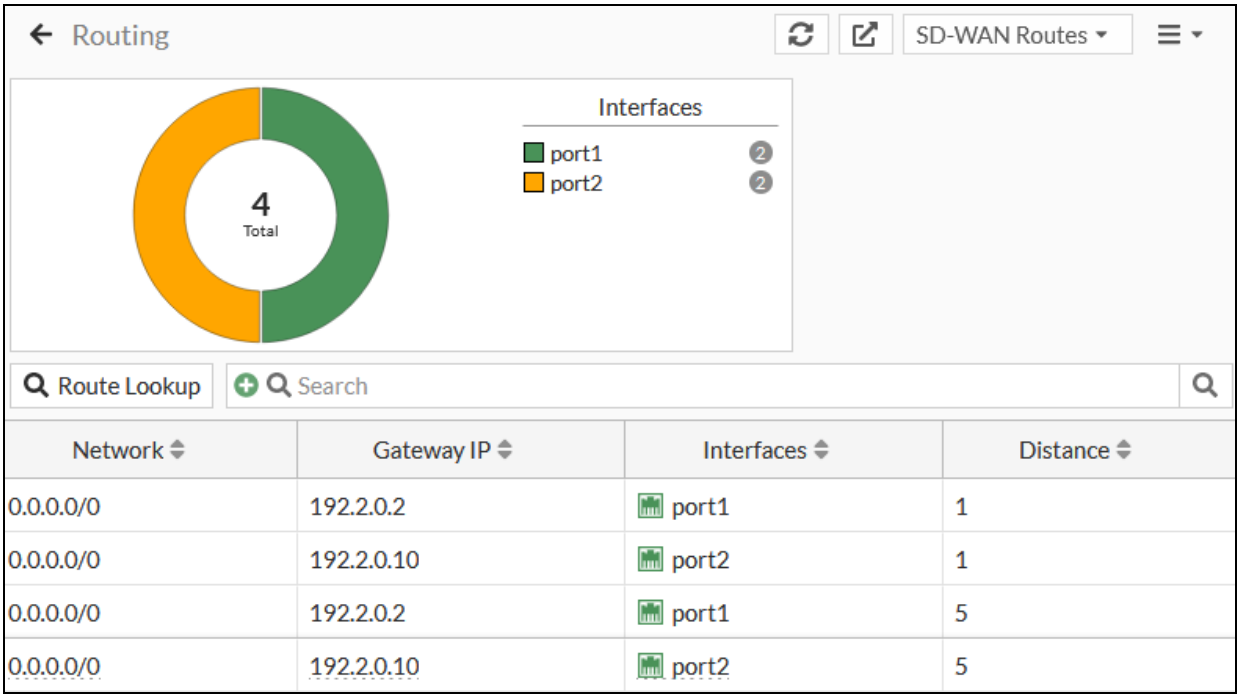
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	192.2.0.2	port1	1	Static
0.0.0.0/0	192.2.0.10	port2	1	Static
10.0.1.0/24	0.0.0.0	port5	0	Connected
172.16.0.0/16	172.16.0.2	port4	10	Static
172.16.0.0/29	0.0.0.0	port4	0	Connected
192.2.0.0/29	0.0.0.0	port1	0	Connected
192.2.0.8/29	0.0.0.0	port2	0	Connected
192.168.0.0/24	0.0.0.0	port10	0	Connected

2. Click **Static & Dynamic**, and then select **SD-WAN Routes**.
   Your page should look similar to the following example:



Network	Gateway IP	Interfaces	Distance
0.0.0.0/0	192.2.0.2	port1	1
0.0.0.0/0	192.2.0.10	port2	1
0.0.0.0/0	192.2.0.2	port1	5
0.0.0.0/0	192.2.0.10	port2	5

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

There are two default routes for each interface with the same gateway but different distances. Why?

The default routes with a distance of 5 correspond to the static default route that FortiGate creates for each interface that is configured as a DHCP client. (For more information, review what you did in Exercise 1: To check the routing table on page 12

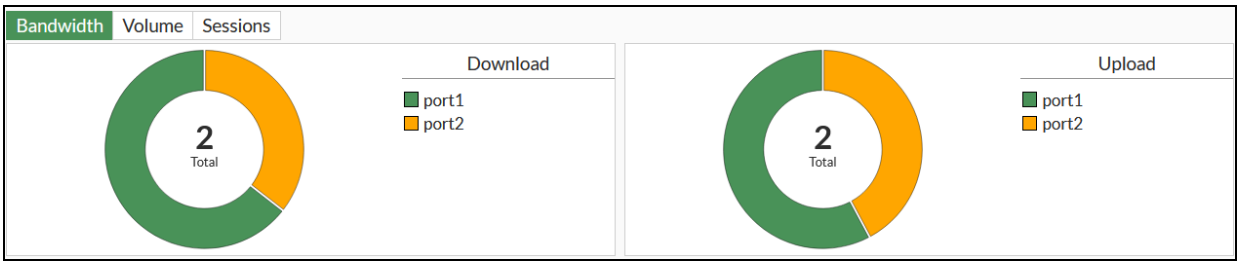
The routes with a distance of 1 correspond to the route you configured for the underlay zone in Exercise 1. By default, FortiGate assigns a distance of 1 to routes defined for SD-WAN zones. For routes defined for individual interfaces, FortiGate assigns a default distance of 10.

Monitor DIA Traffic Distribution

You will use the SD-WAN page on the FortiGate GUI to monitor the DIA traffic distribution. Next, you will view the traffic logs to obtain additional details.

To monitor DIA traffic distribution

1. Continuing on the branch1_fgt GUI, click **Network** > **SD-WAN**, and then click the **SD-WAN Zones** tab.
2. Click **Bandwidth** to display the SD-WAN distribution graphs based on bandwidth.
   Your page should look similar to the following example:



The traffic distribution in this example may be different from yours.

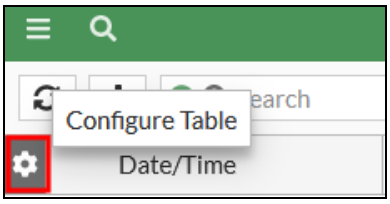
3. Hover over each graph to display the bandwidth that each member (port1 and port2) uses.
4. Click the **Volume** and **Sessions** graphs to explore them.

To view SD-WAN traffic logs

1. Continuing on the branch1_fgt GUI, click **Log & Report** > **Forward Traffic**.
2. Hover over the upper-left corner of the log table to display the table column settings icon.
   A gear icon is displayed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



3. Click the gear icon, and then click **Destination Interface**, **SD-WAN Quality**, and **SD-WAN Rule Name**.
4. Click **Apply** to save the settings.
   Your page should look similar to the following example:

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
Dropbox	Accept (UTM Allowed)	DIA (1)	port2		
Facebook	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
Salesforce	Accept (UTM Allowed)	DIA (1)	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
Microsoft.Portal	Accept (UTM Allowed)	DIA (1)	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
LinkedIn	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
Salesforce	Accept (UTM Allowed)	DIA (1)	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
Dropbox	Accept (UTM Allowed)	DIA (1)	port2		
Facebook	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA

5. Browse the log table, and then confirm the following:
   - **SalesForce** and **Microsoft.Portal** traffic matches the **Critical-DIA** rule, and uses **port1**.
   - **Facebook** and **LinkedIn** traffic matches the **Non-Critical-DIA** rule, and uses **port2**.

You may notice that, initially, traffic for some applications does not match the expected rule. This is because of the application learning phase, which you will learn more about in another lab. However, eventually, traffic should end up matching the expected rule.

Stop and think!

Logs for all other traffic (DNS, HTTP_BROWSER, and so on) show no information in the **SD-WAN Quality** and **SD-WAN Rule Name** columns. Why?

The traffic does not match any of the configured SD-WAN rules. As a result, it matches the implicit SD-WAN rule. The SD-WAN implicit rule load balances sessions based on the FIB contents.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

All other traffic is always forwarded to the same port (this can be port1 or port2). The implicit rule is not load balancing the traffic. Why?

By default, the implicit rule load balances the traffic based on the source IP address of the connection. Because all traffic is sourced from the same IP address (branch1_client), the selected outgoing interface is always the same. You will learn more about implicit rule load balancing in another lab.

6. Keep the internet traffic generator running on branch1_client.

Bring Down port1

You will bring down port1 to force FortiGate to forward all internet traffic to port2.

To bring down port1

1. Connect to the WAN simulator HTTP interface, and then locate **BR1-ISP1**.
2. Click **DOWN** to bring down the link on port1 on branch1_fgt.

3. On the branch1_fgt GUI, click **Network** > **SD-WAN**, and then click the **Performance SLAs** tab.
   port1 is down (red down arrow). Your page should look similar to the following example:

Name	Detect Server	Packet Loss	Latency	Jitter
Corp_HC	198.18.1.1 198.18.1.2	port1: port2: 0.00%	port1: port2: 1.08ms	port1: port2: 0.22ms

Monitor SD-WAN Events and Traffic Logs

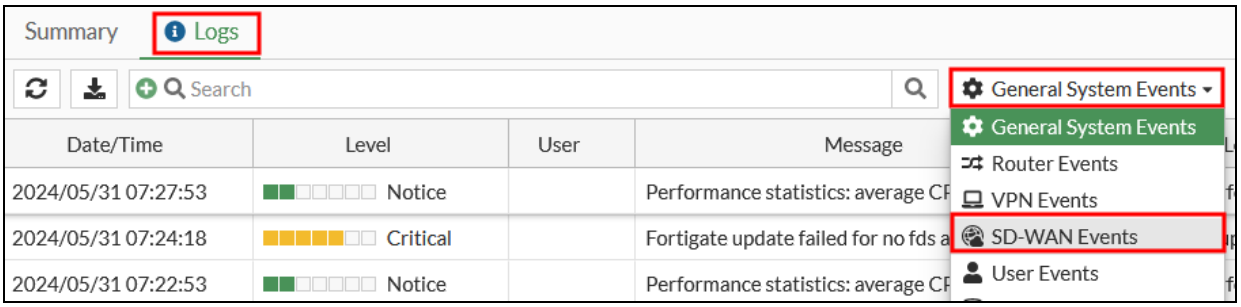
You will review SD-WAN events and traffic logs that the previous action triggered.

To monitor SD-WAN events and traffic logs

1. Continuing on the branch1_fgt GUI, click **Log & Report** > **System Events** > **Logs**.
2. In the top bar, click **General System Events**, and then select **SD-WAN Events**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

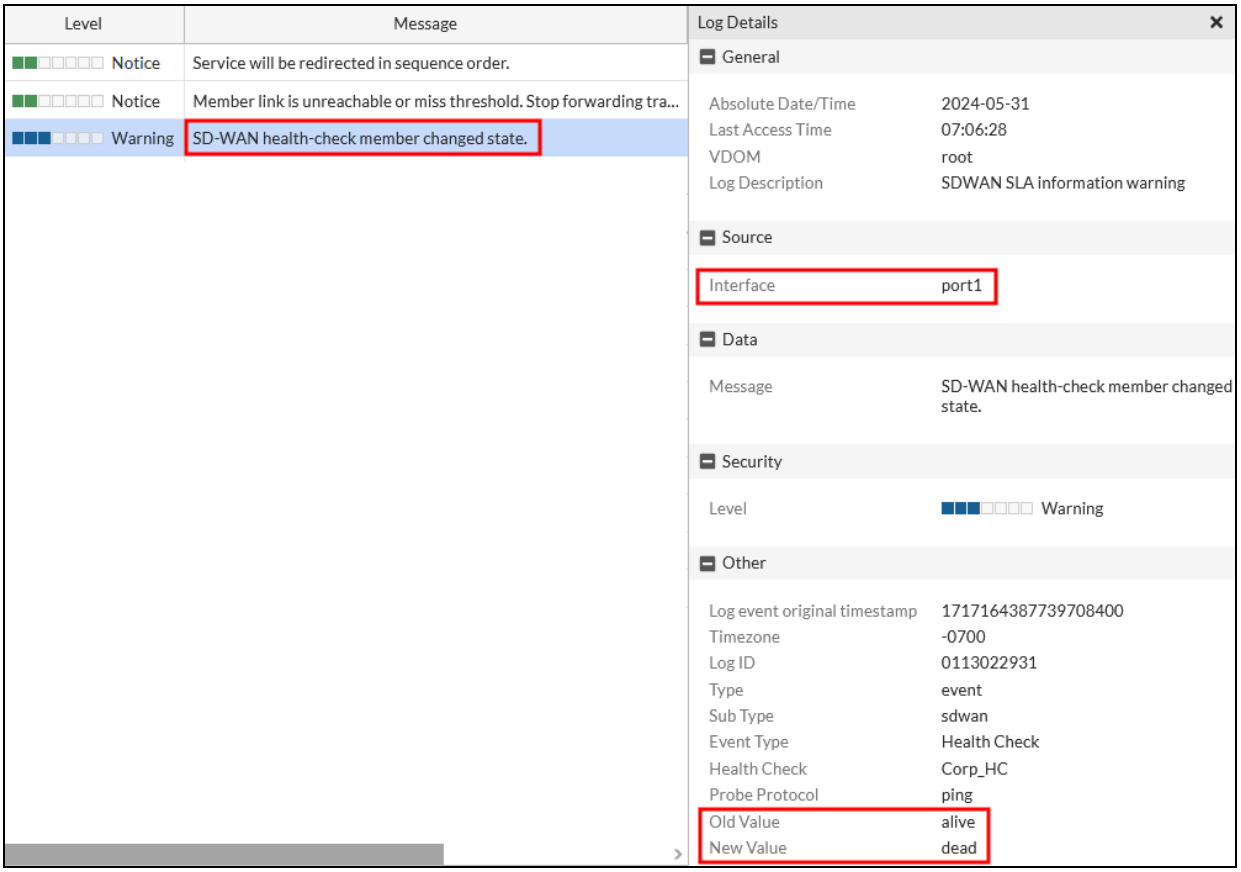
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



3. Look for the three recent message logs that are shown in the following image:

Level	Message	Log Description
Notice	Service will be redirected in sequence order.	SDWAN status
Notice	Member link is unreachable or miss threshold. Stop forwarding traffic.	SDWAN status
Warning	SD-WAN health-check member changed state.	SDWAN SLA information warning

4. Double-click the log with the **SD-WAN health-check member changed state** message to see the log details. Your page should look similar to the following example:

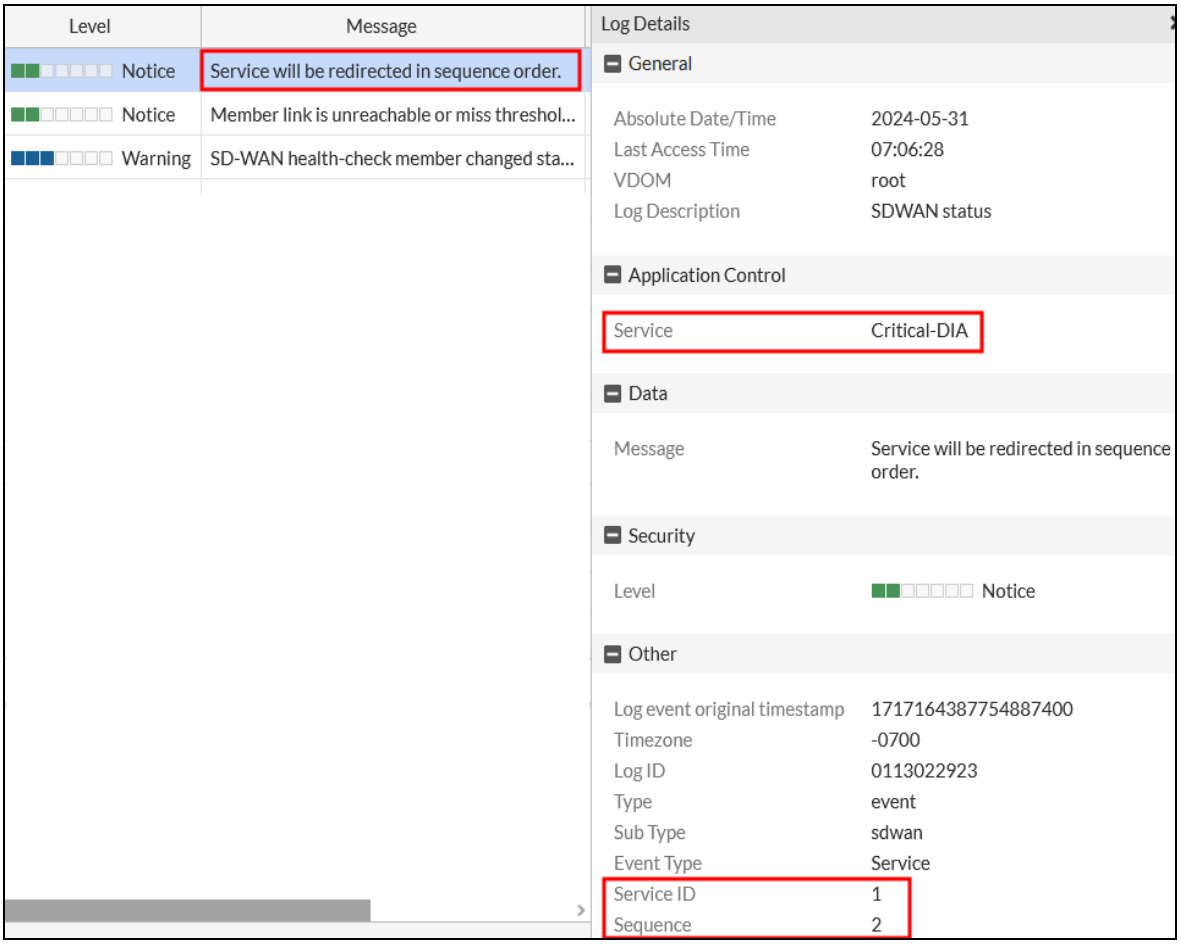


The log indicates that **port1** was marked **dead**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

5. Double-click the log with the **Service will be redirected in sequence order** message to see the log details.
Your page should look similar to the following example:



The log indicates that the **Critical-DIA** rule (ID 1) was updated. The new sequence (outgoing interface list) now contains member ID 2 only (port2). You will learn more about the outgoing interface list in another lab.

6. Click **Log & Report** > **Forward Traffic**.
Your page should look similar to the following example:

Facebook	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
LinkedIn	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
Microsoft.Portal	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Critical-DIA
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
HTTPS.BROWSER	Accept (UTM Allowed)	DIA (1)	port2		
Salesforce	Accept (UTM Allowed)	DIA (1)	port2	Seq_num(2 port2 underlay), alive, selected	Critical-DIA

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

All traffic is now forwarded to port2.

Bring Up port1

You will bring up port1 and confirm that the original traffic distribution is restored.

To bring up port1

1. Continuing on the WAN simulator HTTP interface, scroll up and locate **BR1-ISP1**.
2. Click **UP** to bring up the link on port1 on branch1_fgt.

Take the Expert Challenge!

Use the FortiGate GUI to confirm that:

- port1 is now marked **alive**.
- The outgoing interface list for rule ID 1 (Critical-DIA) is now **1,2**.
- Traffic distribution is restored to the original.

If you require assistance, or to verify your work, review the procedure described previously in this exercise.

3. On branch1_client, press `Ctrl+C` to stop the traffic generator.

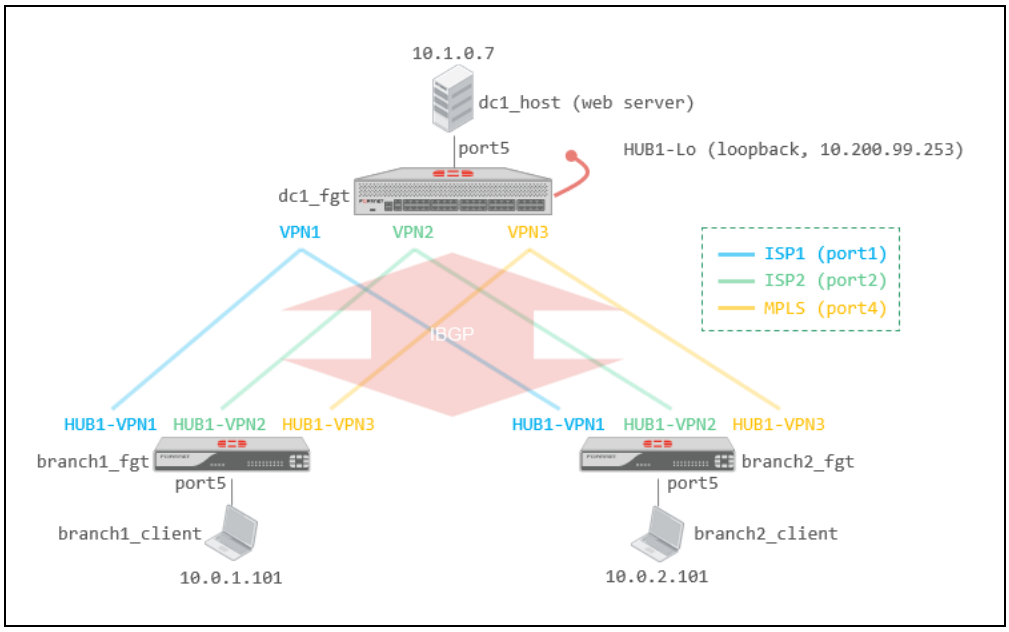
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 2: Centralized Management

In this lab, you will configure the same direct internet access (DIA) SD-WAN setup you configured on branch1_fgt, on branch2_fgt. First, you will import existing SD-WAN settings on branch1_fgt to an SD-WAN template on FortiManager. Next, you will use the SD-WAN template to deploy DIA on branch2_fgt. You will also monitor DIA traffic on FortiManager.

Finally, you will use the SD-WAN overlay template on FortiManager to deploy the following hub-and-spoke dial-up IPsec VPN topology:



In the topology, branch1_fgt and branch2_fgt are dial-up clients, and dc1_fgt is a dial-up server. The three devices connect with three underlays, ISP1 on port1, ISP2 on port2, and MPLS on port4.

You will deploy overlays for three underlays (ISP1, ISP2, and MPLS) and use BGP as the routing protocol on those overlay links.

Note that there is no separate FortiAnalyzer. Instead, you will configure devices to send logs to FortiManager, which has the FortiAnalyzer features enabled. To help you with the device identification, the FortiGate devices branch1_fgt and branch2_fgt use the default GUI color jade (green), the hub device dc1_fgt uses neutrino (dark blue), and the FortiManager GUI uses mariner (blue).

Objectives

- Add all devices to FortiManager
- Deploy DIA using central management (SD-WAN templates)
- Use the SD-WAN overlay template to configure IPsec VPN tunnels for the overlay and the corresponding BGP routing
- Monitor SD-WAN and IPsec tunnels on FortiManager

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Time to Complete

Estimated: 90 minutes

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Configuring SD-WAN on FortiManager

In this exercise, you will add branch1_fgt and branch2_fgt to FortiManager. Next, you will create an SD-WAN template with settings imported from branch1_fgt. Finally, you will use the template to deploy DIA on branch2_fgt.

Add branch1_fgt and branch2_fgt to FortiManager

You will add branch1_fgt and branch2_fgt to FortiManager.

To add branch1_fgt and branch2_fgt to FortiManager

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Device & Groups**.
3. Click **Add Device**.

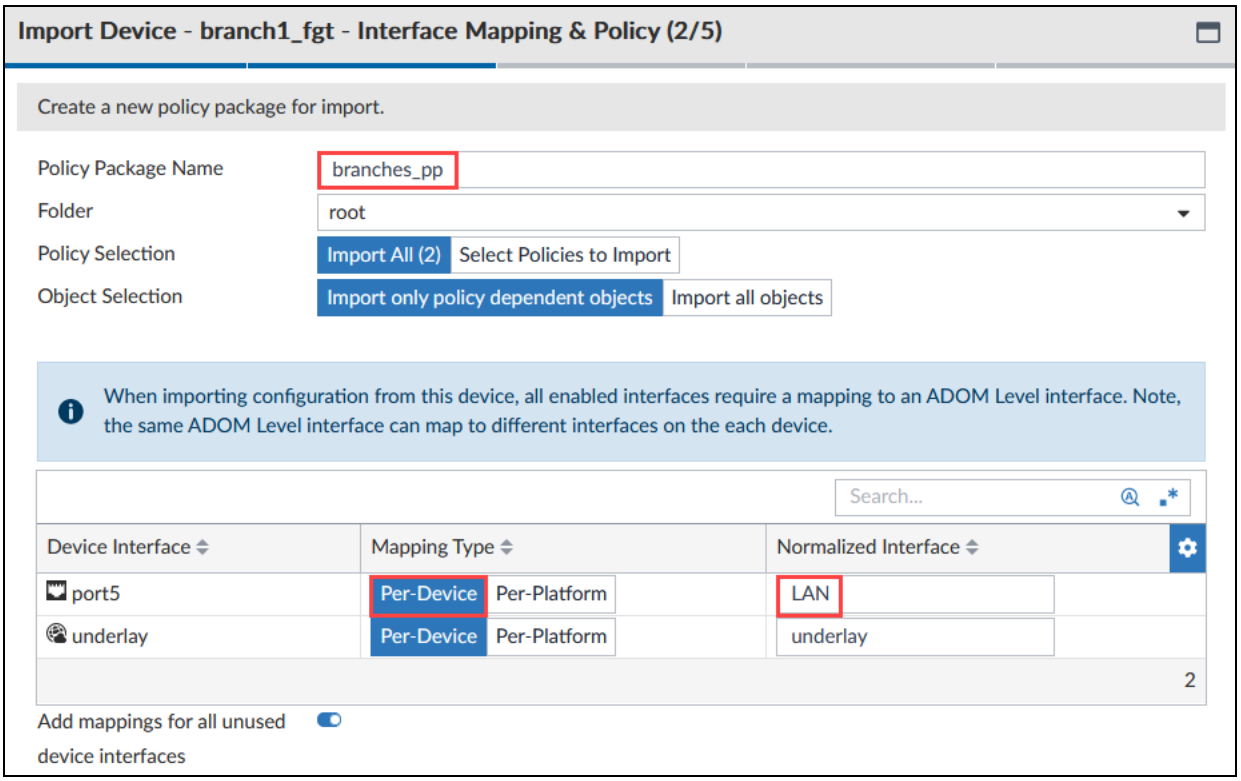
4. Click **Discover Device**, and then configure the following settings:

Field	Value
IP Address	192.168.0.31
Use legacy device login	Enabled
User Name	admin
Password	password

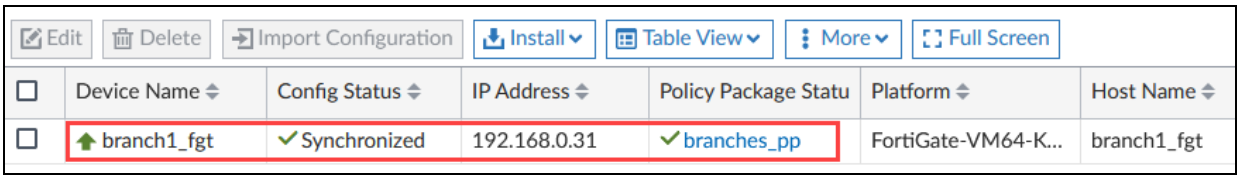
5. Click **Next**.
6. Review the information about the discovered device, and then click **Next**.
7. Wait until the **Add Device** task is completed, and then click **Import Now**.
8. Select **Import Policy Package**, and then click **Next**.
9. In the **Policy Package Name** field, type `branches_pp`.
10. In the port5 device interface settings, in the **Mapping Type** column, select **Per-Device**, and then in the **Normalized Interface** column, type `LAN`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



11. Click **Next**.
12. Review the objects to import, and then click **Next**.
13. Wait until the **Import Device** task is completed, and then click **Finish**.
14. Click **Device & Groups** > **Managed FortiGate** to display the list of managed devices.
    Your page should look similar to the following example:

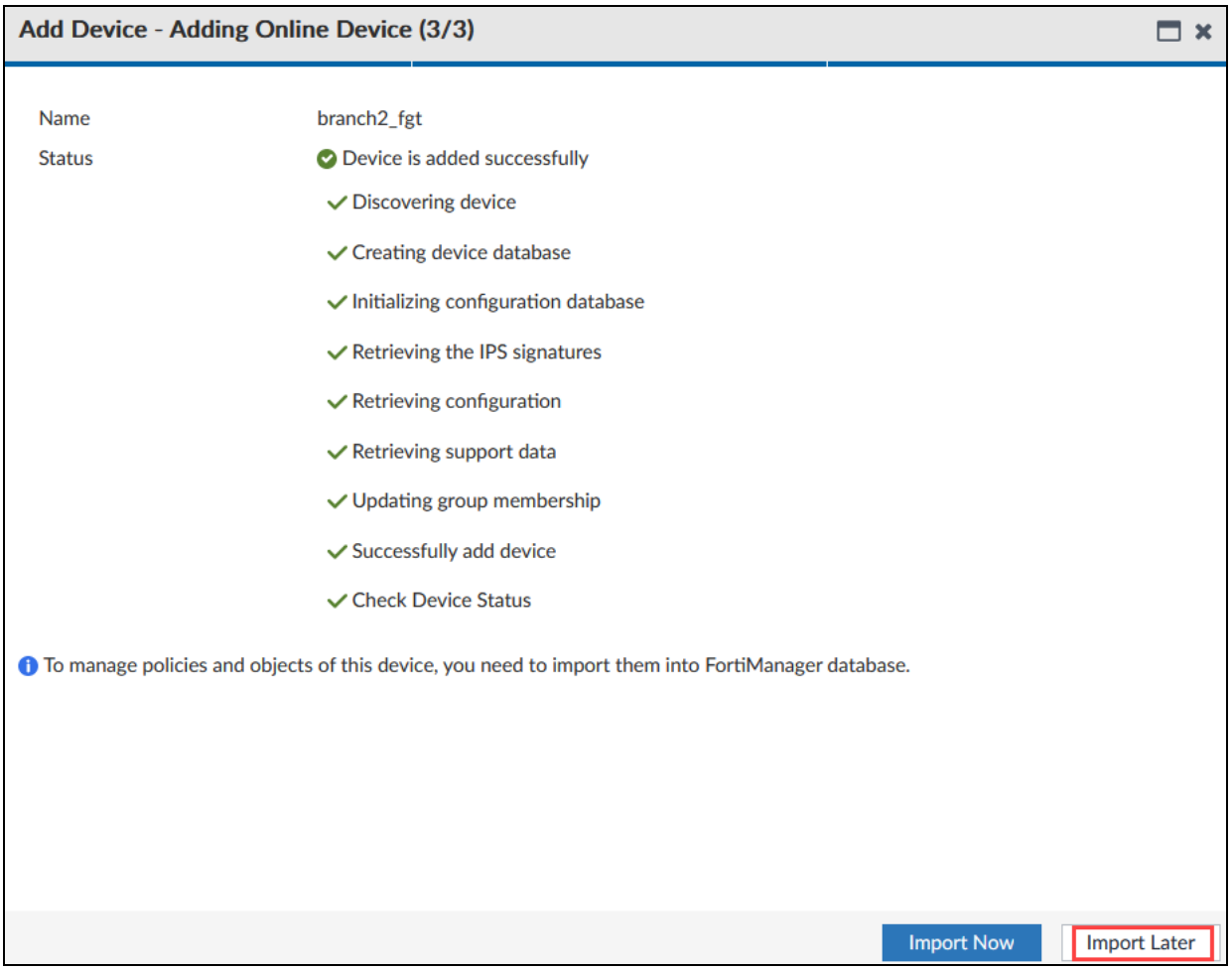


For better readability, you can drag and drop the columns to rearrange them.

15. Repeat steps 2–5 for branch2_fgt, but use the IP address `192.168.0.32` and the same administrator credentials.
16. Click **Import Later**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

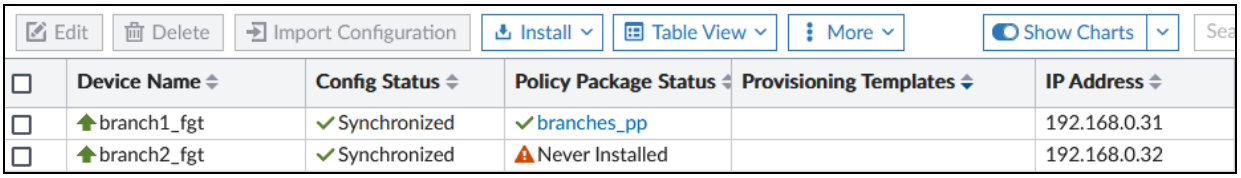
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



You don't need to import policies and objects from branch2_fgt because branch2_fgt will use the **branches_pp** policy package that you created when you onboarded branch1_fgt.

17. Click **Device & Groups** > **Managed FortiGate** to display the list of managed devices.
18. Drag and drop the **Policy Package Status** and **Provisioning Templates** columns to the right of the **Config Status** column so you can see them without having to scroll to the right.

    Your page should look similar to the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

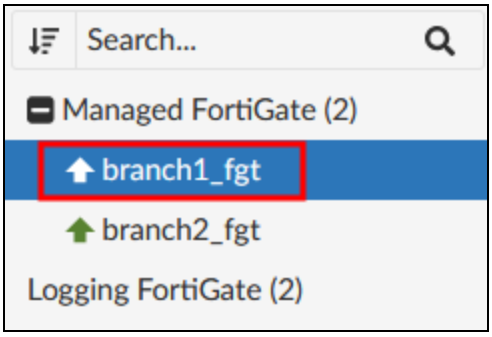
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Import SD-WAN Settings Into the SD-WAN Template

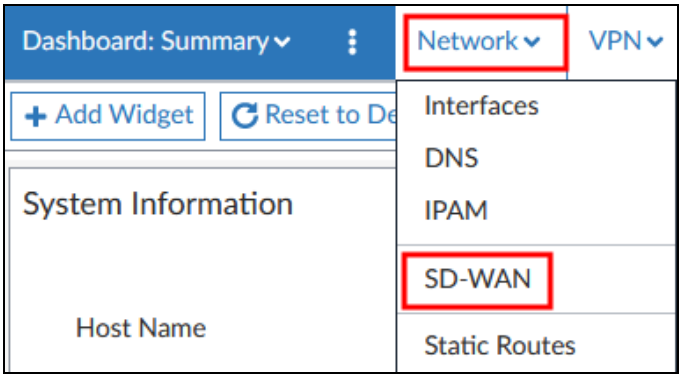
First, you will view the current SD-WAN settings on branch1_fgt (per-device management). Next, you will import the settings into an SD-WAN template for central SD-WAN management purposes.

To view the per-device SD-WAN settings of branch1_fgt

1. Continuing on the FortiManager GUI, expand **Managed FortiGate**, and then click **branch1_fgt**.



2. Click **Network** > **SD-WAN** to display the device SD-WAN settings.



Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

SD-WAN

SD-WAN Status

SD-WAN Zones

+ Create New | Edit | Delete | Where Used | Search...

ID	Interface	Gateway	Cost	Priority	Status
virtual-wan-link					
underlay					
1	port1	0.0.0.0	0	1	Enable
2	port2	0.0.0.0	0	1	Enable

4

Create VPN

SD-WAN Rules

+ Create New | Edit | Delete | More | Search...

ID	Name	Source	Destination	Criteria	Members	Performance SLA	Port	Protocol	Status
1	Critical-DIA	LAN-net	Microsoft.Portal Salesforce		port1 port2			any	Enable
2	Non-Critical-DIA	LAN-net	Facebook LinkedIn Game		port2			any	Enable
	sd-wan	All	All	Source IP	All			any	

3

Performance SLA

+ Create New | Edit | Delete | Where Used | Search...

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Corp_HC	198.18.1.1, 198.18.1.2				5	5

1

Neighbor

+ Create New | Edit | Delete | Search...

IP	Role	Interface Member	Performance SLA	SLA
No record found.				

0

Duplication

+ Create New | Edit | Delete | Search...

ID	Source Address	Destination Address	Service	Packet Duplication	Packet Discard Duplication
No record found.					

0

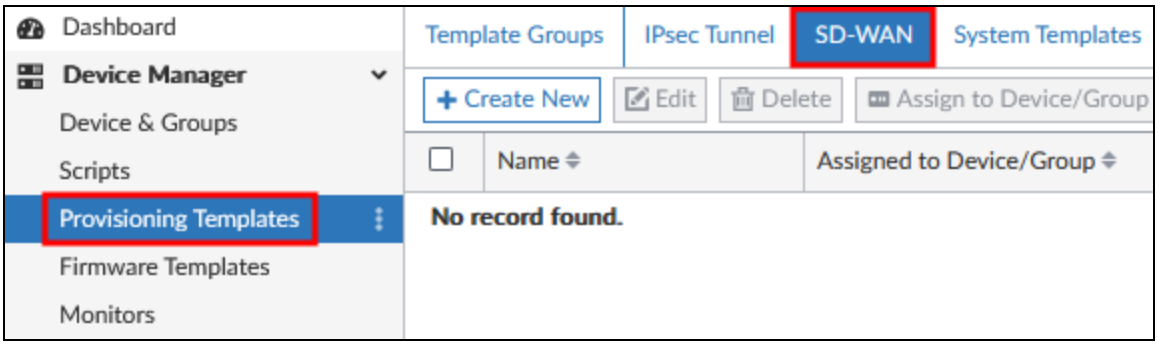
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The **Gateway** field for **port1** and **port2** is set to `0.0.0.0`. You will change this setting to use metadata variables later in this lab.

To import the SD-WAN settings of branch1_fgt into the SD-WAN template

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.



2. Click **More**, and then select **Import** to import the settings into the template.

3. Configure the following settings:

Field	Value
Name	branches
Device	branch1_fgt (root)

4. Click **OK** to import the branch1_fgt SD-WAN settings as the template.
5. Double-click **branches** to view the template settings, and then compare them with the per-device SD-WAN settings of branch1_fgt.

   Both per-device and template settings should be the same.
6. Click **Cancel**.

Configure the SD-WAN Template

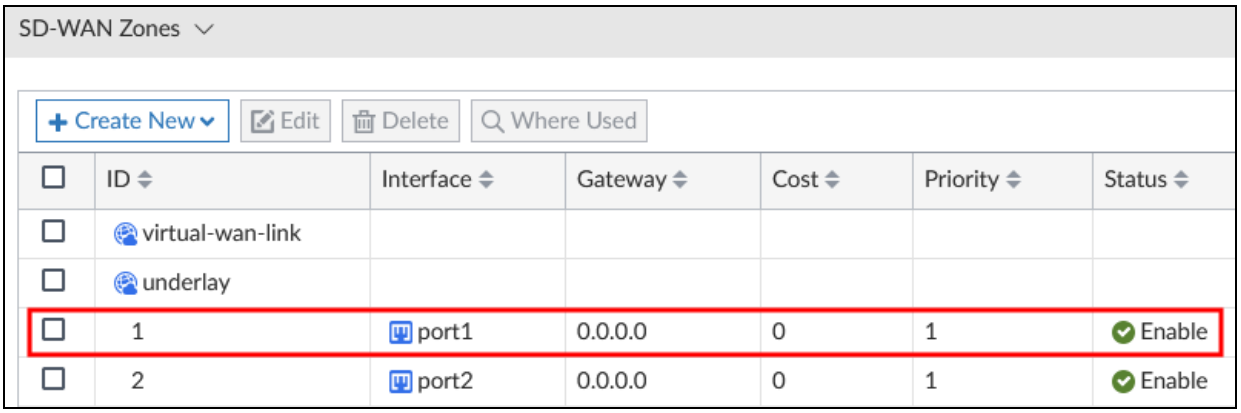
You will configure the template to use metadata variables for the gateway settings. After that, you will configure branch1_fgt and branch2_fgt as the template targets.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To configure metadata variables for the SD-WAN member gateway settings

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
2. Double-click **branches** to edit the template settings.
3. In the **SD-WAN Zones** section, double-click **port1** to edit the member settings.

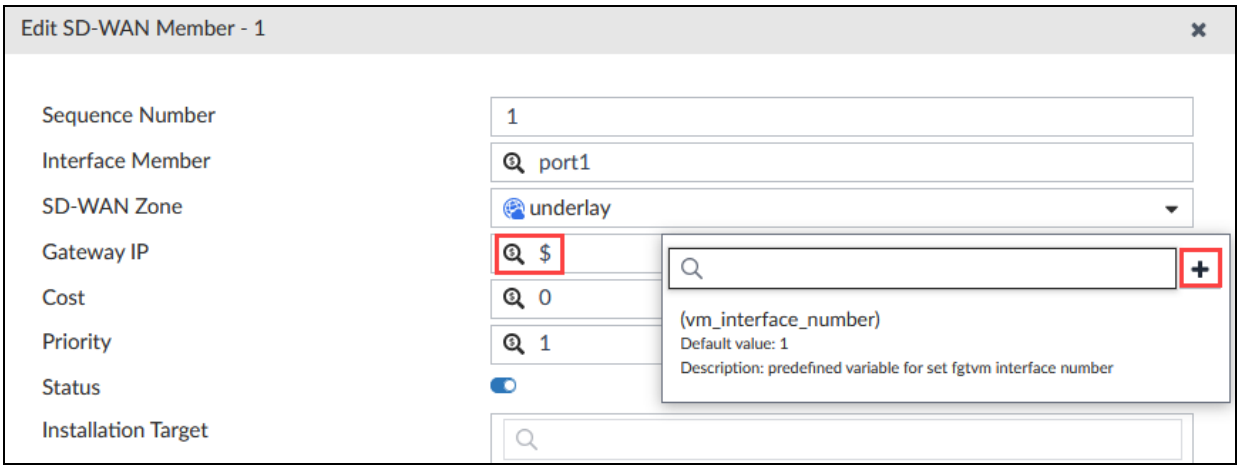


SD-WAN members are always part of a zone, by default the virtual-wan-link zone.

To move a member from one zone to the other, open the target zone and select the member.

4. In the **Gateway IP** field, type `$` to replace `0.0.0.0`.
   A window appears where you can select existing metadata variables or create new variables.

   Your page should look similar to the following example:



5. Click **+** to create a new variable.
6. Create a new metadata variable with the following settings:

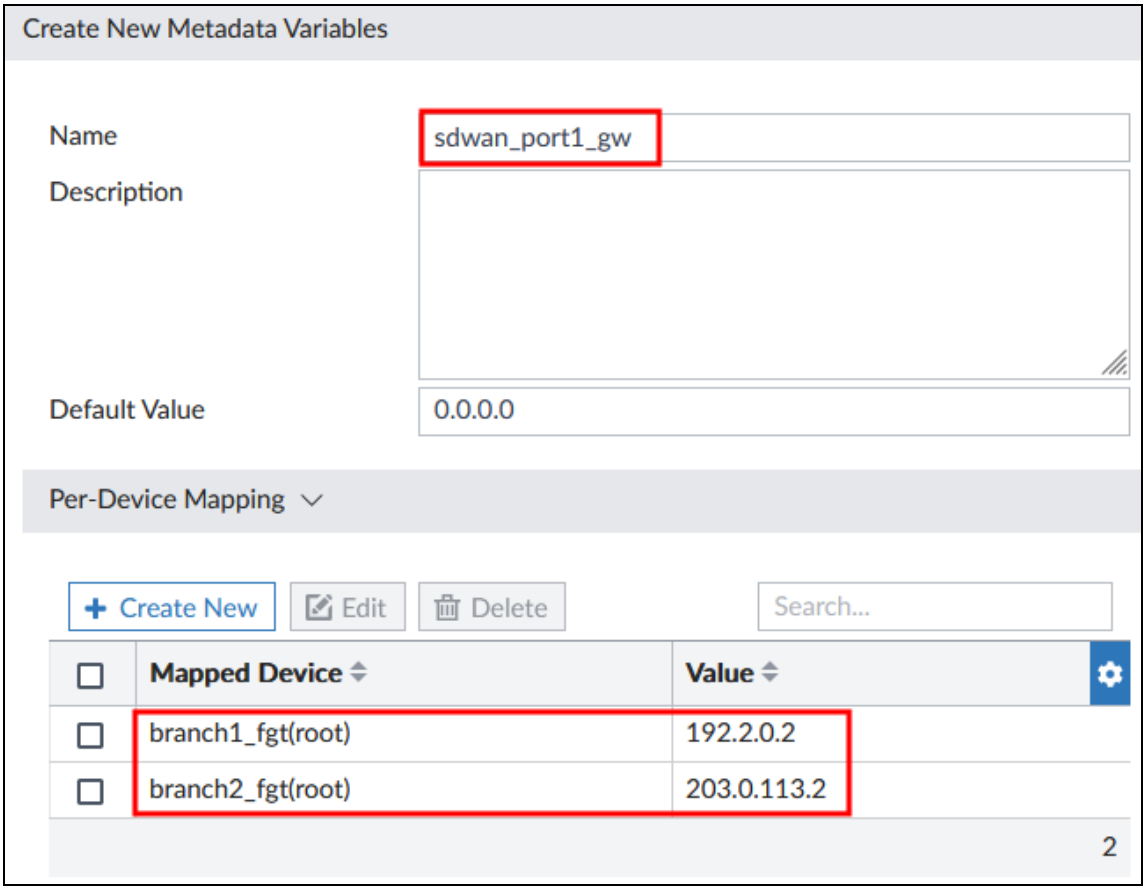
Field	Value
Name	sdwan_port1_gw

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Default Value	0.0.0.0
Per-Device Mapping	Expand this section, click **Create New**, and then configure the following settings: 1. In the **Mapped Device** field, select **branch1_fgt [global]**. 2. In the **Value** field, type `192.2.0.2`. 3. Click **OK** to save the settings. Click **Create New** again, and then configure the following settings: 1. In the **Mapped Device** field, select **branch2_fgt [global]**. 2. In the **Value** field, type `203.0.113.2`. 3. Click **OK** to save the settings.

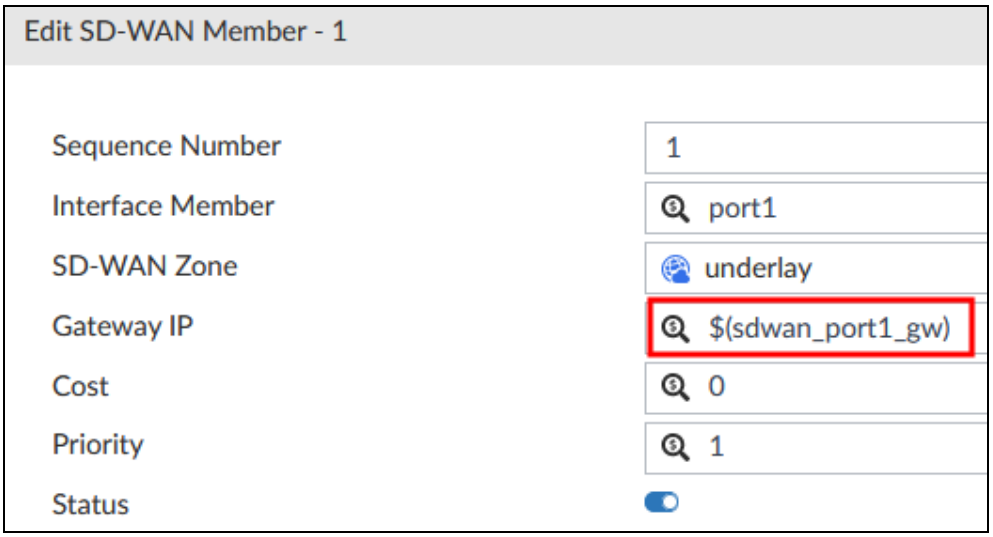
Your page should look similar to the following example:



7. Click **OK** to save the settings.
8. In the **Gateway IP** field of **port1**, select the **$(sdwan_port1_gw)** metadata variable you configured.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

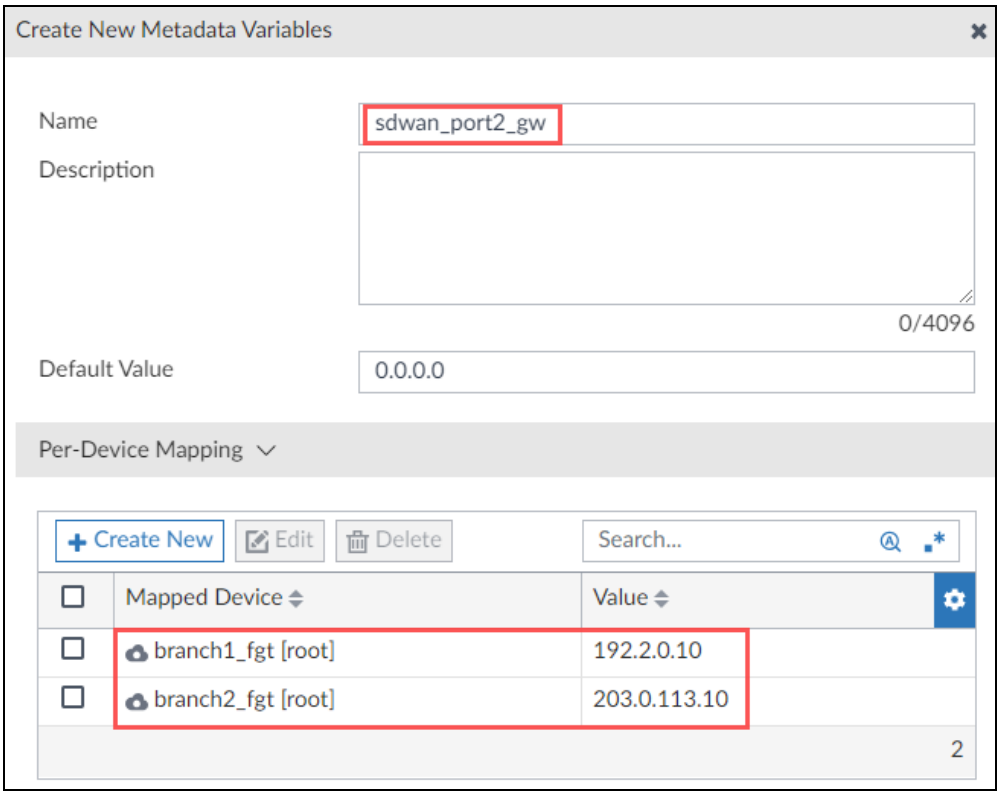


9. Click **OK** to save the settings.
10. Repeat the procedure to configure a metadata variable for the port2 gateway, using the following settings:

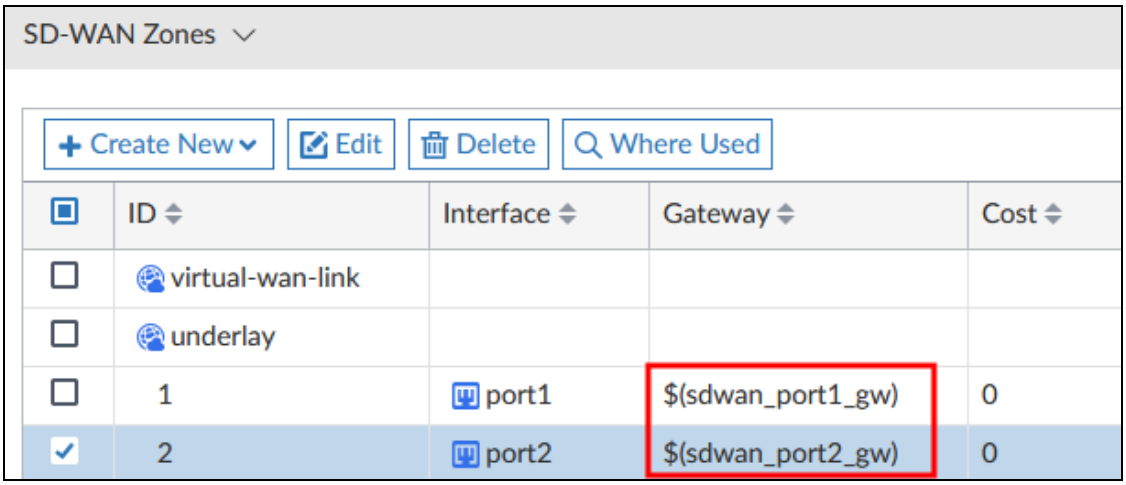
Field	Value
Name	sdwan_port2_gw
Default Value	0.0.0.0
Per-Device Mapping	Expand this section, click **Create New**, and then configure the following settings: 1. In the **Mapped Device** field, select **branch1_fgt [global]**. 2. In the **Value** field, type `192.2.0.10`. 3. Click **OK** to save the settings. Click **Create New**, and then configure the following settings: 1. In the **Mapped Device** field, select **branch2_fgt [global]**. 2. In the **Value** field, type `203.0.113.10`. 3. Click **OK** to save the settings.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



After you complete the procedure for the port1 and port2 gateways, the **SD-WAN Zones** section of your template should look similar to the following example:



11. Click **OK** to save the template settings.

> **Stop and think!**
>
> Do you need to configure metadata variables?
>
> You don't. Your underlay members are configured as DHCP clients, and the member gateway setting was configured for automatic detection. As a result, gateway detection was already working on branch1_fgt, and would have also worked on branch2_fgt. However, it is important to know how to use metadata variables in case the members require manual configuration.

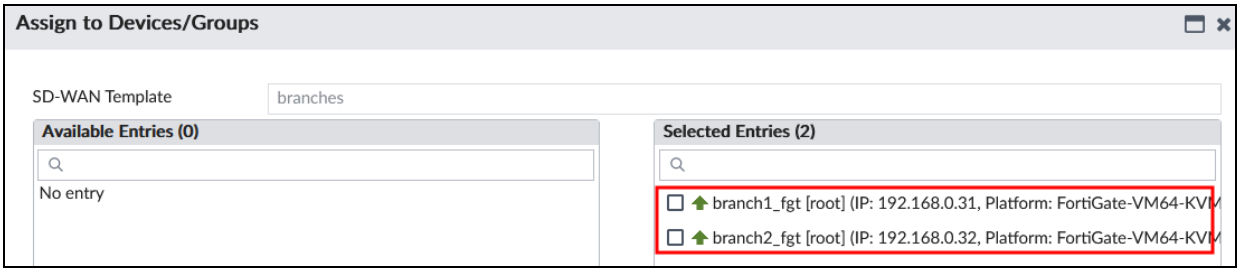
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To configure branch1_fgt and branch2_fgt as targets for the SD-WAN template

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
2. Select the checkbox for the **branches** template, and then click **Assign to Device/Group**.

3. In the **Available Entries** section, move **branch1_fgt** and **branch2_fgt** to the **Selected Entries** section.



4. Click **OK** to save the settings.

Review and Create Metadata Variables

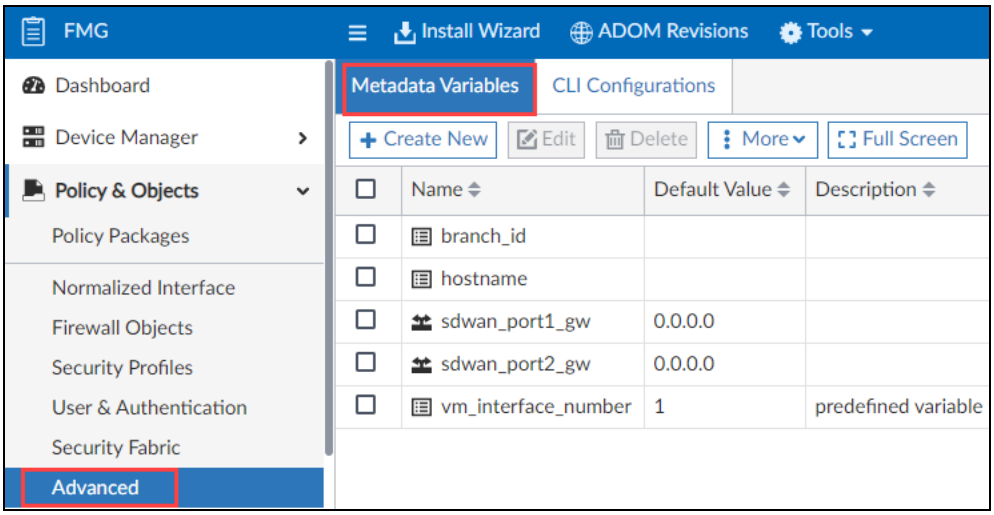
You can create metadata variables by typing $ in any field that has a magnifying glass, as you did to create **sdwan_port1_gw**. You can also review, edit, and create metadata variables in the ADOM object configuration menu or import them from a CSV or JSON file.

To review, edit, and update metadata variables

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Advanced**.
2. Click **Metadata Variables**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



On this page, you can review and manage the metadata variables that you created, or create new variables.

The **vm_interface_number** metadata variable is predefined on every FortiManager. The **branch_id** variable and host name have been predefined for you.

3. Double-click **hostname**.
4. Expand the **Per-Device Mapping** section, and then click **Create New**.
5. Create the following mapping:

Field	Value
Mapped Device	branch1_fgt [global]
Value	branch1_fgt

6. Click **OK**.
7. Repeat steps 4-6 to create a mapping with the following values:

Field	Value
Mapped Device	branch2_fgt [global]
Value	branch2_fgt

8. Click **OK**.

To import metadata variables from a CSV file

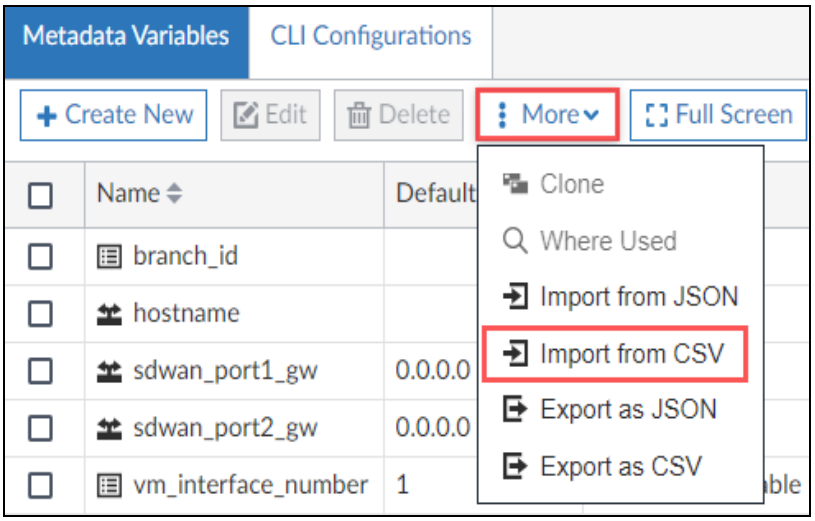
1. Connect to the Local-Client VM, and then log in with the following credentials:
   - Username: `Administrator`
   - Password: `password`
2. Open Firefox, and then enter `https://192.168.0.15` to connect to the FortiManager GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Alternatively, you can click the **fmg** bookmark.

3. Log in to the FortiManager GUI with the following credentials:
   - Username: `admin`
   - Password: `password`
4. Click **Policy & Objects** > **Advanced** > **Metadata Variables**.
5. Click **More**, and then select **Import from CSV**.



6. Click **Add Files**.
7. Navigate to **Desktop** > **Resources** > **SD-WAN**, and then select the `metadata_variables.csv` file.
8. Click **Open**.

The CSV file has been prepared for you. It defines the per-device values for the `branch_id` metadata variable and defines other metadata variables that you will use throughout the lab exercises.

The following image shows an example of a metadata variable CSV file that defines values for two devices, `branch1_fgt` and `branch2_fgt`. It is presented as a table to make it easier to read.

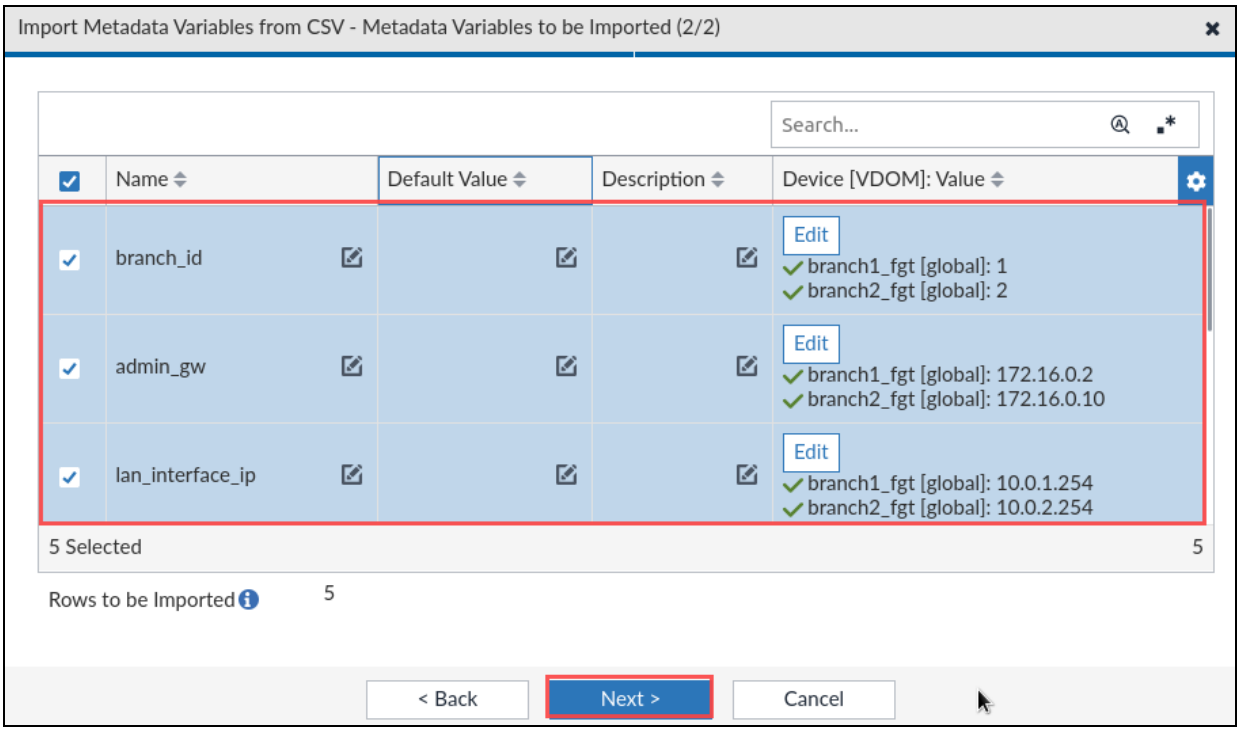
variable_name	default_value	description	device	VDOM	mapped_value
branch_id			branch1_fgt		1
branch_id			branch2_fgt		2
lan_interface_ip			branch1_fgt		10.0.1.254
lan_interface_ip			branch2_fgt		10.0.2.254

FortiManager prompts you to review the metadata variables that will be updated or created.

Your page should look similar to the following example:

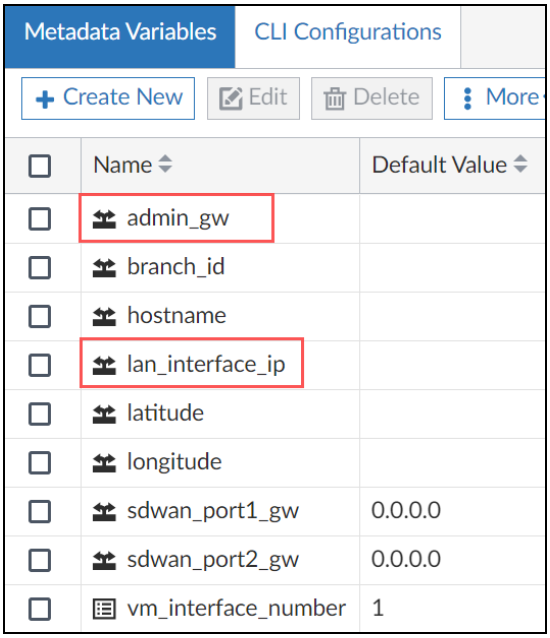
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



9. Review the output, and then click **Next**.

   FortiManager creates metadata variables, such as **lan_interface_ip** and **admin_gw**, and updates the per-device mapping for these variables and the **branch_id** variable.

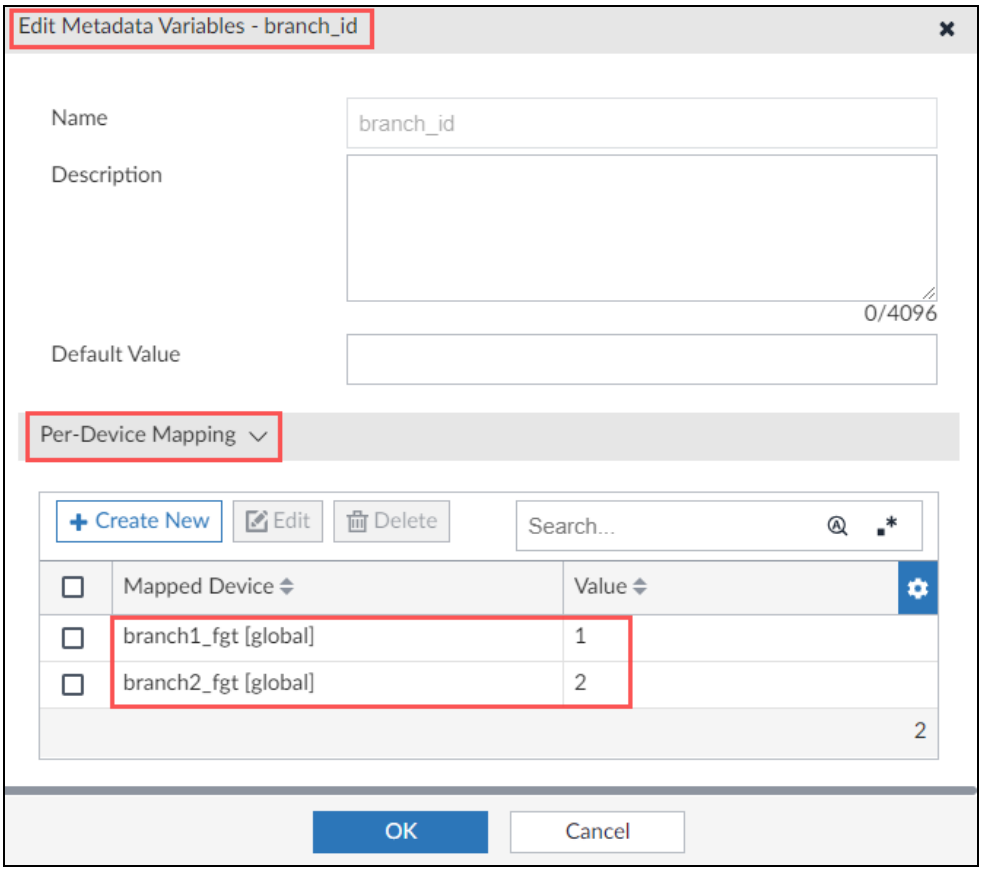


10. Double-click the **branch_id** variable, and then review the settings.

    FortiManager defined the per-device mapping for branch1_fgt and branch2_fgt.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



11. Click **Cancel**.

Use the **Import from CSV** and **Import from JSON** features, and the corresponding export features, **Export as CSV** and **Export as JSON**, to easily define new metadata variables and the corresponding per-device mapping.

Configure the Device Settings and Policy Package

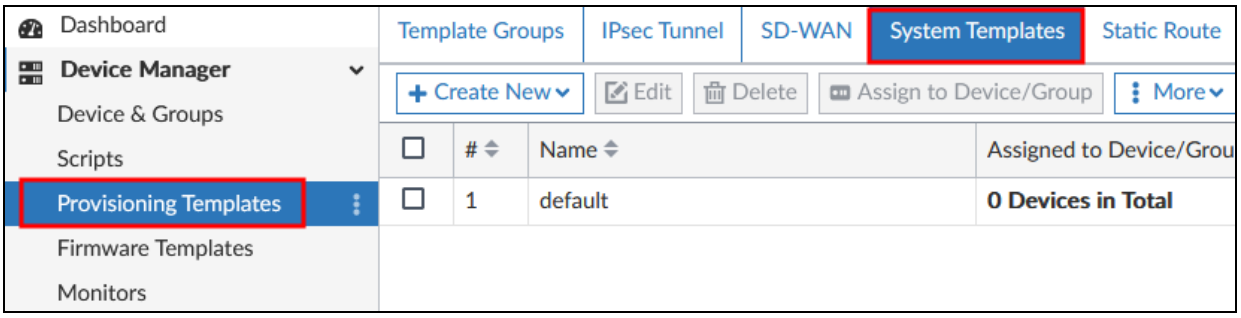
First, you will configure a system template for enabling FortiAnalyzer logging on both branch1_fgt and branch2_fgt. Next, you will configure a static route template by importing existing static routes from branch1_fgt, and then you will assign the template to both branch1_fgt and branch2_fgt. Next, you will edit a firewall address object for branch2_fgt. Finally, you will add branch2_fgt as a target for the **branches_pp** policy package you imported from branch1_fgt.

To configure device administrative settings and FortiAnalyzer logging

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **System Templates**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

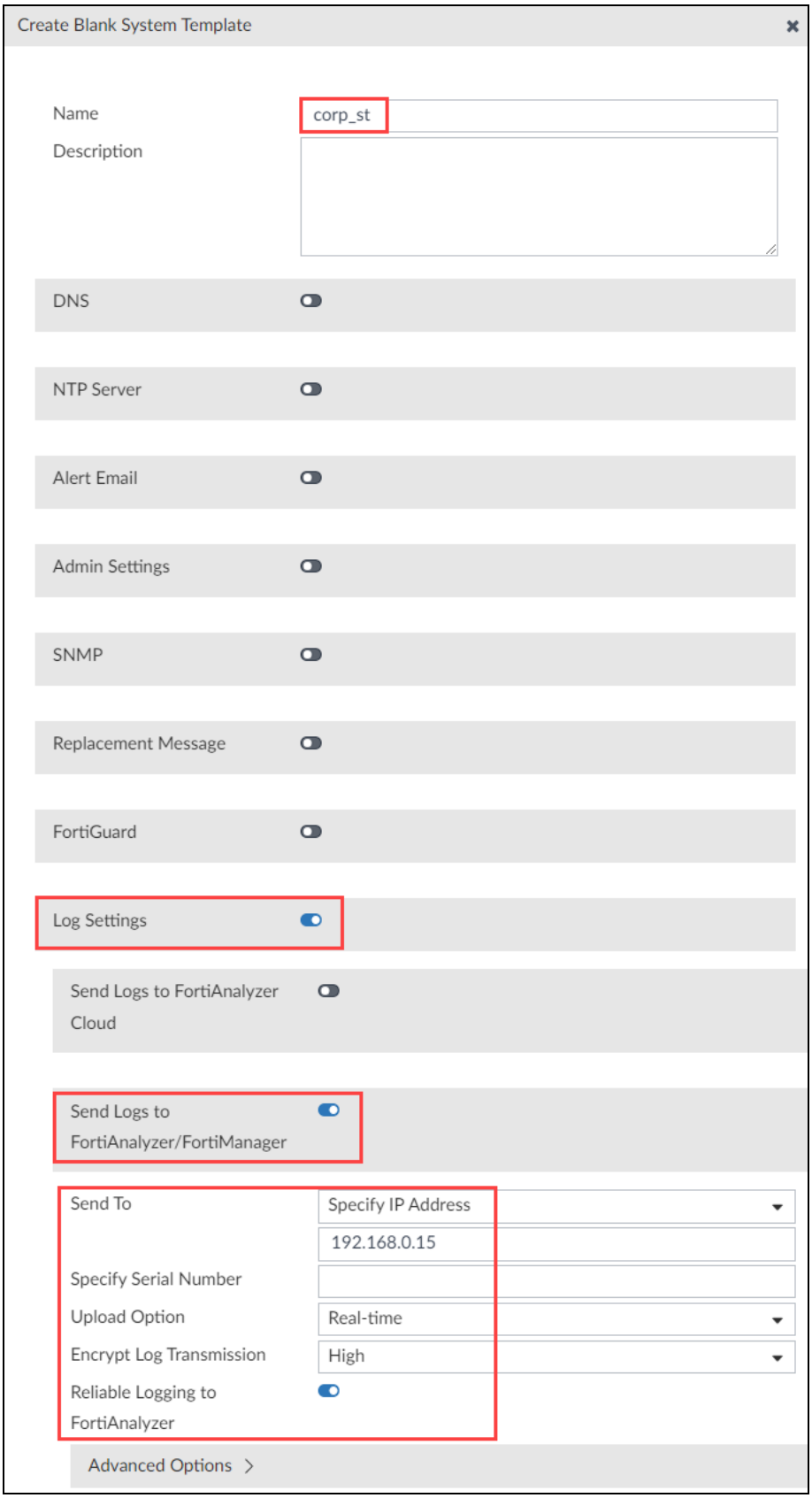


2. Click **Create New** > **Blank Template**.
3. In the **Name** field, type `corp_st`.
4. Enable **Log Settings**, and then enable the second setting, which is **Send Logs to FortiAnalyzer/FortiManager**.
5. Configure the following settings:

Field	Value
Send to	Select **Specify IP Address**, and then type `192.168.0.15`.
Upload Option	Real-time
Encrypt Log Transmission	High
Reliable Logging to FortiAnalyzer	Enabled

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



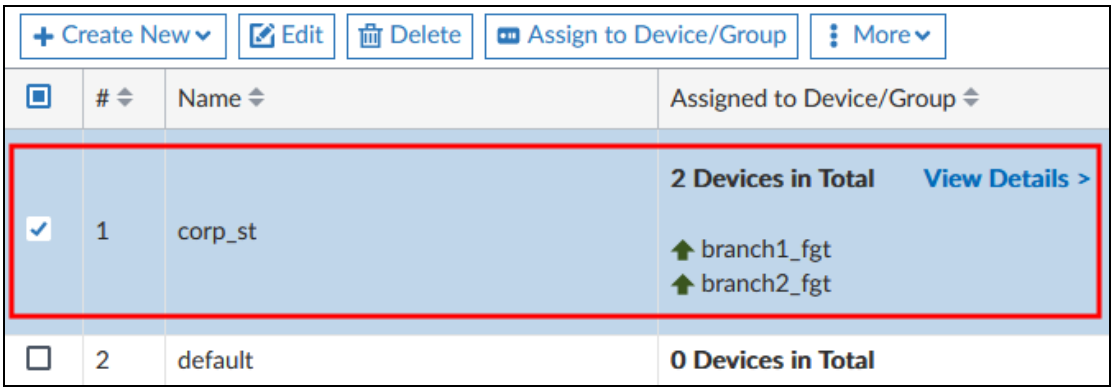
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Do *not* enable **Send Logs to FortiAnalyzer Cloud**. In this lab, you are using FortiAnalyzer features on the local FortiManager, so you *must* enable **Send Logs to FortiAnalyzer/FortiManager**.

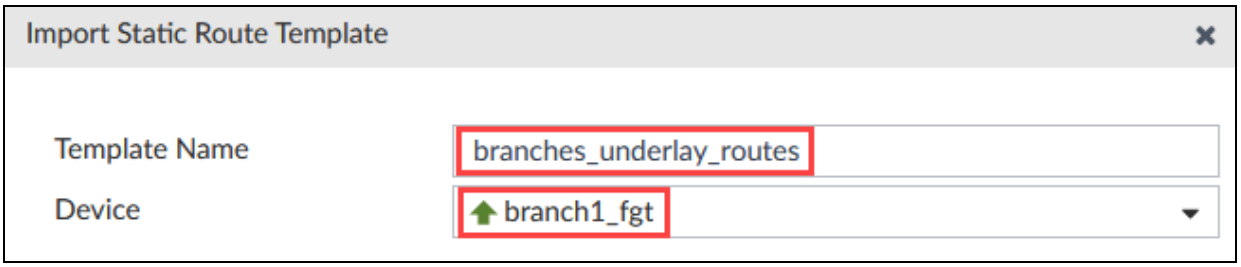
6. Click **OK** to create the template and save the settings.
7. Click **Provisioning Templates** > **System Templates**.
8. Select **corp_st**, and then click **Assign to Device/Group**.
9. Move **branch1_fgt** and **branch2_fgt** to the **Selected Entries** list.
10. Click **OK** to save the settings.

    Your page should look similar to the following example:



To configure a static route template

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **Static Route**.
2. Click **More**, and then click **Import**.
3. In the **Template Name** field, type `branches_underlay_routes`.
4. In the **Device** field, select **branch1_fgt**.

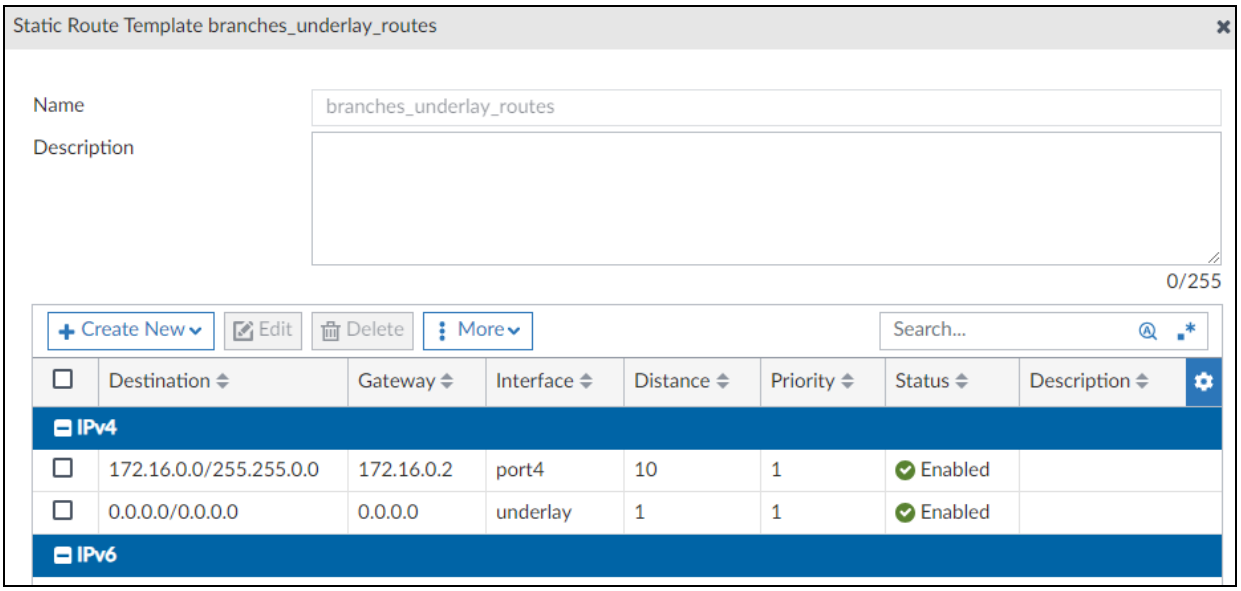


5. Click **OK**.
6. Edit the **branches_underlay_routes** template that you created.

    Your output should look similar to the following image:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



The template contains the two static routes that are defined on branch1_fgt. The first route connects the device to the lab management network and the second route corresponds to the static route you defined in Lab 1.

7. Edit the route to **172.16.0.0/255.255.0.0**, and then in the **Gateway Address** field, type `$` to replace the address.
8. Select the **admin_gw** metadata variable, which you defined in a previous procedure, when you imported the metadata CSV file.
9. Click **OK** to validate the route update.
10. Click **OK** to validate the template update.
11. Select **branches_underlay_routes**, and then click **Assign to Device/Group**.
12. Move **branch1_fgt** and **branch2_fgt** to the **Selected Entries** list.
13. Click **OK**.

To edit the firewall address object

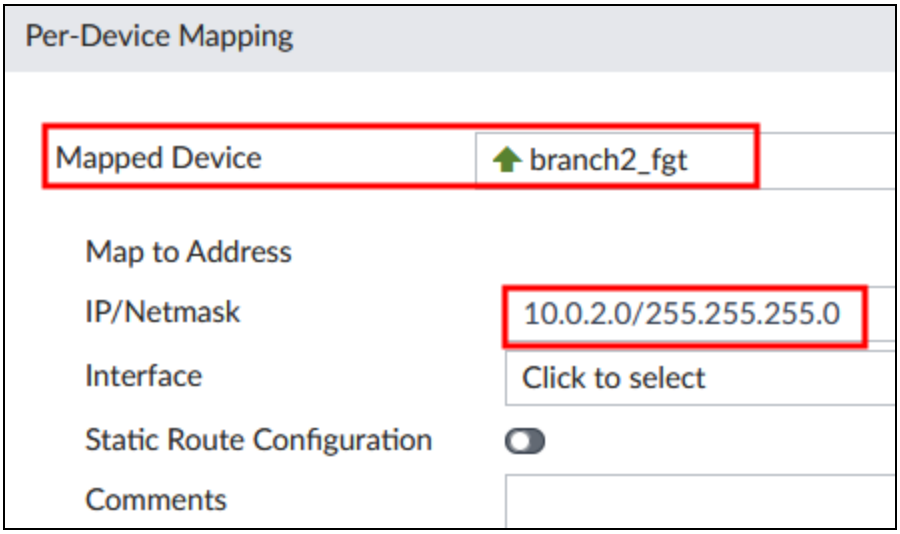
1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Firewall Objects**.
2. Click **Addresses**.
3. Double-click the **LAN-net** address object, and then configure the following settings:

Field	Value
Per-Device Mapping	Expand this section.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Mapped Device	Click **Create New**, and then configure the following settings: 1. In the **Mapped Device** field, select **branch1_fgt**. 2. In the **Map to Address IP/Netmask** field, type `10.0.1.0/24`. 3. Click **OK** to save the settings. Click **Create New** again, and then configure the following settings: 1. In the **Mapped Device** field, select **branch2_fgt**. 2. In the **Map to Address IP/Netmask** field, type `10.0.2.0/24`. 3. Click **OK** to save the settings.



4. Click **OK** to save the settings.

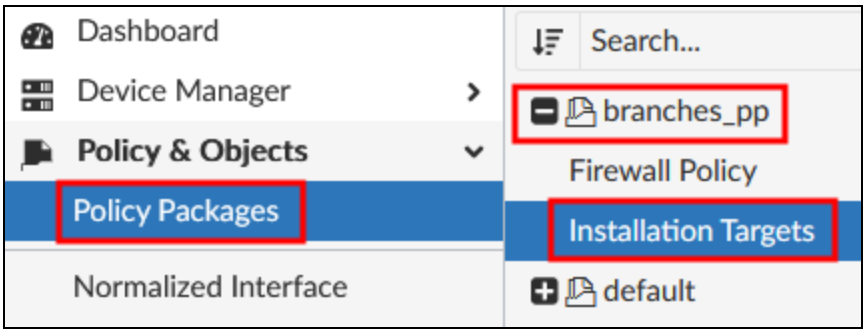
LAN-net is now a dynamic firewall address object. You added a per-device mapping rule that FortiManager uses when it pushes the object to the managed devices. The goal is for FortiManager to use the correct value based on the target device.

To add branch2_fgt as a policy package target

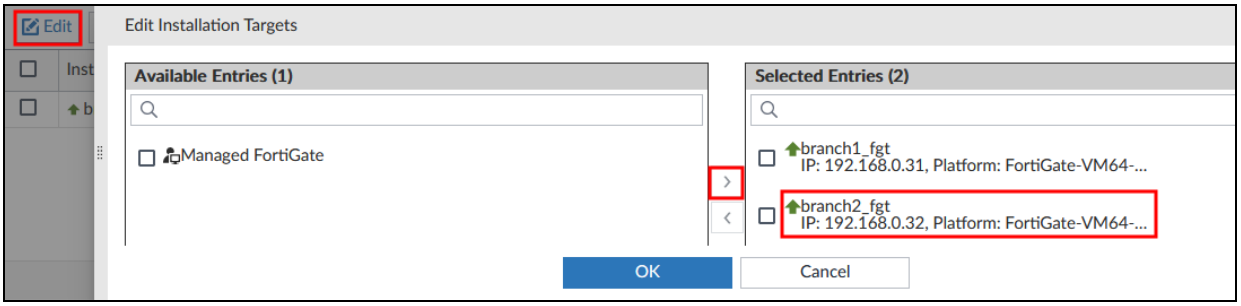
1. Continuing on the FortiManager GUI, click **Policy Packages**, expand **branches_pp**, and then click **Installation Targets**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

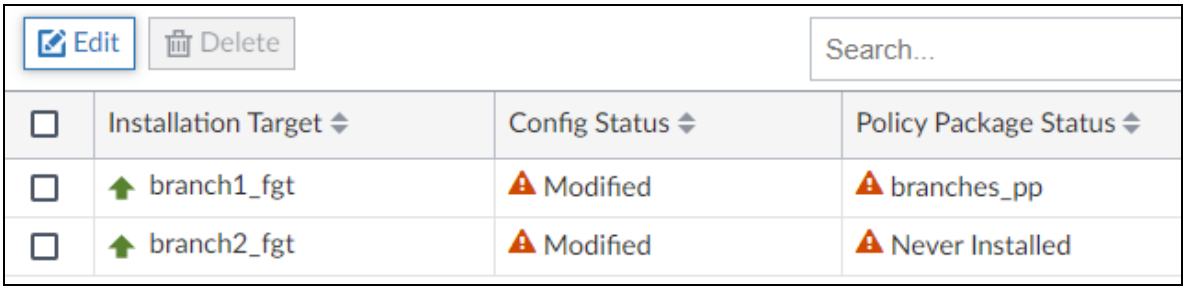
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



2. Click **Edit**, and then move **branch2_fgt** to the **Selected Entries** list.



3. Click **OK** to save the settings.
   Your page should look similar to the following example:



Install the Device Settings and Policy Package

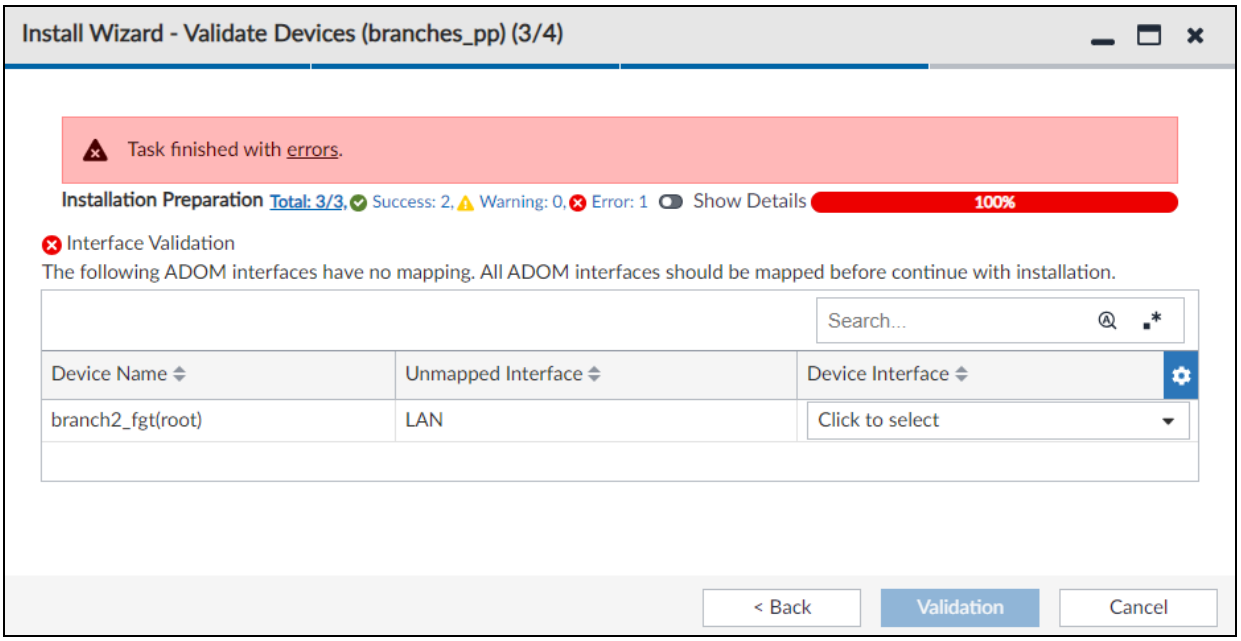
You will install the device settings and policy package on both branch1_fgt and branch2_fgt.

To install the device settings and policy package

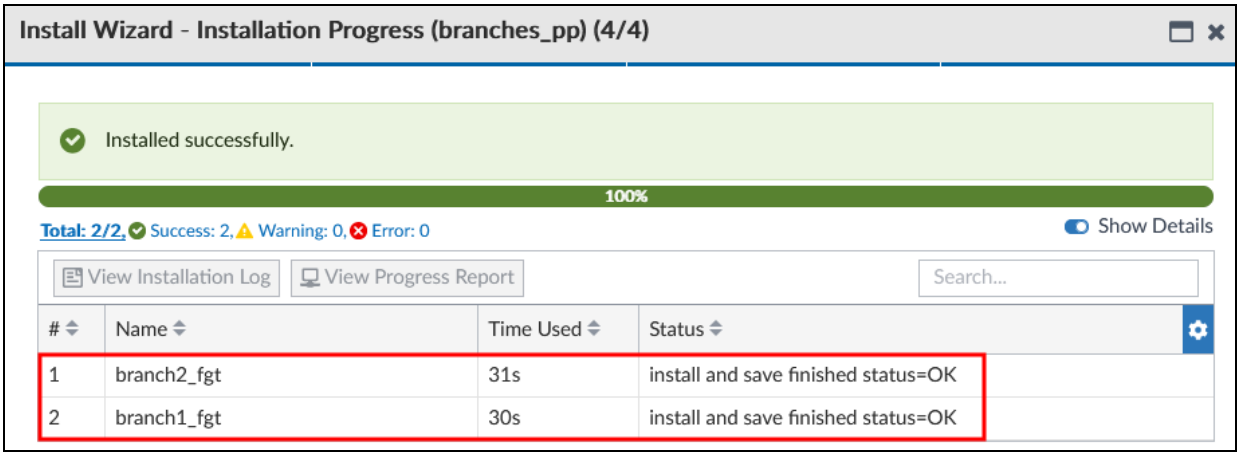
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Policy Package & Device Settings**, and then in the **Policy Package** field, select **branches_pp**.
3. Click **Next**.
4. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
   After a few seconds, FortiManager shows an **Interface Validation** message similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



5. In the **Device Interface** field, select **port5**, and then click **Validation**.
6. Wait for the new validation to complete, and then click **Install** to install the configuration on both devices.
7. Wait for the installation to finish.
   Your page should look similar to the following example:



8. Click **Finish**.

Verify Installed Settings and Logging

You will verify installed settings on branch1_fgt and branch2_fgt by connecting to them over SSH. After that, you will verify that FortiManager is receiving logs from branch1_fgt and branch2_fgt.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To verify installed settings on branch1_fgt and branch2_fgt

1. Open an SSH session to branch1_fgt, and another to branch2_fgt.
2. Log in to the FortiGate CLI with the following credentials:
   - Username: `admin`
   - Password: `password`
3. Enter the following commands on both branch1_fgt and branch2_fgt to verify that the configuration was installed:

```
show system sdwan
show firewall policy
show firewall address LAN-net
show router static
```

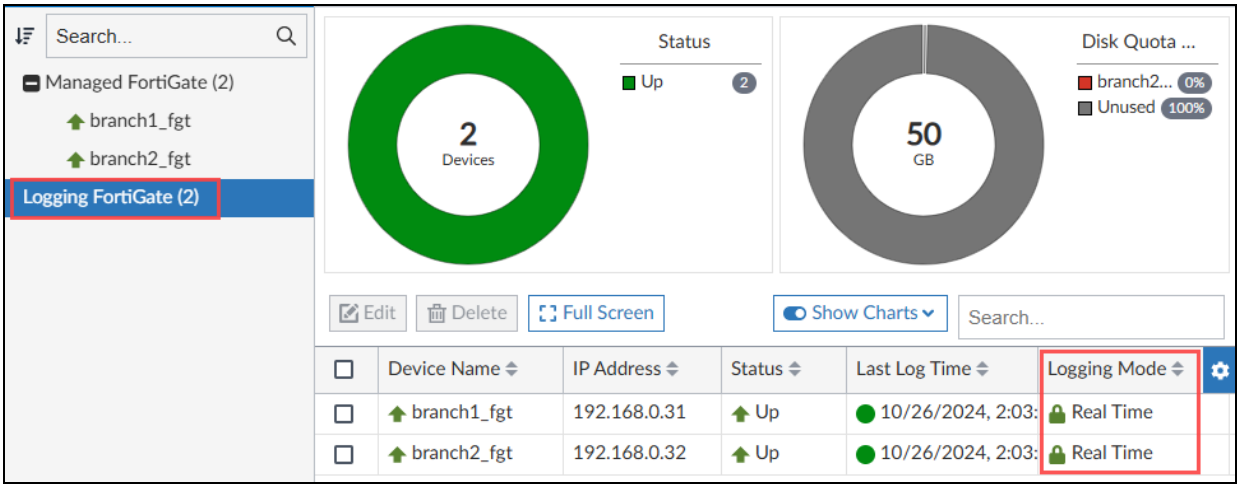
FortiManager included a note to identify the static route that was created with a template.

```
set comment "[ [Created by Static Route Template: branches_
underlay_routes]"
```

The template set the distance for this static route to 1. This is the default distance for static routes through an SD-WAN zone. By default, FortiGate set a distance of 1 for static routes over SD-WAN zones to prioritize them over static routes through individual interfaces (default distance of 10).

To verify logging to FortiAnalyzer (FortiManager)

1. Continuing on the FortiManager GUI, click **Device Manager** > **Device & Groups**.
2. Click **Logging FortiGate**.
   Your page should look similar to the following example:



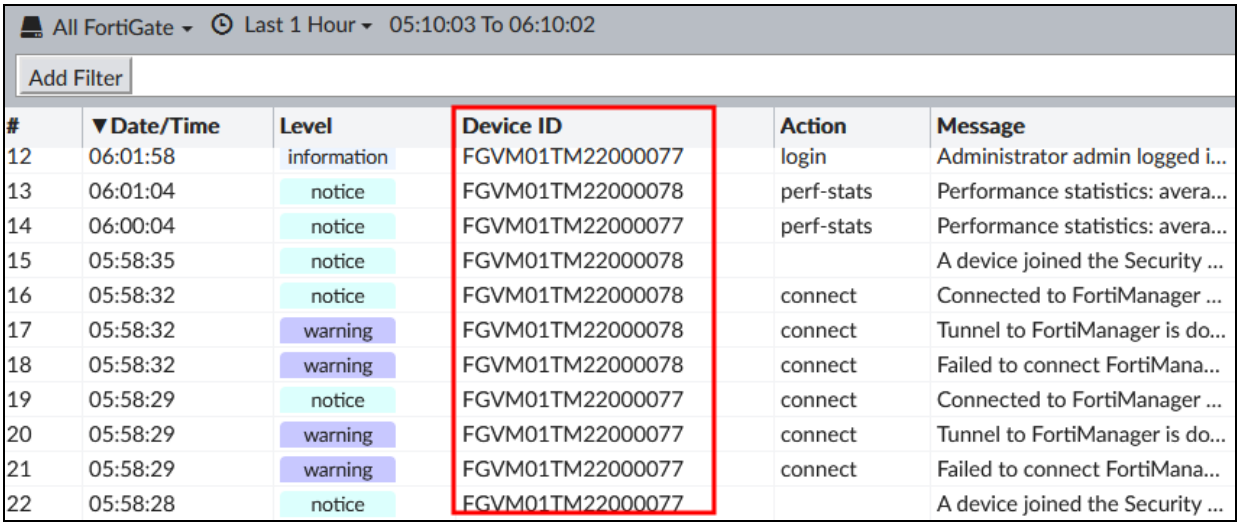
You can drag and drop the columns to reorder them.

The green lock beside **Real Time** indicates that FortiManager is receiving logs from the managed devices and that encrypted log transmission is enabled.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

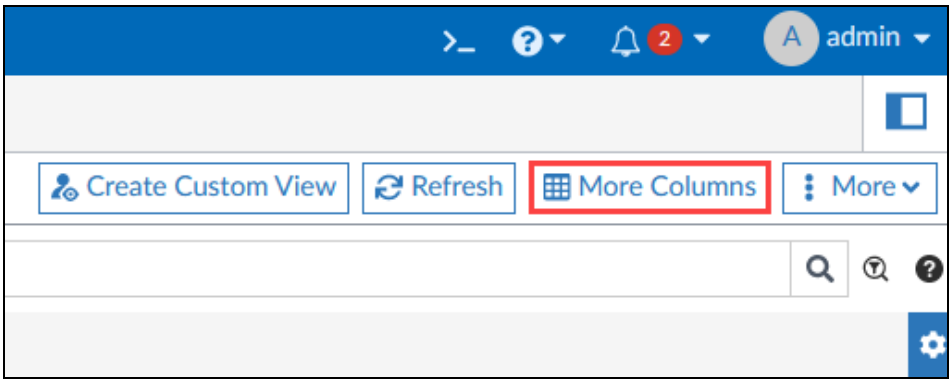
3. Click **Log View**, and then click **Event** > **All Types**.
   Your page should look similar to the following example:



#	▼Date/Time	Level	Device ID	Action	Message
12	06:01:58	information	FGVM01TM22000077	login	Administrator admin logged i...
13	06:01:04	notice	FGVM01TM22000078	perf-stats	Performance statistics: avera...
14	06:00:04	notice	FGVM01TM22000077	perf-stats	Performance statistics: avera...
15	05:58:35	notice	FGVM01TM22000078		A device joined the Security ...
16	05:58:32	notice	FGVM01TM22000078	connect	Connected to FortiManager ...
17	05:58:32	warning	FGVM01TM22000078	connect	Tunnel to FortiManager is do...
18	05:58:32	warning	FGVM01TM22000078	connect	Failed to connect FortiMana...
19	05:58:29	notice	FGVM01TM22000077	connect	Connected to FortiManager ...
20	05:58:29	warning	FGVM01TM22000077	connect	Tunnel to FortiManager is do...
21	05:58:29	warning	FGVM01TM22000077	connect	Failed to connect FortiMana...
22	05:58:28	notice	FGVM01TM22000077		A device joined the Security ...

Serial numbers (**Device ID** column) of managed devices may be different in your lab.

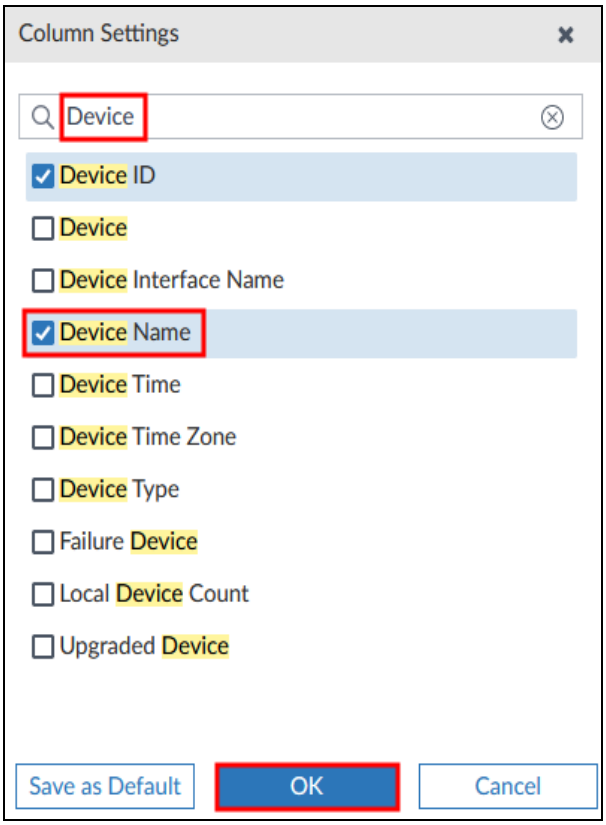
4. In the upper-right corner, click the column setting icon.
   The page display may differ according to your screen size.



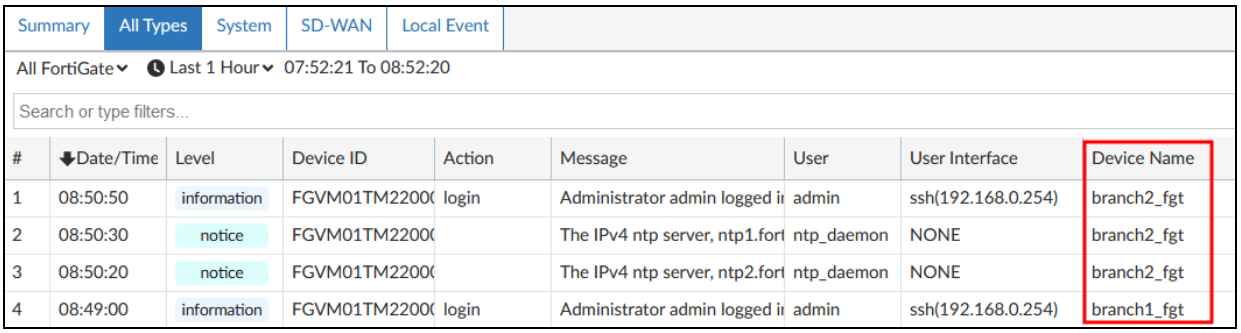
5. In the search box, type `Device`, and then in the list, select the **Device Name** checkbox.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



6. Click **OK** to save the settings.
   Your page should look similar to the following example:



#	Date/Time	Level	Device ID	Action	Message	User	User Interface	Device Name
1	08:50:50	information	FGVM01TM2200	login	Administrator admin logged i	admin	ssh(192.168.0.254)	branch2_fgt
2	08:50:30	notice	FGVM01TM2200		The IPv4 ntp server, ntp1.fort	ntp_daemon	NONE	branch2_fgt
3	08:50:20	notice	FGVM01TM2200		The IPv4 ntp server, ntp2.fort	ntp_daemon	NONE	branch2_fgt
4	08:49:00	information	FGVM01TM2200	login	Administrator admin logged i	admin	ssh(192.168.0.254)	branch1_fgt

The logs now include the device name for easier identification.

You can drag and drop the columns to reorder them.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Monitoring DIA Traffic on FortiManager

In this exercise, first, you will generate internet traffic from branch1_client and branch2_client and trigger a failure of port1 on branch1_fgt. Next, you will monitor DIA traffic distribution and logs using the SD-WAN tools that are available on FortiManager.

Generate Internet Traffic and Trigger an Interface Failure

You will generate internet traffic from branch1_client and branch2_client using the traffic generator tool.

To generate internet traffic from branch1_client and branch2_client

1. Open an SSH session to branch1_client.
2. Log in with the following credentials:
   - Username: `root`
   - Password: `password`
3. Enter the following commands:
   ```
   cd /fortipoc/traffic/
   ./trafficgenerator.sh
   ```
   Your output shows a turning progress bar.
4. Repeat the previous steps on branch2_client.

To bring down port1 on branch1_fgt

1. Connect to the WAN simulator HTTP interface, and then locate **BR1-ISP1**.
2. Click **DOWN** to bring down the link on port1 on branch1_fgt.

Monitor DIA Traffic Distribution

You will use the SD-WAN monitor on FortiManager to monitor the DIA traffic distribution on both devices.

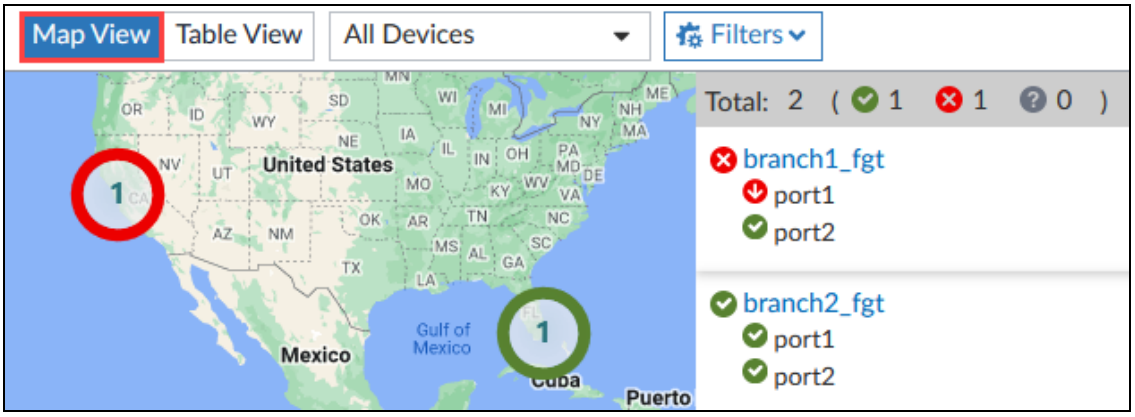
To monitor DIA traffic distribution

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

2. Click **Device Manager** > **Monitors**, and then click **SD-WAN Monitor** > **Map View**.
   Your page should look similar to the following example:

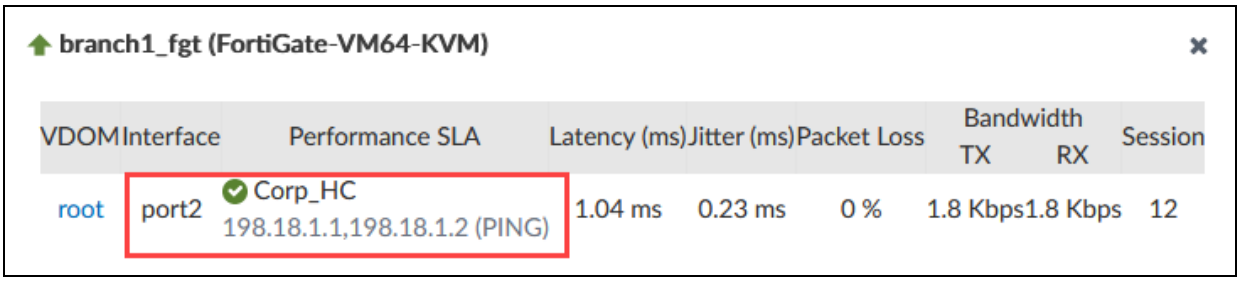


FortiManager takes 10–30 seconds to load the map the first time you display this page.

branch1_fgt and branch2_fgt are located in Sunnyvale and Miami, respectively.

You may need to zoom out before you can see the managed devices on the map.

3. Hover over the icons beside the port name on both branch1_fgt and branch2_fgt.
   A new window opens and displays additional details for each port. The following image shows an example of port2 on branch1_fgt:



branch1_fgt (FortiGate-VM64-KVM)

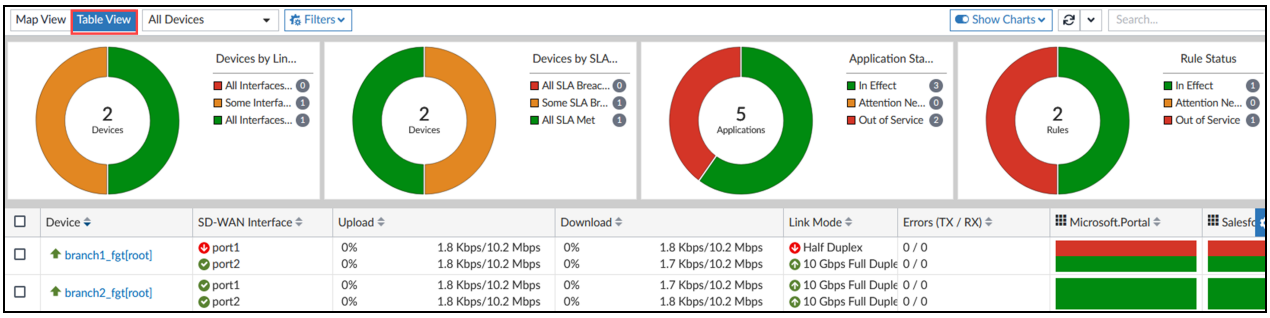
VDOM	Interface	Performance SLA	Latency (ms)	Jitter (ms)	Packet Loss	Bandwidth TX	Bandwidth RX	Session
root	port2	Corp_HC 198.18.1.1,198.18.1.2 (PING)	1.04 ms	0.23 ms	0 %	1.8 Kbps	1.8 Kbps	12

Some browsers requires you to place the mouse exactly on the interface status icon (green or red circle) to view the interface statistics.

4. Click **Table View**.
   Your page should look similar to the following example:

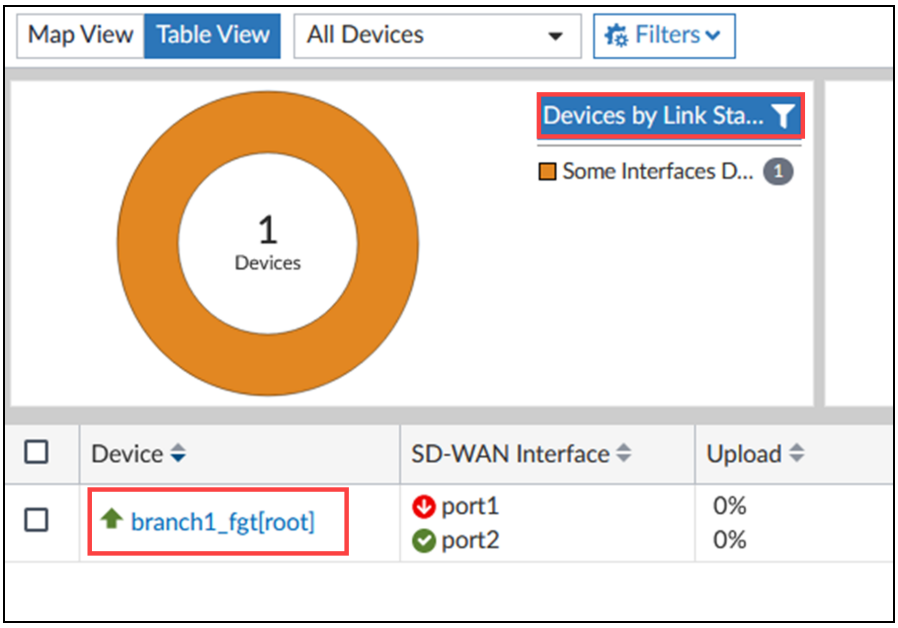
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



5. On the first circle graph, **Devices by Link Status**, click the orange part of the graph.
   This sets the corresponding filter. The table now displays only devices that have some interfaces down.

   Your output should look similar to the following image:



6. Click the filter icon to remove it.
7. In the device list table, check the **Upload** and **Download** values.

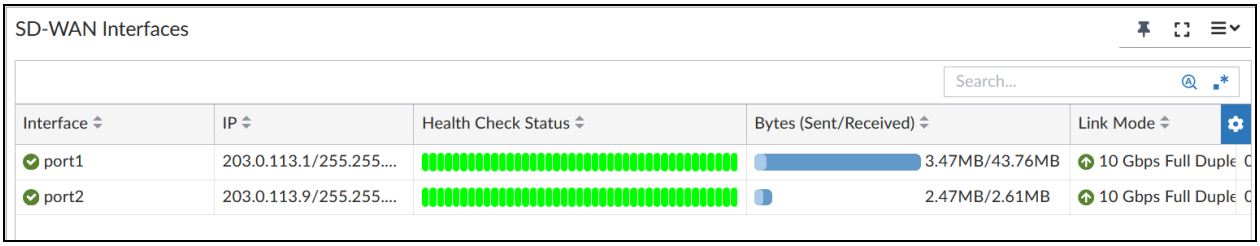
> **Stop and think!**
>
> The port details show that bandwidth is utilized, and that the member has active sessions. However, the upload and download utilization bars show 0% for both FortiGate devices.
>
> Why?
>
> The usage percentage that appears on the bars is calculated based on the `estimated-upstream-bandwidth` and `estimated-downstream-bandwidth` settings, which you haven't configured yet. Because those settings are not configured, FortiManager doesn't know the bandwidth capacity of the ports, and therefore, cannot determine the usage percentage.

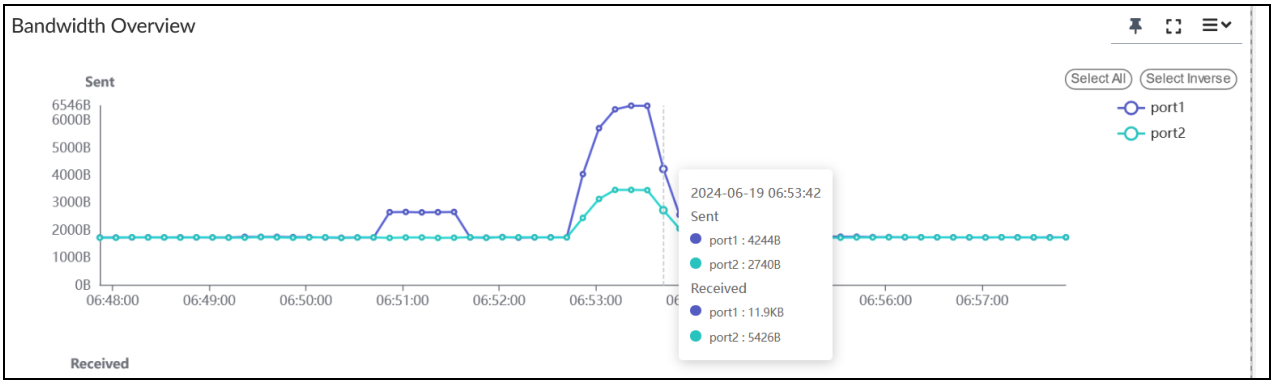
8. Click **branch2_fgt** to view more details about the device.
9. Scroll down the page to view the graphs and tables that are available.
10. Hover over the graphs to see additional details.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Your page should look similar to the following example. Note that you might need to scroll down to see the second graph.





The page shows the health check status for port1 and port2, the status of all configured SD-WAN rules on branch2_fgt, and their preferred members. The page also indicates the speed and amount of traffic measured on each port.

You can hover over the graphs to view more details.

Note that, by default, FortiManager stores SD-WAN statistics over 10 minutes. If you want to keep data over a longer period of time, you must enable this feature by entering the following commands:

```
config system admin setting
   set sdwan-monitor-history enable
end
```

When you enable extended statistic storage, by default FortiManager stores the statistics for 180 days. This can quickly fill up the disk storage capacity. You can adjust the data retention duration with the following commands:

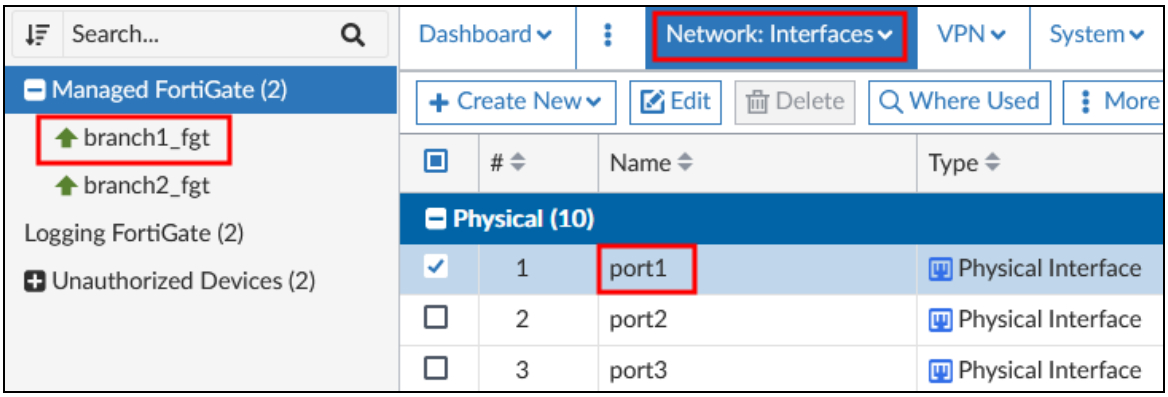
```
config system admin setting
   set rtm-max-monitor-by-days <nb of days>
end
```

To configure the estimated bandwidth settings

1. Continuing on the FortiManager GUI, click **Device Manager** > **Device & Groups**, expand **Managed FortiGate**, and then click **branch1_fgt**.
2. Click **Network** > **Interfaces**, and then in the **Physical** section, double-click **port1** to edit the port settings.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

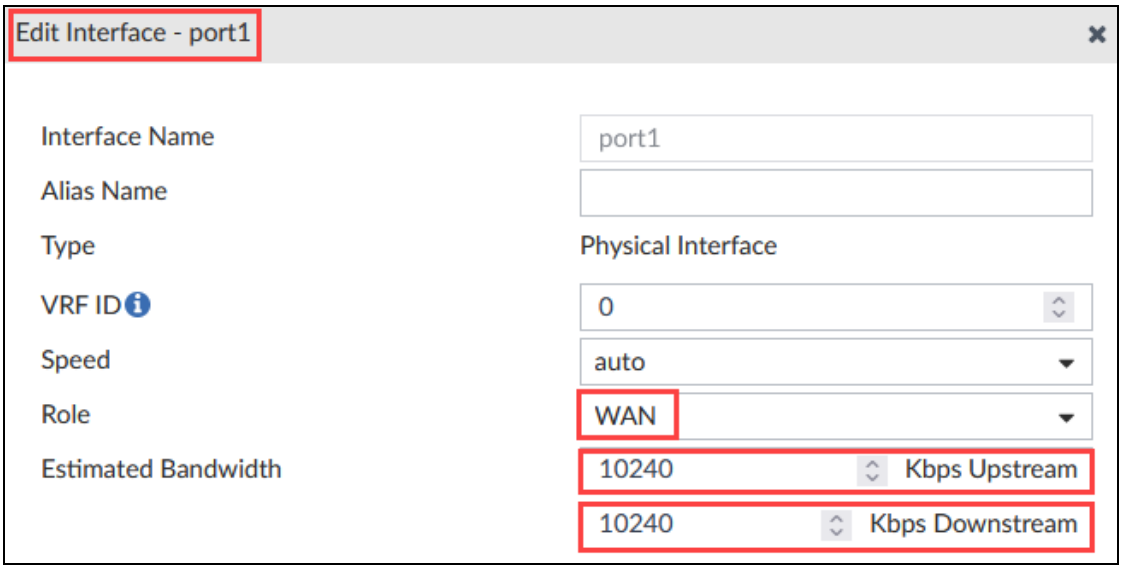


3. Configure the following settings:

Field	Value
Role	WAN
Estimated Bandwidth	In both the **Kbps Upstream** and **Kbps Downstream** fields, type `10240`.

You can set the estimated bandwidth only for WAN interfaces. Therefore, you must set the interface role before you can see the **Kbps Upstream** and **Kbps Downstream** fields.

The ports can handle more than 10 Mbps bandwidth, but you will use a lower bandwidth value for now, so it's easier to see the change in the usage percentage.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

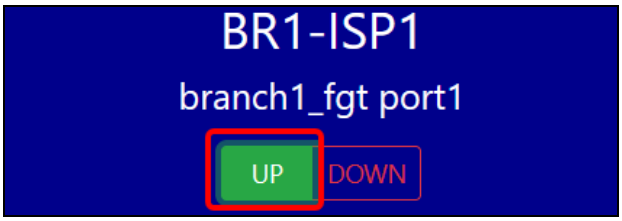
4. Click **OK** to save the settings.
5. Repeat the previous steps to configure the estimated bandwidth values on port2 on branch1_fgt, and on port1 and port2 on branch2_fgt—use `10240` Kbps for all ports.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on all devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To bring up port1

1. Continuing on the WAN simulator HTTP interface, scroll up and locate **BR1-ISP1**.
2. Click **UP** to bring up the link on port1 on branch1_fgt.



To monitor member bandwidth utilization

Take the Expert Challenge!

Use the FortiManager SD-WAN monitor to confirm that port1 and port2 on branch1_fgt and branch2_fgt now show a usage percentage. For example:

Device	SD-WAN Interface	Upload		Download	
branch1_fgt[root]	port1	0%	1.8 Kbps/10.2 Mbps	0%	1.8 Kbps/10.2 Mbps
	port2	24%	2.4 Mbps/10.2 Mbps	2430%	248.8 Mbps/10.2 Mbps
branch2_fgt[root]	port1	0%	1.8 Kbps/10.2 Mbps	0%	1.8 Kbps/10.2 Mbps
	port2	0%	1.8 Kbps/10.2 Mbps	0%	1.8 Kbps/10.2 Mbps

If you require assistance, or to verify your work, review the procedure described earlier in this exercise.

FortiGate calculates the upload and download percentage by comparing the actual upload and download speed and the estimated bandwidth configured for the interface. In this exercise, you configured an estimated bandwidth that is lower than the actual link capability. This is why you can see percentages that are above 100%.

1. If you want to generate additional traffic, you can connect to branch1_client, and then enter the following command:
```
wget http://128.66.0.1/files/linix.iso
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

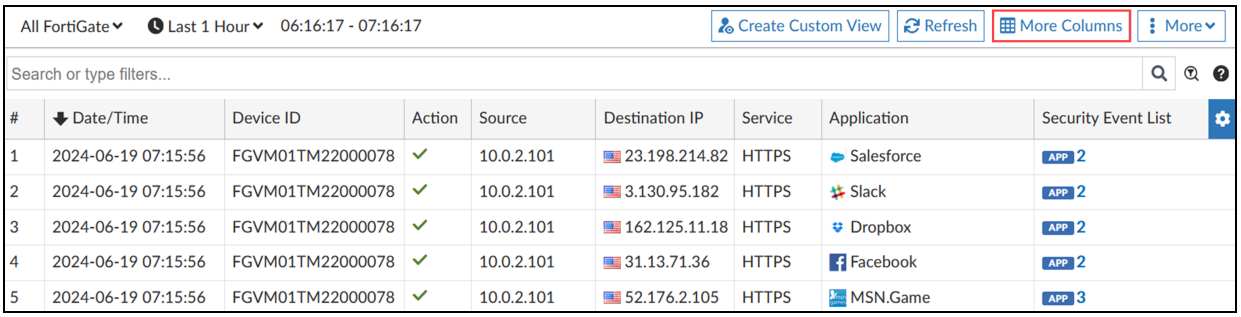
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

View Traffic Logs

You will view the traffic logs on FortiAnalyzer (feature activated on FortiManager) to confirm SD-WAN is steering traffic on both branch1_fgt and branch2_fgt.

To view SD-WAN traffic logs

1. Continuing on the FortiManager GUI, click **Log View**, and then click **Traffic**.
   Your page should look similar to the following example:



#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Security Event List
1	2024-06-19 07:15:56	FGVM01TM22000078	✓	10.0.2.101	23.198.214.82	HTTPS	Salesforce	APP 2
2	2024-06-19 07:15:56	FGVM01TM22000078	✓	10.0.2.101	3.130.95.182	HTTPS	Slack	APP 2
3	2024-06-19 07:15:56	FGVM01TM22000078	✓	10.0.2.101	162.125.11.18	HTTPS	Dropbox	APP 2
4	2024-06-19 07:15:56	FGVM01TM22000078	✓	10.0.2.101	31.13.71.36	HTTPS	Facebook	APP 2
5	2024-06-19 07:15:56	FGVM01TM22000078	✓	10.0.2.101	52.176.2.105	HTTPS	MSN.Game	APP 3

The serial numbers (**Device ID** column) of the managed devices may be different in your lab.

2. In the upper-right corner, click **More Columns**.
3. Select **Destination Interface**, **SD-WAN Quality**, and **SD-WAN Rule Name**.

Use the column settings search box to quickly find the columns.

4. Click **OK** to save the settings.
   Your page should look similar to the following example:

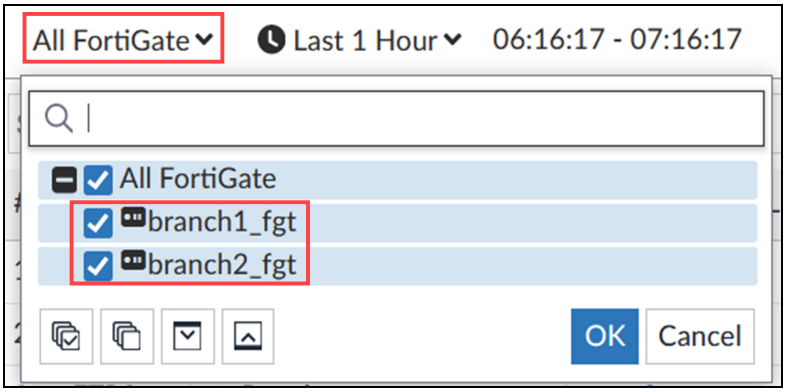
Application	Security Event List	Destination I	SD-WAN Quality	SD-WAN Rule Name
Salesforce	APP 2	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
Slack	APP 2	port1		
Dropbox	APP 2	port1		
Facebook	APP 2	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
MSN.Game	APP 3	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
Atlassian.Cloud	APP 2	port1		
Microsoft.Portal	APP 2	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

SD-WAN is steering traffic based on the detected application.

If you want to display logs for a specific device, in the upper-left corner, click **All FortiGate** to select the managed device you want to display logs for.



5. On branch1_client and branch2_client, press `Ctrl+C` to stop the traffic generator.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

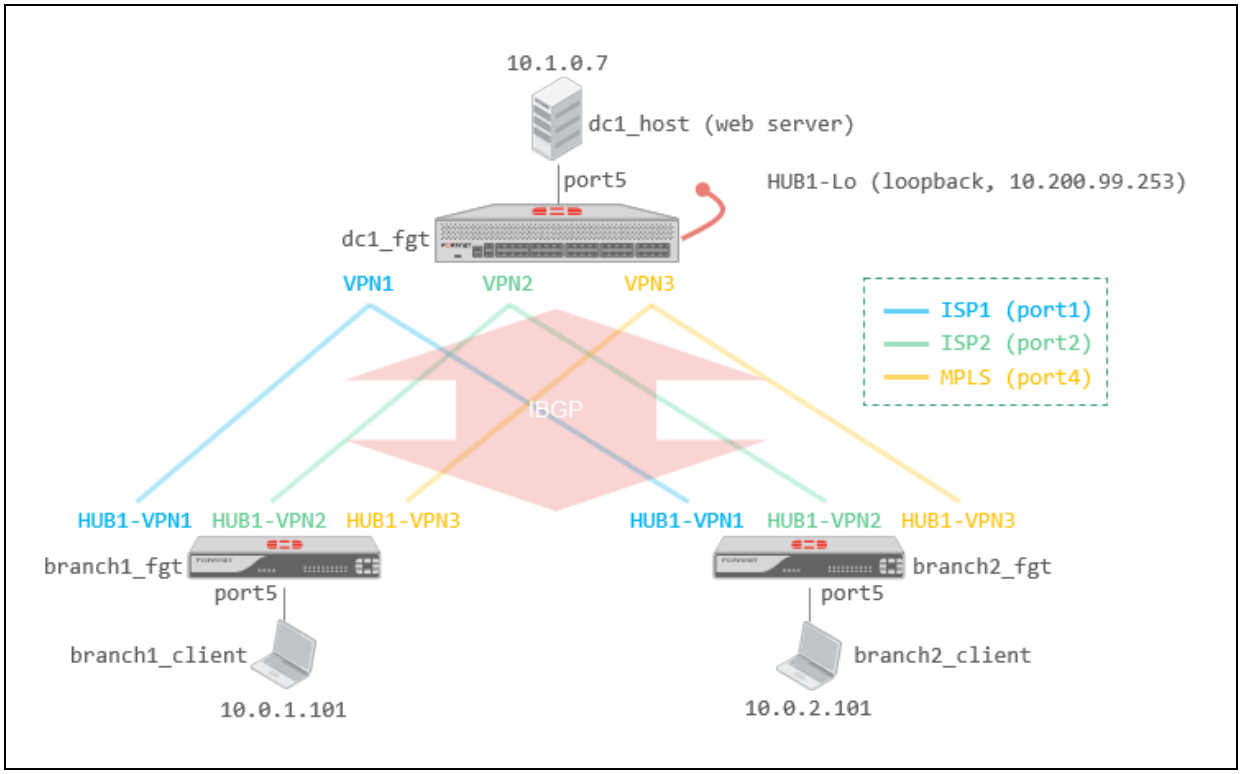
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 3: Configuring the Overlay With the SD-WAN Overlay Template

In this exercise, you will use the SD-WAN overlay template to configure IPsec VPN tunnels for the overlay and BGP for routing on the overlay. The template will guide you and prepare, with the elements you provide, a configuration that follows Fortinet recommendations. You will start from the configuration you reached at the end of the previous exercise:

- FortiManager manages branch1_fgt and branch2_fgt.
- SD-WAN is configured on branch1_fgt and branch2_fgt, with rules to steer the traffic over the underlay (port1 and port2).

The objective of this exercise is to configure the overlay and create the topology shown in the following diagram:



To keep things simple, administrative domains (ADOM) are not enabled on the FortiManager that you use for the lab exercises.

Remember that you can use multiple ADOMs on FortiManager to logically group the managed devices. However, all the devices that an SD-WAN overlay template configures must be in the same ADOM.

Additionally, you can configure multiple SD-WAN overlay templates per ADOM.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Add dc1_fgt to FortiManager

To use the SD-WAN overlay template, it is mandatory that the FortiManager manages the hub. Therefore, as a preliminary step, you will add the hub device, dc1_fgt, to FortiManager.

To add dc1_fgt to FortiManager

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Device & Groups**.
3. Click **Add Device**.

4. Click **Discover Device**, and then configure the following settings:

Field	Value
IP Address	192.168.0.41
Use legacy device login	Enabled
User Name	admin
Password	password

5. Click **Next**.
6. Review the details about the device discovered, and then click **Next**.
7. Wait until the **Add Device** task is completed, and then click **Import Now**.
8. Select **Import Policy Package**, and then click **Next**.
9. In the **Policy Package Name** field, type `dc_pp`, and then click **Next**.
10. If FortiManager prompts you about object conflicts, select **Use Value From FortiManager**, and then click **Next**.
11. Click **Next**.
12. Wait for the import task to complete, and then click **Finish**.
13. Click **Policy & Objects** > **Advanced** > **Metadata Variables**.
14. Double-click the **hostname** variable to edit it.
15. Configure the following settings to create a per-device mapping:

Field	Value
Mapped Device	dc1_fgt [global]
Value	dc1_fgt

16. Click **OK** to validate the metadata variable update.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

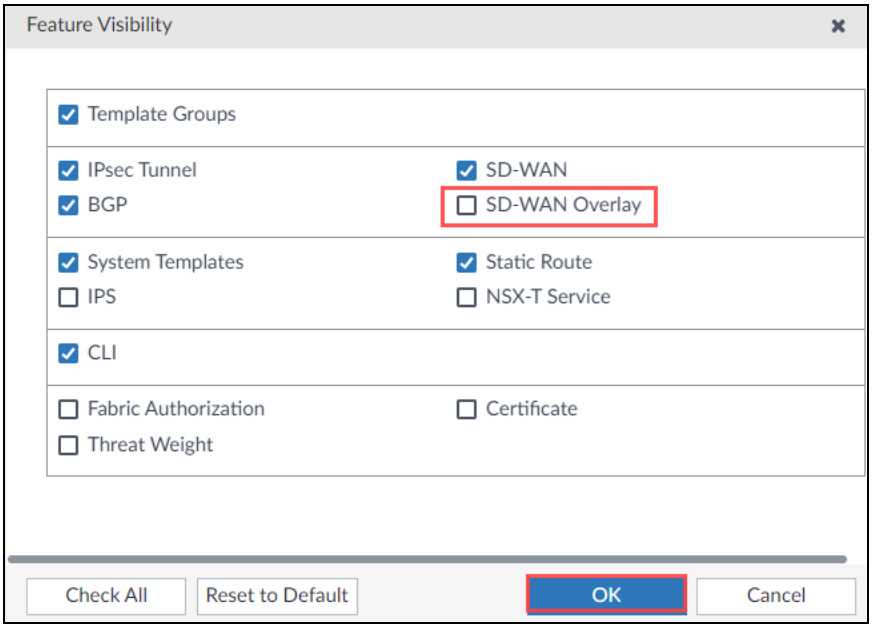
Visit us: Brave-Dumps.com

Configure the Overlay Tunnels With the SD-WAN Overlay Template

You will use the SD-WAN overlay template to configure the IPsec overlay and BGP routing configuration. The **SD-WAN Overlay Template** wizard will guide you through the configuration.

To prepare the SD-WAN overlay template

1. Click **Device Manager** > **Provisioning Templates** > **Feature Visibility**.



2. Select the **SD-WAN Overlay** checkbox, and then click **OK**.
   FortiManager displays a new tab called **SD-WAN Overlay**.
3. Click **SD-WAN Overlay**, and then click **Create New**.
4. In the **Name** field, type `Corp-SOT` (for *Corp*orate *S*D-WAN *O*verlay *T*emplate).
5. Select the **Single HUB** topology.
6. Expand the **Advanced** menu, and then configure the following settings:

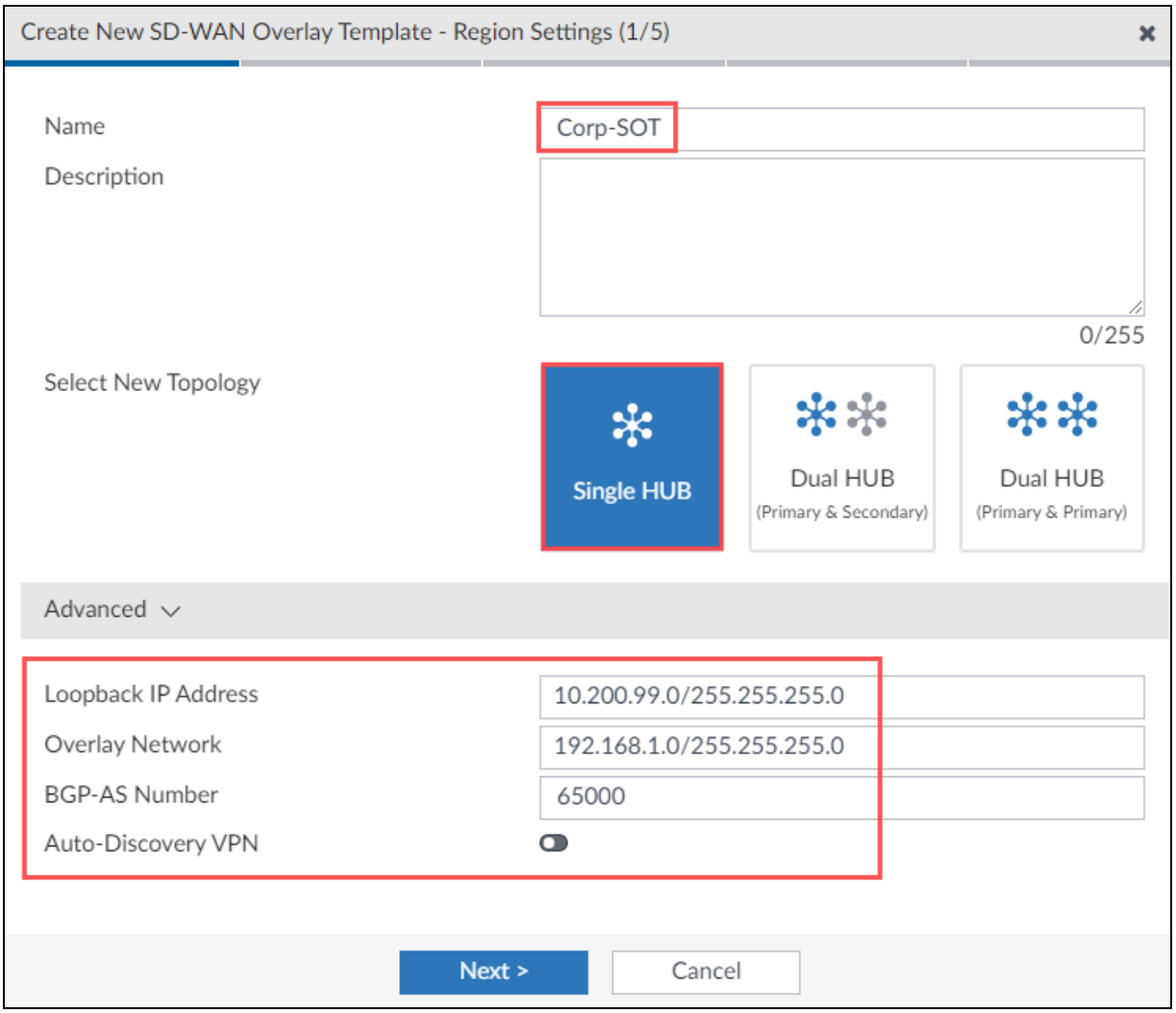
Field	Value
Loopback IP Address	10.200.99.0/255.255.255.0
Overlay Network	192.168.1.0/255.255.255.0
BGP-AS Number	65000 (default)
Auto-Discovery VPN	Disabled (default)

The **Region Settings (1/5)** page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Visit us: Brave-Dumps.com



Note the progress bar at the top of the **SD-WAN Overlay** template pages. It helps you to visualize how much of the configuration you have completed and how much you have left to do.

7. Click **Next**.
8. On the **Role Assignment (2/5)** page, configure the following settings:

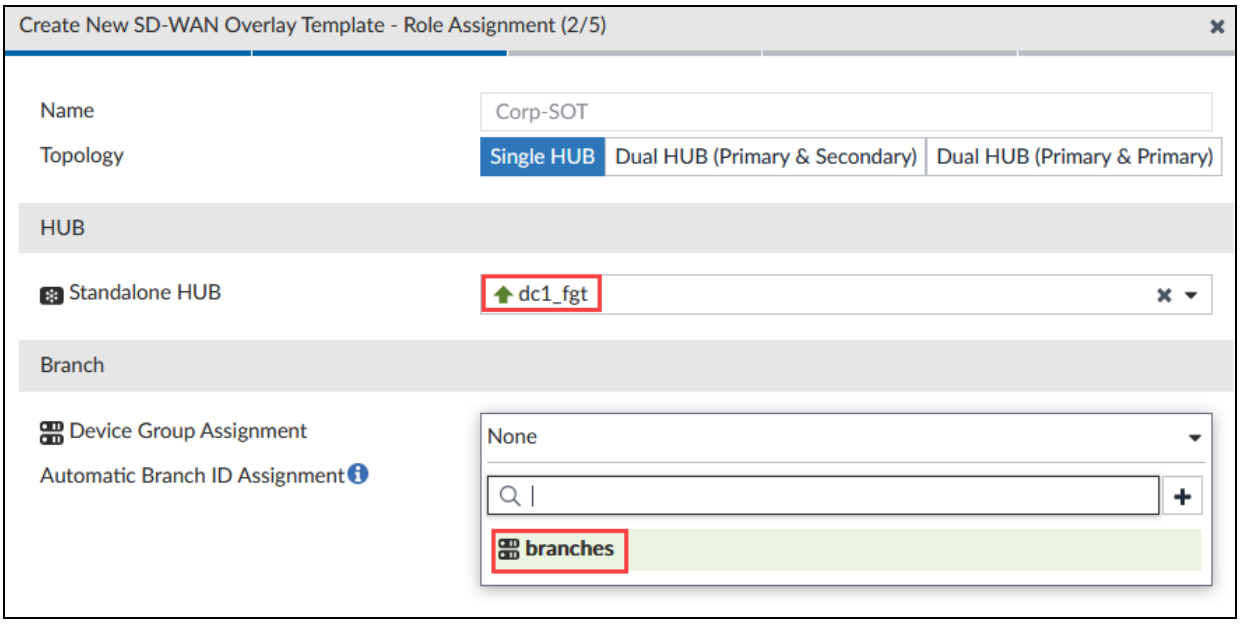
Field	Value
HUB - Standalone HUB	dc1_fgt

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Visit us: Brave-Dumps.com

Field	Value
Branch - Device Group Assignment	Click the drop-down list, and then click **+** to create a device group for the branches. Configure a device group with the following settings: • **Group Name**: Type `branches`. • **Add Members**: Select **branch1_fgt** and **branch2_fgt**. Click **Add** to validate the member selection, and then click **OK** to validate the group definition. Select the **branches** group that you created.
Automatic Branch ID Assignment	Disabled



9. Click **Next** to validate the role assignment and move to the next page.
10. On the **Network Configuration (3/5)** page, in the **HUB** section, configure the following settings:

Field	Value
Underlay	In the **WAN Underlay 1** field, type `port1`. In the **WAN Underlay 2** field, type `port2`. Click **+** to add a third WAN underlay, and then type `port4`.
Network Advertisement	Select **Connected**, and then click **+**. Type `port5` as the **Interface 1** interface to advertise the network connected to the LAN interface.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

11. In the **Branch** section, configure the following settings:

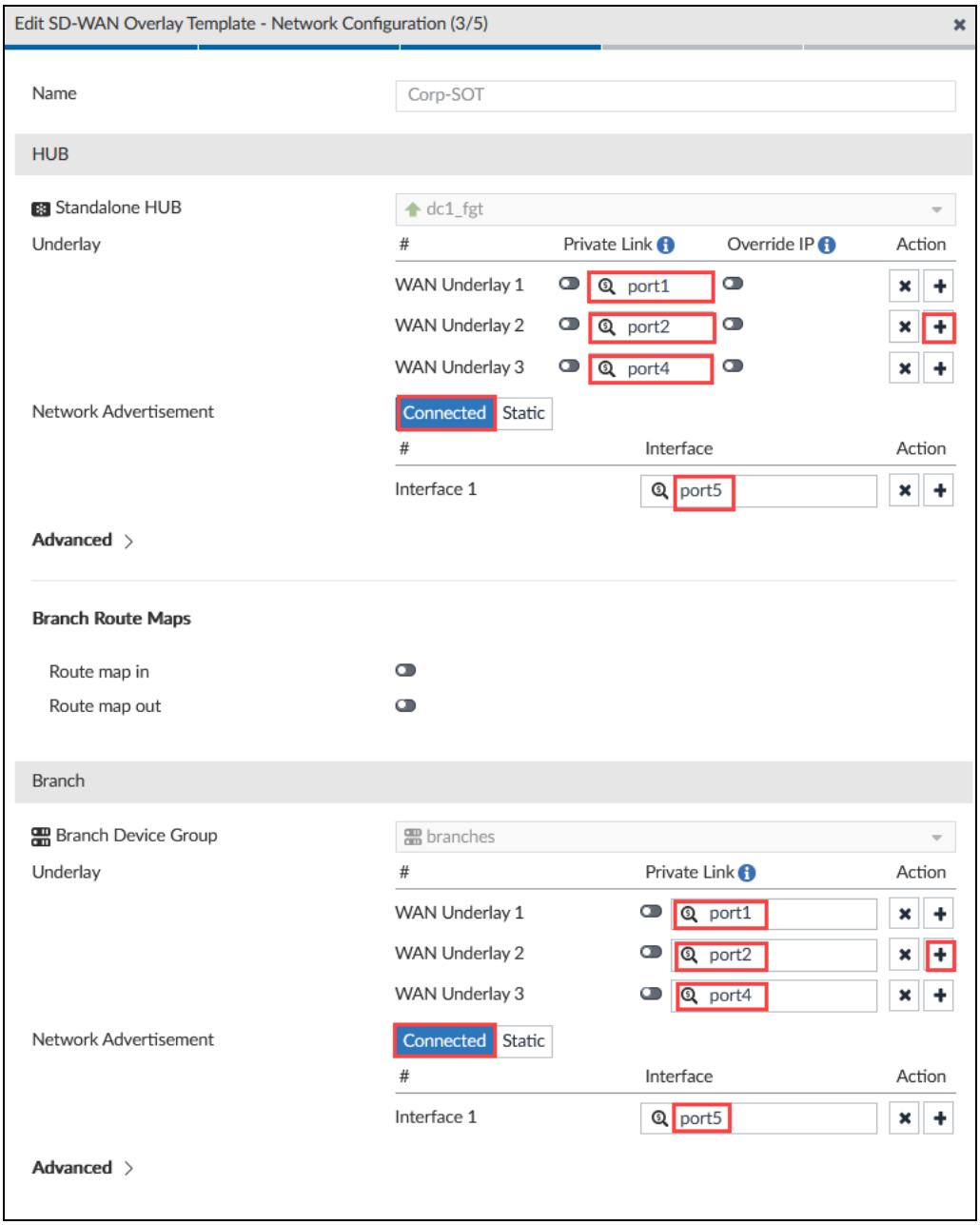
Field	Value
Underlay	In the **WAN Underlay 1** field, type `port1`. In the **WAN Underlay 2** field, type `port2`. Click **+** to add a third WAN underlay, and then type `port4`.
Network Advertisement	Select **Connected**, and then click **+**. Type `port5` as the **Interface 1** interface to advertise the network connected to the LAN interface.

Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Visit us: Brave-Dumps.com



When you select **Connected** in the **Network Advertisement** field, FortiManager creates a template that instructs BGP to advertise networks connected to port5 only. In this topology, that corresponds to the LAN subnet.

Do *not* enable the **Private Link** option.

The SD-WAN overlay template defines the BGP settings, but does not create overlays for interfaces that are configured as private links. You can use this setting for secured connections, such as MPLS, that you don't want to define overlay tunnels for.

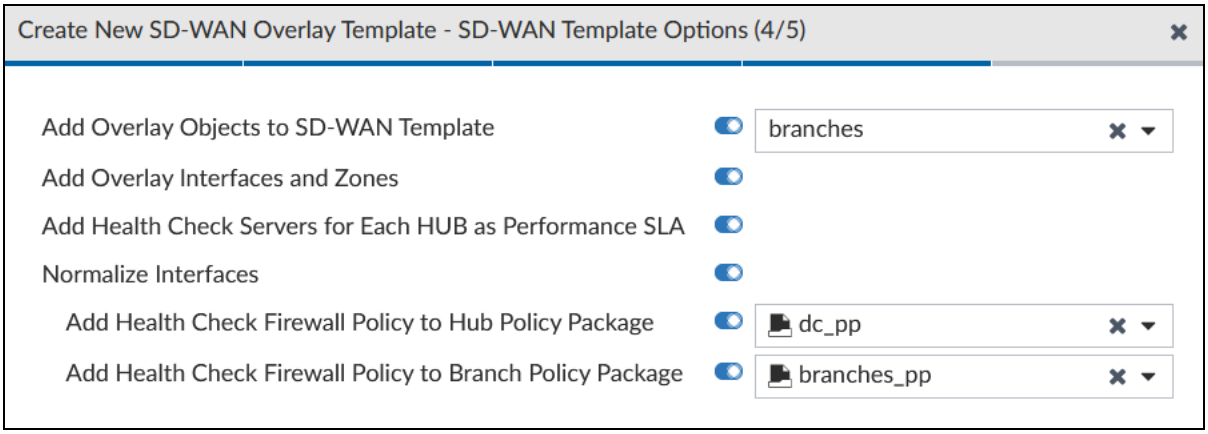
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

12. Click **Next** to move to the next page.
13. On the **SD-WAN Template Options (4/5)** page, configure the following settings:

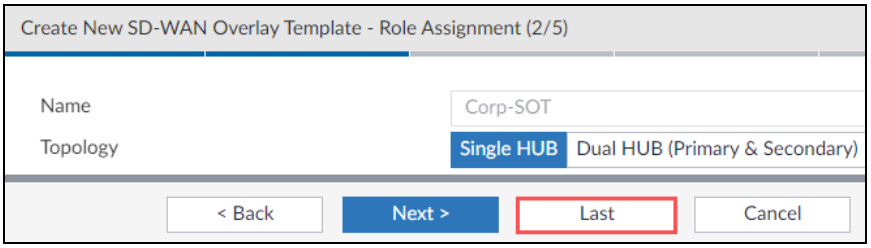
Field	Value
Add Overlay Objects to SD-WAN Template	Enabled In the drop-down list, select the **branches** SD-WAN template.
Add Overlay Interfaces and Zones	Enabled
Add Health Check Servers for Each HUB as Performance SLA	Enabled
Normalize Interfaces	Enabled
Add Health Check Firewall Policy to Hub Policy Package	Enabled, and then select **dc_pp**.
Add Health Check Firewall Policy to Branch Policy Package	Enabled, and then select **branches_pp**.

Your page should look similar to the following example:



14. Click **Next** to move to the next page.
15. Review the settings on the **Summary (5/5)** page.

On the SD-WAN overlay template summary page, if you detect a configuration element that you want to adjust, click the section title to go to the corresponding configuration page. When you are finished, click **Last** to return to the summary.

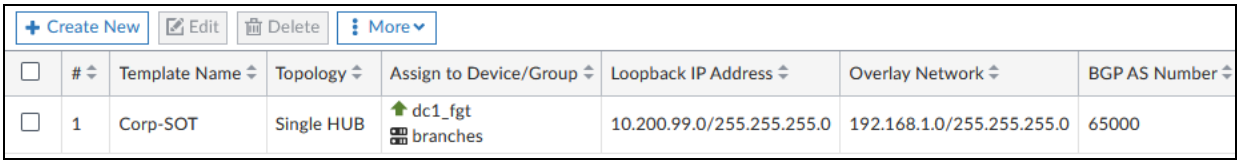


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

16. Once you have completed the summary review, click **Finish** to complete the SD-WAN overlay template configuration.

    Your page should look similar to the following example:



Review, Adjust, and Install the Overlay Configuration

The SD-WAN overlay template tool created multiple templates using the settings that you configured, and Fortinet recommended parameters and values for SD-WAN overlay tunnels with BGP routing. You will review these templates. Next, you will install the changes on the hub and spoke devices. Finally, you will check the health of the new overlay tunnels.

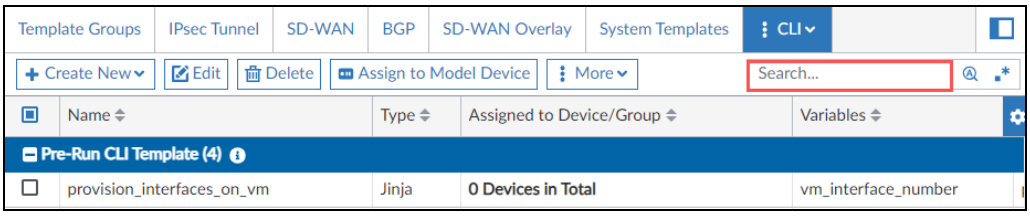
To review the CLI templates

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **CLI**.

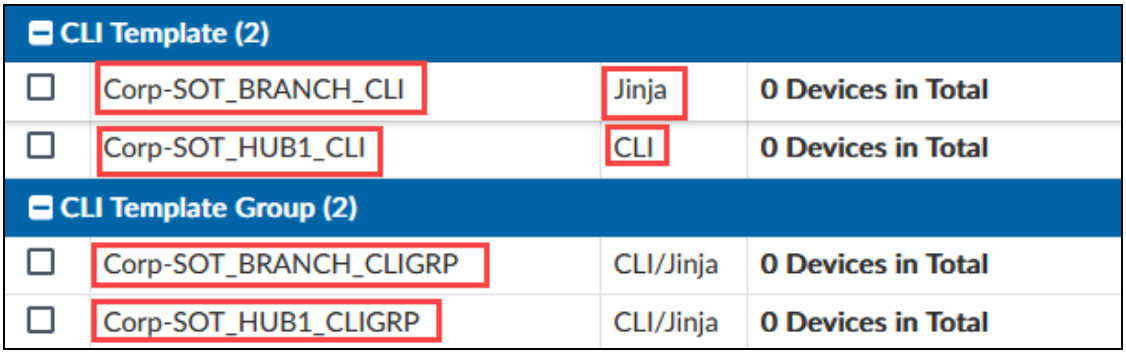
   The SD-WAN overlay template adds a prefix to the template name it creates with the name that you entered for the overlay: **Corp-SOT**. You can see two templates: **Corp-SOT_BRANCH_CLI** and **Corp_SOT_HUB1_CLI**. The template types are Jinja and CLI, respectively. These templates create loopback addresses, and for the branches, the BGP router ID.

2. In the search box, type `corp` to filter the CLI templates.

   Note that the search is not case sensitive.



   FortiManager adds the templates to the CLI template groups, **Corp-SOT_BRANCH_CLIGRP** and **Corp-SOT_HUB1_CLIGRP**, respectively.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

On your FortiManager, you can see additional templates. These templates were predefined for you and you will need them in other labs. Do *not* delete them.

3. Double-click **Corp-SOT_Branch_CLI** to review the template.
4. Click **Cancel**.
5. Double-click **Corp-SOT_HUB1_CLI** to review the template.
6. Click **Cancel**.

Stop and think!

The SD-WAN overlay template process prepared a Jinja script for the branches and a CLI template for the hub. Why?

The CLI template for the hub is simple. It configures a single loopback IP address defined for HUB1. (For dual-hub topologies, FortiManager defines a CLI template for each hub device). Such configuration is easily defined with CLI commands.

The CLI template for branches must scale to a number of branches that is not known in advance. This single Jinja script can assign a different loopback IP address and a different router ID on each branch device. The loopback IP address and the router ID are defined with a predefined part and a value derived from the branch ID.

The formula to define the router-id is `{{'10.200.99.0'|ipmath(branch_id|int)}}`.

For information about Jinja use on FortiManager, see Jinja filters and functions.

To review the IPsec tunnel templates

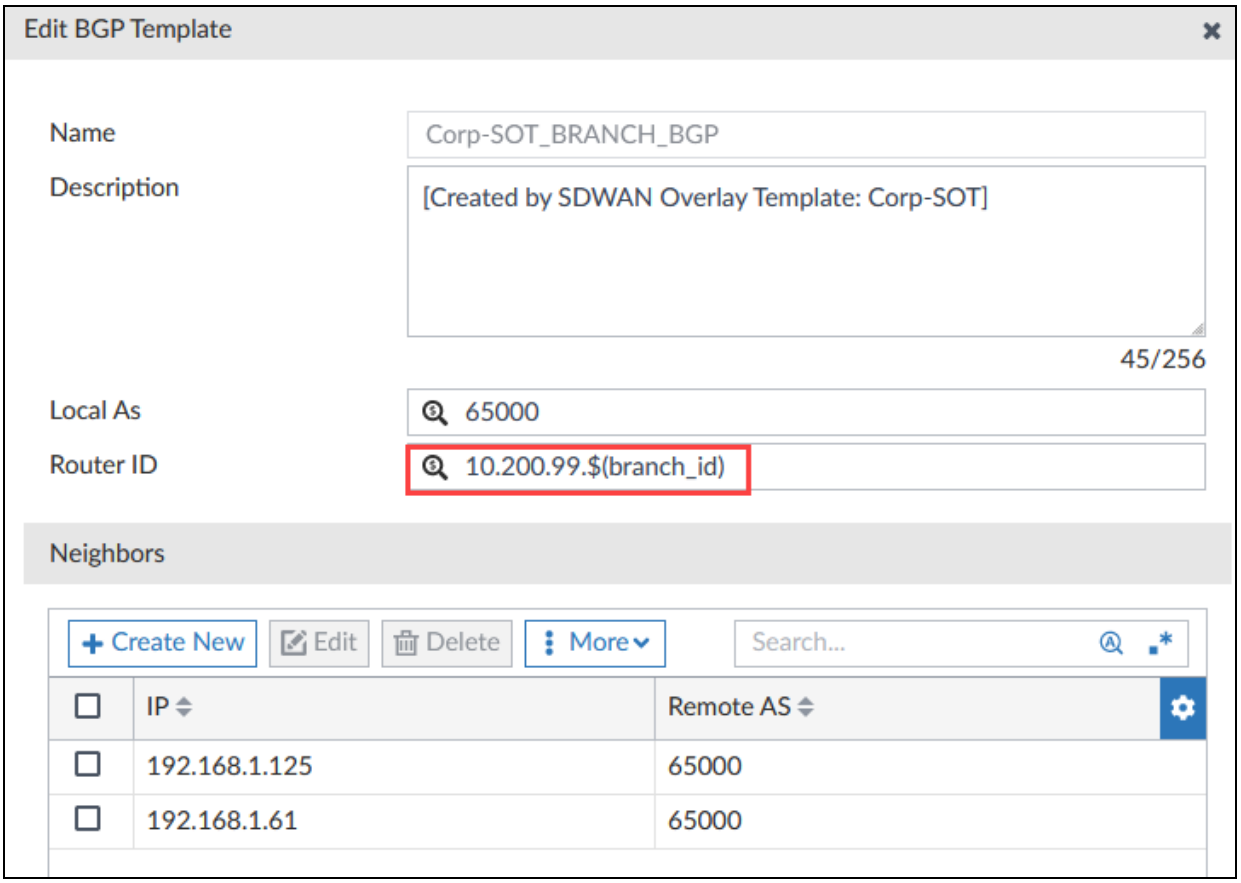
1. Click **Provisioning Template** > **IPsec Tunnel**.
2. Review the **Corp-SOT_BRANCH_IPsec** and **Corp-SOT_HUB1_IPsec** templates.
   Each template contains three tunnel definitions: **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3** for the branches and **VPN1**, **VPN2**, and **VPN3** for the hub.
3. Click **Cancel** to exit the IPsec template menu.
   You will review the tunnel definition in detail in the next lab.

To review the BGP template

1. Click **Provisioning Templates** > **BGP**.
2. Review the **Corp-SOT_BRANCH_BGP** template.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



When you select the **Automatic Branch ID Assignment** option for your device group, FortiManager assigns an ID to each device in the device group. For this purpose, it creates the **branch_id** metadata variable. Alternatively, administrators can assign a **branch_id** value for each branch device.

Stop and think!

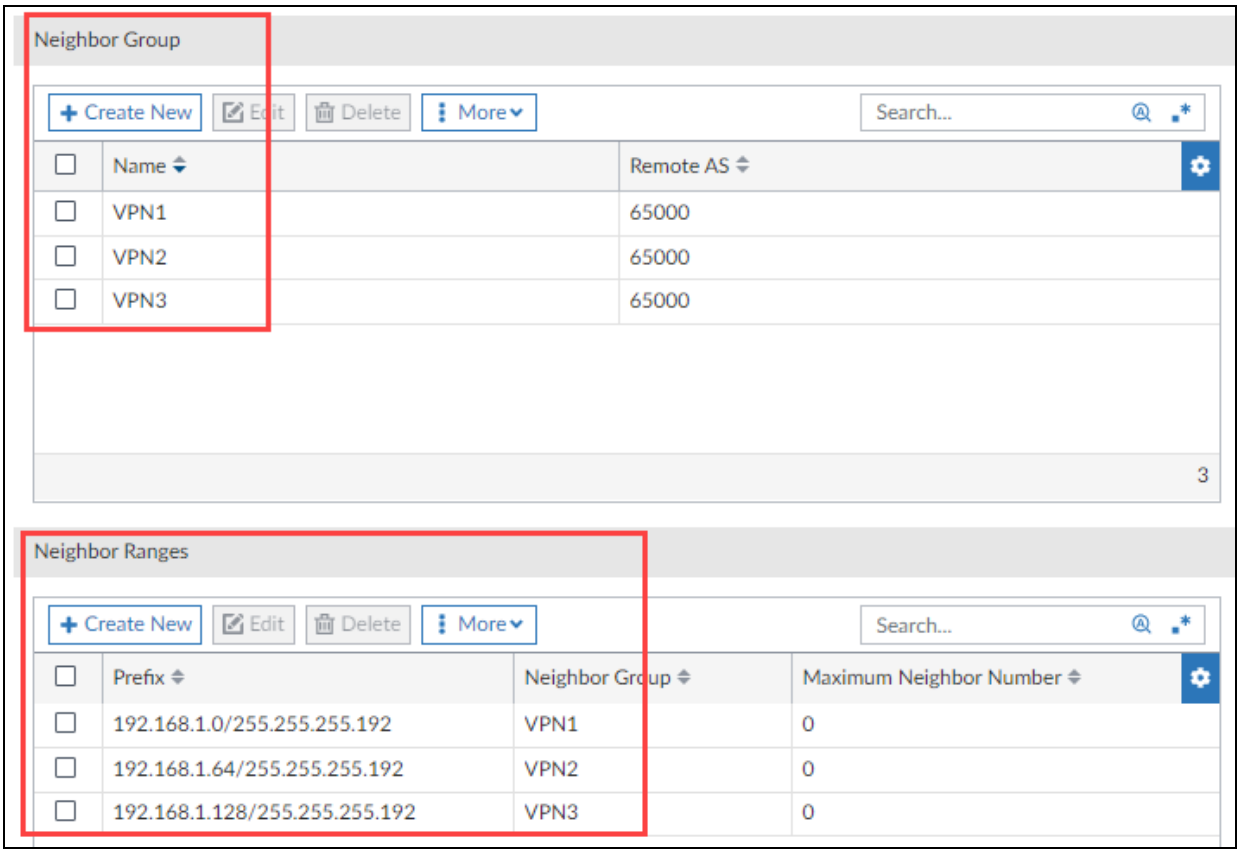
The BGP template defines the router ID for each branch device with a fixed IP address part and the branch ID. What happens if you want to deploy a device with ID 382?

To complement the router ID definition in the BGP template, and to accommodate topologies with more than 255 devices, the SD-WAN overlay template proceeds with a second definition of the router ID with a Jinja script. Because FortiManager applies CLI scripts after the BGP templates, the script overrides the template definition for the router ID and allows you to deploy devices with IDs greater than 255.

3. Click **Cancel**.
4. Review the **Corp-SOT_HUB1_BGP** template.
5. Note the router ID defined with a static value, and the **Neighbor Group** and **Neighbor Ranges** definitions. The template defines one neighbor group and one prefix range per VPN—VPN1, VPN2, and VPN3.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



6. Click **Cancel**.

To review the SD-WAN template

1. Click **Provisioning Templates** > **SD-WAN**, and then edit the **branches** template to review the changes the SD-WAN overlay template made.
   - You can see a new zone, **HUB1**, with three interface members: **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**. These are the three overlay IPsec tunnel interfaces.
   - port1 and port2, which were previously in the **underlay** zone, have moved to the **WAN1** and **WAN2** zones. The SD-WAN overlay template also created a zone for port4. You will move port1 and port2 to the **underlay** zone.

> The SD-WAN overlay template placed the underlay interfaces, port1 and port2, in new underlay zones called **WAN1** and **WAN2**. Because you will continue to use SD-WAN rules and the firewall policy that you created previously, and defined with the zone named **underlay**, you must place the port1 and port2 interfaces back in the underlay zone.
>
> If you don't want the SD-WAN overlay template to modify the zone and member definition in your SD-WAN template, you must not select the **Add Overlay Interface and Zones** setting in step 4. In this case, you must manually define members and zones for your overlays.

2. In the **SD-WAN Zones** table, double-click **underlay** to edit the zone.
3. In the **Interface Members** section, select **port1** and **port2**, and then click **OK** to validate the member selection.
4. Click **OK** to validate the zone edition.

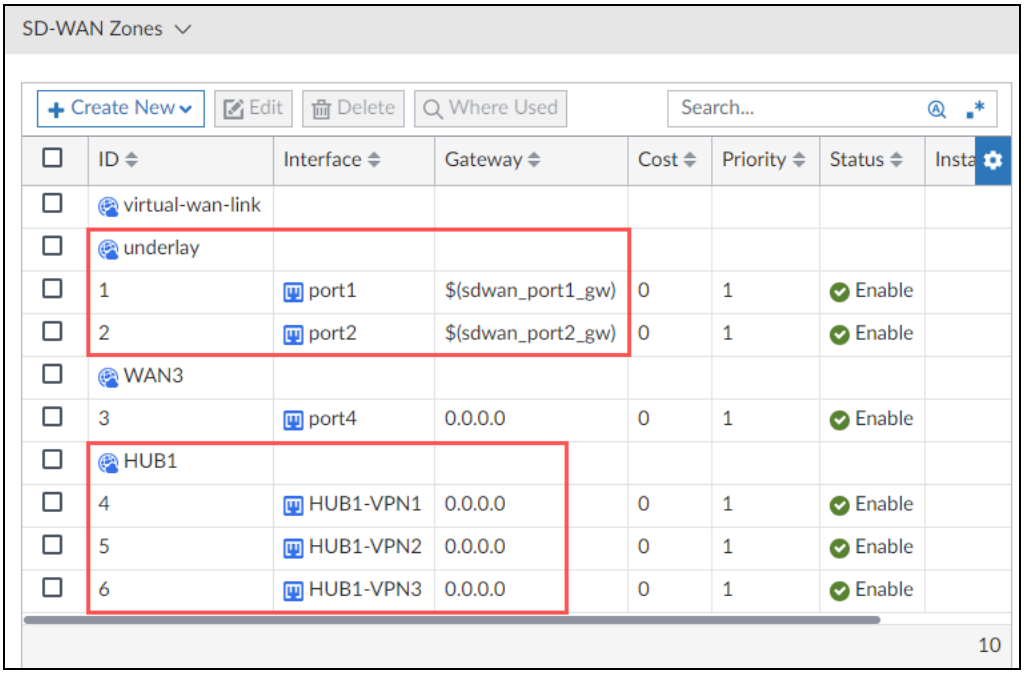
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

5. Click **OK** to validate the template edition.
6. Edit the **branches** template again, select the **WAN1** and **WAN2** zones, and then click **Delete**.

After you remove all ports from a zone, you cannot delete this zone immediately. First, you must validate the template update.

Your output should look similar to the following example:



FortiManager places each underlay interface in a zone. Keep the single member zone **WAN3**, which contains the **port4** interface.

7. Scroll down to the **Performance SLA** section, and then note the new **HUB1_HC** health check.

   The SD-WAN overlay template created this performance SLA to monitor the health of the overlay links. It uses the loopback address on the hub as a detection server.
8. Click **OK** to validate the template update.

Stop and think!

The SD-WAN overlay template created multiple templates but, for all templates you reviewed, the **Assigned to Device /Group** list is empty. Why? Do you need to manually assign them to the hub and the branches?

No. The SD-WAN overlay template created the templates and grouped them. A group is assigned to each device.

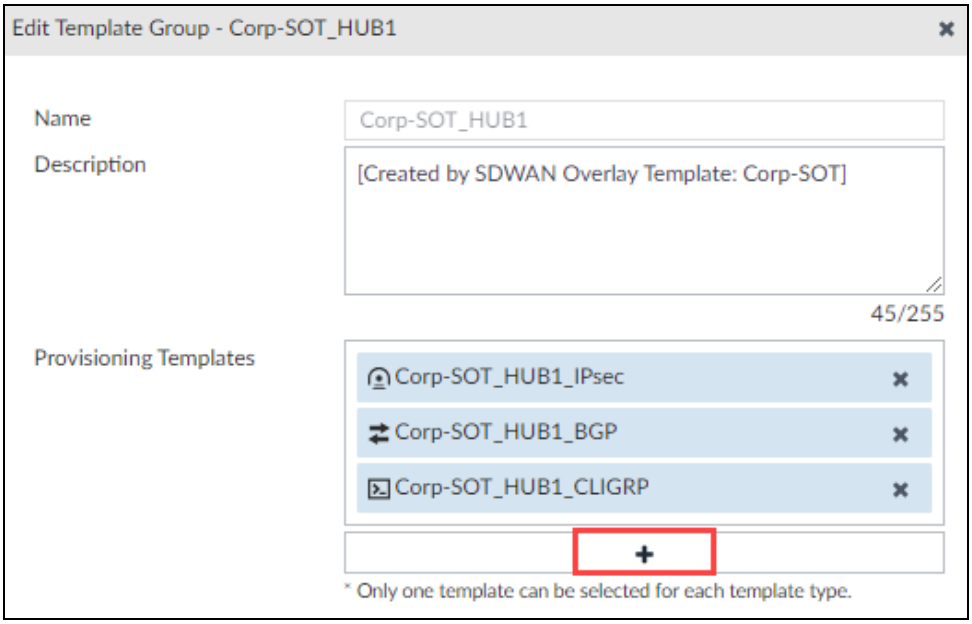
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To review and adjust the template groups

1. Click **Provisioning Template** > **Template Groups**.
2. Review the groups that are assigned to the branches and hub.

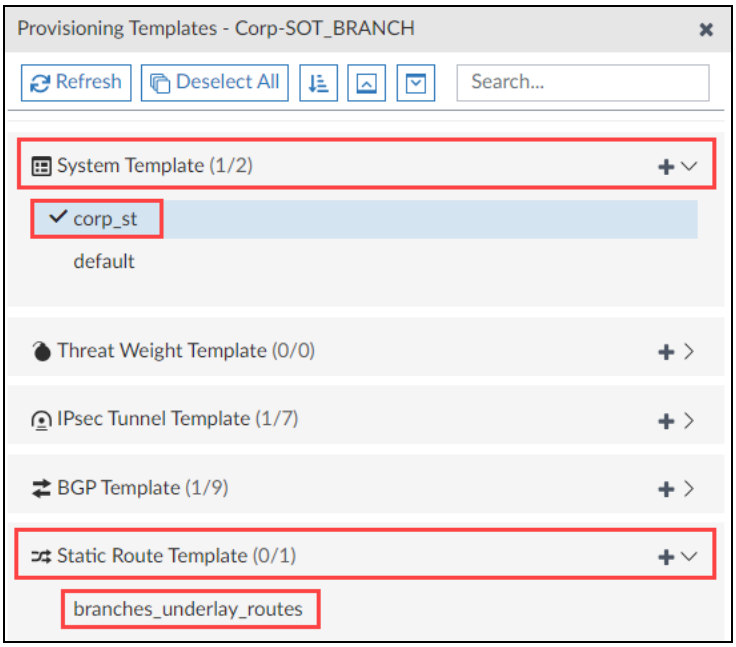
   The template groups contain the templates that the SD-WAN overlay template created or updated. The groups don't include the template that you previously assigned to the device.
3. Double-click the **Corp-SOT_HUB1** template group to edit it.
4. Click **+** to add a new template to the group.



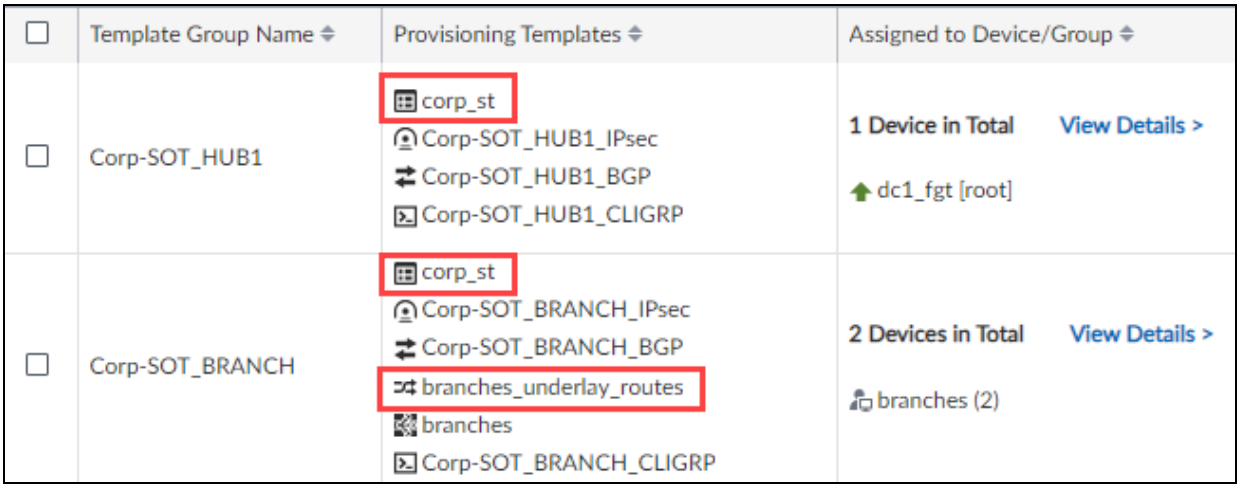
5. Expand the **System Template** section, select **corp_st**, and then click **OK** to validate the selection.
6. Click **OK** to validate the template group changes.
7. Double-click the **Corp-SOT_BRANCH** template group to edit it.
8. Repeat steps 3–5 to add the **corp_st** system template to the group.
9. Expand the **Static Route Template** section, select **branches_underlay_routes**, and then click **OK** to validate the selection.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



10. Click **OK** to validate the template group changes.
Your output should look like the following image:



Template Group Name	Provisioning Templates	Assigned to Device/Group
Corp-SOT_HUB1	corp_st Corp-SOT_HUB1_IPsec Corp-SOT_HUB1_BGP Corp-SOT_HUB1_CLIGRP	1 Device in Total View Details > dc1_fgt [root]
Corp-SOT_BRANCH	corp_st Corp-SOT_BRANCH_IPsec Corp-SOT_BRANCH_BGP branches_underlay_routes branches Corp-SOT_BRANCH_CLIGRP	2 Devices in Total View Details > branches (2)

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

How does FortiManager considers parameters defined in multiple templates? For example, what happens with the BGP router ID for branches? It is defined with the formula `10.200.99.$(branch_id)` in the BGP template and with a Jinja script and the formula `set router-id {{'10.200.99.0'|ipmath (branch_id|int)}}` in the **Corp-SOT_BRANCH_CLI** CLI template.

FortiManager applies the templates in the following predefined order: the system template, the IPsec template, the BGP template, and the CLI templates. If the administrator defines multiple CLI templates, FortiManager applies them in the order you can see in the CLI template group. For parameters that appear in two templates, FortiManager overrides any conflicting settings with the value defined in the last template that was applied.

On the branches, FortiManager applies the router ID as it is defined in the last template that was applied. This is the value from the Jinja script included in the CLI template group.

To install the configuration changes

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Policy Packages & Device Settings**.
3. In the **Policy Package** field, select **branches_pp**, and then click **Next**.
4. Select the **branches** device group, **branch1_fgt** and **branch2_fgt**, and then click **Next**.
5. Click **Install** to install the configuration on the two devices.
6. Wait for the installation to finish, and then click **Finish**.
7. Repeat the procedure to install the device setting changes, and the **dc_pp** policy package on **dc1_fgt**.

Monitor the Status of the Overlay Tunnels

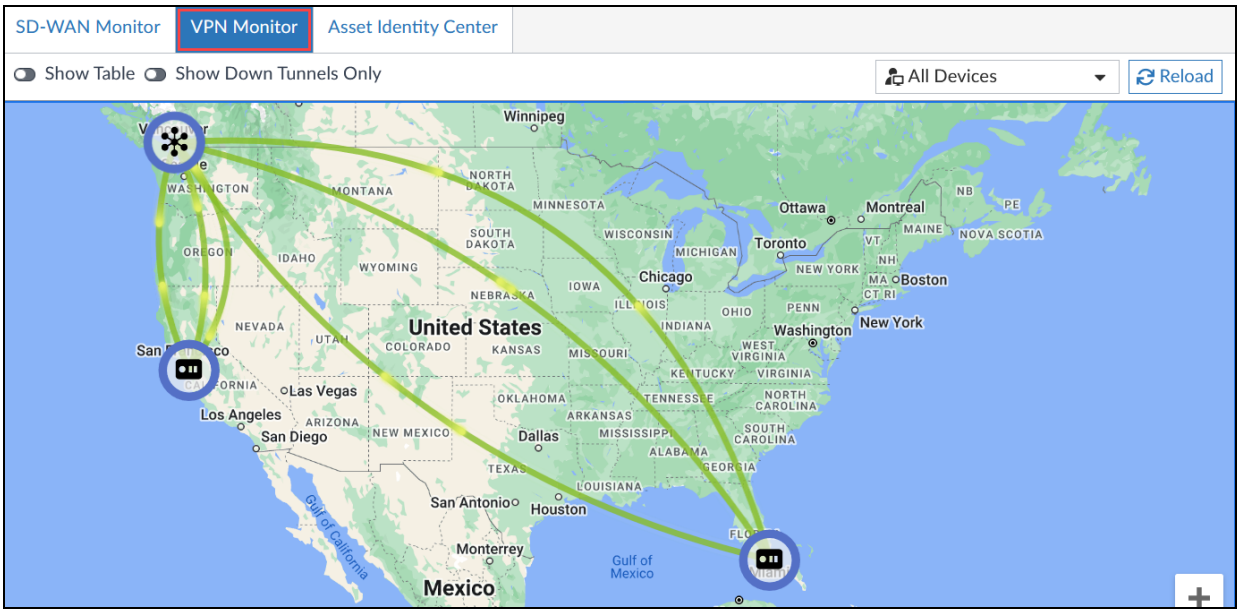
The SD-WAN overlay template creates IPsec tunnels to build the SD-WAN overlay network and defines the BGP routing on it. You will confirm that the tunnels are correctly established and review the BGP routes that are established.

To verify the health of the overlays

1. Continuing on the FortiManager GUI, click **Device Manager** > **Monitors** > **VPN Monitor**.
   It defaults to the map view. Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



The hub, dc1_fgt, is located in Vancouver.

The branch devices, branch1_fgt and branch2_fgt, are located in Sunnyvale and Miami, respectively.

There are three tunnels between each branch device and the hub.

You may need to zoom out before you can see the managed devices on the map.

2. Select **Show Table**.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Device	Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
branch1_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	27.3 MB	27.3 MB
branch1_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	27.3 MB	27.3 MB
branch1_fgt[root]	HUB1-VPN3	automatic	172.16.1.5	172.16.1.5	533.3 KB	533.3 KB
branch2_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	27.3 MB	27.3 MB
branch2_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	27.3 MB	27.3 MB
branch2_fgt[root]	HUB1-VPN3	automatic	172.16.1.5	172.16.1.5	533.1 KB	533.2 KB
dc1_fgt[root]	VPN1_0	dialup	203.0.113.1	Branch2	27.3 MB	27.3 MB
dc1_fgt[root]	VPN1_1	dialup	192.2.0.1	Branch1	27.3 MB	27.3 MB

Each branch device has established three tunnels to the hub:

- On port1: **HUB1-VPN1**, with remote gateway 100.64.1.1
- On port2: **HUB1-VPN2**, with remote gateway 100.64.1.9
- On port4: **HUB1-VPN3**, with remote gateway 172.16.1.5

On the hub, dc1_fgt, there are six tunnels:

- On port1: **VPN1_0** and **VPN1_1** for tunnels from branch2_fgt and branch1_fgt
- On port2: **VPN2_0** and **VPN2_1** for tunnels from branch2_fgt and branch1_fgt
- On port4: **VPN3_0** and **VPN3_1** for tunnels from branch2_fgt and branch1_fgt

3. Open an SSH session to branch1_fgt.
4. Log in to the FortiGate CLI with the following credentials:
   - Username: `admin`
   - Password: `password`
5. Enter the following commands to review the BGP peering and routing table:

```
get router info bgp summary
get router info routing-table all
```

Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.1, local AS number 65000
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.61    4      65000       6       6        1    0    0 00:02:27        1
192.168.1.125   4      65000       6       6        1    0    0 00:02:33        1
192.168.1.189   4      65000       6       6        1    0    0 00:02:33        1

Total number of neighbors 3


branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:02:17, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:02:17, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:02:17, [1/0]
C       10.200.99.1/32 is directly connected, Branch-Lo
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
C       192.168.1.0/26 is directly connected, HUB1-VPN1
C       192.168.1.1/32 is directly connected, HUB1-VPN1
C       192.168.1.64/26 is directly connected, HUB1-VPN2
C       192.168.1.65/32 is directly connected, HUB1-VPN2
C       192.168.1.128/26 is directly connected, HUB1-VPN3
C       192.168.1.129/32 is directly connected, HUB1-VPN3
```

branch1_fgt has a route to the corporate LAN 10.1.0.0 using the three overlay tunnels.

6. Repeat steps 4–5 to check the routing table on dc1_fgt.
   Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
dc1_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.253, local AS number 65000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 44 seconds

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.1     4      65000      10      10        2    0    0 00:06:00        1
192.168.1.2     4      65000      10      10        4    0    0 00:05:51        1
192.168.1.65    4      65000      10      10        1    0    0 00:06:02        1
192.168.1.66    4      65000      11      10        4    0    0 00:05:52        1
192.168.1.129   4      65000      10      10        3    0    0 00:05:56        1
192.168.1.130   4      65000      10      10        3    0    0 00:05:54        1

Total number of neighbors 6
```

```
dc1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.2, port1, [1/0]
                 [10/0] via 100.64.1.10, port2, [1/0]
B       10.0.1.0/24 [200/0] via 192.168.1.1 (recursive is directly connected, VPN1), 00:07:48, [1/0]
                    [200/0] via 192.168.1.65 (recursive is directly connected, VPN2), 00:07:48, [1/0]
                    [200/0] via 192.168.1.130 (recursive is directly connected, VPN3), 00:07:48, [1/0]
B       10.0.2.0/24 [200/0] via 192.168.1.2 (recursive is directly connected, VPN1), 00:07:45, [1/0]
                    [200/0] via 192.168.1.66 (recursive is directly connected, VPN2), 00:07:45, [1/0]
                    [200/0] via 192.168.1.129 (recursive is directly connected, VPN3), 00:07:45, [1/0]
C       10.1.0.0/24 is directly connected, port5
C       10.200.99.253/32 is directly connected, HUB1-Lo
C       100.64.1.0/29 is directly connected, port1
C       100.64.1.8/29 is directly connected, port2
S       172.16.0.0/16 [10/0] via 172.16.1.6, port4, [1/0]
C       172.16.1.0/24 is directly connected, port4
C       192.168.0.0/24 is directly connected, port10
C       192.168.1.0/26 is directly connected, VPN1
C       192.168.1.61/32 is directly connected, VPN1
C       192.168.1.64/26 is directly connected, VPN2
C       192.168.1.125/32 is directly connected, VPN2
C       192.168.1.128/26 is directly connected, VPN3
C       192.168.1.189/32 is directly connected, VPN3
```

dc1_fgt has six BGP neighbors, one on each underlay link. It has three routes to each branch local subnet, 10.0.1.0/24 and 10.0.2.0/24, using each overlay tunnel for each branch device.

Stop and think!

What is the next configuration step?

The SD-WAN overlay template helped you configure the overlay tunnels and BGP routing to direct the traffic through them. It has also created an SD-WAN overlay zone called **HUB1** and placed the tunnels in it.

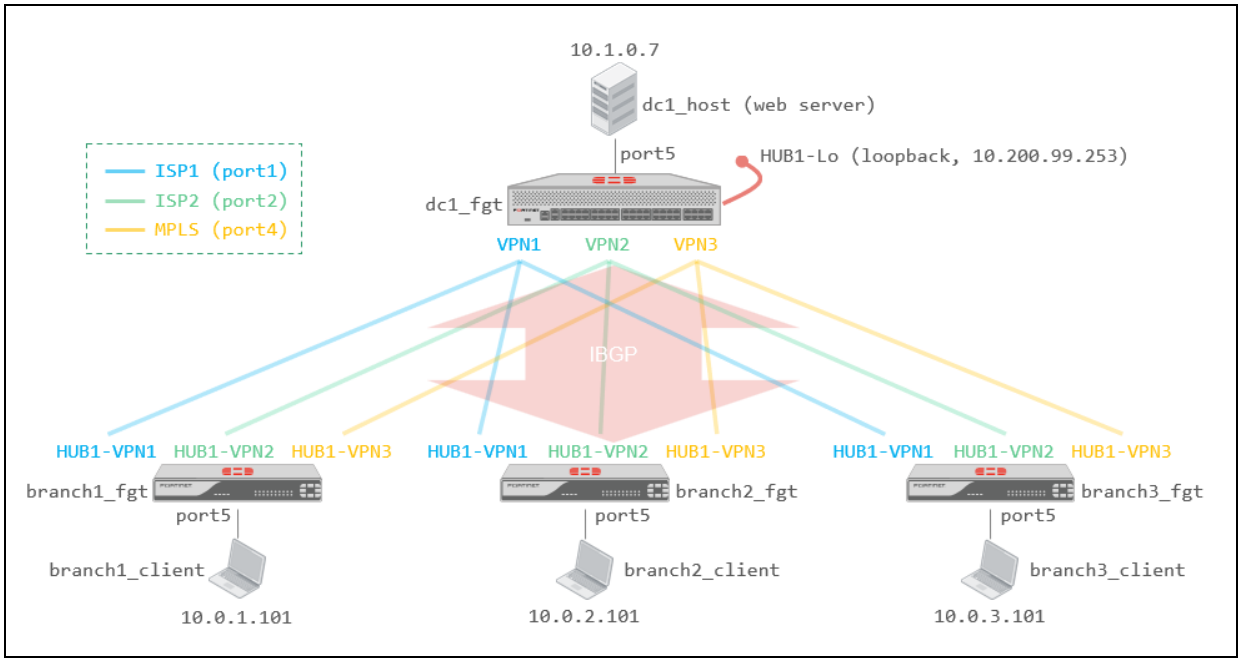
The administrator must now configure the firewall policies and SD-WAN rules to steer the traffic according to the requirements.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 3: Zero-Touch Provisioning of SD-WAN Branches

In this lab, you will use the zero-touch provisioning (ZTP) concept to onboard a third branch to your SD-WAN topology. First, you will configure SD-WAN rules and firewall policies for the overlay topology that you configured in the previous lab. Next, you will adjust the configuration and onboard a third branch using ZTP techniques. Finally, you will monitor your SD-WAN deployment using FortiManager.



In the topology, branch1_fgt, branch2_fgt, and branch3_fgt are dial-up clients, and dc1_fgt is a dial-up server. The four devices connect with three underlays—ISP1 on port1, ISP2 on port2, and MPLS on port4.

Objectives

- Configure SD-WAN rules for the overlays
- Adjust the FortiManager configuration to allow ZTP
- Onboard a third branch with ZTP
- Review the ZTP onboarding results on FortiGate and FortiManager

Time to Complete

Estimated: 90 minutes

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Configuring Firewall Policies and SD-WAN Rules

In this exercise, you will create SD-WAN rules and firewall policies to steer and secure the traffic routed through the overlay VPN topology that you created in the previous lab.

Configure Firewall Policies

First, you will add new rules to the policy packages to allow traffic between the branch devices and the hub, through the overlay tunnels. Next, you will configure the VPN tunnels as SD-WAN members of the overlay zone. Finally, you will install the changes and verify the configuration on the FortiGate CLI.

To configure firewall policies on the branches to allow traffic through the overlay tunnels

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Policy & Objects** > **Policy Packages**.
3. Click **branches_pp** > **Firewall Policy**.
   Your page should look similar to the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action
Corp-SOT_BBLK (1/1 Total:1)								
1	Health Check Access	Branch-Lo	HUB1	Corp-SOT_Br_Loopback	Corp-SOT_Loopback	always	ALL	Accept
2	DIA	LAN	underlay	LAN-net	all	always	ALL	Accept
Implicit (3/3 Total:1)								
3	Implicit Deny	any	any	all all	all all	always	ALL	Deny

4. Click **Create New** > **Create New**.
5. Configure the following settings to create a new firewall policy:

Field	Value
Name	To Hub-Overlay
Incoming Interface	LAN
Outgoing Interface	HUB1 (This is the overlay zone that the SD-WAN overlay template created.)
Action	Accept
Other parameters	Default values

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

6. Click **OK** to save the settings.

> **Stop and think!**
>
> Did you configure a normalized interface called **HUB1**? Remember that on FortiManager, firewall policies can reference only normalized interfaces. Yet, **HUB1** is available as a possible source or destination for the firewall policy.
>
> When you create an SD-WAN zone with the SD-WAN template, FortiManager automatically creates a corresponding normalized interface.

7. Right-click the **To Hub-Overlay** firewall policy that you created, and then click **Clone Reverse**.
8. Double-click the cloned policy to edit it, and then configure the following setting:

Field	Value
Name	From Hub-Overlay

9. Click **OK** to save the settings.
   Your page should look similar to the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action
Corp-SOT_BBLK (1/1 Total:1)								
1	Health Check Access	Branch-Lo	HUB1	Corp-SOT_Br_Loopback	Corp-SOT_Loopback	always	ALL	Accept
2	DIA	LAN	underlay	LAN-net	all	always	ALL	Accept
3	To Hub-Overlay	LAN	HUB1	all	all	always	ALL	Accept
4	From Hub-Overlay	HUB1	LAN	all	all	always	ALL	Accept
Implicit (5/5 Total:1)								
5	Implicit Deny	any	any	all all	all all	always	ALL	Deny

You require only one firewall policy in each direction that references the overlay zone. Using SD-WAN zones greatly reduces the number of policies that are required for your deployment.

Take the Expert Challenge!

For better readability of the firewall policy list, you can add sections to separate policy blocks.

Create one section named `Underlay` to group policies that allow traffic through underlay links and another section named `Overlay` for the two policies through the overlay links. Select a different color for each section.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see "Configuring Firewall Policies and SD-WAN Rules" on page 91.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To create a section header in a policy package

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
2. Click **branches_pp** > **Firewall Policy**.
3. Right-click the **DIA** policy, and then select **Add Section**.
4. In the **Name** field, type `Underlay`, enable **Color**, and then select a color.
5. Click **OK** to validate the section creation.
6. Repeat steps 3–5 to create an `Overlay` section above the **To Hub-Overlay** policy 3—select a different color.
   Your output should look similar to the following example:

#	Name	From	To	Source	Destination
Corp-SOT_BBLK (1/1 Total:1)					
1	Health Check Access	Branch-Lo	HUB1	Corp-SOT_Br_Loopback	Corp-SOT_Loopback
Underlay (2/2 Total:1)					
2	DIA	LAN	underlay	LAN-net	all
Overlay (3/4 Total:2)					
3	To Hub-Overlay	LAN	HUB1	all	all
4	From Hub-Overlay	HUB1	LAN	all	all
Implicit (5/5 Total:1)					
5	Implicit Deny	any	any	all all	all all

To configure firewall policies on the hub to allow traffic through the overlay tunnels

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
2. Click **dc_pp** > **Firewall Policy**.
   Your page should look similar to the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action
Corp-SOT_HBLK (1/1 Total:1)								
1	Health Check Access	VPN1 VPN2 VPN3	HUB-Lo	Corp-SOT_Overlay_Network	Corp-SOT_Loopback	always	ALL	Accept
2	allow-all	any	any	all	all	always	ALL	Accept
Implicit (3/3 Total:1)								
3	Implicit Deny	any	any	all all	all all	always	ALL	Deny

SD-WAN is not defined on the hub. Therefore, for the policies definition, you cannot use zones. You must use the VPN1, VPN2, and VPN3 tunnel interface that the SD-WAN overlay template created.

The policy to allow heath-check traffic was created by the SD-WAN overlay template.

3. Click the **allow-all** policy, and then click **Delete**.
4. Click **Create New** > **Create New**, and then configure the following settings:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Name	To Branches-VPN
Incoming Interface	port5
Outgoing Interface	VPN1, VPN2, VPN3
Source	Corp-net
Destination	Corp-net
Action	Accept

5. Click **OK**.
6. Repeat the steps above, or use the **Clone** and **Clone Reverse** features, to create the following firewall policies:

Name	Incoming Interface	Outgoing Interface	Source	Destination	Action
From Branches-VPN	VPN1, VPN2, VPN3	port5	Corp-net	Corp-net	Accept
Branch to Branch	VPN1, VPN2, VPN3	VPN1, VPN2, VPN3	Corp-net	Corp-net	Accept

The **Corp-net** firewall address object has been preconfigured for you.

After you configure all of the policies, your page should look similar to the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action
Corp-SOT_HBLK (1/1 Total:1)								
1	Health Check Access	VPN1 VPN2 VPN3	HUB-Lo	Corp-SOT_Overlay_Net...	Corp-SOT_Loopback	always	ALL	Accept
2	To Branches-VPN	port5	VPN1 VPN2 VPN3	Corp-net	Corp-net	always	ALL	Accept
3	From Branches-VPN	VPN1 VPN2 VPN3	port5	Corp-net	Corp-net	always	ALL	Accept
4	Branch to Branch	VPN1 VPN2 VPN3	VPN1 VPN2 VPN3	Corp-net	Corp-net	always	ALL	Accept
Implicit (5/5 Total:1)								
5	Implicit Deny	any	any	all all	all all	always	ALL	Deny

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The policy order on your device might be different. Because each policy refers to a different source and destination pair, the policy order will not impact the policy matching behavior.

Configure an SD-WAN Rule for the Overlays

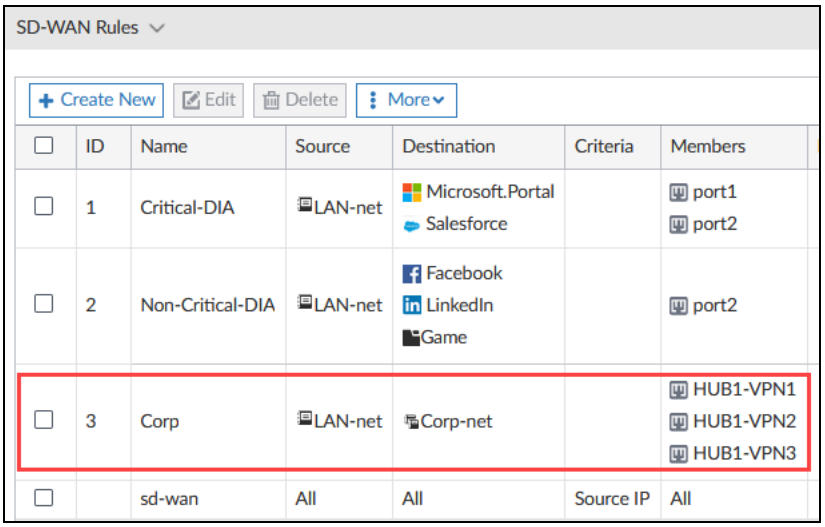
You will configure a basic manual rule for the overlays.

To configure an SD-WAN rule for the overlays

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
2. Double-click the **branches** SD-WAN template to edit it.
3. Expand the **SD-WAN Rules** section, and then click **Create New**.
4. Configure the following settings:

Field	Value
Name	Corp
Source	In the **Source Address** field, select **LAN-net**.
Destination	In the **Address** field, select the **Corp-net** address group.
Outgoing Interfaces	1. In the **Strategy** field, select **Manual**. 2. In the **Interface Preference** field, select **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**.

5. Click **OK** to save the settings.
   The **SD-WAN Rules** section in your template should look similar to the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The members must be ordered as shown in the image—**HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**. You can drag and drop the members to reorder them, if required.

6. Click **OK** to save the template settings.

To install the device settings

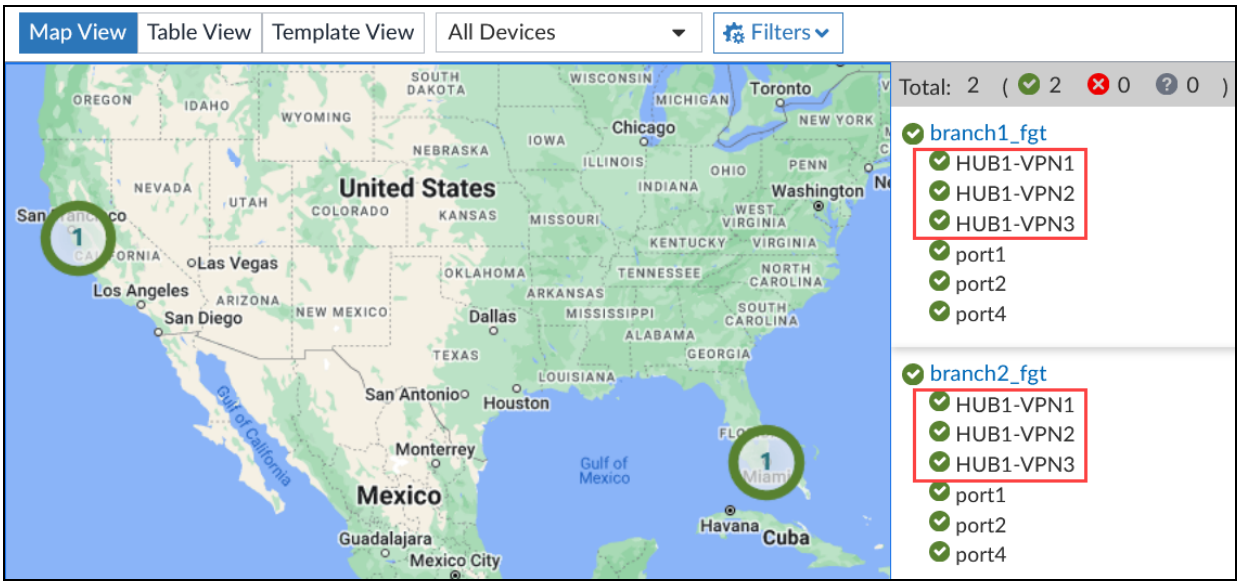
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Policy Package & Device Settings**.
3. Select the **branches_pp** policy package, and then click **Next**.
4. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
5. Click **Install** to install the configuration on both devices.
6. Wait for the installation to finish.
7. Click **Finish**.
8. Repeat the steps above to install the **dc_pp** policy package on the **dc1_fgt** hub device.

Verify the Overlays as SD-WAN Members

You will verify the overlays as SD-WAN members using the FortiManager GUI and FortiGate CLI.

To verify the overlays using FortiManager

1. Continuing on the FortiManager GUI, click **Device Manager** > **Monitors** > **SD-WAN Monitor** > **Map View**. Your page should look similar to the following example:



Note that you might need to adjust the map size to view the circle for FortiGate devices.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The overlay tunnels, **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**, are configured as SD-WAN members and are up (green check mark).

To verify the overlays using the FortiGate CLI

1. Open one SSH session to branch1_fgt, and another to branch2_fgt.
2. Log in to each device with the following credentials:
   - Username: `admin`
   - Password: `password`
3. On each device, enter the following commands to verify the SD-WAN members and zones:

```
show system sdwan
diagnose sys sdwan zone
diagnose sys sdwan member
```

The following image shows an example of branch2_fgt:

```
branch2_fgt # show system sdwan
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "underlay"
        next
        edit "WAN3"
        next
        edit "HUB1"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
            set gateway 203.0.113.2
        next
        edit 2
            set interface "port2"
            set zone "underlay"
            set gateway 203.0.113.10
        next
        edit 3
            set interface "port4"
            set zone "WAN3"
        next
        edit 4
            set interface "HUB1-VPN1"
            set zone "HUB1"
        next
        edit 5
            set interface "HUB1-VPN2"
            set zone "HUB1"
        next
        edit 6
            set interface "HUB1-VPN3"
            set zone "HUB1"
        next
    end
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch2_fgt # diag sys sdwan zone
Zone HUB1 index=4
        members(3): 20(HUB1-VPN1) 21(HUB1-VPN2) 22(HUB1-VPN3)
Zone WAN3 index=3
        members(1): 6(port4)
Zone underlay index=2
        members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
        members(0):
```

```
branch2_fgt # diag sys sdwan member
Member(1): transport-group: 0, interface: port1, flags=0x0 , gateway: 203.0.113.2, source 203.0.113.1, prior
Member(2): transport-group: 0, interface: port2, flags=0x0 , gateway: 203.0.113.10, source 203.0.113.9, prio
Member(3): transport-group: 0, interface: port4, flags=0x0 ,source 172.16.0.9, priority: 1 1024, weight: 0
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xc , gateway: 100.64.1.1, source 192.168.1.2, pr
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xc , gateway: 100.64.1.9, source 192.168.1.66, p
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xc , gateway: 172.16.1.5, source 192.168.1.130,
```

The overlay tunnels were configured as SD-WAN members by the SD-WAN overlay template and placed in the `HUB1` zone.

4. Enter the following command to verify the tunnel IDs:

```
diagnose vpn tunnel list
```

```
branch2_fgt # branch2_fgt # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----------------------------------------------------
name=HUB1-VPN1 ver=2 serial=1 203.0.113.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1
status=up dst_mtu=1500 weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/568 options[0238]=npu create_dev frag-rf
c  role=primary accept_traffic=1 overlay_id=1
```

Note that the image above shows only the beginning of the output for this command.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Onboarding a New Branch With ZTP

In Lab 2, you added branch2_fgt to FortiManager and to the SD-WAN topology using a step-by-step process. In this exercise, you will use ZTP techniques to add branch3_fgt to your SD-WAN topology. Note that you can use the ZTP process the same way to onboard 100 devices, and even more, simultaneously.

To add branches to your SD-WAN topologies, first, you will create a device blueprint. Then, you will add the branch using a CSV file. Then, you will see ZTP in action and onboard a device from factory default settings to a member of the SD-WAN topology, with rules and overlay tunnels configured.

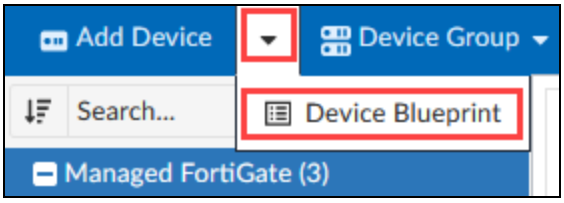
ZTP is optimized to work with metadata variables. Because, in the first two labs, you used other techniques, such as dynamic firewall objects or user-defined normalized interfaces, you will perform some preliminary tasks and use scripts to accommodate those parameters. This is a common scenario when you use ZTP to extend a topology that is already in production.

Create Device Blueprints

You will create a device blueprint to instruct FortiManager how to associate specific types of devices with the required provisioning templates. branch3_fgt is a FortiGate VM. You will create two blueprints—one for the FortiGate VM and one for the FortiGate 40F hardware model.

To create device blueprints

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Device & Groups**.
3. Beside **Add Device**, in the drop-down list, select **Device Blueprint**.



4. Click **Create New**, and then configure the following settings:

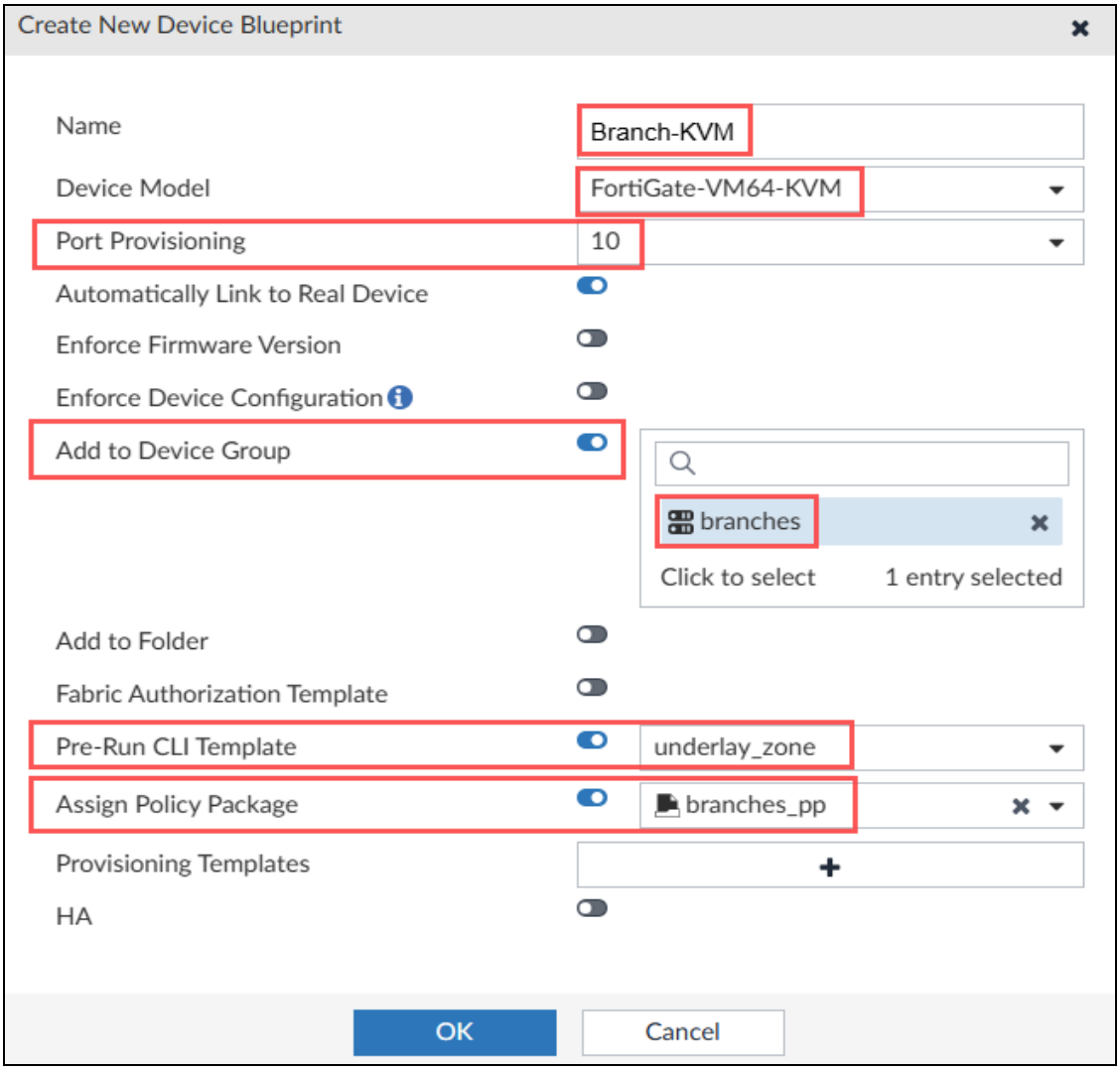
Field	Value
Name	Branch-KVM
Device Model	FortiGate-VM64-KVM
Port Provisioning	10
Automatically Link to Real Device	Enabled (default)

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Add to Device Group	Enable, and then select **branches**.
Pre-Run CLI Template	Enable, and then select **underlay_zone**.
Assign Policy Package	Enable, and then select **branches_pp**.

Your page should look similar to the following example:



In the **Device Model** drop-down list, you can see **FortiOS-VM64-KVM** and **FortiGate-VM64-KVM**. Make sure that you select **FortiGate-VM64-KVM**. This is the device type that is used in this lab.

FortiOS VM devices are smaller and used only in specific environments, such as closed networks.

5. Click **OK**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

You didn't select the provisioning template for this device model. Why?

You defined the blueprint to assign all devices of the corresponding type to the device group branches. You have already defined the **Corp-SOT_BRANCH** template group to apply to all devices in the group branches, and therefore, it is enough to define the template with the template group. The **Corp-SOT_BRANCH** template group will apply to all devices in this group.

Stop and think!

What's the purpose of pre-run CLI templates?

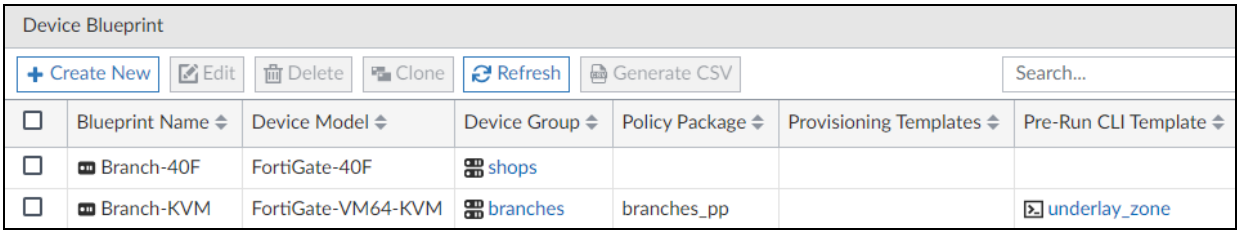
A pre-run CLI template helps with the definition of data or variables that are not defined by other templates, or elements where the definition would come too late in the template execution sequence.

In Lab 2, you created a static route template that references the underlay SD-WAN zone. When onboarding a device with ZTP, the static route template is executed before the SD-WAN template. The underlay_zone pre-run CLI template defines the zone so it is available for the static route template execution.

6. Repeat steps 4–5 to create a device blueprint for the FortiGate 40F devices, using the following settings:

Field	Value
Name	Branch-40F
Device Model	FortiGate-40F
Automatically Link to Real Device	Enabled
Add to Device Group	Enable, and then click **Click to select**. Click **+** to create a new group. Create a group named `shops`, select it, and then click **OK**.

After you create the two blueprints, your page should look similar to the following example:



You have created two blueprints to accommodate two types of FortiGate device models for your branches. As your network evolves and you add new device types, you can create new blueprints to accommodate them, and then assign the necessary groups or templates to them.

7. Click **Close**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

A device group can contain multiple device models, as long as they all share the same policy package, provisioning templates, and other blueprint parameters.

Declare New Devices

FortiManager allows you to declare your *devices to be deployed*—in other words, your branch devices—using a simple CSV file. For ZTP, FortiManager uses this CSV file to make the link between the device specific settings and the configuration that is already prepared, such as templates, blueprints, firewall policies, and so on.

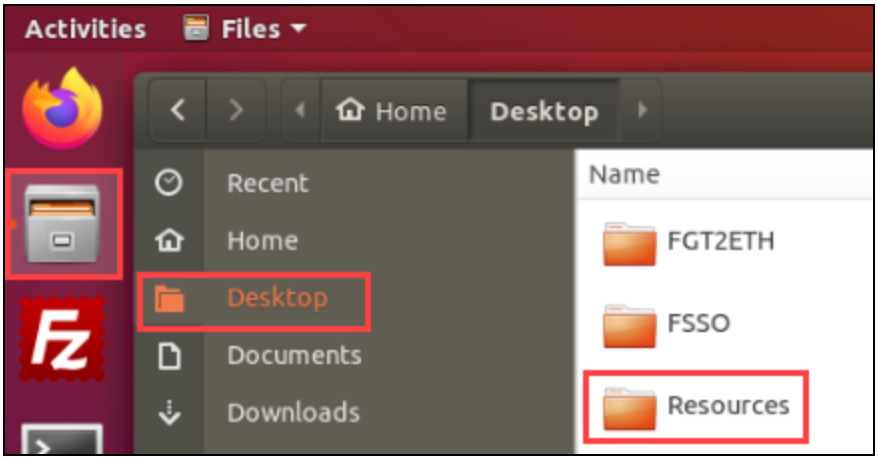
For ZTP deployment, the CSV file must contain the following items:

- The serial number for each FortiGate to be deployed
- The device blueprint to use
- Values for the metadata variables in use

In this task, you will use a CSV file that is already prepared for you, and update it.

To declare the new devices using a CSV file

1. Connect to the Local-client VM, and then log in with the following credentials:
   - Username: `Administrator`
   - Password: `password`
2. Open the **Files** manager, and then navigate to **Desktop** > **Resources**.



3. Double-click the **SD-WAN** folder, and then open the `branches-list.ods` file.

During the planning phase, the project team already prepared the file for you, in the form of a spreadsheet, which contains the device names, device location, and a few other values that correspond to the metadata variables defined in the templates.

It is common when devices are received, that the deployment team must complete the table to perform device onboarding. This is the phase that you will perform now.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

4. Review the columns and the values defined.

   The table contains information for the branches that are already onboarded—**branch1_fgt** and **branch2_fgt**— and two FortiGate 40F devices that are planned for future use. Line 6 contains a device serial number and a few values.

Scroll through the left of the table if you don't see the serial number that was configured for you on line 6.

5. Complete the last line with the following values:

Field	Value
Name	branch3_fgt
hostname	branch3_fgt
branch_id	3
lan_interface_ip	10.0.3.254

This spreadsheet corresponds to data you could receive from administrative teams who register the device serial numbers as they receive devices.

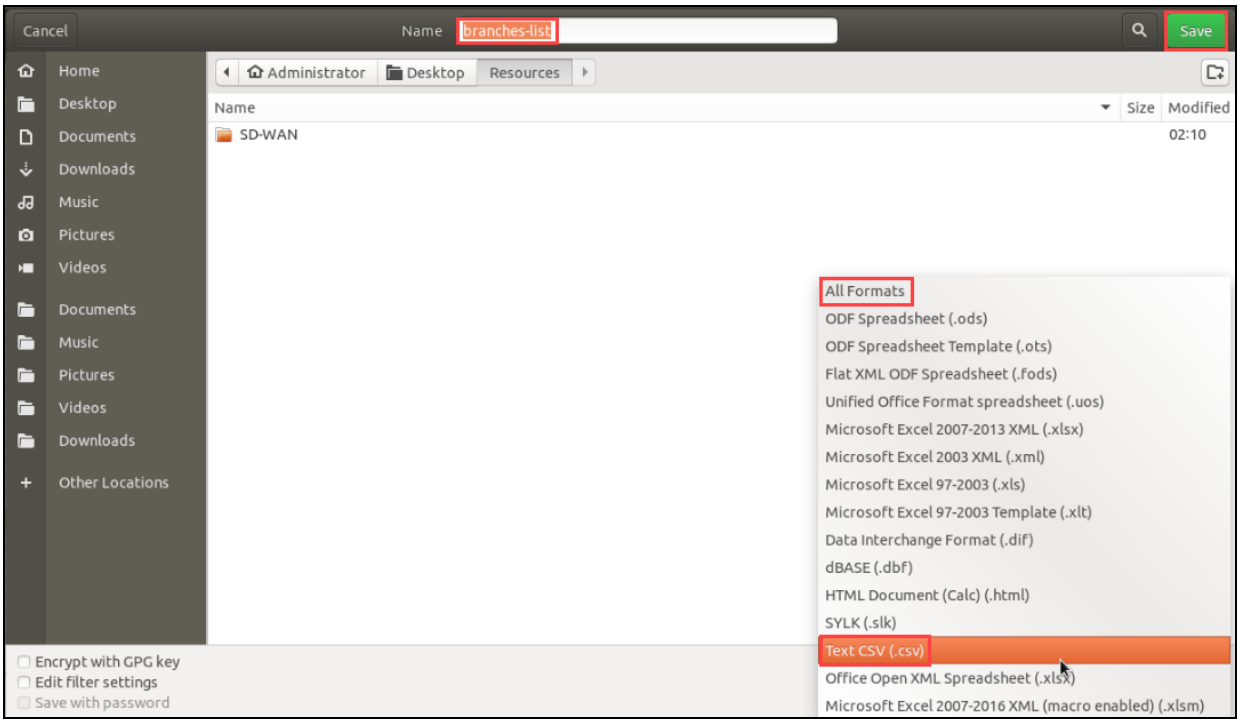
Make sure that you define the variables for every metadata variable that is used in the configuration that FortiManager will push to the device when it onboards it using ZTP.

For devices that have no values defined, FortiManager uses the default values for the metadata variables.

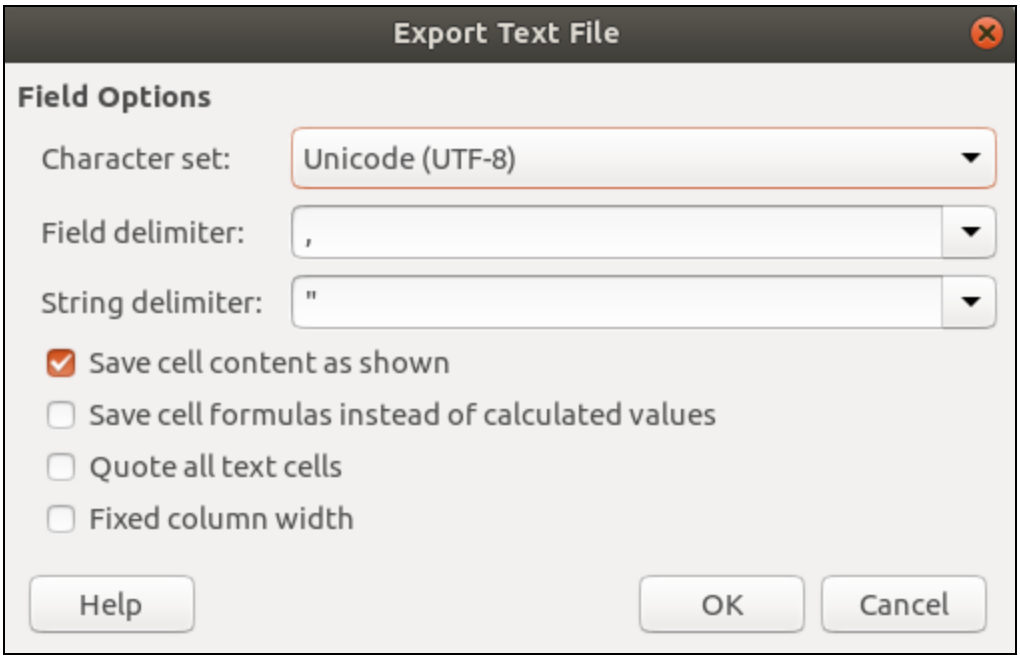
6. Save the file as a spreadsheet with its current `.ods` extension.
7. Click **File** > **Save As**, click **All Formats**, scroll through the list, and then select **Text CSV (.csv)**.
8. Keep the `branches-list` filename, and then click **Save**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



9. When prompted, click **Use Text CSV Format** to confirm the file format selection.
10. In the **Field delimiter** field, keep the comma, and then leave the other fields at the default values.



11. Click **OK**.
12. In the **Files** manager, navigate to **Desktop** > **Resources** > **SD-WAN**.
13. Confirm that you see the following two files: `branches-list.ods` and `branches-list.csv`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

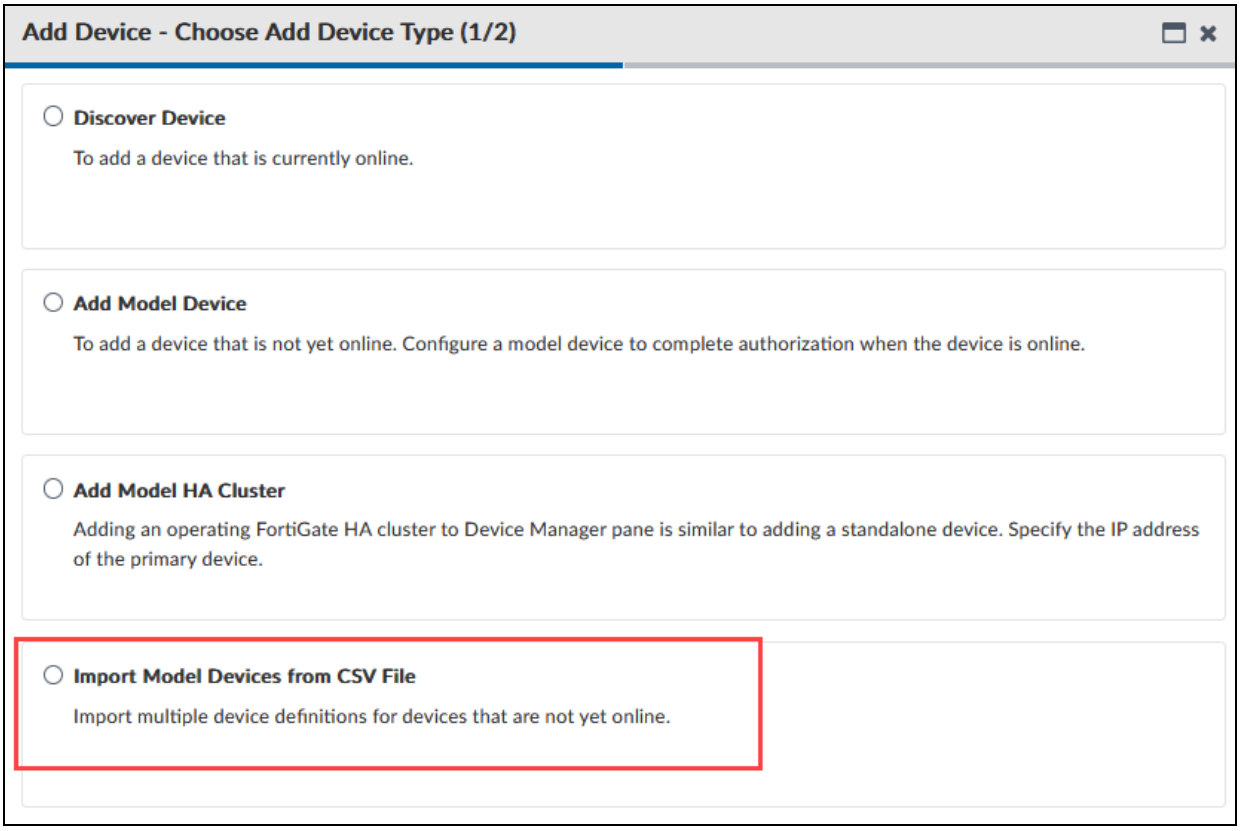
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To import the CSV file into FortiManager

1. Continuing on the Local-client VM, open Firefox, and then enter `https://192.168.0.15` to connect to the FortiManager GUI.

   Alternatively, you can click the **fmg** bookmark.

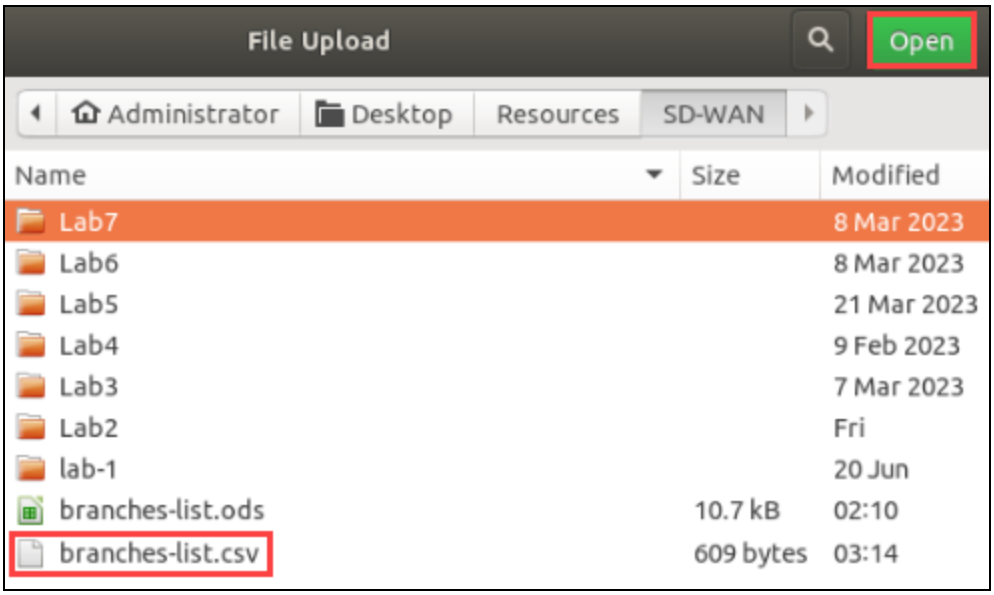
2. Log in to the FortiManager GUI with the following credentials:
   - Username: `admin`
   - Password: `password`
3. Click **Device Manager** > **Device & Groups**, and then click **Add Device**.
4. Select **Import Model Devices from CSV File**.



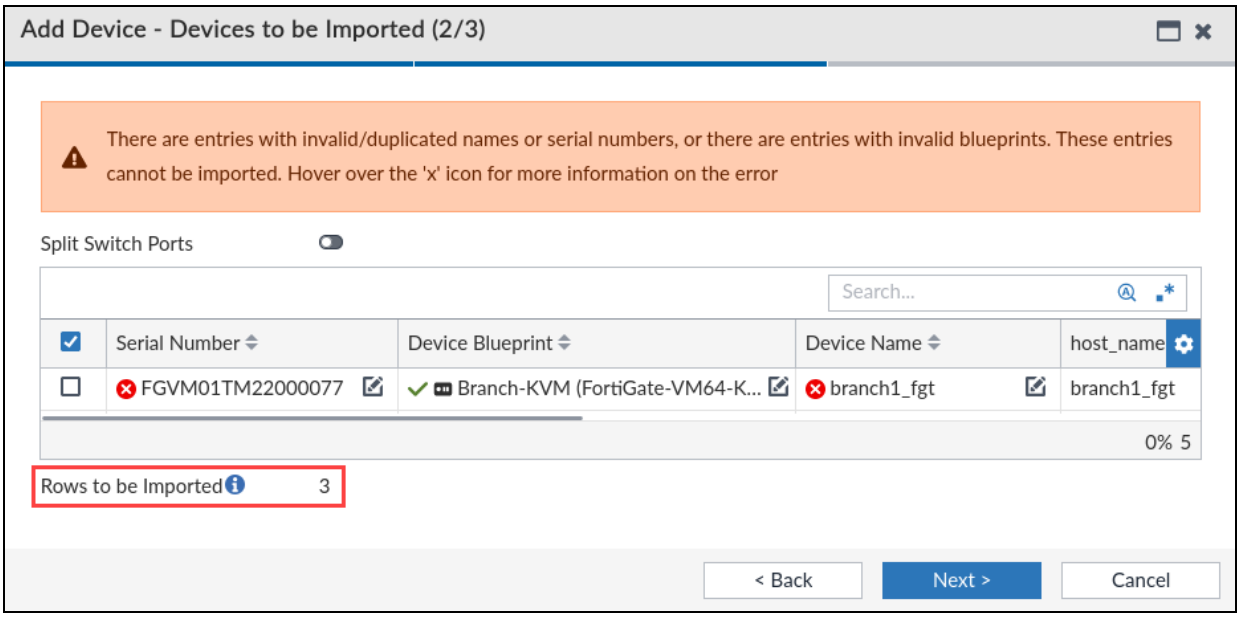
5. In the **Copy Device Dashboard** field, select **branch1_fgt [global]**.
6. In the **Upload** field, click **Add Files**.
7. Navigate to **Desktop** > **Resources** > **SD-WAN**, and then select the `branches-list.csv` CSV file that you prepared in the previous procedure.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



8. Click **Open**.
   A warning message appears, as shown in the following example:



9. Hover over the red x to see details about the warning.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

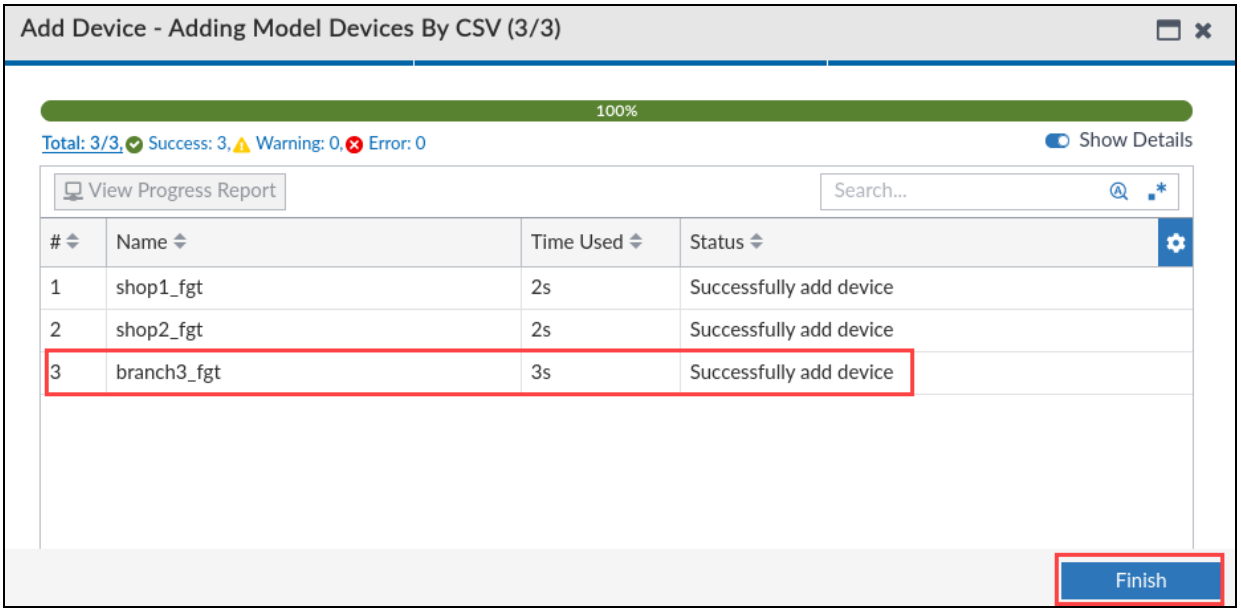
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

FortiManager ignores the lines in CSV files that contain serial numbers or device names that correspond to devices it is already managing. This prevents the overwriting of variable values with unwanted changes for devices that are already in production.

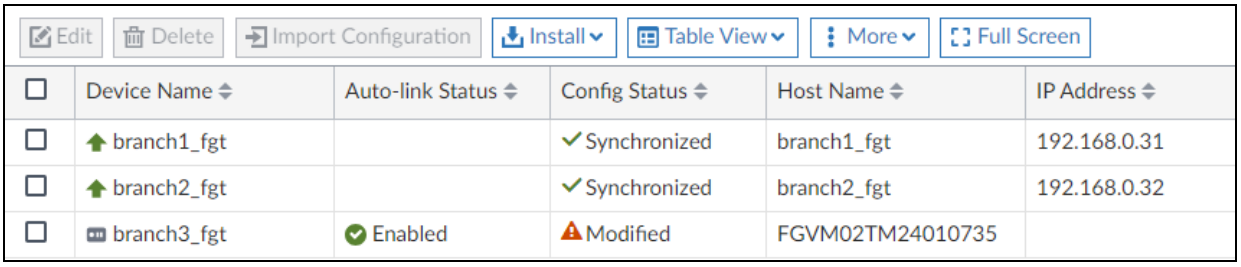
Additionally, this allows the preparation of a CSV file that contains all devices for a project. Some are already installed and others have not been deployed yet.

The value on the **Rows to be Imported** line indicates the number of lines that have valid device definitions. These are lines where FortiManager detected no errors or duplicate devices.

10. Review the **Rows to be Imported** field, and then confirm that FortiManager will import three lines.
11. Click **Next**, and then wait for FortiManager to finish adding the devices.
    Your page should look similar to the following example:



12. Click **Finish**.
13. Click **Device Manager** > **Device & Groups** > **branches**.
    Your page should look similar to the following example:



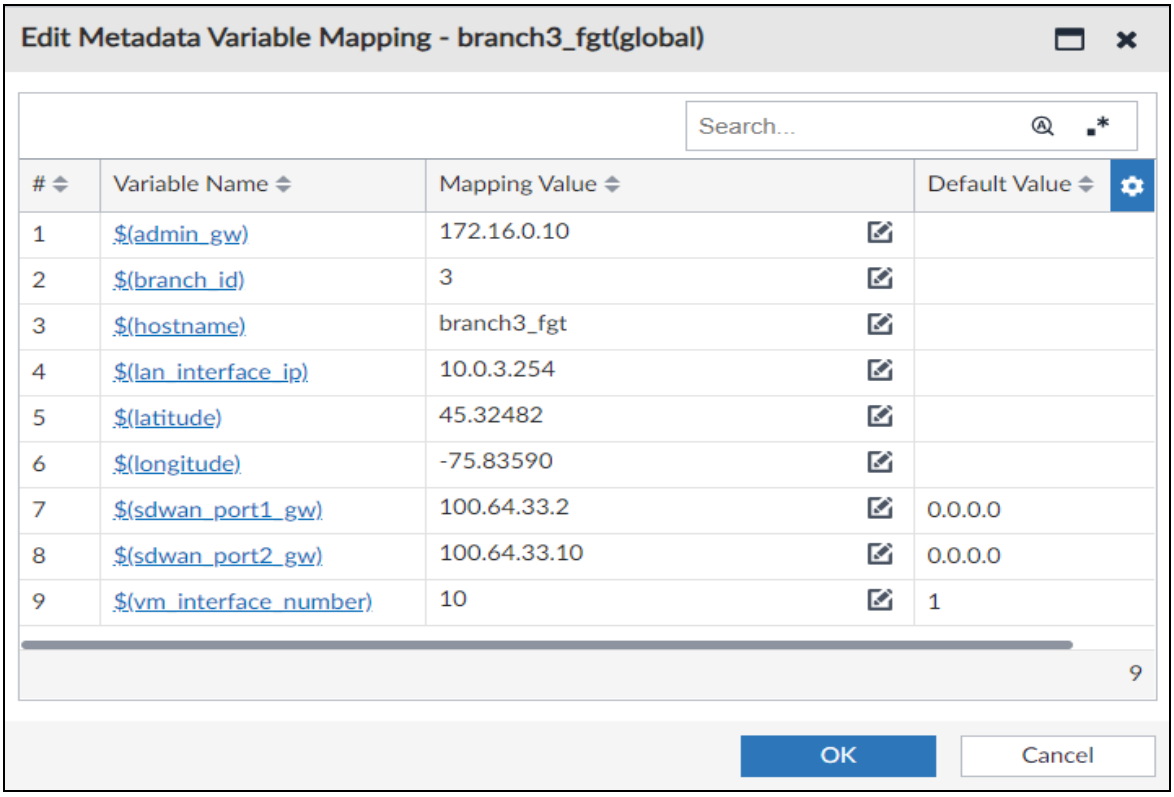
FortiManager shows **branch3_fgt** with a gray device icon and no IP address because it cannot establish a connection with the device yet.

14. Right-click **branch3_fgt**, and then select **Edit Variable Mapping**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Your page should look similar to the following example:



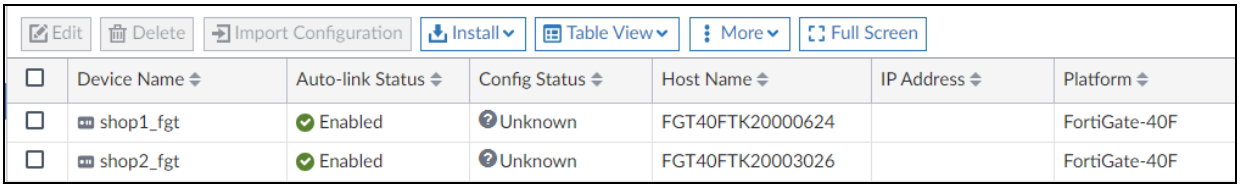
#	Variable Name	Mapping Value	Default Value
1	$(admin_gw)	172.16.0.10	
2	$(branch_id)	3	
3	$(hostname)	branch3_fgt	
4	$(lan_interface_ip)	10.0.3.254	
5	$(latitude)	45.32482	
6	$(longitude)	-75.83590	
7	$(sdwan_port1_gw)	100.64.33.2	0.0.0.0
8	$(sdwan_port2_gw)	100.64.33.10	0.0.0.0
9	$(vm_interface_number)	10	1

9

You can see that FortiManager has set the metadata variable values for **branch3_fgt** according to the entries in the CSV file.

FortiManager defines new metadata variables for any column name in the CSV file that does not correspond to an existing variable.

15. Click **Cancel**.
16. Note the new **shops** device group, and then click it to discover the devices in this group.
    Your page should look similar to the following example:



Device Name	Auto-link Status	Config Status	Host Name	IP Address	Platform
shop1_fgt	Enabled	Unknown	FGT40FTK20000624		FortiGate-40F
shop2_fgt	Enabled	Unknown	FGT40FTK20003026		FortiGate-40F

When the CSV file was imported, FortiManager defined **branch3_fgt** and two shop devices, **shop1_fgt** and **shop2_fgt**. It placed them in the **branches** and **shops** groups respectively.

To update the CLI templates

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **CLI**.
2. Double-click the **global-setting** template to edit it.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

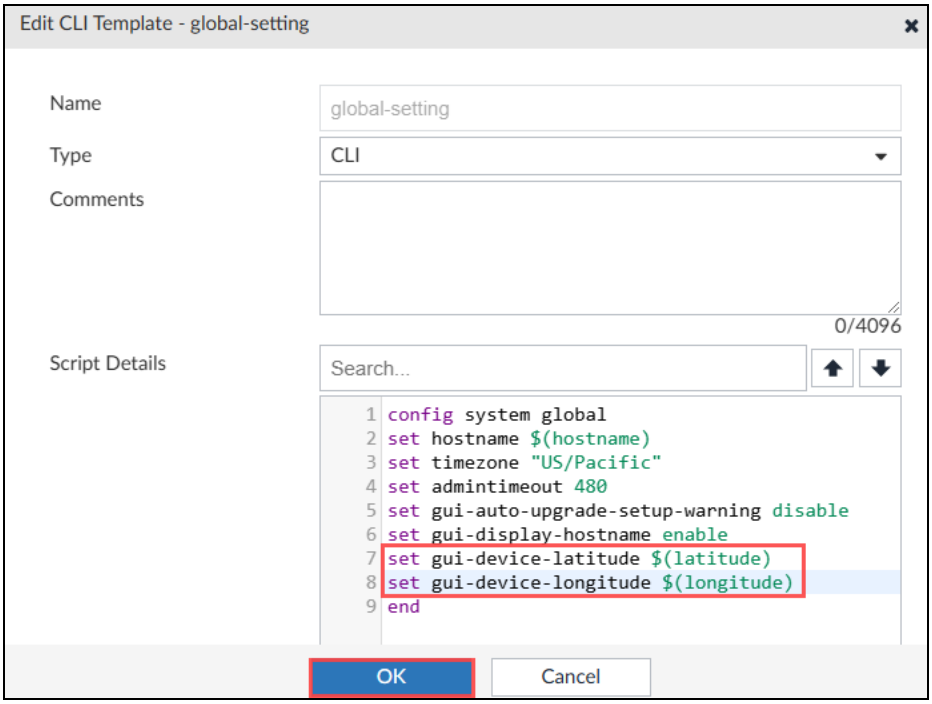
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

This template sets the admin timeout, time zone, and device host name using a metadata variable.

Note the `set gui-display-hostname enable` command. This instructs FortiGate to display the device host name on the GUI login page.

3. Before the `end` line, add the following commands:

```
set gui-device-latitude $latitude
set gui-device-longitude $longitude
```



4. Click **OK**.

When you type `$` in a script, FortiManager prompts you with the list of metadata variables that are already defined. You can select one of the variables or create a new one.

5. Double-click the **LAN-interface** template to edit it.

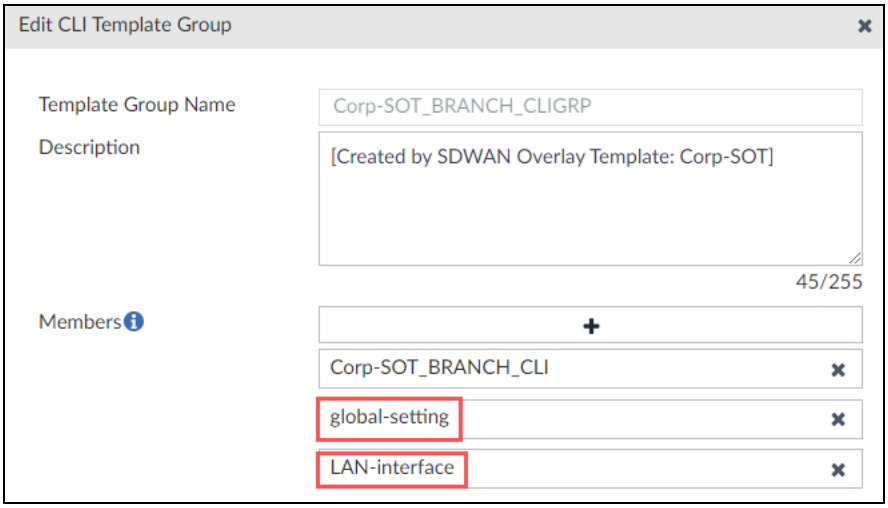
   This template sets the IP address of the LAN interface for each branch device. For each branch device, port5 is the LAN interface. Its IP address is defined with the branch ID metadata variable. It results in 10.0.1.254 for branch1_fgt, 10.0.2.254 for branch2_fgt, and 10.0.3.254 for branch3_fgt.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

This template also sets the DHCP mode for the port2 interface. The device model, FortiGate-VM-KVM, sets the static mode for port2, but in the lab topology, port2 gets its IP address from a DHCP server.

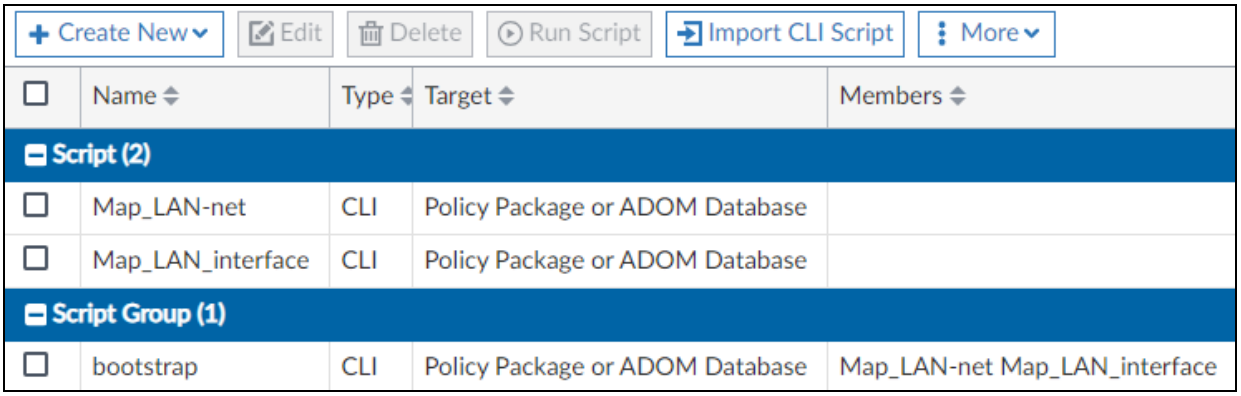
6. Click **Cancel**.
7. Edit **Corp-SOT_BRANCH_CLIGRP**.
8. Click **+**, add the **global-setting** and **LAN-interface** templates to the group, and then click **Close**.



9. Click **OK** to validate the CLI template group update.

To define additional per-device mappings

1. Continuing on the FortiManager GUI, click **Device Manager** > **Scripts**.
   Your output should look similar the following example:

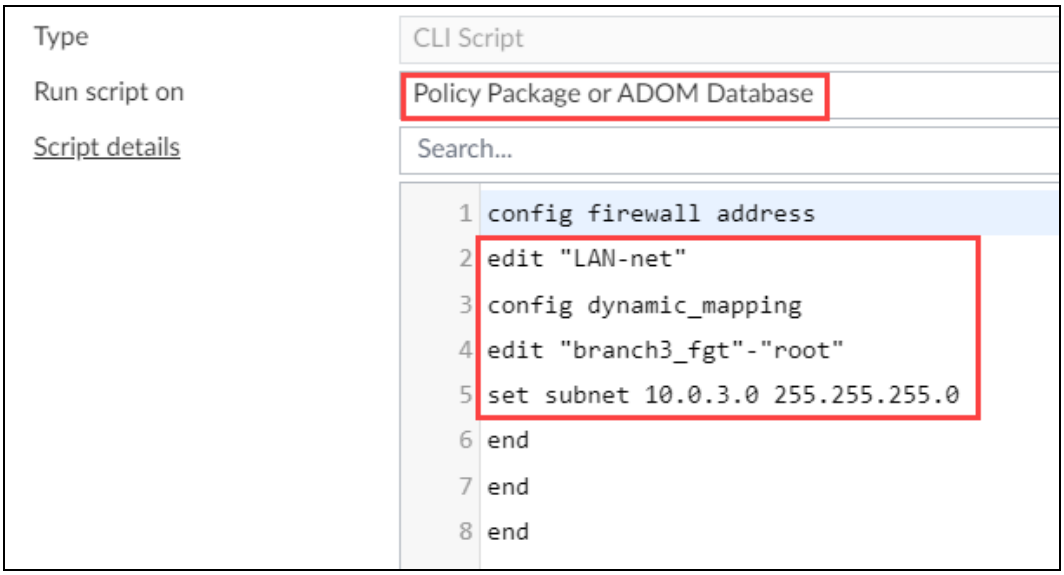


   The **Map_LAN-net** and **Map_LAN_interface** scripts, and the **bootstrap** script group have been predefined for you.

2. Open each script, and then review the content.
   - The **Map_LAN-net** script defines the LAN subnet for **branch3_fgt**.

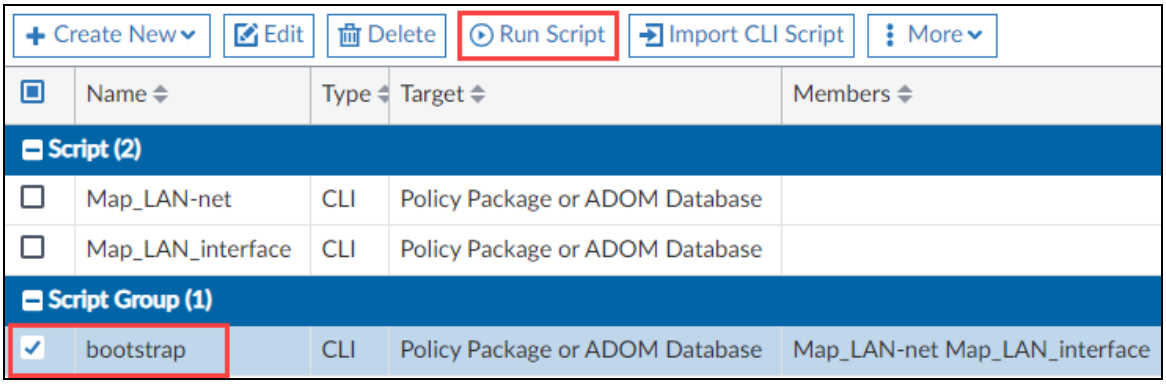
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



- The **Map_LAN_interface** script defines the dynamic mapping between the LAN normalized interface and port5 for **branch3_fgt**.
- Both scripts run on **Policy Package or ADOM Database**.
- The **bootstrap** script group regroups the two scripts.

3. Select the checkbox for **bootstrap**, and then click **Run Script**.



4. Keep the **default** policy package, and then click **Run Now**.
   You keep this policy package because you run these scripts on the ADOM database.
5. Wait for the **Run completed successfully** message, and then click **Close**.

Stop and think!

Why do you need to run these scripts?

In the previous exercise, you defined the LAN-net firewall object and LAN normalized interface with per-device dynamic mapping. This is a common way of configuring such objects, and is extensively used in FortiGate configurations.

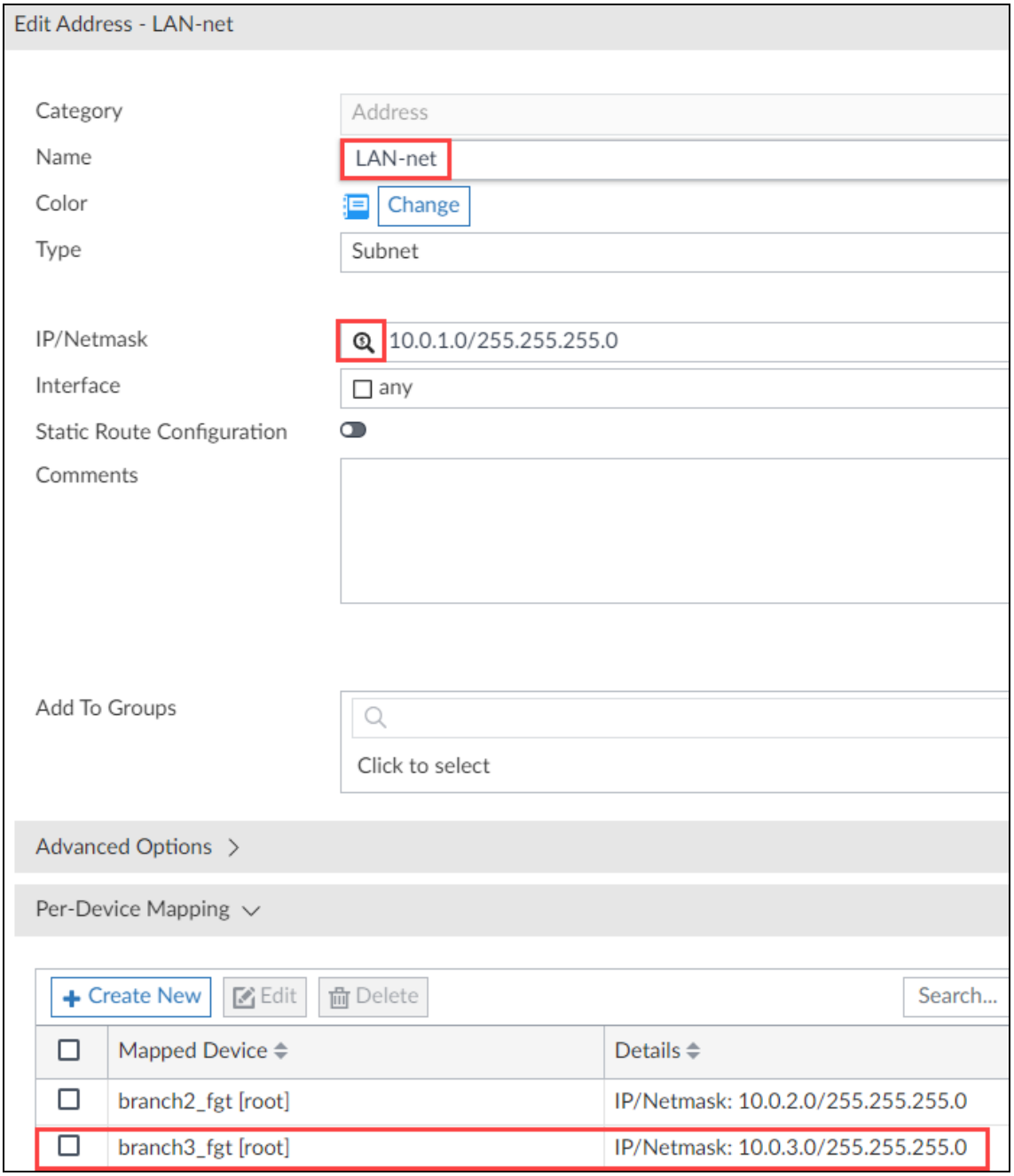
When planning ZTP configuration for the initial FortiGate configuration, you should prioritize the use of metadata variables. For example, you can define firewall addresses with either metadata variables or per-device mapping.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

6. Click **Policy & Objects** > **Firewall Objects** > **Addresses**.
7. Double-click **LAN-net** to edit it.

   Your page should look similar to the following example:



In the **IP/Netmask** field, the magnifying glass indicates that you can define the IP address and netmask for the firewall address objects with metadata variables. In the **Per-Device Mapping** section, you can see the **branch3_fgt** entry that the script created.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

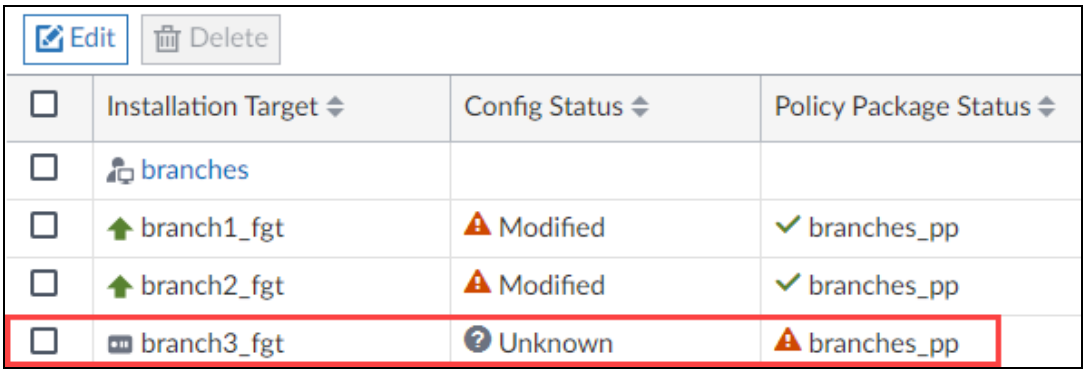
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

If you plan to use ZTP, use metadata variables instead of per-device mapping each time it is applicable. This simplifies ZTP deployment and limits the requirements of the scripts.

8. Click **Cancel**.

To validate the configuration on model devices

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
2. Expand **branches_pp**, and then click **Installation Targets**.



FortiManager added **branch3_fgt** in the installation target list for the **branches_pp** policy package.

3. Click **Install Wizard**, and then select **Install Policy Package & Device Settings**.
4. Select **branches_pp**, and then click **Next**.
5. Select **branch1_fgt**, **branch2_fgt**, and **branch3_fgt**, and then click **Next**.

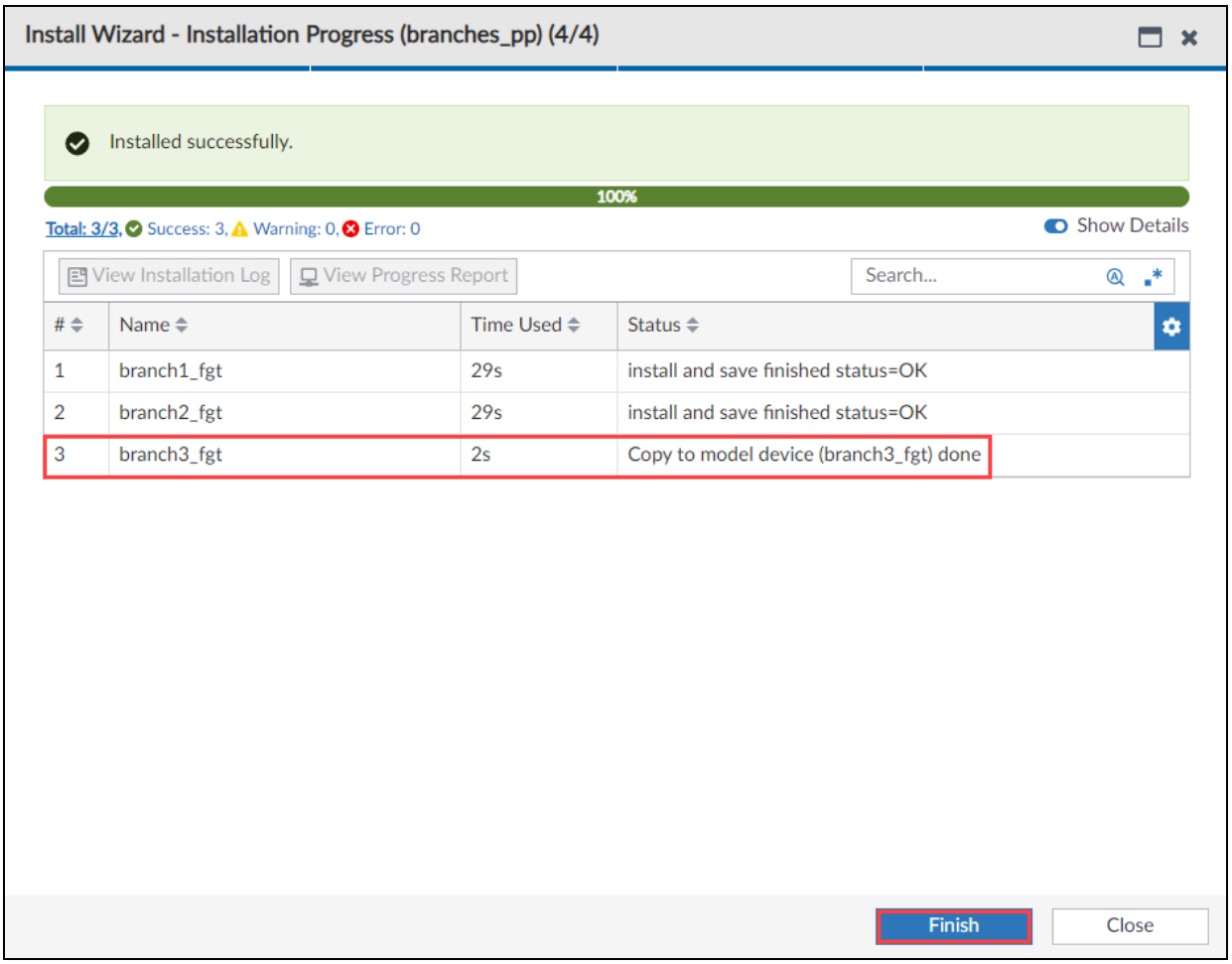
Validating the configuration on model devices is optional. However, these validations can help you identify errors or missing definitions before you onboard new devices.

FortiManager modified the configuration of **branch1_fgt** and **branch2_fgt** because you modified the CLI template group that is assigned to the branch devices.

6. Click **Install**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

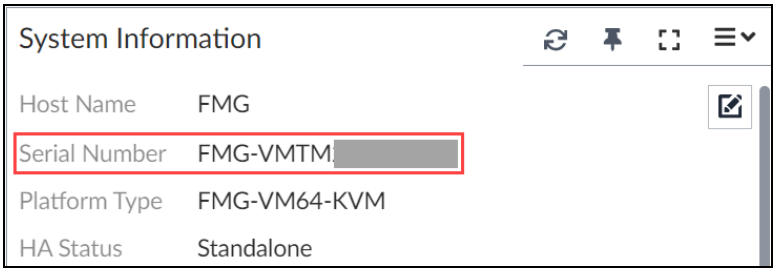
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



7. Wait for the installation to complete, and then click **Finish**.
   FortiManager validates the configuration for the branch3_fgt model device.

To collect the serial number of the FortiManager

1. Continuing on the FortiManager GUI, click **Dashboard**.
2. In the **System Information** widget, note the serial number of the FortiManager.
   You will need this information in the next exercise.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Deploy New Branch Devices

Now that you have prepared the templates and imported the variable values for the devices, you can deploy them and allow them to join your topology. You can use one of the following methods to configure the FortiGate with basic network settings:

- FortiCloud or FortiDeploy
- A local DHCP server with the 240 option code
- CLI script or batch CLI script
- USB drive

Note that the basic configuration must include the central management configuration and FortiManager serial number. FortiManager requires the serial number to authenticate the incoming FortiGate devices in ZTP scenarios.

For this exercise, the basic FortiGate configuration for branch3_fgt was done for you, except the FortiManager IP address and serial number.

To deploy a new branch device

1. Open an SSH session to branch3_fgt, and then log in to the FortiGate CLI with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Enter the following commands:
   ```
   show system interface port10
   show system central-management
   ```
   Your output should look similar to the following example:
   ```
   FortiGate-VM64-KVM # show system interface port10
   config system interface
       edit "port10"
           set vdom "root"
           set ip 192.168.0.33 255.255.255.0
           set allowaccess ping https ssh http fgfm
           set type physical
           set snmp-index 10
       next
   end

   FortiGate-VM64-KVM # sho system central-management
   config system central-management
       set type none
       set allow-push-firmware disable
       set allow-remote-firmware-upgrade disable
       config server-list
           edit 1
               set server-type update rating
               set server-address 192.168.0.15
           next
       end
       set include-default-servers disable
   end
   ```

   port10 is the interface used to connect the branch devices to the management network. It was configured for you with the IP address 192.168.0.33/24.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The device name is not set and there is no central management configured for this device—the central-management type is set to `none`.

3. Enter the following commands to allow central management on branch3_fgt:

```
config system central-management
   set type fortimanager
   set fmg 192.168.0.15
   set serial-number <FortiManager serial number>
end
```

Enter the FortiManager serial number that you collected in the previous exercise. It should be in the form `FMG-VMTMxxxxxxxx`.

When FortiGate boots from factory default settings, it gets its IP address, subnet mask, and network gateway to configure its management interface from the DHCP server. It also gets the DNS and FortiManager IP addresses.

To automatically enable central management on FortiGate, you must configure the option 240.

FortiGate accepts the FortiManager IP address with the option 240 only when it boots with a factory default configuration. This prevents the risk of FortiManager IP address spoofing on device boot or DHCP renew.

4. Continuing on the FortiManager GUI, click **System Settings** > **Task Monitor**.
5. Refresh the browser page.

   After a few minutes, your page should look similar to the following example:

Source	Description	User	Status
Device Manager	Autolinking Device	A Auto link	50%
Install Package	Install package to device from commit	A admin	Success: 3

You might see failures for the first autolink attempts. Autolink should succeed without any other manual action within 2–3 minutes.

6. Wait 1–2 minutes, and then refresh the browser page again.

   Your page should look similar to the following example:

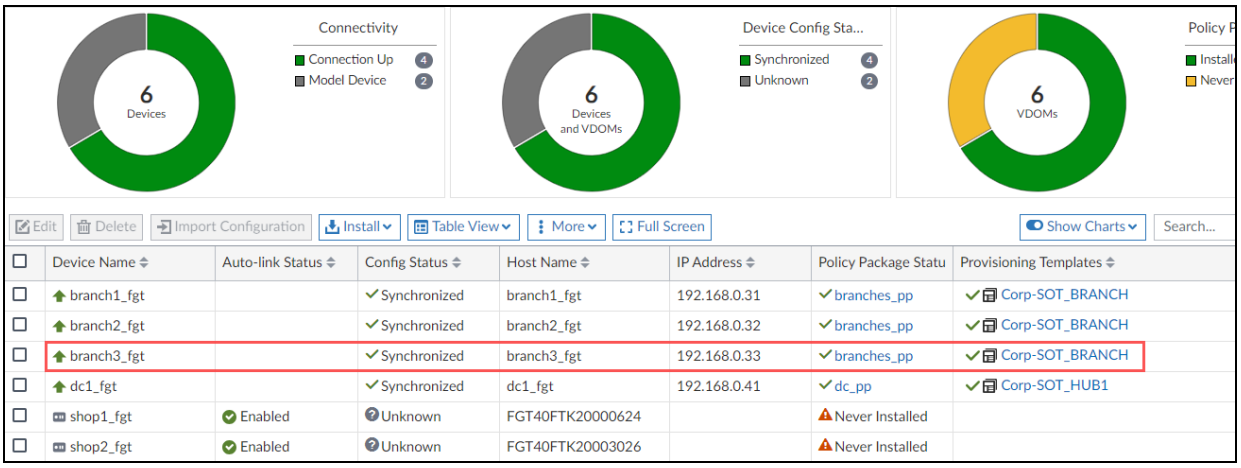
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Source	Description	User	Status	Time Used
Install Configuration	Push config to device	A admin	Success: 1	1m 40s
Device Manager	Autolinking Device	A Auto link	Success: 1	2m 6s
Install Package	Install package to device from commit	A admin	Success: 3	30s

To review the results

1. Click **Device Manager** > **Device & Groups** > **Managed FortiGate**.
   Your page should look similar to the following example:



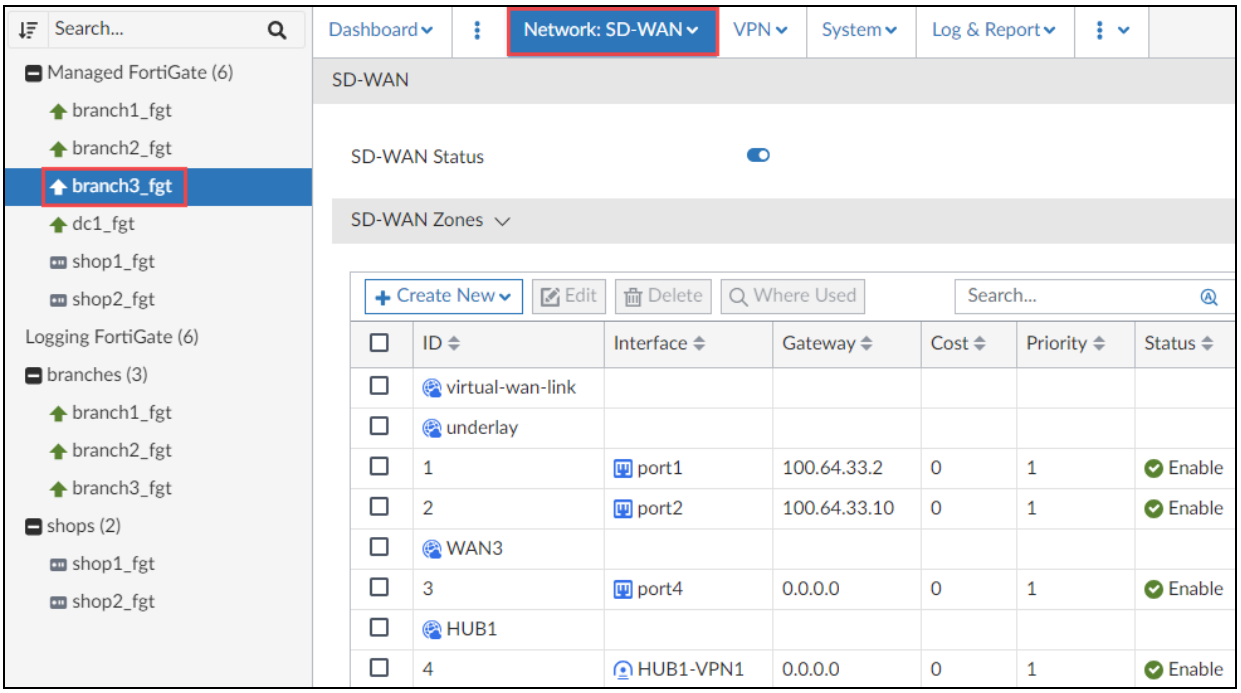
   The **branch3_fgt** FortiGate is managed by FortiManager. It is up and running, and configured with the policy packages and templates, similar to the other branch devices.

   FortiManager manages six devices. The three branch devices and the **dc1_fgt** hub have synchronized configurations and policy packages. The two shop devices are defined, but are not connected yet.

2. Double-click **branch3-fgt**, and then click **Network** > **SD-WAN**.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



FortiManager configured branch3_fgt with an SD-WAN configuration similar to the one installed on the other branches.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 3: Monitoring SD-WAN With FortiManager

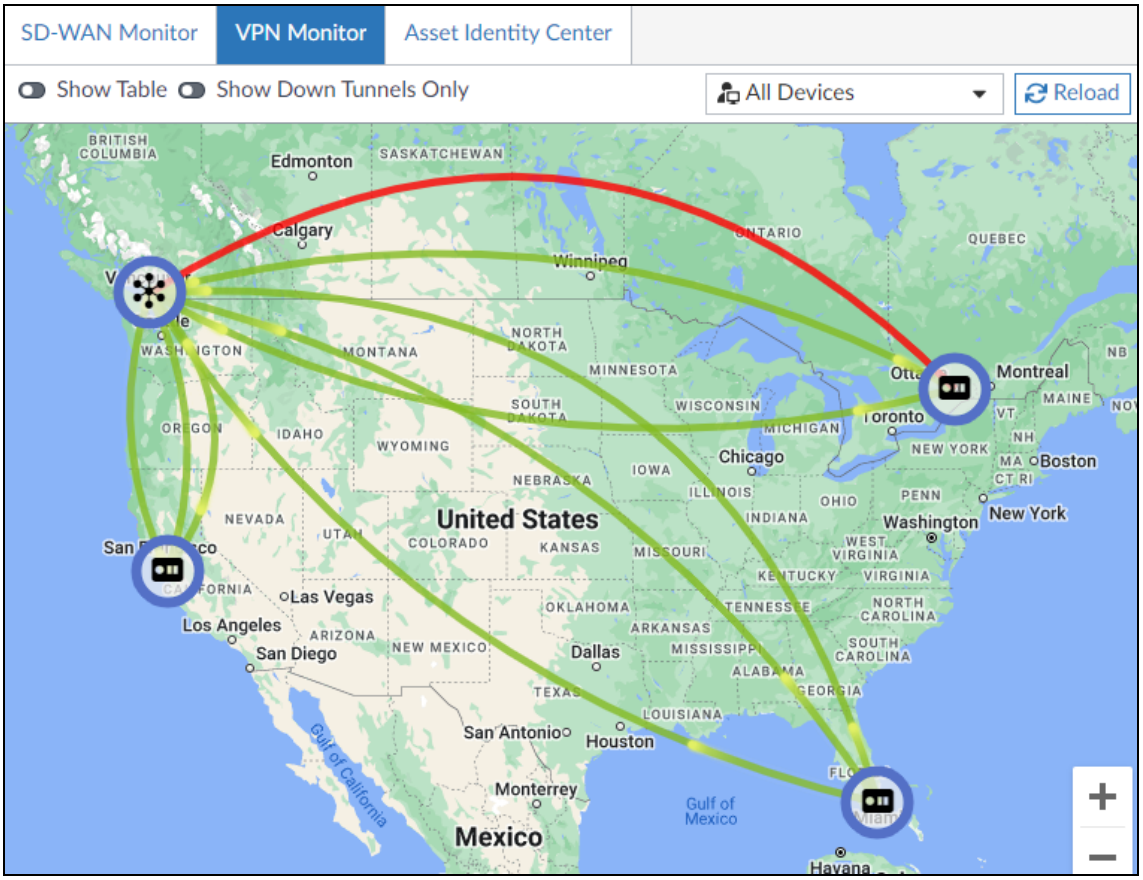
In this exercise, you will use the FortiManager GUI to review the overlay tunnel status and the SD-WAN topology that you deployed in the previous exercises. First, you will discover the menus that are available to monitor the VPN tunnels. Next, you will discover the menus that are available to monitor your SD-WAN topology.

Review the VPN Tunnel Status

In Lab 2, you used the SD-WAN overlay template to configure three overlay VPNs, and in the previous exercise, you used ZTP to push a similar configuration to a third branch device. In this task, you will review the tunnels for those three branch devices on the FortiManager GUI.

To review the VPN tunnel status

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Monitors** > **VPN Monitor**.
   You can view the tunnels on a map. Your page should look similar to the following example:



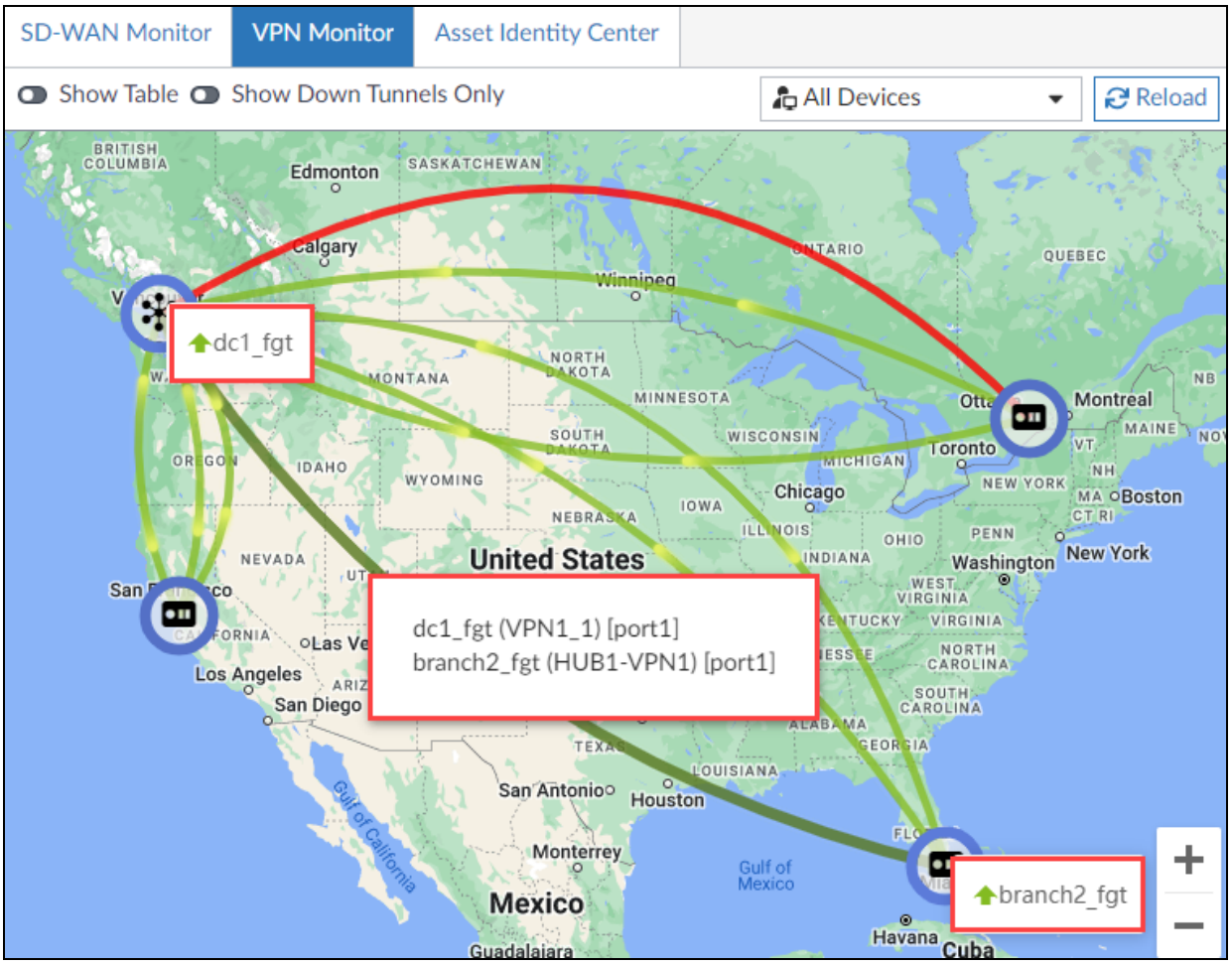
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Note that you might need to adjust the map size to view the four FortiGate devices.

The port4 interface is connected but did not receive an IP address on branch3_fgt. So, it is expected to see the third tunnel down.

3. Hover over some VPN links to see the details.



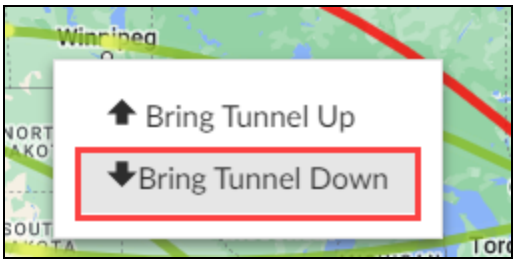
The example above shows the details for the tunnel between branch2_fgt and dc1_fgt. It connects to dc1_fgt on port1 and is identified as VPN1_1. On branch2_fgt, the tunnel is also built on port1 and its name is HUB1-VPN1.

On this map, you can bring tunnels up and down.

4. Right-click a link, and then select **Bring Tunnel Down**.

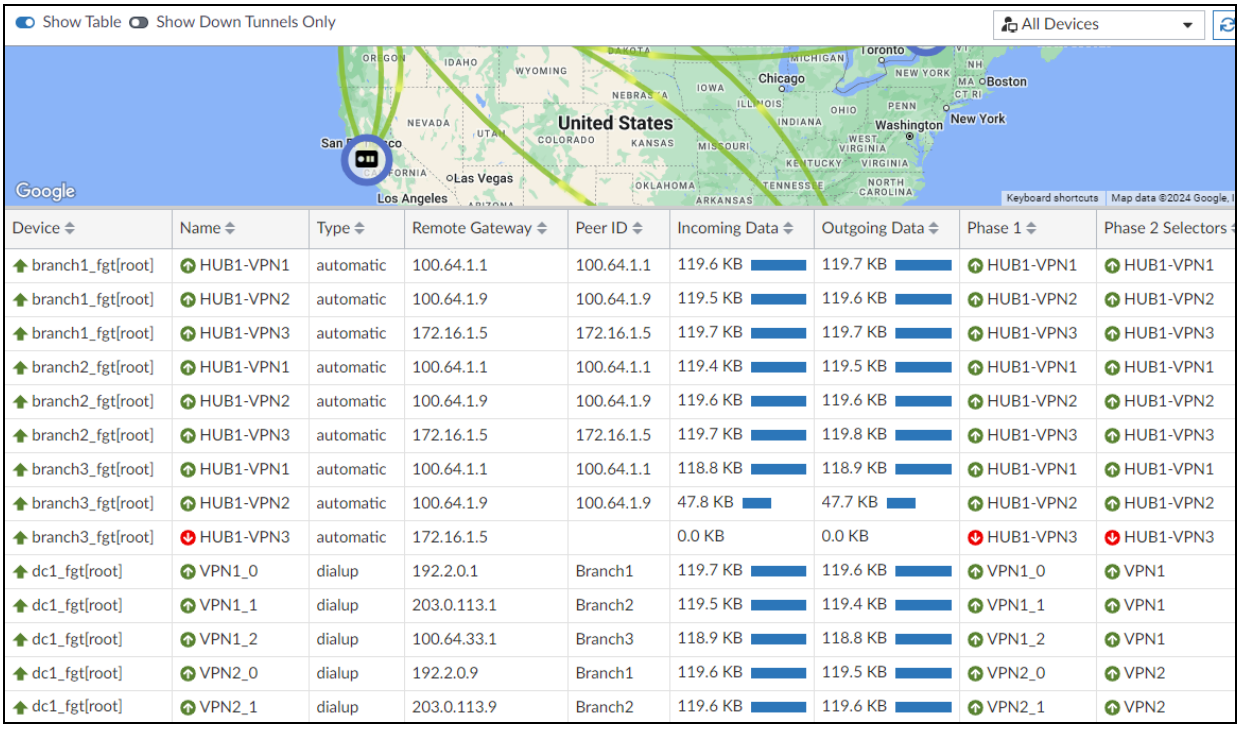
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



5. Click **OK** to validate the warning message.
6. Repeat the previous steps and select **Bring Tunnel Up**.
7. Verify that the link has returned to green to confirm the result.
8. Select **Show Table**.

   Your page should look similar to the following example:



Device	Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
branch1_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	119.6 KB	119.7 KB	HUB1-VPN1	HUB1-VPN1
branch1_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	119.5 KB	119.6 KB	HUB1-VPN2	HUB1-VPN2
branch1_fgt[root]	HUB1-VPN3	automatic	172.16.1.5	172.16.1.5	119.7 KB	119.7 KB	HUB1-VPN3	HUB1-VPN3
branch2_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	119.4 KB	119.5 KB	HUB1-VPN1	HUB1-VPN1
branch2_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	119.6 KB	119.6 KB	HUB1-VPN2	HUB1-VPN2
branch2_fgt[root]	HUB1-VPN3	automatic	172.16.1.5	172.16.1.5	119.7 KB	119.8 KB	HUB1-VPN3	HUB1-VPN3
branch3_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	118.8 KB	118.9 KB	HUB1-VPN1	HUB1-VPN1
branch3_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	47.8 KB	47.7 KB	HUB1-VPN2	HUB1-VPN2
branch3_fgt[root]	HUB1-VPN3	automatic	172.16.1.5		0.0 KB	0.0 KB	HUB1-VPN3	HUB1-VPN3
dc1_fgt[root]	VPN1_0	dialup	192.2.0.1	Branch1	119.7 KB	119.6 KB	VPN1_0	VPN1
dc1_fgt[root]	VPN1_1	dialup	203.0.113.1	Branch2	119.5 KB	119.4 KB	VPN1_1	VPN1
dc1_fgt[root]	VPN1_2	dialup	100.64.33.1	Branch3	118.9 KB	118.8 KB	VPN1_2	VPN1
dc1_fgt[root]	VPN2_0	dialup	192.2.0.9	Branch1	119.6 KB	119.5 KB	VPN2_0	VPN2
dc1_fgt[root]	VPN2_1	dialup	203.0.113.9	Branch2	119.6 KB	119.6 KB	VPN2_1	VPN2

The SD-WAN overlay template configured the branches to establish dial-up VPN tunnels with the hub.

The VPN monitor table shows **automatic** for the tunnels on the branch side—the device that initiated the tunnel. It shows **dialup** on the hub side—the dial-up server.

Review the SD-WAN Status on the SD-WAN Monitor Page

The **SD-WAN Monitor** page provides a centralized view of your SD-WAN deployment. It summarizes data for all managed FortiGate devices. For SD-WAN topologies that are defined with an SD-WAN overlay template, you can

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

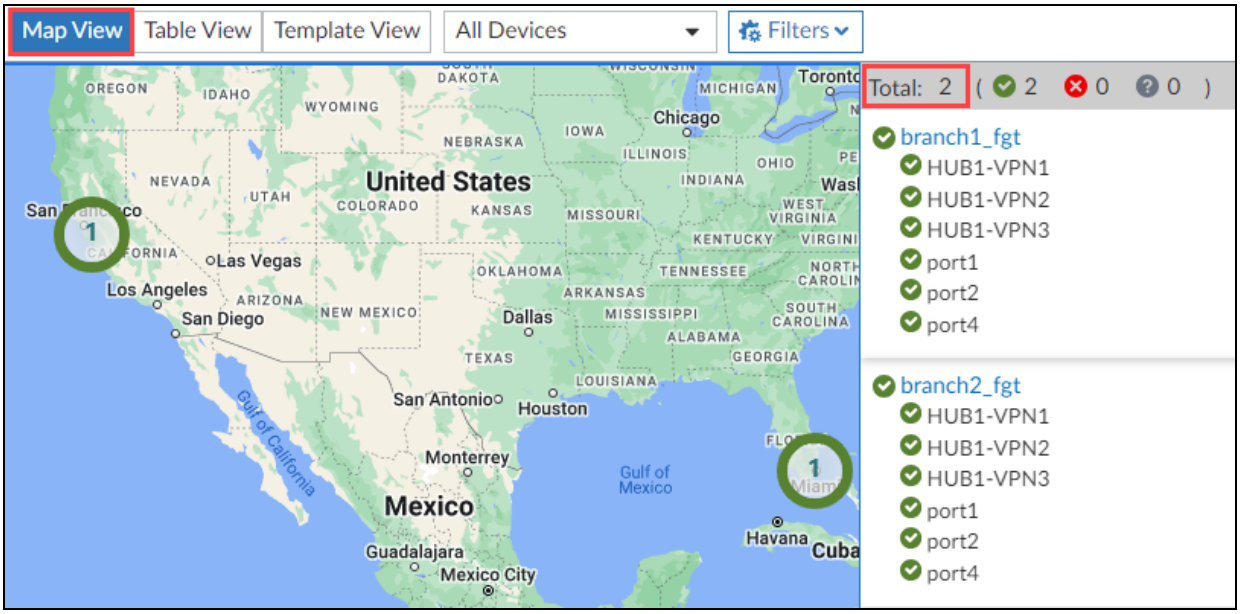
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

choose from three different views: a map, table, or template view. For any SD-WAN devices that FortiManager manages, you can choose between a map or table view.

To review the SD-WAN deployment in the map view

1. Continuing on the FortiManager GUI, click **Device Manager** > **Monitors**, and then select **SD-WAN Monitor** > **Map View**.

   Your page should look similar to the following example:



The list shows only the SD-WAN devices that are visible on the map.

On the map above, you can see two devices, even though three branch devices that this FortiManager manages have an SD-WAN configuration.

Navigate through the map or reduce its scale to view the other device.

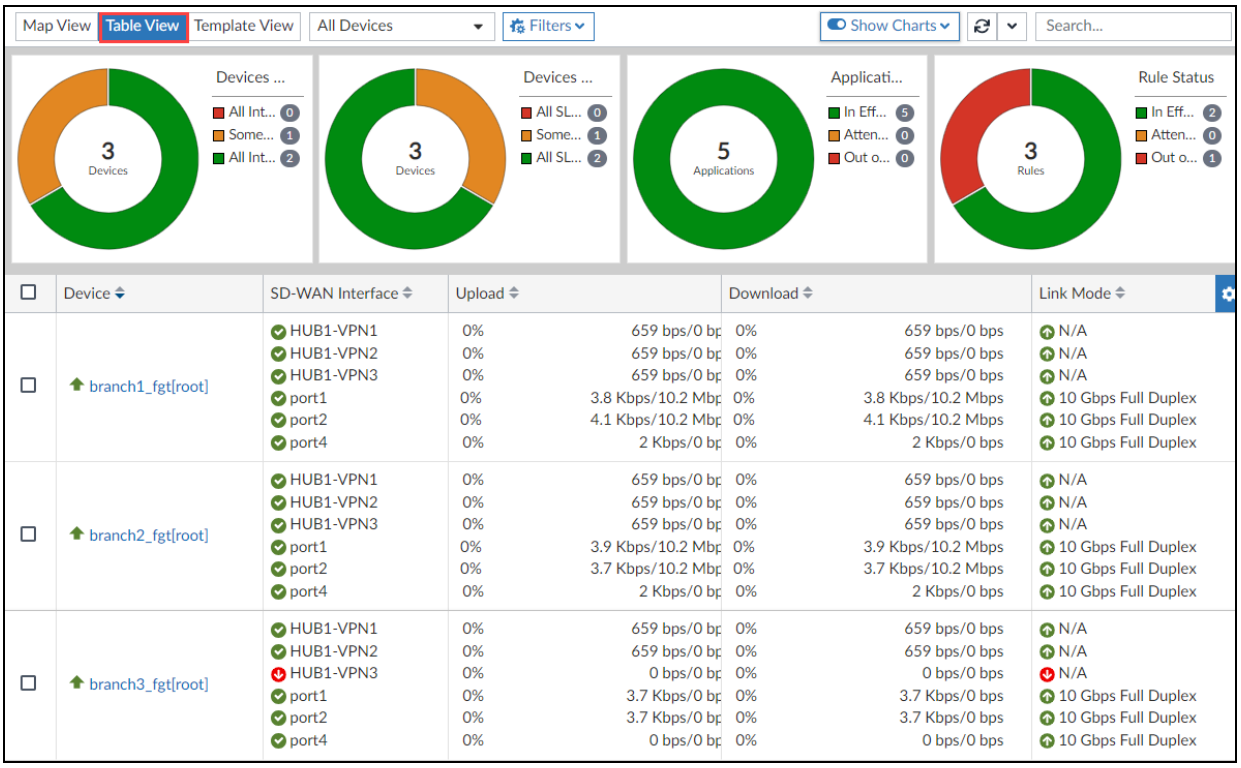
To review the SD-WAN deployment in the table view

1. Click **Table View**.

   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

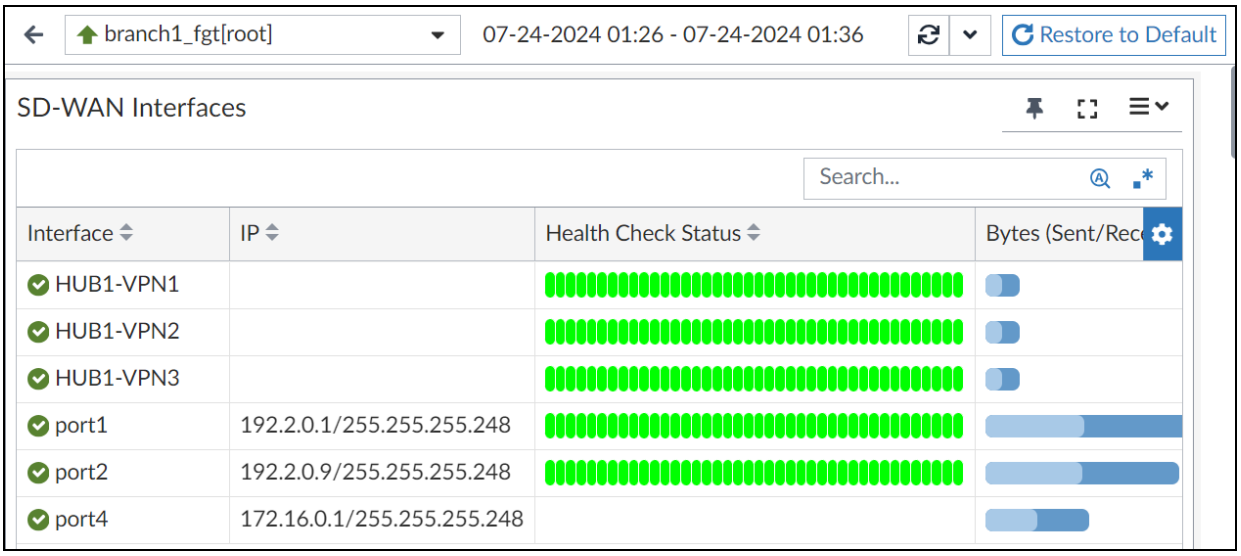
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



On this page, you can click a widget to filter the corresponding devices.

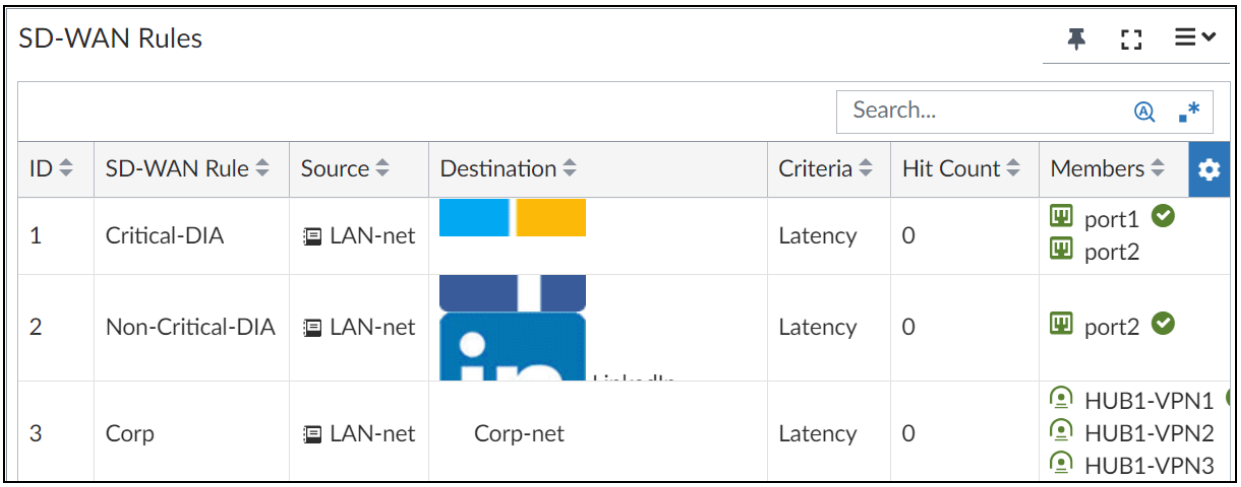
You can click a device name to display a per-device SD-WAN monitor view.

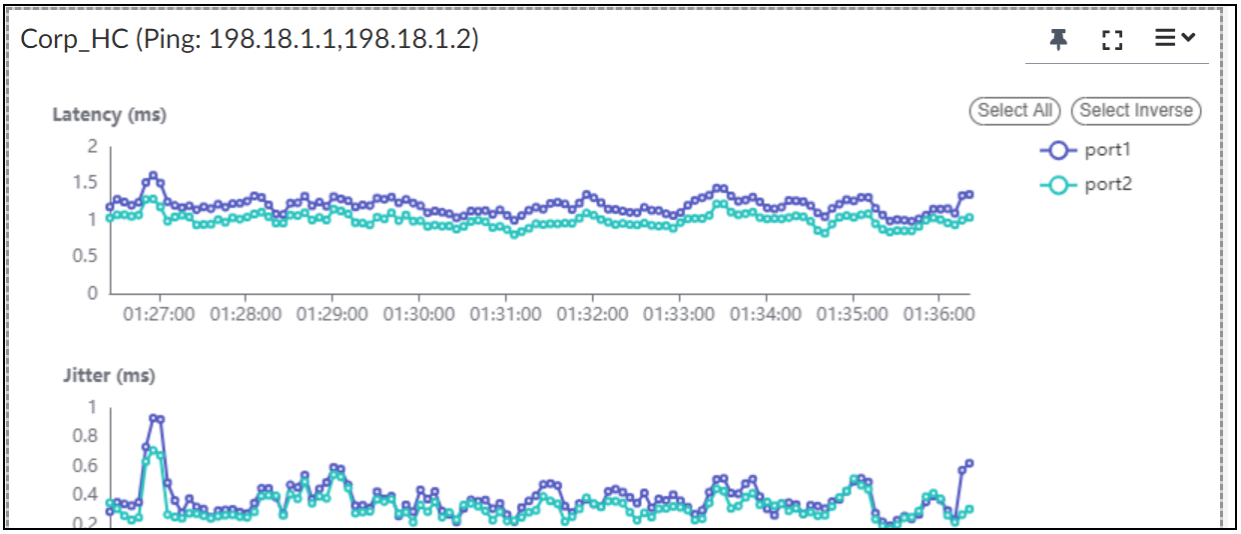
2. Click **branch1_fgt**.
   Your page should look similar to the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

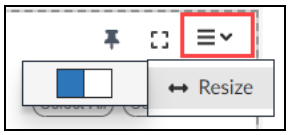




3. Scroll through the page to review the widgets that are available.

This page shows the health check and bandwidth monitoring statistics for the past 10 minutes.

You can use the drop-down menu to resize the widgets. You can also drag and drop the widgets to reorganize the page.



4. Scroll down to the **Corp_HC** health check widget, and then hover over the graph to view details.

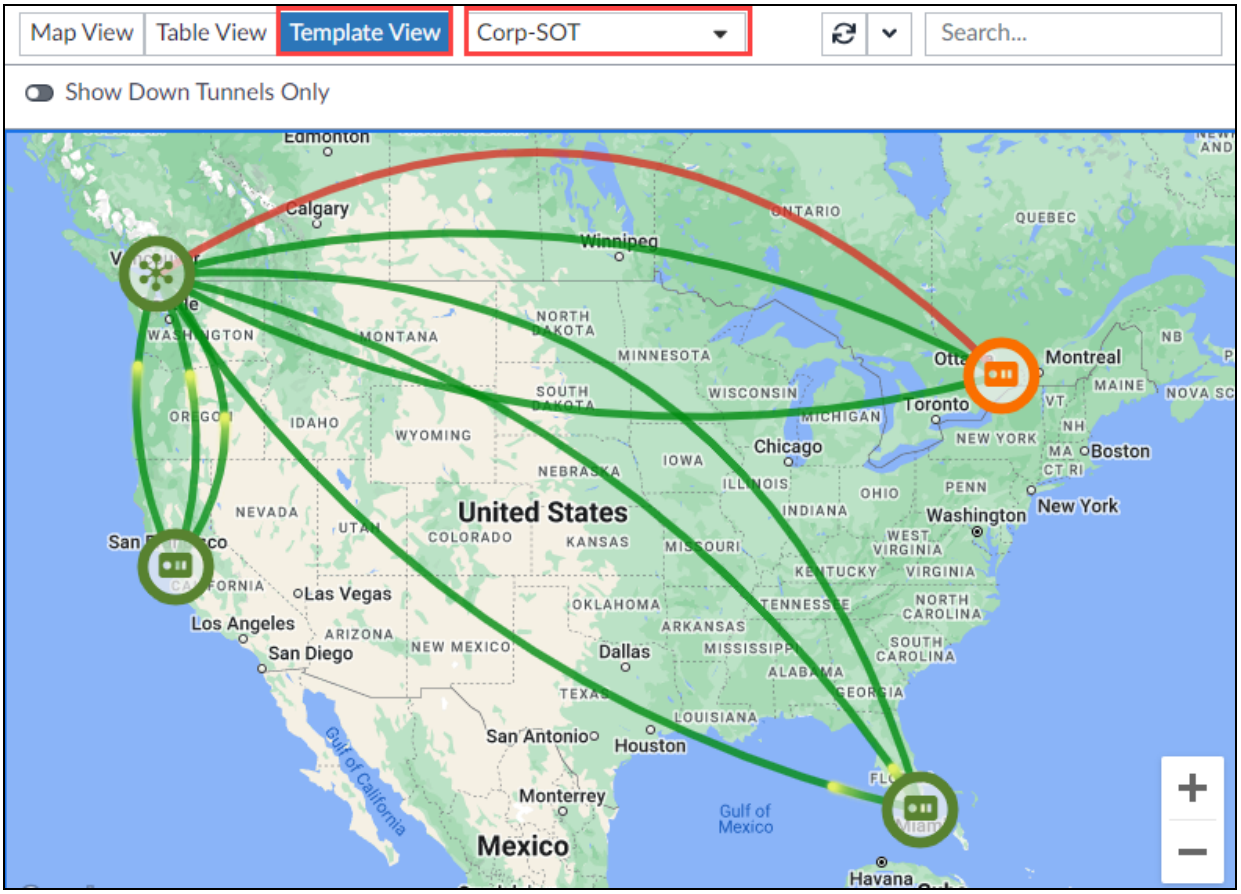
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

5. Click **SD-WAN Monitor** to return to the main view.

To review the SD-WAN deployment in the template view

1. Click **Template View**, and then select the **Corp-SOT** template.
   Your page should look similar to the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

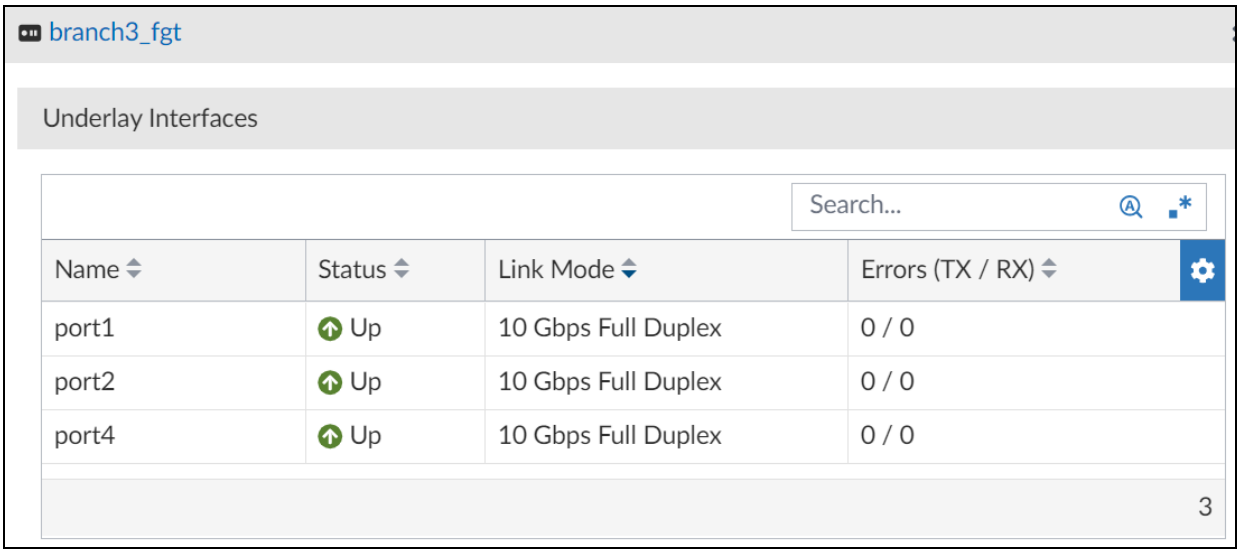
The template view complements the map view and displays the hub devices and the SD-WAN overlay links.

Similar to the VPN monitor map view, it shows the hub devices with a star and branches with a device icon. It displays active tunnels as green, down tunnels as red, and branch devices with some tunnels down as orange.

Remember that the port4 interface of branch3_fgt is connected but did not receive an IP address. So, it is expected to see the third tunnel for branch3_fgt down.

2. Hover over a few devices to see a quick overview.
   - **Hub** role for **dc1_fgt**
   - **Spoke** role for **branch1_fgt** and **branch2_fgt**
   - **Spoke** role and the **HUB1_VPN3** interface is down for **branch3_fgt**
3. Hover over a few tunnels to see basic connection information.
4. Click **branch3_fgt**.

   FortiManager opens a page with the SD-WAN device configuration and some statistics. Your page should look similar to the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Performance SLAs

Search...

Interface	Health Check				Bandwidth
	SLA	Latency (ms)	Jitter (ms)	Packet Loss	
HUB1-VPN1	HUB1_HC #1	2.01 / 255.00	0.78 / 55.00m	0.00 / 1.00%	1.30 kb
HUB1-VPN2	HUB1_HC #1	1.88 / 255.00	0.76 / 55.00m	0.00 / 1.00%	1.32 kb
HUB1-VPN3	HUB1_HC #1	0.00 / 255.00	0.00 / 55.00m	100.00 / 1.00	0.00 bp
port1					7.44 kb
port2					7.49 kb
port4					0.00 bp

6

Drilldown to History View

IPsec VPN

Refresh Bring Tunnel Up Bring Tunnel Down Search...

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1
HUB1-VPN1	100.64.1.1	100.64.1.1	4.5 MB	4.5 MB	HUB1-VPI
HUB1-VPN2	100.64.1.9	100.64.1.9	4.4 MB	4.4 MB	HUB1-VPI
HUB1-VPN3	172.16.1.5		0.0 KB	0.0 KB	HUB1-VPI

3

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Routing - Static & Dynamic

Route Lookup | Search...

Network	Gateway IP	Interfaces	Distance	Type	Tunnel ID
0.0.0.0/0	100.64.33.2	port1	1	static	
0.0.0.0/0	100.64.33.10	port2	1	static	
10.1.0.0/24	192.168.1.61	HUB1-VPN1	200	BGP	
10.1.0.0/24	192.168.1.125	HUB1-VPN2	200	BGP	
10.200.99.3/32	0.0.0.0	Branch-Lo	0	Connected	

On this page, you can click **Drilldown to History View** to have quick link access to the graphs with the device statistics.

5. Scroll through the page to review the data available.
6. Click **Close** to return to the template view.

In **Template View**, you can click a device to get direct access to the following information tables:

- For hubs and spokes: underlay status, IPsec VPN, and static and dynamic routing
- For spokes only: SD-WAN health check

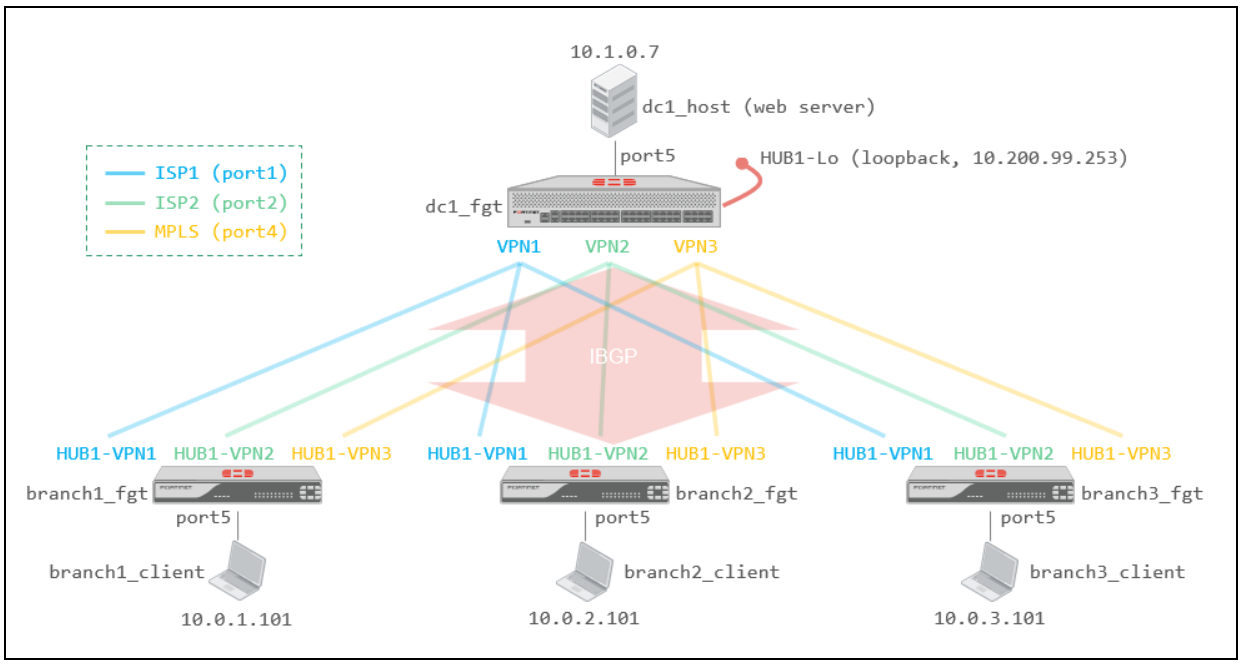
In **Map View** or **Table View**, you can click a device to get direct access to a per-device SD-WAN monitor view.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 4: Members, Zones, and Performance SLAs

In this lab, you will configure active performance service-level agreement (SLA) monitoring for the overlay zone of the SD-WAN topology that you created in the previous labs.



Three communities were configured with the SD-WAN overlay template, one for each overlay (VPN1, VPN2, and VPN3). The HUB1-Lo loopback interface was configured with the template. You will use it as the target server on one of the performance SLAs for overlays.

First, you will configure a performance SLA for overlays. Next, you will increase the latency on the overlays and see the changes introduced in the status of the performance SLAs and overlays. Finally, you will discover how you can use FortiAnalyzer to collect and analyze the SD-WAN logs.

Objectives

- Configure SLA targets
- Use the SD-WAN monitor on the FortiManager GUI, and the FortiGate CLI, to check the status of performance SLAs, SLA targets, and overlays
- Discover how FortiAnalyzer can help you monitor your SD-WAN network
- Analyze traffic logs
- Analyze SD-WAN event logs
- Discover the **Secure SD-WAN Monitor** page
- Discover the **SD-WAN Summary** page

Time to Complete

Estimated: 50 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Using Ping to Actively Monitor the Overlays

In this exercise, you will use the performance SLA named **HUB1_HC**, that the SD-WAN overlay template created, to actively monitor the overlays using the ping protocol. You will also configure two SLA targets for **HUB1_HC**. Finally, you will check the health of the overlays using FortiManager.

Configure an Active Performance SLA (Ping)

You will modify the configuration of **HUB1_HC** to make it suitable for this exercise. To do so, you will review the settings that the overlay template defined and define two SLA targets.

To configure an active performance SLA (ping)

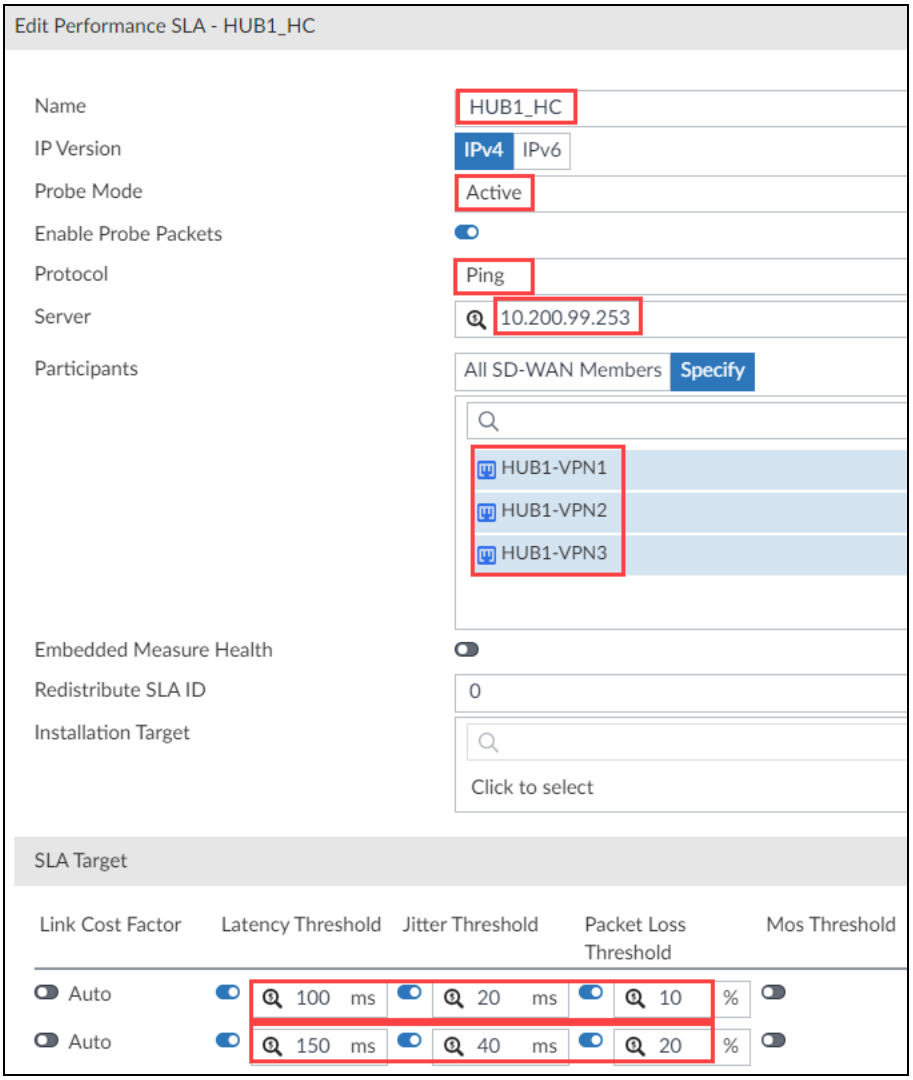
1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Provisioning Templates**, and then click **SD-WAN**.
3. Double-click **branches** to edit the template settings.
4. In the **Performance SLA** section, click **HUB1_HC**, and then click **Edit**.
5. Configure and verify the following settings:

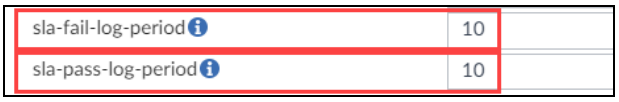
Field	Value
Name	HUB1_HC
Probe Mode	Active
Protocol	Ping
Server	10.200.99.253
Participants	Select **Specify**, and then select **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**.
SLA Target	1. Update the preconfigured SLA target with the following settings: • **Latency Threshold**: 100 • **Jitter Threshold**: 20 • **Packet Loss Threshold**: 10 2. Click **+** to add a second target, and then configure the following settings: • **Latency Threshold**: 150 • **Jitter Threshold**: 40 • **Packet Loss Threshold**: 20

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Advanced Options	Confirm the following settings: • **sla-fail-log-period**: 10 • **sla-pass-log-period**: 10





`10.200.99.253` is the IP address of the loopback interface on dc1_fgt. The loopback interface was configured with the SD-WAN overlay template.

The **sla-fail-log-period** and **sla-pass-log-period** settings instruct FortiGate to generate health check SLA status logs every 10 seconds. The FortiView section on FortiAnalyzer (FortiManager, in this case) uses the logs to generate performance SLA-related graphs.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

6. Click **OK** to save the settings.
7. Continuing in the **Performance SLA** section, click **Corp_HC**, and then click **Edit**.
8. Configure and verify the following settings:

Field	Value
Name	Corp_HC
Probe Mode	Active
Protocol	Ping
Server	**198.18.1.1** and **198.18.1.2**
Participants	Select **Specify**, and then select **port1** and **port2**.
SLA Targets	Click **+** to add an SLA target, and then configure the following settings: • **Latency Threshold**: 150 • **Jitter Threshold**: 25 • **Packet Loss Threshold**: 5
Advanced Options	Configure the following settings: • **sla-fail-log-period**: 10 • **sla-pass-log-period**: 10

9. Click **OK** to save the performance SLA settings.
10. Click **OK** to save the template settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, **branch2_fgt**, and **branch3_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on the three devices.
5. Wait for the installation to finish.
6. Click **Finish**.

Verify the Health of the Overlays

You will use the SD-WAN monitor on FortiManager to check the health of the overlays.

To verify the health of the overlays

1. Continuing on the FortiManager GUI, click **Device Manager** > **Monitors** > **SD-WAN Monitor** > **Map View**.

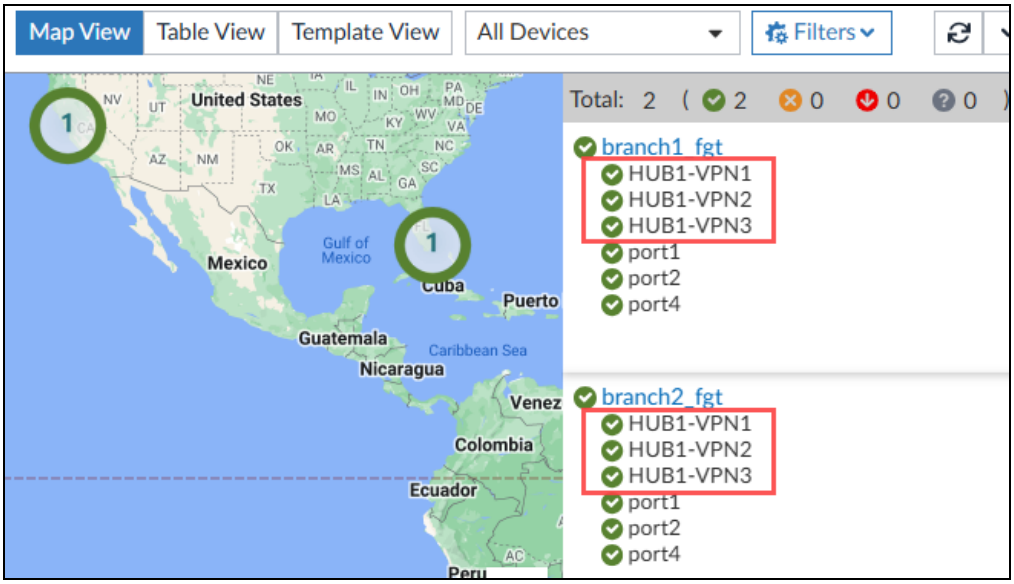
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

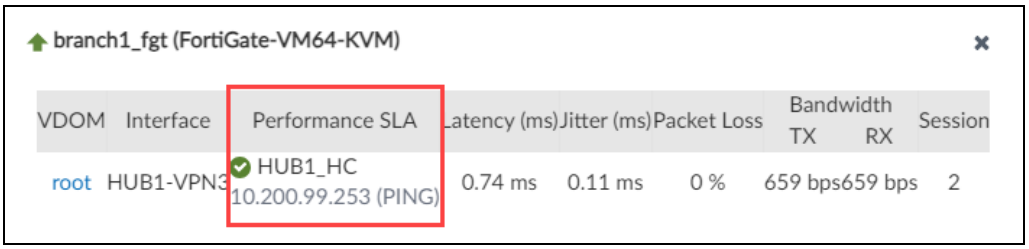
The SD-WAN monitor map view shows the list of members and their status only for the devices that are visible on the map. To view more devices, click **-** to reduce the scale.

Alternatively, you can move the map to view your devices that are located in other parts of the world.

2. Move the map and zoom in or out to view **branch1_fgt** and **branch2_fgt**.
   Your page should look similar to the following example:



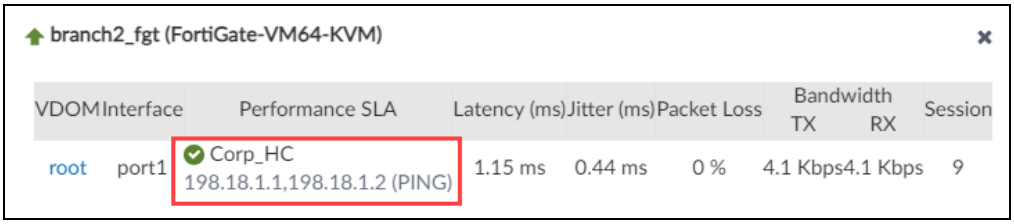
3. Hover over the icons beside **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**, and then check the performance SLA.
   These interfaces use **HUB1_HC** to monitor link performance.



branch1_fgt (FortiGate-VM64-KVM)

VDOM	Interface	Performance SLA	Latency (ms)	Jitter (ms)	Packet Loss	Bandwidth TX	Bandwidth RX	Session
root	HUB1-VPN3	HUB1_HC 10.200.99.253 (PING)	0.74 ms	0.11 ms	0 %	659 bps	659 bps	2

4. Hover over the icons beside **port1** and **port2**, and then check the performance SLA.
   These interfaces use **Corp_HC** to monitor link performance.



branch2_fgt (FortiGate-VM64-KVM)

VDOM	Interface	Performance SLA	Latency (ms)	Jitter (ms)	Packet Loss	Bandwidth TX	Bandwidth RX	Session
root	port1	Corp_HC 198.18.1.1,198.18.1.2 (PING)	1.15 ms	0.44 ms	0 %	4.1 Kbps	4.1 Kbps	9

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To verify the source addresses used for the health check probes

1. Open an SSH session to branch1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Enter the following command to capture probe packets sent to 10.200.99.253:
   `diagnose sniffer packet any "host 10.200.99.253 and icmp" 4 10`

```
branch1_fgt # diag sniffer packet any "host 10.200.99.253 and icmp" 4 10
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.200.99.253 and icmp]
0.331562 HUB1-VPN1 out 192.168.1.1 -> 10.200.99.253: icmp: echo request
0.331632 HUB1-VPN2 out 192.168.1.65 -> 10.200.99.253: icmp: echo request
0.332095 HUB1-VPN3 out 192.168.1.130 -> 10.200.99.253: icmp: echo request
0.333369 HUB1-VPN3 in 10.200.99.253 -> 192.168.1.130: icmp: echo reply
0.333705 HUB1-VPN2 in 10.200.99.253 -> 192.168.1.65: icmp: echo reply
0.333762 HUB1-VPN1 in 10.200.99.253 -> 192.168.1.1: icmp: echo reply
0.835069 HUB1-VPN1 out 192.168.1.1 -> 10.200.99.253: icmp: echo request
0.835200 HUB1-VPN2 out 192.168.1.65 -> 10.200.99.253: icmp: echo request
0.835463 HUB1-VPN3 out 192.168.1.130 -> 10.200.99.253: icmp: echo request
0.837077 HUB1-VPN2 in 10.200.99.253 -> 192.168.1.65: icmp: echo reply
```

The probes use the gateway IP address assigned to each VPN interface as the source address.

The addresses are dynamically assigned and might differ in your lab.

3. Enter the following command to display the routing table:
   `get router info routing-table all`
   You can see the connected routes that are shown in the following image:

```
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
C       192.168.1.0/26 is directly connected, HUB1-VPN1
C       192.168.1.1/32 is directly connected, HUB1-VPN1
C       192.168.1.64/26 is directly connected, HUB1-VPN2
C       192.168.1.65/32 is directly connected, HUB1-VPN2
C       192.168.1.128/26 is directly connected, HUB1-VPN3
C       192.168.1.130/32 is directly connected, HUB1-VPN3
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Testing an Active Performance SLA

In this exercise, you will use the FortiManager GUI and FortiGate CLI to monitor the status of the **HUB1_HC** performance SLA and overlays before and after you increase the latency on the overlays.

Monitor a Performance SLA on the FortiGate CLI

In the previous exercise, you configured a performance SLA to monitor the health and performance of overlays. You will now monitor the behavior of the links when the performance changes.

To monitor a performance SLA on the FortiGate CLI

1. Open an SSH session to branch1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Enter the following command to display the status of the **HUB1_HC** performance SLA:
   `diagnose sys sdwan health-check status HUB1_HC`
   Your output should look similar to the following example:

```
branch1_fgt # diag sys sdwan health-check status HUB1_HC
Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(1.276), jitter(0.421), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.176), jitter(0.373), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
Seq(6 HUB1-VPN3): state(alive), packet-loss(0.000%) latency(0.901), jitter(0.192), mos(4.404),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x3
```

The output includes the different metrics (packet loss, latency, jitter, mos, and bandwidth) that the **HUB1_HC** performance SLA measures on each overlay. Note that all overlays indicate `sla_map=0x3`, which means that the overlays meet the two SLA targets that are configured.

You will learn how to interpret the SLA mapping in another lesson.

3. Enter the following commands to display additional information about the health of the **HUB1-VPN1** overlay:
   `diagnose sys link-monitor interface HUB1-VPN1`
   `diagnose sys sdwan sla-log HUB1_HC 4`
   `diagnose sys sdwan intf-sla-log HUB1-VPN1`
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sys link-monitor interface HUB1-VPN1
Interface(HUB1-VPN1): state(up, since Sun Jul 21 23:53:32 2024), bandwidth(up:659bps, down:659b
ps), session count(IPv4:2, IPv6:0), tx(756183 bytes), rx(756112 bytes), latency(1.50), jitter(0
.32), packet-loss(0.00).
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
Timestamp: Mon Jul 22 02:33:39 2024, vdom root, health-check HUB1_HC, interface: HUB1-VPN1,
 status: up, latency: 1.648, jitter: 0.427, packet loss: 0.000%, mos: 4.403.
Timestamp: Mon Jul 22 02:33:40 2024, vdom root, health-check HUB1_HC, interface: HUB1-VPN1,
 status: up, latency: 1.661, jitter: 0.425, packet loss: 0.000%, mos: 4.403.
Timestamp: Mon Jul 22 02:33:40 2024, vdom root, health-check HUB1_HC, interface: HUB1-VPN1,
 status: up, latency: 1.684, jitter: 0.414, packet loss: 0.000%, mos: 4.403.
Timestamp: Mon Jul 22 02:33:41 2024, vdom root, health-check HUB1_HC, interface: HUB1-VPN1,
 status: up, latency: 1.652, jitter: 0.392, packet loss: 0.000%, mos: 4.403.
Timestamp: Mon Jul 22 02:33:41 2024, vdom root, health-check HUB1_HC, interface: HUB1-VPN1,
 status: up, latency: 1.658, jitter: 0.407, packet loss: 0.000%, mos: 4.403.
```

```
Timestamp: Mon Jul 22 02:35:15 2024, used inbandwidth: 659bps, used outbandwidth: 659bps,
 used bibandwidth: 1318bps, tx bytes: 799044bytes, rx bytes: 798954bytes.
Timestamp: Mon Jul 22 02:35:25 2024, used inbandwidth: 659bps, used outbandwidth: 659bps,
 used bibandwidth: 1318bps, tx bytes: 799844bytes, rx bytes: 799754bytes.
Timestamp: Mon Jul 22 02:35:35 2024, used inbandwidth: 659bps, used outbandwidth: 659bps,
 used bibandwidth: 1318bps, tx bytes: 800644bytes, rx bytes: 800554bytes.
Timestamp: Mon Jul 22 02:35:45 2024, used inbandwidth: 659bps, used outbandwidth: 659bps,
 used bibandwidth: 1318bps, tx bytes: 801444bytes, rx bytes: 801354bytes.
Timestamp: Mon Jul 22 02:35:55 2024, used inbandwidth: 648bps, used outbandwidth: 651bps,
 used bibandwidth: 1299bps, tx bytes: 802244bytes, rx bytes: 802154bytes.
```

- The first command (first output) reports on the **HUB1-VPN1** metrics that the link-monitor process (lnkmtd) measures. Remember that the performance SLA relies on the link-monitor process to measure the member metrics.
- The second command (second output) shows the latency, jitter, packet loss, and mos that the link-monitor measures on member ID 4 (**HUB1-VPN1**). The output shows the results for each probe sent for the last 10 minutes. Because the probes are sent every 500 ms, the output shows two lines per second. The output has been cut to fit the page.
- The third command (third output) shows the measured incoming, outgoing, and bidirectional bandwidth on **HUB1-VPN1** for the last 10 minutes. Bandwidth is measured every 10 seconds. The output has been cut to fit the page.

Test the Performance SLA

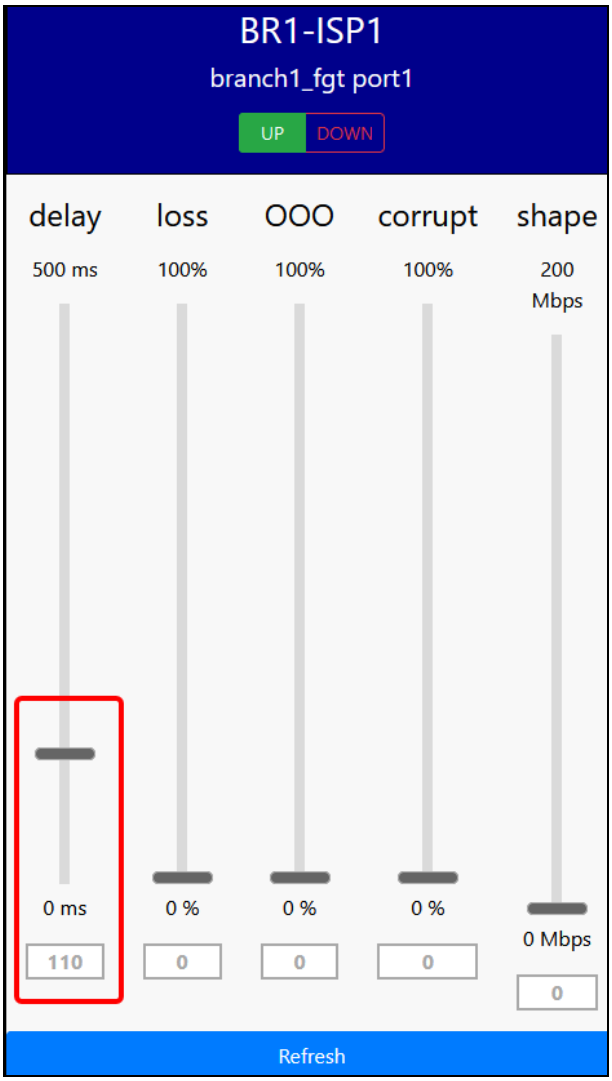
You will increase the latency on one of the two overlays on branch1_fgt, and then see the changes introduced in the overlay and performance SLA status.

To increase the latency on an overlay

1. Access the WAN simulator page.
2. Locate the **BR1-ISP1** and **BR1-ISP2** control panels.
3. On **BR1-ISP1**, use the vertical bar to increase the **delay** to 110 ms.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

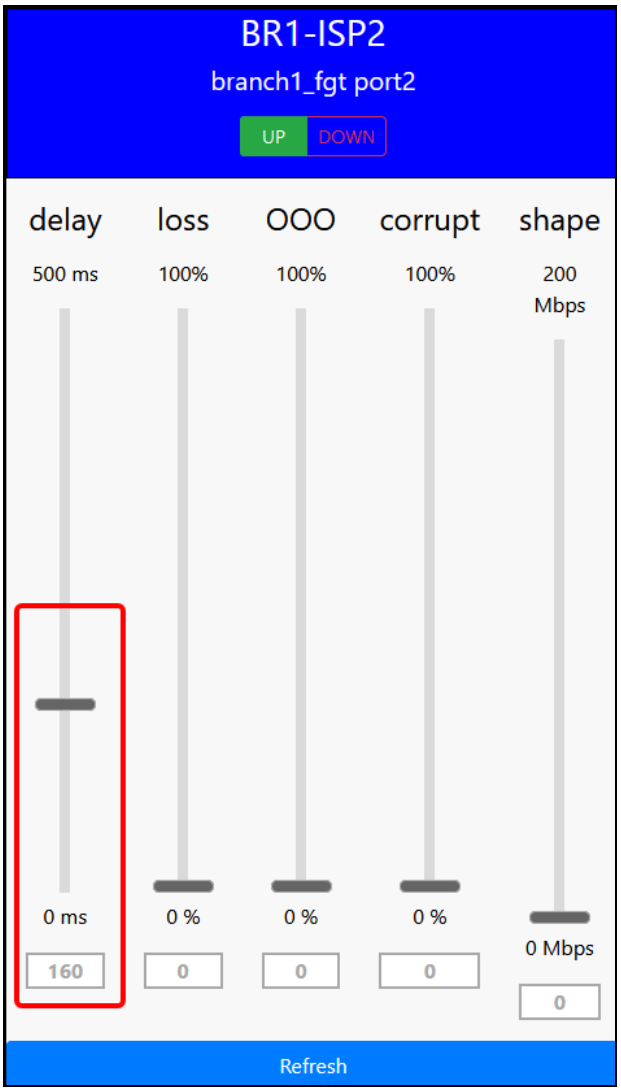
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



4. On **BR1-ISP2**, use the vertical bar to increase the **delay** to 160 ms.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



5. Continuing on the branch1_fgt SSH session, enter the following command to display the status of the **HUB1_HC** performance SLA:

```
diagnose sys sdwan health-check status HUB1_HC
```

Your output should look similar to the following example:

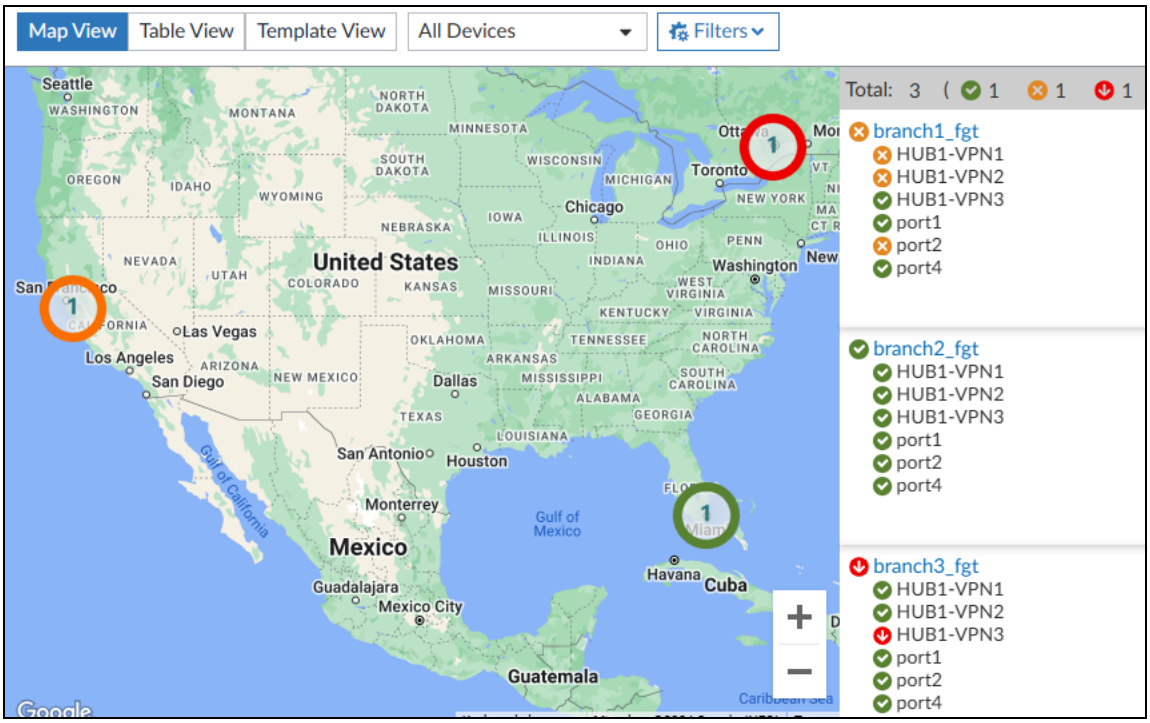
```
branch1_fgt # branch1_fgt # diagnose sys sdwan health-check status HUB1_HC
Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(alive), packet-loss(0.000%) latency(111.663), jitter(0.354), mos(4.342
), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x2
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(161.469), jitter(0.321), mos(4.287
), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x0
Seq(6 HUB1-VPN3): state(alive), packet-loss(0.000%) latency(1.065), jitter(0.150), mos(4.404),
 bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x3
```

The performance SLA status reflects the increased latency on **HUB1-VPN1** and **HUB1-VPN2**. The `sla_map` on **HUB1-VPN1** and **HUB1-VPN2** also changed. The former indicates that only one SLA has been met. The latter indicates that no SLA targets have been met.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

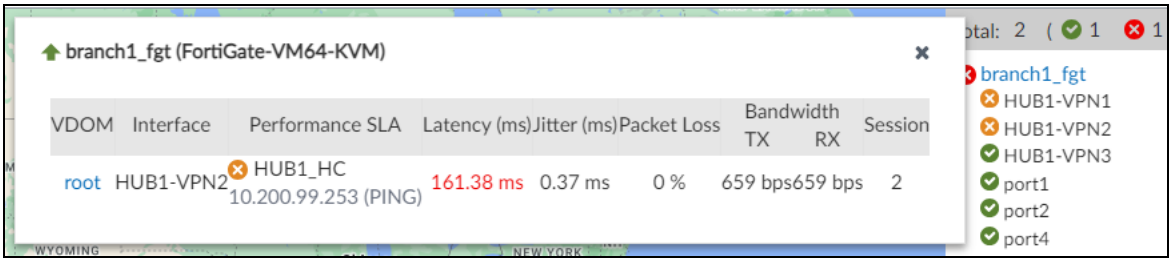
6. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
7. Click **Device Manager** > **Device & Groups** > **Monitors**, and then click **SD-WAN Monitor** > **Map View**.
   Your page should look similar to the following example:



The page reports that **HUB1-VPN1** and **HUB1-VPN2** on **branch1_fgt** are not meeting one or more SLA targets (displayed with an orange icon).

If you zoom out the map to see the three branches, you can see **branch3_fgt** with a red icon for **HUB1-VPN3**. Red icons indicates interfaces that are down.

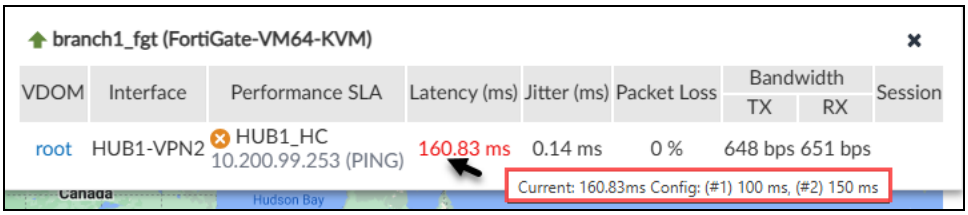
8. Hover over the **HUB1-VPN1** or **HUB1-VPN2** icon on **branch1_fgt** to show more details about the overlay.
   Your page should look similar to the following example:



9. Place your mouse over the latency value to display details about the SLA measured and configured values.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



10. Click **Table View**, and then hover over the **HUB1-VPN1** overlay to show more details about the status of the SLA targets.

    Your page should look similar to the following example:

SLA Target	HUB1_HC#1
Latency (ms)	110.89 / 100
Jitter (ms)	0.18 / 20
Packet Loss (%)	0 / 10
SLA Target	HUB1_HC#2
Latency (ms)	110.89 / 150
Jitter (ms)	0.18 / 40
Packet Loss (%)	0 / 20

The overlay doesn't meet SLA target #1.

11. Hover over the **HUB1-VPN2** overlay.

    Your page should look similar to the following example:

SLA Target	HUB1_HC#1
Latency (ms)	160.83 / 100
Jitter (ms)	0.14 / 20
Packet Loss (%)	0 / 10
SLA Target	HUB1_HC#2
Latency (ms)	160.83 / 150
Jitter (ms)	0.14 / 40
Packet Loss (%)	0 / 20

The overlay doesn't meet SLA targets #1 and #2.

12. Continuing on the WAN simulator page, set the latency of **BR1-ISP1** and **BR1-ISP2** back to 0 ms.
13. Use the SD-WAN monitor on FortiManager and the FortiGate CLI to confirm that both overlays now meet all SLA targets.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 3: Monitoring SD-WAN With FortiAnalyzer

FortiAnalyzer centralizes all log messages that the managed devices send. It stores the log messages, correlates the information received, and presents the information in easy-to-read graphs to help administrators with day-to-day network monitoring tasks or spot troubleshooting tasks.

In this exercise, you will navigate through the menus to understand how you can use FortiAnalyzer to monitor your SD-WAN deployment.

Confirm Log Forwarding on the FortiGate Devices

In a previous lab, you configured the FortiGate devices to send logs to FortiAnalyzer. You also configured SLA health checks to send `sla-fail-log` and `sla-pass-log` messages to FortiAnalyzer. You will review these settings.

To verify the log forwarding configuration on FortiGate

1. Open an SSH session to each branch device, branch1_fgt, branch2_fgt, and branch3_fgt.
2. Log in with the following credentials:
   - Username: `admin`
   - Password: `password`
3. Enter the following command on both branch1_fgt and branch2_fgt to verify that the configuration was installed:
   ```
   show log fortianalyzer setting
   ```

   Your output should look similar to the following example:

   ```
   branch3_fgt # show log fortianalyzer setting
   config log fortianalyzer setting
       set status enable
       set server "192.168.0.15"
       set upload-option realtime
       set reliable enable
   end
   ```

4. Confirm the status, server IP address, and upload option.

To verify SLA-fail and SLA-pass log settings

1. Continuing in the SSH session for each branch, enter the following commands to check the SLA-fail and SLA-pass log settings:
   ```
   config sys sdwan
   show health-check Corp_HC
   show health-check HUB1_HC
   ```

   Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch3_fgt (sdwan) # show health-check Corp_HC
config health-check
    edit "Corp_HC"
        set server "198.18.1.1" "198.18.1.2"
        set sla-fail-log-period 10
        set sla-pass-log-period 10
        set members 1 2
        config sla
            edit 1
                set latency-threshold 150
                set jitter-threshold 25
                set packetloss-threshold 5
            next
        end
    next
end
```

2. Confirm that the `sla-fail-log-period` and `sla-pass-log-period` settings are configured for both health checks.

Analyze Traffic Logs

You will generate internet traffic from branch1_client and branch2_client using the traffic generator tool. Then, you will review the corresponding traffic logs on FortiAnalyzer.

To generate internet traffic from branch1_client and branch2_client

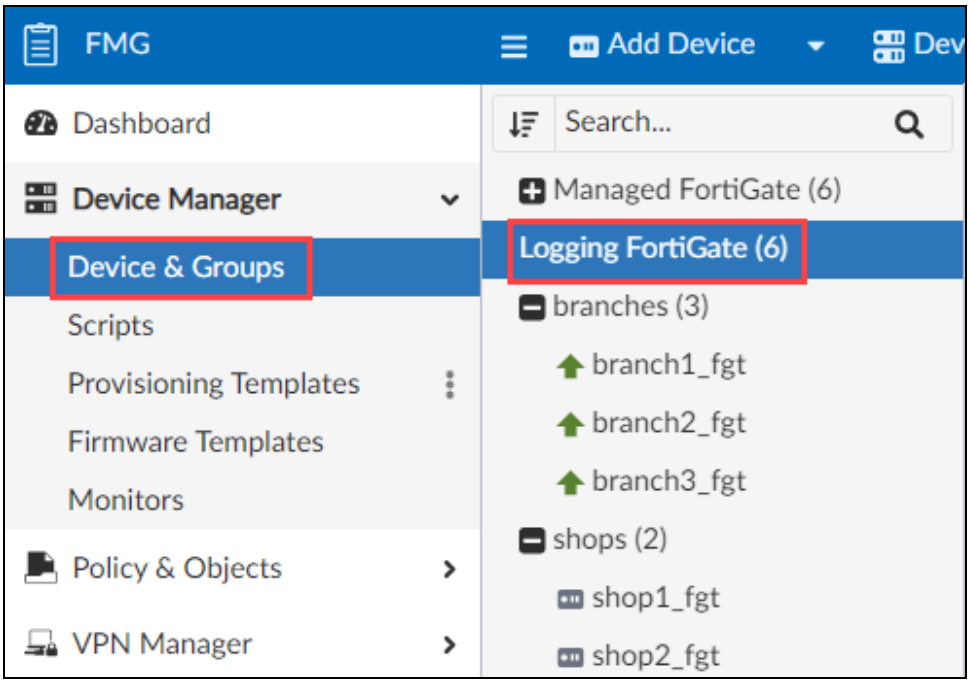
1. Open an SSH session to branch1_client.
2. Log in with the following credentials:
   - Username: `root`
   - Password: `password`
3. Enter the following commands:
   ```
   cd /fortipoc/traffic/
   ./trafficgenerator.sh
   ```
4. Repeat the previous steps on branch2_client.

To verify logging to FortiAnalyzer (FortiManager)

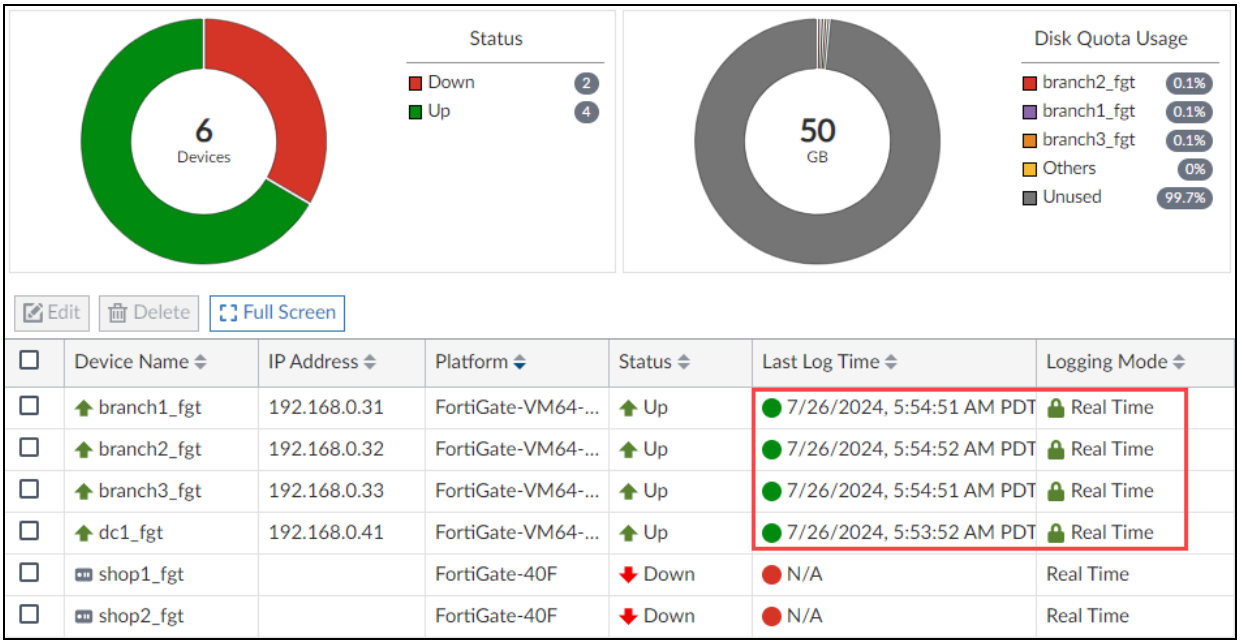
1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Device & Groups**.
3. Click **Logging FortiGate**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



Your page should look similar to the following example:



You can drag and drop the columns to reorganize them.

The green circle in the **Last Log Time** column indicates that FortiAnalyzer is receiving logs from the connected devices.

The green padlock in the **Logging Mode** column indicates that the FortiGate devices send logs to FortiAnalyzer using TCP. No padlock appears for FortiGate devices that send logs using UDP.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To analyze traffic logs

1. Continuing on the FortiManager GUI, click **Log View** > **Traffic**.
   Your page should look similar to the following example:

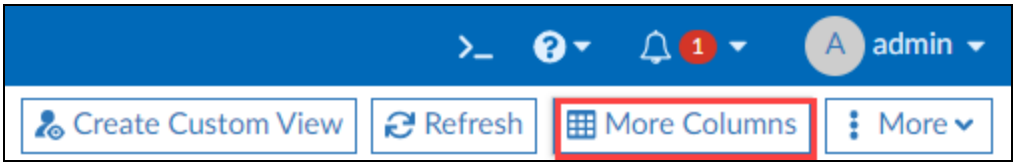
All Devices | Last 1 Hour | 05:22:15 - 06:22:15

Search or type filters...

#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Security Event List	Sent/Received
1	2024-07-26 0	FGVM01TM2200(	✓	127.0.0.1		127.0.0.1	HTTP	HTTP		400.0 B/670.0 B
2	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		23.56.210.39	HTTPS	Microsoft.Portal	APP 2	1.7 KB/5.7 KB
3	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		35.182.106.253	HTTPS	SSL_TLSv1.3	APP 2	1.4 KB/7.5 KB
4	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		23.196.3.191	HTTPS	SSL_TLSv1.3	APP 2	1.7 KB/6.9 KB
5	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		13.107.42.14	HTTPS	LinkedIn	APP 1	1.7 KB/8.0 KB
6	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		23.205.255.239	HTTPS	Salesforce	APP 2	1.6 KB/5.1 KB
7	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		3.143.53.1	HTTPS	Slack	APP 2	1.6 KB/5.1 KB
8	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		162.125.11.18	HTTPS	Dropbox	APP 2	1.7 KB/6.9 KB
9	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		31.13.80.36	HTTPS	Facebook	APP 2	1.9 KB/7.3 KB
10	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		52.176.2.105	HTTPS	MSN.Game	APP 3	2.1 KB/6.6 KB
11	2024-07-26 0	FGVM01TM2200(	✓	10.0.2.101		54.192.51.42	HTTPS	Atlassian.Cloud	APP 2	1.7 KB/9.4 KB
12	2024-07-26 0	FGVM02TM2401(	✓	100.64.33.1		96.45.46.46	tcp/853	tcp/853		7.6 KB/7.4 KB

The serial numbers (**Device ID** column) of managed devices may be different in your lab.

2. In the upper-right corner, click **More Columns**.

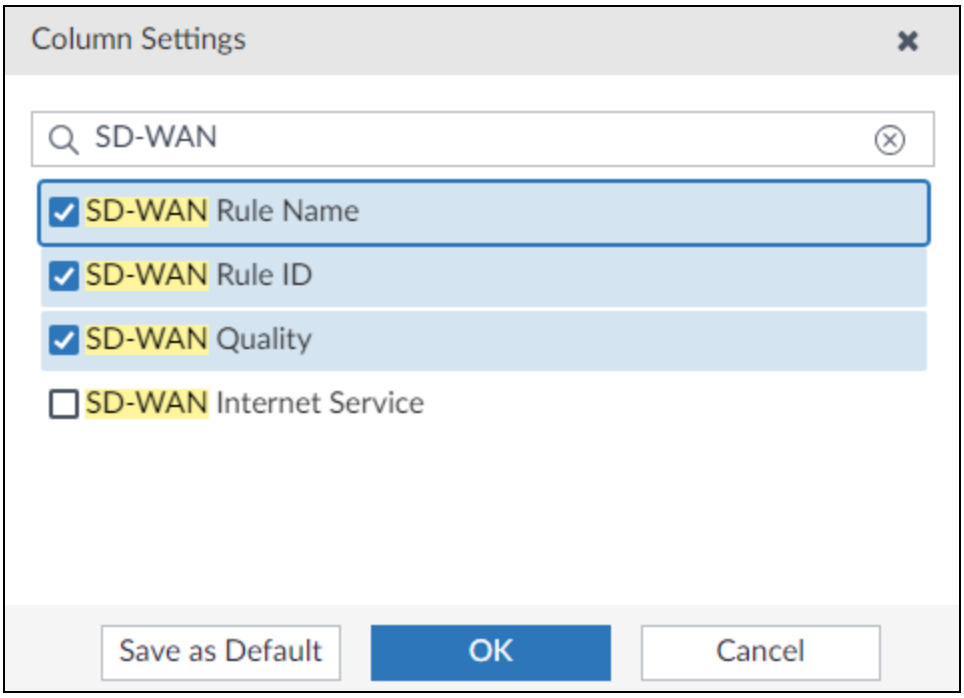


3. Select **Destination Interface**, **SD-WAN Quality**, **SD-WAN Rule ID**, and **SD-WAN Rule Name**.

Use the column settings search box to quickly find the columns.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



4. Click **OK** to save the settings.
   Your page should look similar to the following example:

Application	Sent/Received	Destination Int	SD-WAN Rule Name	SD-WAN Rule ID	SD-WAN Quality
Microsoft.Portal	1.7 KB/5.8 KB	port1	Critical-DIA	1	Seq_num(1 port1 underlay), alive, selected
SSL_TLSv1.3	1.4 KB/7.5 KB	port1		0	
SSL_TLSv1.3	1.7 KB/6.9 KB	port1		0	
Salesforce	1.6 KB/5.3 KB	port1	Critical-DIA	1	Seq_num(1 port1 underlay), alive, selected
Slack	1.6 KB/5.1 KB	port1		0	
Dropbox	1.6 KB/6.8 KB	port1		0	
Facebook	1.7 KB/7.3 KB	port2	Non-Critical-DIA	2	Seq_num(2 port2 underlay), alive, selected
LinkedIn	1.7 KB/7.9 KB	port2	Non-Critical-DIA	2	Seq_num(2 port2 underlay), alive, selected

5. Identify messages for the main SD-WAN rules that are configured: **Critical-DIA** and **Non-Critical-DIA**.
6. Double-click a log message to view details.
7. Expand the **Others** section to see the SD-WAN details contained in the log message.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Application

Application	Salesforce
Application Category	Business
Application Control List	default
Application ID	16920
Application Risk	low
Protocol	6
Service	HTTPS

Data

Duration	5
Received Packets	16
Sent Packets	15

Type

Sub Type	forward
Type	traffic

Others

Date	2024-07-26
Date/Time	2024-07-26 12:36:58
Device Time	2024-07-26 12:36:54
Device Time Zone	-0700
Event Time	1722022614337216432
Policy Name	DIA
Policy Type	policy
Received	5392
SD-WAN Quality	Seq_num(1 port1 underlay), alive, selected
SD-WAN Rule ID	1
SD-WAN Rule Name	Critical-DIA
Sent	1639
Time	12:36:54
apps	Salesforce,SSL
logflag	1
saasinfo	10,0
utmref	BAYAAAAIAAAByAQAAANL6o2bS-qNmcgAAAADS-qNm0vqjZg

FortiAnalyzer displays traffic logs for all managed FortiGate devices.

If you want to display logs for a specific device, in the upper-left corner, click **All FortiGate** to select the managed device you want to display logs for.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

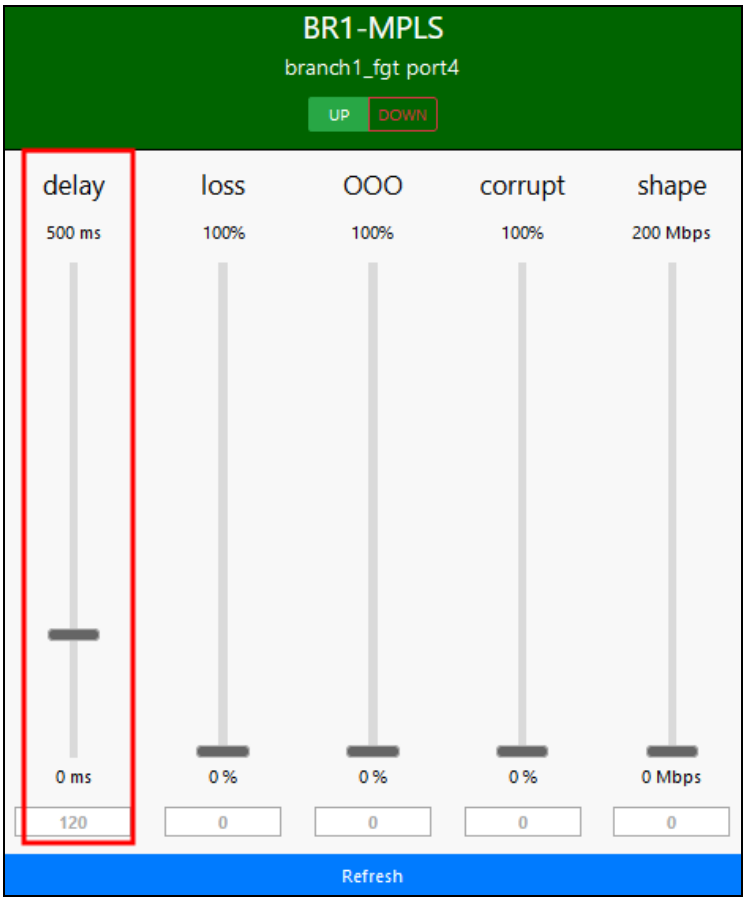
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Analyze Event Logs

You will trigger link down and link up events, and then review the log messages corresponding to these events on FortiAnalyzer.

To trigger events

1. Access the WAN simulator page.
2. Locate the **BR1-ISP1** and **BR1-MPLS** control panels.
3. On **BR1-ISP1**, click **DOWN** to switch the interface off.
4. Wait a few seconds, and then click **UP** to switch the interface back on.
5. On **BR1-MPLS**, use the vertical bar to increase the **delay** to 120 ms.

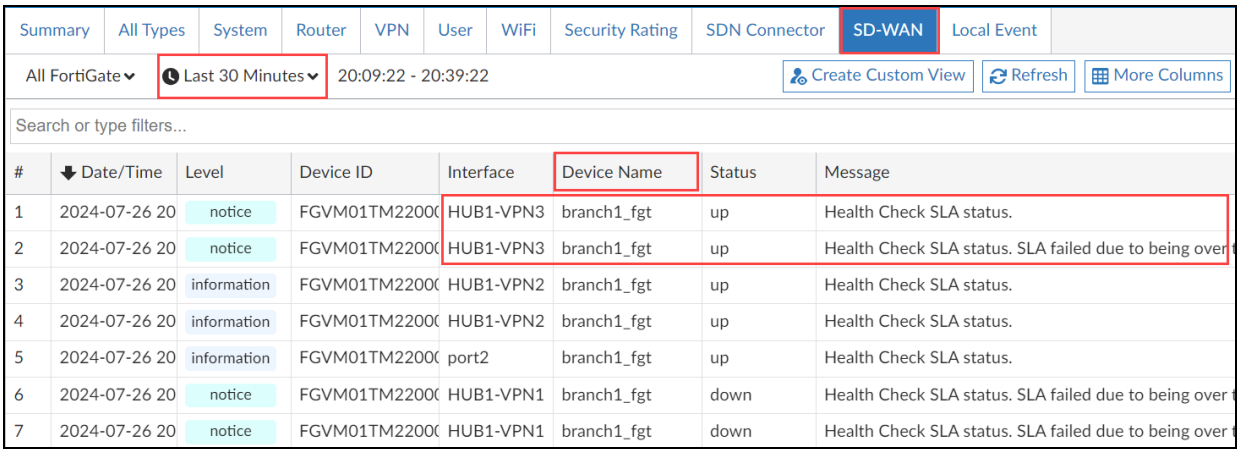


To analyze event logs

1. Continuing on the FortiManager GUI, click **Log View**, and then click **Event** > **SD-WAN**.
2. In the time range drop-down list, select **Last 30 Minutes**.
3. Click **More columns**.
4. Select **Device Name**, and then click **OK** to save the settings.
5. Drag and drop the **Device Name** column beside the **Interface** column.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



6. Identify SLA pass log messages, and then double-click some messages to see details.
7. Click **Other** to see SD-WAN information.

For each device and each interface, FortiAnalyzer receives a health-check SLA status, pass or fail, every 10 seconds.

You see these messages because for each health check, the `sla-fail-log-period` and `sla-pass-log-period` settings are 10.

Stop and think!

FortiAnalyzer receives both SLA pass and SLA fail log messages for the **HUB1-VPN3** interface of device branch1_fgt. Why?

Log details show that the SLA pass message corresponds to the SLA target ID 2 of the **HUB1_HC** health check, while the SLA fail message corresponds to the SLA target ID 1 of the same health check.

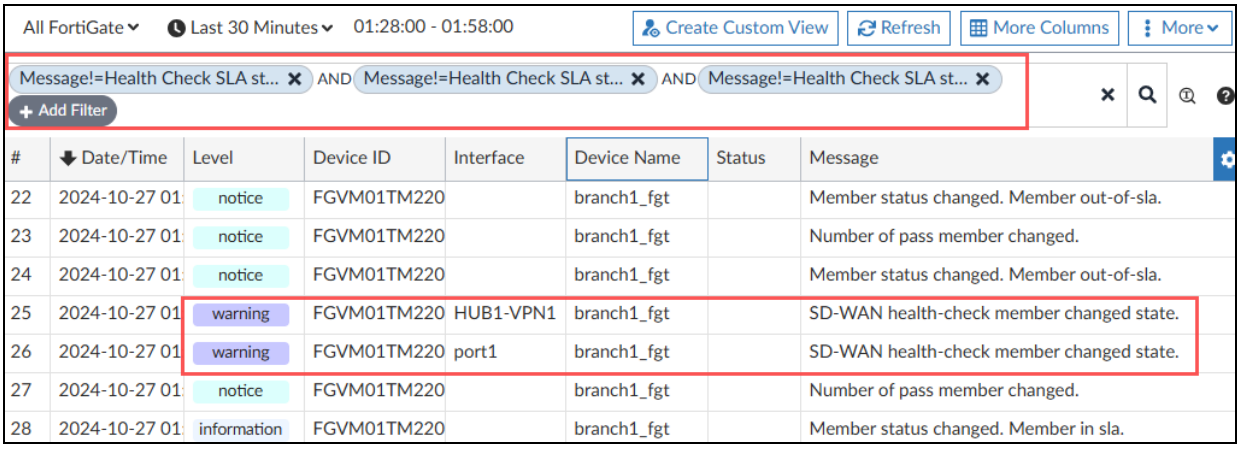
8. Right-click an SLA pass log message, and then select the filter, as shown in the following image, to filter the list to remove the SLA pass log messages:

9. Repeat the previous step to filter out the following:
   - SLA failed due to being over the performance metric threshold [packetloss]
   - SLA failed due to being over the performance metric threshold [latency]

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Your page should look similar to the following example:



10. Identify the log messages related to the **BR1-ISP1** interface shut down.
    You should see the following:
    - Level **warning**: The SD-WAN health-check member changed state for **port1** and **HUB1-VPN1**.
    - Level **notice**:
      - The service prioritized by the SLA will be redirected in sequence order.
      - The member link is unreachable or missed the threshold. Traffic forwarding is stopped.
11. Double-click a message to see the details.
12. Identify log messages related to the **BR1-ISP1** interface going up.
    You should see the following messages (level notice):
    - The SD-WAN health-check member changed state for **port1** and the **HUB1-VPN1** overlay tunnel.
    - Service prioritized by SLA will be redirected in sequence order.
    - The member link is available. Start forwarding traffic.
13. Double-click a message to see the details.

Discover the Secure SD-WAN Monitor Page

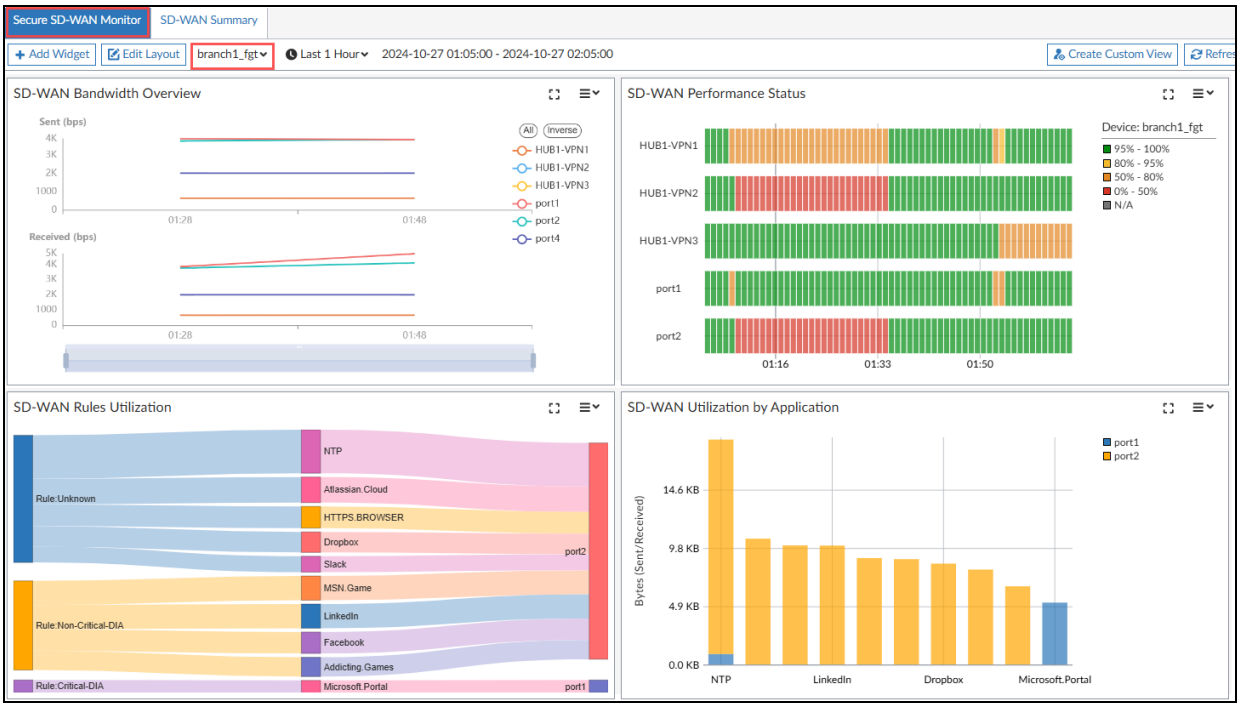
The **Secure SD-WAN Monitor** page provides you with a centralized view of SD-WAN status information for each managed FortiGate. You will discover the available widgets and learn how to use them.

To discover the Secure SD-WAN Monitor page

1. Continuing on the FortiManager GUI, click **FortiView** > **SD-WAN**, and then click **Secure SD-WAN Monitor**.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



2. Review the available widgets and information provided for branch1_fgt.

By default the **Secure SD-WAN Monitor** page displays the statistics for the past hour. You can adjust the time period that FortiManager displays from **Last 5 Minutes** to **Last N Weeks**, or create a custom time period.

Note that if you configure the page to display only the last 5 minutes, you will not see the period when the **SD-WAN Performance Status** widget sees port1 and HUB1-VPN1 as dead.

Discover the SD-WAN Summary Page

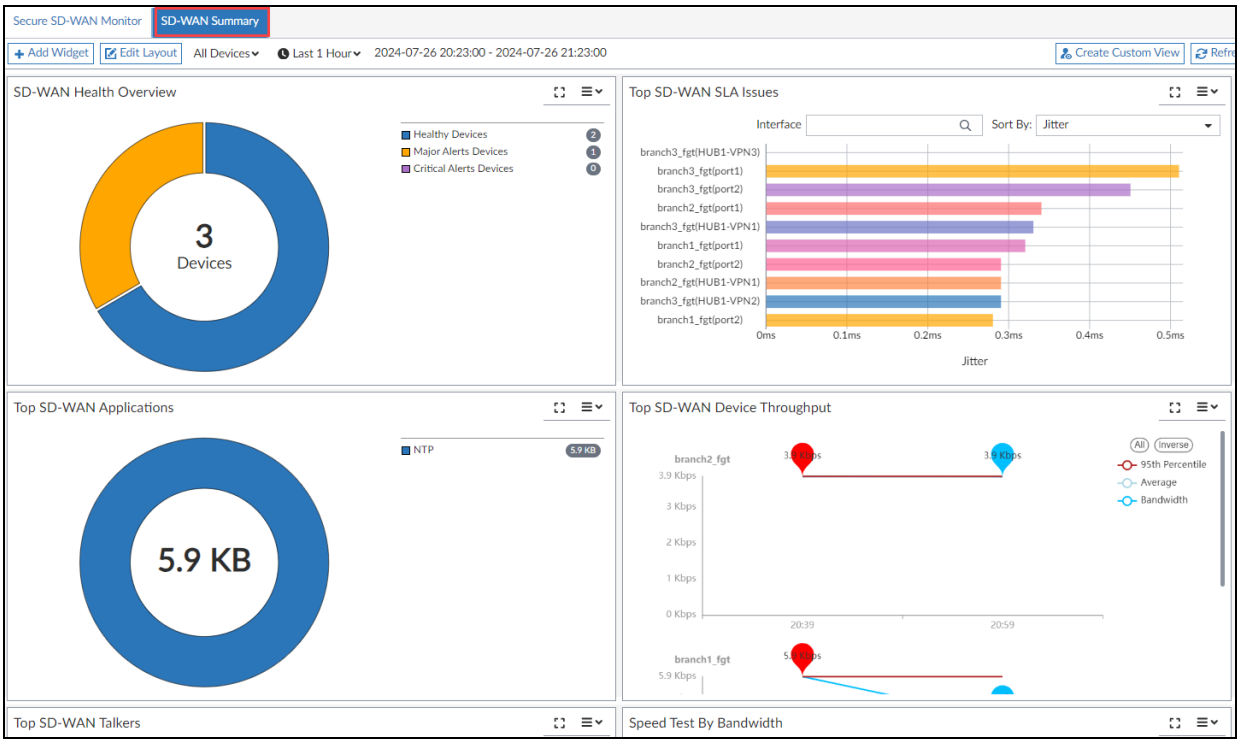
The **SD-WAN Summary** page provides a centralized view of your SD-WAN deployment. It summarizes data for all managed FortiGate devices.

To discover the SD-WAN Summary page

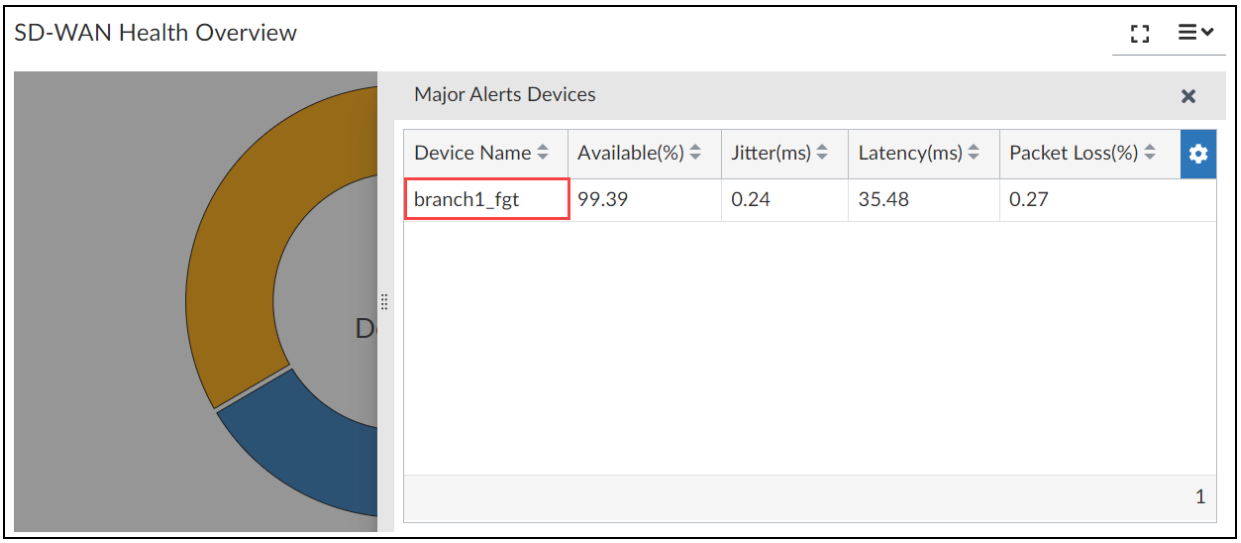
1. Continuing on the FortiManager GUI, click **FortiView** > **SD-WAN Summary**.
2. Make sure that you display the statistics over the **Last 30 Minutes** or **Last 1 Hour**.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



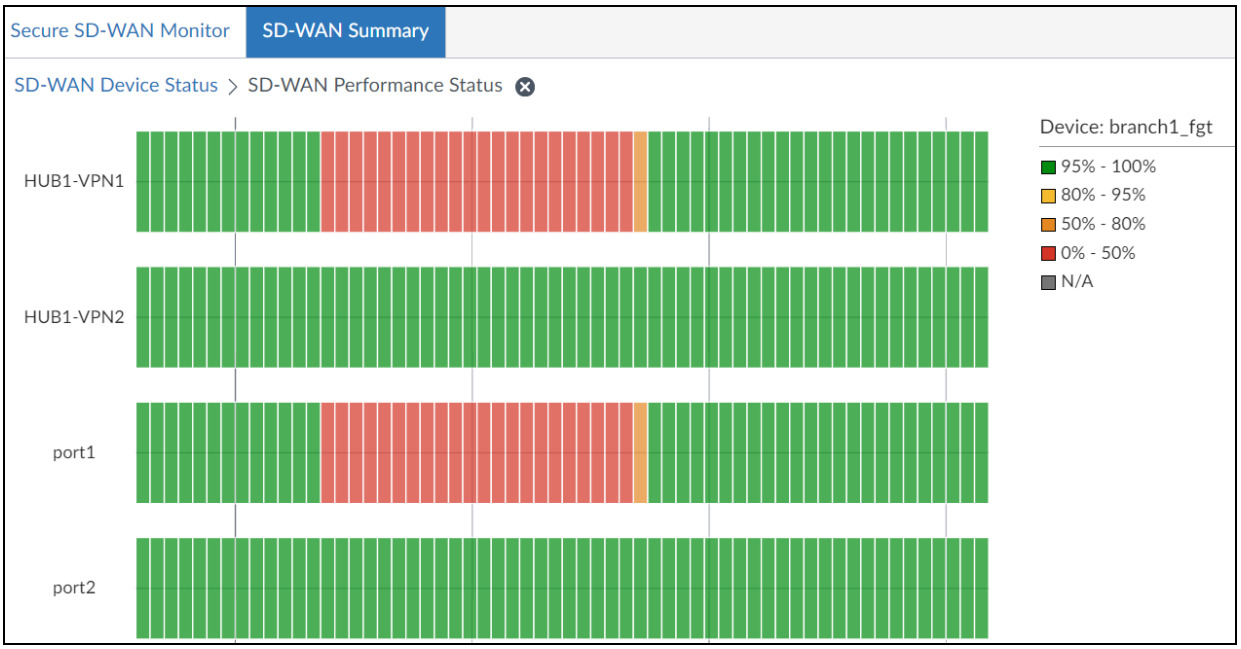
3. Click **Healthy Devices** to display the list of devices identified as healthy.
4. Close the window, and then click **Major Alerts Devices** to display the list of devices identified with an alert.
   Your page should look similar to the following example:



5. Double-click the device name (**branch1_fgt**) to view the cause of the alert.
   Your page should look similar to the following example:

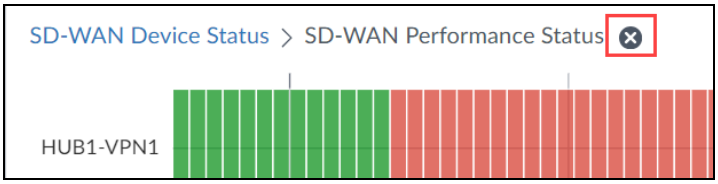
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



The red and orange bars correspond to the downtime and the missed SLA for the **port1** and **HUB1-VPN1** interfaces. The **SD-WAN Health Overview** widget reports this as an alert.

6. Hover over the graphs to see the health check details.
7. Close the window to return to the main **SD-WAN Summary** page.



8. In time range drop-down list, select **Last 5 Minutes**.
9. Review the output of the widget.

> **Stop and think!**
>
> The **SD-WAN Health Overview** widget now shows the three devices as healthy. Why?

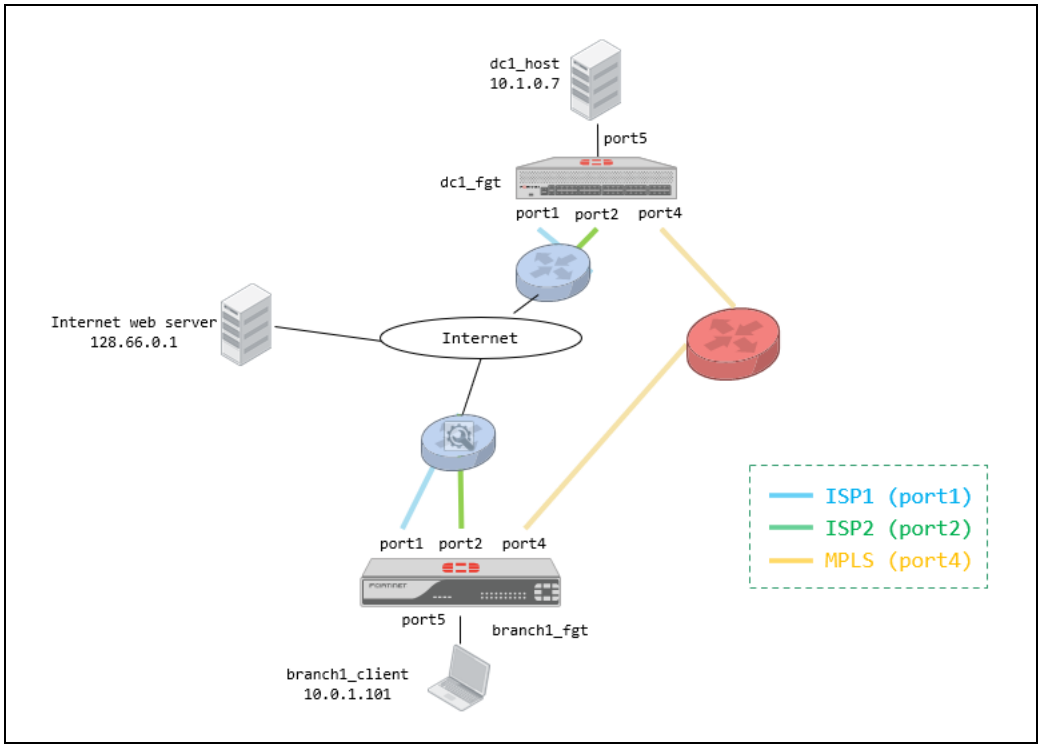
10. On **branch1_client** and **branch2_client**, press `Ctrl+C` to stop the traffic generator.
11. Continuing on the WAN simulator page, set the latency of **BR1-MPLS** back to 0 ms.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 5: Routing and Sessions

In this lab, you will configure a policy route and see the impact it has on an existing SD-WAN configuration. Next, you will configure FortiGate to allow session reevaluation for SNAT traffic. Finally, you will trigger a session reevaluation and monitor the reevaluation steps with CLI commands.



Through these lab exercises, you will use DIA to the web server (`128.66.0.1`) and overlay access to the dc1_host server, located behind the dc1_fgt SD-WAN hub.

Objectives

- Configure a policy route
- Analyze the routing behavior with SD-WAN and a policy route on FortiGate
- Configure FortiGate to allow SNAT session reevaluation on route change
- Monitor a session reevaluation

Time to Complete

Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Testing the Behavior of a Policy Route

In this exercise, you will test the behavior of FortiGate with the combination of policy routes and SD-WAN rules. First, you will check the routing behavior with the SD-WAN configuration that is already installed on the FortiGate. Next, you will configure a policy route and review the routing changes. Finally, you will remove the policy route that you configured.

Configure a Policy Route and Check the Impact on SD-WAN Rules

You will review the current routing behavior. Then, you will configure a policy route and review the impact that it has on the traffic steering that the SD-WAN rules perform.

To test the routing behavior without policy routes

1. Open an SSH session to branch1_client, and then log in with the following credentials:
   - Username: `root`
   - Password: `password`
2. Ping `10.1.0.7` (the dc1_host IP address), and then leave the command running.
3. Open two SSH sessions to branch1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
4. In the first SSH session to branch1_fgt, enter the following commands to check the status of SD-WAN, the sessions, and routing:

```
diagnose sys sdwan service4
get router info routing-table all
diagnose sys session filter dst 10.1.0.7
diagnose sys session list
diagnose netlink interface list | grep HUB1
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # diagnose sys sdwan  service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port1 underlay), alive, selected
    2: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Salesforce(16920,0) Microsoft.Portal(41469,0)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(4), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1),
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2)
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3)
C       10.200.99.1/32 is directly connected, Branch-Lo
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
C       192.168.1.0/26 is directly connected, HUB1-VPN1
C       192.168.1.1/32 is directly connected, HUB1-VPN1
C       192.168.1.64/26 is directly connected, HUB1-VPN2
C       192.168.1.65/32 is directly connected, HUB1-VPN2
C       192.168.1.128/26 is directly connected, HUB1-VPN3
C       192.168.1.129/32 is directly connected, HUB1-VPN3
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

According to the routing in place and the SD-WAN services definition, FortiGate uses the SD-WAN service ID 3 to steer the traffic from the LAN device `10.1.0.101` to the DC host `10.1.0.7`.

```
branch1_fgt # diagnose sys session filter dst 10.1.0.7

branch1_fgt # diagnose sys session list

session info: proto=1 proto_state=00 duration=819 expire=59 timeout=0 refresh_dir=both
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=100.64.1.1/0.0.0.0 vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=68880/820/1 reply=68880/820/1 tuples=2
tx speed(Bps/kbps): 83/0 rx speed(Bps/kbps): 83/0
orgin->sink: org pre->post, reply pre->post dev=7->20/20->7 gwy=192.168.1.61/0.0.0.0
hook=pre dir=org act=noop 10.0.1.101:316->10.1.0.7:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.7:316->10.0.1.101:0(0.0.0.0:0)
misc=0 policy_id=3 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=0000021b tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=4 sdwan_service_id=3
rpdb_link_id=ff000003 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off
total session: 1

branch1_fgt # diagnose netlink interface list | grep HUB1
if=HUB1-VPN1 family=00 type=768 index=20 mtu=1420 link=0 master=0
if=HUB1-VPN2 family=00 type=768 index=21 mtu=1420 link=0 master=0
if=HUB1-VPN3 family=00 type=768 index=22 mtu=1420 link=0 master=0
```

The session list confirms that FortiGate steers the traffic from branch1_client to dc1_host through the SD-WAN member 4, using the SD-WAN service ID 3.

The outgoing interface is HUB1-VPN1. This is the interface with the index 20 in the example. The ID can differ on your device.

5. In the second SSH session to branch1_fgt, enter the following command to capture ping traffic to `10.1.0.7`:
   `diagnose sniffer packet any "host 10.1.0.7 and icmp" 4`
6. Leave the command running.

```
branch1_fgt # diagnose sniffer packet any "host 10.1.0.7 and icmp" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.1.0.7 and icmp]
0.494849 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
0.494880 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
0.616321 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
0.616342 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.495577 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.495629 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.616990 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.617011 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

The sniffer trace provides another confirmation that the ping flows through the HUB1-VPN1 interface.

7. Access the WAN simulator page.
8. Locate the **BR1-ISP1** and **BR1-ISP2** control panels.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

9. Click **DOWN** to bring down the **BR1-ISP1** link on branch1_fgt, port1.
10. In the SSH session to branch1_fgt, where the sniffer is running, check the results.

```
16.309000 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
16.309025 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.332965 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.332998 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.373979 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
17.374006 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

After a few seconds, FortiGate directs the traffic to the HUB1-VPN2 interface.

11. Click **DOWN** to bring down the **BR1-ISP2** link on branch1_fgt, port 2.
12. In the SSH session to branch1_fgt, where the sniffer is running, check the results again.

```
14.391746 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
14.391774 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
15.416298 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
15.416329 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
16.440828 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
16.440868 HUB1-VPN3 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
16.441645 HUB1-VPN3 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
16.441655 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Similarly, after a few seconds. FortiGate directs the traffic to the HUB1-VPN3 interface.

13. In the first SSH session to branch1_fgt, use the commands in step 4 to check the status of SD-WAN, the sessions, and routing.

```
branch1_fgt # diag sys session list

session info: proto=1 proto_state=00 duration=2381 expire=59 timeout=0 refresh_dir=both fla
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=172.16.1.5/0.0.0.0 vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=199668/2377/1 reply=199164/2371/1 tuples=2
tx speed(Bps/kbps): 83/0 rx speed(Bps/kbps): 83/0
orgin->sink: org pre->post, reply pre->post dev=7->22/22->7 gwy=192.168.1.189/0.0.0.0
hook=pre dir=org act=noop 10.0.1.101:316->10.1.0.7:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.7:316->10.0.1.101:0(0.0.0.0:0)
misc=0 policy_id=3 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=0000021b tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=6 sdwan_service_id=3
rpdb_link_id=ff000003 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off
total session: 1

branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3)
C       10.200.99.1/32 is directly connected, Branch-Lo
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.168.0.0/24 is directly connected, port10
C       192.168.1.128/26 is directly connected, HUB1-VPN3
C       192.168.1.129/32 is directly connected, HUB1-VPN3
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

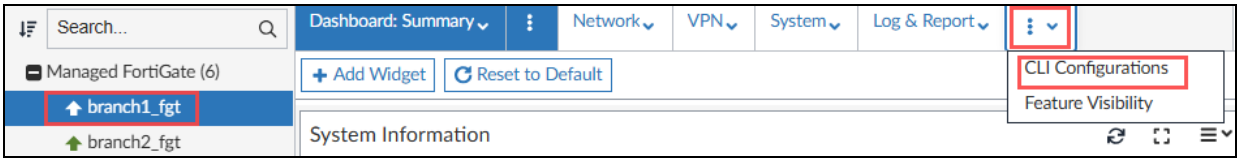
The SD-WAN rule steers the traffic through the member 6, which corresponds to the HUB1-VPN3 interface. Immediately after you shut down the interfaces, FortiGate still shows the three BGP routes to `10.1.0.0/24`. After a few seconds, the BGP routes through the inactive interfaces time out. Then, FortiGate shows only one route to `10.1.0.0/24`.

14. Use the WAN simulator page to bring up **BR1-ISP1** and **BR1-ISP2**.
15. On branch1_client, stop the ping.

To configure a policy route

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Device & Groups** > **Managed FortiGate**, and then click **branch1_fgt**.
3. Click **CLI Configurations**.

   Depending on the size and resolution of your screen, may need to click the expand menu icon first, and then select **CLI Configurations**, as shown in the following image:



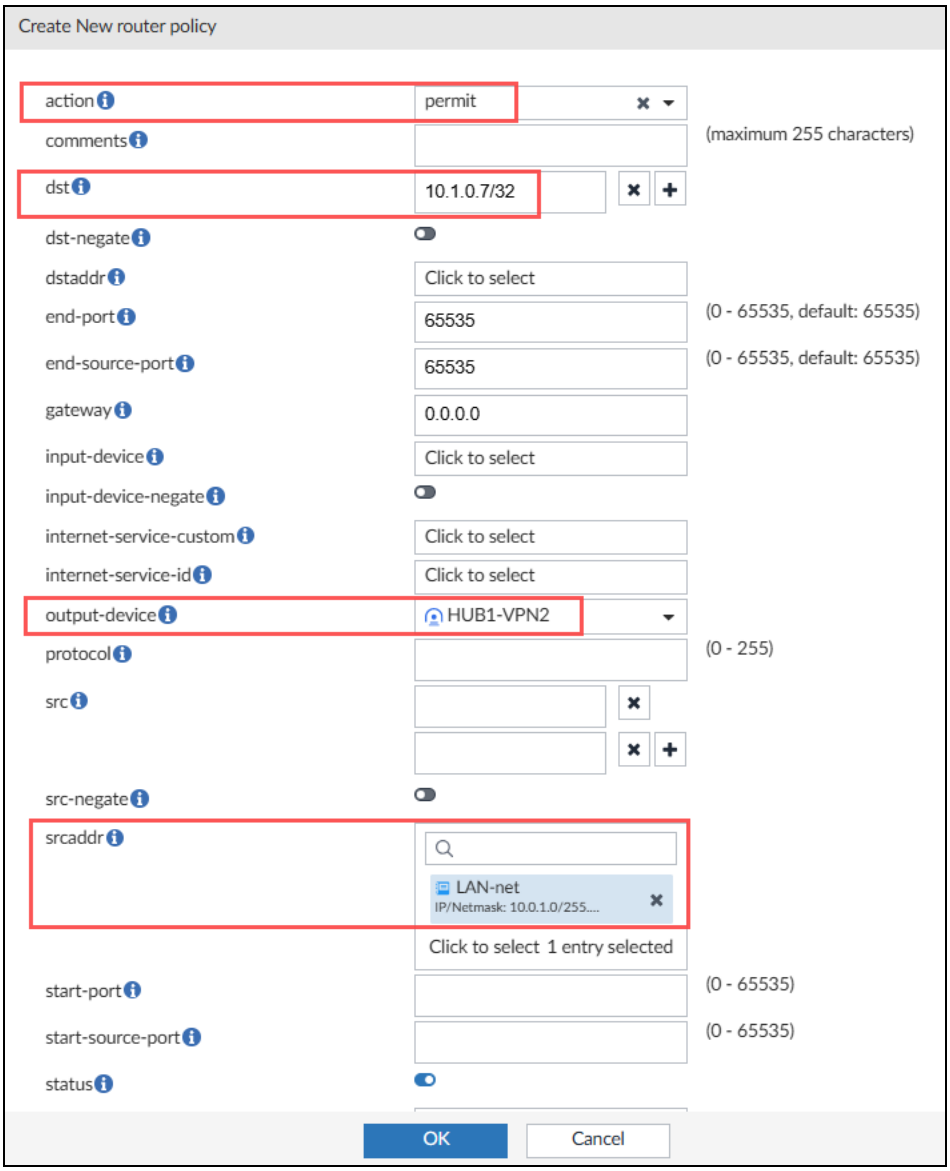
The **CLI Configurations** menu on the FortiManager GUI allows you to define CLI settings that are not directly available in the FortiManager GUI menus.

4. Click **Router** > **Policy**.
5. Click **Create New**, and then configure a policy route with the following settings:

Field	Value
action	permit
dst	10.1.0.7/32
output-device	Select **HUB1-VPN2**.
srcaddr	Select **LAN-net**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



6. Click **OK** to save the settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on the three devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To check the policy route impact on the traffic

1. On the WAN simulator, confirm that all interfaces are up.
2. On branch1_client, ping `10.1.0.7` (the dc1_host IP address), and then leave the command running.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

3. Continuing in the second SSH session to branch1_fgt, check the sniffer output.

   FortiGate directs the ping flow to `HUB1-VPN2`.

```
72.100303 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
72.100333 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
72.101612 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
72.101619 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

4. Continuing in the first SSH session to branch1_fgt, enter the following commands to check the status of SD-WAN, the sessions, and routing:

```
diagnose sys sdwan service4
get router info routing-table all
```

   The output remains similar to the output in the previous task, when you checked the status with all links up.

   The routing table remains unchanged and contains ECMP routes to 10.1.0.0/24 through the three overlays.

```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1),
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2)
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3)
C       10.200.99.1/32 is directly connected, Branch-Lo
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
C       192.168.1.0/26 is directly connected, HUB1-VPN1
C       192.168.1.1/32 is directly connected, HUB1-VPN1
C       192.168.1.64/26 is directly connected, HUB1-VPN2
C       192.168.1.65/32 is directly connected, HUB1-VPN2
C       192.168.1.128/26 is directly connected, HUB1-VPN3
C       192.168.1.129/32 is directly connected, HUB1-VPN3
```

Note that the `get router info routing-table all` command does not display the policy routes. To display the policy route status you can use the `diagnose firewall proute list` command.

5. Enter the following commands to check the session status:

```
diagnose sys session filter dst 10.1.0.7
diagnose sys session list
```

   Your output should be similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # branch1_fgt # diagnose sys session list

session info: proto=1 proto_state=00 duration=201 expire=59 timeout=0 refresh_dir=both
 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=100.64.1.9/0.0.0.0 vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=16884/201/1 reply=16884/201/1 tuples=2
tx speed(Bps/kbps): 79/0 rx speed(Bps/kbps): 79/0
orgin->sink: org pre->post, reply pre->post dev=7->21/21->7 gwy=192.168.1.125/0.0.0.0
hook=pre dir=org act=noop 10.0.1.101:376->10.1.0.7:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.7:376->10.0.1.101:0(0.0.0.0:0)
misc=0 policy_id=3 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=00000747 tos=ff/ff app_list=0 app=0 url_cat=0
route_policy_id=1
rpdb_link_id=80000001 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off
total session: 1
```

The session details confirm that the traffic to 10.1.0.7 is routed through the HUB1-VPN2 interface (interface ID 21).

The session output indicates that the traffic matches the policy ID 1.

6. Continuing in the first SSH session to branch1_fgt, enter the following command:
   `diagnose firewall proute list`
   Your output should be similar to the following example:

```
branch1_fgt # branch1_fgt # diag firewall proute list
list route policy info(vf=root):

id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):
dst(0->0) iif=0(any)
path(1): oif=21(HUB1-VPN2) path_last_used=2024-10-28 03:27:39
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 10.1.0.7/255.255.255.255
hit_count=17 rule_last_used=2024-10-28 03:27:39

id=2130968577(0x7f040001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=3(port1), oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) Microsoft.Portal(41469,0)
hit_count=0 rule_last_used=2024-10-28 01:31:47

id=2130968578(0x7f040002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xfc 0xf
c flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
hit_count=0 rule_last_used=2024-10-28 01:31:47

id=2130968579(0x7f040003) vwl_service=3(Corp) vwl_mbr_seq=4 5 6 dscp_tag=0xfc 0xfc flags=
0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=33 rule_last_used=2024-10-28 02:45:09
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The `diagnose firewall proute list` command lists the policy route that the administrator manually defined and the policy route that FortiGate created from the SD-WAN rules.

7. On branch1_client, stop the ping.

Take the Expert Challenge!

What happens if the HUB1-VPN2 interface goes down? Use the WAN-controller to shut down BR1-ISP2 and check the result.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see To remove the policy route and install the device settings on page 161.

8. Use the WAN simulator page to bring down **BR1-ISP2**.
9. Repeat steps 2–7 in this procedure to check the status of the traffic flow.
   The session output indicates that FortiGate routes the traffic according to the SD-WAN rules.

FortiGate considers a policy route invalid if there is no matching route in the FIB and skips it.

Because FortiGate has no route through HUB1-VPN2 in its FIB, it skips the policy rule. The next rules that apply are the SD-WAN rules.

10. Use the WAN simulator page to bring up **BR1-ISP2**.
11. On branch1_client, stop the ping.

To remove the policy route and install the device settings

1. Continuing on the FortiManager GUI, click **Device Manager** > **Device & Groups** > **Managed FortiGate**, and then click **branch1_fgt**.
2. Click **CLI Configurations** > **Router** > **Policy**.
3. Select the policy route that you created, and then click **Delete**.
4. Click **OK** to validate.
5. Click **Install Wizard**.
6. Select **Install Device Settings (only)**, and then click **Next**.
7. Select **branch1_fgt**, and then click **Next**.
8. Click **Install** to install the configuration on the three devices.
9. Wait for the installation to finish.
10. Click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Monitoring the Reevaluation of Sessions

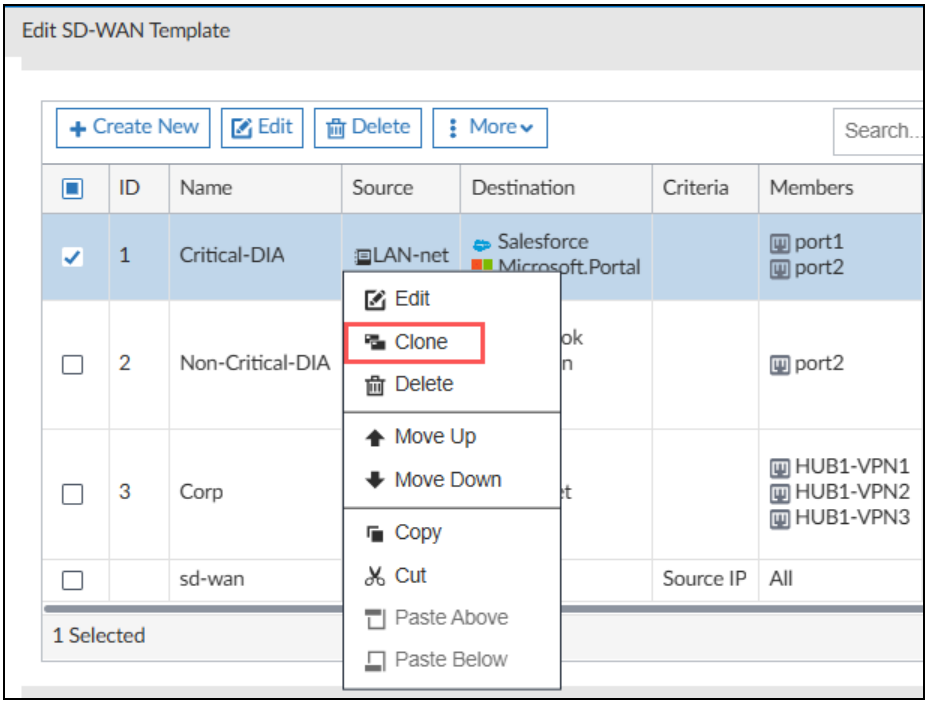
In this exercise, you will monitor how FortiGate reevaluates the session when the degradation of the performance of a link cause SD-WAN to redefine the priority members, and therefore to adjust the policy route table. First, you will configure an SD-WAN rule to steer the traffic to a test web server, using the two underlay interfaces and the lowest cost (SLA) strategy. Next, you will confirm the routing and session behavior when the performance of both links meet the SLA. Finally, you will monitor the session reevaluation when the performance of the link used to steer the traffic degrades.

Monitor the Session Reevaluation When the Link Performance Degrades

First, you will create a new SD-WAN rule dedicated to steering the traffic to the test server. This rule uses the two underlay links, port1 and port2, and the lowest cost strategy. Additionally, because the flow being tested requires SNAT, you will allow SNAT and SNAT route change. Next , you will test the behavior and use FortiGate CLI commands to review the session status.

To configure an SD-WAN rule to steer the traffic to the web server

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Provisioning Templates**, and then click **SD-WAN**.
3. Double-click **branches** to edit the template settings.
4. In the **SD-WAN Rules** section, right-click the **Critical-DIA** rule, and then select **Clone**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

5. Configure, review, or adjust the following settings:

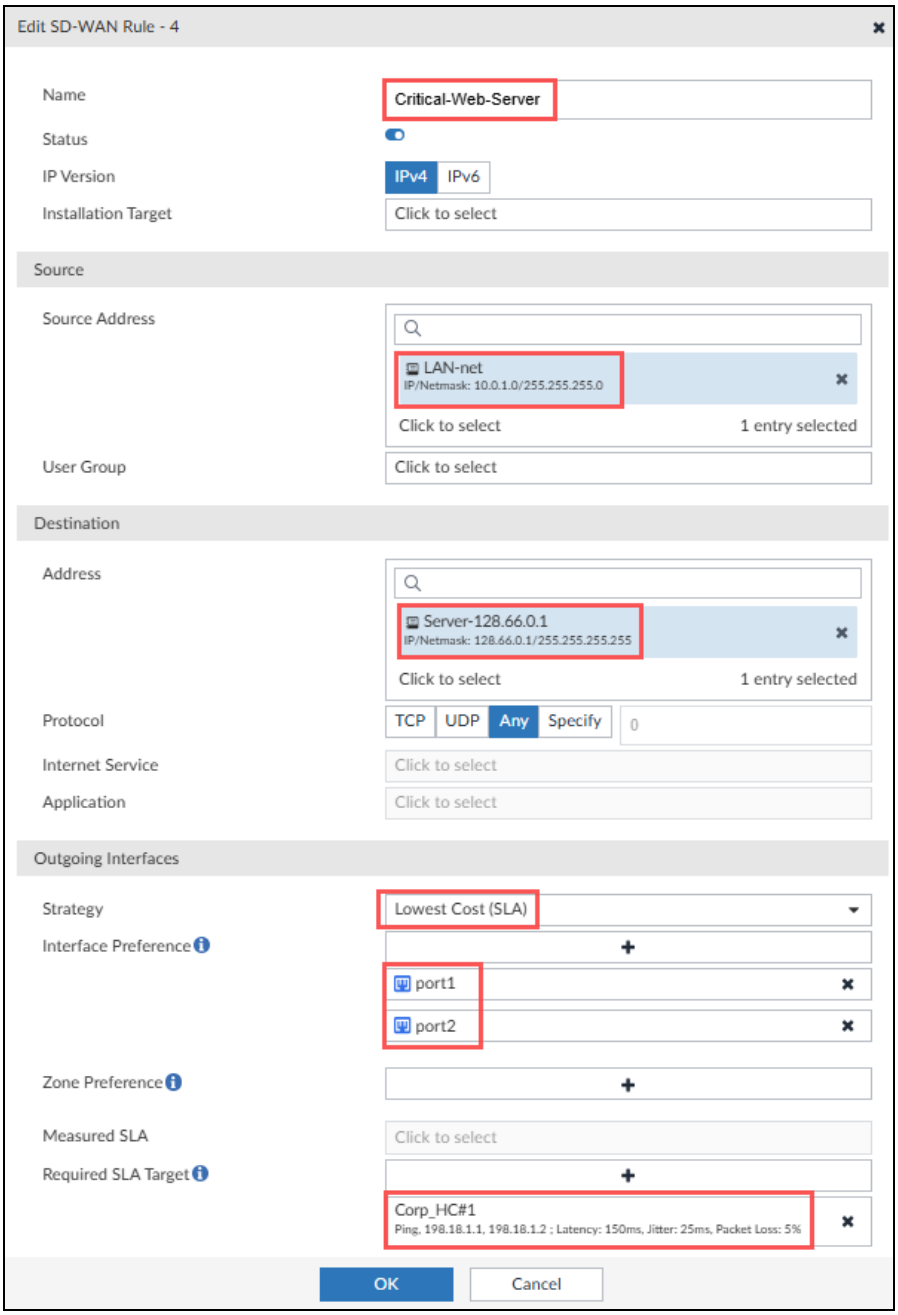
Field	Value
Name	Critical-Web-Server
Source address	LAN-net
Destination	Delete the **Microsoft.Portal** and **Salesforce** applications. In the **Address** field, select **Server-128.66.0.1**.
Outgoing Interfaces	In the **Strategy** field, select **Lowest Cost (SLA)**. In the **Interface Preference** field, select **port1** and **port2**.
Required SLA Target	Select **Corp_HC#1**.

Make sure that you set the configuration priority (or interface preference list configuration) as follows (most preferred first):

- **port1**
- **port2**

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

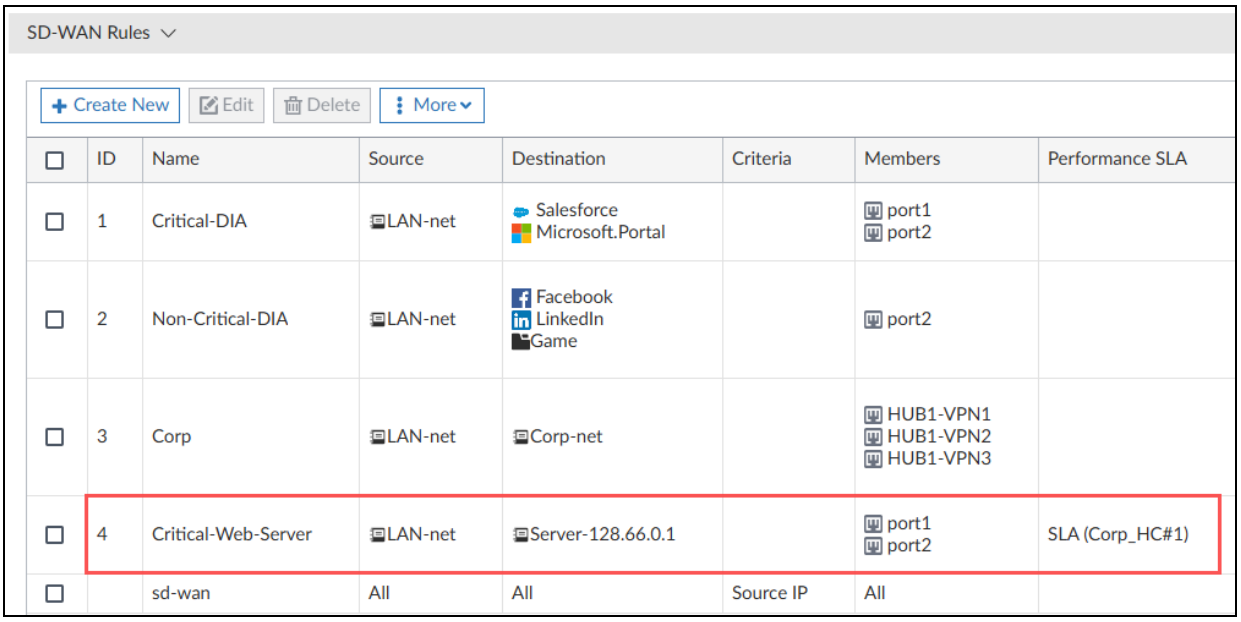
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



6. Click **OK** to save the rule settings.
   The **SD-WAN Rules** section in your template should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

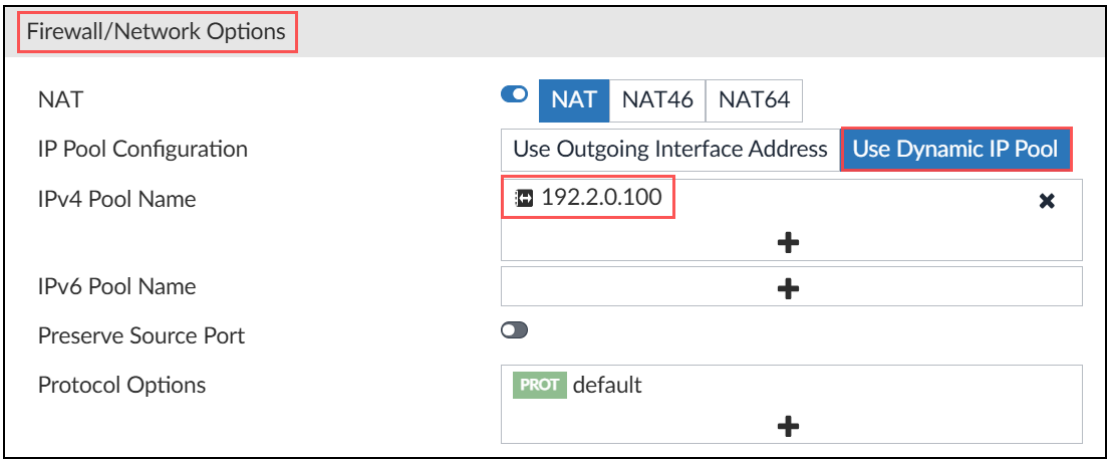
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



7. Click **OK** to validate the template update.

To update the firewall policy to use an IP pool

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Policy Packages**, and then expand **branches_pp**.
2. Double-click the **DIA** policy to edit it.
3. In the **Firewall/Network Options** section, in the **IP Pool Configuration** field, click **Use Dynamic IP Pool**.
4. In the **IPv4 Pool Name** field, click **+**, and then select the **192.2.0.100** pool.
   This IP pool was preconfigured for you.



5. Click **OK** to validate the policy update.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

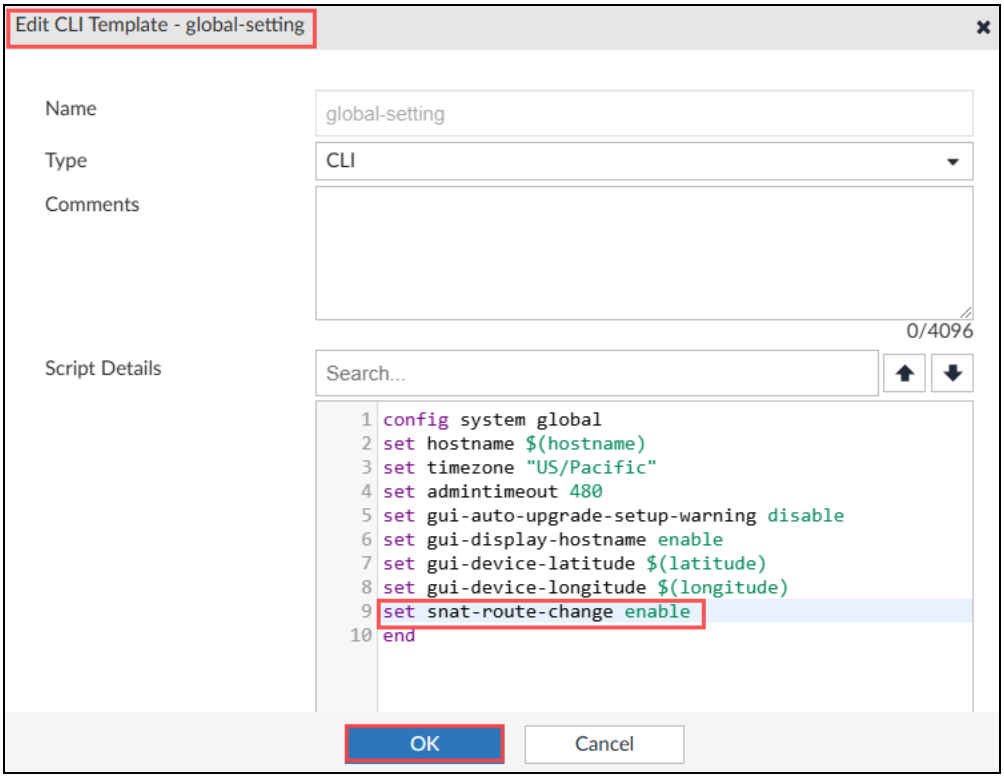
By default, FortiGate uses the outgoing interface IP address as the replacement source address for the traffic that is allowed by a policy configured for NAT. This is know as source NAT (SNAT).

Optionally, you can configure the firewall policy to use the addresses of an IP pool for source NAT. This option allows FortiGate to use, as the SNAT IP address, an IP address that is independent of the outgoing interface.

To allow routing changes for SNAT sessions

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **CLI**.
2. Double-click the **global-setting** template to edit it.
3. Add the following command to the template:
   `set snat-route-change enable`

   Your output should be similar to the following example:



4. Click **OK** to validate the template update.

By default, FortiGate does not perform session reevaluation for SNAT sessions. In other words, FortiGate does not flag SNAT sessions as `dirty`.

You can instruct FortiGate to reevaluate SNAT sessions using the `set snat-route-change enable` command. To avoid a source IP address change when FortiGate reevaluates SNAT sessions, you must use this option together with IP pools.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Policy Package & Device Settings**, and then in the **Policy Package** field, select **branches_pp**.
3. Click **Next**.
4. Select **branch1_fgt**, **branch2_fgt**, and **branch3_fgt**, and then click **Next**.
5. Click **Install** to install the configuration on the branch devices.
6. Wait for the installation to finish.
7. Click **Finish**.

To monitor a session establishment

1. Open two SSH sessions to branch1_client, and then log in with the following credentials:
   - Username: `root`
   - Password: `password`
2. In the first SSH session to branch1_fgt, enter the following commands to check the session establishment details:
   ```
   diagnose debug flow filter addr 128.66.0.1
   diagnose debug enable
   diagnose debug flow trace start 2
   ```
3. In the second SSH session to branch1_fgt, enter the following commands:
   ```
   diagnose sys session filter dst 128.66.0.1
   diagnose sys session list
   ```
   At this stage, the filtered session list should be empty.
4. Open an SSH session to branch1_client, and then log in with the following credentials:
   - Username: `root`
   - Password: `password`
5. Enter the following command and credential to establish an SSH web session to the web server:
   ```
   ssh 128.66.0.1
   password
   ```
   ```
   root@branch1-client-cli:~# ssh 128.66.0.1
   root@128.66.0.1's password:
   Linux www-webserver-lab 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

   The programs included with the Debian GNU/Linux system are free software;
   the exact distribution terms for each program are described in the
   individual files in /usr/share/doc/*/copyright.

   Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
   permitted by applicable law.
   Last login: Sun Oct 27 20:49:55 2024 from 128.66.0.192
   root@www-webserver-lab:~#
   ```
6. Continuing on the first SSH session to branch1_fgt, review the debug flow output.
   Your output should be similar to the following image:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

```
branch1_fgt # diag debug flow trace start 2

branch1_fgt # id=65308 trace_id=9 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(pr
oto=6, 10.0.1.101:42764->128.66.0.1:22) tun_id=0.0.0.0 from port5. flag [S], seq 626932366, ack 0, wi
n 64240"
id=65308 trace_id=9 func=init_ip_session_common line=6127 msg="allocate a new session-000009e3"
id=65308 trace_id=9 func=rpdb_srv_match_input line=1148 msg="Match policy routing id=2131165188: to 1
28.66.0.1 via ifindex-3"
id=65308 trace_id=9 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-192.2.
0.2 via port1"
id=65308 trace_id=9 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=59, len=2"
id=65308 trace_id=9 func=get_new_addr line=1274 msg="find SNAT: IP-192.2.0.100(from IPPOOL), port-427
64"
id=65308 trace_id=9 func=fw_forward_handler line=997 msg="Allowed by Policy-1: SNAT"
id=65308 trace_id=9 func=ip_session_confirm_final line=3141 msg="npu_state=0x1100, hook=4"
id=65308 trace_id=9 func=ids_receive line=466 msg="send to ips"
id=65308 trace_id=9 func=__ip_session_run_tuple line=3474 msg="SNAT 10.0.1.101->192.2.0.100:42764"
id=65308 trace_id=10 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=6, 128.66
.0.1:22->192.2.0.100:42764) tun_id=0.0.0.0 from port1. flag [S.], seq 585950650, ack 626932367, win 6
5160"
id=65308 trace_id=10 func=resolve_ip_tuple_fast line=6030 msg="Find an existing session, id-000009e3
 reply direction"
id=65308 trace_id=10 func=__ip_session_run_tuple line=3487 msg="DNAT 192.2.0.100:42764->10.0.1.101:42
764"
id=65308 trace_id=10 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-0.0.0
.0 via port5"
id=65308 trace_id=10 func=npu_handle_session44 line=1355 msg="Trying to offloading session from port1
 to port5, skb.npu_flag=00000400 ses.state=00002204 ses.npu_state=0x00001108"
id=65308 trace_id=10 func=fw_forward_dirty_handler line=443 msg="state=00002204, state2=00000001, npu
_state=00001108"
id=65308 trace_id=10 func=ids_receive line=466 msg="send to ips"
```

The debug flow shows the details of the session establishment.

The highlighted fields indicates what FortiGates does:

- Allocates a new session—this occurs when FortiGate receives the SYN packet of the SSH session.
- Identifies a matching policy route. The policy route ID indicates a policy route related to ISDN or SD-WAN.
- Finds a route through port1.
- Determines that the flow requires SNAT and identifies the SNAT IP address.
- Finds the firewall policy that allows the flow.
- Analyzes the first reply packet (SYN-ACK) and associate it to the session created with the packet in the original direction.

7. Continuing on the second SSH session to branch1_fgt, check the session list.
   Your output should be similar to the following image:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

```
branch1_fgt # diagnose sys session list

session info: proto=6 proto_state=11 duration=328 expire=3274 timeout=3600 refresh_dir=both
00000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3317/18/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:42764->128.66.0.1:22(192.2.0.100:42764)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:42764(10.0.1.101:42764)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:42764(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=000009e3 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=4
rpdb_link_id=ff000004 ngfwid=n/a
npu_state=0x001108
no_ofld_reason:  redir-to-ips denied-by-nturbo
total session: 1
```

From the session list output, you can see that:

- FortiGate flagged the session with `may_dirty`.
- FortiGate applies SNAT to this flow and translates the source IP address to `192.2.0.100`.
- The policy ID 1 allows this flow.
- FortiGate uses the SD-WAN rule ID 4 to steer this flow and the outgoing interface is the SD-WAN member with the sequence ID 1.

To monitor the session behavior when the link performance degrades

1. Connect to the WAN simulator HTTP interface, and then locate **BR1-ISP1**.
2. For the **BR1-ISP1** interface, use the vertical bar to increase the **delay** to 180 ms.
3. Continuing on the second SSH session to branch1_fgt, enter the following commands:
   ```
   diagnose sys sdwan service4 4
   diagnose sys session list
   ```
   Your output should be similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

```
branch1_fgt # diagnose sys sdwan service4 4

Service(4): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 port2 underlay), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(1 port1 underlay), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        128.66.0.1-128.66.0.1


branch1_fgt # diagnose sys session list

session info: proto=6 proto_state=11 duration=888 expire=3565 timeout=3600 refresh_dir=both flags=
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3489/20/1 reply=3897/18/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:42764->128.66.0.1:22(192.2.0.100:42764)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:42764(10.0.1.101:42764)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:42764(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=000009e3 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=4
rpdb_link_id=ff000004 ngfwid=n/a
npu_state=0x001008
no_ofld_reason:  redir-to-ips
total session: 1
```

FortiGate updates the order of the SD-WAN members to reflect the performance degradation for the link on port1, and flagged all `may_dirty` session as `dirty`.

FortiGate did not yet change the SD-WAN members associated with the session.

4. Continuing on the first SSH session to branch1_fgt, enter the following command to restart the debug flow:
   `diagnose debug flow trace start 2`
5. Continuing on the branch1_client session, press `Enter` to generate traffic to the web server.
6. On the first SSH session to branch1_fgt, check the debug flow output.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

```
branch1_fgt # diag debug flow trace start 2

branch1_fgt # id=65308 trace_id=11 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(p
roto=6, 10.0.1.101:42764->128.66.0.1:22) tun_id=0.0.0.0 from port5. flag [.], seq 626934808, ack 5859
53604, win 501"
id=65308 trace_id=11 func=resolve_ip_tuple_fast line=6030 msg="Find an existing session, id-000009e3,
original direction"
id=65308 trace_id=11 func=rpdb_srv_match_input line=1148 msg="Match policy routing id=2131165188" to
128.66.0.1 via ifindex-4"
id=65308 trace_id=11 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-192.2
.0.10 via port2"
id=65308 trace_id=11 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=60, len=2
"
id=65308 trace_id=11 func=get_new_addr line=1274 msg="find SNAT: IP-192.2.0.100(from IPPOOL) port-60
484"
id=65308 trace_id=11 func=ids_receive line=466 msg="send to ips"
id=65308 trace_id=11 func=__ip_session_run_tuple line=3474 msg="SNAT 10.0.1.101->192.2.0.100:42764"
id=65308 trace_id=12 func=print_pkt_detail line=5942 msg="vd-root:0 received a packet(proto=6, 128.66
.0.1:22->192.2.0.100:42764) tun_id=0.0.0.0 from port1. flag [.], seq 585953604, ack 626934876, win 50
1"
id=65308 trace_id=12 func=resolve_ip_tuple_fast line=6030 msg="Find an existing session, id-000009e3,
reply direction"
id=65308 trace_id=12 func=__ip_session_run_tuple line=3487 msg="DNAT 192.2.0.100:42764->10.0.1.101:42
764"
id=65308 trace_id=12 func=__vf_ip_route_input_rcu line=1988 msg="find a route: flag=00000000 gw-0.0.0
.0 via port5"
id=65308 trace_id=12 func=npu_handle_session44 line=1355 msg="Trying to offloading session from port1
 to port5, skb.npu_flag=00000400 ses.state=00002284 ses.npu_state=0x00001108"
id=65308 trace_id=12 func=fw_forward_dirty_handler line=443 msg="state=00002284, state2=00004001, npu
_state=00001108"
id=65308 trace_id=12 func=ids_receive line=466 msg="send to ips"
```

The debug flow shows that FortiGate reevaluated the first packet in each direction for the session that already exists. It matches the same policy route, but this time, it directs the traffic through port2.

7. Continuing on the second SSH session to branch1_fgt, enter the following command:

   `diagnose sys session list`

   Your output should be similar to the following example:

```
branch1_fgt # diagnose sys session list

session info: proto=6 proto_state=11 duration=1493 expire=3276 timeout=3600 refresh_dir=both
000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3853/25/1 reply=4217/21/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->4/4->7 gwy=192.2.0.10/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:42764->128.66.0.1:22(192.2.0.100:42764)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:42764(10.0.1.101:42764)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:42764(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=000009e3 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=4
rpdb_link_id=ff000004 ngfwid=n/a
npu_state=0x001008
no_ofld_reason:  redir-to-ips
total session: 1
```

You can see the result of the session reevaluation, with port2 (interface index 4, SD-WAN member 2) as the new outgoing interface. FortiGate removed the `dirty` flag.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

8. On the branch1_client session, enter `exit` to close the SSH session to the web server.
9. On the WAN simulator page, set the latency of **BR1-ISP1** back to 0 ms.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 6: Rules

In this lab, you will configure and test the following rule strategies: best quality, lowest cost (SLA), and lowest cost (SLA) with load balancing. You will use FortiManager and the configuration that you set up in the previous labs.

Objectives

- Configure best quality, lowest cost (SLA), and lowest cost (SLA) with load balancing rules
- Test the rule behavior when the link performance degrades

Time to Complete

Estimated: 50 minutes

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

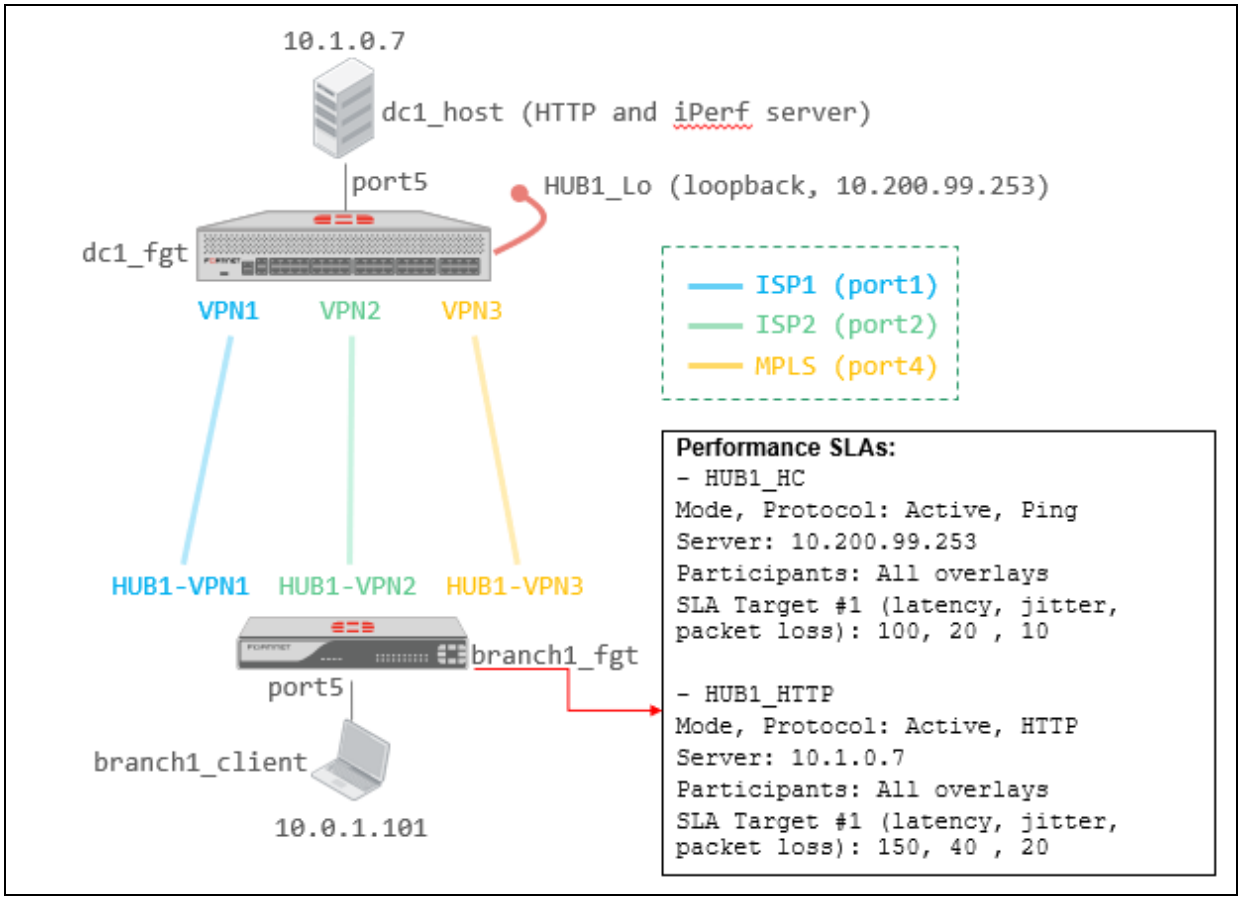
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Configuring and Testing Rule Strategies

In this exercise, you will configure an SD-WAN rule to steer traffic between branch1_client and dc1_host. You will use best quality as the first strategy, then lowest cost (SLA), and finally combine load balancing with the lowest cost (SLA) strategy. Next, you will test each strategy by generating traffic between branch1_client and dc1_host, while changing the link metrics using the WAN simulator, and then you will observe the changes in the outgoing interface list and traffic steering.

You will update the configuration on branch1_fgt only and focus on the topology elements shown in the following image:



Configure and Test a Best Quality Rule

First, you will configure a rule that uses best quality as the strategy and latency as the metric. Next, you will test the rule by generating ping traffic and changing the condition of the links.

To configure a best quality rule

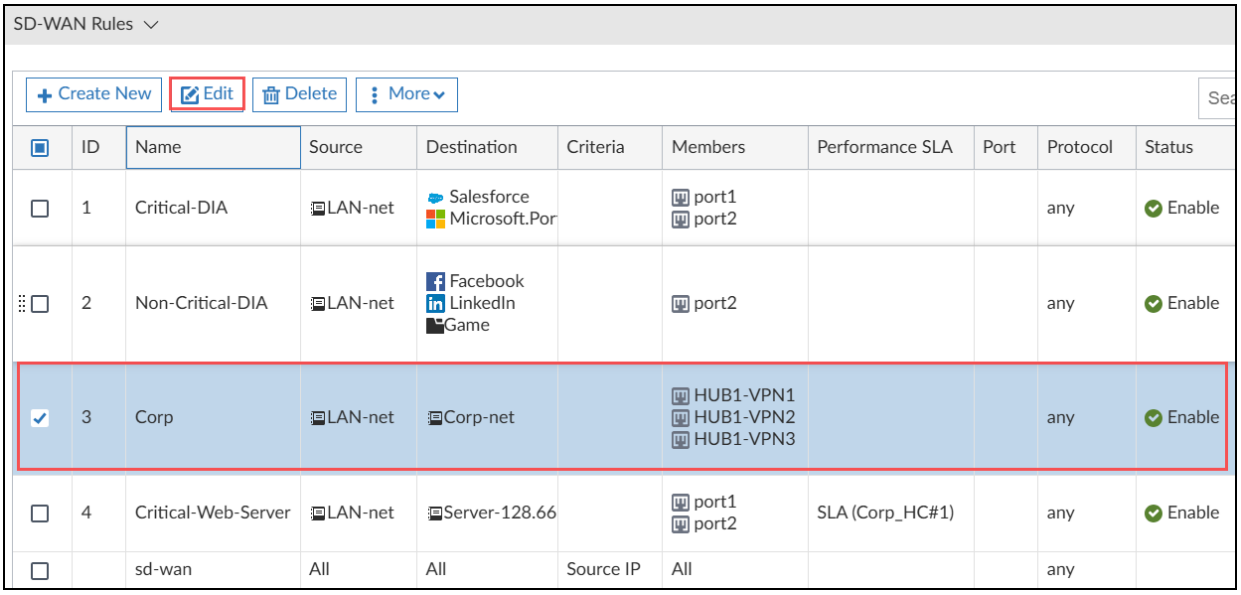
1. Connect to the FortiManager GUI, and then log in with the following credentials:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

- Username: `admin`
- Password: `password`

2. Click **Device Manager** > **Provisioning Templates**, and then click **SD-WAN**.
3. Double-click **branches** to edit the template settings.
4. In the **SD-WAN Rules** section, select the checkbox for the **Corp** rule, and then click **Edit**.



5. Configure the following settings:

Field	Value
Name	Best_Quality_Latency
Source address	LAN-net
Destination address	Corp-net
Outgoing Interfaces	1. In the **Strategy** field, select **Best Quality**. 2. In the **Interface Preference** field, select **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**. 3. Drag and drop the interfaces to organize them in the following order: **HUB1-VPN1**, **HUB1-VPN2**, **HUB1-VPN3**.
Measured SLA	Select **HUB1_HC**.
Quality Criteria	Select **Latency**.

Make sure that you set the configuration priority (or interface preference list configuration) as follows (most preferred first):

- **HUB1-VPN1**
- **HUB1-VPN2**
- **HUB1-VPN3**

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

6. Click **OK** to save the rule settings.

   The **SD-WAN Rules** section in your template should look similar to the following example:

SD-WAN Rules

Create New | Edit | Delete | More | Search...

	ID	Name	Source	Destination	Criteria	Members	Performance SLA
	1	Critical-DIA	LAN-net	Salesforce Microsoft.Portal		port1 port2	
	2	Non-Critical-DIA	LAN-net	Facebook LinkedIn Game		port2	
	3	Best_Quality_Latency	LAN-net	Corp-net	Latency	HUB1-VPN1 HUB1-VPN2 HUB1-VPN3	HUB1_HC
	4	Critical-Web-Server	LAN-net	Server-128.66.0.1		port1 port2	SLA (Corp_HC#1)
		sd-wan	All	All	Source IP	All	

7. Click **OK** to save the template settings.

To adjust the performance SLA

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
2. Double-click **branches** to edit the template settings, and then locate the **Performance SLA** section.
3. Double-click **HUB1_HC** to edit it, and then delete the second SLA target.

SLA Target

Link Cost Factor	Latency Threshold	Jitter Threshold	Packet Loss Threshold	Mos Threshold	Priority IN-SLA	Priority OUT-SLA	Action
Auto	100 ms	20 ms	10 %		0	0	
Auto	150 ms	40 ms	20 %		0	0	

4. Click **OK** to save the performance SLA update.
5. Click **OK** to save the template settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** only, and then click **Next**.
4. Click **Install** to install the configuration on branch1_fgt.
5. Wait for the installation to finish.
6. Click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To test a best quality rule

1. Open two SSH sessions to branch1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Access the WAN simulator page.
3. Locate the **BR1-ISP1**, **BR1-ISP2**, and **BR1-MPLS** control panels.
4. Use the vertical bar to increase the **delay** of each link to the following values:

Link Name	Delay
BR1-ISP1	100 ms
BR1-ISP2	110 ms
BR1-MPLS	120 ms

5. In the first SSH session to branch1_fgt, enter the following command to display the rule status:
   `diagnose sys sdwan service4`
   Focus on `Service(3)`, displayed at the end of the output. Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
link-cost-factor(latency), link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 101.662  selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 111.472  selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 121.093  selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

By default, FortiGate calculates the member latency and jitter based on the last 30 health check probes. For this reason, you may have to wait a few seconds before FortiGate can reflect the actual latency.

After a few seconds, FortiGate reflects the actual latency for the links. `HUB1-VPN1` is the preferred member.

6. In the second SSH session to branch1_fgt, enter the following command to capture ping traffic to `10.1.0.7`:
   `diagnose sniffer packet any "host 10.1.0.7 and icmp" 4 | grep HUB`
7. Leave the command running.
8. Open an SSH session to branch1_client, and then log in with the following credentials:
   - Username: `root`
   - Password: `password`

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

9. Ping `10.1.0.7` and leave the command running.
10. In the second SSH session to branch1_fgt, view the sniffer output.

    Your output should look similar to the following example:

```
0.701436 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
0.803204 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.701825 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.803241 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

According to the rule status, FortiGate prefers HUB1-VPN1, and therefore picked that member to steer the ping traffic.

11. Use the WAN simulator to reduce the latency of HUB1-VPN2 (**BR1-ISP2**) to 95 ms.
12. On branch1_fgt, check the rule status and sniffer again.

Stop and think!

The latency of HUB1-VPN2 is now the lowest among all the members. Yet, FortiGate still prefers HUB1-VPN1 and steers traffic to it. Why?

Remember the `link-cost-threshold` setting, which is set to 10 by default. The setting gives an advantage to members with a higher configuration priority. The corrected metric (CM) for HUB1-VPN1, which factors in the advantage, is determined by dividing its actual latency by 1.10. Assuming an actual latency of 100 ms, the CM would be about 91 ms (100 / 1.10).

13. Use the WAN simulator to reduce the latency of HUB1-VPN2 (**BR1-ISP2**) to 85 ms.
14. On branch1_fgt, check the rule status and sniffer again.

    Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
link-cost-factor(latency), link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 86.402, selected
    2: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 101.582, selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 121.034, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

```
6.414135 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
6.500592 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
7.414000 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
7.500381 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

HUB1-VPN2 beats the advantage given to HUB1-VPN1. FortiGate now prefers HUB1-VPN2, and therefore picked that member to steer the ping traffic.

15. Use the WAN simulator to increase the latency of HUB1-VPN2 (**BR1-ISP2**) to 95 ms.
16. On branch1_fgt, check the rule status and sniffer again.

Stop and think!

The latency of HUB1-VPN2 is still the lowest. Yet, FortiGate now prefers HUB1-VPN1 and steers traffic to it. Why?

FortiGate allows a quick recovery of the highest priority member (HUB1-VPN1) by considering its CM when competing against other lower-priority members. In this case, the CM of HUB1-VPN1 (~91 ms) is lower than the actual latency of HUB1-VPN2 (~95 ms).

17. Use the WAN simulator to increase the latency of HUB1-VPN2 (**BR1-ISP2**) to 110 ms.
18. On branch1_fgt, check the rule status to confirm that the latency of HUB1-VPN2 is ~110 ms.
19. Use the WAN simulator to reduce the latency of HUB1-VPN3 (**BR1-MPLS**) to 95 ms.
20. On branch1_fgt, check the rule status again.
    Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(4), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
link-cost-factor(latency), link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 101.551, selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 96.043, selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 111.313, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

HUB1-VPN3 moved up in the list because its real latency is lower than the CM of HUB1-VPN2 (~100 ms).

21. Use the WAN simulator to increase the latency of HUB1-VPN3 (**BR1-MPLS**) to 115 ms.
22. On branch1_fgt, check the rule status again.
    Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(5), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
link-cost-factor(latency), link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 101.655, selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 111.459, selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 115.396, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

FortiGate placed HUB1-VPN2 back above HUB1-VPN3.

23. Use the WAN simulator to reduce the latency of all three overlays back to 0 ms.
24. On branch1_client, stop the ping to `10.1.0.7`.
25. On branch1_fgt, stop the sniffer.
26. Keep the SSH sessions to branch1_client and branch1_fgt open because you will need them for the next task.

Configure and Test a Lowest Cost (SLA) Rule

First, you will configure a rule that uses lowest cost (SLA) as the strategy, and two SLA targets, one based on ICMP and another based on HTTP. Next, you will test the rule by generating ping traffic and changing the SLA status of the links.

To define an SLA target for the HTTP protocol

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **Performance SLA** section, click **Create New**.
4. Configure the following settings:

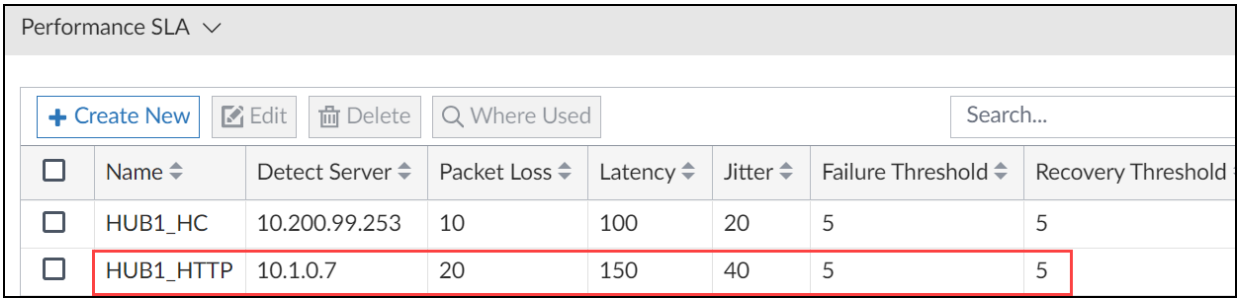
Field	Value
Name	HUB1_HTTP
Protocol	HTTP
Servers	10.1.0.7

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Participants	Click **Specify**, and then select **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**.
SLA target	Click **+**, and then configure the following targets: • Latency: 150 • Jitter: 40 • Packet loss: 20
Advanced Options	In the **source** field, type `$`, and then select **lan_interface_ip**.

5. Click **OK** to validate the performance SLA definition.



6. Click **OK** to validate the SD-WAN template update.

You must configure a source IP address for the **HUB1_HTTP** performance SLA to check the performance with traffic that mimics traffic from the branch FortiGate LAN.

This enables the hub firewall policies, which control traffic from the branch LAN to the corporate network behind the hub, to allow the probe packet.

To configure a lowest cost (SLA) rule

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **SD-WAN Rules** section, double-click **Best_Quality_Latency** to edit the rule settings.
4. Configure the following settings:

Field	Value
Name	Lowest_Cost
Outgoing Interfaces	1. In the **Strategy** field, select **Lowest Cost (SLA)**. 2. Keep the current **Interface Preference** settings.
Required SLA Target	1. Select **HUB1_HC#1** and **HUB1_HTTP#1**. 2. Move **HUB1_HC#1** above **HUB1_HTTP#1**.

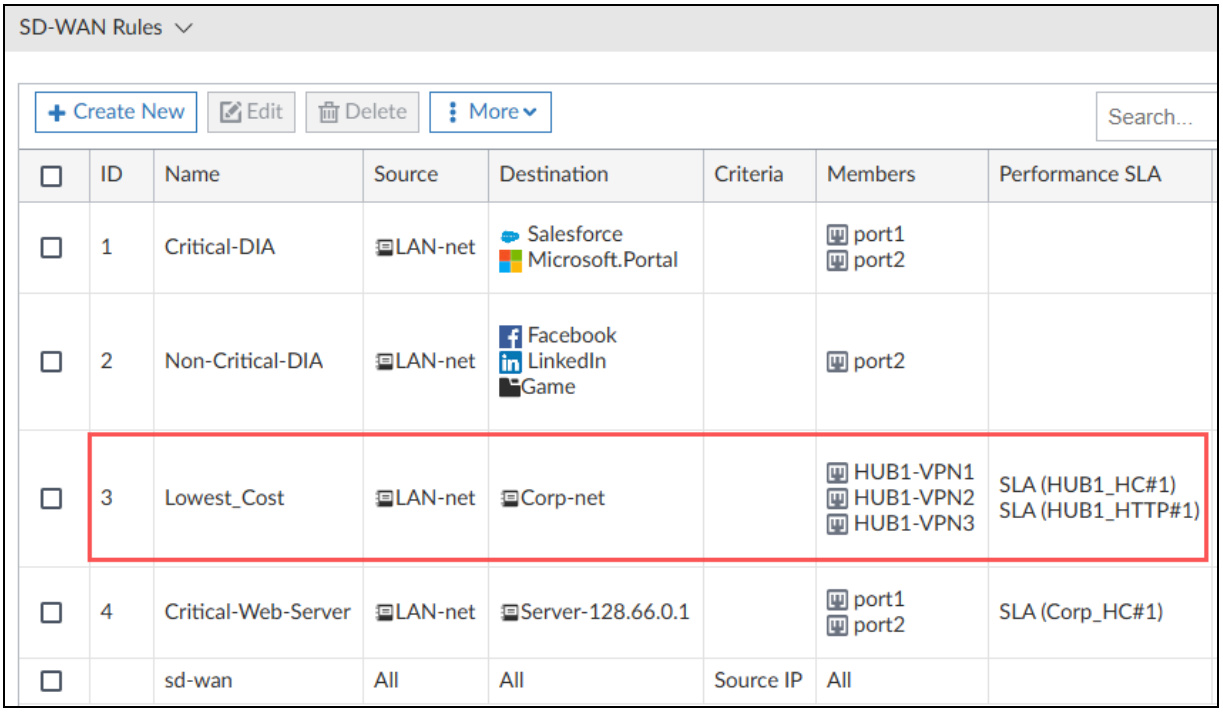
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Make sure that you set the configuration priority (or interface preference list configuration) as follows (most preferred first):

- **HUB1-VPN1**
- **HUB1-VPN2**
- **HUB1-VPN3**

5. Click **OK** to save the settings.
   The **SD-WAN Rules** section in your template should look similar to the following example:



ID	Name	Source	Destination	Criteria	Members	Performance SLA
1	Critical-DIA	LAN-net	Salesforce Microsoft.Portal		port1 port2	
2	Non-Critical-DIA	LAN-net	Facebook LinkedIn Game		port2	
3	Lowest_Cost	LAN-net	Corp-net		HUB1-VPN1 HUB1-VPN2 HUB1-VPN3	SLA (HUB1_HC#1) SLA (HUB1_HTTP#1)
4	Critical-Web-Server	LAN-net	Server-128.66.0.1		port1 port2	SLA (Corp_HC#1)
	sd-wan	All	All	Source IP	All	

6. Click **OK** to save the template settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** only, and then click **Next**.
4. Click **Install** to install the configuration on branch1_fgt.
5. Wait for the installation to finish.
6. Click **Finish**.

To test a lowest cost (SLA) rule

1. Continuing on the branch1_client SSH session, ping `10.1.0.7`, and then leave the command running.
2. In the first SSH session to branch1_fgt, enter the following command to display the rule status:
   ```
   diagnose sys sdwan service4
   ```
   Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x3), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x3), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x3), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

3. In the second SSH session to branch1_fgt, enter the following command to capture ping traffic to `10.1.0.7`:
   `diagnose sniffer packet any "host 10.1.0.7 and icmp" 4 | grep HUB`
4. Leave the command running.
   Your output should look similar to the following example:

```
1.057058 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.058487 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
2.058207 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
2.060009 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

According to the rule status, FortiGate prefers HUB1-VPN1, and therefore picked that member to steer the ping traffic.

5. Use the WAN simulator to increase the latency of HUB1-VPN1 (**BR1-ISP1**) to 160 ms, so it fails to meet both SLA targets.
6. On branch1_fgt, check the rule status and sniffer again.
   Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x3), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x3), gid(0), cfg_order(2), local cost(0), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

```
0.227372 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
0.228614 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.228086 HUB1-VPN2 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.229472 HUB1-VPN2 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

HUB1-VPN1 fails to meet both SLA targets, and therefore is placed at the bottom of the outgoing interface list. HUB1-VPN2 and HUB1-VPN3 have the same SLA status (`0x3`) and cost (`0`), yet FortiGate picks HUB1-VPN2 to steer ping traffic. Why?

In the lowest cost (SLA) strategy, when multiple members have the same SLA status and cost, FortiGate uses the configuration priority as the tiebreaker. HUB1-VPN2 has a higher configuration priority than HUB1-VPN3, and therefore it becomes the preferred member.

Next, you will change the member cost, and then observe its impact in the outgoing interface list.

7. On the FortiManager GUI, edit the **branches** SD-WAN template, and then, in the **SD-WAN Zones** section, configure the following settings:

Member	Field	Value
HUB1-VPN2	Cost	10
HUB1-VPN3	Cost	5

8. Save the template changes, and then install the device settings on branch1_fgt.
9. On branch1_fgt, check the rule status and sniffer again.
   Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x3), gid(0), cfg_order(2), local cost(5), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x3), gid(0), cfg_order(1), local cost(10), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

```
0.245264 HUB1-VPN3 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
0.246722 HUB1-VPN3 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.246694 HUB1-VPN3 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.247815 HUB1-VPN3 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

HUB1-VPN3 now has a lower cost than HUB1-VPN2, and therefore becomes the preferred member.

10. Use the WAN simulator to increase the latency of all three overlays to 160 ms.
11. On branch1_fgt, check the rule status and sniffer again.
    Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(5), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local cost(5), selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(1), local cost(10), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

```
0.113675 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
0.952979 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.114340 HUB1-VPN1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.954414 HUB1-VPN1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
```

All overlays fail to meet all SLA targets. However, HUB1-VPN1 becomes the preferred member because it has the lowest cost.

12. Use the WAN simulator to reduce the latency of all three overlays back to 0 ms.
13. On branch1_client, stop the ping to `10.1.0.7`.
14. On branch1_fgt, stop the sniffer.
15. Keep the SSH sessions to branch1_client and branch1_fgt open because you will need them for the next task.

Configure and Test a Lowest Cost (SLA) and Load Balancing Rule

First, you will configure a rule that maximizes the bandwidth usage by allowing load balancing with a lowest cost (SLA) strategy. You will define two SLA targets for this rule. Next, you will test the rule by generating iPerf traffic and changing the SLA status of the links.

To configure a rule to maximize the bandwidth availability

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
2. Double-click **branches** to edit the template settings.
3. In the **SD-WAN Rules** section, double-click **Lowest_Cost** to edit the rule settings.
4. Configure the following settings:

Field	Value
Name	Maximize_Bandwidth
Destination	Select UDP as protocol

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

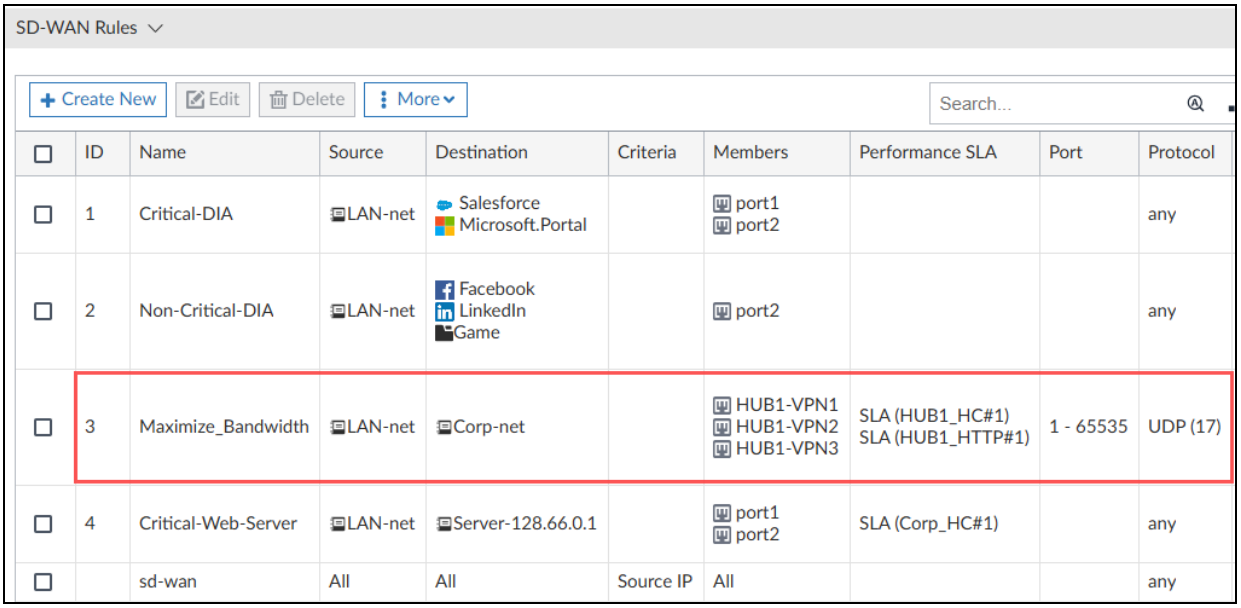
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Outgoing Interfaces	1. In the **Strategy** field, select **Lowest Cost (SLA)**. 2. Keep the current **Interface Preference** settings. 3. Enable **Load Balancing**.
Required SLA Target	Keep the current selected SLA targets, **HUB1_HC#1** and **HUB1_HTTP#1**.

Make sure that you set the configuration priority (or interface preference list configuration) as follows (most preferred first):

- **HUB1-VPN1**
- **HUB1-VPN2**
- **HUB1-VPN3**

5. Click **OK** to save the settings.
   The **SD-WAN Rules** section in your template should look similar to the following example:



ID	Name	Source	Destination	Criteria	Members	Performance SLA	Port	Protocol
1	Critical-DIA	LAN-net	Salesforce Microsoft.Portal		port1 port2			any
2	Non-Critical-DIA	LAN-net	Facebook LinkedIn Game		port2			any
3	Maximize_Bandwidth	LAN-net	Corp-net		HUB1-VPN1 HUB1-VPN2 HUB1-VPN3	SLA (HUB1_HC#1) SLA (HUB1_HTTP#1)	1 - 65535	UDP (17)
4	Critical-Web-Server	LAN-net	Server-128.66.0.1		port1 port2	SLA (Corp_HC#1)		any
	sd-wan	All	All	Source IP	All			any

6. Click **OK** to save the template settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** only, and then click **Next**.
4. Click **Install** to install the configuration on **branch1_fgt**.
5. Wait for the installation to finish.
6. Click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Visit us: Brave-Dumps.com

To test a load balancing and lowest cost (SLA) rule

1. Open an SSH session to dc1_host, and then log in with the following credentials:
   - Username: `root`
   - Password: `password`
2. Enter the following command to start iPerf in server mode:
   `iperf3 -s`
3. In the branch1_client SSH session, enter the following command to generate iPerf traffic to `10.1.0.7`:
   `iperf3 -c 10.1.0.7 -u -b 1M -P 6 -t 3600 -l 1000`

The additional options in the command instruct iPerf to generate six UDP streams at a rate of 1 Mbps each. The UDP packet length will be 1000 bytes and traffic will be generated for an hour (3600 seconds).

Your output should look similar to the following example:

```
root@branch1-client-cli:~# iperf3 -c 10.1.0.7 -u -b 1M -P 6 -t 3600 -l 1000
Connecting to host 10.1.0.7, port 5201
[  4] local 10.0.1.101 port 33730 connected to 10.1.0.7 port 5201
[  6] local 10.0.1.101 port 47945 connected to 10.1.0.7 port 5201
[  8] local 10.0.1.101 port 59270 connected to 10.1.0.7 port 5201
[ 10] local 10.0.1.101 port 46358 connected to 10.1.0.7 port 5201
[ 12] local 10.0.1.101 port 42522 connected to 10.1.0.7 port 5201
[ 14] local 10.0.1.101 port 56903 connected to 10.1.0.7 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[  6]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[  8]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[ 10]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[ 12]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[ 14]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[SUM]   0.00-1.00   sec   668 KBytes  5.47 Mbits/sec  684
```

4. In the first SSH session, enter the following command to display the rule status:
   `diagnose sys sdwan service4 3`
   Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(17): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x3), gid(3), num of pass(2), selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x3), gid(3), num of pass(2), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

When you check SD-WAN services on the CLI, you can see the hash mode for any rule that has load balancing enabled. In the example above, the rule strategy is `SLA` (lowest cost (SLA)), and the load balancing algorithm is `round-robin` (equal distribution).

You can combine the `manual` or `SLA` strategies with a load balancing algorithm.

5. In the second SSH session to branch1_fgt, enter the following command to capture the first 30 packets of iPerf UDP traffic to `10.1.0.7`:
   `diagnose sniffer packet any "host 10.1.0.7 and udp port 5201" 4 30 | grep HUB`
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sniffer packet any "host 10.1.0.7 and udp port 5201" 4 30 | grep HUB
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.1.0.7 and udp port 5201]
0.041437 HUB1-VPN1 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.041678 HUB1-VPN2 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.041786 HUB1-VPN3 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
0.041898 HUB1-VPN1 out 10.0.1.101.44527 -> 10.1.0.7.5201: udp 1000
0.042173 HUB1-VPN2 out 10.0.1.101.41218 -> 10.1.0.7.5201: udp 1000
0.042281 HUB1-VPN3 out 10.0.1.101.35304 -> 10.1.0.7.5201: udp 1000
0.042472 HUB1-VPN1 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.042630 HUB1-VPN2 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.042728 HUB1-VPN3 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
0.042882 HUB1-VPN1 out 10.0.1.101.44527 -> 10.1.0.7.5201: udp 1000
0.043051 HUB1-VPN2 out 10.0.1.101.41218 -> 10.1.0.7.5201: udp 1000
0.043147 HUB1-VPN3 out 10.0.1.101.35304 -> 10.1.0.7.5201: udp 1000
0.043327 HUB1-VPN1 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.043497 HUB1-VPN2 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.043590 HUB1-VPN3 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
```

According to the rule status, all members have the same SLA status. Therefore, FortiGate uses all the members to distribute the traffic.

From the sniffer output, you can tell that each member handles two sessions, for a total of six sessions (round-robin distribution).

6. Use the WAN simulator to increase the latency of HUB1-VPN1 (**BR1-ISP1**) to 110 ms, so that it fails to meet one of the SLA targets.
7. On branch1_fgt, check the rule status and sniffer again.
   Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(17): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x3), gid(3), num of pass(2), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x2), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Visit us: Brave-Dumps.com

```
0.032329 HUB1-VPN2 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.032651 HUB1-VPN3 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.032868 HUB1-VPN2 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
0.033219 HUB1-VPN3 out 10.0.1.101.44527 -> 10.1.0.7.5201: udp 1000
0.033437 HUB1-VPN2 out 10.0.1.101.41218 -> 10.1.0.7.5201: udp 1000
0.033594 HUB1-VPN3 out 10.0.1.101.35304 -> 10.1.0.7.5201: udp 1000
```

FortiGate placed `HUB1-VPN1` at the bottom of the list because it meets the fewest number of SLA targets. Therefore, FortiGate distributes the iPerf traffic between the other two members, as shown in the sniffer output.

8. Use the WAN simulator to increase the latency of all three overlays to 160 ms.
9. On branch1_fgt, check the rule status and sniffer again.

   Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(10), TOS(0x0/0x0), Protocol(17): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(3):
    1: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

```
0.082843 HUB1-VPN3 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.082925 HUB1-VPN2 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.082983 HUB1-VPN1 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
0.083119 HUB1-VPN3 out 10.0.1.101.44527 -> 10.1.0.7.5201: udp 1000
0.083179 HUB1-VPN2 out 10.0.1.101.41218 -> 10.1.0.7.5201: udp 1000
0.083541 HUB1-VPN1 out 10.0.1.101.35304 -> 10.1.0.7.5201: udp 1000
0.083596 HUB1-VPN3 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.083839 HUB1-VPN2 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.084249 HUB1-VPN1 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
0.084306 HUB1-VPN3 out 10.0.1.101.44527 -> 10.1.0.7.5201: udp 1000
0.084359 HUB1-VPN2 out 10.0.1.101.41218 -> 10.1.0.7.5201: udp 1000
0.084411 HUB1-VPN1 out 10.0.1.101.35304 -> 10.1.0.7.5201: udp 1000
0.084463 HUB1-VPN3 out 10.0.1.101.34363 -> 10.1.0.7.5201: udp 1000
0.084875 HUB1-VPN2 out 10.0.1.101.41902 -> 10.1.0.7.5201: udp 1000
0.084936 HUB1-VPN1 out 10.0.1.101.43468 -> 10.1.0.7.5201: udp 1000
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

All overlays have the same SLA status (none meet any SLA targets). Because the members have the same SLA status, FortiGate uses all of them to distribute traffic.

10. On the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
11. Double-click **branches** to edit the template settings.
12. In the **SD-WAN Rules** section, double-click **Maximize_Bandwidth** to edit the rule settings.
13. In the **Advanced Options** section, set **minimum-sla-meet-members** to `1`.

14. Click **OK** to save the settings.
15. Click **OK** to save the template settings.
16. Install the device settings on branch1_fgt.
17. On branch1_fgt, check the rule status again.
    Your output should look similar to the following example:

```
Service(3): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(17): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Service disabled caused by no outgoing path no minimum SLA meet.
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.1.0.0-10.1.0.255
```

The rule was disabled because none of the members met at least one SLA target. When you set the **minimum-sla-meet-members** setting to `1`, FortiGate requires the rule to have at least one member that meets one or more SLA targets. Otherwise, the rule is disabled.

Because the rule is disabled, the traffic matches the implicit rule, which means that FortiGate performs standard forwarding information base (FIB) routing.

18. Use the WAN simulator to reduce the latency of all three overlays back to 0 ms.
19. Close all the SSH sessions (branch1_fgt, branch1_client, and dc1_host).

To return to manual mode

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **SD-WAN**.
2. Double-click **branches** to edit the template settings.
3. In the **SD-WAN Rules** section, double-click the **Maximize_Bandwidth** rule to edit the rule settings.
4. Configure the following settings:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Name	Corp
Strategy	Manual

5. Click **OK** to save the settings.
6. In the **Performance SLA** section, delete **HUB1_HTTP**.
7. Click **OK** to save the template update.

To install the device settings

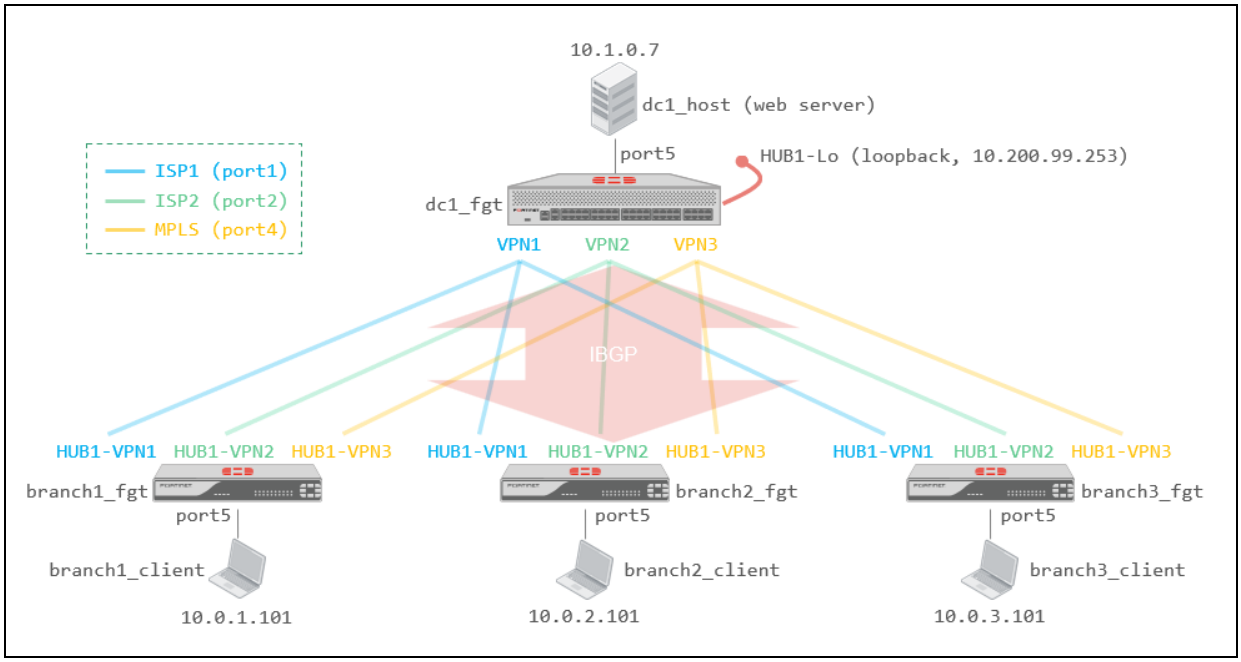
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** only, and then click **Next**.
4. Click **Install** to install the configuration on **branch1_fgt**.
5. Wait for the installation to finish.
6. Click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 7: SD-WAN Overlay Design and Best Practices

In this lab, you will review in detail the IPsec overlay and BGP configuration that the SD-WAN overlay template applied. Then, you will learn how to adjust the IPsec and BGP configurations to address specific requirements. The following diagram summarizes the hub-and-spoke topology in use:



Objectives

- Review the IPsec overlay and BGP settings that the SD-WAN overlay template applied
- Configure advanced IPsec overlay and BGP settings

Time to Complete

Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Reviewing the Overlay and BGP Configurations

In this exercise, you will review in detail the IPsec and BGP configurations that you applied using the SD-WAN overlay template. First, you will review the overlay tunnel configuration. Next, you will review the BGP setup for your hub-and-spoke topology that the SD-WAN overlay template applied. Finally, you will fine-tune your IPsec and BGP settings to speed up SD-WAN convergence, failover, and recovery.

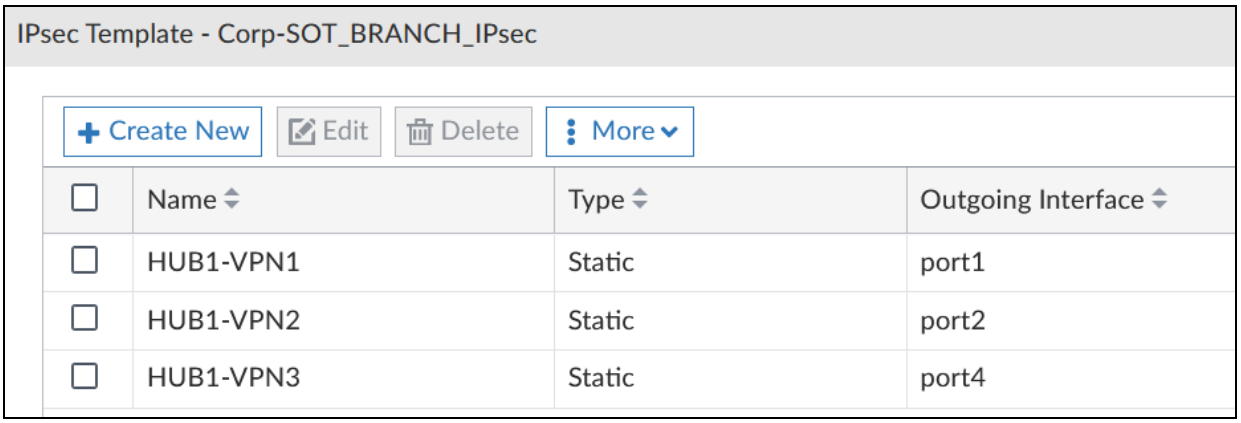
Review the Overlay Configuration

You will review the IPsec tunnel configuration that the SD-WAN overlay template applied. First, you will review the configuration applied to the branch devices. Next, you will review the configuration applied to the hub device. For each type of device, you will review the GUI template on FortiManager, and then the CLI output on FortiGate.

To review the VPN tunnel configuration on the branch devices

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Provisioning Templates** > **IPsec Tunnel**.
3. Double-click **Corp-SOT_BRANCH_IPsec** to view the IPsec tunnel settings for the branch devices.
   You can see three tunnels configured: **HUB1-VPN1**, **HUB1-VPN2**, and **HUB1-VPN3**.

   Your page should look similar to the following example:



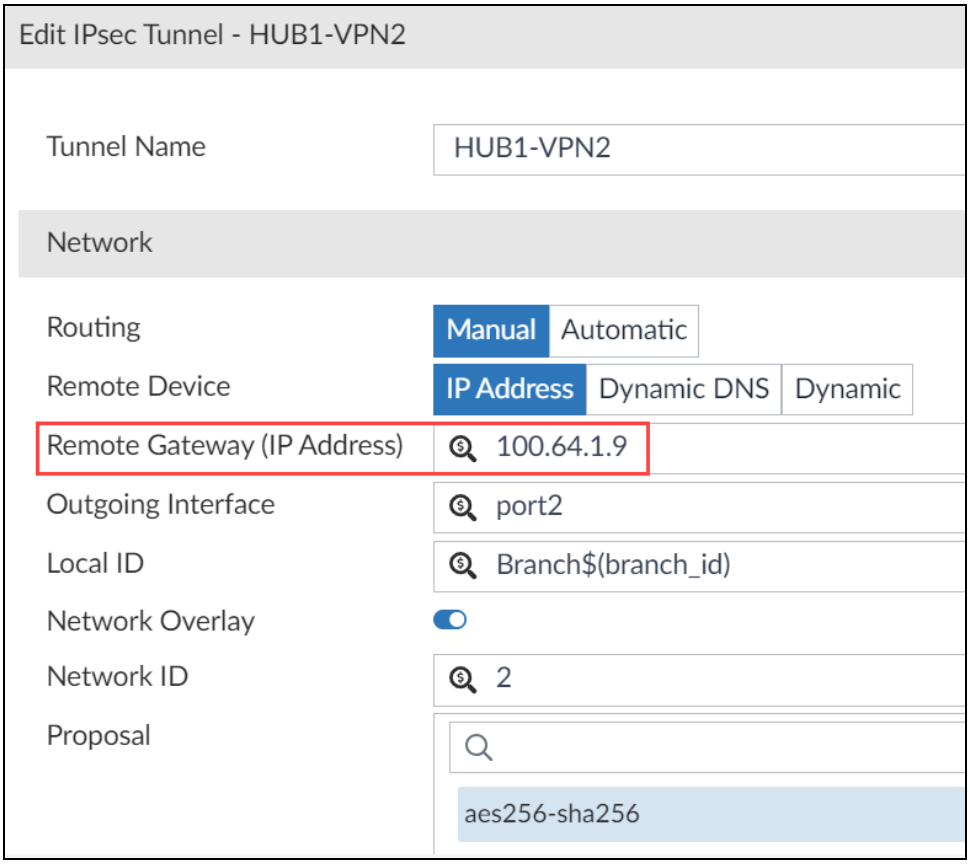
The three tunnel definitions are grouped in the same template. This is mandatory because you can apply only one IPsec tunnel template to each FortiGate. However, each template can contain multiple tunnel definitions.

4. Double-click each line to review the settings.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The three tunnels have similar configurations, but different remote gateways and outgoing interfaces.



The tunnels are defined according to Fortinet best practice recommendations for hub-and-spoke topology. This includes:

- **aes256-sha256** as a single proposal for the hash and encryption algorithm. This allows a good balance between security and performance.
- Pre-shared key authentication

Visible in the **Advanced Options** section:

- IPsec in tunnel mode
- IKE version 2
- DH groups 5 and 14
- **mode-cfg** enabled

5. Click **Cancel**.
6. Click **Cancel** to go back to the **IPsec Tunnel** menu.
7. Open an SSH session on one FortiGate branch device, and then log in to the FortiGate CLI with the following credentials:
   - Username: `admin`
   - Password: `password`
8. Enter the following commands to display the IPsec tunnel configuration:
   ```
   show vpn ipsec phase1-interface
   ```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
show vpn ipsec phase2-interface
```

Your output should look similar to the following examples:

```
branch1_fgt # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set localid "Branch1"
        set comments "VPN: HUB1-VPN1 [Created by IPSEC Template]"
        set network-overlay enable
        set network-id 1
        set remote-gw 100.64.1.1
        set psksecret ENC hn5xwcIhzivXtzLBf3iJNp/WJx7+uFMxF5V+IFnPF
ruQ6Z84PxmU72dnaxKI4bx8qG1k0/A0RqGT9rBZRX2gYYEOD9VevFYAslek1E7PBmFr
    next
    edit "HUB1-VPN2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set localid "Branch1"
        set comments "VPN: HUB1-VPN2 [Created by IPSEC Template]"
        set network-overlay enable
        set network-id 2
        set remote-gw 100.64.1.9
        set psksecret ENC pr6RmLd34w2rZmmcvDDpT4SXRBlZrX7b1IA1+mVDl
KwJfnSRrBQyKyM+Z8mvzDsG58Tvu4x5FFNEGMbSvOaPV3qW24+ekmhtATsdoz5Za1kc
    next
    edit "HUB1-VPN3"
        set interface "port4"
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # branch1_fgt # show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "HUB1-VPN1"
        set phase1name "HUB1-VPN1"
        set proposal aes256-sha256
        set auto-negotiate enable
        set comments "VPN: HUB1-VPN1 [Created by IPSEC Template]"
    next
    edit "HUB1-VPN2"
        set phase1name "HUB1-VPN2"
        set proposal aes256-sha256
        set auto-negotiate enable
        set comments "VPN: HUB1-VPN2 [Created by IPSEC Template]"
    next
    edit "HUB1-VPN3"
        set phase1name "HUB1-VPN3"
        set proposal aes256-sha256
        set auto-negotiate enable
        set comments "VPN: HUB1-VPN3 [Created by IPSEC Template]"
    next
end
```

The CLI output shows the settings that are configured according to the SD-WAN overlay template and the options that you selected when you used it. This includes:

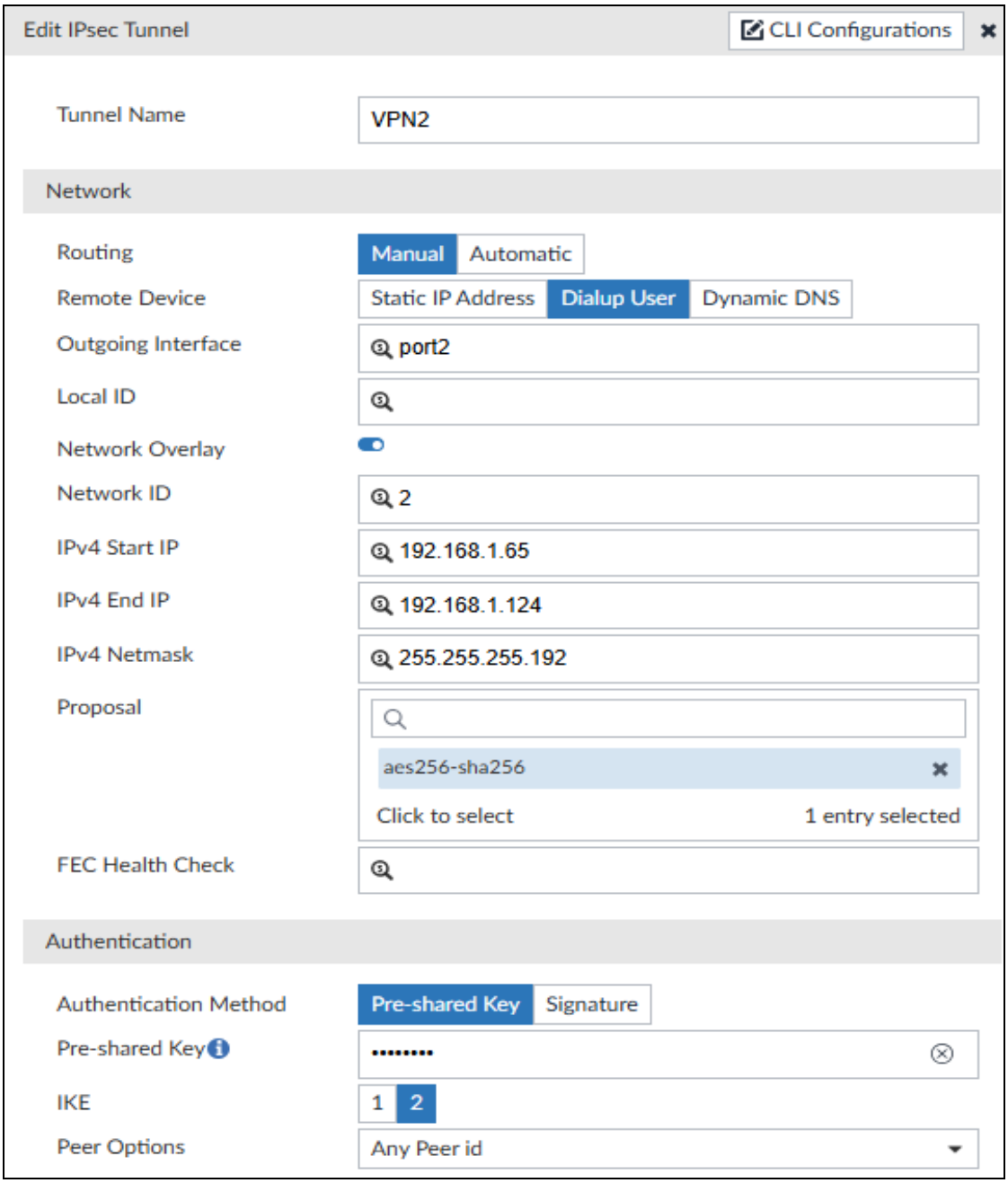
- The settings that you already reviewed in the GUI configuration.
- A `localid` set to the device name
- `net-device` set to `enable`. This creates a kernel device for every tunnel. This setting is required to support ADVPN shortcuts.
- `add-route` set to `disable` for compatibility with the choice of dynamic routing
- `network-overlay` set to `enable` to allow the configuration of network IDs
- One `network-id` per VPN gateway. Associate tunnels with overlay networks.

To review the VPN tunnel configuration on the hub

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **IPsec Tunnel**.
2. Double-click **Corp-SOT_HUB1_IPsec** to view the template settings.
   You can see three tunnels of the **Dynamic** type configured: **VPN1**, **VPN2**, and **VPN3**.
3. Double-click one of them to review the configuration.
   The following example shows the page for **VPN2**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



On the hub, the tunnels are also defined according to Fortinet best practice recommendations for hub-and-spoke topology. This includes:

- Dial-up server—dynamic (**Dialup User**) remote device type
- **aes256-sha256** as a single proposal for the hash and encryption algorithm
- Pre-shared key authentication
- Network overlay enabled and the definition of network IDs
- Definition of the range for IP addresses allocated to the dial-up tunnels

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

4. Click **Cancel** to go back to the **IPsec Tunnel** menu.
5. Open an SSH session on dc1_fgt, and then log in to the FortiGate CLI with the following credentials:
   - Username: `admin`
   - Password: `password`
6. Enter the following commands to display the IPsec tunnel configuration:

```
show vpn ipsec phase1-interface
show vpn ipsec phase2-interface
```

   You output should look similar to the following examples:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
dc1_fgt # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "VPN1"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set comments "VPN: VPN1 [Created by IPSEC Template]"
        set network-overlay enable
        set network-id 1
        set ipv4-start-ip 192.168.1.1
        set ipv4-end-ip 192.168.1.60
        set ipv4-netmask 255.255.255.192
        set psksecret ENC gAjpFX97z5BaNrasFjJfCI7kefFkUwGyRrC
sWuixZooJbwHrgC5wF1wiNscGQgHMmluy1lmMjY3dkVA
        set dpd-retryinterval 60
    next
    edit "VPN2"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set comments "VPN: VPN2 [Created by IPSEC Template]"
        set network-overlay enable
        set network-id 2
        set ipv4-start-ip 192.168.1.65
        set ipv4-end-ip 192.168.1.124
        set ipv4-netmask 255.255.255.192
        set psksecret ENC 87lfUGU8OkoCFsjNnQOOo0rQ4xd/7oKKz3x
QpPEEkLtZv7bBMVrwgoGv7oBX8YRj5JTQllmMjY3dkVA
        set dpd-retryinterval 60
    next
    edit "VPN3"
        set type dynamic
        set interface "port4"
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
dc1_fgt # show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "VPN1"
        set phase1name "VPN1"
        set proposal aes256-sha256
        set comments "VPN: VPN1 [Created by IPSEC Template]"
    next
    edit "VPN2"
        set phase1name "VPN2"
        set proposal aes256-sha256
        set comments "VPN: VPN2 [Created by IPSEC Template]"
    next
    edit "VPN3"
        set phase1name "VPN3"
        set proposal aes256-sha256
        set comments "VPN: VPN3 [Created by IPSEC Template]"
    next
end
```

On the hub, the `net-device` setting is set to `disable`. This setting is compatible with the `net-device` setting that is set to `enable` at the branch level for ADVPN deployment. It helps to improve performance on hub devices that usually handle a high number of IPsec tunnels.

To verify the active overlays on the FortiGate CLI

1. Continuing in the SSH sessions for the branch device and hub dc1_fgt, enter the following command to verify the tunnel IDs:

   `diagnose vpn tunnel list`

   The following images show examples of the first part of the output:

```
branch2_fgt # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=HUB1-VPN1 ver=2 serial=1 203.0.113.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/568 options[0238]=npu create_dev frag-rf
```

```
branch3_fgt # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=HUB1-VPN1 ver=2 serial=1 100.64.33.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1
status=up dst_mtu=1500 weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/568 options[0238]=npu create_dev frag-rf
c  role=primary accept_traffic=1 overlay_id=1
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

The tunnel ID for HUB1-VPN1 is identical on all three branches. Why?

The tunnel ID is a parameter that is local to the device. Keeping the same IDs on every branch simplifies the configuration and management.

FortiGate uses the interface IP address of the remote end of the tunnel as the tunnel ID.

2. Enter the following command to verify the tunnel list:

```
get vpn ipsec tunnel summary
```

The following image shows the output on dc1_fgt:

```
dc1_fgt # get vpn ipsec tunnel summary
'VPN1_0' 100.64.33.1:0  selectors(total,up): 1/1  rx(pkt,err): 18392/0  tx(pkt,err): 18391/0
'VPN1_1' 192.2.0.1:0  selectors(total,up): 1/1  rx(pkt,err): 54640/0  tx(pkt,err): 36782/0
'VPN1_2' 203.0.113.1:0  selectors(total,up): 1/1  rx(pkt,err): 18595/0  tx(pkt,err): 18385/0
'VPN2_0' 192.2.0.9:0  selectors(total,up): 1/1  rx(pkt,err): 54625/0  tx(pkt,err): 36773/0
'VPN2_1' 100.64.33.9:0  selectors(total,up): 1/1  rx(pkt,err): 18390/0  tx(pkt,err): 18389/0
'VPN2_2' 203.0.113.9:0  selectors(total,up): 1/1  rx(pkt,err): 18594/0  tx(pkt,err): 18384/0
'VPN3_0' 172.16.0.1:0  selectors(total,up): 1/1  rx(pkt,err): 54635/0  tx(pkt,err): 36779/0
'VPN3_1' 172.16.0.9:0  selectors(total,up): 1/1  rx(pkt,err): 18585/0  tx(pkt,err): 18375/0
```

This command lists the tunnels that are established.

To verify the SD-WAN members and zones on the FortiGate CLI

1. Continuing in the SSH sessions, enter the following commands to verify the SD-WAN members and zones:

```
diagnose sys sdwan zone
diagnose sys sdwan member
```

The following image shows an example of the output for branch3_fgt:

```
branch3_fgt # diagnose sys sdwan zone
Zone HUB1 index=4
        members(3): 20(HUB1-VPN1) 21(HUB1-VPN2) 22(HUB1-VPN3)
Zone WAN3 index=3
        members(1): 6(port4)
Zone underlay index=2
        members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
        members(0):

branch3_fgt # diagnose sys sdwan member
Member(1): transport-group: 0, interface: port1, flags=0x0 , gateway: 100.64.33.2, priority: 1 1024, wei
ght: 0
Member(2): transport-group: 0, interface: port2, flags=0x0 , gateway: 100.64.33.10, source 100.64.33.9,
priority: 1 1024, weight: 0
Member(3): transport-group: 0, interface: port4, flags=0x0 ,priority: 1 1024, weight: 0
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xc , gateway: 100.64.1.1, source 192.168.1.2
, priority: 1 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xc , gateway: 100.64.1.9, source 192.168.1.6
7, priority: 1 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xc , gateway: 172.16.1.5, priority: 1 1024,
weight: 0
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

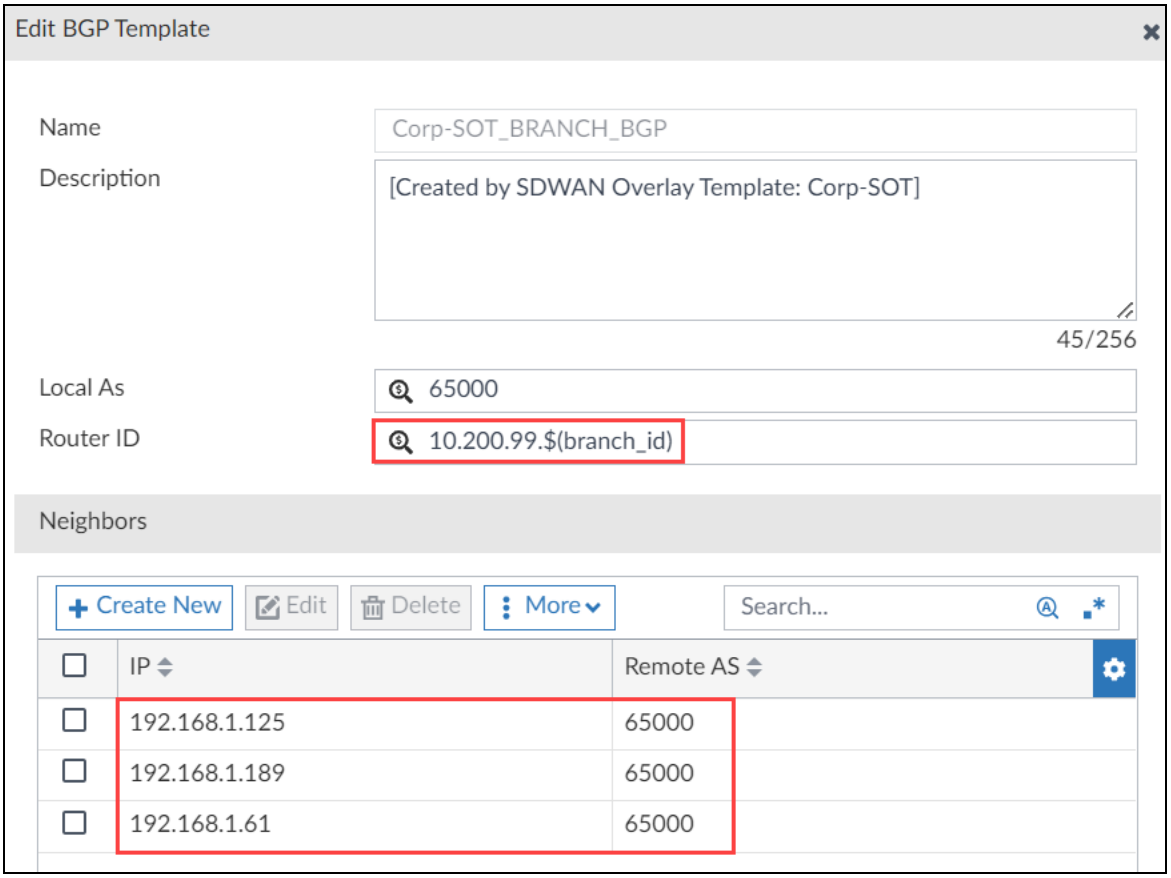
> **Stop and think!**
>
> You didn't configure a gateway for the overlays. However, FortiGate displays a gateway address for each of them. Why?
>
> You must not configure a gateway address for members that are IPsec tunnels. FortiGate automatically determines the gateway address. That is, FortiGate uses the IPsec tunnel ID as the gateway address.

Review the BGP Configuration

You will review the BGP configuration that the SD-WAN overlay template applied. The BGP configuration of the branch devices and the hub follow Fortinet best practices and recommendations for hub-and-spoke topologies in an SD-WAN context.

To review and adjust the BGP configuration on the branch devices

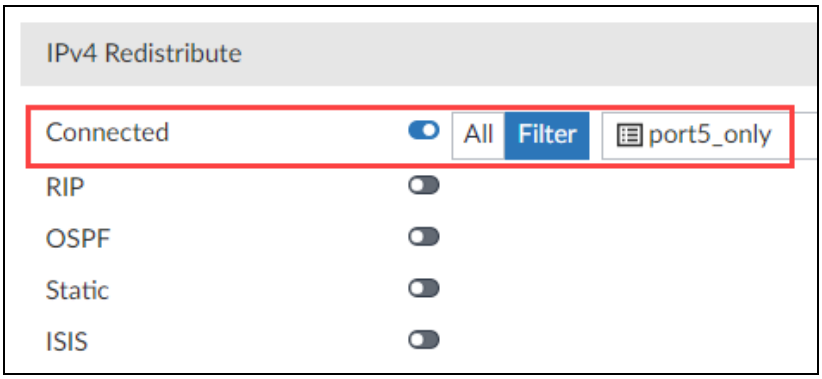
1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **BGP**.
2. Double-click the **Corp-SOT_BRANCH_BGP** template to review it.
   Your page should look similar to the following example:



3. Scroll down to the **IPv4 Redistribute** section.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



According to the predefined settings in the SD-WAN overlay template, and the options that you selected when you configured it, the BGP configuration on the branch devices includes the following settings:

- The router ID is defined with a fixed part—10.200.99—and the branch ID.
- A BGP neighbor is defined for each overlay.
- Each branch device advertises the subnets that are connected to the port5 interface. This corresponds to the branch local subnet.

4. Click **Cancel**.
5. Continuing in the SSH session for the branch device, enter the following command:

```
show router bgp
```

Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # show router bgp
config router bgp
    set as 65000
    set router-id 10.200.99.1
    set ibgp-multipath enable
    set graceful-restart enable
    config neighbor
        edit "192.168.1.125"
            set advertisement-interval 1
            set capability-graceful-restart enable
            set link-down-failover enable
            set soft-reconfiguration enable
            set description "HUB1-VPN2"
            set interface "HUB1-VPN2"
            set remote-as 65000
            set connect-timer 10
        next
        edit "192.168.1.189"
            set advertisement-interval 1
            set capability-graceful-restart enable
            set link-down-failover enable
            set soft-reconfiguration enable
            set description "HUB1-VPN3"
            set interface "HUB1-VPN3"
            set remote-as 65000
            set connect-timer 10
            set update-source "HUB1-VPN3"
        next
        edit "192.168.1.61"
            set advertisement-interval 1
```

Note the following settings:

- `link-down-failover` is enabled. This setting instructs FortiGate to clear a BGP peering after the interface in use goes down.
- `soft-reconfiguration` is enabled. This setting instructs FortiGate to save the received routes in a separate table, which is useful for troubleshooting, and is required to soft reset BGP peerings after a change.

To review the BGP configuration on the hub

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **BGP**.
2. Double-click the **Corp-SOT_HUB1_BGP** template to review it.

   The template defines the following:

   - No neighbors
   - Three neighbor groups: VPN1, VPN2, and VPN3
   - Three neighbor range definitions—one for each neighbor group
3. Click **Cancel**.
4. Continuing in the SSH session for dc1_fgt, enter the following command:

   `show router bgp`

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Your output should look similar to the following example:

```
dc1_fgt # show router bgp
config router bgp
    set as 65000
    set router-id 10.200.99.253
    set ibgp-multipath enable
    set graceful-restart enable
    config neighbor-group
        edit "VPN1"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
        edit "VPN2"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
        edit "VPN3"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
        next
    end
    config neighbor-range
        edit 1
            set prefix 192.168.1.0 255.255.255.192
            set neighbor-group "VPN1"
        next
```

The BGP configuration on the hub contains the following settings:

- Three neighbor groups, one for each overlay. Neighbor groups are useful to limit the route propagation within a single neighbor group when using route reflection.
- The `soft-reconfiguration` and `link-down-failover` settings are enabled for each group. Both settings have the same effect as in the spoke.
- One neighbor address range is defined for each group.

To verify the overlay address and BGP peering

1. Open an SSH session to branch1_fgt, and another to branch2_fgt or branch3_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. In both SSH sessions, enter the following command to display the overlay addresses:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
diagnose ip address list | grep HUB
```

On branch1_fgt, your output should look similar to the following example:

```
branch1_fgt # diagnose ip address list | grep HUB
IP=192.168.1.2->192.168.1.2/255.255.255.192 index=20 devname=HUB1-VPN1
IP=192.168.1.66->192.168.1.66/255.255.255.192 index=21 devname=HUB1-VPN2
IP=192.168.1.130->192.168.1.130/255.255.255.192 index=22 devname=HUB1-VPN3
```

The overlay addresses may be different in your output.

3. In both SSH sessions, enter the following commands to display the status of BGP peerings and the BGP routes in the routing table:

```
get router info bgp summary
get router info routing-table bgp
```

On branch2_fgt, your output should look similar to the following example:

```
branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.2, local AS number 65000
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.61    4      65000     143     144        1    0    0 02:02:53        1
192.168.1.125   4      65000     145     144        1    0    0 02:02:53        1
192.168.1.189   4      65000     144     145        1    0    0 02:02:54        1

Total number of neighbors 3


branch2_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 02:02:34, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 02:02:34, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 02:02:34, [1/0]
```

Remember that branch3_fgt has only two active underlay links. Therefore, for this device, you see only two active BGP neighbors and two BGP routes to the hub device.

4. In the SSH session to dc1_fgt, enter the same two commands.
   Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
dc1_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.253, local AS number 65000
BGP table version is 7
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 33 seconds

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.1     4      65000  347139  347136        6    0    0 00:48:06        1
192.168.1.2     4      65000  346975  347028        6    0    0 00:48:09        1
192.168.1.3     4      65000  346927  347090        6    0    0 00:24:48        1
192.168.1.65    4      65000  346974  346959        6    0    0 00:48:07        1
192.168.1.66    4      65000  346997  346934        6    0    0 00:48:09        1
192.168.1.67    4      65000  347010  346913        6    0    0 00:24:57        1
192.168.1.129   4      65000  347138  346957        6    0    0 00:48:08        1
192.168.1.130   4      65000  346995  347057        6    0    0 00:48:07        1

Total number of neighbors 8


dc1_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.1.0/24 [200/0] via 192.168.1.1 (recursive is directly connected, VPN1), 00:48:37, [1/0]
                    [200/0] via 192.168.1.65 (recursive is directly connected, VPN2), 00:48:37, [1/0]
                    [200/0] via 192.168.1.130 (recursive is directly connected, VPN3), 00:48:37, [1/0]
B       10.0.2.0/24 [200/0] via 192.168.1.2 (recursive is directly connected, VPN1), 00:48:39, [1/0]
                    [200/0] via 192.168.1.66 (recursive is directly connected, VPN2), 00:48:39, [1/0]
                    [200/0] via 192.168.1.129 (recursive is directly connected, VPN3), 00:48:39, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.3 (recursive is directly connected, VPN1), 00:08:15, [1/0]
                    [200/0] via 192.168.1.67 (recursive is directly connected, VPN2), 00:08:15, [1/0]
```

Stop and think!

The branches learn routes to the corporate LAN 10.1.0.0/24 through each overlay. However, branch2_fgt has no route to branch1_fgt or branch3_fgt. More generally, branch devices don't have routes to each other. Why?

A BGP router learns routes from each device that it establishes a BGP peering with. In this topology, the dc1_fgt hub establishes peering with each branch device, through each overlay. However, there is no direct connection between the branch devices, and consequently no peering between them. The hub learns the routes that each branch device advertises. The branch devices learn only the route to the hub.

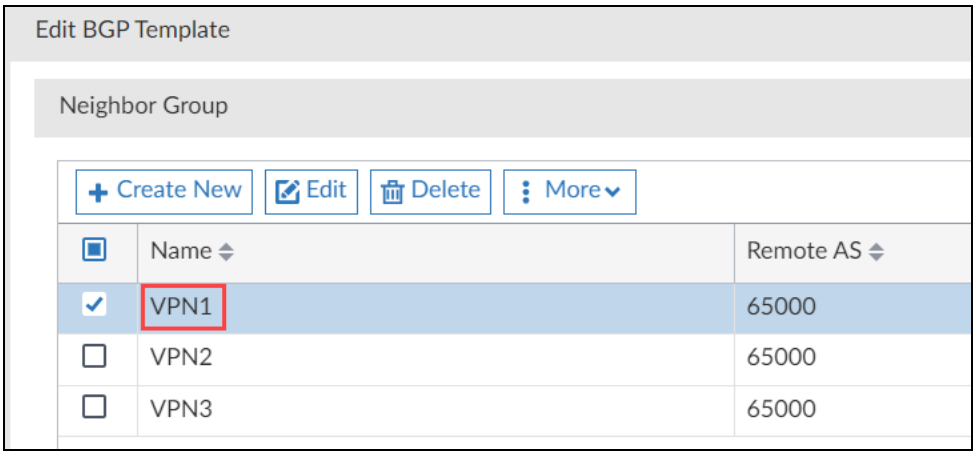
To avoid the need for full mesh, but still allow communication between branch devices, in the next procedure, you will configure route reflection. You will enable the hub as a route reflector server. Then, all other IBGP routers in the topology—the branches—will become route reflector clients. This allows the hub to advertise the routes that it learns from one branch device to the other branch devices.

To allow route reflection on the hub

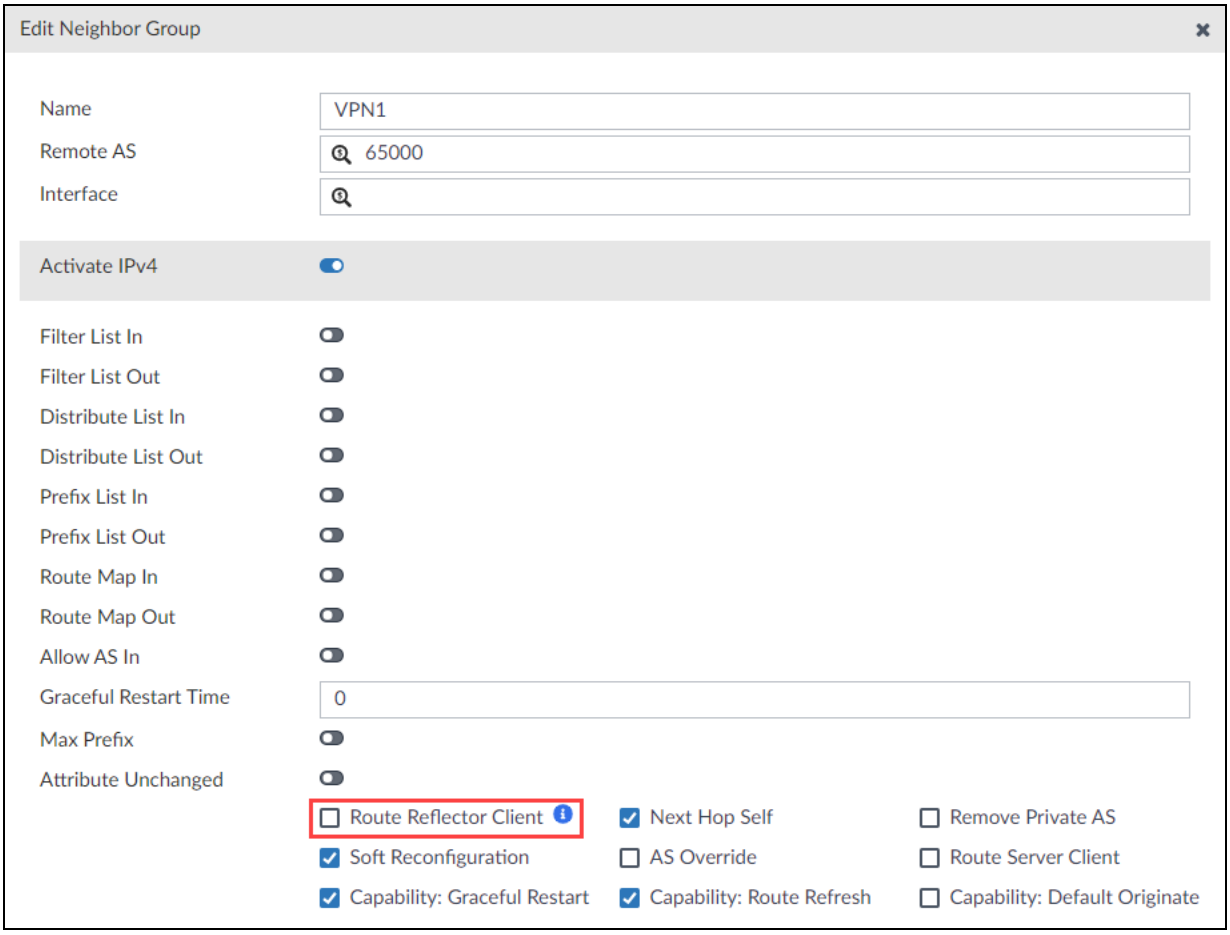
1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **BGP**.
2. Double-click the **Corp-SOT_HUB1_BGP** template to edit it.
3. In the **Neighbor Group** section, double-click **VPN1** to edit it.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



4. In the **Activate IPv4** section, select the **Route Reflector Client** checkbox to activate it.



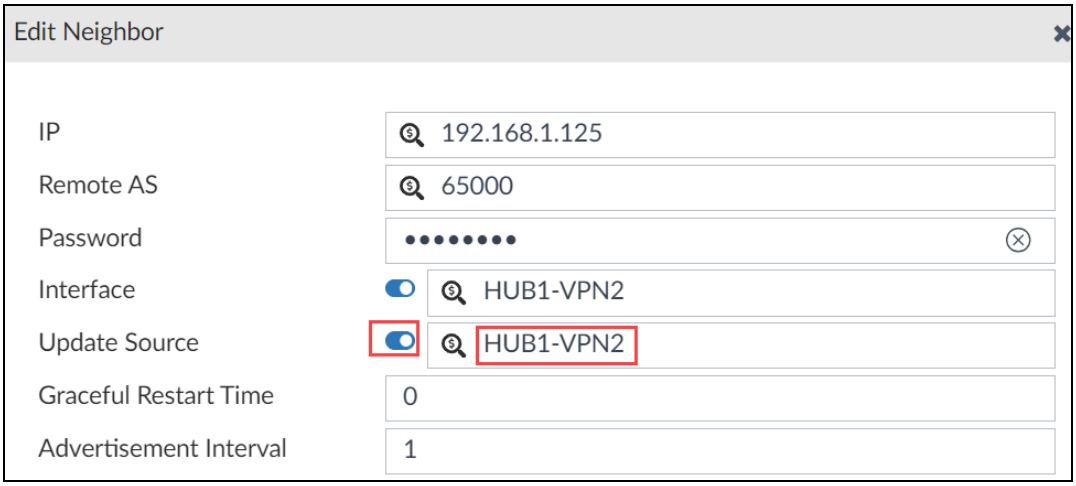
5. Click **OK** to save the neighbor group update.
6. Repeat the previous steps to activate the **Route Reflector Client** for **VPN2** and **VPN3**.
7. Click **OK** to save the template update.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To refine the BGP configuration on the branch devices

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **BGP**.
2. Double-click the **Corp-SOT_BRANCH_BGP** template to edit it.
3. In the **Neighbors** section, double-click the first entry to edit it.
4. Enable **Update Source**, and then in the field, type the tunnel interface name, as shown in the following example. Make sure that you use the tunnel name that is configured for the interface as the update source .



5. Repeat steps 3–4 to enable **Update Source** and set the interface name for each neighbor.
6. Click **OK** to save the template update.

The **interface** setting that is defined for a BGP neighbor enables listing on port 179 for that interface. The interface acts as a *passive* BGP peer. It does not initiate or start the BGP peering itself, but waits for incoming BGP connections. If the BGP peering goes down for any reason, the neighbourship will stay inactive or idle until the remote BGP peer initiates the session.

The **Update Source** setting allows FortiGate to initiate the BGP peering through the interface. The interface becomes an *active* BGP peer.

To install the configuration changes on the devices

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, **branch2_fgt**, **branch3_fgt**, and **dc1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on the hub and branch devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To review the routing updates

1. In the SSH sessions for the branch devices, enter the following commands to display the status of BGP peerings and BGP routes in the routing table:

```
get router info bgp summary
get router info routing-table bgp
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

For example, on branch2_fgt, your output should look similar to the following example:

```
branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.2, local AS number 65000
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.61    4      65000  347041  346990        5    0    0 00:01:36        3
192.168.1.125   4      65000  346949  347010        5    0    0 00:01:36        3
192.168.1.189   4      65000  346973  347152        5    0    0 00:01:36        3

Total number of neighbors 3


branch2_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.1.0/24 [200/0] via 192.168.1.1 [3] (recursive is directly connected, HUB1-VPN1), 00:01:14, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.3 [3] (recursive is directly connected, HUB1-VPN1), 00:01:14, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:01:14, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:01:14, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:01:14, [1/0]
```

Each branch learns the route to the other branch LAN subnets through hub dc1_fgt.

Stop and think!

A BGP peering is established for each overlay. The branch device learns other BGP prefixes from dc1_fgt. The `10.1.0.0/24` prefix is sourced from dc1_fgt, and the `10.0.branch-id.0/24` prefix is sourced from the other branch device and reflected by dc1_fgt. The hub prefix is learned over each overlay, but the branch device prefixes are not. Why?

The paths over the other overlays are not shown because you didn't configure additional paths on the branch devices and dc1_fgt. In the next task, you will configure additional paths so the branch devices learn the nine different paths that are available for the `10.0.branch-id.0/24` prefix (three prefixes per overlay).

To test the failover scenario

1. Access the WAN simulator HTTP interface.
2. Locate **DC1-ISP1**, and then click **DOWN** to bring down the link on port1 on dc1_fgt.
3. In any of the branch SSH sessions, enter the following commands to monitor the overlays and BGP status:
   ```
   diagnose sys sdwan health-check status HUB1_HC
   get ipsec tunnel list
   get router info bgp summary
   ```
4. Focus on the output that is relevant to the HUB1-VPN1 overlay.

   Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch2_fgt # diag sys sdwan health-check status HUB1_HC
Health Check(HUB1_HC):
Seq(4 HUB1-VPN1): state(dead), packet-loss(16.000%) sla_map=0x0
Seq(5 HUB1-VPN2): state(alive), packet-loss(0.000%) latency(1.171), jitter(0.222), mos(4.404),
 bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(6 HUB1-VPN3): state(alive), packet-loss(0.000%) latency(0.841), jitter(0.180), mos(4.404),
 bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x1

branch2_fgt # get ipsec tunnel list
NAME=HUB1-VPN1 REMOTE-GW=100.64.1.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=42802

NAME=HUB1-VPN2 REMOTE-GW=100.64.1.9:0
        P2NAME=HUB1-VPN2 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=37588

NAME=HUB1-VPN3 REMOTE-GW=172.16.1.5:0
        P2NAME=HUB1-VPN3 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=27369


branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.2, local AS number 65000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.61    4      65000     304     305        3    0    0 00:01:36        2
192.168.1.125   4      65000     311     305        2    0    0 01:28:27        2
192.168.1.189   4      65000     308     304        2    0    0 01:28:29        2

Total number of neighbors 3
```

The performance SLA marked HUB1-VPN1 down shortly after bringing down port1 on dc1_fgt. However, the IPsec tunnel and BGP peering remain up.

5. Repeat the previous commands every few seconds to track the status of the overlay and BGP.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

Eventually (after about 2 minutes), the tunnel and BGP peering go down. For example:

```
branch2_fgt # branch2_fgt # get ipsec tunnel list
NAME=HUB1-VPN1 REMOTE-GW=100.64.1.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0
.0/0.0.0.0 STATUS=down

NAME=HUB1-VPN2 REMOTE-GW=100.64.1.9:0
        P2NAME=HUB1-VPN2 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0
.0/0.0.0.0 STATUS=up TIMEOUT=37224

NAME=HUB1-VPN3 REMOTE-GW=172.16.1.5:0
        P2NAME=HUB1-VPN3 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0
.0/0.0.0.0 STATUS=up TIMEOUT=27005


branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.2, local AS number 65000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.61    4      65000     304     307        0    0    0    never Active
192.168.1.125   4      65000     319     311        2    0    0 01:34:32        2
192.168.1.189   4      65000     317     311        2    0    0 01:34:34        2

Total number of neighbors 3
```

Why?

Although it is not shown in the output, the tunnel and BGP peering go down because of dead peer detection (DPD) and the hold timer expiration, respectively. Both DPD and BGP timers are set to the default values. In the next task, you will adjust the timers to speed up SD-WAN convergence, failover, and recovery.

6. On the WAN simulator page, locate **DC1-ISP1**, and then click **UP** to bring up the link on port1 on dc1_fgt.

Fine-Tune IPsec and BGP

You will adjust some IPsec and BGP settings to speed up SD-WAN convergence, failover, and recovery. You will also configure additional paths on dc1_fgt and the branches to exchange all available routes between them.

This is a practice exercise to show you how adjusting settings and timers can impact the convergence and failover time. Short timers are not suitable for all networks, especially if they are subject to unstable links with occasional short link down. You should carefully review the advantages and disadvantages before you perform such adjustments on a live network.

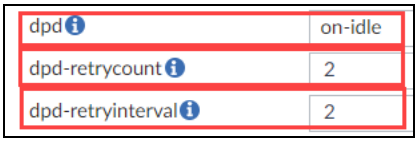
To fine-tune IPsec on the hub and branch devices

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates**, and then click **IPsec Tunnel**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

2. Double-click **1-Corp-SOT_BRANCH_IPsec_fine-tune** to edit it.
3. Edit one tunnel, and then review the **Advanced Options**.
   For each tunnel, the following settings have been modified for you:



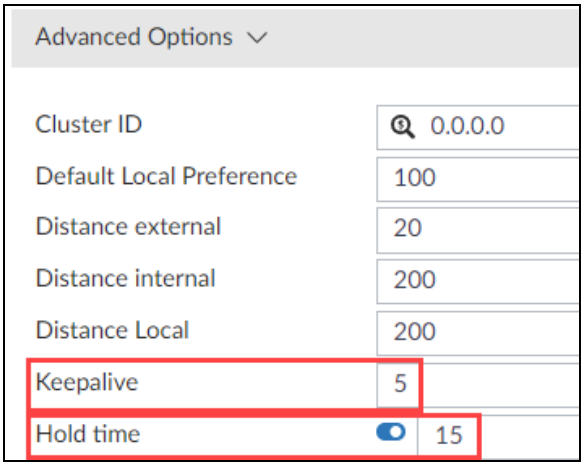
4. Click **Cancel**, and then click **Cancel** again to exit the template.
5. Double-click the **2-Corp-SOT_HUB1_IPsec_fine-tune** template.
6. Edit one tunnel definition, and then review the **Advanced Options**.
   The **dpd-retrycount** and **dpd-retryinterval** settings have been modified similarly on each hub tunnel.

In the IPsec phase 1 configuration, the **dpd-mode**, **dpd-retrycount**, and **dpd-retryinterval** settings are set to **on-idle**, `2`, and `2`, respectively. With these settings, DPD should detect a tunnel that is down 6 seconds after connectivity is lost.

7. Click **Cancel**, and then click **Cancel** again to exit the template.

To fine-tune BGP on the hub and branches

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates**, and then click **BGP**.
   The following template has been configured for you based on the templates that the SD-WAN overlay template created:
   - **3-Corp-SOT_BRANCH_BGP_fine-tune**
   - **4-Corp-SOT_HUB1_BGP-fine-tune**
2. Double-click **3-Corp-SOT_BRANCH_BGP_fine-tune**.
   Similar to the updates that were done for the hub, the following BGP settings have been updated for you:



3. Double-click a neighbor definition to edit it.
4. Expand the **Advanced Options** section.
   The following settings have been updated on each neighbor definition for you:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Additional Path	Receive
Connect Timer	1

For the branch devices, the BGP configuration is modified as follows to instruct the branch devices to accept the additional paths that they receive from the hub:

- For each neighbor definition on the branch template, the **additional-path** setting is set to **receive**. This setting instructs FortiGate to accept additional paths from a BGP neighbor.

For the branch devices, the BGP configuration is modified as follows to speed up link failure detection and BGP convergence:

- The **keepalive-timer**, **holdtime-timer**, and **advertisement-interval** settings are set to `5`, `15`, and `1`, respectively, to speed up routing convergence and failover.
- For each neighbor definition on the branch template, the **connect-timer** setting is set to `1`. This setting speeds up the frequency of the connection attempts that FortiGate makes to establish a BGP peering.

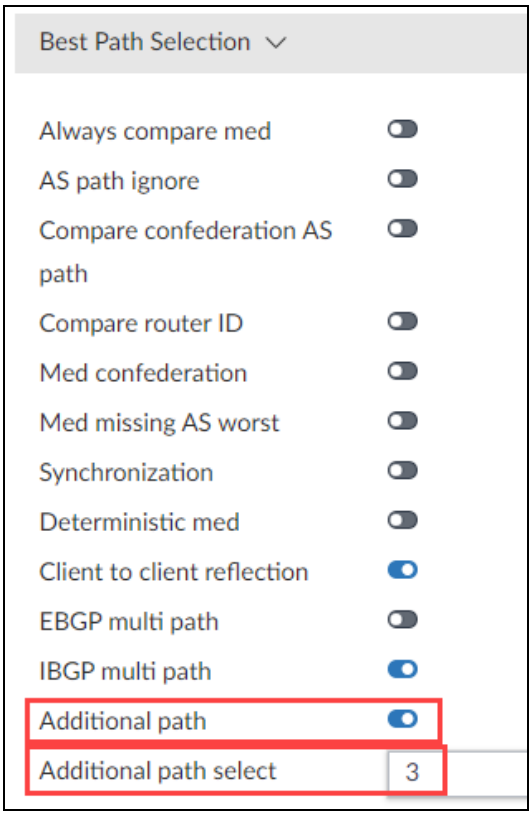
5. Click **Cancel** exit the template.
6. Double-click **4-Corp-SOT_HUB1_BGP-fine-tune**.
   The BGP settings shown in the following image have been updated for you:

Advanced Options

Cluster ID	0.0.0.0
Default Local Preference	100
Distance external	20
Distance internal	200
Distance Local	200
Keepalive	5
Hold time	15

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

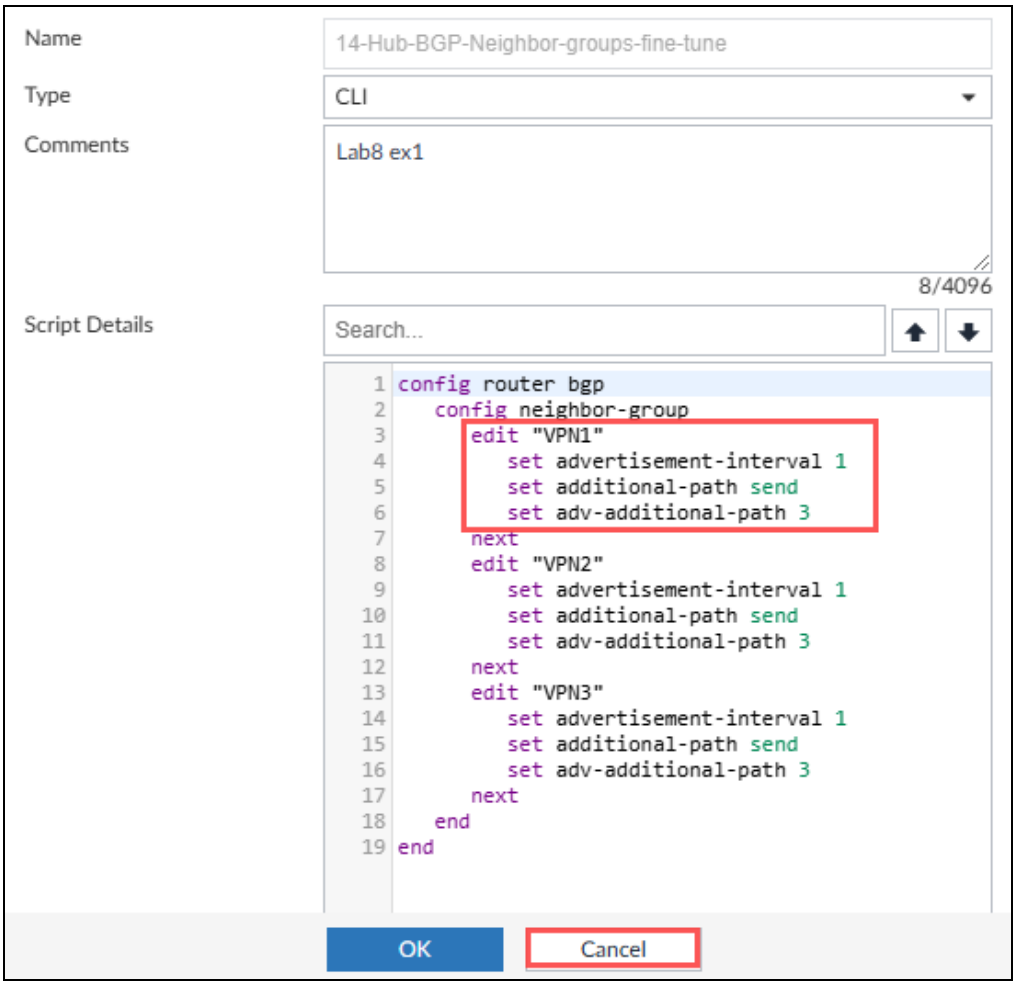
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



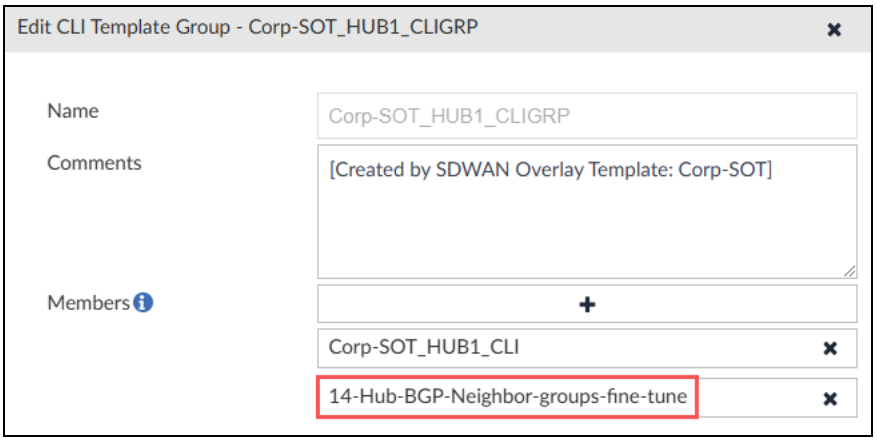
7. Click **Cancel** exit the template.
8. Continuing in the **Provisioning Templates** section, click **CLI**.
9. Double-click **14-Hub-BGP-Neighbor-groups-fine-tune** to edit and review it.
   Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



10. Click **Cancel**.
11. Double-click the CLI template group **Corp-SOT_HUB1_CLIGRP** to edit it.
12. Click **+** , and then select **14-Hub-BGP-Neighbor-groups-fine-tune**.



13. Click **OK** to validate the group update.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

For the hub, the BGP configuration is modified as follows to allow the advertisement of additional paths between the branch devices:

- The **additional-path** and **additional-path-select** settings are set to **enable** and `3`, respectively. The result is that dc1_fgt can identify up to three additional paths per prefix.
- Inside each neighbor-group, the `additional-path` and `adv-additional-path` settings are set to `send` and `3`, respectively. The result is that dc1_fgt can identify up to three additional paths per prefix for the specified neighbors, and send them to the branch devices.

For the hub, the BGP configuration is modified as follows to speed up link failure detection and BGP convergence:

- The **keepalive-timer**, **holdtime-timer**, and `advertisement-interval` settings are set to `5`, `15`, and `1`, respectively, to speed up routing convergence and failover.

To update the template groups

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **Template Groups**.
2. Double-click **Corp-SOT_HUB1** to edit it.
3. Click **+** to edit the provisioning template list.
4. Expand the **IPsec Tunnel Template** section, and then select **2-Corp-SOT_HUB1_IPsec_fine_tune**.
5. Expand the **BGP Tunnel Template** section, and then select **4-Corp-SOT_HUB1_BGP_fine_tune**.
6. Click **OK** to validate the template selection, and then click **OK** to validate the group update.
7. Repeat steps 2–6 to edit the **Corp-SOT_BRANCH group**.
   Select the following templates:

Field	Value
IPsec Tunnel Template	1-Corp-SOT_BRANCH_IPsec_fine_tune
BGP Template	3-Corp-SOT_BRANCH_BGP_fine_tune

Your template group selection should look like the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

	Template Group Name	Provisioning Templates	Assigned to Device/Group
☐	Corp-SOT_HUB1	corp_st 2-Corp-SOT_HUB1_IPsec_fine_tune 4-Corp-SOT_HUB1_BGP-fine-tune Corp-SOT_HUB1_CLIGRP	1 Device in Total View dc1_fgt [root]
☐	Corp-SOT_BRANCH	corp_st 1-Corp-SOT_BRANCH_IPsec_fine_tune 3-Corp-SOT_BRANCH_BGP_fine-tune branches_underlay_routes branches Corp-SOT_BRANCH_CLIGRP	3 Devices in Total View branches (3)

To install the configuration changes on the devices

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, **branch2_fgt**, **branch3_fgt**, and **dc1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on the hub and branch devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To review the behavior changes

1. In any of the branch SSH sessions, enter the following commands to display the status of BGP peerings and the BGP routes in the routing table:

```
get router info bgp summary
get router info routing-table bgp
```

For example, on branch2_fgt, your output should look similar to the following example:

```
branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.200.99.2, local AS number 65000
BGP table version is 26
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.61    4      65000     617     598       24    0    0 00:10:02        6
192.168.1.125   4      65000     539     517       24    0    0 00:10:02        6
192.168.1.189   4      65000     528     508       25    0    0 00:10:00        6

Total number of neighbors 3


branch2_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.1.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 00:09:59, [1/0]
                    [200/0] via 192.168.1.65 [3] (recursive is directly connected, HUB1-VPN2), 00:09:59, [1/0]
                    [200/0] via 192.168.1.129 [3] (recursive is directly connected, HUB1-VPN3), 00:09:59, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.3 [3] (recursive is directly connected, HUB1-VPN1), 00:10:02, [1/0]
                    [200/0] via 192.168.1.67 [3] (recursive is directly connected, HUB1-VPN2), 00:10:02, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:10:05, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:10:05, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:10:05, [1/0]
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

The routing table now displays nine available paths for the `10.0.branch-id.0/24` prefix. Some of the routes are duplicate routes. You can see the duplicate routes in the output of the `get router info routing-table database` command.

Remember that the port4 interface of branch3_fgt is connected but did not receive an IP address on branch3_fgt. So, you should see only two BGP peerings with branch3_fgt.

2. Use the WAN simulator page to bring down DC1-ISP1 again to verify the faster convergence.
3. In any of the branch SSH sessions, enter the following commands multiple times to monitor the status of the HUB1-VPN1 overlay and BGP status:

```
diagnose sys sdwan health-check status HUB1_HC
get ipsec tunnel list
get router info bgp summary
```

The tunnel and BGP peering are now brought down much faster, which speeds up network convergence and failover.

4. Use the WAN simulator page to bring up DC1-ISP1.

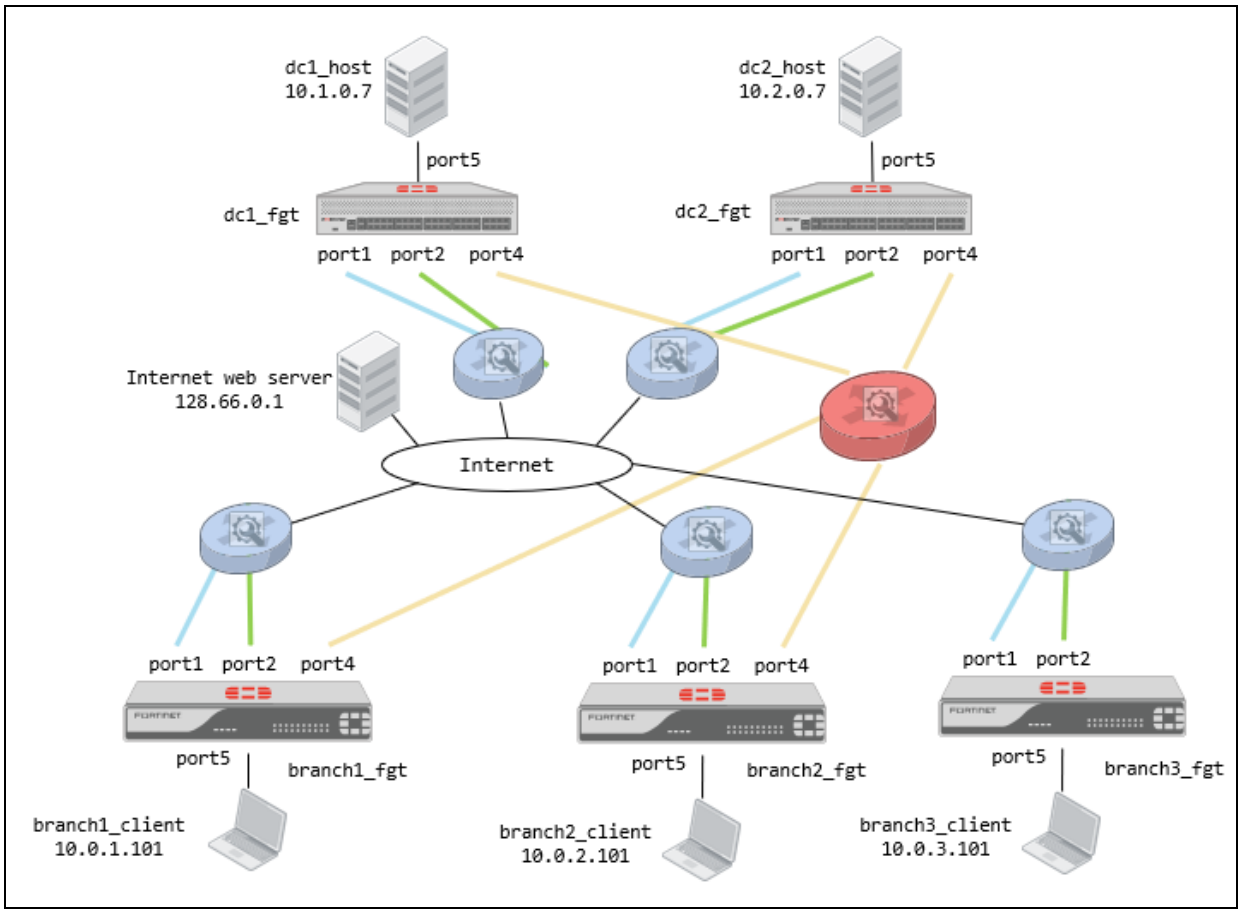
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 8: SD-WAN Dual Hub Deployment

In this lab, you will expand the topology and add a second hub for redundancy and prepare the configuration for auto-discovery VPN (ADVPN). First, you will use the SD-WAN overlay template to convert your SD-WAN topology to a dual hub with a primary hub and a secondary hub. Next, you will review and update the configuration that the SD-WAN overlay template applied.

The following image shows the target SD-WAN deployment:



Objectives

- Add a second hub and adjust the SD-WAN topology to a dual hub with a primary hub and a secondary hub
- Understand the configuration changes and the routing

Time to Complete

Estimated: 90 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Updating the SD-WAN Overlay Template for a Dual Hub Topology

In this exercise, you will add a secondary hub to your network and update your single-hub SD-WAN topology to a dual-hub topology with a primary hub and a secondary hub. First, you will add a device for the second hub to FortiManager. Next, you will update the SD-WAN overlay template to define the required changes on the existing branch devices, the dc1_fgt hub, and the secondary device, the dc2_fgt hub. Finally, you will install the changes and verify them on the FortiManager GUI.

Add dc2_fgt to FortiManager

Similar to what you did for the other devices, you will add the hub device, dc2_fgt, to FortiManager. The basic network configuration for this new hub device has been done for you.

To add dc2_fgt to FortiManager

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Device & Groups**.
3. Click **Add Device**.

4. Click **Discover Device**, and then configure the following settings:

Field	Value
IP Address	192.168.0.42
Use legacy device login	Enabled
User Name	admin
Password	password

5. Click **Next**.
6. Review the details about the device that FortiManager discovered, and then click **Next**.
7. Wait until the **Add Device** task is completed, and then click **Import Later**.
   You don't need to import the policy package for this device because you will use the policy package that you created for the primary hub dc1_fgt.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

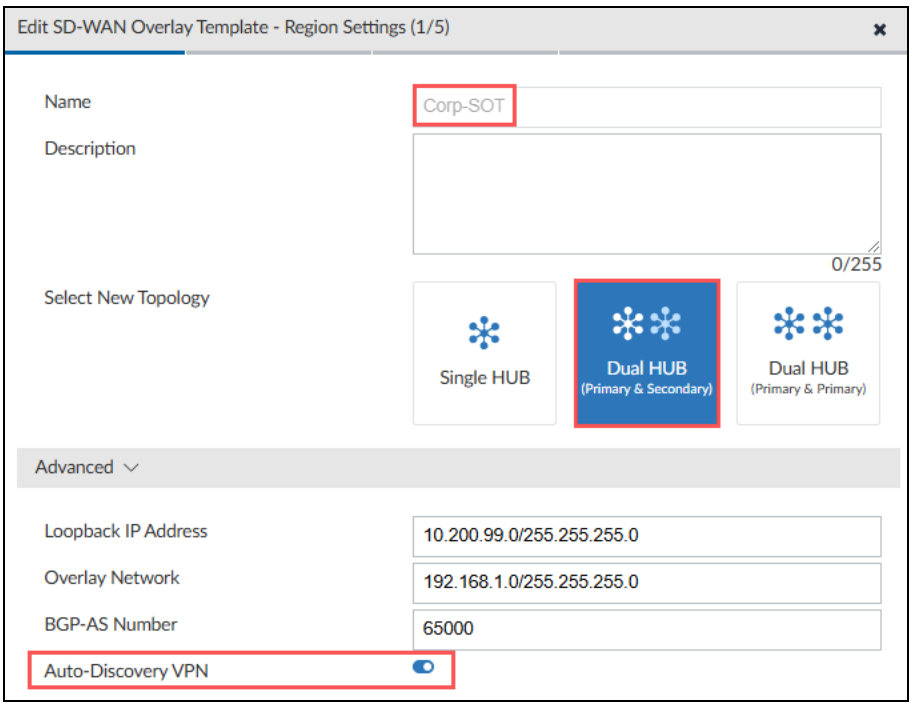
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Update the SD-WAN Overlay Template for a Dual Hub Topology

You will use the **Corp-SOT** SD-WAN overlay template that you created in a previous lab, and update it from a single-hub topology template to a dual-hub topology template. This time you will configure FortiManager to set up a template for an ADVPN topology. You will test ADVPN in the next lab.

To update the SD-WAN overlay template for a dual-hub topology

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates**, and then click **SD-WAN Overlay**.
2. Select **Corp-SOT**, and then click **Edit**.
3. Click **Dual HUB (Primary & Secondary**.
4. Click **Advanced**, and then enable **Auto-Discovery VPN**.



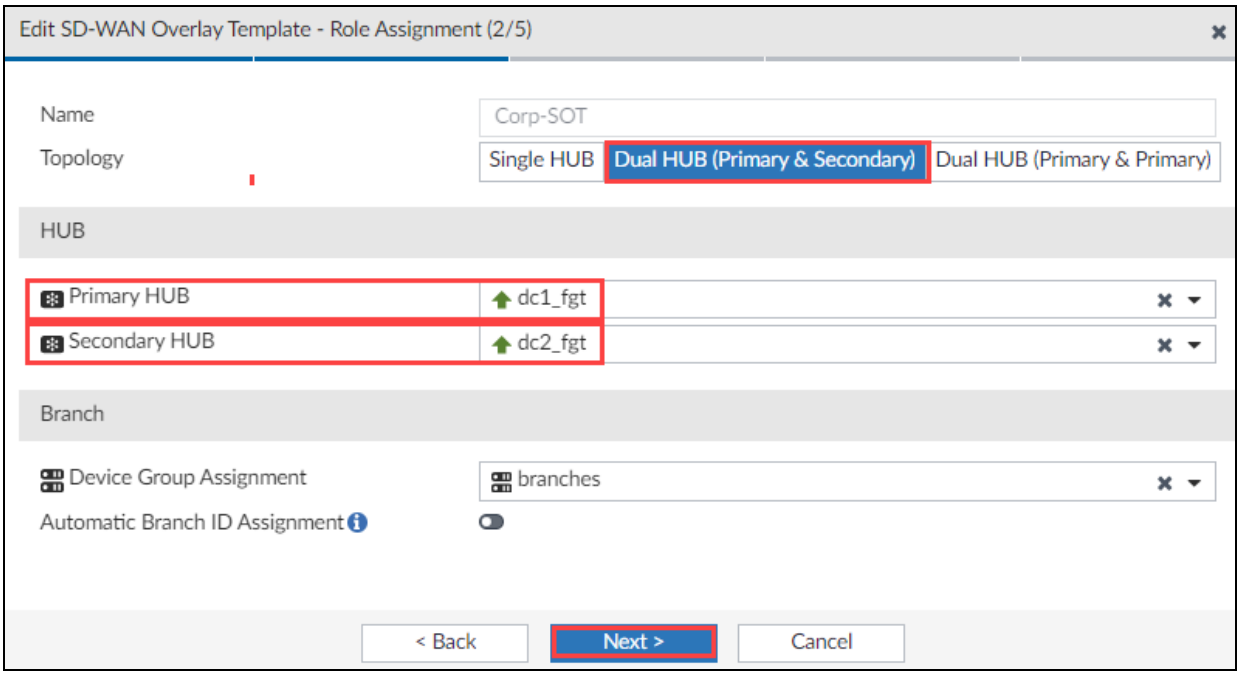
5. Click **Next**.
6. On the **Role Assignment (2/5)** page, configure the following settings:

Field	Value
Topology	Dual HUB (Primary & Secondary)
Hub	Primary HUB: dc1_fgt Secondary HUB: dc2_fgt
Branch	Device Group Assignment: branches

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Visit us: Brave-Dumps.com



7. Click **Next**.

When you select **Dual HUB (Primary & Secondary)** or **Dual HUB (Primary & Primary)**, FortiManager generates similar configurations, except for one difference. In a **Primary & Secondary** deployment, FortiManager assigns the secondary hub interfaces a higher cost than the primary hub interfaces.

8. On the **Network Configuration (3/5)** page, in the **HUB** section, configure the following settings for the **Primary HUB** and **Secondary HUB**:

Field	Value
Underlay	In the **WAN Underlay 1** field, type `port1`. In the **WAN Underlay 2** field, type `port2`. Click **+** to add a third WAN underlay, and then type `port4`.
Network Advertisement	Select **Connected**, and then click **+**. In the **Interface 1** field, type `port5` to advertise the network that is connected to the LAN interface.

When you update an SD-WAN overlay template from a single-hub to a dual-hub topology, you must reenter the configuration for the primary hub.

For this lab topology, the primary hub and secondary hub use the same ports as the WAN underlay interfaces. However, the SD-WAN overlay template allows administrators to select different interfaces for the primary and secondary hubs.

9. In the **Branch** section, confirm that the following settings are configured:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

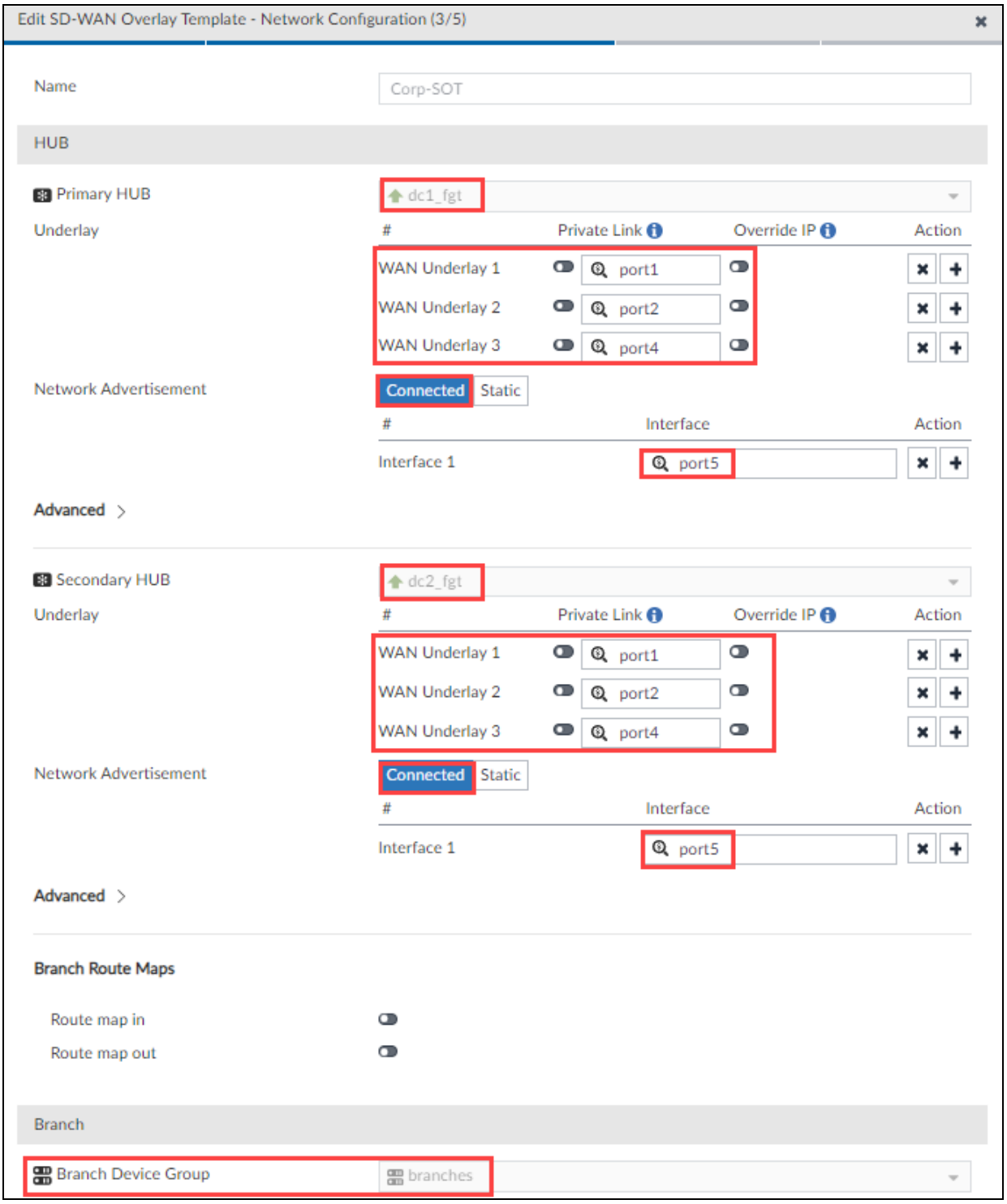
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Underlay	**WAN Underlay 1**: port1 **WAN Underlay 2**: port2 **WAN Underlay 3**: port4
Network Advertisement	Select **Connected**. **Interface 1**: port5.

Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

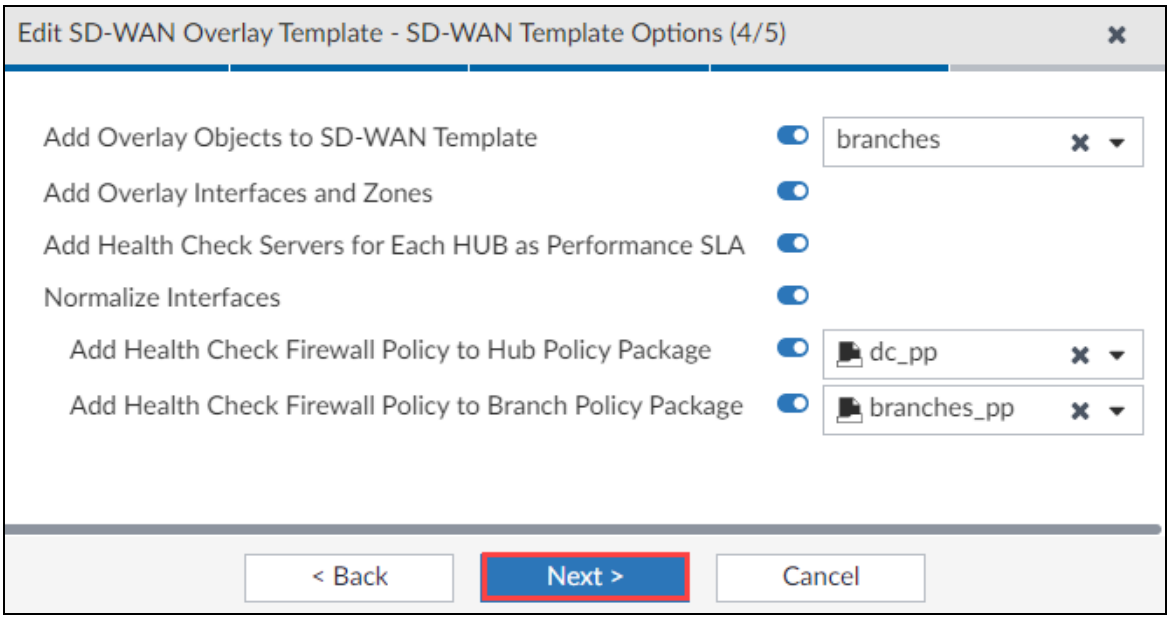
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



10. Click **Next**.
11. Review the **SD-WAN Template Options (4/5)** page.
    You do not need to make any changes. Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



12. Click **Next**.
13. On the **Summary (5/5)** page, review the settings.
14. After you complete the summary review, click **Finish** to complete the SD-WAN overlay template update.
    Your page should look similar to the following example:

Template Name	Topology	Assign to Device/Group	Loopback IP Address	Overlay Network	BGP AS Number
Corp-SOT	Dual HUB (Primary & Secondary)	dc1_fgt dc2_fgt branches	10.200.99.0/255.255.255.0	192.168.1.0/255.255.255.0	65000

Review, Adjust, and Install the Configurations

The SD-WAN overlay template tool creates new templates for the secondary hub and updates the multiple templates that were created previously. All of these templates use the settings that you configured—and Fortinet recommended settings and values for SD-WAN overlay tunnels with BGP routing—in a dual-hub context, with a primary hub and a secondary hub. The templates prepare the configurations of the branch devices and the hub for ADVPN. You will review these templates, and then you will install the changes on the hub and branch devices.

To review and adjust the template groups

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Template** > **Template Groups**.
2. Review the groups that are assigned to the branch devices and hubs.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Template Group Name	Provisioning Templates	Assigned to Device/Group
Corp-SOT_HUB1	corp_st Corp-SOT_HUB1_IPsec Corp-SOT_HUB1_BGP Corp-SOT_HUB1_CLIGRP	1 Device in Total View dc1_fgt [root]
Corp-SOT_BRANCH	corp_st Corp-SOT_BRANCH_IPsec Corp-SOT_BRANCH_BGP branches_underlay_routes branches Corp-SOT_BRANCH_CLIGRP	3 Devices in Total View branches (3)
Corp-SOT_HUB2	Corp-SOT_HUB2_IPsec Corp-SOT_HUB2_BGP Corp-SOT_HUB2_CLIGRP	1 Device in Total View dc2_fgt [root]

As a reminder, in the previous lab, in the last section, Fine-Tune IPsec and BGP on page 212, you used a cloned template to fine-tune BGP and IPsec settings. The template groups were defined as shown in the following example:

Template Group Name	Provisioning Templates	Assigned to Device
Corp-SOT_HUB1	corp_st 2-Corp-SOT_HUB1_IPsec_fine_tunned 4-Corp-SOT_HUB1_BGP-fine-tune Corp-SOT_HUB1_CLIGRP	1 Device in Total dc1_fgt [root]
Corp-SOT_BRANCH	corp_st 1-Corp-SOT_BRANCH_IPsec_fine_tun... 3-Corp-SOT_BRANCH_BGP_fine-tune branches_underlay_routes branches Corp-SOT_BRANCH_CLIGRP	3 Devices in Total branches (3)

FortiManager creates new templates and a new template group for the secondary hub: **Corp-SOT_HUB2**.

It creates also new BGP and IPsec templates for HUB1 and the branch devices.

It keeps the system template that the administrator assigned previously to the groups, and the CLI templates that the administrator previously added to the CLI template group.

3. Select **Corp-SOT_HUB2**, and then click **Edit**.
4. Click **+** to add a new template to the group.
5. Expand the **System Template** section, select **corp_st**, and then click **OK** to validate the selection.
6. Click **OK** to validate the template group changes.

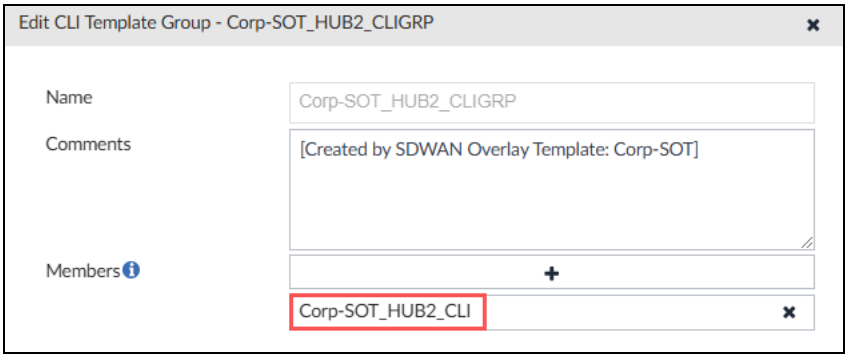
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To review the CLI templates

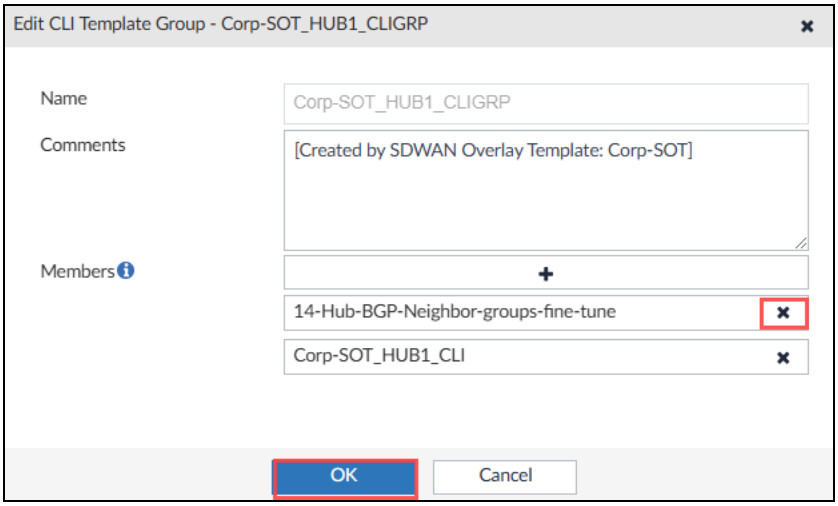
1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **CLI**.
2. Review the **Corp-SOT_HUB2_CLIGRP** template group.
   The group contains a single CLI template.

   Your output should look similar to the following example:



   The CLI template defines the hub loopback interface, similar to the single-hub topology.

3. Double-click **Corp-SOT_HUB1_CLIGRP** to edit it.
   This CLI group contains two templates: The template defined by the SD-WAN overlay template and the template that you added in the previous lab.
4. Click **x** to remove the **14-Hub-BGP-Neighbor-groups-fine-tune** template from the group.



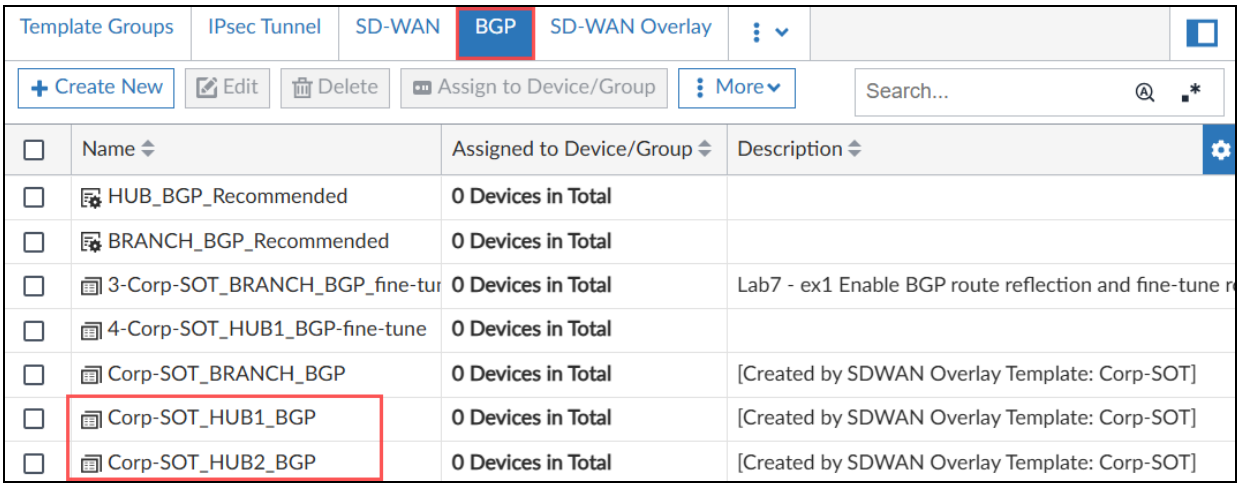
5. Click **OK** to validate the group update.

To review the BGP templates

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **BGP**.
2. Review the **Corp-SOT_HUB1_BGP** and **Corp-SOT_HUB2_BGP** templates.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Edit BGP Template - Corp-SOT_HUB2_BGP

CLI Configurations

Name: Corp-SOT_HUB2_BGP

Description: [Created by SDWAN Overlay Template: Corp-SOT]

45/256

Local As: 65000

Router ID: 10.200.99.252

Neighbors

Create New | Edit | Delete | More | Search...

IP	Remote AS
No record found.	

0

Neighbor Group

Create New | Edit | Delete | More | Search...

Name	Remote AS
VPN1	65000
VPN2	65000
VPN3	65000

3

Neighbor Range

Create New | Edit | Delete | More | Search...

Prefix	Neighbor Group	Maximum Neighbor Number
192.168.1.128/255.255.255.224	VPN1	0
192.168.1.160/255.255.255.224	VPN2	0
192.168.1.192/255.255.255.224	VPN3	0

3

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

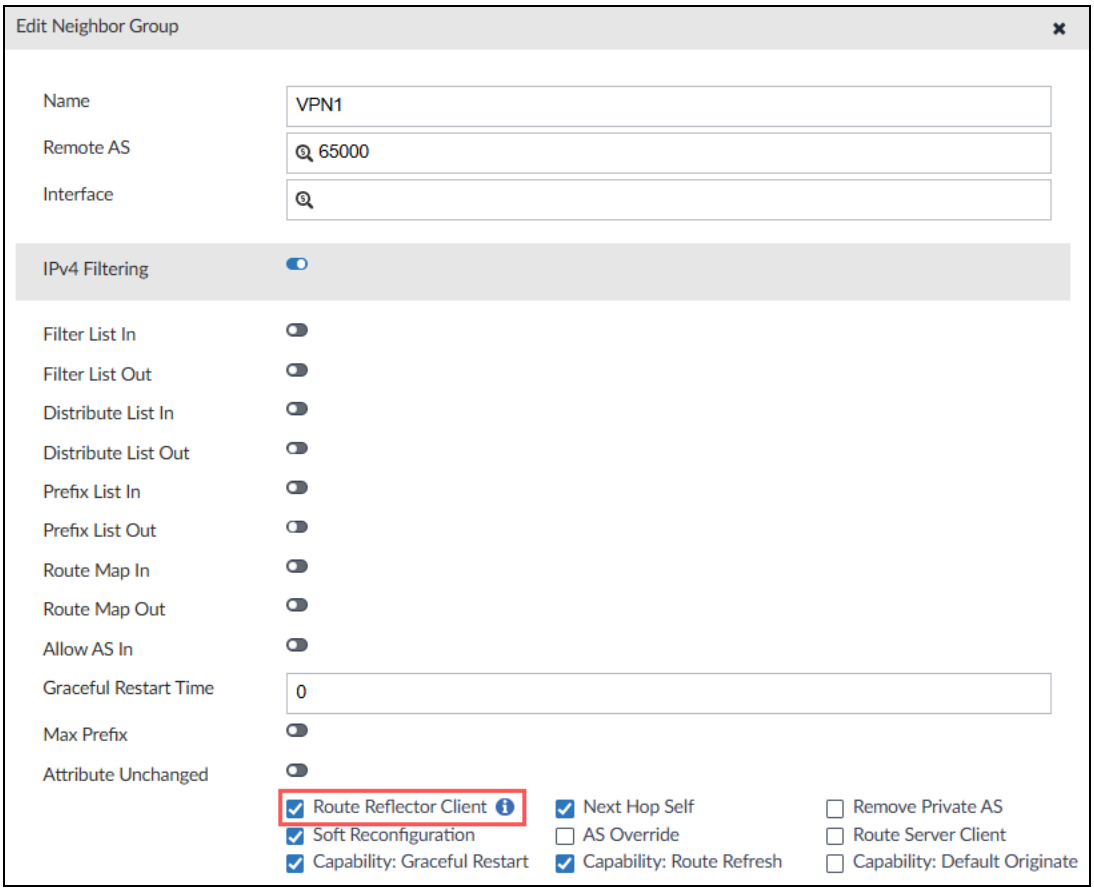
The BGP templates define the router ID with static values—10.200.99.252 for dc2_fgt and 10.200.99.253 for dc1_fgt.

The templates define three groups—VPN1, VPN2, and VPN3—similar to the groups that are defined for the single-hub topology.

The neighbor ranges are adjusted to distribute the available IP addresses between both hubs.

- With one hub and three overlays, the BGP template defines three address ranges with a 26-bit mask (255.255.255.192).
- With two hubs and three overlays, the BGP template defines six address ranges with a 27-bit mask (255.255.255.224).

3. Edit the **Corp-SOT_HUB2_BGP** template.
4. In the **Neighbor Group** section, double-click **VPN1** to edit it.
5. Note the **Route Reflector Client** setting.
   The checkbox is selected, which means it is enabled.



6. Click **Cancel** to exit the template edition.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

When you select the **Auto-Discovery VPN**option in the SD-WAN overlay template, FortiManager defines the IPsec and the BGP templates with the settings recommended for ADVPN with BGP per overlay. This includes enabling **Route Reflector Client** for each neighbor group on the hub.

7. Edit the **Corp-SOT_BRANCH_BGP** template.
8. Double-click a neighbor definition to edit it.
   Note that the **Update Source** parameter that you configured for the single-hub topology is no longer set.
9. Click **Cancel** to exit the neighbor definition, and then click **Cancel** to exit the template definition.

The template defines six neighbors, one for each overlay and to each hub.

Stop and think!

Why is the update source information not configured for the branch neighbors?

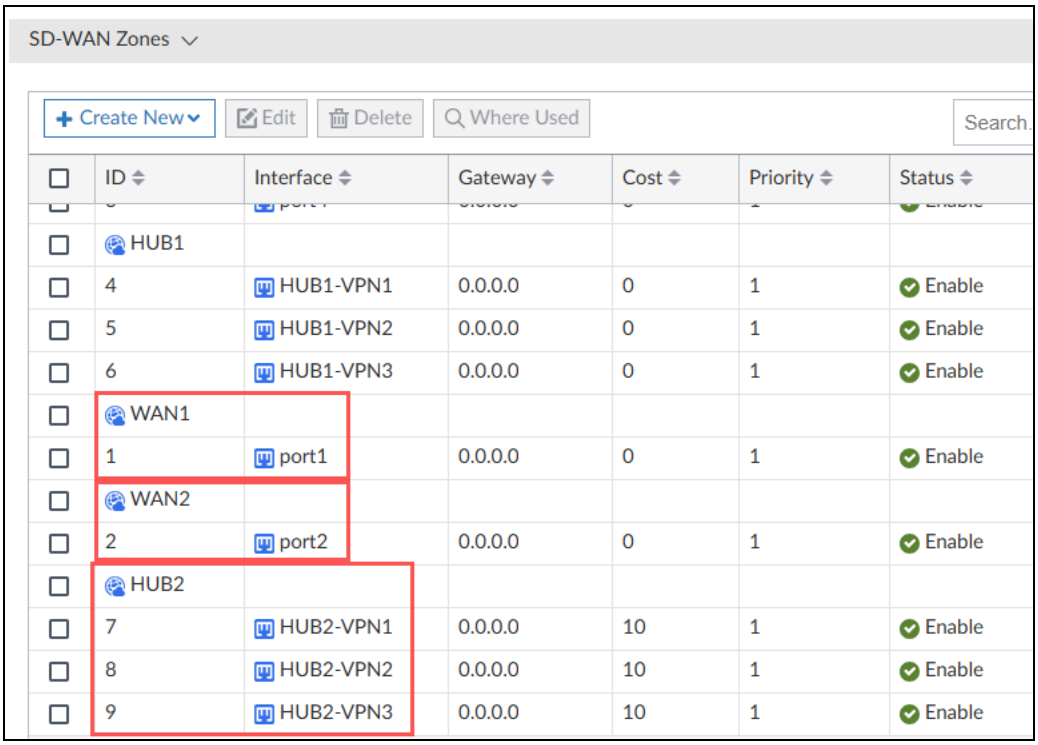
When FortiManager converts the SD-WAN overlay template from a single-hub topology to a dual-hub topology, it creates new templates for both hubs and the branch devices. However, it does not remove or modify the system or CLI templates that are assigned to HUB1 and the branch groups.

To review the zones and SD-WAN member configuration

1. Click **Provisioning Templates** > **SD-WAN**, and then edit the **branches** template to review the changes the SD-WAN overlay template update triggered.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



- You can see a new zone, **HUB2**, with three interface members: **HUB2-VPN1**, **HUB2-VPN2**, and **HUB2-VPN3**. These are the three overlay IPsec tunnel interfaces to the secondary hub.
- port1 and port2, which were previously in the **underlay** zone, have moved to the **WAN1** and **WAN2** zones. The SD-WAN overlay template also created a zone for port4. You will move port1 and port2 back to the **underlay** zone.

The SD-WAN overlay template placed the underlay interfaces, port1 and port2, in new underlay zones called **WAN1** and **WAN2**. Because you will continue to use SD-WAN rules and the firewall policy that you created previously, and defined with the zone named **underlay**, you must place the port1 and port2 interfaces back in the underlay zone.

If you don't want the SD-WAN overlay template to modify the zone and member definition in your SD-WAN template, disable the **Add Overlay Interface and Zones** option on the **SD-WAN Template Option (4/5)** page in the wizard. If you do this, you must manually define members and zones for your overlays.

---

2. In the **Interface Members** table, double-click **underlay** to edit the zone.
3. Under **Interface Members**, select **port1** and **port2**, and then click **OK** to validate the member selection.
4. Click **OK** to validate the zone edition.
5. Click **OK** to validate the template edition.
6. Edit the **branches** template again, select the **WAN1** and **WAN2** zones, and then click **Delete**.

After you remove all ports from a zone, you cannot immediately delete the zone. First, you must validate the template update.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Your output should look similar to the following example:

SD-WAN Zones

Create New | Edit | Delete | Where Used | Search...

ID	Interface	Gateway	Cost	Priority	Status	Installation Target
underlay						
1	port1	0.0.0.0	0	1	Enable	
2	port2	0.0.0.0	0	1	Enable	
WAN3						
3	port4	0.0.0.0	0	1	Enable	
HUB1						
4	HUB1-VPN1	0.0.0.0	0	1	Enable	
5	HUB1-VPN2	0.0.0.0	0	1	Enable	
6	HUB1-VPN3	0.0.0.0	0	1	Enable	
HUB2						
7	HUB2-VPN1	0.0.0.0	10	1	Enable	
8	HUB2-VPN2	0.0.0.0	10	1	Enable	
9	HUB2-VPN3	0.0.0.0	10	1	Enable	

7. Click **OK** to validate the template edition.

To review the policy packages

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
2. Expand the **dc_pp** policy package, and then click **Installation Targets**.
   Your page should look similar to the following example:

Installation Target	Config Status	Policy Package Status
dc1_fgt	Modified	dc_pp
dc2_fgt	Modified	Never Installed

The SD-WAN overlay template assigned the **dc_pp** policy package to the **dc2_fgt** device.

3. Click **Firewall Policy** to review the policy defined for the **dc_pp** policy package.

The policies allow traffic within the **Corp-net** corporate subnet (10.0.0.0/8). The policies are generic, and you do not need to update them to accommodate the secondary hub device.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

4. Click **Policy Packages** > **branches_pp** > **Firewall Policy**.
5. Double-click the **To Hub-Overlay** policy to edit it.
6. In the **Outgoing Interface** field, add **HUB2**.
   If you don't see HUB2 in the interface list, refresh your browser page.
7. Click **OK** to validate the policy update.
8. Repeat steps 5–7 to add **HUB2** as the incoming interface for the **From HUB-Overlay** policy.

#	Name	From	To	Source	Destination
Corp-SOT_BBLK (1/1 Total:1)					
1	Health Check Access	Branch-Lo	HUB1 HUB2	Corp-SOT_Br_...	Corp-SOT_Loo...
Underlay (2/2 Total:1)					
2	DIA	LAN	underlay	LAN-net	all
Overlay (3/4 Total:2)					
3	To Hub-Overlay	LAN	HUB1 HUB2	all	all
4	From Hub-Overlay	HUB1 HUB2	LAN	all	all
Implicit (5/5 Total:1)					
5	Implicit Deny	any	any	all all	all all

To install the configuration changes

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Policy Packages & Device Settings**.
3. In the **Policy Package** field, select **branches_pp**, and then click **Next**.
4. Select the three branches, and then click **Next**.
5. Click **Install** to install the configuration on the devices.
6. Wait for the installation to complete, and then click **Finish**.
7. Click **Install Wizard** again.
8. In the **Policy Package** field, select **dc_pp**, and then click **Next**.
9. Select **dc1_fgt** and **dc2_fgt**, and then click **Next**.
10. Click **Install Preview**, and then review the configuration changes for **dc1_fgt**.
    FortiManager will update the VPN interfaces, IPsec phase1, and neighbor-range definition.
11. Review the configuration changes for **dc2_fgt**.
    FortiManager will configure IPsec tunnels, BGP routes, and firewall policies.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

Why did the SD-WAN overlay template update the configuration on dc1_fgt?

With one hub device and three underlay links, the SD-WAN overlay template subdivided the address range allocated for the overlay into four subnets (/26 - 255.255.255.192, which is 61 host addresses per subnet).

With two hub devices and three underlay links, the SD-WAN overlay template must further subdivide the allocated address range. It now requires six subnets, one for each overlay and each hub. Therefore, it subdivided the /24 address range into eight subnets (/27 - 255.255.255.224, which is 30 host addresses per subnet).

12. Click **Close** to exit the install preview.
13. Click **Install** to install the configuration on the devices.
14. Wait for the installation to complete, and then click **Finish**.

Stop and think!

Which configuration changes did the addition of the secondary hub device trigger in the configuration of each branch device?

The addition of the secondary hub device triggers the following configuration changes:

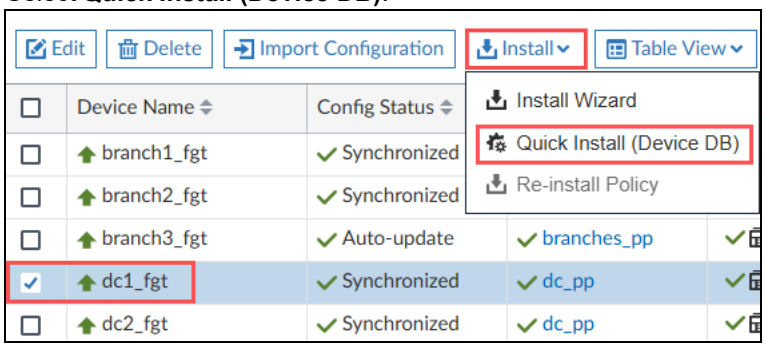
- Three IPsec tunnels and the corresponding interfaces—HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3—were created.
- A new SD-WAN zone, HUB2, which contains the HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3 members, was created.
- A new health check, HUB2_HC, was added.
- The firewall policy to allow health checks to both HUB1 and HUB2 was updated.
- Three new BGP neighbors were created through the tunnels to HUB2.
- The BGP neighbors to HUB1 were updated, because of the new address ranges.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

If FortiManager didn't install the configuration changes on one hub, or if you want to force the reinstallation of the database configuration to a device, you can perform the following steps:

1. Click **Device Manager** > **Device & Groups**.
2. Select a device, and then click the installation icon.
3. Select **Quick Install (Device DB)**.



4. Click **OK** confirm the installation of the configuration.
5. Wait for the installation to complete and then click **Finish**.

Review the Device Status and Topology

Now that you have installed the configuration changes on the branches and two hub devices, you will review the result on the FortiManager GUI monitor page.

To review the device status

1. Continuing on the FortiManager GUI, click **Device Manager** > **Device & Groups** > **Managed FortiGate**.
2. Confirm that you see the three branches and two hubs.

   For each of the devices, you should see a green check mark in the **Config Status**, **Policy Package Status**, and **Provisioning Templates** columns.

   Your page should look similar to the following example:

Device Name	Auto-link Status	Config Status	Host Name	IP Address	Policy Package Statu	Provisioning Templates
branch1_fgt		Synchronized	branch1_fgt	192.168.0.31	branches_pp	Corp-SOT_BRANCH
branch2_fgt		Synchronized	branch2_fgt	192.168.0.32	branches_pp	Corp-SOT_BRANCH
branch3_fgt		Synchronized	branch3_fgt	192.168.0.33	branches_pp	Corp-SOT_BRANCH
dc1_fgt		Synchronized	dc1_fgt	192.168.0.41	dc_pp	Corp-SOT_HUB1
dc2_fgt		Synchronized	dc2_fgt	192.168.0.42	dc_pp	Corp-SOT_HUB2
shop1_fgt	Enabled	Unknown	FGT40FTK200006		Never Installed	
shop2_fgt	Enabled	Unknown	FGT40FTK200030		Never Installed	

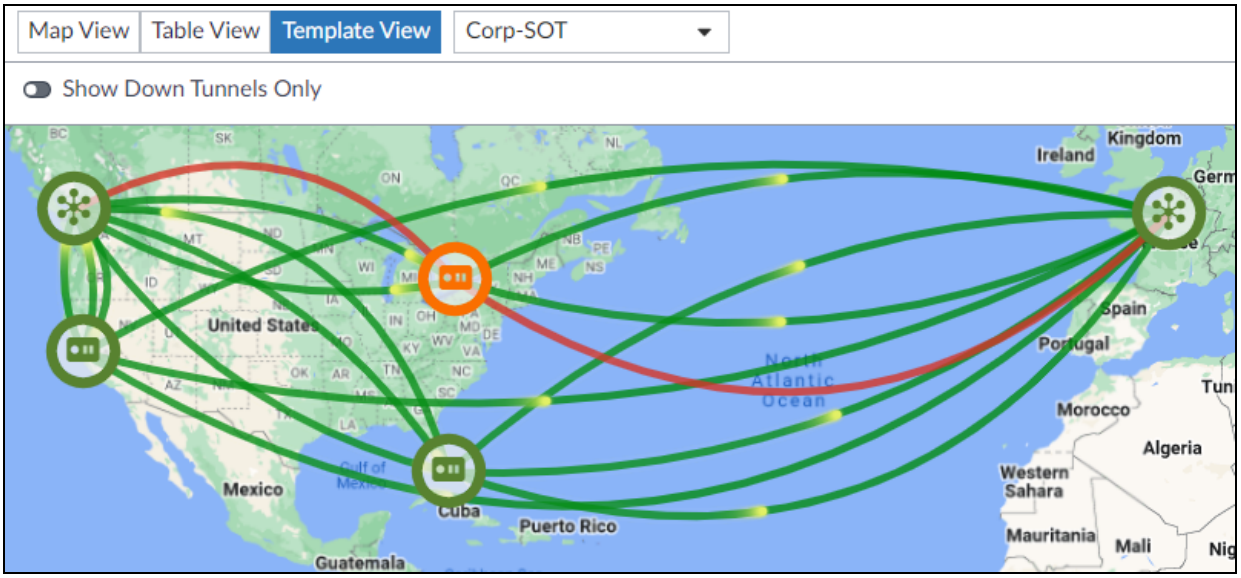
To review the SD-WAN topology and overlay links

1. Click **Device Manager** > **Monitors** > **SD-WAN Monitor**.
2. Select **Template View**, and then select **Corp-SOT**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Your page should look similar to the following example:



The primary hub is located in Vancouver. The secondary hub is located in Paris. Remember that branch3_fgt has no connection on port4, so it is expected that the tunnels defined on port4 remain down.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Refining the Dual Hub Configuration

In this exercise, first you will review the configurations that the SD-WAN overlay template applied to the devices. Next, you will configure an SD-WAN rule to steer the traffic to one hub or the other, according to the link status.

Review the Configuration on the Branches

In the previous exercise, with the SD-WAN monitor tool, you verified that the IPsec tunnels were up and that each branch device had SD-WAN interfaces to HUB2. Now, you will review and adjust the SD-WAN configuration to take advantage of the dual-hub topology.

To verify the routing on branch1_fgt

1. Open an SSH session to branch1_fgt.
2. Log in with the following credentials:
   - Username: `admin`
   - Password: `password`
3. Enter the following command:
   `get router info routing-table bgp`
   Your output should look similar to the following example:

```
branch1_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.2.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 14:07:50, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 14:07:50, [1/0]
                    [200/0] via 192.168.1.130 [3] (recursive is directly connected, HUB2-VPN1), 14:07:50, [1/0]
                    [200/0] via 192.168.1.162 [3] (recursive is directly connected, HUB2-VPN2), 14:07:50, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.1 [3] (recursive is directly connected, HUB1-VPN1), 14:07:50, [1/0]
                    [200/0] via 192.168.1.33 [3] (recursive is directly connected, HUB1-VPN2), 14:07:50, [1/0]
                    [200/0] via 192.168.1.129 [3] (recursive is directly connected, HUB2-VPN1), 14:07:50, [1/0]
                    [200/0] via 192.168.1.161 [3] (recursive is directly connected, HUB2-VPN2), 14:07:50, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 14:07:50, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 14:07:50, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 14:07:50, [1/0]
B       10.2.0.0/24 [200/0] via 192.168.1.157 (recursive via HUB2-VPN1 tunnel 100.64.1.3), 14:07:51, [1/0]
                    [200/0] via 192.168.1.189 (recursive via HUB2-VPN2 tunnel 100.64.1.11), 14:07:51, [1/0]
                    [200/0] via 192.168.1.221 (recursive via HUB2-VPN3 tunnel 172.16.1.1), 14:07:51, [1/0]
```

When you enable the ADVPN option on the SD-WAN overlay template, FortiManager adjusts the BGP templates to allow route reflection.

branch1_fgt learned the route to the dc2_fgt local subnet 10.2.0.0/24 through the three overlay interfaces—HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3.

branch1_fgt has equal cost routes to branch2_fgt, through two reflected routes through HUB1, and two routes through HUB2.

Similarly, branch1_fgt has four equal cost routes to the branch3_fgt local subnets, two through HUB1 and two through HUB2.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

branch1_fgt learned three routes to each hub but only four reflected routes to branch2_fgt— two through each hub. Why?

The number of reflected routes depends on the number or routes available *and* on the number of reflected routes configured on the hub. In the next task you will update the configuration of the reflected route on the hubs.

To verify and update the configuration of the reflected route on the hubs

1. Open an SSH session to dc1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Enter the following commands:
   ```
   show router bgp
   show full router bgp | grep ad
   ```
   Your output should look similar to the following example. Note that the first output is truncated to display only the relevant part.

```
dc1_fgt # show router bgp
config router bgp
    set as 65000
    set router-id 10.200.99.253
    set ibgp-multipath enable
    set additional-path enable
    set graceful-restart enable
    set additional-path-select 255
    config neighbor-group
        edit "VPN1"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
            set additional-path send
            set route-reflector-client enable
        next
        edit "VPN2"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
            set additional-path send
            set route-reflector-client enable
        next
        edit "VPN3"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65000
            set additional-path send
            set route-reflector-client enable
        next
    end
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

At the BGP level, dc1 fgt configuration enables additional paths (`set additional-path enable`), and allows up to 255 additional paths (`set additional-path-select 255`). Each neighbor group is configured to send additional paths (`set additional-path send`).

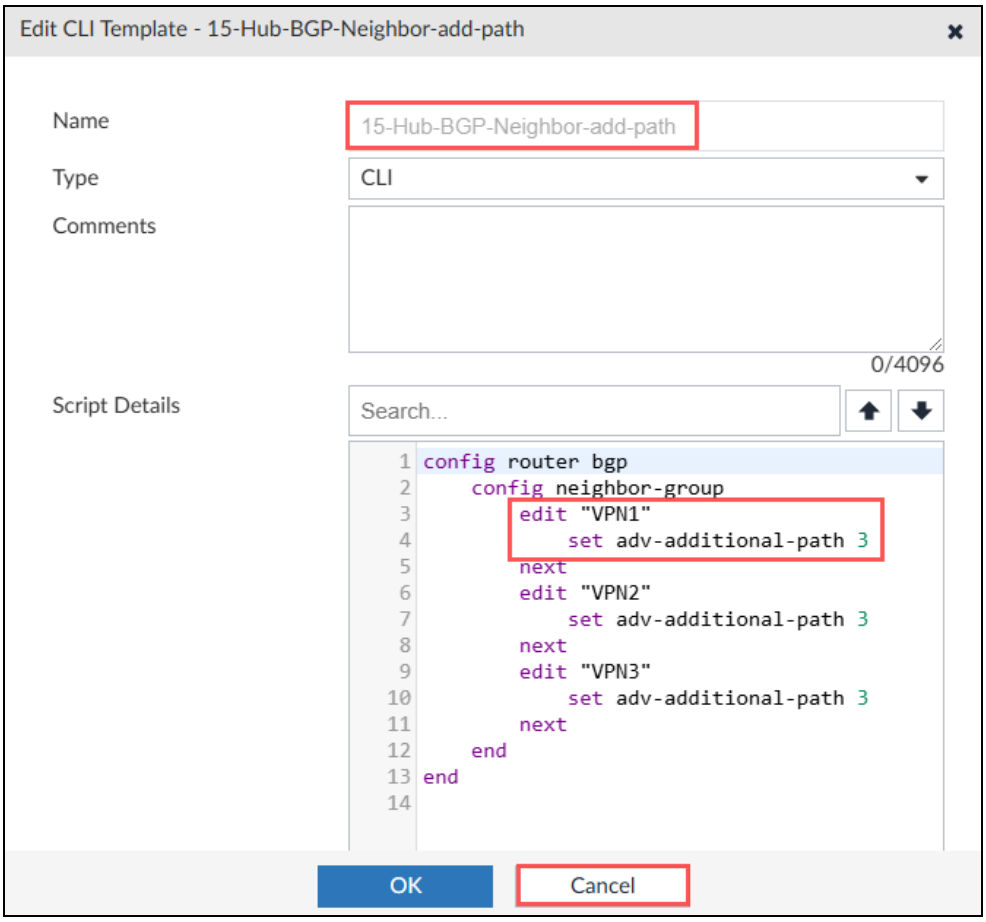
```
dc1_fgt # show full router bgp | grep ad
    set additional-path enable
    set additional-path6 disable
    set additional-path-vpnv4 disable
    set additional-path-vpnv6 disable
    set additional-path-select 255
    set cross-family-conditional-adv disable
            set advertisement-interval 30
            set additional-path send
            set additional-path6 disable
            set additional-path-vpnv4 disable
            set additional-path-vpnv6 disable
            set adv-additional-path 2
            set advertisement-interval 30
            set additional-path send
            set additional-path6 disable
            set additional-path-vpnv4 disable
            set additional-path-vpnv6 disable
            set adv-additional-path 2
            set advertisement-interval 30
            set additional-path send
            set additional-path6 disable
            set additional-path-vpnv4 disable
            set additional-path-vpnv6 disable
            set adv-additional-path 2
```

The configuration details displayed with the `show full` command show that, by default, FortiGate advertises only two additional paths for each neighbor group.

3. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
4. Click **Device Manager** > **Provisioning Templates** > **CLI**.
5. Double-click the **15-Hub-BGP-Neighbor-add-path** template to edit it.

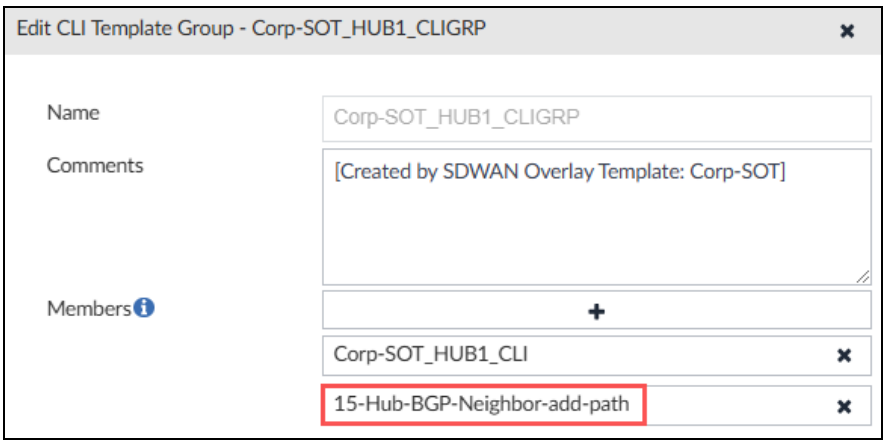
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



The template instructs the hub to advertise three additional paths for each neighbor group.

6. Click **Cancel**.
7. Double click the **Corp-SOT_HUB1_CLIGRP** CLI template group to edit it.
8. Click **+**, and then select **15-Hub-BGP-Neighbor-add-path**.



9. Click **OK** to validate the template update.
10. Repeat steps 7–9 to add **15-Hub-BGP-Neighbor-add-path** to the **Corp-SOT_HUB2_CLIGRP** CLI template group.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

To install the configuration changes on the hubs

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **dc1_fgt** and **dc2_fgt**, and then click **Next**.
4. Wait for the installation to complete, and then click **Finish**.

To verify the routing on branch1_fgt

1. Open an SSH session to branch1_fgt.
2. Log in with the following credentials:
   - Username: `admin`
   - Password: `password`
3. Enter the following command:
   `get router info routing-table bgp`
   Your output should look similar to the following example:

```
branch1_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.2.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 00:03:09, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 00:03:09, [1/0]
                    [200/0] via 192.168.1.65 [3] (recursive is directly connected, HUB1-VPN3), 00:03:09, [1/0]
                    [200/0] via 192.168.1.130 [3] (recursive is directly connected, HUB2-VPN1), 00:03:09, [1/0]
                    [200/0] via 192.168.1.162 [3] (recursive is directly connected, HUB2-VPN2), 00:03:09, [1/0]
                    [200/0] via 192.168.1.193 [3] (recursive is directly connected, HUB2-VPN3), 00:03:09, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.1 [3] (recursive is directly connected, HUB1-VPN1), 00:03:09, [1/0]
                    [200/0] via 192.168.1.33 [3] (recursive is directly connected, HUB1-VPN2), 00:03:09, [1/0]
                    [200/0] via 192.168.1.129 [3] (recursive is directly connected, HUB2-VPN1), 00:03:09, [1/0]
                    [200/0] via 192.168.1.161 [3] (recursive is directly connected, HUB2-VPN2), 00:03:09, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 00:03:09, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 00:03:09, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 00:03:09, [1/0]
B       10.2.0.0/24 [200/0] via 192.168.1.157 (recursive via HUB2-VPN1 tunnel 100.64.1.3), 00:03:59, [1/0]
                    [200/0] via 192.168.1.189 (recursive via HUB2-VPN2 tunnel 100.64.1.11), 00:03:59, [1/0]
                    [200/0] via 192.168.1.221 (recursive via HUB2-VPN3 tunnel 172.16.1.1), 00:03:59, [1/0]
```

   branch1_fgt now learns six routes to branch2_fgt, three through each hub. However, branch1_fgt learns four routes to branch3_fgt. This is expected because branch3_fgt establishes only two tunnels to each hub.

> **Stop and think!**
>
> In the SD-WAN overlay template, you selected **Dual HUB (Primary & Secondary)**, but there is no difference at the routing level. The branch devices have equal cost routes to both hubs. Why?
>
> The SD-WAN overlay template didn't apply a distinction between the primary hub and secondary hub at the BGP routing level. It differentiates the hub preference with the SD-WAN member cost.

To verify and update the SD-WAN configuration

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Provisioning Templates**, and then select **SD-WAN**.
3. Double-click the **branches** template to edit it.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

SD-WAN Zones

+ Create New | Edit | Delete | Where Used | Searc

ID	Interface	Gateway	Cost	Priority	Status
underlay					
1	port1	0.0.0.0	0	1	Enable
2	port2	0.0.0.0	0	1	Enable
WAN3					
3	port4	0.0.0.0	0	1	Enable
HUB1					
4	HUB1-VPN1	0.0.0.0	0	1	Enable
5	HUB1-VPN2	0.0.0.0	0	1	Enable
6	HUB1-VPN3	0.0.0.0	0	1	Enable
HUB2					
7	HUB2-VPN1	0.0.0.0	10	1	Enable
8	HUB2-VPN2	0.0.0.0	10	1	Enable
9	HUB2-VPN3	0.0.0.0	10	1	Enable

The SD-WAN members in the HUB1 zone have a cost of 0, while the SD-WAN members in the HUB2 zone have a cost of 10.

4. Expand the **Performance SLA** section.
   Your page should look similar to the following example:

Performance SLA

+ Create New | Edit | Delete | Where Used | Search...

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Corp_HC	198.18.1.1, 198.18.1.2	5	150	25	5	5
HUB1_HC	10.200.99.253	1	255	55	5	5
HUB2_HC	10.200.99.252	1	255	55	5	5

The SD-WAN overlay template created two health checks, one for each hub. These health checks use the hub loopback IP addresses as the detection server.

5. Double-click **HUB1_HC** to edit it, and then configure the following settings to update the SLA targets:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

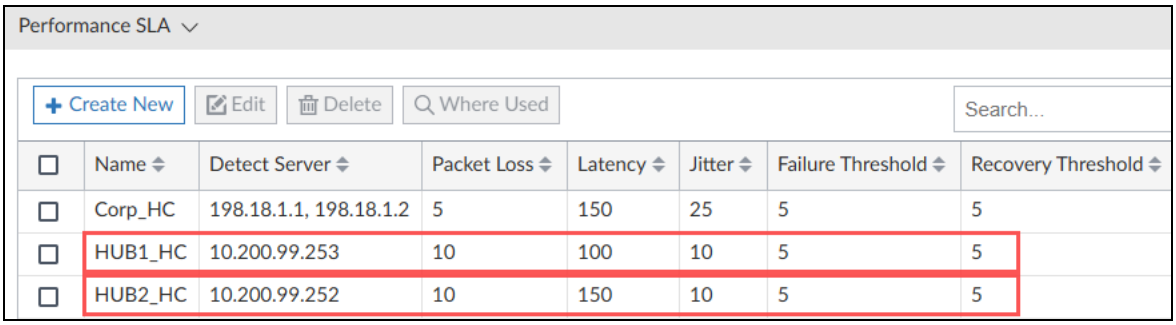
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Field	Value
Latency Threshold	100
Jitter Threshold	10
Packet Loss Threshold	10

6. Click **OK** to validate the health check update.
7. Double-click **HUB2_HC**, and then update the SLA target with the following threshold values:

Field	Value
Latency Threshold	150
Jitter Threshold	10
Packet Loss Threshold	10

8. Click **OK** to validate the health check update.
   Your page should look similar to the following example:



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Corp_HC	198.18.1.1, 198.18.1.2	5	150	25	5	5
HUB1_HC	10.200.99.253	10	100	10	5	5
HUB2_HC	10.200.99.252	10	150	10	5	5

9. Expand the **SD-WAN Rules** section.
   Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

SD-WAN Rules

Create New | Edit | Delete | More

	ID	Name	Source	Destination	Criteria	Members	Performance SLA
	1	Critical-DIA	LAN-net	Microsoft.Portal Salesforce		port1 port2	
	2	Non-Critical-DIA	LAN-net	Facebook LinkedIn Game		port2	
	3	Corp	LAN-net	Corp-net		HUB1-VPN1 HUB1-VPN2 HUB1-VPN3	
		sd-wan	All	All	Source IP	All	

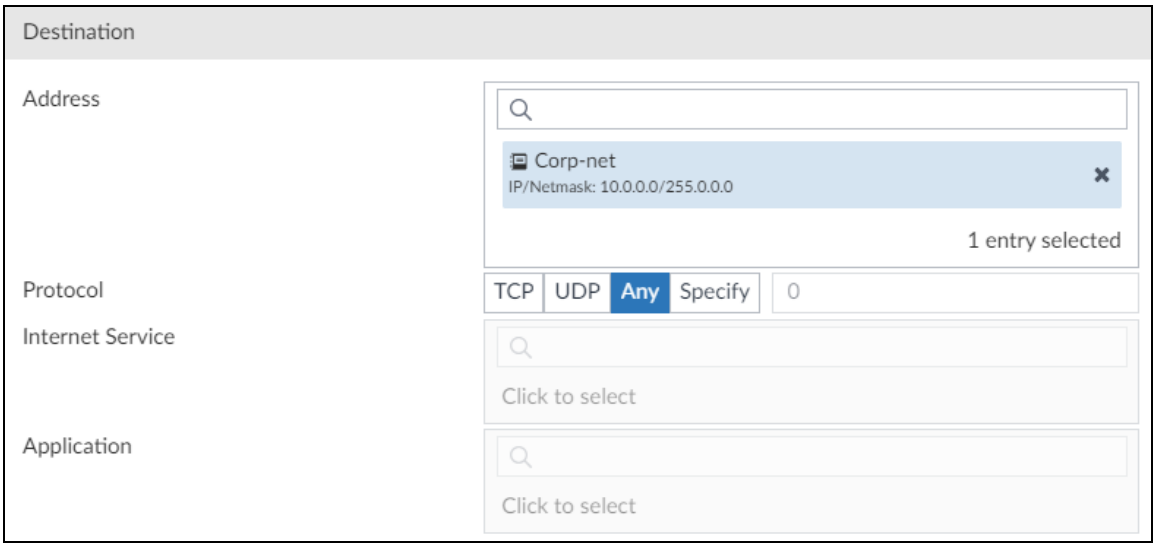
The **Corp** SD-WAN rule that you previously defined can steer HUB1 traffic through the HUB1 SD-WAN overlay interfaces only.

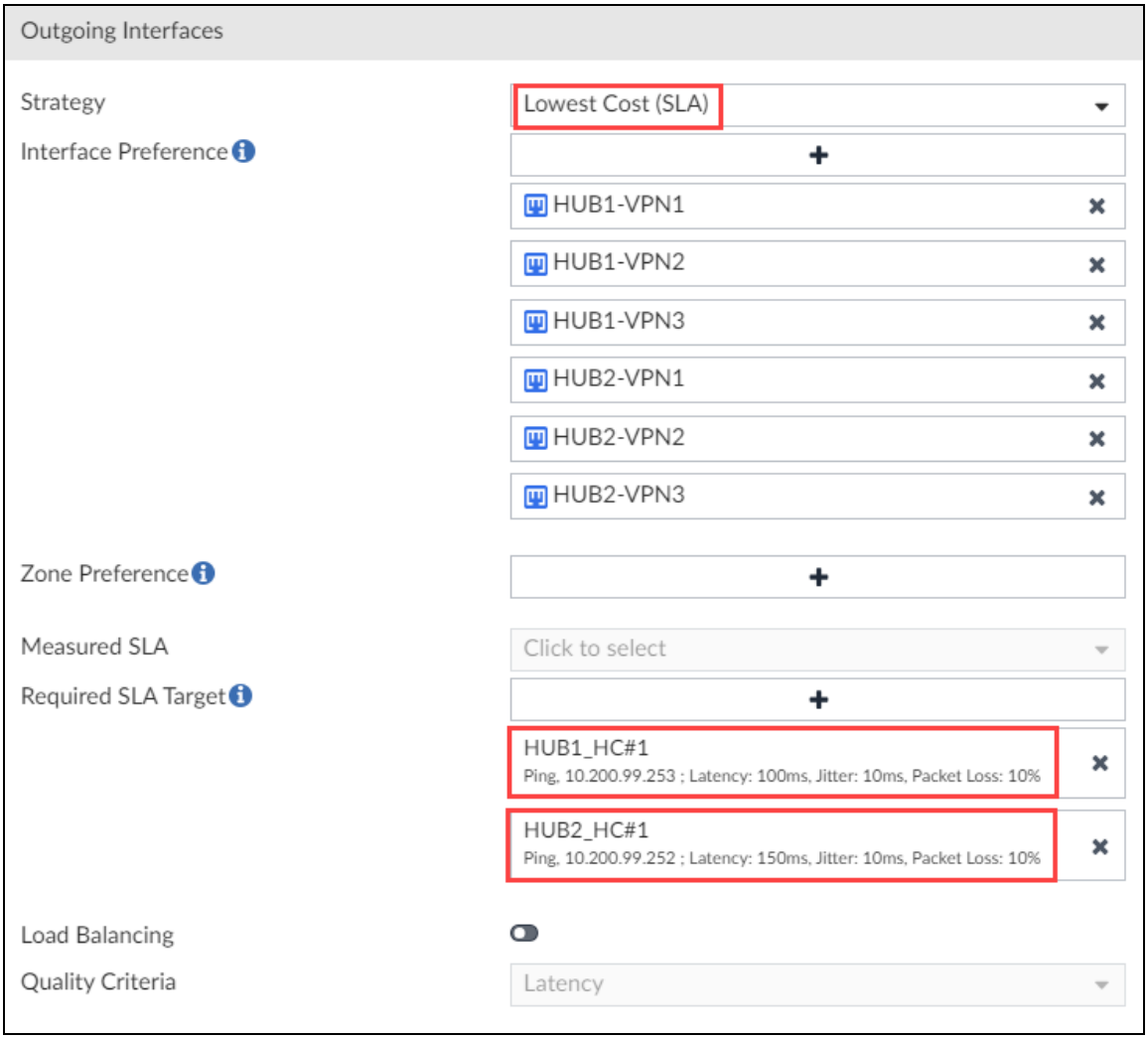
10. Double-click the **Corp** SD-WAN rule, and then configure the following settings:

Field	Value
Destination protocol	Any
Strategy	Lowest Cost (SLA)
Interface Preference	HUB1-VPN1 HUB1-VPN2 HUB1-VPN3 HUB2-VPN1 HUB2-VPN2 HUB2-VPN3
Required SLA Target	Click **+**, and then select **HUB1_HC#1** and **HUB2_HC#1**.
Load Balancing	disabled

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com





11. Click **OK** to validate the SD-WAN rule update.
12. Click **OK** to validate the template update.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Stop and think!

You defined the service with six overlay interfaces, three for each hub, and you selected two health checks, one on the HUB1 loopback IP address and one on the HUB2 loopback IP address. What will be the result?

The HUB1_HC#1 health check monitors the status of the HUB1-VPN1, HUB1-VPN2, and HUB1-VPN3 interfaces. The HUB2_HC#1 health check monitors the status of the HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3 interfaces.

To improve interface monitoring, you can use a single SLA target for HUB1 and HUB2. For example, if the two hubs connect to common devices, such file servers, you can use them as health check devices.

To install the configuration changes on the branches

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select the three branch devices, and then click **Next**.
4. Wait for the installation to complete, and then click **Finish**.

To review the configuration on branch1_fgt

1. Open an SSH session to branch1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Enter the following commands:

```
diagnose sys sdwan service4 3
show firewall policy 3
show firewall policy 4
```

Your output should be similar to the following example:

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(10), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(6):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    4: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    5: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    6: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # show firewall policy 3
config firewall policy
    edit 3
        set name "To Hub-Overlay"
        set uuid d3328fe2-45b5-51ef-9fda-d34f7b593c8a
        set srcintf "port5"
        set dstintf "HUB1" "HUB2"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end

branch1_fgt # show firewall policy 4
config firewall policy
    edit 4
        set name "From Hub-Overlay"
        set uuid dce1cee0-45b5-51ef-d4e3-d8cb3f99da93
        set srcintf "HUB1" "HUB2"
        set dstintf "port5"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

The **Corp** SD-WAN rule can now steer traffic through dc1_fgt and dc2_fgt.

Members in the HUB1 zone are in SLA target 1 (HUB1_HC#1).

Members in the HUB2 zone are in SLA target 2 (HUB2_HC#1).

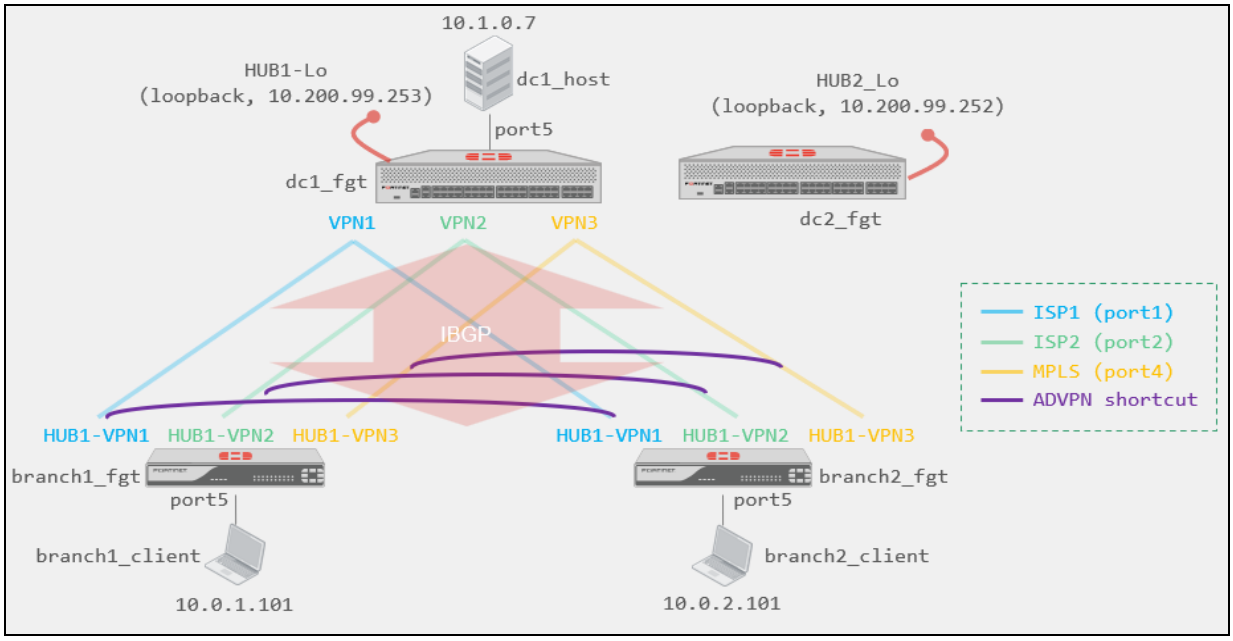
Because of the interface configuration order and the cost that is assigned to the overlay interfaces, the branches steer traffic through dc1_fgt in priority.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 9: ADVPN

In this lab, first you will review and update the auto-discovery VPN (ADVPN) configuration that you applied using the SD-WAN overlay template in the previous lab. This ADVPN configuration allows the devices to negotiate shortcuts between the branches. Next, you will test the behavior of the shortcut tunnel on the hub-and-spoke topology shown in the following diagram:



Note that IPsec tunnels and IBGP routing are established between the branches and the second hub, dc2_fgt, but are not represented in this diagram.

Objectives

- Configure ADVPN
- Monitor the establishment of the ADVPN tunnel

Time to Complete

Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Configuring ADVPN

In this exercise, you will review and update the ADVPN configuration that you applied using the SD-WAN overlay template in the previous lab. By enabling the **Auto-Discovery VPN** option, FortiManager applied BGP for route reflection and IPsec templates with ADVPN to allow shortcut tunnels.

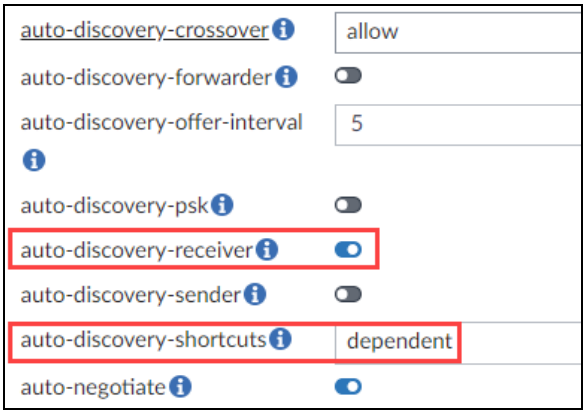
Configure Basic ADVPN

You will use FortiManager to review the ADVPN configuration that the SD-WAN overlay template applied.

To review the ADVPN settings on the IPsec templates

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **Device Manager** > **Provisioning Templates**, and then click **IPsec Tunnel**.
3. Double-click **Corp-SOT_BRANCH_IPsec** to edit it.
4. Select one tunnel, and then click **Edit**.
5. Expand the **Advanced Options** section.
6. Review the following settings required for ADVPN:

Field	Value
add-route	Disabled
auto-discovery-receiver	Enabled
auto-discovery-shortcuts	dependent
net-device	Enabled



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

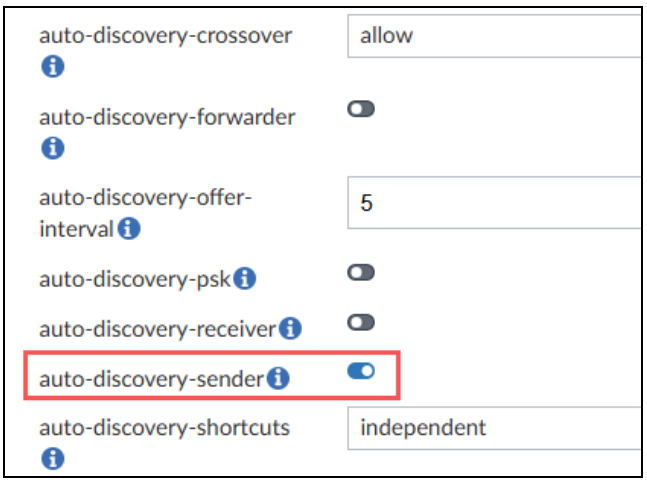
In the configuration of IPsec phase 1, the `net-device` and `auto-discovery-receiver` settings are enabled on each overlay. The first setting is required for ADVPN to work on the spokes. The second setting configures FortiGate to signal the hub that the device can negotiate shortcuts.

The `auto-discovery-shortcuts` setting is set to `dependent` to bring down shortcut tunnels if the parent tunnel goes down.

The `add-route` setting is set to `disable` so the tunnel will not create static routes and use dynamic routing instead.

7. Click **Cancel** to exit the tunnel definition.
   FortiManager configured the settings related to ADVPN for each tunnel definition on the branches in the same way.
8. Click **Cancel** to exit the template definition.
9. Double-click **Corp-SOT_HUB1_IPsec** to open it.
10. Select one tunnel, and then click **Edit**.
11. Expand the **Advanced Options** section.
12. Review the following settings required for ADVPN:

Field	Value
add-route	Disabled
auto-discovery-receiver	Disabled
auto-discovery-sender	Enabled
net-device	Disabled



FortiManager configured the settings related to ADVPN for each tunnel definition on each hub in the same way.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

In the configuration of IPsec phase 1, the `net-device` setting is disabled, and the `auto-discovery-sender` setting is enabled on each overlay. The first setting is required for ADVPN to work on hubs, and the second setting configures FortiGate to facilitate shortcut negotiation between spokes.

13. Click **Cancel** to exit the tunnel definition.
14. Click **Cancel** to exit the template definition.

Prevent Cross Overlay Shortcuts

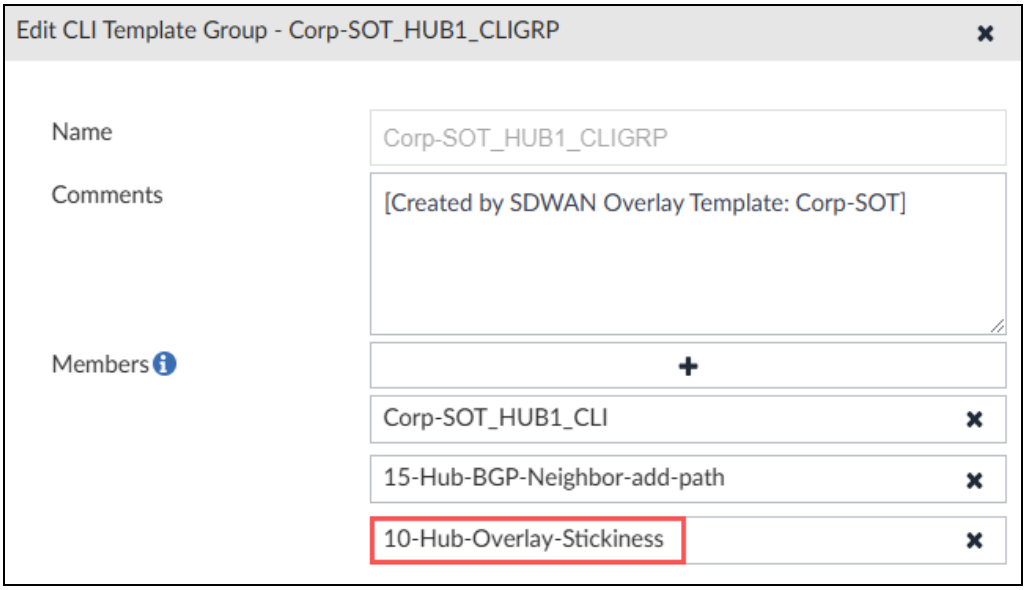
By default, FortiGate can establish shortcuts between every available overlay. This can lead to invalid shortcuts. For example, traffic will not be able to reach its destination if FortiGate establishes a shortcut between a multiprotocol label switching (MPLS) interface and an Ethernet interface. To prevent cross overlay shortcut establishment, you will configure overlay stickiness using policy routes.

To configure overlay stickiness

1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates**, and then click **CLI**.
2. Double-click **10-Hub-Overlay Stickiness**, and then examine the CLI template.

There are three policy routes, one for each overlay. Each policy route instructs FortiGate to keep the traffic within the overlay.

3. Click **Cancel**.
4. Edit the **Corp-SOT_HUB1_CLIGRP** CLI template group.
5. In the **Members** field, click **+**, and then add the **10-Hub-Overlay Stickiness** CLI template.
6. Do *not* remove the CLI templates that are already applied to the hub.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

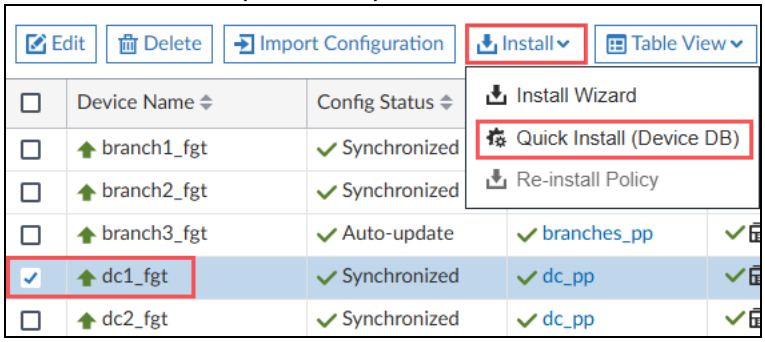
7. Click **OK**.
8. Repeat steps 4–7 to add the **10-Hub-Overlay Stickiness** CLI template to **Corp-SOT_HUB2_CLIGRP**.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Select **Install Device Settings (only)**, and then click **Next**.
3. Select **dc1_fgt**, and **dc2_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on all devices.
5. Wait for the installation to complete, and then click **Finish**.

If FortiManager didn't install the configuration changes on one hub, or if you want to force the reinstallation of the database configuration to a device, you can perform the following steps:

1. Click **Device Manager** > **Device & Groups**.
2. Select a device, and then click the installation icon.
3. Select **Quick Install (Device DB)**.



4. Click **OK** confirm the installation of the configuration.
5. Wait for the installation to complete and then click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Monitoring ADVPN Tunnels

In this exercise, first you will test and monitor the establishment of ADVPN tunnels. Next, you will refine the configuration to set an ADVPN idle timeout.

Monitor ADVPN Tunnels

First, you will test the establishment of ADVPN tunnels by sending ping traffic from the device located on branch1_fgt LAN (branch1_client) to the device located behind branch2_fgt. You will monitor the traffic and the establishment of shortcut tunnels. Next, you will monitor the tunnels and the behavior of the shortcut tunnels when the performance of some links degrades.

To test the establishment of ADVPN tunnels

1. Open an SSH session to branch1_fgt, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Enter the following commands:

```
get ipsec tunnel list
diagnose sys sdwan service4 3
get router info routing-table details 10.0.2.101
get router info routing-table details 10.0.3.101
```

   Your output should be similar to the following example:

```
branch1_fgt # get ipsec tunnel list
NAME=HUB1-VPN1 REMOTE-GW=100.64.1.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=42446

NAME=HUB1-VPN2 REMOTE-GW=100.64.1.9:0
        P2NAME=HUB1-VPN2 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=42448

NAME=HUB1-VPN3 REMOTE-GW=172.16.1.5:0
        P2NAME=HUB1-VPN3 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=42447

NAME=HUB2-VPN1 REMOTE-GW=100.64.1.3:0
        P2NAME=HUB2-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=36558

NAME=HUB2-VPN2 REMOTE-GW=100.64.1.11:0
        P2NAME=HUB2-VPN2 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=36554

NAME=HUB2-VPN3 REMOTE-GW=172.16.1.1:0
        P2NAME=HUB2-VPN3 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=36554
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # diag sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(6):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    4: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    5: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    6: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
branch1_fgt # get router info routing-table details 10.0.2.101

Routing table for VRF=0
Routing entry for 10.0.2.0/24
  Known via "bgp", distance 200, metric 0, best
  Last update 00:12:38 ago
  * vrf 0 192.168.1.2 priority 1 (recursive is directly connected, HUB1-VPN1)
  * vrf 0 192.168.1.34 priority 1 (recursive is directly connected, HUB1-VPN2)
  * vrf 0 192.168.1.66 priority 1 (recursive is directly connected, HUB1-VPN3)
  * vrf 0 192.168.1.2 priority 1 (recursive is directly connected, HUB1-VPN1)
  * vrf 0 192.168.1.34 priority 1 (recursive is directly connected, HUB1-VPN2)
  * vrf 0 192.168.1.66 priority 1 (recursive is directly connected, HUB1-VPN3)
  * vrf 0 192.168.1.2 priority 1 (recursive is directly connected, HUB1-VPN1)
  * vrf 0 192.168.1.34 priority 1 (recursive is directly connected, HUB1-VPN2)
  * vrf 0 192.168.1.66 priority 1 (recursive is directly connected, HUB1-VPN3)
  * vrf 0 192.168.1.130 priority 1 (recursive is directly connected, HUB2-VPN1)
  * vrf 0 192.168.1.162 priority 1 (recursive is directly connected, HUB2-VPN2)
  * vrf 0 192.168.1.193 priority 1 (recursive is directly connected, HUB2-VPN3)
  * vrf 0 192.168.1.130 priority 1 (recursive is directly connected, HUB2-VPN1)
  * vrf 0 192.168.1.162 priority 1 (recursive is directly connected, HUB2-VPN2)
  * vrf 0 192.168.1.193 priority 1 (recursive is directly connected, HUB2-VPN3)
  * vrf 0 192.168.1.130 priority 1 (recursive is directly connected, HUB2-VPN1)
  * vrf 0 192.168.1.162 priority 1 (recursive is directly connected, HUB2-VPN2)
  * vrf 0 192.168.1.193 priority 1 (recursive is directly connected, HUB2-VPN3)
```

The six overlay IPsec tunnels are up.

HUB1-VPN1 is the preferred member, followed by HUB1-VPN2, HUB1-VPN3, and then the three members that connect to dc2_fgt (HUB2).

The best routes to `10.0.2.101` and to `10.0.3.101` are any of the 18 paths through the overlays.

3. Continuing in the branch1_fgt SSH session, enter the following command to capture ping traffic to branch2_client:
   `diagnose sniffer packet any "host 10.0.2.101 and icmp" 4`

4. Open two SSH sessions to branch1_client, and then log in with the following credentials:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

- Username: `root`
- Password: `password`

5. In the first SSH session, ping `10.0.2.101`, and after a few seconds press `ctrl+C` to stop the ping.

Stop and think!

The time to live (TTL) is 61 for the first ping and 62 for subsequent pings. Why?

```
root@branch1-client-cli:~# ping 10.0.2.101
PING 10.0.2.101 (10.0.2.101) 56(84) bytes of data.
64 bytes from 10.0.2.101: icmp_seq=1 ttl=61 time=2.48 ms
64 bytes from 10.0.2.101: icmp_seq=2 ttl=62 time=1.06 ms
64 bytes from 10.0.2.101: icmp_seq=3 ttl=62 time=1.23 ms
64 bytes from 10.0.2.101: icmp_seq=4 ttl=62 time=1.73 ms
```

The TTL changes from 61 to 62 when branch1_fgt establishes the shortcut. Before the shortcut is established, the traffic goes through the hub. When the shortcut between the two branches is established, traffic goes through the shortcut, resulting in one less step for the ICMP packets.

6. In the first SSH session, restart the ping to `10.0.2.101`, and then leave the ping running.
7. In the second SSH session, ping `10.0.3.101`, and then leave the ping running.
8. In the branch1_fgt SSH session, examine the sniffer output.

```
branch1_fgt # diagnose sniffer packet any "host 10.0.2.101 and icmp" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.2.101 and icmp]
28.906370 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
28.906575 HUB1-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
28.909890 HUB1-VPN1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
28.909936 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
29.907583 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
29.907650 HUB1-VPN1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
29.910034 HUB1-VPN1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
29.910062 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

The packets are initially routed through the `HUB1-VPN1` overlay, the parent tunnel, and then through the shortcut (`HUB1-VPN1_0`).

9. In the branch1_fgt SSH session, stop the sniffer, and then enter the following commands:

```
get ipsec tunnel list
diagnose sys sdwan service4 3
get router info routing-table details 10.0.2.101
get router info routing-table details 10.0.3.101
```

Your output should be similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # get ipsec tunnel list
NAME=HUB1-VPN1_0 REMOTE-GW=203.0.113.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=192.168.1.1/192.168.1.1 PROXY-ID-DESTINATION=192.168.1.2/192.1
68.1.2 STATUS=up TIMEOUT=43053
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=43056

NAME=HUB1-VPN1_1 REMOTE-GW=100.64.33.1:4500
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=192.168.1.1/192.168.1.1 PROXY-ID-DESTINATION=192.168.1.3/192.1
68.1.3 STATUS=up TIMEOUT=43088
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=43085

NAME=HUB1-VPN1 REMOTE-GW=100.64.1.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=34886

NAME=HUB1-VPN2 REMOTE-GW=100.64.1.9:0
        P2NAME=HUB1-VPN2 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=34888

NAME=HUB1-VPN3 REMOTE-GW=172.16.1.5:0
        P2NAME=HUB1-VPN3 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=34888

NAME=HUB2-VPN1 REMOTE-GW=100.64.1.3:0
        P2NAME=HUB2-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=34856
```

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(11), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Member sub interface(8):
    3: seq_num(4), interface(HUB1-VPN1):
       1: HUB1-VPN1_0(30)
       2: HUB1-VPN1_1(31)
  Members(8):
    1: Seq_num(4 HUB1-VPN1_1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(4 HUB1-VPN1_0 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    4: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    5: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    6: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    7: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    8: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # get router info routing-table details 10.0.2.101

Routing table for VRF=0
Routing entry for 10.0.2.0/24
  Known via "bgp", distance 200, metric 0, best
  Last update 00:08:41 ago
  * vrf 0 192.168.1.2 priority 1 (recursive is directly connected, HUB1-VPN1_0)
  * vrf 0 192.168.1.34 priority 1 (recursive is directly connected, HUB1-VPN2)
  * vrf 0 192.168.1.66 priority 1 (recursive is directly connected, HUB1-VPN3)
  * vrf 0 192.168.1.2 priority 1 (recursive is directly connected, HUB1-VPN1_0)
  * vrf 0 192.168.1.34 priority 1 (recursive is directly connected, HUB1-VPN2)
  * vrf 0 192.168.1.66 priority 1 (recursive is directly connected, HUB1-VPN3)
  * vrf 0 192.168.1.2 priority 1 (recursive is directly connected, HUB1-VPN1_0)
  * vrf 0 192.168.1.34 priority 1 (recursive is directly connected, HUB1-VPN2)
  * vrf 0 192.168.1.66 priority 1 (recursive is directly connected, HUB1-VPN3)
  * vrf 0 192.168.1.130 priority 1 (recursive is directly connected, HUB2-VPN1)
  * vrf 0 192.168.1.162 priority 1 (recursive is directly connected, HUB2-VPN2)
  * vrf 0 192.168.1.193 priority 1 (recursive is directly connected, HUB2-VPN3)
  * vrf 0 192.168.1.130 priority 1 (recursive is directly connected, HUB2-VPN1)
  * vrf 0 192.168.1.162 priority 1 (recursive is directly connected, HUB2-VPN2)
  * vrf 0 192.168.1.193 priority 1 (recursive is directly connected, HUB2-VPN3)
  * vrf 0 192.168.1.130 priority 1 (recursive is directly connected, HUB2-VPN1)
  * vrf 0 192.168.1.162 priority 1 (recursive is directly connected, HUB2-VPN2)
  * vrf 0 192.168.1.193 priority 1 (recursive is directly connected, HUB2-VPN3)
```

The shortcuts to branch2_fgt and to branch3_fgt appear in the IPsec tunnel list.

The shortcuts are listed in the rule status, and placed at the top of the outgoing interface list. That is, the shortcuts are the preferred members.

The shortcuts replace the parent tunnel as the best route to 10.0.2.101 and 10.0.3.101.

10. On the second SSH session to branch1_client, stop the ping to 10.0.3.101.
    Now you will concentrate on the shortcut between branch1_fgt and branch2_fgt.

To test the behvior of ADVPN when link performance degrades

1. In the branch1_fgt SSH session, restart the sniffer command:
   `diagnose sniffer packet any "host 10.0.2.101 and icmp" 4`
2. On the WAN simulator page, increase the delay on **BR1-ISP1** to 110 ms, so the overlay doesn't meet the SLA target to HUB1.

You increased the latency on the traffic forwarded to branch1_fgt over HUB1-VPN1, specifically in the network segment between branch1_fgt and ISP1. The latency between ISP1 and dc1_fgt is not impacted.

3. In the branch1_fgt SSH session, examine the sniffer output.
   Your output should be similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
36.910858 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
36.910882 HUB1-VPN1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
37.023050 HUB1-VPN1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
37.023075 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
37.910918 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
37.910955 HUB1-VPN2 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
37.913994 HUB1-VPN2 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
37.914007 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
38.912194 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
38.912260 HUB1-VPN2_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
38.914084 HUB1-VPN2_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
38.914097 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

The traffic is initially routed to the HUB1-VPN1_0 shortcut.

Because of a service-level agreement (SLA) change, the traffic fails over to HUB1-VPN2. You may see an intermediate failover to HUB1-VPN1, the parent tunnel. This depends on how quickly FortiGate detects the SLA change on the parent tunnel.

Remember that in the previous exercise, you configured overlay stickiness on the hub. So, a tunnel change also occurs for the traffic between the hub and branch2_fgt.

Finally, the traffic fails over to another shortcut (HUB1-VPN2_0), which is negotiated over HUB1-VPN2.

4. In the branch1_fgt SSH session, stop the sniffer, and then check the rule status again.

Your output should be similar to the following example:

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(15), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Member sub interface(9):
    2: seq_num(5), interface(HUB1-VPN2):
       1: HUB1-VPN2_0(32)
    9: seq_num(4), interface(HUB1-VPN1):
       1: HUB1-VPN1_0(30)
       2: HUB1-VPN1_1(31)
  Members(9):
    1: Seq_num(5 HUB1-VPN2_0 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    4: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    5: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    6: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
    7: Seq_num(4 HUB1-VPN1_0 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    8: Seq_num(4 HUB1-VPN1_1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    9: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

The new shortcut (HUB1-VPN2_0) is listed in the rule status, and placed at the top of the outgoing interface list. That is, the new shortcut is now the preferred member.

The HUB1-VPN1_0 and HUB1-VPN1_1 shortcuts and their parent tunnel don't meet any SLA targets, and therefore, are placed at the bottom of the outgoing interface list.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

5. In the branch1_fgt SSH session, restart the sniffer command.
6. On the WAN simulator page, increase the delay on **BR1-ISP2** to 110 ms, so the overlay doesn't meet the SLA target to HUB1.
7. Examine the sniffer output.

   You will see similar behavior to what you saw in the previous test:

   - The traffic is initially routed to the HUB1-VPN2_0 shortcut.
   - Because of an SLA change, the traffic may fail over to the parent tunnel, but then it fails over to HUB1-VPN3.
   - Finally, the traffic fails over to another shortcut (HUB1-VPN3_0), which is negotiated over HUB1-VPN3.

```
135.869768 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
135.869792 HUB1-VPN2_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
135.981928 HUB1-VPN2_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
135.981940 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
136.870979 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
136.871034 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
136.873028 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
136.873054 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
137.871967 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
137.872104 HUB1-VPN3_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
137.873307 HUB1-VPN3_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
137.873322 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

8. In the branch1_fgt SSH session, stop the sniffer, and then check the IPsec tunnel list again.

   Your output should be similar to the following example:

```
branch1_fgt # get ipsec tunnel list
NAME=HUB1-VPN1_0 REMOTE-GW=203.0.113.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=192.168.1.1/192.168.1.1 PROXY-ID-DESTINATION=192.168.1.2/192.1
68.1.2 STATUS=up TIMEOUT=42626
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=42629

NAME=HUB1-VPN1_1 REMOTE-GW=100.64.33.1:4500
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=192.168.1.1/192.168.1.1 PROXY-ID-DESTINATION=192.168.1.3/192.1
68.1.3 STATUS=up TIMEOUT=42661
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=42658

NAME=HUB1-VPN2_0 REMOTE-GW=203.0.113.9:0
        P2NAME=HUB1-VPN2 PROXY-ID-SOURCE=192.168.1.33/192.168.1.33 PROXY-ID-DESTINATION=192.168.1.34/19
2.168.1.34 STATUS=up TIMEOUT=42960
        P2NAME=HUB1-VPN2 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=42958

NAME=HUB1-VPN3_0 REMOTE-GW=172.16.0.9:0
        P2NAME=HUB1-VPN3 PROXY-ID-SOURCE=192.168.1.65/192.168.1.65 PROXY-ID-DESTINATION=192.168.1.66/19
2.168.1.66 STATUS=up TIMEOUT=43131
        P2NAME=HUB1-VPN3 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=43134

NAME=HUB1-VPN1 REMOTE-GW=100.64.1.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STATUS=up
 TIMEOUT=34459
--More--
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Three shortcuts are negotiated to branch2_fgt, one for each overlay, but only one is currently used.

The lifetime of the shortcuts is inherited from the parent IPsec settings (default is 43200 seconds). That is, idle shortcuts remain up until they reach the lifetime.

In the next task, to save system resources, you will configure an idle timeout for the shortcuts.

9. In the branch1_fgt SSH session, restart the sniffer command.
10. On the WAN simulator page, increase the delay on **BR1-MPLS** to 110 ms, so the overlay doesn't meet the SLA target to HUB1.
11. Examine the sniffer output.

    You will see similar behavior to what you saw in the previous test:

    - The traffic is initially routed to the HUB1-VPN3_0 shortcut.
    - Due to an SLA change, the traffic fails over to HUB2-VPN1.
    - Finally, the traffic fails over to another shortcut (HUB2-VPN1_0), which is negotiated over HUB2-VPN1.

```
9.056713 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
9.056737 HUB1-VPN3_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
9.167951 HUB1-VPN3_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
9.167988 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
10.057386 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
10.057456 HUB2-VPN1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
10.171253 HUB2-VPN1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
10.171288 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
11.057496 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
11.057592 HUB2-VPN1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
12.077352 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
12.077365 HUB2-VPN1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
12.188837 HUB2-VPN1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
12.188863 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

12. In the branch1_fgt SSH session, stop the sniffer, and then check the rule status again.

    Your output should be similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(64), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Member sub interface(11):
    2: seq_num(7), interface(HUB2-VPN1):
       1: HUB2-VPN1_0(44)
    7: seq_num(4), interface(HUB1-VPN1):
       1: HUB1-VPN1_0(40)
       2: HUB1-VPN1_1(41)
    9: seq_num(5), interface(HUB1-VPN2):
       1: HUB1-VPN2_0(42)
    11: seq_num(6), interface(HUB1-VPN3):
       1: HUB1-VPN3_0(43)
  Members(11):
    1: Seq_num(7 HUB2-VPN1_0 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    2: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    3: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    4: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
    5: Seq_num(4 HUB1-VPN1_1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    6: Seq_num(4 HUB1-VPN1_0 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    7: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    8: Seq_num(5 HUB1-VPN2_0 HUB1), alive, sla(0x0), gid(0), cfg_order(1), local cost(0), selected
    9: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(1), local cost(0), selected
    10: Seq_num(6 HUB1-VPN3_0 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local cost(0), selected
    11: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

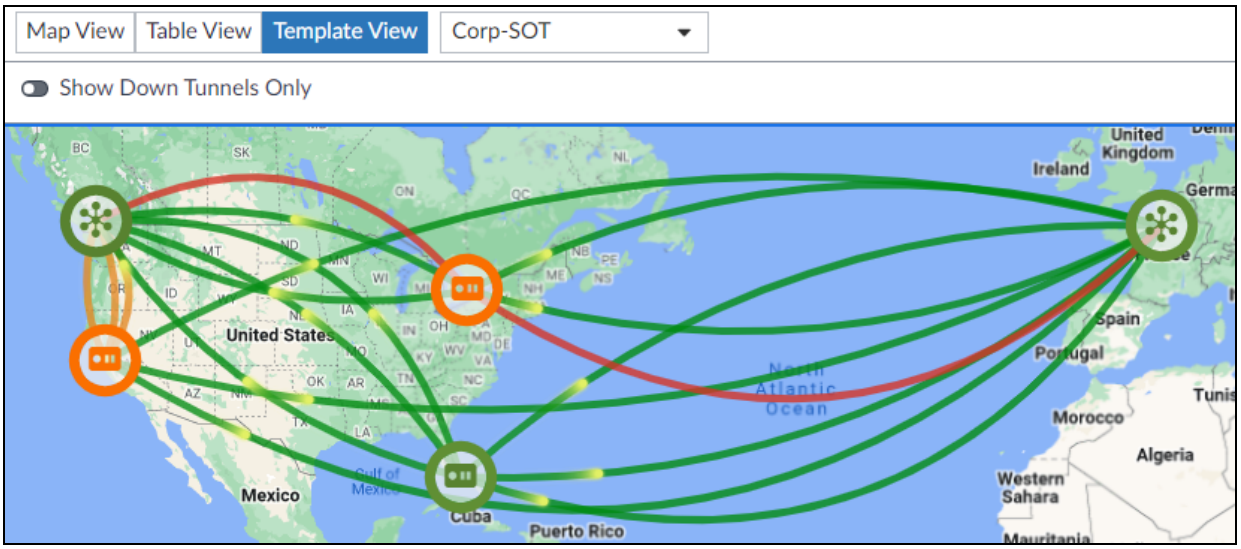
All tunnels and shortcut tunnels through HUB1 do not meet the SLA targets (sla (0x0)).

The HUB2-VPN1_0 shortcut and its parent tunnel, HUB2-VPN1, meet one SLA target, and therefore are placed at the top of the outgoing interface list.

13. Connect to the FortiManager GUI, and then log in with the following credentials:
    - Username: `admin`
    - Password: `password`
14. Click **Device Manager** > **Monitor**, and then select **SD-WAN Monitor** > **Template View**.
    Your page should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



The tunnel between branch1_fgt and dc1_fgt are out of SLA and appear in orange on the map. The tunnels between branch1_fgt and dc2_fgt remain green because they meet their assigned SLA targets.

Remember that the port4 interface of branch3_fgt is connected but did not receive an IP address. So, it is expected that the third tunnel for branch3_fgt is down.

15. Click **Device Manager** > **Monitor**, and then select **VPN Monitor** > **Show Table**.
Your page should be similar to the following example:

Device	Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
branch1_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	2.7 MB	913.5 KB	HUB1-VPN1	HUB1-VPN1
branch1_fgt[root]	HUB1-VPN1_0	dialup	203.0.113.1	Branch2	127.3 KB	127.3 KB	HUB1-VPN1_0	HUB1-VPN1
branch1_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	2.7 MB	912.6 KB	HUB1-VPN2	HUB1-VPN2
branch1_fgt[root]	HUB1-VPN2_0	dialup	203.0.113.9	Branch2	121.9 KB	121.9 KB	HUB1-VPN2_0	HUB1-VPN2
branch1_fgt[root]	HUB1-VPN3	automatic	172.16.1.5	172.16.1.5	2.7 MB	913.2 KB	HUB1-VPN3	HUB1-VPN3
branch1_fgt[root]	HUB1-VPN3_0	dialup	172.16.0.9	Branch2	117.6 KB	117.6 KB	HUB1-VPN3_0	HUB1-VPN3
branch1_fgt[root]	HUB2-VPN1	automatic	100.64.1.3	100.64.1.3	127.6 KB	127.2 KB	HUB2-VPN1	HUB2-VPN1
branch1_fgt[root]	HUB2-VPN1_0	dialup	203.0.113.1	Branch2	85.5 KB	85.5 KB	HUB2-VPN1_0	HUB2-VPN1
branch1_fgt[root]	HUB2-VPN2	automatic	100.64.1.11	100.64.1.11	127.5 KB	127.1 KB	HUB2-VPN2	HUB2-VPN2
branch1_fgt[root]	HUB2-VPN3	automatic	172.16.1.1	172.16.1.1	127.5 KB	127.0 KB	HUB2-VPN3	HUB2-VPN3
branch2_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	100.64.1.1	126.8 MB	41.0 MB	HUB1-VPN1	HUB1-VPN1
branch2_fgt[root]	HUB1-VPN1_0	dialup	192.2.0.1	Branch1	127.3 KB	127.3 KB	HUB1-VPN1_0	HUB1-VPN1
branch2_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	100.64.1.9	126.8 MB	41.0 MB	HUB1-VPN2	HUB1-VPN2
branch2_fgt[root]	HUB1-VPN2_0	dialup	192.2.0.9	Branch1	121.9 KB	122.0 KB	HUB1-VPN2_0	HUB1-VPN2

FortiManager lists the shortcut tunnels with one entry in each direction.

The example above highlights the shortcut that was established between branch1_fgt and branch2_fgt over the port1 interfaces.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

16. On the WAN simulator page, reduce the delay on **BR1-ISP1**, **BR1-ISP2**, and **BR1-MPLS** back to 0 ms.
17. Continuing in the branch1_fgt SSH session, check the rule status again.
    Your output should be similar to the following example:

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(12), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Member sub interface(10):
    2: seq_num(4), interface(HUB1-VPN1):
       1: HUB1-VPN1_0(30)
    4: seq_num(5), interface(HUB1-VPN2):
       1: HUB1-VPN2_0(31)
    6: seq_num(6), interface(HUB1-VPN3):
       1: HUB1-VPN3_0(32)
    8: seq_num(7), interface(HUB2-VPN1):
       1: HUB2-VPN1_0(33)
  Members(10):
    1: Seq_num(4 HUB1-VPN1_0 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2_0 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    4: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    5: Seq_num(6 HUB1-VPN3_0 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    6: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    7: Seq_num(7 HUB2-VPN1_0 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    8: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    9: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    10: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

18. In the branch1_fgt SSH session, restart the sniffer command, and then confirm that the traffic flows through the HUB1-VPN1_0 shortcut tunnel.
19. In the branch1_fgt SSH session, stop the sniffer.
20. In the branch1_client SSH session, stop the ping.

Check VPN Log Messages

In the FortiGate event logs, you will display event logs related to ADVPN shortcuts and master tunnels.

To check VPN log messages

1. Continuing in the branch1_fgt SSH session, enter the following commands to filter ADVPN shortcut log messages and review them:

```
execute log filter device memory
execute log filter category event
execute log filter field advpnsc 1
execute log display
```

Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # exec log display
60 logs found.
10 logs returned.
58.2% of logs has been searched.

1: date=2024-08-28 time=06:41:36 eventtime=1724852495384762361 tz="-0700"
logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" log
desc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunne
l-stats" remip=203.0.113.1 locip=192.2.0.1 remport=500 locport=500 outintf
="port1" srccountry="Reserved" cookies="2419d2248bcd6b4e/21a344af34e0e9e3"
 user="Branch2" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A"
 assignip=N/A vpntunnel="HUB2-VPN1 0" tunnelip=0.0.0.0 tunnelid=2336136538
 tunneltype="ipsec" duration=13756 sentbyte=3289196 rcvdbyte=3289196 nexts
tat=600 fctuid="N/A" advpnsc=1

2: date=2024-08-28 time=06:41:36 eventtime=1724852495384668985 tz="-0700"
logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" log
desc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunne
l-stats" remip=172.16.0.9 locip=172.16.0.1 remport=500 locport=500 outintf
="port4" srccountry="Reserved" cookies="f6ed97ceb58537ca/21d614f47a9a2903"
 user="Branch2" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A"
 assignip=N/A vpntunnel="HUB1-VPN3 0" tunnelip=0.0.0.0 tunnelid=2336136536
 tunneltype="ipsec" duration=13770 sentbyte=4403492 rcvdbyte=4403492 nexts
tat=600 fctuid="N/A" advpnsc=1

3: date=2024-08-28 time=06:41:36 eventtime=1724852495384643628 tz="-0700"
logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" log
desc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunne
l-stats" remip=203.0.113.9 locip=192.2.0.9 remport=500 locport=500 outintf
="port2" srccountry="Reserved" cookies="f5845cf8c796d4a2/9dcf177766ee2db1"
 user="Branch2" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A"
 assignip=N/A vpntunnel="HUB1-VPN2 0" tunnelip=0.0.0.0 tunnelid=2336136518
 tunneltype="ipsec" duration=13784 sentbyte=4408048 rcvdbyte=4408048 nexts
tat=600 fctuid="N/A" advpnsc=1
```

FortiGate displays only log messages that are related to the shortcut tunnels.

2. Enter the following commands to update the filter and display VPN logs that are related to master tunnels:

```
execute log filter field advpnsc 0
execute log display
```

Your output should look similar to the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
branch1_fgt # exec log filter field advpnsc 0

branch1_fgt # exec log display
24 logs found.
10 logs returned.
15.7% of logs has been searched.

1: date=2024-08-28 time=06:41:36 eventtime=1724852495384511739 tz="-0700"
logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" log
desc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunne
l-stats" remip=172.16.1.1 locip=172.16.0.1 remport=500 locport=500 outintf
="port4" srccountry="Reserved" cookies="7013d338d5e6847b/a61f90a892e4b31e"
 user="172.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N
/A" assignip=192.168.1.194 vpntunnel="HUB2-VPN3" tunnelip=N/A tunnelid=233
6136512 tunneltype="ipsec" duration=14967 sentbyte=1232271 rcvdbyte=123277
7 nextstat=600 fctuid="N/A" advpnsc=0

2: date=2024-08-28 time=06:41:36 eventtime=1724852495384488992 tz="-0700"
logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" log
desc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunne
l-stats" remip=172.16.1.5 locip=172.16.0.1 remport=500 locport=500 outintf
="port4" srccountry="Reserved" cookies="87828c6ad8f8256a/2477f54f4846369d"
 user="172.16.1.5" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N
/A" assignip=192.168.1.65 vpntunnel="HUB1-VPN3" tunnelip=N/A tunnelid=2336
136527 tunneltype="ipsec" duration=14968 sentbyte=9039996 rcvdbyte=2792580
5 nextstat=600 fctuid="N/A" advpnsc=0
```

3. Enter the following command to reset the log filter:
   `execute log filter reset`
4. Enter the following commands to clear the shortcuts:
   ```
   diagnose vpn ike gateway clear name HUB1-VPN1_0
   diagnose vpn ike gateway clear name HUB1-VPN2_0
   diagnose vpn ike gateway clear name HUB1-VPN3_0
   diagnose vpn ike gateway clear name HUB2-VPN1_0
   ```
5. Check the IPsec tunnel list to confirm that all the shortcuts were cleared.

Configure an Idle Timeout for ADVPN

You will configure an idle timeout for ADVPN to save system resources.

To configure an idle timeout for ADVPN

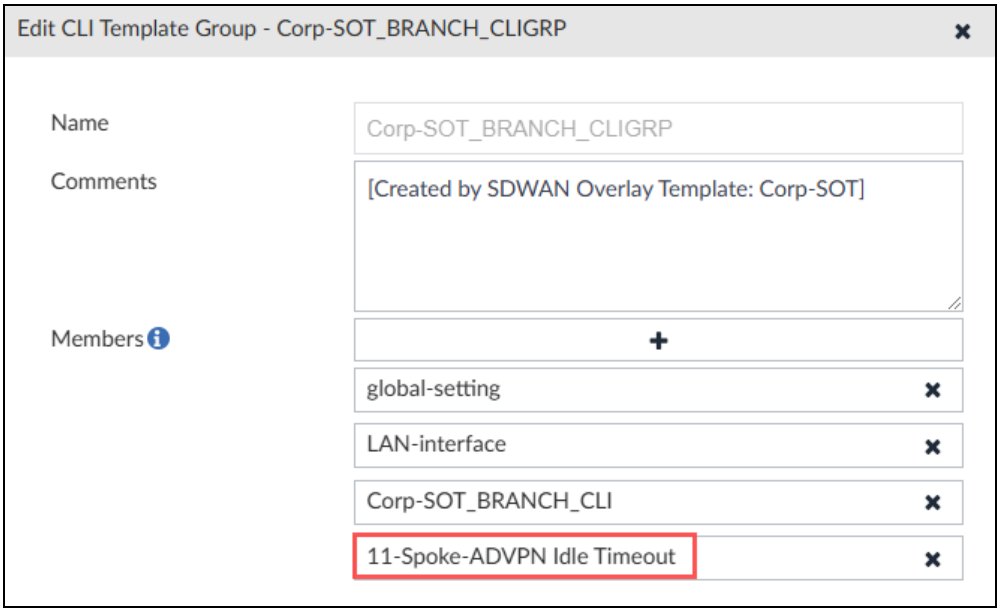
1. Continuing on the FortiManager GUI, click **Device Manager** > **Provisioning Templates** > **CLI**.
2. Double-click **11-Spoke-ADVPN Idle Timeout** to view the CLI template settings.
3. Examine the CLI template.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

In the IPsec phase 1 configuration, each overlay has the `idle-timeout` setting enabled and the `idle-timeoutinterval` setting set to `5` minutes.

4. Click **Cancel** to exit the CLI template.
5. Double-click the **Corp-SOT_BRANCH_CLIGRP** CLI template group to edit its settings.
6. In the **Members** list, add **11-Spoke-ADVPN Idle Timeout**.



7. Click **OK** to save the settings.
8. Install the device settings on the branch devices.
9. In the branch1_client SSH session, ping `10.0.2.101`, and then leave the ping running.
10. In the branch1_fgt SSH session, verify that the shortcut over HUB1-VPN1 was negotiated.
    Your output should look similar to the following example:

```
branch1_fgt # get ipsec tunnel list
NAME=HUB1-VPN1_0 REMOTE-GW=203.0.113.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=192.168.1.1/192.168.1.1 PROXY-ID-DESTINATION=192.168.1.2/
192.168.1.2 STATUS=up TIMEOUT=43128
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STAT
US=up TIMEOUT=43123

NAME=HUB1-VPN1 REMOTE-GW=100.64.1.1:0
        P2NAME=HUB1-VPN1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 STAT
US=up TIMEOUT=39426
```

The shortcut appears in the IPsec list. The timeout value displayed with this command remains close to 43200.

11. In the branch1_fgt SSH session, enter the following commands to enable debug for the IKE process:
    `diagnose debug application ike -1`

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
diagnose debug console timestamp enable
diagnose debug enable
```

12. In the branch1_client SSH session, stop the ping.
13. Wait 5 minutes.

Take the Expert Challenge!

Review the log messages related to the establishment of the ADVPN shortcuts on FortiAnalyzer. Use the filter to display shortcut-related messages only.

If you require assistance, or to verify your work, use the step-by-step instructions that follow: To filter ADVPN log messages on FortiAnalyzer on page 270.

After you complete the challenge, review the debug putput on the branch1_fgt SSH session.

14. In the branch1_fgt SSH session, monitor the output.

    After 5 minutes, the debug displays messages indicating that the shortcut timed out, as shown in the following example:

```
branch1_fgt # diag debug enable

branch1_fgt # 2024-09-04 03:30:57.516363 ike :shrank heap by 159744 bytes
2024-09-04 03:35:58.412206 ike V=root:0:HUB1-VPN1_0: connection idle time-out
2024-09-04 03:35:58.416031 ike V=root:0:HUB1-VPN1_0: going to be deleted
2024-09-04 03:35:58.419545 ike V=root:0:HUB1-VPN1_0: flushing
2024-09-04 03:35:58.422609 ike V=root:0:HUB1-VPN1_0: deleting IPsec SA with SPI 5dd83b48
2024-09-04 03:35:58.426204 ike V=root:0:HUB1-VPN1_0:HUB1-VPN1: deleted IPsec SA with SPI 5dd83b48,
 SA count: 0
2024-09-04 03:35:58.430373 ike V=root:0:HUB1-VPN1_0: sending SNMP tunnel DOWN trap for HUB1-VPN1
2024-09-04 03:35:58.435335 ike V=root:0:HUB1-VPN1_0:HUB1-VPN1: delete
2024-09-04 03:35:58.438743 ike V=root:0:HUB1-VPN1_0: deleting IPsec SA with SPI 5dd83b47
2024-09-04 03:35:58.442771 ike V=root:0:HUB1-VPN1_0:HUB1-VPN1: deleted IPsec SA with SPI 5dd83b47,
 SA count: 0
2024-09-04 03:35:58.447307 ike V=root:0:HUB1-VPN1_0: sending SNMP tunnel DOWN trap for HUB1-VPN1
2024-09-04 03:35:58.451776 ike V=root:0:HUB1-VPN1_0:HUB1-VPN1: delete
2024-09-04 03:35:58.454861 ike V=root:0:HUB1-VPN1_0: flushed
```

Stop and think!

FortiGate monitors the shortcut using ping. The ping probes are sent to the address of the remote end over the shortcut. Therefore, the shortcut is not really idle. Why did it time out?

FortiGate does not consider health check probes to be user traffic. Therefore, health check probes don't prevent a shortcut from timing out.

15. In the branch1_fgt SSH session, enter the following commands to stop the debug and check the tunnel list:

```
diagnose debug disable
diagnose debug reset
get ipsec tunnel list
```

16. Confirm that you see the six tunnels to the hubs but no shortcuts.

To filter ADVPN log messages on FortiAnalyzer

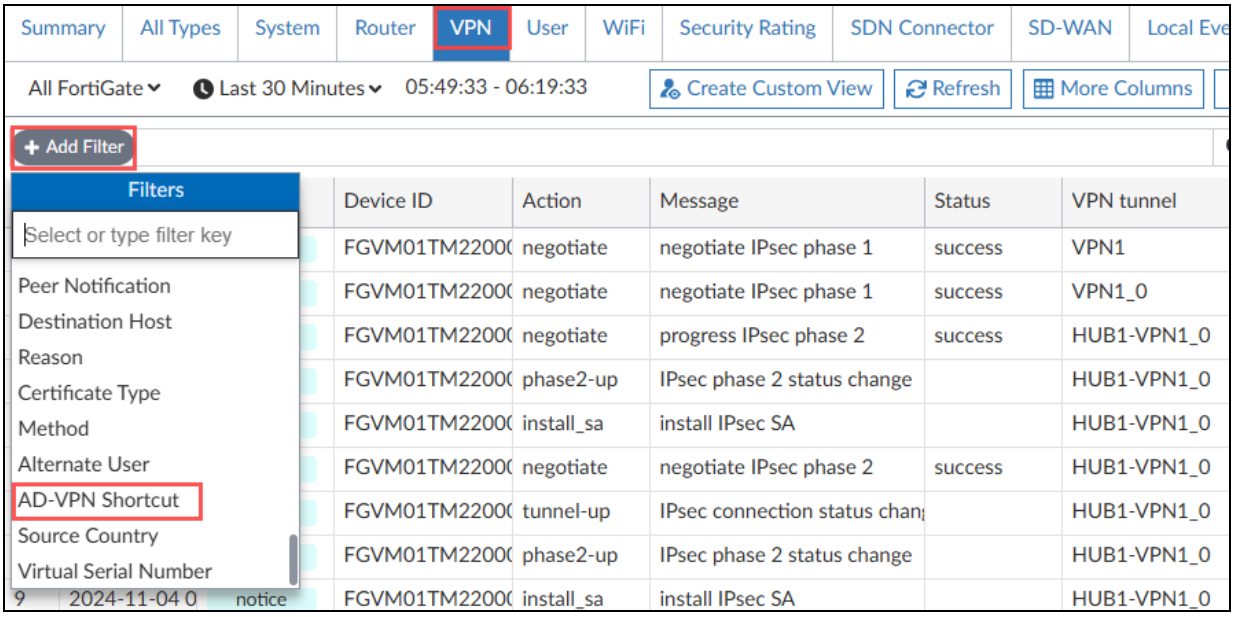
1. Continuing on the FortiManager GUI, click **Log View** > **Event** > **VPN**.

   The page displays logs related to VPN tunnels and VPN tunnel shortcuts.

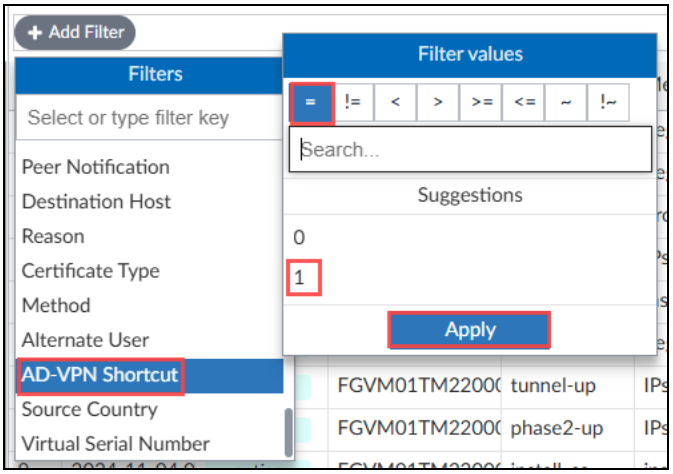
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

2. Click **Add Filter**.
3. Select **AD-VPN Shortcut**.

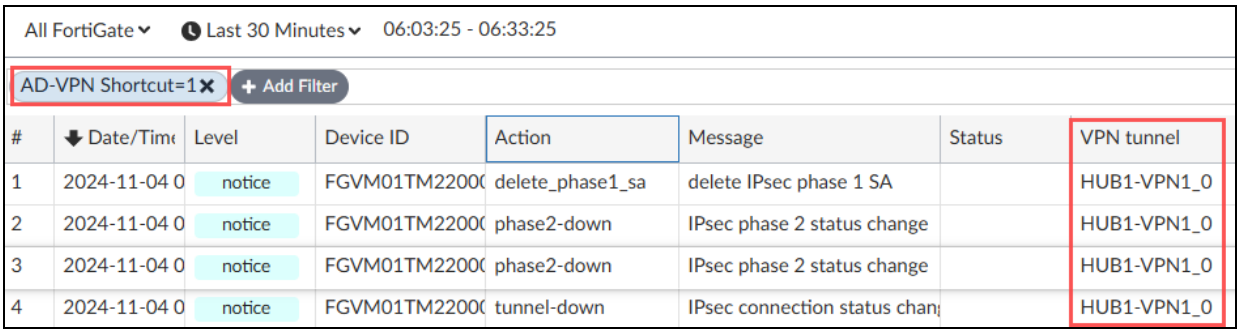


4. Click **=**, and then select **1** to display log messages related to ADVPN shortcuts only.



5. Click **Apply**.

   Your page should look similar to the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Lab 10: SD-WAN Troubleshooting

In this lab, you will put the concepts that you learned into practice by troubleshooting the following SD-WAN deployments:

- Spoke-to-spoke traffic (single hub)
- Direct internet access (DIA) traffic
- SD-WAN rules on a hub-and-spoke topology with DIA, remote internet access (RIA), and site-to-site traffic

In each exercise, you will load the required configuration, troubleshoot the issues reported, identify the root cause, and fix the issues.

You will configure the FortiManager to be offline because you will not use it in this lab. You will access the FortiGate devices directly to troubleshoot and fix the issues described.

Objectives

- Troubleshoot static routing in an SD-WAN context
- Troubleshoot routing issues in SD-WAN
- Troubleshoot session reevaluation in SD-WAN
- Troubleshoot SD-WAN rules

Time to Complete

Estimated: 120 minutes

Prerequisites

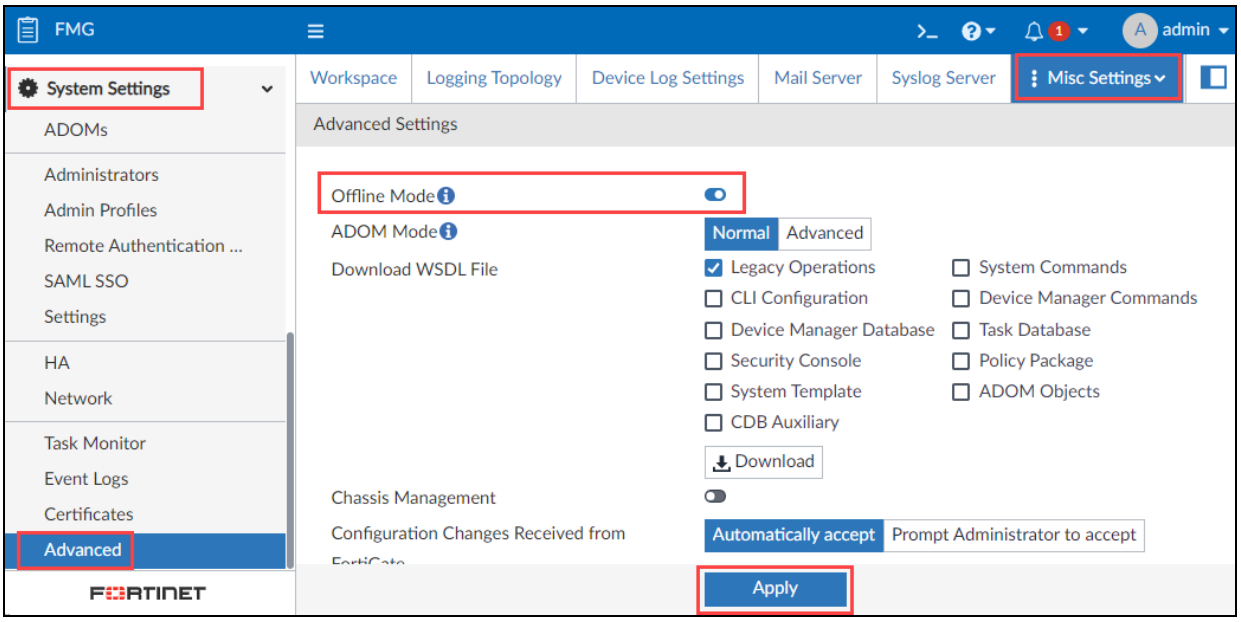
Before you begin this lab, you must configure FortiManager to be offline, and restore a configuration file to the branch1_fgt, branch2_fgt, and dc1_fgt FortiGate devices.

To configure FortiManager to be offline

1. Connect to the FortiManager GUI, and then log in with the following credentials:
   - Username: `admin`
   - Password: `password`
2. Click **System Settings** > **Advanced**, and then click **Misc Settings**.
3. Enable **Offline Mode**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

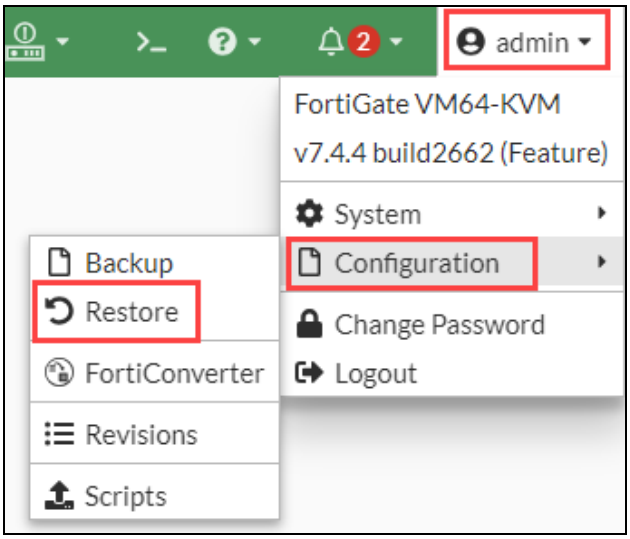
DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



4. Click **Apply**.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the Local-Client VM, open a browser, and then log in to the branch1_fgt GUI with the following credentials:
   - Username: `admin`
   - Password: `password`
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-10** > **Exercise-1**, select the `lab10-ex1-branch1_fgt_7-4-4_initial.conf` file, and then click **Open**.
6. Click **OK**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt and dc1_fgt.
   Use the following configuration files:

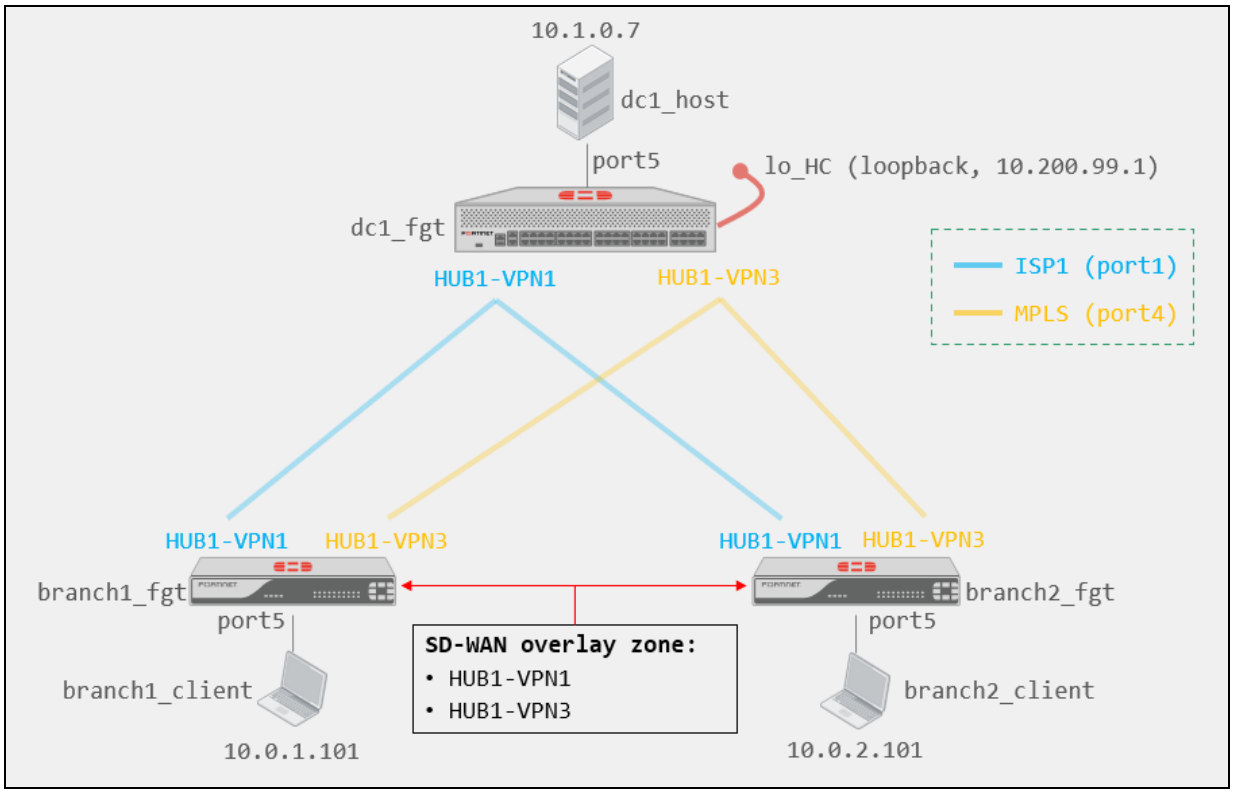
Device	Configuration file
branch2_fgt	lab10-ex1-branch2_fgt_7-4-4_initial.conf
dc1_fgt	lab10-ex1-dc1_fgt_7-4-4_initial.conf

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 1: Troubleshooting Spoke-to-Spoke Traffic (Single Hub)

In this lab, you will troubleshoot spoke-to-spoke traffic in the following preconfigured topology:



Configuration

This is a hub-and-spoke deployment with two overlays. The overlays are used to route traffic between the spokes.

Problem Description

When the administrator generates traffic from branch1_client to branch2_client, the traffic is always routed over HUB1-VPN3 (MPLS link). However, the MPLS link is expensive, and therefore, the administrator wants to use HUB1-VPN3 for spoke-to-spoke traffic only when HUB1-VPN1 goes down. That is:

1. branch1_fgt must use HUB1-VPN1 as the primary member to route traffic to branch2_fgt.
2. branch1_fgt must use HUB1-VPN3 to route traffic to branch2_fgt only if HUB1-VPN1 is detected to be down.
3. After HUB1-VPN1 recovers, spoke-to-spoke traffic must be routed through HUB1-VPN1 again.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Objective

To complete this exercise, you must fix all the issues described.

Solution Requirements

- Focus on branch1_fgt only. Don't make changes on any other device in the network.
- On branch1_fgt, don't change the existing SD-WAN rule configuration. Spoke-to-spoke traffic must match SD-WAN rule ID 3. You can change other parts of the configuration.
- To optimize the branch1_fgt configuration, static routes and firewall policies must reference SD-WAN zones and not the individual members.
- To fix all issues reported, you must perform multiple configuration changes.

Tips for Troubleshooting

- Remember the key routing principles of SD-WAN.
- To simulate spoke-to-spoke traffic, ping branch2_client (`10.0.2.101`) from branch1_client (`10.0.1.101`).
- To simulate link failover and recovery, bring BR1-ISP1 down and back up again on the WAN simulator.
- Use debug flow to determine how FortiGate processes packets to branch2_client.

```
diagnose debug flow filter addr 10.0.2.101
diagnose debug flow filter proto 1
diagnose debug flow trace start 100
diagnose debug console timestamp enable
diagnose debug enable
```

- Use the sniffer to capture ingress and egress packets.

```
diagnose sniffer packet any "host 10.0.2.101 and icmp" 4 0 l
```

- View session details to verify the matching SD-WAN rule and firewall policy.

```
diagnose sys session filter dst 10.0.2.101
diagnose sys session filter proto 1
diagnose sys session list
```

- Check the routing table using the following command:

```
get router info routing-table all
```

- Check the SD-WAN configuration using the following commands:

```
show system sdwan
diagnose sys sdwan zone
diagnose sys sdwan member
diagnose firewall proute list
diagnose ip proute match <dst> <src> <link> <proto> <dport>
diagnose sys sdwan service4 3
diagnose sys sdwan health-check status Corp_HC
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Remember to bring BR1-ISP1 back up when you finish the exercise.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Solution

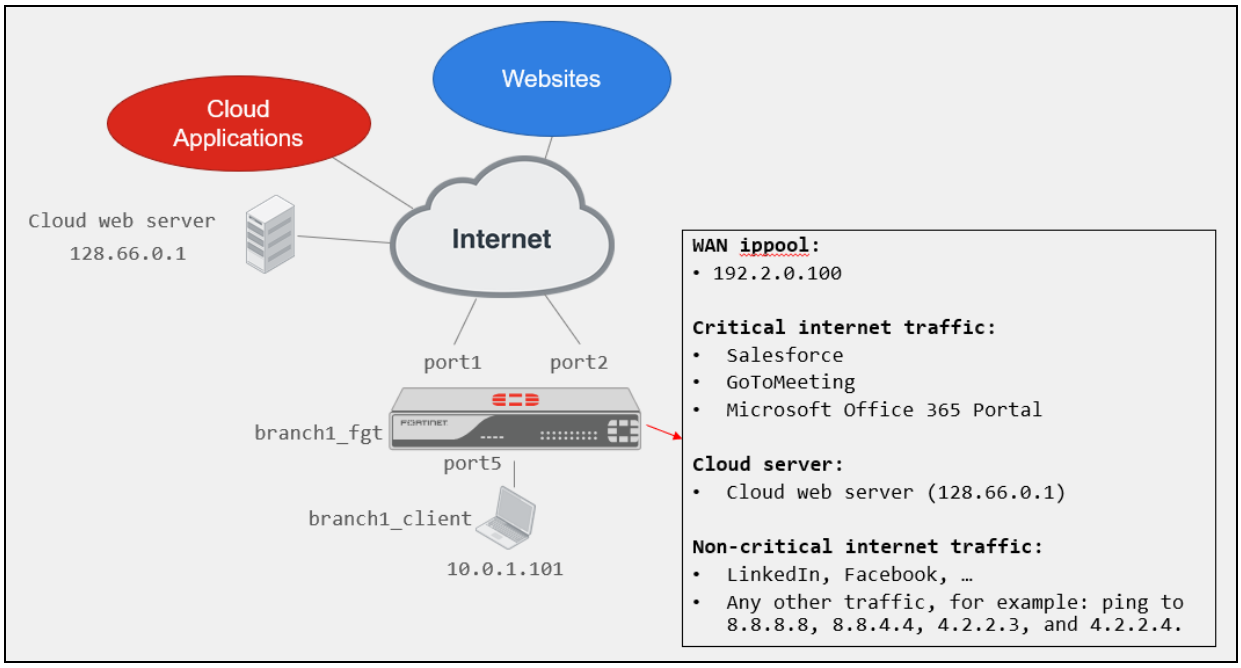
If you require assistance with this exercise, see the *Solution Slides* lesson in the *Study Guide*.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 2: Troubleshooting DIA Traffic

In this lab, you will troubleshoot direct internet access (DIA) traffic in the following preconfigured topology:



Prerequisites

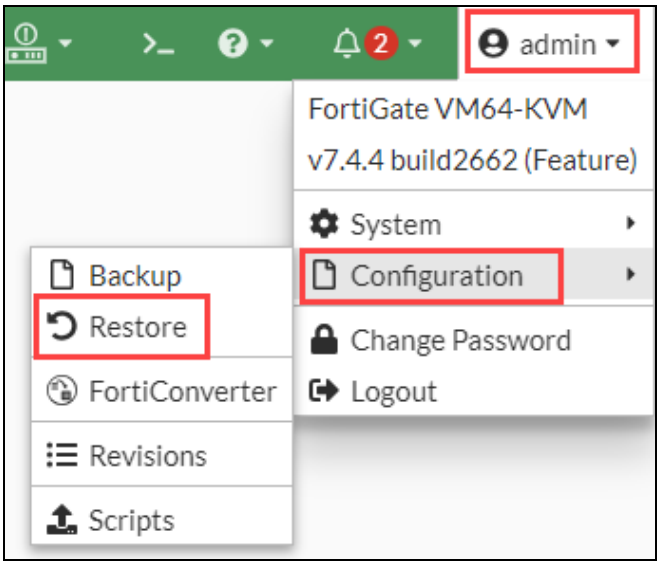
Before you begin this lab, you must restore a configuration file to branch1_fgt.

To restore the branch1_fgt configuration file

1. On the Local-Client VM, open a browser, and then log in to the branch1_fgt GUI with the following credentials:
   - Username: `admin`
   - Password: `password`
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-10** > **Exercise-2**, select the `lab10-ex2-branch1_fgt_7-4-4-initial.conf` file, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.

Configuration

This is a DIA deployment with two underlays. The underlays are used to route traffic to the internet. SD-WAN rules have been configured to steer traffic for critical applications (GoToMeeting, Salesforce, and the Microsoft Office 365 portal) and the cloud web server (`128.66.0.1`).

Problem Description

The administrator has identified the following issues:

- **Issue 1**: If both port1 and port2 are alive, and the administrator generates internet traffic, critical traffic is routed to port1, which is expected. However, non-critical traffic is load balanced across port1 and port2. The administrator wants port2 to be used only if port1 goes down.
- **Issue 2**: During a failover from port1 to port2 (port1 is dead), existing TCP sessions time out. For example, an SSH connection to the internet web server (`128.66.0.1`) from branch1_client times out during the failover. The administrator wants existing TCP sessions to fail over to port2 successfully and not time out.
- **Issue 3**: After existing sessions fail over to port2 successfully, the administrator wants those sessions to fail back to port1 after port1 recovery.
- **Issue 4**: When port1 is dead, and new sessions are established through port2, the sessions don't fail over to port1 after port1 recovers. Instead, the sessions continue using port2. The administrator wants these sessions to fail over to port1.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Objective

To complete this lab, you must fix all the issues described.

Solution Requirements

- Focus on branch1_fgt only. Don't make changes on any other device in the network.
- On branch1_fgt, don't change the existing SD-WAN rule configuration. You can change other parts of the configuration.
- Internet traffic must be SNATed with IP pool `192.2.0.100`.
- To fix all issues reported, you must perform multiple configuration changes.

Tips for Troubleshooting

- Remember the SNAT conditions for session reevaluation.
- You can also generate internet traffic by pinging any of the following addresses: `4.2.2.3`, `4.2.2.4`, `8.8.8.8`, and `8.8.4.4`. You can then view the traffic logs to identify how traffic is being routed.
- To simulate failover and failback of existing sessions, you can initially establish an SSH connection to the internet web server (`128.66.0.1`) by running the `ssh 128.66.0.1` command from branch1_client. Then, log in using the username `root` and password `password`. The SSH session should remain up (it should continue to respond to user commands) during failover and failback. If the SSH session becomes unresponsive, it is an indication that the session timed out.
- To simulate link failure and recovery, bring BR1-ISP1 down and back up again on the WAN simulator.
- Use debug flow to know how packets are processed.

```
diagnose debug flow filter addr <target-addr>
diagnose debug flow trace start 100
diagnose debug console timestamp enable
diagnose debug enable
```

- Use the sniffer to capture ingress and egress packets.

```
diagnose sniffer packet any "host <target-addr>" 4 0 l
```

- View session details to verify the matching SD-WAN rule and firewall policy.

```
diagnose sys session filter dst <target-addr>
diagnose sys session list
```

- Check the routing table using the following command:

```
get router info routing-table all
```

- Check the system configuration.

```
show system sdwan
show firewall policy
show system interface
diagnose sys sdwan zone
diagnose sys sdwan member
diagnose sys sdwan service4
diagnose sys sdwan health-check status Corp_HC
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Remember to bring BR1-ISP1 back up when you finish the exercise. Also, remember to stop any traffic generation on branch1_client by pressing `Ctrl+C` in the SSH session.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Solution

If you require assistance with this exercise, see the *Solution Slides* lesson in the *Study Guide*.

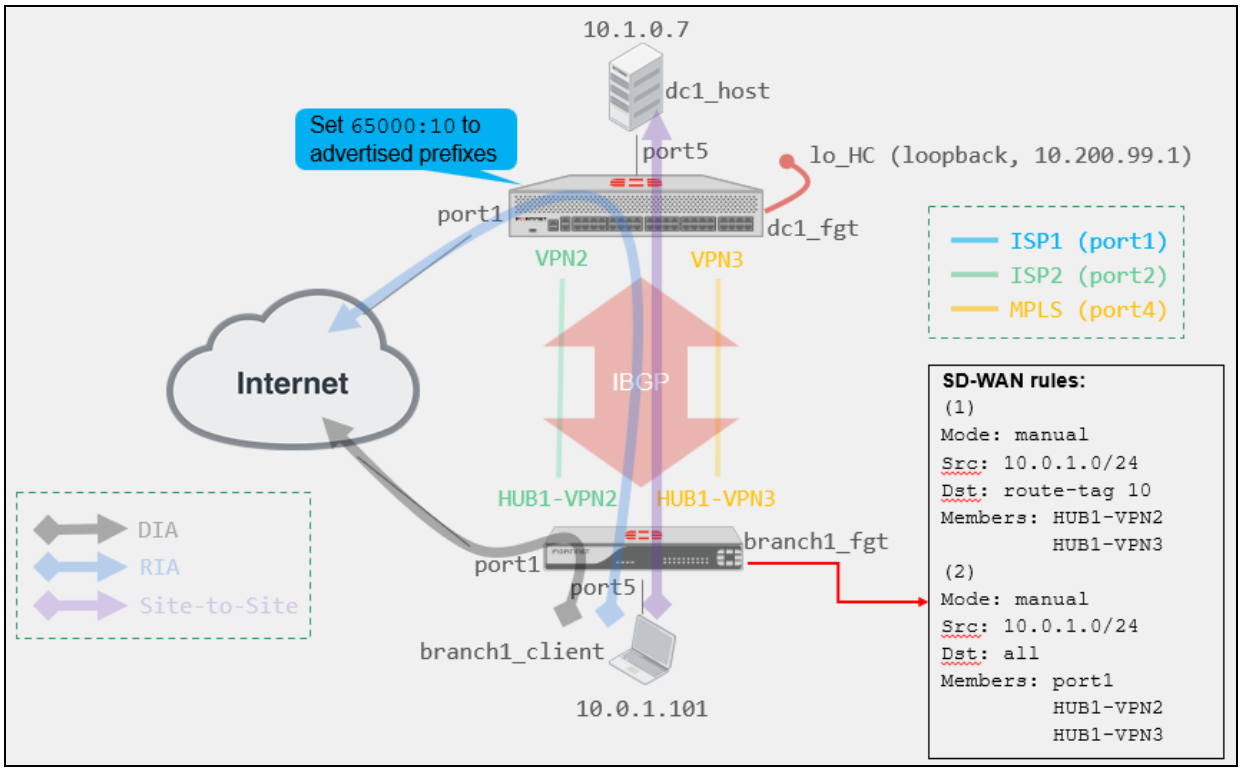
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Exercise 3: Troubleshooting Rules

In this exercise, you will troubleshoot SD-WAN rules used for steering DIA, RIA, and site-to-site traffic.

The following topology has been preconfigured for you:



Prerequisites

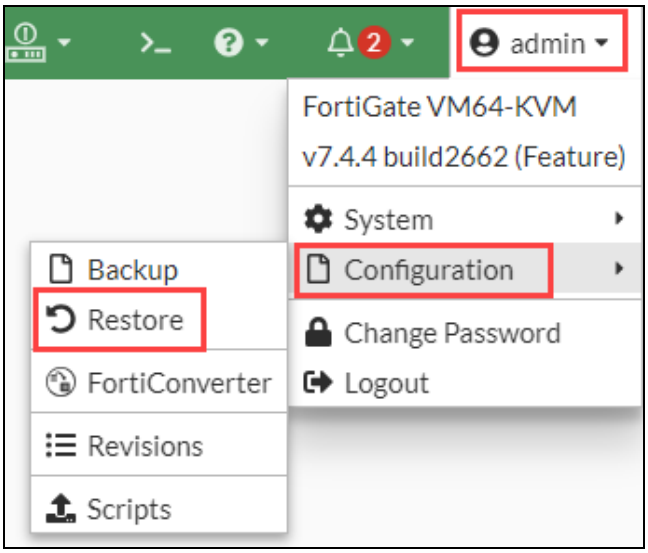
Before you begin this lab, you must restore a configuration file to branch1_fgt, branch2_fgt, and dc1_fgt. Note that although you must restore a configuration file to branch2_fgt, you will not be using branch2_fgt in this exercise.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the Local-Client VM, open a browser, and then log in to the branch1_fgt GUI with the following credentials:
   - Username: `admin`
   - Password: `password`
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-10** > **Exercise-3**, select `lab10-ex3-branch1_fgt_7-4-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt and dc1_fgt.
   Use the following configuration files:

Device	Configuration file
branch2_fgt	lab10-ex3-branch2_fgt_7-4-4_initial.conf
dc1_fgt	lab10-ex3-dc1_fgt_7-4-4_initial.conf

Configuration

This is a hub-and-spoke deployment with one underlay (port1) and two overlays (HUB1-VPN2 and HUB1-VPN3). port2 and HUB1-VPN1 are configured but are not used for steering traffic. There are rules configured to steer DIA, RIA, and site-to-site traffic.

IBGP is used for exchanging routing information between the sites. On dc1_fgt, the administrator assigned the community `65000:10` to advertised prefixes. On branch1_fgt, the administrator assigned prefixes that match the `65000:10` community a route tag of `10`.

Problem Description

The administrator has identified the following issue:

- **Issue 1**: The administrator configured SD-WAN rule 2 to steer DIA and RIA traffic. When port1 is up, internet traffic must be routed through port1 (DIA). When port1 is down, internet traffic must fail over to the overlays (RIA).

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

However, when port1 is down, branch1_fgt drops internet traffic.

- **Issue 2**: The administrator configured SD-WAN rule 1 in manual mode. However, the administrator wants branch1_fgt to prefer the member with the best route to the destination. This way, the administrator can control the member preference by advertising, from dc1_fgt, a better route over its preferred overlay, and without having to change the configuration on the branch.

Objective

To complete this lab, you must fix all the issues described.

Solution Requirements

- Unless otherwise stated, focus on branch1_fgt only. Don't make changes on any other device in the network.
- On branch1_fgt, do *not* change the existing IPsec or firewall policy configuration. You can change the SD-WAN rule settings, except the mode in use and the member and zone preference lists. You can add a new static route but you cannot modify the existing routes.

Tips for Troubleshooting

- Remember the SD-WAN rule lookup process.
- To test DIA and RIA traffic, you can ping, from the branch client, any of the following addresses: `4.2.2.3`, `4.2.2.4`, `8.8.8.8`, and `8.8.4.4`. To test site-to-site traffic, you can ping the dc1_host (`10.1.0.7`).
- To simulate link failure on port1, bring BR1-ISP1 down using the WAN simulator.
- Use the `debug flow` commands to determine how packets are processed.

```
diagnose debug flow filter addr <target-addr>
diagnose debug flow trace start 100
diagnose debug console timestamp enable
diagnose debug enable
```

- Use the `sniffer` command to capture ingress and egress packets.

```
diagnose sniffer packet any "host <target-addr>" 4 0 l
```

- View session details to verify the matching SD-WAN rule and firewall policy.

```
diagnose sys session filter dst <target-addr>
diagnose sys session list
```

- Check routing information using the following commands:

```
get router info routing-table all
get router info bgp community 65000:10
show router bgp
show router route-map
show router community-list
```

- Check the system configuration using the following commands:

```
show system sdwan
show firewall policy
show system interface
diagnose sys sdwan zone
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com


```
diagnose sys sdwan member
diagnose sys sdwan service4
diagnose firewall proute list
diagnose sys sdwan health-check status Corp_HC
diagnose sys sdwan health-check status HUB1_HC
```

- To confirm that rule 1 prefers the member with the best route (issue 3), enter the following commands on dc1_fgt to advertise a prefix for `10.1.0.7/32` over VPN3:

```
config router bgp
   config neighbor-group
      edit VPN3
         set route-map-out prefer-dc1_host
      next
   end
end
execute router clear bgp all soft
```

Do *not* make any other changes to dc1_fgt.

Remember to bring BR1-ISP1 back up when you finish the exercise.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

Solution

If you require assistance with this exercise, see the *Solutions* lesson in the *Study Guide*.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Visit us: Brave-Dumps.com

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com