

DO NOT REPRINT

© FORTINET



Enterprise Firewall Lab Guide

for FortiOS 7.2

FORTINET®
Training Institute

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.fortiguards.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>



5/5/2023

TABLE OF CONTENTS

Firmware Version	7
Network Topology	8
Lab 1: Network Security Architecture	9
Exercise 1: Integrating the Physical Interface	11
Review ISFW port3 Settings and References	11
Exercise 2: Integrating Interfaces With Legacy SD-WAN (Optional)	14
Integrate the External Interfaces With SD-WAN	14
Lab 2: Hardware Acceleration	16
Lab 3: Security Fabric	17
Exercise 1: Configuring the Security Fabric	20
Configure the Security Fabric on NGFW-1	20
Configure the Security Fabric on DCFW	23
Configure the Security Fabric on ISFW	26
Monitor the FortiTelemetry Connection	27
Exercise 2: Examining the Physical and Logical Topology Views	29
View the Physical Topology	29
View the Logical Topology	30
Exercise 3: Configuring the Automation Stitch, Trigger, and Action	31
Configure the Automation	31
Test the Automation Stitch and View the Email Alert	33
Lab 4: High Availability	37
Exercise 1: Configuring FGSP	39
Network Topology	39
Change the Firewall Rules on Linux Router	39
Configure FGSP and Test Session Synchronization	40
Test Session Synchronization Between NGFW-1 and NGFW-2	41
Exercise 2: Analyzing VRRP Failover	43
Network Topology	43
Verify the VRRP Configuration on NGFW-1 and NGFW-2	43
Test VRRP Link Failover Between NGFW-1 and NGFW-2	44
Enable the VRRP Virtual MAC Address	46
Exercise 3: Configuring a Virtual Cluster	48
Network Topology	48

Verify the HA Status.....	50
Configure VDOM Partitioning.....	51
Exercise 4: Analyzing Traffic Distribution.....	54
Network Topology.....	54
Analyze Traffic Distribution.....	54
Perform a Failover and Analyze the Traffic.....	56
Reset the NGFW-2 Cluster Member to Factory Settings.....	57
Lab 5: Central Management.....	59
Exercise 1: Registering FortiGate Devices on FortiManager.....	62
Register NGFW-1 on FortiManager.....	62
Register DCFW on FortiManager.....	66
Register ISFW on FortiManager.....	66
Check the FortiGate Registrations.....	66
Lab 6: OSPF.....	68
Exercise 1: Configuring OSPF.....	69
Configure OSPF on NGFW-1.....	69
Configure OSPF on DCFW.....	71
Configure OSPF on ISFW.....	71
Check the OSPF Status on NGFW-1.....	71
Check the OSPF Status on DCFW and ISFW.....	73
Check Connectivity.....	73
Exercise 2: Configuring BFD.....	74
Configure BFD on NGFW-1.....	74
Configure BFD on DCFW.....	75
Configure BFD on ISFW.....	75
Test BFD Detection of a Neighbor Failure.....	76
Lab 7: BGP.....	78
Exercise 1: Configuring BGP.....	79
Configure BGP on NGFW-1.....	79
Exercise 2: Configuring Prefix Lists.....	83
Check the Routing.....	83
Create a Prefix List.....	83
Clear the BGP Connections.....	85
Verify the Prefix List.....	85
Exercise 3: Configuring a Loopback Interface as a BGP Source.....	87
Configure a Loopback Interface as a BGP Source on NGFW-1.....	87
Configure BGP on ISFW.....	92
Establish the BGP connection.....	95
Lab 8: FortiGuard and Security Profiles.....	97
Exercise 1: Configuring Web Filtering and Antivirus.....	98
Configure a Web Filter Profile.....	98

Configure an Antivirus Profile.....	99
Apply the Security Profiles.....	99
Install the Policy.....	101
Test the Web Filter.....	102
Exercise 2: Analyzing Web Filtering Traffic.....	103
Network Topology.....	103
Objective.....	103
Analyze the Web Traffic.....	104
Exercise 3: Analyzing Antivirus.....	107
Network Topology.....	107
Objective.....	107
Analyze the FTP Traffic.....	107
Exercise 4: Implementing Application Control in NGFW Policy-Based Mode.....	110
Enable Policy-Based NGFW Mode.....	110
Configure SSL Inspection and Central SNAT Policies.....	111
Configure the Security Policy and Test Application Control.....	112
Lab 9: IPS.....	115
Exercise 1: Configuring IPS.....	116
Configure the IPS Profile.....	116
Apply the IPS Profile.....	117
Install the Policy.....	118
Configure the VIP.....	118
Configure the Firewall Policy.....	119
Install the Policy.....	120
Test the IPS.....	121
Check the Attack Logs.....	121
Check the Attack Statistics.....	122
Exercise 2: Creating IPS Custom Signatures.....	123
Capture and Analyze the Traffic.....	123
Review and Install the IPS Custom Signature.....	126
Test the IPS Custom Signature.....	127
Lab 10: IPsec VPN (IKEv2).....	129
Exercise 1: Using the VPN Manager.....	130
Create a VPN Community.....	130
Add NGFW-1, Spoke-1, and Spoke-2 as Managed Devices.....	132
Install the VPN Configuration.....	138
Configure the Firewall Policies.....	139
Install the Policy Packages.....	144
Check the Status of the VPN Tunnel.....	146
Lab 11: Auto-Discovery VPN.....	148
Exercise 1: Configuring ADVPN and IBGP.....	149

DO NOT REPRINT
© FORTINET

Configure ADVPN and IBGP on NGFW-1.....149

Configure ADVPN and IBGP on the Spokes.....151

Bring Up the Static IPsec Tunnels.....153

Check the BGP Routes 154

Bring Up the On-Demand Tunnel.....155

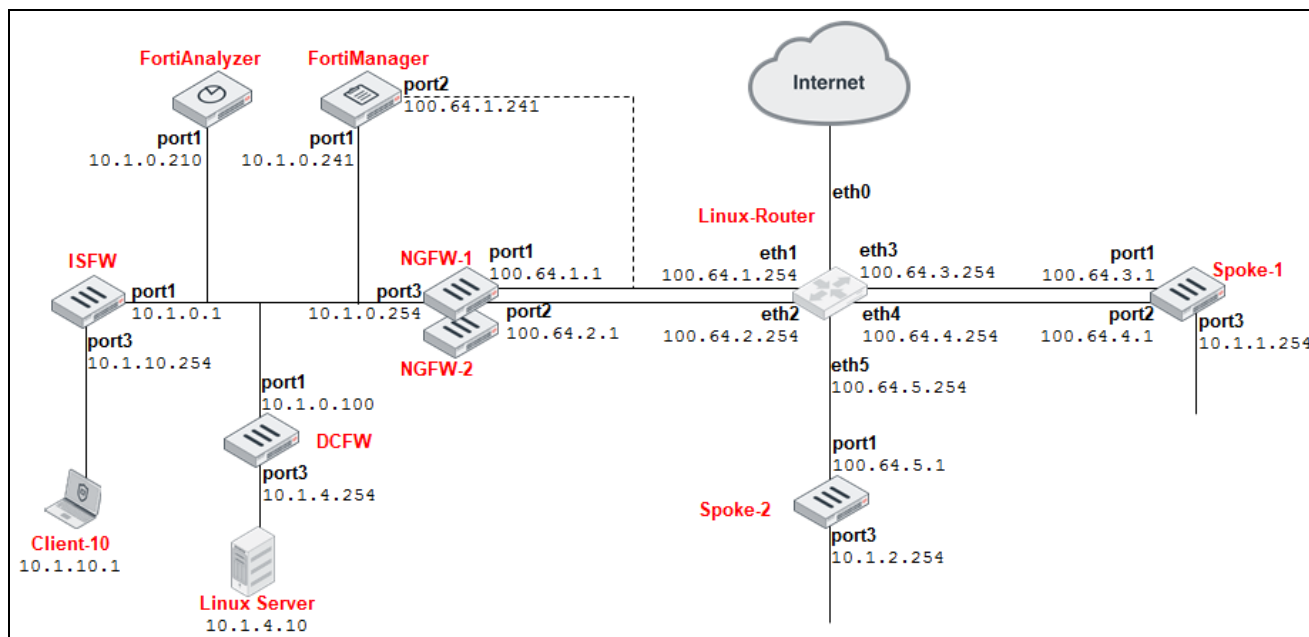
Verify the On-Demand Tunnel.....156

Firmware Version

The Enterprise Firewall course content is based on the following products and firmware versions:

Product	Firmware Version
FortiGate	7.2.4
FortiManager	7.2.2
FortiAnalyzer	7.2.2

Network Topology



Lab 1: Network Security Architecture

In this lab, you will integrate a FortiGate physical interface with another type of interface based on the best practice of segmenting enterprise networks. You will migrate the physical interface settings and references to the target interface.

Objectives

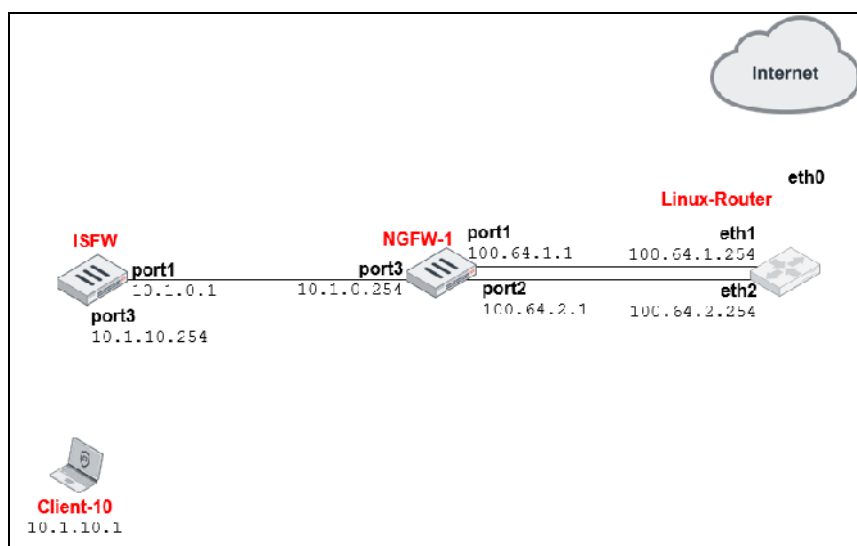
- Integrate port3 on ISFW with a software switch
- Integrate port1 and port2 on NGFW with an SD-WAN virtual interface

Time to Complete

Estimated: 25 minutes

Which Network Segment Will You Work On?

In this lab, you will access ISFW and NGFW.



VM Usernames and Passwords

VM	Username	Password
Client-10	student	password
ISFW	admin	password
DCFW	admin	password

VM	Username	Password
NGFW-1	admin	password
NGFW-2	admin	password
Spoke-1	admin	password
Spoke-2	admin	password
FortiManager	admin	password
FortiAnalyzer	admin	password

Exercise 1: Integrating the Physical Interface

In this exercise, you will integrate the port3 physical interface on ISFW with another type of interface based on the best practice of segmenting the internal enterprise network. You will migrate the interface to a new interface and transfer its configuration, such as IP address and other references to firewall objects, to the new interface.

Review ISFW port3 Settings and References

First, you will review the current interface settings and references of port3 on ISFW. Then, you will integrate port3 with a new software switch and migrate the configuration of port3 to the target interface.

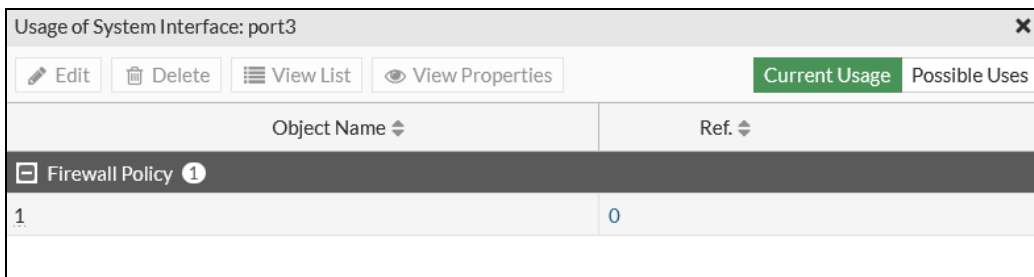
To review port3 network settings

1. Log in to the ISFW GUI with the username `admin` and password `password`.
2. Click **Network > Interfaces**.
3. Double-click **port3** to view the interface configuration.
4. Review the interface settings.

All existing interface settings will move to the target interface.

5. Click **References**.

You should see a list of objects the interface currently references.

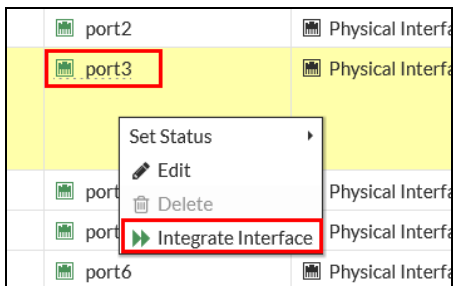


Object Name	Ref.
Firewall Policy 1	
1	0

6. In the upper-right corner, click **X**.
7. Click **Cancel**.

To integrate port3 with a new software switch

1. Continuing on the ISFW GUI, click **Network > Interfaces**.
2. Right-click **port3**, and then click **Integrate Interface** to start the wizard.



3. On the **Select Migration Option** wizard tab, make sure **Migrate to Interface** is selected.
4. Click **Next**.
5. On the **Select/Create interface** wizard tab, select **Create a new Interface**.
6. Enable **Port configuration**.



The configuration of the physical interface overwrites the configuration of the target interface.

7. In the **Name** field, type **LAN**.
8. In the **Type** field, select **Software Switch**.
9. Click **Next**.
10. On the **Review Settings** wizard tab, click **Create**.

Move port3 into an interface

✓ Select Migration Option > ✓ Select/Create Interface > 3 Review Settings > 4 Summary

The following objects will be updated. Object set to 'Replace Instance' will attempt to update occurrences of port3 to LAN.

Name	Object Type	Action
LAN	System Interface	Create New

References

Name	Object Type	Action
1	Firewall Policy	Replace Instance Delete Entry

< Back Create

11. Click **OK** to confirm.
12. Click **Close**.

The new software switch is now created.

Name	Type	Members	IP/Netmask	Administrative Access	Ref.
LAN	Software Switch	port3	10.1.10.254/255.255.255.0	PING HTTPS SSH HTTP	1



Make sure the new software switch **LAN** received the correct IP address and the administrative access settings that were on port3.

Stop and think!

Why did port3 relocate from the list of ISFW physical network interfaces?

The target interface is a software switch and is using port3 as a member interface. Creating a virtual interface on FortiGate requires that at least one interface is a member. Only the virtual interface is configurable. A member cannot be assigned an IP address or administrative access settings.

Exercise 2: Integrating Interfaces With Legacy SD-WAN (Optional)

In this exercise, you will integrate the port1 and port2 physical interfaces on NGFW-1 with the legacy SD-WAN virtual interface based on the best practice of segmenting the edge firewall to steer traffic sourced from the internal network and destined to different cloud applications and websites on the internet.



This exercise is not intended to cover the complete SD-WAN setup and apply all recommended settings. The **Integrate Interface** feature helps to implement networking requirements, such as segmentation, without causing further disruption to FortiGate.

Integrate the External Interfaces With SD-WAN

Take the Expert Challenge!

On the NGFW-1 GUI, enable the default SD-WAN zone, and then integrate port1 and port2 with the SD-WAN zone virtual-wan-link.

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

To enable the SD-WAN zone

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

```
config system sdwan
  set status enable
end
```

The default SD-WAN zone is now enabled and ready to integrate interfaces.

To integrate port1 with the SD-WAN zone

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Network > Interfaces**.
3. Right-click **port1**, and then click **Integrate Interface** to start the wizard.
4. On the **Select Migration Option** wizard tab, select **Migrate to SD-WAN**.
5. In the **Target SD-WAN zone** field, select **virtual-wan-link**.
6. Click **Next**.
7. On the **Review Settings** wizard tab, click **Apply**.
8. Click **OK** to confirm.
9. Click **Close**.

port1 is now part of the SD-WAN zone.

To integrate port2 with the SD-WAN zone

1. Continuing on the NGFW-1 GUI, repeat the previous procedure and integrate port2 with the SD-WAN zone.

Lab 2: Hardware Acceleration

There is no lab associated with this lesson.

Lab 3: Security Fabric

In this lab, you will learn how to configure the Fortinet Security Fabric. After you configure the Security Fabric, you will access the physical and logical topology views. You will also learn how to create a Security Fabric automation stitch, trigger, and action, and view email alerts that the automation stitch generates.

Objectives

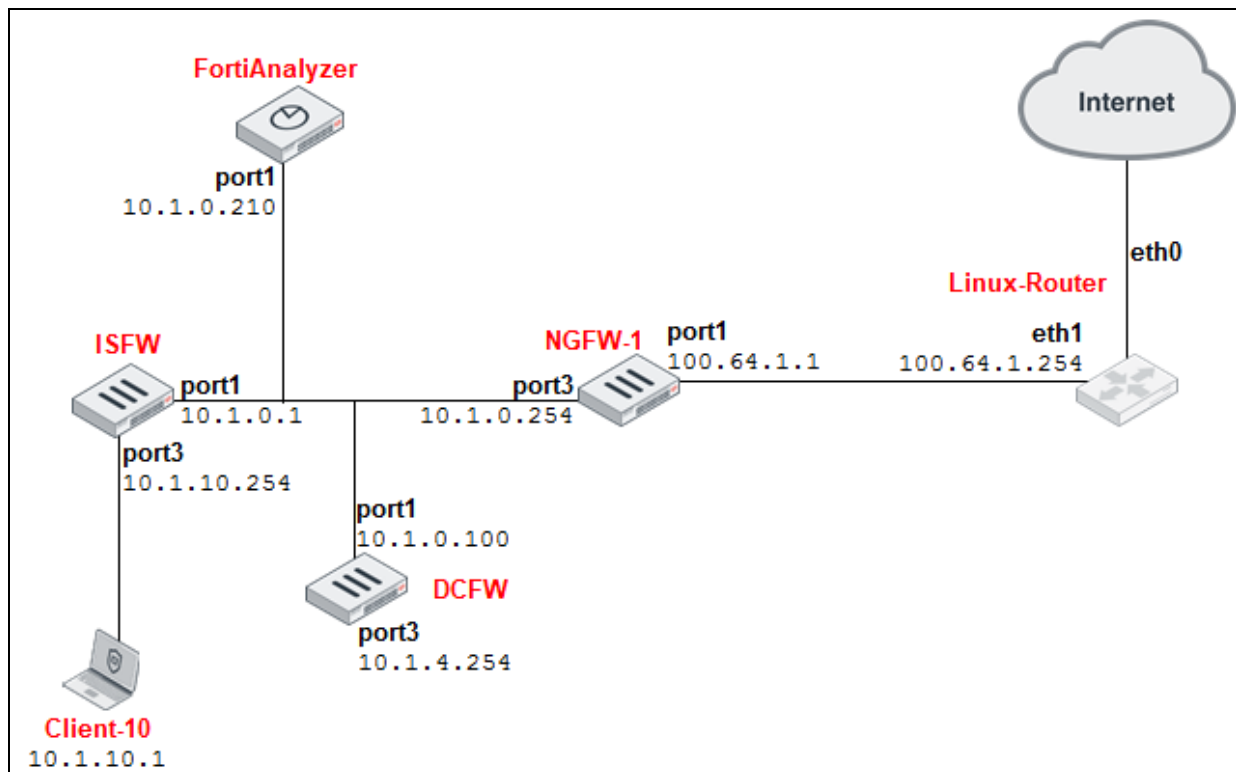
- Use the Security Fabric to share traffic and threat information among multiple FortiGate devices
- Use the Security Fabric topology view to see logical and physical views of your network topology
- Use Security Fabric automation to generate email alerts

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

In this lab, you will configure the ISFW, DCFW, and NGFW-1 FortiGate devices.

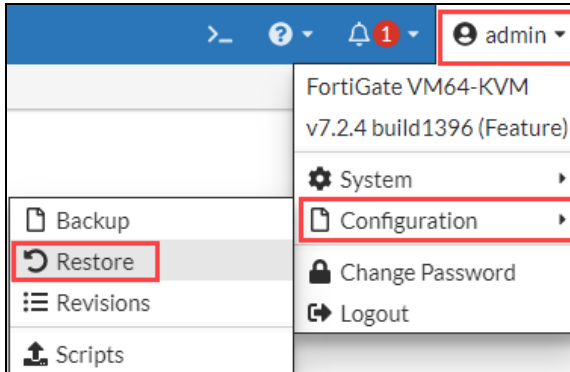


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

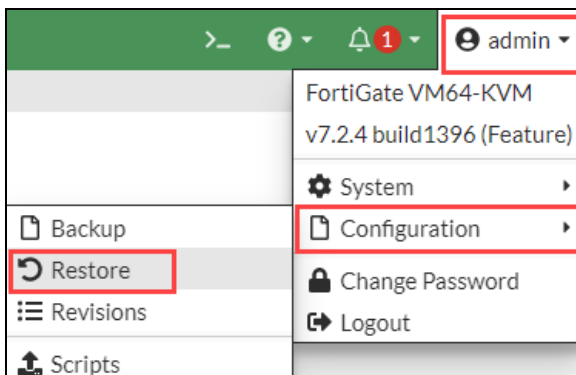
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI at 10.1.0.254 with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > Security_Fabric**, select `NGFW-1_Fabric_initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the DCFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the DCFW GUI at 10.1.0.100 with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.

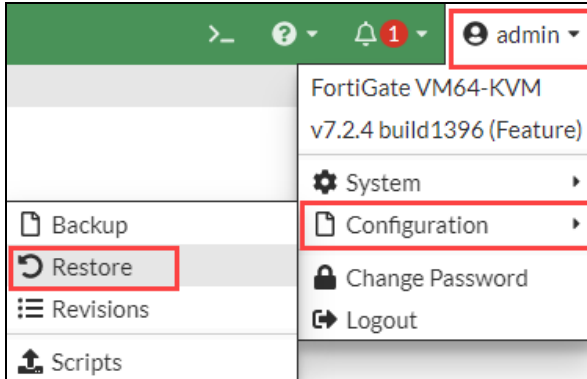


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > Security_Fabric**, select `DCFV_Fabric_initial.conf`, and then click **Open**.

5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW GUI at 10.1.10.254 with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > Security_Fabric**, select `ISFW_Fabric_initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring the Security Fabric

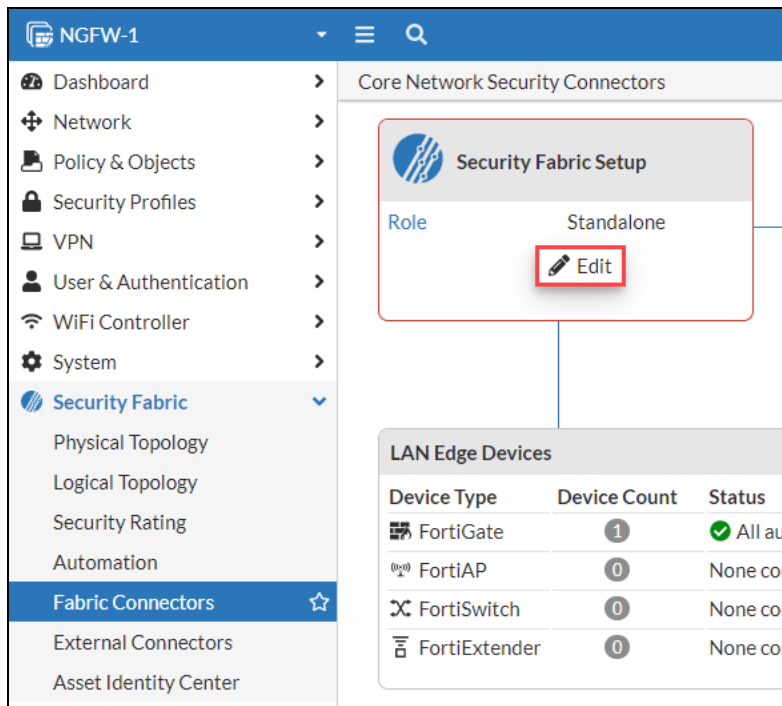
In this exercise, you will configure the Security Fabric in the lab network.

Configure the Security Fabric on NGFW-1

You will configure the root of the Security Fabric tree.

To configure the Security Fabric on NGFW-1

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Security Fabric > Fabric Connectors**.
3. In the **Core Network Security Connectors** section, click **Security Fabric Setup**, and then click **Edit**.



4. In the **Security Fabric Settings** window, in the **Security Fabric role** field, select **Serve as Fabric Root**. Selecting **Serve as Fabric Root** requires that you then set up FortiAnalyzer logging.
5. In the **Logging Settings** window, in the **Status** field, select **Enabled**, and then in the **Server** field, type `10.1.0.210`.
6. Click **OK**, and then click **Accept** to confirm that you want to connect to FortiAnalyzer.
7. In the FortiAnalyzer status notification window, click **Close**.
8. Enable **Allow other Security Fabric devices to join**, and then select **port3**.
9. In the **Fabric name** field, type `fortinet`.

Security Fabric Settings

Settings Info

Security Fabric role: Standalone **Serve as Fabric Root** Join Existing Fabric

Allow other Security Fabric devices to join: ☒

port3 +

Fabric name: fortinet

Device authorization: None

FortiCloud account enforcement: ☒

Allow downstream device REST API access: ☐

Fabric global object: ☒

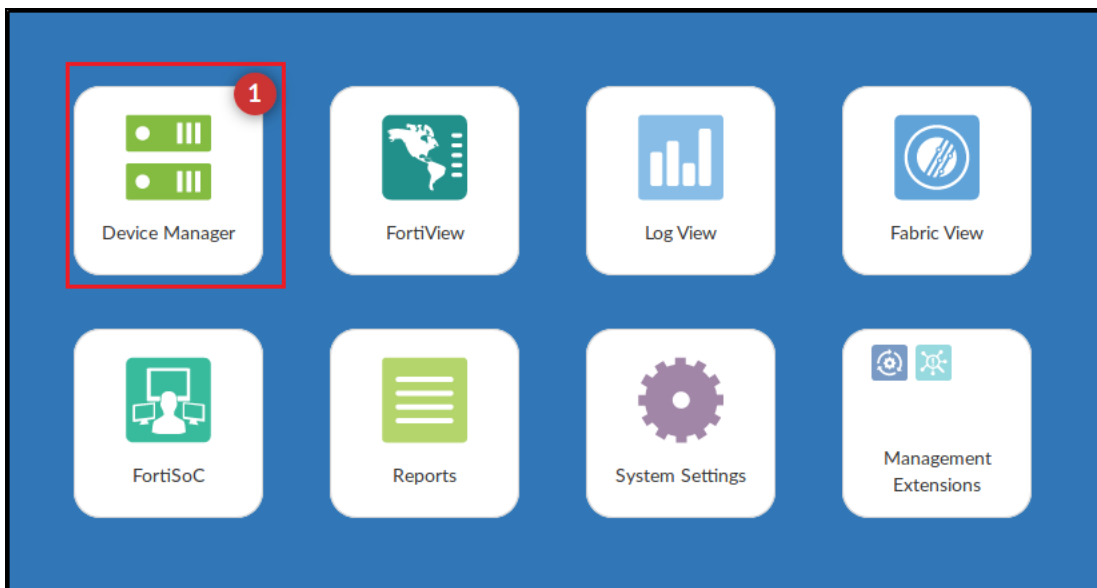
SAML Single Sign-On: ☐

Management IP/FQDN:

10. Click **OK**.

To authorize NGFW-1 on FortiAnalyzer

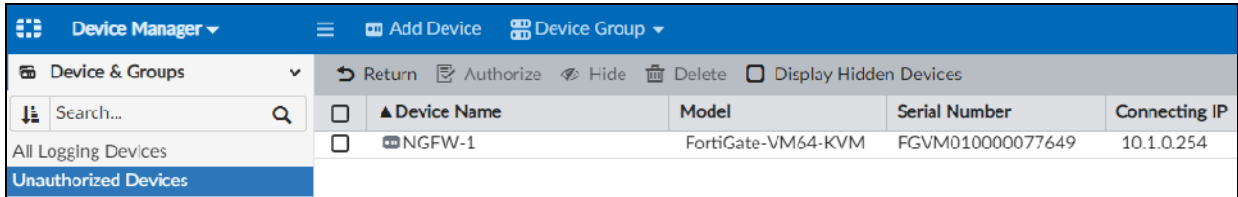
1. Continuing on the NGFW-1 GUI, click **Security Fabric > Fabric Connectors**.
2. In the **Logging & Analytics** section, click **Edit**.
An **Unauthorized** connection status is displayed.
3. Click **Cancel**, and then click **Cancel** again to close the window.
4. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
5. Click **Device Manager**.



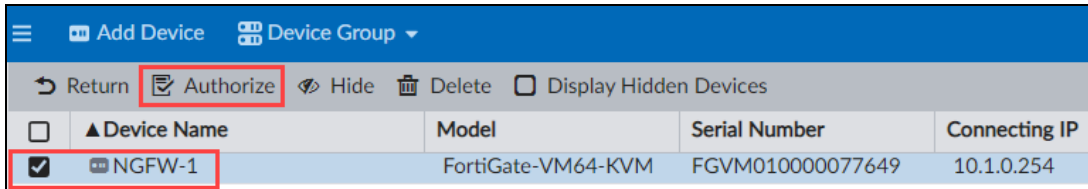
6. Click **Unauthorized Devices**.



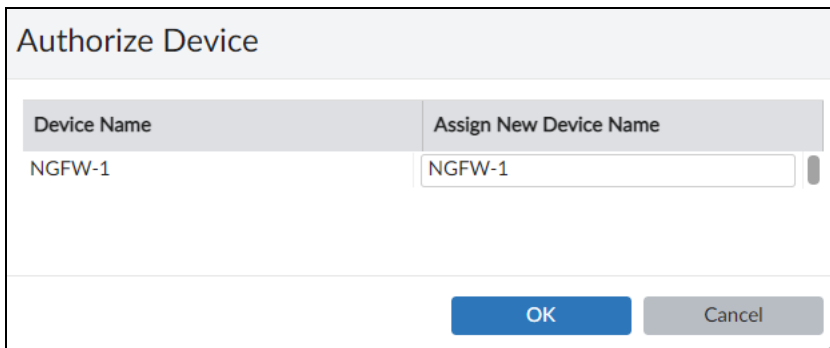
NGFW-1 appears as an unauthorized device.



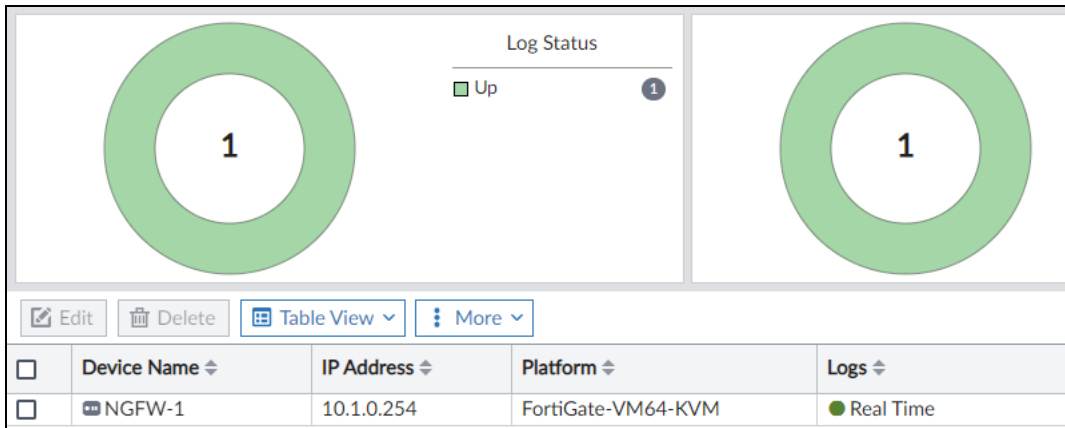
- Click **NGFW-1**, and then click **Authorize**.



The **Authorize Device** wizard opens.



- Click **OK**, and then after the progress bar reaches 100%, click **Close**.
NGFW-1 is added as a registered device.



9. Select **NGFW-1** again, and then click **Edit**.
10. Configure the following settings:

Field	Value
Admin user	admin
Password	password

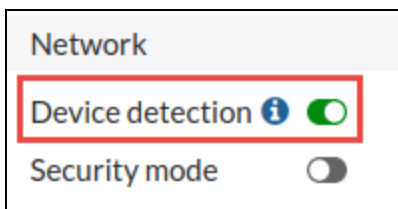
11. Click **OK**.

Configure the Security Fabric on DCFW

You will enable device detection on port3 of DCFW. After that, you will configure it as one of the branches of the Security Fabric tree.

To enable device detection on DCFW

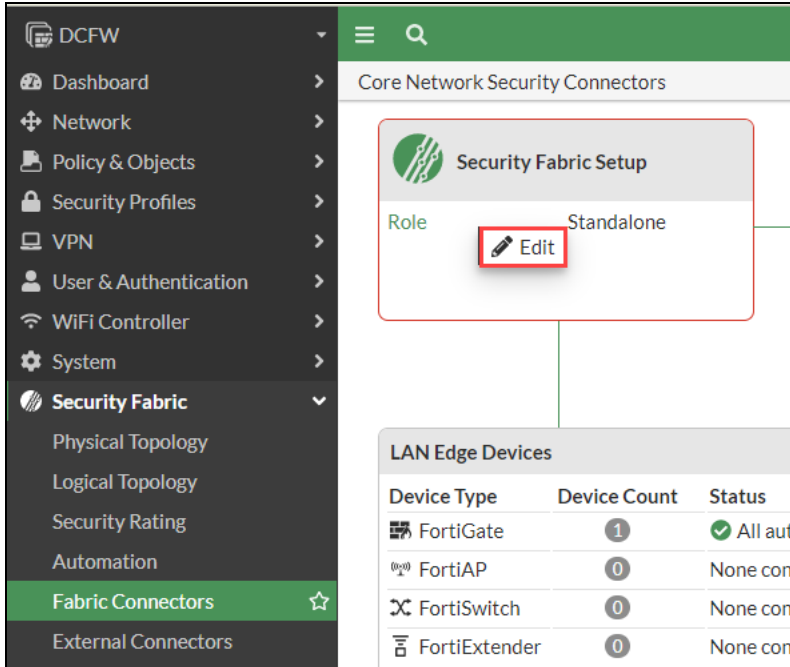
1. Log in to the DCFW GUI with the username `admin` and password `password`.
2. Click **Network > Interfaces**, and then expand the **Physical Interface** section.
3. Click **port3**, and then click **Edit**.
4. In the **Network** section, enable **Device detection**.



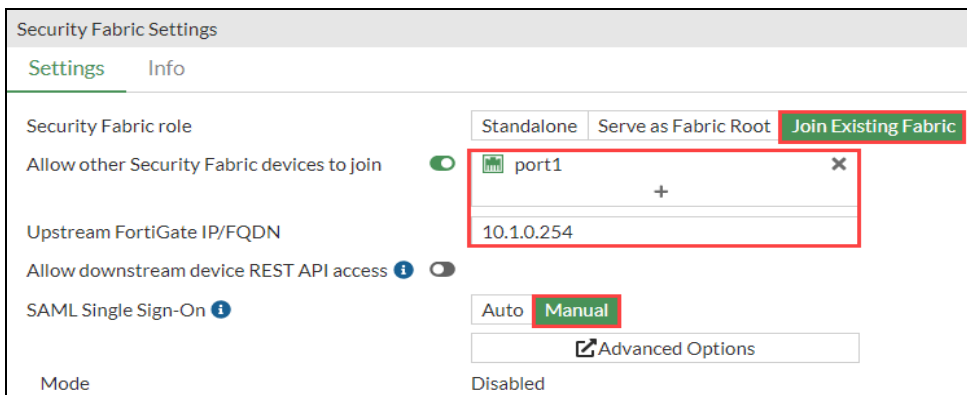
5. Click **OK**.

To enable the Security Fabric on DCFW

1. Continuing on the DCFW GUI, click **Security Fabric > Fabric Connectors**.
2. In the **Core Network Security Connectors** section, click **Security Fabric Setup**, and then click **Edit**.



3. In the **Security Fabric Settings** section, in the **Security Fabric role** field, select **Join Existing Fabric**.
4. Enable **Allow other Security Fabric devices to join**, and then select **port1**.
5. In the **Upstream FortiGate IP/FQDN** field, type **10.1.0.254**.
6. In the **SAML Single Sign-On** field, select **Manual**.



7. Click **OK**.
8. Click **OK**.

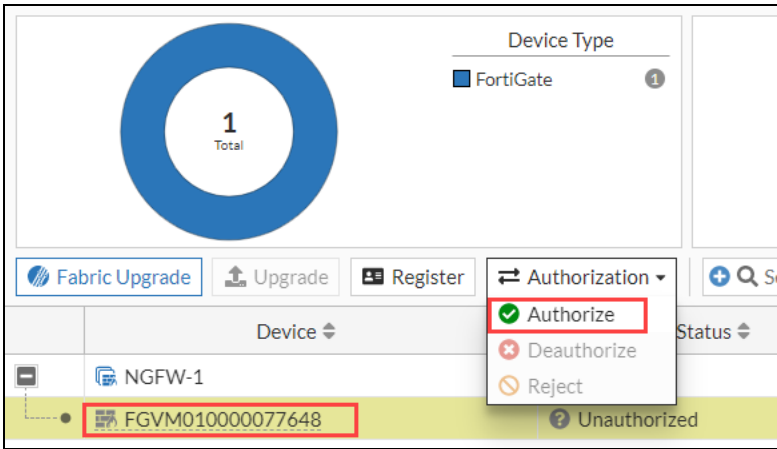
Stop and think!

Why didn't you have to configure the FortiAnalyzer IP address on DCFW?

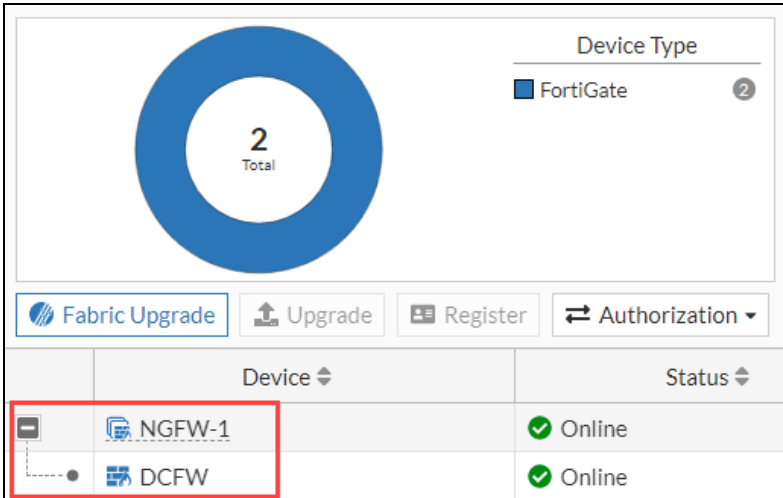
All branch FortiGate devices in a Security Fabric retrieve the FortiAnalyzer IP address from the root FortiGate.

To authorize DCFW on NGFW-1

- 1. Return to the NGFW-1 GUI, and then click **System > Fabric Management**.
- 2. Click the device with the **Unauthorized** status, and then select **Authorize**.



The NGFW-1 displays the DCFW as part of the Security Fabric. It may take few minutes to authorize. You may need to refresh the page.



To authorize DCFW on FortiAnalyzer



Only the FortiAnalyzer settings are retrieved from the root FortiGate. You still have to authorize each branch FortiGate on FortiAnalyzer.

- 1. Return to the FortiAnalyzer GUI, and then click **Unauthorized Devices**.
DCFW appears as an unauthorized device.

Add Device Device Group			
Return Authorize Hide Delete Display Hidden Devices			
☐	Device Name	Model	Serial Number
☐	DCFW	FortiGate-VM64-KVM	FGVM010000077648
			Connecting IP 10.1.0.100

- Click **DCFW**, and then click **Authorize**.
- Click **OK**, and then after the progress bar reaches 100%, click **Close**.
DCFW is added as a registered device.

Edit Delete Table View More				
☐	Device Name	IP Address	Platform	Logs
☐	DCFW	10.1.0.100	FortiGate-VM64-KVM	Real Time
☐	fortinet			
☐	NGFW-1*	10.1.0.254	FortiGate-VM64-KVM	Real Time

- Click **DCFW**, and then click **Edit**.
- Configure the following settings:

Field	Value
Admin user	admin
Password	password

- Click **OK**.
- Wait a few seconds, and then refresh the screen.
You should see DCFW as part of the Security Fabric.

Edit Delete Table View More				
☐	Device Name	IP Address	Platform	Logs
☐	fortinet			
☐	DCFW	10.1.0.100	FortiGate-VM64-KVM	Real Time
☐	NGFW-1*	10.1.0.254	FortiGate-VM64-KVM	Real Time

Configure the Security Fabric on ISFW

Follow the previous steps to configure the Security Fabric on ISFW. You must do the following:

- Enable device detection on port3.
- Enable the Security Fabric on ISFW.
- Authorize ISFW from NGFW-1.
- Authorize ISFW from FortiAnalyzer.
- Configure the correct ISFW administrator credentials on FortiAnalyzer.

Monitor the FortiTelemetry Connection

You will use CLI commands to check the status of the FortiTelemetry connection between DCFW, ISFW, and NGFW-1.

To monitor the FortiTelemetry connection

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following CLI command:

```
diagnose sys csf downstream
```

The system displays the DCFW and ISFW FortiTelemetry connection information.

```
1: FGVM010000077646 (10.1.0.1) Management-IP: Management-port:0 parent:
  FGVM010000077649
path:FGVM010000077649:FGVM010000077646
data received: Y downstream intf:port1 upstream intf:port3 upstream vdom:root admin-
  port:443
authorizer:FGVM010000077649
2: FGVM010000077648 (10.1.0.100) Management-IP: Management-port:0 parent:
  FGVM010000077649
path:FGVM010000077649:FGVM010000077648
data received: Y downstream intf:port1 upstream intf:port3 upstream vdom:root admin-
  port:443
authorizer:FGVM010000077649
```

4. Enter the following command to display Security Fabric statistics:

```
diagnose test application csfd 1
```

The status of DCFW and ISFW should appear as `link-ok SSL-ok auth-ok hello-ok`.

```
Dump CSF daemon info
group name: fortinet
group pwd: *
status: Active
accept auth by cert: y
forticloud account enforcement: y
Upstream info
N/A
Downstream info
device total: 2
# 1
sn: FGVM010000077646
ip: 10.1.0.1
port: 22268
status: link-ok SSL-ok hello-ok auth-ok
no response: 1

# 2
sn: FGVM010000077648
ip: 10.1.0.100
port: 18028
status: link-ok SSL-ok hello-ok auth-ok
```

no response: 0

Exercise 2: Examining the Physical and Logical Topology Views

You will examine the different Security Fabric topology views.

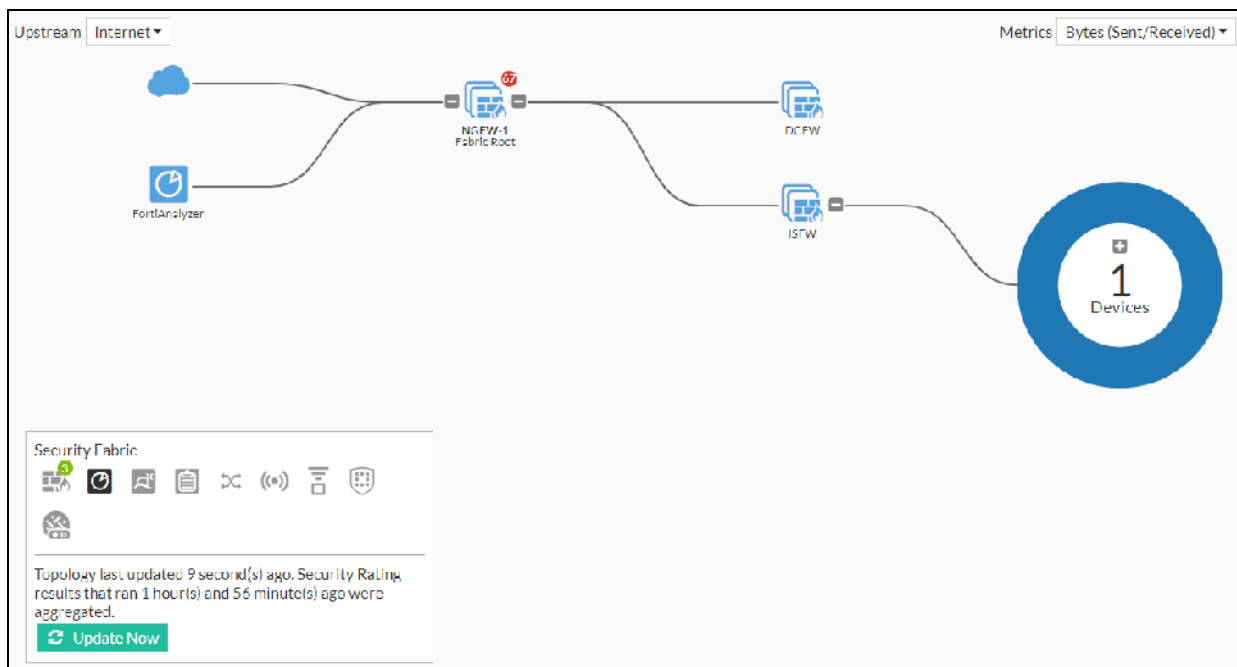
View the Physical Topology

The physical topology displays the network devices and how they are connected.

To display the physical topology

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Security Fabric > Physical Topology**.

Your physical topology should look similar to the following example:



Your topology view might not match what is shown in the example. At a minimum, you should see NGFW-1, ISFW, and DCFW in the topology view.

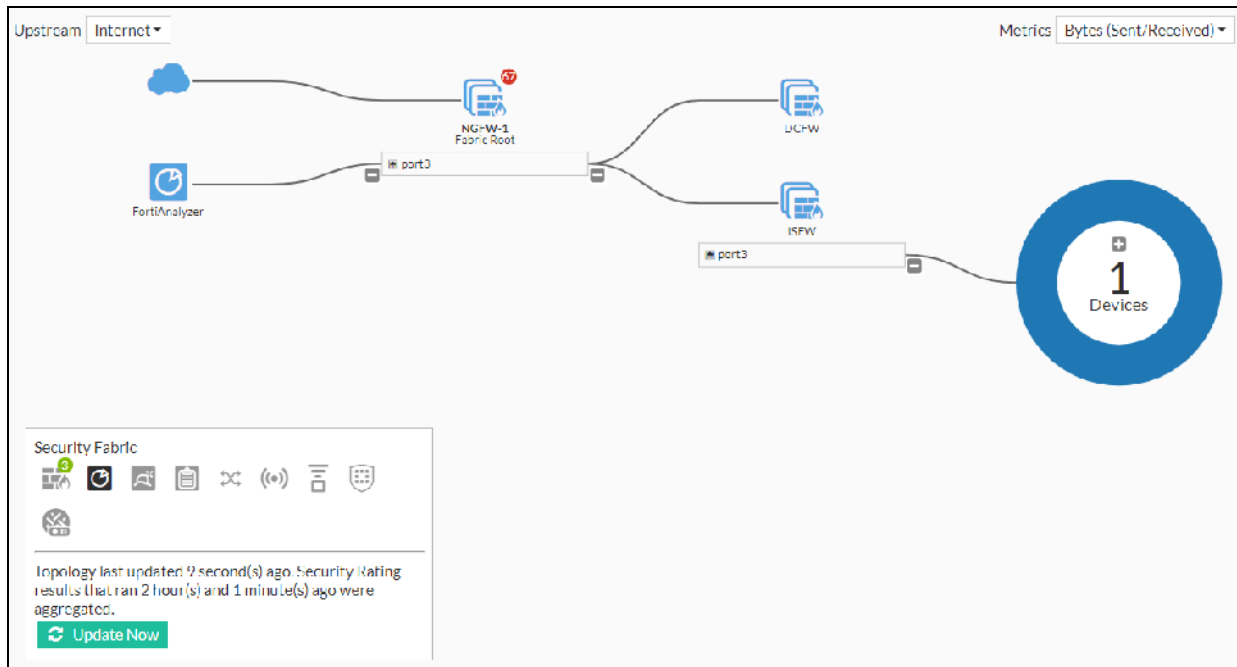
View the Logical Topology

The logical topology displays the interfaces where each device is connected.

To display the logical topology

1. Continuing on the NGFW-1 GUI, click **Security Fabric > Logical Topology**.

Your logical topology should look similar to the following example:



Your topology view might not match what is shown in the example. At a minimum, you should see NGFW-1, ISFW, and DCFW in the topology view, and the respective interface connections.

Exercise 3: Configuring the Automation Stitch, Trigger, and Action

In this exercise, you will configure the automation stitch on NGFW-1 to send email alerts for WAN link failures. An automation stitch includes a trigger and an action, which you will create.

Configure the Automation

You will create a trigger and an action on NGFW-1, and then add them to the stitch.

To configure the automation action on NGFW-1

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Security Fabric > Automation**.
3. In the **Automation** window, click **Action**.
4. Click **Create New**, and then in the **Notification** section, select **Email**.
5. Configure the following settings to create a new action:

Field	Value
Name	Link_Down_Email
From	fortinet@training.lab
To	admin@training.lab
Subject	WAN Link Down

Your configuration should look like the following image:

Create New Automation Action

Email Send a custom email to the specified recipient(s).

Name: Link_Down_Email

Minimum interval: 0 second(s)

Description: 0/255

Email

From: fortinet@training.lab

To: admin@training.lab

Subject: WAN Link Down

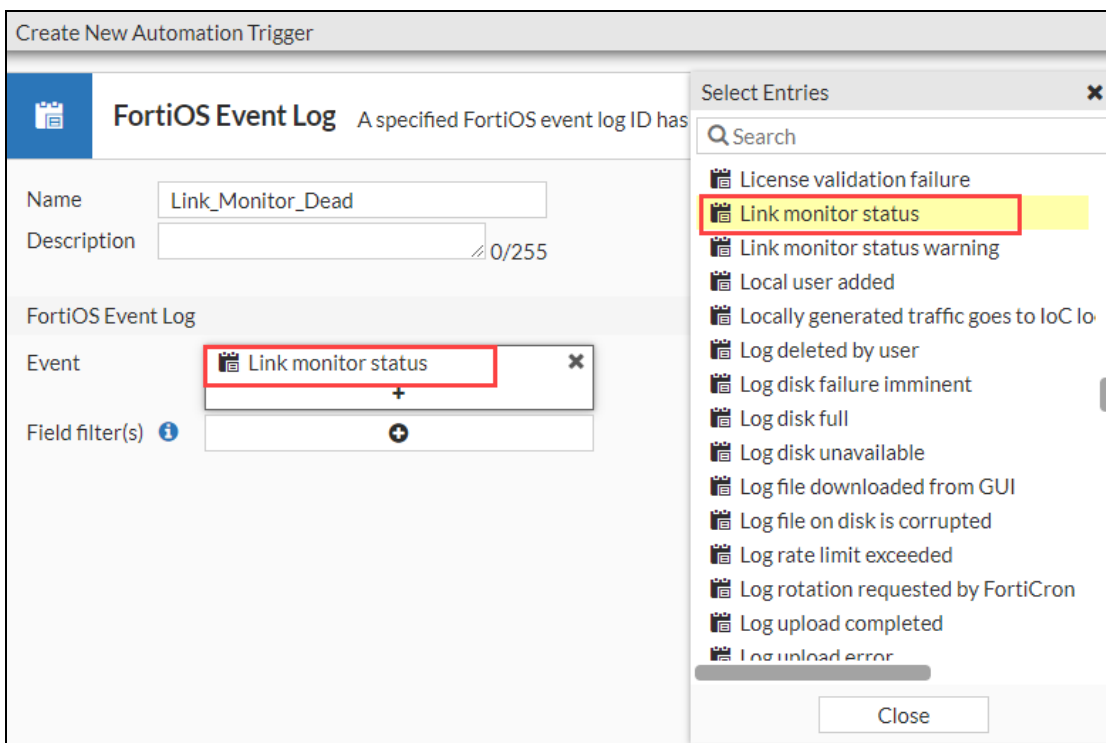
Body: %log%

Replacement message: ☐

6. Click **OK**.

To configure the automation trigger on NGFW-1

1. Continuing on the NGFW-1 GUI, in the **Automation** window, click **Trigger**.
2. Click **Create New**, and then in the **Miscellaneous** section at the bottom of the page, select **FortiOS Event Log**.
3. In the **Name** field, type `Link_Monitor_Dead`.
4. In the **FortiOS Event Log** section, in the **Event** field, click **+**, and then select **Link monitor status**.
You can use the search field to find the event.



5. Click **Close**.
6. In the **Field filter(s)** field, click **+**.
7. In the **Field name** field, type `msg`, and then in the **Value** field, type the following text:

`Link Monitor initial state is dead, protocol: ping`

Make sure that you don't type a period (.) at the end of the text. Your configuration should look like the following image:

Create New Automation Trigger

FortiOS Event Log A specified FortiOS event log ID has occurred. [CHANGE TYPE](#)

Name: Link_Monitor_Dead

Description: 0/255

FortiOS Event Log

Event: Link monitor status

Field filter(s): msg : Link Monitor initial state is dead, protoc

OK Cancel

8. Click **OK**.

Stop and think!

Why do you configure **Field filter(s)** on the automation trigger?

The main event ID on FortiGate can have multiple log fields. To filter on a specific log field in an event that triggers the stitch, you can use filters. In this exercise, you must look for a log where the link monitor state is *dead*. By default, the email body includes all the fields from the log event that triggered the stitch.

To configure the automation stitch on NGFW-1 on the CLI

1. Log in to the NGFW-1 CLI with the username `admin` and password `password`.
2. Enter the following commands to configure the automation stitch:

```
config system automation-stitch
  edit WAN_Link_Dead
    set trigger Link_Monitor_Dead
    config actions
      edit 1
        set action Link_Down_Email
      next
    end
  next
end
```

Test the Automation Stitch and View the Email Alert

You will test the automation stitch by forcing a link failure, and then view the email alert.



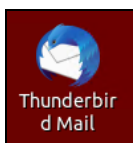
The link monitor is already configured on NGFW-1 to monitor the status of both port1 and port2 routes.



An SMTP mail server is required for email alerts to operate. Because configuring a mail server is out of scope for this lab, one was configured for you. You can view the email service configuration on the NGFW-1 GUI by clicking **System > Settings**, and then scrolling down to the **Email Service** configuration.

To force a link failure and view the email alert

1. On the Client-10 VM, on the desktop, open Mozilla Thunderbird.



2. Continuing on the NGFW-1 CLI session, enter the following commands to modify the port2 link monitor:

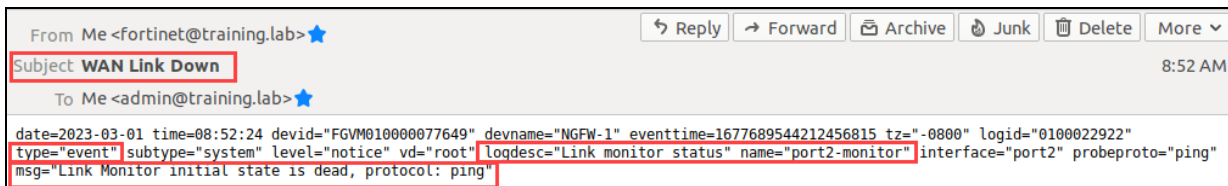
```
config system link-monitor
edit port2-monitor
set server 100.64.2.13
next
end
```

3. Wait a few seconds.

Because the host 100.64.2.13 does not exist in the lab network, the link health monitor does not receive any replies. Because of this, the link health monitor assumes that the port2 internet connection is down, and triggers the automation stitch to send an email alert.

4. Leave the NGFW-1 CLI session open.
5. On the Client-10 VM, in Mozilla Thunderbird, select the inbox of the admin@training.lab email account. You should see a message in the admin inbox with a subject of "WAN Link Down".
6. If an email does not appear in the inbox, wait 30 seconds, and then click **Get Messages** again.
7. Open the email alert, and then review the log message.

As you can see, the log message is in raw format. The log message body provides information about an event.



8. When you are finished, close the Thunderbird email client.

To view system events on NGFW-1

1. Return to the NGFW-1 GUI, and then click **Log & Report > System Events > General System Events**.
2. Verify that NGFW-1 detected the link failure and triggered the stitch.

Dashboard	Summary	Logs
Network	Search	
Policy & Objects		
Security Profiles		
VPN		
User & Authentication		
WiFi Controller		
System		
Security Fabric		
Log & Report		
Forward Traffic		
Local Traffic		
Sniffer Traffic		
System Events		

Date/Time	Level	User	Message	Log Description
			stitch:WAN_Link_Dead is triggered.	Automation stitch triggered
			Static route on interface port12 may be removed by link...	Routing information changed
			he state is changed from 0 to 1	Link monitor status
			Link Monitor initial state is dead, protocol: ping	Link monitor status
		admin	Edit system.link-monitor 1	Object attribute configured
		admin	Edit user:email:setting	Attribute configured
			he state is changed from 1 to 0	Link monitor status
			Link Monitor initial state is alive, protocol: ping	Link monitor status
			Static route on interface port2 may be added by link-mon...	Routing information changed

- Select the **Automation stitch triggered** log, and then in the upper-right corner, click **Details** to view the details. You should see the following details:

Log Details	
General	
Absolute Date/Time	
Last Access Time	
VDOM	root
Log Description	Automation stitch triggered
Event	
From	log
Message	stitch:WAN_Link_Dead is triggered.
Other	
ID	7205592600156307456
itime	2023-03-01 06:59:23
Log ID	0100046600
Type	event
Sub Type	system
Log event original timestamp	1677682762212694500
Stitch	WAN_Link_Dead
Trigger	Link Monitor Dead
Timezone	-0800
Stitch Action	Link Down_email
csf	fortinet
D-Time	2023-03-01 06:59:22
I-Time	1677682763
Device Name	NGFW-1

4. Locate the log with the **Link monitor status** description.

This is the event that triggered the email alert using the automation stitch.

Log & Report	2023/03/01 08:52:25	■■■■■■■■	switch WAN Link Dead is triggered.	Automation stitch triggered
Forward Traffic	2023/03/01 08:52:23	■■■■■■■■	Static route on interface port2 may be removed by link...	Routing information changed
Local Traffic	2023/03/01 08:52:23	■■■■■■■■	he state is changed from 0 to 1	Link monitor status
Sniffer Traffic	2023/03/01 08:52:23	■■■■■■■■	Link Monitor initial state is dead, protocol: ping	Link monitor status
System Events				

5. Select the **Link monitor status** log, and then in the upper-right corner, click **Details** to view the details.

You should see the following details:

Log Details		×
General		
Absolute Date/Time	2023-03-01	
Last Access Time	08:52:23	
VDOM	root	
Log Description	Link monitor status	
Source		
Interface	port2	
Device ID	FGVM010000077649	
Security		
Level	Notice	
Event		
Probe Protocol	ping	
Message	Link Monitor initial state is dead, protocol: ping	
Other		

You can see that the event includes the log field that you included in the automation trigger.



To view the list of available fields for a log, see the *FortiOS Log Message Reference* located at <https://docs.fortinet.com/document/fortigate/7.2.4/fortios-log-message-reference>.

Lab 4: High Availability

In this lab, you will configure virtual clustering and distribute traffic between two FortiGate devices in the virtual cluster.

Objectives

- Configure FortiGate Session Life Support Protocol (FGSP) between NGFW-1 and NGFW-2
- Analyze session synchronization between NGFW-1 and NGFW-2
- Analyze Virtual Router Redundancy Protocol (VRRP) configuration and test link failover
- Configure a virtual cluster between NGFW-1 and NGFW-2 using VDOM partitioning
- Analyze traffic distribution across two virtual clusters
- Perform a failover to make NGFW-1 the primary device to handle all traffic

Time to Complete

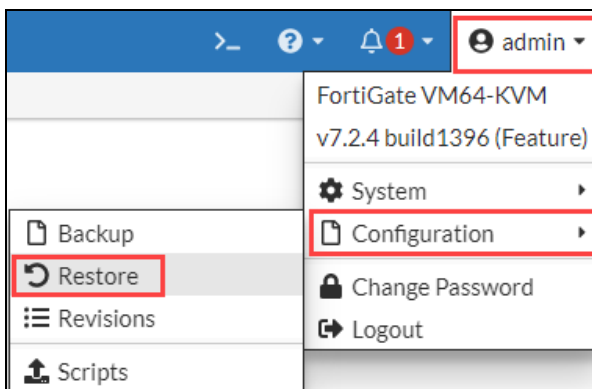
Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices and change the default route on the Client-10 VM. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

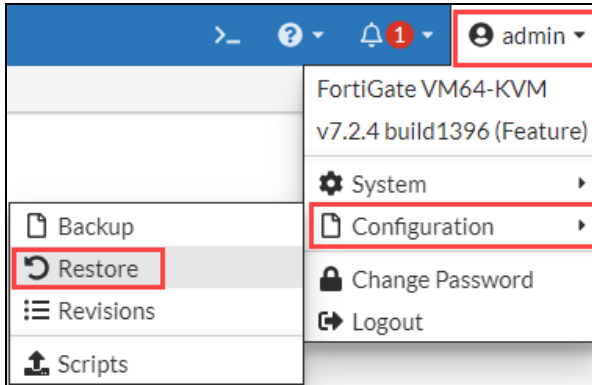
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > HA**, select `NGFW-1_FGSP_VRRP_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the NGFW-2 configuration file

1. On the Client-10 VM, open a browser, and then log in to the NGFW-2 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.

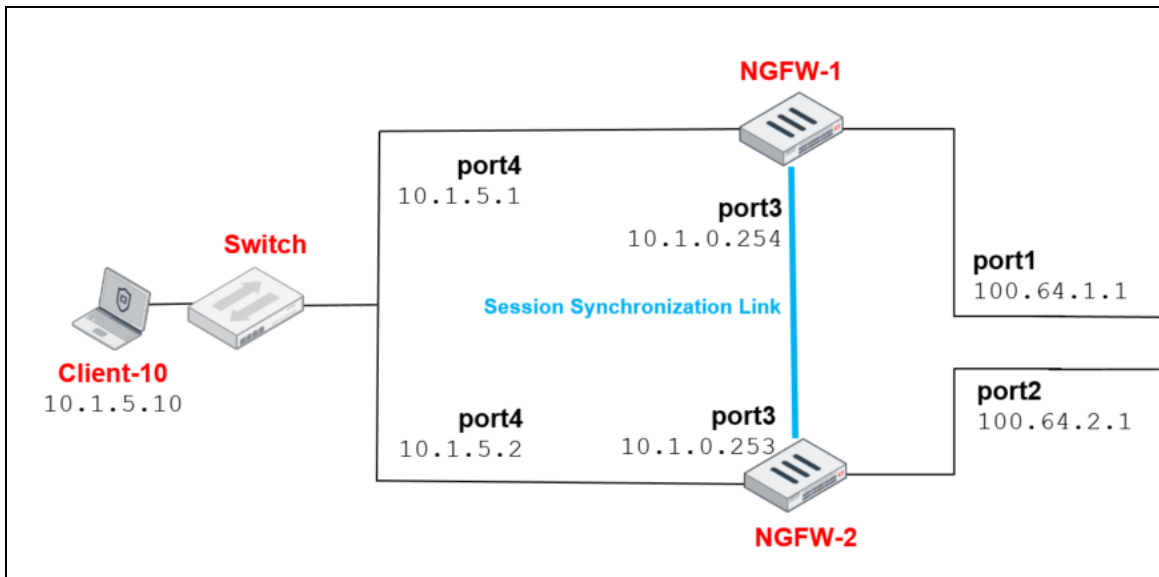


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > HA**, select `NGFW-2_FGSP_VRRP_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring FGSP

In this exercise, you will configure FGSP on NGFW-1 and NGFW-2. Port3 on NGFW-1 and NGFW-2 is in the same LAN subnet. You will apply the session synchronization using a layer 3 connection.

Network Topology



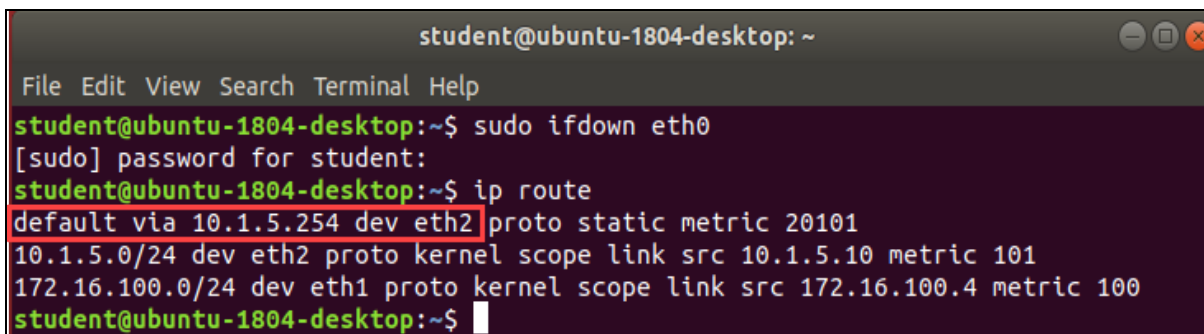
Change the Firewall Rules on Linux Router

You must run a script on the Client-10 VM to change the default route.

To change the default route on the Client-10 VM

1. Connect to the Client-10 VM.
2. Open a terminal session, and then enter the following command:

```
sudo ifdown eth0
```
3. For [sudo] password for student, enter password.
4. Enter `ip route` to verify that the default route is through the gateway IP 10.1.5.254.



```
student@ubuntu-1804-desktop: ~  
File Edit View Search Terminal Help  
student@ubuntu-1804-desktop:~$ sudo ifdown eth0  
[sudo] password for student:  
student@ubuntu-1804-desktop:~$ ip route  
default via 10.1.5.254 dev eth2 proto static metric 20101  
10.1.5.0/24 dev eth2 proto kernel scope link src 10.1.5.10 metric 101  
172.16.100.0/24 dev eth1 proto kernel scope link src 172.16.100.4 metric 100  
student@ubuntu-1804-desktop:~$
```

5. Close the terminal window.

Configure FGSP and Test Session Synchronization

Before you test the session synchronization, you will configure FGSP between NGFW-1 and NGFW-2.

To configure FGSP on NGFW-1

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following CLI commands to enable FGSP on NGFW-1:

```
config system standalone-cluster  
  set standalone-group-id 5  
  set group-member-id 1  
  config cluster-peer  
    edit 1  
      set peerip 10.1.0.253  
    next  
  end  
end
```

4. Leave the SSH session open.

To configure FGSP on NGFW-2

1. Connect over SSH to NGFW-2.
2. Log in with the username `admin` and password `password`.
3. Enable FGSP on NGFW-2 following the procedure you used for NGFW-1 and using the following information:

Command	Variable
<code>standalone-group-id</code>	5
<code>group-member-id</code>	2
<code>peerip</code>	10.1.0.254



The `standalone-group-id` must be the same value for all members. The ID can be between 1–255. The `group-member-id` can be between 1–15 and must be different for each member in the same group.

Test Session Synchronization Between NGFW-1 and NGFW-2

By default, FGSP only synchronizes TCP sessions. First, you will test TCP session synchronization, and then you will enable ICMP and NAT session synchronization later.

To test TCP sessions

1. Connect to the Client-10 VM.
2. On the Client-10 VM, open a browser, and then log in to the DCFW GUI at 10.1.0.100 with the username `admin` and password `password`.
3. Return to the NGFW-1 SSH session, and then enter the following command to view the session information:

```
get sys session list | grep 10.1.0.100:80
```

The result should be similar to the following output:

```
NGFW-1 # get sys session list | grep 10.1.0.100:80
tcp      3538    10.1.5.10:45572 -          10.1.0.100:80 -
tcp      3599    10.1.5.10:45564 -          10.1.0.100:80 -
```

4. On the NGFW-2 SSH session, enter the same command to view the session information:

```
get sys session list | grep 10.1.0.100:80
```

The result should be similar to the following output:

```
NGFW-2 # get sys session list | grep 10.1.0.100:80
tcp      3483    10.1.5.10:45572 -          10.1.0.100:80 -
tcp      3482    10.1.5.10:45564 -          10.1.0.100:80 -
```

Both FortiGate devices show the same TCP session.

To enable NAT and ICMP session synchronization

1. Connect over SSH to NGFW-1.
2. Enter the following CLI commands to enable ICMP and NAT session synchronization on NGFW-1:

```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-nat enable
end
```

3. Leave the SSH session open.

To test ICMP session synchronization

1. On the Client-10 VM, open a terminal window, type `ping 4.2.2.2`, and then press `Enter`.
2. Do not close the terminal window.
3. Connect over SSH to NGFW-2.

4. Log in with the username `admin` and password `password`.
5. Enter the following command to view the session:

```
# get system session list | grep icmp
```

The result should be similar to the following output:

```
NGFW-2 # get sys session list | grep icmp
icmp      58      10.1.5.10:24060 100.64.1.1:24060 4.2.2.2:8
```

6. Enter the same command on NGFW-1 to match the session information.

The source and destination IP addresses and ports on both sessions must match because this is the same session.

Stop and think!

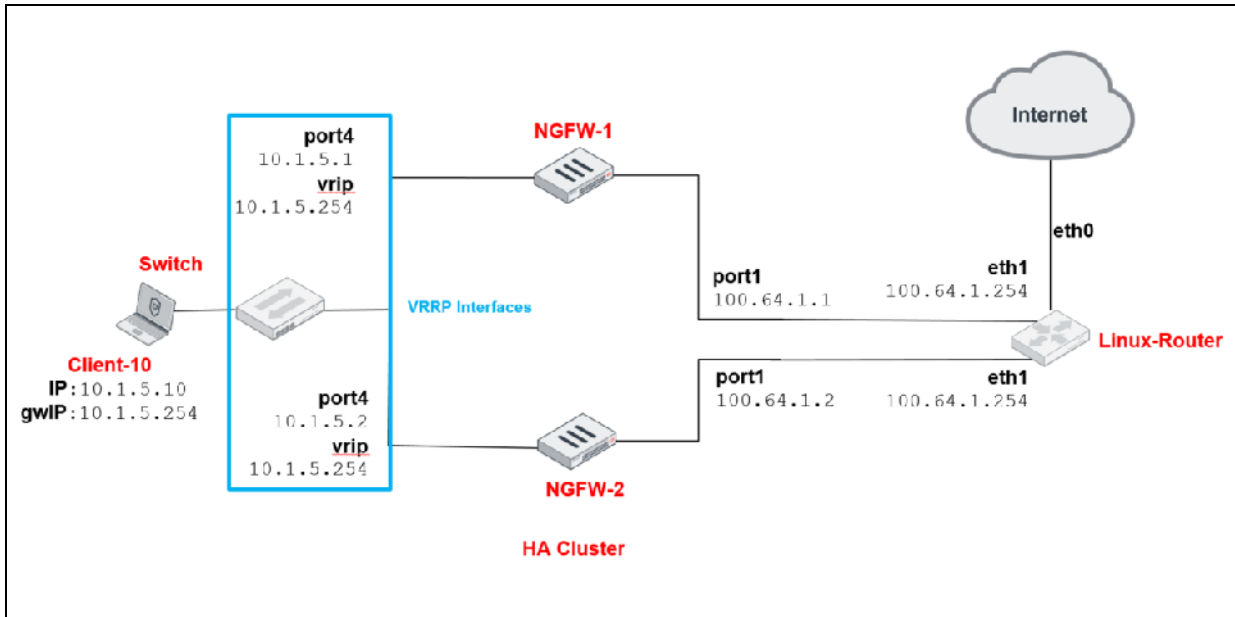
Why did you run the `set session-pickup-nat enable` command on NGFW-1?

This is because the firewall policy on NGFW-1 has NAT enabled and, by default, FGSP does not synchronize NAT sessions.

Exercise 2: Analyzing VRRP Failover

In this exercise, you will examine the VRRP link failover on NGFW-1 and NGFW-2. VRRP is configured between NGFW-1 and NGFW-1 using port4. You will also enable the virtual MAC address on the VRRP configuration.

Network Topology



Verify the VRRP Configuration on NGFW-1 and NGFW-2

Before you test the VRRP failover, you will verify the VRRP configuration on NGFW-1 and NGFW-2.

To verify the VRRP configuration on NGFW-1

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following CLI commands to view the VRRP configuration on NGFW-1:

```
config system interface
# edit port4
# show
```

You should see the following settings:

```
NGFW-1 (interface) # edit port4

NGFW-1 (port4) # show
config system interface
  edit "port4"
    set vdom "root"
    set ip 10.1.5.1 255.255.255.0
    set allowaccess ping https
    set type physical
  config vrrp
    edit 1
      set vrgrp 1
      set vrip 10.1.5.254
      set priority 255
      set vrdest 8.8.8.8
      set vrdest-priority 30
    next
  end
  set snmp-index 4
next
end
```

To verify the VRRP configuration on NGFW-2

You will verify the VRRP configuration on NGFW-2. Try to do this yourself using the procedure you followed for NGFW-1.

1. Connect over SSH to NGFW-2.
2. Log in with the username `admin` and password `password`.
3. Verify the VRRP configuration on port4 of NGFW-2.



The `set priority` value determines which device becomes the primary router in the VRRP setup. Because the NGFW-1 priority is 255, it is the primary router. The NGFW-2 priority is set to 50.

The `set vrdest-priority` setting is used when the primary router is unable to reach the destination or has failed. The `set priority` value for the backup device must be higher than the destination priority of the primary router. Otherwise, failover doesn't work for a WAN link failure.

Test VRRP Link Failover Between NGFW-1 and NGFW-2

You will verify the client VM network configuration and ARP table information, and then test the failover.

To view the client machine gateway IP address, default route, and ARP table

1. On the Client-10 VM, open a terminal window.
2. Type `ip route`, and then press `Enter` to view the default route through the gateway IP address.

You should see the following output:

```
student@ubuntu-1804-desktop: ~  
File Edit View Search Terminal Help  
student@ubuntu-1804-desktop:~$ sudo ifdown eth0  
[sudo] password for student:  
student@ubuntu-1804-desktop:~$ ip route  
default via 10.1.5.254 dev eth2 proto static metric 20101  
10.1.5.0/24 dev eth2 proto kernel scope link src 10.1.5.10 metric 101  
172.16.100.0/24 dev eth1 proto kernel scope link src 172.16.100.4 metric 100  
student@ubuntu-1804-desktop:~$
```

3. Enter `arp -a` to see the ARP table on the Client-10 VM.

You should see that the NGFW-1 port4 MAC address is assigned to the gateway or VRRP router IP address 10.1.5.254.

```
student@ubuntu-1804-desktop:~$ arp -a  
? (10.1.5.1) at 02:09:0f:00:0e:02 [ether] on eth2  
gateway (10.1.5.254) at 02:09:0f:00:0e:02 [ether] on eth2  
? (10.1.5.2) at 02:09:0f:00:0e:03 [ether] on eth2  
? (172.16.100.1) at fe:ff:ff:00:00:0d [ether] on eth1
```

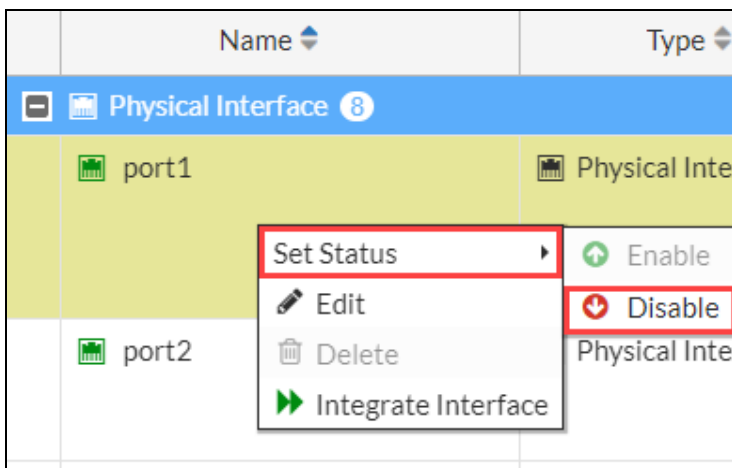
You can verify MAC address information on NGFW-1 by entering the `get router info vrrp` command.



```
NGFW-1 # get router info vrrp  
Interface: port4, primary IP address: 10.1.5.1  
UseVMAC: 0, SoftSW: 0, EmacVlan: 0 BrPortIdx: 0, PromiseCount: 0  
HA mode: primary (0:0:1) VRRP primary number: 1  
VRID: 1 version: 2  
vrip: 10.1.5.254, priority: 255 (255,30), state: PRIMARY  
adv_interval: 1, preempt: 1, ignore_dft: 0 start_time: 3  
primary_adv_interval: 100, accept: 1  
vrmac: 02:09:0f:00:0e:02  
vrdat: 8.8.8.8  
vrgrp: 1
```

To verify the link failover

1. On the NGFW-1 GUI, click **Network > Interfaces**.
2. Right-click **port1**, and then click **Set Status > Disable** to disable the interface.



3. Return to the Client VM.
4. On the terminal window, enter `arp -a` to see the updated ARP table.

```
student@ubuntu-1804-desktop:~$ arp -a
? (10.1.5.1) at 02:09:0f:00:0e:02 [ether] on eth2
gateway (10.1.5.254) at 02:09:0f:00:0e:03 [ether] on eth2
? (10.1.5.2) at 02:09:0f:00:0e:03 [ether] on eth2
? (172.16.100.1) at fe:ff:ff:00:00:0d [ether] on eth1
```

You should see that the MAC address has been updated to the NGFW-2 port4 MAC address.



When the new primary takes over, it sends gratuitous ARPs to associate the VRRP router IP address with the MAC address of the new primary (or the FortiGate interface that became the new primary).

Enable the VRRP Virtual MAC Address

You will enable the VRRP virtual MAC address. The VRRP virtual MAC address is a shared MAC address that the primary FortiGate adopts. If the primary FortiGate fails, the same virtual MAC address is picked up by the new primary FortiGate, allowing all devices on the network to transparently connect to the default route using the same virtual MAC address. By default, this feature is disabled and must be enabled on all FortiGate devices in a VRRP domain.

To enable the VRRP virtual MAC address

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to enable the VRRP virtual MAC address:

```
config system interface
  edit port4
    set vrrp-virtual-mac enable
  end
```

4. Repeat the command on NGFW-2.

To verify the new virtual MAC address

1. Enter `get router info vrrp` to verify the change on NGFW-2.

You should see the following output:

```
NGFW-2 # get router info vrrp
Interface: port4, primary IP address: 10.1.5.2
UseVMAC: 1, SoftSW: 0, EMacVlan: 0 BrPortIdx: 0, PromiscCount: 1
HA mode: primary (0:0:1) VRRP primary number: 1
VRID: 1 version: 2
  vrip: 10.1.5.254, priority: 50 (50,0), state: PRIMARY
  adv_interval: 1, preempt: 1, ignore_dft: 0 start_time: 3
  primary_adv_interval: 100, accept: 1
  vrmac: 00:00:5e:00:01:01
  vrdest: 8.8.8.8
  vrgrp: 1
```

2. On the Client-10 VM terminal window, enter `arp -a`.
The gateway MAC address must match the new virtual MAC address.

```
student@ubuntu-1804-desktop:~$ arp -a
? (10.1.5.1) at 02:09:0f:00:0e:02 [ether] on eth2
gateway (10.1.5.254) at 00:00:5e:00:01:01 [ether] on eth2
? (10.1.5.2) at 02:09:0f:00:0e:03 [ether] on eth2
? (172.16.100.1) at fe:ff:ff:00:00:0d [ether] on eth1
```

Stop and think!

Why do you see the 00:00:5e:00:01:01 MAC address?

This is because the last octet is based on the VRRP router ID using the following format:

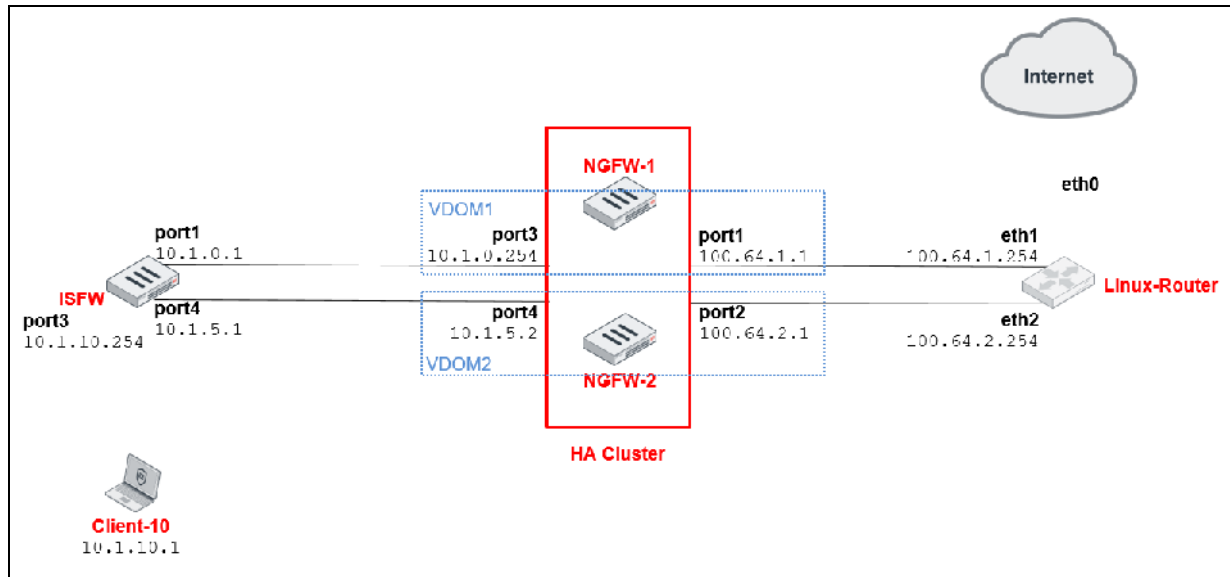
00-00-5E-00-01-<VRID_hex>

Where <VRID_hex> is the VRRP router ID in hexadecimal format. In the lab, the group ID is 1, and therefore the address is 00:00:5e:00:01:01.

Exercise 3: Configuring a Virtual Cluster

In this exercise, you will configure a virtual cluster between NGFW-1 and NGFW-2. HA is configured between NGFW-1 and NGFW-2. Using VDOM partitioning, you will configure virtual clustering between VDOM1 and VDOM2 in a way that traffic for VDOM1 will be processed by NGFW-1, and traffic for VDOM2 will be processed by NGFW-2.

Network Topology



Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices and revert the default route on the Client-10 VM. The configuration files are located on the desktop of the Client-10 VM.

To change the default route on the Client-10 VM

1. Connect to the Client-10 VM.
2. Open a terminal session, and then enter the following command:

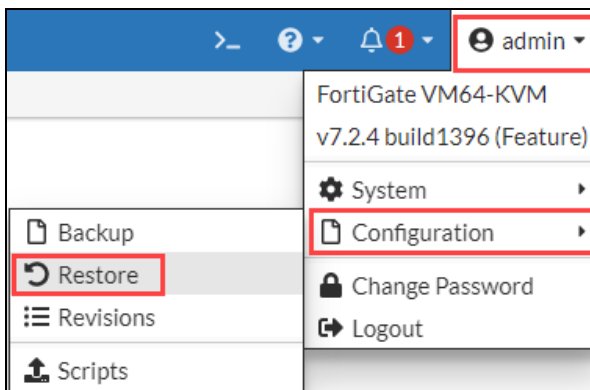
```
sudo ifup eth0
```
3. For [sudo] password for student, enter password.
4. Enter `ip route` to verify that the default route through gateway IP 10.1.10.254 has the highest priority.

```
student@ubuntu-1804-desktop: ~  
File Edit View Search Terminal Help  
student@ubuntu-1804-desktop:~$ sudo ifup eth0  
[sudo] password for student:  
student@ubuntu-1804-desktop:~$ ip route  
default via 10.1.10.254 dev eth0 onlink  
default via 10.1.5.254 dev eth2 proto static metric 20101  
10.1.5.0/24 dev eth2 proto kernel scope link src 10.1.5.10 metric 101  
10.1.10.0/24 dev eth0 proto kernel scope link src 10.1.10.1  
169.254.0.0/16 dev eth0 scope link metric 1000  
172.16.100.0/24 dev eth1 proto kernel scope link src 172.16.100.4 metric 100  
student@ubuntu-1804-desktop:~$
```

5. Close the terminal window.

To restore the NGFW-1 configuration file

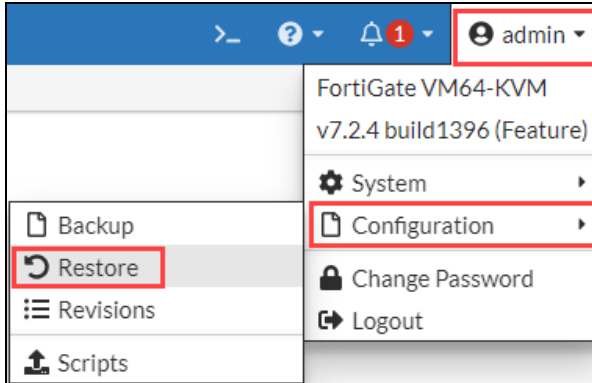
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > HA**, select `NGFW-1_VCluster_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the NGFW-2 configuration file

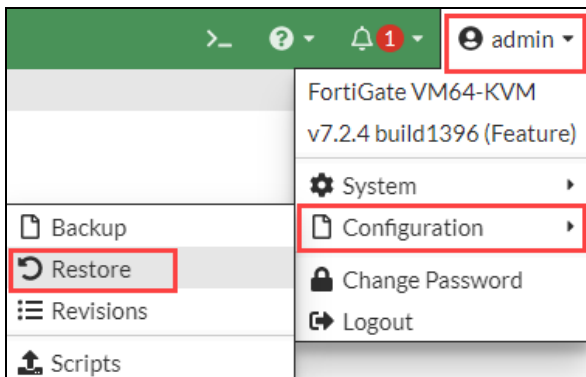
1. On the Client-10 VM, open a browser, and then log in to the NGFW-2 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > HA**, select `NGFW-2_VCluster_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > HA**, select `ISFW_VCluster_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Verify the HA Status

Before you configure VDOM partitioning, you will check the HA synchronization status between NGFW-1 and NGFW-2.

To check the HA status

- 1. Log in to the NGFW-1 GUI with the username admin and password password.
- 2. Click **System** > **HA**, and then analyze the information displayed.

FortiGate VM64

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

NGFW-1 (Primary)

Refresh

Edit

Remove device from HA cluster

Status	Priority	Hostname	Serial No.	Role
Synchronized	200	NGFW-1	FGVM010000077649	Primary
Synchronized	100	NGFW-2	FGVM010000077650	Secondary

Two green check marks indicate both devices are in sync with each other, and NGFW-1 is acting as the primary and NGFW-2 is acting as a secondary device.



Ensure that both devices are in sync before moving to the next task.

Configure VDOM Partitioning

You will configure VDOM1 for virtual cluster 1 and VDOM2 for virtual cluster 2.

To configure VDOM partitioning

- 1. Continuing on the NGFW-1 GUI, click **System** > **HA**.
- 2. Select **NGFW-1**, and then click **Edit**.

FortiGate VM64

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

NGFW-1 (Primary)

Refresh

Edit

Remove device from HA cluster

Status	Priority	Hostname	Serial No.	Role
Synchronized	200	NGFW-1	FGVM010000077649	Primary
Synchronized	100	NGFW-2	FGVM010000077650	Secondary

- 3. Enable **VDOM Partitioning**.
- 4. Click **Create New**.
- 5. In the **New Virtual Cluster** window, change **Device priority** to 50, and then add **VDOM2** to the **Virtual domains** field.

Your configuration should look like the following example:

Mode

Active-Passive

Synchronize management VDOM

Cluster Settings

Group ID0

Group name

fortinet

Password

.....

Change

Session pickup

Heartbeat interfaces

port7

Management Interface Reservation

VDOM Partitioning

Create New

Edit

Delete

Search

Virtual Cluster	Override	Priority	VDOM	Monitor Interfaces
1		128	VDOM1 root	
2		50	VDOM2	

- 6. Click **OK**.
- 7. Click **OK**.

To verify the virtual clustering status

1. Continuing on the NGFW-1 GUI, click **System > HA**.
Your HA setup should look like the following example:

FortiGate VM64-KVM

FortiGate VM64-KVM

NGFW-1 (Primary)NGFW-2 (Secondary)

RefreshEditRemove device from HA cluster

Status	Priority	Hostname	Serial No.	Virtual Domains	Role
Virtual cluster 1					
Synchronized	128	NGFW-1	FGVM010000077649	VDOM1 root	Primary
Synchronized	100	NGFW-2	FGVM010000077650	VDOM1 root	Secondary
Virtual cluster 2					
Synchronized	50	NGFW-1	FGVM010000077649	VDOM2	Secondary
Synchronized	128	NGFW-2	FGVM010000077650	VDOM2	Primary

You should see NGFW-1 as the primary for virtual cluster 1 and NGFW-2 as the primary for virtual cluster 2.

Stop and think!

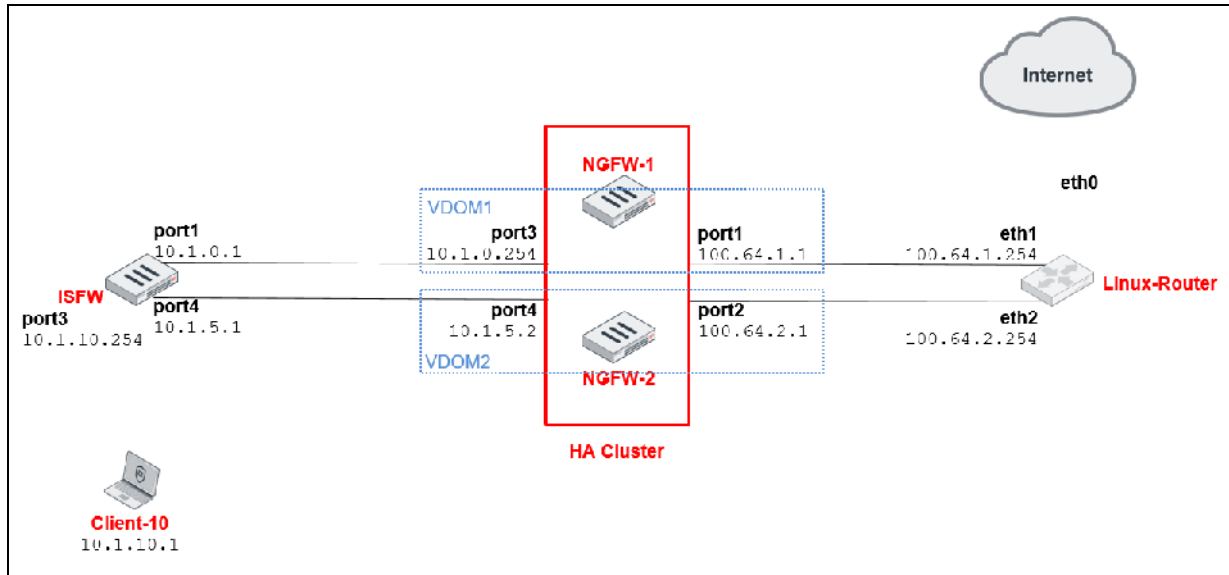
How did NGFW-2 become the primary for virtual cluster 2?

The default priority for virtual clusters is 128. On NGFW-1, we configured this priority as 50, which is lower than the default value. Because the priority is the deciding factor in selecting a primary device in our setup, the device with the highest priority is elected as the primary for a particular cluster.

Exercise 4: Analyzing Traffic Distribution

In this exercise, you will analyze traffic distribution across two virtual clusters. You will also perform a failover to make NGFW-1 the primary device to handle all traffic.

Network Topology



For this lab environment, we are simulating traffic through individual virtual clusters from Client-10. We configured routing on ISFW in such a way that traffic to 8.8.8.8 will pass through VDOM1 and traffic to 4.2.2.2 will pass through VDOM2.

For more information, review the interface and routing configuration on ISFW, NGFW-1, and NGFW-2.

Analyze Traffic Distribution

You will generate traffic by running a continuous ping from the Client-10 VM, and then analyze traffic distribution using the sniffer.

To generate traffic

1. On the Client-10 VM, open a terminal session, and then enter the following command to start a continuous ping to 8.8.8.8:

```
ping 8.8.8.8
```
2. Open a new terminal session, and then enter the following command to start a continuous ping to 4.2.2.2:

```
ping 4.2.2.2
```
3. Keep both terminal windows open and leave the ping running.

To analyze traffic for virtual cluster 1

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to view the active ICMP sessions on VDOM1:

```
config vdom
edit VDOM1
get system session list | grep icmp
```

You should see the session information for the continuous ping going to 8.8.8.8.

```
NGFW-1 (VDOM1) # get sys session list | grep icmp
icmp      59      10.1.10.1:3457    100.64.1.1:63873 8.8.8.8:8
```

To analyze traffic for virtual cluster 2

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to view the active ICMP sessions on VDOM2:

```
config vdom
edit VDOM2
get system session list | grep icmp
```

Stop and think!

Why do you not see traffic destined to 4.2.2.2?

You are sending 4.2.2.2 traffic through VDOM2, which belongs to virtual cluster 2. NGFW-2 is the primary device for virtual cluster 2. You must connect to NGFW-2 to see traffic destined to 4.2.2.2.

4. Continuing on the same SSH session, enter the following commands to connect to NGFW-2:

```
end
config global
execute ha manage 0 admin
```

5. At the prompt, type the password `password`, and then press `Enter`.
6. Enter the following commands to view the active ICMP sessions on VDOM2:

```
config vdom
edit VDOM2
get system session list | grep icmp
```

You should see session information for the continuous ping going to 4.2.2.2.

```
NGFW-2 (VDOM2) # get sys session list | grep icmp
icmp      59      10.1.5.1:63872    100.64.2.1:63872 4.2.2.2:8
```

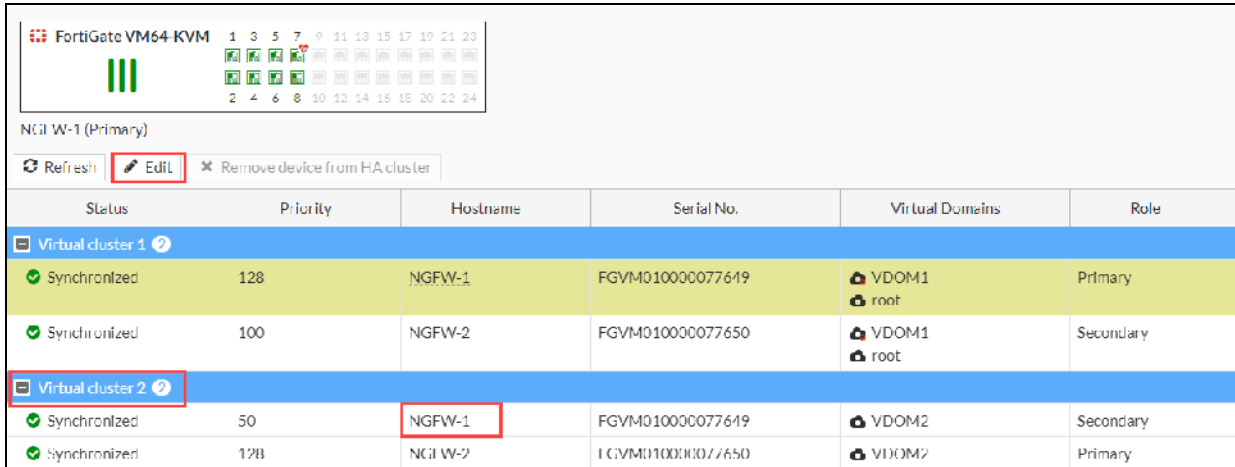
7. Close the SSH window.

Perform a Failover and Analyze the Traffic

You will perform a manual failover for virtual cluster 2 by increasing the priority for NGFW-1. Then, you will analyze the traffic.

To perform a manual failover

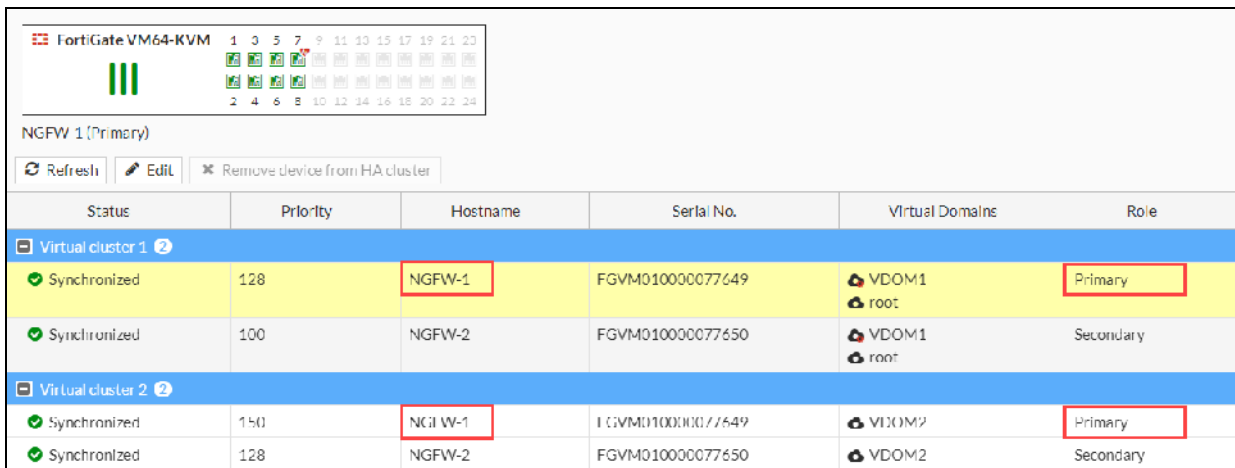
1. Continuing on the NGFW-1 GUI, click **System > HA**.
2. Select **NGFW-1** for virtual cluster 2, and then click **Edit**.



Status	Priority	Hostname	Serial No.	Virtual Domains	Role
Virtual cluster 1					
Synchronized	128	NGFW-1	FGVM010000077649	VDOM1 root	Primary
Synchronized	100	NGFW-2	FGVM010000077650	VDOM1 root	Secondary
Virtual cluster 2					
Synchronized	50	NGFW-1	FGVM010000077649	VDOM2	Secondary
Synchronized	128	NGFW-2	FGVM010000077650	VDOM2	Primary

3. In the **VDOM partitioning** field, select **2**, click **Edit**, and then change the **Device priority** field to 150.
4. Click **OK**.
5. Click **OK** to save the **HA** settings.

After you change the priority, you should see NGFW-1 as the primary for both virtual clusters.



Status	Priority	Hostname	Serial No.	Virtual Domains	Role
Virtual cluster 1					
Synchronized	128	NGFW-1	FGVM010000077649	VDOM1 root	Primary
Synchronized	100	NGFW-2	FGVM010000077650	VDOM1 root	Secondary
Virtual cluster 2					
Synchronized	150	NGFW-1	FGVM010000077649	VDOM2	Primary
Synchronized	128	NGFW-2	FGVM010000077650	VDOM2	Secondary

To analyze traffic after a failover



After the failover, NGFW-1 will process all traffic.

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to view the active ICMP sessions on VDOM2:

```
config vdom
edit VDOM2
get system session list | grep icmp
```

You should see that the session for 4.2.2.2 is now active on NGFW-1.

```
NGFW-1 (VDOM2) # get sys session list | grep icmp
icmp      59      10.1.5.1:63872   100.64.2.1:63872 4.2.2.2:8
```

4. You can now close the session window.

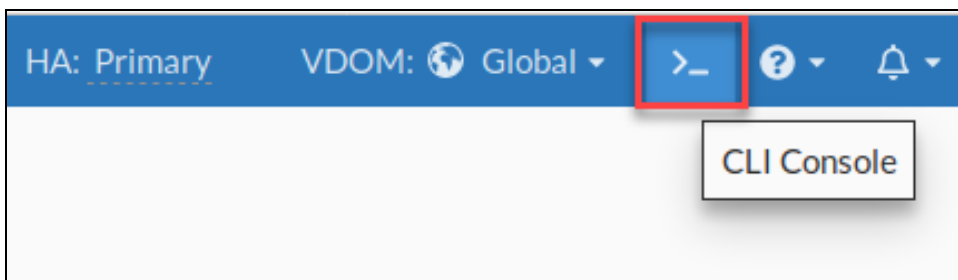
Reset the NGFW-2 Cluster Member to Factory Settings



Before you begin the next lab, you *must* reset the NGFW-2 cluster member to factory settings.

To reset the NGFW-2 cluster member to factory settings

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click `>_` to open the **CLI Console** window from the GUI.



3. On the CLI, enter the following command:

```
execute ha manage 0 admin
```
4. When you are prompted for the password to access NGFW-2, enter the password `password`.
The prompt changes to reflect that you are now logged in to NGFW-2.
5. Enter the following commands:

```
config global
```

```
execute factoryreset keepvmlicense
```

6. When you are asked to confirm that you want to reset this FortiGate device, enter `y`.
The reset proceeds.
7. In the upper-right corner, click **X** to close the CLI window.

Lab 5: Central Management

FortiManager is one of the key pieces of an enterprise firewall solution. Without it, managing multiple FortiGate devices would be cumbersome. Using FortiManager, you can centralize the management of all FortiGate devices and create common security policies that can be shared easily by multiple devices. In enterprise networks, FortiManager ADOMs are used to organize your FortiGate devices into groups whose members all share similar security roles and policies.

Objectives

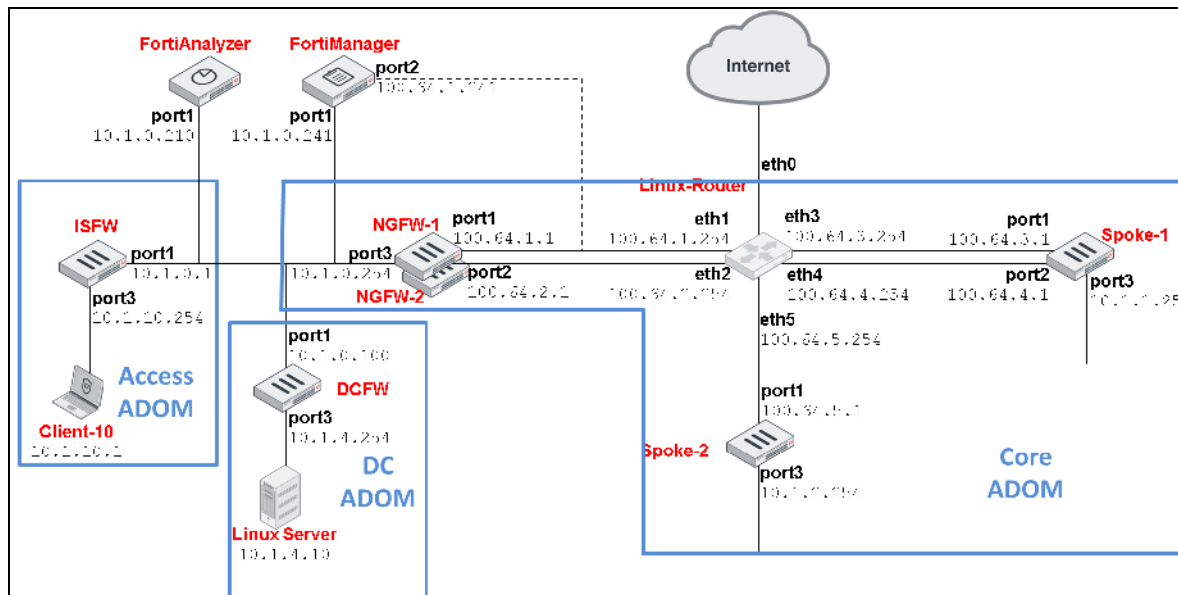
- Configure FortiGate devices and FortiManager to centralize the management of the enterprise network
- Use ADOMs to group FortiGate devices based on their security roles in the enterprise network

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

In this lab, you will configure the NGFW-1, DCFW, and ISFW to use FortiManager for central management. Because the security roles of the three firewalls are different, they will be assigned to different FortiManager ADOMs. Three ADOMs have already been created on FortiManager. The **Core** ADOM will contain NGFW-1, Spoke-1, and Spoke-2. The **Access** ADOM will contain ISFW. The Data Center (**DC**) ADOM will contain DCFW. Spoke-1 and Spoke-2 are already registered to FortiManager and added to the **Core** ADOM. You will add the other FortiGate devices.

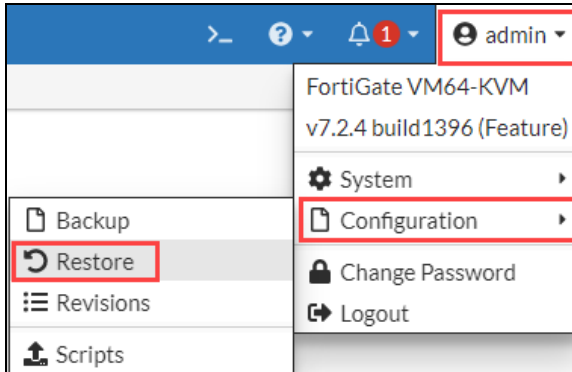


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

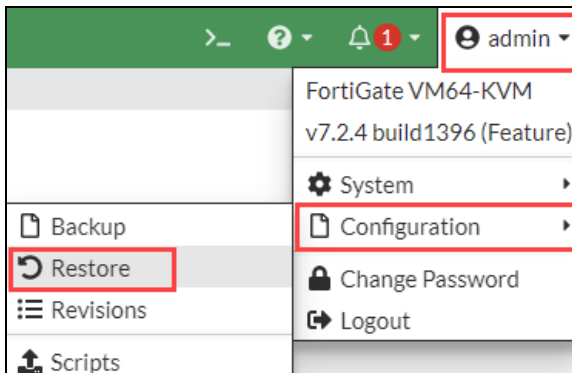
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI at 10.1.0.254 with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > Central_Management**, select `NGFW-1_Central_Management_initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the DCFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the DCFW GUI at 10.1.0.100 with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.

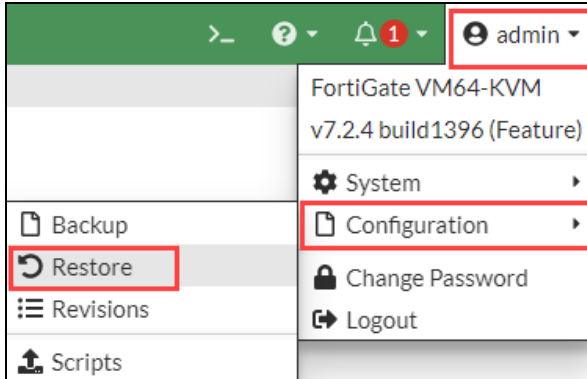


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > Central_Management**, select `DCFw_Central_Management_initial.conf`, and then click **Open**.

5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW GUI at 10.1.10.254 with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > Enterprise-FW > Central_Management**, select `ISFW_Central_Management_initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Registering FortiGate Devices on FortiManager

You will register three FortiGate devices (NGFW-1, DCFW, and ISFW) on FortiManager.

Register NGFW-1 on FortiManager

You will register NGFW-1 on FortiManager. After that, you will import the policies.



To simplify the setup process for these labs, the FortiGate devices have been preconfigured to validate their licenses on the local FortiManager. For this reason, the FortiGate devices are listed initially as `unregistered` on FortiManager. FortiManager adds a FortiGate to the unregistered list each time an unknown FortiGate contacts FortiManager for any reason.

In this case, the FortiGate devices contact FortiManager when they boot to validate the licenses. As a result, the auto-discovery method for registering FortiGate devices on FortiManager will not work until the administrator manually deletes the devices from the unregistered list.

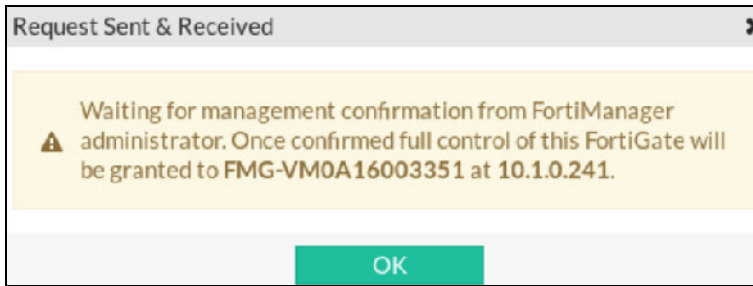
One alternative, which is what you will do in this lab, is to use the manual registration method.

To add FortiManager to the NGFW-1 configuration

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors** > **Central Management**, and then click **Edit**.
3. In the **IP/Domain name** field, type the FortiManager IP address `10.1.0.241`.

Central Management Settings	
Settings	Info
Status	☒ Enabled ☐ Disabled
Type	☒ On-Premises ☐ FortiGate Cloud ☐ FortiManager Cloud
Connection status	☒ Not Managed Refresh
Mode	☒ Normal ☐ Backup
IP/Domain name	10.1.0.241 +

4. Click **OK**.
The system displays the following message:



5. Click **OK**.
6. In the system message window that indicates that this FortiGate isn't authorized on FortiManager, click **Close**. You will authorize devices directly on FortiManager.

To register NGFW-1 on FortiManager

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **Device Manager**.
4. Click **Unauthorized Devices**.

Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode
FGVM010000077646	FortiGate-VM64	FGVM010000077646	10.1.0.19443	FortiGate 7.2, build 1396	Configuration & Logging
FGVM010000077648	FortiGate-VM64	FGVM010000077648	10.1.0.100-9443	FortiGate 7.2, build 1396	Configuration & Logging
FGVM010000077649	FortiGate-VM64-KVM	FGVM010000077649	10.1.0.254	FortiGate 7.2.4, build 1396 (GA)	Configuration & Logging
FGVM010000077650	FortiGate-VM64	FGVM010000077650	10.1.0.253.9443	FortiGate 7.2, build 1396	Configuration & Logging

5. Select **FGVM010000077649**, and then click **Authorize**.
6. In the **Add the following device(s) to ADOM** field, select **Core**.
7. Rename the device to **NGFW-1**.

Device Name	Assign New Device Name	Assign Policy Package	Assign Provisioning Template	Assign Dashboard Config
FGVM010000077...	NGFW-1	Click to select	+	Click to select

8. Click **OK**.
Wait until FortiManager finishes registering the device.
9. Click **Close**.

To import the NGFW-1 policies

1. Continuing on the FortiManager GUI, click **ADOM: root**.



2. Click **Core**.
3. Click **NGFW-1** to select it, and then click **Import Configuration**.

☐	Device Name	Config Status	Host Name	IP Address	
☒	NGFW-1	✓ Synchronized	NGFW-1	10.1.0.254	
☐	Spoke-1	✓ Auto-update	Spoke-1	100.64.3.1	
☐	Spoke-2	✓ Synchronized	Spoke-2	100.64.5.1	

4. Select the **Import Policy Package** checkbox, and then click **Next**.

Import Device - NGFW-1 - Select Import Type (1/1)

☒ **Import Policy Package**
Import policy package used by the selected device.

☐ **Import AP Profiles or FortiSwitch Templates**
Automatically import FortiAP profile and FortiSwitch template from selected device. For objects have the same name, configuration from device database will be used.

Next >
Cancel

5. Keep the default values for the **Policy Package Name** and **Folder**, and then select **Import All (3)** and **Import only policy dependent objects**.
6. Configure the following interface mappings as **Per-Device**:

Device Interface	Normalized Interface
port1	external
port2	backup
port3	internal

Import Device - NGFW-1 - Interface Mapping & Policy (2/5)

Create a new policy package for import.

Policy Package Name: NGFW-1

Folder: root

Policy Selection: **Import All (3)** Select Policies to Import

Object Selection: **Import only policy dependent objects** Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Search...

Device Interface	Mapping Type		Normalized Interface	
port1	Per-Device	Per-Platform	external	
port2	Per-Device	Per-Platform	backup	
port3	Per-Device	Per-Platform	internal	

- Click **Next**.
The import wizard reports conflicts.
- Keep the default values for the FortiGate, and then click **Next**.

Import Device - NGFW-1 - Object Conflicts (3/5)

The following objects were found having conflicts. Please confirm your settings, then continue.

Conflicts (2)

Download Conflict File

Search...

Category	Name	Use Value From	
		FortiGate	FortiManager
Firewall Profile-Protocol-Options (1)	default	FortiGate	FortiManager View Conflicts
Firewall SSL-SSH-Profile (1)	nc-inspection	FortiGate	FortiManager View Conflicts

2

Next > Cancel

- Click **Next**.
- Click **Next**.
Wait until FortiManager finishes importing the policies.
- Click **Finish**.
- Select **NGFW-1** again, and then click **Edit**.
- Configure the following settings:

Field	Value
Admin user	admin
Password	password

14. Click **OK**.

Register DCFW on FortiManager

You will register DCFW on FortiManager. Try to do it yourself using the procedure you followed to register NGFW.

To register DCFW on FortiManager

1. Add FortiManager to the FortiGate configuration.
2. Register FortiGate on FortiManager—use the device name **DCFW** and add it to the **DC** ADOM.
3. Import the policies—use the following interface mappings as **Per-Device**:

Device Interface	Normalized Interface
port1	external
port3	internal

Register ISFW on FortiManager

You will register ISFW on FortiManager. Try to do it yourself using the procedure you followed to register NGFW.

To register ISFW on FortiManager

1. Add FortiManager to the FortiGate configuration.
2. Register FortiGate on FortiManager—use the device name **ISFW** and add it to the **Access** ADOM.
3. Import the policies—use the same interface mappings you used for DCFW.

Device Interface	Normalized Interface
port1	external
port3	internal

Check the FortiGate Registrations

You will confirm that all FortiGate devices are registered to the correct FortiManager ADOM. You will also check that the policies were imported correctly.

To check the FortiGate registrations

1. Connect over SSH to FortiManager.
2. Log in with the username admin and password password.
3. Enter the following command:
diagnose dvm device list
4. Read the output and confirm that there are five devices being managed.
5. Confirm that each FortiGate is registered to the correct ADOM.

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE          OID      SN              HA      IP      NAME      ADOM      IPS      FIRMWARE
fmgfaz-managed 309      FGVM010000077648 - 10.1.0.100 DCFW      DC        6.00741 (regular) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:DC pkg:[imported]DCFW
unregistered   285      FGVM010000077650 - 10.1.0.253:9443 FGVM010000077650 root      N/A      7.0 MR2 (1396)
| - STATUS: dev-db: unknown; conf: unknown; cond: unregistered; dm: none; conn: unknown
| - vdom:[3]root flags:0 adom:root pkg:[never-installed]
fmgfaz-managed 273      FGVM010000077646 - 10.1.0.1 ISFW      Access    6.00741 (regular) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:Access pkg:[imported]ISFW
fmgfaz-managed 297      FGVM010000077649 a-p 10.1.0.254 NGFW-1     Core      6.00741 (regular) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:Core pkg:[imported]NGFW-1
HA cluster member: FGVM010000077649 (primary); conn: up; conf: in sync
fmgfaz-managed 321      FGVM010000077651 - 100.64.3.1 Spoke-1    Core      6.00741 (extended) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
| - vdom:[3]root flags:0 adom:Core pkg:[unknown]Spokes
fmgfaz-managed 333      FGVM010000077652 - 100.64.5.1 Spoke-2    Core      6.00741 (extended) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:Core pkg:[unknown]Spokes
```

6. Confirm that the policies for each FortiGate were imported to the correct policy package.

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE          OID      SN              HA      IP      NAME      ADOM      IPS      FIRMWARE
fmgfaz-managed 309      FGVM010000077648 - 10.1.0.100 DCFW      DC        6.00741 (regular) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:DC pkg:[imported]DCFW
unregistered   285      FGVM010000077650 - 10.1.0.253:9443 FGVM010000077650 root      N/A      7.0 MR2 (1396)
| - STATUS: dev-db: unknown; conf: unknown; cond: unregistered; dm: none; conn: unknown
| - vdom:[3]root flags:0 adom:root pkg:[never-installed]
fmgfaz-managed 273      FGVM010000077646 - 10.1.0.1 ISFW      Access    6.00741 (regular) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:Access pkg:[imported]ISFW
fmgfaz-managed 297      FGVM010000077649 a-p 10.1.0.254 NGFW-1     Core      6.00741 (regular) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:Core pkg:[imported]NGFW-1
HA cluster member: FGVM010000077649 (primary); conn: up; conf: in sync
fmgfaz-managed 321      FGVM010000077651 - 100.64.3.1 Spoke-1    Core      6.00741 (extended) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
| - vdom:[3]root flags:0 adom:Core pkg:[unknown]Spokes
fmgfaz-managed 333      FGVM010000077652 - 100.64.5.1 Spoke-2    Core      6.00741 (extended) 7.0 MR2 (1396)
| - STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
| - vdom:[3]root flags:0 adom:Core pkg:[unknown]Spokes
```

Stop and think!

You might have noticed that Spoke-1 and Spoke-2 are sharing the same policy package (**Spokes**). Why?

Spoke-1 and Spoke-2 should always share the same security policies so they can share the same policy package. This simplifies management, as you will see later. Each change made in the **Spoke** policy package is applied to both spokes automatically.

Lab 6: OSPF

In this lab, on FortiManager, you will configure the FortiGate devices to use OSPF as the dynamic routing protocol for the enterprise network. You will also configure BFD to monitor OSPF neighbors to detect one-way failure faster.

Objectives

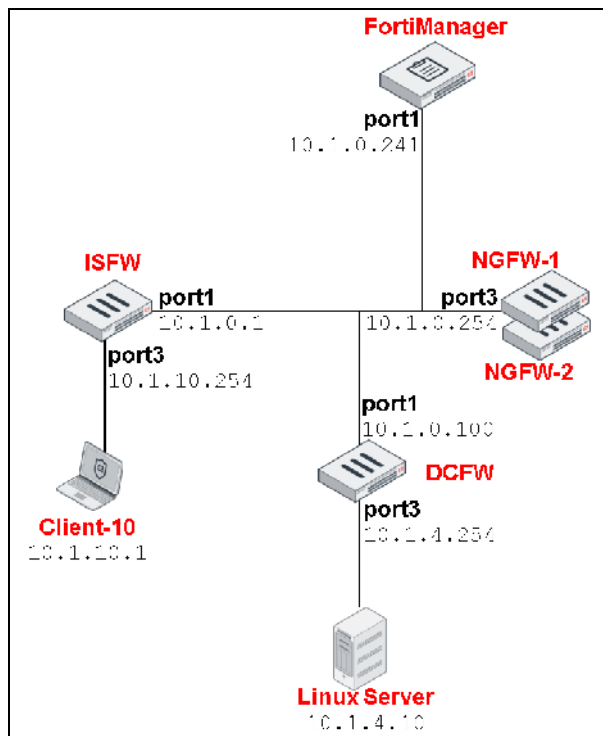
- Use OSPF to dynamically distribute the routes inside an enterprise network
- Diagnose the status of an OSPF network
- Implement BFD routing to monitor OSPF routing operations
- Trigger a one-way failure to reflect the status of the OSPF neighbors

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

On FortiManager, you will configure OSPF and BFD between ISFW, DCFW, and NGFW-1.



Prerequisites

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

Exercise 1: Configuring OSPF

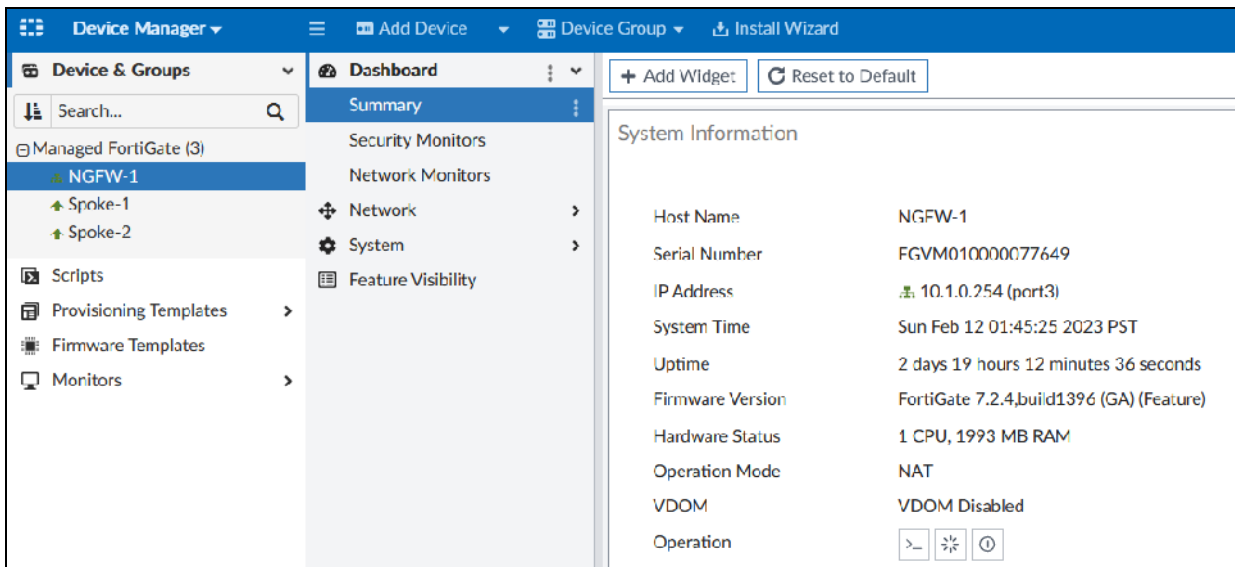
In this exercise, you will configure OSPF on the three FortiGate devices that are part of the hub network: ISFW, DCFW, and NGFW-1. The objective is to remove all static routes from the three firewalls and use only OSPF to route traffic internally. You will use a single OSPF area (0.0.0.0).

Configure OSPF on NGFW-1

You will configure OSPF on NGFW-1. Next, you will remove the two static routes, and then install the changes.

To configure OSPF

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **Device Manager**.
4. Click **NGFW-1** to display its dashboard.



5. Click **Network > OSPF**.
6. In the **Router ID** field, type 0.0.0.1.
7. Create a new area, and configure the following settings:

Field	Value
Area	0.0.0.0
Type	Regular
Authentication	None

8. Click **OK**.
9. Create a new network, and configure the following settings:

Field	Value
IP/Netmask	10.1.0.0/24
Area	0.0.0.0

10. Click **OK**.
11. Click **Apply**.

To remove the static routes

1. Continuing on the FortiManager GUI, click **Network > Static Routes**.
2. Select the two static routes used to route internal traffic (don't select the default routes), and then click **Delete**.

Dashboard	+	Create New	Edit	Clone	Delete	Search...
Network						
Interfaces						
IPAM						
SD-WAN						
Static Routes						
OSPF						

	#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
Static Route (4)									
☒	1	1	10.1.10.0/255.255.255.0	10.1.0.1	port3	10	1	Enable	
☐	2	2	0.0.0.0/0.0.0.0	100.64.1.254	port1	10	1	Enable	
☒	3	3	10.1.4.0/255.255.255.0	10.1.0.100	port3	10	1	Enable	
☐	4	4	0.0.0.0/0.0.0.0	100.64.2.254	port2	10	21	Enable	

3. Click **OK** to confirm.

To install the configuration changes

1. Continuing on the FortiManager GUI, in the **Device Manager** of the **Core ADOM**, click **Managed FortiGate**.
2. Observe the **Config Status** of **NGFW-1**.
It should appear as **Modified**.
3. Click **NGFW-1** to select it, and then click **Install > Install Wizard**.

Edit	Delete	Import Configuration	Install	Table View
------	--------	----------------------	---------	------------

	Device Name	Config Status	Host Name	IP
☒	NGFW-1	Modified	NGFW-1	10.1.0.1
☐	Spoke-1	Auto-update	Spoke-1	100.64.1.254
☐	Spoke-2	Synchronized	Spoke-2	100.64.2.254

4. Verify that the **Install Device Settings (only)** page is displayed, and then click **Next**.
5. Verify that only **NGFW-1** is selected, and then click **Next**.
6. Click **Install**.
Wait until the installation finishes.
7. Click **Finish**.

The **Config Status** of **NGFW-1** changes to **Synchronized**.

Configure OSPF on DCFW

You will configure OSPF on DCFW through FortiManager. Try to do this yourself using the procedure you followed to configure OSPF on NGFW-1.

To configure OSPF on DCFW

1. On the FortiManager **DC** ADOM, configure OSPF on DCFW using the following settings:

Field	Value
Router ID	0.0.0.2
Area	0.0.0.0
Network	10.1.4.0/24 and 10.1.0.0/24

2. Delete the static route used to route internal traffic (don't select the default route).
3. Install the configuration changes for DCFW.

Configure OSPF on ISFW

You will configure OSPF on ISFW through FortiManager. Try to do this yourself using the procedure you followed to configure OSPF on NGFW-1.

To configure OSPF on ISFW

1. On the FortiManager **Access** ADOM, configure OSPF on ISFW using the following settings:

Field	Value
Router ID	0.0.0.3
Area	0.0.0.0
Network	10.1.10.0/24 and 10.1.0.0/24

2. Delete the static route used to route internal traffic (don't select the default route).
3. Install the configuration changes for ISFW.

Check the OSPF Status on NGFW-1

You will run the OSPF diagnostic commands on NGFW-1 to verify OSPF operation.

To check the OSPF status on NGFW-1

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

```
get router info ospf neighbor
```

You should see that NGFW-1 has two neighbors: DCFW and ISFW. The `State` column should display `Full`.

```
NGFW-1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID    Pri   State           Dead Time   Address      Interface
0.0.0.3        1     Full/DRother    00:00:32    10.1.0.1     port3
0.0.0.2        1     Full/Backup     00:00:34    10.1.0.100   port3
```

Stop and think!

The three FortiGate devices are connected to the same broadcast network (`10.1.0.0/24`). Can you identify from this output what the designated router (DR) is?

The `State` of the designated router is displayed as `Full/DR`. If neither of the two routers display this state, it means that the designated router is the local FortiGate which, in this case, is NGFW-1.

4. Enter the following command:

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

You should see that NGFW has learned the routes to subnets `10.1.4.0/24` and `10.1.10.0/24` through OSPF.

```
NGFW-1 # 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 100.64.1.254, port1, [1/0]
      [10/0] via 100.64.2.254, port2, [21/0]
C     10.1.0.0/24 is directly connected, port3
O     10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:07:34, [1/0]
O     10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:02:25, [1/0]
C     100.64.1.0/24 is directly connected, port1
C     100.64.2.0/24 is directly connected, port2
C     172.16.100.0/24 is directly connected, port8
```

Check the OSPF Status on DCFW and ISFW

You will run OSPF diagnostic commands on DCFW and ISFW to verify OSPF operation.

Take the Expert Challenge!

1. Connect over SSH to DCFW.
2. Enter the following commands to verify OSPF operation on DCFW:
 - `get router info ospf neighbor`
 - `get router info routing-table all`
3. Connect over SSH to ISFW.
4. Enter the following commands to verify OSPF operation on ISFW:
 - `get router info ospf neighbor`
 - `get router info routing-table all`

After you complete the challenge, see [Check Connectivity on page 73](#).

Check Connectivity

You will confirm that the FortiGate devices are routing traffic properly by running a ping from Client-10 to the Linux server.

To check connectivity

1. On the Client-10 VM, open a terminal window.
2. Run a ping to the Linux server (10.1.4.10).

The ping should succeed, confirming that the FortiGate devices are correctly routing the traffic between the 10.1.10.0/24 and 10.1.4.0/24 subnets.

Exercise 2: Configuring BFD

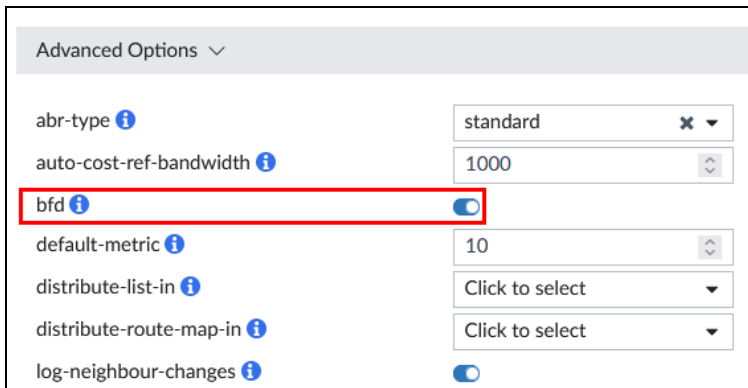
You will configure bidirectional forwarding detection (BFD) routing for OSPF for faster convergence of the routing protocol when detecting a one-way device failure. The objective is to configure BFD on the OSPF interfaces that participate in the dynamic routing protocol, as well as on OSPF routing settings on each FortiGate, and then test a one-way failure scenario.

Configure BFD on NGFW-1

You will configure BFD at the OSPF protocol level and interface level on NGFW using the advanced options on FortiManager, and then install the changes.

To configure BFD at the OSPF protocol level

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **Device Manager**.
4. Click **NGFW-1** to display its dashboard.
5. Click **Network > OSPF**.
6. Expand the **Advanced Options** section, and then enable **bfd**.



The screenshot shows the 'Advanced Options' section of the FortiManager GUI for OSPF configuration. The 'bfd' option is highlighted with a red box and is enabled (indicated by a blue toggle switch). Other options visible include 'abr-type' set to 'standard', 'auto-cost-ref-bandwidth' set to '1000', 'default-metric' set to '10', 'distribute-list-in' set to 'Click to select', 'distribute-route-map-in' set to 'Click to select', and 'log-neighbour-changes' set to 'off'.

7. Click **Apply**.

To configure BFD at the interface level

1. Continuing on the FortiManager GUI, click **Network > Interfaces**.
2. Select **port3**, and then click **Edit**.
3. Expand the **Advanced Options** section.
4. In the **bfd** field, select **enable**.
5. Click **OK**.
6. Click **OK** to save the new normalized interface mapping.

To install the configuration changes

1. Continuing on the FortiManager GUI, in the **Device Manager** of the **Core ADOM**, click **Managed FortiGate**.
2. Observe the **Config Status** of **NGFW-1**.
It should appear as **Modified**.
3. Click **NGFW-1** to select it, and then click **Install > Install Wizard**.

Edit Delete Import Configuration Install Table View				
☐	Device Name	Config Status	Host Name	IP
☒	NGFW-1	Modified	NGFW-1	10.0.0.1
☐	Spoke-1	Auto-update	Spoke-1	10.0.0.2
☐	Spoke-2	Synchronized	Spoke-2	10.0.0.3

4. Verify that the **Install Device Settings (only)** page is displayed, and then click **Next**.
5. Verify that only **NGFW-1** is selected, and then click **Next**.
6. Click **Install**.
Wait until the installation finishes.
7. Click **Finish**.
The **Config Status** of **NGFW-1** changes to **Synchronized**.

Configure BFD on DCFW

You will configure BFD at the OSPF protocol level and interface level on DCFW. Try to do this yourself using the procedure you followed to configure BFD on NGFW-1.

To configure BFD at the OSPF protocol level and interface level

1. On the FortiManager **DC ADOM**, click **DCFW** to display its dashboard.
2. Enable BFD at the OSPF protocol level and the **port1** interface level.
3. Install the configuration changes for DCFW.

Configure BFD on ISFW

You will configure BFD at the OSPF protocol level and interface level on ISFW. Try to do this yourself using the procedure you followed to configure BFD on NGFW-1.

To configure BFD at the OSPF protocol level and interface level

1. On the FortiManager **Access ADOM**, click **ISFW** to display its dashboard.
2. Enable BFD at the OSPF protocol level and the **port1** interface level.
3. Install the configuration changes for ISFW.

Test BFD Detection of a Neighbor Failure

You will run the BFD diagnostic commands on NGFW-1 to verify the OSPF routing table and BFD neighbor details. The objective is to replicate a one-way failure on DCFW using a preconfigured local-in policy on DCFW to block BFD UDP packets and trigger a failure.

To check the current BFD status on NGFW-1

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

```
get router info bfd neighbor
```

You should see that NGFW-1 has two neighbors: DCFW and ISFW. The `State` column should display `UP`.



Don't close the SSH session.

```
NGFW-1 # get router info bfd neighbor
```

OurAddress	NeighAddress	State	Interface	LDesc/RDesc
10.1.0.254	10.1.0.100	UP	port3	2/2
10.1.0.254	10.1.0.1	UP	port3	1/2

To enable a local-in policy on DCFW

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **DC**.
3. Click **Policy & Objects**.
4. Click **DCFW > IPv4 Local In Policy**.



If you can't see **IPv4 Local In Policy**, you can enable it using the following steps:

1. Click **Tools > Feature Visibility**.
2. In the **Policy** section, enable **IPv4 Local In Policy**.
3. Click **OK**.

5. Right-click the policy ID **1**, and then click **Enable**.
6. Click **Install Wizard**.
7. Verify that the **Install Policy Package & Device Settings** page is displayed, and then click **Next**.
8. Click **Next**, and then click **Install**.

To check the updated BFD status on NGFW-1

1. On the NGFW-1 CLI, enter the following command:

```
get router info bfd neighbor
```

You should see that NGFW-1 has updated the `State` column for one of its neighbors, which should display `DOWN`.

```
NGFW-1 # get router info bfd neighbor
```

OurAddress	NeighAddress	State	Interface	LDesc/RDesc
10.1.0.254	10.1.0.100	DOWN	port3	4/11
10.1.0.254	10.1.0.1	UP	port3	3/7



This should result in the routing entries for this OSPF neighbor being removed from the OSPF routing table.

However, due to limitations in the current lab setup, you created only a one-way failure, by blocking the incoming BFD packets on DCFW. This made BFD on the other routers detect this router as dead, and then update its BFD state to `DOWN`.

The OSPF protocol eventually receives updated link state advertisements (LSAs) from DCFW, and then updates the routing table, which makes DCFW available again.

Lab 7: BGP

In this lab, you will configure BGP routing between NGFW-1 and Linux-Router. You will also configure a loopback interface on NGFW-1 as a BGP source.

Objectives

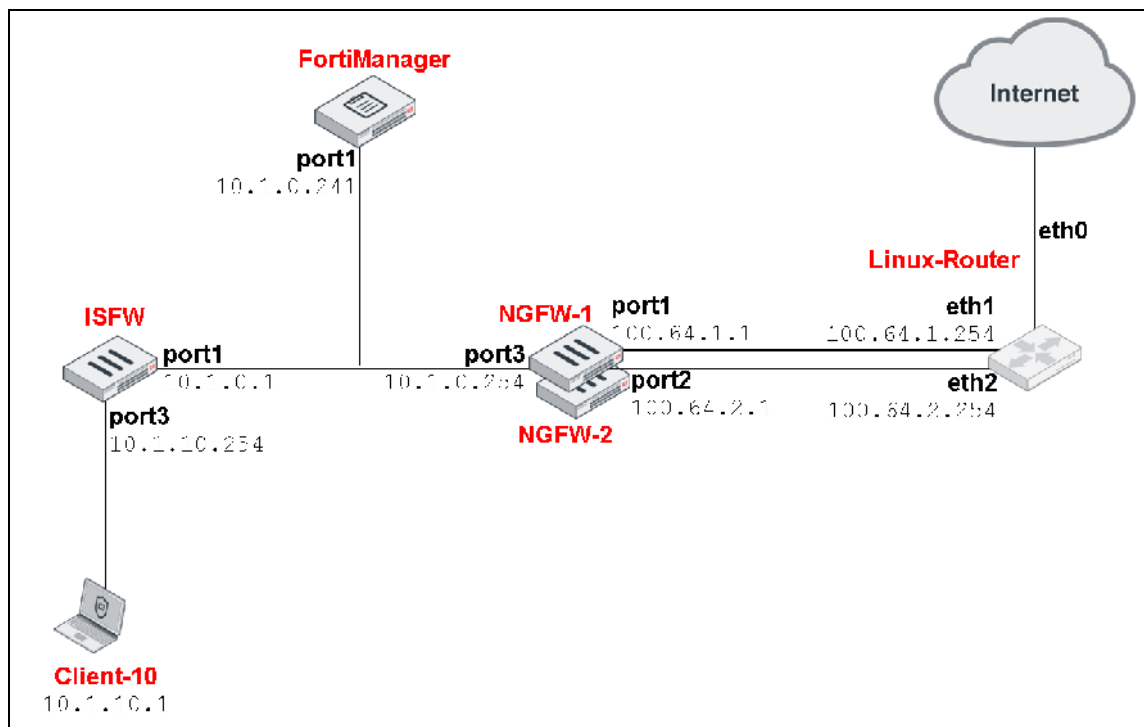
- Configure BGP using FortiManager
- Diagnose the status of a BGP network
- Implement a loopback interface as a BGP source

Time to Complete

Estimated: 35 minutes

Which Network Segment Will You Work On?

In this lab, you will configure NGFW-1 and ISFW using FortiManager.



Prerequisites

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

Exercise 1: Configuring BGP

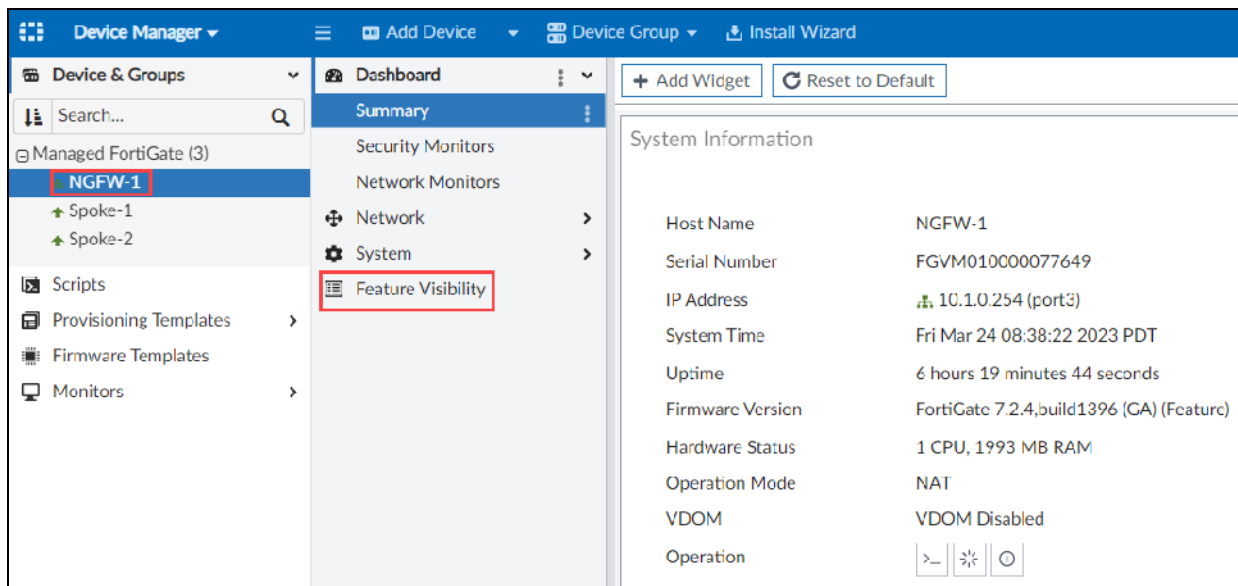
NGFW-1 has two connections to the internet—one using port1 and the other using port2. Linux-Router is the ISP router and is advertising default routes using BGP. You will configure BGP on NGFW-1 to receive the two default routes from the ISP.

Configure BGP on NGFW-1

Since NGFW-1 is currently managed by FortiManager, you must perform the BGP configuration on FortiManager, and then install it on NGFW-1. You will also delete the static default routes currently installed on NGFW-1. By default, the BGP settings are hidden on the FortiManager GUI. The first step is to display the BGP settings.

To display the BGP settings on the FortiManager GUI

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **Device Manager**.
4. Click **NGFW-1**.



5. Click **Feature Visibility**.
6. Click **Customize**.
7. In the **Network** section, select the **BGP** checkbox.

8. Click **OK**.

To configure BGP

1. Continuing on the FortiManager GUI, click **Network > BGP**.
2. Configure the following settings:

Field	Value
Local AS	65100
Router ID	172.16.1.254

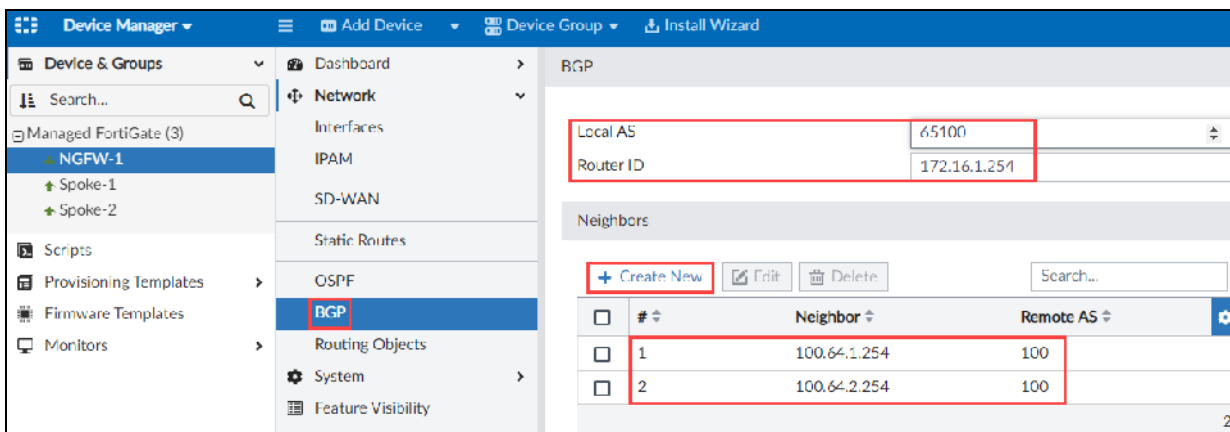
3. Create a neighbor with the following settings:

Field	Value
IP	100.64.1.254
Remote AS	100

4. Click **OK**.
5. Create a second neighbor with the following settings:

Field	Value
IP	100.64.2.254
Remote AS	100

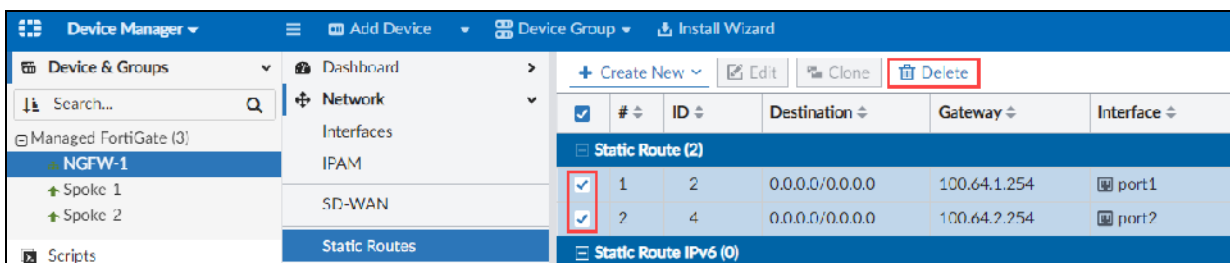
6. Click **OK**.



7. Click **Apply**.

To remove the static routes

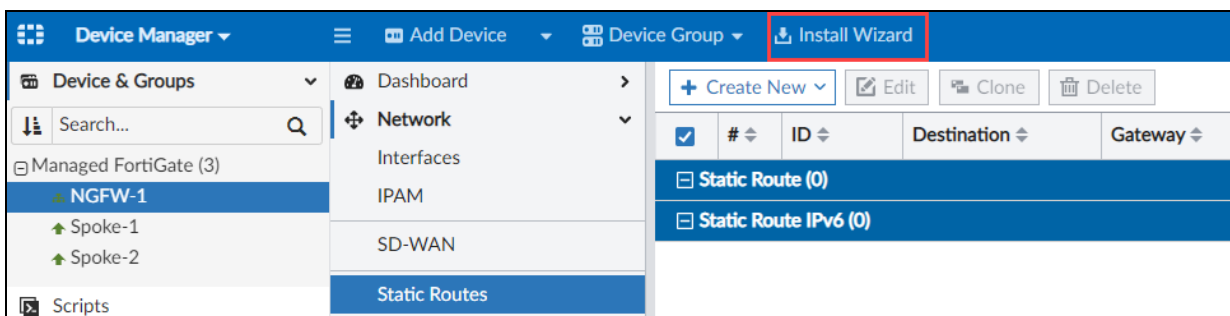
1. Continuing on the FortiManager GUI, click **Network > Static Routes**.
2. Click the two default static routes to select them, and then click **Delete**.



3. Click **OK**.

To install the BGP configuration

1. Continuing on the FortiManager GUI, click **Install Wizard**.



2. Verify that **Install Device Settings (only)** is displayed, and then click **Next**.
3. Verify that **NGFW-1** is selected, and then click **Next**.
4. Click **Install**.
Wait until the installation finishes.
5. Click **Finish**.



You can check the installation and BGP status on NGFW-1 using the following commands:

```
get router info bgp summary  
get router info bgp neighbor
```

Exercise 2: Configuring Prefix Lists

In this exercise, you will create a prefix list denying the subnet 8.8.8.8/32, and then apply it to the prefixes learned from the ISP.

Check the Routing

The ISP (Linux-Router) is mistakenly advertising the prefix 8.8.8.8/32 through one of the links. You will use routing and BGP CLI commands on NGFW-1 to check the 8.8.8.8/32 route.

To verify the routing

1. On NGFW-1, use the built-in sniffer on a ping from Client-10 to 8.8.8.8.
2. Enter the following commands to check the routing table:

```
get router info routing-table all  
get router info routing-table database
```



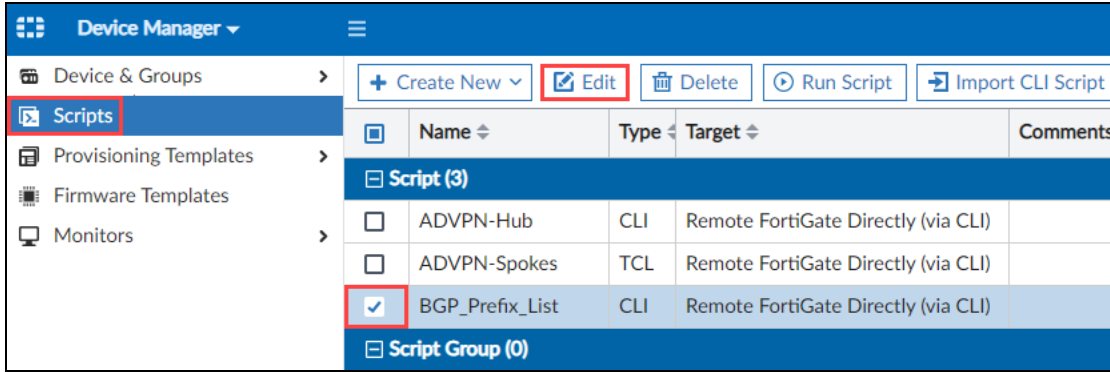
The administrator expects the default BGP route using port1 to be the primary link for all internet traffic. This verification shows that all traffic destined for the IP address 8.8.8.8 is using port2 instead.

Create a Prefix List

Prefix lists are available only using the CLI. You will run a script from FortiManager to configure one prefix list on NGFW-1.

To create a prefix list

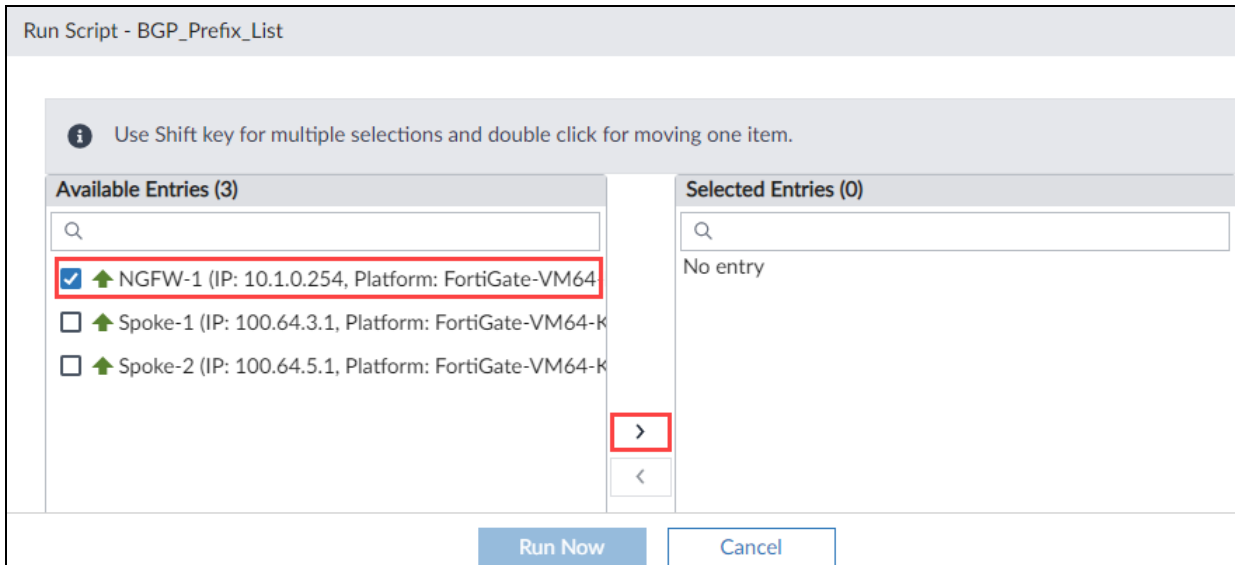
1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **Device Manager**.
4. Click **Scripts**.
5. Select the **BGP_Prefix_List** script, and then click **Edit**.



- View the CLI commands in the script.



- Click **Cancel**.
- Right-click the **BGP_Prefix_List** script, and then select **Run Script**.
- Move **NGFW-1** from the **Available Entries** section to the **Selected Entries** section, and then click **Run Now**.



10. Make sure NGFW-1 is the only device listed in the pop-up window, and then click **OK**.
11. Wait for the script to finish running.
The script has been configured to apply the CLI commands directly on FortiGate.
12. Click **Close**.

Clear the BGP Connections

You will clear the BGP connections so the new prefix list can take effect.

To clear the BGP connections

1. Return to the NGFW-1 CLI, and then enter the following command:

```
execute router clear bgp all
```



The traffic is affected when you execute this command, so you must use it with caution.

Verify the Prefix List

You will verify that the prefix list is working as expected.

To verify the prefix list

1. Continuing on the NGFW-1 CLI, enter the following command:

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

```
NGFW-1 # 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
B* 0.0.0.0/0 [20/0] via 100.64.1.254 (recursive is directly connected, port1,
    00:01:26, [1/0])
C 10.1.0.0/24 is directly connected, port3
O 10.1.4.0/24 [110/2] via 10.1.0.100, port3, 01:18:51, [1/0]
O 10.1.10.0/24 [110/2] via 10.1.0.1, port3, 01:28:51, [1/0]
C 100.64.1.0/24 is directly connected, port1
C 100.64.2.0/24 is directly connected, port2
C 172.16.100.0/24 is directly connected, port8
```

The 8.8.8.8/32 route through port2 has been removed. Although the ISP (Linux-Router) is still advertising the prefix, NGFW-1 is not adding it to its BGP database or the routing table.

Exercise 3: Configuring a Loopback Interface as a BGP Source

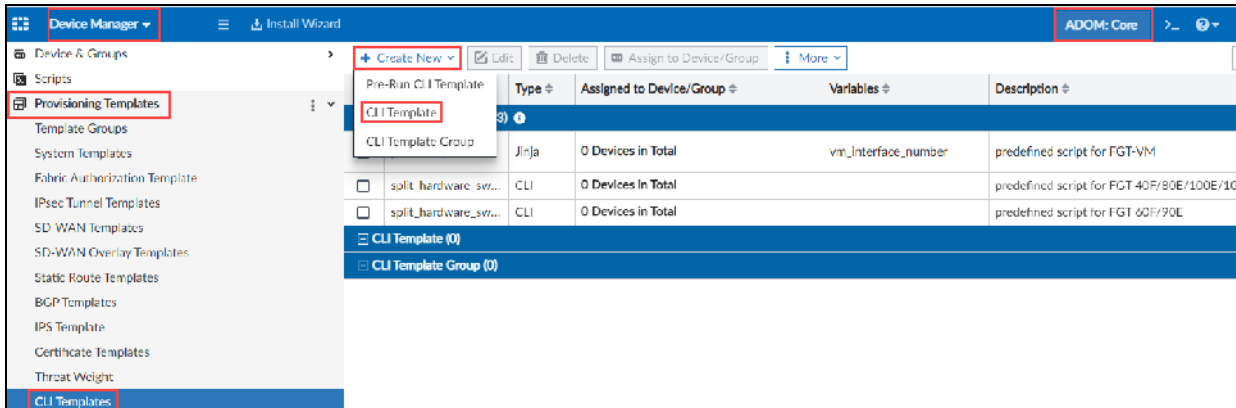
In this exercise, you will create a loopback interface on NGFW-1, configure BGP on NGFW-1 and ISFW, and then establish a BGP connection.

Configure a Loopback Interface as a BGP Source on NGFW-1

Since NGFW-1 is managed by FortiManager, you must perform the loopback configuration on FortiManager, and then install the configuration on NGFW-1.

To create the CLI template

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **Device Manager**.
4. Click **Provisioning Templates**.
5. Click **CLI Templates**.
6. Click **Create New**, and then select **CLI Template**.



7. Configure the following settings:

Field	Value
Template Name	Loopback_NGFW1
Type	CLI Script

Field	Value
Script Details	config system interface edit loopback_NGFW1 set vdom root set ip 10.2.0.254 255.255.255.0 set type loopback next end

Your configuration should match the following example:

Create New CLI Template

Template Name

Loopback_NGFW1

Type

CLI Script

Description

Script Details

Search...

1 config system interface

2 edit loopback_NGFW1

3 set vdom root

4 set ip 10.2.0.254 255.255.255.0

5 set type loopback

6 next

7 end

OK

Cancel

8. Click **OK**.

To install the loopback interface configuration

- 1. Continuing on the FortiManager GUI, in the **CLI Template** section, select the **Loopback_NGFW1** checkbox.
- 2. Click **Assign to Device/Group**.

+ Create New ▾

Edit

Delete

Assign to Device/Group

☐	Name ▾	Type ▾	Assigned to Device/Group ▾
Pre-Run CLI Template (3) ⓘ			
☐	provision_interfac...	Jinja	0 Devices in Total
☐	split_hardware_sw...	CLI	0 Devices in Total
☐	split_hardware_sw...	CLI	0 Devices in Total
CLI Template (1)			
☒	Loopback_NGFW1	CLI	0 Devices in Total
CLI Template Group (0)			

3. Move NGFW-1 from the **Available Entries** section to the **Selected Entries** section , and then click **OK**.

Assign to Devices/Groups

CLI Template

Loopback_interface

Use Shift key for multiple selections and double click for moving one item.

Available Entries (3)

☒ NGFW-1 [root] (IP: 10.1.0.254, Platform: FortiGate-VM64-KVM)

☐ Spoke-1 [root] (IP: 100.64.3.1, Platform: FortiGate-VM64-KVM)

☐ Spoke-2 [root] (IP: 100.64.5.1, Platform: FortiGate-VM64-KVM)

>

<

Selected Entries (0)

No entry

OK

Cancel

4. Click **Install Wizard**.

Install Wizard Create New Edit Delete Assign to Device/Group		
Name	Type	Assigned to Device/Group
Pre-Run CLI Template (3)		
provision_interfac...	Jinja	0 Devices in Total
split_hardware_sw...	CLI	0 Devices in Total
split_hardware_sw...	CLI	0 Devices in Total
CLI Template (1)		
☒ Loopback_NGFW1	CLI	1 Device in Total NGFW-1 (root)

- Verify that **Install Device Settings (only)** is displayed, and then click **Next**.
- Verify that **NGFW-1** is selected, and then click **Next**.
- Click **Install**.
- Wait until the installation finishes.
- Click **Finish**.

To configure BGP on NGFW-1

- Continuing on the FortiManager GUI, click **Scripts**.
- Click **Create New**, and then select **Script**.

Device Manager Create New Edit Delete Run Script Import CLI Script					
Device & Groups					
Scripts	Script		Type	Target	Comments
Provisioning Templates	Script Group				
Firmware Templates					
Monitors					
	☐ ADVPN-Hub	CLI		Remote FortiGate Directly (via CLI)	
	☐ ADVPN-Spokes	TCL		Remote FortiGate Directly (via CLI)	
	☐ BGP_Prefix_List	CLI		Remote FortiGate Directly (via CLI)	

- In the **Script Name** field, type `BGP_NGFW1`.
- In the **Run script on** field, select **Remote FortiGate Directly (via CLI)**.
- In the **Script details** field, type:

```

config router bgp
set as 65100
set router-id 172.16.1.254
config neighbor
edit 10.1.0.1
set remote-as 65200
set update-source loopback_NGFW1
    
```

```
next
end
```

Your configuration should match the following example:

Create New Script

[View Sample Script]

Script Name: BGP_NGFW1

Comments:

Type: CLI Script

Run script on: Remote FortiGate Directly (via CLI)

Script details

```
1 config router bgp
2 set as 65100
3 set router-id 172.16.1.254
4 config neighbor
5 edit 10.1.0.1
6 set remote-as 65200
7 set update-source loopback_NGFW1
8 next
9 end
```

OK Cancel

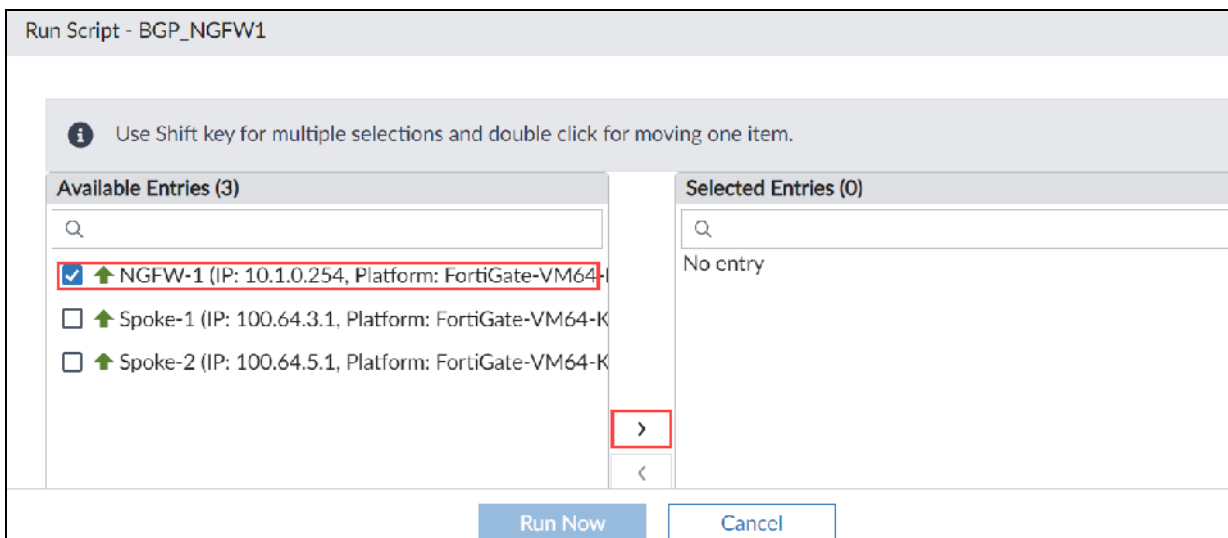


When you use a loopback interface as a BGP source, you must explicitly set `update-source` in the BGP configuration.

6. Click **OK**.

To install the BGP configuration on NGFW-1

1. Right-click the **BGP_NGFW1** script, and then select **Run Script**.
2. Move NGFW-1 from the **Available Entries** section to the **Selected Entries** section, and then click **Run Now**.



3. Make sure NGFW-1 is the only device listed in the pop-up window, and then click **OK**.
4. Wait for the script to finish running.
The script has been configured to apply the CLI commands directly on FortiGate.
5. Click **Close**.

Configure BGP on ISFW

Since ISFW is managed by FortiManager, you must perform the BGP configuration on FortiManager, and then install the configuration on ISFW.

Take the Expert Challenge!

Create a new script using the information in the following table, and then run the configuration on ISFW:

Field	Value
Script Name	BGP_ISFW
AS	65200
router-id	10.1.0.1
neighbor	10.2.0.254
remote-as	65100

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

After you complete the challenge, see [Establish the BGP connection on page 95](#).

To configure BGP on ISFW

1. Continuing on the FortiManager GUI, click **ADOM: Core**.

ADOM: Core				
+ Create New ▾ Edit Delete Run Script Import CLI Script More ▾				
☐	Name ▾	Type ▾	Target ▾	Comments ▾
Script (4)				
☐	ADVPN-Hub	CLI	Remote FortiGate Directly (via CLI)	
☐	ADVPN-Spokes	TCL	Remote FortiGate Directly (via CLI)	
☐	BGP_NGFW1	CLI	Remote FortiGate Directly (via CLI)	
☐	BGP_Prefix_List	CLI	Remote FortiGate Directly (via CLI)	

2. Click **Access**.

Select an ADOM		
root (1) FortiGate 7.2	Access (1) FortiGate 7.2	Core (3) FortiGate 7.2
DC (1) FortiGate 7.2	FortiNAC FortiNAC	Global Database Global 7.2

3. Click **Scripts**.
4. Click **Create New**, and then select **Script**.
5. In the **Script Name** field, type `BGP_ISFW`.
6. In the **Run script on** field, select **Remote FortiGate Directly (via CLI)**.
7. In the **Script details** field, type:

```
config router bgp
set as 65200
set router-id 10.1.0.1
config neighbor
edit 10.2.0.254
set remote-as 65100
next
end
end
```

Your configuration should match the following example:

Create New Script

[View Sample Script]

Script Name: BGP_ISFW

Comments:

Type: CLI Script

Run script on: Remote FortiGate Directly (via CLI)

Script details:

```
1 config router bgp
2 set as 65200
3 set router-id 10.1.0.1
4 config neighbor
5 edit 10.2.0.254
6 set remote-as 65100
7 next
8 end
9 end
```

OK Cancel

8. Click **OK**.

To install the BGP configuration on ISFW

1. Right-click the **BGP_ISFW** script, and then select **Run Script**.
2. Move ISFW from the **Available Entries** section to the **Selected Entries** section, and then click **Run Now**.

Run Script - BGP_ISFW

Use Shift key for multiple selections and double click for moving one item.

Available Entries (1):

- ☒ ISFW (IP: 10.1.0.1, Platform: FortiGate-VM64-KVM)

Selected Entries (0):

No entry

> <

Run Now Cancel

3. Make sure ISFW is the only device listed in the pop-up window, and then click **OK**.
4. Wait for the script to finish running.

The script has been configured to apply the CLI commands directly on FortiGate.

5. Click **Close**.

Establish the BGP connection

You will verify the BGP status, finalize the BGP configuration, and establish the BGP connection.

To verify the BGP status

1. Connect over SSH to ISFW.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

```
get router info bgp neighbors
```

You should see that the bgp neighbor is not directly connected.

```
ISFW # get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.2.0.254, remote AS 65100, local AS 65200, external link
BGP version 4, remote router ID 0.0.0.0
BGP state = Idle
Not directly connected EBGP
Last read          , hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Received 0 messages, 0 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
NLRI treated as withdraw: 0
Minimum time between advertisement runs is 30 seconds
```

Stop and think!

Why is the peer not directly connected?

Because a loopback interface adds one hop, you must enable multihop in the BGP configuration.

To finalize the BGP configuration on ISFW

1. Continuing on the FortiManager GUI, select **BGP_ISFW**, and then click **Edit**.

Device Manager

ADOM: Access

Device & Groups

Scripts

Provisioning Templates

Firmware Templates

Monitors

+ Create New

Edit

Delete

Run Script

Import CLI Script

More

☐	Name	Type	Target	Comments
Script (2)				
☒	BGP_ISFW	CLI	Remote FortiGate Directly (via CLI)	
☐	IPS	CLI	Policy Package or ADOM Database	
Script Group (0)				

2. In the **Script details** field, type `set ebgp-enforce-multihop enable`.

The script should look similar to the following example:

```
config router bgp
set as 65200
set router-id 10.1.0.1
config neighbor
edit 10.2.0.254
set ebgp-enforce-multihop enable
set remote-as 65100
next
end
end
```

3. Click **OK**.
4. Right-click the **BGP_ISFW** script, and then select **Run Script**.
5. Move ISFW from the **Available Entries** section to the **Selected Entries** section, and then click **Run Now**.
6. Make sure ISFW is the only device listed in the pop-up window, and then click **OK**.
7. Wait for the script to finish running.
The script has been configured to apply the CLI commands directly on FortiGate.
8. Click **Close**.

To confirm the BGP connection establishment

1. Connect over SSH to ISFW.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

```
get router info bgp summary
```

You should see that the bgp connection is established.

```
ISFW # get router info bgp summary

VRF 0 BGP router identifier 10.1.0.1, local AS number 65200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.2.0.254  4      65100    10      9         0    0    0 00:06:38      1

Total number of neighbors 1
```



You may see the BGP state showing `Connect`. You can then enter the command `get router info bgp summary` again to confirm that the bgp connection is established.

Lab 8: FortiGuard and Security Profiles

In this lab, you will configure web filtering and antivirus on FortiManager. Then, you will test the configuration by generating traffic from Client-10. Additionally, you will configure application control and test application traffic.

Objectives

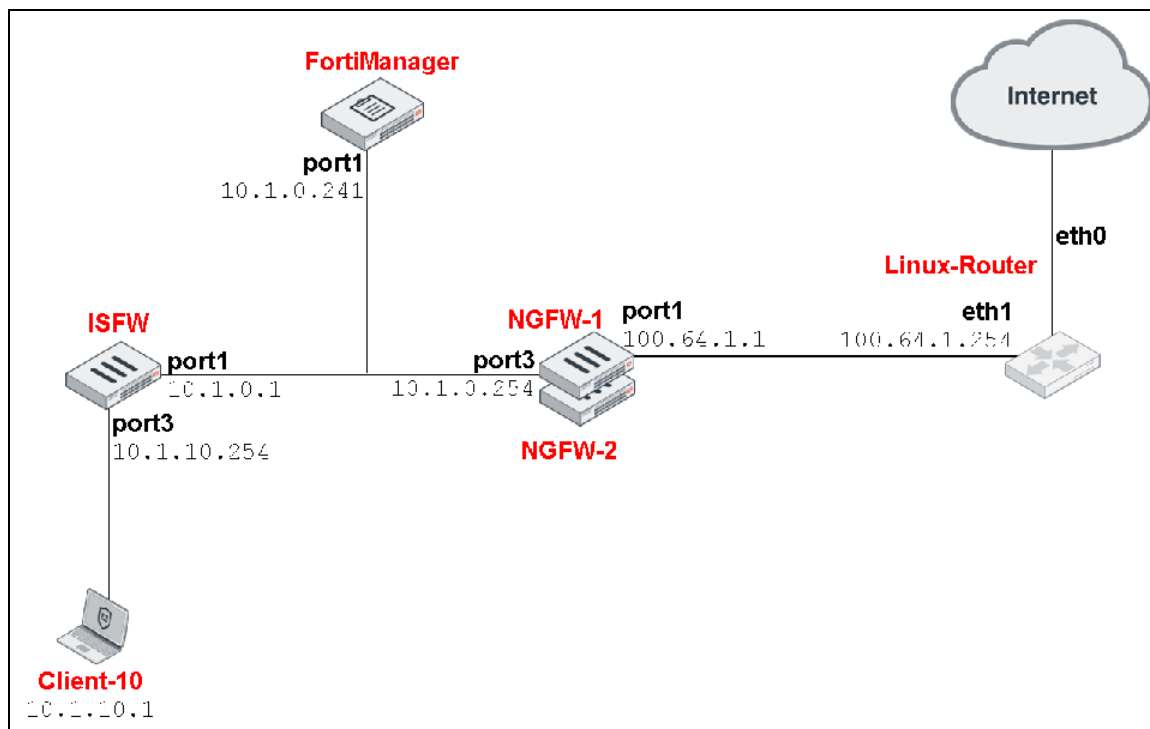
- Harden the security of the clients by using web filtering and antivirus
- Use web filtering to block traffic to unwanted sites
- Configure and test application control in NGFW policy mode

Time to Complete

Estimated: 55 minutes

Which Network Segment Will You Work On?

You will configure web filtering and antivirus on ISFW. Then, you will generate test traffic from Client-10.



Prerequisites

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

Exercise 1: Configuring Web Filtering and Antivirus

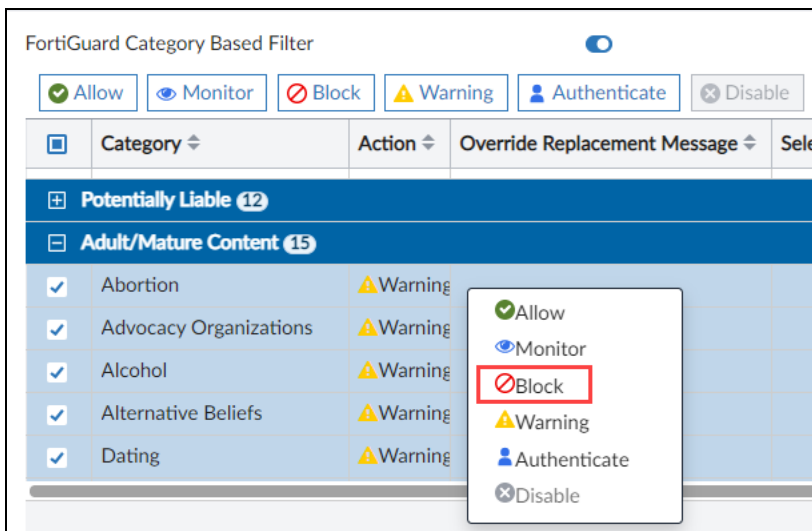
In this exercise, you will start hardening the network. You will install web filtering and antivirus on ISFW to protect the clients that are connected behind it.

Configure a Web Filter Profile

You will configure a web filtering profile with the FortiGuard categories that you want to block.

To configure a web filter profile

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Access**.
3. Click **Policy & Objects**.
4. Click **Object Configurations > Security Profiles > Web Filter**.
5. Click **Create New**.
6. In the **Name** field, type `Block`.
7. In the **Feature Set** field, select **Proxy-based**.
8. Enable **FortiGuard Category Based Filter**.
9. Right-click the category **Unrated**, and then select **Allow**.
10. Select all the subcategories, one at a time, for the following categories:
 - **Adult/Mature Content**
 - **Bandwidth Consuming**
11. Right-click, and then select **Block**.



12. In the **Change Note** field, type some text because this field is required to proceed.
13. Click **OK**.

Configure an Antivirus Profile

You will configure an antivirus profile to block malware.

To configure an antivirus profile

1. Continuing on the FortiManager GUI, click **Security Profiles > AntiVirus**.
2. Click **Create New**.
3. In the **Name** field, type `Block`.
4. In the **Feature Set** field, select **Proxy-based**.
5. In the **Inspected Protocols** section, enable **HTTP**, **SMTP**, **POP3**, **IMAP**, and **FTP**.

The screenshot shows the FortiManager GUI for configuring an Antivirus Profile. The 'Name' field is set to 'Block'. The 'Comments' field is empty. The 'Scan Mode' is set to 'Default'. The 'AntiVirus Scan' is set to 'Block'. The 'Feature Set' is set to 'Proxy-based'. The 'Inspected Protocols' section shows 'HTTP', 'SMTP', 'POP3', 'IMAP', and 'FTP' all enabled with blue toggle switches. 'MAPI' and 'SSH' are disabled with grey toggle switches. Red boxes highlight the 'Proxy-based' feature set and the enabled protocols.

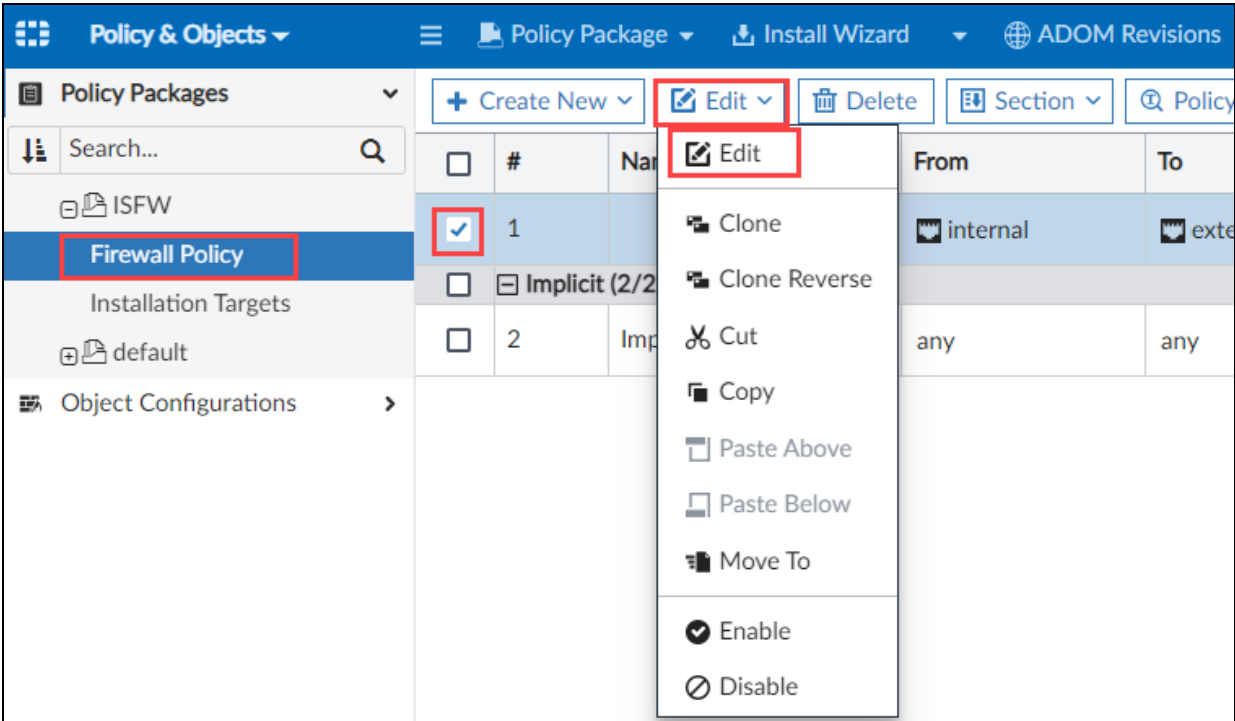
6. In the **Change Note** field, type some text because this field is required to proceed.
7. Click **OK**.

Apply the Security Profiles

You will modify the existing policy in the FortiManager policy package to apply the web filter and antivirus profiles that you created.

To apply the security profiles

- 1. Continuing on the FortiManager GUI, click **Policy Packages**.
- 2. Click **ISFW > Firewall Policy**.
- 3. Select the first policy at the top of the list, and then click **Edit > Edit**.



- 4. Configure the following settings:

Field	Value
Inspection Mode	Proxy-based
AntiVirus Profile	Block
Web Filter Profile	Block
SSL/SSH Inspection	certificate-inspection

The configuration should look like the following example:

Action:

Inspection Mode:

Proxy HTTP(S) Traffic: ☐

Firewall/Network Options

NAT: ☐

Protocol Options: default

Disclaimer Options

Display Disclaimer: ☐

Security Profiles

Profile Type:

AntiVirus Profile: Block

Web Filter Profile: Block

Video Filter:

DNS Filter:

Application Control:

IPS:

SSH Filter:

SSL/SSH Inspection: certificate-inspection

5. In the **Change Note** field, type some text because this field is required to proceed.
6. Click **OK**.

Install the Policy

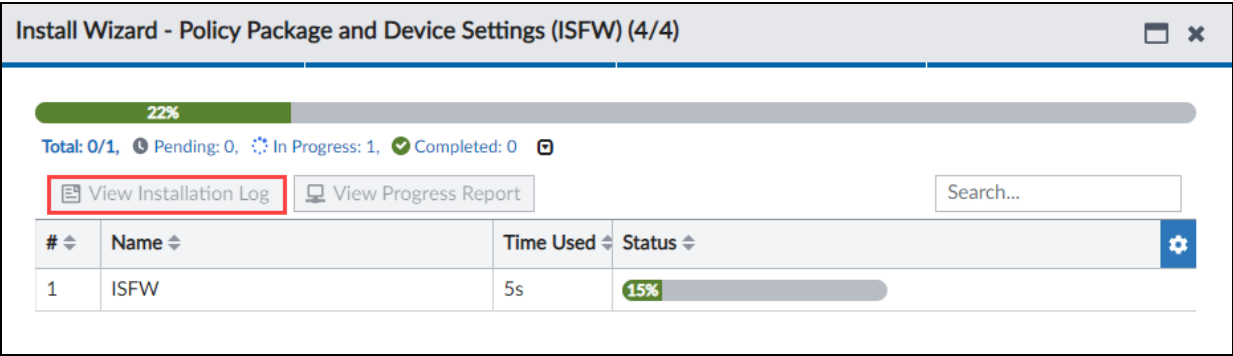
You will install the policy and object changes on ISFW.

To install the policy

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. On the **Install Policy Package & Device Settings** window, confirm that the **ISFW** policy package is selected.
3. Click **Next**.

4. Confirm that **ISFW** is selected, and then click **Next**.
5. Click **Install Preview** to see the changes that will be applied to the FortiGate.
6. On the **Install Preview** page, click **Close**.
7. Click **Install**.

Wait until the installation finishes. If the installation stalls at 15%, view the install logs to confirm that the installation was successful, and then click **Cancel** to close the installation window.



8. Click **Finish**.

Test the Web Filter

You will confirm that ISFW is not allowing access to websites that belong to blocked FortiGuard categories.

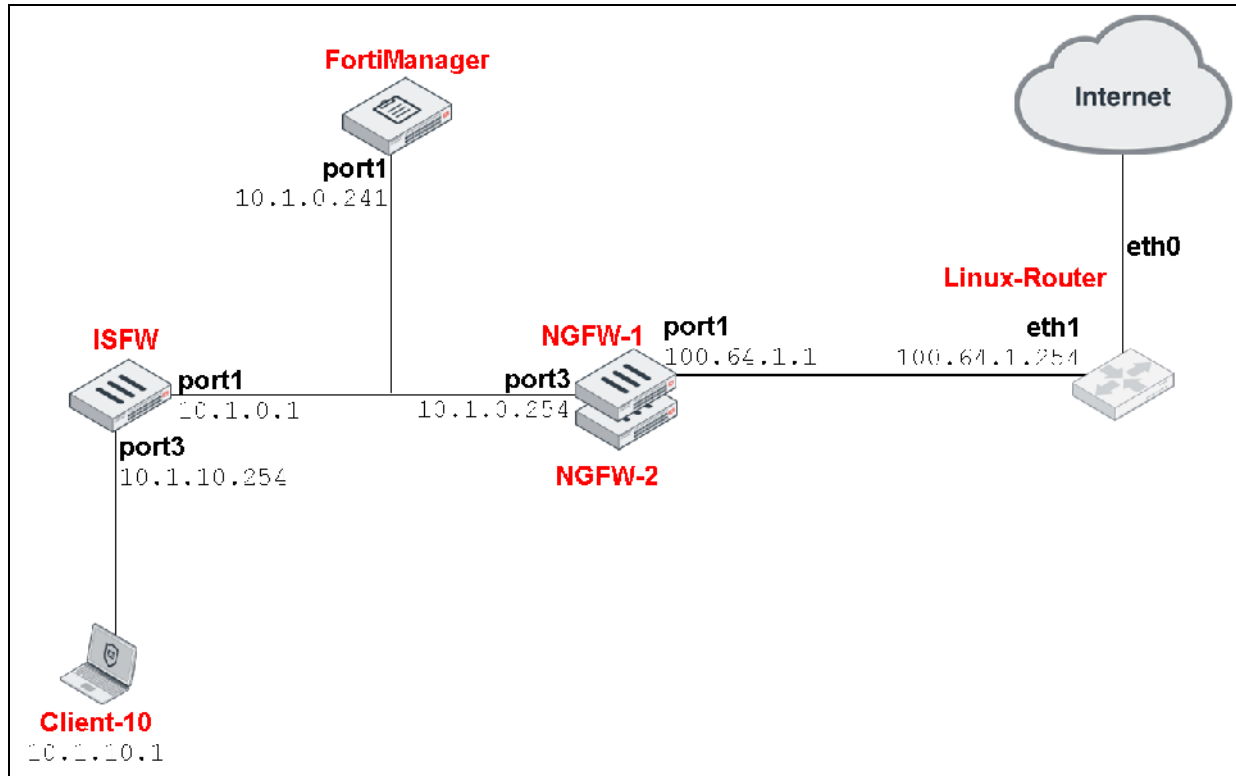
To test the web filter

1. Connect to the Client-10 VM.
2. On the Client-10 VM, open a browser, and then try to connect to the following websites:
 - www.internet-radio.com
 - www.tunein.com

You can see that these websites are blocked because they belong to blocked categories.

Exercise 2: Analyzing Web Filtering Traffic

Network Topology



Objective

In the previous exercises, you configured ISFW to apply web filtering to the internet traffic coming from Client-10. The applied web filter blocks the following FortiGuard categories:

- Bandwidth Consuming
- Adult/Mature Content
- Security Risk

Many restricted sites seem to be correctly blocked, such as:

- www.internet-radio.com
- www.tunein.com

However, the following site is not blocked. According to users, it should be blocked because it belongs to the Security Risk category.

- www.eicar.org

Analyze the Web Traffic

You will test to see if the website is accessible, and then run diagnose commands on ISFW to find the website category. Then, you will check if the category is one of the blocked categories.

To access the website

1. Connect to the Client-10 VM.
2. Open a browser, and then try to connect to the following website:
 - www.eicar.org

You can see that this website is not blocked.

To run CLI commands to diagnose the issue

1. On the ISFW CLI, log in with the username `admin` and password `password`.
2. Enter the following command to clear the ISFW web filtering cache:

```
diagnose test application urlfilter 2
```
3. Enable the following real-time debug while browsing the website:

```
diagnose debug application urlfilter -1
diagnose debug enable
```
4. On the Client-10 VM, on the browser, refresh page to reload the website.
5. Return to the ISFW CLI, can you see how FortiGuard is categorizing the website?
6. Look for the `www.eicar.org` hostname in the log.

You can see the following details:

```
user="N/A" src=10.1.10.1 sport=49714 dst=89.238.73.97 dport=443 service="https"
cat=50 url_cat=50 ip_cat=0 hostname="www.eicar.org" url="/"
```

The website is categorized as 50.

7. Enter the following CLI command to verify the category codes:

```
get webfilter categories
```

You can see that number 50 is mapped to the `Information and Computer Security` subcategory in the `General Interest - Business` main category.

```

85 Domain Parking
87 Personal Privacy
89 Auction
g07 General Interest - Business:
31 Finance and Banking
41 Search Engines and Portals
43 General Organizations
49 Business
50 Information and Computer Security
51 Government and Legal Organizations
52 Information Technology
53 Armed Forces
56 Web Hosting
81 Secure Websites
84 Web-based Applications
92 Charitable Organizations
93 Remote Access
94 Web Analytics
95 Online Meeting
97 URL Shortening
g21 Unrated
0 Unrated
g22 Local Categories
140 custom1
141 custom2
ISFW #

```

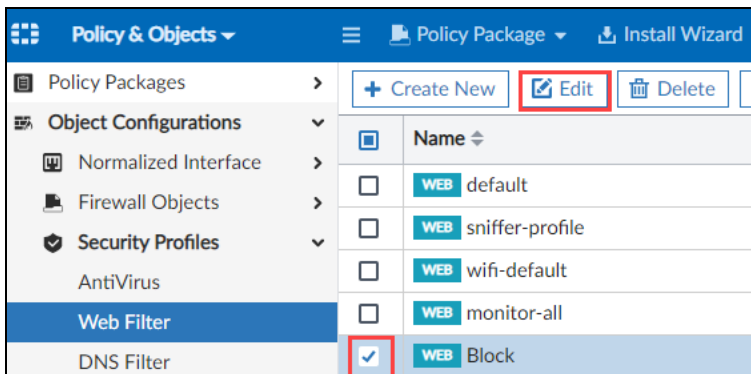


After you finish, disable the real-time debug, using the following commands:

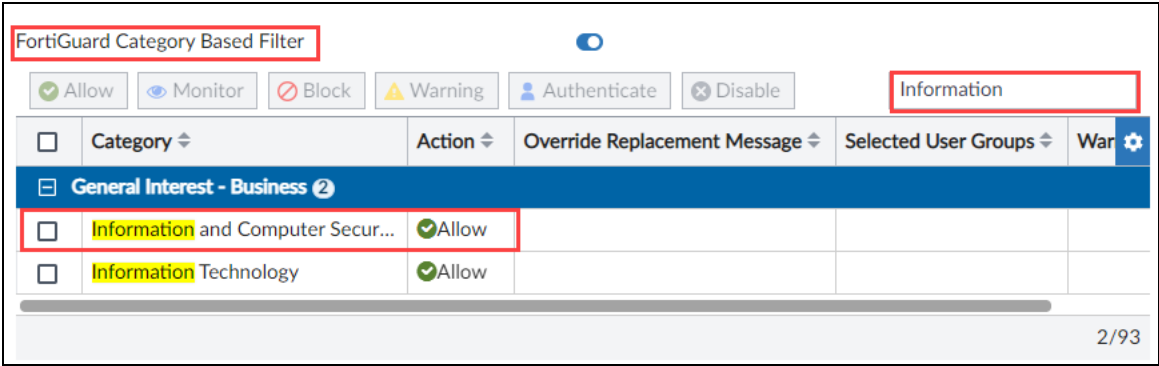
- `diagnose debug application urlfilter 0`
- `diagnose debug disable`

To verify the category action on the security profile

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Access**.
3. Click **Policy & Objects**.
4. Click **Object Configurations** > **Security Profiles** > **Web Filter**.
5. Select the **Block** checkbox, and then click **Edit**.



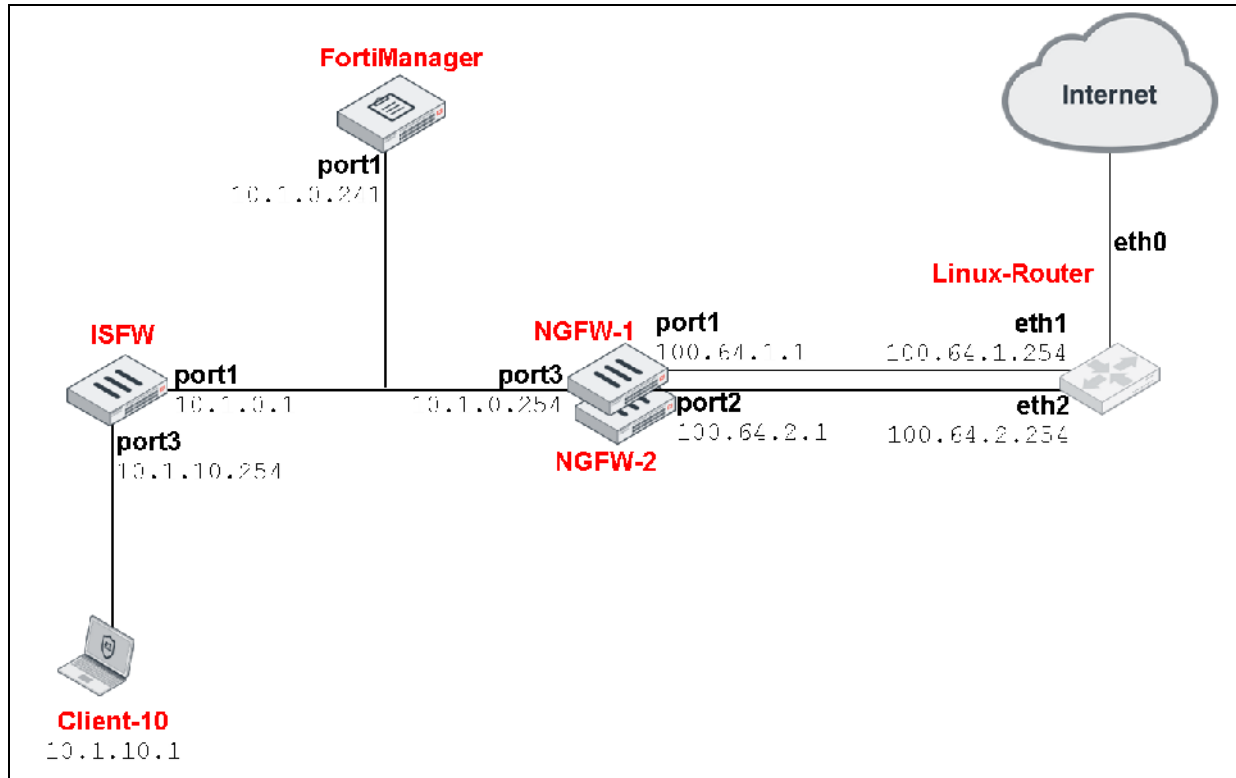
6. In the **FortiGuard Category Based Filter** section, in the **Search** field, type `information` to find the category.



In the **Block** web filter profile, the category action is set to **Allow**, and therefore the www.eicar.org website is allowed.

Exercise 3: Analyzing Antivirus

Network Topology



Objective

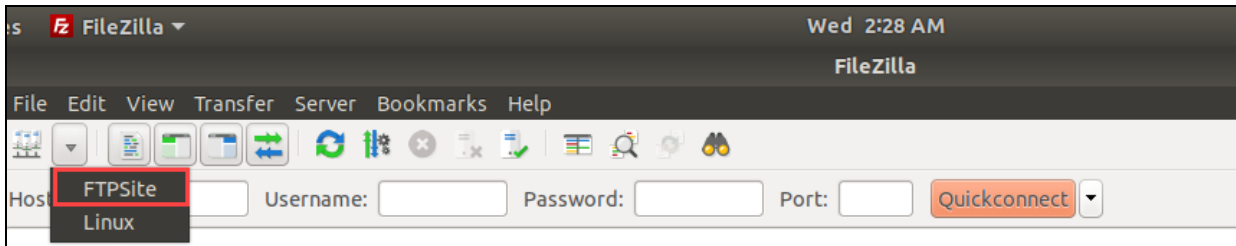
Even though you enabled antivirus on ISFW, a user connecting from Client-10 complains that it's still possible to download the `eicar.com` virus sample located at the 100.64.3.254 FTP server. Use the diagnose commands available on ISFW to find out why FortiGate isn't blocking the FTP file transfer.

Analyze the FTP Traffic

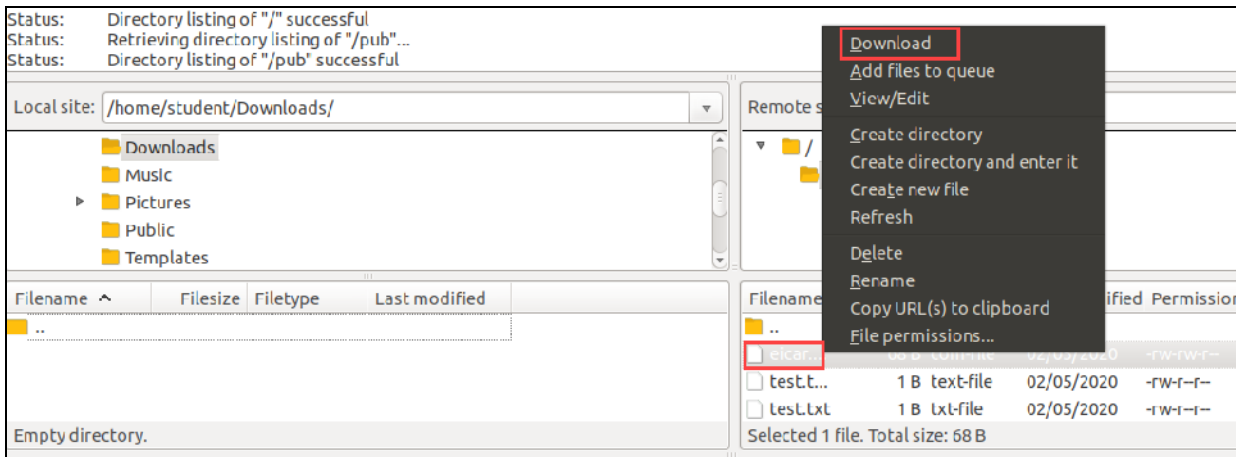
You will test the virus sample download, and then run diagnose commands available on ISFW to find out why FortiGate isn't blocking the FTP file transfer.

To test antivirus

1. On the Client-10 VM, open FileZilla.
2. In the **Site Manager** field, select **FTPSite**.



3. Select **Desktop** as the local site folder, and **pub** as the remote site folder.
4. Right-click the `eicar.com` file, and then select **Download**.



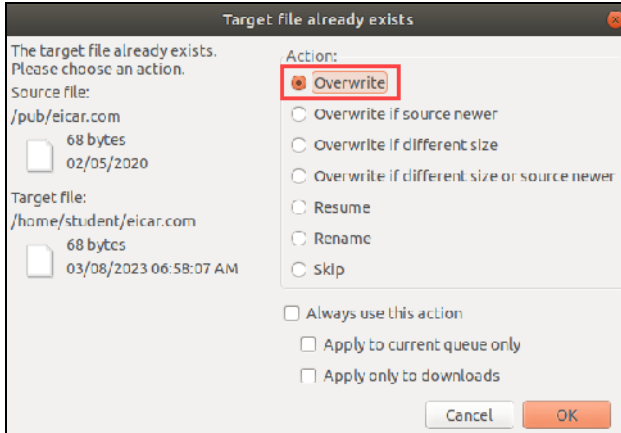
Why isn't ISFW detecting the EICAR virus?

To capture FTP packets and analyze the packet flow

1. Continuing on the ISFW CLI, enter the following commands to view the FTP packet flow:

```
diagnose debug flow filter addr 100.64.3.254
diagnose debug flow trace start 10
diagnose debug enable
```
2. Enter the following command to capture the FTP packets:

```
diagnose sniffer packet any "host 100.64.3.254" 4
```
3. Connect to the Client-10 VM.
4. In the FileZilla application, right-click the `eicar.com` file, and then select **Download** to download the file again.
5. In the **Target file already exists** window, in the **Action** field, verify that **Overwrite** is selected.



6. Click **OK** to download the file.
7. Connect to the ISFW CLI.

The output should look like the following example:

```
ISFW # diagnose sniffer packet any "host 100.64.3.254" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 100.64.3.254]
id=65308 trace_id=3 func=print_pkt_detail line=5939 msg="vd-root:0 received a packet(proto=6, 10.1.
10.1:57112->100.64.3.254:222) tun_id=0.0.0.0 from port3. flag [S], seq 2418829254, ack 0, win 29200
"
id=65308 trace_id=3 func=init_ip_session_common line=6121 msg="allocate a new session-0000644c, tun
_id=0.0.0.0"
id=65308 trace_id=3 func=__vf_ip_route_input_rcu line=2012 msg="find a route: flag=00000000 gw=10.1
.0.254 via port1"
id=65308 trace_id=3 func=__iprope_tree_check line=531 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=3 func=fw_forward_handler line=930 msg="Allowed by Policy-1:"
id=65308 trace_id=3 func=ip session confirm final line=3189 msg="npu state=0x100, hook=4"
10.727571 port3 in 10.1.10.1.57112 -> 100.64.3.254.222: syn 2418829254
10.727753 port1 out 10.1.10.1.57112 -> 100.64.3.254.222: syn 2418829254
10.742849 port1 in 100.64.3.254.222 -> 10.1.10.1.57112: syn 848797941 ack 2418829255
10.742876 port3 out 100.64.3.254.222 -> 10.1.10.1.57112: syn 848797941 ack 2418829255
10.743242 port3 in 10.1.10.1.57112 -> 100.64.3.254.222: ack 848797942
10.743254 port1 out 10.1.10.1.57112 -> 100.64.3.254.222: ack 848797942
10.748505 port1 in 100.64.3.254.222 -> 10.1.10.1.57112: psh 848797942 ack 2418829255
```

Packet Flow

Packet Capture

Stop and think!

Can you confirm from the output that FortiGate is inspecting the traffic? If it isn't, can you explain why?

This is because the FTP connection between the FTP client and server is using a non-standard FTP port (222). The antivirus profile on FortiGate is configured to inspect traffic on standard FTP port 21, and therefore allow the client to download the virus sample file.



Delete the `eiicar.com` file from the desktop.

Exercise 4: Implementing Application Control in NGFW Policy-Based Mode

On an NGFW firewall, there are two modes that you can use to implement application control in security policies: policy-based mode and profile-based mode. In policy-based NGFW mode, you can implement application control directly in security policies without using application control profiles.

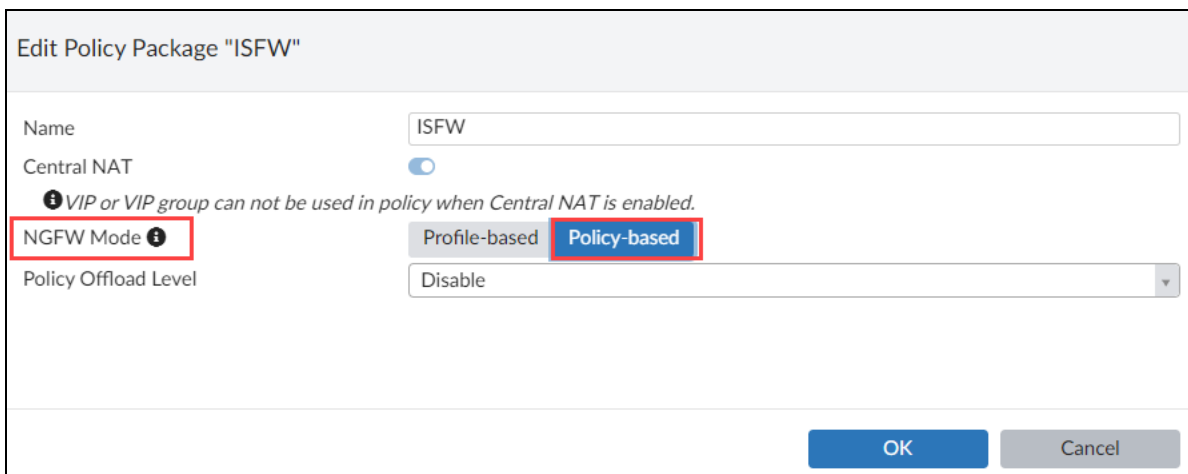
In this exercise, you will enable policy-based NGFW mode on FortiGate, and then implement application control in the security policy to explicitly allow access to only the LinkedIn web application and block access to all other web applications.

Enable Policy-Based NGFW Mode

You will change the NGFW mode on ISFW from profile-based to policy-based.

To enable policy-based NGFW mode

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Access**, and then click **Policy & Objects**.
3. In the **Policy Packages** section, right-click **ISFW**, and then click **Edit**.
4. In the **Edit Policy Package "ISFW"** window, in the **NGFW Mode** field, select **Policy-based**.



Edit Policy Package "ISFW"

Name: ISFW

Central NAT: ☒

! VIP or VIP group can not be used in policy when Central NAT is enabled.

NGFW Mode: Profile-based **Policy-based**

Policy Offload Level: Disable

OK Cancel

5. Click **OK**.



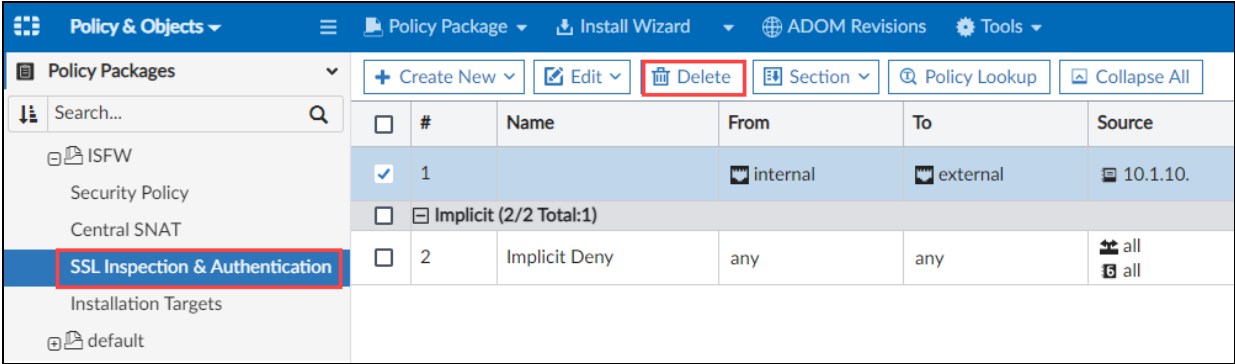
Changing NGFW modes removes the existing firewall policies. To pass traffic in policy-based NGFW mode, FortiGate requires three types of policies to be configured. This is unlike a profile-based NGFW mode setup, where only one policy is required.

Configure SSL Inspection and Central SNAT Policies

You will modify the default SSL inspection policy to use the deep-inspection SSL inspection profile, and then create a central SNAT policy.

To modify the SSL inspection policy

- Continuing on the FortiManager GUI, click **ISFW > SSL Inspection & Authentication**.
- Select the policy at the top of the list, and then click **Delete**.



- Click **OK**.
- Click **Create New > Create New**.
- In the **Security Profiles** section, in the **SSL/SSH Inspection** field, select the **certificate-inspection** profile, and then click **Close**.
- In the **Change Note** field, type some text because this field is required to proceed.
- Click **OK**.

To create the central SNAT policy

- Continuing on the FortiManager GUI, click **ISFW > Central SNAT**.



If you can't see **Central SNAT**, you can enable it by doing the following:

- Click **Tools > Feature Visibility**.
- In the **Policy** section, enable **Central SNAT**.
- Click **OK**.

- Click **Create New > Create New**.
- Configure the following settings:

Field	Value
Incoming Interface	internal
Outgoing Interface	external

Field	Value
Source Address	all
Destination Address	all

Your configuration should look like the following image:

Create New Central SNAT ✕

Type

IPv4

IPv6

Incoming Interface

internal

+

Outgoing Interface

external

+

Source Address

all

+

Destination Address

all

+

NAT

NAT

☒

NAT

NAT46

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Protocol

Any

TCP

UDP

STCP

Specify

0

4. In the **Change Note** field, type some text because this field is required to proceed.
5. Click **OK**.

Configure the Security Policy and Test Application Control

You will create a security policy to apply the application signature required to allow access to the LinkedIn web application and block access to all other web applications.

To create a security policy to allow the LinkedIn web application

1. Continuing on the FortiManager GUI, click **ISFW > Security Policy**.
2. Click **Create New > Create New**.
3. Configure the following settings:

Field	Value
Name	Allow_LinkedIn

Field	Value
Incoming Interface	internal
Outgoing Interface	external
Source	all
Destination	all
Application	LinkedIn DNS SSH FTP

Tip: Type `LinkedIn` in the search box in the right section to locate it easily.

4. Verify that the **Action** field is set to **Accept**.
Your configuration should look like the following image:

Name ⓘ

Policy Mode ⓘ

Incoming Interface

Outgoing Interface

Source

Destination

Schedule

Service

Application

URL Category

Action

Firewall/Network Options

NAT

Allow LinkedIn

StandardLearn Mode

internal✕

+

external✕

+

all✕

+

all✕

+

always✕

+

App DefaultSpecify

FTP✕

SSH✕

DNS✕

LinkedIn✕

+

+

AcceptDeny

Firewall/Network Options

NAT

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

OKCancel

5. In the **Change Note** field, type some text because this field is required to proceed.
6. Click **OK**.



FortiGate policy-based NGFW follows the concept of precedence to evaluate security policies. If traffic does not match the created security policy, it is processed by the implicit security policy, which denies access to all other web application traffic.

To install the policy on ISFW

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that the **ISFW** policy package is selected, and then click **Next**.
3. Confirm that the **ISFW** device is selected, and then click **Next**.
4. Click **Install Preview** to see the changes that will be applied to the FortiGate.
5. On the **Install Preview** page, click **Close**.
6. Click **Install**.
Wait until the installation is successful.
7. Click **Finish**.

To test policy-based NGFW mode application control

1. On the Client-10 VM, open a new browser tab, and then go to the following URL:
`https://www.linkedin.com`
FortiGate allows the website to load properly.
2. Open a new tab, and then go to the following URL:
`https://www.facebook.com`
FortiGate blocks access to the Facebook web application according to the implicit security policy.
3. Log in to the ISFW GUI with the username `admin` and password `password`.
4. Click **Login Read-Only**.
5. Click **Log & Report > Security Events > Application Control**.
6. Review the logs that allowed access to the LinkedIn web application.

Time	Source	Destination	Application Name	Action	Application User	Application Details	Log Details
07:32:08	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:32:08	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:32:08	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:32:06	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:32:06	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:32:06	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:32:03	10.1.10.1	111.111.111.111 (www.linkedin.com)	LinkedIn	Pass			
07:31:51	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:51	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:51	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:51	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:50	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:50	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:50	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:50	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			
07:31:48	10.1.10.1	8.8.8.8 (dns.google)	DNS	Pass			

Application Control
Application Name: LinkedIn
Application ID: 16332
Category: SocialMedia
Application Risk: Low
Protocol: 6
Service: SSL
Message: SocialMedia: LinkedIn

Action
Action: Pass
Policy UUID: 225f054-c273-51ed-129f-0c6c44c-bcac6
Policy type: Security

Security
Level: Information

Lab 9: IPS

In this lab, you will configure FortiGate to protect a web server using intrusion prevention system (IPS) inspection. Next, you will test the configuration by generating suspicious traffic from outside the network, and then sending it to the server. Finally, you will use the information gathered by the built-in sniffer to write a custom IPS signature.

Objectives

- Use IPS to protect a web server
- Monitor IPS operation
- Create and test custom IPS signatures

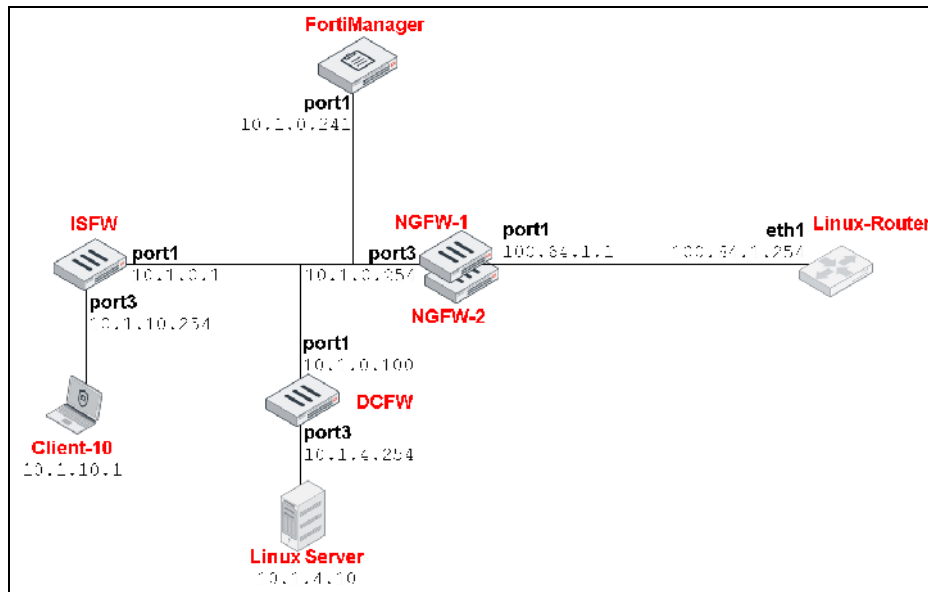
Time to Complete

Estimated: 60 minutes

Which Network Segment Will You Work On?

In the first exercise, you will configure IPS inspection on DCFW. You will also configure a virtual IP (VIP) on NGFW-1. Then, you will generate suspicious traffic from Linux-Router to the Linux server.

In the second exercise, you will work on Client-10 and ISFW.



Prerequisites

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

Exercise 1: Configuring IPS

You will protect the Linux server by applying an IPS profile to the incoming traffic. Then, to allow access to the server from outside the network, you will configure a virtual IP (VIP) on NGFW-1.

Configure the IPS Profile

You will use a preconfigured IPS profile and change its configuration to enable logging.

To configure the IPS profile

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **DC**.
3. Click **Policy & Objects**.
4. Click **Object Configurations > Security Profiles > Intrusion Prevention**.
5. Click **protect_http_server** to select it, and then click **Edit**.
6. Click the existing IPS filter, and then click **Edit**.
7. In the **Packet Logging** field, select **Enable**.

IPS Signatures and Filters

+ Create New Edit Delete Move Up Move Down Search...

☒	Details	Exempt IPs	Action	Packet Logging	Status
☒	Location: server Protocol: HTTP	0	Default	Disabled	Default

Edit IPS Signatures and Filters

Type: Filter Signature

Action: Default

Packet Logging: Enable Disable

Status: Enable Disable Default

Filter: Location: server Protocol: HTTP

Edit Filter

Advanced Options >

OK Cancel

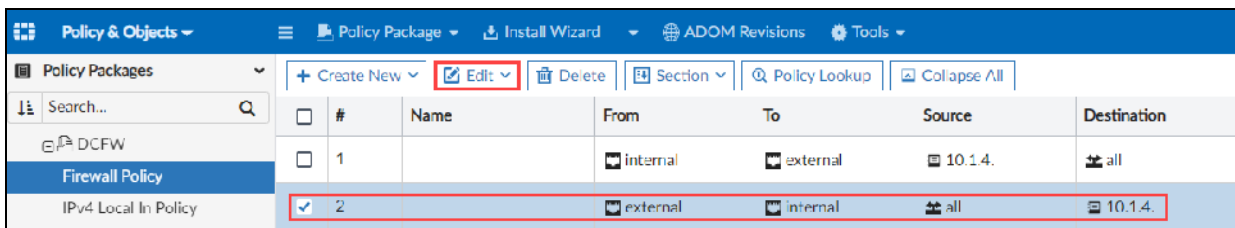
8. Click **OK** to close the window.
9. In the **Change Note** field, type some text because this field is required to proceed.
10. Click **OK**.

Apply the IPS Profile

You will apply the IPS profile to the incoming firewall policy on DCFW.

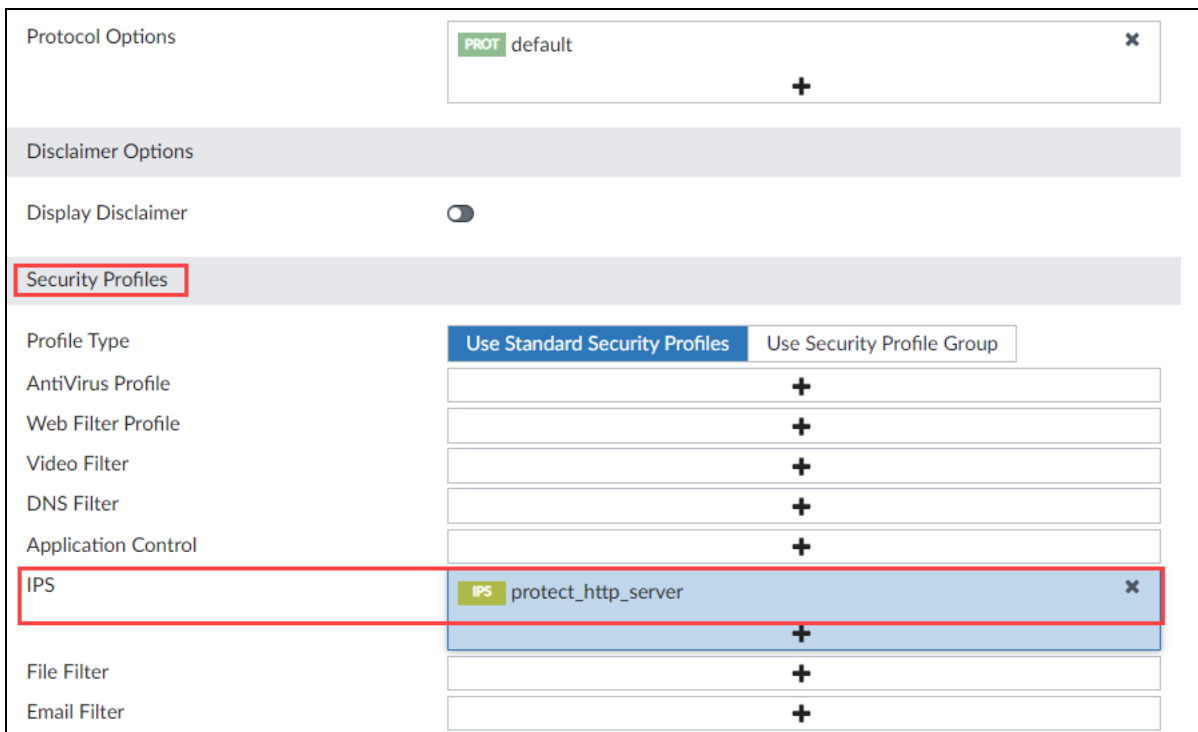
To apply the IPS profile

1. Continuing on the FortiManager GUI, click **Policy Packages**.
2. Click **DCFW > Firewall Policy**.
3. Click policy sequence **2** to select it, and then click **Edit > Edit**.



	#	Name	From	To	Source	Destination
☐	1		internal	external	10.1.4.	all
☒	2		external	internal	all	10.1.4.

4. In the **Security Profiles** section, in the **IPS** field, click **+**, and then select **protect_http_server**.
5. Click **Close**.



Profile Type	Use Standard Security Profiles	Use Security Profile Group
AntiVirus Profile		+
Web Filter Profile		+
Video Filter		+
DNS Filter		+
Application Control		+
IPS	IPS protect_http_server	+
File Filter		+
Email Filter		+

6. In the **Change Note** field, type some text because this field is required to proceed.
7. Click **OK**.

Install the Policy

You will install the policy and object changes on DCFW.

To install the policy

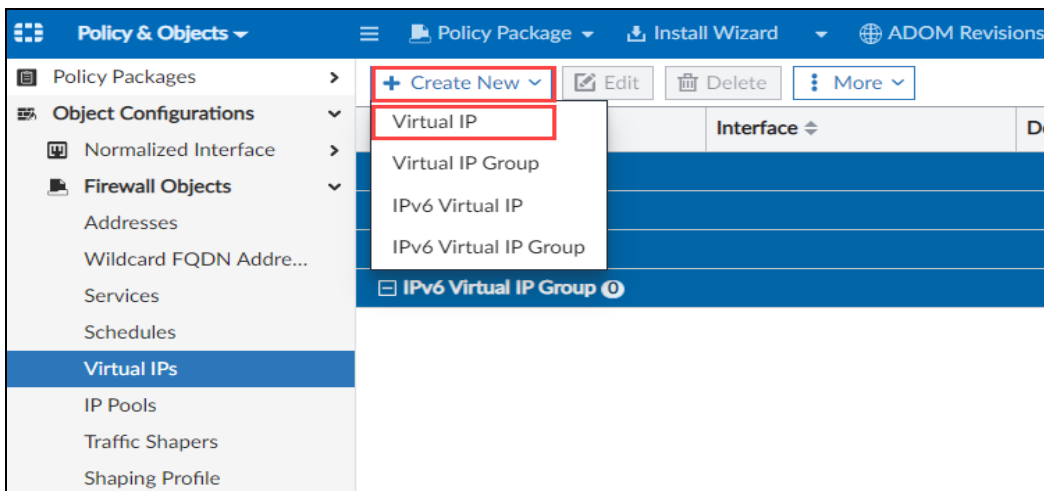
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that the **DCFW** policy package is selected, and then click **Next**.
3. Confirm that the **DCFW** device is selected, and then click **Next**.
4. Click **Install Preview** to see the changes that will be applied to the FortiGate.
5. On the **Install Preview** page, click **Close**.
6. Click **Install**.
Wait until the installation finishes.
7. Click **Finish**.

Configure the VIP

First, you will create the VIP object. The VIP maps the external-facing IP address 100.64.1.10 to the internal-facing IP address 10.1.4.10. Next, you will create an incoming firewall policy using the VIP object as the destination. Finally, you will install the changes on NGFW-1.

To configure the VIP

1. Continuing on the FortiManager GUI, navigate to the **Core ADOM**.
2. Click **Object Configurations > Firewall Objects > Virtual IPs**.
3. Click **Create New > Virtual IP**.



4. Configure the following settings:

Field	Value
Name	Linux_Server
Interface	external
Type	Static NAT
External IP Address/Range	100.64.1.10
Mapped IP Address/Range	10.1.4.10

5. In the **Change Note** field, type some text because this field is required to proceed.
6. Click **OK**.

Configure the Firewall Policy

You will create an incoming firewall policy using the VIP object as the destination.

To configure the firewall policy

1. Continuing on the FortiManager GUI, click **Policy Packages**.
2. Click **NGFW-1 > Firewall Policy**.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	Inbound Access
Incoming Interface	external
Outgoing Interface	internal
IPv4 Source Address	all
IPv4 Destination Address	Select VIRTUAL IP(1) > Linux_Server .
Service	HTTP
Schedule	always
Action	Accept
Log Traffic	Log All Sessions

Your configuration should match the following example:

Install the Policy

Name ⓘ	Inbound Access	
Incoming Interface	external	×
	+	
Outgoing Interface	internal	×
	+	
Source	all	×
	+	
Negate Source	☐	
IP/MAC Based Access Control ⓘ		+
Destination	Linux_Server	×
	+	
Negate Destination	☐	
Service	HTTP	×
	+	
Schedule	always	×
	+	
Action	☒ Accept ☐ Deny ☐ IPSEC	
Inspection Mode	☒ Flow-based ☐ Proxy-based	

5. In the **Change Note** field, type some text because this field is required to proceed.
6. Click **OK**.

Install the Policy

You will install the policy and object changes on NGFW-1.

To install the policy

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that the **NGFW-1** policy package is selected, and then click **Next**.
3. Confirm that the **NGFW-1** device is selected, and then click **Next**.
4. Click **Install Preview** to see the changes that will be applied to the FortiGate.
5. On the **Install Preview** page, click **Close**.
6. Click **Install**.
Wait until the installation finishes.
7. Click **Finish**.

Test the IPS

You will run a vulnerability scanner from Linux-Router to the Linux server. This will test the IPS configuration and block some of the traffic as an attack.

To test the IPS

1. Connect to the Client-10 VM.
2. Open PuTTY.
3. Connect over SSH to the Linux-Router saved session.
4. Log in with the username `student` and password `password`.
5. Enter the following command:

```
sudo nikto -h 100.64.1.10
```
6. Type the password `password`, and then press `Enter`.
Let the scan run for approximately 5 minutes.
7. Press `Ctrl+C` to end the scan.
8. Close PuTTY.

Check the Attack Logs

You will review the attack logs.

To check the attack logs

1. Log in to the DCFW GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.
3. Click **Log & Report > Security Events > Intrusion Prevention**.



The **Intrusion Prevention** logs section does not appear if there are no IPS logs. FortiGate displays this section after it creates logs. After the attacks, if this menu item does not appear, log out of the FortiGate GUI, and then log in again to refresh it.

4. Analyze all the attack logs that are generated.

Check the Attack Statistics

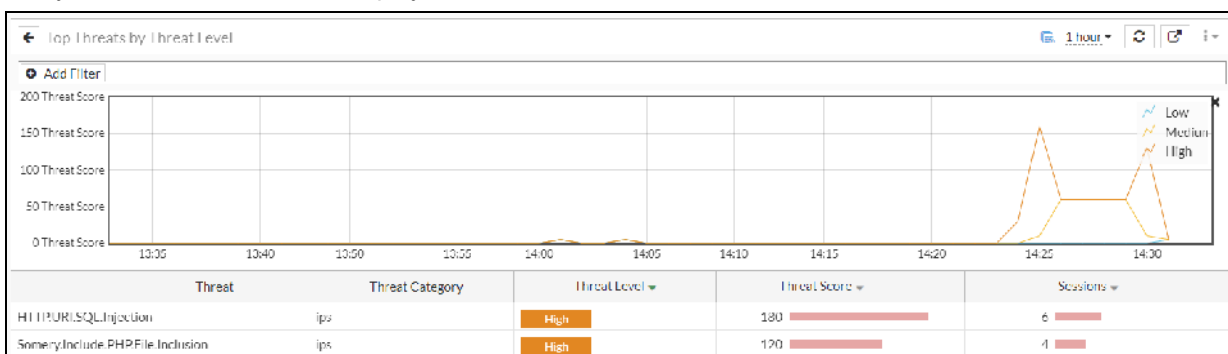
Date/Time	Severity	Source	Protocol	Action	Count	Attack Name
		100.64.1.254	6	dropped		MamboVideoDB.Class.Xml...
		100.64.1.254	6	dropped		SomeryInclude.PHPFile.Inc...
		100.64.1.254	6	dropped		SomeryInclude.PHPFile.Inc...
		100.64.1.254	6	dropped		SomeryInclude.PHPFile.Inc...
		100.64.1.254	6	dropped		SomeryInclude.PHPFile.Inc...
		100.64.1.254	6	dropped		NuclearDB.Root.Path.Para...
		100.64.1.254	6	dropped		NuclearDB.Root.Path.Para...
		100.64.1.254	6	dropped		NuclearBB.Root.Path.Para...
		100.64.1.254	6	dropped		NetworkActivWeb.Server.X...
		100.64.1.254	6	dropped		NetworkActivWeb.Server.X...
		100.64.1.254	6	dropped		NetworkActivWeb.Server.X...

Check the Attack Statistics

You will review FortiView to check the attack statistics.

To check the attack statistics

1. Continuing on the DCFW GUI, click **Dashboard > Security**.
2. Click anywhere on the **Top Threats by Threat Level** widget.
3. Analyze the information that is displayed.



Exercise 2: Creating IPS Custom Signatures

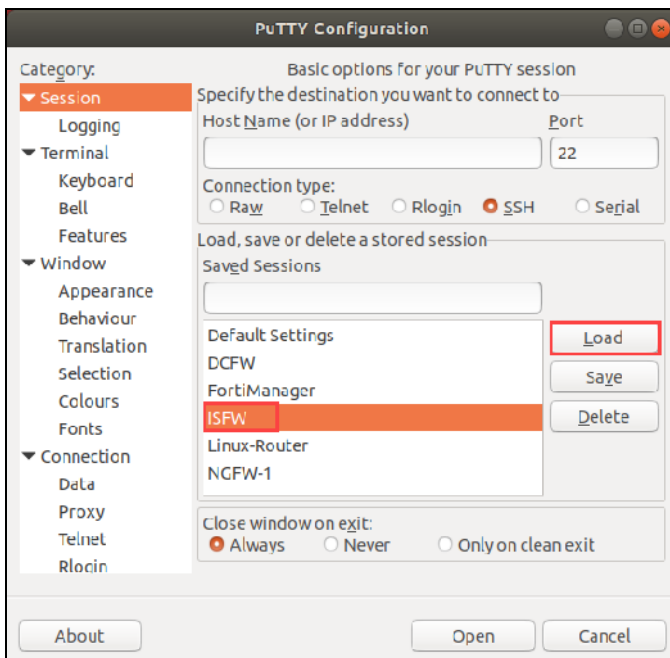
In this exercise, you will create an IPS custom signature, based on information taken from a packet capture, to block files downloaded using FTP.

Capture and Analyze the Traffic

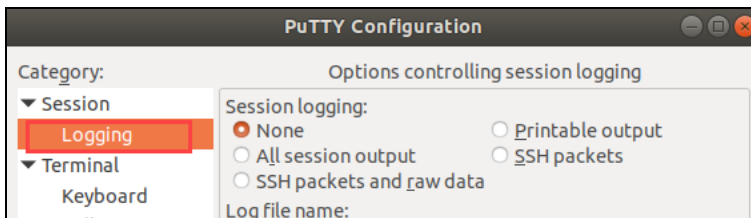
You will run the sniffer on the FTP traffic while downloading a file from an FTP server. Then, you will use a Perl script to convert the packet capture to a PCAP file that you can analyze using Wireshark. The objective of the analysis is to identify the information in the packet payload you can use to block FTP downloads.

To start the packet capture

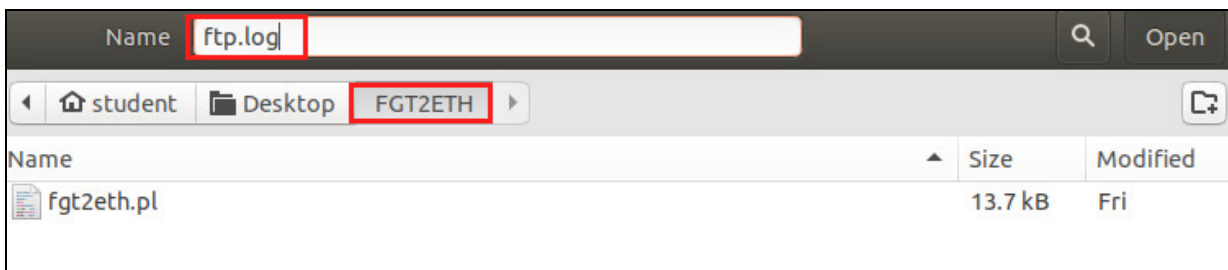
1. Connect to the Client-10 VM.
2. Open PuTTY.
3. Click **ISFW** to select the saved session, and then click **Load**.



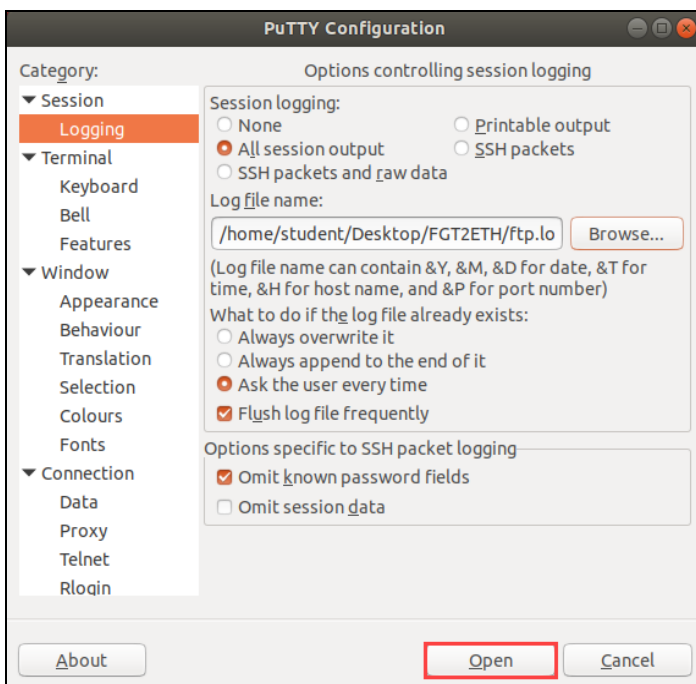
4. Click **Session > Logging**.



5. Click **All session output**.
6. Click **Browse**.
7. Click **Desktop > FGT2ETH**.
8. In the **Name** field, type `ftp.log`.



9. Click **Open**.
10. Click **Open**.

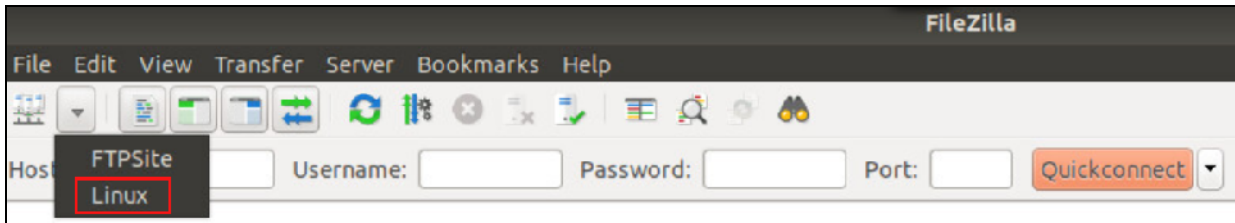


11. Log in with the username `admin` and password `password`.
12. Enter the following command to start the sniffer:
`diagnose sniffer packet port3 "port 21" 3`

Leave the PuTTY session running in the background.

To generate FTP traffic

1. On the Client-10 VM, open FileZilla.
2. In the **Site Manager** field, select **Linux**.



3. Select **Student > Desktop** as the local site folder, and **pub** as the remote site folder.
4. Right-click the `test.text` file, and then select **Download**.
5. Return to the PuTTY window, and then press `Ctrl+C`.
You should see the captured packets.
6. Close the PuTTY window.
7. Delete the `test.text` file from the desktop.

To convert the capture to PCAP

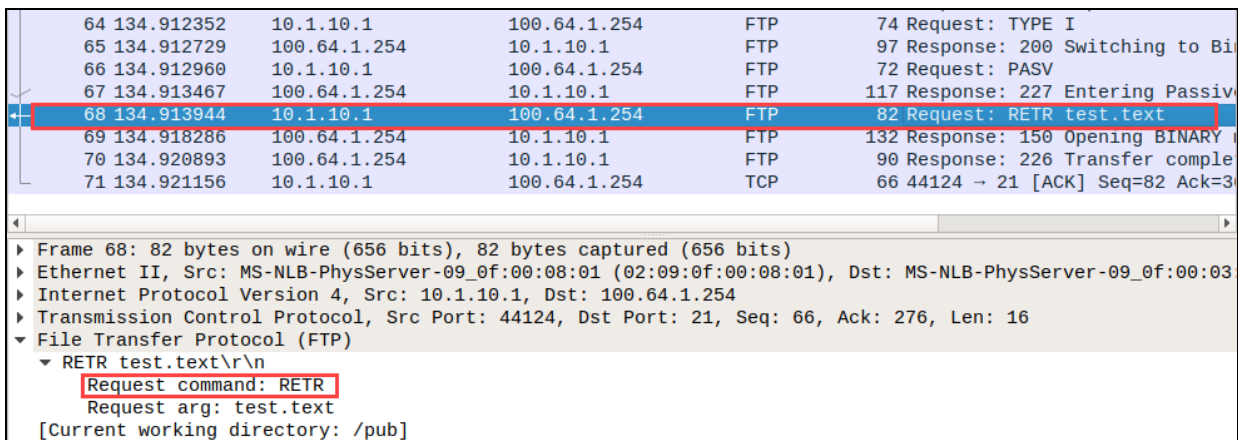
1. On the Client-10 VM, open a terminal window.
2. Enter the following commands:

```
cd Desktop/FGT2ETH/
./fgt2eth.pl -in ftp.log
```

The Perl script converts the `ftp.log` file to a PCAP file with the name `ftp.log.pcap`.
3. Close the terminal window.

To analyze the PCAP file

1. On the Client-10 VM desktop, double-click the **FGT2ETH** folder.
2. Double-click the `ftp.log.pcap` file.
This starts Wireshark and opens the file for analysis.
3. View the information in the packets captured.



Verify that FileZilla used the `FTP RETR` command to request the download. You will use this information to create the custom signature.

Review and Install the IPS Custom Signature

You will use the information you gathered in the previous steps to create an IPS custom signature that will block all FTP download requests. On FortiManager, you will add the custom signature to an IPS profile, and then push the configuration change to ISFW.

To review the custom signature

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Access**.
3. Click **Policy & Objects**.
4. Click **Object Configuration**.
5. Click **Security Profiles > IPS Signatures**.
6. Click **Block.FTP.RETR**, and then click **Edit**.
7. Review the custom signature.

The signature will block any FTP packets coming from the client where the payload contains the pattern `RETR`.

8. Click **Cancel**.

To apply the custom signature to an IPS profile

1. Continuing on the FortiManager GUI, click **Security Profiles > Intrusion Prevention**.
2. Click **protect_client** to select it, and then click **Edit**.
3. Under **IPS Signatures and Filters**, select **Block.FTP.RETR**, and then click **Edit**.
4. In the **Action** field, select **Reset**.
5. In the **Status** field, select **Enable**.
6. In the **Signatures** section, verify that **Block.FTP.RETR** is selected.

Edit IPS Signatures and Filters

Type: Filter Signature

Action: Reset

Packet Logging: Enable Disable

Status: Enable Disable Default

Rate-based Setting: Default Specify

Exempt IPs: 0 Edit

Signatures

Name	CVE-ID
Block.FTP.RETR	

OK Cancel

7. Click **OK**.
8. In the **Change Note** field, type some text because this field is required to proceed.
9. Click **OK**.

To apply the IPS profile to a security policy

1. Continuing on the FortiManager GUI, click **Policy Packages**.
2. Click **ISFW > Security Policy**.
3. Click policy sequence **1** to select it.
4. Click **Edit > Edit**.
5. In the **Security Profiles** section, set the **IPS** field to **protect_client**.
6. Click **Close**.
7. In the **Change Note** field, type some text because this field is required to proceed.
8. Click **OK**.

To install the policy

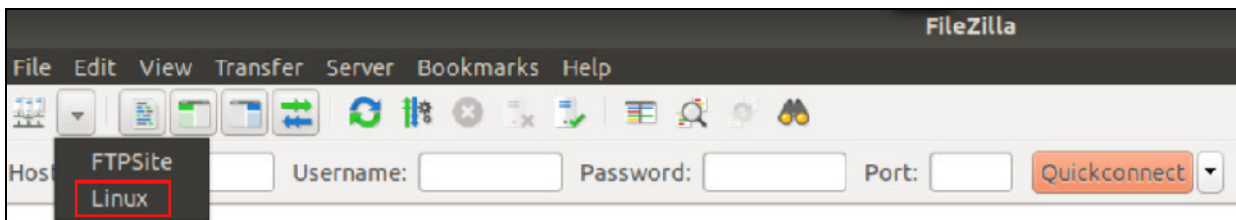
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Verify that the **ISFW** policy package is selected.
3. Click **Next**.
4. Verify that **ISFW** is selected, and then click **Next**.
5. Click **Install Preview** to see the changes that will be applied to the FortiGate.
6. On the **Install Preview** page, click **Close**.
7. Click **Install**.
Wait until the installation finishes.
8. Click **Finish**.

Test the IPS Custom Signature

You will test the IPS custom signature by generating FTP traffic from Client-10.

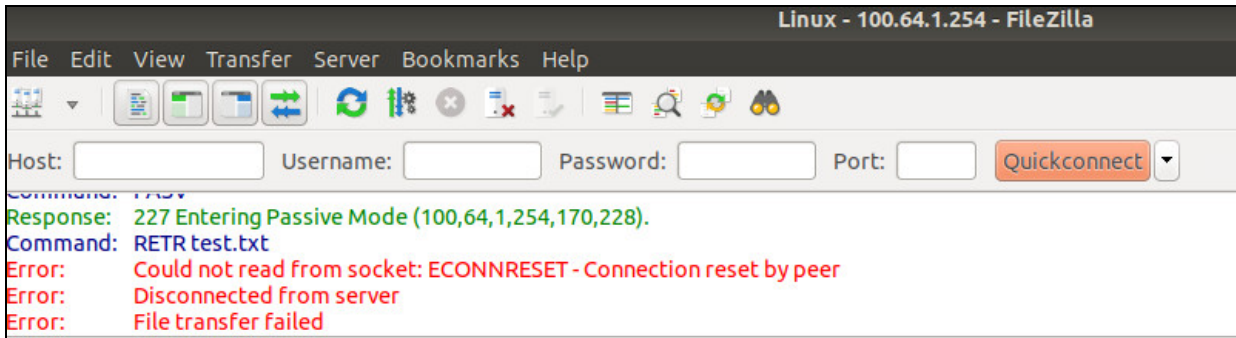
To test the IPS custom signature

1. On the Client-10 VM, open FileZilla, and then connect to the Linux site again.



2. Select **Desktop** as the local site folder, and **pub** as the remote site folder.
3. Right-click the `test.text` file, and then select **Download**.

You will see the following error messages:



If you run the sniffer on the FTP traffic now, you will capture a reset (RST) packet that FortiGate sent to drop the TCP connection after the packet with the `RETR` command was received.

- Log in to the ISFW GUI with the username `admin` and password `password`.
- Click **Login Read-Only**.
- Click **Log & Report > Security Events > Intrusion Prevention**.

You should see the log messages showing the name of the IPS sensor that blocked the packets.

Date/Time		Severity	Source	Protocol	User	Action	Attack Name	Count
2023/03/02 07:57:05		■■■■■	10.1.10.1	6		reset	Block.FTP.RETR	
2023/03/02 07:57:05		■■■■■	10.1.10.1	6		reset	Block.FTP.RETR	
2023/03/02 07:57:05		■■■■■	10.1.10.1	6		reset	Block.FTP.RETR	



The **Intrusion Protection** logs section does not appear if there are no IPS logs. FortiGate shows it after creating logs. After the attacks, if this menu item does not appear, log out of the FortiGate GUI, and then log in again to refresh it.

Lab 10: IPsec VPN (IKEv2)

In this lab, you will configure a hub-and-spoke VPN network using the FortiManager VPN manager.

Objectives

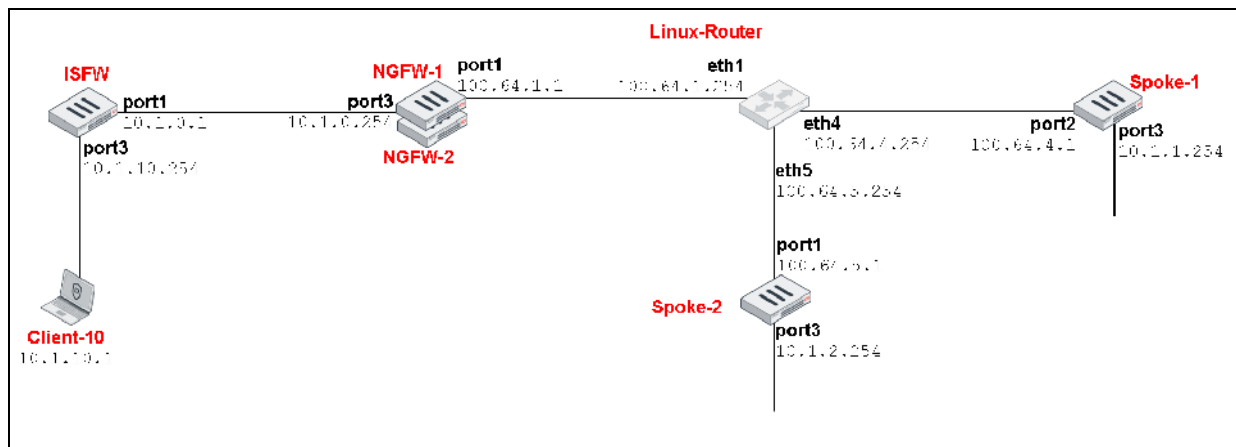
- Configure multiple IPsec VPN tunnels using the VPN manager on FortiManager
- Run CLI commands to gather the IPsec status

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

You will work on NGFW-1, Spoke-1, and Spoke-2.



Prerequisites

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

Exercise 1: Using the VPN Manager

In this exercise, you will configure IPsec tunnels between the spokes and NGFW-1, using the VPN manager on FortiManager. You will configure NGFW-1 as a hub, and the other two FortiGate devices as spokes. You will:

1. Configure a VPN community.
2. Add each of the FortiGate devices to the community as managed devices.
3. Install the VPN configuration.
4. Add the firewall policies.
5. Install the firewall policy configuration.

At the end of the lab, you will use CLI commands to display IPsec tunnel information.

Create a VPN Community

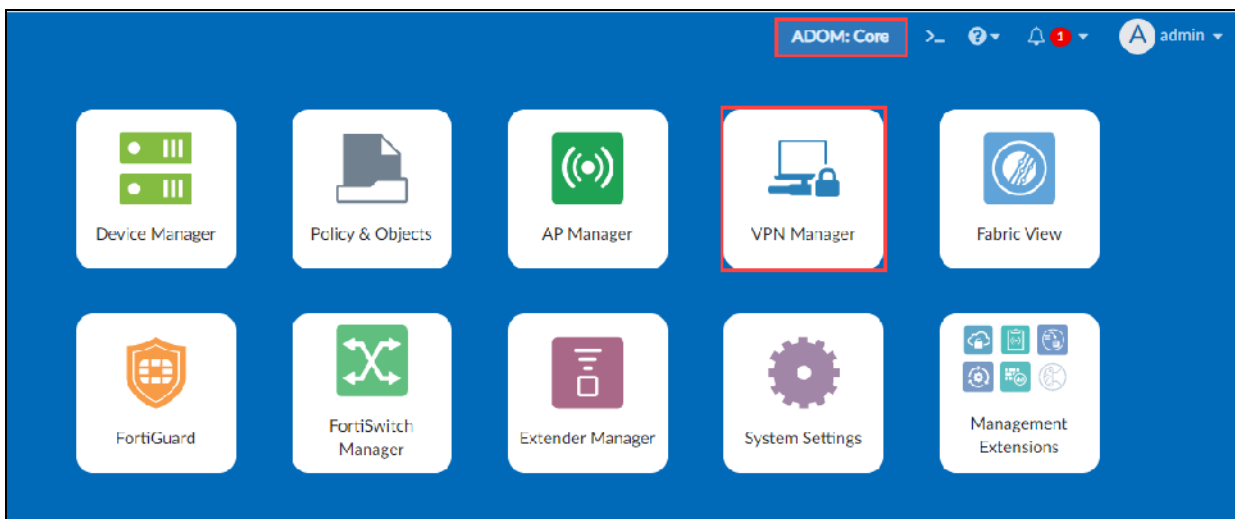
You will create a new VPN community using the central VPN manager. VPN communities allow users to create a specific type of VPN topology for FortiGate devices that share a similar IPsec configuration. Within the same VPN topology, users can assign different roles to the FortiGate devices, such as hub or spoke.



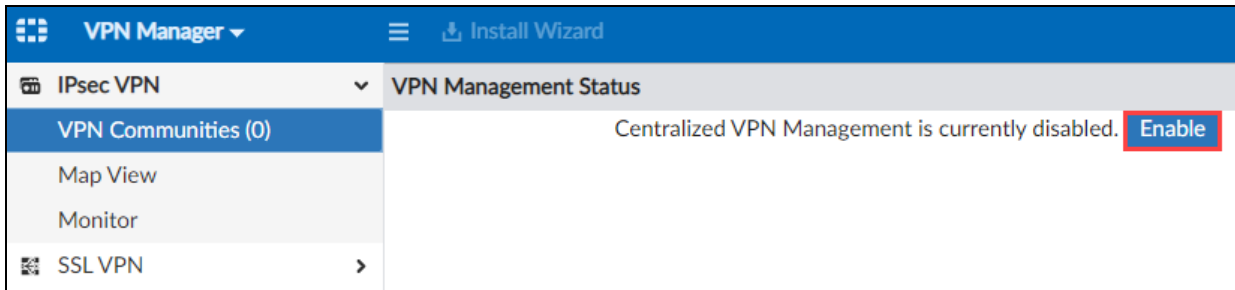
All FortiGate devices for use in this lab (NGFW-1, Spoke-1, and Spoke-2) were already added to the **Core** ADOM.

To create a VPN community

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **VPN Manager**.
4. Click **IPsec VPN > VPN Communities**.

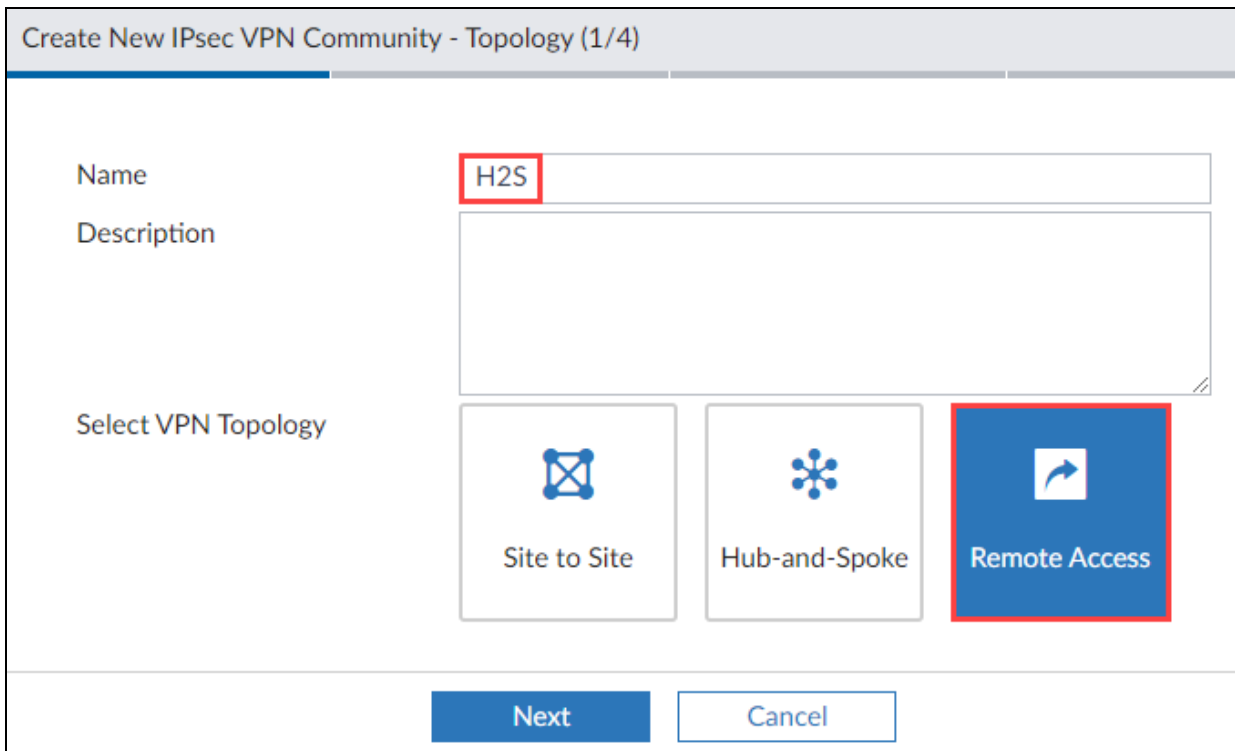


5. Click **Enable**.



6. Click **Create New**.
7. In the **Name** field, type `H2S`.
8. Click **Remote Access**.

Your configuration should match the following example:



9. Click **Next**.
10. In the **Authentication** section, click **Pre-Shared Key**.
11. In the **Pre-shared Key Type** section, click **Specify**, and in the text field, type `fortinet`.
12. In the **IKE Version** section, click **2**.

Your configuration should match the following example:

Create New IPsec VPN Community - Authentication & Encryption (2/4)

Authentication **Pre-Shared Key** Certificates

Pre-Shared Key Type Generate (random) **Specify**

fortinet

Encryption

IKE Security (Phase 1)

Properties

IKE Version 1 **2**

Encryption	Authentication	Action
------------	----------------	--------

Back Next Cancel

13. Click **Next**.
14. Click **Next**.
15. Review the settings on the **Summary** page, and then click **OK**.

Create New IPsec VPN Community - Summary (4/4)

Name H2S

Topology Remote Access

Authentication Pre-shared Key (Specify)

Encryption

IKE Security (Phase 1)

Properties

Back **OK** Cancel

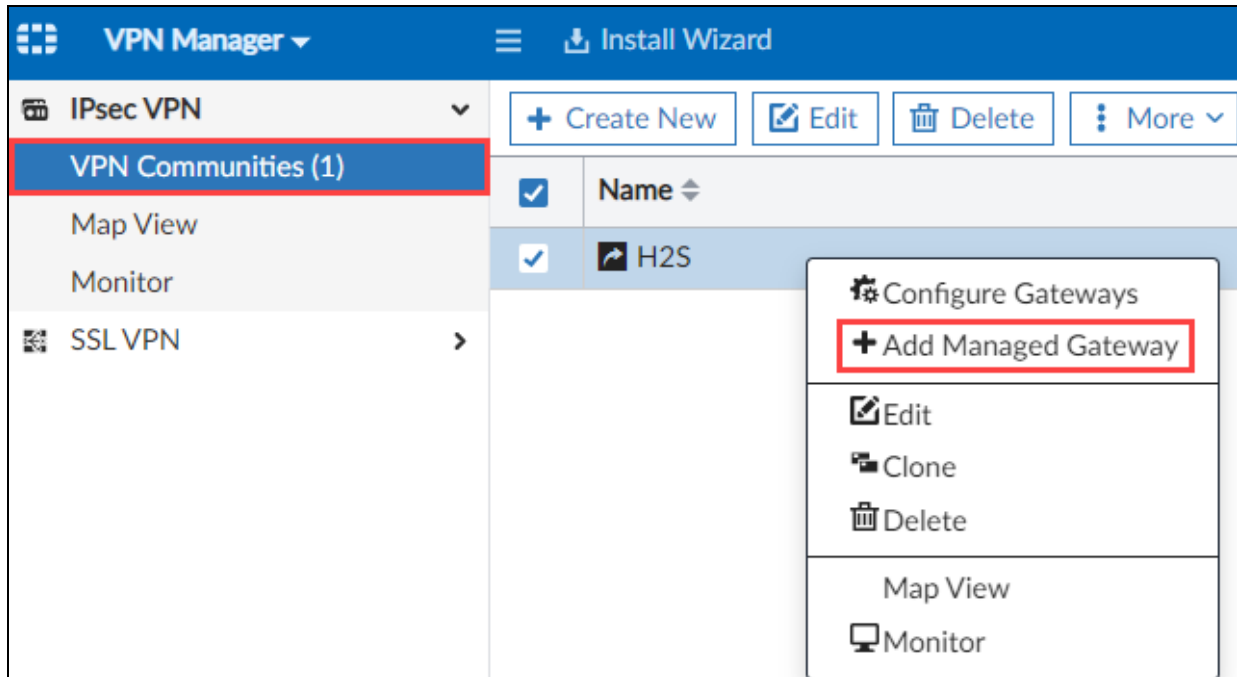
Add NGFW-1, Spoke-1, and Spoke-2 as Managed Devices

After you create a VPN community, you must add gateways to the topology. Now, you will assign roles (hub or spoke) to the FortiGate devices. First, you will add NGFW-1 to the VPN community as a hub device. Then, you will

add Spoke-1 and Spoke-2 as spoke devices.

To add NGFW-1 as a hub

1. Continuing on the FortiManager GUI, click **VPN Communities**.



2. Right-click **H2S**, and then select **Add Managed Gateway**.
The **VPN Gateway Setup Wizard** opens.
3. In the **Protected Subnet** section, click **Click to select**.
4. In the drop-down list, select **all**, and then click **OK**.

Create New VPN Gateway - Protected Network (1/5)

Protected Network

Device

Default VPN Interface

Local Gateway

Advanced

Protected Subnet

Click to select

Selected 1 (Total: 29)

- ☐ FQDN:auth.gfx.ms
- ☐ upg_softwareupdate.vmware.com
- ☐ FQDN:softwareupdate.vmware.com
- ☒ all
- ☐ gmail.com
- ☐ login.microsoft.com
- ☐ login.microsoftonline.com

IP/Netmask: 0.0.0.0/0.0.0.0

OK Cancel

Next Cancel

5. Click **Next**.
6. In the **Role** section, verify that **Hub** is selected, and then in the **Device** field, select **NGFW-1**.

Create New VPN Gateway - Device (2/5)

Protected Network

Device

Default VPN Interface

Local Gateway

Advanced

Role

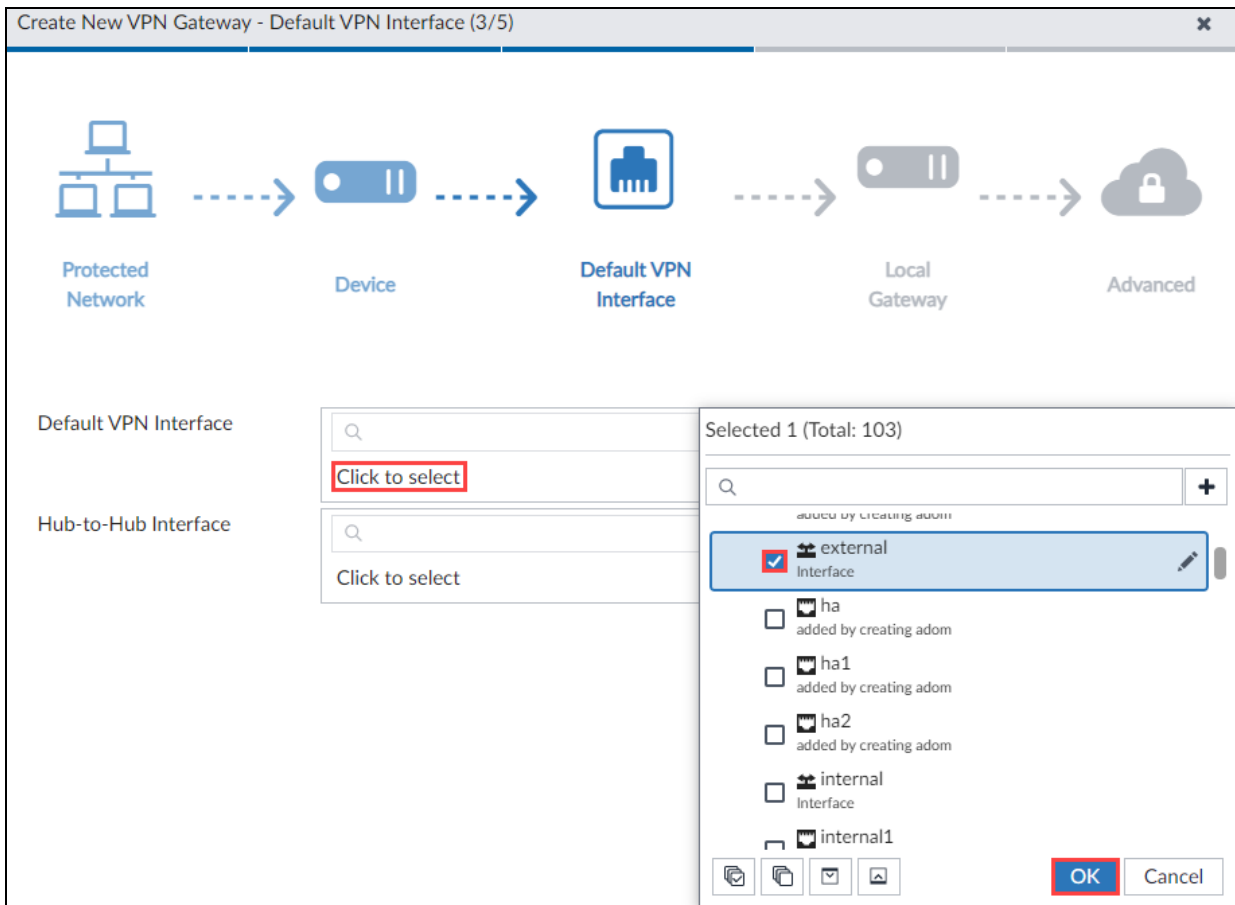
Hub Spoke

Device

NGFW-1[root]

7. Click **Next**.
8. In the **Default VPN Interface** section, click **Click to select**.

9. In the drop-down list, select **external**, and then click **OK**.



10. Click **Next**.
11. Keep the **Local Gateway** field set to 0 . 0 . 0 . 0, and then click **Next**.
12. In the **Accept Peer Type** section, select **Any Peer ID**.
13. Disable **Add Route**.

Create New VPN Gateway - Advanced (5/5)

Protected Network Device Default VPN Interface Local Gateway Advanced

Local ID:

Routing: **Manual (via Device Manager)** Automatic

Summary Network(s):

Seq#	Network	Priority	Action
+			

Accept Peer Type: **Any Peer ID** Peer ID Dialup Group Peer Peer Group

XAUTH Type: **Disable** PAP Server CHAP Server AUTO Server

Enable IKE Configuration: ☐

Method ("mode config"):

Add Route: ☒

Advanced Options >

13. Click **OK**.

NGFW-1 is added as a managed gateway, with the hub role.

H2S				
+ Create New Edit Delete More Search...				
☐	Name	Role	Default VPN Interface	Protected Subnet
☐	NGFW-1[root] View Details >	Hub	external	all

14. Click **Return**.

To add Spoke-1 as a spoke

- Continuing on the FortiManager GUI, right-click **H2S**, and then select **Add Managed Gateway**. The **VPN Gateway Setup Wizard** starts.
- In the **Protected Subnet** section, click **Click to select**.
- In the drop-down list, select **all**, and then click **OK**.
- Click **Next**.
- In the **Role** section, click **Spoke**, and then in the **Device** drop-down list, select **Spoke-1**.
- Click **Next**.
- In the **Default VPN Interface** section, click **Click to select**.
- In the drop-down list, select **external**, and then click **OK**.
- Click **Next**.

10. Keep the **Local Gateway IP Address** field set to 0.0.0.0, and then click **Next**.
11. Disable **Enable IP Assignment**.

Create New VPN Gateway - Advanced (5/5)

Protected Network Device Default VPN Interface Local Gateway Advanced

Local ID:

Routing: **Manual (via Device Manager)** Automatic

XAUTH Type: **Disable** Client

Enable IKE Configuration: ☐

Method ("mode config"):

Enable IP Assignment: ☒

IPv4 Netmask:

Add Route: ☐

Advanced Options >

10. Click **OK**.
Spoke-1 is added as another managed gateway, with the spoke role.

H2S

+ Create New Edit Delete More Search...

☐	Name	Role	Default VPN Interface	Protected Subnet	
☐	NGFW-1[root] View Details >	Hub	external	all	
☐	Spoke-1 (root) View Details >	Spoke	external	all	

2

Return

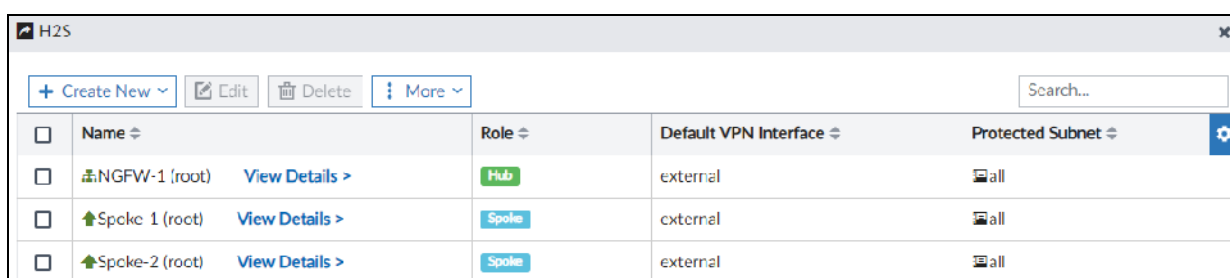
11. Click **Return**.

To add Spoke-2 as a spoke

1. Continuing on the FortiManager GUI, right-click **H2S**, and then select **Add Managed Gateway**.
The **VPN Gateway Setup Wizard** opens.

2. In the **Protected Subnet** section, click **Click to select**.
3. In the drop-down list, select **all**, and then click **OK**.
4. Click **Next**.
5. In the **Role** section, click **Spoke**, and then in the **Device** field, select **Spoke-2**.
6. Click **Next**.
7. In the **Default VPN Interface** section, click **Click to select**.
8. In the drop-down list, select **external**, and then click **OK**.
9. Click **Next**.
10. Keep the **Local Gateway IP Address** field set to 0 . 0 . 0 . 0, and then click **Next**.
11. Disable **Enable IP Assignment**.
10. Click **OK**.

Spoke-2 is added as another managed gateway, with the spoke role.



☐	Name	Role	Default VPN Interface	Protected Subnet
☐	NGFW-1 (root) View Details >	Hub	external	all
☐	Spoke 1 (root) View Details >	Spoke	external	all
☐	Spoke-2 (root) View Details >	Spoke	external	all

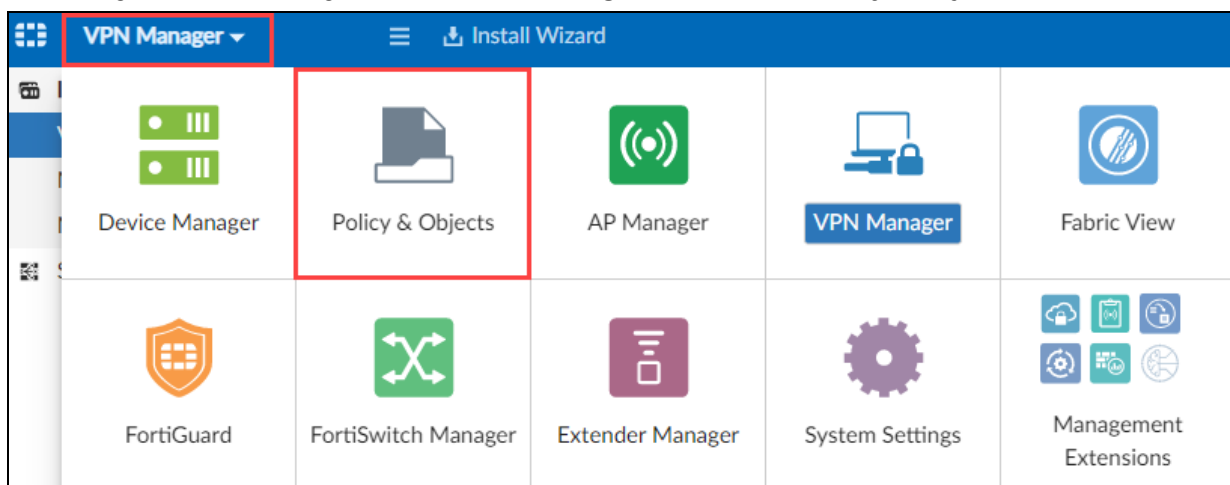
11. Click **Return**.

Install the VPN Configuration

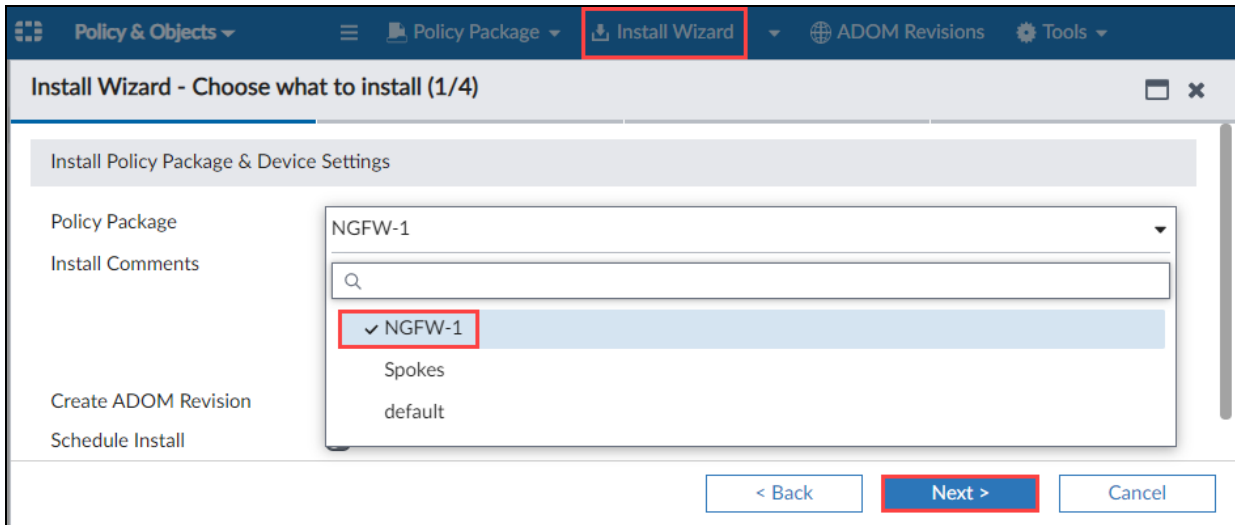
Before you create firewall policies, you must install the VPN settings on the FortiGate devices. This creates the IPsec virtual interfaces that are required for the firewall policies.

To install the VPN configuration on NGFW-1

1. Continuing on the FortiManager GUI, click **VPN Manager**, and then click **Policy & Objects**.



2. Click **Install Wizard**.
3. In the **Policy Package** field, select **NGFW-1**.



4. Click **Next**.
5. Confirm that **NGFW-1** is selected, and then click **Next**.
6. Click **Install Preview** to see the changes that will be applied to FortiGate.
7. On the **Install Preview** page, click **Close**.
8. Click **Install**.
Wait until the installation finishes.
9. Click **Finish**.

To install the VPN configuration on both spokes

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. In the **Policy Package** field, select **Spokes**.
3. Click **Next**.
4. Confirm that both **Spoke-1** and **Spoke-2** are selected, and then click **Next**.
5. Click **Install**.
Wait until the installation finishes.
6. Click **Finish**.

Configure the Firewall Policies

After you install the VPN configuration on all FortiGate devices, you can configure the firewall policies to allow IPsec traffic to pass.

On NGFW-1, you will configure three firewall policies to achieve the following:

- Allow traffic from the spokes to NGFW-1
- Allow traffic from NGFW-1 to the spokes
- Allow traffic between the spokes

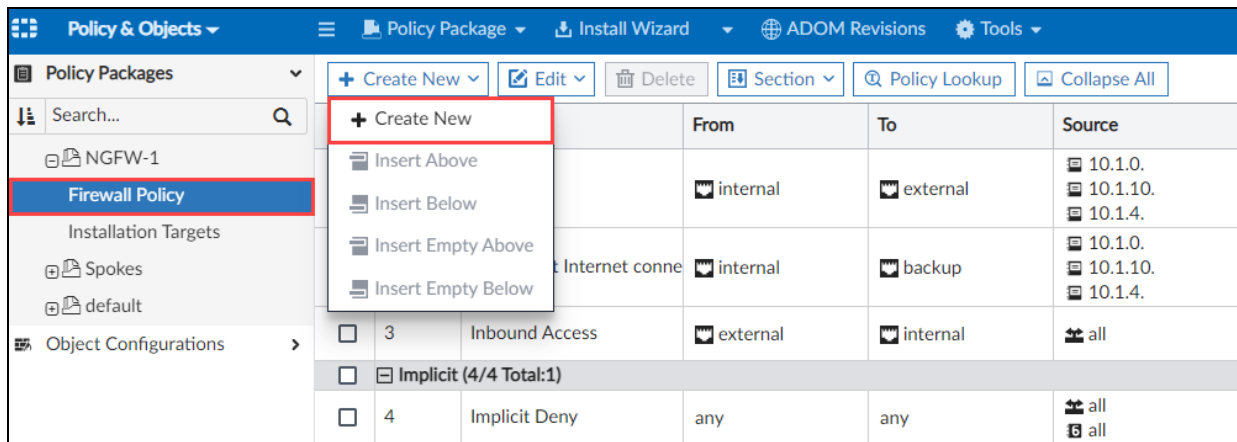
On the spokes, you will configure two firewall policies to achieve the following:

- Allow traffic from the spokes to NGFW-1
- Allow traffic from NGFW-1 to the spokes

Because Spoke-1 and Spoke-2 share the same policy package, you will create the firewall policies in one policy package (**Spokes**). Then, you will push the changes to both FortiGate devices. This is the advantage of having multiple FortiGate devices with the same security policies sharing the same policy package.

To configure the firewall policies for traffic between NGFW-1 and the spokes

1. Continuing on the FortiManager GUI, click **NGFW-1 > Firewall Policy**.
2. Click **Create New**, and then select **Create New**.



3. Configure the following settings:

Field	Value
Name	Internal to IPsec
Incoming Interface	internal
Outgoing Interface	vpnmgr_H2S_hub2spoke
Source Address	all
Destination Address	all
Service	ALL
Schedule	always
Action	Accept
Log Allowed Traffic	All Sessions

4. In the **Change Note** field, type some text because this field is required to proceed.
5. Click **OK**.

Your configuration should match the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action	Secur
1	Internet	internal	external	10.1.0.10.1.10.10.1.4.	all	always	ALL	Accept	SSL no-prot def
2	Redundant Internet connec	internal	backup	10.1.0.10.1.10.10.1.4.	all	always	ALL	Accept	SSL no-prot def
3	Inbound Access	external	internal	all	Linux_Server	always	HTTP	Accept	SSL no-prot def
4	Internal to IPsec	internal	vpnmgr_H2S_hub2	all	all	always	ALL	Accept	SSL no-prot def
Implicit (5/5 Total)									
5	Implicit Deny	any	any	all	all	always	ALL	Deny	

- Click **Create New**, and then select **Create New**.
- Configure the following settings:

Field	Value
Name	IPsec to Internal
Incoming Interface	vpnmgr_H2S_hub2spoke
Outgoing Interface	internal
Source Address	all
Destination Address	all
Service	ALL
Schedule	always
Action	Accept
Log Allowed Traffic	All Sessions

- In the **Change Note** field, type some text because this field is required to proceed.
- Click **OK**.



You can also create this reverse firewall policy by selecting the previous firewall policy, and with a right click, you select **Clone Reverse**.

To configure the firewall policy for traffic between spokes

- Continuing on the FortiManager GUI, click **Create New**, and then select **Create New**.
- Configure the following settings:

Field	Value
Name	Spoke to Spoke

Field	Value
Incoming Interface	vpnmgr_H2S_hub2spoke
Outgoing Interface	vpnmgr_H2S_hub2spoke
Source Address	all
Destination Address	all
Service	ALL
Schedule	always
Action	Accept
Log Allowed Traffic	All Sessions

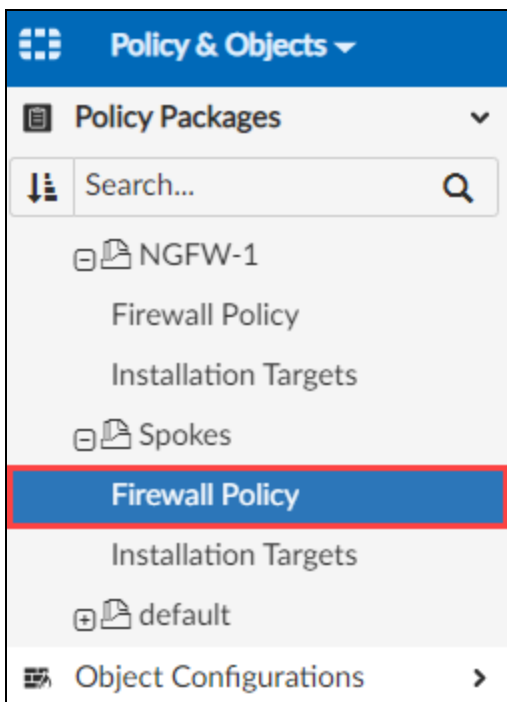
3. In the **Change Note** field, type some text because this field is required to proceed.
4. Click **OK**.

Your configuration should match the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action
1	Internet	internal	external	10.1.0, 10.1.10, 10.1.4	all	always	ALL	Accept
2	Redundant Internet connec	internal	backup	10.1.0, 10.1.10, 10.1.4	all	always	ALL	Accept
3	Inbound Access	external	Internal	all	Linux_Server	always	HTTP	Accept
4	Internal to IPsec	internal	vpnmgr_H2S_hub2spoke	all	all	always	ALL	Accept
5	IPsec to Internal	vpnmgr_H2S_hub2spoke	internal	all	all	always	ALL	Accept
6	Spoke to Spoke	vpnmgr_H2S_hub2spoke	vpnmgr_H2S_hub2spoke	all	all	always	ALL	Accept
Implicit (7/7 Total:1)								
7	Implicit Deny	any	any	all	all	always	ALL	Deny

To configure the firewall policies on the spokes

1. Continuing on the FortiManager GUI, click **Spokes > Firewall Policy**.



2. Click **Create New**, and then select **Create New**.
3. Configure the following settings:

Field	Value
Name	Internal to IPsec
Incoming Interface	internal
Outgoing Interface	vpnmgr_H2S_spoke2hub
Source Address	all
Destination Address	all
Service	ALL
Schedule	always
Action	Accept
Log Allowed Traffic	All Sessions

4. In the **Change Note** field, type some text because this field is required to proceed.
5. Click **OK**.
6. Click **Create New**, and then select **Create New**.
7. Configure the following settings:

Field	Value
Name	IPsec to Internal
Incoming Interface	vpnmgr_H2S_spoke2hub
Outgoing Interface	internal
Source Address	all
Destination Address	all
Service	ALL
Schedule	always
Action	Accept
Log Allowed Traffic	All Sessions

- In the **Change Note** field, type some text because this field is required to proceed.
- Click **OK**.

Your configuration should match the following example:

#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	Log
1		internal	external	all	all	always	ALL	✓ Accept	no-inspection	Log Security Events
2	Internal to IPsec	internal	vpnmgr_H2S_spok	all	all	always	ALL	✓ Accept	no-inspection	Log All Sessions
3	IPsec to Internal	vpnmgr_H2S_spok	internal	all	all	always	ALL	✓ Accept	no-inspection	Log All Sessions
Implicit (4/4 Total)										
4	Implicit Deny	any	any	all	all	always	ALL	✗ Deny		No Log

Stop and think!

Look at the VPN zone name for the spokes. Is it the same one as the one you used when you configured NGFW-1? If not, why is it different?

FortiManager created three separate VPN zones (**vpnmgr_H2S_spoke2hub**, **vpnmgr_H2S_hub2spoke**, and **vpnmgr_H2S_mesh**). Depending on the role defined for each managed gateway, FortiManager pushed different VPN zones to the corresponding FortiGate devices. The **vpnmgr_H2S_hub2spoke** zone will be used only when defining the firewall policy on the hub, and the **vpnmgr_H2S_spoke2hub** zone will be used only when defining the firewall policy on the spokes.

Install the Policy Packages

First, you will install the **NGFW-1** policy package, and then you will install the **Spokes** policy package.

Take the Expert Challenge!

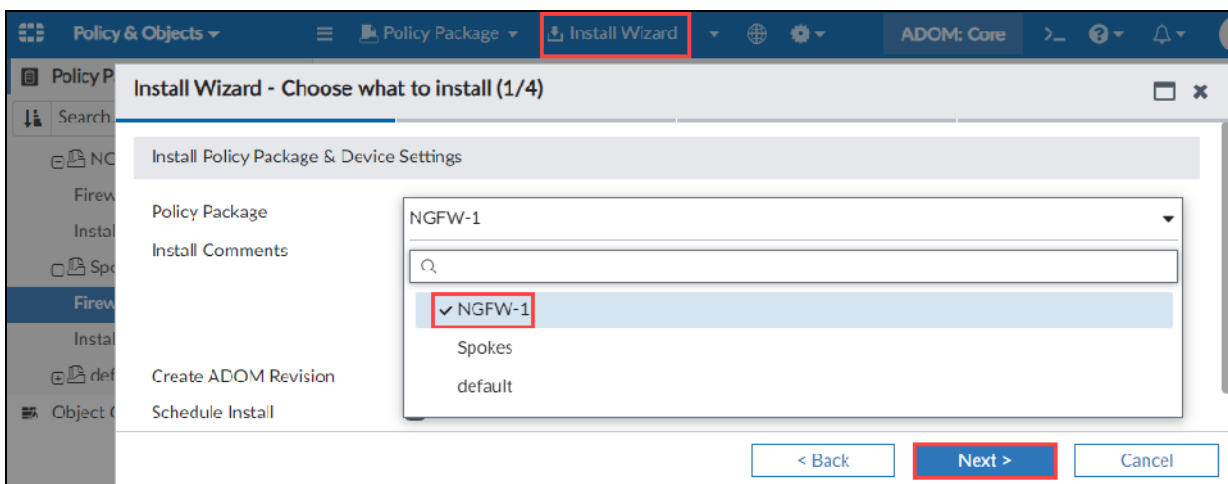
- Install the **NGFW-1** policy package on NGFW-1.
- Install the **Spokes** policy package on Spoke-1 and Spoke-2.

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

After you complete the challenge, see [Check the Status of the VPN Tunnel on page 146](#).

To install the NGFW-1 policy package on NGFW-1

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. In the **Policy Package** field, select **NGFW-1**.



3. Click **Next**.
4. Verify that the **NGFW-1** device is selected, and then click **Next**.
5. Click **Install**.
Wait until the installation finishes.
6. Click **Finish**.

To install the Spokes policy package on Spoke-1 and Spoke-2

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. In the **Policy Package** field, select **Spokes**.
3. Click **Next**.
4. Verify that both the **Spoke-1** and **Spoke-2** devices are selected, and then click **Next**.
5. Click **Install**.
Wait until the installation finishes.
6. Click **Finish**.

Check the Status of the VPN Tunnel

You won't be able to send traffic through the tunnel yet, because the routing component is still missing. However, you will check the VPN tunnel status on both Spoke-1 and Spoke-2. You can do this in the FortiGate GUI, FortiManager GUI, or FortiGate CLI. In this procedure, you will use the FortiGate CLI.

To check the VPN tunnel on Spoke-1

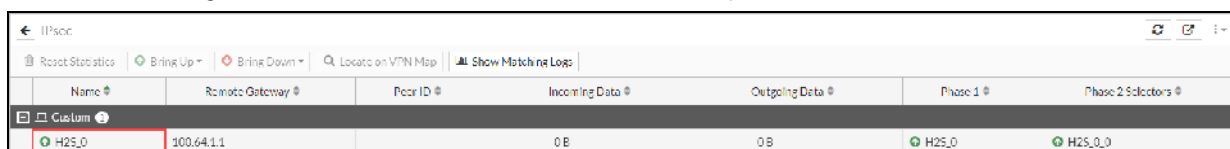
1. Connect over SSH to **Spoke-1**.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

```
diagnose vpn tunnel up H2S_0_0
diagnose vpn tunnel list name H2S_0
```

The first command will bring the tunnel up, if it's not already established. The `diagnose vpn tunnel list` command displays the current IPsec SA information for all active tunnels. The `diagnose vpn tunnel list name <tunnel name>` command provides SA information about a specific tunnel.

4. Log in to the Spoke-1 GUI with the username `admin` and password `password`.
5. Click **Login Read-Only**.
6. Click **Dashboard > Network**.
7. Click anywhere on the **IPsec** widget.

You should see a green arrow, which indicates that the tunnel is up.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
H2S_0	100.64.1.1		0 B	0 B	H2S_0	H2S_0_0

To check the VPN tunnel on Spoke-2

1. Connect over SSH to **Spoke-2**.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

```
diagnose vpn tunnel up H2S_0_0
diagnose vpn tunnel list name H2S_0
```

The first command will bring the tunnel up, if it's not already established.

4. Log in to the Spoke-2 GUI with the username `admin` and password `password`.
5. Click **Login Read-Only**.
6. Click **Dashboard > Network**.
7. Click anywhere on the **IPsec** widget.

You should see a green arrow, which indicates that the tunnel is up.

To confirm the IPsec VPN IKE version 2 configuration

1. Connect over SSH to **NGFW-1**.
2. Log in with the username `admin` and password `password`.

3. Enter the following command:

```
get vpn ipsec tunnel details
```

You should see an output similar to the following example:

```
NGFW-1 # get vpn ipsec tunnel details

gateway
  name: 'H2S_0_0'
  local-gateway: 100.64.1.1:0 (static)
  remote-gateway: 100.64.3.1:0 (dynamic)
  dpd-link: on
  mode: ike-v2
  interface: 'port1' (3)
  rx packets: 0 bytes: 0 errors: 0
  tx packets: 0 bytes: 0 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'H2S_0_0'
    auto-negotiate: disable
    mode: tunnel
    src: 0:0.0.0.0-255.255.255.255:0
    dst: 0:0.0.0.0-255.255.255.255:0
  SA
    lifetime/rekey: 1800/1688
    mtu: 1280
    tx-esp-seq: 1
    replay: enabled
    qat: 0
    inbound
      spi: f6f7e7ae
      enc: aes-cb b53c38d231212ca7c7447fca2e91a240
      auth: sha256 eb29b788dec9a60ba203edebd3a0bb7e215dfbc5e6bc54ed6feb0259f9a7c581
    outbound
      spi: 19ab6560
      enc: aes-cb a5e65748fe61397411b7256a53fab885
      auth: sha256 31f0df873e783d44cc31854f2e86bb78a27ba9da3d287c0250dd2b2ae0569832
  NPU acceleration: none
```



This output confirms that the mode is `ike-v2` and DPD is negotiated `on-demand`.

Lab 11: Auto-Discovery VPN

You will modify the IPsec VPN configuration to enable auto-discovery VPN (ADVPN). You will create an on-demand tunnel between the two spokes. You will configure IBGP with route reflector enabled on the hub device to manage the routing. Since ADVPN parameters aren't available on the FortiManager GUI, you will push the required settings using CLI and TCL scripts.

Objectives

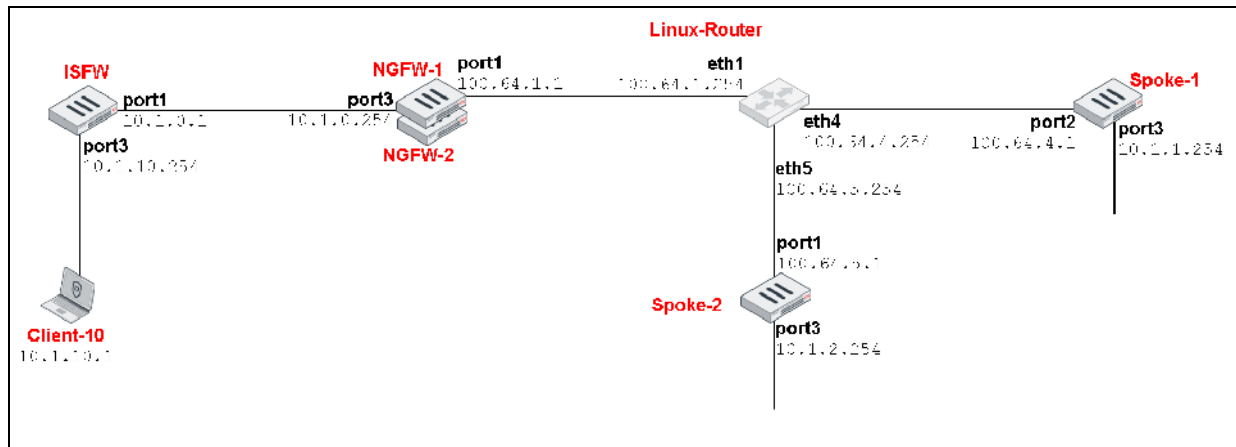
- Configure ADVPN to dynamically create IPsec tunnels between spokes
- Use TCL scripts to run individualized configuration changes on multiple FortiGate devices

Time to Complete

Estimated: 30 minutes

Which Network Segment Will You Work On?

In this lab, you will configure NGFW-1, Spoke-1, and Spoke-2 for ADVPN. You will test the connectivity between Spoke-1 and NGFW-1, between Spoke-2 and NGFW-1, and finally, between both spokes.



Prerequisites

You must complete the previous lab before you start this one. If you haven't done so, tell your instructor.

Exercise 1: Configuring ADVPN and IBGP

In this exercise, you will configure ADVPN on NGFW-1 and the two spokes.

Configure ADVPN and IBGP on NGFW-1

You will run a script to enable the auto-discovery sender option, and configure IBGP and the IPsec interfaces on NGFW-1.

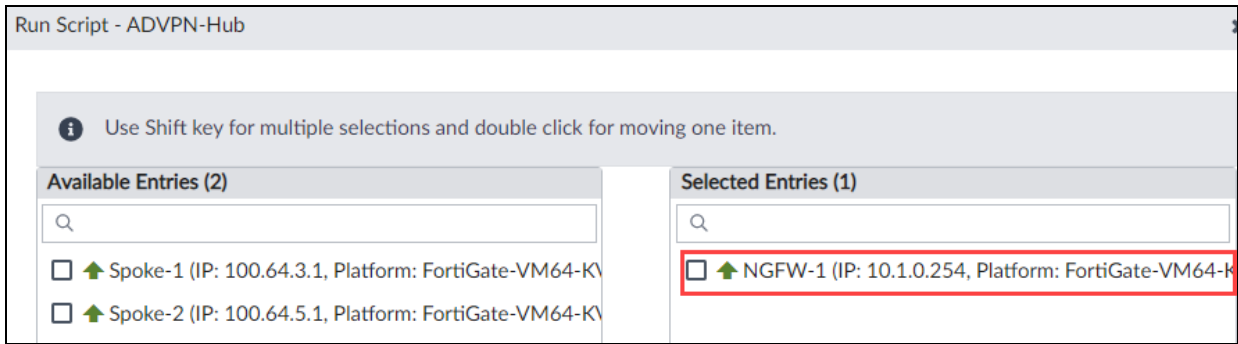
You will use a script on FortiManager to push the phase-1 ADVPN option. The script also contains the IBGP configuration and IP address for the IPsec interface. The script is already created on FortiManager.

To configure ADVPN and IBGP on NGFW-1

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **Core**.
3. Click **Device Manager**.
4. Click **Scripts**.
5. Right-click the **ADVPN-Hub** script, and then select **Edit**.
The contents of the script appear.
6. Review the commands.

```
1 config vpn ipsec phase1-interface
2 edit "H2S_0"
3 set net-device disable
4 set auto-discovery-sender enable
5 set add-route disable
6 next
7 end
8 config system interface
9 edit "H2S_0"
10 set vdom "root"
11 set ip 172.16.1.1 255.255.255.255
12 set remote-ip 172.16.1.254/24
13 next
14 end
15 config router bgp
16 set as 65100
17 set router-id 172.16.1.1
18 config neighbor-group
19 edit "advpn"
20 set remote-as 65100
21 set next-hop-self enable
22 set route-reflector-client enable
23 next
24 end
25 config neighbor-range
26 edit 1
27 set prefix 172.16.1.0 255.255.255.0
28 set neighbor-group "advpn"
29 next
30 end
31 config network
32 edit 1
33 set prefix 10.1.0.0 255.255.255.0
34 next
35 end
36 end
```

7. Click **Cancel**.
8. Right-click the **ADVPN-Hub** script again, and then select **Run Script**.
9. Move **NGFW-1** from the **Available Entries** section to the **Selected Entries** section, and then click **Run Now**.



10. Make sure NGFW-1 is the only device listed in the pop-up window, and then click **OK**.
11. Wait for the script to finish running.
The script has been configured to run the CLI commands directly on FortiGate.
12. Click **Close**.

Configure ADVPN and IBGP on the Spokes

You will configure ADVPN and IBGP on the spokes. You will run a TCL script to enable the auto-discovery receiver option, configure IBGP, and configure the IPsec interface. The TCL script does the following:

1. Retrieves the FortiGate host name
2. Extracts the spoke number from the host name
3. Configures ADVPN and IBGP using the spoke number to configure the BGP router ID, network to advertise, and IP address of the IPsec interface

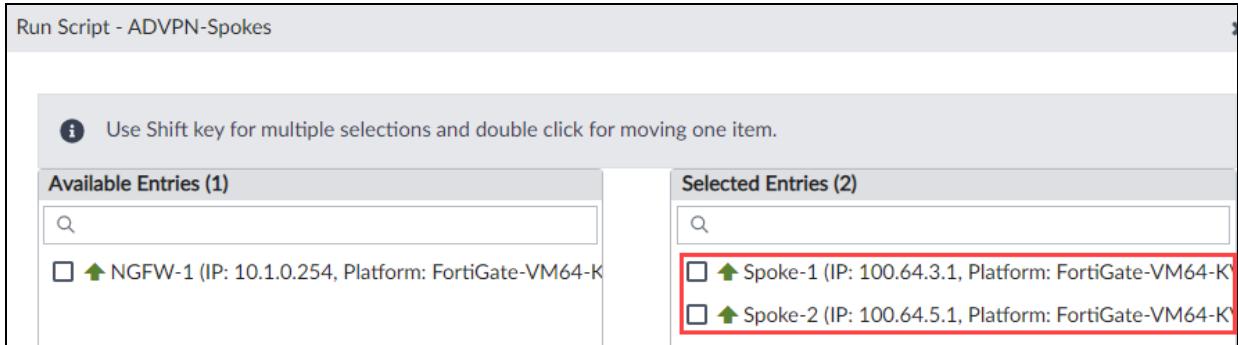
To configure ADVPN and IBGP on the spokes

1. Continuing on the FortiManager GUI, right-click the **ADVPN-Spokes** script, and then select **Edit**.
The contents of the script appear.

```
1 #!  
2 # Procedure for executing CLI commands  
3 proc do_cmd {cmd} {  
4 puts [exec "$cmd\n" "# " 15]  
5 }  
6  
7 # Extract the host name  
8 set query [exec "get system status | grep Hostname\n" "# "]  
9 set pos [lsearch $query "**Spoke*"]  
10 set hostname [lindex $query $pos]  
11  
12 # Extract the spoke number from the host name  
13 set len [string length $hostname]  
14 set pos2 [expr [string last - $hostname] + 1]  
15 set spokenum [string range $hostname $pos2 $len]  
16 set spokenumplusone [expr $spokenum + 1]  
17  
18 # Configure ADVPN and IBGP  
19 do_cmd "config vpn ipsec phase1-interface"  
20 do_cmd "edit H2S_0"  
21 do_cmd "set auto-discovery-receiver enable"  
22 do_cmd "set net-device enable"  
23 do_cmd "next"  
24 do_cmd "end"  
25 do_cmd "config system interface"  
26 do_cmd "edit H2S_0"  
27 do_cmd "set ip 172.16.1.$spokenumplusone 255.255.255.255"  
28 do_cmd "set remote-ip 172.16.1.1/24"  
29 do_cmd "next"  
30 do_cmd "end"  
31 do_cmd "config router bgp"  
32 do_cmd "set as 65100"  
33 do_cmd "set router-id 172.16.1.$spokenumplusone"  
34 do_cmd "config neighbor"  
35 do_cmd "edit 172.16.1.1"  
36 do_cmd "set remote-as 65100"  
37 do_cmd "set send-community6 disable"  
38 do_cmd "next"  
39 do_cmd "end"  
40 do_cmd "config network"  
41 do_cmd "edit 1"  
42 do_cmd "set prefix 10.1.$spokenum.0 255.255.255.0"  
43 do_cmd "next"  
44 do_cmd "end"  
45 do_cmd "end"
```

2. Review the commands.
3. Click **Cancel**.
4. Right-click the **ADVPN-Spokes** script again, and then select **Run Script**.

5. Move **Spoke-1** and **Spoke-2** from the **Available Entries** section to the **Selected Entries** section, and then click **Run Now**.



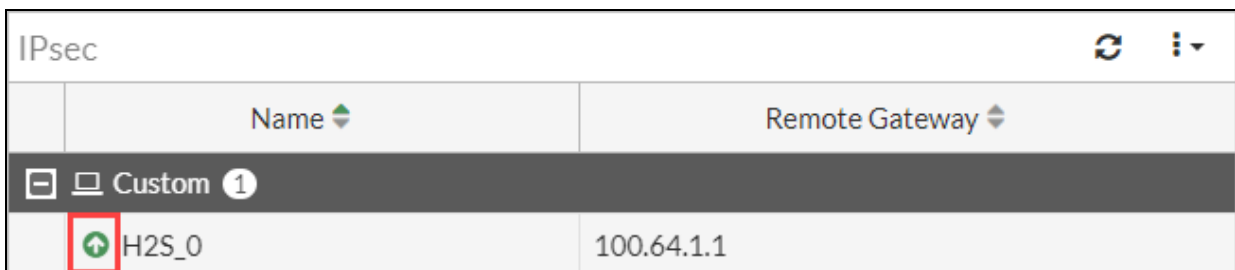
6. Make sure Spoke-1 and Spoke-2 are the only devices listed in the pop-up window, and then click **OK**.
7. Wait for the script to finish running.
The script has been configured to run the CLI commands directly on the FortiGate devices.
8. Click **Close**.

Bring Up the Static IPsec Tunnels

Before you generate traffic to trigger the on-demand tunnel, it's a good idea to verify that the BGP route databases are in sync. But first, and in case the tunnels between the spokes and hub closed after the last configuration changes, you will reconnect the tunnels.

To bring up the IPsec tunnel on Spoke-1

1. Connect over SSH to Spoke-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:
`diagnose vpn tunnel up H2S_0_0`
This command brings up the tunnel that you have just created.
4. Log in to the Spoke-1 GUI with the username `admin` and password `password`.
5. Click **Login Read-Only**.
6. Click **Dashboard > Network**.
7. In the **IPsec** widget, verify that the tunnel is up.



To bring up the IPsec tunnel on Spoke-2

1. Connect over SSH to Spoke-2.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:
`diagnose vpn tunnel up H2S_0_0`
This command brings up the tunnel that you have just created.
4. Log in to the Spoke-2 GUI with the username `admin` and password `password`.
5. Click **Login Read-Only**.
6. Click **Dashboard > Network**.
7. Click anywhere on the **IPsec** widget.
Verify that the tunnel is up.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
H2S_0	100.64.1.1		978 B	929 B	H2S_0	H2S_0_0

Check the BGP Routes

You will check that BGP is up between the FortiGate devices.

To check the BGP routes

1. Log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.
3. Click **Dashboard > Network**.
4. Click anywhere on the **Routing** widget.

The routing table should look similar to the following example:

Network	Gateway IP	Interface	Distance	Type
0.0.0.0	100.64.1.254	port1	20	BGP
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.1.0/24		H2S_0	200	BGP
10.1.2.0/24		H2S_0	200	BGP
10.1.4.0/24	10.1.0.100	port1	110	OSPF
10.1.100.0/24	10.1.0.1	port1	110	OSPF
10.2.0.0/24	0.0.0.0	loopback NGFW1	0	Connected
100.64.1.0/24	0.0.0.0	port1	0	Connected
100.64.2.0/24	0.0.0.0	port1	0	Connected
172.16.1.0/24		H2S_0	0	Connected
172.16.1.1/32		H2S_0	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

5. Return to the Spoke-1 GUI, and then click **Dashboard > Network > Routing**.
The routing table should look similar to the following example:

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	100.64.3.254	port1	10	Static
10.1.0.0/24		H2S_0	200	IBGP
10.1.1.0/24	0.0.0.0	port3	0	Connected
10.1.2.0/24		H2S_0	200	BGP
100.64.3.0/24	0.0.0.0	port1	0	Connected
100.64.4.0/24	0.0.0.0	port2	0	Connected
172.16.1.0/24		H2S_0	5	Static
172.16.1.1/32		H2S_0	5	Static
172.16.1.2/32		H2S_0	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

6. Return to the Spoke-2 GUI, and then click **Dashboard > Network > Routing**.

The routing table should look similar to the following example:

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	100.64.3.254	port1	10	Static
10.1.0.0/24		H2S_0	200	BGP
10.1.1.0/24		H2S_0	200	IBGP
10.1.2.0/24	0.0.0.0	port3	0	Connected
100.64.3.0/24	0.0.0.0	port1	0	Connected
172.16.1.0/24		H2S_0	5	Static
172.16.1.1/32		H2S_0	5	Static
172.16.1.2/32		H2S_0	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

Bring Up the On-Demand Tunnel

You will bring up the on-demand tunnel between Spoke-1 and Spoke-2 by generating traffic.

To bring up the on-demand tunnel

- Return to Spoke-2 CLI, and then enter the following command:
`diagnose sniffer packet any 'icmp' 4`
- Return to the Spoke-1 CLI, and then enter the following commands:
`execute ping-options source 10.1.1.254`
`execute ping 10.1.0.1`
These commands ping ISFW from Spoke-1.
- Enter the following ping to trigger the on-demand tunnel:
`execute ping 10.1.2.254`
- Return to the Spoke-2 CLI.

The output should look similar to the following output:

```
H2S_0 in 10.1.1.254 -> 10.1.2.254: icmp: echo request
H2S_0 out 10.1.2.254 -> 10.1.1.254: icmp: echo reply
H2S_0_0 in 10.1.1.254 -> 10.1.2.254: icmp: echo request
H2S_0_0 out 10.1.2.254 -> 10.1.1.254: icmp: echo reply
```

Stop and think!

Why is Spoke-2 receiving the echo request directly through the H2S_0 tunnel and then the H2S_0_0 tunnel?

Before ADVPN creates a shortcut between the two spokes, the traffic travels through the hub, meaning the H2S_0 tunnel. When you bring the the shortcut up, the icmp request is then transferred directly through the automatic-discovery VPN interface H2S_0_0.

- The output should look similar to the following example:

The spoke-to-spoke traffic flows through the shortcut.

Fortinet Vouchers & Dumps are Available on [Brave-Dumps.com](https://bravedumps.com)



This table displays a list of IPsec VPN tunnels. It provides other information, including the status of the ADVPNs H2S_0_0 for Spoke-1 and Spoke-2.

DO NOT REPRINT
© FORTINET

Brave-Dumps.com



FORTINET®



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© 2023 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