

Index: 1.0

Use Case: Introduction

Objective Title: Introduction

Points: 0

Objective Section

Objective Text:



Welcome

to the

Constructing a Secure SD-WAN Architecture Lab

In this Fast Track, you implement SD-WAN via FortiManager to remotely setup IPSEC VPN tunnels between headquarter's datacenter and two branch offices. You then setup SD-WAN on the two branch FortiGate devices at the same time.

Index: 1.0 (a)

Use Case: Introduction

Objective Title: Topology

Points: 0

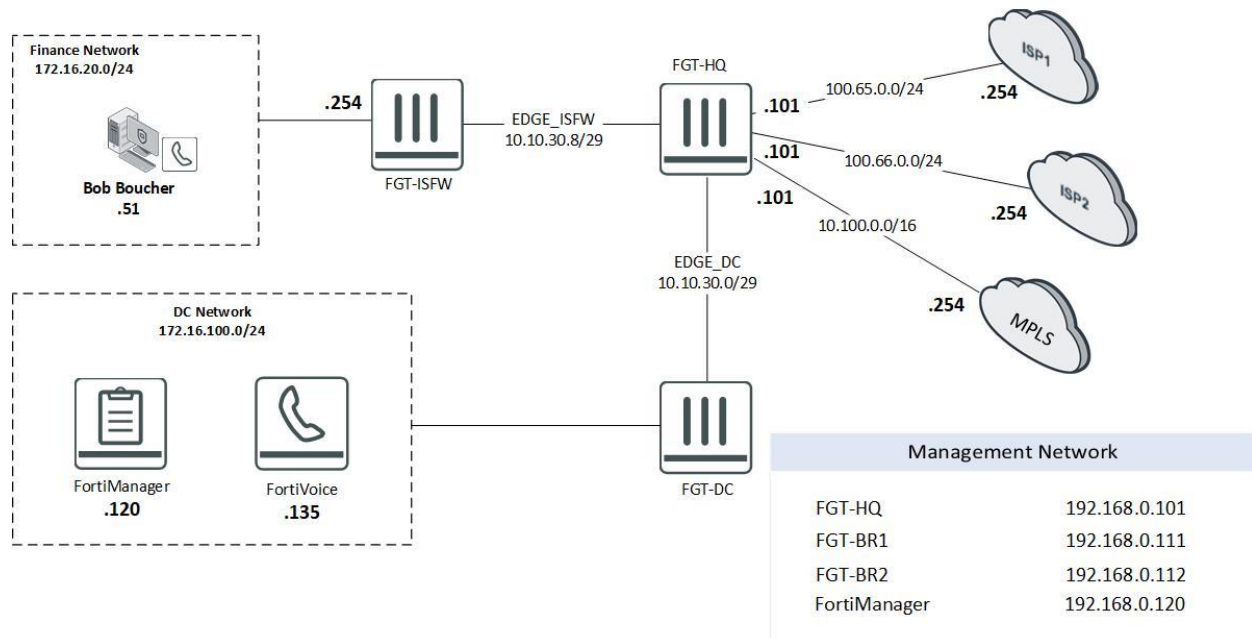
----- **Objective Section** -----

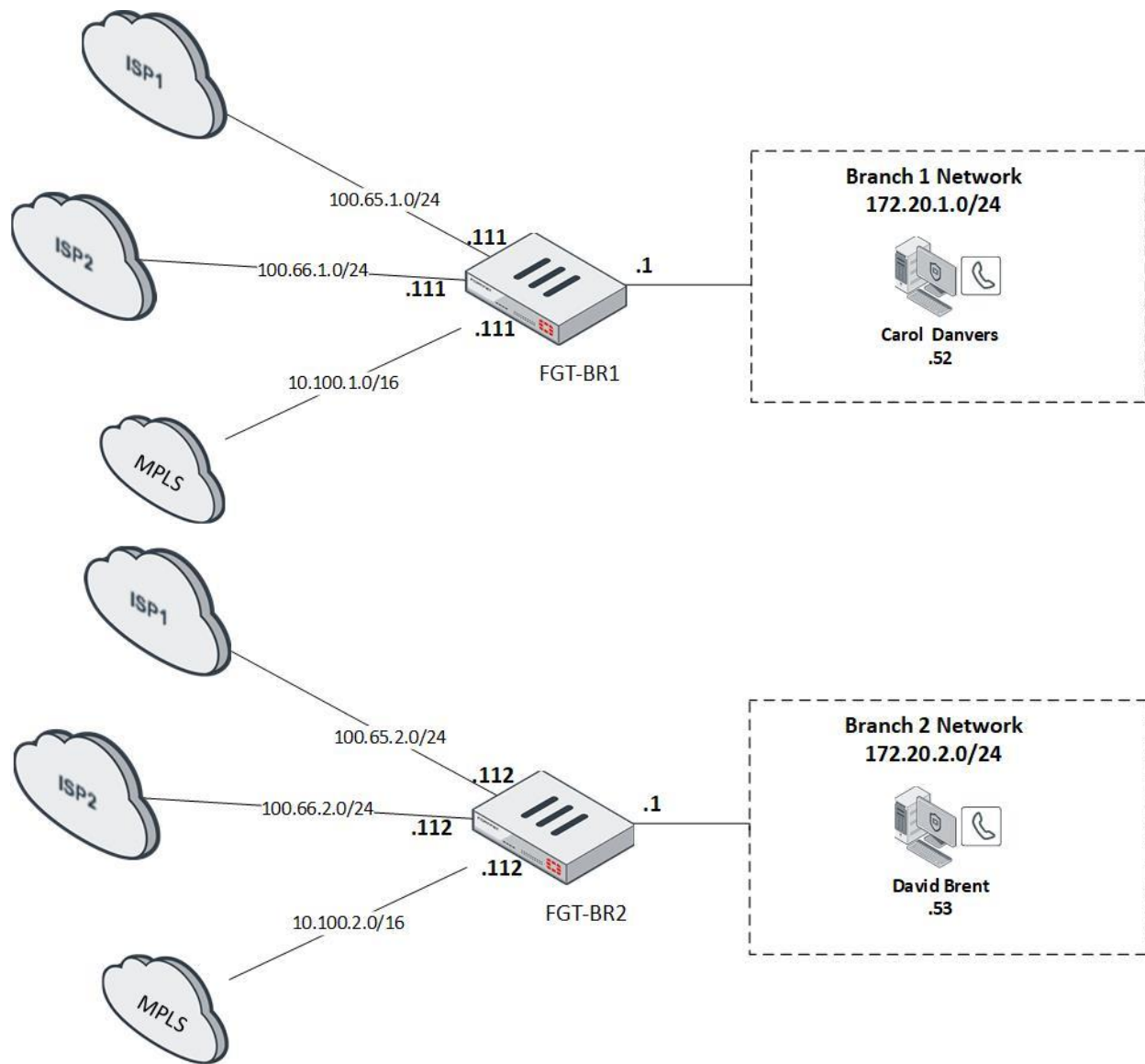
Objective Text:

Network Topology

The lab environment represents a fictional company, AcmeCorp. It has a headquarters (HQ) data center and two branch offices (Branch 1 and Branch 2). Previously, AcmeCorp backhauled all the internet traffic from the branch offices to HQ for processing. Now, due to the use of cloud-based solutions increasing and leased lines becoming more expensive, AcmeCorp is deploying FortiGate devices at the branch offices to allow direct connectivity to the internet, as well as using internet service provider (ISP) links to augment the multiprotocol label switching (MPLS) leased line to HQ.

A FortiManager and a FortiVoice appliance are installed in the HQ Data Center. The Fortifone software is also installed on all of the workstations.





Index: 1.0 (b)

Use Case: Introduction

Objective Title: Agenda

Points: 0

----- **Objective Section** -----

Objective Text:

Agenda

| | Topic | Time |
|--------|-------------------------------------|------------|
| Lab 1: | Introduction – Topology and Agenda | 2 Minutes |
| Lab 2: | Configuring SD-WAN via FortiManager | 30 Minutes |

Index: 2.0

Use Case: Configure SD-WAN via FortiManager

Objective Title: Configure SD-WAN via FortiManager

Points: 0

----- **Objective Section** -----

Objective Text:

Configure SD-WAN via FortiManager

Currently, AcmeCorp backhauls all the internet traffic from the branch offices to HQ for processing. They want to deploy FortiGate devices at the branch offices to allow direct connectivity to the internet. This will not only offload much of the traffic off of the multiprotocol label switching (MPLS) leased line, but the internet service provider (ISP) link will also act as a backup for the MPLS link.

In this exercise, you use FortiManager to remotely configure SD-WAN between the branch offices and HQ. You will also create an SD-WAN zone to control local internet breakout.

Index: 2.0 (a)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Setting up IPsec VPN

Points: 10

----- Objective Section -----

Objective Text:

Setting up IPsec VPN

Background

AcmeCorp is using FortiManager to centrally provision and manage its devices. At the headquarters (HQ) in Sunnyvale, AcmeCorp has a core FortiGate (**FGT-HQ**). There are currently two FortiGate devices that are operational but not fully configured at branch offices in Ottawa and New York (**FGT-BR1** and **FGT-BR2**). AcmeCorp deployed FortiGate devices at the branches to allow the use of the ISP link to augment their MPLS leased line to HQ.

As it will be using the internet as part of its connections between HQ and the branches, they will be implementing VPNs. As such, AcmeCorp needs to add an IPsec VPN over its internet link to HQ from the Branches. FortiManager allows centralized management of VPNs, which includes configuring the VPNs as well as monitoring the VPNs.

Task

For this objective, we will be working on the FortiManager. From the Lab Activity tab, click **FortiManager** in the side bar lab menu, then select HTTPS to connect to the **FortiManager**.

Log in using the following credentials:

Username: admin **Password:** Fortinet1!

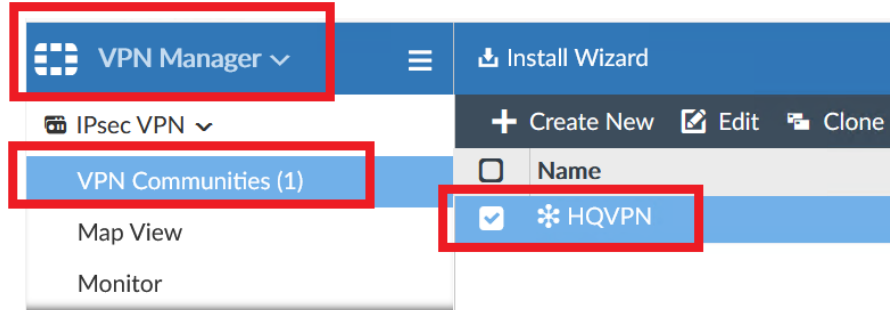
A VPN community (**HQVPN**) is already configured. To view this community on the FortiManager, click **VPN Manager > IPsec VPN** and select **HQVPN**.

Your goal for this objective is to add the FortiGate devices (**FGT-HQ**, **FGT-BR1**, and **FGT-BR2**) to the community.

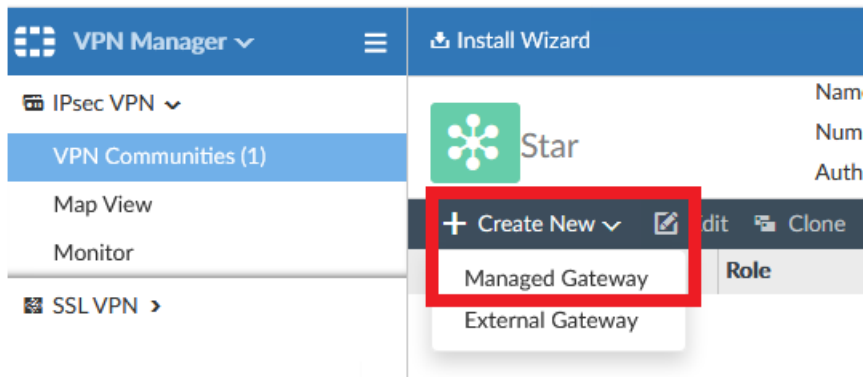
Add Devices to VPN Community

Use the following steps to add devices to the VPN community:

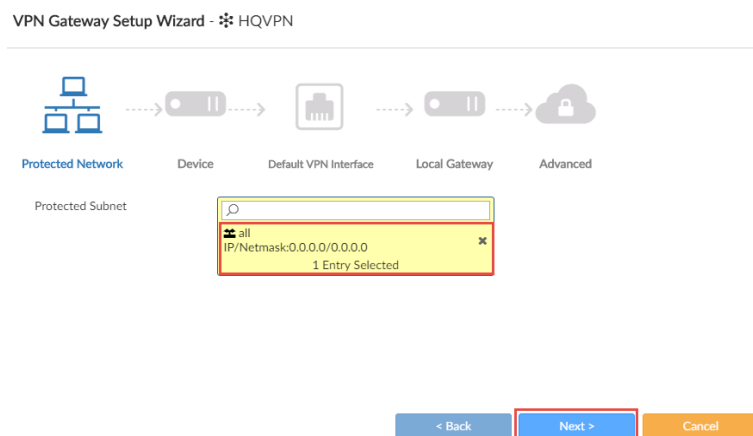
1. Click **VPN Manager > IPsec VPN**.
2. In the tree menu on the left, select **VPN Communities**.
3. Double click on **HQVPN**.



4. Click **Create New** and select **Managed Gateway** from the drop-down menu.



4. When the wizard opens, select **all** for the **Protected Subnet** and click **OK**.
5. Click **Next**.



6. For **Role**, select **Hub** and for **Device**, select **FGT-HQ**.

7. Click **Next**.

The screenshot shows the 'VPN Gateway Setup Wizard - HQVPN' at the 'Device' step. A progress bar at the top indicates the current step. Below the title, a diagram shows the flow: Protected Network (laptop icon) -> Device (router icon) -> Default VPN Interface (server icon) -> Local Gateway (router icon) -> Advanced (cloud icon). The 'Device' step is highlighted. Below the diagram, the 'Role' is set to 'Hub' (selected with a radio button) and 'Spoke' is unselected. The 'Device' dropdown menu shows 'FGT-HQ' with a green upward arrow. At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (active), and 'Cancel'.

8. For **Default VPN Interface**, select **ISP_1** (a dynamic interface that was previously configured).

9. Click **Next**.

The screenshot shows the 'VPN Gateway Setup Wizard - HQVPN' at the 'Default VPN Interface' step. The progress bar and diagram are the same as in step 7. The 'Default VPN Interface' dropdown menu is highlighted with a red box and shows 'ISP_1' with a green upward arrow. Below it, the 'Hub-to-Hub Interface' dropdown menu shows 'None' and is labeled '(Required for multiple Hubs)'. At the bottom, the 'Next >' button is highlighted with a red box, along with the '< Back' and 'Cancel' buttons.

10. Leave **Local Gateway** blank.

11. Click **Next**.

12. For **Advanced Options**, leave the default values and click **OK**.

The screenshot shows the 'VPN Gateway Setup Wizard - HQVPN' at the 'Advanced Options' step. The progress bar and diagram are the same as in step 7. The 'Local ID' field is empty. The 'Routing' section has 'Manual (via Device Manager)' selected with a radio button, and 'Automatic' is unselected. The 'Summary Network(s)' table has one row with 'Seq#' 1, 'Network' (empty dropdown), and 'Priority' 1. Below the table, there is a link 'Advanced Options >'. At the bottom, there are three buttons: '< Back' (disabled), 'OK' (active and highlighted with a red box), and 'Cancel'.

13. Create two additional managed gateway policies to add **FGT-BR1** and **FGT-BR2**. Set **Role** to **Spoke** and **Device** to the appropriate branch FortiGate. Use the same settings as the first managed gateway policy for the rest of the configuration.

14. When you have configured all three gateway policies, your screen should look like this:

VPN Manager

IPsec VPN

VPN Communities (1)

Map View

Monitor

SSL VPN

Install Wizard

Star

Name : HQVPN

Number of VPN : 3

Authentication: Pre-shared Key

Create New

Edit

Clone

Delete

Column Settings

| | Name | Role | Default VPN Interface | Protected Subn |
|--------------------------|-----------------|-------|-----------------------|----------------|
| <input type="checkbox"/> | ↑ FGT-HQ[root] | Hub | ISP_1 | all |
| <input type="checkbox"/> | ↑ FGT-BR1[root] | Spoke | ISP_1 | all |
| <input type="checkbox"/> | ↑ FGT-BR2[root] | Spoke | ISP_1 | all |

Index: 2.0 (b)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Installing the Managed Gateway Policies

Points: 10

----- Objective Section -----

Objective Text:

Installing the Managed Gateway Policies

Background

Now that you have the managed gateway policy packages created, you need to install them onto the appropriate FortiGate.

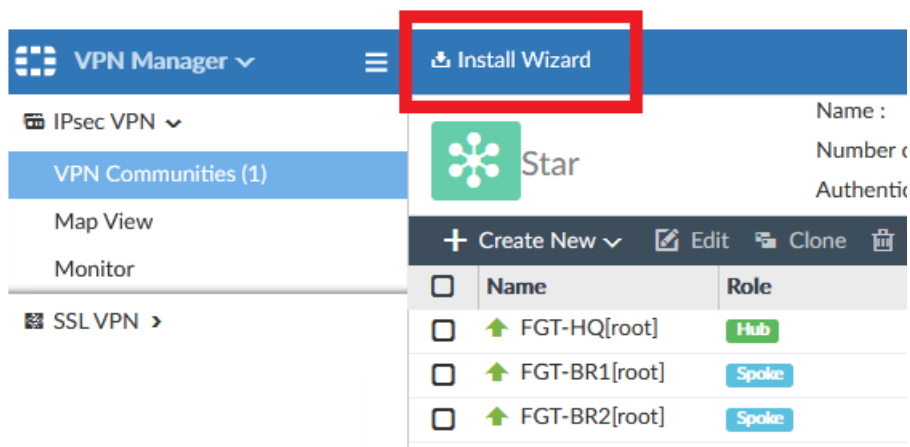
Task:

Your goal for this objective is to install the hub package on **FGT-HQ**, and the spoke packages on **FGT-BR1** and **FGT-BR2**. For all three devices, use the **Install Policy Package & Device Settings** option.

Push Gateway Policies

Use the following steps to install the managed gateway policies:

1. Click **Install Wizard**.



2. Click **Install Policy Package & Device Settings** and set **Policy Package** to **FG-HQ**. Click **Next**.

Install Wizard

Install Policy Package & Device Settings

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: **FGT-HQ**

Comment:
 0/127

☐ Create ADOM Revision

☐ Schedule Install

☐ **Install Device Settings (only)**

Next > **Cancel**

3. Verify that **FGT-HQ** is selected and click **Next**.

Install Wizard - Policy Package and Device Setting (FGT-HQ)

Please select one or more devices to install (ⓘ Use checkbox or Ctrl or Shift key for multiple selections)

| <input checked="" type="checkbox"/> | ▲ Device Name | IP Address | Platform |
|-------------------------------------|---------------|---------------|----------------|
| <input checked="" type="checkbox"/> | ● FGT-HQ | 192.168.0.101 | FortiGate-VM64 |

< Back **Next >** **Cancel**

4. After **Installation Preparation** completes, click **Install**.

Install Wizard - Policy Package (FGT-HQ)

Installation Preparation **Total: 3/3**, ✔ Success: 3, ⚠ Warning: 0, ✖ Error: 0 ⓘ

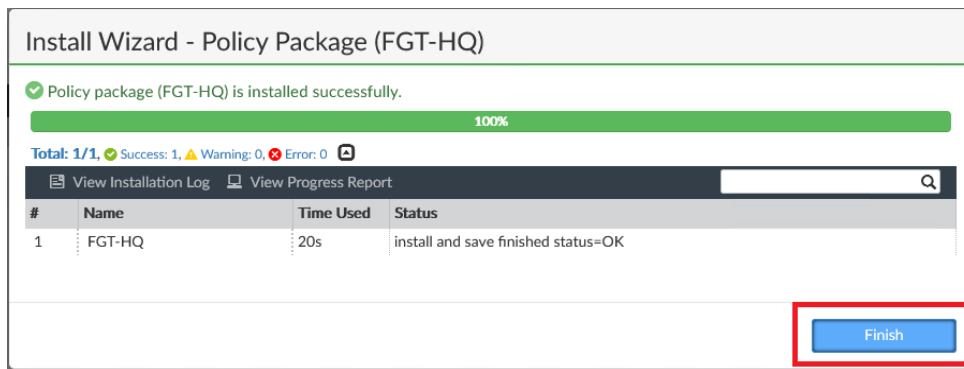
- ✔ Interface Validation
- ✔ Policy and Object Validation
- ✔ Ready to Install

Install Preview **Policy Package Diff**

| <input type="checkbox"/> | Device Name | Status | Action |
|-------------------------------------|--------------|-----------------|--------|
| <input checked="" type="checkbox"/> | FGT-HQ[root] | ● Connection Up | |

Install **Cancel**

5. After the installation completes, click **Finish**.



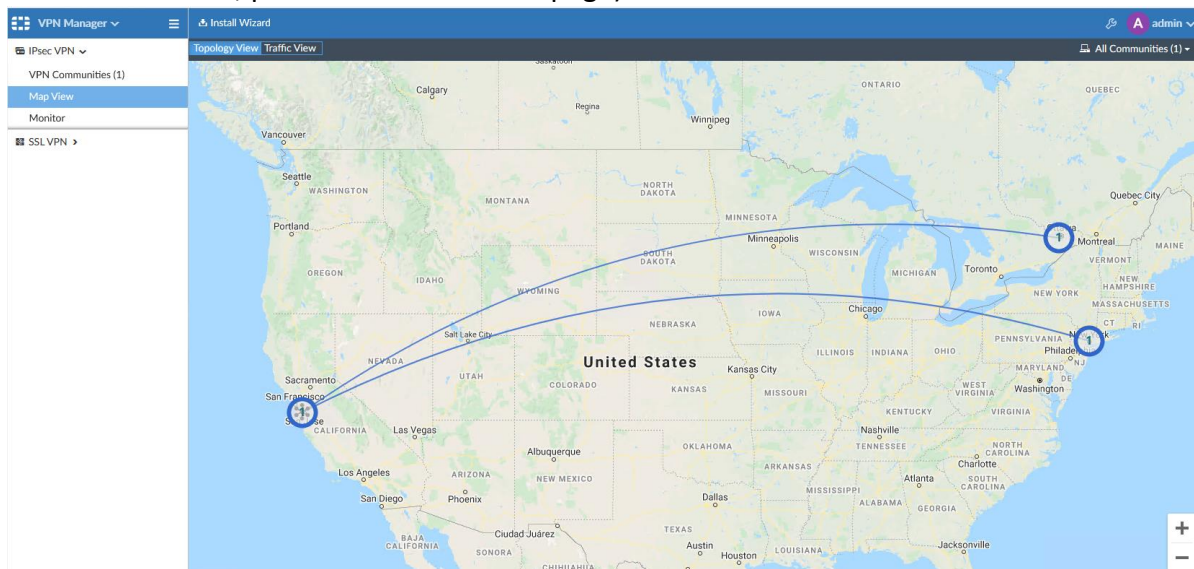
6. Use the installation wizard again to install the **FG-Branch** policy on **FGT-BR1** and **FGT-BR2**.

Monitor View

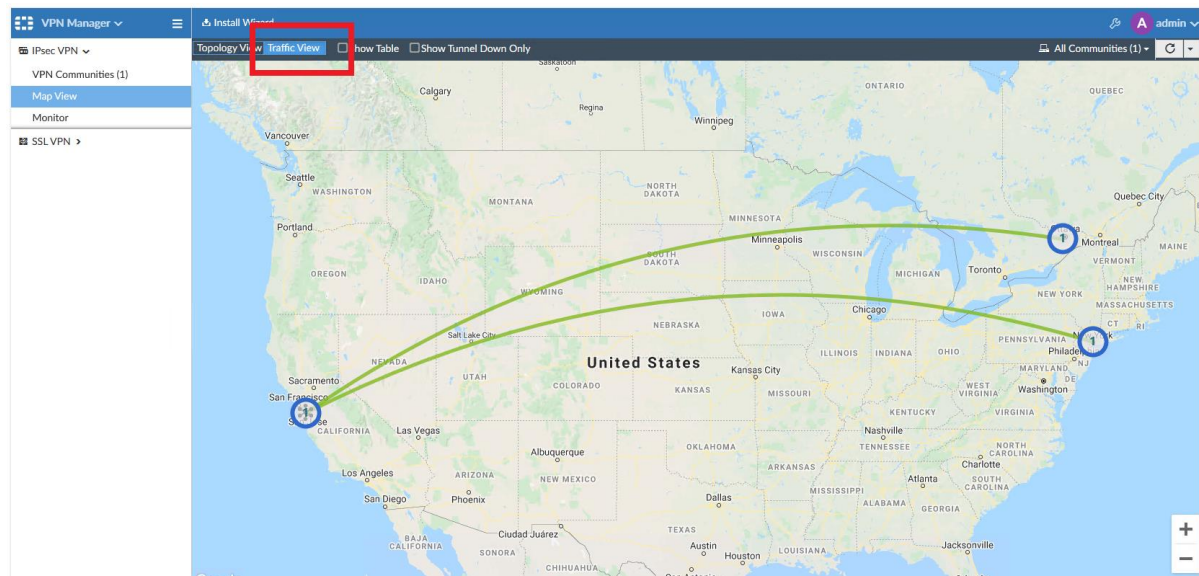
1. Once you have installed the policy, click **VPN Manager > Monitor**. You can see that the tunnels are all up. Note that it may take a moment for the tunnels to come up.

| | Status | Device | P1 Name | Type | Remote Gateway |
|--------------------------|--------|---------------|---------|-----------|----------------|
| <input type="checkbox"/> | Up | FGT-BR1[root] | HQVPN_1 | automatic | 100.65.0.101 |
| <input type="checkbox"/> | Up | FGT-BR2[root] | HQVPN_1 | automatic | 100.65.0.101 |
| <input type="checkbox"/> | Up | FGT-HQ[root] | HQVPN_2 | automatic | 100.65.1.111 |
| <input type="checkbox"/> | Up | FGT-HQ[root] | HQVPN_3 | automatic | 100.65.2.112 |

2. Click **Map View** to show the tunnels on a world map (if the map does not appear after about 30 seconds, press F5 to refresh the page).



2. Click **Traffic View** to see network traffic flowing between the protected subnets.



Index: 2.0 (c)

Use Case: Configure SD-WAN via FortiManager

Objective Title: VPN Tunnel Endpoints

Points: 10

----- Objective Section -----

Objective Text:

VPN Tunnel Endpoints

Background

To complete the IPsec VPN configuration, you need to configure the tunnel endpoint addresses (you can find them in the interface pages from the devices in **Device Manager > Device & Groups**).

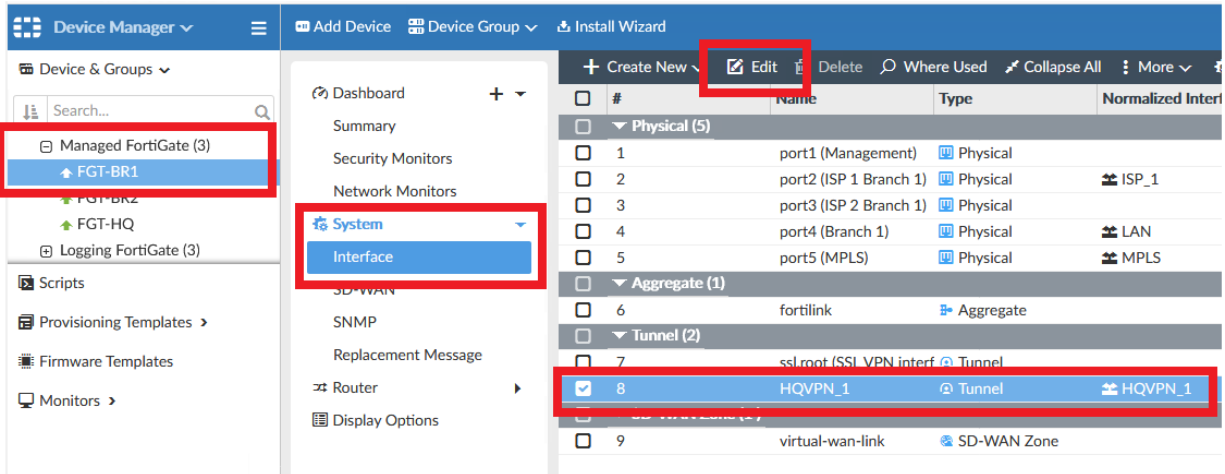
Task

Your goal for this objective is to edit the IPsec tunnel endpoints

Set Tunnel Endpoints

Use the following steps to set the tunnel endpoint addresses:

1. Click **Device Manager > Device & Groups**.
2. Under **Managed FortiGate** in the left hand pane, click **FGT-BR1**.
3. Expand the **System** drop-down menu and select **Interface**.
4. Select **HQVPN_1** and click **Edit**.



- In the **Address** section, set **IP/Network** to 10.10.1.2/32 and **Remote IP** to 10.10.1.1/32.

Edit Interface

Interface Name: HQVPN_1

Alias Name:

Type: Tunnel

Interface: port2

VRF ID: 0

Role: Undefined

Address

Addressing Mode: Manual

IP/Netmask: 10.10.1.2/255.255.255.255

Remote IP: 10.10.1.1/255.255.255.255

DHCPv6 Prefix Delegation: OFF

Shaping Profile: OFF

- Click **OK**.
- Under **Managed FortiGate**, click **FGT-BR2**.
- Edit **HQVPN_1**.
- In the **Address** section, set **IP/Network** to 10.10.2.2/32 and **Remote IP** to 10.10.2.1/32.

| Edit Interface | |
|--------------------------|------------------------------|
| Interface Name | HQVPN_1 |
| Alias Name | |
| Type | Tunnel |
| Interface | port2 |
| VRF ID ⓘ | 0 |
| Role | Undefined |
| Address | |
| Addressing Mode | Manual |
| IP/Netmask | 10.10.2.2/255.255.255.255 |
| Remote IP | 10.10.2.1/255.255.255.255 |
| DHCPv6 Prefix Delegation | <input type="checkbox"/> OFF |
| Shaping Profile | <input type="checkbox"/> OFF |

9. Click **OK**.
10. Under **Managed FortiGate**, click **FGT-HQ**.
11. Edit **HQVPN_2**.
12. In the **Address** section, set **IP/Network** to 10.10.1.1/32 and **Remote IP** to 10.10.1.2/32.

| Edit Interface | |
|--------------------------|------------------------------|
| Interface Name | HQVPN_2 |
| Alias Name | |
| Type | Tunnel |
| Interface | port6 |
| VRF ID ⓘ | 0 |
| Role | Undefined |
| Address | |
| Addressing Mode | Manual |
| IP/Netmask | 10.10.1.1/255.255.255.255 |
| Remote IP | 10.10.1.2/255.255.255.255 |
| DHCPv6 Prefix Delegation | <input type="checkbox"/> OFF |
| Shaping Profile | <input type="checkbox"/> OFF |

13. Click **OK**.
14. Edit **HQVPN_3**.
15. In the **Address** section, set **IP/Network** to 10.10.2.1/32 and **Remote IP** to 10.10.2.2/32.

Edit Interface

Interface Name: HQVPN_3

Alias Name:

Type: Tunnel

Interface: port6

VRF ID: 0

Role: Undefined

Address

Addressing Mode: Manual

IP/Netmask: 10.10.2.1/255.255.255.255

Remote IP: 10.10.2.2/255.255.255.255

DHCPv6 Prefix Delegation: OFF

Shaping Profile: OFF

16. Click **OK**.

Push Configurations

1. To push the configuration on to the FortiGate devices, click on **Install Wizard**.
2. Select **Install Device Settings (only)**
3. Click **Next**.
4. Confirm that all three devices are selected
5. Click **Next**.

Install Wizard - Device Settings only

Please select one or more devices to install (Use checkbox or Ctrl or Shift key for multiple selections) Search...

| <input checked="" type="checkbox"/> | Device Name | IP Address | Platform |
|-------------------------------------|-------------|---------------|----------------|
| <input checked="" type="checkbox"/> | FGT-BR1 | 192.168.0.111 | FortiGate-VM64 |
| <input checked="" type="checkbox"/> | FGT-BR2 | 192.168.0.112 | FortiGate-VM64 |
| <input checked="" type="checkbox"/> | FGT-HQ | 192.168.0.101 | FortiGate-VM64 |

< Back Next > Cancel

6. After the **Installation Preparation** completes, click **Install**

Install Wizard - Device Settings

Only successfully validated device may be installed. Please confirm and click "Install" button to continue.

Install Preview

| <input type="checkbox"/> | Device Name | Status | Action |
|-------------------------------------|-------------|---------------|--------|
| <input checked="" type="checkbox"/> | FGT-BR1 | Connection Up | |
| <input checked="" type="checkbox"/> | FGT-BR2 | Connection Up | |
| <input checked="" type="checkbox"/> | FGT-HQ | Connection Up | |

Install Cancel

7. When the installation is complete, click **Finish**.

Install Wizard - Device Settings

✔ Device Settings is installed successfully.

100%

Total: 6/6, ✔ Success: 6, ⚠ Warning: 0, ❌ Error: 0

[View Installation Log](#) [View Progress Report](#)

| # | Name | Time Used | Status |
|---|---------------|-----------|-------------------------------------|
| 1 | FGT-BR1 | 18s | install and save finished status=OK |
| 2 | FGT-BR1[copy] | 23s | Installation to real device done |
| 3 | FGT-BR2 | 18s | install and save finished status=OK |
| 4 | FGT-BR2[copy] | 23s | Installation to real device done |
| 5 | FGT-HQ | 18s | install and save finished status=OK |
| 6 | FGT-HQ[copy] | 23s | Installation to real device done |

Finish

Index: 2.0 (d)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Creating an SD-WAN Template for FGT-BR1

Points: 10

----- Objective Section -----

Objective Text:

Creating an SD-WAN Template

Background

AcmeCorp wants to use both the MPLS leased line and the IPsec links you previously created to route traffic back to HQ when the branch offices need to utilize corporate resources.

Along with VPNs, you can also centrally manage SD-WAN from FortiManager.

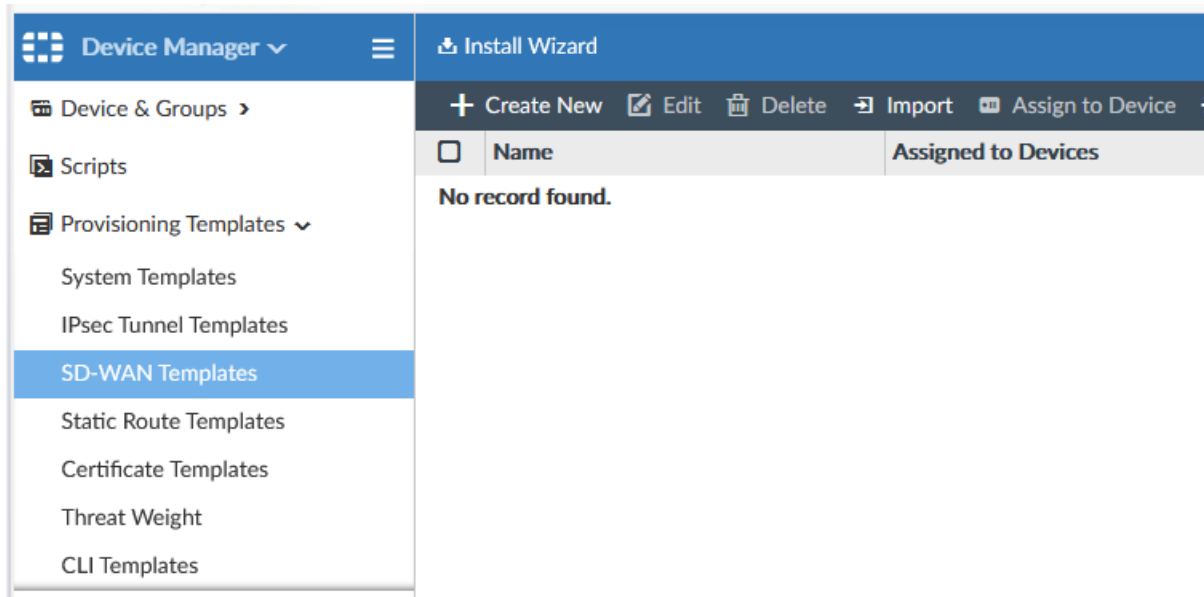
Task

Your goal for this objective is to set up SD-WAN by creating a new SD-WAN template.

SD-WAN Template

Use the following steps to create an SD-WAN template:

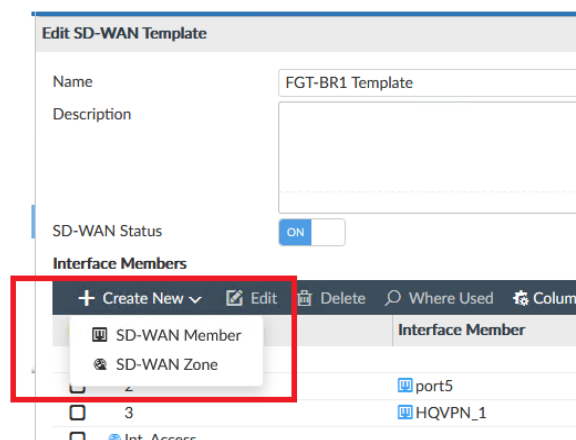
1. Expand the **Provisioning Templates** section.



2. Select **SD-WAN Templates** and click **Create New**.
3. Set **Name** as FGT-BR1 Template.

Interface Members

1. In the **Interface member** section, click **Create New > SD-WAN Member**.



2. Enter the following information:
 - Interface Member:** port2
 - Gateway IP:** 100.65.1.254
3. Leave the other values at default

Edit SD-WAN Interface Member

| | |
|------------------|--|
| Sequence Number | 1 |
| Interface Member | port2 |
| SD-WAN Zone | Internet_Access |
| Gateway IP | 100.65.1.254 |
| Cost | 0 |
| Status | <input checked="" type="checkbox"/> ON |

OK Cancel

4. click **Create New > SD-WAN Member** again.

5. Enter the following information:

Interface Member: port5

Gateway IP: 10.100.0.101

Edit SD-WAN Interface Member

| | |
|------------------|--|
| Sequence Number | 2 |
| Interface Member | port5 |
| SD-WAN Zone | virtual-wan-link |
| Gateway IP | 10.100.0.101 |
| Cost | 0 |
| Status | <input checked="" type="checkbox"/> ON |

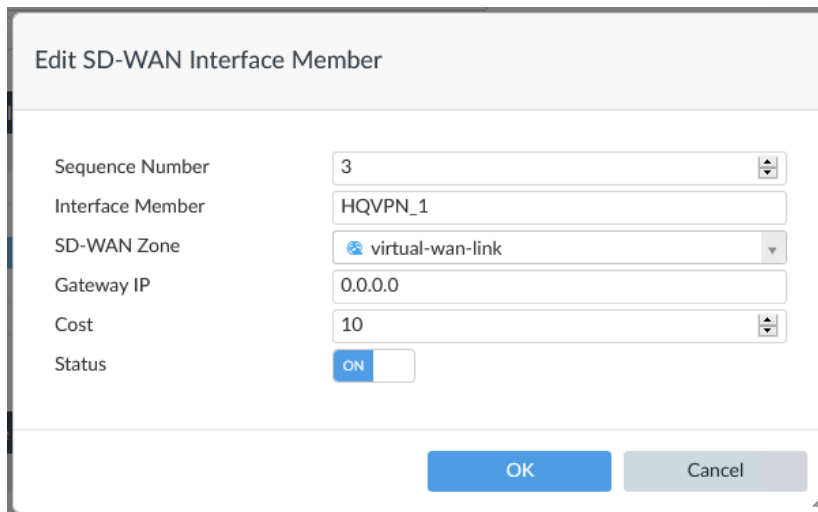
OK Cancel

6. click **Create New > SD-WAN Member** one more time.

7. Enter the following information:

Interface Member: HQVPN_1

Cost: 10



Edit SD-WAN Interface Member

| | |
|------------------|--|
| Sequence Number | 3 |
| Interface Member | HQVPN_1 |
| SD-WAN Zone | virtual-wan-link |
| Gateway IP | 0.0.0.0 |
| Cost | 10 |
| Status | <input checked="" type="checkbox"/> ON |

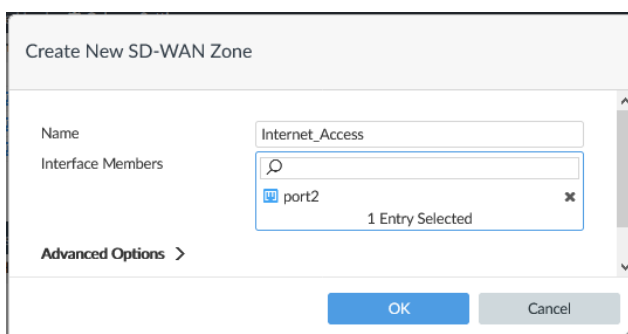
OK Cancel

Note: the cost values are used by the SD-WAN rules later.

SD-WAN Zone for Internet Breakout

SD-WAN zones are a way of logically grouping the SD-WAN interface members. They can then be used in firewall policies to allow for more granular control.

1. Still in the **Interface Member** section, click **Create New > SD-WAN Zone**.
2. Set **Name** as `Internet_Access`.
3. Select **port2** as the **Interface member**.



Create New SD-WAN Zone

| | |
|--------------------|---|
| Name | Internet_Access |
| Interface Members | <input type="text"/> <div> <input checked="" type="checkbox"/> port2 </div> <div>1 Entry Selected</div> |
| Advanced Options > | |

OK Cancel

8. Click **OK**

SD-WAN Status

ON

Interface Members

| + Create New ▾ Edit Delete Where Used Column Settings ▾ | | | | | |
|---|------------------|------------------|----------|--------------|------|
| <input type="checkbox"/> | ID | Interface Member | Status | Gateway | Cost |
| <input type="checkbox"/> | virtual-wan-link | | | | |
| <input type="checkbox"/> | 2 | port5 | ✓ Enable | 10.100.0.101 | 0 |
| <input type="checkbox"/> | 3 | HQVPN_1 | ✓ Enable | 0.0.0.0 | 10 |
| <input type="checkbox"/> | Internet_Access | | | | |
| <input type="checkbox"/> | 1 | port2 | ✓ Enable | 100.65.1.254 | 0 |

Performance SLA

1. In the **Performance SLA** section, click **Create New**.
2. Set **Name** to HQ_SLA.
3. Leave the **Detect Protocol** set to **PING**.
4. Click the plus sign to the right of the **HealthCheck-Server** field.
5. Enter **10.10.30.2**
5. Leave **Participants** set to **Specify**, and add both **port5** and **HQVPN_1** as members.
6. In the SLA section, click **Create New**.
7. Enter 10 for each threshold.
8. Click **OK** to save the SLA.

Create New SLA

Jitter Threshold ☒ 10 Milliseconds

Latency Threshold ☒ 10 Milliseconds

Packet Loss Threshold ☒ 10 %

OK

Cancel

9. Click **OK** again to save all settings.

Create New Performance SLA

Name: HQ_SLA

IP Version: IPv4

Detect Protocol: Ping

Health-Check Server: 10.10.30.2

Participants: All SD-WAN Members **Specify**

port5
HQVPN_1
2 Entries Selected

Enable Probe Packets: ☒

SLA

| ID | Latency Threshold (Millisecond) | Jitter Threshold (Milliseconds) | Packet Loss Threshold (%) |
|----|---------------------------------|---------------------------------|---------------------------|
| 1 | 10 | 10 | 10 |

Link Status

Interval: 500 Milliseconds

Failure Before Inactive: 5 (max 3600)

Restore Link After: 5 (max 3600)

Action When Inactive

Update Static Route: ☒

Cascade Interfaces: ☒

Advanced Options

OK Cancel

SD-WAN Rule for HQ Traffic

This rule will guide all traffic intended for the main office (FG-HQ) through the MPLS link, while using the VPN for backup in the event the MPLS link goes down.

1. Click **Create New** in the **SD-WAN Rules** section.
2. Set **Name** as HQ_Rule_1.
3. Set **Source Address** to all.
4. Set **Destination Address** to HQ_Networks.
5. Set **Outgoing Interface Strategy** to **Lowest Cost (SLA)**.
6. For **Interface Preference**, select port5 and HQVPN_1.
7. Set **Required SLA Target** to HQ_SLA#1.

Create New SD-WAN Rule

Name: HQ_Rule_1

IP Version: IPv4

Source

Source Address: all
IP/Netmask: 0.0.0.0/0.0.0.0
1 Entry Selected

Users: Click here to select

User Groups: Click here to select

Destination

Address: HQ Networks
Group Members (3): DC_Network, Finance_Network, Sales_Network
1 Entry Selected

Route Tag: 0

Protocol: TCP UDP **ANY** Specify 0

Type of Service: 0x00 Bit Mask 0x00

Outgoing Interfaces

Strategy: Manual Best Quality **Lowest Cost (SLA)** Maximize Bandwidth (SLA)

Interface Preference: port5 HQVPN_1
2 Entries Selected

Required SLA Target: HQ SLA#1
Ping: 10.10.30.2; Latency: 10ms, Jitter: 10ms, Packet Loss: 10%
1 Entry Selected

Advanced Options >

OK Cancel

8. Click **OK** to complete the rule.

SD-WAN Rule for Internet Traffic

This rule will direct any traffic not intended for HQ to the ISP_1 interface, allowing direct internet access.

1. Click **Create New** again in the **SD-WAN Rules** section.
2. Set **Name** as **Internet**.
3. Set **Source Address** and **Destination Address** to **all**.
Note: You can create rules for specific applications or internet services (for example, Microsoft Office 365, Salesforce, Microsoft Teams, Amazon, or Dropbox) but for the
4. Set **Outgoing Interface Strategy** to **Manual**.
5. For **Interface Preference**, select port2.

Create New SD-WAN Rule

Name:

IP Version:

Source

Source Address:
IP/Netmask: 0.0.0.0/0.0.0.0
1 Entry Selected

Users:

User Groups:

Destination

Address:
IP/Netmask: 0.0.0.0/0.0.0.0
1 Entry Selected

Route Tag:

Protocol: Specify:

Type of Service: Bit Mask:

Outgoing Interfaces

Strategy:

Interface Preference:
1 Entry Selected

Advanced Options >

6. Click **OK**.

7. Click **OK** again to complete the SD-WAN template.

Edit SD-WAN Template

Name:

Description:

SD-WAN Status: ☒ ON

Interface Members

| ID | Interface Member | Status | Gateway | Cost |
|------------------|------------------|--------|---------|------|
| virtual-wan-link | | | | |
| 2 | port5 | Enable | 0.0.0.0 | 0 |
| 3 | HQVPN_1 | Enable | 0.0.0.0 | 0 |
| Int_Access | | | | |
| 1 | port2 | Enable | 0.0.0.0 | 0 |

Performance SLA

| Name | Health-Check Server | Detect Protocol | Failure Threshold | Recovery Threshold |
|-----------------------|---------------------|-----------------|-------------------|--------------------|
| Default_AWS | aws.amazon.com | HTTP | 5 | 10 |
| Default_DNS | (System DNS) | DNS | 5 | 10 |
| Default_FortiGuard | fortiguard.com | HTTP | 5 | 10 |
| Default_Gmail | gmail.com | Ping | 5 | 10 |
| Default_Google Search | www.google.com | HTTP | 5 | 10 |
| Default_Office_365 | www.office.com | HTTP | 5 | 10 |
| SLA1 | 10.10.30.2 | Ping | 5 | 5 |

SD-WAN Rules

| ID | Name | Source | Destination | Criteria | Members |
|----|--------|--------|-------------|-----------|---------------|
| 1 | R1 | all | HQ_Networks | SLA1#1 | port5 HQVPN_1 |
| 2 | R2 | all | all | Latency | port2 |
| | sd-wan | ALL | ALL | Source IP | ALL |

Index: 2.0 (e)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Cloning a Template

Points: 0

----- **Objective Section** -----

Objective Text:

Cloning a Template

Background

Now that you have a template for the FGT-BR1 device, you can easily create other templates based on this one. In this exercise, you will create a template for FGT-BR2, based on this template.

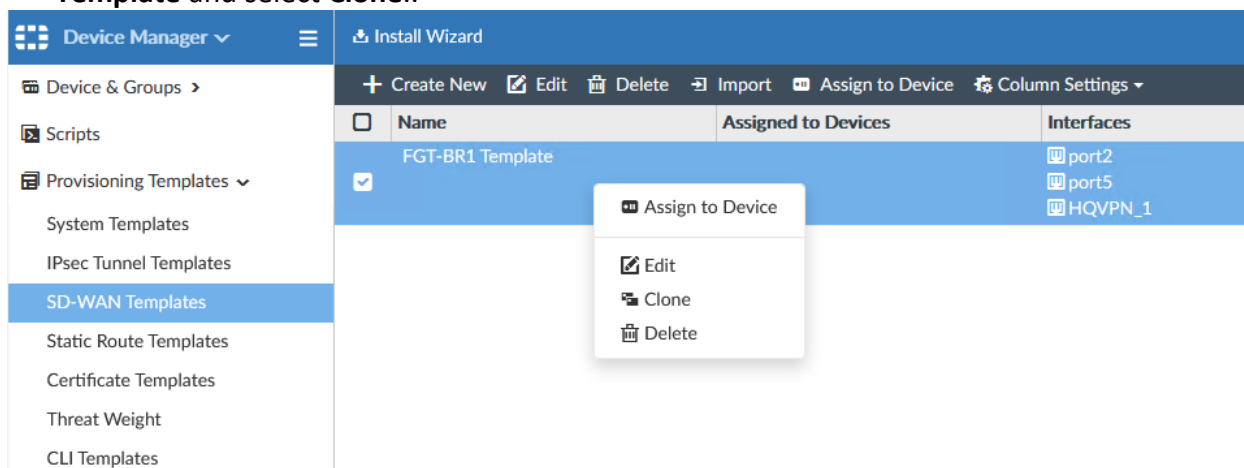
Task

Your goal for this objective is to clone the FGT-BR1 SD-WAN Template for FGT-BR2.

Clone an SD-WAN Template

Use the following steps to clone an SD-WAN template:

1. While still at **Provisioning Templates > SD-WAN Templates**, right-Click on **FGT-BR1 Template** and select **Clone..**



2. Change the name to **FGT-BR2 Template**.

3. Select and edit the Interface Member for port2
4. Change the Gateway IP address to 100.65.2.254

Edit SD-WAN Interface Member

Sequence Number

1

Interface Member

port2

SD-WAN Zone

Int_Access

Gateway IP

100.65.2.254

Cost

0

Status

ON

OK

Cancel

5. Click **OK**.

For the purposes of this lab, this is the only change that we will make to this template, but note that we could have made changes to any of the other sections (SLA, Rules, etc).

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

| + Create New Edit Delete Import Assign to Device Column Settings | | | |
|--|------------------|---------------------|--|
| | Name | Assigned to Devices | Interfaces |
| <input type="checkbox"/> | FGT-BR1 Template | | <input type="checkbox"/> port2 <input type="checkbox"/> port5 <input type="checkbox"/> HQVPN_1 |
| <input type="checkbox"/> | FGT-BR2 Template | | <input type="checkbox"/> port2 <input type="checkbox"/> port5 <input type="checkbox"/> HQVPN_1 |

Index: 2.0 (f)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Assign and Install the Template

Points: 10

----- Objective Section -----

Objective Text:

Assign and Install the Template

Background

Now that you have created the SD-WAN templates, you can assign the templates to the branch FortiGate devices and install them.

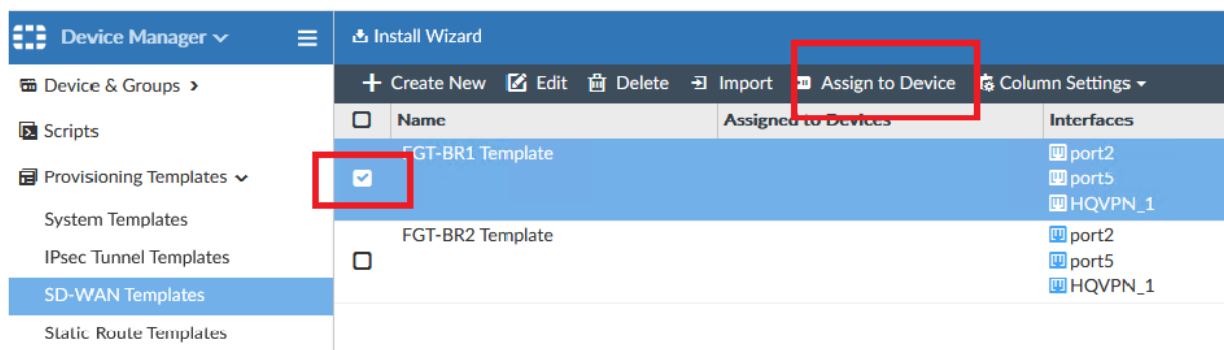
Task

Your goal for this objective is to assign the SD-WAN templates to the branch FortiGate devices and push the install.

Assign Devices to Template

Use the following steps to assign and install the SD-WAN template:

1. Select **FGT-BR1 Template** and click **Assigned Devices**.



2. Select **FGT-BR1** and move it to the **Selected Entries** column.

Assign to Device

SD-WAN Template FGT-BR1 Template

Available Entries (2)

- ☐ FGT-BR2 [root] (IP: 192.168.0.112, Platform: FortiGate-VM64)
- ☐ FGT-HQ [root] (IP: 192.168.0.101, Platform: FortiGate-VM64)

Selected Entries (1)

- ☐ FGT-BR1 [root] (IP: 192.168.0.111, Platform: FortiGate-VM64)

OK Cancel

- Click **OK**.
- Repeat the steps above, and assign FGT-BR2 to the FGT-BR2 Template.

| Install Wizard | | | |
|--|------------------|---------------------|--|
| + Create New Edit Delete Import Assign to Device Column Settings | | | |
| <input type="checkbox"/> | Name | Assigned to Devices | Interfaces |
| <input type="checkbox"/> | FGT-BR1 Template | ↑ FGT-BR1 [root] | <input type="checkbox"/> port2 <input type="checkbox"/> port5 <input type="checkbox"/> HQVPN_1 |
| <input type="checkbox"/> | FGT-BR2 Template | ↑ FGT-BR2 [root] | <input type="checkbox"/> port2 <input type="checkbox"/> port5 <input type="checkbox"/> HQVPN_1 |

Push the configurations to Devices

- Click **Install Wizard**.
- Select **Install Device Settings (only)** and click **Next**.

Install Wizard

☐ Install Policy Package & Device Settings
☒ **Install Device Settings (only)**

Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.

Comment

Next > Cancel

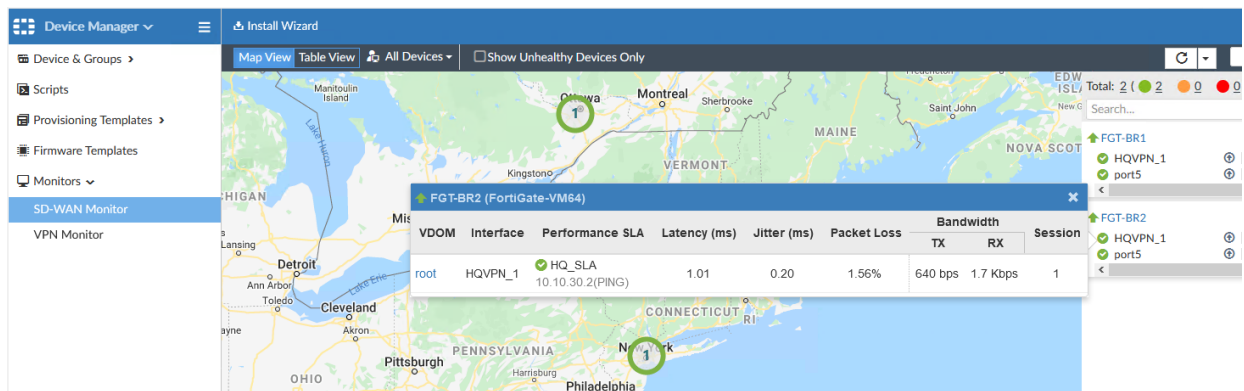
- Confirm that both **FGT-BR1** and **FGT-BR2** are selected and click **Next**.
- When prompted, click **Install**.

5. When the installation is finished, click **Finish**.

Monitor the SD-WAN

1. To monitor the SD-WAN, expand Monitors and select **SD-WAN Monitor**.
2. Click **Map View** (if the map does not appear after about 30 seconds, press **F5** to refresh the page).

This view displays SD-WAN enabled devices on Google Map with color-coded icons. You can view bandwidth usage on the right. If you hover over the green checkmark of an interface, you can view health performance statistics for each SD-WAN link member.



3. Click **Table View**. This view provides information on each SD-WAN link member, such as link status, applications performance, and bandwidth usage.

Index: 2.0 (g)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Edit Default Route

Points: 10

----- **Objective Section** -----

Objective Text:

Edit Default Route

Background

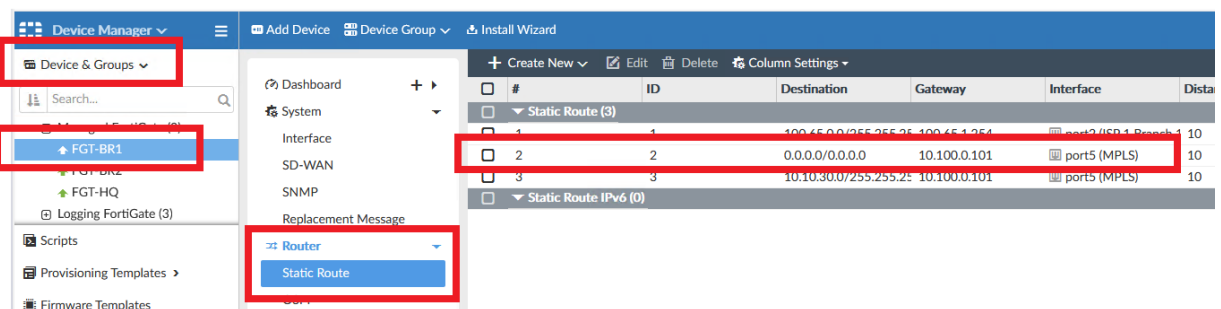
Now that you have the basic SD-WAN configurations done and installed on the devices, you still need to alter the default route to use the SD-WAN virtual interface on the two branch FortiGate devices.

Tasks

In this exercise, you edit the default route on the branch devices to use the SD-WAN virtual interface as the egress interface.

Edit the Default Route

1. Navigate to **Device Manager > Devices & Groups**.
2. Select **FGT-BR1** from the left hand pane.
3. Select **Static routes** from the **Router** drop down menu.



4. Select the default route [**Destination:** 0.0.0.0/0.0.0.0, **Gateway:**10.100.0.101 , **port5(MPLS)**] and click **Edit**.
5. Change **Device** option to **SD-WAN**.

Edit Static Route

Destination ⓘ **Subnet** Named Address Internet Service

0.0.0.0/0.0.0.0

Device SD-WAN

Administrative Distance 1

Status ON

Description

Advanced Options >

6. Click **OK**.

7. Select **FGT-BR2** and edit its default route to use **SD-WAN**.

Push Policies

1. Click **Install Wizard**.

2. Click **Install Policy Package & Device Settings** and set **Policy Package** to **FG-Branch**. Click **Next**.

Install Wizard

☒ **Install Policy Package & Device Settings**
Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package FG-Branch

Comment

☐ Create ADOM Revision

☐ Schedule Install

☐ Install Device Settings (only)

Next > Cancel

3. Confirm that both branch devices are selected and click **Next**.

Install Wizard - Policy Package and Device Setting (FG_Branch)

Please select one or more devices to install ⓘ Use checkbox or Ctrl or Shift key for multiple selections Search...

| Device Name | IP Address | Platform |
|---|---------------|----------------|
| <input checked="" type="checkbox"/> FGT-BR1 | 192.168.0.111 | FortiGate-VM64 |
| <input checked="" type="checkbox"/> FGT-BR2 | 192.168.0.112 | FortiGate-VM64 |

< Back Next > Cancel

4. After **Installation Preparation** completes, click **Install**.
5. After the installation completes, click **Finish**.

Index: 2.0 (h)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Examining the Configurations

Points: 0

----- Objective Section -----

Objective Text:

Examining the Configurations

Task

In this objective, you will have a look at the settings that FortiManager pushed out to the FortiGates.

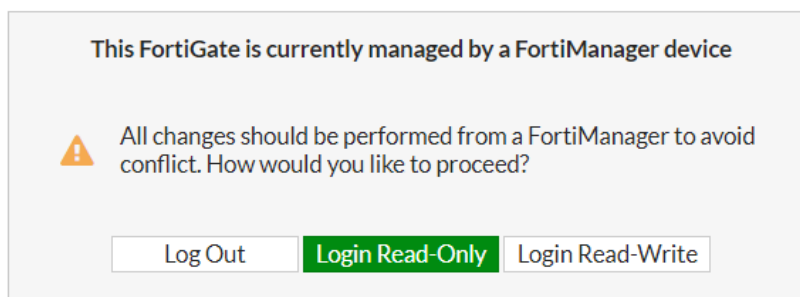
Verify configurations pushed to FGT-BR1

1. Return to Lab Activity tab, click on **FGT-BR1** on the sidebar menu, and select the **HTTPS** option.

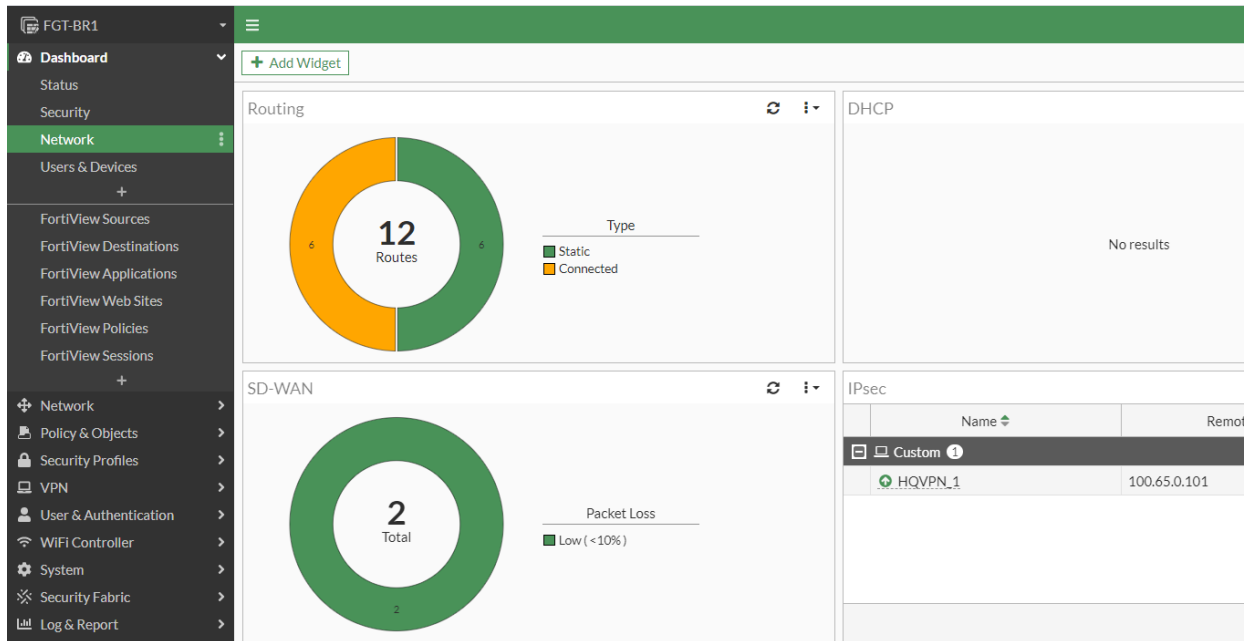
Username: admin

Password: Fortinet1!

2. You are presented with a warning that this FortiGate is managed by FortiManager. Select **Login Read-Only**.



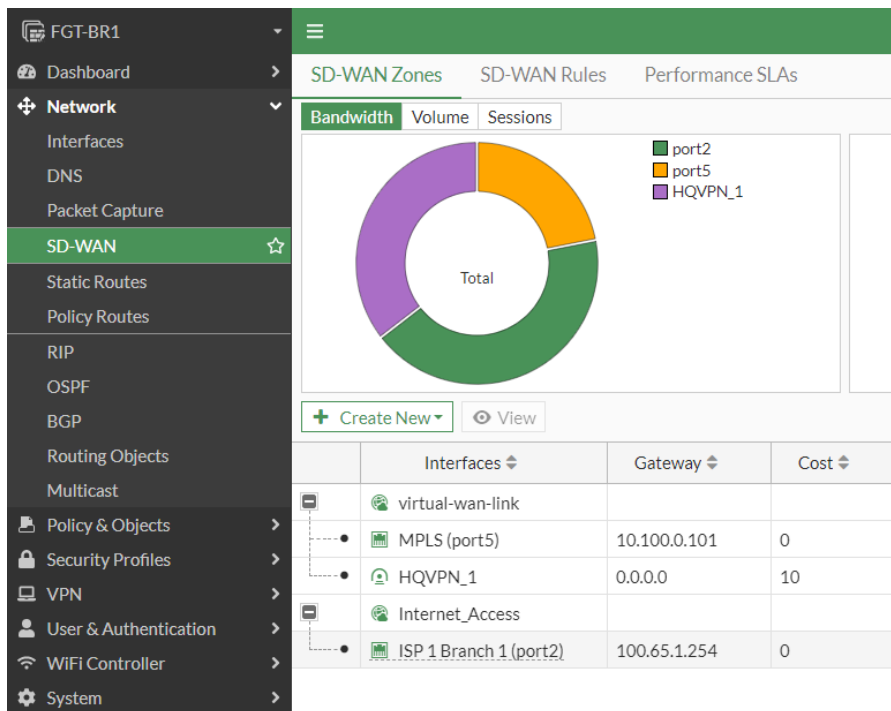
3. Click **Dashboard > Network**. Notice that the **IPsec** widget lists the **HQVPN_1** tunnel and there are 10 routes in the **Routing** widget.



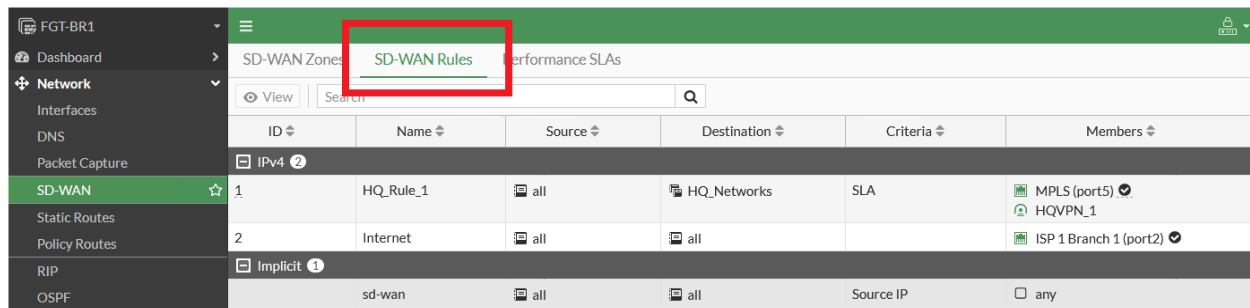
4. Click on the **Routing** widget to inspect the routes.

SD-WAN settings

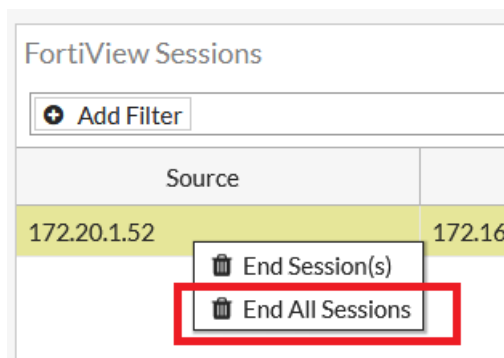
1. Click **Network** > **SD-WAN**.
2. Expand the zones to display the member interfaces.



3. Click the **SD-WAN Rules** tab



- Review the two rules that you created. The checkmark next to the interface member indicates which interface the rule is currently favoring to pass traffic through. In the above screenshot, any traffic destined to HQ uses the MPLS lines (with HQVPN_1 as backup) and all other traffic flows through the local internet breakout.
- Click **Dashboard > FortiView Sessions**.
- Right Click on any session, and select **End All Sessions**



- Click **OK**.

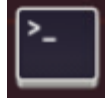
Generate traffic

- Return to the Lab Activity tab and click on **Bob** (in Finance), then select the **RDP** option to access Bob's workstation.



- Open FortiFone

3. Likewise, click on **Carol** (under the Branch 1 section) then select **RDP** to access her workstation.

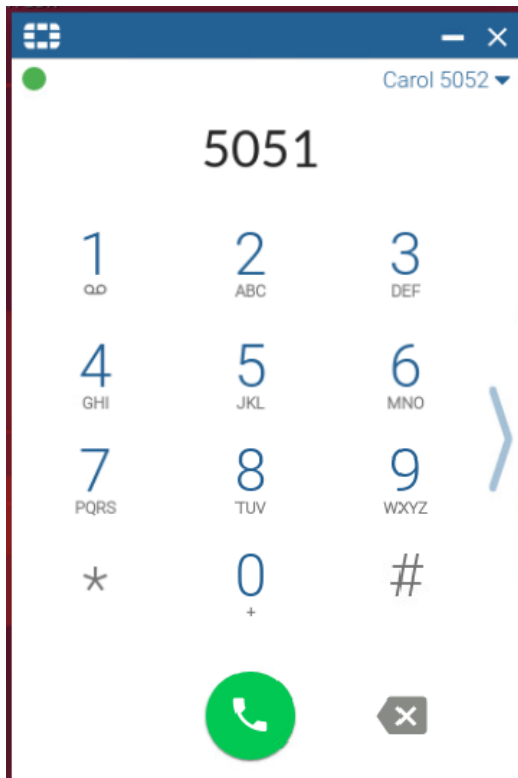


4. Open Terminal and ping 172.16.100.135.
5. After a few pings, press Ctrl C and then ping 8.8.8.8.

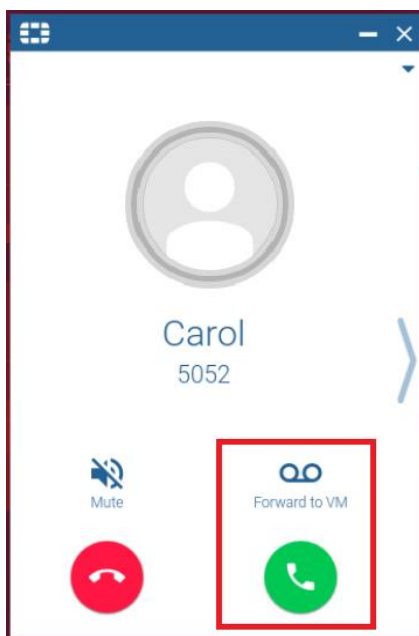
```
carol@ubuntu-desktop: ~  
carol@ubuntu-desktop:~$ ping 172.16.100.135  
PING 172.16.100.135 (172.16.100.135) 56(84) bytes of data.  
64 bytes from 172.16.100.135: icmp_seq=1 ttl=61 time=2.01 ms  
64 bytes from 172.16.100.135: icmp_seq=2 ttl=61 time=1.29 ms  
64 bytes from 172.16.100.135: icmp_seq=3 ttl=61 time=1.69 ms  
64 bytes from 172.16.100.135: icmp_seq=4 ttl=61 time=1.66 ms  
64 bytes from 172.16.100.135: icmp_seq=5 ttl=61 time=1.32 ms  
^C  
--- 172.16.100.135 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 1.293/1.594/2.010/0.265 ms  
carol@ubuntu-desktop:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=5.26 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=4.91 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=4.88 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=4.93 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=5.18 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=110 time=5.03 ms  
64 bytes from 8.8.8.8: icmp_seq=7 ttl=110 time=5.06 ms  
^C  
--- 8.8.8.8 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6009ms  
rtt min/avg/max/mdev = 4.881/5.035/5.263/0.133 ms
```



3. Open FortiFone
4. Dial 5051 and click the green phone button.



5. Return to the browser tab for Bob's workstation.
6. Click on the green phone icon to answer the phone.



7. Return to **FGT-BR1** and Click **Dashboard > FortiView Sessions**.
8. Right-click one of the column headings.

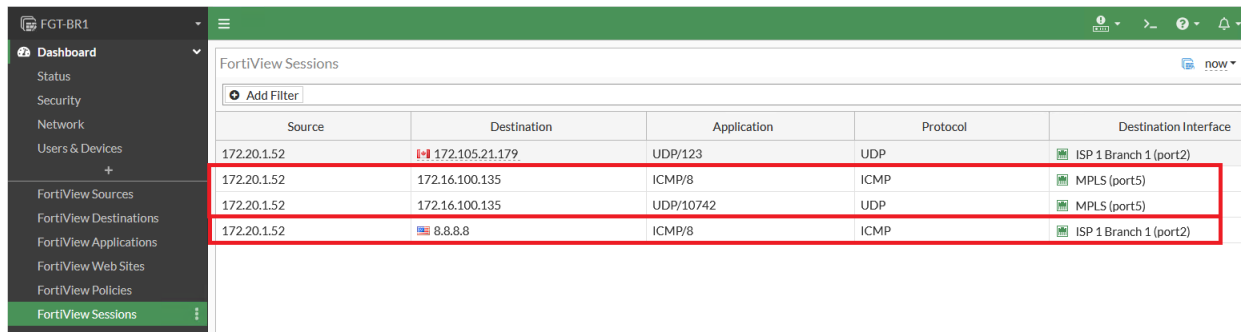
9. Deselect the following to clean things up:

- Device
- Source Port
- Destination Port
- Bytes
- Packets
- Duration

10. Select **Destination Interface** and **Source Interface**.

11. Click **Apply**.

12. Notice that the ping (ICMP) to 172.16.100.135 and the softphone (both traffic going back to the HQ) are directed through the MPLS interface, and the ping to 8.8.8.8 (internet) is going out the local internet breakout.



The screenshot shows the FortiView Sessions page in the FortiGate web interface. The left sidebar contains navigation options: Dashboard, Status, Security, Network, Users & Devices, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, and FortiView Sessions (highlighted). The main area displays a table of sessions with columns: Source, Destination, Application, Protocol, and Destination Interface. Three rows are highlighted with red boxes:

| Source | Destination | Application | Protocol | Destination Interface |
|-------------|----------------|-------------|----------|------------------------|
| 172.20.1.52 | 172.105.21.179 | UDP/123 | UDP | ISP 1 Branch 1 (port2) |
| 172.20.1.52 | 172.16.100.135 | ICMP/8 | ICMP | MPLS (port5) |
| 172.20.1.52 | 172.16.100.135 | UDP/10742 | UDP | MPLS (port5) |
| 172.20.1.52 | 8.8.8.8 | ICMP/8 | ICMP | ISP 1 Branch 1 (port2) |

Note: Other applications on the Ubuntu device may also be generating internet traffic.

When you click **Continue** on the FortiFIED app, the MPLS network will be disabled to simulate a failure and cause the SD-WAN rule to fail over to the other link.

Index: 2.0 (i)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Verify the Failover

Points: 0

----- Objective Section -----

Objective Text:

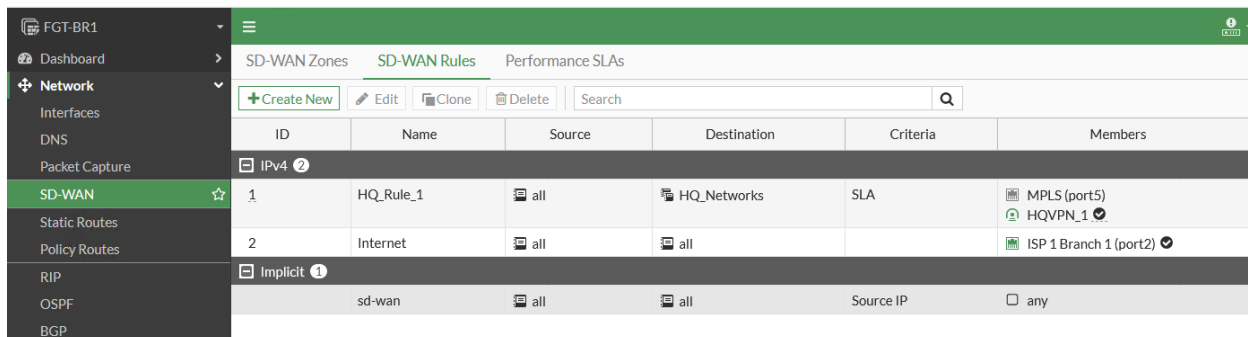
Verify the Failover

Background

A failure in the MPLS line was simulated in order to see the SD-WAN automatically failover to the HQVPN_1 interface, which in this scenario, was acting as the backup to the MPLS lines

Task

1. Return to the **FGT-BR1** browser tab.
2. Click **Network > SD-WAN > SD-WAN Rules**.

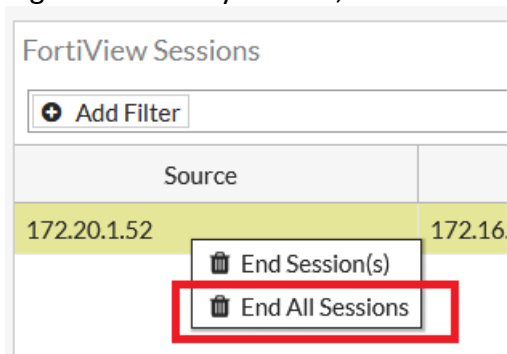


The screenshot shows the FortiManager interface for configuring SD-WAN rules. The left sidebar shows the navigation tree with 'SD-WAN' selected. The main area displays a table of SD-WAN rules. Rule 1, named 'HQ_Rule_1', is selected and shows its configuration: Source is 'all', Destination is 'HQ_Networks', Criteria is 'SLA', and Members are 'MPLS (port5)' and 'HQVPN_1'. Rule 2, named 'Internet', has Source 'all' and Destination 'all', with Member 'ISP 1 Branch 1 (port2)'. An 'Implicit' rule is also shown at the bottom with Source 'sd-wan' and Destination 'all'.

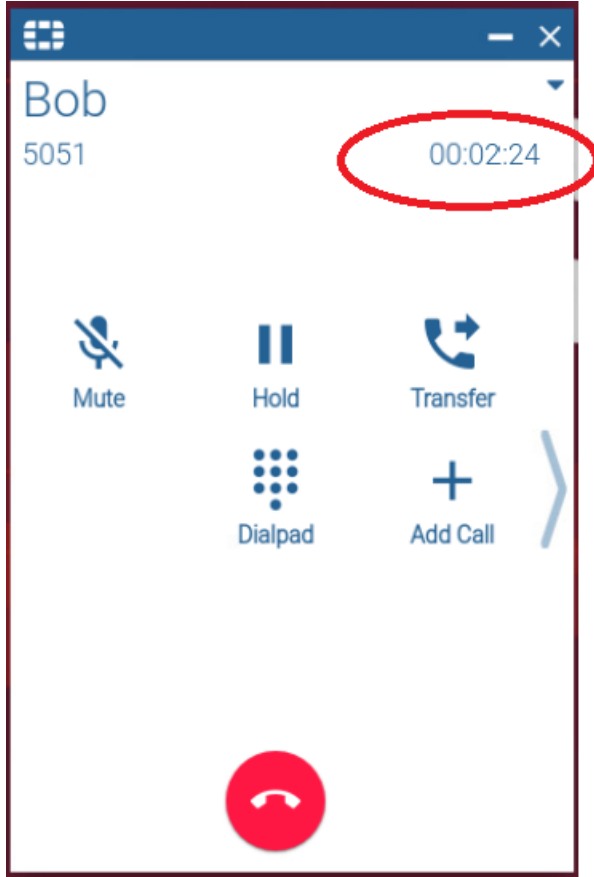
| ID | Name | Source | Destination | Criteria | Members |
|----------|-----------|--------|-------------|-----------|-------------------------|
| 1 | HQ_Rule_1 | all | HQ_Networks | SLA | MPLS (port5) HQVPN_1 |
| 2 | Internet | all | all | | ISP 1 Branch 1 (port2) |
| Implicit | | sd-wan | all | Source IP | any |


3. Confirm that the rules are now directing traffic to HQ via the HQVPN_1 tunnel.
Note: you may have to refresh the page

4. Click **Dashboard > FortiView Sessions**.
5. Right Click on any session, and select **End All Sessions**



6. Click **OK**.
7. Return to Carol's Workstation tab.
8. Open **Terminal** and ping **172.16.100.135**.
9. After a few pings, press Ctrl C and now ping **8.8.8.8**.
10. Notice that the softphone is still connected.



11. Return to **FGT-BR1** browser tab
 12. Click **Dashboard > FortiView Sessions**.
 13. Refresh the page. ( button at top right)
- Note:** You may need to reset the column headings.

| Source | Destination | Application | Protocol | Destination Interface |
|-------------|----------------|-------------|----------|------------------------|
| 172.20.1.52 | 8.8.8.8 | ICMP/8 | ICMP | ISP 1 Branch 1 (port2) |
| 172.20.1.52 | 172.16.100.135 | ICMP/8 | ICMP | HQVPN_1 |
| 172.20.1.52 | 172.16.100.135 | UDP/10742 | UDP | HQVPN_1 |

14. Now traffic to HQ is going through the HQVPN_1 tunnel.

When you click **Continue** on the FortiFIED app, the MPLS network will be re-enabled and cause the SD-WAN rule to once again favor the MPLS link.

Index: 2.0 (j)

Use Case: Configure SD-WAN via FortiManager

Objective Title: Verify return to MPLS

Points: 0

----- Objective Section -----

Objective Text:

Verify the Return to MPLS

Background

In the previous objective, a failure in the MPLS line was simulated in order to see the SD-WAN automatically failover to the HQVPN_1 interface, which in this scenario, was acting as the backup to the MPLS lines. The MPLS link has now been fixed, and the SD-WAN rule will once again favor the MPLS link

Task

1. Return to the **FGT-BR1** browser tab.
2. Click **Network > SD-WAN > SD-WAN Rules**.

| ID | Name | Source | Destination | Criteria | Members |
|----------|-----------|--------|-------------|-----------|-------------------------|
| 1 | HQ_Rule_1 | all | HQ_Networks | SLA | MPLS (port5) HQVPN_1 |
| 2 | Internet | all | all | | ISP 1 Branch 1 (port2) |
| Implicit | | | | | |
| | sd-wan | all | all | Source IP | any |

Note: that the rule still favors the HQVPN_1 link.

3. Click the **Performance SLAs** tab.

| SD-WAN Zones SD-WAN Rules Performance SLAs | | | | | |
|--|--|--|---|---|-------------------|
| Packet Loss Latency Jitter | | | | | |
| No data | | | | | |
| + Create New Edit Delete Search | | | | | |
| Name | Detect Server | Packet Loss | Latency | Jitter | Failure Threshold |
| Default_AWS | http://aws.amazon.com/ | | | | 5 |
| Default_DNS | 208.91.112.53 208.91.112.52 (System DNS) | | | | 5 |
| Default_FortiGuard | http://fortiguard.com/ | | | | 5 |
| Default_Gmail | gmail.com | | | | 5 |
| Default_Google Search | http://www.google.com/ | | | | 5 |
| Default_Office_365 | http://www.office.com/ | | | | 5 |
| HQ_SLA | 10.10.30.2 | HQVPN_1: 0.00% MPLS (port5): 52.00% | HQVPN_1: 0.99ms MPLS (port5): 0.59ms | HQVPN_1: 0.13ms MPLS (port5): 0.10ms | 5 |

As you can see in the screenshot above, the MPLS link doesn't yet meet the SLA thresholds.

- Refresh the browser page every few seconds until the MPLS link meets the SLA requirements.

| | | | | | |
|--------|------------|---------------------------------------|---|---|---|
| HQ_SLA | 10.10.30.2 | HQVPN_1: 0.00% MPLS (port5): 0.00% | HQVPN_1: 0.99ms MPLS (port5): 0.58ms | HQVPN_1: 0.16ms MPLS (port5): 0.11ms | 5 |
|--------|------------|---------------------------------------|---|---|---|

- Return to the SD-WAN Rules tab.

| SD-WAN Zones SD-WAN Rules Performance SLAs | | | | | |
|--|-----------|--------|-------------|-----------|------------------------|
| + Create New Edit Clone Delete Search | | | | | |
| ID | Name | Source | Destination | Criteria | Members |
| IPv4 2 | | | | | |
| 1 | HQ_Rule_1 | all | HQ_Networks | SLA | MPLS (port5) HQVPN_1 |
| 2 | Internet | all | all | | ISP 1 Branch 1 (port2) |
| Implicit 1 | | | | | |
| | sd-wan | all | all | Source IP | any |

Note that the MPLS link is now the favored link again.

Index: 3.0

Use Case: Conclusion

Objective Title: End of Session

Points: 0

Objective Section

Objective Text:

FORTINET®

Fast Tracks

You have successfully completed the
SD-WAN
Hands-On Lab

Thank You

To get more information on this or other Fortinet solutions, please consider looking at **Fortinet's NSE** training.

