SD-WAN
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.fortiguard.com

Fortinet Training Program Information

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

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

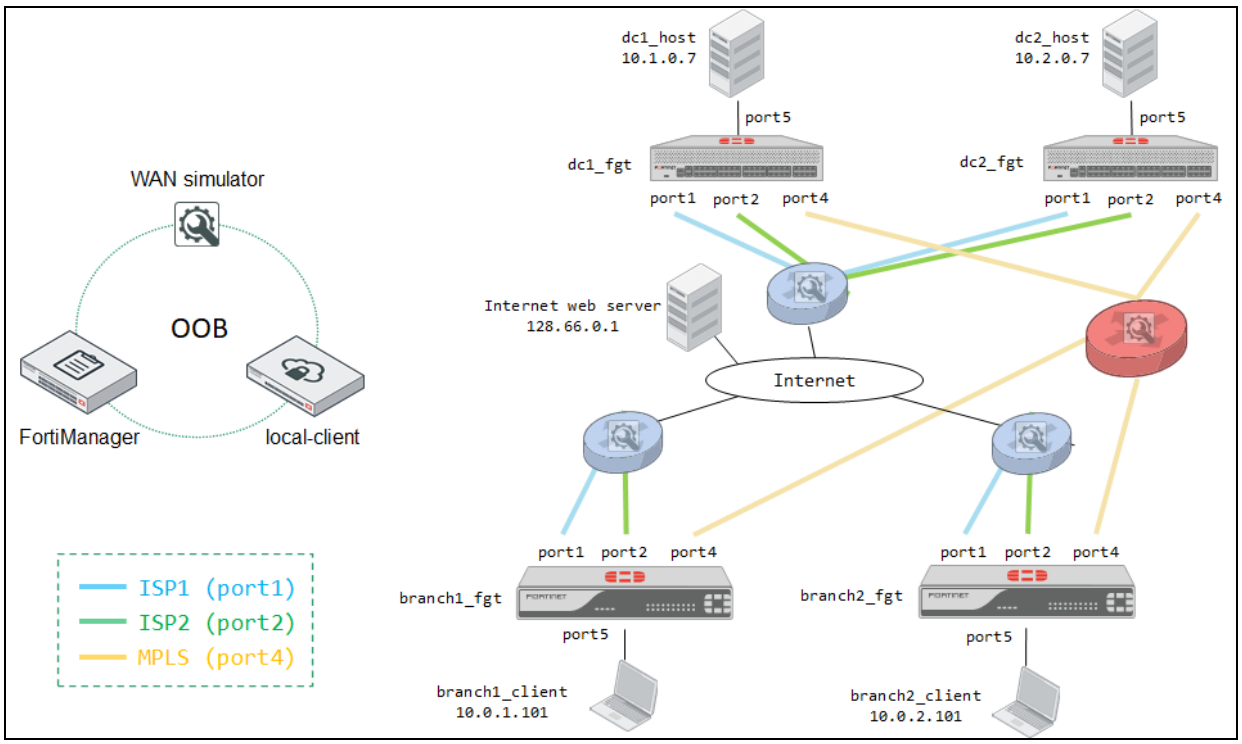
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

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

3/30/2023

TABLE OF CONTENTS

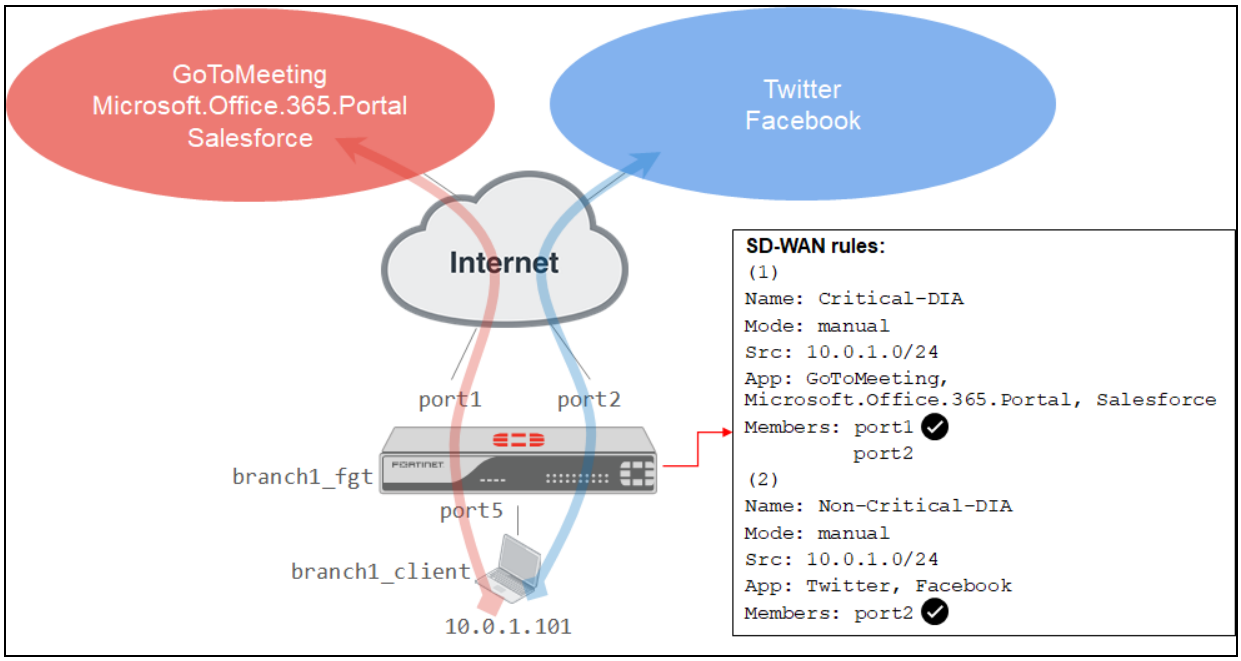
Network Topology



Device	port1	port2	port4	port5
branch1_fgt	192.2.0.1	192.2.0.9	172.16.0.1	10.0.1.254
branch2_fgt	203.0.113.1	203.0.113.9	172.16.0.9	10.0.2.254
dc1_fgt	100.64.1.1	100.64.1.9	172.16.1.5	10.1.0.1
dc2_fgt	100.64.2.1	100.64.2.9	172.16.2.5	10.2.0.1

Lab 1: Basic DIA Setup

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



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

Objectives

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

Time to Complete

Estimated: 50 minutes

Exercise 1: Configuring a Basic DIA Setup

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

Configure a Zone and Members for DIA

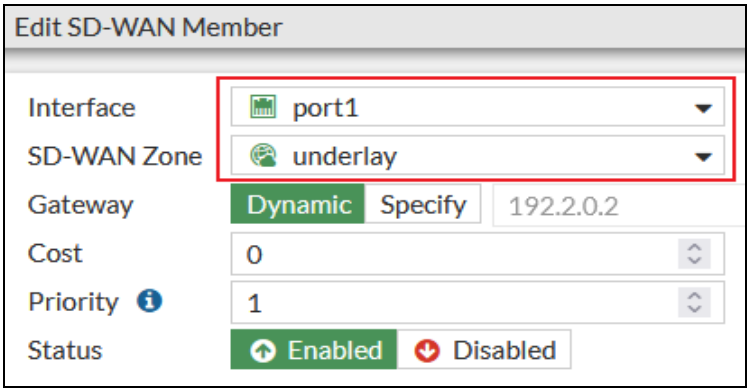
You will configure the underlay zone, and then add port1 and port2 as members.

To create an SD-WAN zone

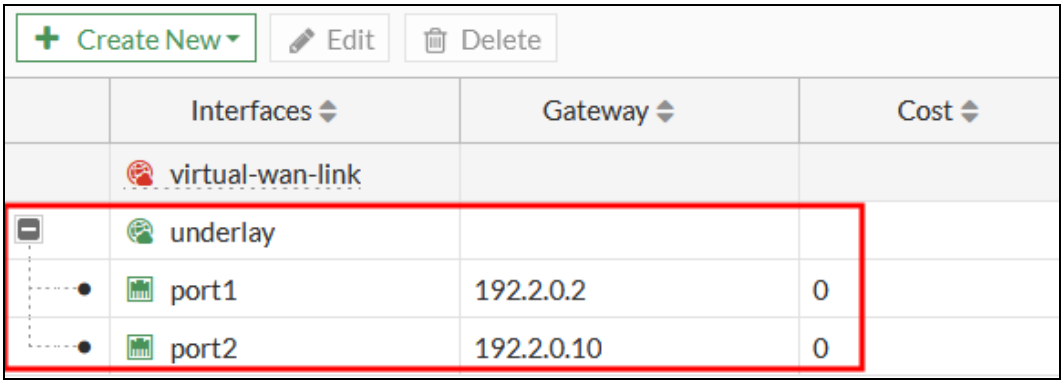
1. Access the branch1_fgt GUI, and then log in with the username `admin` and password `password`.
2. Click **Network** > **SD-WAN**, and then click the **SD-WAN Zones** tab.
3. Click **Create New** > **SD-WAN Zone** to add an SD-WAN zone.
4. In the **Name** field, type `underlay`.

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

Field	Value
Interface	port1
SD-WAN Zone	underlay



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



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

Stop and think!

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

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

Configure a Performance SLA

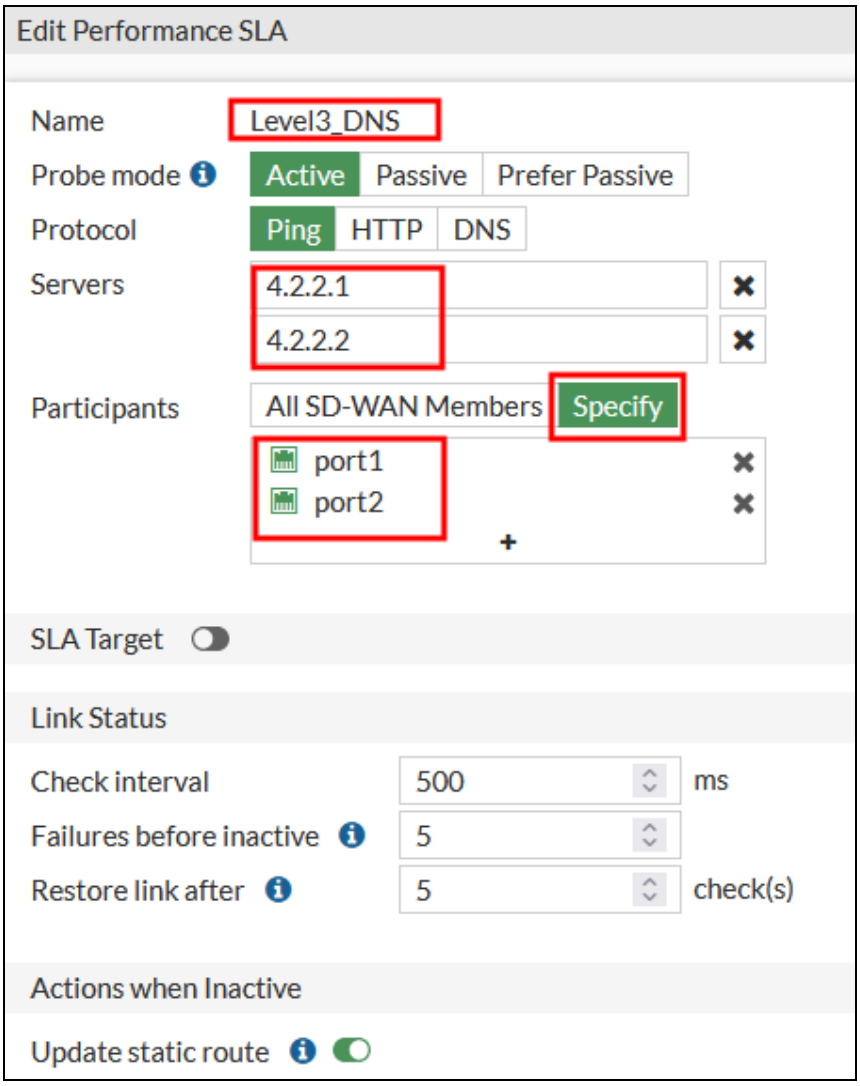
You will configure a performance SLA for monitoring the health of port1 and port2.

To configure a performance SLA

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

Field	Value
Name	Level3_DNS
Server	4.2.2.1 Click **+**, and then type `4.2.2.2`.

Field	Value
Participants	Click **Specify**, and then select **port1** and **port2**.



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

Name	Detect Server	Packet Loss	Latency	Jitter
Level3_DNS	4.2.2.1 42.2.2	port1: 0.00% port2: 0.00%	port1: 23.91ms port2: 23.77ms	port1: 0.29ms port2: 0.26ms

6. Click **Dashboard** > **Network**, and then click the **Routing** widget.
   Your page should look similar to the following example:

Network	Gateway IP	Interfaces	Distance	Type
10.0.1.0/24	0.0.0.0	port5	0	Connected
172.16.0.0/16	172.16.0.2	port4	10	Static
172.16.0.0/29	0.0.0.0	port4	0	Connected
192.2.0.0/29	0.0.0.0	port1	0	Connected
192.2.0.8/29	0.0.0.0	port2	0	Connected
192.168.0.0/24	0.0.0.0	port10	0	Connected
10.0.101.0/24	0.0.0.0	vl_lan_ts	0	Connected

Stop and think!

There are no routes to 4.2.2.1 and 4.2.2.2, yet the performance SLA shows that port1 and port2 are up. Why?

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

Configure Rules

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

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

To enable GUI visibility for application detection

1. Open an SSH session to branch1_fgt.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to enable the visibility of application detection for SD-WAN rules:

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

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

To configure rules

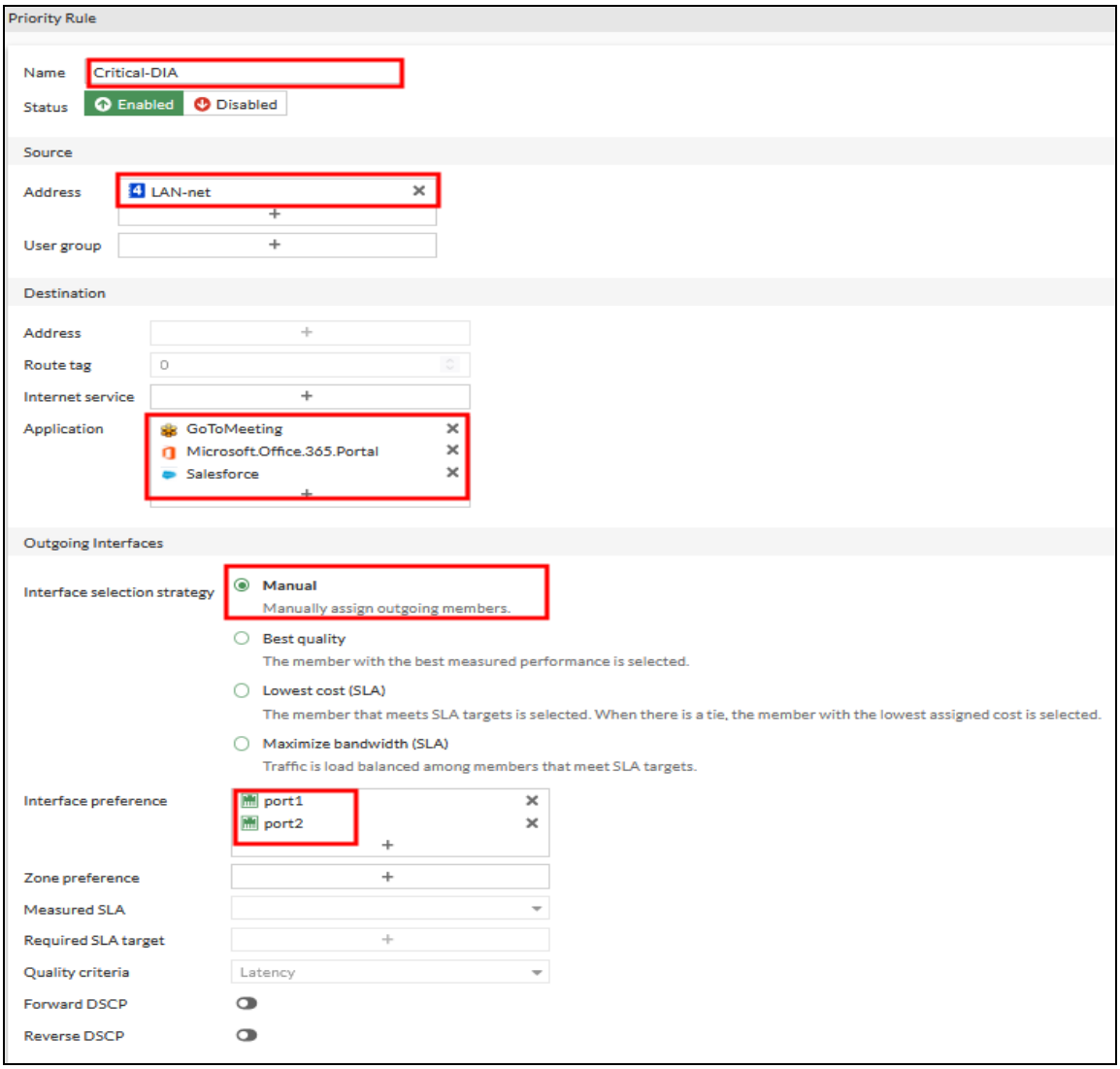
1. Return to the branch1_fgt GUI, and then refresh the browser page.
2. Click **Network** > **SD-WAN**, and then click the **SD-WAN Rules** tab.

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

Field	Value
Name	Critical-DIA
Source address	LAN-net
Application	Select **GoToMeeting**, **Microsoft.Office.365.Portal**, and **Salesforce**.
Outgoing Interfaces	Select **Manual**.
Interface preference	Select **port1**, and then select **port2**.

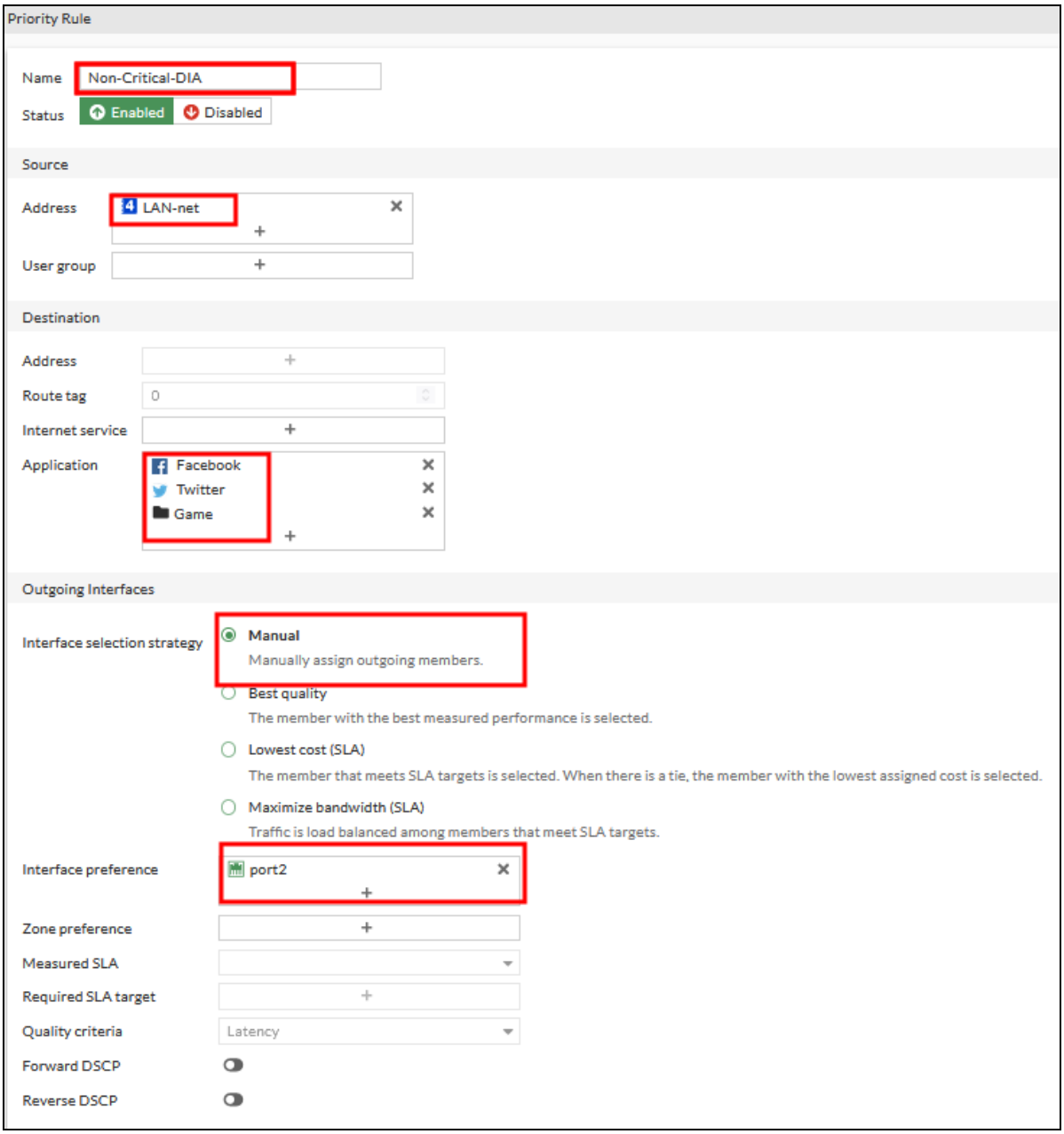
The **LAN-net** firewall address object was preconfigured.

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



5. Click **OK** to save the settings.
6. Repeat the previous steps to configure a rule for non-critical traffic using the following settings:

Field	Value
Name	Non-Critical-DIA
Source address	LAN-net
Application	Select **Apps**, and then select **Twitter** and **Facebook**. Select **Category**, and then select **Game**.
Outgoing Interfaces	Select **Manual**.
Interface preference	Select **port2**.



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

ID	Name	Source	Destination	Criteria	Members
IPv4 2					
1	Critical-DIA	LAN-net	GoToMeeting Microsoft.Office.365.Portal Salesforce		port1 port2
2	Non-Critical-DIA	LAN-net	Twitter Facebook Game		port2
Implicit 1					
	sd-wan	all	all	Source IP	any

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

Configure a Static Route and Firewall Policy

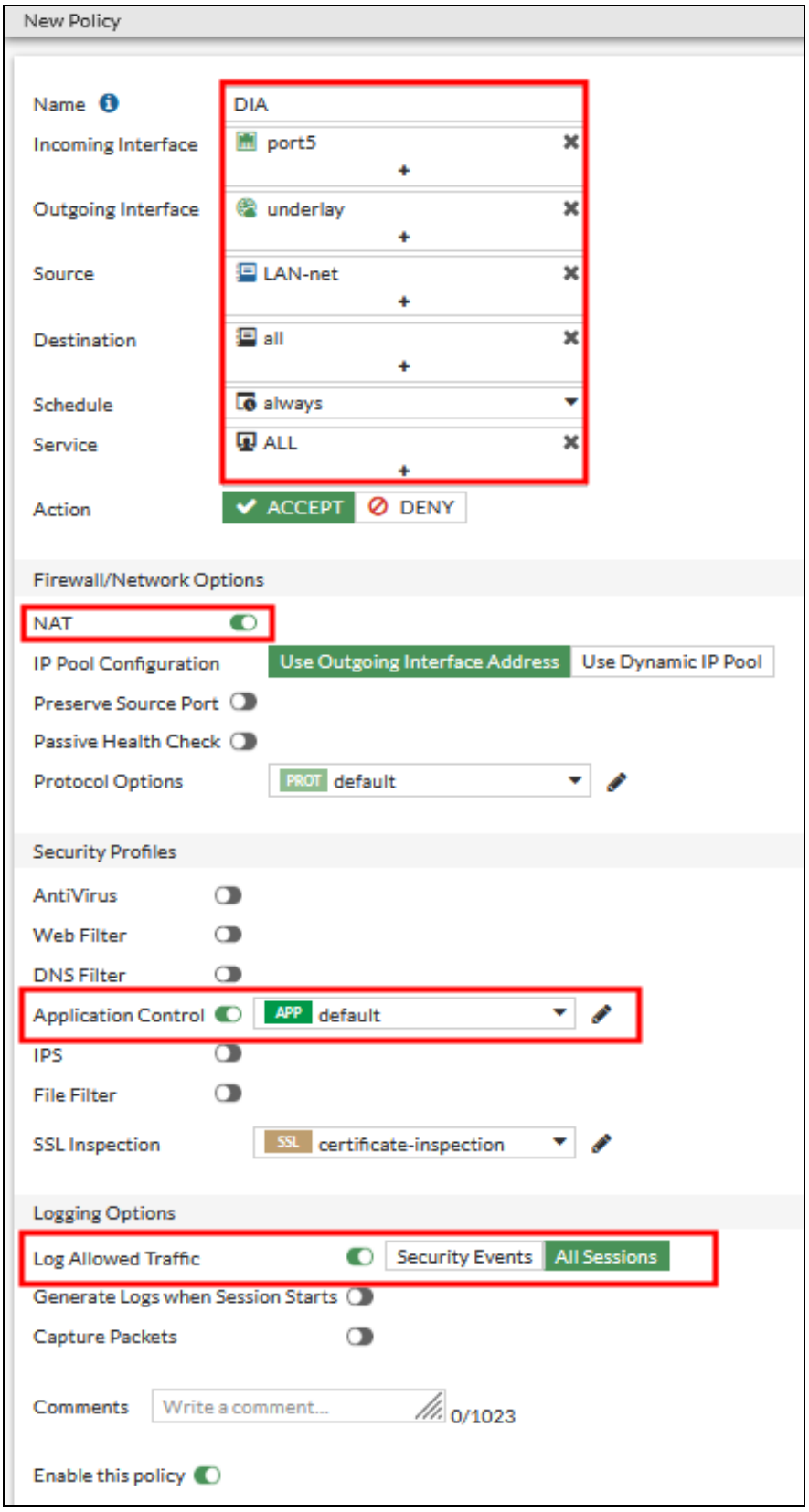
You will configure a static route and firewall policy for routing and allowing SD-WAN traffic. Both objects will reference the underlay zone.

To configure a static route and firewall policy

1. Continuing on the branch1_fgt GUI, click **Network** > **Static Routes**.
2. Click **Create New** to add a static route.
3. In the **Interface** field, select **underlay**.
4. Click **OK** to save the settings.
5. Click **Policy & Objects** > **Firewall Policy**.
6. Click **Create New** to add a firewall policy.
7. Configure the following settings:

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

Field	Value
Service	ALL
NAT	Enable
Security Profiles	Enable **Application Control**, and then select **default**.
Log Allowed Traffic	Enable this setting, and then select **All Sessions**.



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

Exercise 2: Monitoring DIA Traffic

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

Generate Internet Traffic From branch1_client

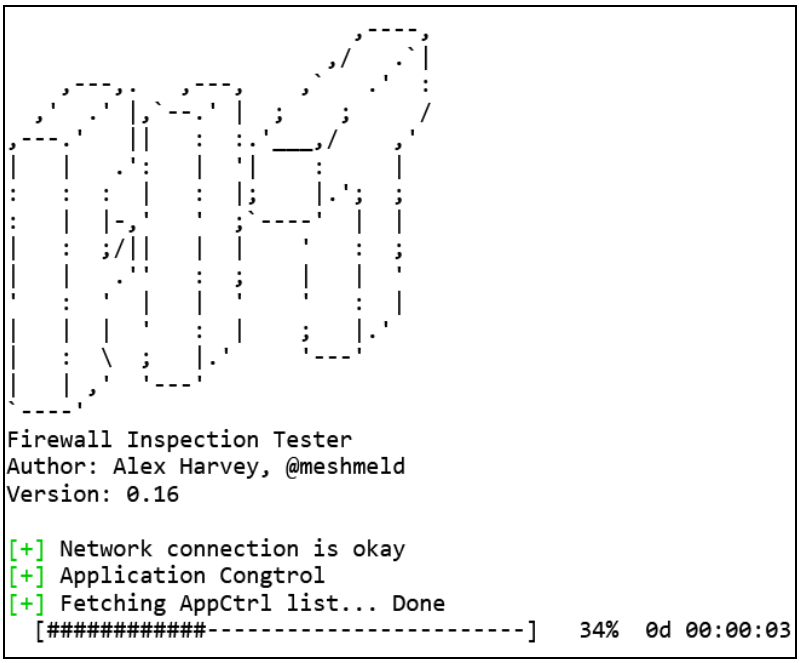
You will generate internet traffic from branch1_client using the traffic generator tool.

To generate internet traffic from branch1_client

1. Open an SSH session to branch1_client.
2. Log in with the username `root` and password `password`.
3. Enter the following commands:

```
cd /fortipoc/fit/
./myfit.sh
```

Your output should look similar to the following example:



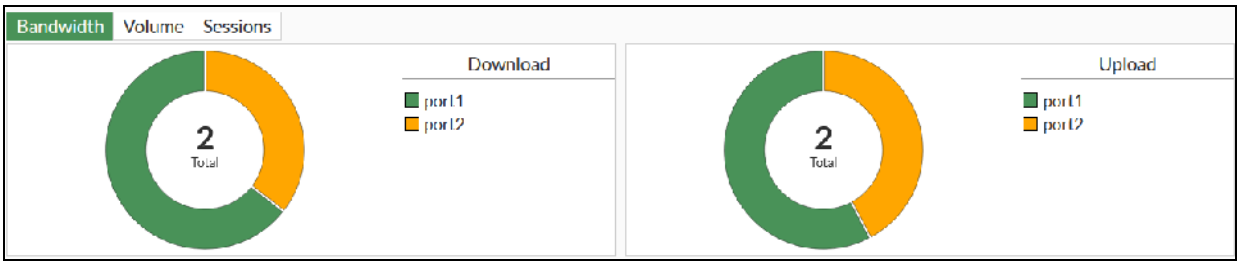
branch1_client is generating various types of internet traffic.

Monitor DIA Traffic Distribution

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

To monitor DIA traffic distribution

1. Access the branch1_fgt GUI, and then log in with the username `admin` and password `password`.
2. Click **Network** > **SD-WAN**, and then click the **SD-WAN Zones** tab.
3. Click **Bandwidth** to display SD-WAN distribution graphs based on bandwidth.
   Your page should look similar to the following example:



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

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

To view SD-WAN traffic logs

1. Continuing on the branch1_fgt GUI, click **Log & Report** > **Forward Traffic**.
2. Hover over the upper-left corner of the log table to display the table column settings icon.
   A gear icon is displayed.
3. Click the gear icon, and then click **Destination Interface**, **SD-WAN Quality**, and **SD-WAN Rule Name**.
4. Click **Apply** to save the settings.
   Your page should look similar to the following example:

Application Name	Result	Policy Name	Destination Interface	SD WAN Quality	SD WAN Rule Name
Twitter	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Non Critical DIA
Twitter	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Non-Critical-DIA
Microsoft.Office.365.Portal	Accept (UTM Allowed)	DIA	port1	Seq_num(1 port1), alive, selected	Critical-DIA
DNS	Accept (122 B / 254 B)	DIA	port2		
DNS	Accept (120 B / 348 B)	DIA	port2		
DNS	Accept (130 B / 388 B)	DIA	port2		
DNS	Accept (128 B / 378 B)	DIA	port2		
DNS	Accept (120 B / 348 B)	DIA	port2		
Microsoft.Office.365.Portal	Accept (UTM Allowed)	DIA	port1	Seq_num(1 port1), alive, selected	Critical-DIA
Salesforce	Accept (UTM Allowed)	DIA	port1	Seq_num(1 port1), alive, selected	Critical-DIA
Microsoft.Office.365.Portal	Accept (UTM Allowed)	DIA	port1	Seq_num(1 port1), alive, selected	Critical DIA
Salesforce	Accept (UTM Allowed)	DIA	port1	Seq_num(1 port1), alive, selected	Critical-DIA
GoToMeeting	Accept (UTM Allowed)	DIA	port1	Seq_num(1 port1), alive, selected	Critical-DIA
Twitter	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Non-Critical-DIA
Twitter	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Non-Critical-DIA
DNS	Accept (114 B / 218 B)	DIA	port2		

5. Browse the log table, and confirm the following:
   - **GotoMeeting**, **SalesForce**, and **Microsoft.Office.365.Portal** traffic matches the **Critical-DIA** rule, and uses **port1**.
   - **Facebook** and **Twitter** traffic matches the **Non-Critical-DIA** rule, and uses **port2**.

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

Stop and think!

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

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

Stop and think!

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

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

6. Keep the internet traffic generator running on branch1_client.

Bring Down port1

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

To bring down port1

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

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

Name	Detect Server	Packet Loss	Latency	Jitter
Level3_DNS	4.2.2.1 4.2.2.2	port1: port2: 0.00%	port1: port2: 23.43ms	port1: port2: 0.32ms

Monitor SD-WAN Events and Traffic Logs

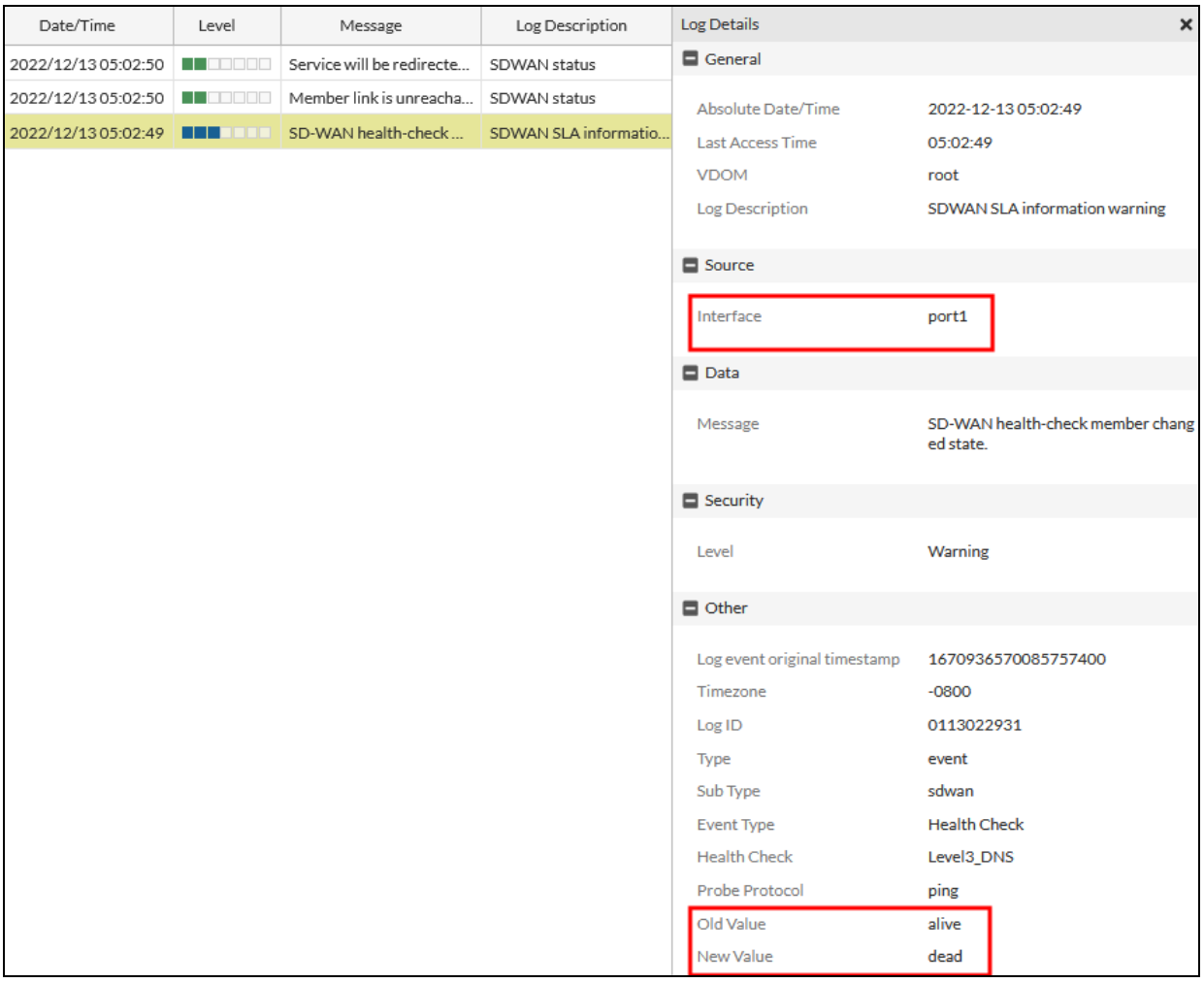
You will review SD-WAN events and traffic logs triggered by the previous action.

To monitor SD-WAN events and traffic logs

1. Continuing on the branch1_fgt GUI, click **Log & Report** > **System Events** > **Logs**.
2. In the top bar, click **General System Events**, and then select **SD-WAN Events**.
3. Look for the following three recent message logs:

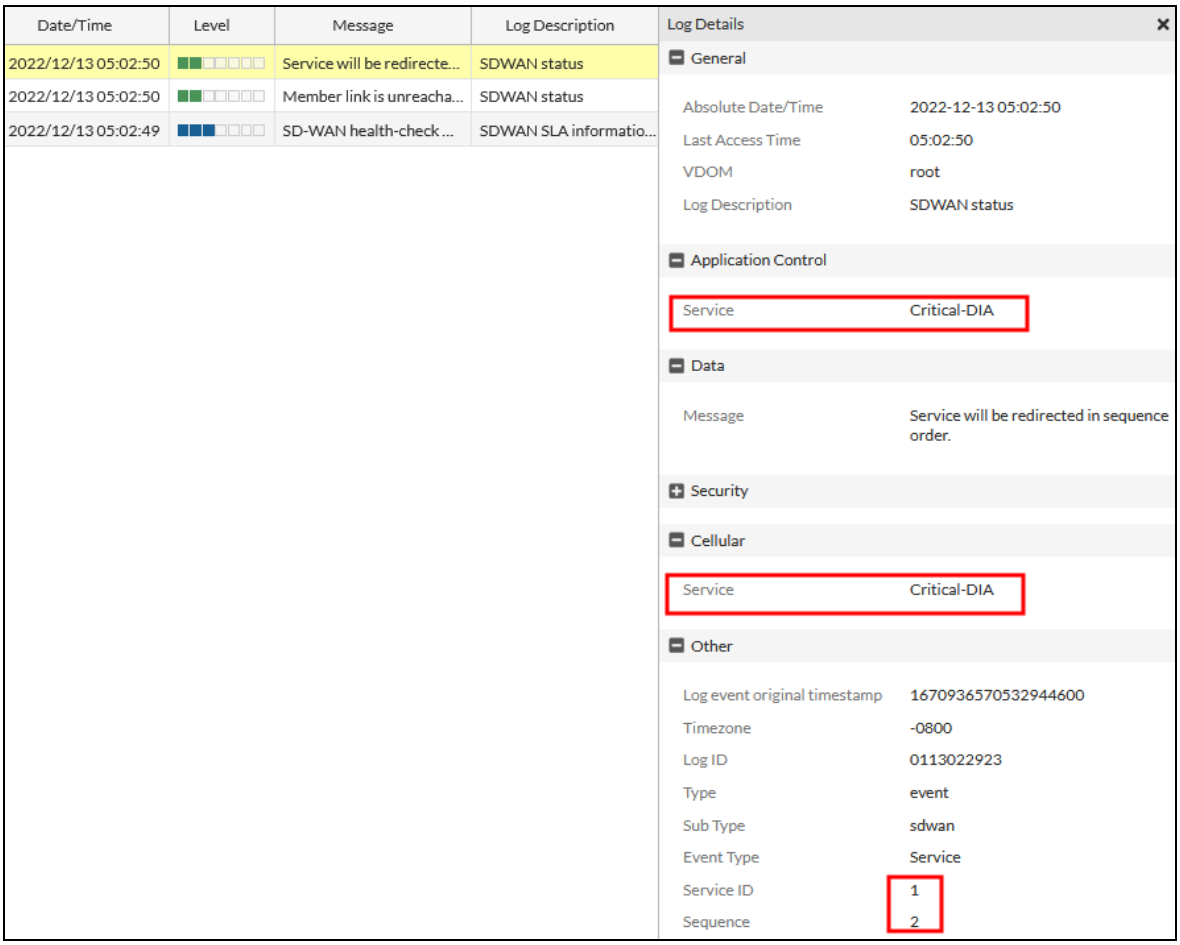
Date/Time	Level	Message	Log Description
2022/12/13 05:02:50		Service will be redirected in sequence order.	SDWAN status
2022/12/13 05:02:50		Member link is unreachable or miss threshold. Stop forwarding traffic.	SDWAN status
2022/12/13 05:02:49		SD-WAN health-check member changed state.	SDWAN SLA information warning

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



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

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



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

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

Application Name	Result	Policy ...	Destina...	SD-WAN Quality	SD-WAN Rule Name
Salesforce	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Critical-DIA
Microsoft.Office.365.Portal	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Critical-DIA
Twitter	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Non-Critical-DIA
Twitter	Accept (UTM Allowed)	DIA	port2	Seq_num(2 port2), alive, selected	Non-Critical-DIA
DNS	Accept (124 B / 226 B)	DIA	port2		

All traffic is now forwarded to port2.

Bring Up port1

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

To bring up port1

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

Take the Expert Challenge!

Use the FortiGate GUI to confirm that:

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

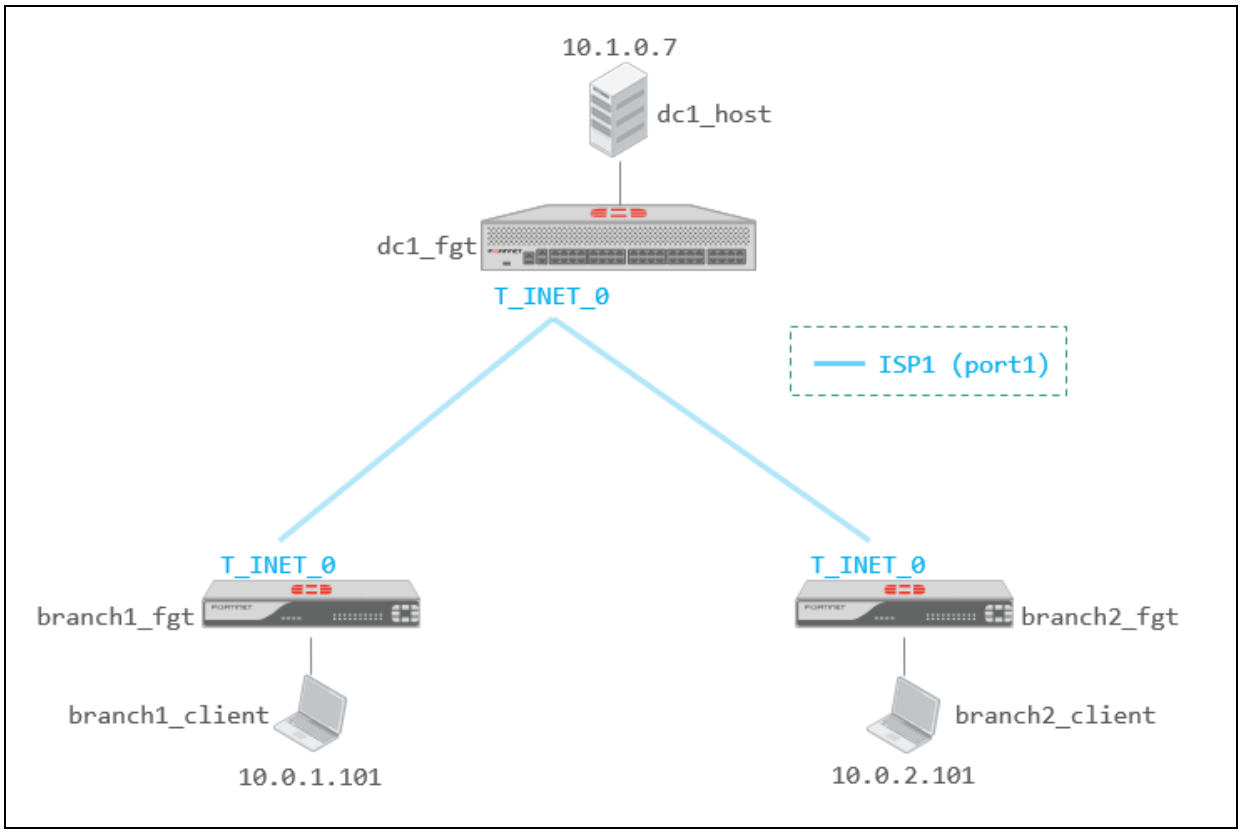
If you require assistance, or to verify your work, review the procedure described previously in this exercise.

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

Lab 2: Centralized Management

In this lab, you will configure the same DIA SD-WAN setup you configured on branch1_fgt, on branch2_fgt. For this, you will import existing SD-WAN settings on branch1_fgt to an SD-WAN template on FortiManager. You will then use the SD-WAN template to deploy DIA on branch2_fgt. You will also monitor DIA traffic on FortiManager.

After that, you will use IPsec recommended templates on FortiManager to deploy the following hub-and-spoke dial-up IPsec VPN topology:



In the topology, branch1_fgt and branch2_fgt are dial-up clients, and dc1_fgt is a dial-up server. You will use static routing for the VPN, and you will also verify that the tunnels come up and that there is spoke-to-hub and spoke-to-spoke connectivity.

Note that you will deploy overlays for one underlay only (ISP1). You can follow the same procedure for overlays established over the other underlays (ISP2 and MPLS), but these will be automatically configured for you in another lab. Also note that there is no separate FortiAnalyzer. Instead, you will configure devices to send logs to FortiManager, which has the FortiAnalyzer features enabled.

Objectives

- Add all devices to FortiManager
- Deploy DIA using central management (SD-WAN templates)

- Configure firewall policies, static routes, normalized interfaces, metadata variables, and firewall address objects to deploy SD-WAN and the VPN
- Monitor SD-WAN on FortiManager
- Configure a hub-and-spoke dial-up IPsec VPN using IPsec recommended templates
- Use the SD-WAN overlay template to configure IPsec VPN tunnels for the overlay and BGP routing

Time to Complete

Estimated: 135 minutes

Prerequisites

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

Exercise 1: Configuring SD-WAN on FortiManager

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

Add branch1_fgt and branch2_fgt to FortiManager

You will add branch1_fgt and branch2_fgt to FortiManager.

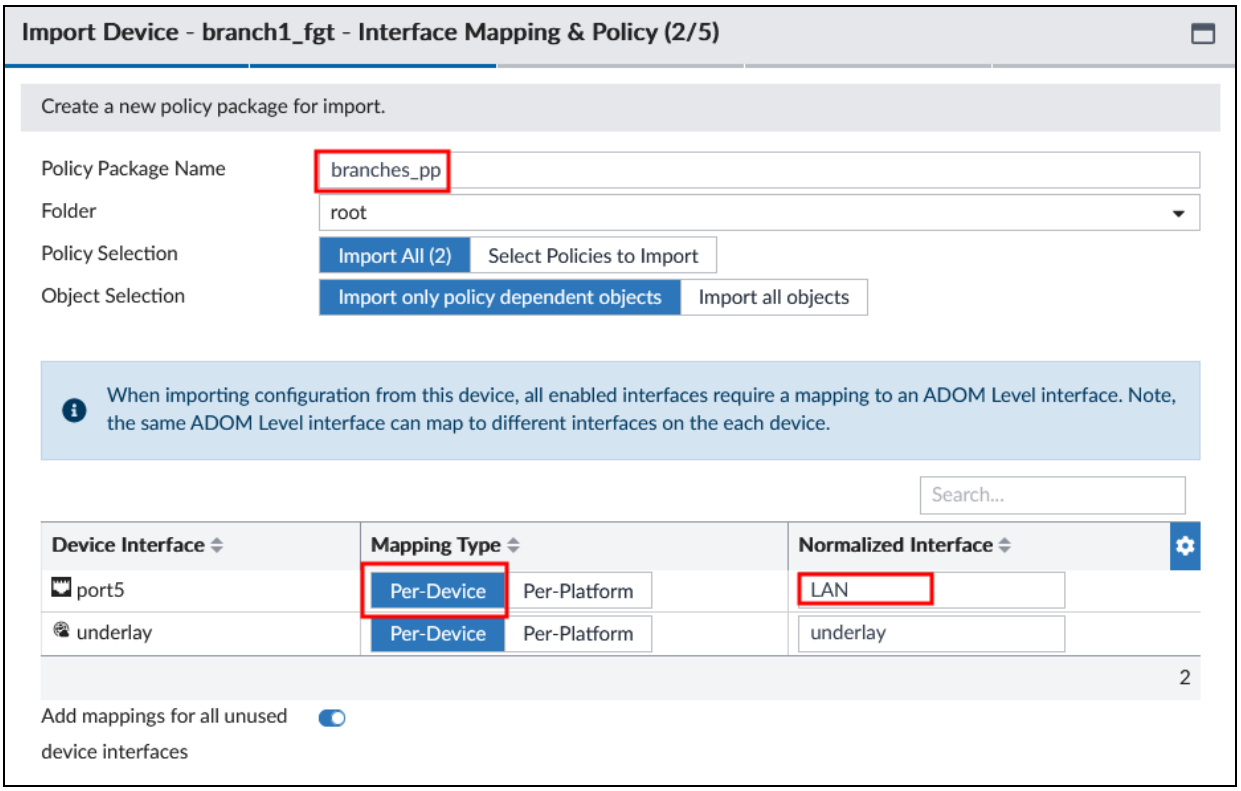
To add branch1_fgt and branch2_fgt to FortiManager

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Add Device**.

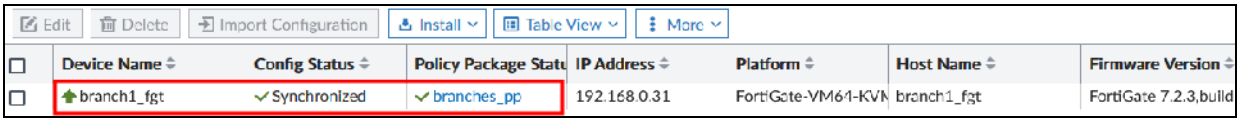
3. Click **Discover Device**, and then configure the following settings:

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

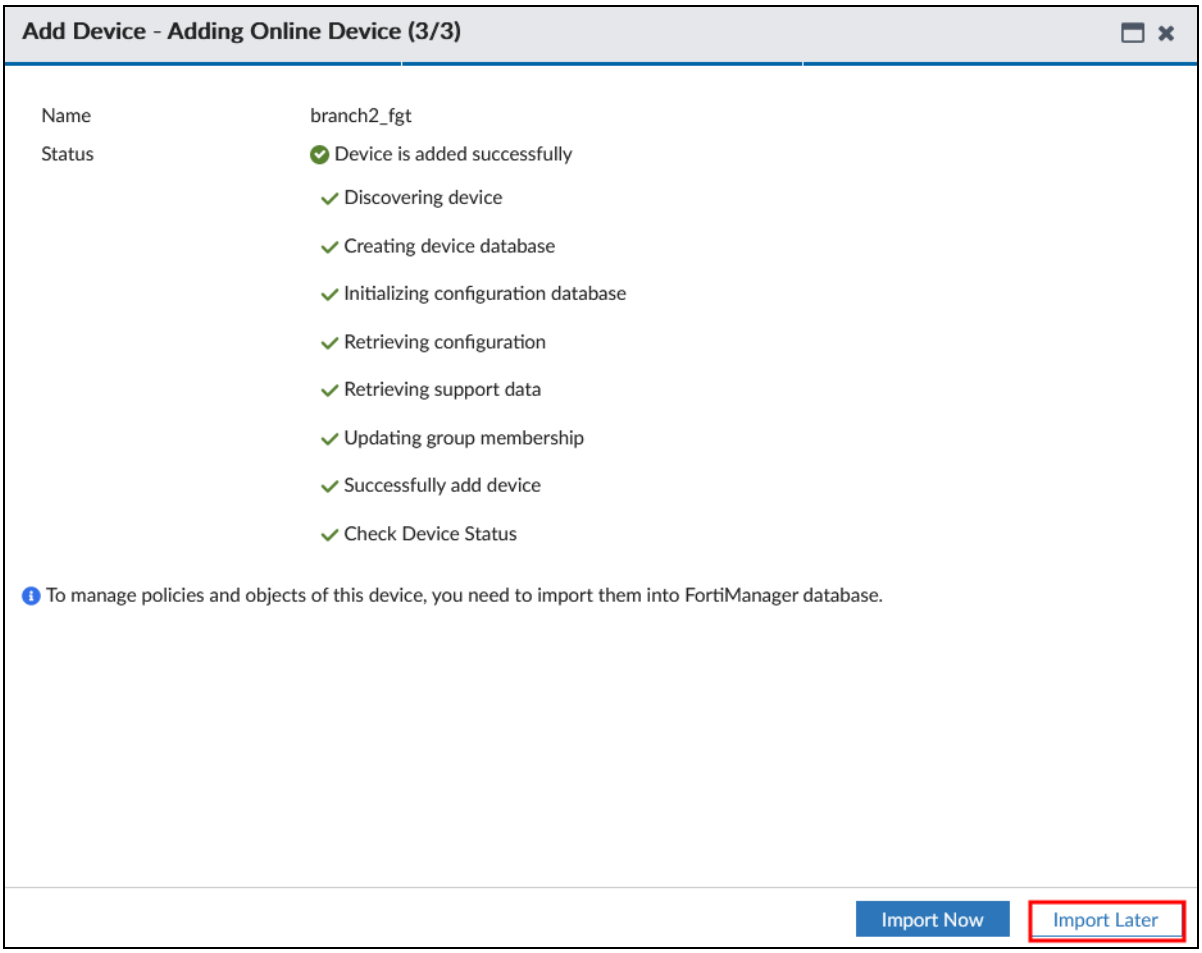
4. Click **Next**.
5. Click **Next**, and then wait until the **Add Device** task is completed.
6. Click **Import Now**.
7. Select **Import Policy Package**, and then click **Next**.
8. In the **Policy Package Name** field, type `branches_pp`.
9. In the port5 device interface settings, in the **Mapping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



10. Click **Next**.
11. Click **Next**, wait until the **Ready to Import screen** appears, and then review the imported objects.
12. Click **Next**, and then wait until the **Import Device** task is completed.
13. Click **Finish**.
14. Click **Device & Groups** > **Managed FortiGate** to display the list of managed devices.
    Your page should look similar to the following example:



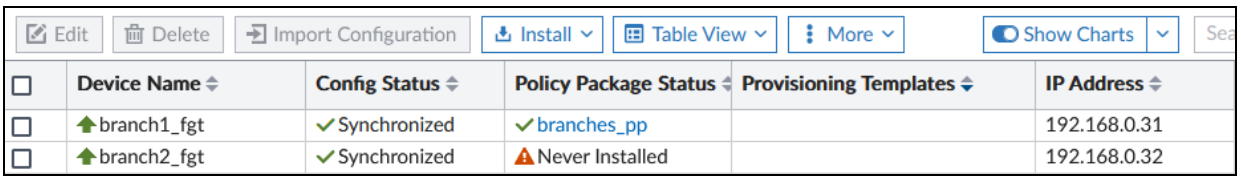
15. Repeat steps 2–5 for branch2_fgt, but use the IP address 192.168.0.32 and the same administrator credentials.
16. Click **Import Later**.



You don't need to import policies and objects from branch2_fgt because you will push them from FortiManager.

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

    Your page should look similar to the following example:

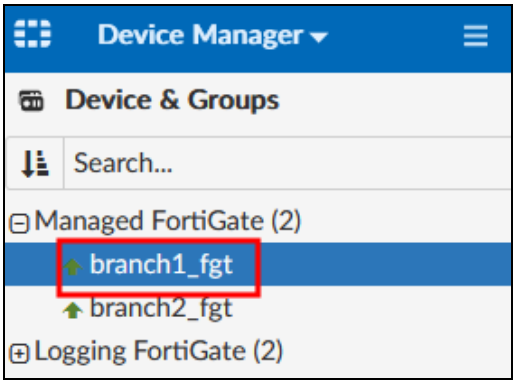


Import SD-WAN Settings Into the SD-WAN Template

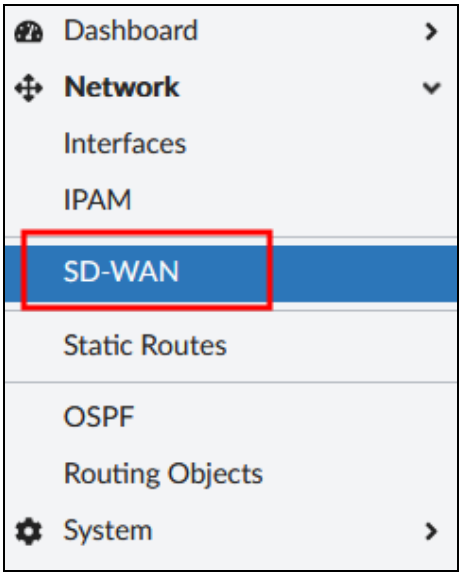
First, you will view the current SD-WAN settings on branch1_fgt (per-device management), and then you will import the settings into an SD-WAN template for central SD-WAN management purposes.

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

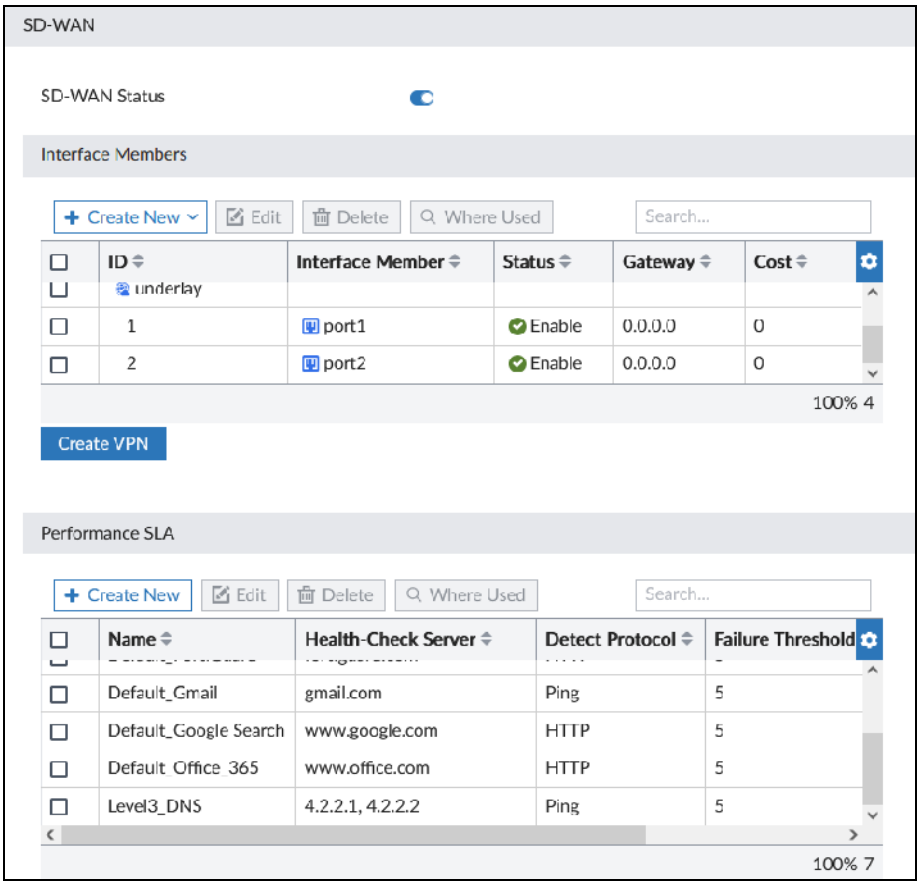
1. Continuing on the FortiManager GUI, expand **Managed FortiGate**, and then click **branch1_fgt**.

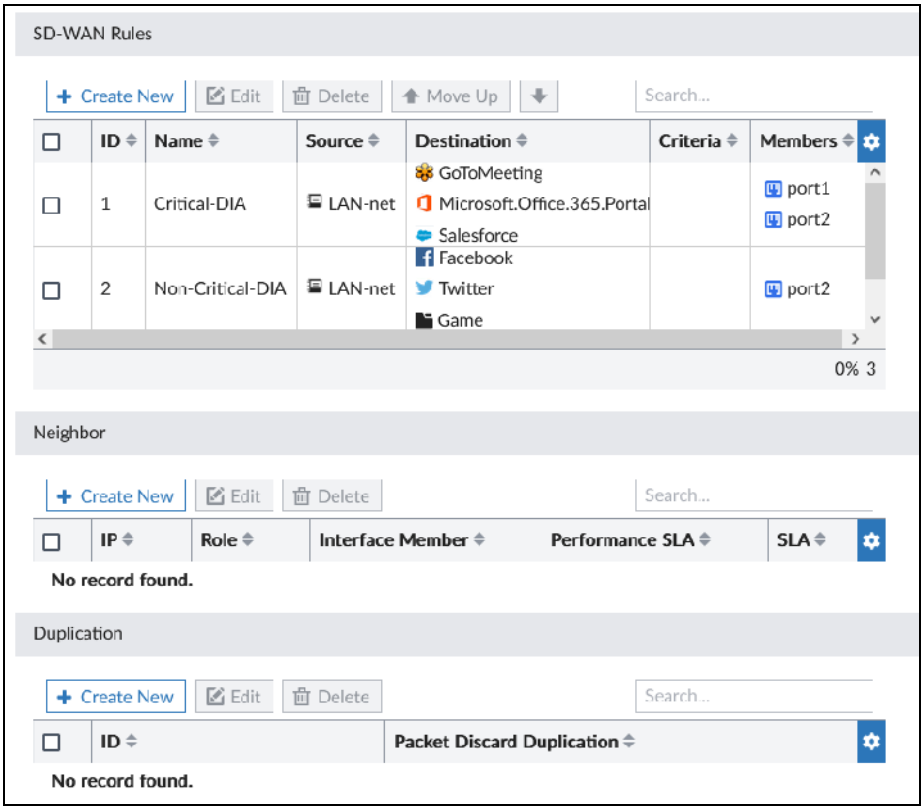


2. Click **Network** > **SD-WAN** to display the device SD-WAN settings.



Your page should look similar to the following example:

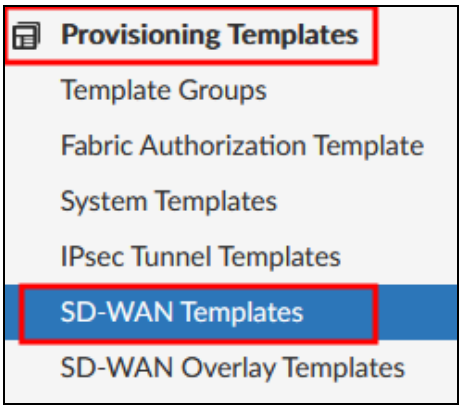




The **Gateway** setting for **port1** and **port2** is set to `0.0.0.0`. You will change this setting to use metadata variables later in this lab.

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

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



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

3. Configure the following settings:

Field	Value
Name	branches
Device	branch1_fgt (root)

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

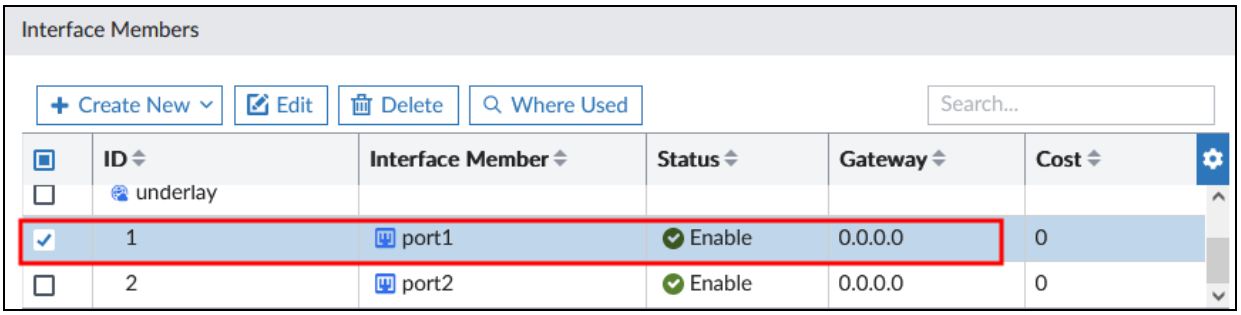
   Both per-device and template settings should be the same.

Configure the SD-WAN Template

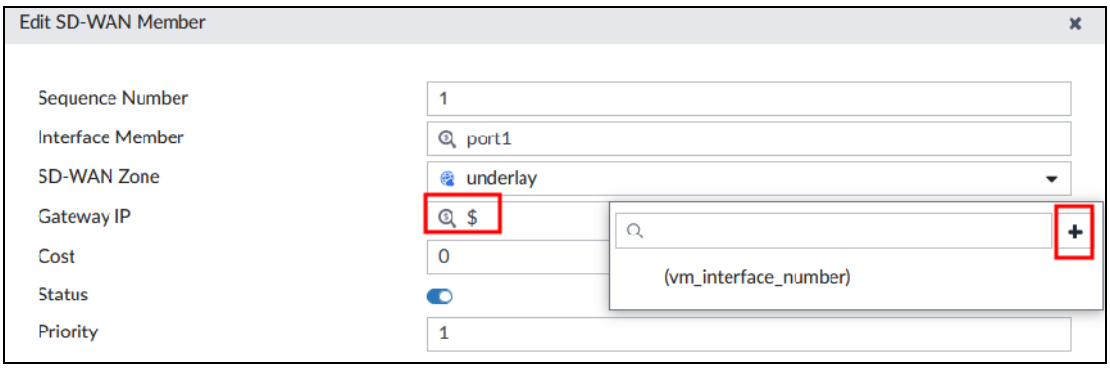
You will configure the template to use metadata variables for the gateway settings. After that, you will configure branch1_fgt and branch2_fgt as the template targets.

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

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



4. In the **Gateway IP** field, replace `0.0.0.0` with `$`.
   A window appears where you can select existing metadata variables or create new variables.
5. Click **+** to create a new variable.
   Your page should look similar to the following example:

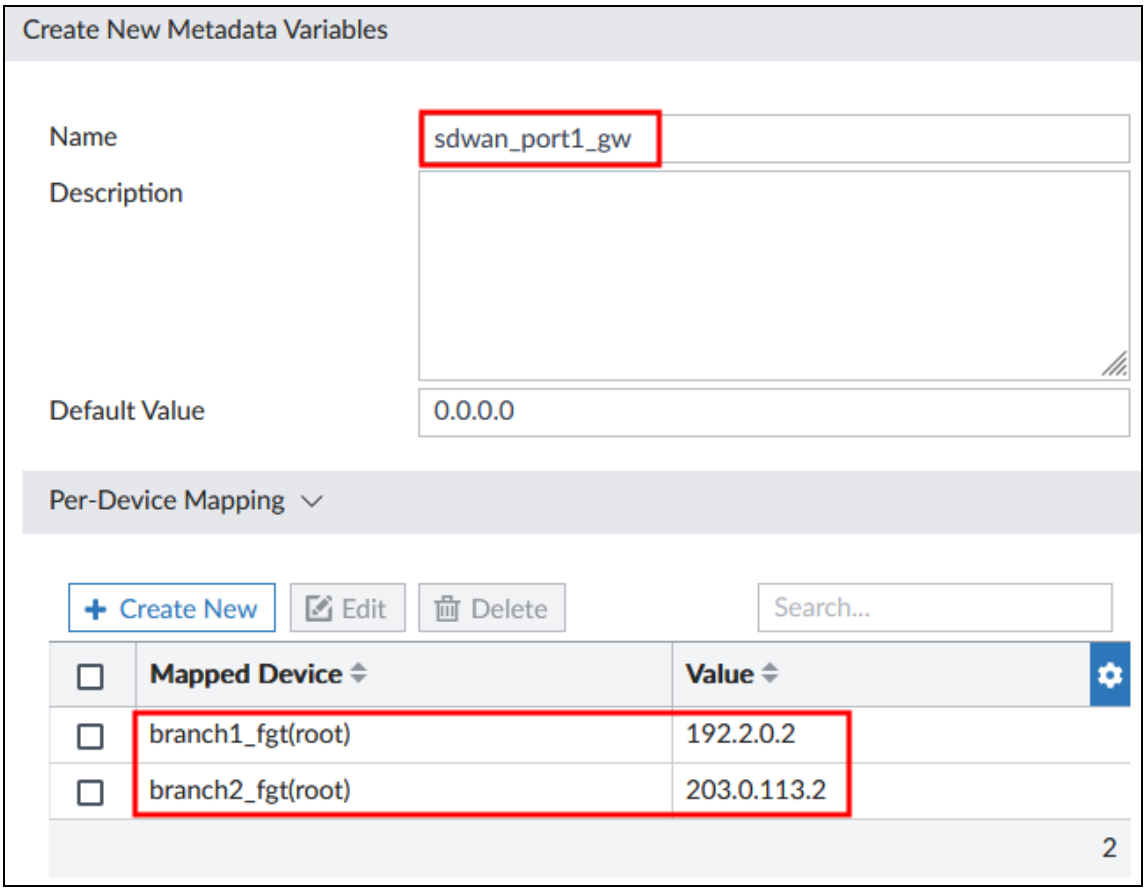


6. Create a new metadata variable with the following settings:

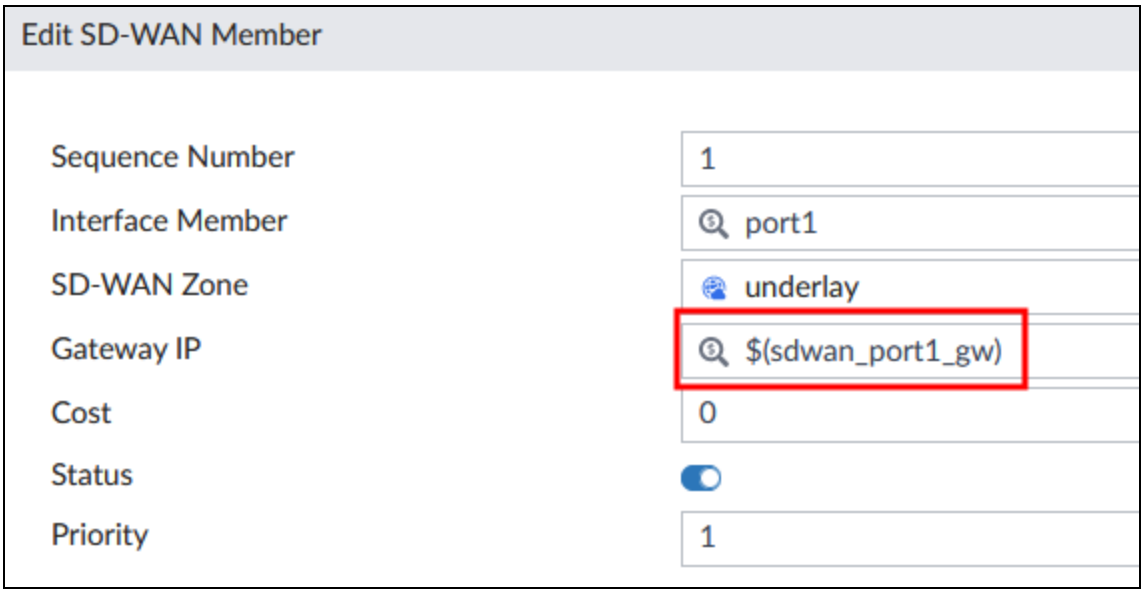
Field	Value
Name	sdwan_port1_gw
Default Value	0.0.0.0

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

Your page should look similar to the following example:



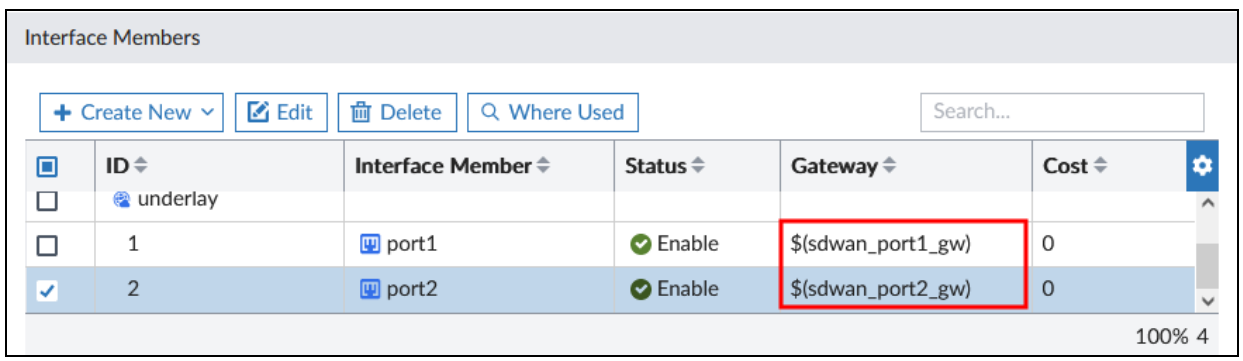
7. Click **OK** to save the settings.
8. In the **Gateway** field of **port1**, make sure that you select the **$(sd_wan_port1_gw)** metadata variable you configured.



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

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

The **Interface Members** section of your template should look similar to the following example:



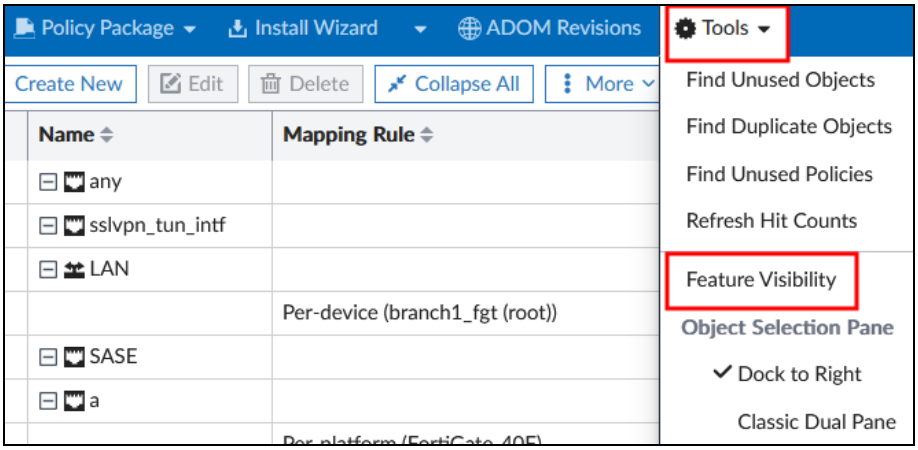
11. Click **OK** to save the template settings.

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

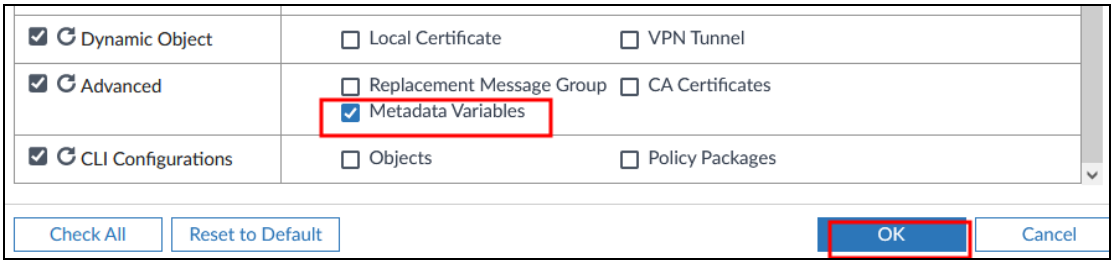
To review, edit, and update metadata variables

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

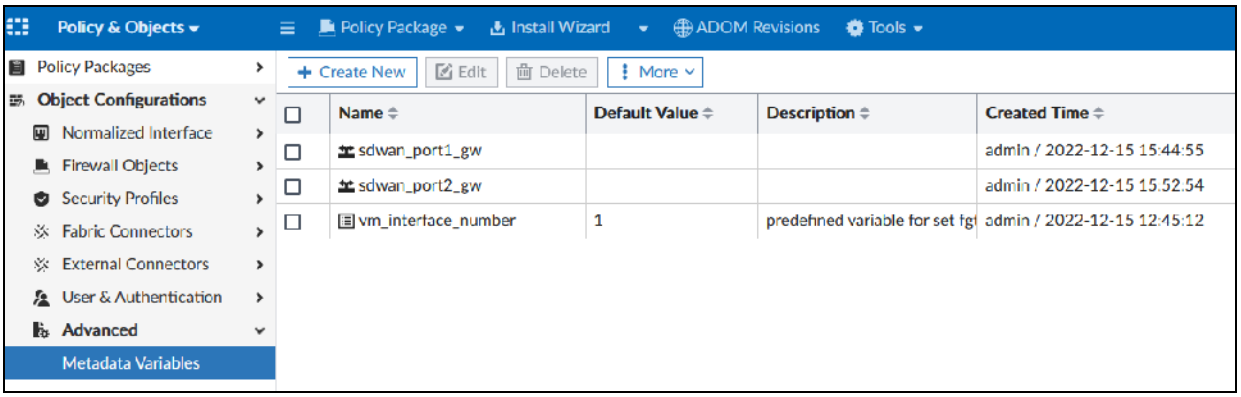
1. Continuing on the FortiManager GUI, click **Device Manager** > **Policy & Objects**.
2. Select **Tools** > **Feature Visibility**.



3. In the **Advanced** section, select the **Metadata Variables** checkbox.
4. Click **OK** to validate the change.



You can now manage metadata variables by clicking **Object Configurations** > **Advanced** > **Metadata Variables**.



If you upgrade FortiManager from version 7.0 to version 7.2, the meta fields configured are automatically converted to metadata variables. For reference, you can view meta fields by clicking **System settings** > **Advanced**.

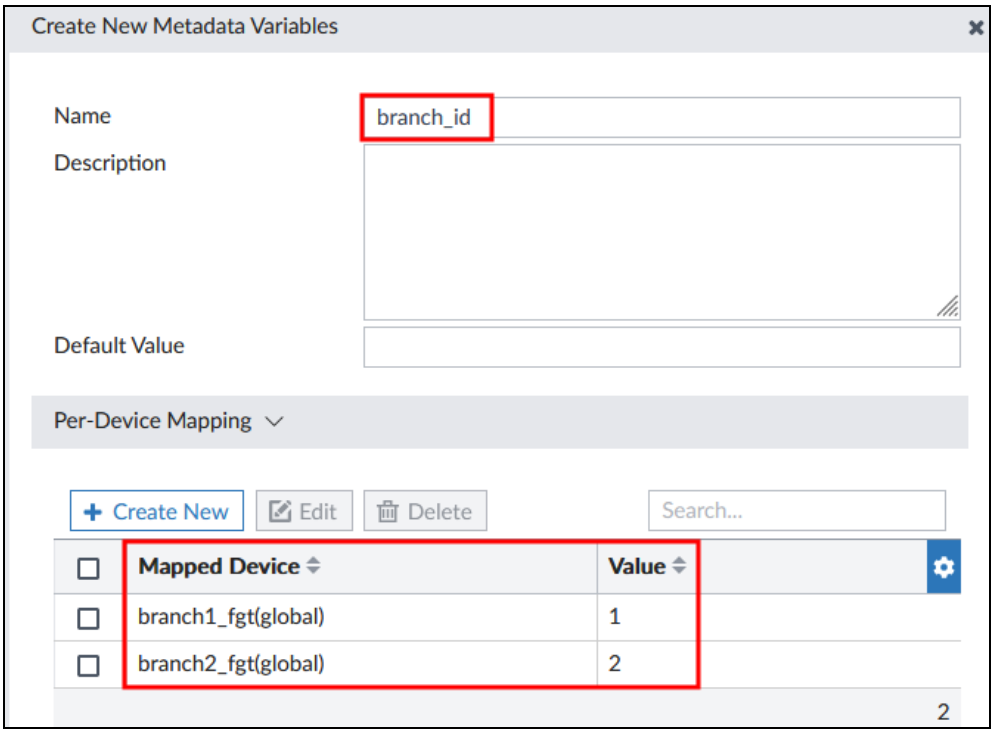
To configure branch_id and Branch_Local_Subnet metadata variables

You will create a metadata variable to assign a branch ID to each branch device. This metadata variable will be used later in this lab.

1. Continuing on the FortiManager GUI, click **Object Configurations** > **Advanced** > **Metadata Variables**.
2. Click **Create New** to create a new metadata variable.
3. In the **Name** field, type `branch_id`.
4. Expand the **Per-Device Mapping** section.
5. Configure the following settings to create branch ID entries for branch1_fgt and branch2_fgt:

Field	Value
Mapped Device	branch1_fgt (global)
Value	1
Mapped Device	branch2_fgt (global)
Value	2

Your page should look like the following example:



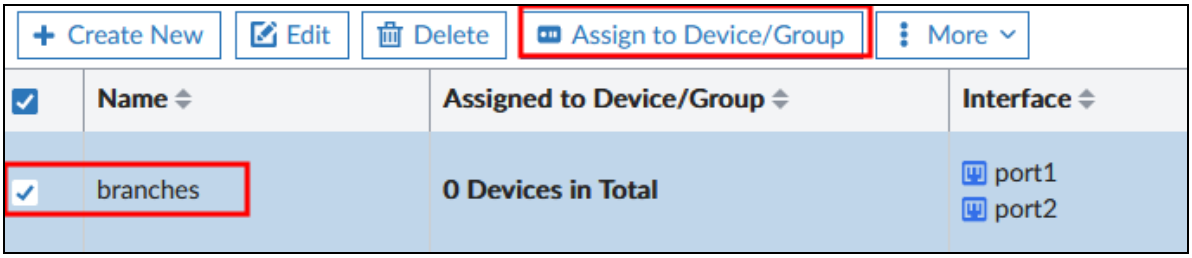
6. Click **OK** to save the settings.
7. Repeat the procedure to create Branch_Local_Subnet metadata variable with the following settings:

Field	Value
Name	Branch_Local_Subnet
Per-Device Mapping	**Mapped Device** / **Value** branch1_fgt(root) / 10.0.1.0/24 branch2_fgt(root) / 10.0.2.0/24

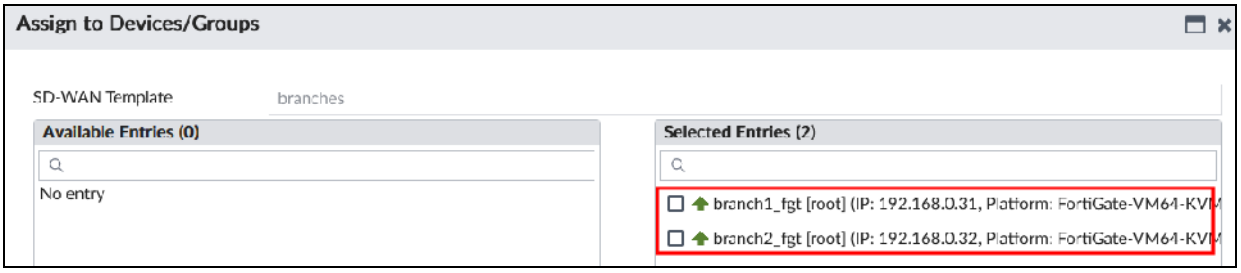
8. Click **OK** to save the settings.

To configure branch1_fgt and branch2_fgt as template targets

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



3. Move **branch1_fgt** and **branch2_fgt** to the **Selected Entries** list.



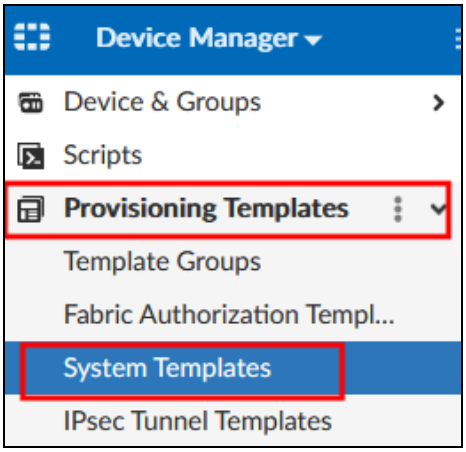
4. Click **OK** to save the settings.

Configure the Device Settings and Policy Package

First, you will configure a system template for enabling FortiAnalyzer logging on both branch1_fgt and branch2_fgt. After that, you will configure a static default route for the underlay zone on branch2_fgt. Then, you will edit a firewall address object for branch2_fgt. Finally, you will add branch2_fgt as a target for the **branches_pp** policy package you imported from branch1_fgt.

To configure FortiAnalyzer logging

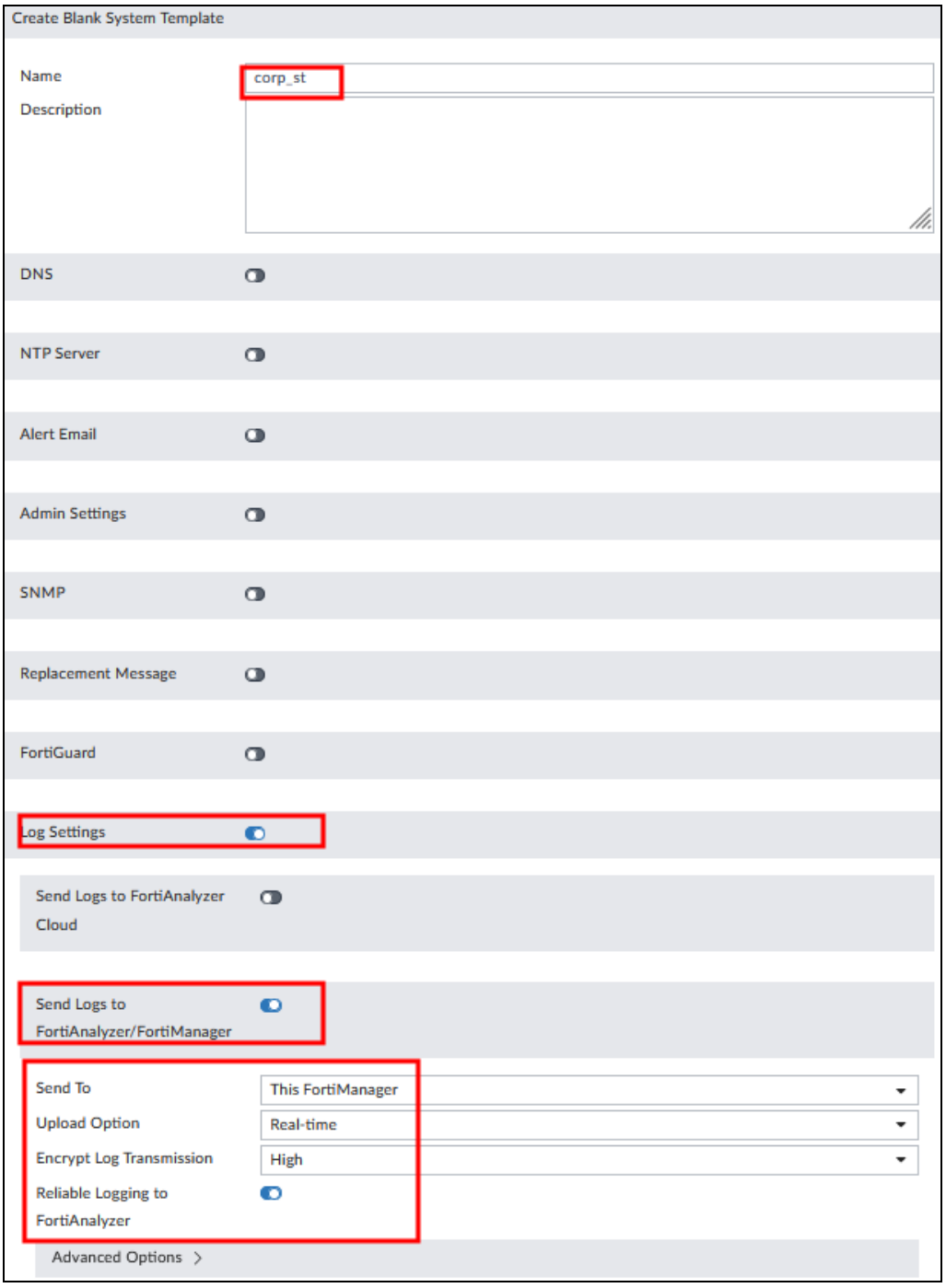
1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **System Templates**.



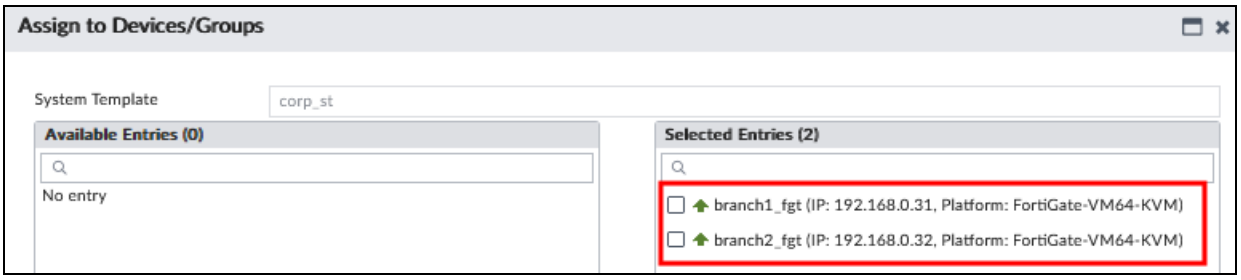
2. Click **Create New** > **Blank Template**.
3. In the **Name** field, type `corp_st`.
4. Enable **Log Settings**, and then enable the second setting, which is **Send Logs to FortiAnalyzer/FortiManager**.
5. Configure the following settings:

Field	Value
Send to	This FortiManager
Upload Option	Select **Real-time**.
Encrypt Log Transmission	High

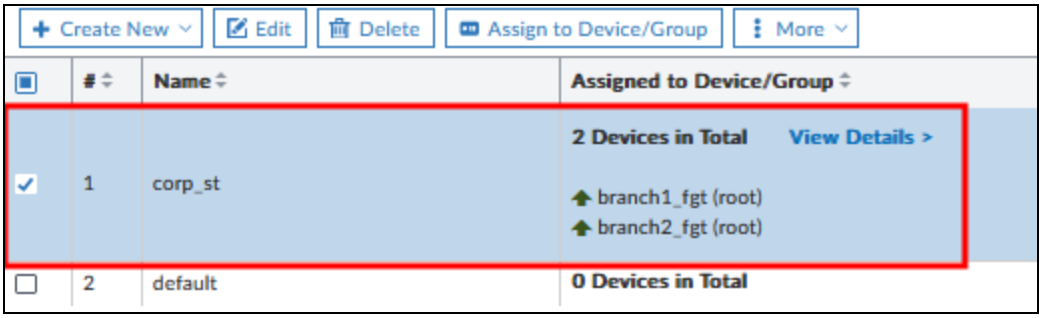
Field	Value
Reliable Logging to FortiAnalyzer	Enabled



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



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

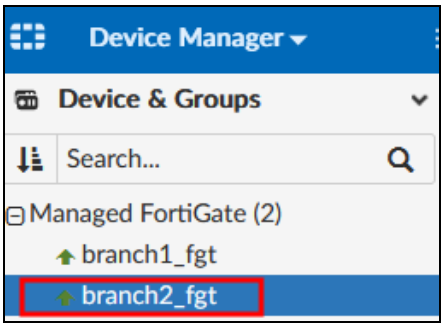


To install the device settings

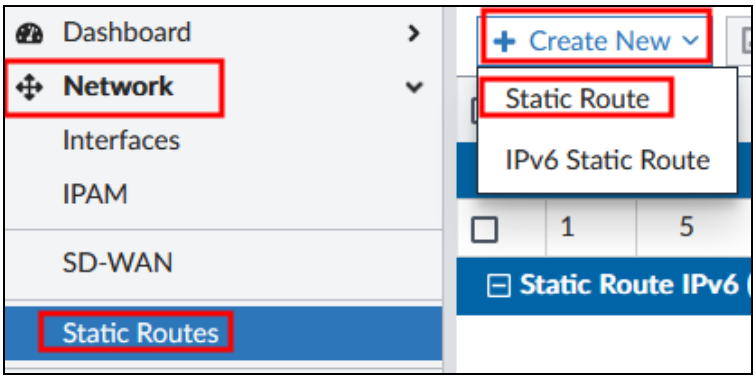
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on all devices.
5. Wait for the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

To configure a static default route on branch2_fgt

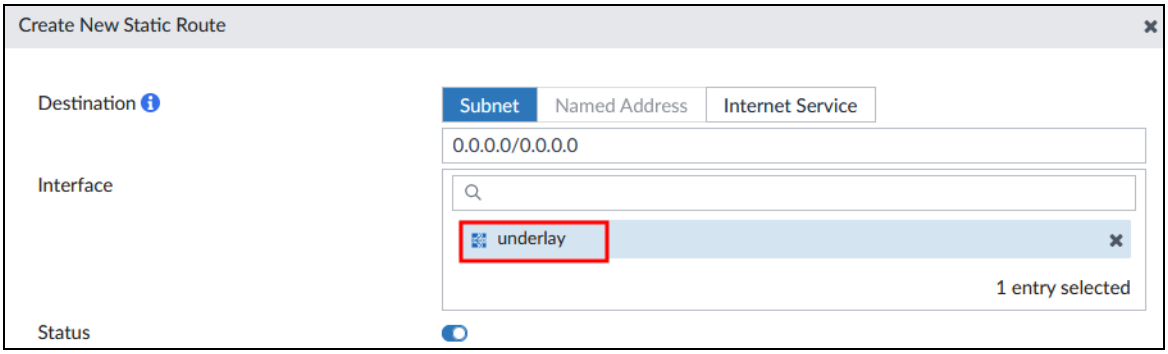
1. Continuing on the FortiManager GUI, click **Device & Groups** > **Device & Groups**, expand **Managed FortiGate**, and then click **branch2_fgt**.



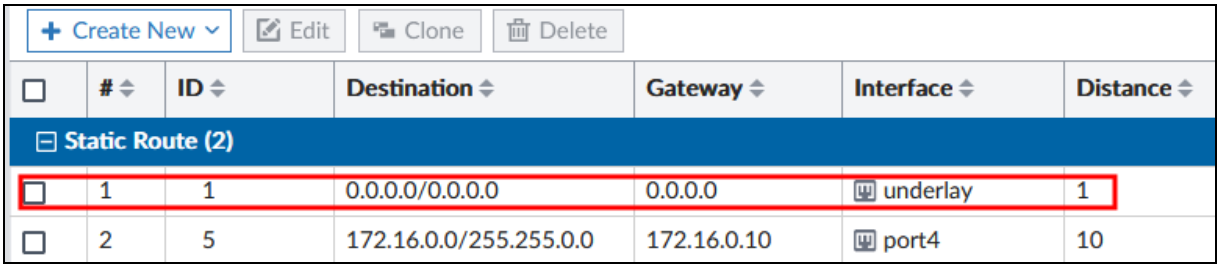
2. Click **Network** > **Static Route**, and then click **Create New** > **Static Route**.



3. In the **Destination** field, keep the default value.
4. In the **Interface** field, select **underlay**.

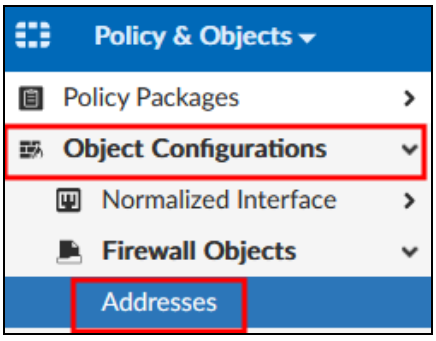


5. Click **OK** to save the settings.
   Your page should look similar to the following example:



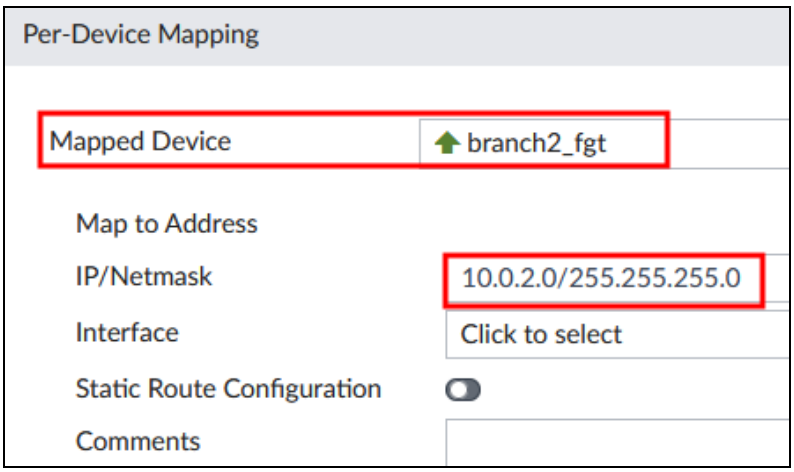
To edit the firewall address object

1. Continuing on the FortiManager GUI, click **Device Manager** > **Policy & Objects**.
2. Click **Object Configurations**, and then click **Firewall Objects** > **Addresses**.



3. Double-click the **LAN-net** address object, and then configure the following settings:

Field	Value
Per-Device Mapping	Expand this section.
Per-Device Mapping table	Click **Create New**, and then configure the following settings: 1. In the **Mapped Device** field, select **branch2_fgt**. 2. In the **Map to Address IP/Netmask** field, type `10.0.2.0/24`. 3. Click **OK** to save the per-device mapping.

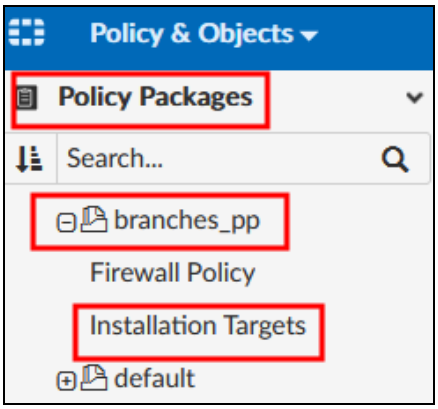


4. Click **OK** to save the settings.

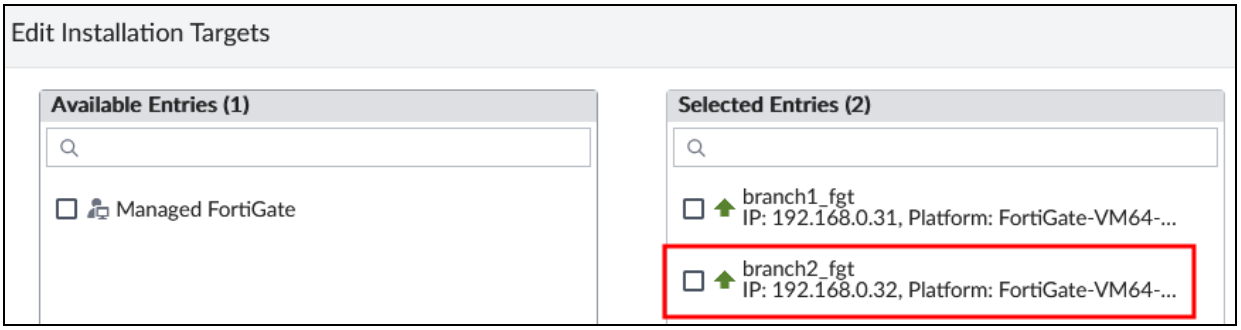
LAN-net is now a dynamic firewall address object. You added a per-device mapping rule that FortiManager uses when it pushes the object to the managed devices. The goal is for FortiManager to use the correct value based on the target device.

To add branch2_fgt as a policy package target

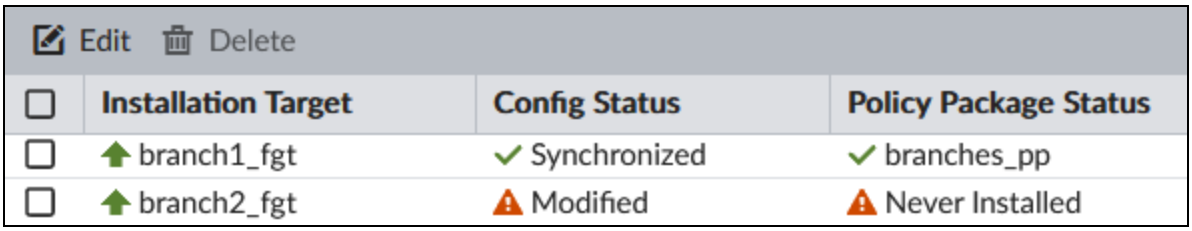
1. Continuing on the FortiManager GUI, click **Policy Packages**, expand **branches_pp**, and then click **Installation Targets**.



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



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

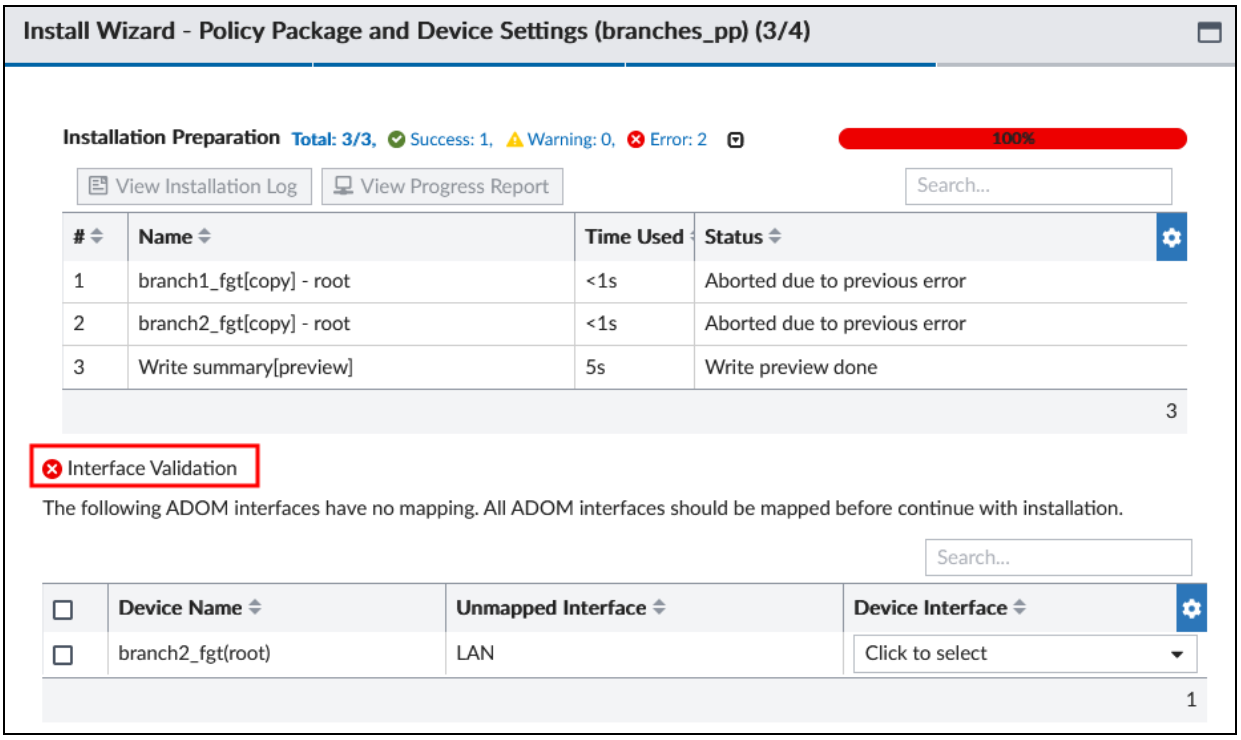


Install the Device Settings and Policy Package

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

To install the device settings and policy package

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

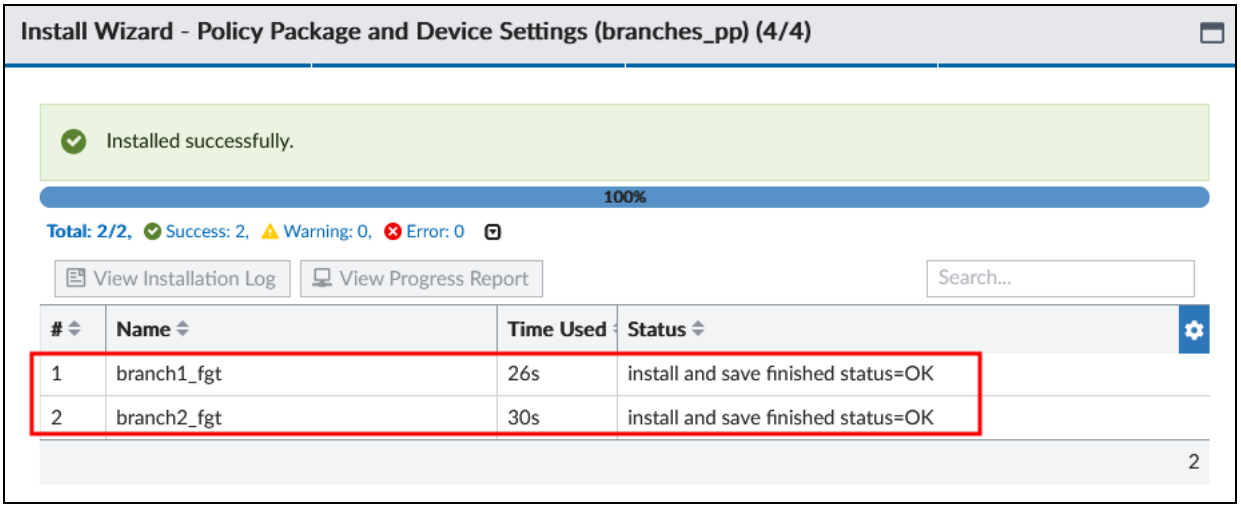


Stop and think!

Why is FortiManager showing this page?

The policy package references the LAN normalized interface. The normalized interface doesn't have a mapping configured for branch2_fgt, which is why FortiManager requires you to configure it.

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



8. Click **Finish**.

Verify Installed Settings and Logging

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

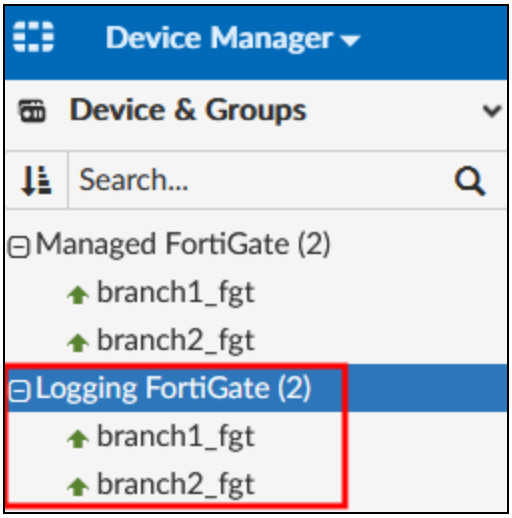
To verify installed settings on branch1_fgt and branch2_fgt

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

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

To verify logging to FortiAnalyzer (FortiManager)

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Device Manager**.
2. Expand **Logging FortiGate**.



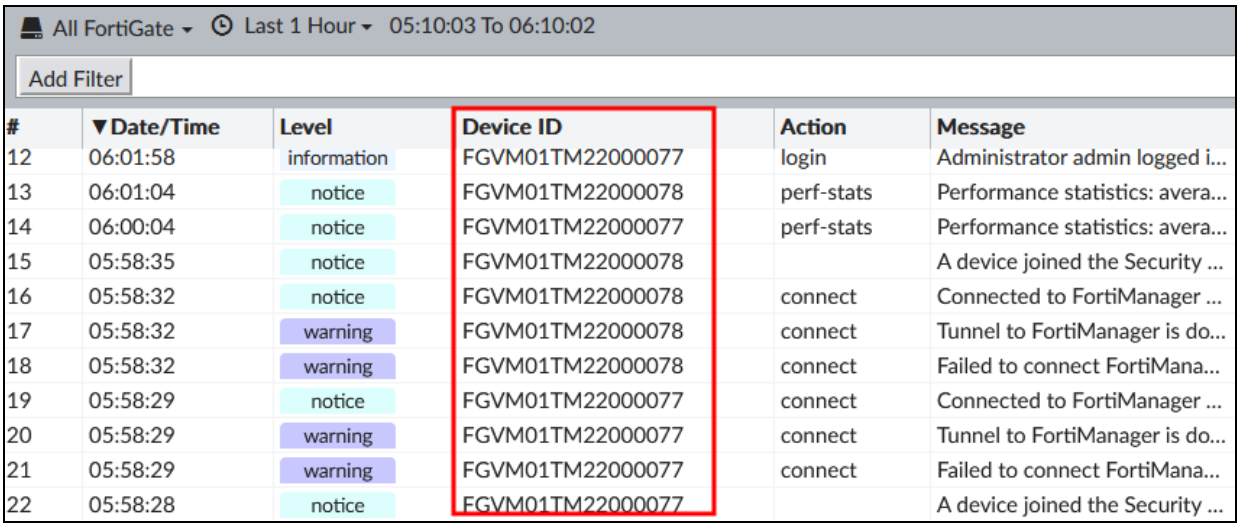
Your page should look similar to the following example:

	Device Name	IP Address	Platform	Logs
☐	branch1_fgt	192.168.0.31	FortiGate-VM64-KVM	Real Time
☐	branch2_fgt	192.168.0.32	FortiGate-VM64-KVM	Real Time

You can drag and drop the columns to reorder them.

The green circle beside **Real Time** indicates that FortiManager is receiving logs from the managed devices.

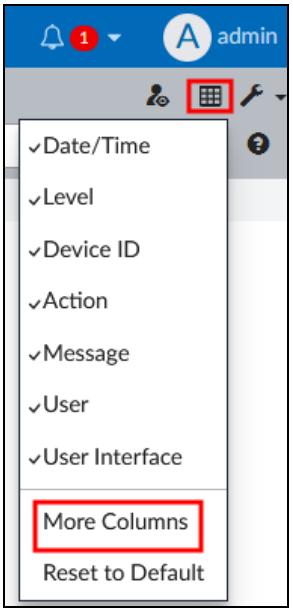
3. Click **Device Manager** > **Log View**, and then click **Event** > **All Types**.
   Your page should look similar to the following example:



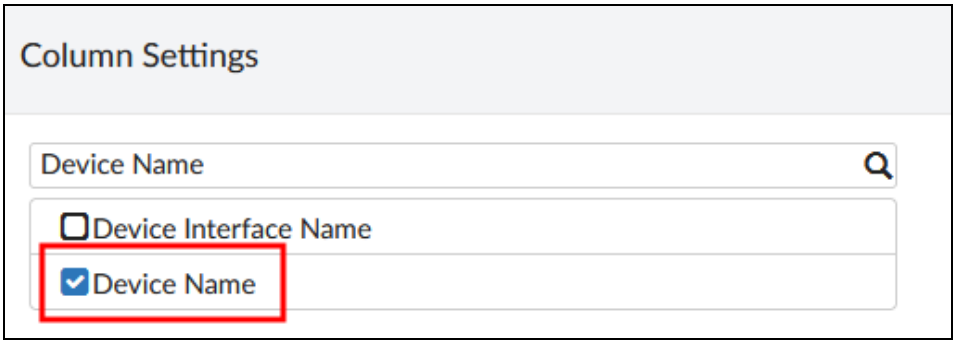
#	▼Date/Time	Level	Device ID	Action	Message
12	06:01:58	information	FGVM01TM22000077	login	Administrator admin logged i...
13	06:01:04	notice	FGVM01TM22000078	perf-stats	Performance statistics: avera...
14	06:00:04	notice	FGVM01TM22000077	perf-stats	Performance statistics: avera...
15	05:58:35	notice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

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

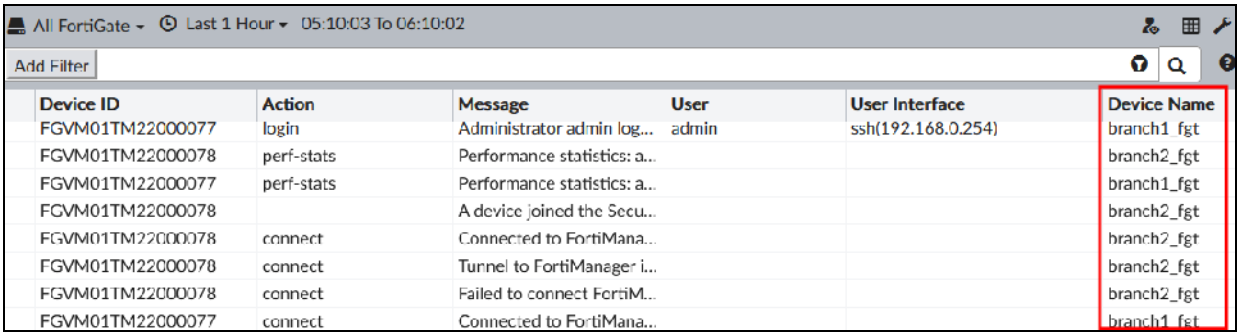
4. In the upper-right corner, click the column setting icon, and then click **More Columns**.



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



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



The logs now include the device name for easier identification.

You can drag and drop the columns to reorder them.

Exercise 2: Monitoring DIA Traffic on FortiManager

In this exercise, you will first generate internet traffic from branch1_client and branch2_client. After that, you will monitor DIA traffic distribution and logs using the SD-WAN tools available on FortiManager.

Generate Internet Traffic From branch1_client and branch2_client

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

To generate internet traffic from branch1_client and branch2_client

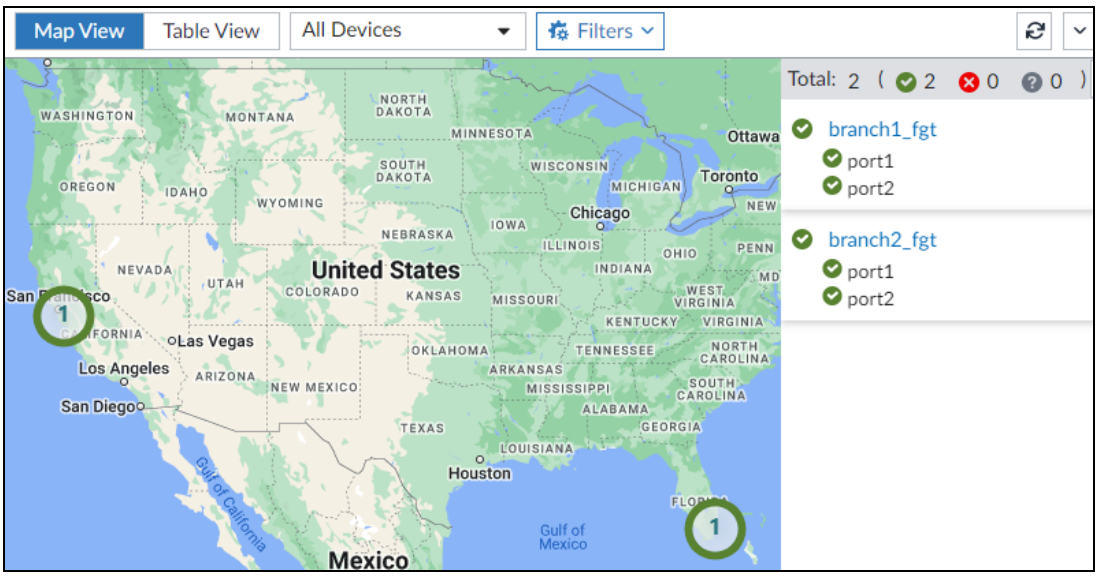
1. Open an SSH session to branch1_client.
2. Log in with the username `root` and password `password`.
3. Enter the following commands:
   ```
   cd /fortipoc/fit/
   ./myfit.sh
   ```
4. Repeat the previous steps on branch2_client.

Monitor DIA Traffic Distribution

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

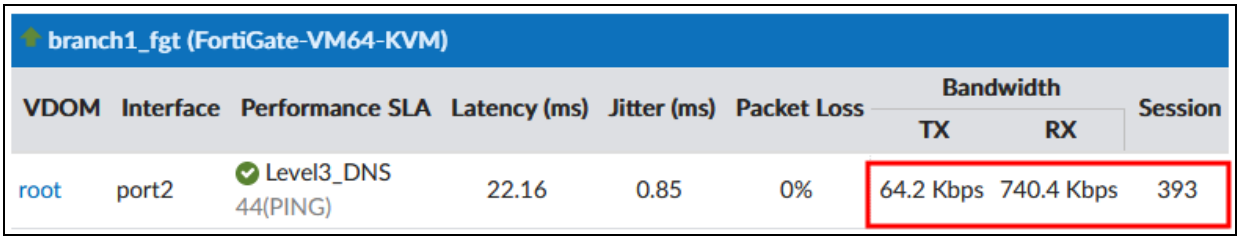
To monitor DIA traffic distribution

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Monitors** > **SD-WAN Monitor**.
   Your page should look similar to the following example:

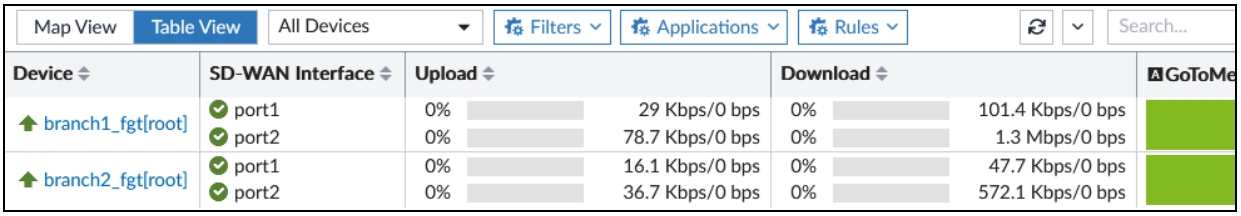


- branch1_fgt and branch2_fgt are located in Sunnyvale and Miami, respectively.
- You may need to zoom out before you can see the managed devices on the map.

3. Hover over the ports on both branch1_fgt and branch2_fgt.
   Your page should display additional details for each port. The following image shows an example of port2 on branch1_fgt:



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



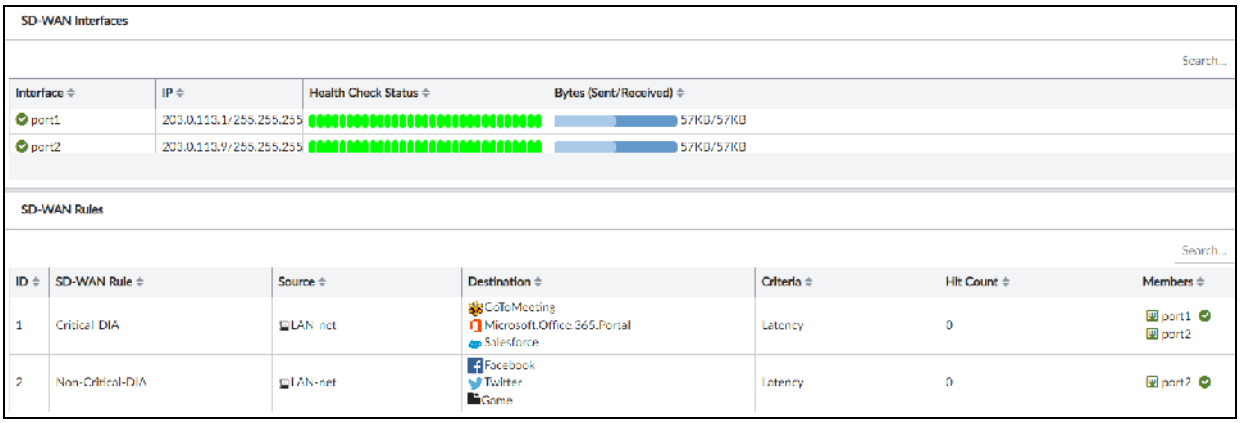
Stop and think!

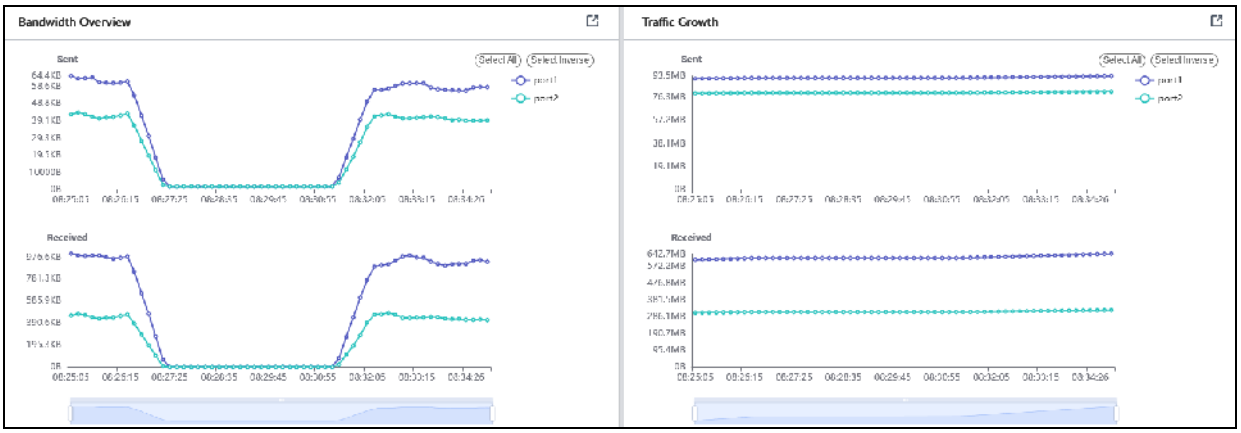
The port details show bandwidth is utilized, and that the member has active sessions. However, the upload and download utilization bars show 0% for both FortiGate devices.

Why?

The usage percentage that appears on the bars is calculated based on the `estimated-upstream-bandwidth` and `estimated-downstream-bandwidth` settings, which you haven't configured yet. Because those settings are not configured, FortiManager doesn't know the bandwidth capacity of the ports, and therefore, is unable to determine the usage percentage.

5. Click **branch2_fgt** to view more details about the device.
   Your page should look similar to the following example:





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

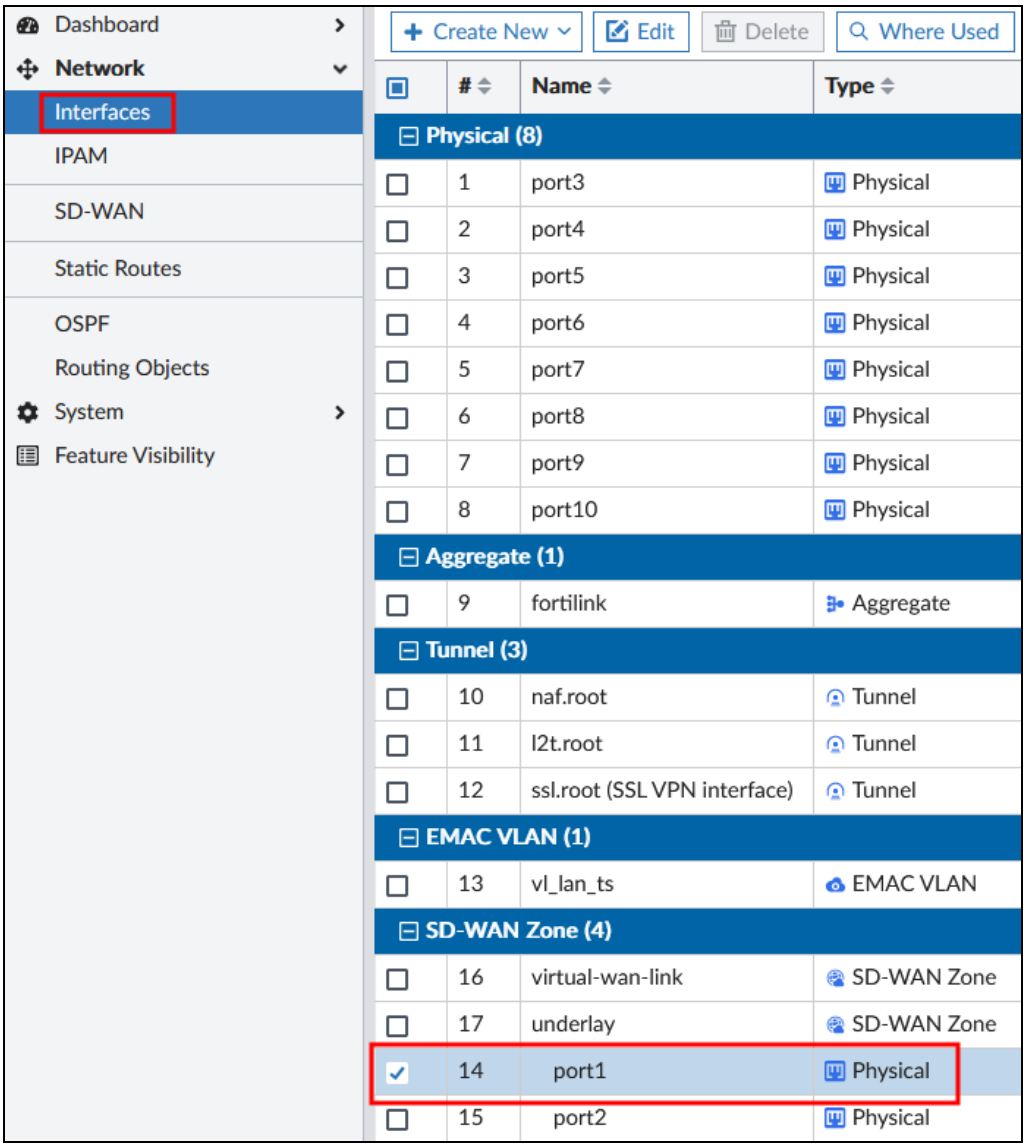
You can hover over the graphs to view more details.

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

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

To configure the estimated bandwidth settings

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



3. Configure the following settings:

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

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

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

4. Click **OK** to save the settings.
5. Click **OK** to validate the warning message about normalized interface mapping.
6. Repeat the previous procedure to configure the estimated bandwidth values on port2 on branch1_fgt, and on port1 and port2 on branch2_fgt.
   Use `10240` Kbps for all ports.

To install the device settings

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

To monitor member bandwidth utilization

Take the Expert Challenge!

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

Device	SD-WAN Interface	Upload		Download	
branch1_fgt[root]	port1	0%	30 Kbps/10.2 Mbps	1%	104.9 Kbps/10.2 Mbps
	port2	1%	79.8 Kbps/10.2 Mbps	13%	1.3 Mbps/10.2 Mbps
branch2_fgt[root]	port1	0%	32.2 Kbps/10.2 Mbps	1%	106.5 Kbps/10.2 Mbps
	port2	1%	79.5 Kbps/10.2 Mbps	13%	1.3 Mbps/10.2 Mbps

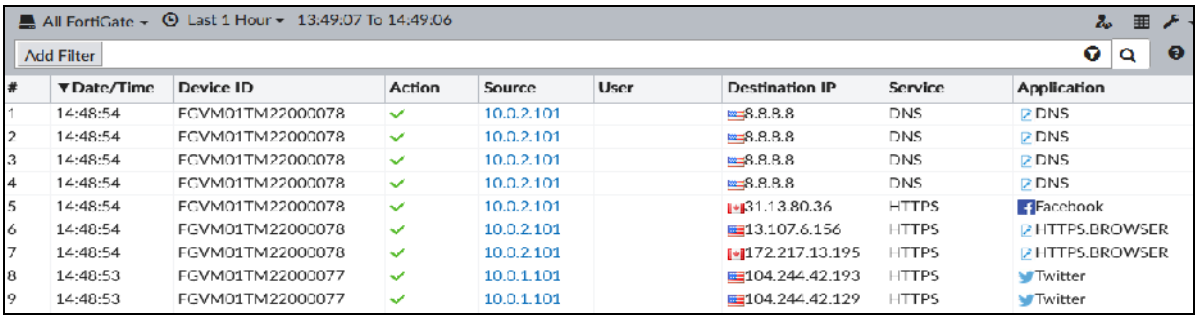
If you require assistance, or to verify your work, review the procedure described previously in this exercise.

View Traffic Logs

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

To view SD-WAN traffic logs

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



#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application
1	14:48:54	FGVM01TM22000078	✓	10.0.2.101		8.8.8.8	DNS	DNS
2	14:48:54	FGVM01TM22000078	✓	10.0.2.101		8.8.8.8	DNS	DNS
3	14:48:54	FGVM01TM22000078	✓	10.0.2.101		8.8.8.8	DNS	DNS
4	14:48:54	FGVM01TM22000078	✓	10.0.2.101		8.8.8.8	DNS	DNS
5	14:48:54	FGVM01TM22000078	✓	10.0.2.101		31.13.80.36	HTTPS	Facebook
6	14:48:54	FGVM01TM22000078	✓	10.0.2.101		13.107.6.156	HTTPS	HTTPS.BROWSER
7	14:48:54	FGVM01TM22000078	✓	10.0.2.101		172.217.13.195	HTTPS	HTTPS.BROWSER
8	14:48:53	FGVM01TM22000077	✓	10.0.1.101		104.244.42.193	HTTPS	Twitter
9	14:48:53	FGVM01TM22000077	✓	10.0.1.101		104.244.42.129	HTTPS	Twitter

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

2. In the upper-right corner, click the column setting icon, and then click **More Columns**.

3. Select **Destination Interface**, **SD-WAN Quality**, and **SD-WAN Rule Name**.

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

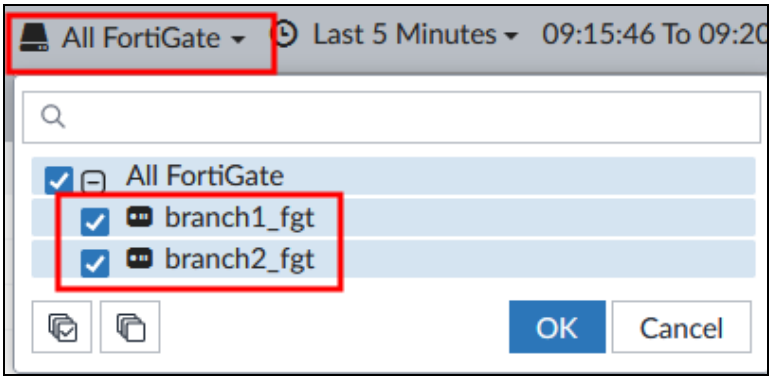
4. Click **OK** to save the settings.

Your page should look similar to the following example:

Application	Sent/Received	Security Event List	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
Salesforce	1.9 KB/25.9 ...	APP 2	port1	Seq_num(1 port1),...	Critical-DIA
Microsoft.Office.365.Portal	1.6 KB/48.3 ...	APP 1	port1	Seq_num(1 port1),...	Critical-DIA
Twitter	2.2 KB/46.8 ...	APP 2	port2	Seq_num(2 port2),...	Non-Critical-DIA
Twitter	1.3 KB/4.7 KB	APP 2	port2	Seq_num(2 port2),...	Non-Critical-DIA
Facebook	1.9 KB/27.0 ...	APP 2	port2	Seq_num(2 port2),...	Non-Critical-DIA
Facebook	2.0 KB/26.9 ...	APP 2	port2	Seq_num(2 port2),...	Non-Critical-DIA
DNS	120.0 B/348....		port2		
DNS	118.0 B/162....		port2		

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

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



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

Exercise 3: Configuring an IPsec VPN Using the FortiManager IPsec Recommended Templates

In this exercise, you will configure a hub-and-spoke dial-up IPsec VPN between branch1_fgt, branch2_fgt, and dc1_fgt, using FortiManager IPsec recommended templates. You will configure dc1_fgt as a hub, and the other two FortiGate devices as spokes. You will do the following:

1. Add dc1_fgt to FortiManager.
2. Configure object mappings for dc1_fgt.
3. Create a VPN IPsec hub and spoke configuration with recommended templates.
4. Create a CLI template for advanced IPsec parameters.
5. Install the VPN configuration.
6. Map the VPN interfaces.
7. Configure the firewall policies.
8. Configure static routes for the branches.
9. Configure FortiAnalyzer logging for dc1_fgt.
10. Install the remaining configuration on devices.
11. Verify that the tunnels come up.

Add dc1_fgt to FortiManager

You will add the dc1_fgt FortiGate to FortiManager.

To add dc1_fgt to FortiManager

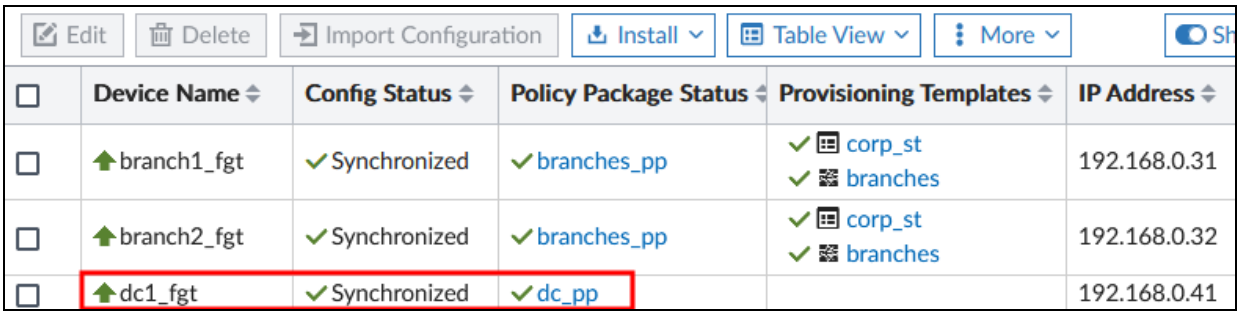
1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Add Device**.

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

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

4. Click **Next**.
5. Click **Next**, and then wait until the **Add Device** task is completed.

6. Click **Import Now**.
7. Select **Import Policy Package**, and then click **Next**.
8. In the **Policy Package Name** field, type `dc_pp`.
9. Click **Next**.
10. Click **Next**, and then wait until the **Import Device** task is completed.
11. Click **Finish**.
12. Click **Managed FortiGate** to display the list of managed devices.
    Your page should look similar to the following example:



Configure Mappings for dc1_fgt

You will configure a mapping on the LAN-net firewall address object for dc1_fgt. This mapping is required to define the protected networks during the VPN configuration. You will also configure a mapping for the LAN normalized interface.

To configure a firewall address object mapping for dc1_fgt

1. Continuing on the FortiManager GUI, click **Device Manager** > **Policy & Objects**.
2. Click **Object Configurations**, **Firewall Objects**, and then click **Addresses**.
3. Double-click the **LAN-net** address object.
4. In the **Per-Device Mapping** table, click **Create New**, and then do the following:
   a. In the **Mapped Device** field, select **dc1_fgt**.
   b. In the **Map to Address** > **IP/Netmask** field, type `10.1.0.0/24`.
   c. Click **OK** to save the settings.
5. Click **OK** to save the settings.

To configure a normalized interface mapping for dc1_fgt

1. Continuing on the FortiManager GUI, click **Object Configurations**, and then click **Normalized Interface** > **Normalized Interface**.
2. Double-click the **LAN** normalized interface to edit the entry.
3. In the **Per-Device Mapping** table, click **Create New**, and then do the following:
   a. In the **Mapped Device** field, select **dc1_fgt**.
   b. In the **Mapped Interface Name** field, select **port5**.
   c. Click **OK** to save the settings.

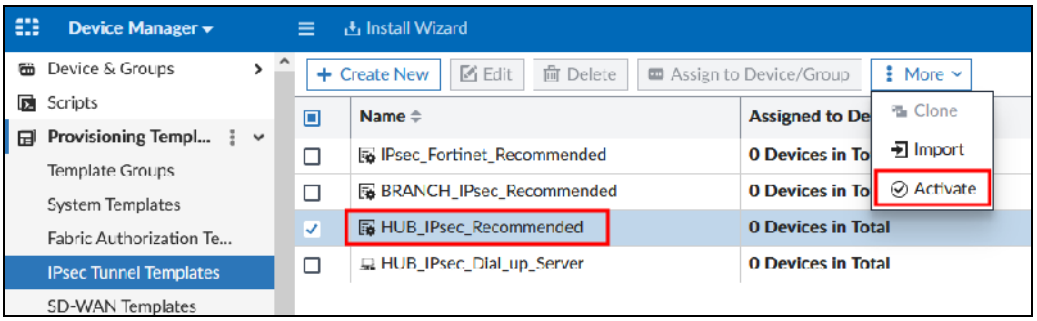
4. Click **OK** to save the settings.

Create VPN IPsec Hub and Spoke Configurations With Recommended Templates

You will use IPsec tunnel recommended templates to prepare a dial-up server for IPsec hub and IPsec configuration for branch devices.

To create an IPsec dial-up server hub template

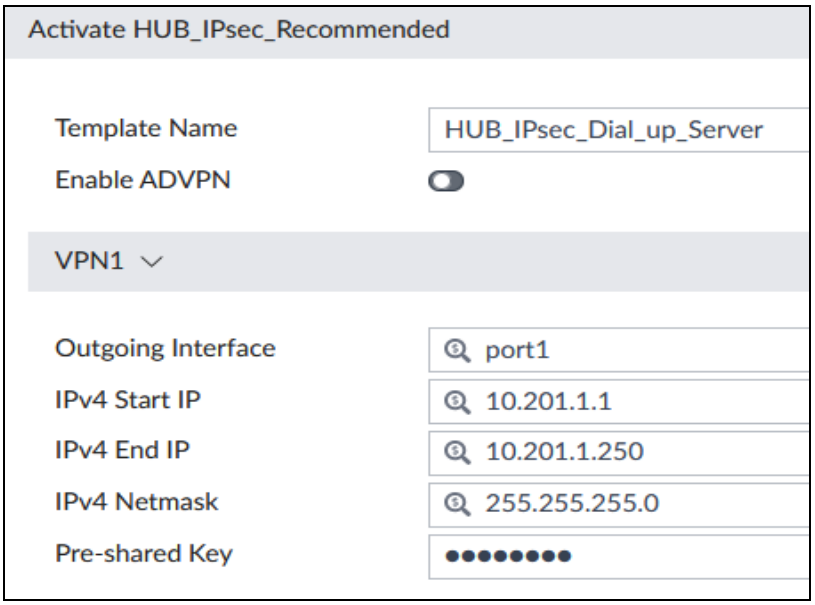
1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Device Manager** > **Provisioning Templates** > **IPsec Tunnel Templates**.
2. Select **HUB_IPsec_Recommended**.
3. Click **More** > **Activate** to start the template configuration wizard.



4. Configure the following settings:

Field	Value
Template Name	HUB_IPsec_Dial_up_Server
Outgoing Interface	port1
IPv4 Start IP	10.201.1.1
IPv4 End IP	10.201.1.250
IPv4 Netmask	255.255.255.0
Pre-shared Key	password

Your page should look similar to the following example:



5. Click **OK** to save the settings.
6. Edit the **HUB_IPsec_Dial_up_Server** template you created.
   It contains one VPN tunnel called **VPN1**—the template determines the default tunnel naming.
7. Double-click **VPN1**, and then edit the following settings:

Field	Value
Tunnel Name	T_INET_0
Advanced Options	Enable **add-route**.

8. Continuing on the **VPN1** menu, edit the following settings for the phase2:

Field	Value
Phase2 Name	T_INET_0
Keep Alive	Enable
Key Life	1800

9. Click **OK** to save the settings.
10. Click **OK**, and then click **Return** to return to the tunnel templates list.

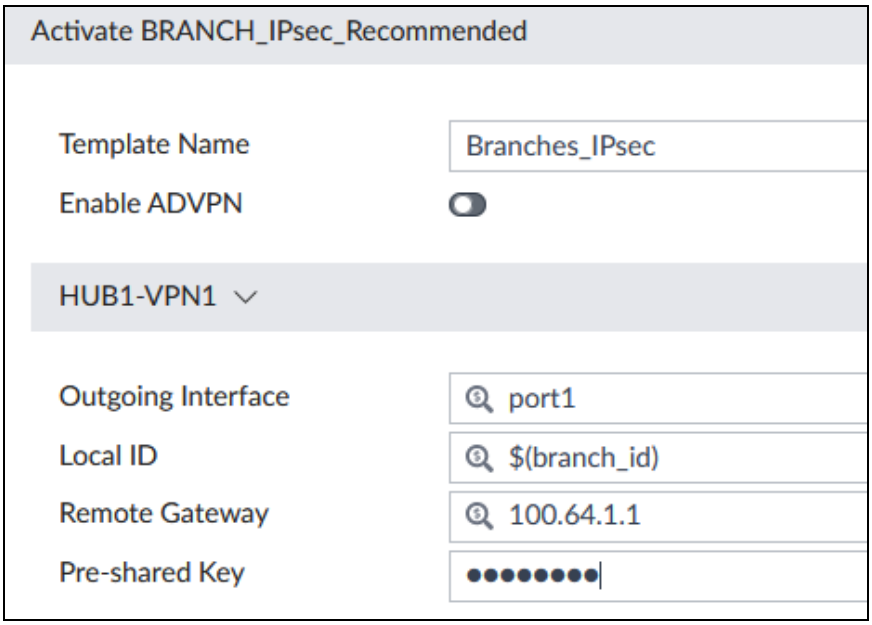
Note that you can apply only one IPsec tunnel template per device. However, if you want to configure multiple tunnels on one device, you can add tunnel instances to the template.

To create an IPsec tunnel template for branches

1. Select **BRANCH_IPsec_Recommended**.
2. Click **More** > **Activate** to start the template configuration wizard.
3. Configure the following settings:

Field	Value
Template Name	Branches_IPsec
Outgoing Interface	port1
Local ID	Type `$`, and then select the **branch_id** metadata variable.
Remote Gateway	100.64.1.1
Pre-shared Key	password

Your page should look similar to the following example:



4. Click **OK** to save the settings.
5. Edit the **Branches_IPsec** template you created.
   It contains one VPN tunnel called **HUB1-VPN1**.
6. Double-click **HUB1-VPN1**, and then edit the following settings for the phase1:

Field	Value
Tunnel Name	T_INET_0
Advanced Options	disable mode-cfg

7. Continuing on the **HUB1-VPN1** menu, edit the following settings for the phase2:

Field	Value
Phase2 Name	T_INET_0
Keep Alive	Enable
Key Life	1800

8. Click **OK** to save the settings.
9. Click **OK**, and then click **Return** to return to the tunnel templates list.

IPsec recommended templates are designed for a hub-and-spoke topology with dynamic routing. In this exercise, you will use a hub-and-spoke topology with static routing. This requires the adjustment of the `mode-cfg` and `add-route` advanced options.

To assign a tunnel template to devices

1. Select the **HUB_IPsec_Dial_up_Server** template.
2. Click **Assign to Device/Group**.
3. Select **dc1_fgt [root]**, and then click **OK** to validate.
4. Select the **Branches_IPsec** template.
5. Click **Assign to Device/Group**.
6. Select **branch1_fgt [root]** and **branch2_fgt [root]**.
7. Click **OK** to validate.

Create a CLI Template for Advanced IPsec Parameters

You will use a CLI template to define the local subnet as a phase2 source subnet. Because the local subnet is different on each device, you will use metadata variables.

To create a CLI template

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Device Manager**, and then click **Provisioning Templates** > **CLI Templates**.
2. Click **Create New** > **CLI Template**.
3. Update the following settings:

Field	Value
Template Name	IPsec_P2_advanced
Type	CLI Script

Field	Value

Script details	Type the following commands:
	`config vpn ipsec phase2-interface`
	`  edit T_INET_0`
	`  set src-subnet $(Branch_Local_Subnet)`
	`  next`
	`end`

4. Click **OK** to validate.

For the CLI script, when you type `$`, FortiManager automatically lists the available metadata variables. You can then select `Branch_Local_Subnet` in the list.

5. Select the **IPsec_P2_advanced** template, and then assign it to branch1_fgt and branch2_fgt.

Install the VPN Configuration

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

To install the VPN configuration on branch1_fgt, branch2_fgt, and dc1_fgt

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**.
3. Click **Next**.
4. Confirm that **branch1_fgt**, **branch2_fgt**, and **dc1_fgt** are selected, and then click **Next**.
5. Click **Install Preview** to see the changes that will be applied to the FortiGate devices.
6. On the **Install Preview** page, click **Close**.
7. Click **Install**.
   Wait until the installation finishes.
8. Click **Finish**.

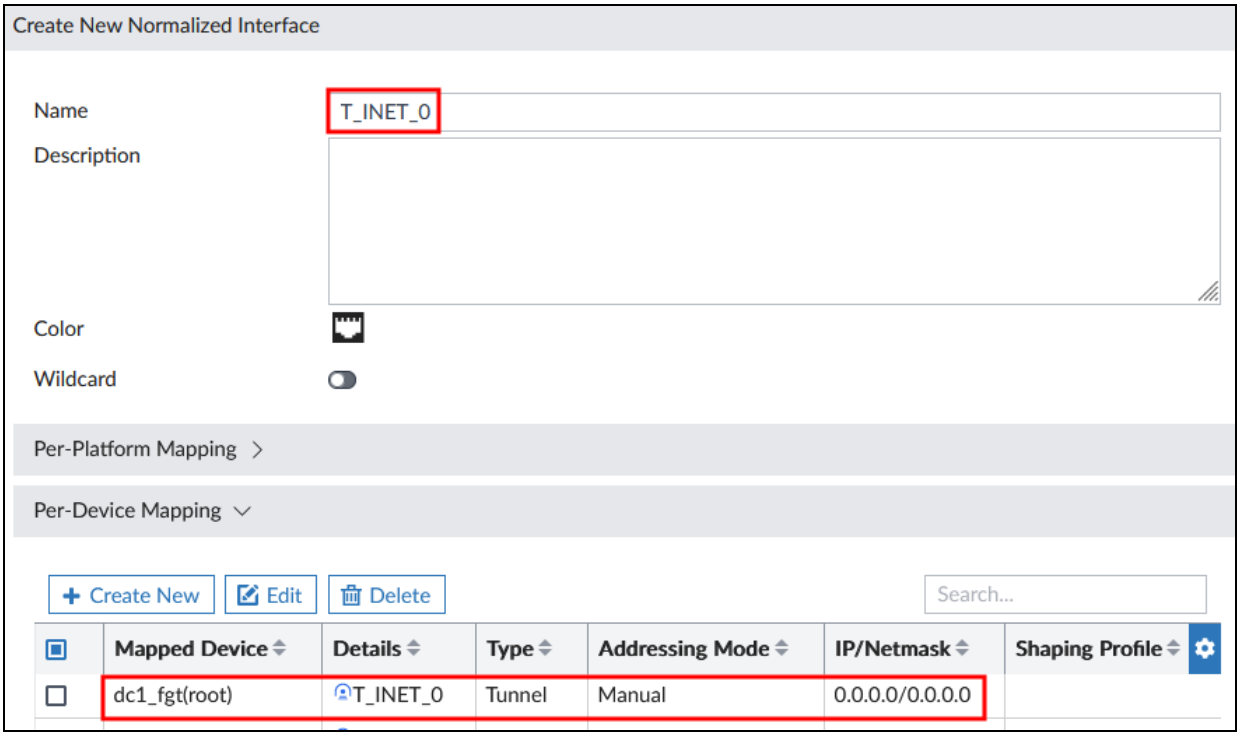
Map the VPN Interfaces

Now that you have installed the VPN configuration on all the FortiGate devices, you will map the VPN interfaces to a dynamic interface on FortiManager.

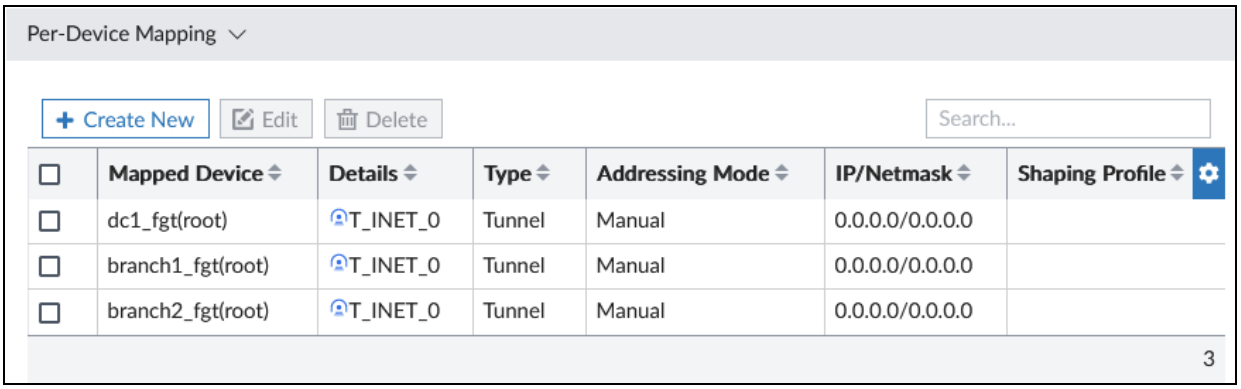
To map the VPN interfaces

1. Continuing on the FortiManager GUI, click **Device Manager** > **Policy & Objects** > **Object Configurations**.
2. Click **Normalized Interface** > **Normalized Interface**.
3. Click **Create New**.

4. In the **Name** field, type `T_INET_0`.
5. In the **Per-Device Mapping** section, click **Create New**, and then in the **Mapped Device** field, select **dc1_fgt**.
6. In the **Mapped Interface Name** field, select **T_INET_0**, and then click **OK**.



7. Repeat the previous steps to add the **T_INET_0** per-device mapping for branch1_fgt and branch2_fgt.
Your page should look similar to the following example:



8. After you add the VPN interfaces mapping for all three FortiGate devices, click **OK** to validate the settings.

Configure the Firewall Policies

After you map the VPN interfaces, you can configure the firewall policies to allow IPsec traffic to pass.

You will configure the following firewall policies on the branches:

- Allow traffic from the branch to dc1_fgt
- Allow traffic from dc1_fgt to the branch

You will configure the following firewall policies on dc1_fgt:

- Allow traffic from the branches to dc1_fgt
- Allow traffic from dc1_fgt to the branches
- Allow traffic between the branches

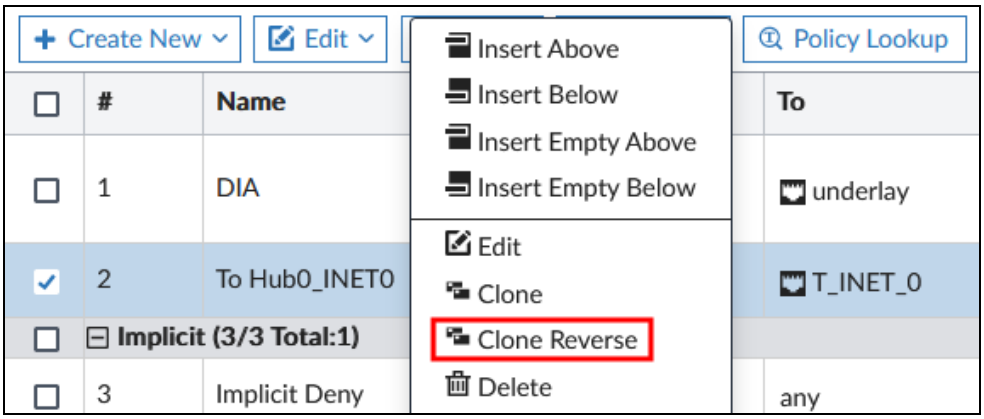
Because the branches share the same policy package, you will create the firewall policies in one policy package (**branches_pp**). Similarly, you will configure firewall policies for dc1_fgt in the **dc_pp** policy package. Then, you will push the changes to all FortiGate devices.

To configure the firewall policies on the branches

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

Field	Value
Name	To Hub0-INET0
Incoming Interface	LAN
Outgoing Interface	T_INET_0
Source	LAN-net
Destination	all
Service	ALL
Schedule	always
Action	Accept
Inspection-Mode	Flow-based
NAT	Disable
Logging Options	Enable **Log Allowed Traffic**, and then select **All Sessions**.

5. Click **OK**.
6. Right-click the **To Hub0_INET0** policy you created, and then select **Clone Reverse** to create a similar policy in the reverse direction.



7. Double-click the policy that the clone reverse function created, and then in the **Name** field, type **From Hub0-INET0**.
8. Ensure that the policy has the following settings:

Field	Value
Name	From Hub0-INET0
Incoming Interface	T_INET_0
Outgoing Interface	LAN
Source	all
Destination	LAN-net
Service	ALL
Schedule	always
Action	Accept
Inspection-Mode	Flow-based
NAT	Disable
Logging Options	Enable **Log Allowed Traffic**, and then select **All Sessions**.

9. Click **OK**.

To configure the firewall policies on dc1_fgt

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

Field	Value
Name	To Branch-INET0
Incoming Interface	LAN
Outgoing Interface	T_INET_0
Source	LAN-net
Destination	all
Service	ALL
Schedule	always
Action	Accept
Inspection Mode	Flow-based
NAT	Disable
Logging Options	Enable **Log Allowed Traffic**, and then select **All Sessions**.

5. Click **OK**.
6. Right-click the **To Branch-INET0** policy you created, and then select **Clone Reverse** to create a similar policy in the reverse direction.
7. Double-click the policy that the clone reverse function created, and then in the **Name** field, type **From Branch-INET0**.
8. Ensure that the policy has the following settings:

Field	Value
Name	From Branch-INET0
Incoming Interface	T_INET_0
Outgoing Interface	LAN
Source	all
Destination	LAN-net
Service	ALL
Schedule	always
Action	Accept
Inspection Mode	Flow-based
NAT	Disable
Logging Options	Enable **Log Allowed Traffic**, and then select **All Sessions**.

9. Click **OK**.
10. Click **Create New** again.
11. Configure the following settings:

Field	Value
Name	Branch to Branch-INET0
Incoming Interface	T_INET_0
Outgoing Interface	T_INET_0
Source	all
Destination	all
Service	ALL
Schedule	always
Action	Accept
Inspection Mode	Flow-based
NAT	Disable
Logging Options	Enable **Log Allowed Traffic**, and then select **All Sessions**.

12. Click **OK**.

Configure a Static Route on the Branches

You will configure a static route for the VPN traffic on the branches. You don't need to configure static routes on dc1_fgt because these will be automatically installed by IKE after the tunnel comes up.

To configure a static route on branch1_fgt

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Device Manager** > **Device & Groups**, expand **Managed FortiGate**, and then click **branch1_fgt**.
2. Click **Network** > **Static Routes**, and then click **Create New** > **Static Route**.
3. Configure the following settings:

Field	Value
Destination	Click **Subnet**, and then type `10.0.0.0/8`.
Interface	Select **T_INET_0**.

4. Click **OK** to save the settings.
5. Repeat the same procedure to add the same static route for branch2_fgt.

Configure FortiAnalyzer Logging on dc1_fgt

You will add dc1_fgt as a target in the **corp_st** system template you configured for the branches.

To configure FortiAnalyzer logging on dc1_fgt

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **System Templates**.
2. Select **corp_st**, and then click **Assign to Device/Group**.
3. Move **dc1_fgt** to the **Selected Entries** list.
4. Click **OK** to save the settings.

Install the Configuration on Devices

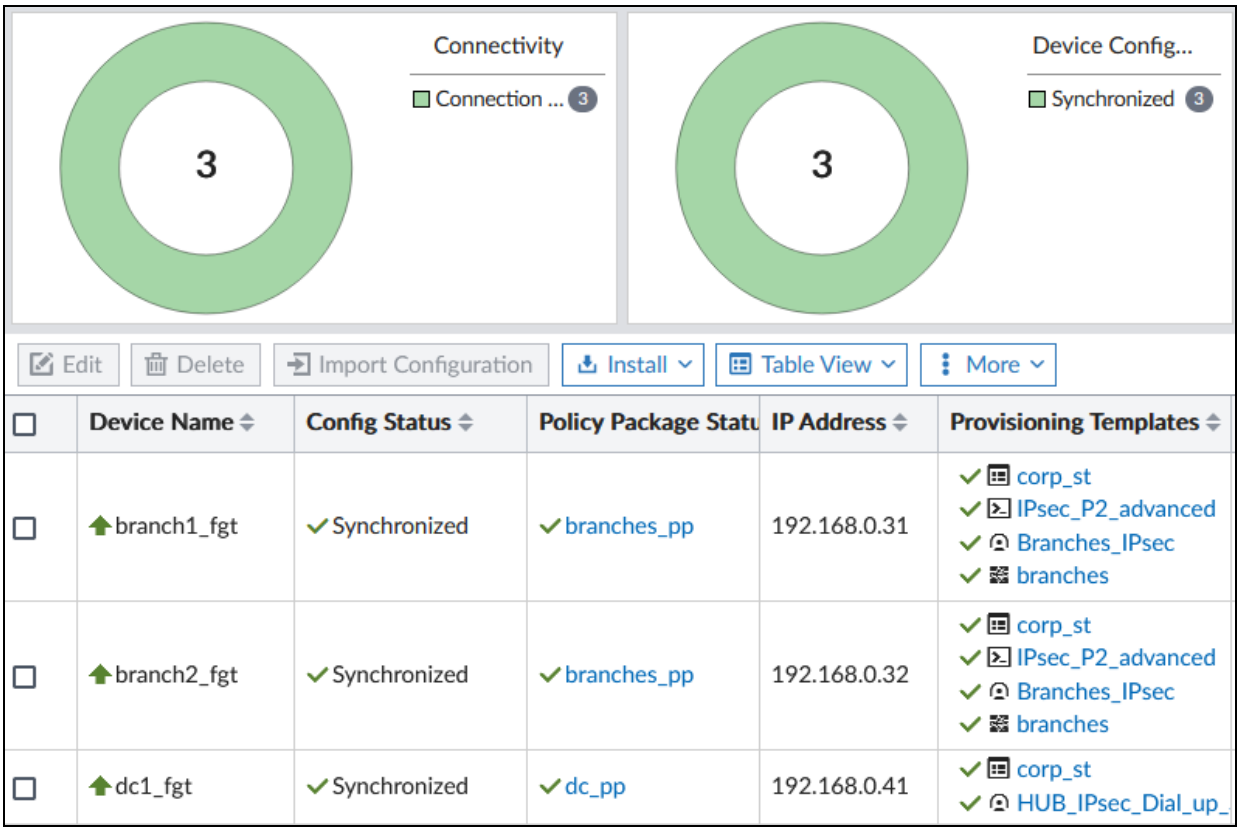
You will install the policy package on each device. For branch1_fgt and branch2_fgt, you will also install the static routes. For dc1_fgt, you will also install the FortiAnalyzer logging settings.

To install the configuration on branch1_fgt and branch2_fgt

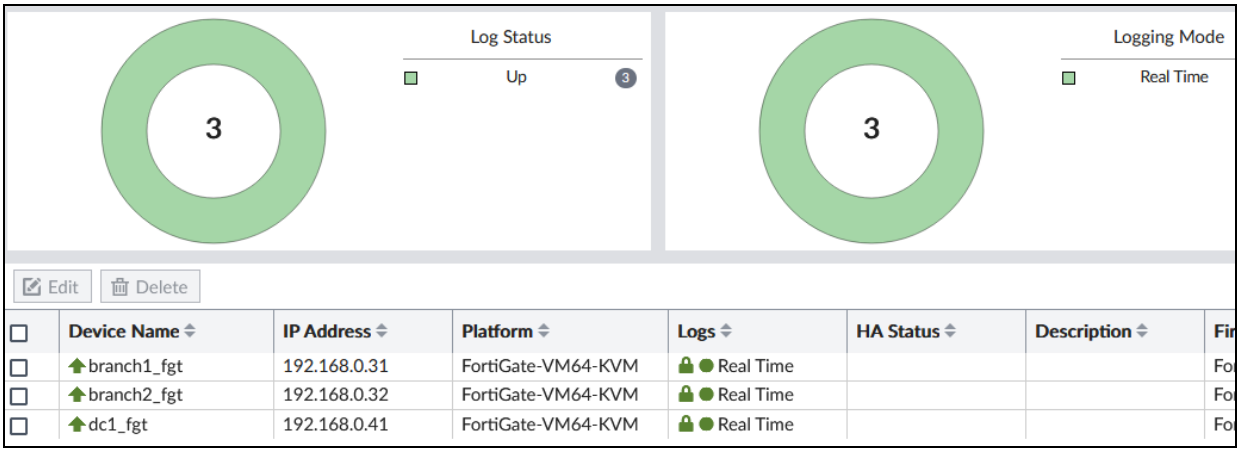
1. Continuing on the FortiManager GUI, click **Device Manager** > **Policy & Objects**, and then click **Install Wizard**.
2. Verify that **Install Policy Package & Device Settings** is selected.
3. In the **Policy Package** field, select **branches_pp**.
4. Click **Next**.
5. Verify that both **branch1_fgt** and **branch2_fgt** devices are selected, and then click **Next**.
6. Click **Install**.
   Wait until the installation finishes.
7. Click **Finish**.

To install the configuration on dc1_fgt

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Verify that **Install Policy Package & Device Settings** is selected.
3. In the **Policy Package** field, select **dc_pp**.
4. Click **Next**.
5. Verify that **dc1_fgt** is selected, and then click **Next**.
6. Click **Install**.
   Wait until the installation finishes.
7. Click **Finish**.
8. Click **Policy & Objects** > **Device Manager** > **Device & Groups**, and then click **Managed FortiGate** to display the list of managed devices.
   Your page should look similar to the following example:



9. Click **Logging FortiGate** to display the list of managed devices.
Your page should look similar to the following example:



All managed devices are synchronized and logging to FortiManager. You will verify tunnels and connectivity in the next exercise.

Exercise 4: Verifying the IPsec VPN

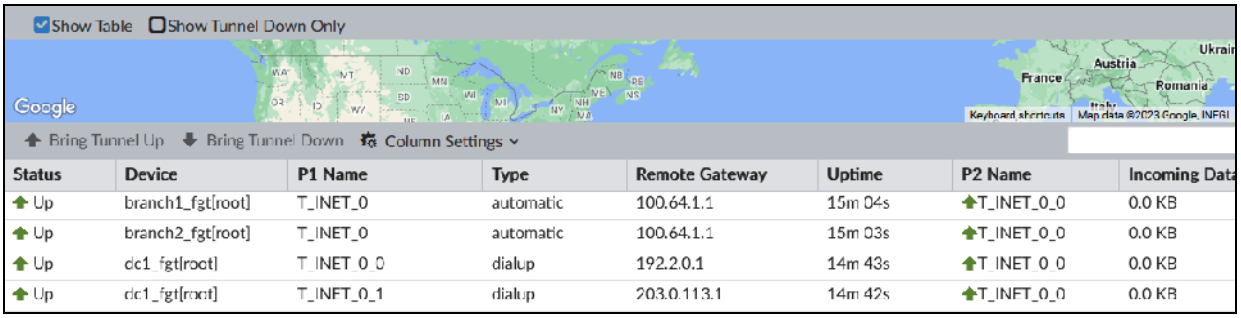
In this exercise, you will verify that the IPsec tunnels you configured using IPsec tunnel templates came up. After that, you will test connectivity across the tunnels by generating spoke-to-hub and spoke-to-spoke traffic.

Verify That the Tunnels Are Up

You will verify that the tunnels are up using FortiManager and the FortiGate CLI.

To verify that the tunnels are up

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Monitors** > **VPN Monitor**.
3. Select the **Show Table** checkbox.
   Your page should look similar to the following example:



Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Up	branch1_fgt[root]	T_INET_0	automatic	100.64.1.1	15m 04s	T_INET_0_0	0.0 KB
Up	branch2_fgt[root]	T_INET_0	automatic	100.64.1.1	15m 03s	T_INET_0_0	0.0 KB
Up	dc1_fgt[root]	T_INET_0_0	dialup	192.2.0.1	14m 43s	T_INET_0_0	0.0 KB
Up	dc1_fgt[root]	T_INET_0_1	dialup	203.0.113.1	14m 42s	T_INET_0_0	0.0 KB

4. Open an SSH session to each device (branch1_fgt, branch2_fgt, and dc1_fgt).
5. Log in with the username `admin` and password `password`.
6. On each device, enter the following commands to verify the tunnel status and routing table:

```
get ipsec tunnel list
get router info routing-table all
```

   The following image shows an example of branch1_fgt:

```
branch1_fgt # branch1_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0_0 PROXY-ID-SOURCE=10.0.1.0/255.255.255.0 PROXY-ID-DESTINATION
=0.0.0.0/0.0.0.0 STATUS=up TIMEOUT=500


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

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
S       10.0.0.0/8 [10/0] via T_INET_0 tunnel 100.64.1.1, [1/0]
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10

Routing table for VRF=10
C       10.0.101.0/24 is directly connected, vl_lan_ts
```

The following image shows an example of dc1_fgt:

```
dc1_fgt # dc1_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=0.0.0.0:0

NAME=T_INET_0_0 REMOTE-GW=192.2.0.1:0
        P2NAME=T_INET_0_0 PROXY-ID-SOURCE=0.0.0.0/255.255.255.255 PROXY-ID-DESTINATIO
N=10.0.1.0/10.0.1.255 STATUS=up TIMEOUT=274

NAME=T_INET_0_1 REMOTE-GW=203.0.113.1:0
        P2NAME=T_INET_0_0 PROXY-ID-SOURCE=0.0.0.0/255.255.255.255 PROXY-ID-DESTINATIO
N=10.0.2.0/10.0.2.255 STATUS=up TIMEOUT=276


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

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.2, port1, [1/0]
                  [10/0] via 100.64.1.10, port2, [1/0]
S       10.0.1.0/24 [15/0] via T_INET_0 tunnel 10.201.1.1, [1/0]
S       10.0.2.0/24 [15/0] via T_INET_0 tunnel 10.201.1.2, [1/0]
C       10.1.0.0/24 is directly connected, port5
C       100.64.1.0/29 is directly connected, port1
C       100.64.1.8/29 is directly connected, port2
S       172.16.0.0/16 [10/0] via 172.16.1.6, port4, [1/0]
C       172.16.1.0/24 is directly connected, port4
C       192.168.0.0/24 is directly connected, port10
```

The tunnels are up and the static routes were installed. On dc1_fgt, the static routes were automatically installed by FortiOS based on the remote protected network: `10.0.1.0/24` for branch1_fgt and `10.0.2.0/24` for branch2_fgt.

You will test VPN connectivity in the next task.

Verify Connectivity Across the VPN

You will test connectivity across the tunnels by generating spoke-to-hub and spoke-to-spoke traffic.

To verify connectivity across the VPN

1. Open an SSH session to dc1_fgt.
2. Log in with the username `admin` and password `password`.
3. Enter the following command on branch1_fgt to capture ICMP traffic from branch1_client:
   `diagnose sniffer packet any "host 10.0.1.101 and icmp" 4`
4. Leave the sniffer running.
5. Open an SSH session to branch1_client.
6. Log in with the username `root` and password `password`.
7. Ping `10.1.0.7` (dc1_host), and then leave the ping running.
   You should be able to ping the address.
8. Check the SSH session on dc1_fgt.
   Your output should look similar to the following example:

```
dc1_fgt # diagnose sniffer packet any "host 10.0.1.101 and icmp" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.1.101 and icmp]
5.215759 T_INET_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
5.215799 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
5.216099 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
5.216112 T_INET_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
6.216723 T_INET_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
6.216744 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
6.216953 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
6.216961 T_INET_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

9. On branch1_client, stop the ping.
10. Ping `10.0.2.101` (branch2_client), and then leave the ping running.
    You should be able to ping the address.
11. Check the SSH session on dc1_fgt.
    Your output should look similar to the following example:

```
22.667317 T_INET_0 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
22.667397 T_INET_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
22.669510 T_INET_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
22.669540 T_INET_0 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
23.668790 T_INET_0 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
23.668816 T_INET_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
23.670432 T_INET_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
23.670442 T_INET_0 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

12. On branch1_client, stop the ping.

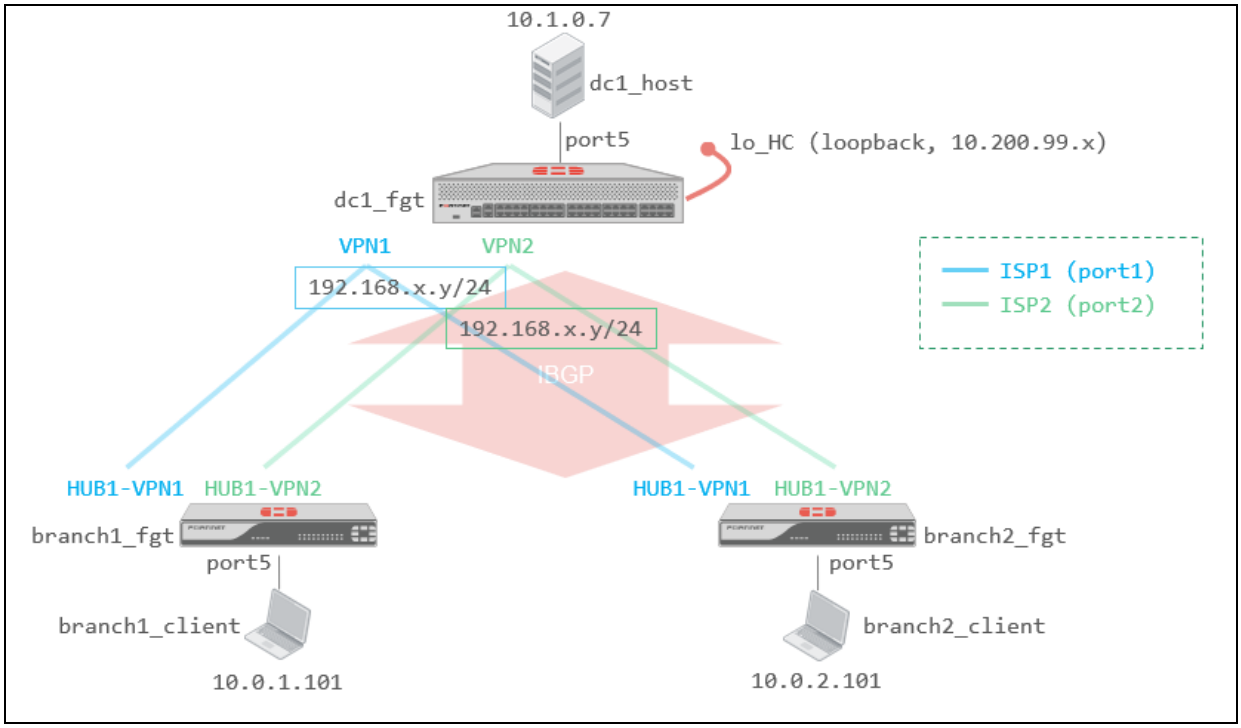
Both spoke-to-hub and spoke-to-spoke connectivity is working. Optionally, you can test the connectivity from branch2_client and dc1_host.

Exercise 5: Configuring the Overlay With the SD-WAN Overlay Template

In this exercise, you will use the SD-WAN overlay template to configure IPsec VPN tunnels for the overlay and BGP for routing on the overlay. The template will guide you and prepare, with the elements you provide, a configuration that follows Fortinet recommendations. You will start from the following configuration, which is similar to the one you reached at the end of exercise 2, and has no IPsec overlay tunnels:

- FortiManager manages branch1_fgt, branch2_fgt, and dc1_fgt.
- SD-WAN is configured on branch1_fgt and branch2_fgt, with rules to steer the traffic over the underlay (port1 and port2).

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



Prerequisites

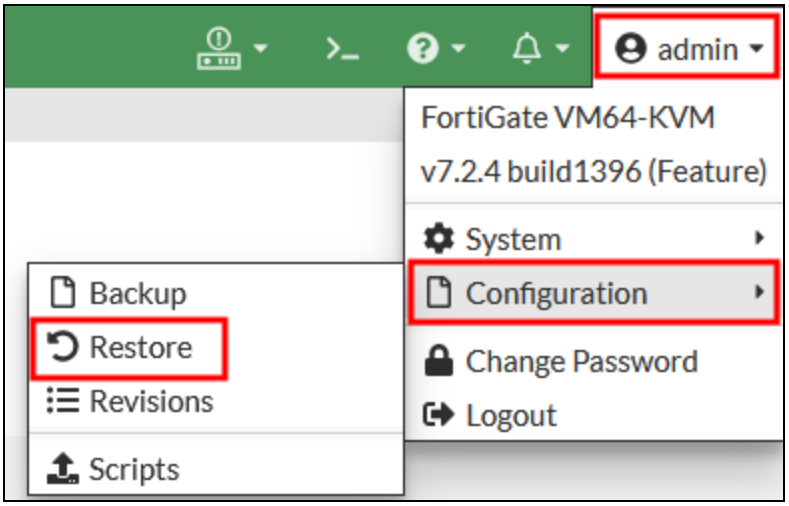
Before you begin this exercise, you must restore the configuration files for branch1_fgt, branch2_fgt, and dc1_fgt, as well as FortiManager.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the Local-Client VM, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-**

Write, and then click **Yes** to confirm.

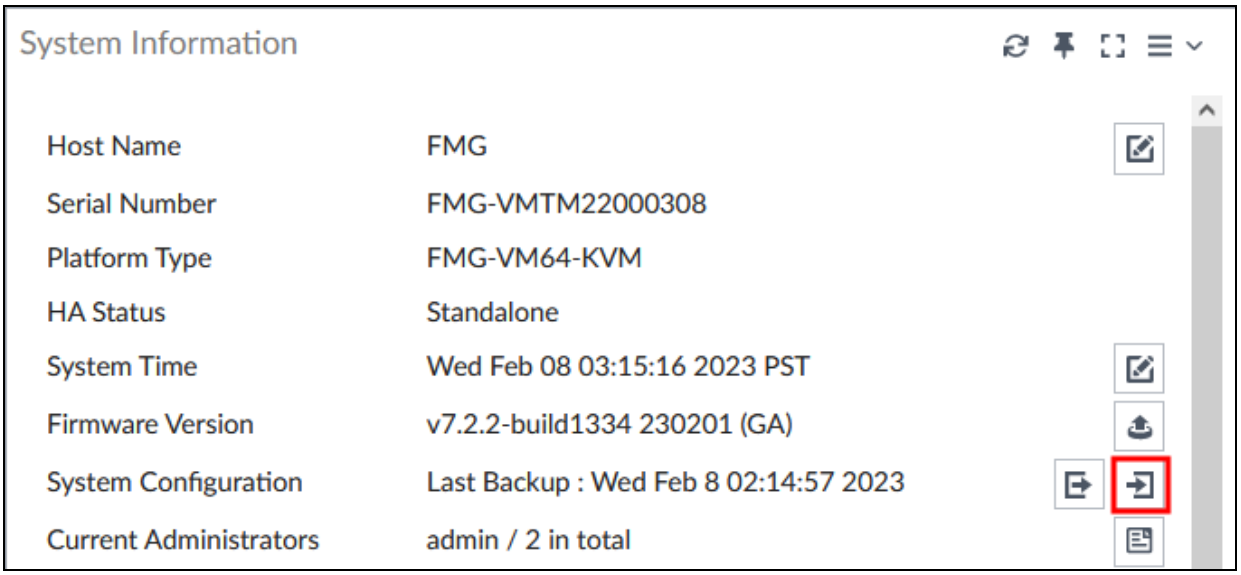
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



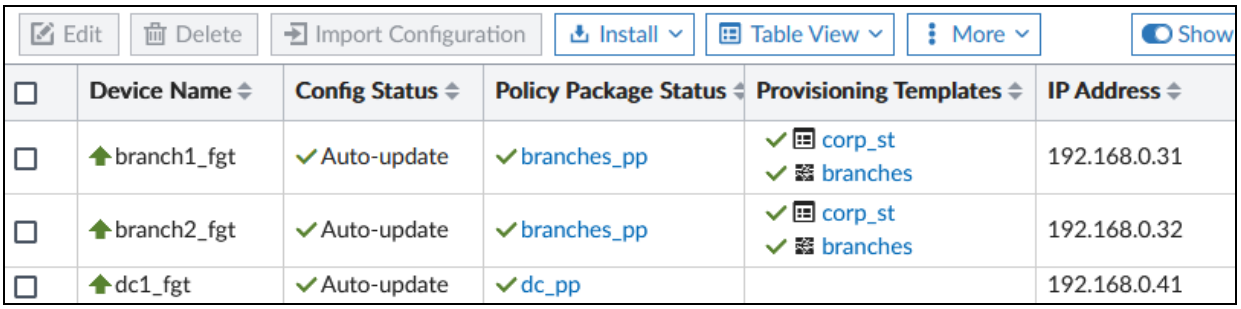
4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab2** > **Exercise-5**, select `lab2-ex5-branch1_fgt_7-2-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt.
   Use the following configuration file: `lab2-ex5-branch2_fgt_7-2-4_initial.conf`.
9. Repeat the previous steps to restore the configuration files on dc1_fgt.
   Use the following configuration file: `lab2-ex5-dc1_fgt_7-2-4_initial.conf`.

To restore the FortiManager configuration file

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root** > **System Settings**, and then click **Dashboard**.
3. In the **System Information** widget, click the **configuration restore** icon.



4. Click **Browse** to find the local file to upload.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab2** > **Exercise-5**, select `lab2-ex5-SYS_FMG_7-2-2_initial.dat`, and then click **OK**.
6. Wait until the file is uploaded and FortiManager finishes rebooting.
7. Log in to the FortiManager GUI with the username `admin` and password `password`.
8. Click **root** > **System Settings**, and then click **Advanced** > **Advanced Settings**.
9. For the **Offline Mode** option, select **Disable**.
10. Click **Apply** to save the settings.
11. Click **System Settings** > **Device Manager** > **Device & Groups** > **Managed FortiGate**.
    You can see three managed devices—branch1_fgt, branch2_fgt, and dc1_fgt.
12. Confirm that the three devices—branch1_fgt, branch2_fgt, and dc1_fgt—are correctly managed (green up arrow) and have a **Config Status** of either **Synchronized** or **Auto-update**.
    Your page should look similar to the following example:



Configure the Overlay With the SD-WAN Overlay Template

You will use the SD-WAN overlay template to configure the IPsec overlay and BGP routing configuration. FortiManager will guide you through a few pages where you will enter the specific parameters for the network.

To prepare the SD-WAN overlay template

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager** > **Device & Groups** > **Managed FortiGate**.
3. In the top bar, click **Device Group**, select **Create New Group**, and then configure the following settings:

Field	Value
Group Name	Branches
Device Name	• Click **Add Member**, and then select **branch1_fgt** and **branch2_fgt**. • Click **Add** to validate the device selection.

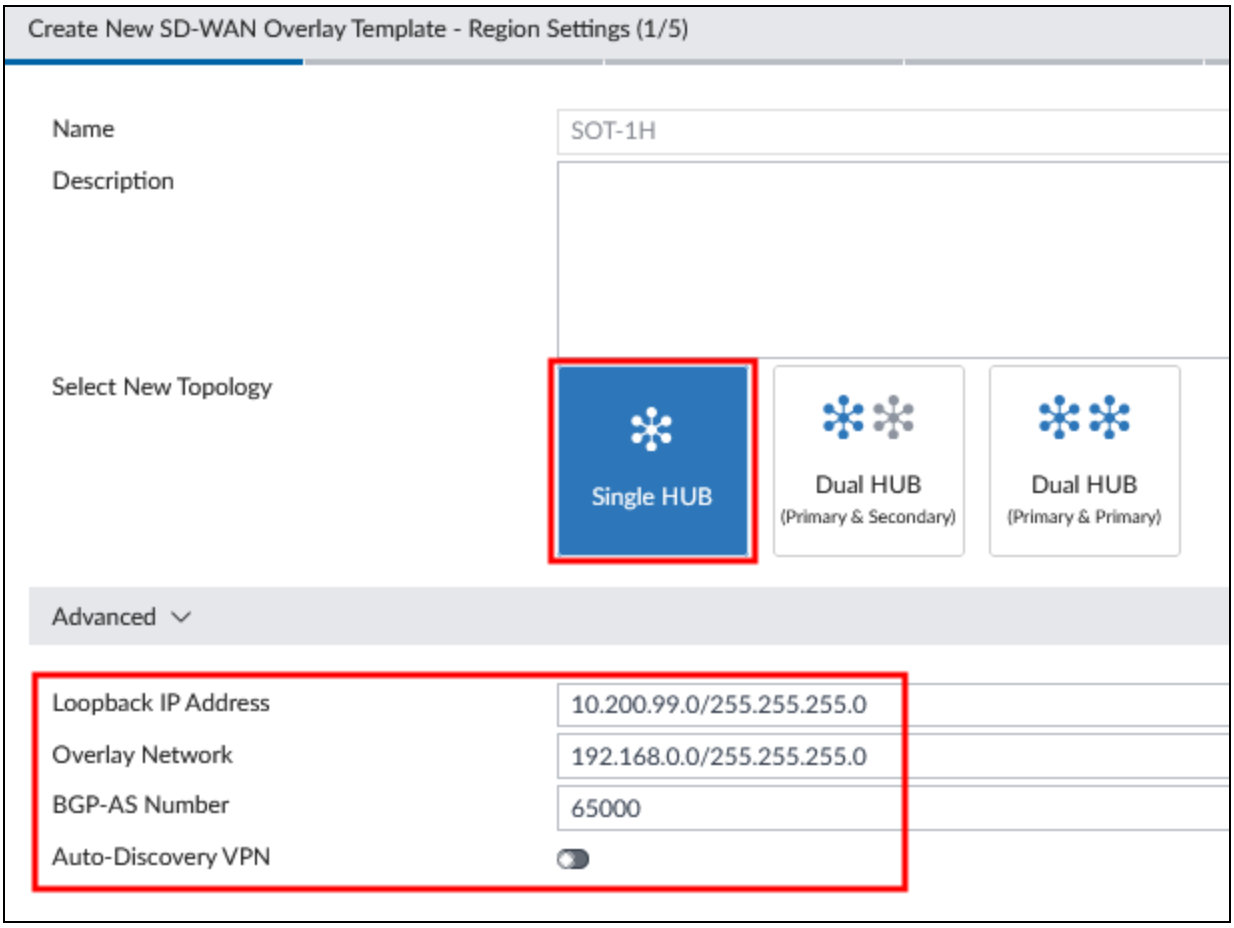
4. Click **OK** to validate the device group creation.

To use the SD-WAN overlay template, it is mandatory to group the branch devices in a device group. When the network expands, you can add additional devices to the device group, and then the devices are automatically configured with the template settings.

5. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Overlay Templates**.
6. Click **Create New**.
7. In the **Name** field, type `SOT-1H`, and then click **OK** to validate.
8. Select **Single HUB**.
9. Expand the **Advanced** menu, and then configure the following settings:

Field	Value
Loopback IP Address	10.200.99.0/255.255.255.0
Overlay Network	192.168.0.0/255.255.255.0
BGP-AS Number	65000 (default)
Auto-Discovery VPN	Disable (default)

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



10. Click **Next**, and then on the **Role Assignment (2/5)** page, configure the following settings:

Field	Value
HUB - Standalone HUB	dc1_fgt
Branch - Device Group Assignment	Branches

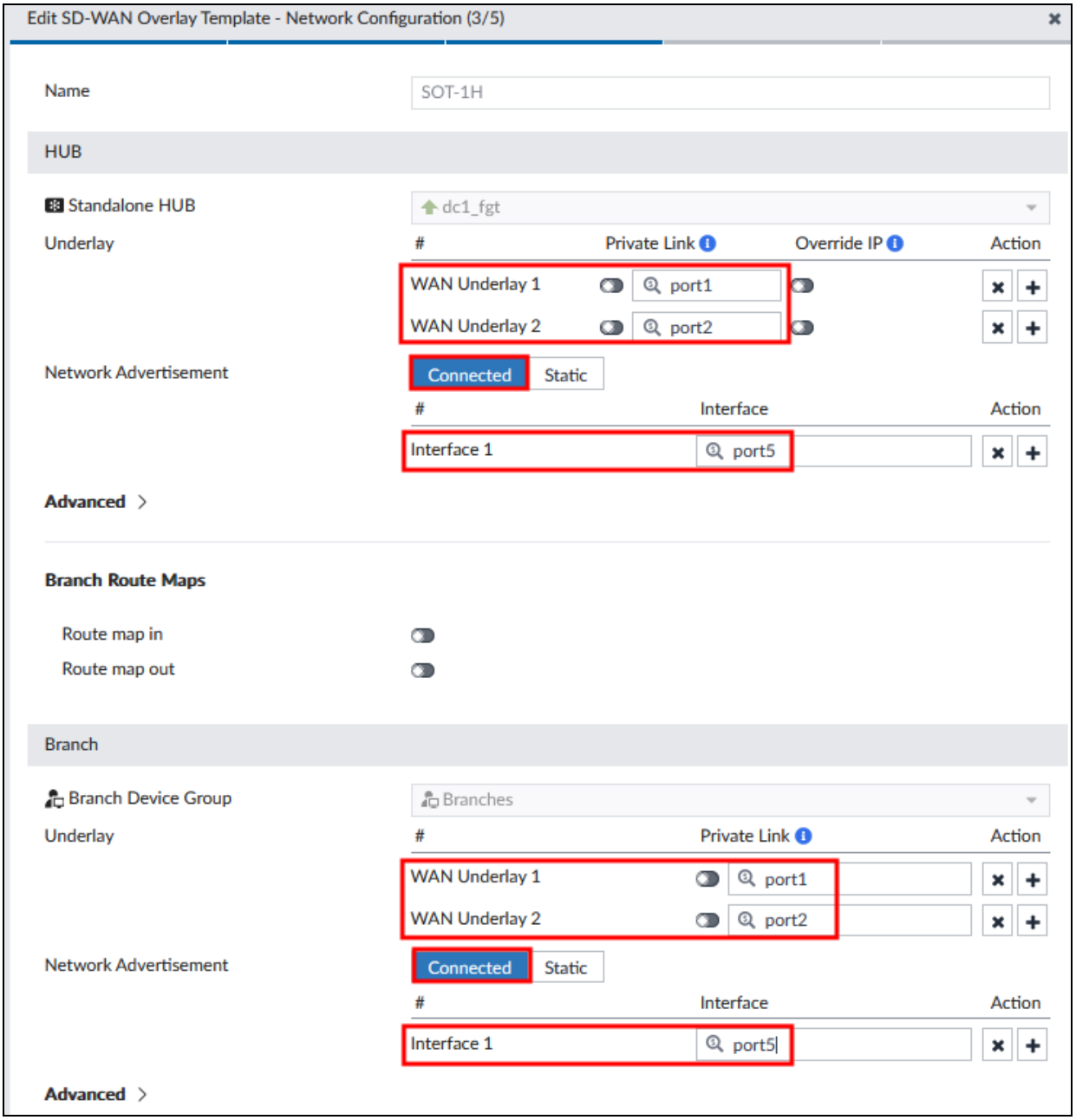
11. Click **Next** to move to the next page.
12. On the **Network Configuration (3/5)** page, in the **HUB** section, configure the following settings:

Field	Value
Underlay	In the **WAN Underlay 1** field, type `port1`. In the **WAN Underlay 2** field, type `port2`.
Network Advertisement	Select **Connected**, and then type `port5` as the **Interface 1** interface to advertise the network connected to the LAN interface.

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

Field	Value
Underlay	In the **WAN Underlay 1** field, type `port1`. In the **WAN Underlay 2** field, type `port2`.
Network Advertisement	Select **Connected**, and then type `port5` as the **Interface 1** interface to advertise the network connected to the LAN interface.

Your page should look similar to the following example:

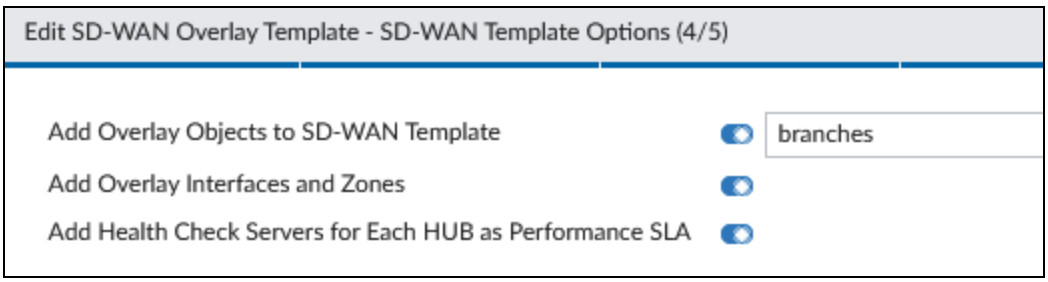


By selecting **Connected** in the **Network Advertisement** field, FortiManager creates a template that instructs BGP to advertise networks connected to interface port5 only. In our topology, that corresponds to the LAN subnet.

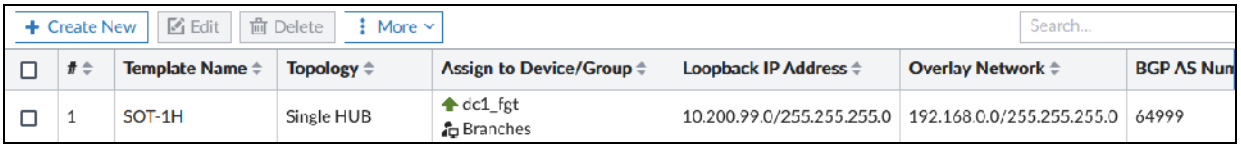
14. Click **Next** to move to the next page.
15. On the **SD-WAN Template Options (4/5)** page, configure the following settings:

Field	Value
Add Overlay Objects to SD-WAN Template	Enable In the drop-down list, select the **branches** SD-WAN template.
Add Overlay Interfaces and Zones	Enable
Add Health Check Servers for Each HUB as Performance SLA	Enable

Your page should look similar to the following example:



16. Click **Next** to move to the next page.
17. Review the settings on the **Summary (5/5)** page, and then click **Finish** to complete the SD-WAN overlay template.
Your page should look similar to the following example:



Review and Install the Overlay the SD-WAN Overlay Template Created

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

To review and adjust the templates created

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

You can see two templates: **SOT-1H_BRANCH_CLI** and **SOT-1H_HUB1_CLI**. These templates create loopback addresses and, for the branches, the BGP router ID. You can double-click the template names to review them.

The templates are added to CLI template groups, **SOT-1H_BRANCH_CLIGRP** and **SOT-1H_HUB1_CLIGRP**, respectively.

2. Click **Provisioning Templates** > **BGP Templates**.
3. Review the two templates: **SOT-1H_BRANCH_BGP** and **SOT-1H_HUB1_BGP**.
4. Click **SD-WAN Templates**, and then edit the branches template to review the changes the SD-WAN overlay template made.

   You can see a new zone, **HUB1**, with two interface members: **HUB1-VPN1** and **HUB1-VPN2**. These are the two overlay IPsec tunnel interfaces.

   port1 and port2, which were previously in the **underlay** zone, have been moved to the **WAN1** and **WAN2** zones. You will move them back to the **underlay** zone.

The SD-WAN overlay template placed the underlay interfaces, port1 and port2, in new underlay zones called **WAN1** and **WAN2**. Because you will continue to use SD-WAN rules and the firewall policy that you created previously, and defined with the zone named **underlay**, you must place the port1 and port2 interfaces back in the underlay zone.

5. In the **Interface Members** table, double-click **underlay** to edit the zone.
6. Under **Interfaces Members**, select **port1** and **port2**, and then click **OK** to validate the member selection.
7. Click **OK** to validate the zone edition.
8. Click **OK** to save the changes on the branches template.
9. Click **IPsec Tunnel Templates**.
10. Review the **SOT-1H_BRANCH_IPsec** and **SOT-1H_HUB1_IPsec** templates.

    Each template contains two tunnel definitions: **HUB1-VPN1** and **HUB1-VPN2** for the branches and **VPN1** and **VPN2** for the hub.

Stop and think!

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

No. The SD-WAN overlay template has created the template and grouped them in template groups. It's a group that is assigned to each device.

11. Click **Template Groups**, and then review the groups assigned to the branches and hub.

    The template groups contain the templates created or updated by the SD-WAN overlay template. They don't include the template that you assigned to the device before.
12. Double-click the **SOT-1H_HUB1** template group to edit it.
13. Click **+** to add a new template to the group.
14. Expand the **System Template** section, select **corp_st**, and then click **OK** to validate the selection.
15. Click **OK** to validate the template group.

16. Double-click the **SOT-1H_BRANCH** template group to edit it.
17. Repeat the previous steps to add the **corp_st** system template to the group.

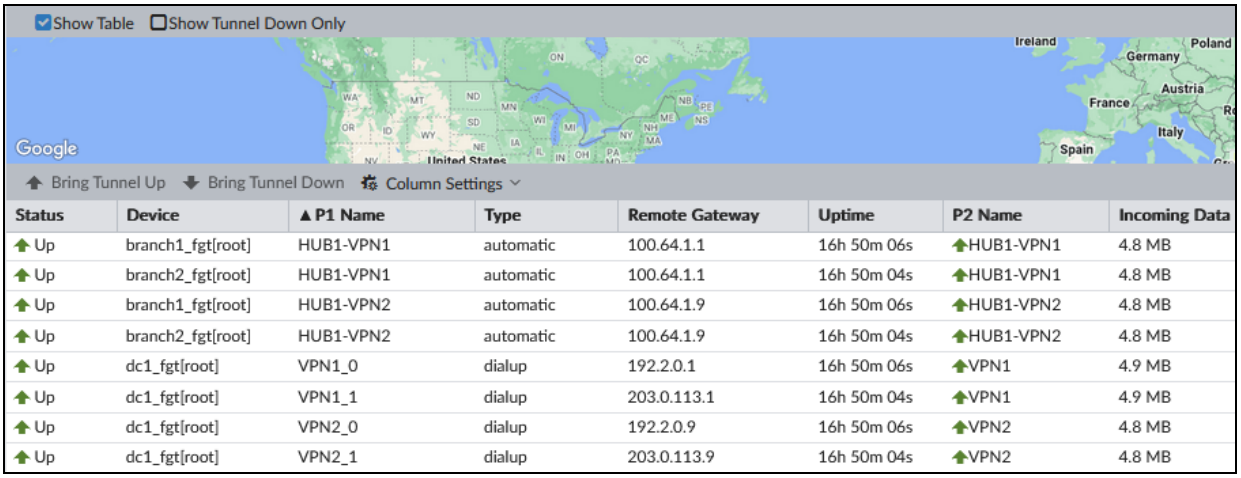
To install the configuration changes

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Review the device selection—make sure that **branch1_fgt**, **branch2_fgt**, and **dc1_fgt** are selected—and then click **Next**.
4. Click **Install** to install the configuration on the three devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To verify the health of the overlays

1. Continuing on the FortiManager GUI, click **Monitors** > **VPN Monitor**.
2. Select **Show Table**.

   Your page should look similar to the following example:



Status	Device	▲P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Up	branch1_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	16h 50m 06s	HUB1-VPN1	4.8 MB
Up	branch2_fgt[root]	HUB1-VPN1	automatic	100.64.1.1	16h 50m 04s	HUB1-VPN1	4.8 MB
Up	branch1_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	16h 50m 06s	HUB1-VPN2	4.8 MB
Up	branch2_fgt[root]	HUB1-VPN2	automatic	100.64.1.9	16h 50m 04s	HUB1-VPN2	4.8 MB
Up	dc1_fgt[root]	VPN1_0	dialup	192.2.0.1	16h 50m 06s	VPN1	4.9 MB
Up	dc1_fgt[root]	VPN1_1	dialup	203.0.113.1	16h 50m 04s	VPN1	4.9 MB
Up	dc1_fgt[root]	VPN2_0	dialup	192.2.0.9	16h 50m 06s	VPN2	4.8 MB
Up	dc1_fgt[root]	VPN2_1	dialup	203.0.113.9	16h 50m 04s	VPN2	4.8 MB

   Each branch device has established two tunnels to the hub:

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

   On the hub dc1_fgt you can see four tunnels:

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

3. Open an SSH session to branch1_fgt.
4. Log in with the username `admin` and password `password`.
5. Enter the following commands to review the BGP peering and routing table:

   ```
   get router info bgp summary
   ```

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

   Your output should look similar to the following example:

```
branch1_fgt # get router info bgp summary

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

Neighbor      V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.0.61  4      65000    1186    1179        1    0    0 17:14:00        1
192.168.0.125 4      65000    1184    1181        1    0    0 17:13:59        1

Total number of neighbors 2


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

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.0.61 (recursive is directly connected, HUB1-VPN1), 17:13:42, [1/0]
                    [200/0] via 192.168.0.125 (recursive is directly connected, HUB1-VPN2), 17:13:42, [1/0]
C       10.200.99.1/32 is directly connected, Branch1-Lo
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
C       192.168.0.0/26 is directly connected, HUB1-VPN1
C       192.168.0.1/32 is directly connected, HUB1-VPN1
C       192.168.0.64/26 is directly connected, HUB1-VPN2
C       192.168.0.65/32 is directly connected, HUB1-VPN2
```

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

Stop and think!

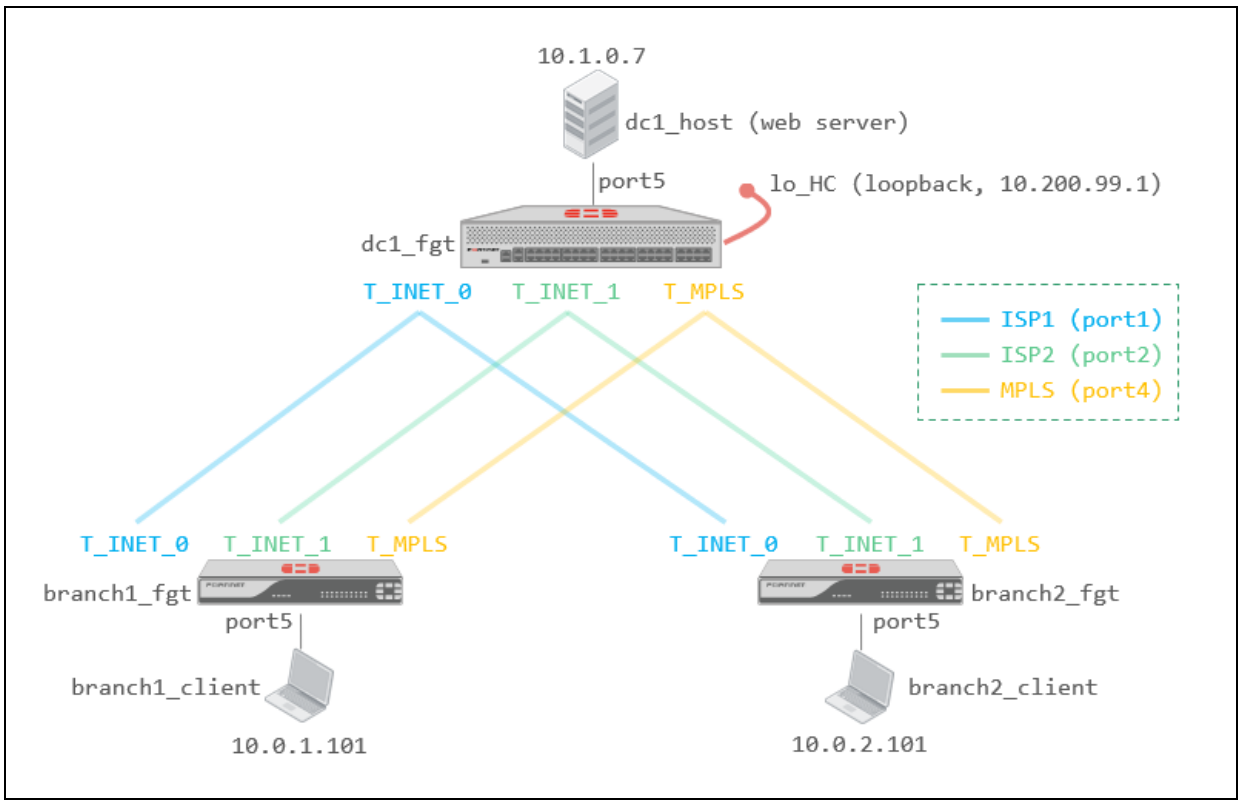
What is the next configuration step?

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

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

Lab 3: Members, Zones, and Performance SLAs

In this lab, you will configure an overlay zone and its members using FortiManager. The VPN tunnels have been preconfigured for you. The following topology has been preconfigured for you:



Three communities were configured, one for each overlay (ISP1, ISP2, and MPLS). The lo_HC loopback interface is also preconfigured and you will use it as the target server on one of the performance SLAs for overlays.

You will configure two performance SLAs for overlays, one using ping as the protocol, and another using HTTP. You will also increase the latency on the overlays and see the changes introduced in the status of the performance SLAs and overlays.

Objectives

- Configure zones and members for overlays
- Use ping and HTTP to actively monitor the performance and health of overlays
- Configure SLA targets
- Use the SD-WAN monitor on FortiManager and the FortiGate CLI to check the status of performance SLAs, SLA targets, and overlays

Time to Complete

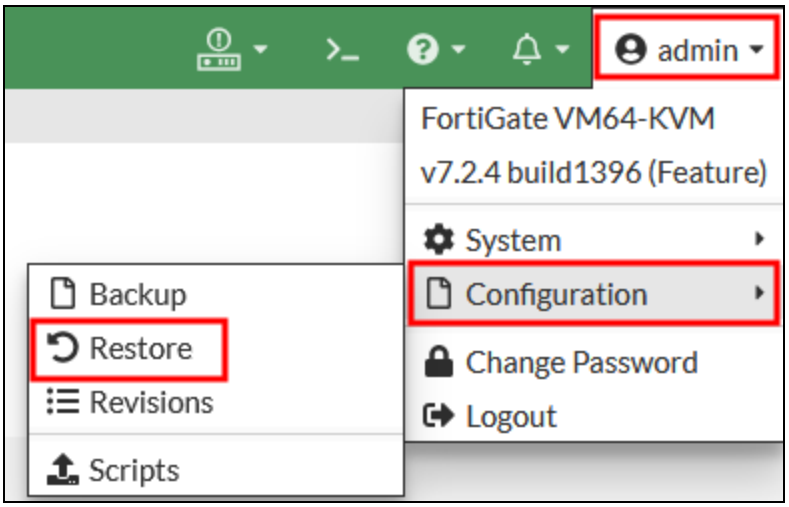
Estimated: 110 minutes

Prerequisites

Before you begin this lab, you must restore the configuration files for branch1_fgt, branch2_fgt, and dc1_fgt, as well as FortiManager.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the local-client, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

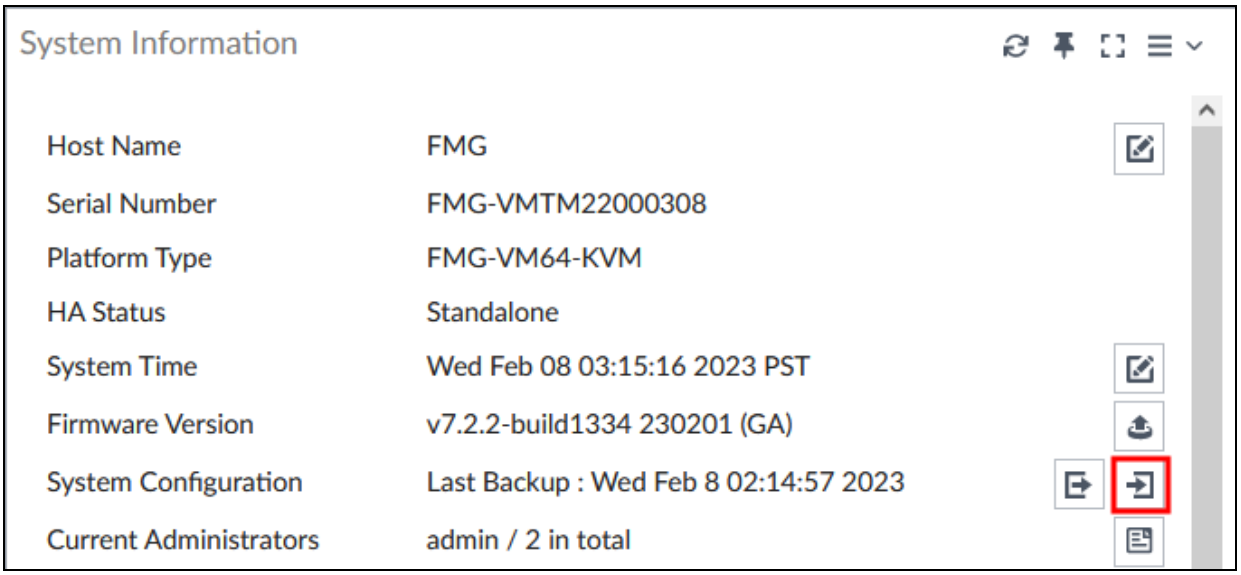


4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-3**, select `lab3-branch1_fgt_7-2-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt and dc1_fgt.
   Use the following configuration files:

Device	Configuration filename
branch2_fgt	`lab3-branch2_fgt_7-2-4_initial.conf`
dc1_fgt	`lab3-dc1_fgt_7-2-4_initial.conf`

To restore the FortiManager configuration file

1. On the local-client, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root** > **System Settings**, and then click **Dashboard**.
3. In the **System Information** widget, click the configuration restore icon.



4. Click **Browse** to indicate the local file to upload.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-3**, select `lab3-SYS_FMG_7-2-2_initial.dat`, and then click **OK**.
6. Wait until the file is uploaded and FortiManager finishes rebooting.
7. Log in to the FortiManager GUI with the username `admin` and password `password`.
8. Click **root** > **System Settings**, and then click **Advanced** > **Advanced Settings**.
9. In the **Offline Mode** field, select **Disable**.
10. Click **Apply** to save the settings.

Exercise 1: Configuring SD-WAN Zones and Members

In this exercise, you will review the existing VPN configuration and its status. After that, you will configure the VPN tunnels as SD-WAN members and place them in a separate zone called the overlay zone. Finally, you will verify the resulting configuration on FortiManager and the FortiGate CLI.

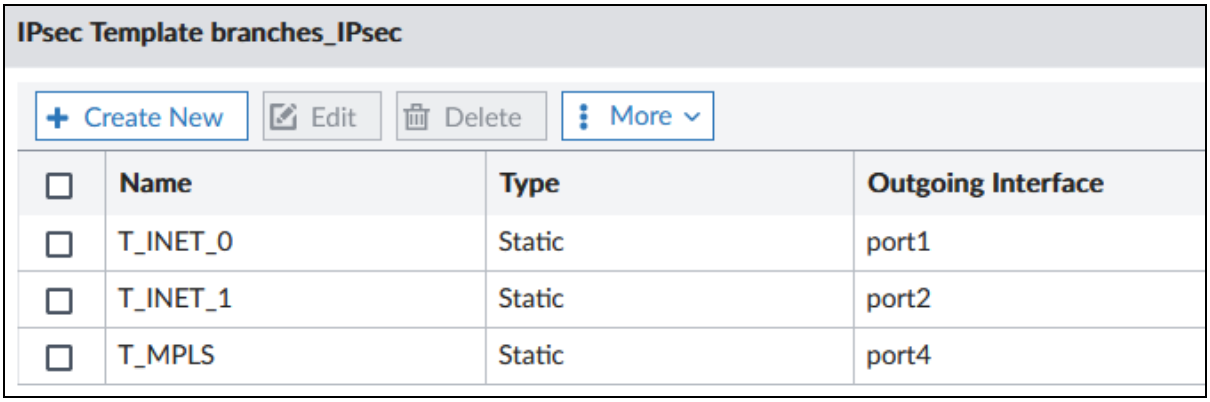
Review the VPN Tunnels and Their Status

In lab 2, you configured the **T_INET_0** overlay. In this lab, the **T_INET_1** and **T_MPLS** overlays have been preconfigured for you. You will review the existing configuration and status of the tunnels on both FortiManager and the FortiGate CLI.

To review the VPN tunnels configuration and their status

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **IPsec Tunnel Templates**.
3. Double-click **branches_IPsec** to view the template settings.
   You can see three tunnels configured: **T_INET_0**, **T_INET_1**, and **T_MPLS**.

   Your page should look similar to the following example:



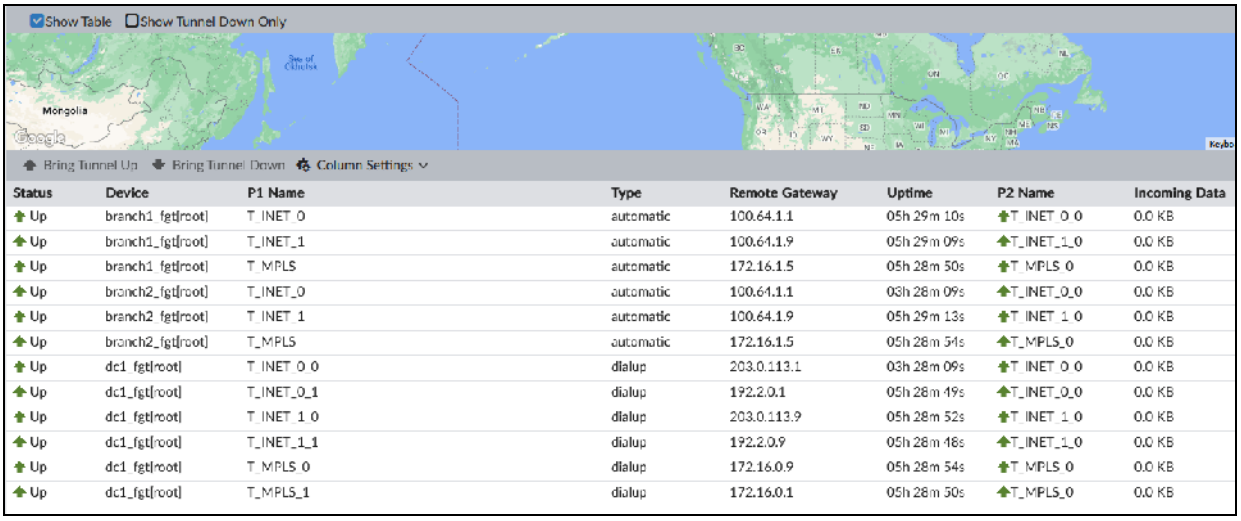
4. Double-click each line to review the settings.
   The three tunnels have similar configurations, but different outgoing interfaces and remote gateways.

The three tunnels definitions are grouped within the same template. This is mandatory because you can apply only one IPsec tunnel template to each FortiGate. However, each template can contains multiple tunnel definitions.

5. Click **Return** to go back to the IPsec tunnel menu.
6. Double-click **hubs_IPsec** to view the template settings.
   You can see three tunnels configured: **T_INET_0**, **T_INET_1**, and **T_MPLS**.

7. Click **Return** to go back to the IPsec tunnel menu.
8. Click **Monitors** > **VPN Monitor**.
9. Select **Show Table**.

   Your page should look similar to the following example:



Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Up	branch1_fgt[root]	T_INET_0	automatic	100.64.1.1	05h 29m 10s	T_INET_0_0	0.0 KB
Up	branch1_fgt[root]	T_INET_1	automatic	100.64.1.9	05h 29m 09s	T_INET_1_0	0.0 KB
Up	branch1_fgt[root]	T_MPLS	automatic	172.16.1.5	05h 28m 50s	T_MPLS_0	0.0 KB
Up	branch2_fgt[root]	T_INET_0	automatic	100.64.1.1	03h 28m 09s	T_INET_0_0	0.0 KB
Up	branch2_fgt[root]	T_INET_1	automatic	100.64.1.9	05h 29m 13s	T_INET_1_0	0.0 KB
Up	branch2_fgt[root]	T_MPLS	automatic	172.16.1.5	05h 28m 54s	T_MPLS_0	0.0 KB
Up	dc1_fgt[root]	T_INET_0_0	dialup	203.0.113.1	03h 28m 09s	T_INET_0_0	0.0 KB
Up	dc1_fgt[root]	T_INET_0_1	dialup	192.2.0.1	05h 28m 19s	T_INET_0_0	0.0 KB
Up	dc1_fgt[root]	T_INET_1_0	dialup	203.0.113.9	05h 28m 52s	T_INET_1_0	0.0 KB
Up	dc1_fgt[root]	T_INET_1_1	dialup	192.2.0.9	05h 28m 18s	T_INET_1_0	0.0 KB
Up	dc1_fgt[root]	T_MPLS_0	dialup	172.16.0.9	05h 28m 54s	T_MPLS_0	0.0 KB
Up	dc1_fgt[root]	T_MPLS_1	dialup	172.16.0.1	05h 28m 50s	T_MPLS_0	0.0 KB

There are six tunnels configured in total, and all of them are up (green up arrow).

If you don't see the tunnels established and up, check the FortiManager status in the top bar. Offline mode must be disabled.

10. Open an SSH session to each device (branch1_fgt, branch2_fgt, and dc1_fgt).
11. Log in with the username `admin` and password `password`.
12. On each device, enter the following commands to verify the tunnel status and routing table:

```
get ipsec tunnel list
get router info routing-table all
```

The following image shows an example of branch1_fgt:

```
branch1_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0_0 PROXY-ID-SOURCE=10.0.1.0/255.255.255.0 PROXY-ID-DESTINATION=
0.0.0.0/0.0.0.0 STATUS=up TIMEOUT=999

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1_0 PROXY-ID-SOURCE=10.0.1.0/255.255.255.0 PROXY-ID-DESTINATION=
0.0.0.0/0.0.0.0 STATUS=up TIMEOUT=999

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS_0 PROXY-ID-SOURCE=10.0.1.0/255.255.255.0 PROXY-ID-DESTINATION=0.
0.0.0/0.0.0.0 STATUS=up TIMEOUT=1005


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

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
S       10.0.0.0/8 [10/0] via T_INET_0 tunnel 100.64.1.1, [1/0]
                   [10/0] via T_INET_1 tunnel 100.64.1.9, [1/0]
                   [10/0] via T_MPLS tunnel 172.16.1.5, [1/0]
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10

Routing table for VRF=10
C       10.0.101.0/24 is directly connected, vl_lan_ts
```

Configure an SD-WAN Zone

You will configure a zone for the IPsec overlays. After that, you will install the changes. You must install the zone first, before you can reference it in firewall policies and static routes.

To configure an SD-WAN zone

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **Interface Members** section, click **Create New** > **SD-WAN Zone**.
4. In the **Name** field, type `overlay`.
5. Click **OK** to save the settings.
6. Click **OK** to save the template settings.

To install the device settings

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

Configure VPN Tunnels as SD-WAN Members

First, you will remove the references to the VPN tunnels in firewall policies. Instead of referencing the tunnels, you will reference the overlay zone. Otherwise, you won't be able to configure the VPN tunnels as SD-WAN members. You will also make the same change for static routes. Next, you will configure the VPN tunnels as SD-WAN members of the overlay zone. Finally, you will install the changes and verify the configuration on the FortiGate CLI.

To reference the overlay zone in firewall policies

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

#	Name	From	To	Source	Destination	Schedule	Service
1	DIA	LAN	underlay	LAN-net	all	always	ALL
2	To Hub0-INET0	LAN	T_INET_0	LAN-net	all	always	ALL
3	From Hub0-INET0	T_INET_0	LAN	all	LAN-net	always	ALL
4	To Hub0-INET1	LAN	T_INET_1	LAN-net	all	always	ALL
5	From Hub0-INET1	T_INET_1	LAN	all	LAN-net	always	ALL
6	To Hub0-MPLS	LAN	T_MPLS	LAN-net	all	always	ALL
7	From Hub0-MPLS	T_MPLS	LAN	all	LAN-net	always	ALL

3. Double-click the **To Hub0-INET0** firewall policy to edit it.
4. Configure the following settings:

Field	Value
Name	Replace `To Hub0-INET0` with `To Hub0-Overlay`.
Outgoing Interface	Remove **T_INET_0**, and then add **overlay**.

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

Stop and think!

Did you configure a normalized interface called **overlay**? Remember that on FortiManager, firewall policies can reference only normalized interfaces. Yet **overlay** is available as a possible source or destination for the firewall policy.

When you create an SD-WAN zone with the SD-WAN template, FortiManager automatically creates a corresponding normalized interface.

6. Double-click the **From Hub0-INET0** firewall policy to edit it.
7. Configure the following settings:

Field	Value
Name	Replace `From Hub0-INET0` with `From Hub0-Overlay`.
Incoming Interface	Remove **T_INET_0**, and then add **overlay**.

8. Click **OK** to save the settings.
9. Select the firewall policies with sequence numbers **4**, **5**, **6**, and **7**, and then click **Delete** to delete the firewall policies that reference the **T_INET_1** and **T_MPLS** interfaces.
   Your page should look similar to the following example:

#	Name	From	To	Source	Destination	Schedule	Service
1	DIA	LAN	underlay	LAN-net	all	always	ALL
2	To Hub0-Overlay	LAN	overlay	LAN-net	all	always	ALL
3	From Hub0-Overlay	overlay	LAN	all	LAN-net	always	ALL

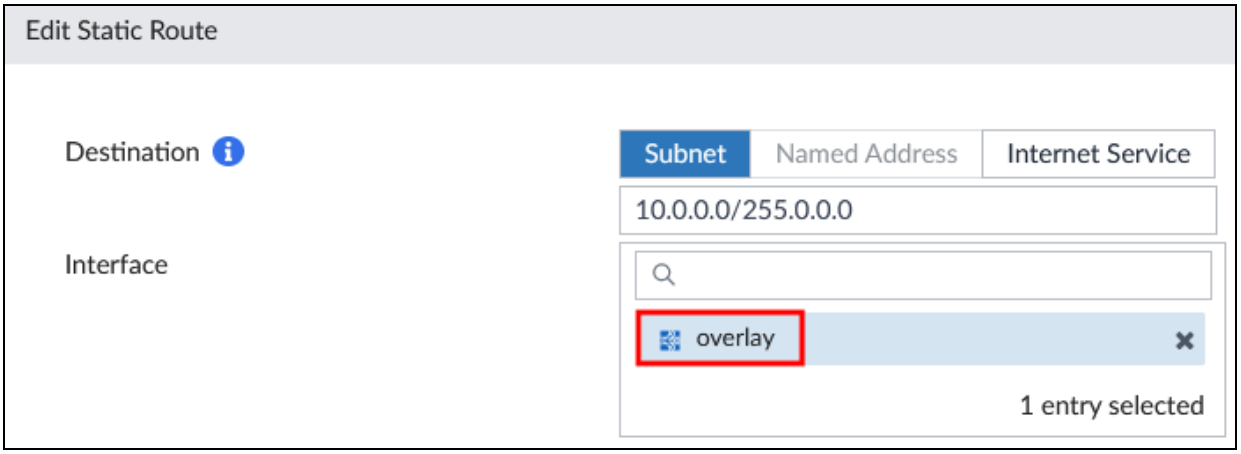
You require only one firewall policy in each direction that references the overlay zone. Using SD-WAN zones greatly reduces the number of policies required for your deployment.

To reference the overlay zone in static routes

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Device Manager**.
2. Click **Device & Groups** > **Managed FortiGate**, and then click **branch1_fgt**.
3. Click **Network** > **Static Route**.
   Your page should look similar to the following example:

	#	ID	Destination	Gateway	Interface	Distance	Priority	Status
Static Route (5)								
	1	1	10.0.0.0/255.0.0.0	0.0.0.0	T_INET_0	10	1	Enable
	2	2	0.0.0.0/0.0.0.0	0.0.0.0	underlay	1	1	Enable
	3	3	10.0.0.0/255.0.0.0	0.0.0.0	T_INET_1	10	1	Enable
	4	4	10.0.0.0/255.0.0.0	0.0.0.0	T_MPLS	10	1	Enable
	5	5	172.16.0.0/255.255.0.0	172.16.0.2	port4	10	1	Enable

4. Double-click the route with ID **1** to edit it.
5. In the **Interface** field, remove the reference to **T_INET_0**, and then select **overlay** in the list.



6. Click **OK** to save the settings.
7. Select the routes that reference the **T_INET_1** and **T_MPLS** interfaces (ID **3** and **4**), and then click **Delete** to delete them.

   Your page should look similar to the following example:

	#	ID	Destination	Gateway	Interface	Distance	Priority	Status
Static Route (3)								
	1	1	10.0.0.0/255.0.0.0	0.0.0.0	overlay	1	1	Enable
	2	2	0.0.0.0/0.0.0.0	0.0.0.0	underlay	1	1	Enable
	3	5	172.16.0.0/255.255.0.0	172.16.0.2	port4	10	1	Enable

You require only one static route that references the overlay zone. FortiGate automatically creates ECMP routes for the members in the zone. For this reason, you can delete the other two individual static routes.

8. Repeat the previous procedure on branch2_fgt.

   There should be only one route to `10.0.0.0/8` that references the overlay zone, as the following example shows:

	#	ID	Destination	Gateway	Interface	Distance	Priority	Status
Static Route (3)								
	1	1	10.0.0.0/255.0.0.0	0.0.0.0	overlay	1	1	Enable
	2	2	0.0.0.0/0.0.0.0	0.0.0.0	underlay	1	1	Enable
	3	5	172.16.0.0/255.255.0.0	172.16.0.2	port4	10	1	Enable

To install device settings and a policy package

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Click **Back**, and then select **Install Policy Package & Device Settings**.
3. In the **Policy Package** field, select **branches_pp**, and then click **Next**.
4. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
5. Click **Install** to install the configuration on both devices.
6. Wait for the installation to finish.
7. Click **Finish**.

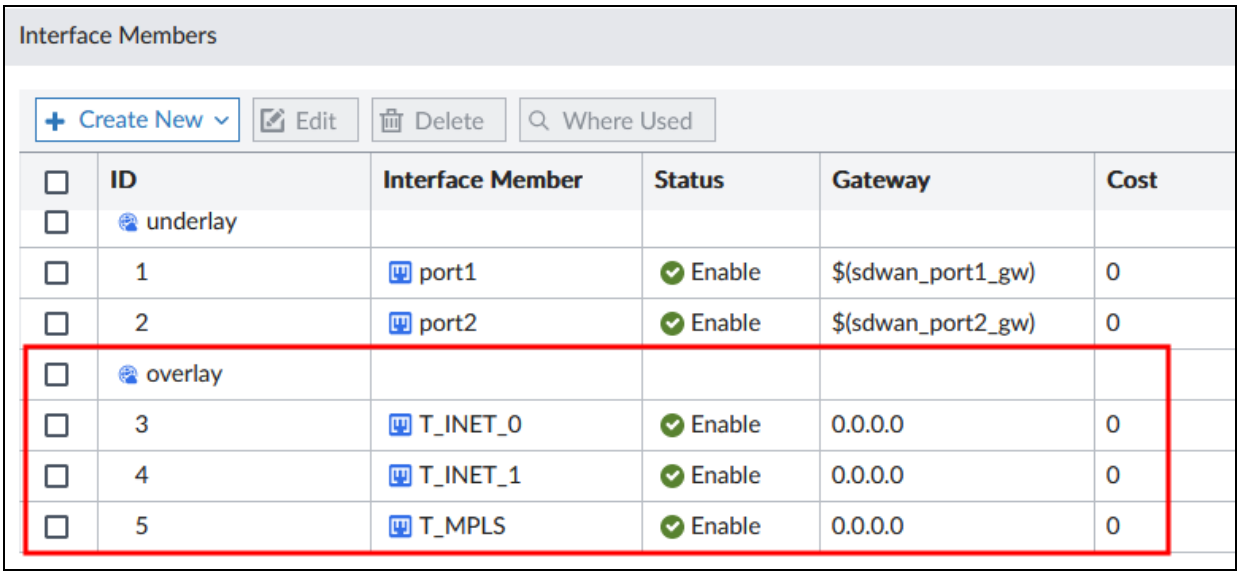
To configure VPN tunnels as SD-WAN members

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **Interface Members** section, click **Create New** > **SD-WAN Member**.
4. Configure the following settings:

Field	Value
Interface Member	T_INET_0
SD-WAN Zone	overlay

In the **Interface Member** field, make sure you type the name exactly as it is spelled above, including capitalization. Otherwise, the installation will fail.

5. Click **OK** to save the settings.
6. Repeat the previous procedure first for **T_INET_1**, and then for **T_MPLS**.
   The **Interface Members** section in your template should look similar to the following example:



The IDs for **T_INET_0**, **T_INET_1**, and **T_MPLS** should be **3**, **4**, and **5**, respectively. If you followed the order of the instructions, those should be the assigned member IDs.

Configure an SD-WAN Rule for the Overlays

You will configure a basic manual rule for the overlays.

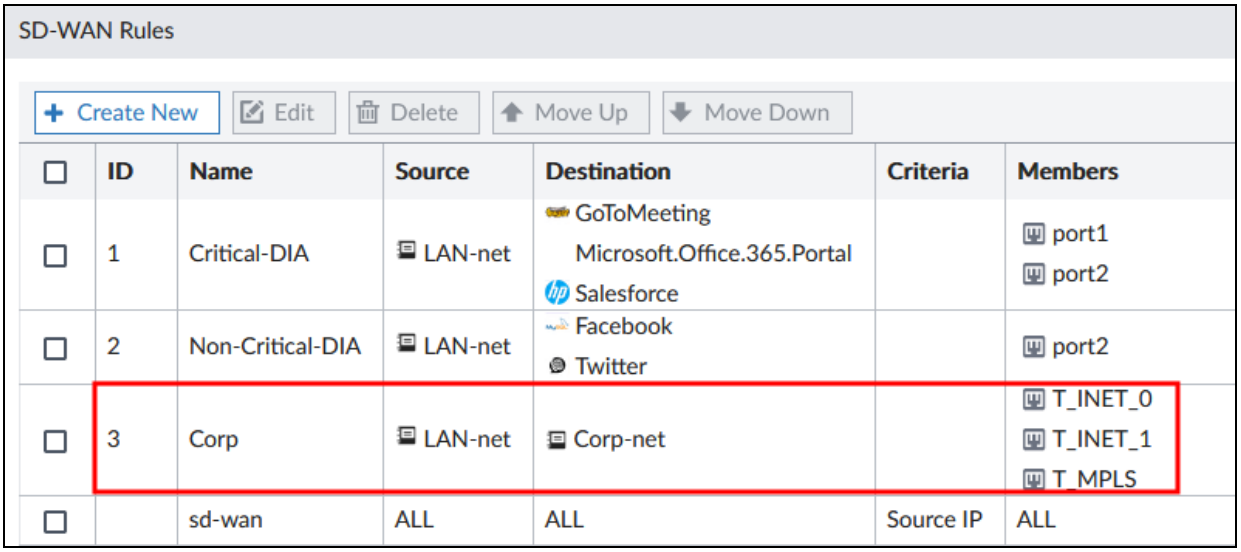
To configure an SD-WAN rule for the overlays

1. Continuing on the FortiManager GUI, in the **SD-WAN Rules** section, click **Create New**.
2. Configure the following settings:

Field	Value
Name	Corp
Source	In the **Source Address** field, select **LAN-net**.
Destination	In the **Address** field, select **Corp-net**.
Outgoing Interfaces	• In the **Strategy** field, select **Manual**. • In the **Interface Preference** field, select **T_INET_0**, **T_INET_1**, and **T_MPLS**.

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

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



The members must be ordered as displayed, **T_INET_0**, **T_INET_1**, and **T_MPLS**. You can drag and drop the members to reorder them, if required.

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

To install the device settings

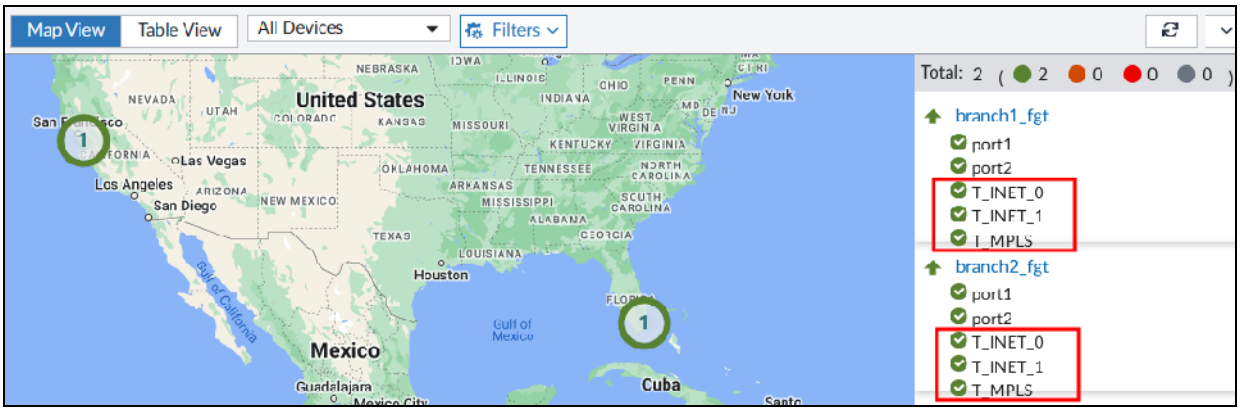
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on both devices.
5. Wait for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

Verify the Overlays as SD-WAN Members

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

To verify the overlays using FortiManager

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



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

The overlays are configured as SD-WAN members and are up (green up arrow).

To verify the overlays using the FortiGate CLI

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

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

The following image shows an example of branch2_fgt:

```
branch2_fgt # show system sdwan
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "underlay"
        next
        edit "overlay"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
            set gateway 203.0.113.2
        next
        edit 2
            set interface "port2"
            set zone "underlay"
            set gateway 203.0.113.10
        next
        edit 3
            set interface "T_INET_0"
            set zone "overlay"
        next
        edit 4
            set interface "T_INET_1"
            set zone "overlay"
        next
        edit 5
            set interface "T_MPLS"
            set zone "overlay"
        next
    end
```

```
branch2_fgt # diagnose sys sdwan zone
Zone overlay index=3
        members(3): 20(T_INET_0) 21(T_INET_1) 22(T_MPLS)
Zone underlay index=2
        members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
        members(0):

branch2_fgt # diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 203.0.113.2, priority: 1 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 203.0.113.10, priority: 1 1024, weight: 0
Member(3): interface: T_INET_0, flags=0xc , gateway: 100.64.1.1, priority: 1 1024, weight: 0
Member(4): interface: T_INET_1, flags=0xc , gateway: 100.64.1.9, priority: 1 1024, weight: 0
Member(5): interface: T_MPLS, flags=0xc , gateway: 172.16.1.5, priority: 1 1024, weight: 0
```

The overlays were configured as SD-WAN members and placed in the `overlay` zone.

Stop and think!

You didn't configure a gateway for the overlays. Yet, FortiGate displays a gateway address for each of them. Why?

You must not configure a gateway address for members that are IPsec tunnels. FortiGate automatically determines the gateway address. That is, FortiGate uses the IPsec tunnel ID as the gateway address. You can view the tunnel ID (`tun_id` in the CLI) in the output of the `diagnose vpn tunnel list` command.

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

```
diagnose vpn tunnel list
```

```
branch2_fgt # branch2_fgt # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=T_INET_0 ver=2 serial=1 203.0.113.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1 dst_
mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_dev frag-rfc
  role=primary accept_traffic=1 overlay_id=0
```

Exercise 2: Using Ping to Actively Monitor the Overlays

In this exercise, you will configure a performance SLA named **VPN_PING** that you will use to actively monitor the overlays using the ping protocol. You will also configure two SLA targets for **VPN_PING**. After that, you will check the health of the overlays using FortiManager.

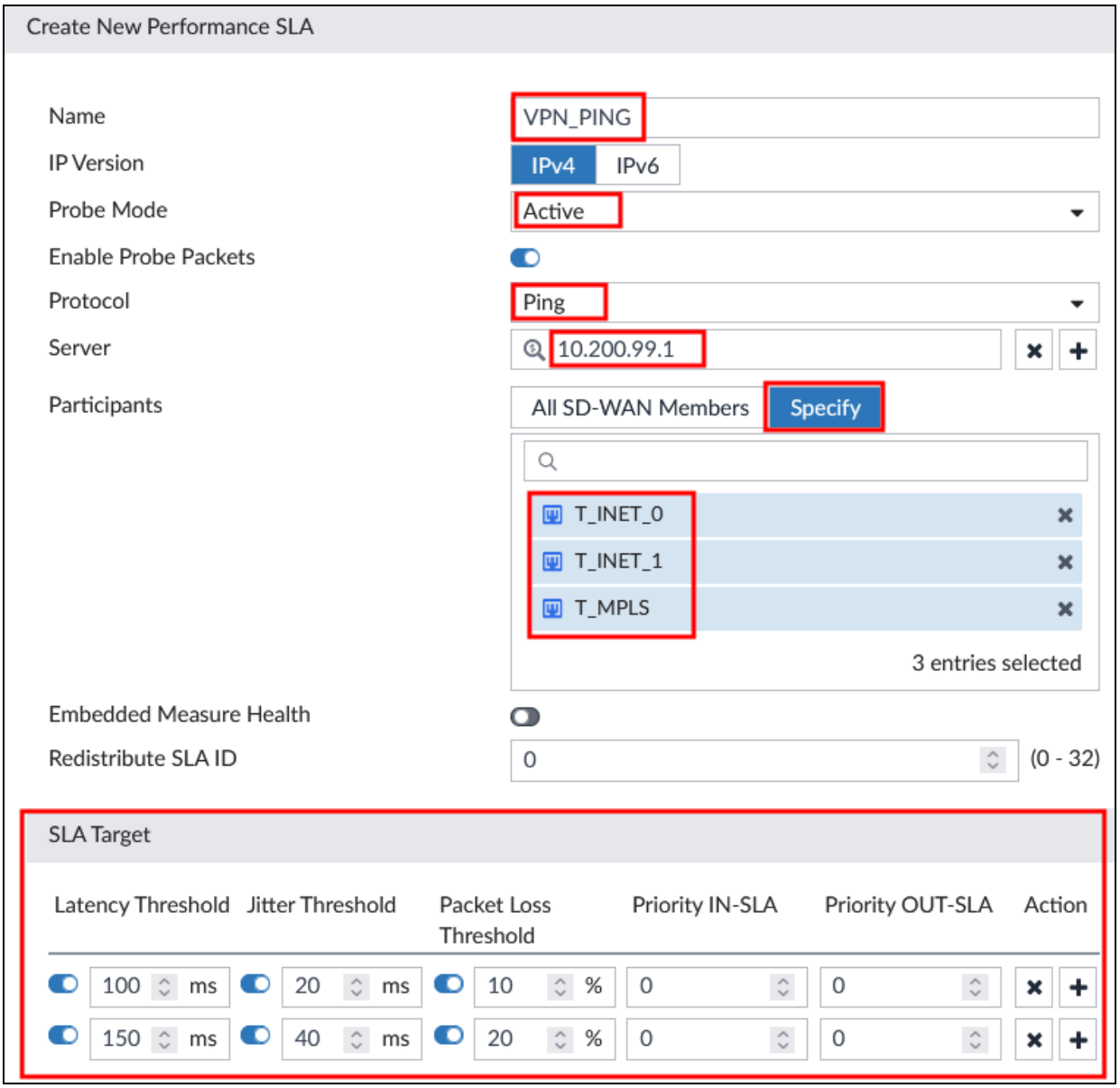
Configure an Active Performance SLA (Ping)

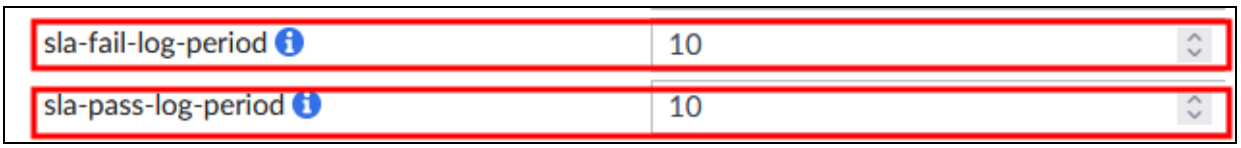
You will configure a performance SLA to monitor the health and performance of the overlays. You will configure ping as the protocol and two SLA targets.

To configure an active performance SLA (ping)

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **SD-WAN Templates**.
3. Double-click **branches** to edit the template settings.
4. In the **Performance SLA** section, click **Create New**.
5. Configure the following settings:

Field	Value
Name	VPN_PING
Probe Mode	Active
Protocol	Ping
Server	10.200.99.1
Participants	Select **Specify**, and then select **T_INET_0**, **T_INET_1**, and **T_MPLS**.
SLA Targets	1. Click **Add Target**, and then configure the following settings: • **Latency Threshold**: 100 • **Jitter Threshold**: 20 • **Packet Loss Threshold**: 10 2. Click **+** to add a second target, and then configure the following settings: • **Latency Threshold**: 150 • **Jitter Threshold**: 40 • **Packet Loss Threshold**: 20
Advanced Options	Configure the following settings: • **sla-fail-log-period**: 10 • **sla-pass-log-period**: 10





`10.200.99.1` is the address of the loopback interface on dc1_fgt. The loopback interface and firewall policies on dc1_fgt allowing the incoming probe traffic have been preconfigured for you.

The `sla-fail-log-period` and `sla-pass-log-period` settings instruct FortiGate to generate health check SLA status logs every 10 seconds. The FortiView pane on FortiAnalyzer (FortiManager, in our case) uses the logs to generate performance SLA-related graphs.

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

To install the device settings

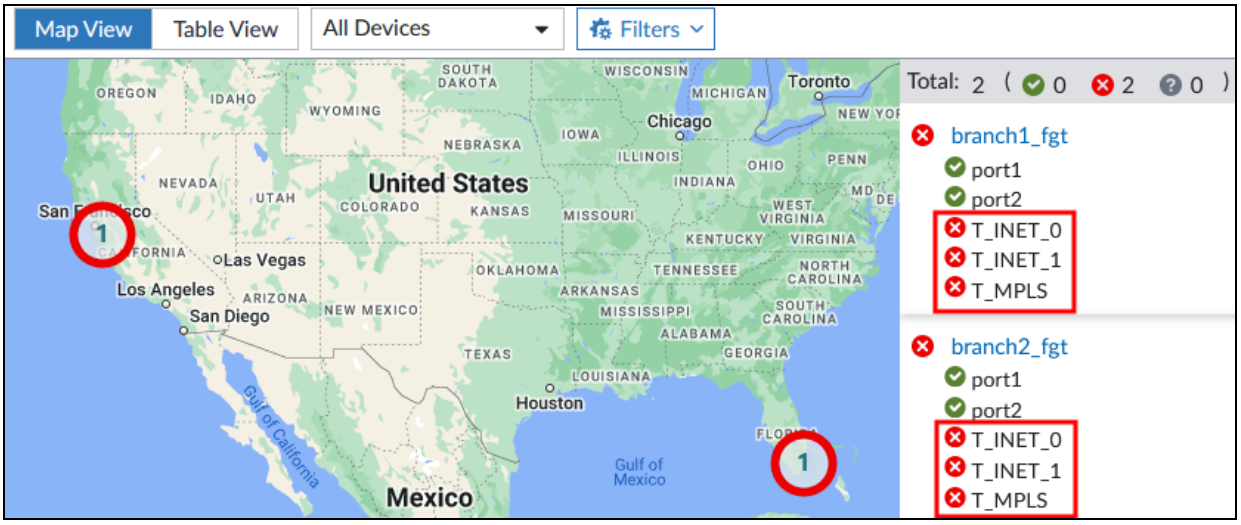
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on both devices.
5. Wait for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

Verify the Health of the Overlays

You will use the SD-WAN monitor on FortiManager to check the health of the overlays.

To verify the health of the overlays

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



You configured a performance SLA for the overlays. However, the overlays are currently marked as down (red x). Next, you will find out the reason.

2. Open an SSH session to branch1_fgt.
3. Log in with the username `admin` and password `password`.
4. Enter the following command to capture probe packets to 10.200.99.1:
   `diagnose sniffer packet any "host 10.200.99.1 and icmp" 4 10`

The `10` at the end of the command indicates the number of packets to capture. That is, the sniffer command will stop after capturing 10 packets.

Your output should look similar to the following example:

```
branch1_fgt # diagnose sniffer packet any "host 10.200.99.1 and icmp" 4 10
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.200.99.1 and icmp]
0.269825 T_MPLS out 192.2.0.1 -> 10.200.99.1: icmp: echo request
0.269857 T_INET_1 out 192.2.0.1 -> 10.200.99.1: icmp: echo request
0.269887 T_INET_0 out 192.2.0.1 -> 10.200.99.1: icmp: echo request
0.772872 T_MPLS out 192.2.0.1 -> 10.200.99.1: icmp: echo request
0.772921 T_INET_1 out 192.2.0.1 -> 10.200.99.1: icmp: echo request
0.772994 T_INET_0 out 192.2.0.1 -> 10.200.99.1: icmp: echo request
1.265240 T_MPLS out 192.2.0.1 -> 10.200.99.1: icmp: echo request
1.265409 T_INET_1 out 192.2.0.1 -> 10.200.99.1: icmp: echo request
1.265484 T_INET_0 out 192.2.0.1 -> 10.200.99.1: icmp: echo request
1.769091 T_MPLS out 192.2.0.1 -> 10.200.99.1: icmp: echo request
```

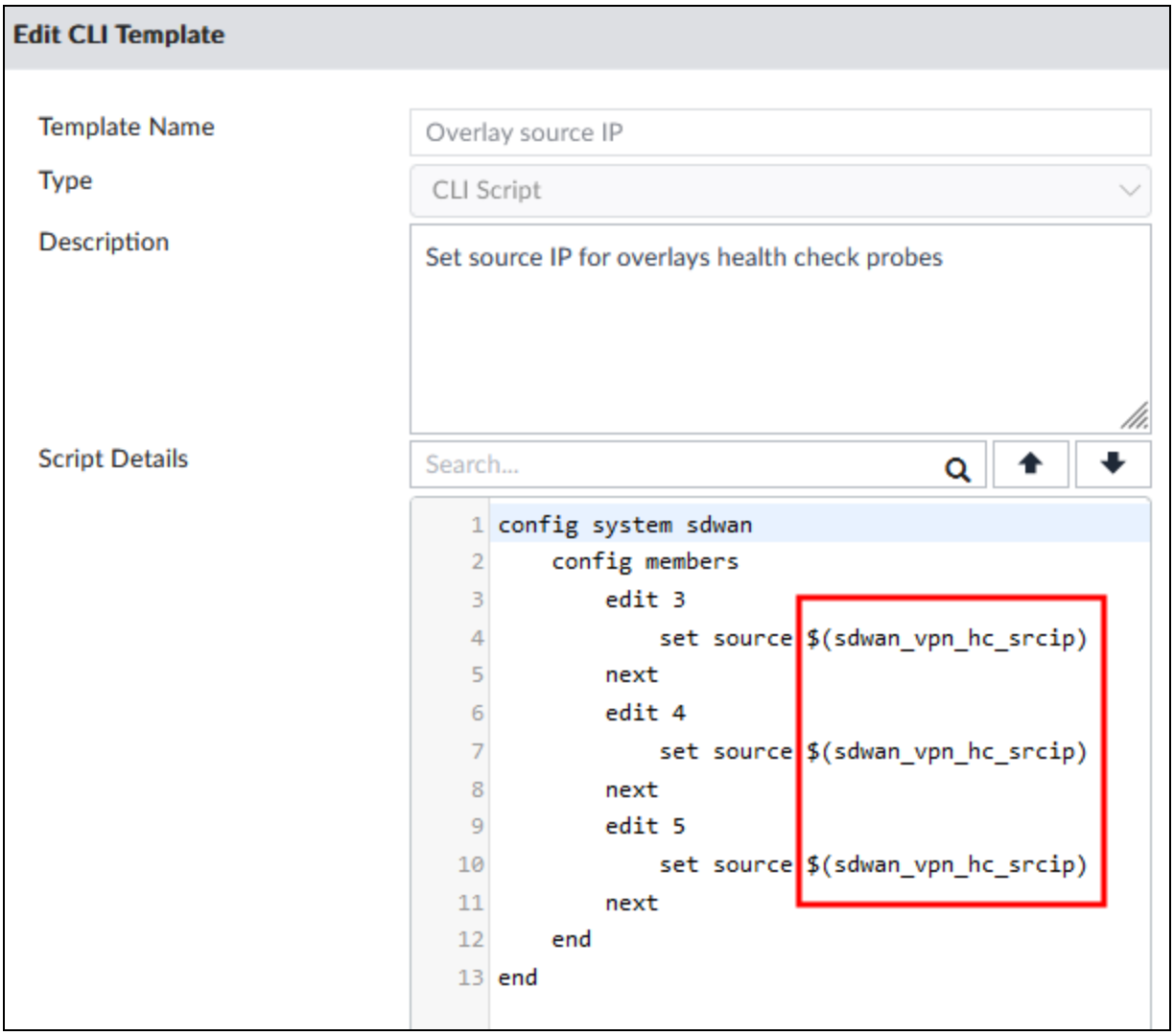
Stop and think!

FortiGate is sending ICMP echo requests to `10.200.99.1`, but there are no replies. Why?

The overlays don't have an IP address assigned to them. Therefore, FortiGate uses the address of the interface with the lowest index number (port1) as the source address (`192.2.0.1`). However, the `192.2.0.1` address is not routable within the overlay, which is why there are no replies. Next, you will fix this issue by using metadata variables and a CLI template to assign a source address for probes on overlays. In another lab, you will assign an address to the overlays.

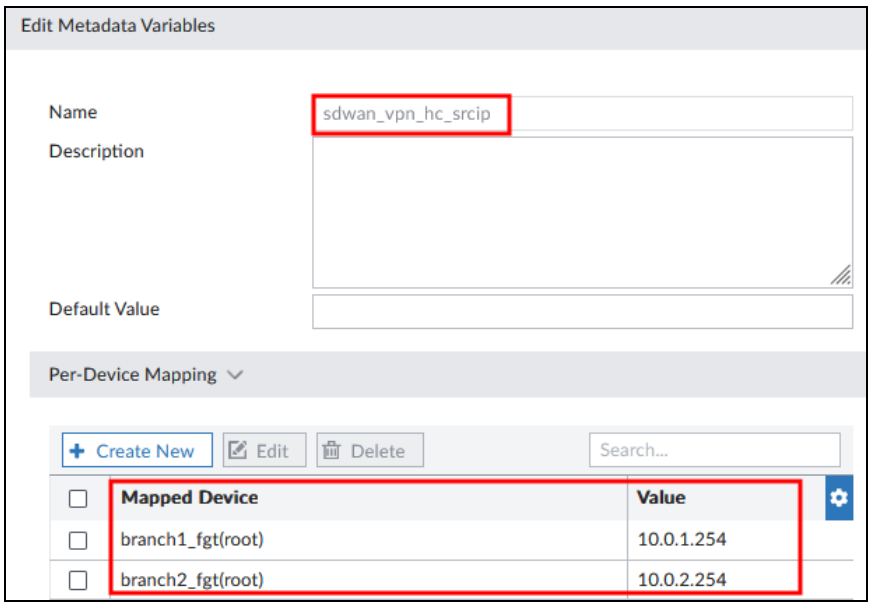
To configure the source IP for health check probes on the overlays

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **CLI Templates**.
2. Expand **CLI Template**, and then double-click **Overlay source IP** to view the CLI template details.
   Your page should look similar to the following example:



The CLI template configures the `source` setting on each overlay (members `3`, `4`, and `5`). The CLI template also references the metadata variable `sdwan-vpn-hc-srcip`. Both the CLI template and the metadata variable have been preconfigured for you.

`sdwan-vpn-hc-srcip` resolves to the LAN interface address (port5 address) on each branch. You can view the metadata variable details on the **Policy & Objects** page. Click **Device Manager** > **Policy & Objects**, and then click **Object Configurations** > **Advanced** > **Metadata Variables**. Double-click the `sdwan-vpn-hc-srcip` metadata variable to view its settings. Your page should look similar to the following example:

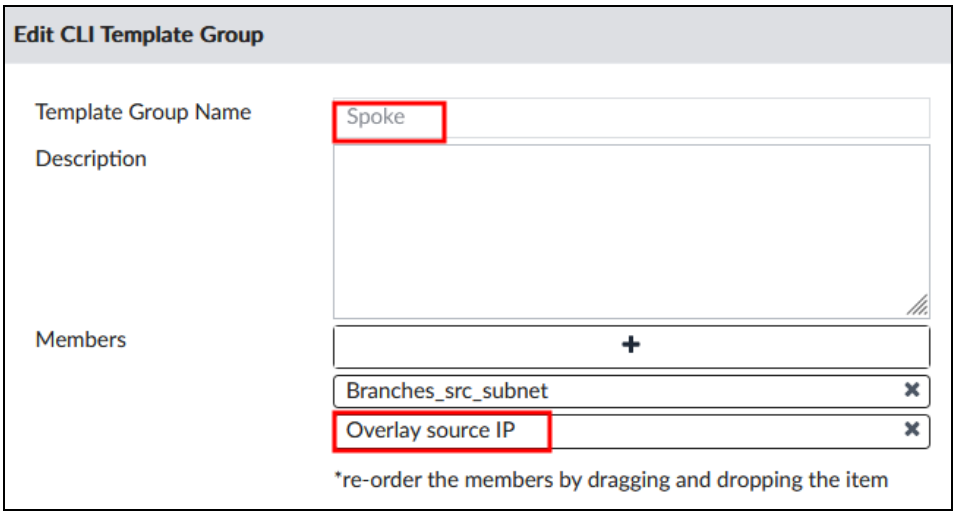


3. Click **Cancel** to exit the CLI template page.

You can see that a CLI template group is already configured and assigned to the branches devices (branch1_fgt and branch2_fgt). Because you can assign only one CLI template or CLI template group to a FortiGate, if you need to assign multiple CLI templates to a device, you must combine them in a CLI template group.

The **Branches_src_subnet** template is required to add the branches source subnet to IPsec tunnels configurations.

4. Double-click the **Spoke** CLI template group to edit it.
5. Click **+** to add a member to the template, and then select **Overlay source IP**.
   Your page should look similar to the following example:



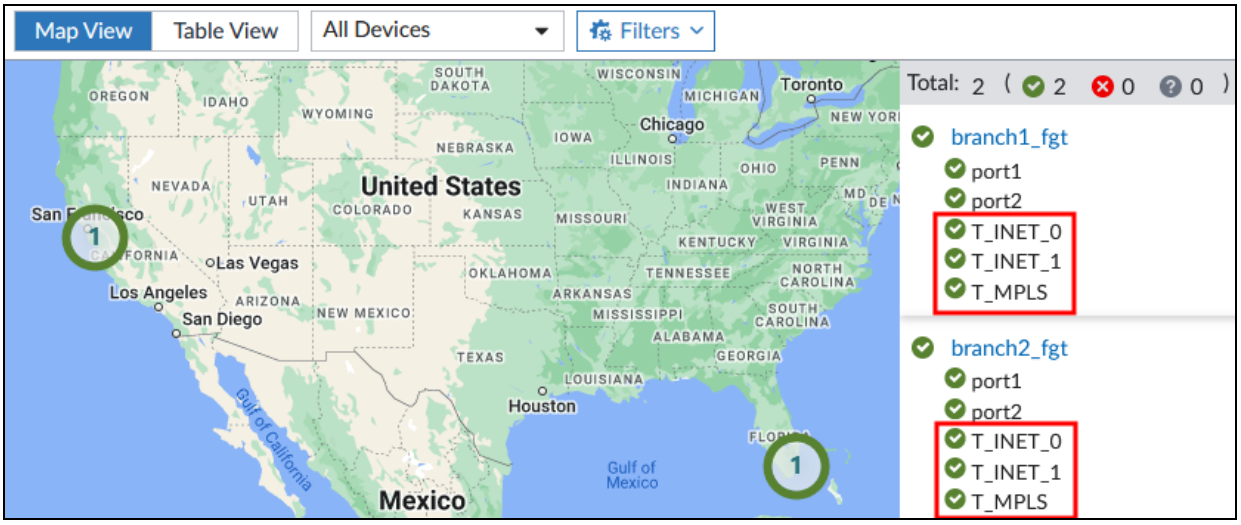
6. Click **OK** to validate the CLI template selection.
7. Click **OK** to validate the template group update.

To install the device settings

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

To verify the health of the overlays

1. Continuing on the FortiManager GUI, go to the **SD-WAN Monitor** page.
   Your page should look similar to the following example:



The overlays are now shown as up (green check mark).

2. Continuing in the branch1_fgt SSH window, enter the following command to capture probe packets to 10.200.99.1:
`diagnose sniffer packet any "host 10.200.99.1 and icmp" 4 10`
Your output should look similar to the following example:

```
branch1_fgt # diagnose sniffer packet any "host 10.200.99.1 and icmp" 4 10
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.200.99.1 and icmp]
0.150293 T_MPLS out 10.0.1.254 -> 10.200.99.1: icmp: echo request
0.150826 T_INET_1 out 10.0.1.254 -> 10.200.99.1: icmp: echo request
0.150930 T_INET_0 out 10.0.1.254 -> 10.200.99.1: icmp: echo request
0.152306 T_MPLS in 10.200.99.1 -> 10.0.1.254: icmp: echo reply
0.152338 T_INET_1 in 10.200.99.1 -> 10.0.1.254: icmp: echo reply
0.152551 T_INET_0 in 10.200.99.1 -> 10.0.1.254: icmp: echo reply
0.645708 T_MPLS out 10.0.1.254 -> 10.200.99.1: icmp: echo request
0.645850 T_INET_1 out 10.0.1.254 -> 10.200.99.1: icmp: echo request
0.645934 T_INET_0 out 10.0.1.254 -> 10.200.99.1: icmp: echo request
0.646971 T_MPLS in 10.200.99.1 -> 10.0.1.254: icmp: echo reply
```

The probes now use the LAN interface address as the source, and now there are replies. For branch1_fgt, the source address is `10.0.1.254`, and for branch2_fgt, it should be `10.0.2.254`. You can run the same sniffer command on branch2_fgt to verify the source address.

Exercise 3: Testing an Active Performance SLA

In this exercise, you will use FortiManager and the FortiGate CLI to monitor the status of the **VPN_PING** performance SLA and overlays before and after you increase the latency on the overlays.

Monitor a Performance SLA on the FortiGate CLI

In the previous exercise, you configured a performance SLA to monitor the health and performance of overlays. You will now monitor SD-WAN link behavior when the performance changes.

To monitor a performance SLA on the FortiGate CLI

1. Open an SSH session to branch1_fgt.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to display the status of the **VPN_PING** performance SLA:
   `diagnose sys sdwan health-check status VPN_PING`
   Your output should look similar to the following example:

```
branch1_fgt # branch1_fgt # diagnose sys sdwan health-check status VPN_PING
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(1.499), jitter(0.357), mos(4.403),
 bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x3
Seq(4 T_INET_1): state(alive), packet-loss(0.000%) latency(1.988), jitter(0.265), mos(4.403
), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.903), jitter(0.288), mos(4.403
), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

The output includes the different metrics (packet loss, latency, jitter, mos, and bandwidth) that the **VPN_PING** performance SLA measures on each overlay. Note that all overlays indicate `sla_map=0x3`, which means that the overlays meet the two SLA targets configured.

4. Enter the following commands to display additional information about the health of the **T_INET_0** overlay:
   ```
   diagnose sys link-monitor interface T_INET_0
   diagnose sys sdwan sla-log VPN_PING 3
   diagnose sys sdwan intf-sla-log T_INET_0
   ```
   Your output should look similar to the following example:

```
branch1_fgt # branch1_fgt # diagnose sys link-monitor interface T_INET_0
Interface(T_INET_0): state(up, since Tue Jan 17 07:21:50 2023), bandwidth(up:640bps, down:
640bps), session count(IPv4:1, IPv6:0), tx(454179 bytes), rx(413120 bytes), latency(1.68),
 jitter(0.32), packet-loss(0.00).
```

```
Timestamp: Tue Jan 17 08:49:40 2023, vdom root, health-check VPN_PING, interface: T_INET_0
, status: up, latency: 1.809, jitter: 0.479, packet loss: 0.000%, mos: 4.403.
Timestamp: Tue Jan 17 08:49:40 2023, vdom root, health-check VPN_PING, interface: T_INET_0
, status: up, latency: 1.786, jitter: 0.452, packet loss: 0.000%, mos: 4.403.
Timestamp: Tue Jan 17 08:49:41 2023, vdom root, health-check VPN_PING, interface: T_INET_0
, status: up, latency: 1.800, jitter: 0.416, packet loss: 0.000%, mos: 4.403.
Timestamp: Tue Jan 17 08:49:41 2023, vdom root, health-check VPN_PING, interface: T_INET_0
, status: up, latency: 1.778, jitter: 0.395, packet loss: 0.000%, mos: 4.403.
Timestamp: Tue Jan 17 08:49:42 2023, vdom root, health-check VPN_PING, interface: T_INET_0
, status: up, latency: 1.769, jitter: 0.381, packet loss: 0.000%, mos: 4.403.
Timestamp: Tue Jan 17 08:49:42 2023, vdom root, health-check VPN_PING, interface: T_INET_0
, status: up, latency: 1.786, jitter: 0.408, packet loss: 0.000%, mos: 4.403.
```

```
Timestamp: Tue Jan 17 08:51:30 2023, used inbandwidth: 640bps, used outbandwidth: 640bps,
used bibandwidth: 1280bps, tx bytes: 471579bytes, rx bytes: 430520bytes.
Timestamp: Tue Jan 17 08:51:40 2023, used inbandwidth: 640bps, used outbandwidth: 640bps,
used bibandwidth: 1280bps, tx bytes: 472379bytes, rx bytes: 431320bytes.
Timestamp: Tue Jan 17 08:51:50 2023, used inbandwidth: 640bps, used outbandwidth: 640bps,
used bibandwidth: 1280bps, tx bytes: 473179bytes, rx bytes: 432120bytes.
Timestamp: Tue Jan 17 08:52:00 2023, used inbandwidth: 640bps, used outbandwidth: 640bps,
used bibandwidth: 1280bps, tx bytes: 473979bytes, rx bytes: 432920bytes.
Timestamp: Tue Jan 17 08:52:10 2023, used inbandwidth: 640bps, used outbandwidth: 640bps,
used bibandwidth: 1280bps, tx bytes: 474779bytes, rx bytes: 433720bytes.
Timestamp: Tue Jan 17 08:52:20 2023, used inbandwidth: 640bps, used outbandwidth: 640bps,
used bibandwidth: 1280bps, tx bytes: 475579bytes, rx bytes: 434520bytes.
```

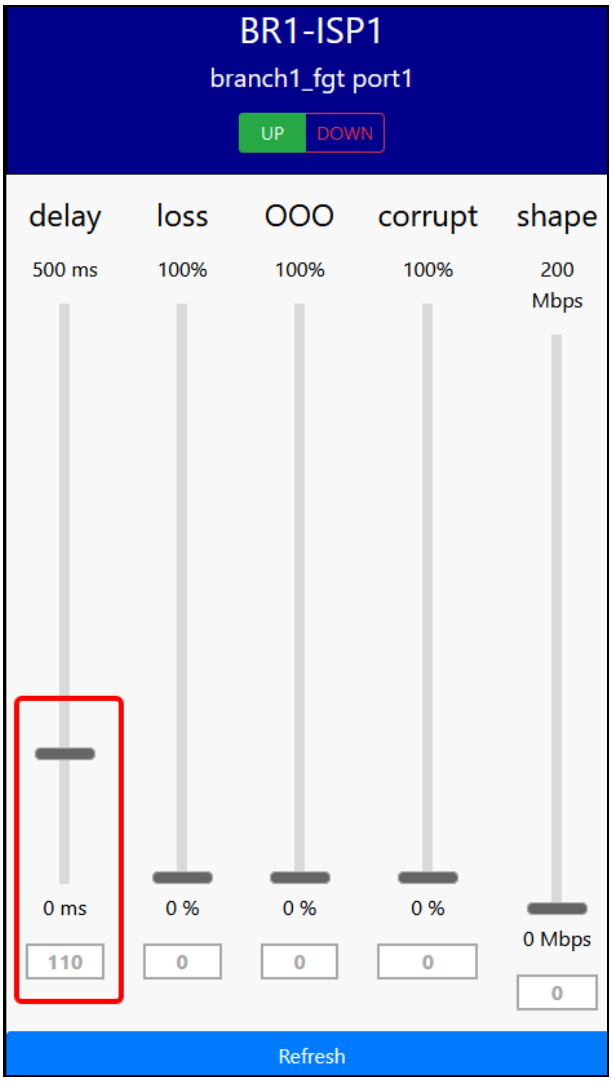
- The first command (first output) reports on the **T_INET_0** metrics that the link-monitor process (lnkmtd) measures. Remember that the performance SLA relies on the link-monitor process to measure the member metrics.
- The second command (second output) shows the latency, jitter, packet loss, and mos that the link-monitor measures on member ID 3 (**T_INET_0**). The output shows the results for each probe sent for the last 10 minutes. Because the probes are sent every 500 ms, the output shows two lines per second. The output has been cut to fit the page.
- The third command (third output) shows the measured incoming, outgoing, and bidirectional bandwidth on **T_INET_0** for the last 10 minutes. Bandwidth is measured every 10 seconds. The output has been cut to fit the page.

Test the Performance SLA

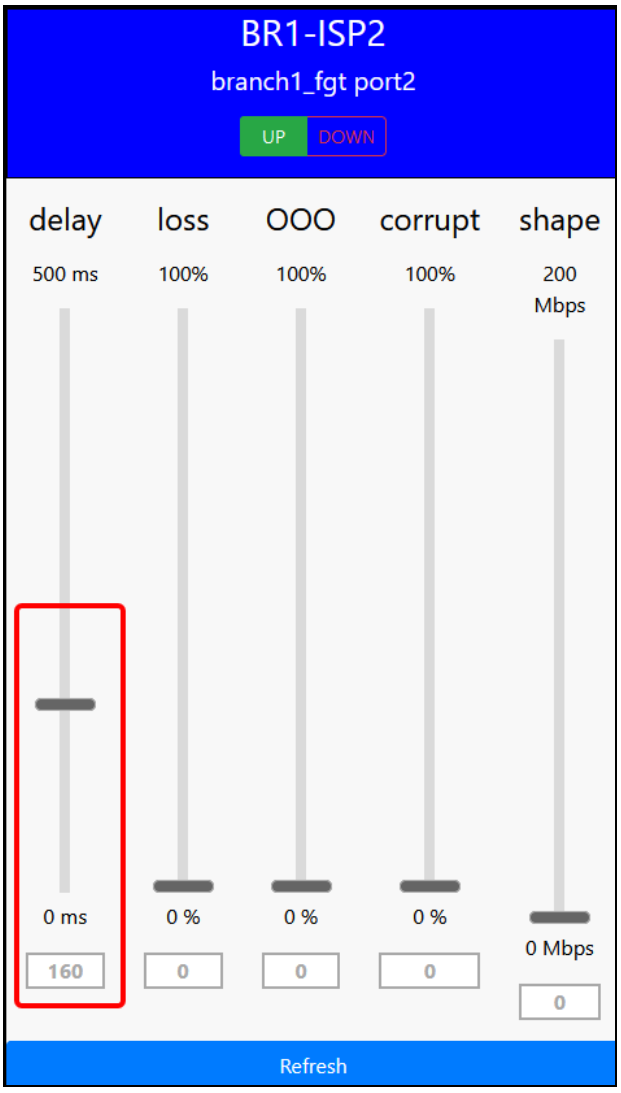
You will increase the latency on two of the overlays on branch1_fgt, and then see the changes introduced in the overlay and performance SLA status.

To increase the latency on an overlay

1. Access the wan simulator page.
2. Locate the **BR1-ISP1** and **BR1-ISP2** control panels.
3. On **BR1-ISP1**, use the vertical bar to increase the **delay** to 110 ms.



4. On **BR1-ISP2**, use the vertical bar to increase the **delay** to 160 ms.



5. Continuing on the branch1_fgt SSH session, enter the following command to display the status of the **VPN_PING** performance SLA:

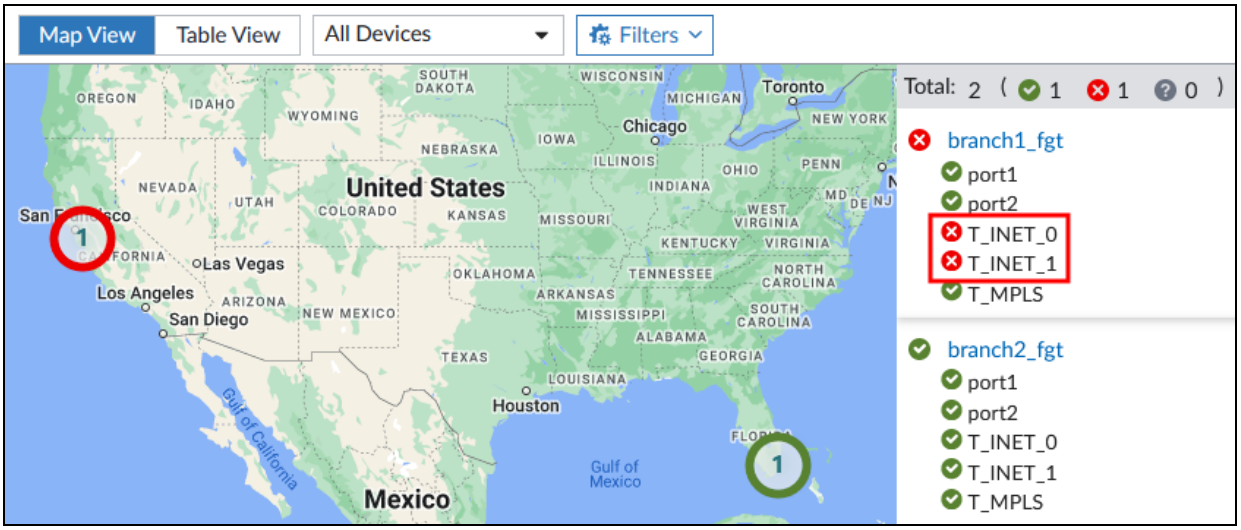
```
diagnose sys sdwan health-check status VPN_PING
```

Your output should look similar to the following example:

```
branch1_fgt # branch1_fgt # diagnose sys sdwan health-check status VPN_PING
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(1.389), jitter(0.263), mos(4.403)
, bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x3
Seq(4 T_INET_1): state(alive), packet-loss(0.000%) latency(162.019), jitter(0.324), mos(4.
285), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x0
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(111.984), jitter(0.334), mos(4.
342), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x2
```

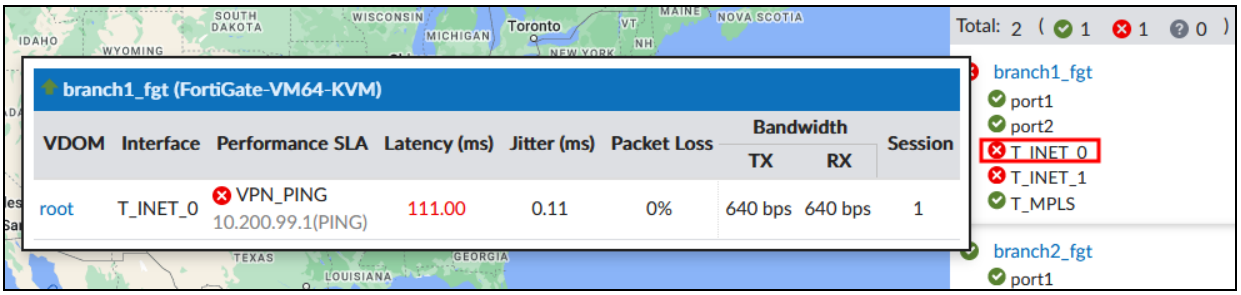
The performance SLA status reflects the increased latency on **T_INET_0** and **T_INET_1**. The `sla_map` on **T_INET_0** and **T_INET_1** also changed. The former indicates that only one SLA target is met. The latter indicates that no SLA targets are met. For **T_MPLS**, however, all SLA targets are still met.

6. On the FortiManager GUI, log in with the username `admin` and password `password`.
7. Click **root** > **Device Manager**, and then click **Monitors** > **SD-WAN Monitor**.
   Your page should look similar to the following example:

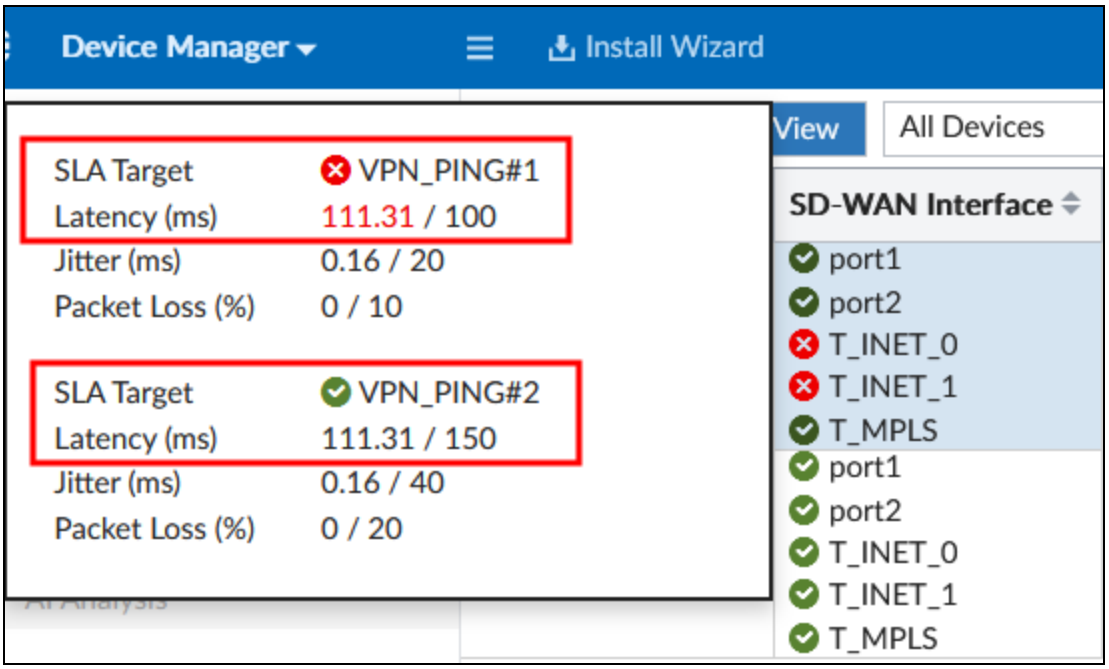


The page reports that **T_INET_0** and **T_INET_1** on **branch1_fgt** are not meeting one or more SLA targets (orange color).

8. Hover over **T_INET_0** on **branch1_fgt** to show more details about the overlay.
   Your page should look similar to the following example:

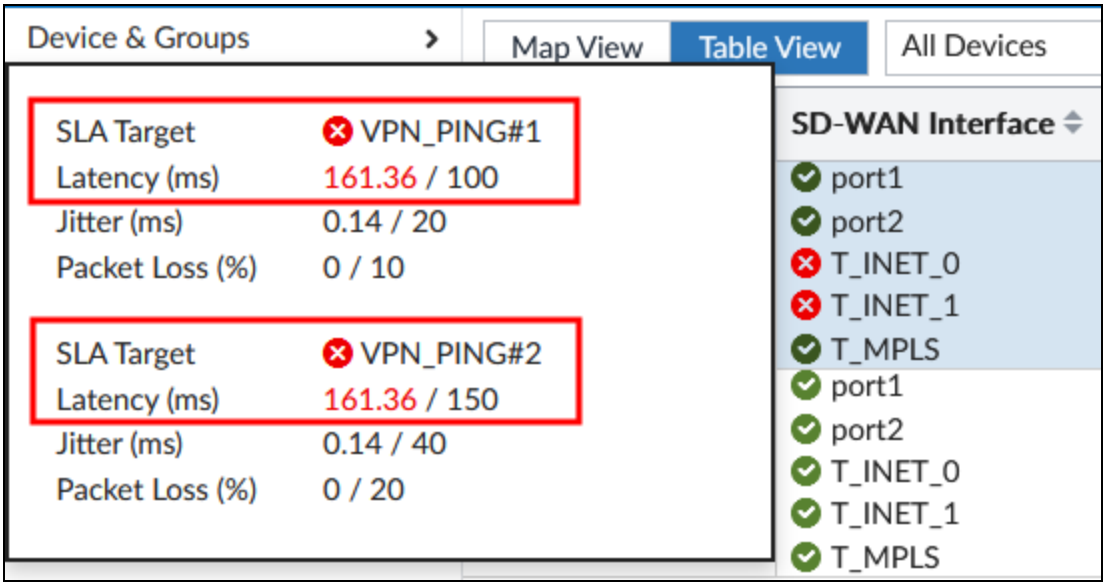


9. In the **Table View**, hover over the red cross beside **T_INET_0** to show more details about the status of the SLA targets.
   Your page should look similar to the following example:



The overlay doesn't meet the SLA target #1.

10. Repeat step 9 for the **T_INET_1** overlay.
Your page should look similar to the following example:



The overlay doesn't meet the SLA targets #1 and #2.

11. Continuing on the wan simulator page, set the latency of **BR1-ISP1** and **BR1-ISP2** back to 0 ms.
12. Use the SD-WAN monitor on FortiManager and the FortiGate CLI to confirm that both overlays now meet all SLA targets.

Exercise 4: Using HTTP to Actively Monitor the Overlays

In this exercise, you will configure a performance SLA named **VPN_HTTP** that you will use to actively monitor the overlays using the HTTP protocol. After that, you will check the performance SLA status using FortiManager and the FortiGate CLI.

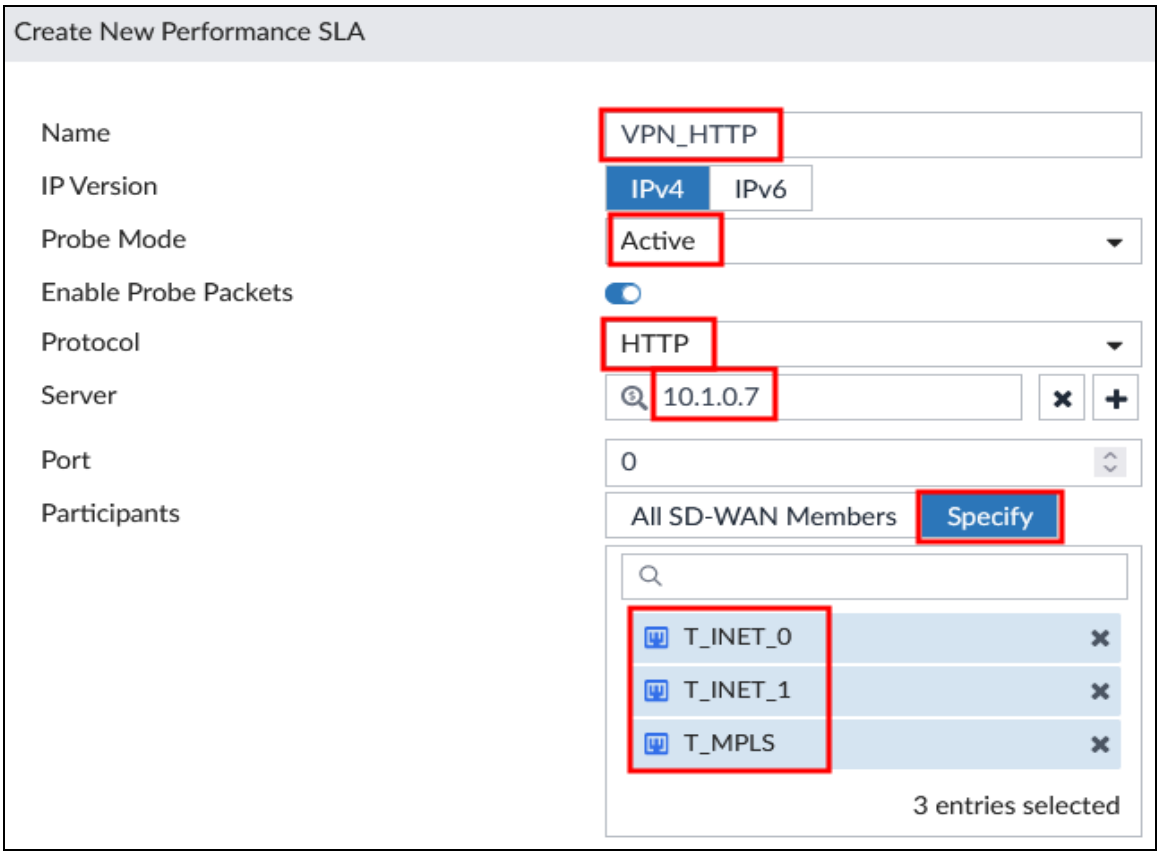
Configure an Active Performance SLA (HTTP)

You will configure a performance SLA to monitor the health and performance of the overlays. You will configure HTTP as the protocol.

To configure an active performance SLA (HTTP)

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **SD-WAN Templates**.
3. Double-click **branches** to edit the template settings.
4. In the **Performance SLA** section, click **Create New**.
5. Configure the following settings:

Field	Value
Name	VPN_HTTP
Probe Mode	Active
Protocol	HTTP
Server	10.1.0.7
Participants	Select **Specify**, and then select **T_INET_0**, **T_INET_1**, and **T_MPLS**.
Advanced Options	Configure the following setting: • **http-match**: fortinet



`10.1.0.7` is the address of dc1_host, which acts as a web server.

The `http-match` setting instructs FortiGate to look for the `fortinet` string in the HTTP response received from the server. If the response includes the string, the probe is considered successful.

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

To install the device settings

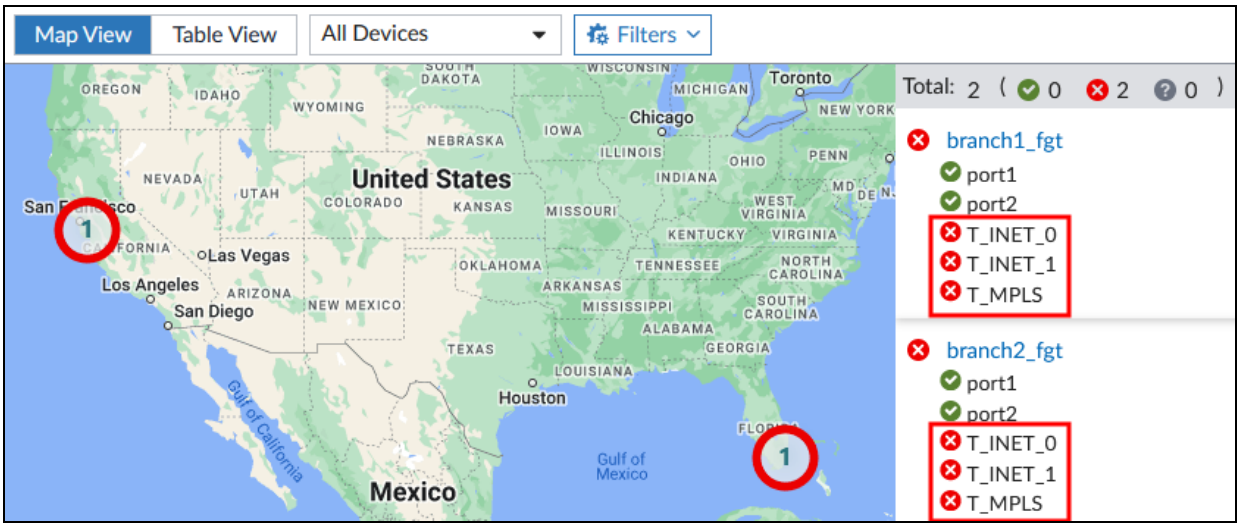
1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt** and **branch2_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on both devices.
5. Wait for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

Verify the Health of the Overlays

You will use the SD-WAN monitor on FortiManager to check the health of the overlays.

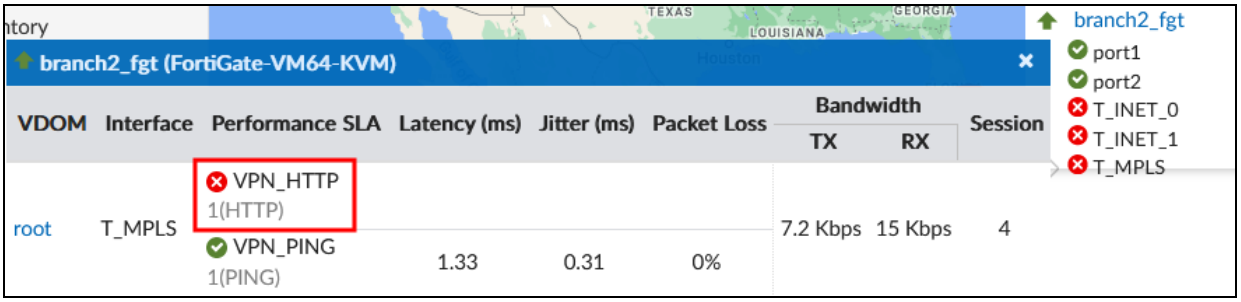
To verify the health of the overlays

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



You configured an HTTP performance SLA for the overlays. However, the overlays are currently marked as down (red x). Next, you will find out the reason.

2. Hover over the impacted overlays to get more details about their status.
   For **T_MPLS** on **branch2_fgt**, your page should look similar to the following example:



The overlay is down for the new HTTP performance SLA. Next, you will find out the reason by using the FortiGate CLI.

3. Open an SSH session to branch2_fgt.
4. Log in with the username `admin` and password `password`.
5. Enter the following command to check the status of the **VPN_HTTP** performance SLA:
   `diagnose sys sdwan health-check status VPN_HTTP`

```
branch2_fgt # diagnose sys sdwan health-check status VPN_HTTP
Health Check(VPN_HTTP):
Seq(5 T_MPLS): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(4 T_INET_1): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(3 T_INET_0): state(dead), packet-loss(100.000%) sla_map=0x0
```

The FortiGate CLI confirms that all overlays are down for the **VPN_HTTP** performance SLA.

6. Enter the following command to check the status of the overlays in SD-WAN rule 3:
   `diagnose sys sdwan service 3`

```
branch2_fgt # diag sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(3):
    1: Seq_num(3 T_INET_0), alive, selected
    2: Seq_num(4 T_INET_1), alive, selected
    3: Seq_num(5 T_MPLS), alive, selected
  Src address(1):
        10.0.2.0-10.0.2.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

Stop and think!

The **VPN_HTTP** performance SLA and SD-WAN monitor on FortiManager report the overlays as down. Yet, the SD-WAN rule status indicates that the overlays are up. Why?

SD-WAN rules consider a member as down when all of its performance SLAs report the member as down. If at least one performance SLA reports the member as up, the rule considers the member up. In this case, the **VPN_PING** performance SLA still reports the overlays as up. This means that the overlays can be used to steer traffic that matches the SD-WAN rule 3.

7. Enter the following command to capture HTTP probes to 10.1.0.7:
   `diagnose sniffer packet any "host 10.1.0.7 and port 80" 4 10`
   Your output should look similar to the following example:

```
branch2_fgt # diagnose sniffer packet any "host 10.1.0.7 and port 80" 4 10
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.1.0.7 and port 80]
0.466554 T_MPLS out 10.0.2.254.12353 -> 10.1.0.7.80: syn 3812383479
0.466946 T_INET_1 out 10.0.2.254.20186 -> 10.1.0.7.80: syn 595376044
0.467198 T_INET_0 out 10.0.2.254.12348 -> 10.1.0.7.80: syn 4062586731
0.468846 T_MPLS in 10.1.0.7.80 -> 10.0.2.254.12353: syn 421514627 ack 3812383480
0.469081 T_MPLS out 10.0.2.254.12353 -> 10.1.0.7.80: ack 421514628
0.469503 T_INET_0 in 10.1.0.7.80 -> 10.0.2.254.12348: syn 2914966047 ack 4062586732
0.469534 T_INET_0 out 10.0.2.254.12348 -> 10.1.0.7.80: ack 2914966048
0.469620 T_INET_1 in 10.1.0.7.80 -> 10.0.2.254.20186: syn 270696338 ack 595376045
0.469636 T_INET_1 out 10.0.2.254.20186 -> 10.1.0.7.80: ack 270696339
0.470478 T_MPLS out 10.0.2.254.12353 -> 10.1.0.7.80: psh 3812383480 ack 421514628
```

FortiGate is exchanging HTTP packets with `10.1.0.7`, so connectivity is fine. You will enable debug for the link monitor to troubleshoot further.

8. Enter the following commands to enable debug for HTTP probes:

```
diagnose debug application link-monitor 64
diagnose debug enable
```

Your output should look similar to the following example:

```
lnkmtd::http_handle_get_response(371): ---> recv failed mon=VPN_HTTP-5-VIRTUAL_WAN_LINK-5 errno=115
lnkmtd::http_handle_get_response(371): ---> recv failed mon=VPN_HTTP-5-VIRTUAL_WAN_LINK-5 errno=9
lnkmtd::http_send_url(405): ---> HTTP send get-url="GET / HTTP/1.1
User-Agent: FortiGate (FortiOS 7.0) Chrome/ Safari/
Host: 10.1.0.7
Keep-Alive: timeout=5
Connection: Keep-Alive
Content-Length: 0

"
lnkmtd::http_handle_get_response(371): ---> recv failed mon=VPN_HTTP-4-VIRTUAL_WAN_LINK-4 errno=11
lnkmtd::http_handle_get_response(371): ---> recv failed mon=VPN_HTTP-4-VIRTUAL_WAN_LINK-4 errno=9
lnkmtd::http_handle_get_response(371): ---> recv failed mon=VPN_HTTP-3-VIRTUAL_WAN_LINK-3 errno=9
lnkmtd::http_handle_get_response(371): ---> recv failed mon=VPN_HTTP-3-VIRTUAL_WAN_LINK-3 errno=9
```

The debug indicates that the HTTP probes fail when processing the HTTP response. That is, the HTTP response doesn't contain the expected string (`fortinet`).

9. Enter the following command to reset the debug settings and stop the debug output:

```
diagnose debug reset
```

10. Open an SSH session to branch2_client.
11. Log in with the username `root` and password `password`.
12. Enter the following command to display the HTTP response that 10.1.0.7 provided:

```
curl 10.1.0.7
```

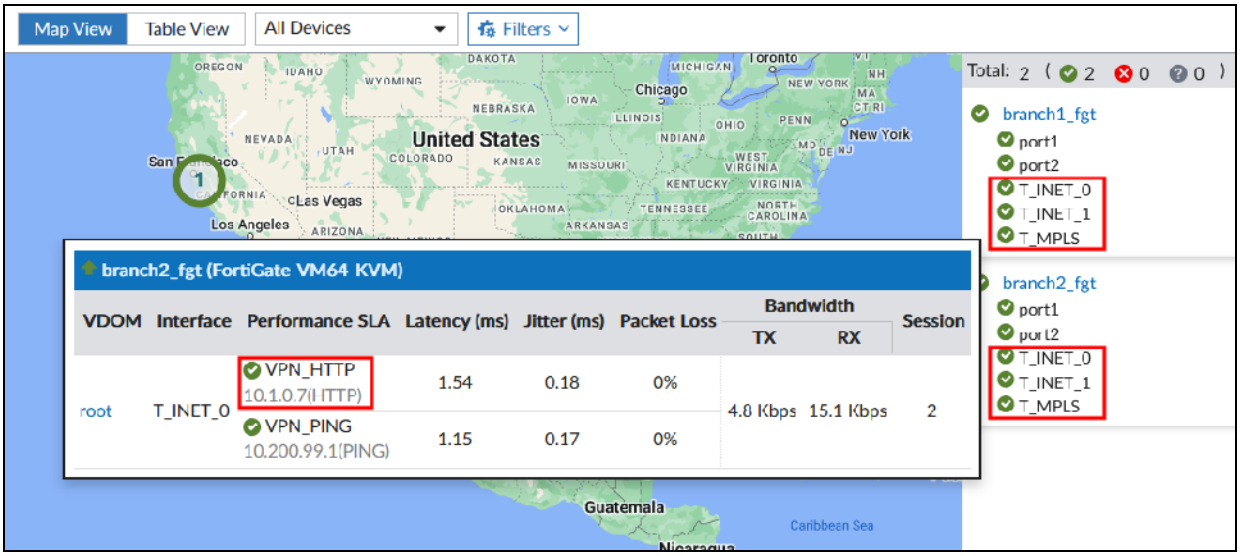
Your output should look similar to the following example:

```
root@branch2-client-cli:~# curl 10.1.0.7
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

The output doesn't include the `fortinet` string. You should use any of the strings shown in the output for the `http-match` setting. You will update the `http-match` setting to use the following string: `successfully`.

13. Continuing on the FortiManager GUI, edit the **VPN_HTTP** performance SLA, and then update the **http-match** setting to use `successfully`.
14. Install the device settings.
15. On FortiManager, confirm that the SD-WAN monitor now reports all overlays as up.

    Your page should look similar to the following example:



16. In the branch2_fgt SSH window, confirm that the **VPN_HTTP** performance SLA is now showing overlays as up.
    Your output should look similar to the following example:

```
branch2_fgt # branch2_fgt # diagnose sys sdwan health-check status VPN_HTTP
Health Check(VPN_HTTP):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(2.364), jitter(0.555), mos(4.403
), bandwidth-up(9999995), bandwidth-dw(9999985), bandwidth-bi(19999980) sla_map=0x0
Seq(4 T_INET_1): state(alive), packet-loss(0.000%) latency(2.758), jitter(0.525), mos(4.4
03), bandwidth-up(10235), bandwidth-dw(10225), bandwidth-bi(20460) sla_map=0x0
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(2.936), jitter(0.503), mos(4.4
02), bandwidth-up(10235), bandwidth-dw(10225), bandwidth-bi(20460) sla_map=0x0
```

17. In the branch2_fgt SSH window, enable debug for the HTTP probes and confirm that the probes are now successful.
    Your output should look similar to the following example:

```
lnkmtd::http_response_check(190): ---> http mon=VPN_HTTP-5-VIRTUAL_WAN_LINK-5
succeed in matching str="successfully"
lnkmtd::http_response_check(190): ---> http mon=VPN_HTTP-4-VIRTUAL_WAN_LINK-4
succeed in matching str="successfully"
lnkmtd::http_response_check(190): ---> http mon=VPN_HTTP-3-VIRTUAL_WAN_LINK-3
succeed in matching str="successfully"
```

18. Enter the following command to reset the debug settings and stop the debug output:

```
diagnose debug reset
```

Lab 4: Routing and Sessions

In this lab, you will put the concepts that you learned in lesson 4 into practice by troubleshooting the following SD-WAN deployments:

- Spoke-to-spoke traffic (single hub)
- Direct internet access (DIA) traffic

For each exercise, you will load the required configuration, troubleshoot the issues reported, identify the root cause, and fix the issues.

You will not use FortiManager in this lab. You will access the FortiGate devices directly to troubleshoot and fix the issues described.

Objectives

- Configure static routing in SD-WAN
- Troubleshoot routing issues in SD-WAN
- Troubleshoot session reevaluation in SD-WAN

Time to Complete

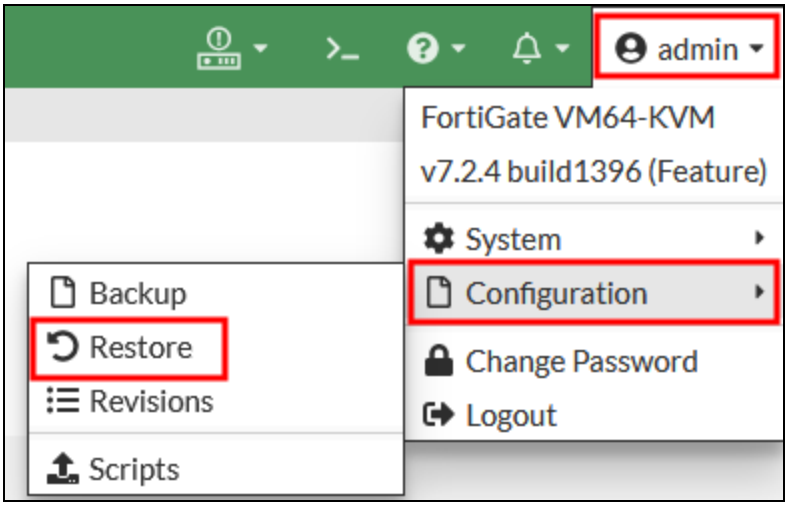
Estimated: 115 minutes

Prerequisites

Before you begin this lab, you must restore a configuration file to the branch1_fgt, branch2_fgt, and dc1_fgt.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the local-client, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

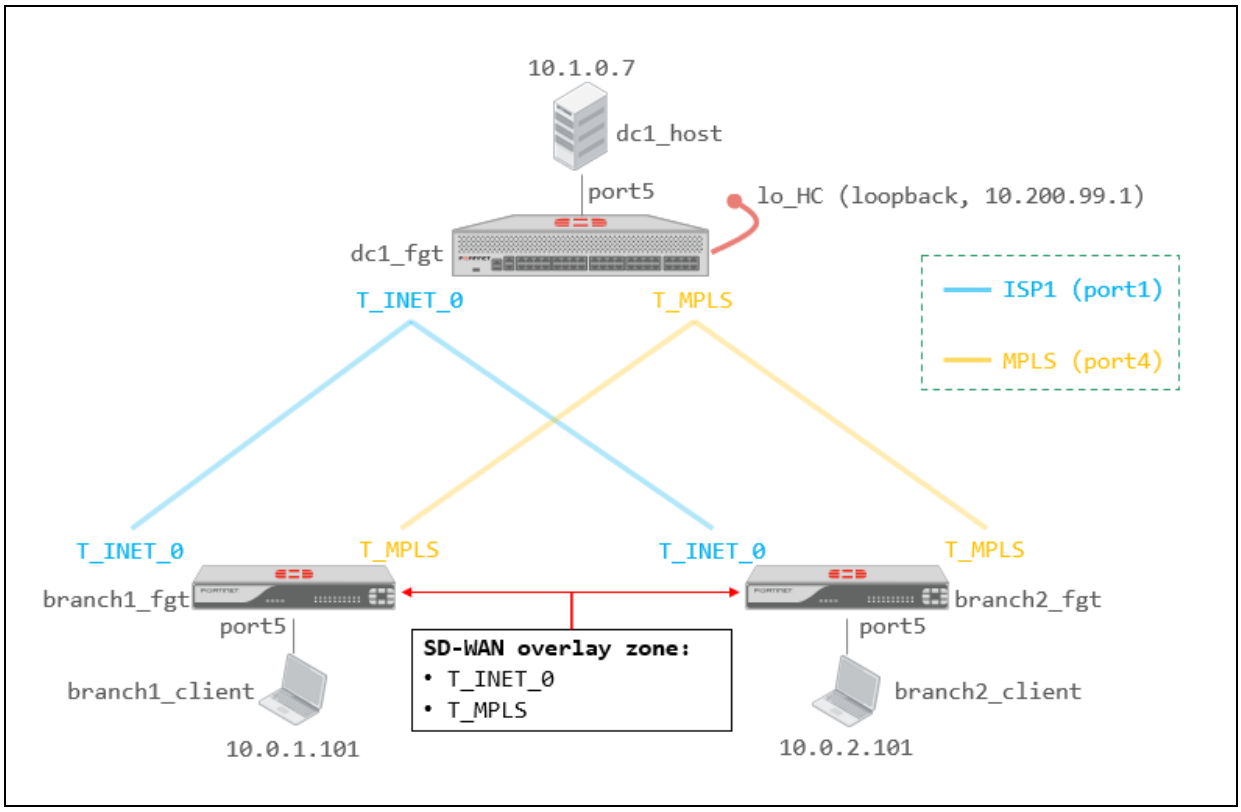


4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-4** > **Exercise-1**, select `lab4-ex1-branch1_fgt_7-2-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt and dc1_fgt.
   Use the following configuration files:

Device	Configuration file
branch2_fgt	`lab4-ex1-branch2_fgt_7-2-4_initial.conf`
dc1_fgt	`lab4-ex1-dc1_fgt_7-2-4_initial.conf`

Exercise 1: Troubleshooting Spoke-to-Spoke Traffic (Single Hub)

In this lab, you will troubleshoot spoke-to-spoke traffic in the following preconfigured topology:



Configuration

This is a hub-and-spoke deployment with two overlays. The overlays are used to route traffic between the spokes.

Problem Description

When the administrator generates traffic from branch1_client to branch2_client, the traffic is always routed over **T_MPLS**. However, the MPLS link is expensive, and therefore, the administrator wants to use **T_MPLS** for spoke-to-spoke traffic only when **T_INET_0** goes down. That is:

1. branch1_fgt must use **T_INET_0** as the primary member to route traffic to branch2_fgt.
2. branch1_fgt must use **T_MPLS** to route traffic to branch2_fgt only if **T_INET_0** is detected to be down.
3. After **T_INET_0** recovers, spoke-to-spoke traffic must be routed back through **T_INET_0**.

Objective

To complete this lab, you must fix all the issues described.

Solution Requirements

- Focus on branch1_fgt only. Don't make changes on any other device in the network.
- On branch1_fgt, don't change the existing SD-WAN rule configuration. Spoke-to-spoke traffic must match SD-WAN rule ID 3. You can change other parts of the configuration.
- To optimize the branch1_fgt configuration, static routes and firewall policies must reference SD-WAN zones and not the individual members.
- To fix all issues reported, you must perform multiple configuration changes.

Tips for Troubleshooting

- Remember the key routing principles of SD-WAN.
- To simulate spoke-to-spoke traffic, ping branch2_client (`10.0.2.101`) from branch1_client (`10.0.1.101`).
- To simulate link failover and recovery, bring **BR1-ISP1** down and back up again on the WAN simulator.
- Use debug flow to determine how FortiGate processes packets to branch2_client.

```
diagnose debug flow filter addr 10.0.2.101
diagnose debug flow filter proto 1
diagnose debug flow trace start 100
diagnose debug console timestamp enable
diagnose debug enable
```

- Use the sniffer to capture ingress and egress packets.

```
diagnose sniffer packet any "host 10.0.2.101 and icmp" 4 0 l
```

- View session details to verify the matching SD-WAN rule and firewall policy.

```
diagnose sys session filter dst 10.0.2.101
diagnose sys session filter proto 1
diagnose sys session list
```

- Check the routing table using the following command:

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

- Check the SD-WAN configuration using the following commands:

```
show system sdwan
diagnose sys sdwan zone
diagnose sys sdwan member
diagnose firewall proute list
diagnose ip proute match <dst> <src> <link> <proto> <dport>
diagnose sys sdwan service 3
diagnose sys sdwan health-check status VPN_PING
```

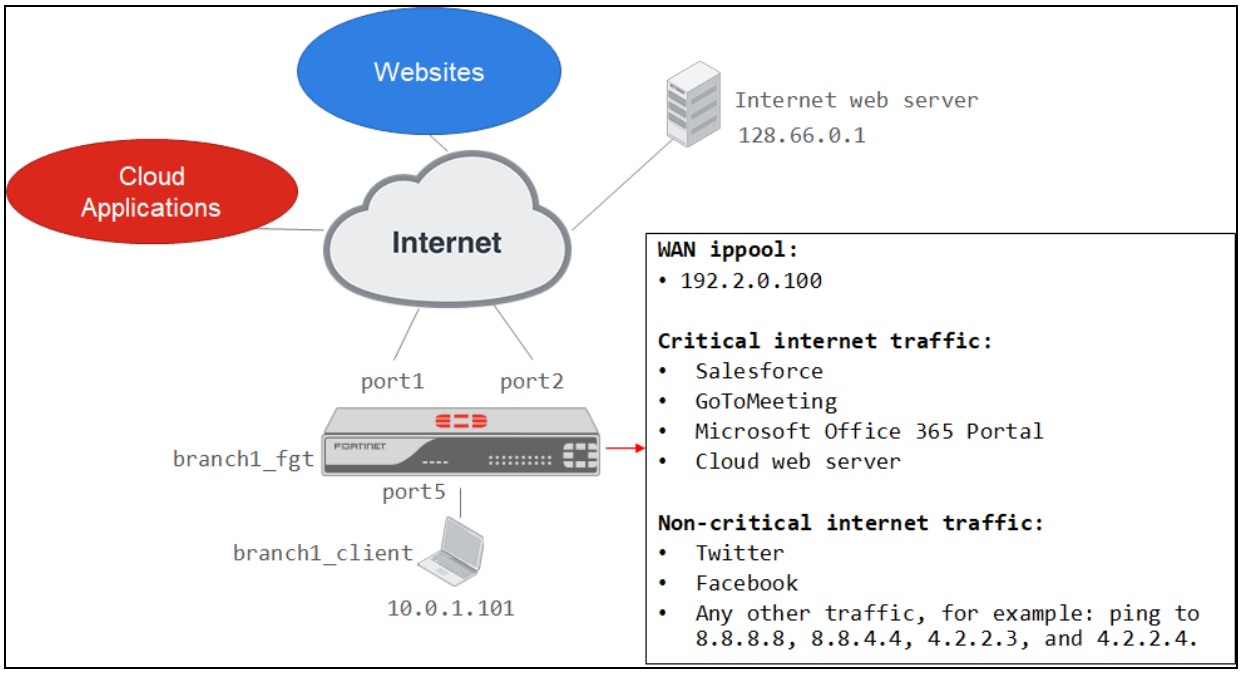
Remember to bring **BR1-ISP1** back up when you finish the exercise.

Solution

If you require assistance with this exercise, see the *Solutions* lesson in the *Study Guide*.

Exercise 2: Troubleshooting DIA Traffic

In this lab, you will troubleshoot direct internet access (DIA) traffic in the following preconfigured topology:

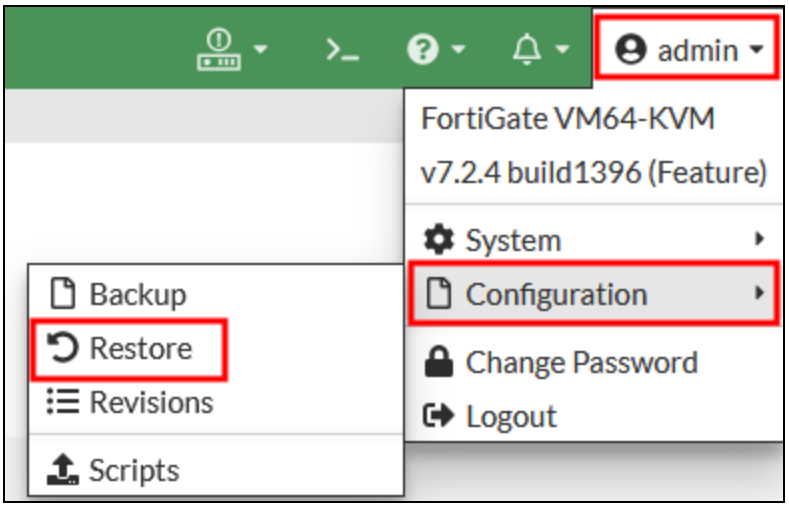


Prerequisites

Before beginning this lab, you must restore a configuration file to branch1_fgt.

To restore the branch1_fgt configuration file

1. On the local-client, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-4** > **Exercise-2**, select `lab4-ex2-branch1_fgt_7-2-4-initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.

Configuration

This is a DIA deployment with two underlays. The underlays are used to route traffic to the internet. SD-WAN rules have been configured to steer traffic for critical applications (GoToMeeting, Salesforce, and the Microsoft Office 365 portal), and for the cloud web server (`128.66.0.1`).

Problem Description

The following issues have been identified by the administrator:

- Issue 1: If both port1 and port2 are alive, and the administrator generates internet traffic, critical traffic is routed to port1, which is expected. However, non-critical traffic is load balanced across port1 and port2. The administrator wants port2 to be used only if port1 goes down.
- Issue 2: During a failover from port1 to port2 (port1 is dead), existing TCP sessions time out. For example, an SSH connection to the internet web server (`128.66.0.1`) from branch1_client times out during the failover. The administrator wants existing TCP sessions to fail over to port2 successfully and to not time out.
- Issue 3: After existing sessions fail over to port2 successfully, the administrator wants those sessions to fail back to port1 after port1 recovery.
- Issue 4: When port1 is dead, and new sessions are established through port2, the sessions don't fail over to port1 after port1 recovery. Instead, the sessions continue using port2. The administrator wants these sessions to fail over to port1.

Objective

To complete this lab, you must fix all the issues described.

Solution Requirements

- Focus on branch1_fgt only. Don't make changes on any other device in the network.
- On branch1_fgt, don't change the existing SD-WAN rule configuration. You can change other parts of the configuration.
- Internet traffic must be SNATed with ippool `192.2.0.100`.
- To fix all issues reported you need to perform multiple configuration changes.

Tips for Troubleshooting

- Remember the SNAT conditions for session reevaluation.
- To simulate critical and non-critical traffic, enter the following commands on branch1_client:

```
cd /fortipoc/fit/
./myfit.sh
```

  You can also generate internet traffic by pinging any of the following addresses: `4.2.2.3`, `4.2.2.4`, `8.8.8.8`, and `8.8.4.4`. You can then view the traffic logs to identify how traffic is being routed.

If you decide to use the traffic generator, remember to stop it when you finish the lab.

- To simulate failover and failback of existing sessions, you can initially establish an SSH connection to the internet web server (`128.66.0.1`) by running the `ssh 128.66.0.1` command from branch1_client. Then, log in using the username `root` and password `password`. The SSH session should remain up (it should continue to respond to user commands) during failover and failback. If the SSH session becomes unresponsive, it is an indication that the session timed out.
- To simulate link failure and recovery, bring **BR1-ISP1** down and back up again on the WAN simulator.
- Use debug flow to know how packets to branch2_client are processed.

```
diagnose debug flow filter addr <target-addr>
diagnose debug flow trace start 100
diagnose debug console timestamp enable
diagnose debug enable
```

- Use the sniffer to capture ingress and egress packets.

```
diagnose sniffer packet any "host <target-addr>" 4 0 l
```

- View session details to verify the matching SD-WAN rule and firewall policy.

```
diagnose sys session filter dst <target-addr>
diagnose sys session list
```

- Check the routing table using the following command:

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

- Check the system configuration.

```
show system sdwan
show firewall policy
show system interface
diagnose sys sdwan zone
diagnose sys sdwan member
diagnose sys sdwan service
diagnose sys sdwan health-check status Level3_DNS
```

Remember to bring **BR1-ISP1** back up when you finish the exercise. Also, remember to stop the traffic generator on branch1_client by pressing `Ctrl+C` in the SSH session.

Solution

If you require assistance with this exercise, see the *Solutions* lesson in the *Study Guide*.

Lab 5: Rules

In this lab, you will configure and test the following rule strategies: best quality, lowest cost (SLA), and maximize bandwidth (SLA). After that, you will troubleshoot rules on a hub-and-spoke topology that uses SD-WAN to steer DIA, RIA, and site-to-site traffic.

For each exercise, you will load the required configuration. You will use FortiManager for the first exercise only.

Objectives

- Configure and test best quality, lowest cost (SLA), and maximize bandwidth (SLA) rules
- Troubleshoot rules

Time to Complete

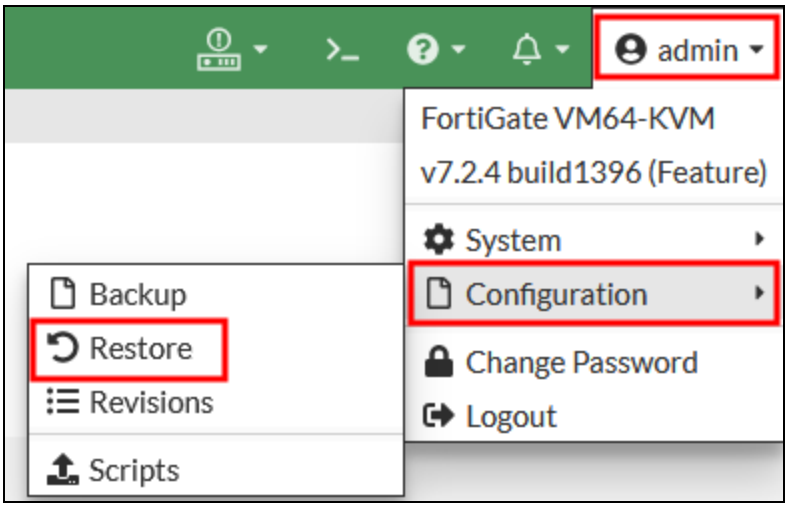
Estimated: 80 minutes

Prerequisites

Before you begin this lab, you must restore the configuration files for branch1_fgt and dc1_fgt, as well as FortiManager.

To restore the branch1_fgt and dc1_fgt configuration files

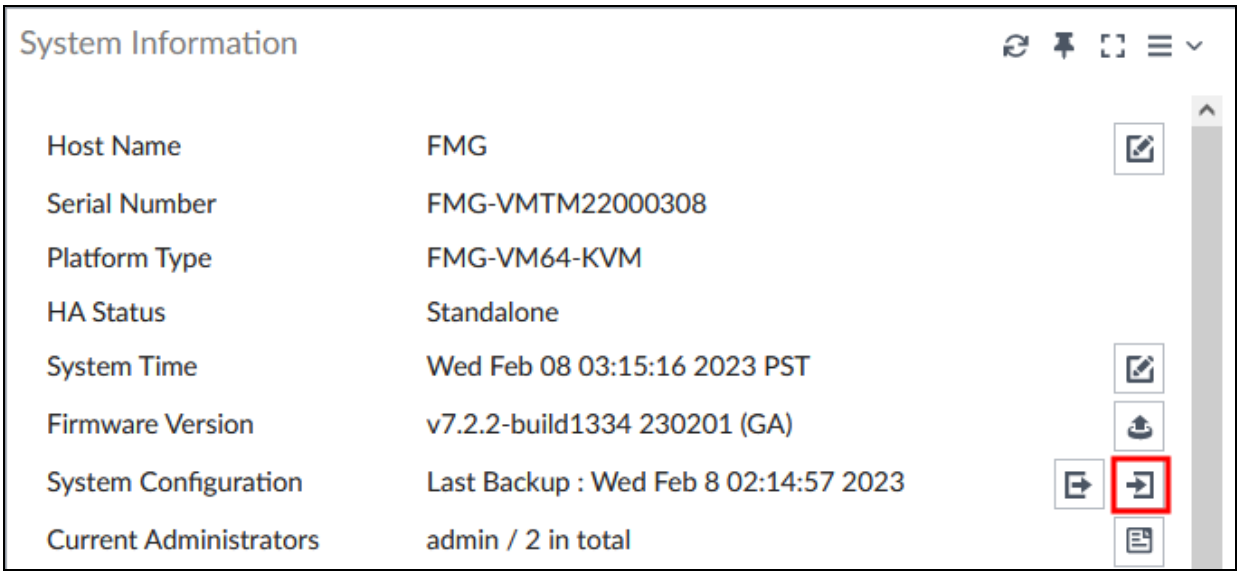
1. On the Local-Client VM, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-5** > **Exercise-1**, select `lab5-ex1-branch1_fgt_7-2-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on dc1_fgt.
   Use the following configuration file: `lab5-ex1-dc1_fgt_7-2-4_initial.conf`.

To restore the FortiManager configuration file

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root** > **System Settings**, and then click **Dashboard**.
3. In the **System Information** widget, click the **configuration restore** icon.

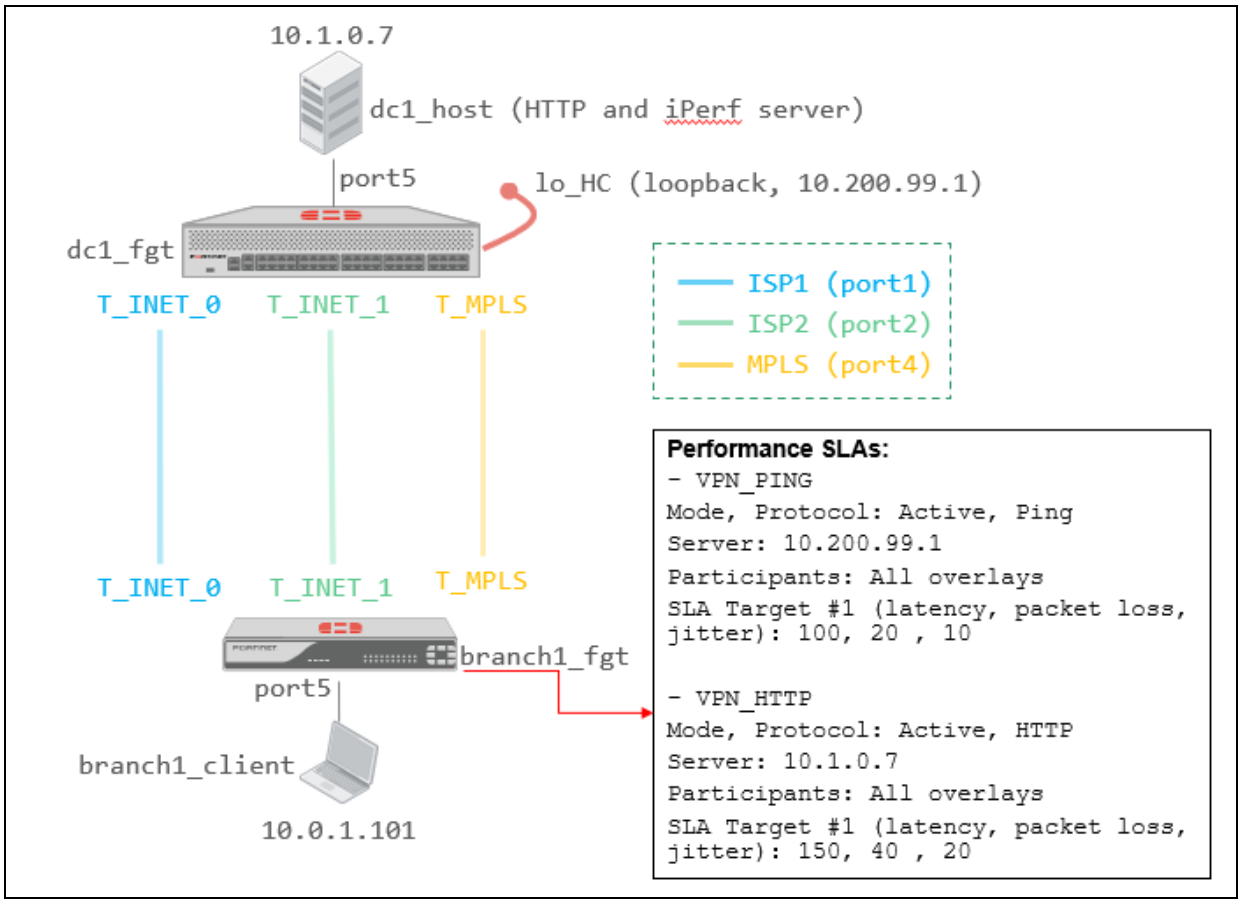


4. Click **Browse** to find the local file to upload.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-5** > **Exercise-1**, select `lab5-ex1-SYS_FMG_7-2-2_initial.dat`, and then click **OK**.
6. Wait until the file is uploaded and FortiManager finishes rebooting.
7. Log in to the FortiManager GUI with the username `admin` and password `password`.
8. Click **root** > **System Settings**, and then click **Advanced** > **Advanced Settings**.
9. For the **Offline Mode** option, select **Disable**.
10. Click **Apply** to save the settings.

Exercise 1: Configuring and Testing Rule Strategies

In this exercise, you will configure an SD-WAN rule to steer traffic between branch1_client and dc1_host. You will first use best quality as the strategy, then lowest cost (SLA), and finally maximize bandwidth (SLA). You will test each strategy by generating traffic between branch1_client and dc1_host, while at the same time changing the link metrics using the WAN simulator and observing the changes in the outgoing interface list and traffic steering.

The following topology has been preconfigured for you:



Configure and Test a Best Quality Rule

You will configure a rule that uses best quality as the strategy and latency as the metric. Next, you will test the rule by generating ping traffic and changing the condition of the links.

To configure a best quality rule

1. Access the FortiManager GUI, and then log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **SD-WAN Templates**.
3. Double-click **branches** to edit the template settings.

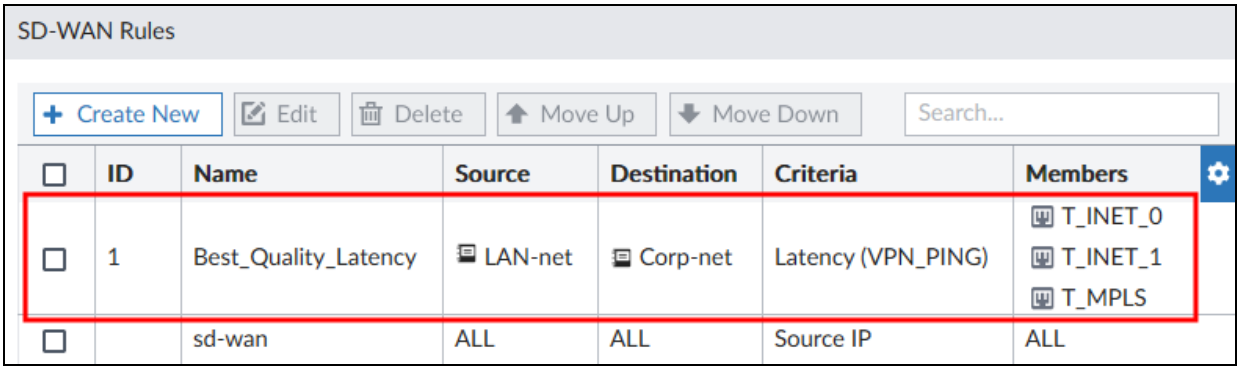
4. In the **SD-WAN Rules** section, click **Create New**.
5. Configure the following settings:

Field	Value
Name	Best_Quality_Latency
Source	In the **Source Address** field, select **LAN-net**.
Destination	• Click **Address**. • In the **Address** field, select **Corp-net**.
Outgoing Interfaces	• For **Strategy**, select **Best Quality**. • In the **Interface Preference** field, select **T_INET_0**, **T_INET_1**, and **T_MPLS**. • Drag and drop to organize the interface in following order: **T_INET_0**, **T_INET_1**, **T_MPLS**.
Measured SLA	Select **VPN_PING**.
Quality Criteria	Select **Latency**.

Make sure that you set the configuration priority (or interface preference list configuration) as follows (most preferred first):

- **T_INET_0**
- **T_INET_1**
- **T_MPLS**

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



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

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.

3. Select **branch1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on **branch1_fgt**.
5. Wait for the installation to finish.
6. Click **Finish**.

To test a best quality rule

1. Open two SSH sessions to branch1_fgt.
2. Log in with the username `admin` and password `password`.
3. Access the WAN simulator page.
4. Locate the **BR1-ISP1**, **BR1-ISP2**, and **BR1-MPLS** control panels.
5. Use the vertical bar to increase the **delay** of each link to the following values:

Link Name	Latency
BR1-ISP1	100 ms
BR1-ISP2	110 ms
BR1-MPLS	120 ms

6. On the first SSH session on branch1_fgt, enter the following command to display the rule status:
`diagnose sys sdwan service`
Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0), alive, latency: 102.086, selected
    2: Seq_num(4 T_INET_1), alive, latency: 111.960, selected
    3: Seq_num(5 T_MPLS), alive, latency: 121.404, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

By default, FortiGate calculates the member latency and jitter based on the last 30 health check probes. For this reason, you may have to wait a few seconds before FortiGate can reflect the actual latency.

After a few seconds, FortiGate reflects the actual latency for the links. `T_INET_0` is the preferred member.

7. On the second SSH session on branch1_fgt, enter the following command to capture ping traffic to `10.1.0.7`:
`diagnose sniffer packet any "host 10.1.0.7 and icmp" 4 | grep T_`

Leave the command running.

8. Open an SSH session to branch1_client.
9. Log in with the username `root` and password `password`.
10. Ping `10.1.0.7` and leave the command running.
11. On the second SSH session on branch1_fgt, view the sniffer output.

    Your output should be similar to the following example:

```
36.144759 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
36.246480 T_INET_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
37.144529 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
37.246857 T_INET_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

According to the rule status, FortiGate prefers T_INET_0, and therefore picked that member to steer the ping traffic.

12. Use the WAN simulator to reduce the latency of T_INET_1 (**BR1-ISP2**) to 95 ms.
13. On branch1_fgt, check the rule status and sniffer again.

Stop and think!

The latency of T_INET_1 is now the lowest among all the members. Yet, FortiGate still prefers T_INET_0 and steers traffic to it. Why?

Remember the `link-cost-threhold` setting, which is set to 10 by default. The setting gives an advantage to members with a higher configuration priority. The corrected metric (CM) for T_INET_0, which factors in the advantage, is determined by dividing its actual latency by 1.10. That is, assuming an actual latency of 100 ms, the CM would be about 91 ms (110 / 1.10).

14. Use the WAN simulator to reduce the latency of T_INET_1 (**BR1-ISP2**) to 85 ms.
15. On branch1_fgt, check the rule status and sniffer again.

    Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(4 T_INET_1), alive, latency: 86.796, selected
    2: Seq_num(3 T_INET_0), alive, latency: 101.762, selected
    3: Seq_num(5 T_MPLS), alive, latency: 121.400, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
41.184052 T_INET_1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
41.273274 T_INET_1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
42.184683 T_INET_1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
42.271708 T_INET_1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

T_INET_1 beat the advantage given to T_INET_0. FortiGate now prefers T_INET_1, and therefore picked that member to steer the ping traffic.

16. Use the WAN simulator to increase the latency of T_INET_1 (**BR1-ISP2**) to 95 ms.
17. On branch1_fgt, check the rule status and sniffer again.

Stop and think!

The latency of T_INET_1 is still the lowest. Yet, FortiGate now prefers T_INET_0 and steers traffic to it. Why?

FortiGate allows a quick recovery of the highest priority member (T_INET_0) by considering its CM when competing against other lower priority members. In this case, the CM of T_INET_0 (~91 ms) is lower than the actual latency of T_INET_1 (~95 ms).

18. Use the WAN simulator to increase the latency of T_INET_1 (**BR1-ISP2**) to 110 ms.
19. On branch1_fgt, check the rule status to confirm latency of T_INET_1 is ~110 ms.
20. Use the WAN simulator to reduce the latency of T_MPLS (**BR1-MPLS**) to 95 ms.
21. On branch1_fgt, check the rule status again.

    Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0), alive, latency: 102.084, selected
    2: Seq_num(5 T_MPLS), alive, latency: 99.307, selected
    3: Seq_num(4 T_INET_1), alive, latency: 111.863, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

T_MPLS moved up in the list because its real latency is lower than the CM of T_INET_1 (~100 ms).

22. Use the WAN simulator to increase the latency of T_MPLS (**BR1-MPLS**) to 115 ms.
23. On branch1_fgt, check the rule status again.
    Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(9), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0), alive, latency: 101.899, selected
    2: Seq_num(4 T_INET_1), alive, latency: 111.747, selected
    3: Seq_num(5 T_MPLS), alive, latency: 115.367, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

FortiGate placed T_INET_1 back above T_MPLS.

24. Use the WAN simulator to reduce the latency of all three overlays back to 0 ms.
25. On branch1_client, stop the ping to `10.1.0.7`.
26. On branch1_fgt, stop the sniffer.
27. Keep the SSH sessions to branch1_client and branch1_ fgt open because you will need them for the next task.

Configure and Test a Lowest Cost (SLA) Rule

You will configure a rule that uses lowest cost (SLA) as the strategy, and two SLA targets. Next, you will test the rule by generating ping traffic and changing the SLA status of the links.

To configure a lowest cost (SLA) rule

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **SD-WAN Rules** section, double-click the **Best_Quality_Latency** rule to edit the rule settings.
4. Configure the following settings:

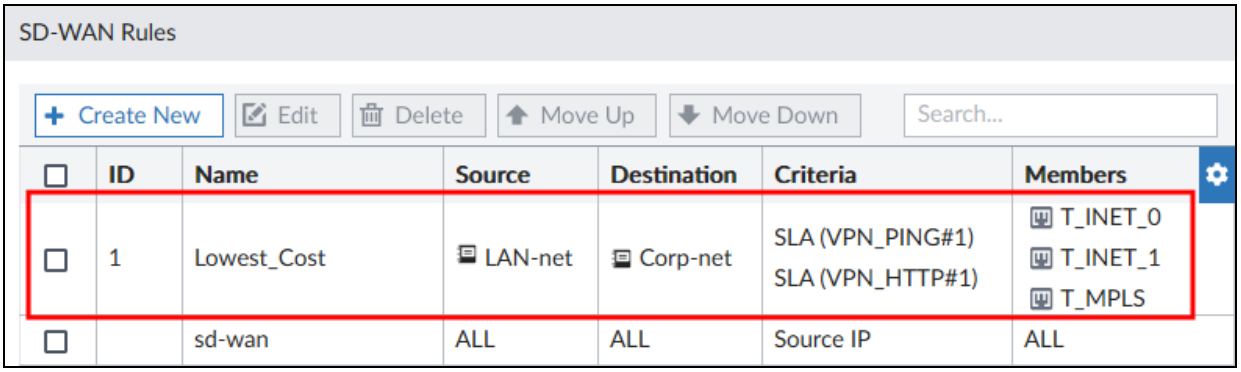
Field	Value
Name	Lowest_Cost

Field	Value
Outgoing Interfaces	• For **Strategy**, select **Lowest Cost (SLA)**. • Keep the current **Interface Preference** settings.
Required SLA Target	• Select **VPN_PING#1**, and **VPN_HTTP#1**. • Move **VPN_PING#1** above **VPN_HTTPS#1**

Set the configuration priority (or interface preference list configuration) to the following (most preferred first):

- **T_INET_0**
- **T_INET_1**
- **T_MPLS**

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



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

To install the device settings

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

To test a lowest cost (SLA) rule

1. Continuing on the branch1_client SSH session, ping `10.1.0.7`, and then leave the command running.
2. On the first SSH session on branch1_fgt, run the following command to display the rule status:
   ```
   diagnose sys sdwan service
   ```
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(3 T_INET_0), alive, sla(0x3), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x3), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 T_MPLS), alive, sla(0x3), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

3. On the second SSH session on branch1_fgt, enter the following command to capture ping traffic to `10.1.0.7`:
   `diagnose sniffer packet any "host 10.1.0.7 and icmp" 4 | grep T_`
   Leave the command running.

   Your output should look similar to the following example:

```
1.309856 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.311411 T_INET_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
2.309892 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
2.311488 T_INET_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

According to the rule status, FortiGate prefers T_INET_0, and therefore picked that member to steer the ping traffic.

4. Use the WAN simulator to increase the latency of T_INET_0 (**BR1-ISP1**) to 160 ms, so it fails to meet both SLA targets.
5. On branch1_fgt, check the rule status and sniffer again.
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 T_INET_1), alive, sla(0x3), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(5 T_MPLS), alive, sla(0x3), gid(0), cfg_order(2), local cost(0), selected
    3: Seq_num(3 T_INET_0), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
0.386778 T_INET_1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
0.388141 T_INET_1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.387307 T_INET_1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.388528 T_INET_1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Stop and think!

T_INET_0 fails to meet both SLA targets, and therefore, is placed at the bottom of the outgoing interface list. T_INET_1 and T_MPLS have the same SLA status (`0x3`) and cost (`0`), yet FortiGate picks T_INET_1 to steer ping traffic. Why?

In the lowest cost (SLA) strategy, when multiple members have the same SLA status and cost, FortiGate uses the configuration priority as the tie-breaker. T_INET_1 has a higher configuration priority than T_MPLS, and therefore it becomes the preferred member.

Next, you will change the member cost, and then observe its impact in the outgoing interface list.

6. On the FortiManager GUI, edit the **branches** SD-WAN template, and then configure the following settings:

Member	Field	Value
T_INET_1	Cost	10
T_MPLS	Cost	5

7. Save the template changes, and then install the device settings on branch1_fgt.
8. On branch1_fgt, check the rule status and sniffer again.
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(5 T_MPLS), alive, sla(0x3), gid(0), cfg_order(2), local cost(5), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x3), gid(0), cfg_order(1), local cost(10), selected
    3: Seq_num(3 T_INET_0), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
5.348513 T_MPLS out 10.0.1.101 -> 10.1.0.7: icmp: echo request
5.349289 T_MPLS in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
6.348906 T_MPLS out 10.0.1.101 -> 10.1.0.7: icmp: echo request
6.349929 T_MPLS in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

T_MPLS now has a lower cost than T_INET_1, and therefore becomes the preferred member.

9. Use the WAN simulator to increase the latency of all three overlays to 160 ms.
10. On branch1_fgt, check the rule status and sniffer again.
    Your output should look similar to the following example:

```
Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(3 T_INET_0), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(5 T_MPLS), alive, sla(0x0), gid(0), cfg_order(2), local cost(5), selected
    3: Seq_num(4 T_INET_1), alive, sla(0x0), gid(0), cfg_order(1), local cost(10), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
6.003520 T_INET_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
6.842271 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
7.004331 T_INET_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
7.843745 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
```

All overlays fail to meet all SLA targets. However, T_INET_0 becomes the preferred member because it has the lowest cost.

11. Use the WAN simulator to reduce the latency of all three overlays back to 0 ms.
12. On the branch1_client, stop the ping to `10.1.0.7`.
13. On the branch1_fgt, stop the sniffer.
14. Keep the SSH sessions to branch1_client and branch1_fgt open because you will need them for the next task.

Configure and Test a Maximize Bandwidth (SLA) Rule

You will configure a rule that uses maximize bandwidth (SLA) as the strategy, and two SLA targets. After that, you will test the rule by generating iperf traffic and changing the SLA status of the links.

To configure a maximize bandwidth (SLA) rule

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **SD-WAN Rules** section, double-click the **Lowest_Cost** rule to edit the rule settings.
4. Configure the following settings:

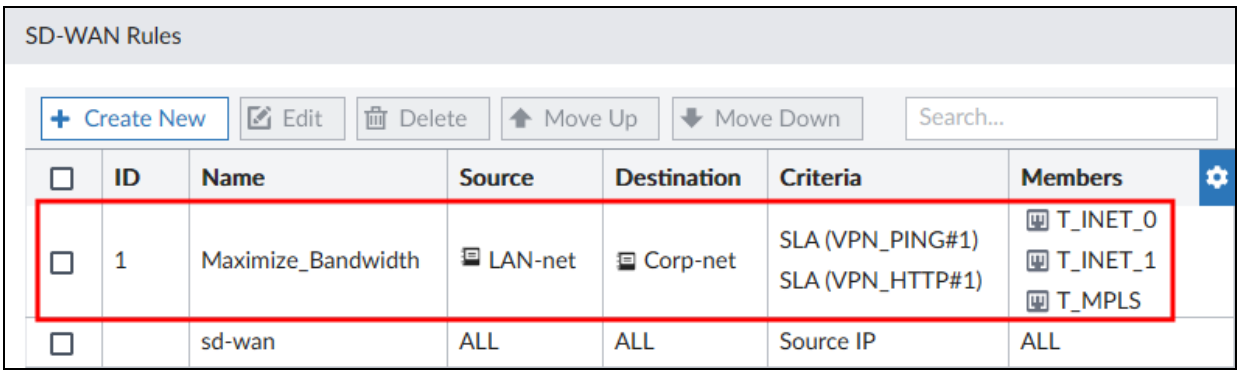
Field	Value
Name	Maximize_Bandwidth
Destination	Select UDP as protocol
Outgoing Interfaces	• For **Strategy**, select **Maximize Bandwidth (SLA)**. • Keep the current **Interface Preference** settings.

Field	Value
Required SLA Target	Keep the current selected SLA targets.

Make sure that the configuration priority (or interface preference list configuration) is the following (most preferred first):

- **T_INET_0**
- **T_INET_1**
- **T_MPLS**

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



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

To install the device settings

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

To test a maximize bandwidth (SLA) rule

1. Open an SSH session to dc1_host.
2. Log in with the password `password`.
3. Enter the following command to start iperf in server mode:
   `iperf3 -s`
4. On the branch1_client SSH session, enter the following command to generate iperf traffic to `10.1.0.7`:
   `iperf3 -c 10.1.0.7 -u -b 1M -P 6 -t 3600 -l 1000`

The additional options in the command instruct iperf to generate six UDP streams at 1-Mbps rate each. The UDP packet length will be 1000 bytes and traffic will be generated for an hour (3600 seconds).

Your output should look similar to the following example:

```
root@branch1-client-cli:~# iperf3 -c 10.1.0.7 -u -b 1M -P 6 -t 3600 -l 1000
Connecting to host 10.1.0.7, port 5201
[  4] local 10.0.1.101 port 33730 connected to 10.1.0.7 port 5201
[  6] local 10.0.1.101 port 47945 connected to 10.1.0.7 port 5201
[  8] local 10.0.1.101 port 59270 connected to 10.1.0.7 port 5201
[ 10] local 10.0.1.101 port 46358 connected to 10.1.0.7 port 5201
[ 12] local 10.0.1.101 port 42522 connected to 10.1.0.7 port 5201
[ 14] local 10.0.1.101 port 56903 connected to 10.1.0.7 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[  6]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[  8]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[ 10]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[ 12]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[ 14]   0.00-1.00   sec   111 KBytes   912 Kbits/sec  114
[SUM]   0.00-1.00   sec   668 KBytes  5.47 Mbits/sec  684
```

5. On the first SSH session, enter the following command to display the rule status:
   `diagnose sys sdwan service`
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Members(3):
    1: Seq_num(3 T_INET_0), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x3), gid(3), num of pass(2), selected
    3: Seq_num(5 T_MPLS), alive, sla(0x3), gid(3), num of pass(2), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

The rule strategy is `load-balance` (maximize bandwidth (SLA)), and the load balancing algorithm is `round-robin` (equal distribution).

6. On the second SSH session on branch1_fgt, enter the following command to capture the first 30 packets of iperf UDP traffic to `10.1.0.7`:
   `diagnose sniffer packet any "host 10.1.0.7 and udp port 5201" 4 30 | grep T_`
   Your output should look similar to the following example:

```
0.063863 T_INET_0 out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.063983 T_INET_1 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.064052 T_MPLS out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
0.064113 T_INET_0 out 10.0.1.101.33383 -> 10.1.0.7.5201: udp 1000
0.064171 T_INET_1 out 10.0.1.101.34531 -> 10.1.0.7.5201: udp 1000
0.064255 T_MPLS out 10.0.1.101.59810 -> 10.1.0.7.5201: udp 1000
```

According to the rule status, all members have the same SLA status. Therefore, FortiGate uses all the members to distribute the traffic.

From the sniffer output, you can tell that each member handles two sessions, for a total of six sessions (round-robin distribution).

7. Use the WAN simulator to increase the latency of T_INET_0 (**BR1-ISP1**) to 110 ms, so that it fails to meet one of the SLA targets.
8. On branch1_fgt, check the rule status and sniffer again.
   Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 T_INET_1), alive, sla(0x3), gid(3), num of pass(2), selected
    2: Seq_num(5 T_MPLS), alive, sla(0x3), gid(3), num of pass(2), selected
    3: Seq_num(3 T_INET_0), alive, sla(0x2), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
0.081871 T_INET_1 out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.081955 T_MPLS out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.082001 T_INET_1 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
0.082017 T_MPLS out 10.0.1.101.33383 -> 10.1.0.7.5201: udp 1000
0.082031 T_INET_1 out 10.0.1.101.34531 -> 10.1.0.7.5201: udp 1000
0.082045 T_MPLS out 10.0.1.101.59810 -> 10.1.0.7.5201: udp 1000
```

FortiGate placed `T_INET_0` at the bottom of the list because it meets the lowest number of SLA targets. Therefore, FortiGate distributes the iPerf traffic between the other two members, as shown in the sniffer output.

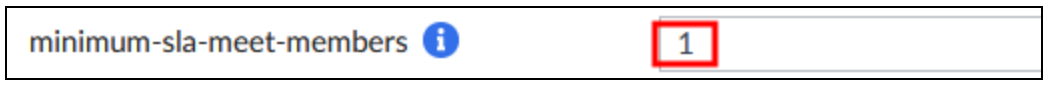
9. Use the WAN simulator to increase the latency of all three overlays to 160 ms.
10. On branch1_fgt, check the rule status and sniffer again.
    Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(7), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Members(3):
    1: Seq_num(5 T_MPLS), alive, sla(0x0), gid(1), num of pass(0), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x0), gid(1), num of pass(0), selected
    3: Seq_num(3 T_INET_0), alive, sla(0x0), gid(1), num of pass(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
0.080720 T_MPLS out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.080803 T_INET_1 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.080858 T_INET_0 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
0.080907 T_MPLS out 10.0.1.101.33383 -> 10.1.0.7.5201: udp 1000
0.080948 T_INET_1 out 10.0.1.101.34531 -> 10.1.0.7.5201: udp 1000
0.080989 T_INET_0 out 10.0.1.101.59810 -> 10.1.0.7.5201: udp 1000
0.081038 T_MPLS out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.081080 T_INET_1 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.081101 T_INET_0 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
0.081158 T_MPLS out 10.0.1.101.33383 -> 10.1.0.7.5201: udp 1000
0.081206 T_INET_1 out 10.0.1.101.34531 -> 10.1.0.7.5201: udp 1000
0.081254 T_INET_0 out 10.0.1.101.59810 -> 10.1.0.7.5201: udp 1000
0.081303 T_MPLS out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.081351 T_INET_1 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.081401 T_INET_0 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
```

All overlays have the same SLA status (none meet any SLA targets). Because the members have the same SLA status, FortiGate uses all of them to distribute traffic.

11. On the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
12. Double-click **branches** to edit the template settings.
13. In the **SD-WAN Rules** section, double-click the **Maximize_Bandwidth** rule to edit the rule settings.
14. In the **Advanced Options** section, set **minimum-sla-meet-members** to `1`.



15. Click **OK** to save the settings.
16. Click **OK** to save the template settings.
17. Install the device settings on branch1_fgt.
18. On branch1_fgt, check the rule status and sniffer again.
    Your output should look similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(3), TOS(0x0/0x0), Protocol(17: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Service disabled caused by no outgoing path no minimum SLA meet.
  Members(3):
    1: Seq_num(3 T_INET_0), alive, sla(0x0), gid(1), num of pass(0), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x0), gid(1), num of pass(0), selected
    3: Seq_num(5 T_MPLS), alive, sla(0x0), gid(1), num of pass(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
0.041631 T_INET_0 out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.041711 T_INET_0 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.041725 T_INET_0 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
0.041738 T_INET_0 out 10.0.1.101.33383 -> 10.1.0.7.5201: udp 1000
0.041751 T_INET_0 out 10.0.1.101.34531 -> 10.1.0.7.5201: udp 1000
0.041763 T_INET_0 out 10.0.1.101.59810 -> 10.1.0.7.5201: udp 1000
0.041774 T_INET_0 out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.041786 T_INET_0 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.041797 T_INET_0 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
0.041809 T_INET_0 out 10.0.1.101.33383 -> 10.1.0.7.5201: udp 1000
0.041821 T_INET_0 out 10.0.1.101.34531 -> 10.1.0.7.5201: udp 1000
0.041832 T_INET_0 out 10.0.1.101.59810 -> 10.1.0.7.5201: udp 1000
0.041844 T_INET_0 out 10.0.1.101.47859 -> 10.1.0.7.5201: udp 1000
0.041856 T_INET_0 out 10.0.1.101.47925 -> 10.1.0.7.5201: udp 1000
0.041868 T_INET_0 out 10.0.1.101.50432 -> 10.1.0.7.5201: udp 1000
```

The rule was disabled because none of the members met at least one SLA target. When you set **minimum-sla-meet-members** to `1`, FortiGate requires the rule to have at least one member that meets one or more SLA targets. Otherwise, the rule is disabled.

Because the rule is disabled, the traffic matches the implicit rule, which means that FortiGate performs standard FIB routing.

Stop and think!

All sessions are routed to T_INET_0. Can you tell why?

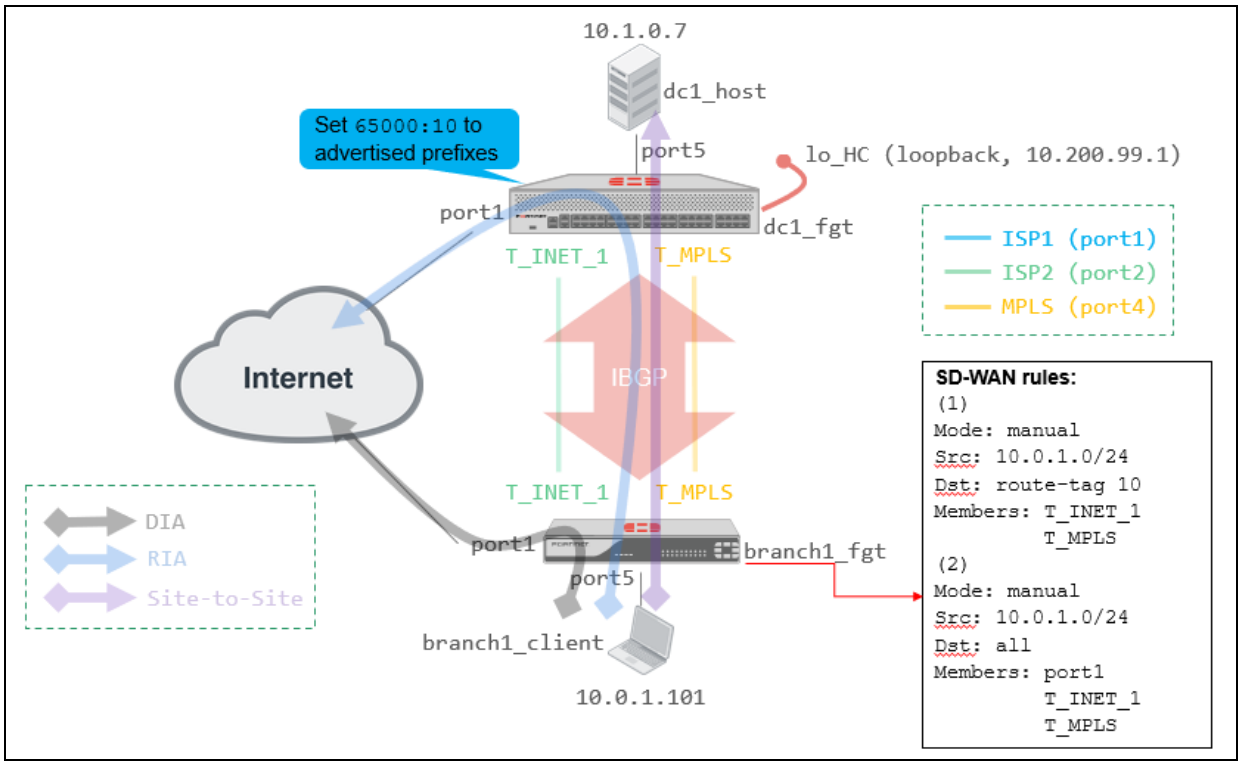
Tip: Check the routing table on branch1_fgt.

19. Use the WAN simulator to reduce the latency of all three overlays back to 0 ms.
20. Close all the SSH sessions (branch1_fgt, branch1_client, and dc1_host).

Exercise 2: Troubleshooting Rules

In this exercise, you will troubleshoot SD-WAN rules used for steering DIA, RIA, and site-to-site traffic.

The following topology has been preconfigured for you:

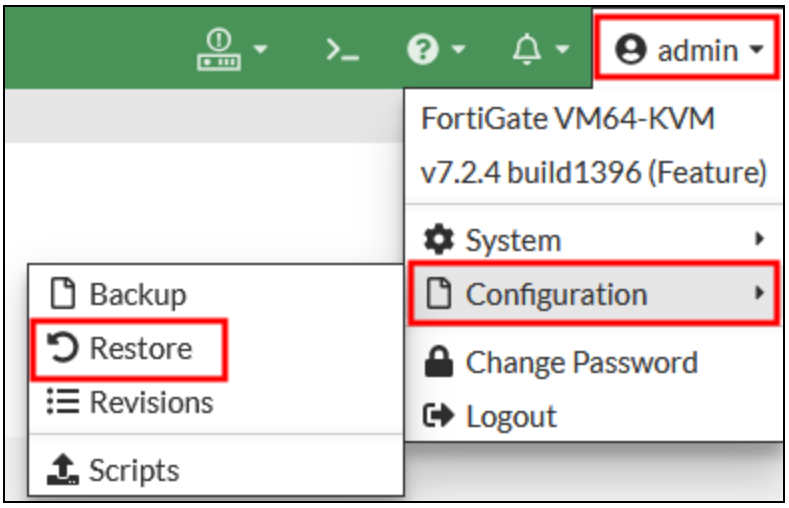


Prerequisites

Before beginning this lab, you must restore a configuration file to branch1_fgt, branch2_fgt, and dc1_fgt. Note that although you must restore a configuration file to branch2_fgt, you will not be using branch2_fgt in this exercise. You will not use FortiManager either.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the local-client, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you get a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-5** > **Exercise-2**, select `lab5-ex2-branch1_fgt_7-2-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt and dc1_fgt.
   Use the following configuration files:

Device	Configuration filename
branch2_fgt	`lab5-ex2-branch2_fgt_7-2-4_initial.conf`
dc1_fgt	`lab5-ex2-dc1_fgt_7-2-4_initial.conf`

Configuration

This is a hub-and-spoke deployment with one underlay (port1) and two overlays (T_INET_1 and T_MPLS). port2 and T_INET_0 are configured but not used for steering traffic. There are rules configured to steer DIA, RIA, and site-to-site traffic.

Internal BGP (IBGP) is used for exchanging routing information between the sites. On dc1_fgt, the administrator assigned the community `65000:10` to advertised prefixes. On branch1_fgt, the administrator assigns prefixes that match the `65000:10` community a route tag of `10`.

Problem Description

The administrator has identified the following issues:

- Issue 1: The administrator configured the SD-WAN rule 2 to steer DIA and RIA traffic. When port1 is up, internet traffic must be routed through port1 (DIA). When port1 is down, internet traffic must fail over to the overlays (RIA). However, when port1 is down, internet traffic is dropped by branch1_fgt.

- Issue 2: The administrator configured the SD-WAN rule 1 to steer traffic to the corporate network (`10.0.0.0/8`). For this, the administrator configured the rule to match the destination based on the BGP routes that are assigned 10 as a route tag. However, when the administrator checks the rule, the rule is disabled because it has no destination.
- Issue 3: The administrator configured the SD-WAN rule 1 in manual mode. However, the administrator wants branch1_fgt to prefer the member with the best route to the destination. This way, the administrator can control the member preference by advertising from dc1_fgt a better route over its preferred overlay, and without having to change the configuration on the branch.

Objective

To complete this lab, you must fix all the issues described.

Solution Requirements

- Unless otherwise stated, focus on branch1_fgt only. Don't make changes on any other device in the network.
- On branch1_fgt, *do not* change the existing IPsec, static route, and firewall policy configuration. You can change the SD-WAN rule settings, except the mode in use and the member and zone preference lists.

Tips for Troubleshooting

- Remember the SD-WAN rule lookup process.
- To test DIA and RIA traffic, you can ping, from the branch client, any of the following addresses: `4.2.2.3`, `4.2.2.4`, `8.8.8.8`, and `8.8.4.4`. To test site-to-site traffic, you can ping the dc1_host (`10.1.0.7`).
- To simulate link failure on port1, bring **BR1-ISP1** down using the WAN simulator.
- Use debug flow to determine how packets are processed:

```
diagnose debug flow filter addr <target-addr>
diagnose debug flow trace start 100
diagnose debug console timestamp enable
diagnose debug enable
```

- Use the sniffer to capture ingress and egress packets:

```
diagnose sniffer packet any "host <target-addr>" 4 0 1
```

- View session details to verify the matching SD-WAN rule and firewall policy:

```
diagnose sys session filter dst <target-addr>
diagnose sys session list
```

- Check routing information using the following commands:

```
get router info routing-table all
get router info bgp community 65000:10
show router bgp
show router route-map
show router community-list
```

- Check the system configuration using the following commands:

```
show system sdwan
show firewall policy
```

```
show system interface
diagnose sys sdwan zone
diagnose sys sdwan member
diagnose sys sdwan service
diagnose firewall proute list
diagnose sys sdwan health-check status Level3_DNS
diagnose sys sdwan health-check status VPN_PING
```

- To confirm that rule 1 prefers the member with the best route (issue 3), enter the following commands on dc1_fgt to advertise a prefix for `10.1.0.7/32` over T_MPLS:

```
config router bgp
   config neighbor-group
      edit Branches_MPLS
         set route-map-out prefer-dc1_host
      next
   end
end
execute router clear bgp all soft
```

Do not make any other changes on dc1_fgt.

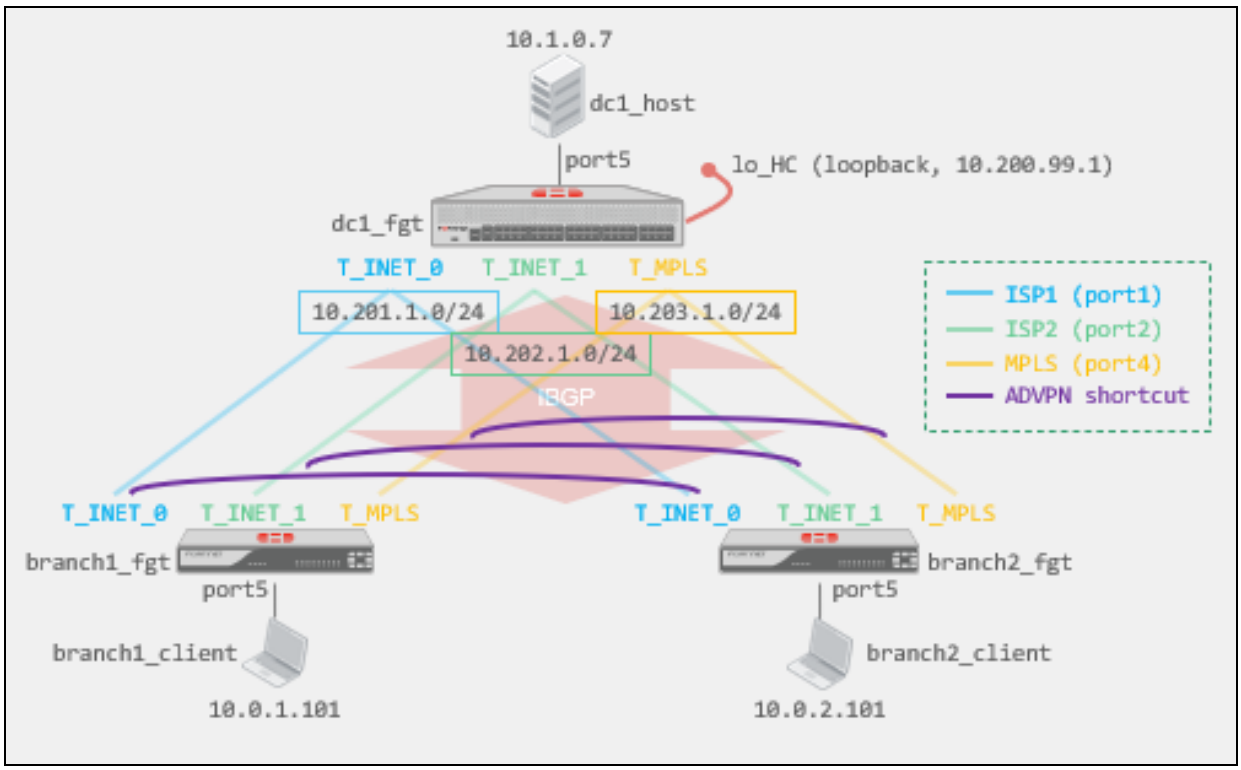
Remember to bring **BR1-ISP1** back up when you finish the exercise.

Solution

If you require assistance with this exercise, see the *Solutions* lesson in the *Study Guide*.

Lab 6: SD-WAN Overlay Design and Best Practices

In this lab, you will configure basic and advanced IPsec overlay and BGP settings for the following hub-and-spoke topology:



After that, you will configure FEC and packet duplication. Finally, you will configure ADVPN to negotiate shortcuts between the branches.

Objectives

- Configure basic and advanced IPsec overlay and BGP settings
- Configure FEC and packet duplication
- Configure ADVPN

Time to Complete

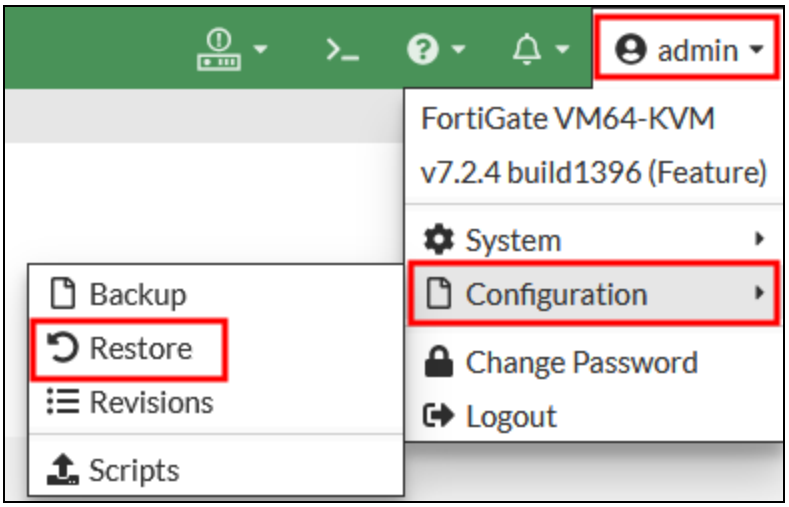
Estimated: 120 minutes

Prerequisites

Before you begin this lab, you must restore the configuration files for branch1_fgt, branch2_fgt, and dc1_fgt, as well as FortiManager.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

1. On the Local-Client VM, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

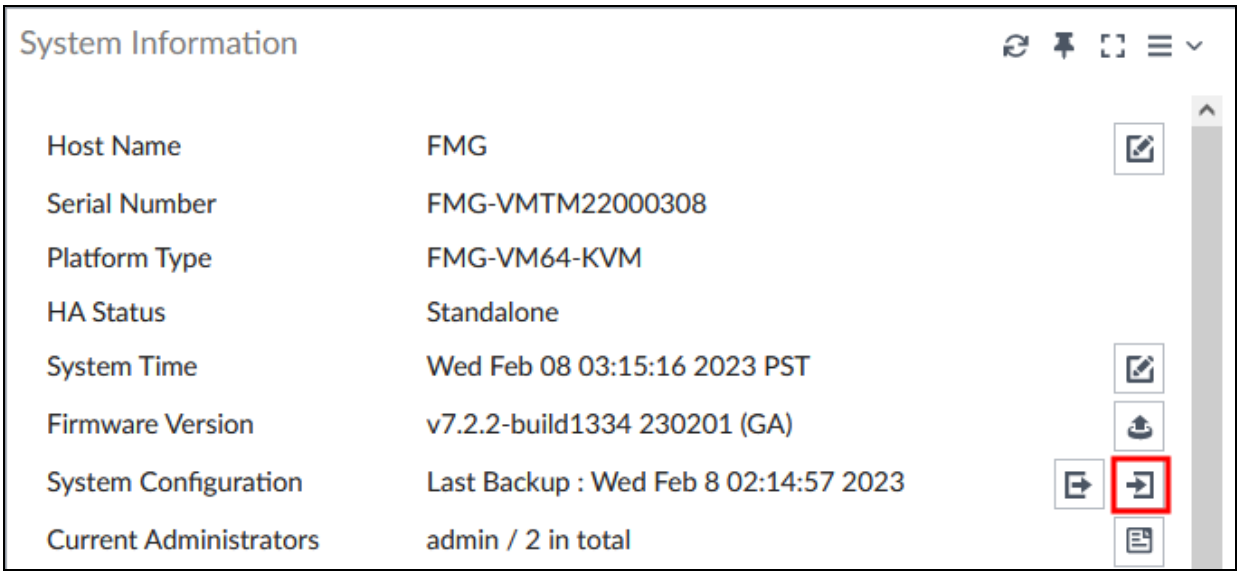


4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-6** > **Exercise-1**, select `lab6-branch1_fgt_7-2-4_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration files on branch2_fgt and dc1_fgt.
   Use the following configuration files:

Device	Configuration
branch2_fgt	`lab6-branch2_fgt_7-2-4_initial.conf`
dc1_fgt	`lab6-dc1_fgt_7-2-4_initial.conf`

To restore the FortiManager configuration file

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **System Settings**, and then click **Dashboard**.
3. In the **System Information** widget, click the **configuration restore** link.



4. Click **Browse** to indicate the local file to upload.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-6** > **Exercise-1**, select `lab6-SYS_FMG_7-2-2_initial.dat`, and then click **OK**.
6. Wait until the file is uploaded and FortiManager finishes rebooting.
7. Log in to the FortiManager GUI with the username `admin` and password `password`.
8. Click **root** > **System Settings**, and then click **Advanced** > **Advanced Settings**.
9. In the **Offline Mode** field, select **Disable**.
10. Click **Apply** to save the settings.

Exercise 1: Configuring Overlays and BGP

In this exercise, you will configure the addresses and BGP configuration that the IPsec overlays use. In previous labs, these settings were preconfigured for you, but this time you will configure them using FortiManager.

First, you will configure the overlay addresses by using IKE mode config. You will also configure a basic BGP setup for your hub-and-spoke topology. Finally, you will fine-tune your IPsec and BGP settings to speed up SD-WAN convergence, failover, and recovery.

Configure Overlay Addresses and Basic BGP

You will assign the addresses using IKE mode config. For BGP, you will configure a basic IBGP setup. On dc1_fgt, you will use neighbor group and neighbor range features because they are required on the dial-up server side.

To configure overlays and basic BGP

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **CLI Templates**.
3. Double-click **Spoke-Overlay addresses and basic BGP** to view the CLI template settings, and then examine the CLI template.

- In the IPsec phase 1 configuration, `mode-cfg` is enabled on each overlay.
- In the BGP configuration, the interface and update-source settings are used to define the interface and source IP address to send the BGP packets from.
- In the BGP configuration, the `$(branch-id)` metadata variable is used to define the correct router ID and network statement for BGP on each branch.

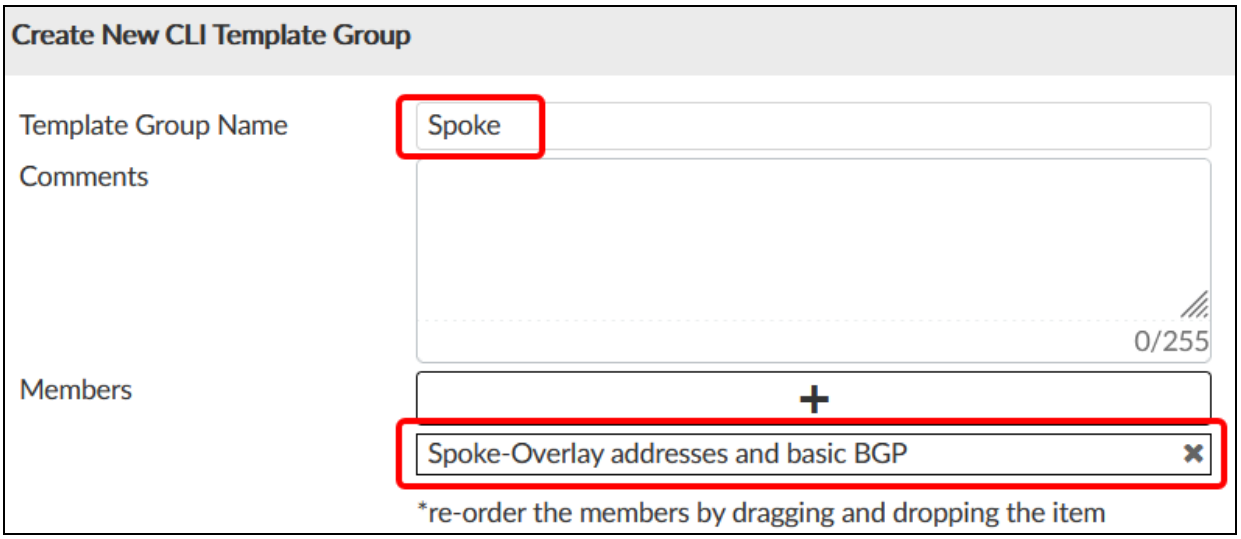
All the metadata variables that you will use in this lesson were preconfigured for you. You can view the metadata variable settings on the **Policy & Objects** page. Click **Device Manager** > **Policy & Objects**, and then click **Object Configurations** > **Advanced** > **Metadata Variables**.

4. Click **Cancel** to exit the CLI template.
5. Double-click **Hub-Overlay addresses and basic BGP** to view the CLI template settings.
6. Examine the CLI template.

- In the system interface configuration for each overlay, the local and remote IP addresses are defined. The `$(dc-id)` metadata variable is used to define the correct IP address to use on each dc (useful if there are multiple hubs).
- In the IPsec phase 1 configuration, `mode-cfg` is enabled on each overlay, and the `$(dc-id)` metadata variable is also used to indicate the right network to use on each dc.
- In the BGP configuration, the `interface` and `update-source` settings are used to define the interface and source IP address to send the BGP packets from. Also, the `route-reflector-client` setting instructs FortiGate to reflect IBGP routes between spokes. All these settings are applied to a `neighbor-group`, which in turn is referenced by a `neighbor-range`.
- In the BGP configuration, the `$(dc-id)` metadata variable is used to define the correct router ID and network statement for BGP.

7. Click **Cancel** to exit the CLI template.
8. Click **Create New** > **CLI Template Group**, and then configure the following settings:

Field	Value
Template Group Name	Spoke
Members	Select **Spoke-Overlay addresses and basic BGP**.



9. Click **OK** to save the settings.
10. Click **Create New** > **CLI Template Group**, and then configure the following settings:

Field	Value
Template Group Name	Hub
Members	Select **Hub-Overlay addresses and basic BGP**.

11. Click **OK** to save the settings.
12. Select the **Spoke** CLI template group, and then click **Assign to Device/Group**.
13. Move **branch1_fgt** and **branch2_fgt** to the **Selected Entries** list.
14. Click **OK** to save the settings.
15. Select the **Hub** CLI template group, and then click **Assign to Device/Group**.
16. Move **dc1_fgt** to the **Selected Entries** list.
17. Click **OK** to save the settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, **branch2_fgt**, and **dc1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on all devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To verify the overlay address and BGP peering

1. Open an SSH session to branch1_fgt, and another to branch2_fgt.
2. Log in with the username `admin` and password `password`.
3. On both SSH sessions, enter the following command to display the overlay addresses:
   ```
   diagnose ip address list | grep T_
   ```
   For example, on branch1_fgt, your output should look similar to the following example:

```
branch1_fgt # diagnose ip address list | grep T_
IP=10.201.1.2->10.201.1.2/255.255.255.0 index=19 devname=T_INET_0
IP=10.202.1.2->10.202.1.2/255.255.255.0 index=20 devname=T_INET_1
IP=10.203.1.1->10.203.1.1/255.255.255.0 index=21 devname=T_MPLS
```

The overlay addresses may be different in your output.

4. On both SSH sessions, enter the following commands to display the status of BGP peerings and the BGP routes in the routing table:
   ```
   get router info bgp summary
   get router info routing-table bgp
   ```
   For example, on branch2_fgt, your output should look similar to the following example:

```
branch2_fgt # get router info bgp summary
VRF 0 BGP router identifier 10.0.2.1, local AS number 65000
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.201.1.254    4      65000       8       7        1    0    0 00:04:13        2
10.202.1.254    4      65000       9       7        2    0    0 00:04:12        2
10.203.1.254    4      65000       9       7        2    0    0 00:03:58        2

Total number of neighbors 3



branch2_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.1.0/24 [200/0] via 10.201.1.2 [3] (recursive is directly connected, T_INET_0), 00:03:33, [1/0]
B       10.1.0.0/24 [200/0] via 10.201.1.254 (recursive is directly connected, T_INET_0), 00:03:40, [1/0]
                    [200/0] via 10.202.1.254 (recursive is directly connected, T_INET_1), 00:03:40, [1/0]
                    [200/0] via 10.203.1.254 (recursive is directly connected, T_MPLS), 00:03:40, [1/0]
```

Stop and think!

There is a BGP peering established over each overlay. The branch is also learning BGP prefixes from dc1_fgt. The `10.1.0.0/24` prefix is sourced from dc1_fgt, and the `10.0.branch-id.0/24` prefix is sourced from the other branch and reflected by dc1_fgt. The former prefix is learned over each overlay, but the latter is not. Why?

The paths over the other overlays are not shown because you didn't configure additional paths on the branches and dc1_fgt. In the next task, you will configure additional paths so the branches show nine different paths for the `10.0.branch-id.0/24` prefix (three prefixes per overlay).

5. Access the WAN simulator page.
6. Locate **DC1-ISP1**, and then click **DOWN** to bring down the link on port1 on dc1_fgt.
7. On any of the branch SSH sessions, enter the following commands to monitor the overlays and BGP status:
   ```
   diagnose sys sdwan health-check status VPN_PING
   get ipsec tunnel list
   get router info bgp summary
   ```
   Focus on the output relevant to the T_INET_0 overlay. Your output should look similar to the following example:

```
branch2_fgt # diagnose sys sdwan health-check status VPN_PING
Health Check(VPN_PING):
Seq(3 T_INET_0): state(dead), packet-loss(7.000%) sla_map=0x0
Seq(4 T_INET_1): state(alive), packet-loss(0.000%) latency(0.917), jitter(0.107), mos(4.404
), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(0.735), jitter(0.108), mos(4.404),
 bandwidth-up(65534999), bandwidth-dw(65534999), bandwidth-bi(131069998) sla_map=0x3

branch2_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.
0 STATUS=up TIMEOUT=1586

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.
0 STATUS=up TIMEOUT=1166

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=1166


branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.0.2.1, local AS number 65000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.201.1.254 4      65000      13      14        4    0    0 00:01:02        2
10.202.1.254 4      65000      18      12        2    0    0 00:08:45        2
10.203.1.254 4      65000      18      13        3    0    0 00:08:41        2

Total number of neighbors 3
```

The performance SLA marked T_INET_0 down shortly after bringing down port1 on dc1_fgt. However, the IPsec tunnel and BGP peering remain up.

8. Repeat the previous commands every few seconds to track the status of the overlay and BGP.

Stop and think!

Eventually (after two minutes or so), the tunnel and the BGP peering goes down. For example:

```
branch2_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.
0.0/0.0.0.0 STATUS=down

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.
0.0/0.0.0.0 STATUS=up TIMEOUT=795

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.
0/0.0.0.0 STATUS=up TIMEOUT=795


branch2_fgt # get router info bgp summary

VRF 0 BGP router identifier 10.0.2.1, local AS number 65000
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRc
d
10.201.1.254 4      65000      13      18        0    0    0    never Active
10.202.1.254 4      65000      26      19        2    0    0 00:15:01        2
10.203.1.254 4      65000      28      20        3    0    0 00:14:57        2

Total number of neighbors 3
```

Why?

Although it is not shown in the output, the tunnel and the BGP peering go down because of DPD and the hold timer expiration, respectively. Both the DPD and BGP timers are set to the default values. In the next task, you will adjust the timers to speed up SD-WAN convergence, failover, and recovery.

9. On the WAN simulator page, locate **DC1-ISP1**, and then click **UP** to bring up the link on port1 on dc1_fgt.

Fine-Tune IPsec and BGP

You will configure some IPsec and BGP settings to speed up SD-WAN convergence, failover, and recovery. You will also configure additional paths on dc1_fgt and the branches to exchange all available routes between them.

To fine-tune IPsec and BGP

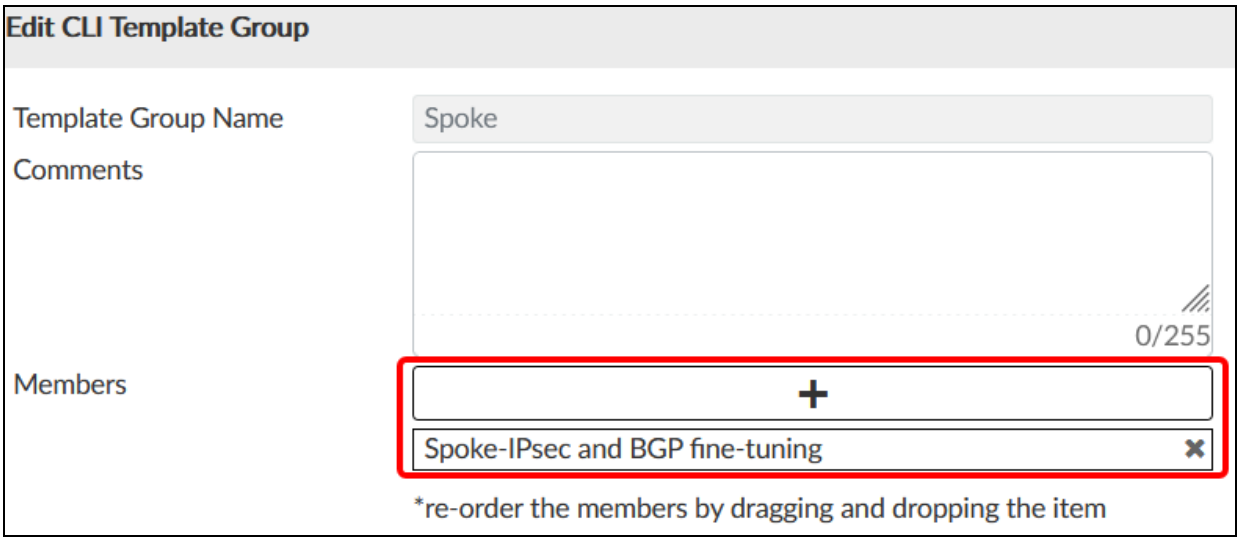
1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **CLI Templates**.
2. Double-click **Spoke-IPsec and BGP fine-tuning** to view the CLI template settings.
3. Examine the CLI template, and identify the differences with the basic IPsec and BGP configuration template for the spokes.

- In the IPsec phase 1 configuration, the `dpd-mode`, `dpd-retrycount`, and `dpd-retryinterval` settings are set to `on-idle`, `2`, and `2`, respectively. With these settings, DPD should detect a tunnel that is down 6 seconds after the connectivity is lost.
- In the BGP configuration, the `soft-reconfiguration`and `link-down-failover`settings are enabled. The former instructs FortiGate to save the received routes in a separate table, which is useful for troubleshooting, and is required to soft reset BGP peerings after a change. The latter instructs FortiGate to clear a BGP peering after the interface in use goes down.
- In the BGP configuration, the `connect-timer` and `additional-path` settings are set to `1` and `receive`, respectively. The former speeds up the frequency of the connection attempts made by FortiGate to establish a BGP peering. The latter instructs FortiGate to accept additional paths from a BGP neighbor.

4. Click **Cancel** to exit the CLI template.
5. Double-click **Hub-IPsec and BGP fine-tuning** to view the CLI template settings.
6. Examine the CLI template and identify the differences with the basic IPsec and BGP configuration template for the hub.

- The DPD settings are set to the same values as in the spoke template. In the BGP configuration, the `soft-reconfiguration` and `link-down-failover` settings are also enabled. All settings have the same effect as in the spoke.
- In the BGP configuration, the `keepalive-timer`, `holdtime-timer`, and `advertisement-interval` settings are set to `5`, `15`, and `1`, respectively, to speed up routing convergence and failover.
- In the BGP configuration, the `additional-path` and `additional-path-select` settings are set to `enable` and `3`, respectively. Also, inside each neighbor-group, the `additional-path` and `adv-additional-path` settings are set to `send` and `3`, respectively. The result is that dc1_fgt can identify up to three additional paths per prefix, and send them to the branches.

7. Click **Cancel** to exit the CLI template.
8. Double-click the **Spoke** CLI template group to edit its settings.
9. In the **Members** list, remove **Spoke-Overlay addresses and basic BGP**, and then add **Spoke-IPsec and BGP fine-tuning**.



10. Click **OK** to save the settings.
11. Double-click the **Hub** CLI template group to edit its settings.
12. In the **Members** list, remove **Hub-Overlay addresses and basic BGP**, and then add **Hub-IPsec and BGP fine-tuning**.
13. Click **OK** to save the settings.
14. Install the device settings on branch1_fgt, branch2_fgt, and dc1_fgt.
15. On any of the branch SSH sessions, enter the following command to display the status of BGP peerings and the BGP routes in the routing table:
    `get router info routing-table bgp`
    For example, on branch2_fgt, your output should look similar to the following example:

```
branch2_fgt # get router info bgp summary
VRF 0 BGP router identifier 10.0.2.1, local AS number 65000
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.201.1.254 4      65000      61      55        5    0    0 00:00:49        4
10.202.1.254 4      65000      81      61        6    0    0 00:00:46        4
10.203.1.254 4      65000      78      59        5    0    0 00:00:50        4

Total number of neighbors 3



branch2_fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.0.1.0/24 [200/0] via 10.201.1.1 [3] (recursive is directly connected, T_INET_0), 00:00:48, [1/0]
                    [200/0] via 10.202.1.2 [3] (recursive is directly connected, T_INET_1), 00:00:48, [1/0]
                    [200/0] via 10.203.1.1 [3] (recursive is directly connected, T_MPLS), 00:00:48, [1/0]
B       10.1.0.0/24 [200/0] via 10.201.1.254 (recursive is directly connected, T_INET_0), 00:01:15, [1/0]
                    [200/0] via 10.202.1.254 (recursive is directly connected, T_INET_1), 00:01:15, [1/0]
                    [200/0] via 10.203.1.254 (recursive is directly connected, T_MPLS), 00:01:15, [1/0]
```

The routing table now displays nine available paths for the `10.0.branch-id.0/24` prefix. Some of the routes are duplicate routes. You can see the duplicate routes in the output of the `get router info routing-table database` command.

16. Use the WAN simulator page to bring down **DC1-ISP1** again to verify the faster convergence.
17. On any of the branch SSH sessions, enter the following commands multiple times to monitor the status of the T_INET_0 overlay and BGP status:

```
diagnose sys sdwan health-check status VPN_PING
get ipsec tunnel list
get router info bgp summary
```

The tunnel and BGP peering are now brought down much faster, which speeds up network convergence and failover.

18. Use the WAN simulator page to bring up **DC1-ISP1**.

Exercise 2: Configuring FEC and Packet Duplication

In this exercise, you will impact the link quality of the T_INET_0 overlay by adding packet loss to the link, which you will then correct by configuring FEC. After that, you will configure packet duplication on SD-WAN, and then verify that FortiGate sends duplicates on the sender side and discards them on the receiver side.

Configure FEC

You will use FortiManager CLI templates to configure FEC on the branches and dc1_fgt. The CLI templates were preconfigured for you.

To configure FEC

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **CLI Templates**.
3. Double-click **Spoke-Enable FEC** to view the CLI template settings, and then examine the CLI template.

- In the IPsec phase 1 configuration, the `fec-egress`setting is enabled on T_INET_0. The `fec-base`, `fec-redundant`, and `fec-send-timeout` settings are set to `20`, `2`, and `8`, respectively. The result is that FortiGate sends 2 parity packets over T_INET_0 for every 20 packets sent through the tunnel over a period of 8 ms.
- In the firewall policy configuration, the `fec` setting is enabled on policy ID 2. Policy ID 2 matches the outgoing traffic through T_INET_0.

4. Click **Cancel** to exit the CLI template.
5. Double-click **Hub-Enable FEC** to view the CLI template settings, and then examine the CLI template.

In the IPsec phase 1 configuration, the `fec-ingress` setting is enabled on T_INET_0. The result is that FortiGate processes incoming parity packets received at T_INET_0.

Stop and think!

FEC is enabled on the outgoing direction on the spoke, and on the incoming direction on the hub. Why?

The packet loss that you will add using the WAN simulator impacts only the outgoing traffic on the spoke. For this reason, you must correct only the outgoing traffic on the spoke, which is also the incoming traffic on the hub. In production networks, you usually want to enable FEC on both directions of the traffic to guard against brownout conditions impacting any direction of the link.

6. Double-click the **Spoke** CLI template group to edit its settings.
7. In the **Members** list, add **Spoke-Enable FEC**.
8. Click **OK** to save the settings.

9. Double-click the **Hub** CLI template group to edit its settings.
10. In the **Members** list, add **Hub-Enable FEC**.
11. Click **OK** to save the settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see t **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, **branch2_fgt**, and **dc1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on all devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To test FEC

1. Access the WAN simulator page.
2. Locate the **DC1-ISP1** control panel.
3. Use the vertical bar to increase the **loss** of the link to 30%.

From dc1_fgt perspective, you introduced packet loss on port1 on the incoming direction (from the branch to dc1_fgt).

4. Open an SSH session to **branch1_fgt**.
5. Log in with the username `admin` and password `password`.
6. Enter the following commands to check the health of the overlays:
   ```
   diagnose sys sdwan health-check status VPN_PING
   diagnose sys sdwan service
   ```
   Your output should be similar to the following example:

```
branch1_fgt # diagnose sys sdwan health-check status VPN_PING
Health Check(VPN_PING):
Seq(3 T_INET_0): state(alive), packet-loss(30.000%) latency(1.434), jitter(0.475), mo
s(4.388), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x0
Seq(4 T_INET_1): state(alive), packet-loss(0.000%) latency(1.247), jitter(0.370), mos
(4.403), bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(0.976), jitter(0.384), mos(4
.404), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0
x3

branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(3):
    1: Seq_num(3 T_INET_0), alive, selected
    2: Seq_num(4 T_INET_1), alive, selected
    3: Seq_num(5 T_MPLS), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

FortiGate calculates the member packet loss based on the last 100 health check probes. For this reason, you may have to wait a few seconds before FortiGate can reflect the latest packet loss.

There is an SD-WAN rule that steers corporate traffic. The preferred member is T_INET_0.

7. Open an SSH session to **branch1_client**.
8. Log in with the username `root` and password `password`.
9. Enter the following command to generate 100 pings to 10.1.0.7 at a 0.2 second interval:
   `ping 10.1.0.7 -i 0.2 -c 100`
   Your ping statistics output should look similar to the following example:

```
--- 10.1.0.7 ping statistics ---
100 packets transmitted, 97 received, 3% packet loss, time 899ms
rtt min/avg/max/mdev = 1.190/2.940/10.988/2.489 ms
```

Stop and think!

The SD-WAN performance SLA reports a ~30% packet loss on T_INET_0. However, when you ping from branch1_client to the dc1_host over T_INET_0, there is only 3% packet loss. Why?

Local traffic, such as the health check probes, is not subject to FEC. Only traffic passing through the firewall is. This is why the ping traffic from branch1_client to dc1_fgt is corrected, and the health check traffic is not.

10. On FortiManager, edit the **Spoke-Enable FEC** CLI template, and set `fec-redundant` to `4`.
11. Save the CLI template settings, and then install the device settings on branch1_fgt and branch2_fgt.

12. On the branch1_client, repeat the ping test, and then examine the ping statistics.
    Your output should look similar to the following example:

```
--- 10.1.0.7 ping statistics ---
100 packets transmitted, 99 received, 1% packet loss, time 896ms
rtt min/avg/max/mdev = 1.172/2.994/10.829/2.738 ms
```

Packet loss is reduced even further after you increased the `fec-redundant` setting.

13. On the branch1_fgt SSH session, enter the following commands:

```
config firewall policy
   edit 2
      set fec disable
   next
end
```

14. On the branch1_client, repeat the ping test, and then examine the ping statistics.
    Your output should look similar to the following example:

```
--- 10.1.0.7 ping statistics ---
100 packets transmitted, 72 received, 28% packet loss, time 964ms
rtt min/avg/max/mdev = 0.981/1.387/1.932/0.180 ms
```

Packet loss increased considerably because FortiGate is no longer generating FEC parity packets.

15. On FortiManager, edit the **Spoke** CLI template group, remove the **Spoke-Enable FEC** CLI template from the **Members** list, and then save the setting.
16. Edit the **Hub** CLI template group, remove the **Hub-Enable FEC** CLI template from the **Members** list, and then save the setting.
17. Click **Device Manager** > **Policy & Objects**.
18. Install the policy package and device settings on branch1_fgt and branch2_fgt.
    Select **branches_pp** as the policy package.
19. Install the device settings on dc1_fgt.
20. On the WAN simulator page, reduce the packet loss on **DC1-ISP1** back to 0%.

Configure Packet Duplication

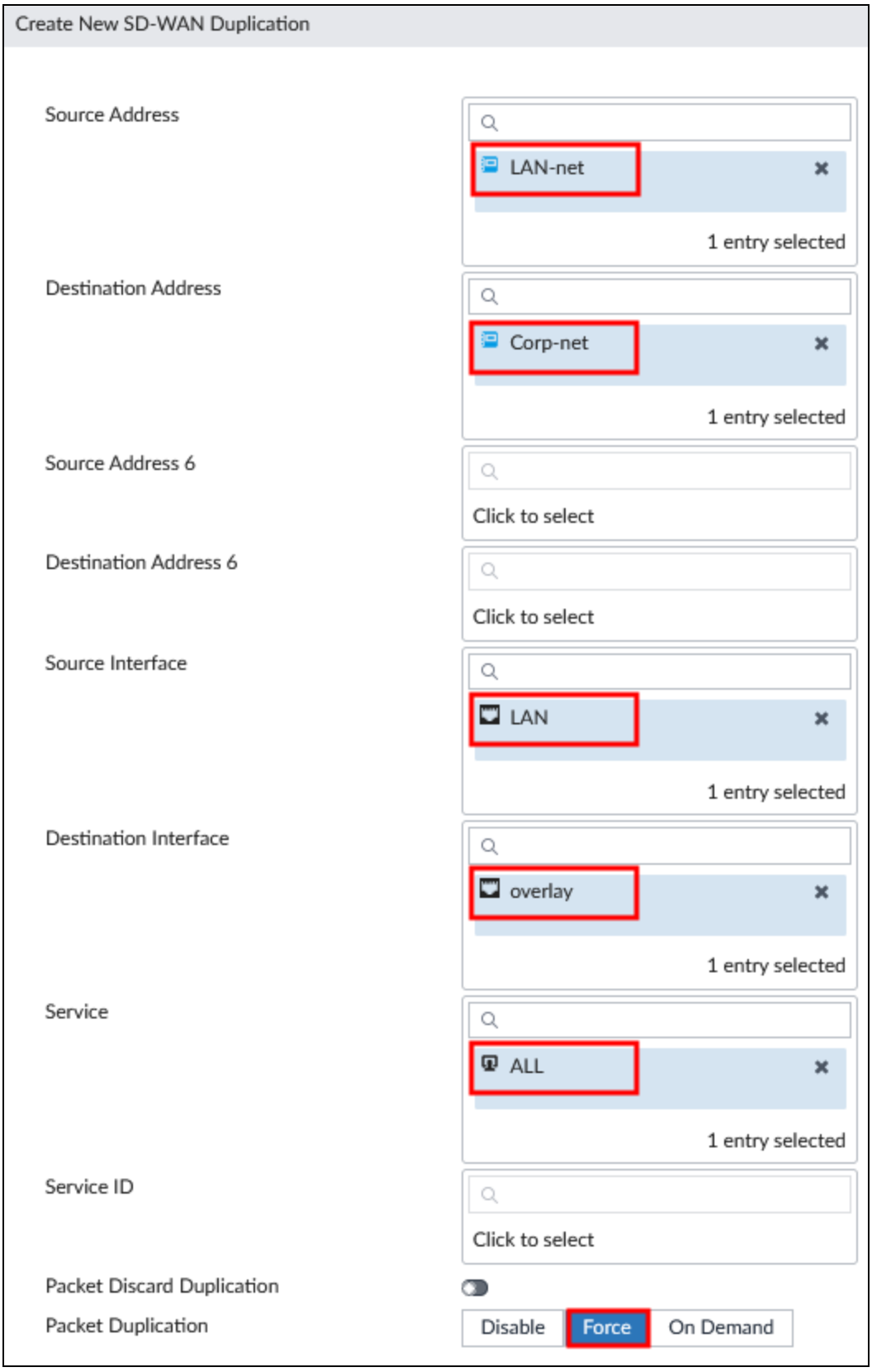
You will configure forced packet duplication using FortiManager SD-WAN templates. You will also configure overlay stickiness on the hub using CLI templates. When you configure overlay stickiness, dc1_fgt prefers to keep

the traffic in the same overlay. Overlay stickiness is also recommended for ADVPN. You will configure ADVPN in another exercise.

To configure packet duplication

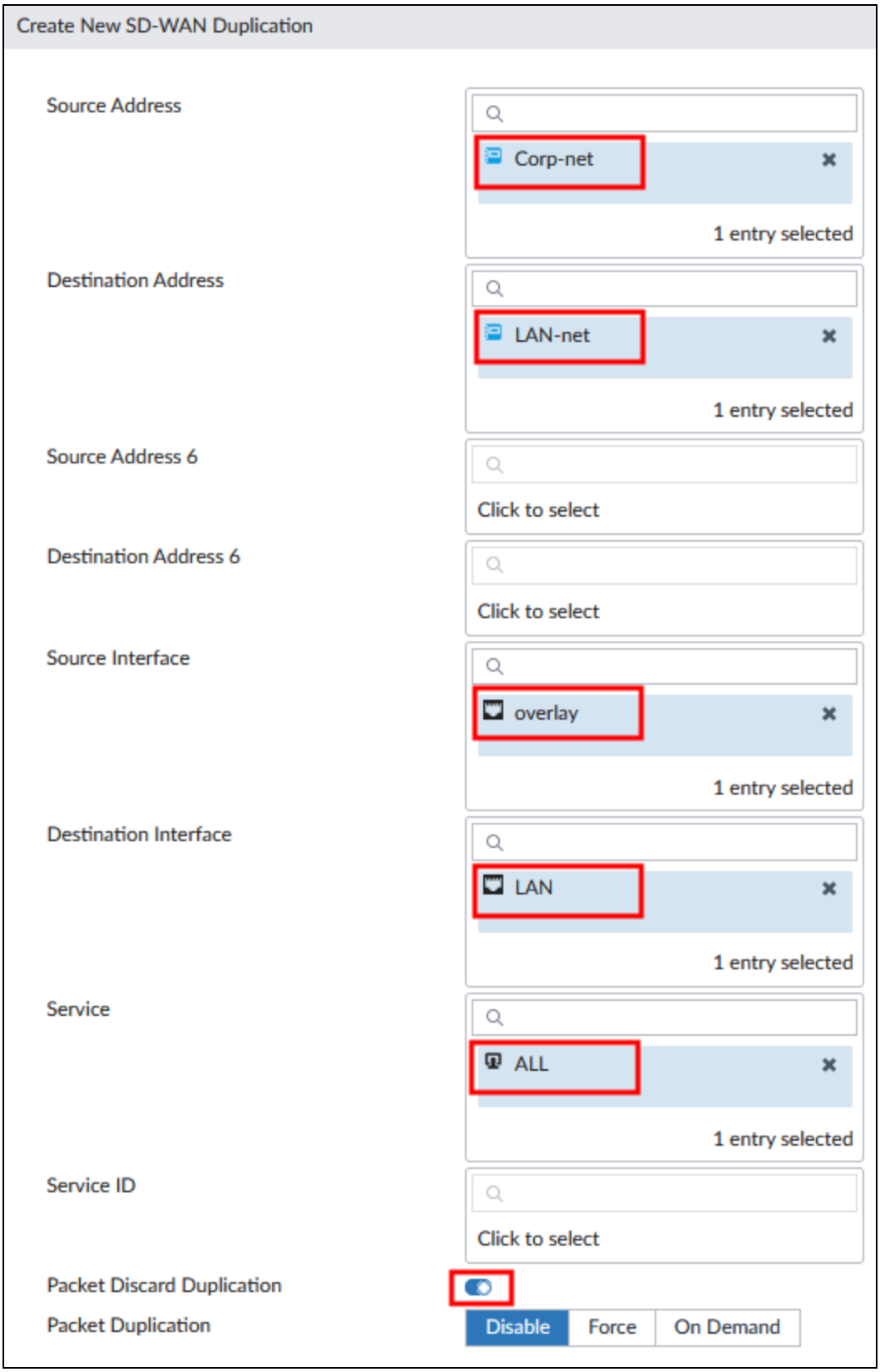
1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **SD-WAN Templates**.
2. Double-click **branches** to edit the template settings.
3. In the **Duplication** section, click **Create New**, and then configure the following settings to configure duplication from LAN to overlay:

Field	Value
Source Address	Select **LAN-net**.
Destination Address	Select **Corp-net**.
Source Interface	Select **LAN**.
Destination Interface	Select **overlay**.
Service	Select **ALL**.
Packet Duplication	Select **Force**.



4. Click **OK** to save the settings.
5. In the **Duplication** section, click **Create New**, and then configure the following settings to configure duplication discard from overlay to LAN:

Field	Value
Source Address	Select **Corp-net**.
Destination Address	Select **LAN-net**.
Source Interface	Select **overlay**.
Destination Interface	Select **LAN**.
Service	Select **ALL**.
Packet Discard Duplication	Enable



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

You didn't configure the `duplication-max-num` setting. Therefore, you will use the default value: `2`. That is, FortiGate forwards up to two copies of the packet—the original packet plus one duplicate.

To configure overlay stickiness

1. Continuing on the FortiManager GUI, edit the **Hub-Overlay Stickiness** CLI template to view its settings, and then examine the CLI template.

There are three policy routes, one for each overlay. Each policy route instructs FortiGate to keep the traffic within the overlay.

2. Edit the **Hub** CLI template group, add the **Hub-Overlay Stickiness** CLI template to the **Members** list, and then save the settings.
3. Install the device settings on branch1_fgt, branch2_fgt, and dc1_fgt.

To test packet duplication

1. On the WAN simulator page, increase the delay on **DC1-ISP1** to 100 ms.

You increased the latency on the traffic forwarded to dc1_fgt over T_INET_0.

By increasing the latency on DC1-ISP1, you ensure that duplicate pings sent over T_INET_0 arrive later than those sent over T_INET_1.

2. On the branch1_fgt SSH session, enter the following command to capture ping traffic to branch2_client:
```
diagnose sniffer packet any "host 10.0.2.101 and icmp" 4
```
3. Open an SSH session to branch2_fgt, and then run the previous sniffer capture command.
4. On the branch1_client, enter the following command to send one ping to branch2_client:
```
ping 10.0.2.101 -c 1
```
You should be able to ping the address.
5. Examine the sniffer output on the branch1_fgt and branch2_fgt SSH sessions.
Your output should look similar to the following example:

```
branch1_fgt #
branch1_fgt # diagnose sniffer packet any "host 10.0.2.101 and icmp" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.2.101 and icmp]
10.828293 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
10.828359 T_INET_1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
10.828450 T_INET_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
10.830646 T_INET_1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
10.830669 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

```
branch2_fgt # diagnose sniffer packet any "host 10.0.2.101 and icmp" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.2.101 and icmp]
21.246341 T_INET_1 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
21.246405 port5 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
21.246796 port5 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
21.246822 T_INET_1 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
21.346335 T_INET_0 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
```

branch1_fgt generates two packets—the original ping packet and one duplicate. One packet is forwarded to T_INET_1 and another to T_INET_0.

On branch2_fgt, the packet that arrives first (T_INET_1) is accepted, and the packet that arrives second (T_INET_0, about 100 ms later) is discarded.

branch2_fgt replies using T_INET_1 (session symmetry), and then branch1_fgt receives the reply packet on the same overlay.

6. Continuing on the FortiManager GUI, edit the branches SD-WAN template, and delete the two packet duplication rules.
7. Install the device settings on branch1_fgt and branch2_fgt.
8. On the WAN simulator page, reduce the delay on **DC1-ISP1** back to 0 ms.

Exercise 3: Configuring ADVPN

In this exercise, you will configure and test ADVPN. After that, you will configure an ADVPN idle timeout.

Configure Basic ADVPN

You will use FortiManager CLI templates to configure ADVPN on the branches and dc1_fgt. The CLI templates were preconfigured for you.

To configure basic ADVPN

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager**, and then click **Provisioning Templates** > **CLI Templates**.
3. Double-click **Spoke-Basic ADVPN** to view the CLI template settings, and then examine the CLI template.

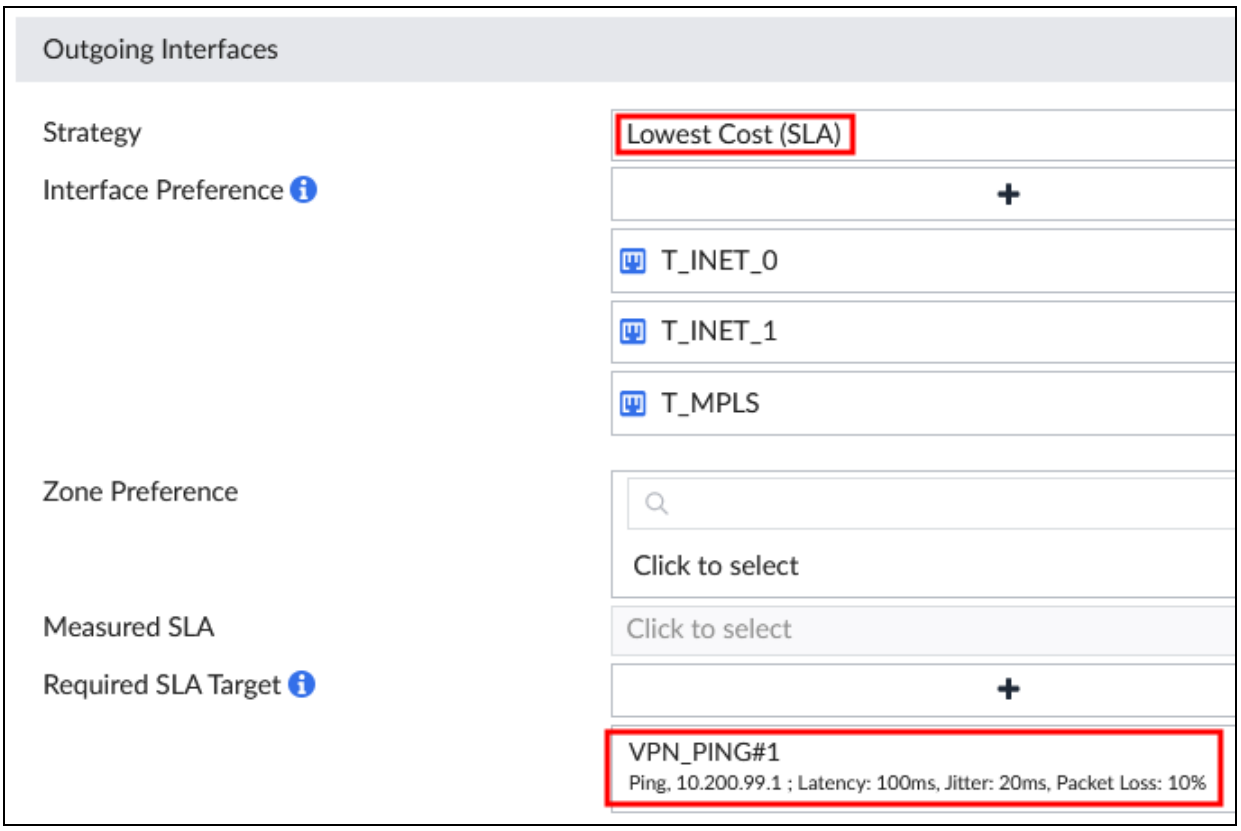
- In the IPsec phase 1 configuration, the `net-device` and `auto-discovery-receiver`settings are enabled on each overlay, respectively. The former is required for ADVPN to work on spokes, and the latter instructs FortiGate to inform the hub that the device can negotiate shortcuts. The `auto-discovery-shortcuts` settings is set to `dependent` to bring down shortcut tunnels if the parent tunnel goes down. The `add-route` setting is set to `disable` so the tunnel will not create static routes and use dynamic routing instead.
- In the system interface configuration, `ping` access is enabled on each overlay. It enables SD-WAN to monitor the health and performance of shortcuts using ping.

4. Click **Cancel** to exit the CLI template.
5. Double-click **Hub-Basic ADVPN** to view the CLI template settings, and then examine the CLI template.

In the IPsec phase 1 configuration, the `net-device`setting is disabled, and the `auto-discovery-sender` setting is enabled on each overlay. The former is required for ADVPN to work on hubs, and the latter instructs FortiGate to facilitate shortcut negotiation between spokes.

6. Click **Cancel** to exit the CLI template.
7. Double-click the **Spoke** CLI template group to edit its settings.
8. In the **Members** list, add **Spoke-Basic ADVPN**.
9. Click **OK** to save the settings.
10. Double-click the **Hub** CLI template group to edit its settings.
11. In the **Members** list, add **Hub-Basic ADVPN**.
12. Click **OK** to save the settings.
13. Click **Provisioning Templates** > **SD-WAN Templates**.
14. Double-click **branches** to edit the template settings.

15. In the **SD-WAN Rules** section, double-click **Corp** to edit the rule settings.
16. In the **Outgoing Interfaces** section:
    - In the **Strategy** field, select **Lowest Cost (SLA)**.
    - In the **Required SLA Target** field, select **VPN_PING#1**.



17. Click **OK** to save the settings.
18. Click **OK** to save the template settings.

To install the device settings

1. Continuing on the FortiManager GUI, click **Install Wizard**.
2. Confirm that you see **Install Device Settings (only)**, and then click **Next**.
3. Select **branch1_fgt**, **branch2_fgt**, and **dc1_fgt**, and then click **Next**.
4. Click **Install** to install the configuration on all devices.
5. Wait for the installation to finish.
6. Click **Finish**.

To test ADVPN

1. Open an SSH session to branch1_fgt.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

```
get ipsec tunnel list
diagnose sys sdwan service
get router info routing-table details 10.0.2.101
```

Your output should be similar to the following example:

```
branch1_fgt # branch1_fgt # get ipsec tunnel  list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/
0.0.0.0 STATUS=up TIMEOUT=1609

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/
0.0.0.0 STATUS=up TIMEOUT=1608

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.
0.0.0 STATUS=up TIMEOUT=1609
```

```
branch1_fgt # branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(3 T_INET_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 T_MPLS), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
branch1_fgt # get router info routing-table details 10.0.2.101

Routing table for VRF=0
Routing entry for 10.0.2.0/24
  Known via "bgp", distance 200, metric 0, best
  Last update 00:30:19 ago
  * vrf 0 10.201.1.2 priority 1 (recursive is directly connected, T_INET_0)
  * vrf 0 10.202.1.2 priority 1 (recursive is directly connected, T_INET_1)
  * vrf 0 10.203.1.1 priority 1 (recursive is directly connected, T_MPLS)
  * vrf 0 10.201.1.2 priority 1 (recursive is directly connected, T_INET_0)
  * vrf 0 10.202.1.2 priority 1 (recursive is directly connected, T_INET_1)
  * vrf 0 10.203.1.1 priority 1 (recursive is directly connected, T_MPLS)
  * vrf 0 10.201.1.2 priority 1 (recursive is directly connected, T_INET_0)
  * vrf 0 10.202.1.2 priority 1 (recursive is directly connected, T_INET_1)
  * vrf 0 10.203.1.1 priority 1 (recursive is directly connected, T_MPLS)
```

- The three overlays are up.
- T_INET_0 is the preferred member, followed by T_INET_1 and T_MPLS.
- The best routes to 10.0.2.101 are any of the nine paths through the overlays.

4. Continuing on the branch1_fgt SSH session, enter the following command to capture ping traffic to branch2_client:
   `diagnose sniffer packet any "host 10.0.2.101 and icmp" 4`
5. Open an SSH session to branch1_client.
6. Log in with the password `password`.

7. Ping `10.0.2.101`, and then leave the ping running.
8. On the branch1_fgt SSH session, examine the sniffer output.

```
13.171671 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
13.171818 T_INET_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
13.175726 T_INET_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
13.175741 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
14.172653 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
14.172685 T_INET_0_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
14.174132 T_INET_0_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
14.174147 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

The packets are initially routed through the overlay (`T_INET_0`, the parent tunnel), and then through the shortcut (`T_INET_0_0`).

9. On the branch1_fgt SSH session, stop the sniffer, and then enter the following commands:

```
get ipsec tunnel list
diagnose sys sdwan service
get router info routing-table details 10.0.2.101
```

Your output should be similar to the following example:

```
branch1_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/
0.0.0.0 STATUS=up TIMEOUT=1218

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/
0.0.0.0 STATUS=up TIMEOUT=1217

NAME=T_INET_0_0 REMOTE-GW=203.0.113.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/
0.0.0.0 STATUS=up TIMEOUT=1722

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.
0.0.0 STATUS=up TIMEOUT=1218
```

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Member sub interface(4):
    2: seq_num(3), interface(T_INET_0):
       1: T_INET_0_0(26)
  Members(4):
    1: Seq_num(3 T_INET_0_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(3 T_INET_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    3: Seq_num(4 T_INET_1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    4: Seq_num(5 T_MPLS), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

```
branch1_fgt # get router info routing-table details 10.0.2.101

Routing table for VRF=0
Routing entry for 10.0.2.0/24
  Known via "bgp", distance 200, metric 0, best
  Last update 00:05:25 ago
  * vrf 0 10.201.1.1 priority 1 (recursive is directly connected, T_INET_0_0)
  * vrf 0 10.202.1.1 priority 1 (recursive is directly connected, T_INET_1)
  * vrf 0 10.203.1.1 priority 1 (recursive is directly connected, T_MPLS)
  * vrf 0 10.201.1.1 priority 1 (recursive is directly connected, T_INET_0_0)
  * vrf 0 10.202.1.1 priority 1 (recursive is directly connected, T_INET_1)
  * vrf 0 10.203.1.1 priority 1 (recursive is directly connected, T_MPLS)
  * vrf 0 10.201.1.1 priority 1 (recursive is directly connected, T_INET_0_0)
  * vrf 0 10.202.1.1 priority 1 (recursive is directly connected, T_INET_1)
  * vrf 0 10.203.1.1 priority 1 (recursive is directly connected, T_MPLS)
```

- The shortcut appears in the IPsec tunnel list.
- The shortcut is listed in the rule status, and placed at the top of the outgoing interface list. That is, the shortcut is the preferred member.
- The shortcut replaces the parent tunnel as the best route to 10.0.2.101.

10. On the branch1_fgt SSH session, restart the sniffer command.
11. On the WAN simulator page, increase the delay on **BR1-ISP1** to 110 ms, so the overlay doesn't meet the SLA target.

You increased the latency on the traffic forwarded to branch1_fgt over T_INET_0, specifically in the network segment between branch1_fgt and ISP1. The latency between ISP1 and dc1_fgt is not impacted.

12. On the branch1_fgt SSH session, examine the sniffer output.
    Your output should be similar to the following example:

```
44.956578 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
44.956591 T_INET_0_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
45.067980 T_INET_0_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
45.068000 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
45.957588 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
45.957612 T_INET_1 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
45.960950 T_INET_1 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
45.960962 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
46.959267 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
46.959294 T_INET_1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
46.960304 T_INET_1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
46.960316 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
47.960679 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
47.960694 T_INET_1_0 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
47.962192 T_INET_1_0 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
47.962209 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

- The traffic is initially routed to the T_INET_0_0 shortcut.
- Due to an SLA change, the traffic fails over to T_INET_1. You may see an intermediate failover to T_INET_0, the parent tunnel. This depends on how quickly FortiGate detects the SLA change on the parent tunnel.
- Remember that in previous exercise you configured overlay stickiness on the hub. So tunnel change occurs also for the traffic between the hub and branch2_fgt.
- Finally, the traffic fails over to another shortcut (T_INET_1_0), which is negotiated over T_INET_1.

13. On the branch1_fgt SSH session, stop the sniffer, and then check the rule status again.

Your output should be similar to the following example:

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(14), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Member sub interface(5):
    2: seq_num(4), interface(T_INET_1):
       1: T_INET_1_0(27)
    5: seq_num(3), interface(T_INET_0):
       1: T_INET_0_0(26)
  Members(5):
    1: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(4 T_INET_1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 T_MPLS), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    4: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    5: Seq_num(3 T_INET_0), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255
```

- The new shortcut (T_INET_1_0) is listed in the rule status, and placed at the top of the outgoing interface list. That is, the new shortcut is now the preferred member.
- The T_INET_0_0 shortcut and its parent tunnel don't meet any SLA targets, and therefore, are placed at the bottom of the outgoing interface list.

14. On the branch1_fgt SSH session, restart the sniffer command.
15. On the WAN simulator page, increase the delay on **BR1-ISP2** to 110 ms, so the overlay doesn't meet the SLA target.
16. Examine the sniffer output.

    You will see similar behavior to what you saw in the previous test:

    - The traffic is initially routed to the T_INET_1_0 shortcut.
    - Due to an SLA change, the traffic may fail over to the parent tunnel, but then it fails over to T_MPLS.
    - Finally, the traffic fails over to another shortcut (T_MPLS_0), which is negotiated over T_MPLS.
17. On the branch1_fgt SSH session, check the IPsec tunnel list.

    Your output should be similar to the following example:

```
branch1_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=445

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=444

NAME=T_INET_0_0 REMOTE-GW=203.0.113.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=948

NAME=T_MPLS_0 REMOTE-GW=172.16.0.9:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 ST
ATUS=up TIMEOUT=1783

NAME=T_INET_1_0 REMOTE-GW=203.0.113.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
STATUS=up TIMEOUT=1597

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0 ST
ATUS=up TIMEOUT=445
```

- There are three shortcuts negotiated, one for each overlay, but only one is currently used.
- The lifetime of the shortcuts are inherited from the parent IPsec settings (1800 seconds). That is, idle shortcuts remain up until the lifetime is reached.
- In the next task, to save system resources, you will configure an idle timeout for the shortcuts.

18. On the WAN simulator page, reduce the delay on **BR1-ISP1** and **BR1-ISP2** back to 0 ms.
19. On the branch1_client, stop the ping.

To check VPN log messages

On the FortiGate event logs, you will display event logs related to ADVPN shortcuts and master tunnels.

1. Continuing on the branch1_fgt SSH session, enter the following commands to filter ADVPN shortcut log messages and review them:

```
execute log filter category event
execute log filter field advpnsc 1
execute log display
```

Your output should look similar to the following example:

```
branch1_fgt # exec log display
36 logs found.
10 logs returned.

11: date=2023-01-18 time=08:42:40 eventtime=1674060160911590297 tz="-0800" logid="0101037141"
type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPs
ec tunnel statistics" action="tunnel-stats" remip=203.0.113.1 locip=192.2.0.1 remport=500 locp
ort=500 outintf="port1" cookies="208a7fe573855e9f/dd844082e2849206" user="N/A" group="N/A" use
ralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_INET_0_0" tunnelip=0.0.0
.0 tunnelid=3587130534 tunneltype="ipsec" duration=1292 sentbyte=108360 rcvdbyte=108440 nextst
at=600 advpnsc=1

12: date=2023-01-18 time=08:32:41 eventtime=1674059560906949826 tz="-0800" logid="0101037141"
type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPs
ec tunnel statistics" action="tunnel-stats" remip=203.0.113.1 locip=192.2.0.1 remport=500 locp
ort=500 outintf="port1" cookies="208a7fe573855e9f/dd844082e2849206" user="N/A" group="N/A" use
ralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_INET_0_0" tunnelip=0.0.0
.0 tunnelid=3587130534 tunneltype="ipsec" duration=692 sentbyte=58044 rcvdbyte=58124 nextstat=
600 advpnsc=1
```

2. Enter the following commands to update the filter and display VPN logs related to master tunnels:

```
execute log filter field advpnsc 0
execute log display
```

Your output should look similar to the following example:

```
branch1_fgt # execute log filter field advpnsc 0

branch1_fgt # execute log display
45 logs found.
10 logs returned.

1: date=2023-01-18 time=09:12:40 eventtime=1674061960902596485 tz="-0800" logid="0101037141" t
ype="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPse
c tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9 remport=500 locpor
t=500 outintf="port2" cookies="d89f84461900921d/8993e91de33a102b" user="N/A" group="N/A" usera
lt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.202.1.2 vpntunnel="T_INET_1" tunnelip=N/
A tunnelid=3587130538 tunneltype="ipsec" duration=5383 sentbyte=581759 rcvdbyte=582088 nextsta
t=600 advpnsc=0

2: date=2023-01-18 time=09:12:40 eventtime=1674061960902587720 tz="-0800" logid="0101037141" t
ype="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPse
c tunnel statistics" action="tunnel-stats" remip=100.64.1.1 locip=192.2.0.1 remport=500 locpor
t=500 outintf="port1" cookies="0796c7b86a8559c0/5bea75186bf0afa4" user="N/A" group="N/A" usera
lt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.201.1.2 vpntunnel="T_INET_0" tunnelip=N/
A tunnelid=3587130537 tunneltype="ipsec" duration=5383 sentbyte=583309 rcvdbyte=582340 nextsta
t=600 advpnsc=0
```

3. Enter the following command to reset the log filter:

```
execute log filter reset
```

4. Enter the following commands to clear the shortcuts:

```
diagnose vpn ike gateway clear name T_INET_0_0
```

```
diagnose vpn ike gateway clear name T_INET_1_0
diagnose vpn ike gateway clear name T_MPLS_0
```

5. On the branch1_fgt SSH session, check the IPsec tunnel list to confirm that all the shortcuts were cleared.

Configure an Idle Timeout for ADVPN

You will configure an idle timeout for ADVPN to save system resources.

To configure an idle timeout for ADVPN

1. Continuing on the FortiManager GUI, click **Provisioning Templates** > **CLI Templates**.
2. Double-click **Spoke-ADVPN Idle Timeout** to view the CLI template settings.
3. Examine the CLI template.

In the IPsec phase 1 configuration, each overlay has the `idle-timeout` setting enabled and the `idle-timeoutinterval` setting set to `5` minutes.

4. Click **Cancel** to exit the CLI template.
5. Double-click the **Spoke** CLI template group to edit its settings.
6. In the **Members** list, add **Spoke-ADVPN Idle Timeout**.
7. Click **OK** to save the settings.
8. Install the device settings on branch1_fgt and branch2_fgt.
9. On the branch1_client SSH session, ping `10.0.2.101`, and then leave the ping running.
10. On the branch1_fgt SSH session, verify that the shortcut over T_INET_0 was negotiated.
    Your output should look similar to the following example:

```
branch1_fgt # get ipsec tunnel list
NAME=T_INET_0 REMOTE-GW=100.64.1.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0
.0 STATUS=up TIMEOUT=933

NAME=T_INET_1 REMOTE-GW=100.64.1.9:0
        P2NAME=T_INET_1 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0
.0 STATUS=up TIMEOUT=939

NAME=T_INET_0_0 REMOTE-GW=203.0.113.1:0
        P2NAME=T_INET_0 PROXY-ID-SOURCE=10.201.1.1/10.201.1.1 PROXY-ID-DESTINATION=0.0.0.0
/0.0.0.0 STATUS=up TIMEOUT=1781
        P2NAME=T_INET_0 PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0
.0 STATUS=up TIMEOUT=1778

NAME=T_MPLS REMOTE-GW=172.16.1.5:0
        P2NAME=T_MPLS PROXY-ID-SOURCE=0.0.0.0/0.0.0.0 PROXY-ID-DESTINATION=0.0.0.0/0.0.0.0
 STATUS=up TIMEOUT=936
```

The shortcut appears in the IPsec list. Notice that the tunnel lifetime is close to 1800 seconds.

11. On the branch1_fgt SSH session, enter the following commands to enable debug for the IKE process:

```
diagnose debug application ike -1
diagnose debug console timestamp enable
diagnose debug enable
```

12. On the branch1_client, stop the ping.
13. On the branch1_fgt SSH session, wait 5 minutes, and then monitor the output.

    After 5 minutes, the debug shows the following messages to indicate that the shortcut timed out:

```
branch1_fgt # diagnose debug enable

branch1_fgt # 2023-03-08 09:14:29.895293 ike shrank heap by 159744 bytes
2023-03-08 09:20:07.698875 ike 0:T_INET_0_0: connection idle time-out
2023-03-08 09:20:07.702081 ike 0:T_INET_0_0: deleting
2023-03-08 09:20:07.704799 ike 0:T_INET_0_0: flushing
2023-03-08 09:20:07.707465 ike 0:T_INET_0_0: deleting IPsec SA with SPI fdcdc936
2023-03-08 09:20:07.710962 ike 0:T_INET_0_0:T_INET_0: deleted IPsec SA with SPI fdcdc936,
SA count: 0
2023-03-08 09:20:07.715647 ike 0:T_INET_0_0: sending SNMP tunnel DOWN trap for T_INET_0
2023-03-08 09:20:07.719917 ike 0:T_INET_0_0: sending tunnel down event for addr 0.0.0.0
2023-03-08 09:20:07.724106 ike 0:T_INET_0_0:T_INET_0: delete
2023-03-08 09:20:07.727058 ike 0:T_INET_0_0: deleting IPsec SA with SPI fdcdc935
2023-03-08 09:20:07.730639 ike 0:T_INET_0_0:T_INET_0: deleted IPsec SA with SPI fdcdc935,
SA count: 0
2023-03-08 09:20:07.735626 ike 0:T_INET_0_0: sending SNMP tunnel DOWN trap for T_INET_0
2023-03-08 09:20:07.739834 ike 0:T_INET_0_0: sending tunnel down event for addr 0.0.0.0
2023-03-08 09:20:07.744133 ike 0:T_INET_0_0:T_INET_0: delete
2023-03-08 09:20:07.747172 ike 0:T_INET_0_0: flushed
```

Stop and think!

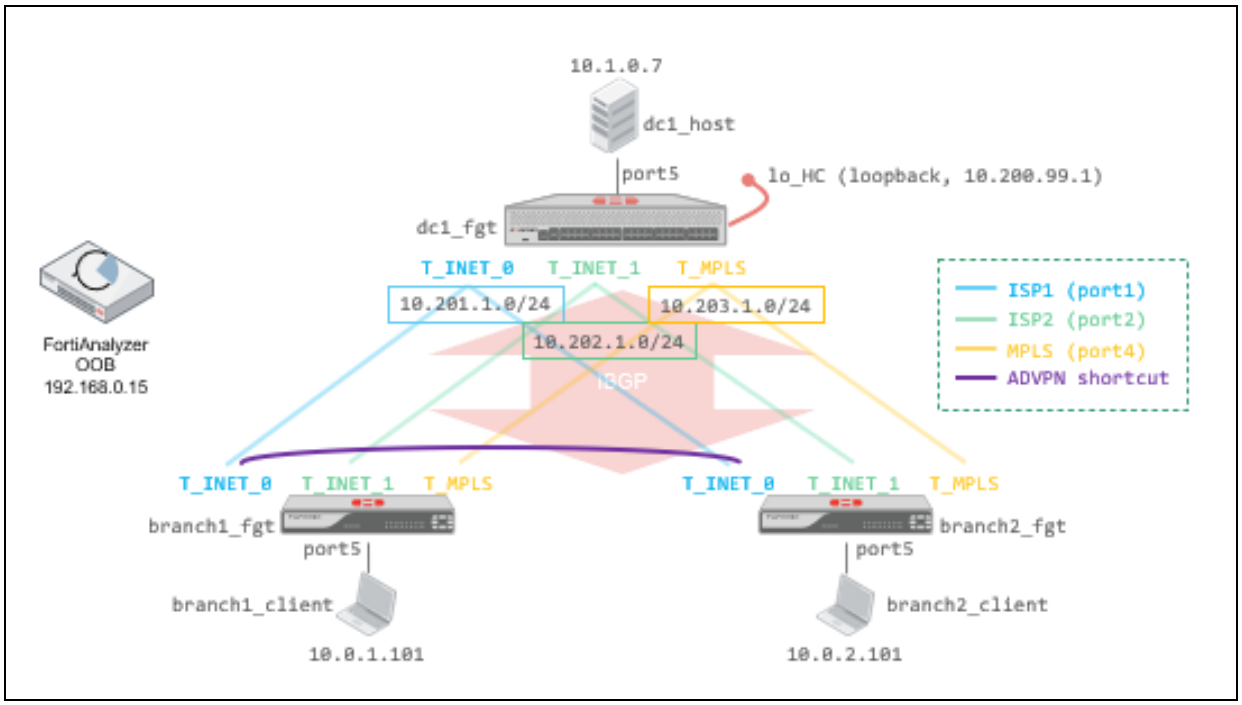
FortiGate monitors the shortcut using ping. The ping probes are sent to the address of the remote end over the shortcut. Therefore, the shortcut is not really idle. Why did it time out?

FortiGate does not consider health check probes to be user traffic. Therefore, health check probes don't prevent a shortcut from timing out.

Lab 7: SD-WAN Monitoring With FortiAnalyzer

In this lab, you will monitor your SD-WAN deployment using FortiAnalyzer. Note that, for this lab exercise, there is no separate FortiAnalyzer. Instead, you will use the FortiAnalyzer features enabled on FortiManager.

The following topology has been preconfigured for you:



Objectives

- Verify log settings on FortiGate devices
- Analyze traffic logs
- Analyze SD-WAN event logs
- Discover the **Secure SD-WAN Monitor** page
- Discover the **SD-WAN Summary** page

Time to Complete

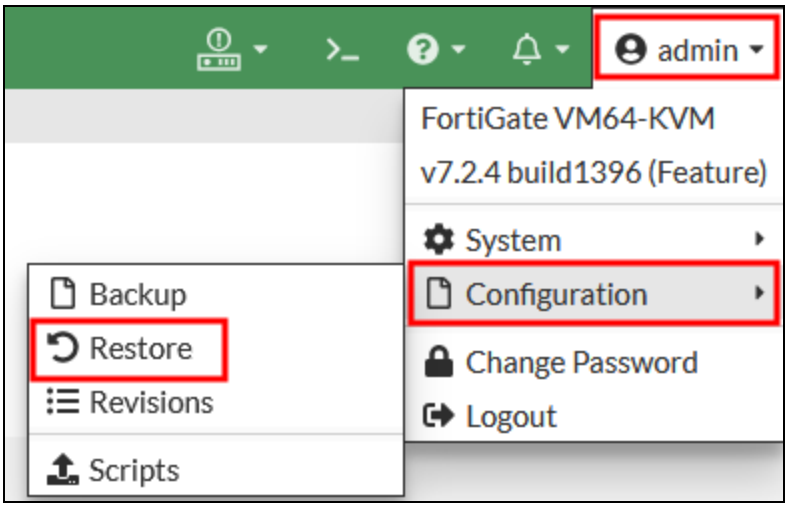
Estimated: 40 minutes

Prerequisites

Before you begin this lab, you must restore a configuration file to branch1_fgt, branch2_fgt, dc1_fgt, and FortiManager.

To restore the branch1_fgt, branch2_fgt, and dc1_fgt configuration files

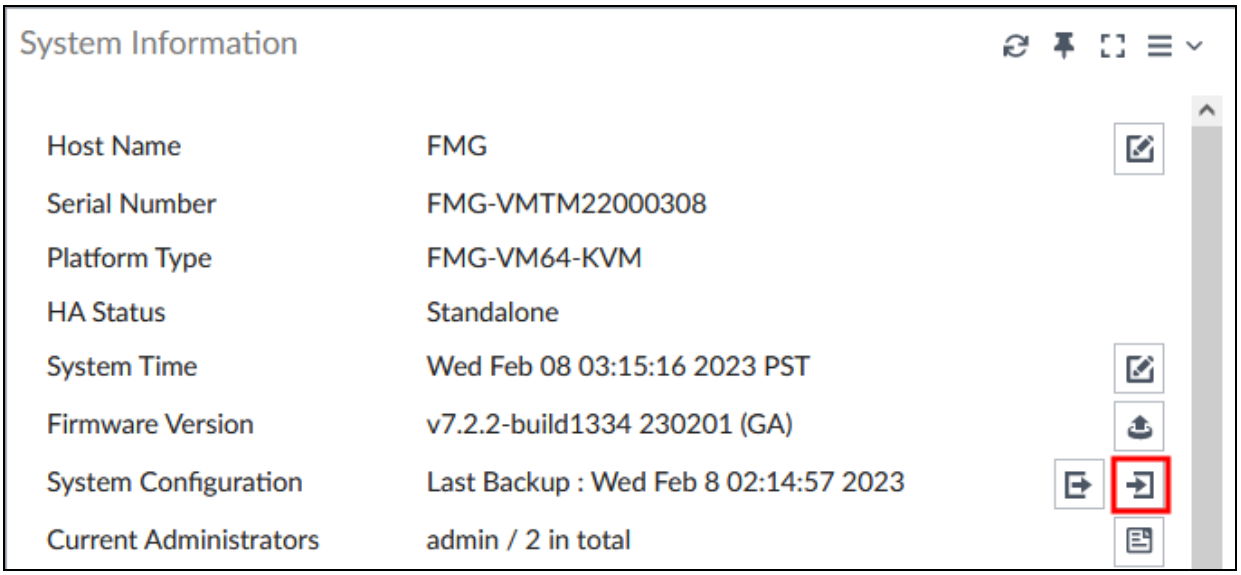
1. On the local-client, open a browser, and then log in to the branch1_fgt GUI with the username `admin` and password `password`.
2. If you receive a warning stating that the FortiGate is currently being managed by FortiManager, click **Login Read-Write**, and then click **Yes** to confirm.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-7**, select `lab7-branch1_fgt_7-2-3_initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to restart.
8. Repeat the previous steps to restore the configuration file on branch2_fgt.
   Use the following configuration file: `lab7-branch2_fgt_7-2-3_initial.conf`.
9. Repeat the previous steps to restore the configuration file on dc1_fgt.
   Use the following configuration file: `lab7-dc1_fgt_7-2-3_initial.conf`.

To restore the FortiManager configuration file

1. On the local-client, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root** > **System Settings**, and then click **Dashboard**.
3. In the **System Information** widget, click the configuration restore icon.



4. Click **Browse** to indicate the local file to upload.
5. Click **Desktop** > **Resources** > **SD-WAN** > **Lab-7**, select `lab7-SYS_FMG_7-2-1_initial.dat`, and then click **OK**.
6. Wait until the file is uploaded and FortiManager finishes rebooting.
7. Log in to the FortiManager GUI with the username `admin` and password `password`.
8. Click **root** > **System Settings**, and then click **Advanced** > **Advanced Settings**.
9. In the **Offline Mode** field, select **Disable**.
10. Click **Apply** to save the settings.

Exercise 1: Monitoring SD-WAN With FortiAnalyzer

FortiAnalyzer centralizes all log messages that the managed devices send. It stores the log messages, correlates the information received, and presents the information in easy-to-read graphs to help administrators with day-to-day network monitoring tasks or punctual troubleshooting tasks.

In this exercise, you will navigate through the FortiAnalyzer menus to understand how you can use it for monitoring your SD-WAN deployment.

Confirm Log Forwarding on the FortiGate Devices

In a previous lab, you configured the FortiGate devices to send logs to FortiAnalyzer. You also configured SLA health checks to send `sla-fail-log` and `sla-pass-log` messages to FortiAnalyzer. You will review these settings.

To verify the log forwarding configuration on FortiGate

1. Open an SSH session to branch1_fgt, and another to branch2_fgt.
2. Log in with the username `admin` and password `password`.
3. Enter the following command on both branch1_fgt and branch2_fgt to verify that the configuration was installed:
   ```
   show log fortianalyzer setting
   ```
   Your output should look similar to the following example:
   ```
   branch1_fgt # show log fortianalyzer setting
   config log fortianalyzer setting
       set status enable
       set server "192.168.0.15"
       set serial "FMG-VMTM22000308"
       set upload-option realtime
       set reliable enable
   end
   ```
4. Confirm the status, server IP address, and upload option.
   The serial number might be different. Note that the serial number refers to a FortiManager. This is because, for this lab, we use FortiAnalyzer features on FortiManager.

To verify SLA-fail and SLA-pass log settings

1. Continuing on the branch1_fgt and branch2_fgt SSH sessions, enter the following commands to check the SLA-fail and SLA-pass log settings:
   ```
   config sys sdwan
   show health-check Level3_DNS
   show health-check VPN_PING
   ```
   Your output should look similar to the following example:

```
branch1_fgt (sdwan) # show health-check Level3_DNS
config health-check
    edit "Level3_DNS"
        set server "4.2.2.1" "4.2.2.2"
        set sla-fail-log-period 10
        set sla-pass-log-period 10
        set members 1 2
        config sla
            edit 1
                set latency-threshold 150
                set jitter-threshold 25
                set packetloss-threshold 5
            next
        end
    next
end
```

2. Confirm that `sla-fail-log-period` and `sla-pass-log-period` are set for both health checks.

Analyze Traffic Logs

You will generate internet traffic from branch1_client and branch2_client using the traffic generator tool. Then, you will review the corresponding traffic logs on FortiAnalyzer.

To generate internet traffic from branch1_client and branch2_client

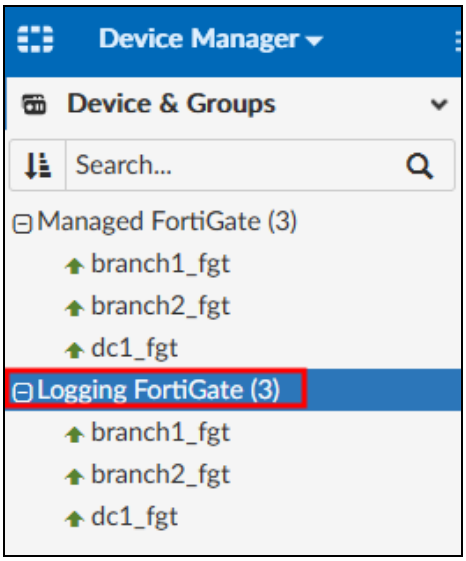
1. Open an SSH session to branch1_client.
2. Log in with the username `root` and password `password`.
3. Enter the following commands:
   ```
   cd /fortipoc/fit/
   ./myfit.sh
   ```
4. Repeat the previous steps on branch2_client.

To generate internet traffic from branch1_client to branch2_client

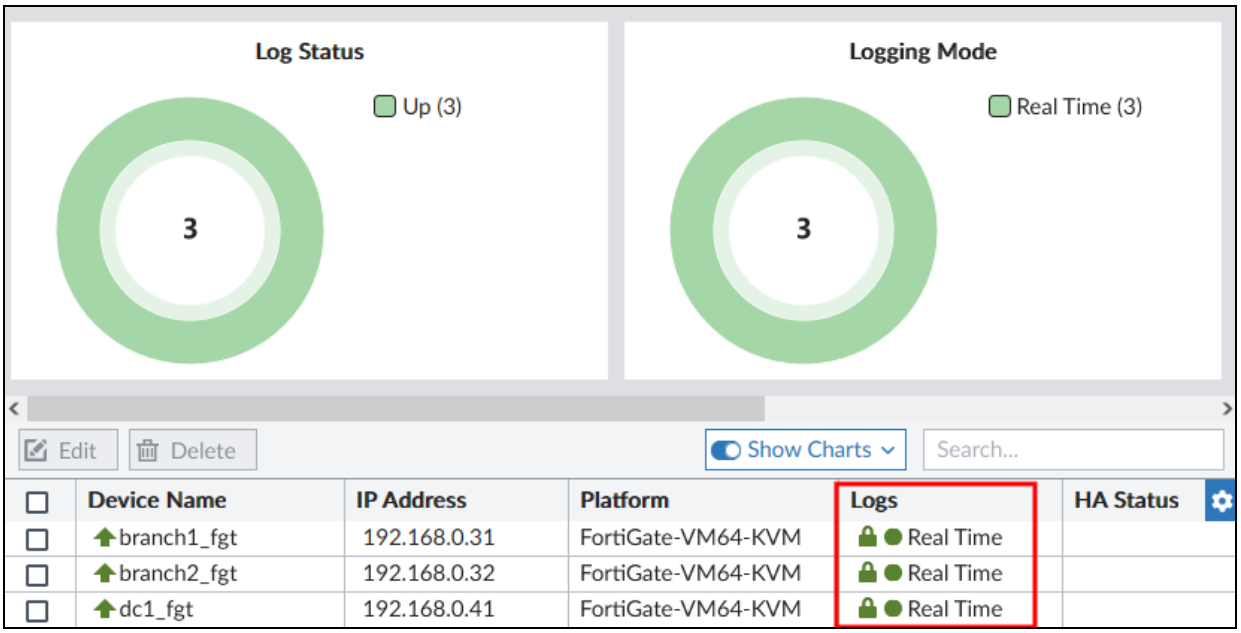
1. Open a second SSH session to branch1_client.
2. Log in with the username `root` and the password `password`.
3. Ping `10.0.2.101`, and then leave the ping running.

To verify logging to FortiAnalyzer (FortiManager)

1. On the FortiManager GUI, log in with the username `admin` and password `password`.
2. Click **root** > **Device Manager** > **Device & Groups**.
3. Click **Logging FortiGate**.



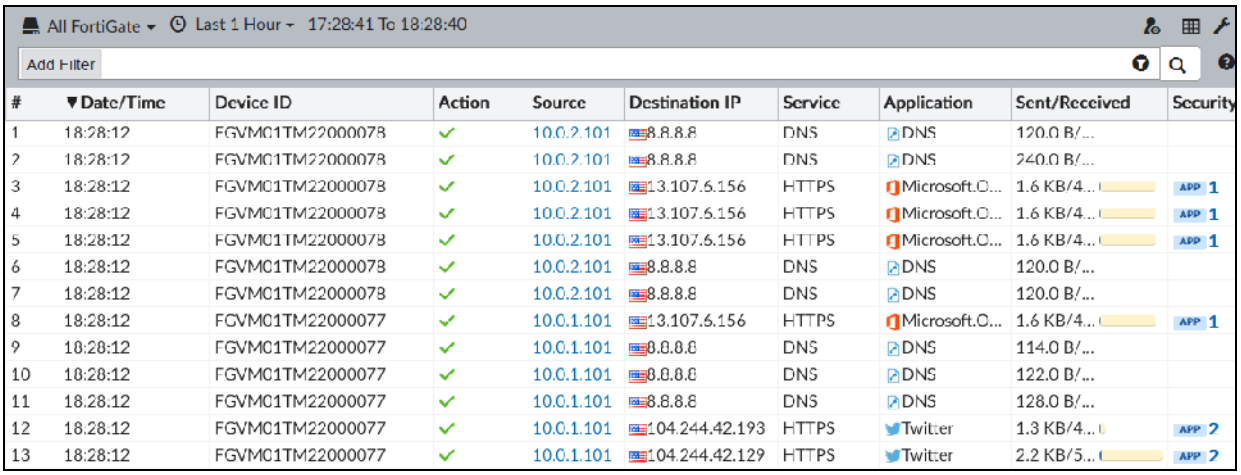
Your page should look similar to the following example:



The green circle beside **Real Time** indicates that FortiAnalyzer is receiving logs from the connected devices.

To analyze traffic logs

1. Continuing on the FortiManager GUI, click **Device Manager** > **Log View**.
2. Click **Traffic**.
   Your page should look similar to the following example:



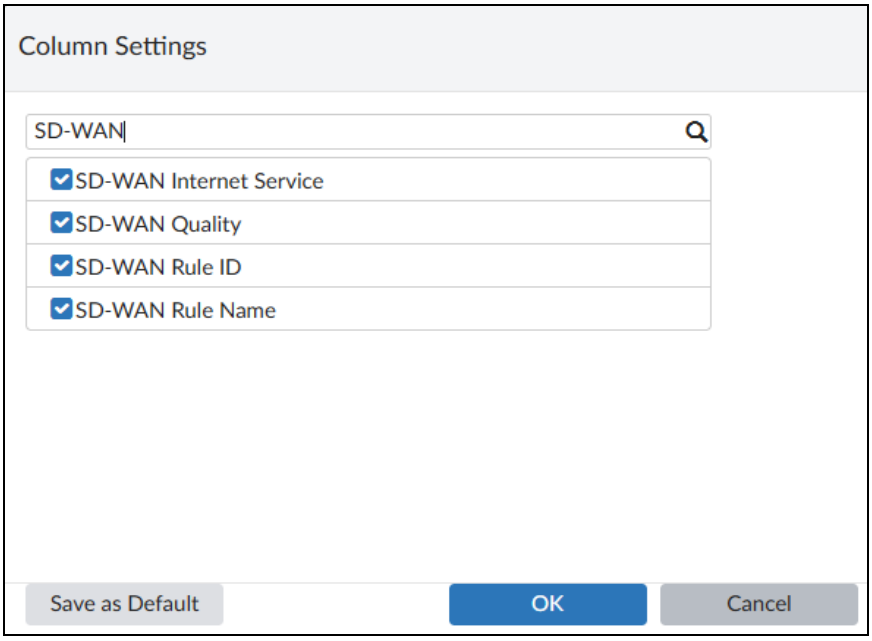
#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received	Security
1	18:28:12	FGVM01TM22000078	✓	10.0.2.101	8.8.8.8	DNS	DNS	120.0 B/...	
2	18:28:12	FGVM01TM22000078	✓	10.0.2.101	8.8.8.8	DNS	DNS	240.0 B/...	
3	18:28:12	FGVM01TM22000078	✓	10.0.2.101	13.107.6.156	HTTPS	Microsoft.O...	1.6 KB/4...	APP 1
4	18:28:12	FGVM01TM22000078	✓	10.0.2.101	13.107.6.156	HTTPS	Microsoft.O...	1.6 KB/4...	APP 1
5	18:28:12	FGVM01TM22000078	✓	10.0.2.101	13.107.6.156	HTTPS	Microsoft.O...	1.6 KB/4...	APP 1
6	18:28:12	FGVM01TM22000078	✓	10.0.2.101	8.8.8.8	DNS	DNS	120.0 B/...	
7	18:28:12	FGVM01TM22000078	✓	10.0.2.101	8.8.8.8	DNS	DNS	120.0 B/...	
8	18:28:12	FGVM01TM22000077	✓	10.0.1.101	13.107.6.156	HTTPS	Microsoft.O...	1.6 KB/4...	APP 1
9	18:28:12	FGVM01TM22000077	✓	10.0.1.101	8.8.8.8	DNS	DNS	114.0 B/...	
10	18:28:12	FGVM01TM22000077	✓	10.0.1.101	8.8.8.8	DNS	DNS	122.0 B/...	
11	18:28:12	FGVM01TM22000077	✓	10.0.1.101	8.8.8.8	DNS	DNS	128.0 B/...	
12	18:28:12	FGVM01TM22000077	✓	10.0.1.101	104.244.42.193	HTTPS	Twitter	1.3 KB/4...	APP 2
13	18:28:12	FGVM01TM22000077	✓	10.0.1.101	104.244.42.129	HTTPS	Twitter	2.2 KB/5...	APP 2

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

3. In the upper-right corner, click the column setting icon, and then click **More Columns**.

4. Select **Destination Interface**, **SD-WAN Internet Service**, **SD-WAN Quality**, **SD-WAN Rule ID**, and **SD-WAN Rule Name**.

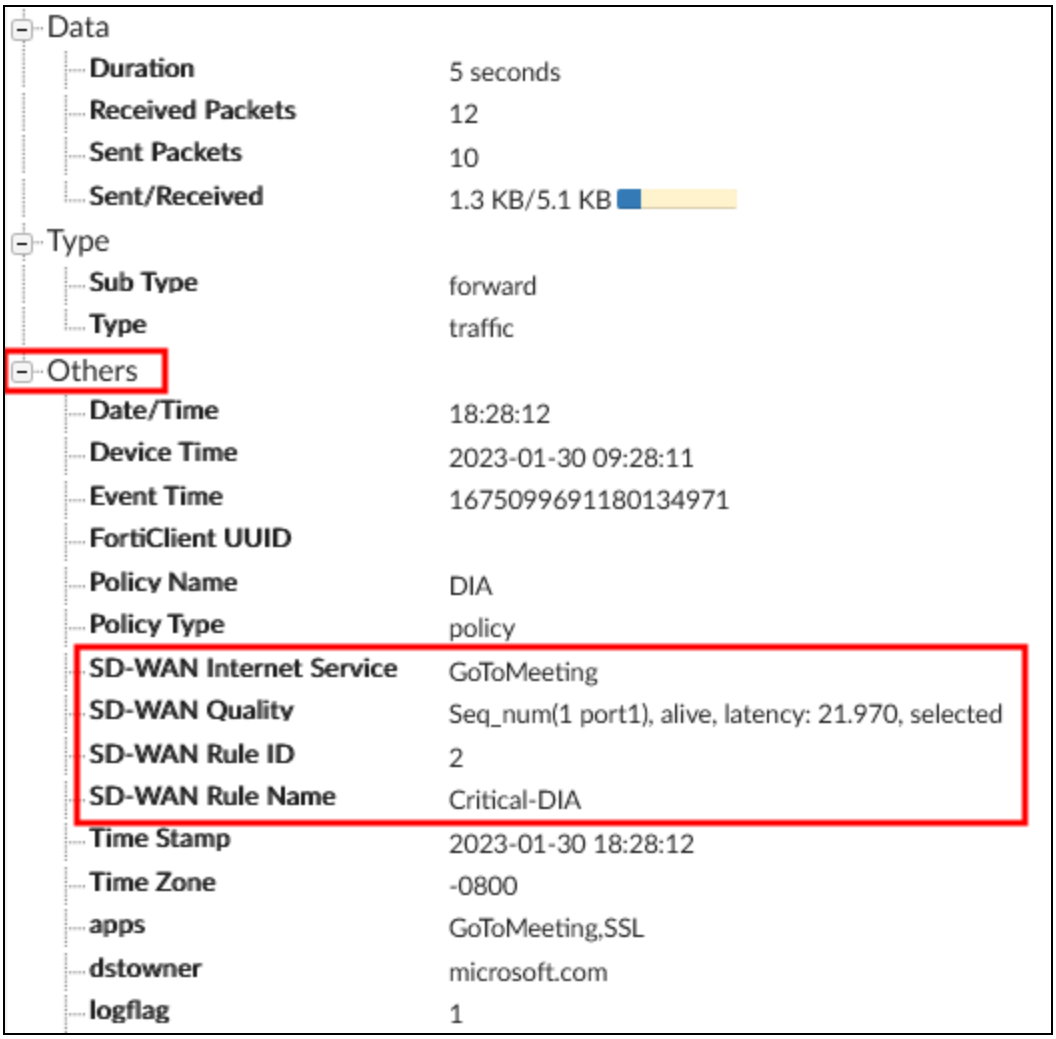
Use the column settings search box to quickly find the columns.



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

Application	Sent/Received	Security Event List	SD-WAN Internet Service	SD-WAN Quality	SD-WAN Rule ...	SD-WAN Rule Name
Twitter	1.3 KB...	APP 2	Twitter	Seq_num(2 port2...	3	Non-Critical-DIA
Twitter	2.2 KB...	APP 2	Twitter	Seq_num(2 port2...	3	Non-Critical-DIA
Microsof...	1.6 KB...	APP 1			0	
DNS	124.0 ...				0	
DNS	128.0 ...				0	
DNS	130.0 ...				0	
GoToMe...	1.3 KB...	APP 2	GoToMeeting	Seq_num(1 port1...	2	Critical-DIA
Salesforce	1.9 KB...	APP 2	Salesforce	Seq_num(1 port1...	2	Critical-DIA
Microsof...	1.7 KB...	APP 1			0	
Microsof...	1.7 KB...	APP 1			0	
DNS	114.0 ...				0	
DNS	122.0 ...				0	
DNS	120.0 ...				0	
Salesforce	2.0 KB...	APP 2	Salesforce	Seq_num(1 port1...	2	Critical-DIA
GoToMe...	1.3 KB...	APP 2	GoToMeeting	Seq_num(1 port1...	2	Critical-DIA
DNS	114.0 ...				0	

6. Identify messages for the main SD-WAN rules configured: **Critical-DIA** and **Non-Critical-DIA**.
7. Double-click a log message to view details.
8. Expand the **Others** submenu to see the SD-WAN details contained in the log message.



FortiAnalyzer displays traffic logs for all managed FortiGate devices.

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

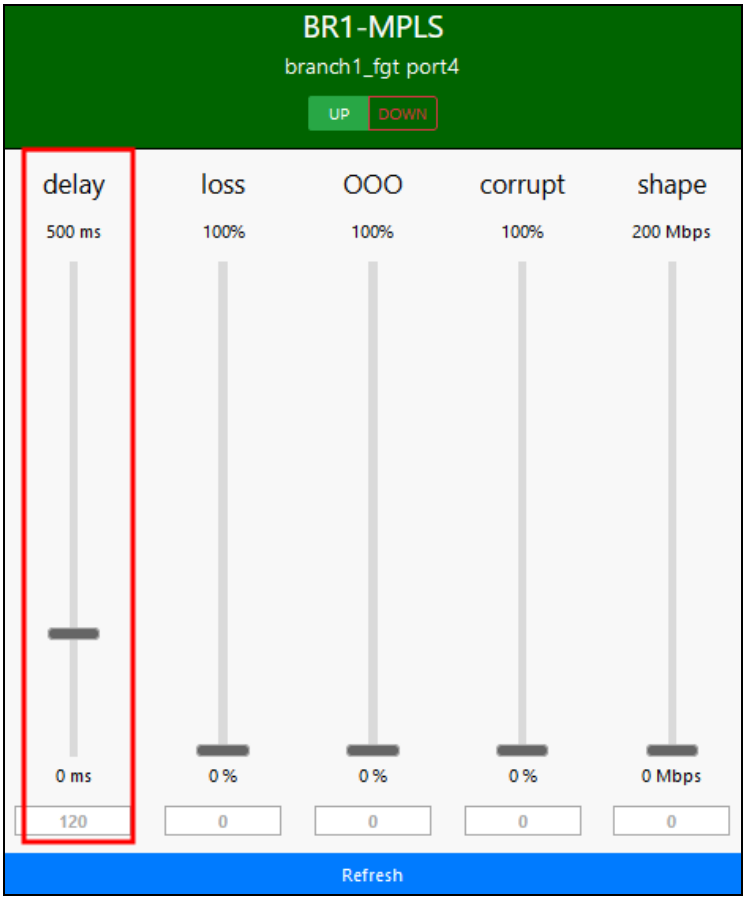
Analyze Event Logs

You will trigger link down and link up events, and then review the log messages corresponding to those events on FortiAnalyzer.

To trigger events

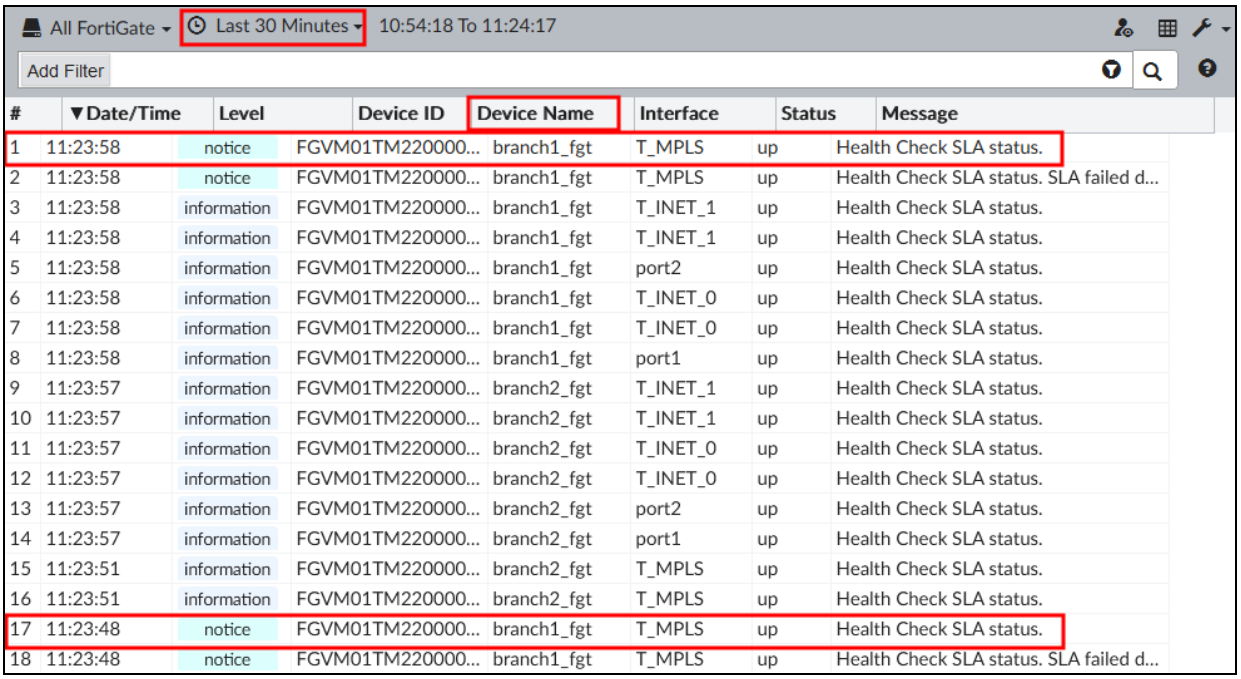
1. Access the WAN simulator page.
2. Locate the **BR1-ISP1** and **BR1-MPLS** control panels.
3. On **BR1-ISP1**, click **DOWN** to switch off the interface.

4. Wait a few seconds, and then click **UP** to switch the interface back on.
5. On **BR1-MPLS**, use the vertical bar to increase the **delay** to 120 ms.



To analyze event logs

1. Continuing on the FortiManager GUI, click **Log View**, and then click **Event** > **SD-WAN**.
2. Click **Last 4 Hours**, and then select **Last 30 Minutes** in the drop-down list.
3. In the upper-right corner, click the column setting icon, and then click **More columns**.
4. Select **Device Name**, and then click **OK** to save the settings.
5. Drag and drop the **Device Name** column beside the **Interface** column.
   Your page should look similar to the following example:



#	Date/Time	Level	Device ID	Device Name	Interface	Status	Message
1	11:23:58	notice	FGVM01TM220000...	branch1_fgt	T_MPLS	up	Health Check SLA status.
2	11:23:58	notice	FGVM01TM220000...	branch1_fgt	T_MPLS	up	Health Check SLA status. SLA failed d...
3	11:23:58	information	FGVM01TM220000...	branch1_fgt	T_INET_1	up	Health Check SLA status.
4	11:23:58	information	FGVM01TM220000...	branch1_fgt	T_INET_1	up	Health Check SLA status.
5	11:23:58	information	FGVM01TM220000...	branch1_fgt	port2	up	Health Check SLA status.
6	11:23:58	information	FGVM01TM220000...	branch1_fgt	T_INET_0	up	Health Check SLA status.
7	11:23:58	information	FGVM01TM220000...	branch1_fgt	T_INET_0	up	Health Check SLA status.
8	11:23:58	information	FGVM01TM220000...	branch1_fgt	port1	up	Health Check SLA status.
9	11:23:57	information	FGVM01TM220000...	branch2_fgt	T_INET_1	up	Health Check SLA status.
10	11:23:57	information	FGVM01TM220000...	branch2_fgt	T_INET_1	up	Health Check SLA status.
11	11:23:57	information	FGVM01TM220000...	branch2_fgt	T_INET_0	up	Health Check SLA status.
12	11:23:57	information	FGVM01TM220000...	branch2_fgt	T_INET_0	up	Health Check SLA status.
13	11:23:57	information	FGVM01TM220000...	branch2_fgt	port2	up	Health Check SLA status.
14	11:23:57	information	FGVM01TM220000...	branch2_fgt	port1	up	Health Check SLA status.
15	11:23:51	information	FGVM01TM220000...	branch2_fgt	T_MPLS	up	Health Check SLA status.
16	11:23:51	information	FGVM01TM220000...	branch2_fgt	T_MPLS	up	Health Check SLA status.
17	11:23:48	notice	FGVM01TM220000...	branch1_fgt	T_MPLS	up	Health Check SLA status.
18	11:23:48	notice	FGVM01TM220000...	branch1_fgt	T_MPLS	up	Health Check SLA status. SLA failed d...

6. Identify SLA pass log messages, and then double-click some messages to see details.
7. Click **Other** to see SD-WAN information.

For each device and each interface, FortiAnalyzer receives a health-check SLA status, pass or fail, every 10 seconds.

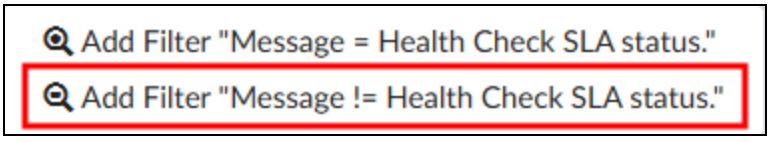
You see those messages because for each health check, the `sla-fail-log-period` and `sla-pass-log-period` settings are set to 10.

Stop and think!

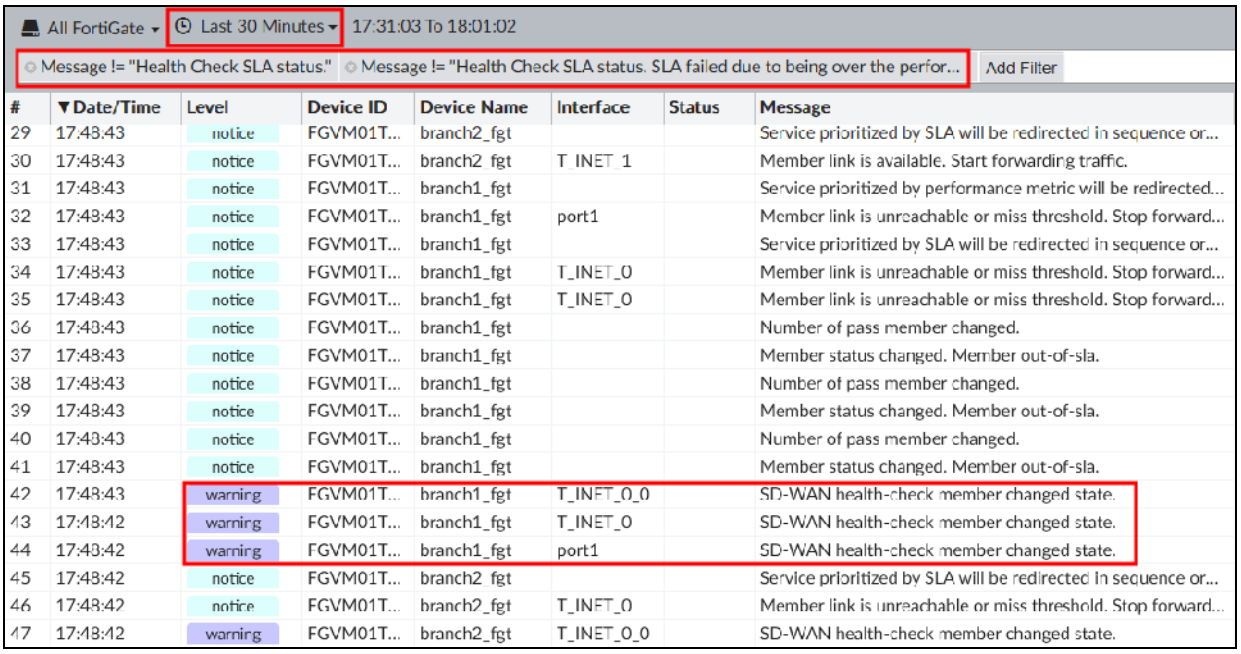
FortiAnalyzer receives both SLA pass and SLA fail log messages for the **T_MPLS** interface of device branch1_fgt. Why?

Log details show that the SLA pass message correspond to the SLA target ID 2 of the **VPN_PING** health check, while the SLA fail message corresponds to the SLA target ID 1 of the same health check.

8. Right-click an SLA pass log message, and then select the filter, as shown in the following image, to filter the list to remove the SLA pass log messages:



9. Repeat the previous step to filter out SLA fail log messages.
   Your page should look similar to the following example:



#	Date/Time	Level	Device ID	Device Name	Interface	Status	Message
29	17:43:43	notice	FGVM01T...	branch2_fgt			Service prioritized by SLA will be redirected in sequence or...
30	17:43:43	notice	FGVM01T...	branch2_fgt	T_INET_1		Member link is available. Start forwarding traffic.
31	17:43:43	notice	FGVM01T...	branch1_fgt			Service prioritized by performance metric will be redirected...
32	17:43:43	notice	FGVM01T...	branch1_fgt	port1		Member link is unreachable or miss threshold. Stop forward...
33	17:43:43	notice	FGVM01T...	branch1_fgt			Service prioritized by SLA will be redirected in sequence or...
34	17:43:43	notice	FGVM01T...	branch1_fgt	T_INET_0		Member link is unreachable or miss threshold. Stop forward...
35	17:43:43	notice	FGVM01T...	branch1_fgt	T_INET_0		Member link is unreachable or miss threshold. Stop forward...
36	17:43:43	notice	FGVM01T...	branch1_fgt			Number of pass member changed.
37	17:43:43	notice	FGVM01T...	branch1_fgt			Member status changed. Member out-of-sla.
38	17:43:43	notice	FGVM01T...	branch1_fgt			Number of pass member changed.
39	17:43:43	notice	FGVM01T...	branch1_fgt			Member status changed. Member out-of-sla.
40	17:43:43	notice	FGVM01T...	branch1_fgt			Number of pass member changed.
41	17:43:43	notice	FGVM01T...	branch1_fgt			Member status changed. Member out-of-sla.
42	17:43:43	warning	FGVM01T...	branch1_fgt	T_INET_0_0		SD-WAN health-check member changed state.
43	17:43:42	warning	FGVM01T...	branch1_fgt	T_INET_0		SD-WAN health-check member changed state.
44	17:43:42	warning	FGVM01T...	branch1_fgt	port1		SD-WAN health-check member changed state.
45	17:43:42	notice	FGVM01T...	branch2_fgt			Service prioritized by SLA will be redirected in sequence or...
46	17:43:42	notice	FGVM01T...	branch2_fgt	T_INET_0		Member link is unreachable or miss threshold. Stop forward...
47	17:43:42	warning	FGVM01T...	branch2_fgt	T_INET_0_0		SD-WAN health-check member changed state.

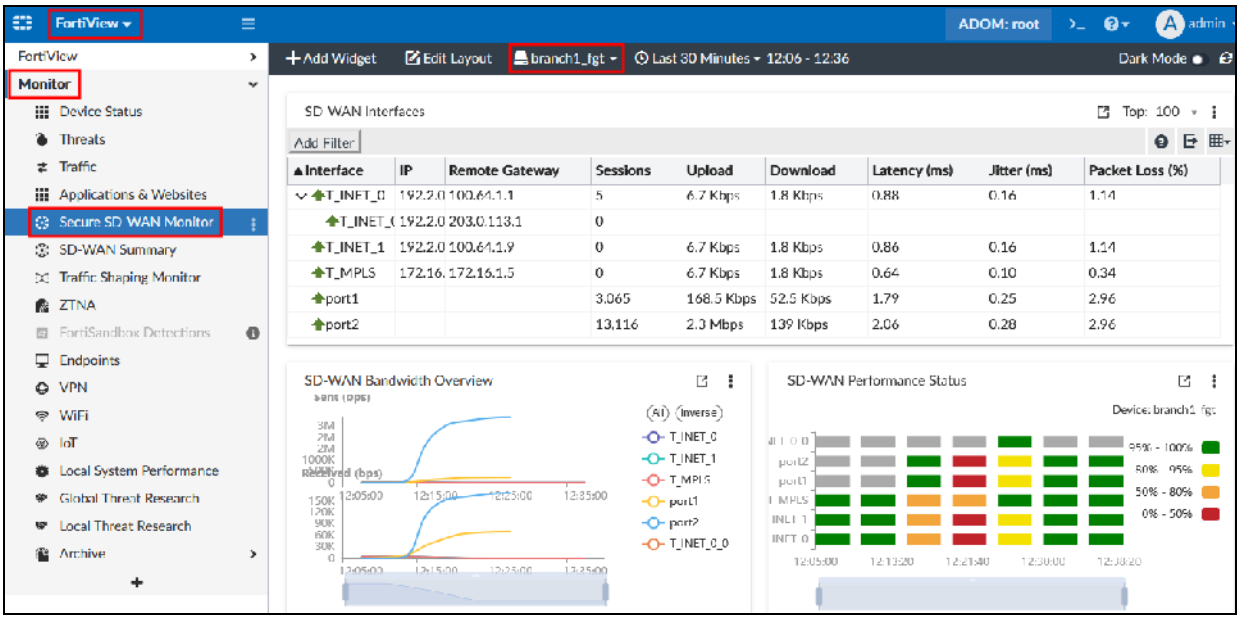
10. Identify the log messages related to the BR1-ISP1 interface shut down.
    You should see the following:
    - The SD-WAN health-check member changed state for port1, overlay tunnel **T_INET_0**, and ADVPN shortcut (level warning).
    - Service prioritized by SLA will be redirected in sequence order (level notice).
    - The member link is unreachable or missed the threshold. Stop forwarding traffic (level notice).
11. Double-click messages to see details.
12. Identify log messages related to the **BR1-ISP1** interface going up.
    You should see the following:
    - The SD-WAN health-check member changed state for port1 and the **T_INET_0** overlay tunnel (level notice).
    - Service prioritized by SLA will be redirected in sequence order (level notice).
    - The member link is available. Start forwarding traffic (level notice).
13. Double-click messages to see details.

Discover the Secure SD-WAN Monitor Page

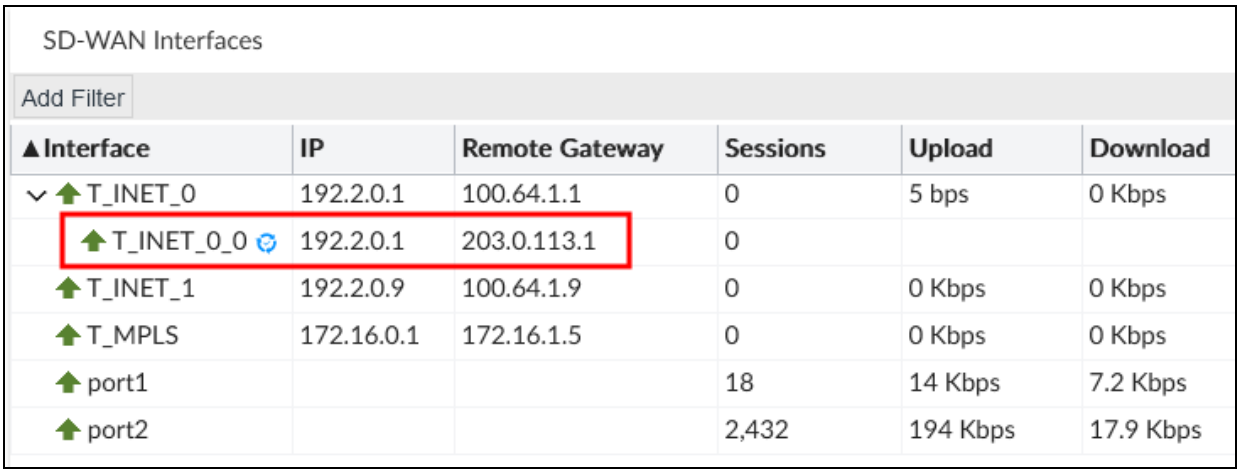
The **Secure SD-WAN Monitor** page provides you with a centralized view of SD-WAN status information for each managed FortiGate. You will discover the widgets available and how to use them.

To discover the Secure SD-WAN Monitor page

1. Continuing on the FortiManager GUI, click **Log View** > **FortiView** > **Monitor**, and then click **Secure SD-WAN Monitor**.
   Your page should look similar to the following example:

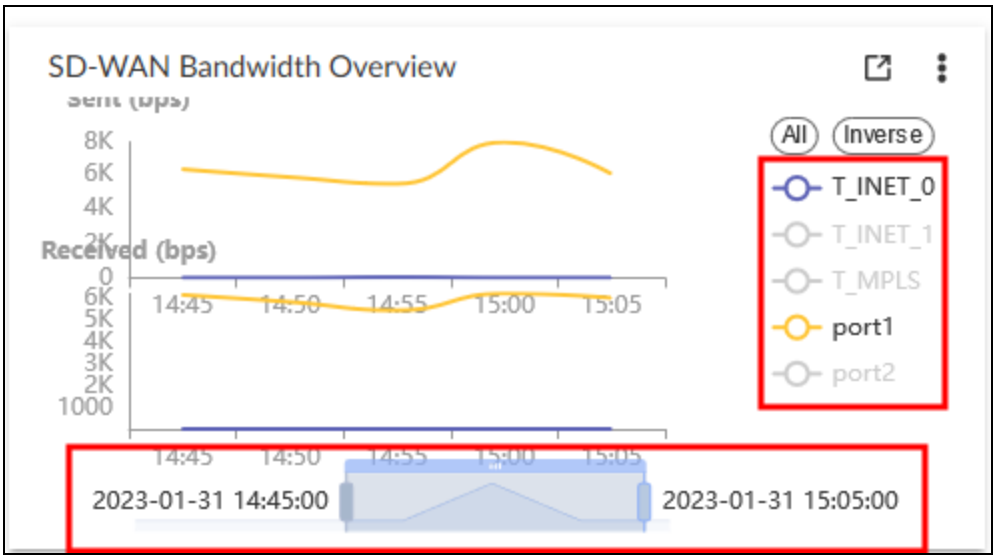


2. Review the widgets available and information provided for branch1_fgt.
3. In the **SD-WAN interfaces** widget, expand the **T_INET_0** tunnel interface to display the established ADVPN shortcut.



4. In the **SD-WAN Bandwidth Overview** widget, click **T_INET_1**, **T_MPLS**, and **port2** to display only the graphs for the port1 interface and **T_INET_0** and **T_INET_0_0** tunnels.
5. Continuing in the **SD-WAN Bandwidth Overview** widget, use the bottom bar to reduce the time period that is displayed.

   This allows you to see additional details for a specific period of time.

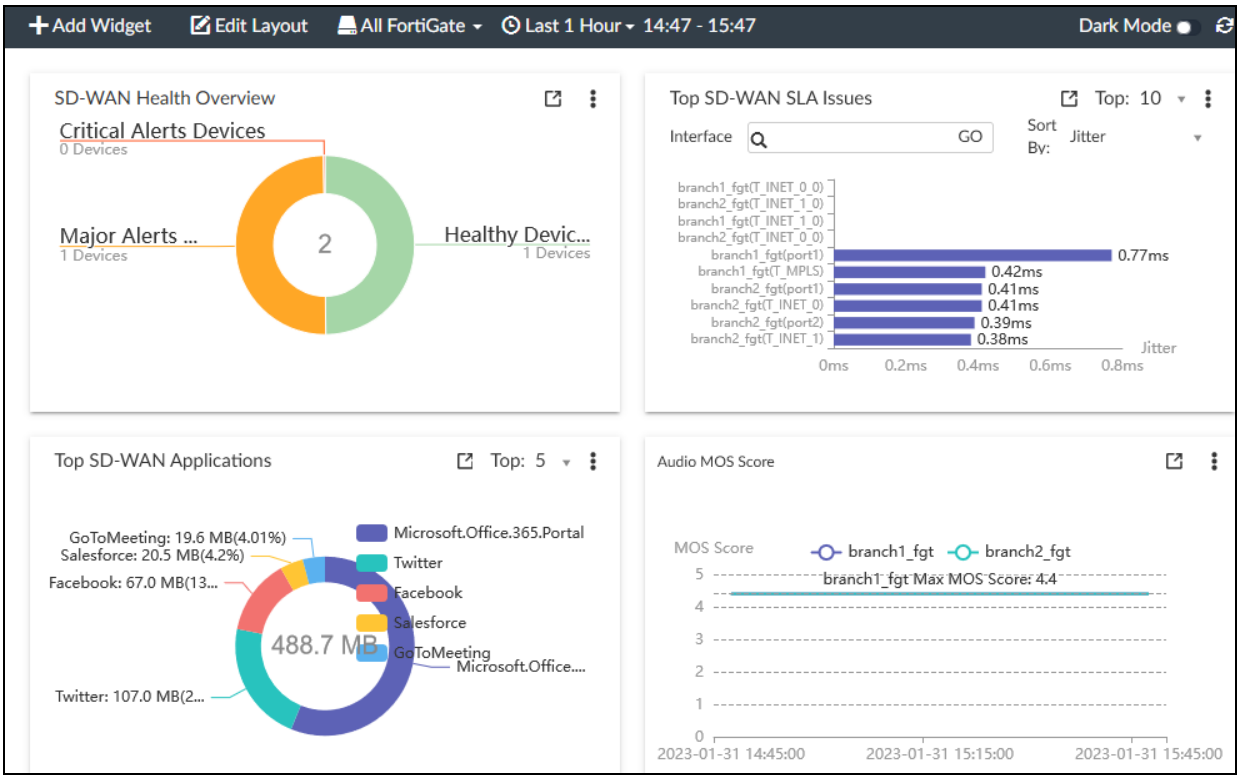


Discover the SD-WAN Summary Page

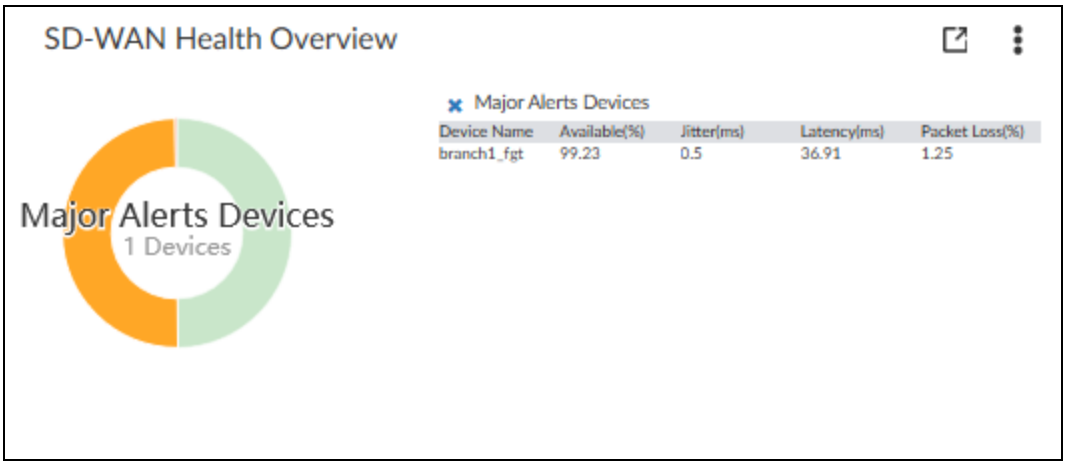
The **SD-WAN Summary** page provides a centralized view of your SD-WAN deployment. It summarizes data for all managed FortiGate devices.

To discover the SD-WAN Summary page

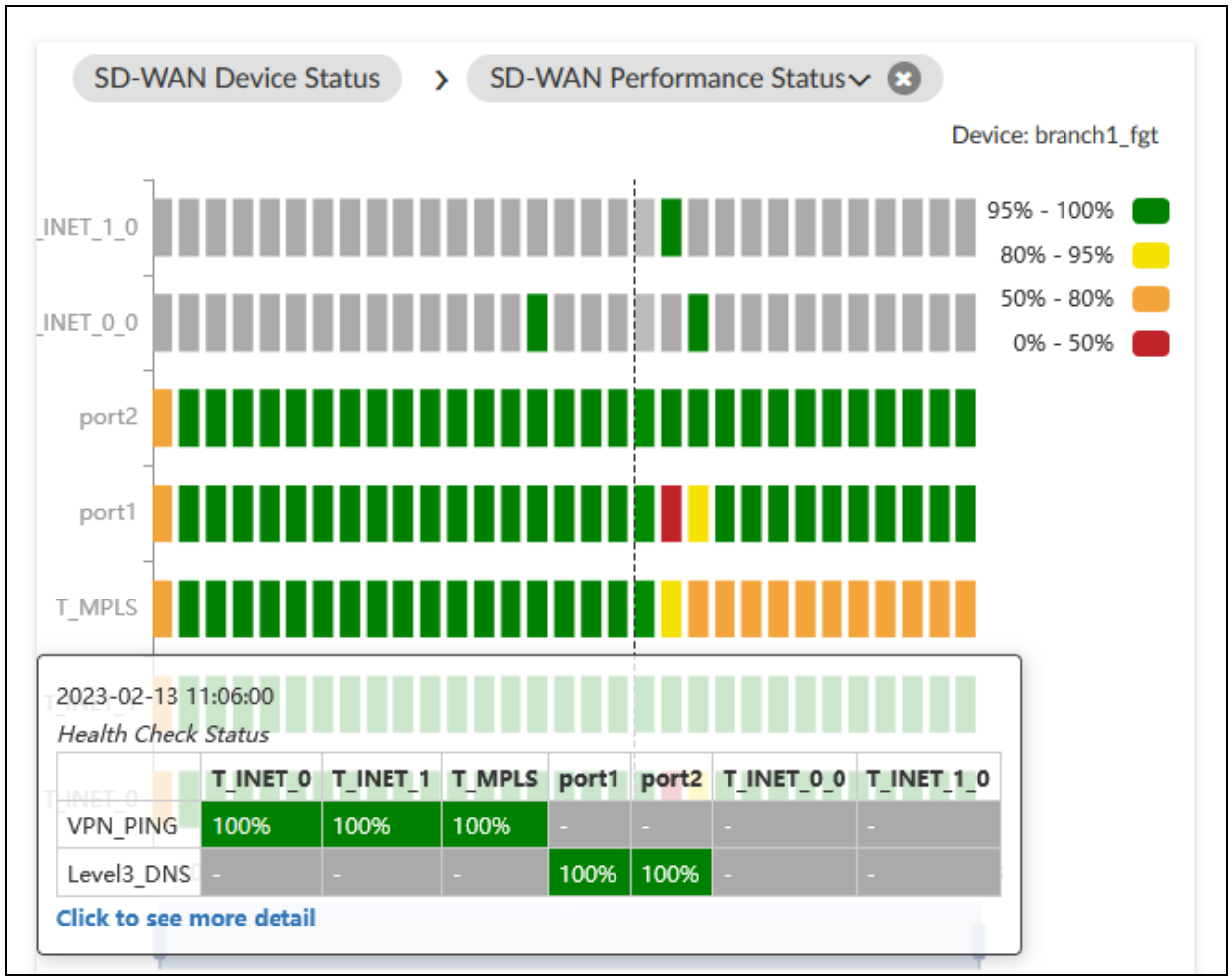
1. Continuing on the FortiManager GUI, click **FortiView** > **SD-WAN Summary**.
   Your page should look similar to the following example:



2. Click the **Healthy Device** link to display the list of devices identified as healthy.
3. Close the window, and then click the **Major Alerts** link to display the list of devices identified with an alert.
   Your page should look similar to the following example:



4. Click the device name (should be **branch1_fgt**) to view the cause of the alert.
   Your page should look similar to the following example:



Note the red or orange bars that correspond to the downtime for the port1 and **T_INET_0** interfaces. The **SD-WAN Health Overview** widget reports it as an alert.

5. Hover over the graphs to see health check details.
6. Close the window to return to the main **SD-WAN Summary** page.
7. In the top bar, open the time period selection menu, and then select **Last 5 Minutes**.
8. Review the widgets output.

Stop and think!

The **SD-WAN Health Overview** widget now shows both devices as healthy. Why?

9. On **branch1_client** and **branch2_client**, press `Ctrl+C` to stop the traffic generator.
10. On the second SSH session for **branch1_client**, stop the ping.
11. Continuing on the WAN simulator page, set the latency of **BR1-MPLS** back to 0 ms.

FORTINET