FortiGate Infrastructure 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

FORTINET®

8/30/2022

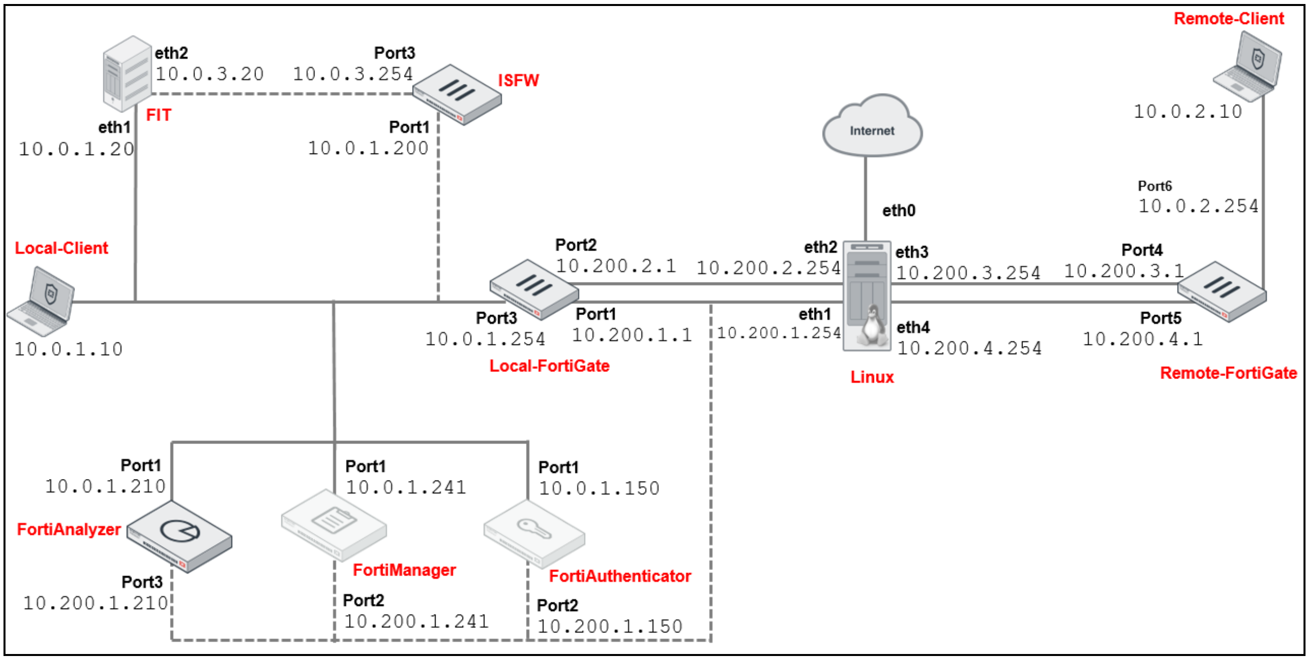
TABLE OF CONTENTS

Change Log

This table includes updates to the *FortiGate Infrastructure 7.2 Lab Guide* dated 6/13/2022 to the updated document version dated 8/30/2022.

Change	Location
Various formatting fixes	Entire guide
Updated URLs to test http	Lab 1, Exercise 1 and 2

Network Topology



Lab 1: Routing

In this lab, you will configure the router settings and test scenarios to learn how FortiGate makes routing decisions.

Objectives

- Route traffic based on the destination IP address, as well as other criteria
- Balance traffic among multiple paths
- Implement route failover
- Implement policy routing
- Diagnose a routing problem

Time to Complete

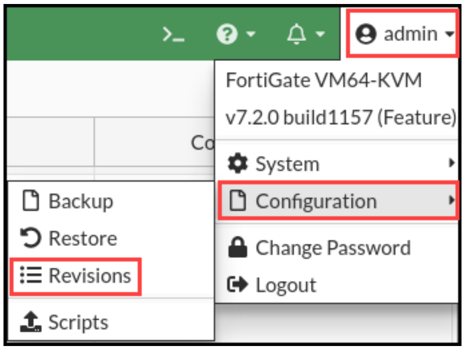
Estimated: 50 minutes

Prerequisites

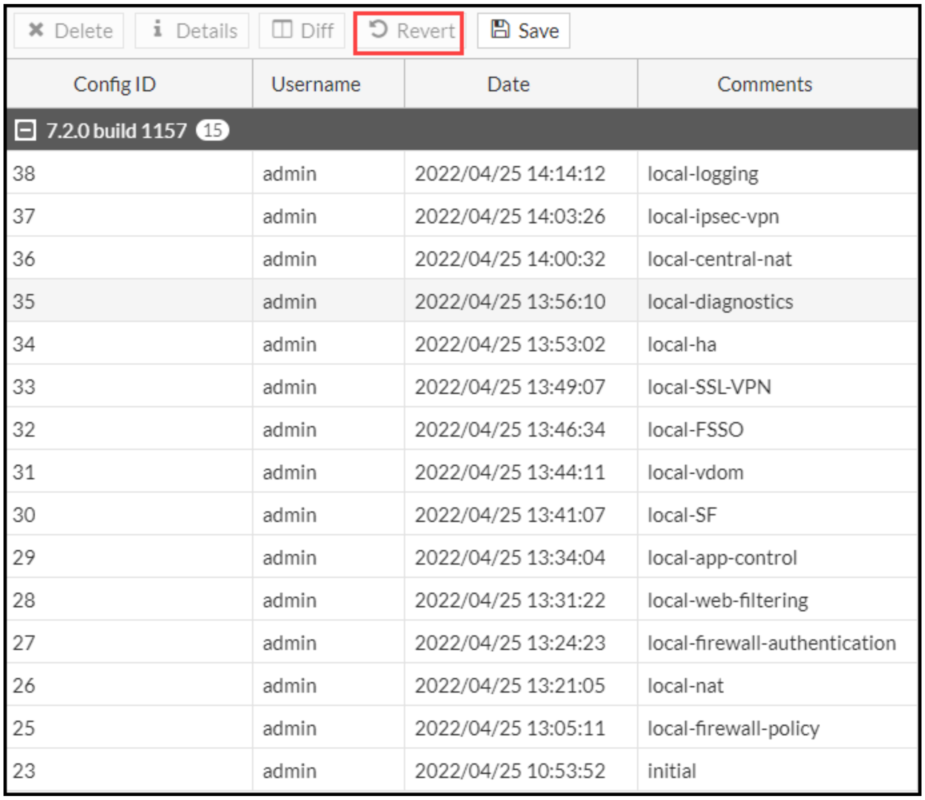
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

VM Usernames and Passwords

VM	Username	Password
Local-Client	Administrator	password
Remote-Client	Administrator	password
Local-FortiGate	admin	password
Remote-FortiGate	admin	password
ISFW	admin	password
FortiAnalyzer	admin	password

Exercise 1: Configuring Route Failover

In the lab network, Local-FortiGate has two interfaces connected to the internet: port1 and port2. In this exercise, you will configure the port1 connection as the primary internet link and the port2 connection as the backup internet link. Local-FortiGate should use the port2 connection only if the port1 connection is down. To achieve this objective, you will configure two default routes with different administrative distances, as well as two link health monitors.

Verify the Routing Configuration

You will verify the existing routing configuration on Local-FortiGate.

Take the Expert Challenge!

On the Local-FortiGate GUI (`admin`/`password`), complete the following:

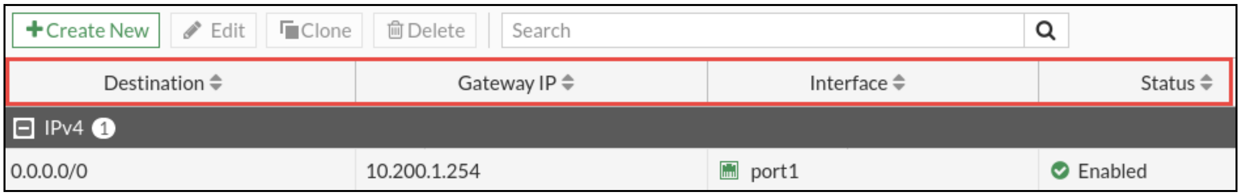
- View the existing static route configuration on Local-FortiGate.
- Enable the **Distance** and **Priority** columns on the static route configuration page.
- Make a note of the **Distance** and **Priority** values of the existing default route.

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

After you complete the challenge, see Configure a Second Default Route on page 12.

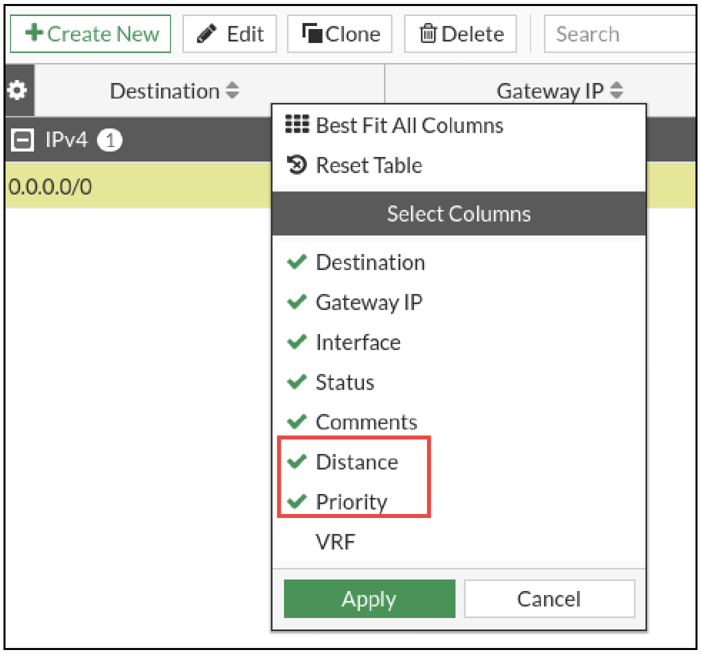
To verify the routing configuration

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Network** > **Static Routes**.
3. Verify the existing default route for **port1**.

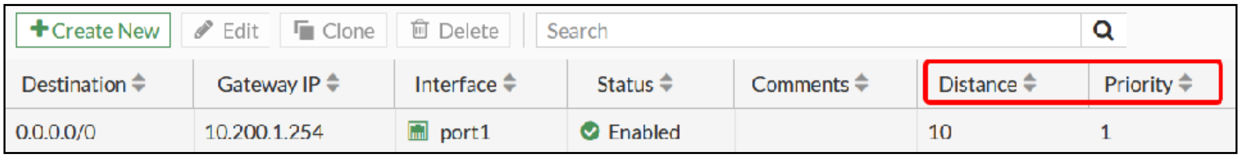


Destination	Gateway IP	Interface	Status
IPv4 1			
0.0.0.0/0	10.200.1.254	port1	✓ Enabled

4. Right-click any of the columns to open the context-sensitive menu.
5. In the **Select Columns** section, select **Distance** and **Priority**, and then click **Apply**.



The **Distance** and **Priority** columns appear in the GUI.



Destination	Gateway IP	Interface	Status	Comments	Distance	Priority
0.0.0.0/0	10.200.1.254	port1	Enabled		10	1

Note that, by default, static routes have a **Distance** value of 10 and a **Priority** value of 1.

Configure a Second Default Route

You will create a second default route using the port2 interface. To make sure this second default route remains the standby route, you will assign it a higher distance.

Take the Expert Challenge!

- On the Local-FortiGate GUI, configure a second default route using **port2**.
- Assign it a **Distance** of `20` and a **Priority** of `5`.

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

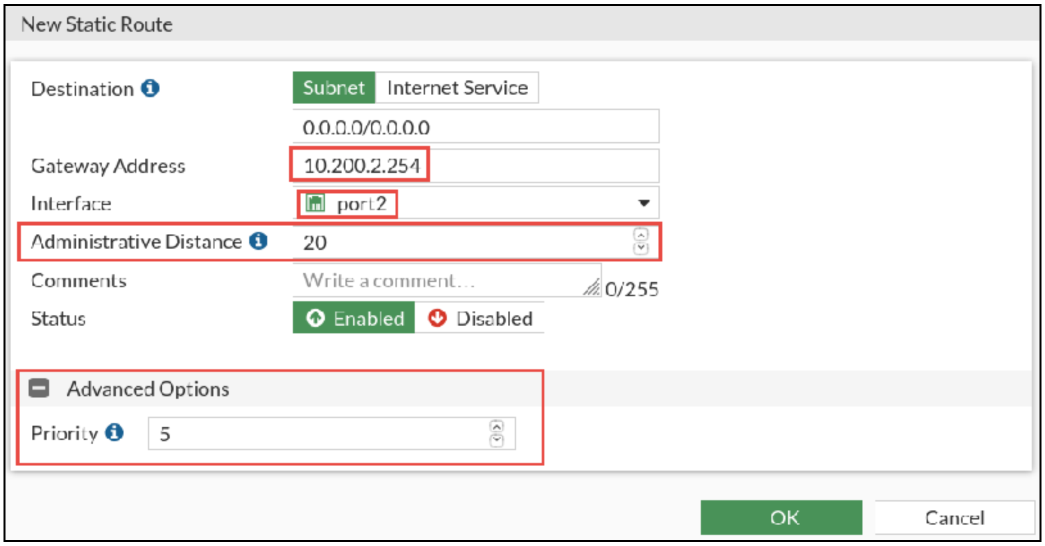
After you complete the challenge, see Configure the Firewall Policies on page 13.

To configure a second default route

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Gateway Address	10.200.2.254
Interface	port2
Administrative Distance	20

4. Click the **+** sign to expand the **Advanced Options** section.
5. In the **Priority** field, type `5`.



New Static Route

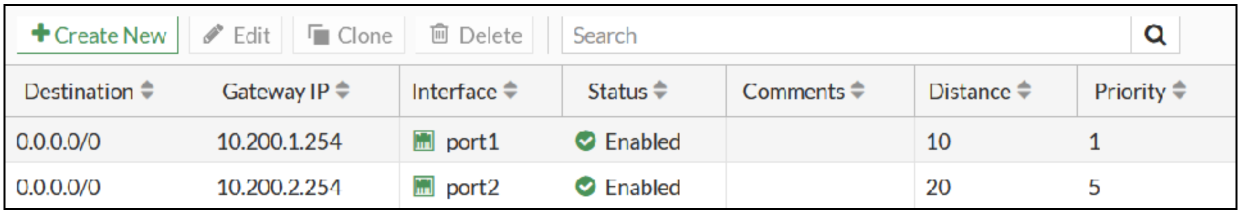
Destination	Subnet / Internet Service 0.0.0.0/0.0.0.0
Gateway Address	10.200.2.254
Interface	port2
Administrative Distance	20
Comments	Write a comment... 0/255
Status	Enabled / Disabled

Advanced Options

Priority	5

6. Click **OK**.

   A second default route is added.



Destination	Gateway IP	Interface	Status	Comments	Distance	Priority
0.0.0.0/0	10.200.1.254	port1	Enabled		10	1
0.0.0.0/0	10.200.2.254	port2	Enabled		20	5

Configure the Firewall Policies

You will modify the existing **Full_Access** firewall policy to log all sessions. You will also create a second firewall policy to allow traffic through the secondary interface.

Take the Expert Challenge!

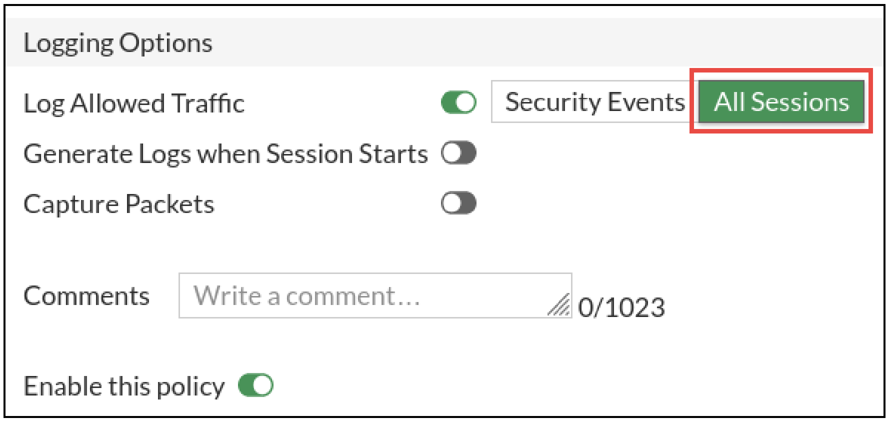
- Continuing on the Local-FortiGate GUI, enable logging for all sessions in the existing **Full_Access** firewall policy.
- Create a second firewall policy named `Backup_Access`.
- Configure the **Backup_Access** policy to allow traffic from **port3** to **port2** with NAT enabled.
- Enable logging on the **Backup_Access** policy for all sessions.

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

After you complete the challenge, see View the Routing Table on page 15

To configure the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the existing **Full_Access** policy to edit it.
3. Enable logging for **All Sessions**.



Logging Options

Log Allowed Traffic: enabled — Security Events | **All Sessions** (selected)

Generate Logs when Session Starts: disabled

Capture Packets: disabled

Comments: Write a comment... 0/1023

Enable this policy: enabled

All Sessions logging ensures that all traffic is logged and not only sessions inspected by security profiles. This will assist you in verifying traffic routing using the **Forward Traffic** logs.

4. Click **OK**.
5. Click **Create New**.
6. Configure a second firewall policy with the following settings:

Field	Value
Name	Backup_Access

Field	Value
Incoming Interface	port3
Outgoing Interface	port2
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	Accept
NAT	Enabled
Log Allowed Traffic	All Sessions

7. Click **OK**.

View the Routing Table

The Local-FortiGate configuration now has two default routes with different distances. You will view the routing table to see which route was installed in the routing table and which route was installed in the routing table database.

To view the routing table

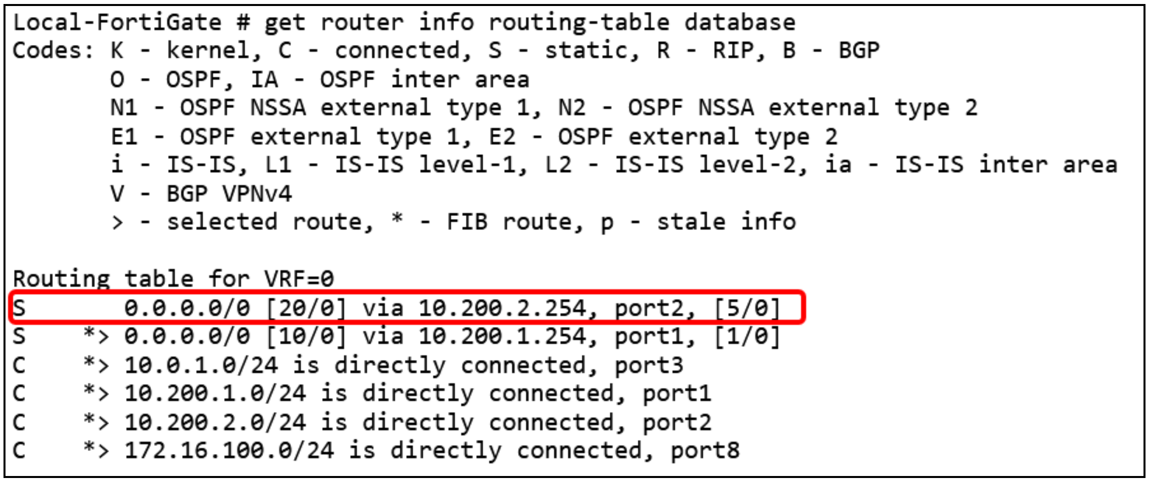
1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to list the routing table entries:

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

   Note that the second default route is not listed.
3. Enter the following command to list the routing table database entries:

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

4. Confirm that the second default route is listed as inactive.



```
Local-FortiGate # get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```

Stop and think!

Why is the port2 default route the standby route?

The port2 default route has a higher administrative distance than the port1 default route. When two or more routes to the same destination have different distances, the higher distance route is not installed in the routing table, but you can still see it in the routing table database.

5. Leave the Local-FortiGate CLI session open.

Configure Link Health Monitors

You will configure two link health monitors to monitor the status of both the port1 and port2 routes.

To configure link health monitoring

1. Continuing on the Local-FortiGate CLI session, enter the following commands to create a link health monitor for port1 on Local-FortiGate:

```
config system link-monitor
   edit port1-monitor
      set srcintf port1
      set server 4.2.2.1
      set gateway-ip 10.200.1.254
      set protocol ping
      set update-static-route enable
   next
end
```

2. Enter the following commands to configure another link health monitor for port2:

```
config system link-monitor
   edit port2-monitor
      set srcintf port2
      set server 4.2.2.2
      set gateway-ip 10.200.2.254
      set protocol ping
      set update-static-route enable
```

```
        next
    end
```

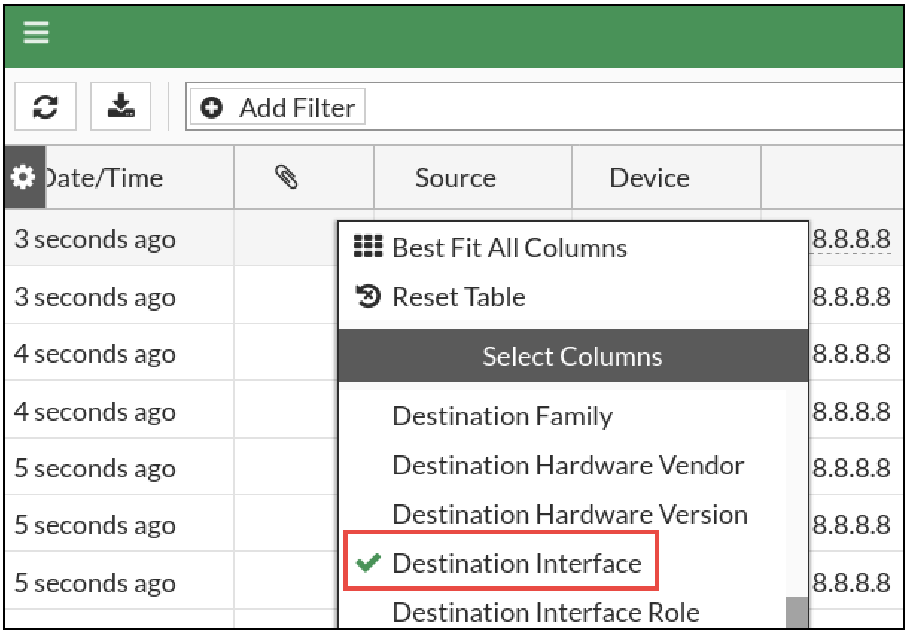
3. Leave your Local-FortiGate CLI session open.

Test the Route Failover

First, you will access various websites and use the **Forward Traffic** logs to verify that the port1 route is being used. Next, you will force a failover by reconfiguring the port1 link health monitor to ping an invalid IP address. You will then generate some more traffic, and use the **Forward Traffic** logs to verify that the port2 route is being used.

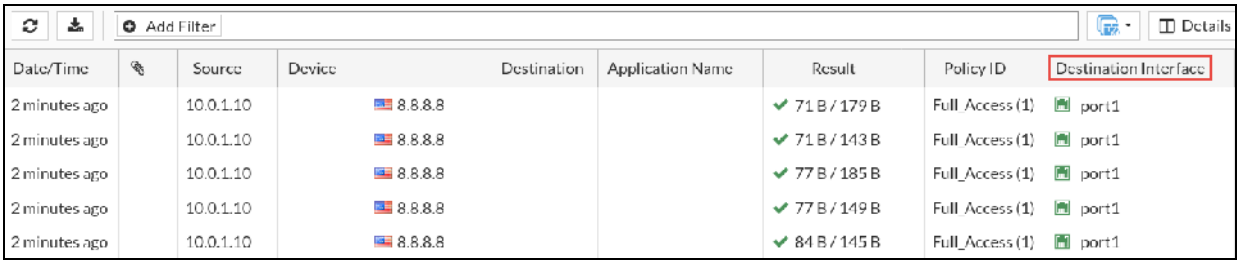
To confirm the port1 route is the primary route

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Right-click any of the columns to open the context-sensitive menu.
3. In the **Select Columns** section, select **Destination Interface**.



Date/Time		Source	Device	
3 seconds ago				8.8.8.8
3 seconds ago				8.8.8.8
4 seconds ago				8.8.8.8
4 seconds ago				8.8.8.8
5 seconds ago				8.8.8.8
5 seconds ago				8.8.8.8
5 seconds ago				8.8.8.8

4. Scroll down in the context-sensitive menu, and then click **Apply**.
   The **Destination Interface** column is displayed.

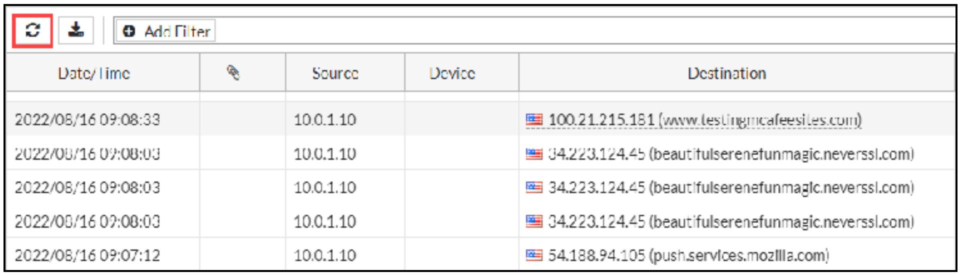


Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2 minutes ago		10.0.1.10		8.8.8.8		✓ 71 B / 179 B	Full_Access (1)	port1
2 minutes ago		10.0.1.10		8.8.8.8		✓ 71 B / 143 B	Full_Access (1)	port1
2 minutes ago		10.0.1.10		8.8.8.8		✓ 77 B / 185 B	Full_Access (1)	port1
2 minutes ago		10.0.1.10		8.8.8.8		✓ 77 B / 149 B	Full_Access (1)	port1
2 minutes ago		10.0.1.10		8.8.8.8		✓ 84 B / 145 B	Full_Access (1)	port1

5. On the Local-Client VM, open a few new tabs in the browser, and visit a few websites, such as:

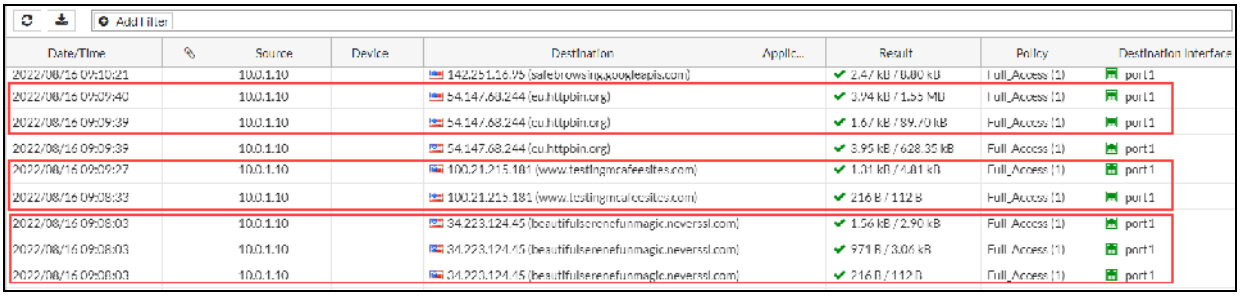
- http://neverssl.com
- http://www.testingmcafeesites.com
- http://eu.httpbin.org

6. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
7. Click the refresh icon.



Date/Time	📎	Source	Device	Destination
2022/08/16 09:08:33		10.0.1.10		100.21.215.181 (www.testingmcafeesites.com)
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)
2022/08/16 09:07:12		10.0.1.10		54.188.94.105 (push.services.mozilla.com)

8. Locate the relevant log entries for the three websites you accessed, and verify that their **Destination Interface** indicates **port1**.



Date/Time	📎	Source	Device	Destination	Applic...	Result	Policy	Destination Interface
2022/08/16 09:10:21		10.0.1.10		142.251.16.95 (safebrowsing.googleapis.com)		✓ 2.47 kB / 8.80 kB	Full_Access (1)	port1
2022/08/16 09:09:40		10.0.1.10		54.147.68.244 (eu.httpbin.org)		✓ 3.94 kB / 1.55 MB	Full_Access (1)	port1
2022/08/16 09:09:39		10.0.1.10		54.147.68.244 (eu.httpbin.org)		✓ 1.67 kB / 89.70 kB	Full_Access (1)	port1
2022/08/16 09:09:39		10.0.1.10		54.147.68.244 (eu.httpbin.org)		✓ 3.95 kB / 628.35 kB	Full_Access (1)	port1
2022/08/16 09:09:27		10.0.1.10		100.21.215.181 (www.testingmcafeesites.com)		✓ 1.31 kB / 4.81 kB	Full_Access (1)	port1
2022/08/16 09:08:33		10.0.1.10		100.21.215.181 (www.testingmcafeesites.com)		✓ 216 B / 112 B	Full_Access (1)	port1
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)		✓ 1.56 kB / 2.90 kB	Full_Access (1)	port1
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)		✓ 971 B / 3.06 kB	Full_Access (1)	port1
2022/08/16 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)		✓ 216 B / 112 B	Full_Access (1)	port1

This verifies that the **port1** route is currently the route in use.

To force the failover

1. Return to the Local-FortiGate CLI session, and then enter the following commands to modify the port1 link monitor:

```
config system link-monitor
   edit port1-monitor
      set server 10.200.1.13
   next
end
```

2. Wait a few seconds.

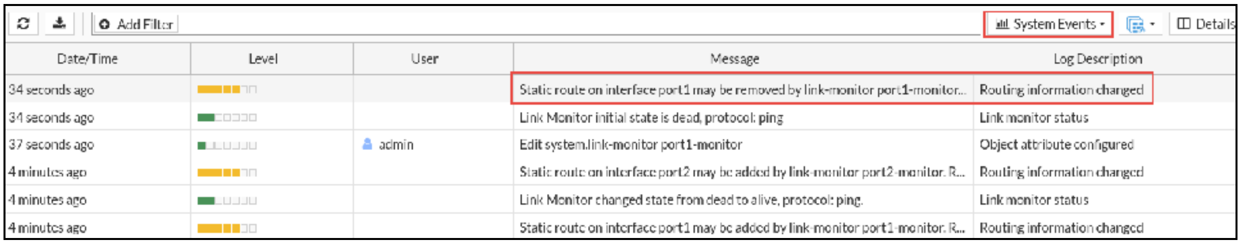
   Because `10.200.1.13` is a non-existent host in the lab network, the link health monitor does not receive any replies. Because of this, the link health monitor assumes that the port1 internet connection is down, and removes the corresponding route from the routing table.

3. Leave your Local-FortiGate CLI session open.

To verify the route change

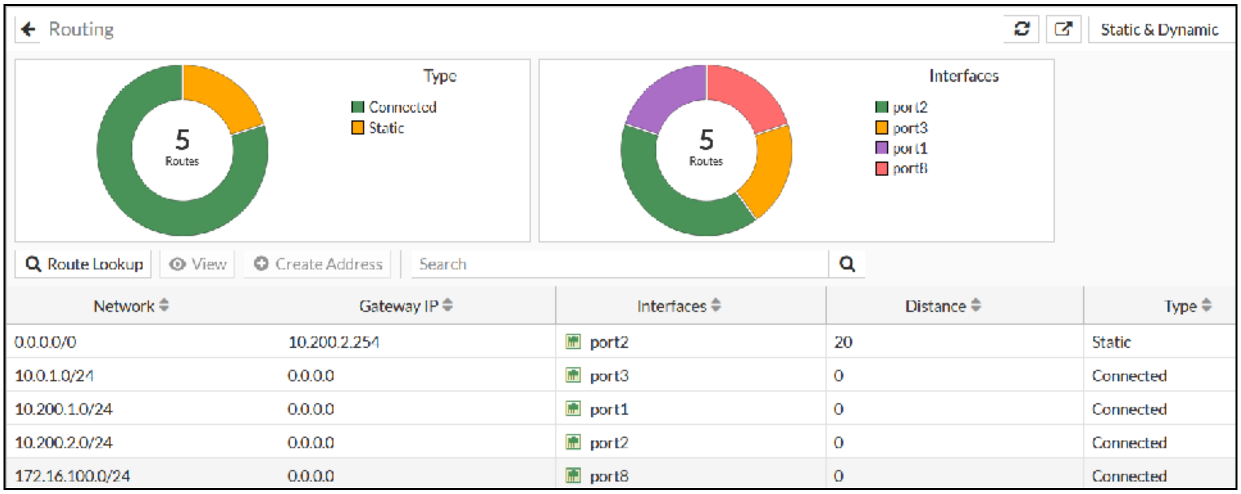
1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **System Events** > **General System Events**.

   Verify that the Local-FortiGate detected the link failure and removed the corresponding **port1** route.



Date/Time	Level	User	Message	Log Description
34 seconds ago			Static route on interface port1 may be removed by link-monitor port1-monitor...	Routing information changed
34 seconds ago			Link Monitor initial state is dead, protocol: ping	Link monitor status
37 seconds ago		admin	Edit system.link-monitor port1-monitor	Object attribute configured
4 minutes ago			Static route on interface port2 may be added by link-monitor port2-monitor. R...	Routing information changed
4 minutes ago			Link Monitor changed state from dead to alive, protocol: ping.	Link monitor status
4 minutes ago			Static route on interface port1 may be added by link-monitor port1-monitor. R...	Routing information changed

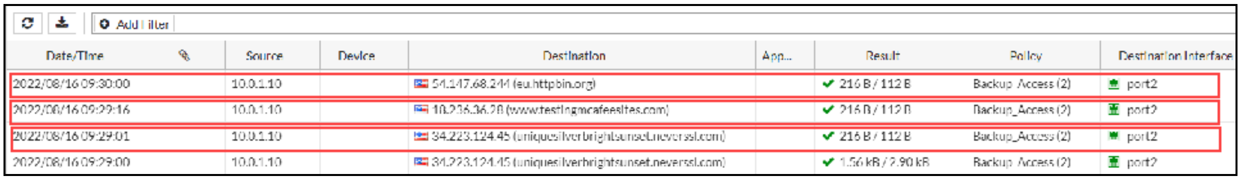
2. Click **Dashboard** > **Network**, and then click **Routing** to expand it to full screen.
3. Verify that the **port2** route replaced the **port1** route in the routing table.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.2.254	port2	20	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

To verify traffic logs

1. On the Local-Client VM, open a few new tabs in the browser, and visit a few websites, such as:
   - http://neverssl.com
   - http://www.testingmcafeesites.com
   - http://eu.httpbin.org
2. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Log & Report** > **Forward Traffic.**
3. Locate the relevant log entries for the three websites you accessed, and verify that their **Destination Interface** indicates **port2**.



Date/Time	Source	Device	Destination	App...	Result	Policy	Destination Interface
2022/08/16 09:30:00	10.0.1.10		54.147.68.244 (eu.httpbin.org)		✓ 216 B / 112 B	Backup_Access (2)	port2
2022/08/16 09:29:16	10.0.1.10		10.236.36.28 (www.testingmcafeesites.com)		✓ 216 B / 112 B	Backup_Access (2)	port2
2022/08/16 09:29:01	10.0.1.10		34.223.124.45 (uniquesilverbrightsunset.neverssl.com)		✓ 216 B / 112 B	Backup_Access (2)	port2
2022/08/16 09:29:00	10.0.1.10		34.223.124.45 (uniquesilverbrightsunset.neverssl.com)		✓ 1.56 kB / 2.90 kB	Backup_Access (2)	port2

This verifies that the Local-FortiGate is using the port2 default route.

Restore the Routing Table

Before starting the next exercise, you will restore the port1 link health monitor server configuration with a valid host address, which will restore the port1 default route as the best route in the routing table.

To restore the port1 health monitor configuration

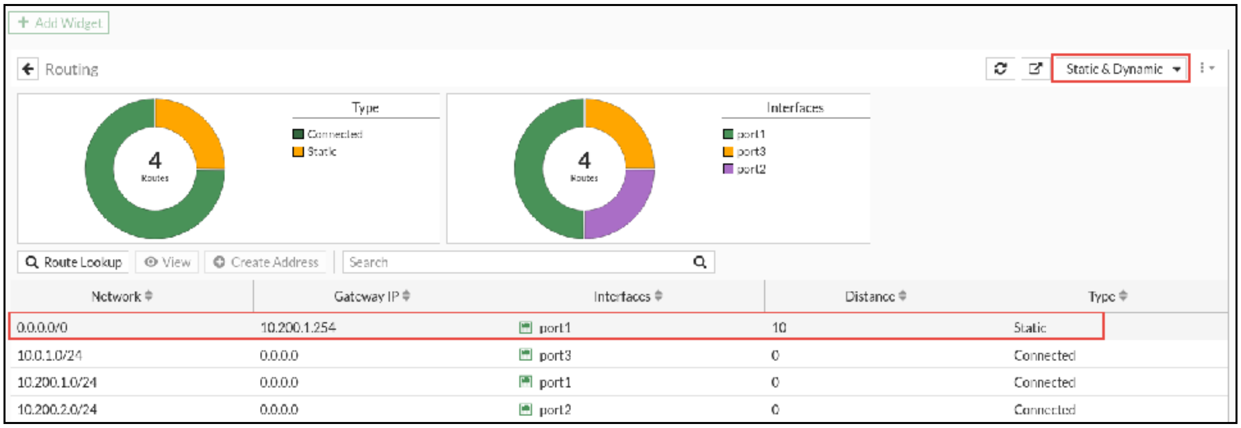
1. Return to the Local-FortiGate CLI session, and then enter the following commands:

```
config system link-monitor
   edit port1-monitor
      set server 4.2.2.1
   next
end
```

2. Close the Local-FortiGate CLI session.

To verify the routing table

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Routing** to expand it to full screen.
2. Verify that the **port1** route replaced the **port2** route in the routing table.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected

3. Close the browser.

Exercise 2: Configuring Equal Cost Multipath and Policy Routing

In this exercise, you will configure equal cost multi-path (ECMP) routing on Local-FortiGate to load balance the internet traffic between port1 and port2. After that, you will configure a policy route to route HTTPS traffic through port1 only.

Configure Administrative Distance

To establish ECMP, first you will configure multiple static routes with the same administrative distance.

Take the Expert Challenge!

On the Local-FortiGate GUI (`admin`/`password`), complete the following:

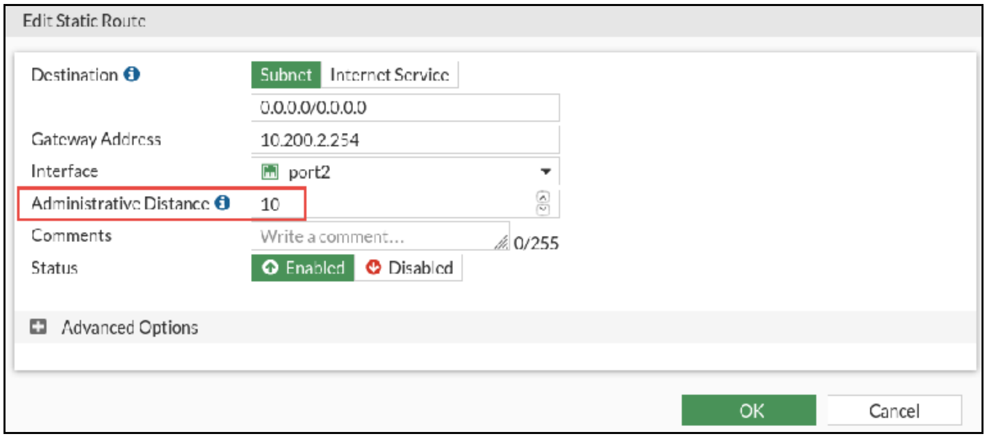
- Change the **port2** static route **Administrative Distance** to `10`.
- Verify that both **port1** and **port2** default routes are present in the routing table.

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

After you complete the challenge, see Change the ECMP Load Balancing Algorithm on page 22.

To configure administrative distance

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Network** > **Static Routes**.
3. Double-click the **port2** static route to edit it.
4. Change the **Administrative Distance** to `10`.



Edit Static Route

Destination: Subnet | Internet Service

0.0.0.0/0.0.0.0

Gateway Address: 10.200.2.254

Interface: port2

Administrative Distance: 10

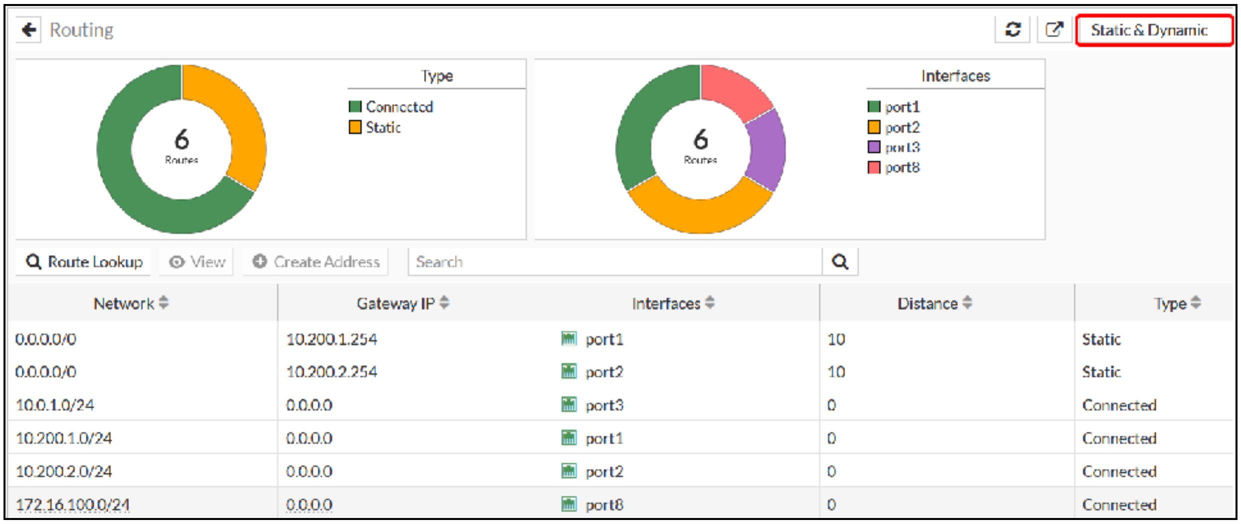
Comments: Write a comment... 0/255

Status: Enabled | Disabled

5. Click **OK**.

To verify the routing table

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Routing** to expand it to full screen.
2. Verify that both default routes are installed in the routing table.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
0.0.0.0/0	10.200.2.254	port2	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

Change the ECMP Load Balancing Algorithm

By default, the ECMP load balancing algorithm is based on source IP address. This works well when there are multiple clients generating traffic. In the lab network, because you have only one client (Local-Client), the source IP address method will not balance any traffic to the second route. Only one route will always be used. For this reason, you will change the load balancing method to use both source and destination IP addresses. Using this method, as long as the traffic goes to multiple destination IP addresses, FortiGate load balances the traffic across both routes.

To modify the ECMP load balancing method

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to change the ECMP load-balancing method:

```
config system settings
   set v4-ecmp-mode source-dest-ip-based
end
```

3. Leave the Local-FortiGate CLI session open.

Verify Traffic Routing

You will generate some HTTP traffic and verify traffic routing using the **Forward Traffic** logs.

Take the Expert Challenge!

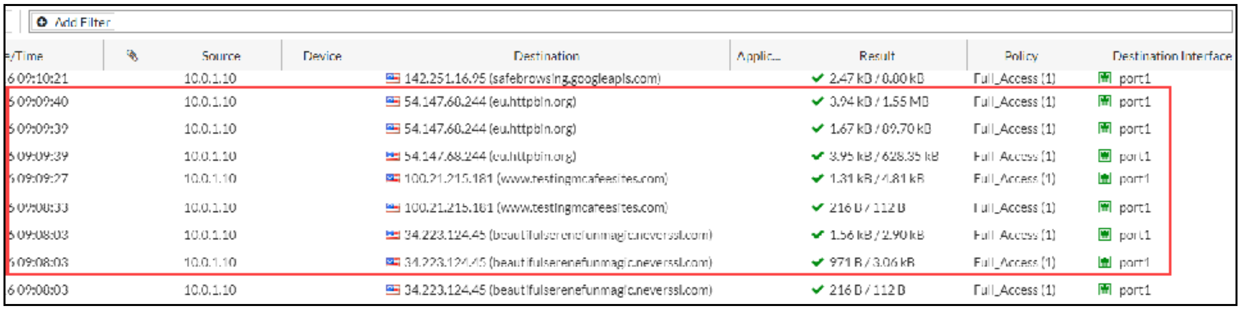
- On the Local-Client VM, open a few new browser tabs, and then generate some HTTP traffic.
- Verify the traffic routing on Local-FortiGate, using the **Forward Traffic** logs.
- Identify why all the outgoing packets are still being routed through **port1**.

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

After you complete the challenge, see Configure Priority on page 24.

To verify traffic routing

1. On the Local-Client VM, open new tabs in the browser, and visit a few websites, such as:
   - http://neverssl.com
   - http://www.testingmcafeesites.com
   - http://eu.httpbin.org
2. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
3. Identify the **Destination Interface** in the relevant log entries for the websites you accessed.



Add Filter

/Time		Source	Device	Destination	Applic...	Result	Policy	Destination Interface
6 09:10:21		10.0.1.10		142.251.16.95 (safebrowsing.googleapis.com)		✓ 2.47 kB / 0.00 kB	Full_Access (1)	port1
6 09:09:40		10.0.1.10		54.147.60.244 (eu.httpbin.org)		✓ 3.94 kB / 1.55 MB	Full_Access (1)	port1
6 09:09:39		10.0.1.10		54.147.60.244 (eu.httpbin.org)		✓ 1.67 kB / 89.70 kB	Full_Access (1)	port1
6 09:09:39		10.0.1.10		54.147.68.244 (eu.httpbin.org)		✓ 3.95 kB / 628.35 kB	Full_Access (1)	port1
6 09:09:27		10.0.1.10		100.21.215.181 (www.testingmcafeesites.com)		✓ 1.31 kB / 4.81 kB	Full_Access (1)	port1
6 09:08:33		10.0.1.10		100.21.215.181 (www.testingmcafeesites.com)		✓ 216 B / 112 B	Full_Access (1)	port1
6 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)		✓ 1.56 kB / 2.90 kB	Full_Access (1)	port1
6 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)		✓ 971 B / 3.06 kB	Full_Access (1)	port1
6 09:08:03		10.0.1.10		34.223.124.45 (beautifulserenefunmagic.neverssl.com)		✓ 216 B / 112 B	Full_Access (1)	port1

Why are all the outgoing packets still being routed through port1?

Stop and think!

The **port2** route is not being used to route internet traffic. Why?

At the beginning of this exercise, you set a distance of 10 on the port2 route but you didn't change its priority. The port2 route priority is still 5 and you configured it in the previous exercise (see Configure a Second Default Route on page 12). In addition, the port1 route has distance and priority values of 10 and 1, respectively.

When two routes to the same destination have the same distance, both remain in the routing table. However, if the priorities are different, the route with the lowest priority value—port1 in this case—is used. To achieve ECMP with static routes, the distance and priority values must be the same for all routes.

Configure Priority

You will change the priority value for the **port2** route to match the **port1** route.

Take the Expert Challenge!

On the Local-FortiGate GUI, modify the static routing configuration so both default routes are eligible for ECMP.

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

After you complete the challenge, see Verify ECMP on page 24

To configure priority

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Double-click the **port2** default route to edit it.
3. Click the **+** sign to expand the **Advanced Options** section.
4. Change the **Priority** value to `1`.
5. Click **OK**.

Verify ECMP

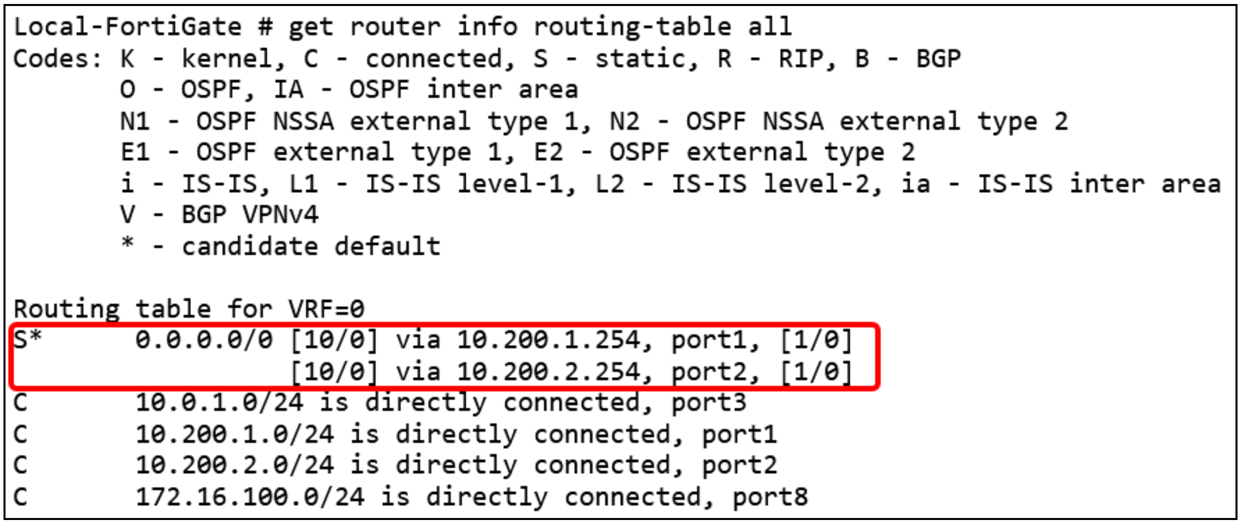
Now that both port1 and port2 routes share the same distance and priority values, they are eligible for ECMP. First, you will verify the routing table, and then you will verify traffic routing using the **Forward Traffic** logs.

To verify the routing table

1. Return to the Local-FortiGate CLI session, and then enter the following command on Local-FortiGate:

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

2. Verify that both default routes are currently active.



```
Local-FortiGate # 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 10.200.1.254, port1, [1/0]
                  [10/0] via 10.200.2.254, port2, [1/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.100.0/24 is directly connected, port8
```

To configure the CLI sniffer

1. Continuing on the Local-FortiGate CLI session, enter the following command:

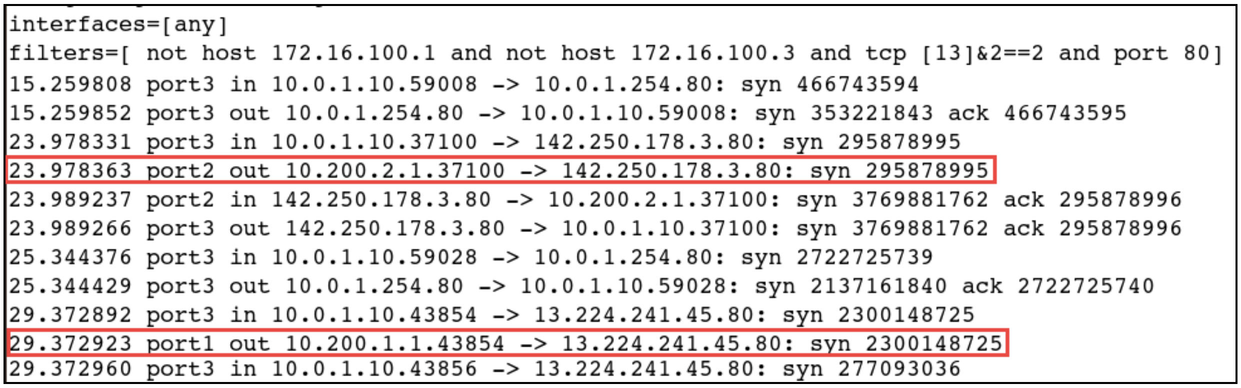
```
diagnose sniffer packet any 'not host 172.16.100.1 and not host 172.16.100.3 and tcp
    [13]&2==2 and port 80' 4
```

The filter `'tcp[13]&2==2'` matches packets with the SYN flag on, so the output will show all SYN packets for port 80 (HTTP).

2. Leave the Local-FortiGate CLI window open in the background.

To verify ECMP routing

1. On the Local-Client VM, open new tabs in the browser, and visit a few websites, such as:
   - http://neverssl.com
   - http://www.testingmcafeesites.com
   - http://eu.httpbin.org
2. Return to the Local-FortiGate CLI session, and then press `Ctrl+C` to stop the sniffer.
3. Analyze the sniffer output.



```
interfaces=[any]
filters=[ not host 172.16.100.1 and not host 172.16.100.3 and tcp [13]&2==2 and port 80]
15.259808 port3 in 10.0.1.10.59008 -> 10.0.1.254.80: syn 466743594
15.259852 port3 out 10.0.1.254.80 -> 10.0.1.10.59008: syn 353221843 ack 466743595
23.978331 port3 in 10.0.1.10.37100 -> 142.250.178.3.80: syn 295878995
23.978363 port2 out 10.200.2.1.37100 -> 142.250.178.3.80: syn 295878995
23.989237 port2 in 142.250.178.3.80 -> 10.200.2.1.37100: syn 3769881762 ack 295878996
23.989266 port3 out 142.250.178.3.80 -> 10.0.1.10.37100: syn 3769881762 ack 295878996
25.344376 port3 in 10.0.1.10.59028 -> 10.0.1.254.80: syn 2722725739
25.344429 port3 out 10.0.1.254.80 -> 10.0.1.10.59028: syn 2137161840 ack 2722725740
29.372892 port3 in 10.0.1.10.43854 -> 13.224.241.45.80: syn 2300148725
29.372923 port1 out 10.200.1.1.43854 -> 13.224.241.45.80: syn 2300148725
29.372960 port3 in 10.0.1.10.43856 -> 13.224.241.45.80: syn 277093036
```

The SYN packets are egressing both `port1` and `port2`. This verifies that Local-FortiGate is now load balancing all internet traffic across both routes.

4. Leave the Local-FortiGate CLI session open.

Configure a Policy Route for HTTPS Traffic

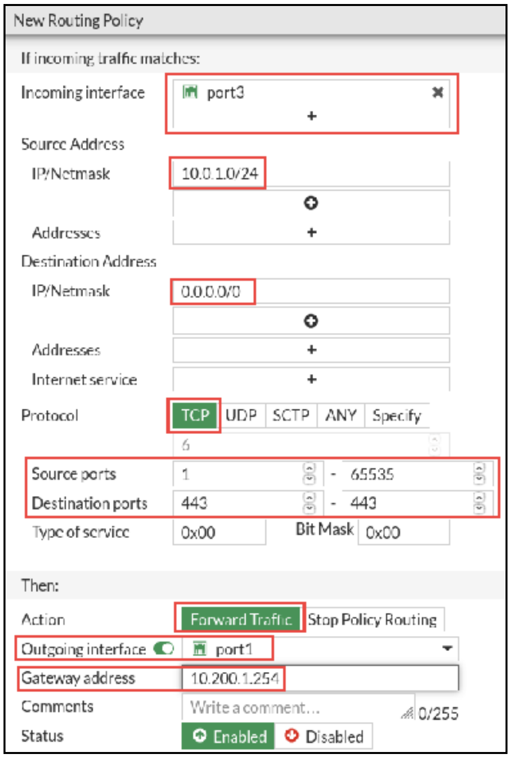
You will force all HTTPS traffic to egress through port1 using a policy route. All other traffic should remain unaffected and balanced between port1 and port2. To implement this, you will configure a policy route.

To configure a policy route for HTTPS traffic

1. Continuing on the Local-FortiGate GUI, click **Network** > **Policy Routes**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Incoming interface	port3
Source Address > IP/Netmask	10.0.1.0/24
Destination Address > IP/Netmask	0.0.0.0/0
Protocol	TCP
Source ports	From 1 to 65535
Destination ports	From 443 to 443
Action	Forward Traffic
Outgoing interface	Enabled and port1
Gateway address	10.200.1.254

The policy route should look like the following example:



New Routing Policy

If incoming traffic matches:

Incoming interface: port3

Source Address
IP/Netmask: 10.0.1.0/24
Addresses:

Destination Address
IP/Netmask: 0.0.0.0/0
Addresses:
Internet service:

Protocol: [✓ TCP] UDP SCTP ANY Specify
6

Source ports: 1 - 65535
Destination ports: 443 - 443
Type of service: 0x00 Bit Mask: 0x00

Then:

Action: [✓ Forward Traffic] Stop Policy Routing
Outgoing interface: port1
Gateway address: 10.200.1.254
Comments: Write a comment... 0/255
Status: [✓ Enabled] Disabled

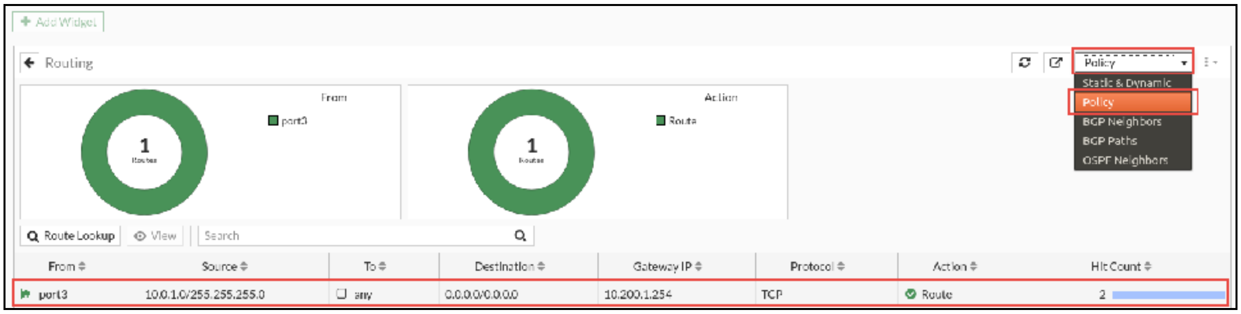
4. Click **OK**.

Verify the Policy Route

First, you will verify the routing table, and then you will verify policy routing by generating HTTPS traffic and viewing the CLI sniffer output.

To verify the policy route table

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Routing** to expand it to fullscreen.
2. In the upper-right corner, click **Static & Dynamic**, and then select **Policy** in the drop-down list.



From	Source	To	Destination	Gateway IP	Protocol	Action	Hit Count
port3	10.0.1.0/255.255.255.0	any	0.0.0.0/0.0.0.0	10.200.1.254	TCP	✓ Route	2

To verify policy routing for HTTPS traffic

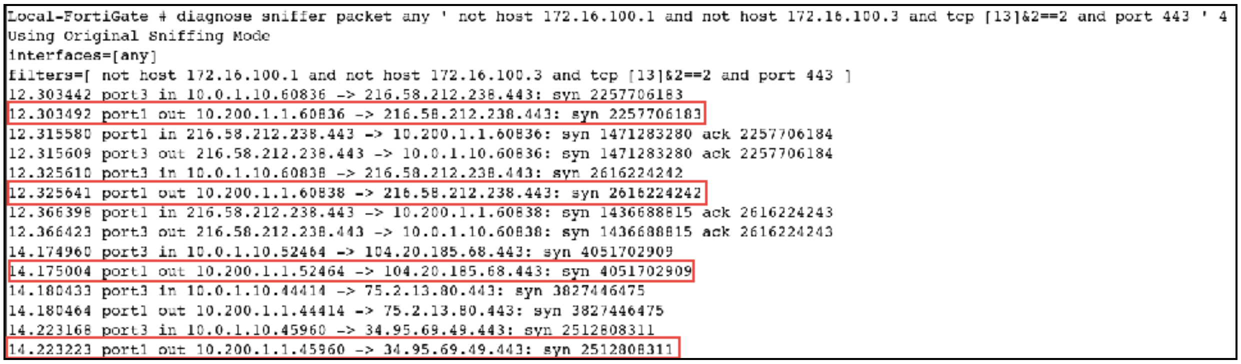
1. Continuing on the Local-FortiGate CLI session, enter the following command on Local-FortiGate:

```
diagnose sniffer packet any 'not host 172.16.100.1 and not host 172.16.100.3 and tcp
    [13]&2==2 and port 443' 4
```

As before, this sniffer filter matches packets with the SYN flag on, but this time for port 443 (HTTPS).

Leave the Local-FortiGate CLI window open in the background.

2. On the Local-Client VM, open new tabs in the browser, and then visit a few HTTPS websites, such as:
   - https://www.fortiguard.com
   - https://support.fortinet.com
3. On the Local-FortiGate CLI session, and then press `Ctrl+C` to stop the sniffer.
4. Analyze the sniffer output.



```
Local-FortiGate # diagnose sniffer packet any ' not host 172.16.100.1 and not host 172.16.100.3 and tcp [13]&2==2 and port 443 ' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[ not host 172.16.100.1 and not host 172.16.100.3 and tcp [13]&2==2 and port 443 ]
12.303442 port3 in 10.0.1.10.60836 -> 216.58.212.238.443: syn 2257706183
12.303492 port1 out 10.200.1.1.60836 -> 216.58.212.238.443: syn 2257706183
12.315580 port1 in 216.58.212.238.443 -> 10.200.1.1.60836: syn 1471283280 ack 2257706184
12.315609 port3 out 216.58.212.238.443 -> 10.0.1.10.60836: syn 1471283280 ack 2257706184
12.325610 port3 in 10.0.1.10.60838 -> 216.58.212.238.443: syn 2616224242
12.325641 port1 out 10.200.1.1.60838 -> 216.58.212.238.443: syn 2616224242
12.366398 port1 in 216.58.212.238.443 -> 10.200.1.1.60838: syn 1436688815 ack 2616224243
12.366423 port3 out 216.58.212.238.443 -> 10.0.1.10.60838: syn 1436688815 ack 2616224243
14.174960 port3 in 10.0.1.10.52464 -> 104.20.185.68.443: syn 4051702909
14.175004 port1 out 10.200.1.1.52464 -> 104.20.185.68.443: syn 4051702909
14.180433 port3 in 10.0.1.10.44414 -> 75.2.13.80.443: syn 3827446475
14.180464 port1 out 10.200.1.1.44414 -> 75.2.13.80.443: syn 3827446475
14.223168 port3 in 10.0.1.10.45960 -> 34.95.69.49.443: syn 2512808311
14.223223 port1 out 10.200.1.1.45960 -> 34.95.69.49.443: syn 2512808311
```

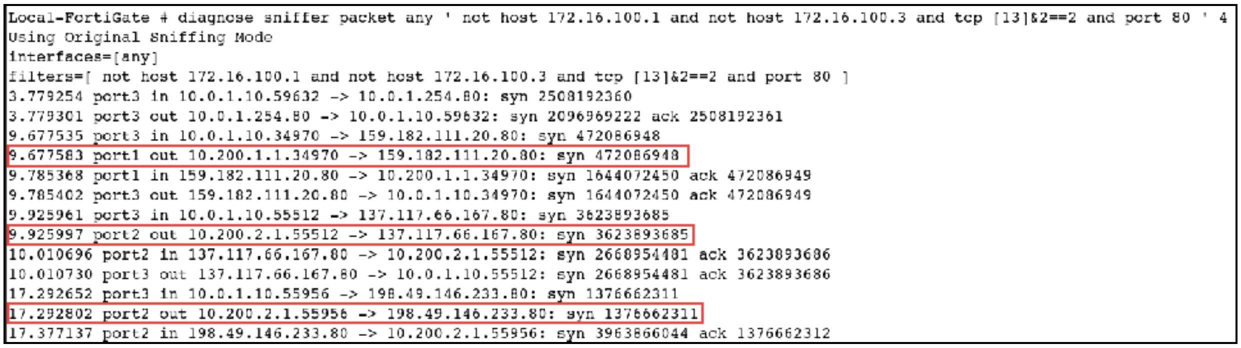
The SYN packets are egressing `port1` only. This verifies that Local-FortiGate is applying the policy route for HTTPS traffic.

To verify non-HTTPS traffic routing

1. Continuing on your Local-FortiGate CLI session, enter the following command:

```
diagnose sniffer packet any 'not host 172.16.100.1 and not host 172.16.100.3 and tcp
    [13]&2==2 and port 80' 4
```

2. On the Local-Client VM, open new tabs in the browser, and then visit a few HTTP websites, such as:
   - http://neverssl.com
   - http://www.testingmcafeesites.com
   - http://eu.httpbin.org
3. On the Local-FortiGate CLI session, press `Ctrl+C` to stop the sniffer.
4. Analyze the sniffer output.



```
Local-FortiGate # diagnose sniffer packet any ' not host 172.16.100.1 and not host 172.16.100.3 and tcp [13]&2==2 and port 80 ' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[ not host 172.16.100.1 and not host 172.16.100.3 and tcp [13]&2==2 and port 80 ]
3.779254 port3 in 10.0.1.10.59632 -> 10.0.1.254.80: syn 2508192360
3.779301 port3 out 10.0.1.254.80 -> 10.0.1.10.59632: syn 2096969222 ack 2508192361
9.677535 port3 in 10.0.1.10.34970 -> 159.182.111.20.80: syn 472086948
9.677583 port1 out 10.200.1.1.34970 -> 159.182.111.20.80: syn 472086948
9.785368 port1 in 159.182.111.20.80 -> 10.200.1.1.34970: syn 1644072450 ack 472086949
9.785402 port3 out 159.182.111.20.80 -> 10.0.1.10.34970: syn 1644072450 ack 472086949
9.925961 port3 in 10.0.1.10.55512 -> 137.117.66.167.80: syn 3623893685
9.925997 port2 out 10.200.2.1.55512 -> 137.117.66.167.80: syn 3623893685
10.010696 port2 in 137.117.66.167.80 -> 10.200.2.1.55512: syn 2668954481 ack 3623893686
10.010730 port3 out 137.117.66.167.80 -> 10.0.1.10.55512: syn 2668954481 ack 3623893686
17.292652 port3 in 10.0.1.10.55956 -> 198.49.146.233.80: syn 1376662311
17.292802 port2 out 10.200.2.1.55956 -> 198.49.146.233.80: syn 1376662311
17.377137 port2 in 198.49.146.233.80 -> 10.200.2.1.55956: syn 3963866044 ack 1376662312
```

HTTP (port 80) traffic remains unaffected by the policy route, and is still load balanced across both `port1` and `port2` routes.

Stop and think!

The Local-FortiGate configuration still has the two link health monitors for port1 and port2. Do they also enable routing failover for ECMP scenarios?

Yes. If Local-FortiGate detects a problem in any of the routes, the link monitor removes the corresponding route, and all internet traffic is routed through the remaining route.

5. Close the Local-FortiGate CLI session and browser.

Lab 2: VDOM Configuration

In this lab, you will examine how to create a virtual domain (VDOM) and configure an inter-VDOM link.

Objectives

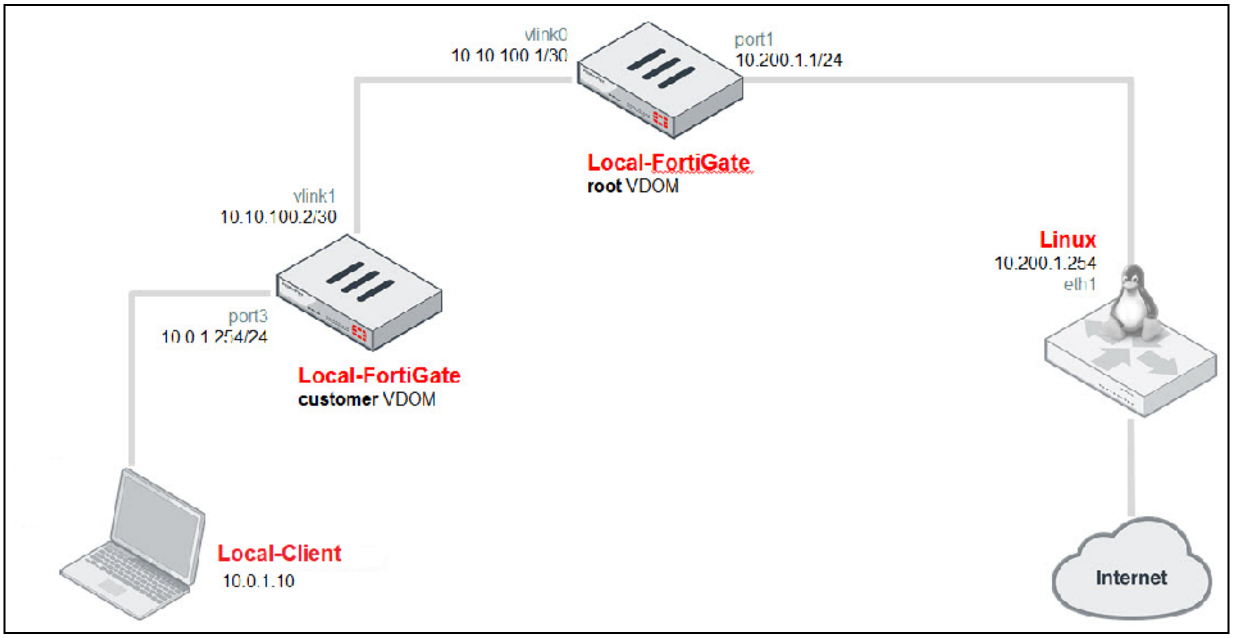
- Use VDOMs to split a FortiGate into multiple virtual devices
- Create an administrative account and limit access to one VDOM
- Use inter-VDOM links to route traffic between VDOMs

Time to Complete

Estimated: 40 minutes

Topology

The goal of this lab is to create the following topology. You will use VDOMs to logically split Local-FortiGate into two virtual firewalls: the root VDOM and the customer VDOM. Both VDOMs are running in NAT mode, so all internet traffic coming from Local-Client must first pass through the customer VDOM, and then through the root VDOM.

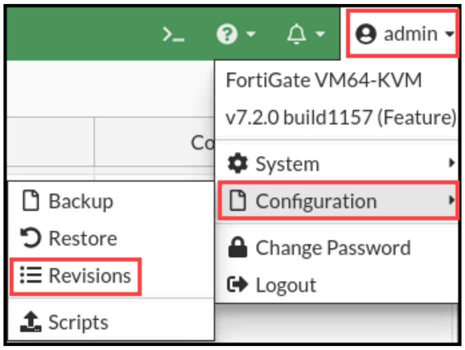


Prerequisites

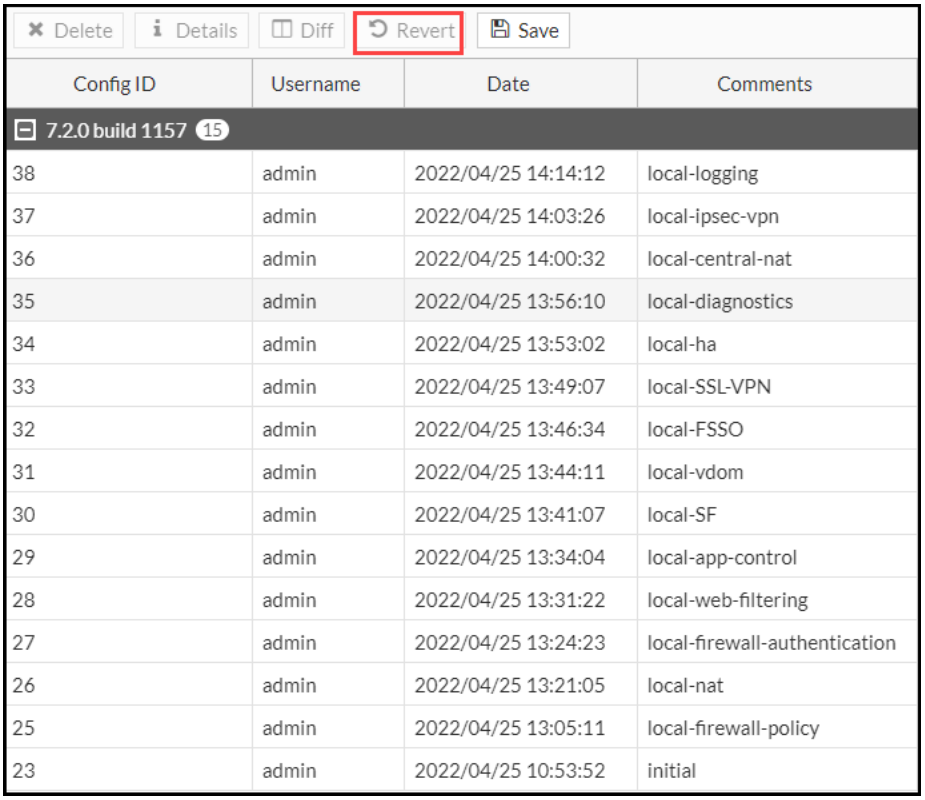
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **local-vdom**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Creating VDOMs and VDOM Objects

In this exercise, you will examine how to add a new VDOM. Then, you will create an inter-VDOM link between the VDOM you added and the root VDOM. You will also create an administrator account that has access to only one VDOM.

The configuration file for this exercise already has VDOMs enabled. You will use only **multi-vdom** mode in this exercise.

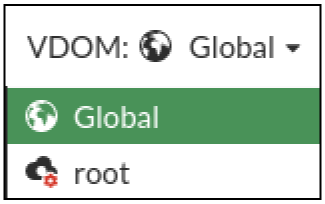
Create a VDOM

A FortiGate with VDOMs enabled includes a root VDOM. You can create additional VDOMs to split the physical FortiGate into multiple virtual firewalls. In the next steps, you will add a second VDOM.

To create a VDOM

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.

   You will notice that the FortiGate menu has changed. This is because VDOMs are enabled. There is now a drop-down list at the top of the menu, and a **VDOM** drop-down list on the title bar. In the **VDOM** drop-down list, you can select global settings or VDOM-specific settings for the root VDOM. The default setting is **Global**.

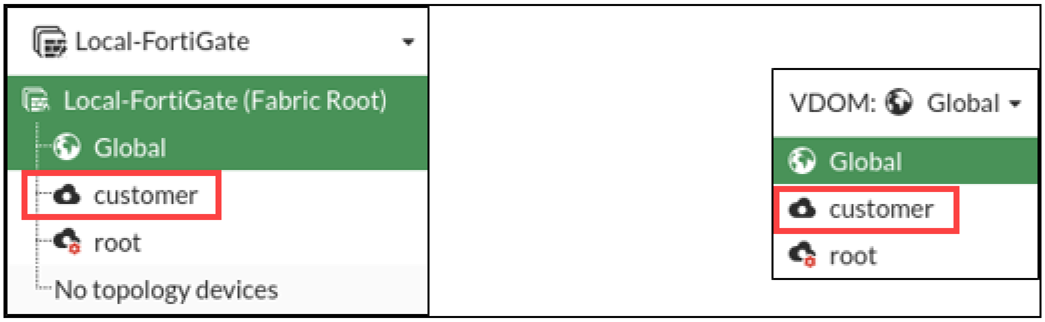


2. In the **VDOM** drop-down list, select **Global**.
3. Click **System** > **VDOM**.
4. Click **Create New**.
5. Configure the following VDOM settings:

Field	Value
Virtual Domain	customer
Type	Traffic
NGFW Mode	Profile-based
WiFi country/region	Canada

6. Click **OK**.

Notice that the drop-down list at the top of the menu and the **VDOM** drop-down list show a third option—the VDOM-specific settings for **customer**.



Create a Per-VDOM Administrator

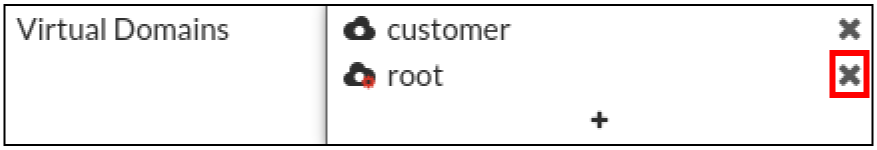
You will create an administrator account that has access to the **customer** VDOM only.

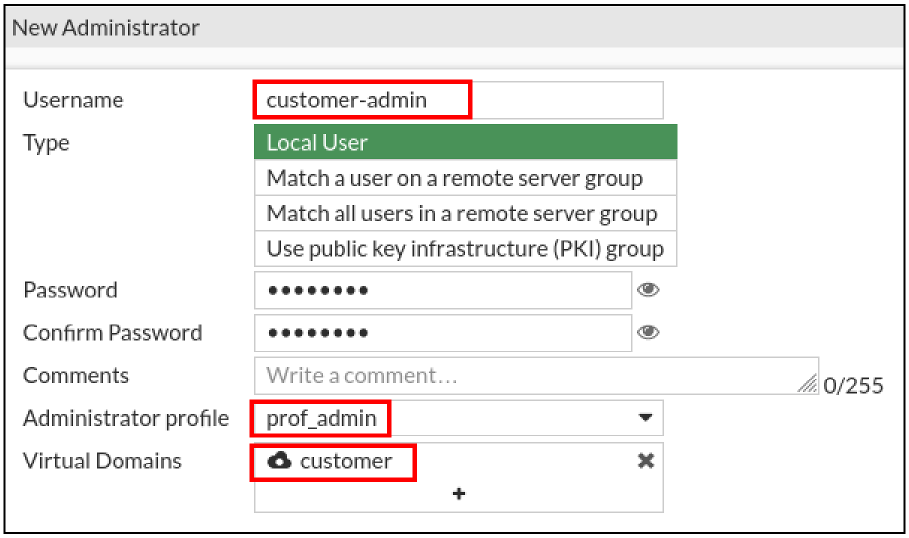
To create a per-VDOM administrator

1. On the Local-FortiGate GUI, click **Global** > **System** > **Administrators**.
2. Click **Create New** > **Administrator**.
3. Configure the following settings:

Field	Value
User Name	customer-admin
Type	Local User
Password	fortinet
Confirm Password	fortinet
Administrator Profile	prof_admin
Virtual Domains	customer

4. In the **Virtual Domains** list, remove **root** to restrict the new administrator's access to **customer**.





New Administrator

Username: customer-admin

Type: Local User

- Local User
- Match a user on a remote server group
- Match all users in a remote server group
- Use public key infrastructure (PKI) group

Password: ••••••••

Confirm Password: ••••••••

Comments: Write a comment... 0/255

Administrator profile: prof_admin

Virtual Domains: customer

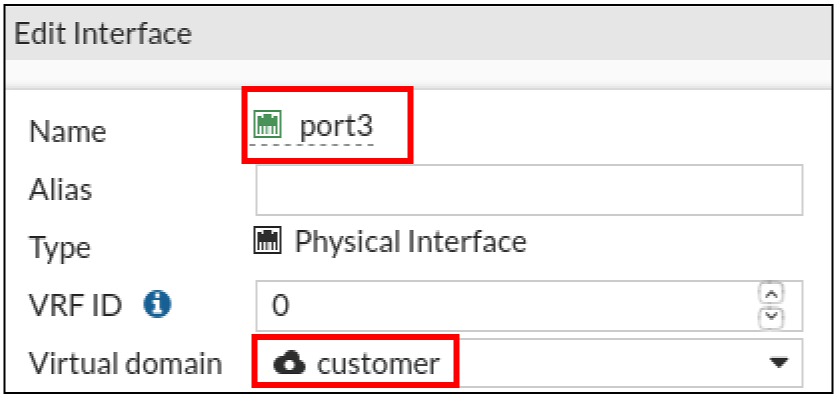
5. Click **OK**.

Move an Interface to a Different VDOM

The **customer-admin** account can log in only through an interface in the **customer** VDOM. Therefore, move the **port3** interface, which connects to the internal network, to the **customer** VDOM.

To move an interface to a different VDOM

1. Continuing on the Local-FortiGate GUI, click **Global** > **Network** > **Interfaces**.
2. Edit **port3**.
3. In the **Virtual Domain** drop-down list, select **customer**.



Edit Interface

Name: port3

Alias:

Type: Physical Interface

VRF ID: 0

Virtual domain: customer

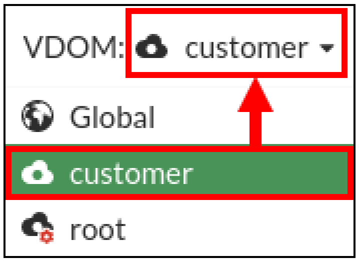
4. Click **OK**.
5. Click **OK** to confirm the configuration.

Add the DNS Service to an Interface

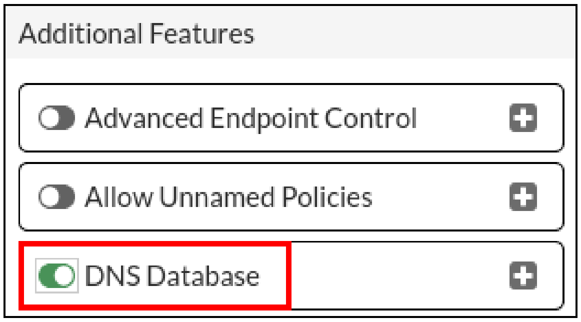
For Local-Client, the DNS server is port3. First, you will enable the DNS database in the **Feature Visibility** section. Then, you will add DNS service to port3.

To enable the DNS database

1. Continuing on the Local-FortiGate GUI, in the VDOM drop-down list, select the **customer** VDOM.



2. Click **System** > **Feature Visibility**.
3. In the **Additional Features** section, enable **DNS Database**.

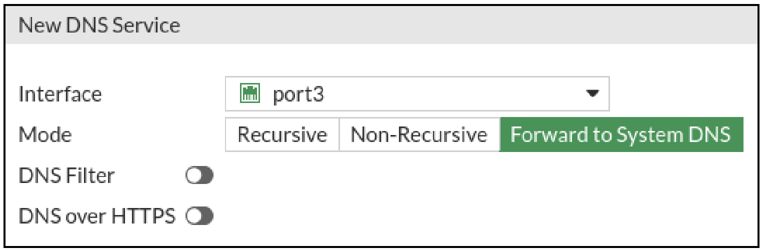


4. Click **Apply**.

To add DNS service to an interface

1. Continuing on the Local-FortiGate GUI, in the **customer** VDOM, click **Network** > **DNS Servers**.
2. Under **DNS Service on Interface**, click **Create New**, and then configure the following settings:

Field	Value
Interface	port3
Mode	Forward to System DNS



New DNS Service

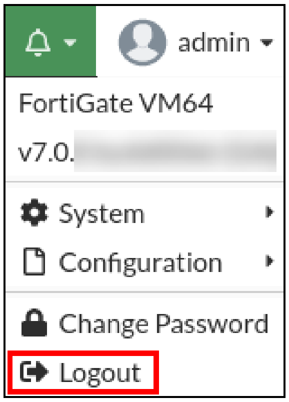
Interface: port3

Mode: Recursive | Non-Recursive | [✓ Forward to System DNS]

DNS Filter ○

DNS over HTTPS ○

3. Click **OK**.
4. Log out of the Local-FortiGate GUI.



Test the Per-VDOM Administrator Account

To see what access is available to the **customer-admin** account, try logging in to the FortiGate-Local GUI as **customer-admin**.

To test the per-VDOM administrator account

1. On the Local-Client VM, open a browser, and then connect to the Local-FortiGate GUI.
2. Log in, but this time, use the administrator name `customer-admin` and password `fortinet`.
3. View the GUI and examine what the VDOM administrator is allowed to control.

   Because the **customer-admin** administrator can access the **customer** VDOM only, the GUI does not display the **Global** configuration settings or the VDOM-specific settings for the **root** VDOM.
4. Log out of the Local-FortiGate GUI, and then log in again with the username `admin` and password `password`.

   This account has access to the global settings and all VDOMs.

> **Stop and think!**
>
> Why is the dashboard different between the two login sessions?
>
> Logging in with the `admin` account gives you full access to the **root** VDOM, as well as the FortiGate system resources. Logging in with the `customer-admin` account gives you access to the **customer** VDOM only, and does not give you access to the system resource details.

Execute Per-VDOM CLI Commands

After you enable VDOMs, the GUI menu structure and CLI tree structure change. You will examine the differences on the CLI for VDOMs.

To execute per-VDOM CLI commands

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Try to run the following command to list the routing table:

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

Did the CLI reject this command? To run this command when VDOMs are enabled, you must specify the VDOM first, in order for FortiGate to know which VDOM routing table to display.

3. To enter the **customer** VDOM context, enter the following commands:

```
config vdom
   edit customer
```

Be careful when you type VDOM names with the `edit` command.

VDOM names are case-sensitive, and the `edit` command can both modify and create a VDOM. For example, if you enter `edit Root`, you will not enter the pre-existing **root** VDOM. Instead, you will create and enter a new VDOM named **Root**.

4. Now that you have specified the VDOM, try looking at the routing table again, using the following command:

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

The command works now. The information displayed in the routing table is specific to the **customer** VDOM. Remember that each VDOM has its own routing table.

5. Go to the root VDOM context, using the following commands:

```
next
   edit root
```

6. Enter the following command to list the routing table:

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

This time, the information displayed in the routing table belongs to the **root** VDOM. You will see that this table is different from the one for the **customer** VDOM.

7. Close the Local-FortiGate CLI session.

Exercise 2: Configuring an Inter-VDOM Link

In this exercise, you will examine how to route traffic between two VDOMs using an inter-VDOM link.

Create an Inter-VDOM Link

You will create an inter-VDOM link to route traffic between two VDOMs.

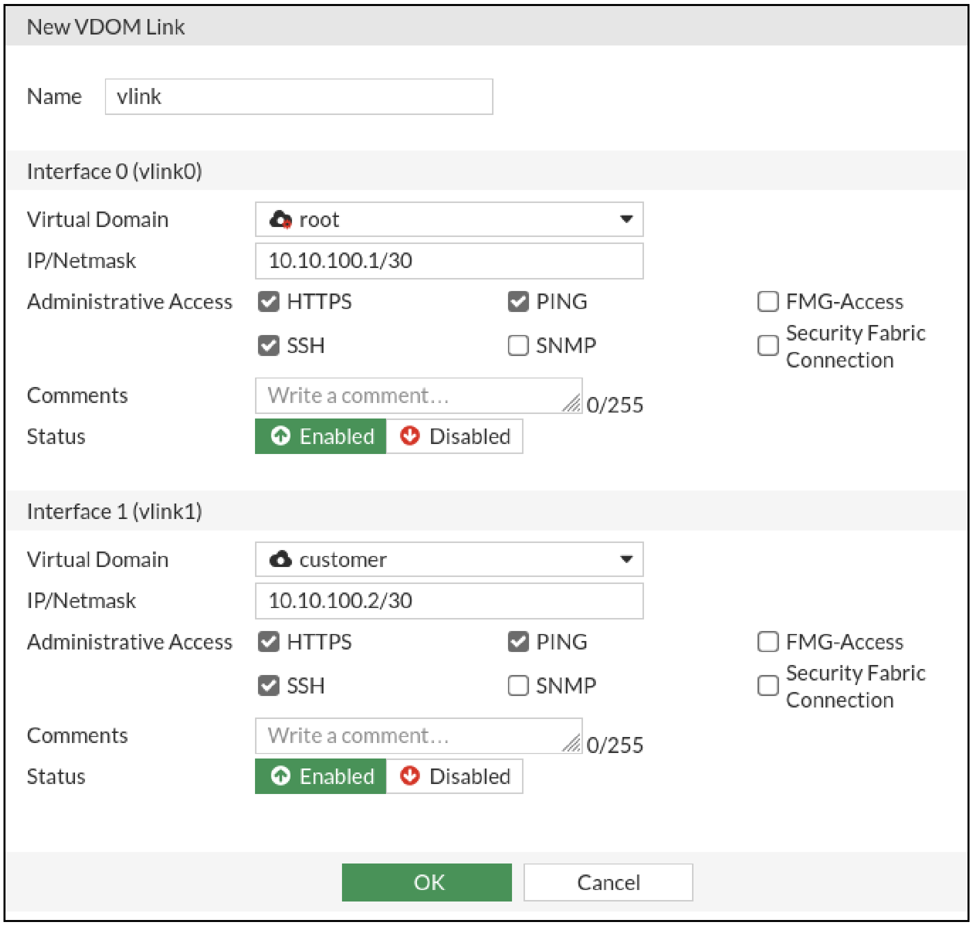
To create an inter-VDOM link

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the **Global** VDOM settings, click **Network** > **Interfaces**.
3. Click **Create New**, and then select **VDOM Link**.
4. In the **Name** field, type `vlink`.
5. In the **Interface 0 (vlink0)** section, configure the following settings:

Field	Value
Virtual Domain	root
IP/Network Mask	10.10.100.1/30
Administrative Access	HTTPS, PING, SSH

6. In the **Interface 1 (vlink1)** section, configure the following settings:

Field	Value
Virtual Domain	customer
IP/Network Mask	10.10.100.2/30
Administrative Access	HTTPS, PING, SSH



New VDOM Link

Name	vlink

Interface 0 (vlink0)

Virtual Domain	root		
IP/Netmask	10.10.100.1/30		
Administrative Access	☑ HTTPS	☑ PING	□ FMG-Access
	☑ SSH	□ SNMP	□ Security Fabric Connection
Comments	Write a comment... 0/255		
Status	Enabled	Disabled	

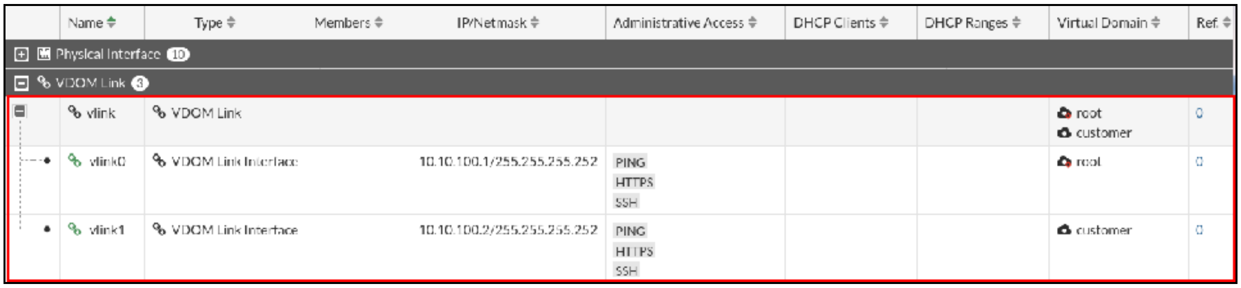
Interface 1 (vlink1)

Virtual Domain	customer		
IP/Netmask	10.10.100.2/30		
Administrative Access	☑ HTTPS	☑ PING	□ FMG-Access
	☑ SSH	□ SNMP	□ Security Fabric Connection
Comments	Write a comment... 0/255		
Status	Enabled	Disabled	

OK Cancel

7. Click **OK**.

After you create the inter-VDOM link, notice the two inter-VDOM subinterfaces that were added in the **root** and **customer** VDOMs (expand **vlink**). These interfaces are named **vlink0** and **vlink1**. You can use them to route traffic between two VDOMs.



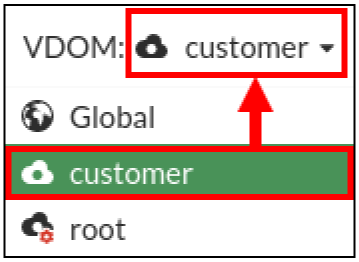
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Virtual Domain	Ref.
Physical Interface 10								
VDOM Link 3								
vlink	VDOM Link						root customer	0
vlink0	VDOM Link Interface		10.10.100.1/255.255.255.252	PING HTTPS SSH			root	0
vlink1	VDOM Link Interface		10.10.100.2/255.255.255.252	PING HTTPS SSH			customer	0

Configure Routing Between VDOMs

You will add the static routes to both VDOMs to route traffic between them. The objective is to have internet traffic from Local-Client cross the **customer** VDOM first, and then cross the **root** VDOM, before the traffic goes to the Linux server and the internet.

To configure routing between VDOMs

1. Continuing on the Local-FortiGate GUI, in the **VDOM** drop-down list, select the **customer** VDOM.



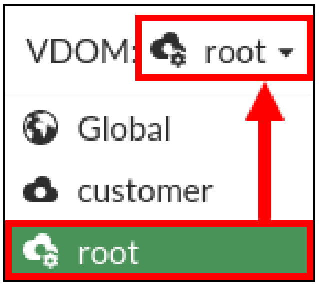
2. Click **Network** > **Static Routes**.
3. Click **Create New** to specify a default route for the **customer** VDOM.
4. Add the following route:

Field	Value
Destination	Subnet 0.0.0.0/0.0.0.0
Gateway Address	10.10.100.1
Interface	vlink1

5. Click **OK**.

   Now, you will specify a route for the **root** VDOM to the internal network.

6. In the **VDOM** drop-down list, select **root**.



7. Click **Network** > **Static Routes**.
8. Click **Create New**.
9. Configure the following route:

Field	Value
Destination	Subnet 10.0.1.0/24
Gateway Address	10.10.100.2
Interface	vlink0

10. Click **OK**.

Configure Firewall Policies for Inter-VDOM Traffic

You will create firewall policies to allow internet traffic to pass through the **customer** and **root** VDOMs.

Take the Expert Challenge!

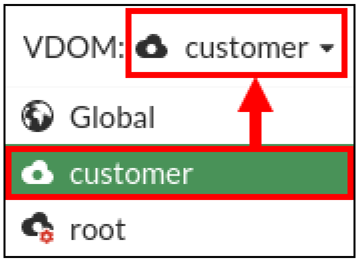
On the Local-FortiGate GUI (`10.0.1.254` | `admin/password`), configure the appropriate firewall policies to allow traffic to flow freely across the inter-VDOM link. This requires two firewall policies, one from **port3** to **vlink1**, and one from **vlink0** to **port1**.

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

After you complete the challenge, see Test the Inter-VDOM Link on page 42.

To configure firewall policies for inter-VDOM traffic for port3 to vlink1

1. Continuing on the Local-FortiGate GUI, in the **VDOM** drop-down list, select **customer**.



2. Click **Policy & Objects** > **Firewall Policy**.
3. Click **Create New**.
4. Configure the following firewall policy to allow traffic to pass from **port3** to **vlink1**:

Field	Value
Name	Internet
Incoming Interface	port3
Outgoing Interface	vlink1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT

Field	Value
NAT	<disable>

5. Click **OK**.

To configure firewall policies for inter-VDOM traffic for vlink0 to port1

1. Continuing on the Local-FortiGate GUI, in the **VDOM** drop-down list, select **root**.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Click **Create New**.
4. Configure the following policy:

Field	Value
Name	Internet
Incoming Interface	vlink0
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	<enable>

5. Click **OK**.

Test the Inter-VDOM Link

You will test your configuration to confirm that internet traffic is being routed through the two VDOMs and the inter-VDOM link.

To test the inter-VDOM link

1. Continuing on the Local-Client VM, open a few browser tabs, and visit a few external HTTP websites, such as:
   - http://www.pearsonvue.com/fortinet/
   - http://cve.mitre.org
   - http://www.eicar.org

   Traffic should be flowing through both VDOMs now.
2. Open a terminal window, and then run a `traceroute` command to an internet public IP address.

```
traceroute 4.2.2.2
```

3. Check the output.

   The first hop IP address is `10.0.1.254`, which is **port3** in the **customer** VDOM. The second hop IP address is `10.10.100.1`, which is the inter-VDOM link in the **root** VDOM. The third hop IP address is `10.200.1.254`, which is the Linux server.

4. Close the terminal and your browser.

Lab 3: Fortinet Single Sign-On Configuration

In this lab, you will test user authentication using FSSO. The lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Local-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Local-Client VM.

Objectives

- Review the SSO configuration on FortiGate
- Test the transparent or automatic user identification by generating user logon events
- Monitor the SSO status and operation

Time to Complete

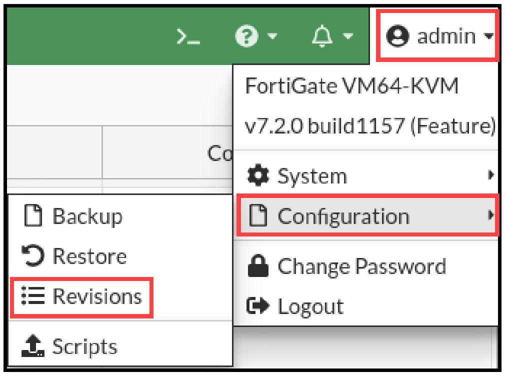
Estimated: 35 minutes

Prerequisites

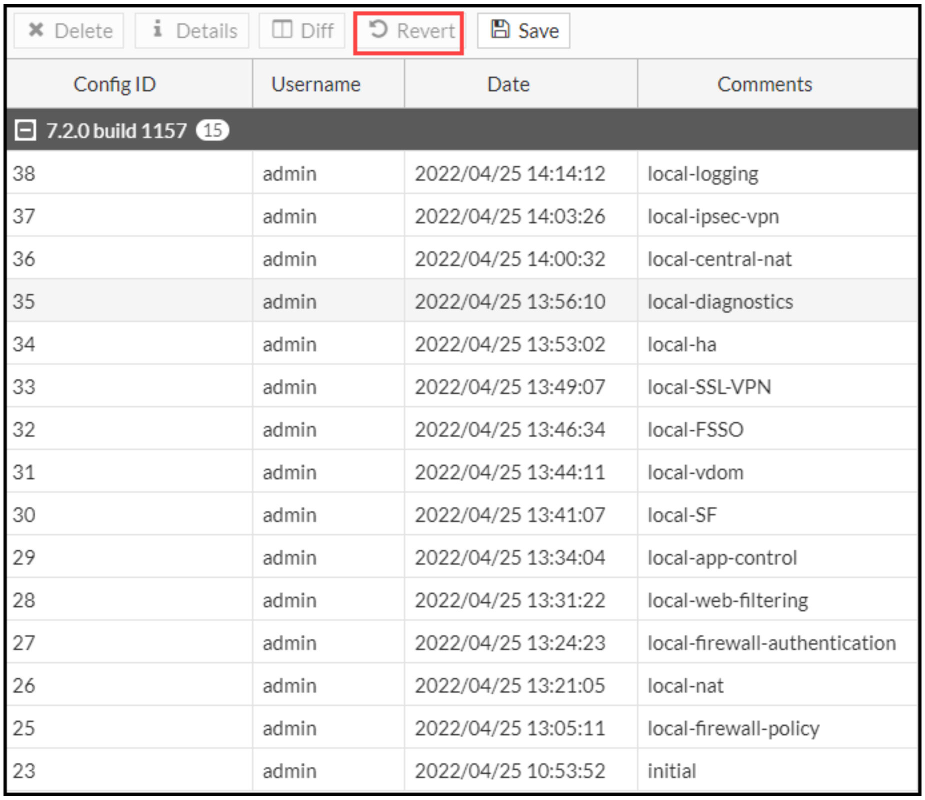
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-FSSO**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Configuring FortiGate for FSSO Authentication

In this exercise, you will configure FortiGate for FSSO and test user authentication. The lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Local-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Local-Client VM.

In the real world, you must configure FortiGate to identify users by polling their logon events using an FSSO agent, and you must install and configure a collector agent. FSSO agents are available on the Fortinet Support website (http://support.fortinet.com).

For FortiGate to communicate and poll information from the FSSO collector agent, you must assign the polled user to a firewall user group, and then add the user group as a source on a firewall policy.

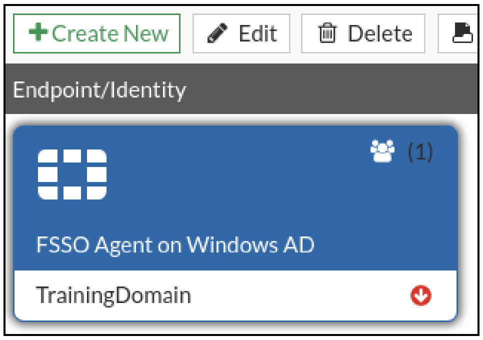
Finally, you can verify the user logon event that FortiGate collects. This event is generated after a user logs in to the Windows Active Directory domain. Therefore, no firewall authentication is required.

Review the FSSO Configuration on FortiGate

You will review the FSSO configuration and FSSO user groups on FortiGate. FSSO allows FortiGate to automatically identify the users who connect using SSO. Then, you will add FSSO user groups to the firewall policies.

To review the FSSO server and FSSO user group configuration on FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **External Connectors**.
3. Select **TrainingDomain**, and then click **Edit**.



4. Review the **Endpoint/Identity** status in the upper-right corner of the screen, and see that the status is **Disconnected**.

   Leave the window open.

To run a script to simulate a user logon event

1. On the Local-Client VM, open a terminal window, and then enter the following commands to simulate a user logon event:

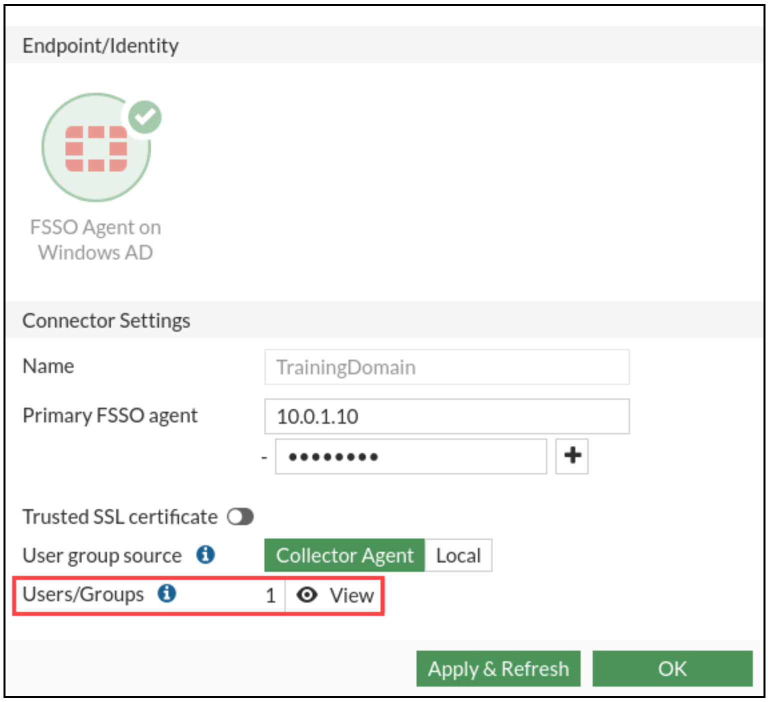
```
cd Desktop/FSSO/
python2 fssoreplay.py -l 8000 -f sample.log
```

2. Keep the terminal window open.

   The script continues to run in the background.

To review the FSSO connection and FSSO user groups

1. Continuing on the **TrainingDomain** window, click **Apply & Refresh**.
2. Select **TrainingDomain**, and then click **Edit**.
3. In the **Users/Groups** field, click **View**.



Endpoint/Identity

Connector Settings

Name: TrainingDomain

Primary FSSO agent: 10.0.1.10

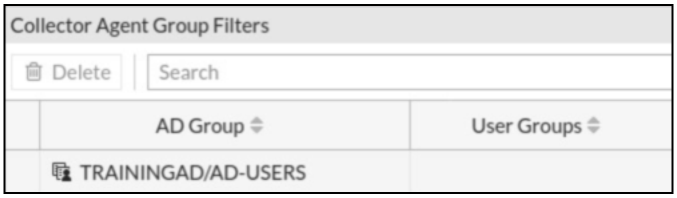
- ••••••••• +

Trusted SSL certificate ○

User group source ℹ: Collector Agent | Local

Users/Groups ℹ: 1 View

The **TRAININGAD/AD-USERS** monitored group is displayed.

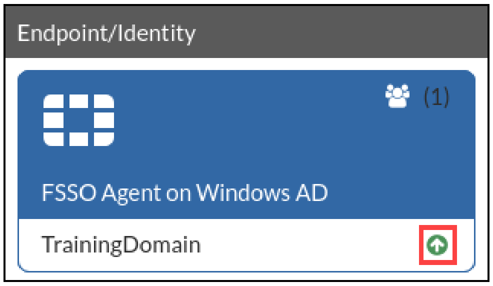


Collector Agent Group Filters

AD Group	User Groups
TRAININGAD/AD-USERS	

4. Click **X** to close the **Collector Agent Group Filters** window.
5. Click **OK**.

   A green up arrow confirms the communication with the FSSO collector agent is up.



To assign the FSSO user to an FSSO user group

1. Continuing on the Local-FortiGate GUI, click **User & Authentication** > **User Groups**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	Training
Type	Fortinet Single Sign-On (FSSO)
Members	TRAININGAD/AD-USERS

The FSSO user is automatically listed because of the selected group type—FSSO.

3. Click **OK**.

Assign FSSO Users to a Firewall Policy

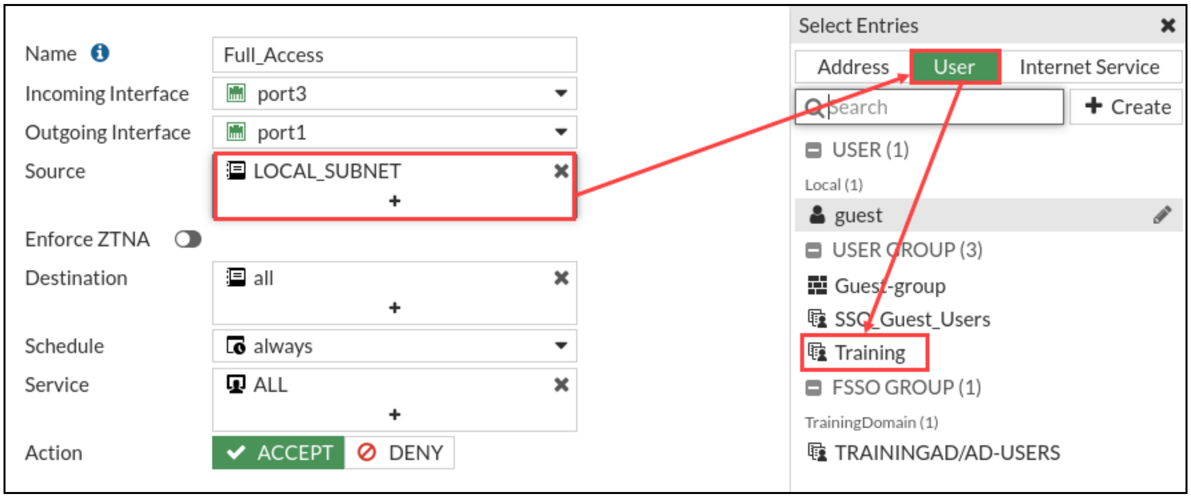
You will assign your FSSO user group as a source on a firewall policy. This allows you to control access to network resources based on user identity.

To test the connection without assigning the FSSO user group to a firewall policy

1. On the Local-Client VM, open a new browser, and then go to https://www.fortinet.com.
   You can see that all users can access the Fortinet website.

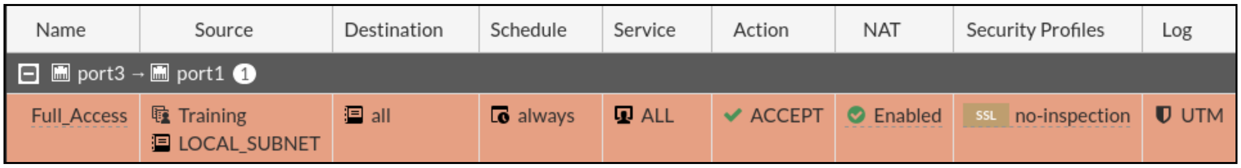
To add the FSSO user group to your firewall policy

1. Return to the browser where you are logged in to the Local-FortiGate GUI, and then click **Policy & Objects** > **Firewall Policy**.
2. Edit the **Full_Access** firewall policy.
3. In the **Source** drop-down list, click **LOCAL_SUBNET**.
4. In the **Select Entries** section, select **User**, and then add the **Training** group.



Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Enforce ZTNA	
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

5. Click **Close**, and then click **OK**.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
port3 → port1 1								
Full_Access	Training LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM

Test FSSO

After a user logs in, they are automatically identified based on their IP address. As a result, FortiGate allows the user to access network resources as policy decisions are made.

To test the connection after assigning the FSSO user to the firewall policy

1. On the Local-Client VM, open a new browser tab, and then go to http://support.fortinet.com.

The Python script that is running on Local-Client is already sending user logon events with the following information:

- **user**: aduser1
- **IP**: 10.0.1.10

In this case, the website loads successfully because aduser1 belongs to the configured user group on a firewall policy.

To review the connection status between the FSSO collector agent and FortiGate

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to show the connection status between FortiGate and each collector agent:

```
diagnose debug enable
diagnose debug authd fsso server-status
```

3. Observe the CLI output.

   Your FortiGate is connected to the FSSO collector agent.

```
Server Name Connection Status Version Address
----------- ----------------- ------- -------
TrainingDomain connected FSAE server 1.1 10.0.1.10
```

To monitor communication between the FSSO collector agent and FortiGate

1. Continuing on the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands:

```
diagnose debug enable
diagnose debug application authd 8256
```

3. On the Local-Client VM, on a terminal window, press `Ctrl`+`C` to stop the script, and then run the following command again to simulate a user logon event:

```
python2 fssoreplay.py -l 8000 -f sample.log
```

4. View the output of the `diagnose` command.

```
[_process_logon: 871]: ADUSER1(10.0.1.10, 0) logged on from TrainingDomain.
[_process_logon:1103]: ADUSER1 (10.0.1.10, 0) from TrainingDomain exists
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100004
fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100005
```

You generated a logon event in the Local-Client VM using the script, and it was forwarded to FortiGate.

5. Enter the following command to stop the debug process:

```
diagnose debug reset
```

To display the FSSO logons

1. Continuing on the Local-FortiGate VM, enter the following command:

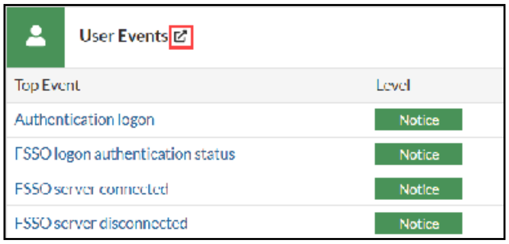
```
diagnose debug authd fsso list
```

2. Review the output, which shows the FSSO logons.

```
----FSSO logons----
IP:10.0.1.10 User: ADUSER1 Groups: TRAINING/AD-USERS Workstation
C7280677811.TRAININGAD.TRAINING.LAB MemberOf: Training TRAININGAD/AD-USE Stale
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

To review the user event logs

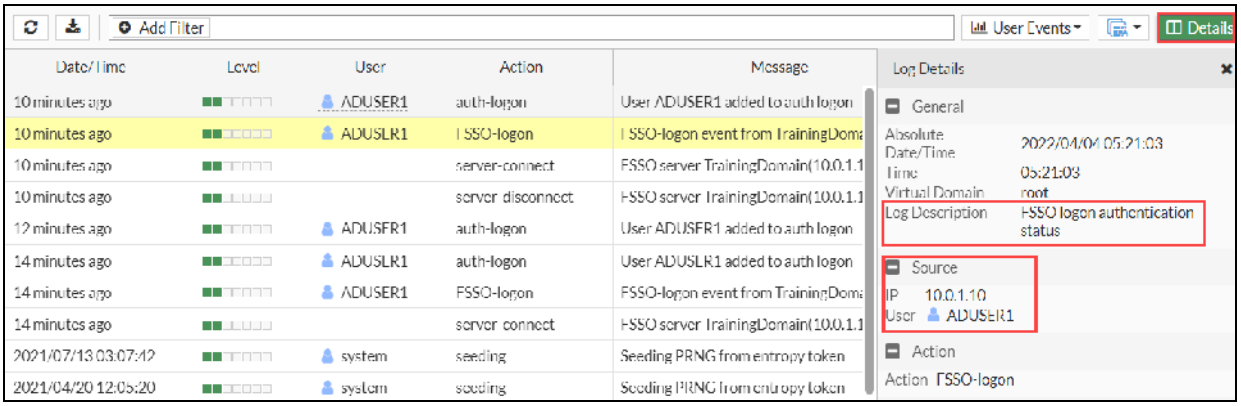
1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Log & Report** > **System Events**, and then click the **View Logs** arrow in the **User Events** widget.



User Events

Top Event	Level
Authentication logon	Notice
FSSO logon authentication status	Notice
FSSO server connected	Notice
FSSO server disconnected	Notice

3. Select a log, and then click **Details** to view more information about it.



Date/Time	Level	User	Action	Message
10 minutes ago		ADUSER1	auth-logon	User ADUSER1 added to auth logon
10 minutes ago		ADUSER1	FSSO-logon	FSSO-logon event from TrainingDoma
10 minutes ago			server-connect	FSSO server TrainingDomain(10.0.1.1
10 minutes ago			server-disconnect	FSSO server TrainingDomain(10.0.1.1
12 minutes ago		ADUSER1	auth-logon	User ADUSER1 added to auth logon
14 minutes ago		ADUSER1	auth-logon	User ADUSER1 added to auth logon
14 minutes ago		ADUSER1	FSSO-logon	FSSO-logon event from TrainingDoma
14 minutes ago			server-connect	FSSO server TrainingDomain(10.0.1.1
2021/07/13 03:07:42		system	seeding	Seeding PRNG from entropy token
2021/04/20 12:05:20		system	seeding	Seeding PRNG from entropy token

Log Details

General

Absolute Date/Time	2022/04/04 05:21:03
Time	05:21:03
Virtual Domain	root
Log Description	FSSO logon authentication status

Source

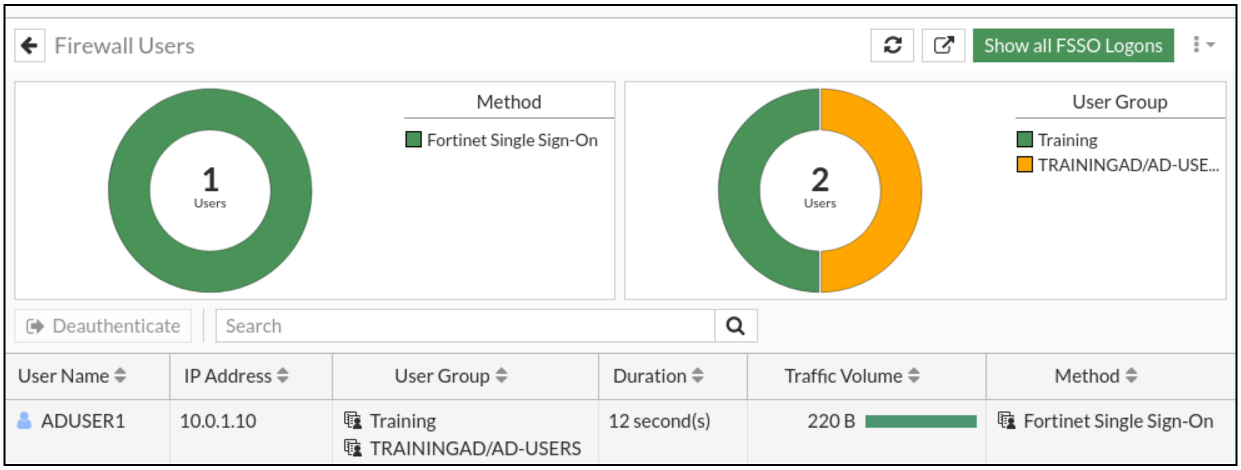
IP	10.0.1.10
User	ADUSER1

Action

Action	FSSO-logon

To monitor FSSO logons

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Users & Devices**, and then double-click **Firewall Users** to expand it to full screen.
2. Click **Show all FSSO Logons**, and then click **Refresh** if the user's details don't appear.



User Name	IP Address	User Group	Duration	Traffic Volume	Method
ADUSER1	10.0.1.10	Training TRAININGAD/AD-USERS	12 second(s)	220 B	Fortinet Single Sign-On

Lab 4: ZTNA

There is no lab associated with this lesson.

Lab 5: SSL VPN

In this lab, you will examine how to configure an SSL VPN connection in tunnel and web modes. You will also manage user groups and portals for an SSL VPN.

Objectives

- Configure and connect to an SSL VPN
- Enable authentication security
- Configure a firewall policy for SSL VPN users to access private network resources
- Customize the SSL VPN portal for web mode
- Configure FortiClient for the SSL VPN connection in tunnel mode

Time to Complete

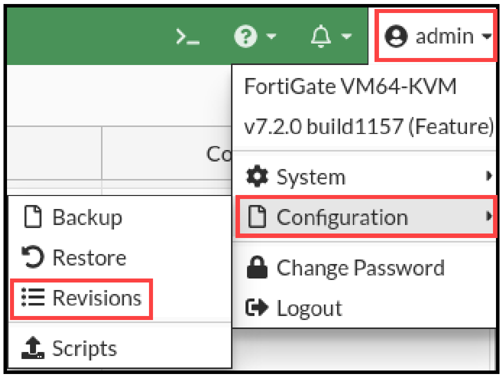
Estimated: 40 minutes

Prerequisites

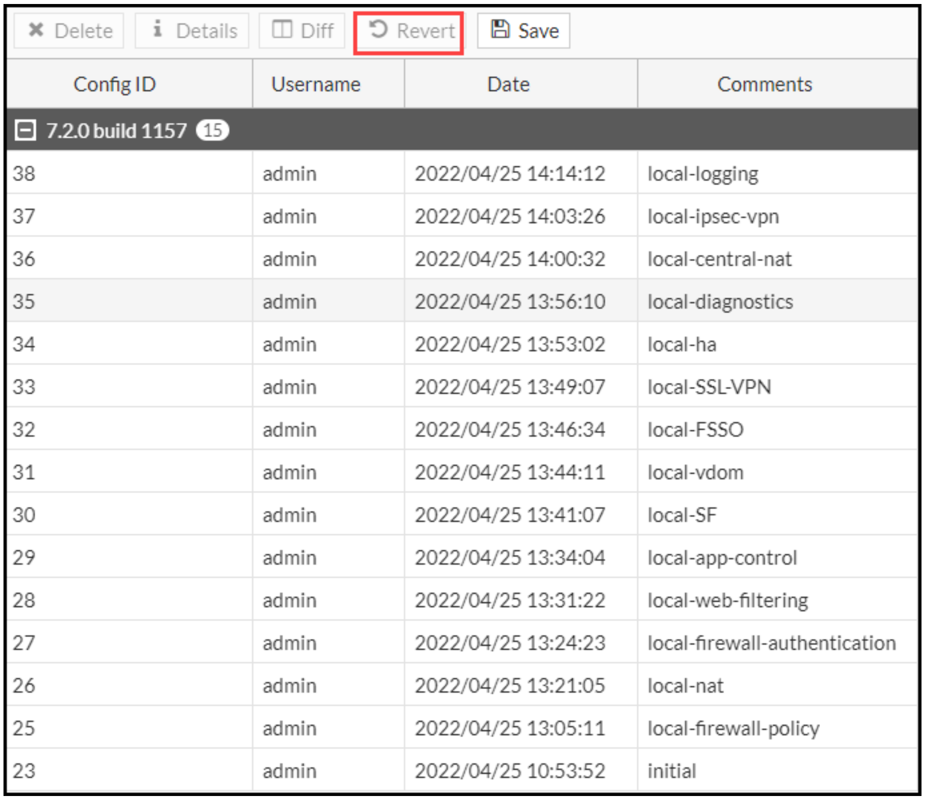
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.
3. Click **+** to expand the list.



4. Select the configuration with the comment **local-SSL-VPN.conf**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

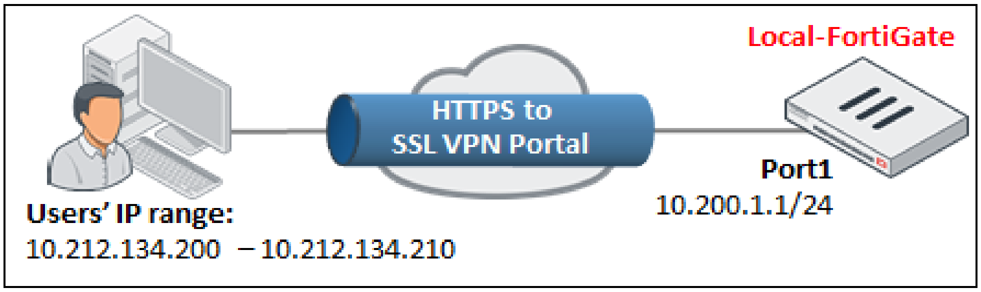
Exercise 1: Configuring Web Mode SSL VPN

On FortiGate, there are two modes you can configure to allow remote access through SSL VPN: web mode and tunnel mode.

In this exercise, you will examine how to test web mode, which allows SSL VPN users to connect from the Remote-Client VM to resources located in the local subnet (`10.0.1.0/24`).

Configure the SSL VPN Settings

You will configure the SSL VPN settings to allow the remote connection shown in the following image:



To create a user for SSL VPN connections

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **User & Authentication** > **User Definition**.
3. Click **Create New**.
4. Click **Local User**, and then click **Next**.
5. Type the following credentials for the remote user, and then click **Next**:

Username	student
Password	fortinet

6. Leave the contact information empty, and click **Next**.
7. For **User Account Status**, verify that **Enabled** is selected.
8. Enable **User Group**, click the **+** that appears, and then in the right pane, select **SSL_VPN_USERS**.
9. Click **Submit**.

The **SSL_VPN_USERS** group was preconfigured for the purpose of this lab.

To review the settings of this group, click **User & Authentication** > **User Groups**.

To configure the SSL VPN settings for web access

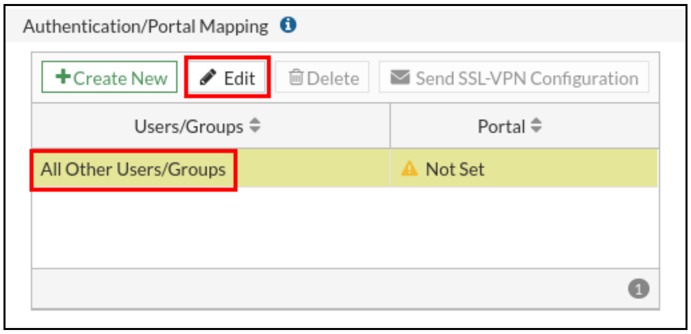
1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Settings**.
2. In the **Connection Settings** section, configure the following settings:

Field	Value
Listen on Interface(s)	port1
Listen on Port	10443
Restrict Access	Allow access from any host
Server Certificate	Fortinet_Factory
Inactive For	3000 seconds

3. In the **Tunnel Mode Client Settings** section, verify the following setting:

Field	Value
Address Range	Automatically assign addresses

4. In the **Authentication/Portal Mapping** section, select **All Other Users/Groups**, and then click **Edit**.



Authentication/Portal Mapping

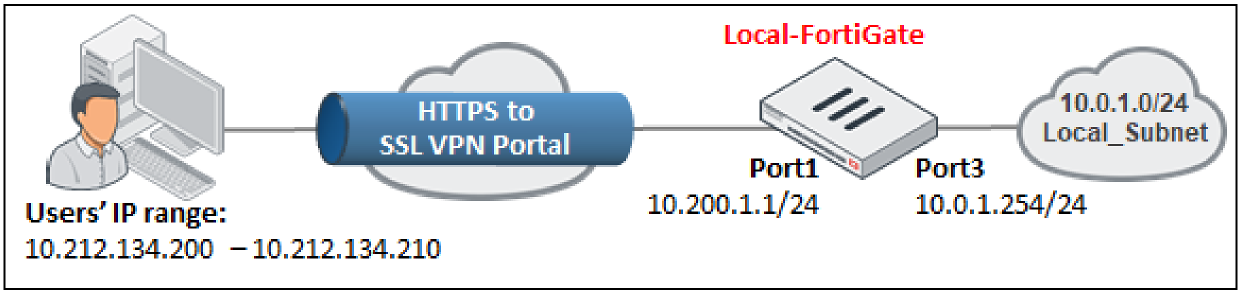
Users/Groups	Portal
All Other Users/Groups	Not Set

5. In the **Portal** drop-down list, select **web-access**, and then click **OK**.
6. Click **Apply** to save the changes.

   Notice the warning message displayed at the top of this page. It indicates that you must create a firewall policy for SSL VPN connections.

Create a Firewall Policy for SSL VPN

You will create a firewall policy that allows traffic to the local subnet (`10.0.1.0/24`) from remote users connected to the SSL VPN portal.



To create a firewall policy for SSL VPN

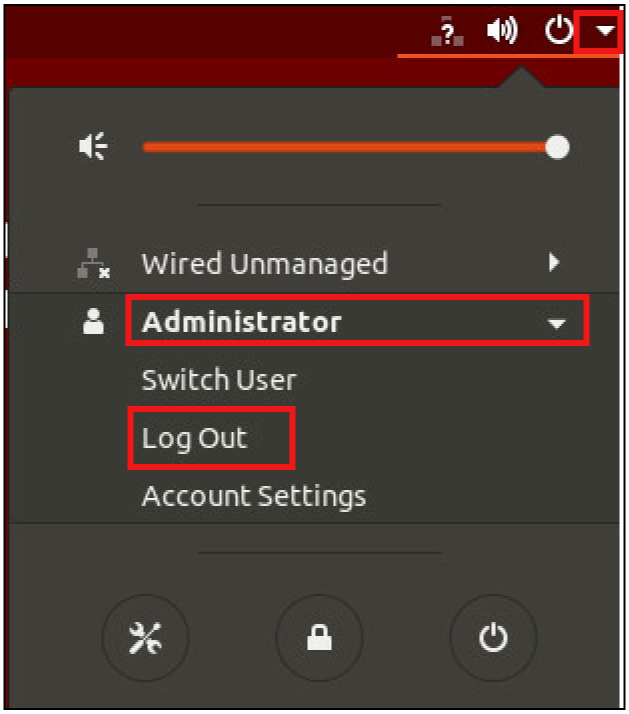
1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then configure the following firewall policy settings:

Field	Value
Name	SSL-VPN-Access
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port3
Source	Address > SSLVPN_TUNNEL_ADDR1 User > SSL_VPN_USERS
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT
Inspection mode	Flow-based
NAT	Disabled

3. Click **OK** to save the configuration.

The SSL VPN firewall policy allows traffic only from users in the **SSL_VPN_Users** group.

4. Log out of the Local-Client VM.

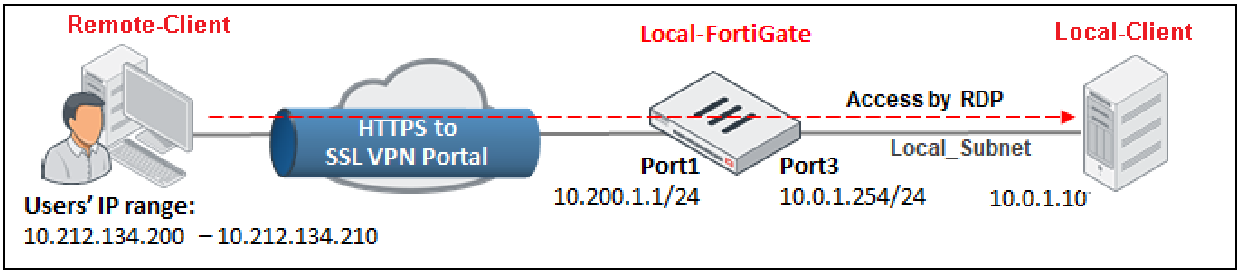


You must log out of the Local-Client VM before proceeding to the next step of the lab.

Test the SSL VPN Access

You will test the SSL VPN by accessing resources remotely in the local subnet (`10.0.1.0/24`).

For this, you will connect to the SSL VPN portal using the Remote-Client VM, and then you will create an RDP connection to the Local-Client VM.



To access the SSL VPN portal

1. In your lab environment, connect to the Remote-Client VM.
2. Open Firefox, and then connect to:
   `https://10.200.1.1:10443/`
   A security warning appears.

Stop and think!

Why do you receive a security warning?

For SSL connections, FortiGate is using a built-in certificate, which is signed by a certificate authority that the browser does not trust.

3. Click **Advanced**, and then click **Accept the Risk and Continue**.

   The remote login page opens.

4. Log in with the username `student` and password `fortinet`.

   The SSL VPN web portal opens. The portal is using default settings.

To test the SSL VPN portal

1. Continuing on the SSL VPN portal where you are logged in as `student`, click **Quick Connection**.

   Notice all the available options the SSL VPN portal allows for connections.

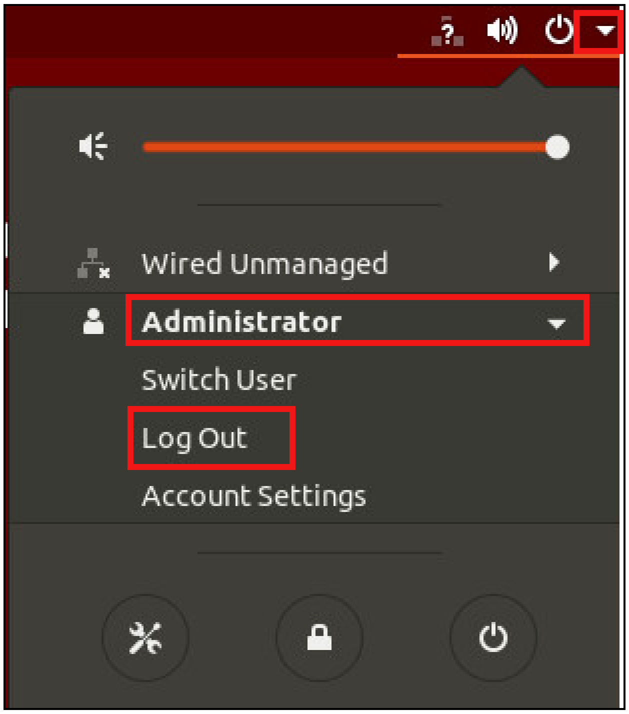
2. Click **RDP**, and then configure the following setting:

Field	Value
Host	10.0.1.10

3. Keep the default values for the remaining settings, and then click **Launch**.
4. Log in with the username `Administrator` and password `password`.
5. Click **OK**.

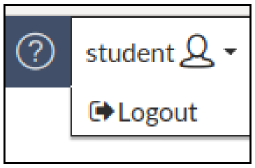
   You are now remotely connected to the Local-Client VM.

6. Log out of the Local-Client RDP session.



You must log out of the Local-Client VM before proceeding to the next step of the lab.

7. Close the web browser that is running the RDP session.
8. In the upper-right corner, click **student** > **Logout** to log out of the SSL VPN portal.



Add an Administrator-Based Bookmark to the SSL VPN Portal

You will customize the SSL VPN portal with a new color and a predefined bookmark.

To customize the SSL VPN portal

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **SSL-VPN Portals**.
3. Select **web-access**, and then click **Edit**.
4. Configure the following settings:

Field	Value
Portal Message	My Portal
Theme	Neutrino
Show Connection Launcher	<disable>
User Bookmarks	<disable>

5. In the **Predefined Bookmarks** section, click **Create New**, and then configure the following settings:

Field	Value
Name	Local-Client VM
Type	HTTP/HTTPS
URL	http://10.0.1.10
Single Sign-On	Disable

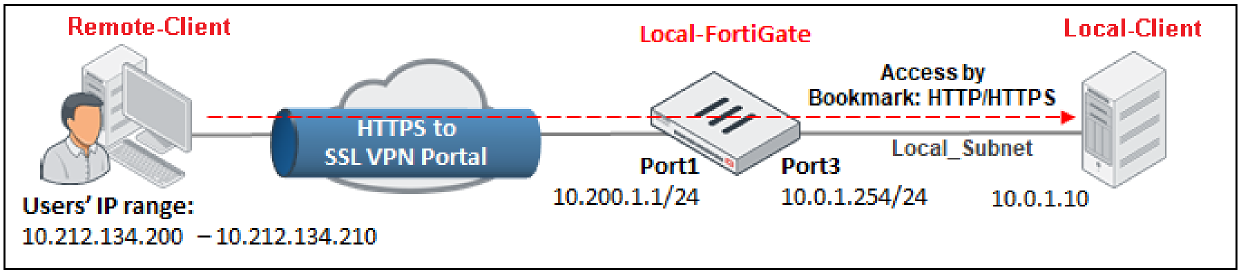
6. Click **OK**.
7. Click **OK** again to save the portal settings.

Test SSL VPN Access Using the Predefined Bookmark

You will connect to the SSL VPN portal on the Remote-Client VM again to access the resources in the local subnet (`10.0.1.0/24`).

For this, you will access the Local-Client VM using the predefined bookmark on the SSL VPN portal.

Notice that the SSL VPN portal looks different and provides fewer settings.



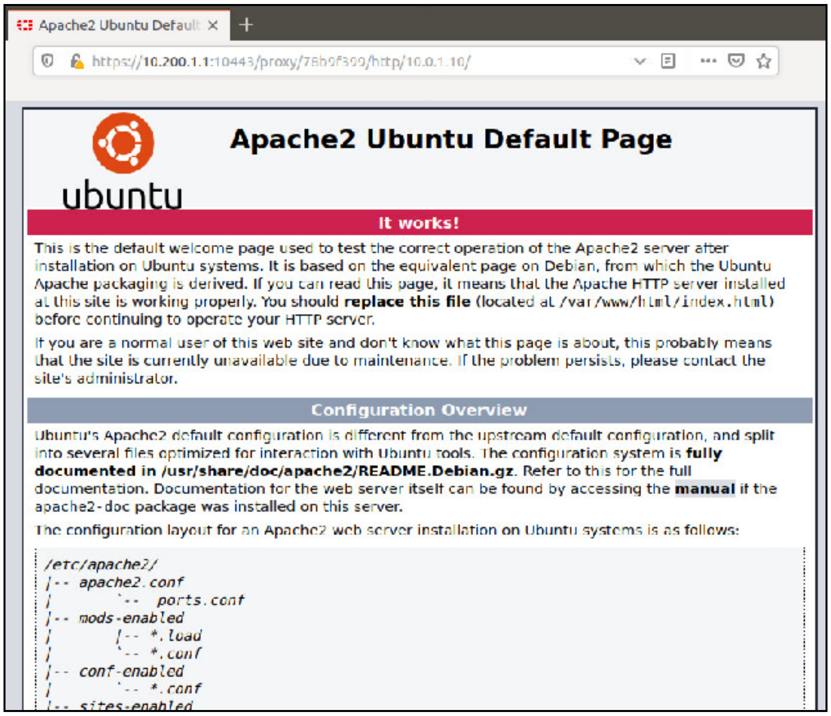
To test the bookmark

1. Return to the Remote-Client VM.
2. Open Firefox, and then reconnect to the SSL VPN portal at:
   `https://10.200.1.1:10443/`
3. Log in with the username `student` and password `fortinet`.

   Notice that the SSL VPN portal no longer allows quick connections or allows you to add bookmarks.

4. Click the **Local-Client VM** bookmark.

   You will connect to the web server running on the Local-Client VM at `10.0.1.10`.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

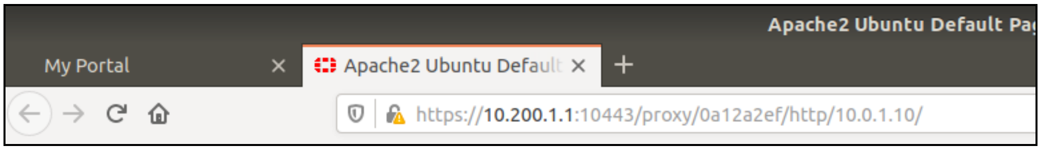
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
```

Examine the Web Mode Mechanism (Reverse HTTP Proxy)

You will examine the reverse HTTP proxy mechanism to learn how SSL VPN connections in web mode work.

To examine the reverse HTTP proxy mechanism

1. Continuing on the Remote-Client VM where you are connected to the web server running on the **Local-Client** VM at `10.0.1.10`, examine the URL in the address bar.



https://10.200.1.1:10443/proxy/0a12a2ef/http/10.0.1.10/

If you were on the local network while accessing the website, the address would be `http://10.0.1.10`. But, because you are accessing the website remotely through the FortiGate HTTP proxy, the URL is different.

Notice the URL structure in the browser address bar:

```
https://10.200.1.1:10443/proxy/..../http/10.0.1.10/
```

What does it mean?

Part of the URL	Description
https://10.200.1.1:10443	Indicates that the connection is SSL/TLS-encrypted, and that the portal is on the FortiGate port1 SSL VPN gateway
/proxy/..../http/	Indicates that the connection is being handled by the FortiGate HTTP reverse proxy
10.0.1.10/	Indicates the destination IP address of the website inside your private network, which you are accessing through the VPN

FortiGate encrypts the connection to the browser, but the destination server IP address in the URL is displayed in cleartext, *not* hidden from users. The secondary connection, from the FortiGate HTTP proxy to the bookmarked website, is not encrypted.

Monitor an SSL VPN User

You will monitor and disconnect an SSL VPN user from the FortiGate GUI.

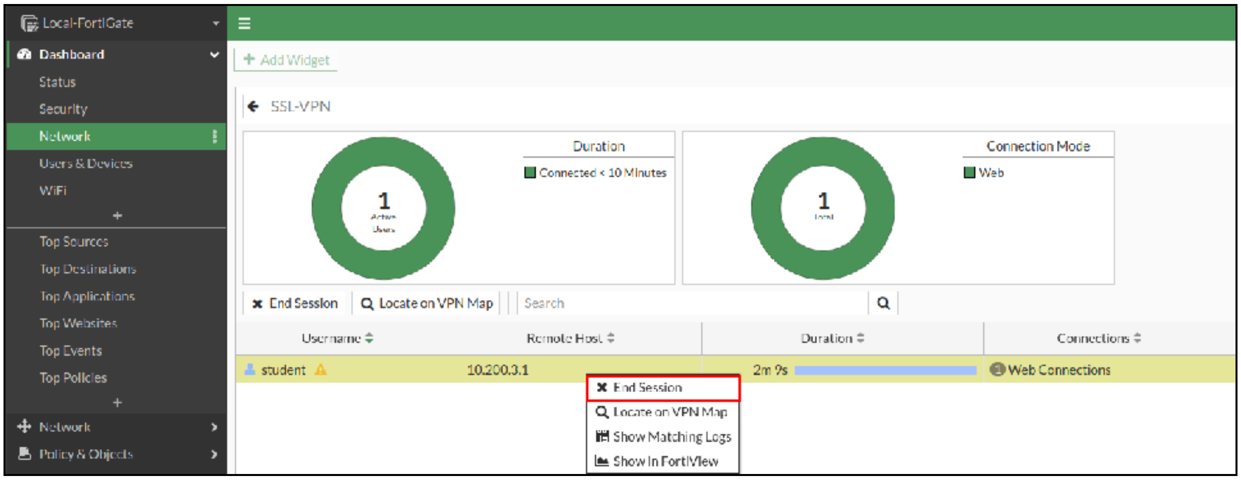
To monitor and disconnect an SSL VPN user

1. Return to the Local-FortiGate GUI.
2. Click **Dashboard** > **Network**, and then view the **SSL-VPN** widget.

   You can see that the student user is connecting from the remote host `10.200.3.1`.

3. Right-click **student**, and then select **End Session**.
4. Click **OK**.

   The student user no longer appears in the SSL VPN monitor.



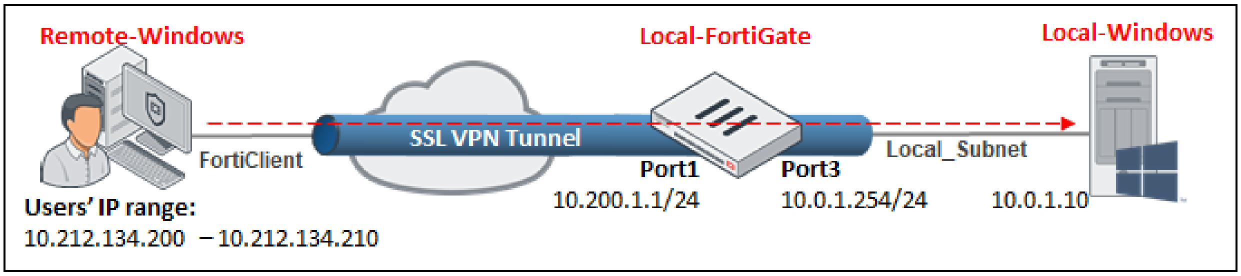
Username	Remote Host	Duration	Connections
student	10.200.3.1	2m 9s	Web Connections

Exercise 2: Configuring SSL VPN Tunnel Mode

In this exercise, you will examine how to change the SSL VPN settings to allow remote access to the resources in the local subnet (`10.0.1.0/24`), but perform a connection in tunnel mode from the Remote-Client VM.

You will use the remote access module of FortiClient, which supports the Fortinet SSL VPN client.

FortiClient is already installed on the Remote-Client VM.



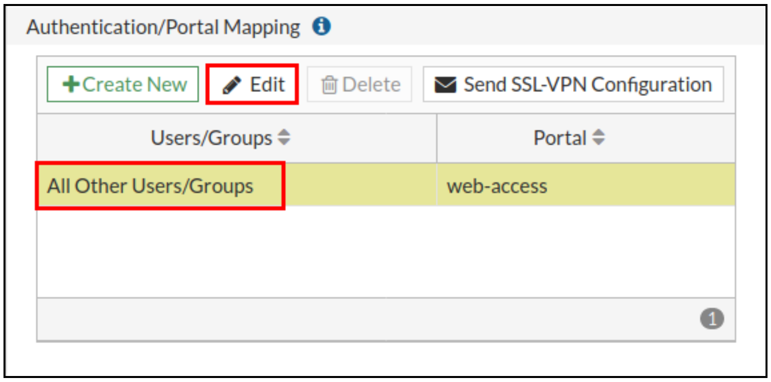
Add Tunnel Mode

You will change the SSL VPN portal mapping settings to use **tunnel-access**, to allow connections in tunnel mode only.

The **full-access** setting available on FortiGate supports both web and tunnel modes.

To add tunnel mode

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **SSL-VPN Settings**.
3. In the **Authentication/Portal Mapping** section, select **All Other Users/Groups**, and then click **Edit**.



Users/Groups	Portal
All Other Users/Groups	web-access

4. In the **Portal** drop-down list, select **tunnel-access**, and then click **OK**.
5. Click **Apply**.

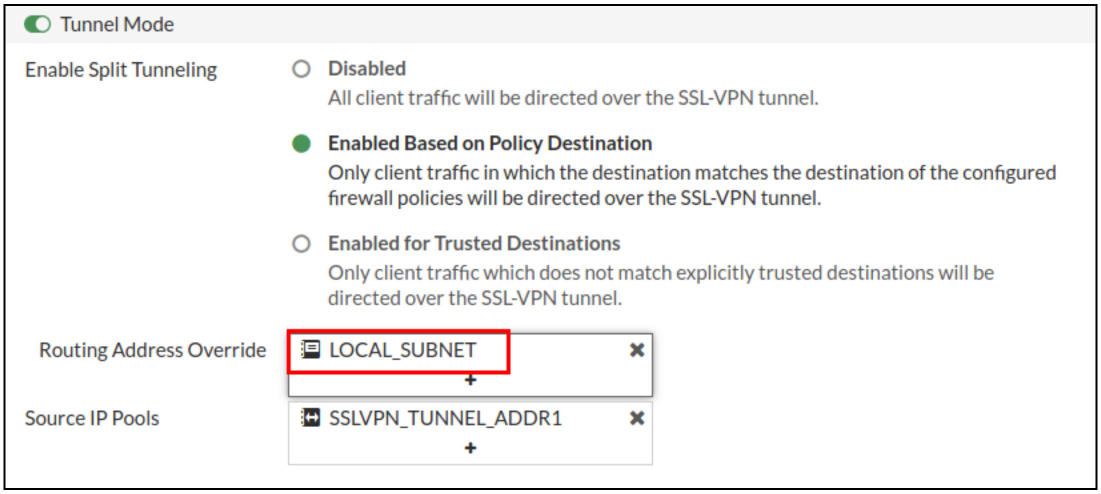
Configure the Routing for Tunnel Mode

You will establish the routing address to use in tunnel mode.

Notice that in tunnel mode, FortiClient establishes one or more routes in the SSL VPN user's host after the tunnel is connected. Traffic destined to the internal subnets is correctly routed through the tunnel.

To configure the routing for tunnel mode

1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Portals**.
2. Select the **tunnel-access** portal, and then click **Edit**.
3. In the **Tunnel Mode** section, set the **Routing Address Override** to **LOCAL_SUBNET**.



Tunnel Mode

Enable Split Tunneling

○ Disabled
All client traffic will be directed over the SSL-VPN tunnel.

● Enabled Based on Policy Destination
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

○ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override: LOCAL_SUBNET

Source IP Pools: SSLVPN_TUNNEL_ADDR1

4. Click **OK**.

Configure FortiClient for SSL VPN Connections

SSL VPN connections in tunnel mode require FortiClient. You will use FortiClient, which is installed on the Remote-Client VM, to test your configuration.

To configure FortiClient for SSL VPN

1. Connect to the Remote-Client VM.
2. Click **Desktop** > **forticlientsslvpn** > **64bit**, and then double-click **forticlientsslvpn** to configure SSL VPN client settings.
3. Configure the following settings for the FortiClient SSLVPN application:

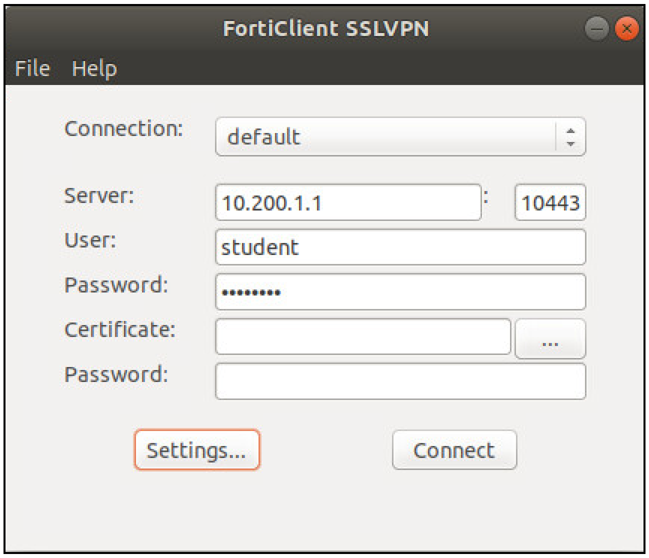
Field	Value
Server	10.200.1.1
Customize port	10443

Test SSL VPN in Tunnel Mode

You will connect using the student account to test tunnel mode.

To connect in tunnel mode

1. Continuing on the FortiClient SSLVPN application, in the **User** field, type `student`, and in the **Password** field, type `fortinet`.



Connection: default

Server: 10.200.1.1 : 10443

User: student

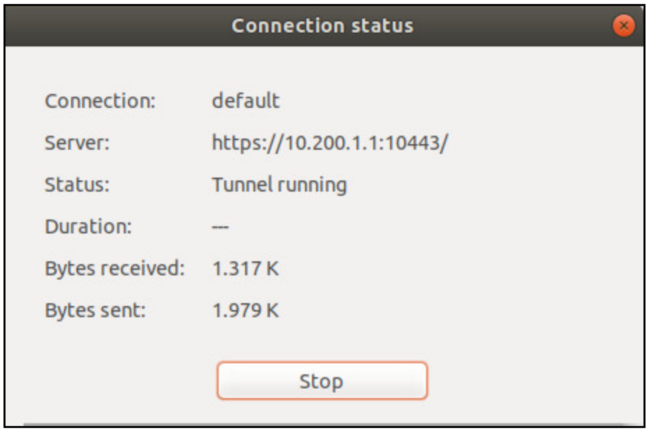
Password: ••••••••

Certificate:

Password:

2. Click **Connect**.
3. Click **Continue** to accept the certificate.

   The tunnel is connected.



Connection: default

Server: https://10.200.1.1:10443/

Status: Tunnel running

Duration: ---

Bytes received: 1.317 K

Bytes sent: 1.979 K

To test the tunnel

1. Continuing on the Remote-Client VM, open Firefox, and then access the following URL:

   `http://10.0.1.10`
2. Look at the URL.

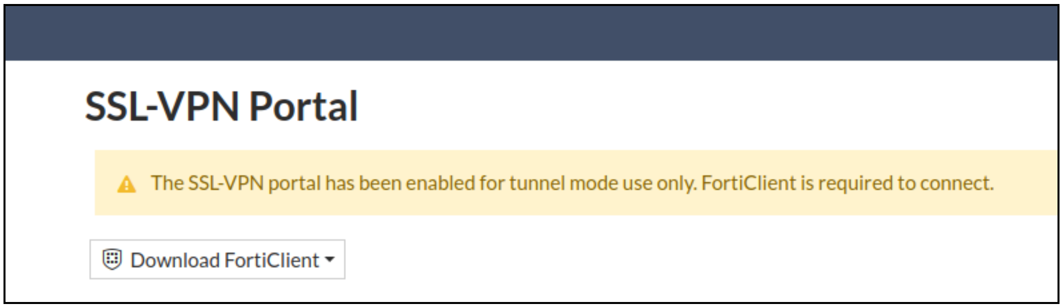
   You are connected to the web server URL as if you were based in the local subnet (`10.0.1.0/24`).

This time, you are not using the reverse HTTP proxy as in the case of web-access mode. The IP traffic is directly encapsulated over HTTPS and sent through the tunnel.

3. Return to FortiClient, and then click **Stop**.

To attempt SSL VPN access by web mode

1. Continuing on the Remote-Client VM, open a web browser, and then log in to the SSL VPN portal at `https://10.200.1.1:10443/` with the username `student` and password `fortinet`.
2. After you log in to the SSL VPN connection, FortiGate displays the following warning message:



SSL-VPN Portal

The SSL-VPN portal has been enabled for tunnel mode use only. FortiClient is required to connect.

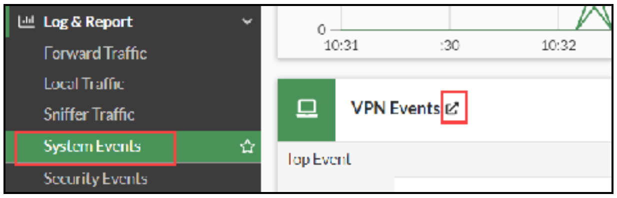
3. Click **student** > **Logout** to log out of the SSL VPN portal.

Review VPN Events

You will review the VPN events for both of the SSL VPN connections you performed in this lab (web and tunnel modes).

To review VPN events for SSL VPN connections

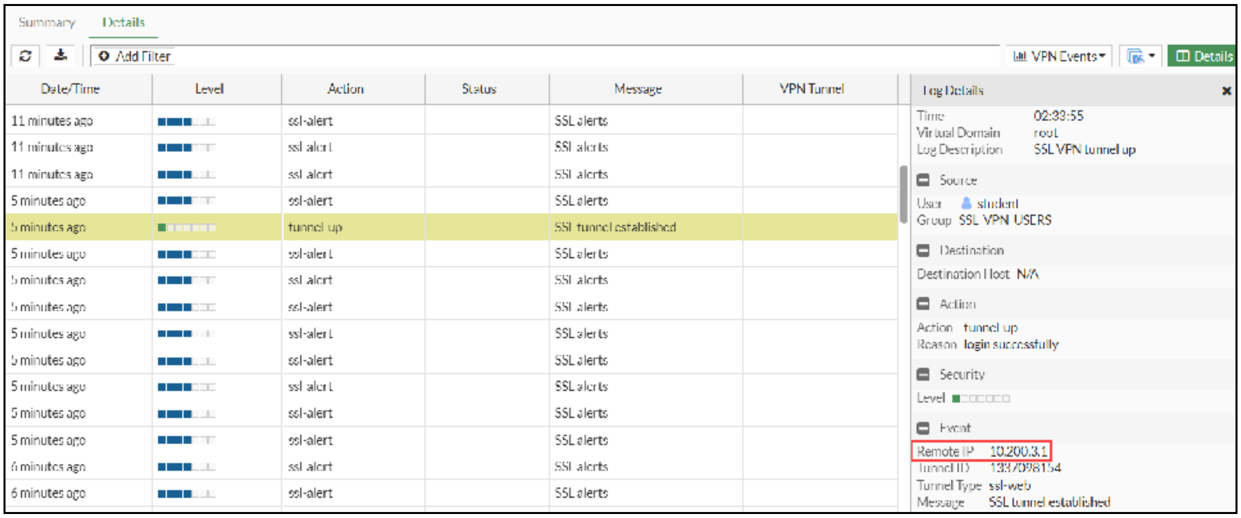
1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Log & Report** > **System Events**, and then click **View Logs** arrow button on the **VPN Events**widget.



3. Compare the log details of the **tunnel-up** logs you see.

   Hint: Use your log filters to filter on **Action** = **tunnel-up**.

   The most recent **tunnel-up** log shows one IP address under **Remote IP**. This log shows the recent connection to the SSL VPN portal. Even though the SSL VPN portal presented a warning message and did not allow remote access to the local resources, FortiGate shows that an SSL VPN connection was established and the tunnel was up.



Date/Time	Level	Action	Status	Message	VPN Tunnel
11 minutes ago	■■■□□	ssl-alert		SSL alerts	
11 minutes ago	■■■□□	ssl-alert		SSL alerts	
11 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■□□□□□	tunnel-up		SSL tunnel established	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
5 minutes ago	■■■□□	ssl-alert		SSL alerts	
6 minutes ago	■■■□□	ssl-alert		SSL alerts	
6 minutes ago	■■■□□	ssl-alert		SSL alerts	

Log Details

Time 02:33:55
Virtual Domain root
Log Description SSL VPN tunnel up

Source
User student
Group SSL VPN USERS

Destination
Destination Host N/A

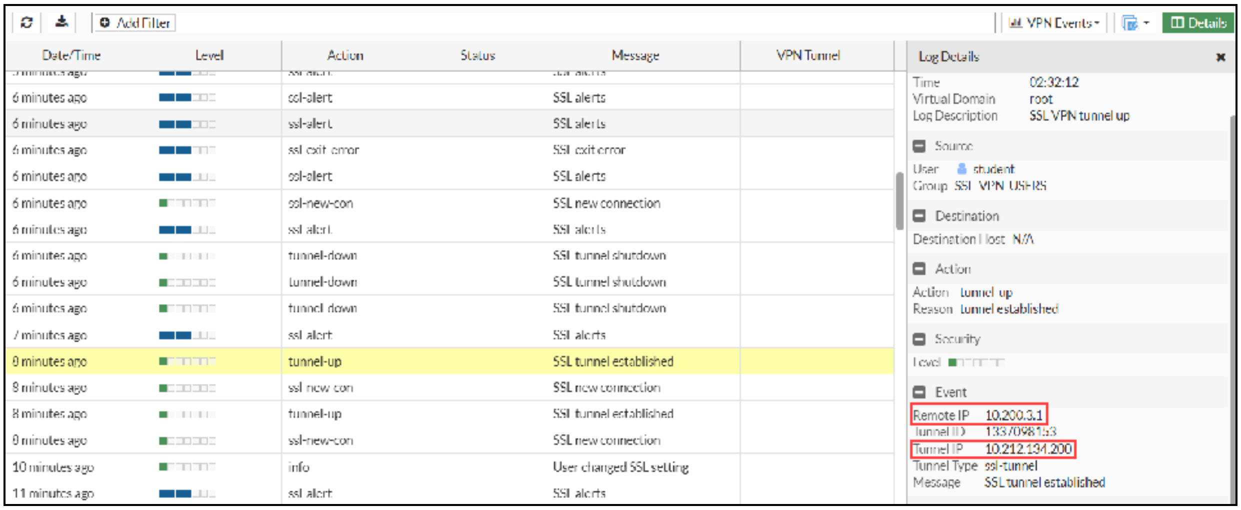
Action
Action tunnel-up
Reason login successfully

Security
Level ■□□□□□

Event
Remote IP 10.200.3.1
Tunnel ID 1337098154
Tunnel Type ssl-web
Message SSL tunnel established

The second most recent **tunnel-up** log in the VPN event list shows the SSL VPN connection in tunnel mode through FortiClient. Notice this log presents two IP addresses:

- **Remote IP**: IP address of the remote user's gateway (egress interface)
- **Tunnel IP**: IP address FortiGate assigns to the virtual network adapter `fortissl`



Date/Time	Level	Action	Status	Message	VPN Tunnel
6 minutes ago	■■■□□	ssl-alert		SSL alerts	
6 minutes ago	■■■□□	ssl-alert		SSL alerts	
6 minutes ago	■■■□□	ssl-exit-error		SSL exit error	
6 minutes ago	■■■□□	ssl-alert		SSL alerts	
6 minutes ago	■□□□□□	ssl-new-con		SSL new connection	
6 minutes ago	■■■□□	ssl-alert		SSL alerts	
6 minutes ago	■□□□□□	tunnel-down		SSL tunnel shutdown	
6 minutes ago	■□□□□□	tunnel-down		SSL tunnel shutdown	
6 minutes ago	■□□□□□	tunnel-down		SSL tunnel shutdown	
7 minutes ago	■■■□□	ssl-alert		SSL alerts	
8 minutes ago	■□□□□□	tunnel-up		SSL tunnel established	
8 minutes ago	■□□□□□	ssl-new-con		SSL new connection	
8 minutes ago	■□□□□□	tunnel-up		SSL tunnel established	
8 minutes ago	■□□□□□	ssl-new-con		SSL new connection	
10 minutes ago	■□□□□□	info		User changed SSL setting	
11 minutes ago	■■■□□	ssl-alert		SSL alerts	

Log Details

Time 02:32:12
Virtual Domain root
Log Description SSL VPN tunnel up

Source
User student
Group SSL VPN USERS

Destination
Destination Host N/A

Action
Action tunnel-up
Reason tunnel established

Security
Level ■□□□□□

Event
Remote IP 10.200.3.1
Tunnel ID 1337098153
Tunnel IP 10.212.134.200
Tunnel Type ssl-tunnel
Message SSL tunnel established

Stop and think!

Aside from SSL VPN connections in web mode showing one IP address and in tunnel mode showing two IP addresses, which other indicator shows how SSL VPN users are connected?

Notice the following **Tunnel Type** indicators in the log details shown in the previous step:

- **ssl-web** is for web mode
- **ssl-tunnel** is for tunnel mode

Lab 6: IPsec VPN Configuration

In this lab, you will configure site-to-site IPsec VPN tunnels between two FortiGate devices. First, you will configure a dial-up tunnel, and then a static tunnel. Then, you will add a second VPN tunnel that will act as a backup tunnel between the FortiGate devices.

Objectives

- Deploy a site-to-site VPN between two FortiGate devices
- Set up dial-up and static remote gateways
- Configure redundant VPNs between two FortiGate devices

Time to Complete

Estimated: 50 minutes

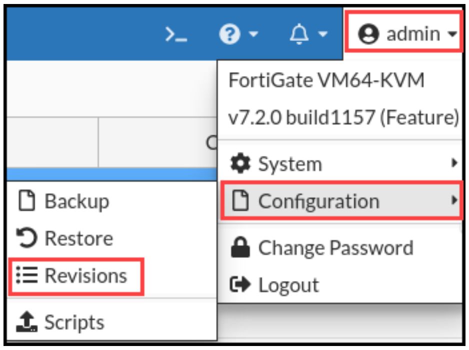
Prerequisites

Before beginning this lab, you must restore a configuration file to Remote-FortiGate and Local-FortiGate.

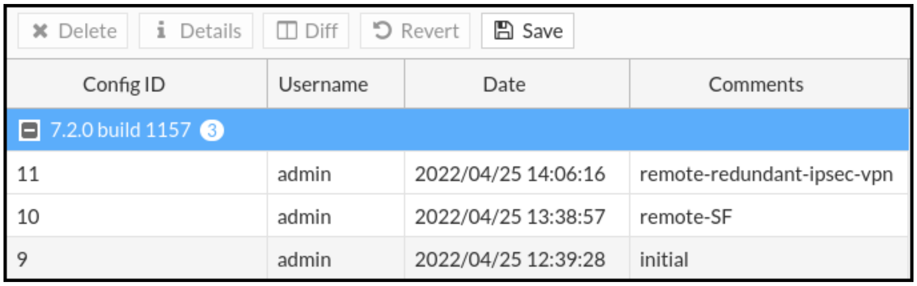
Make sure that you restore the correct configuration on each FortiGate, using the following steps. Failure to restore the correct configuration on each FortiGate will prevent you from doing the lab exercises.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.

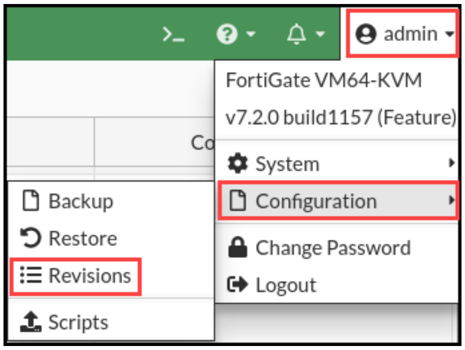


Config ID	Username	Date	Comments
7.2.0 build 1157 (3)			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

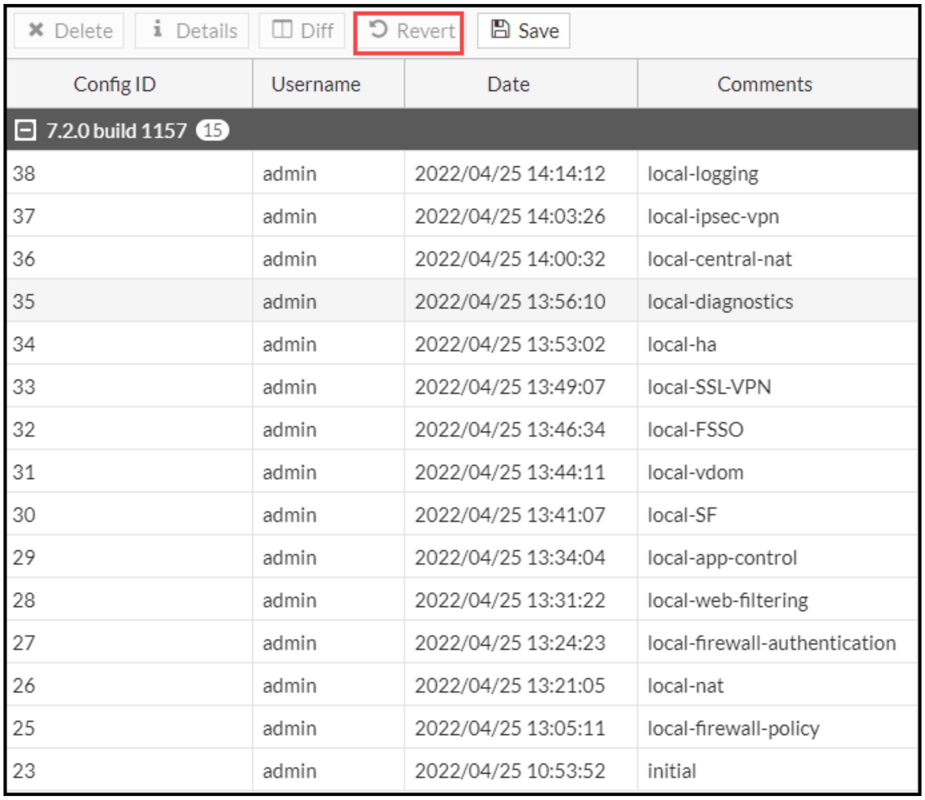
5. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Configuring a Dial-Up IPsec VPN Between Two FortiGate Devices

In this exercise, you will configure a dial-up VPN between Local-FortiGate and Remote-FortiGate. Local-FortiGate will act as the dial-up server and Remote-FortiGate will act as the dial-up client.

Create Phase 1 and Phase 2 on Local-FortiGate (Dial-Up Server)

You will configure the IPsec VPN by creating phase 1 and phase 2.

To create phase 1 and phase 2

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
3. Configure the following settings:

Field	Value
Name	ToRemote
Template type	Custom

4. Click **Next.**
5. In the **Network** section, configure the following settings:

Field	Value
Remote Gateway	Dialup User
Interface	port1
Dead Peer Detection	On Idle

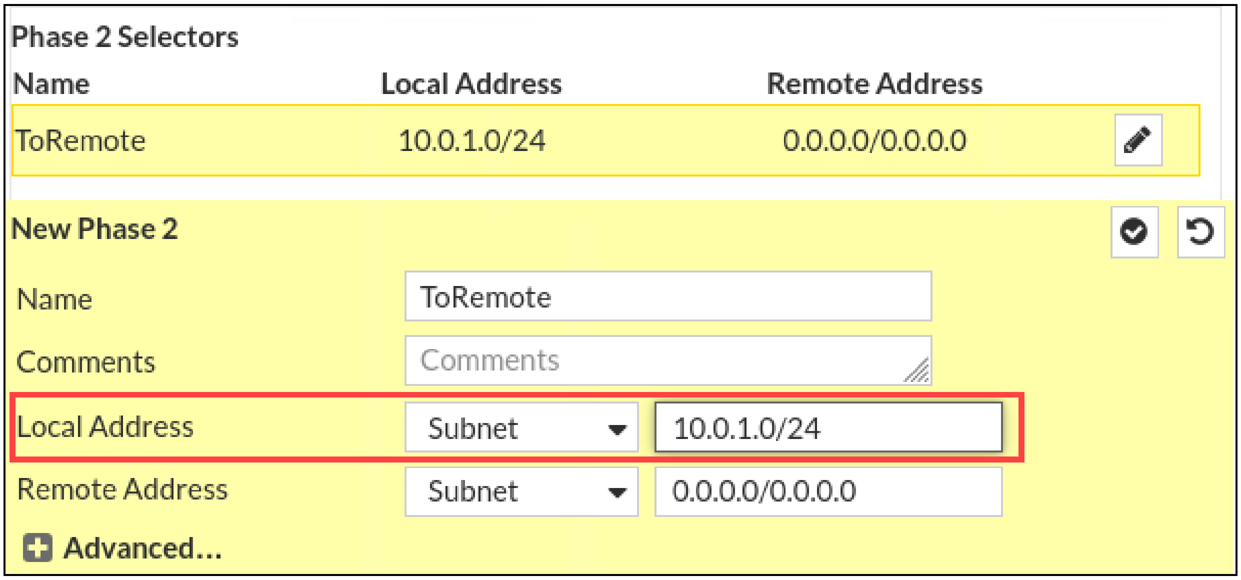
6. In the **Authentication** section, configure the following settings:

Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Mode	Aggressive
Accept Types	Specific peer ID
Peer ID	Remote-FortiGate

Setting a peer ID is useful when there are multiple dial-up tunnels on the FortiGate acting as the dial-up server, and you want dial-up clients to connect to a specific tunnel.

7. In the **Phase 2 Selectors** section, configure the following setting:

Field	Value
Local Address	10.0.1.0/24



Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	10.0.1.0/24	0.0.0.0/0.0.0.0

New Phase 2

Name: ToRemote

Comments: Comments

Local Address: Subnet 10.0.1.0/24

Remote Address: Subnet 0.0.0.0/0.0.0.0

8. Keep the default values for the remaining settings.
9. Click **OK**.

- You do not need to add a static route because it is a dial-up VPN. FortiGate dynamically adds or removes appropriate routes to each dial-up peer, each time the peer VPN is trying to connect.
- Even though you could have configured `10.0.2.0/24` as the **Remote Address** instead of `0.0.0.0/0`, it is more convenient to use the latter for scalability purposes. That is, when you have multiple remote peers, each with different remote subnets, using `0.0.0.0/0` as the remote subnet results in the dial-up server accepting any subnet during the tunnel negotiation. This allows multiple remote peers to use the same phase 2 selector configuration. For this exercise, there is only one remote peer (Remote-FortiGate). Local-FortiGate then learns about the remote subnet `10.0.2.0/24` when Remote-FortiGate connects to the tunnel. However, if there are more remote peers with different remote subnets, you do not need to change the existing dial-up server configuration for the additional remote peers to be able to connect.

Create Firewall Policies for VPN Traffic on Local-FortiGate (Dial-Up Server)

You will create two firewall policies between **port3** and **To Remote**—one for each traffic direction.

To create firewall policies for VPN traffic

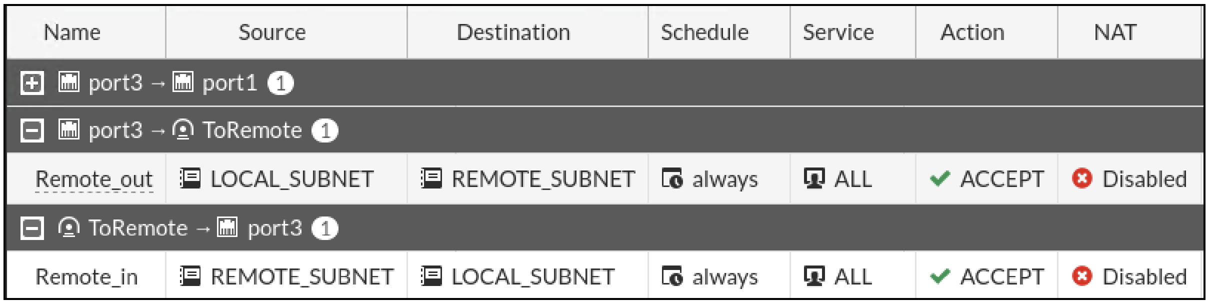
1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Remote_out
Incoming Interface	port3
Outgoing Interface	ToRemote
Source	LOCAL_SUBNET
Destination	REMOTE_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. Click **OK**.
6. Click **Create New** again.
7. Configure the following settings:

Field	Value
Name	Remote_in
Incoming Interface	ToRemote
Outgoing Interface	port3
Source	REMOTE_SUBNET
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

8. In the **Firewall/Network Options** section, disable **NAT**.
9. Click **OK**.



Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port3 → port1 1						
⊟ port3 → ToRemote 1						
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	✖ Disabled
⊟ ToRemote → port3 1						
Remote_in	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	✖ Disabled

Create Phase 1 and Phase 2 on Remote-FortiGate (Dial-Up Client)

You will create phase 1 and phase 2 on Remote-FortiGate.

To create phase 1 and phase 2

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
3. Configure the following settings:

Field	Value
Name	ToLocal
Template type	Custom

4. Click **Next**.
5. In the **Network** section, configure the following settings:

Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.1.1
Interface	port4
Dead Peer Detection	On Idle

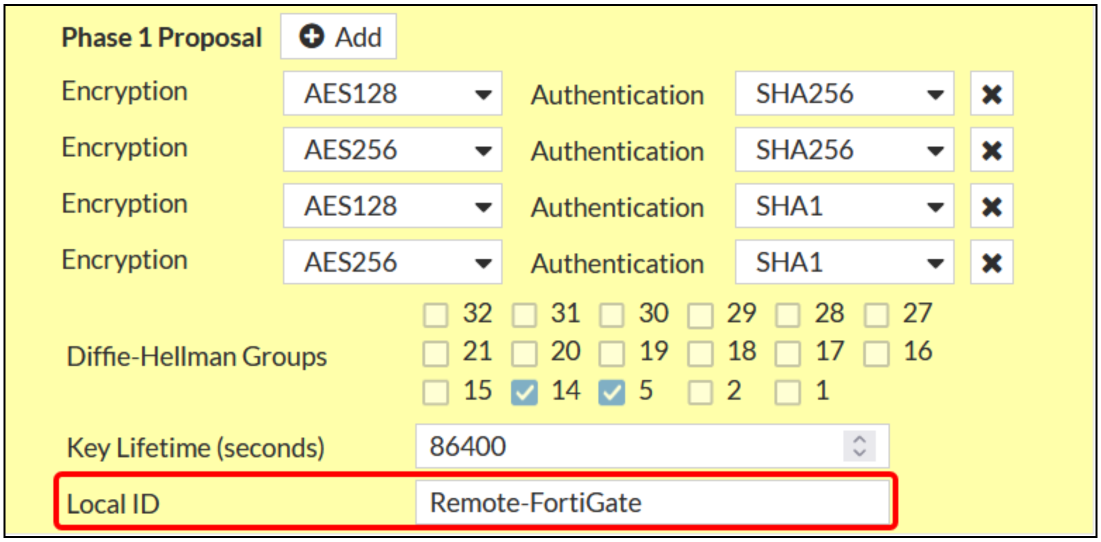
6. In the **Authentication** section, configure the following settings:

Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet

Field	Value
Mode	Aggressive
Accept Types	Any peer ID

7. In the **Phase 1 Proposal** section, configure the following settings:

Field	Value
Local ID	Remote-FortiGate



Phase 1 Proposal ⊕ Add

Encryption	AES128	Authentication	SHA256	✖
Encryption	AES256	Authentication	SHA256	✖
Encryption	AES128	Authentication	SHA1	✖
Encryption	AES256	Authentication	SHA1	✖

Diffie-Hellman Groups
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 ☑ 14 ☑ 5 □ 2 □ 1

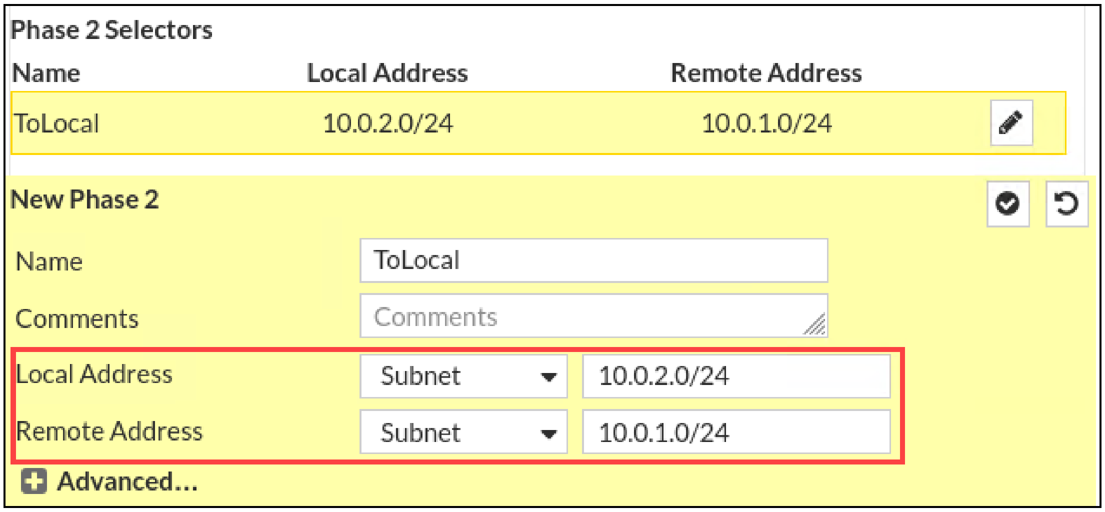
Key Lifetime (seconds) 86400

Local ID Remote-FortiGate

The local ID should be the same as the peer ID that you configured on Local-FortiGate, which is acting as the dial-up server.

8. In the **Phase 2 Selectors** section, configure the following settings:

Field	Value
Local Address	10.0.2.0/24
Remote Address	10.0.1.0/24



Phase 2 Selectors

Name	Local Address	Remote Address
ToLocal	10.0.2.0/24	10.0.1.0/24

New Phase 2

Name: ToLocal

Comments: Comments

Local Address: Subnet 10.0.2.0/24

Remote Address: Subnet 10.0.1.0/24

9. Keep the default values for the remaining settings.
10. Click **OK**.

Except for **Local Address** and **Remote Address**, all phase 1 and phase 2 settings on both VPN peers mirror each other. For dial-up IPsec VPN, the local and remote addresses do not have to mirror for the tunnel to come up.

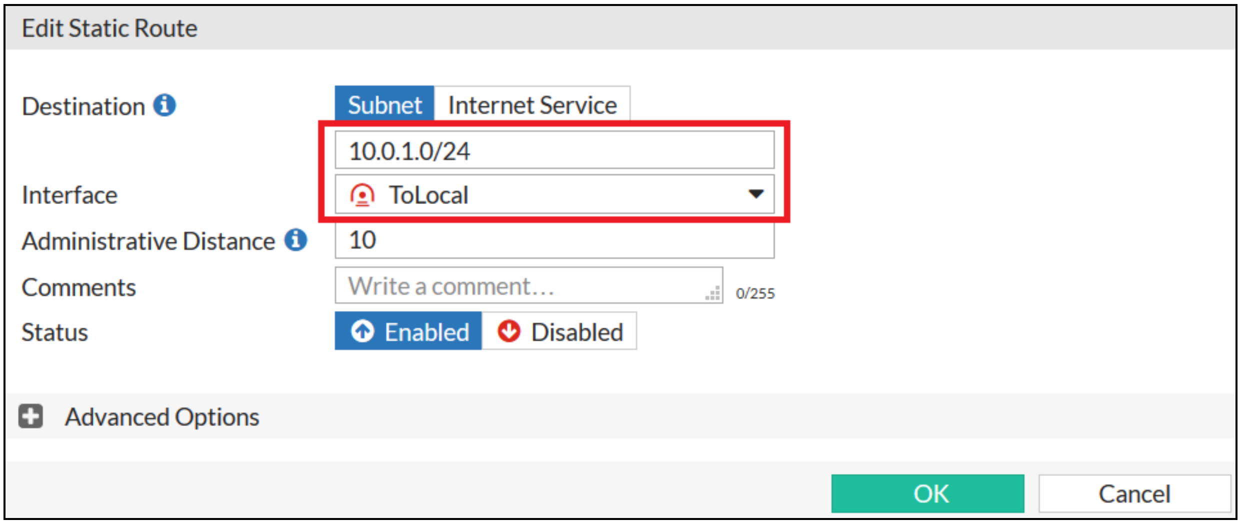
Create a Static Route for VPN Traffic on Remote-FortiGate (Dial-Up Client)

You will create one static route on Remote-FortiGate. This step was not necessary on Local-FortiGate because, as the dial-up server, it automatically adds the route for the remote network after the tunnel comes up.

To create a static route for VPN traffic on Remote-FortiGate

1. On the Remote-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Destination	Subnet 10.0.1.0/24
Interface	ToLocal



Destination: 10.0.1.0/24

Interface: ToLocal

Administrative Distance: 10

Comments:

Status: Enabled

4. Click **OK**.

Create the Firewall Policies for VPN Traffic on Remote-FortiGate (Dial-Up Client)

You will create two firewall policies between **port6** and **To Local**—one for each traffic direction.

To create firewall policies for VPN traffic

1. On the Remote-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**.
3. Configure the following settings:

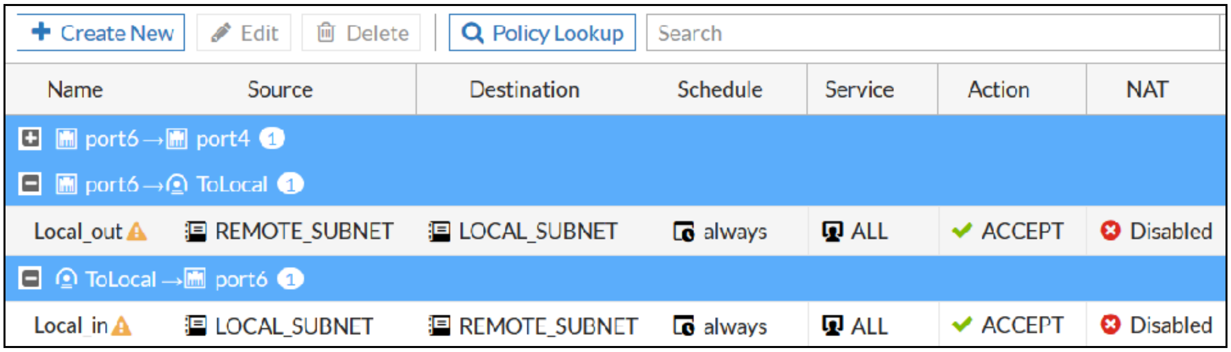
Field	Value
Name	Local_out
Incoming Interface	port6
Outgoing Interface	ToLocal
Source	REMOTE_SUBNET
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. Click **OK**.

6. Click **Create New** again.
7. Configure the following settings:

Field	Value
Name	Local_in
Incoming Interface	ToLocal
Outgoing Interface	port6
Source	LOCAL_SUBNET
Destination	REMOTE_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

8. In the **Firewall/Network Options** section, disable **NAT**.
9. Click **OK**.



Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port6 → port4 1						
⊟ port6 → ToLocal 1						
Local_out ⚠	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	Disabled
⊟ ToLocal → port6 1						
Local_in ⚠	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled

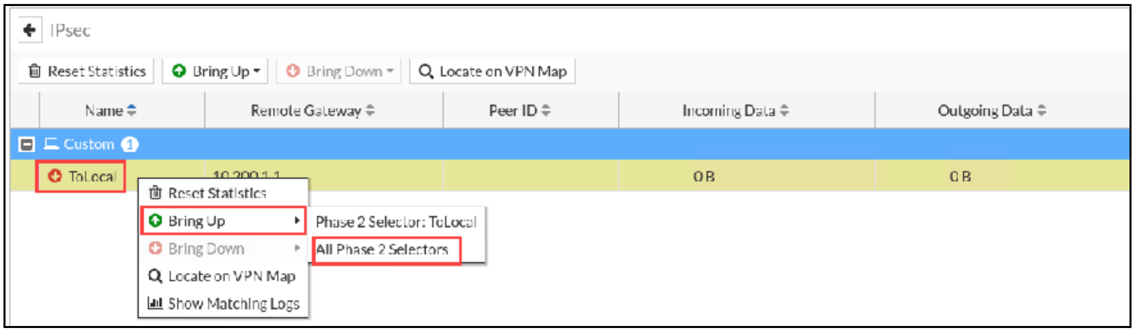
Test and Monitor the VPN

Now that you configured the VPN on both FortiGate devices, you will test the VPN.

To test the VPN

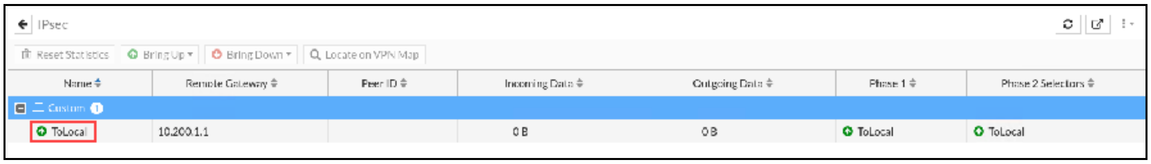
1. On the Remote-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
2. Click the **+** sign beside **Custom** to expand the custom VPN tunnel section.

   Notice that the **ToLocal** VPN is currently down.
3. Right-click the VPN, and then click **Bring Up** > **All Phase 2 Selectors** to bring up the tunnel.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
Custom 1				
ToLocal	10.200.1.1		0 B	0 B

The **Name** column of the VPN now contains a green up arrow, which indicates that the tunnel is up. If required, click the refresh button in the upper-right corner to refresh the widget information.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToLocal	10.200.1.1		0 B	0 B	ToLocal	ToLocal

Stop and think!

Do you always have to manually bring up the tunnel after you create it?

No. With the current configuration, the tunnel will stay down until you manually bring it up, or there is traffic that should be routed through the tunnel. Because you are not generating traffic between the `10.0.2.0/24` and `10.0.1.0/24` subnets yet, the tunnel is still down. If you had generated the required traffic while the tunnel was down, it would have come up automatically.

You can initiate a tunnel only from Remote-FortiGate because it is the dial-up client.

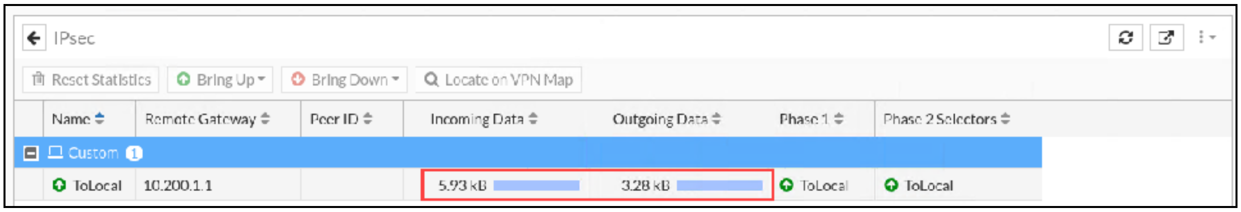
4. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

```
ping 10.0.1.10
```

The ping should work.

5. On the Remote-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
6. Click the refresh button in the upper-right corner multiple times to refresh the widget information.

You will notice that the counters for **Incoming Data** and **Outgoing Data** increase over time. This indicates that the traffic between `10.0.1.10` and `10.0.2.10` is being encrypted successfully and routed through the tunnel.



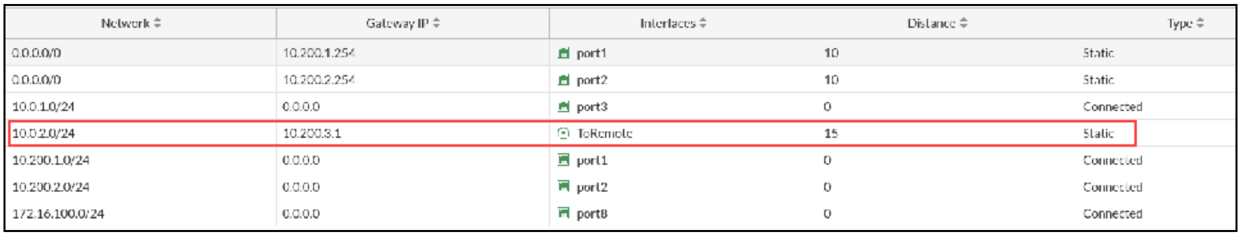
Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToLocal	10.200.1.1		5.93 kB	3.28 kB	ToLocal	ToLocal

7. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **Routing**.

Find the static route that was dynamically added to the FortiGate device.

8. View the route details.

Notice the address listed in the **Gateway IP** column for that route.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
0.0.0.0/0	10.200.2.254	port2	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.0.2.0/24	10.200.3.1	ToRemote	15	Static
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

9. On the Remote-Client VM, press `Ctrl+C` to stop the ping.

Exercise 2: Configuring a Static IPsec VPN Between Two FortiGate Devices

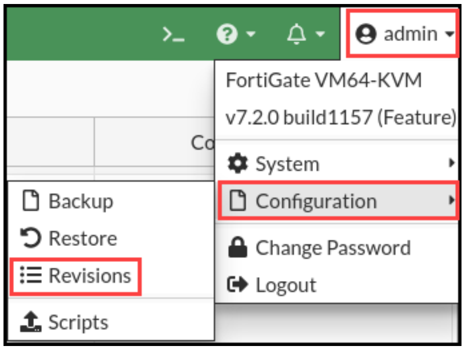
In this exercise, you will configure a static VPN between Local-FortiGate and Remote-FortiGate. You will also configure a static route on Local-FortiGate for VPN traffic.

Before beginning this lab, you must restore a configuration file to Local-FortiGate.

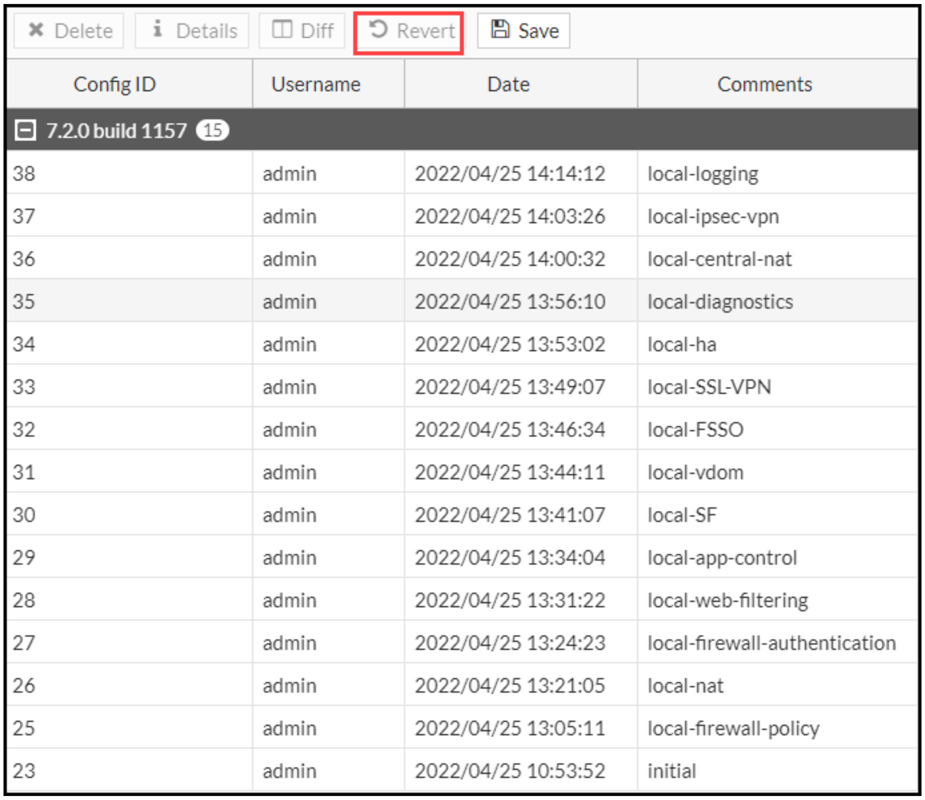
Make sure that you restore the correct configuration on Local-FortiGate, using the following steps. Failure to restore the correct configuration on Local-FortiGate will prevent you from doing the lab exercise.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-ipsec-vpn**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 (15)			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Create Phase 1 and Phase 2 on Local-FortiGate

You will configure the IPsec VPN by creating phase 1 and phase 2.

To create phase 1 and phase 2

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
3. Configure the following settings:

Field	Value
Name	ToRemote
Template type	Custom

4. Click **Next**.
5. In the **Network** section, configure the following settings:

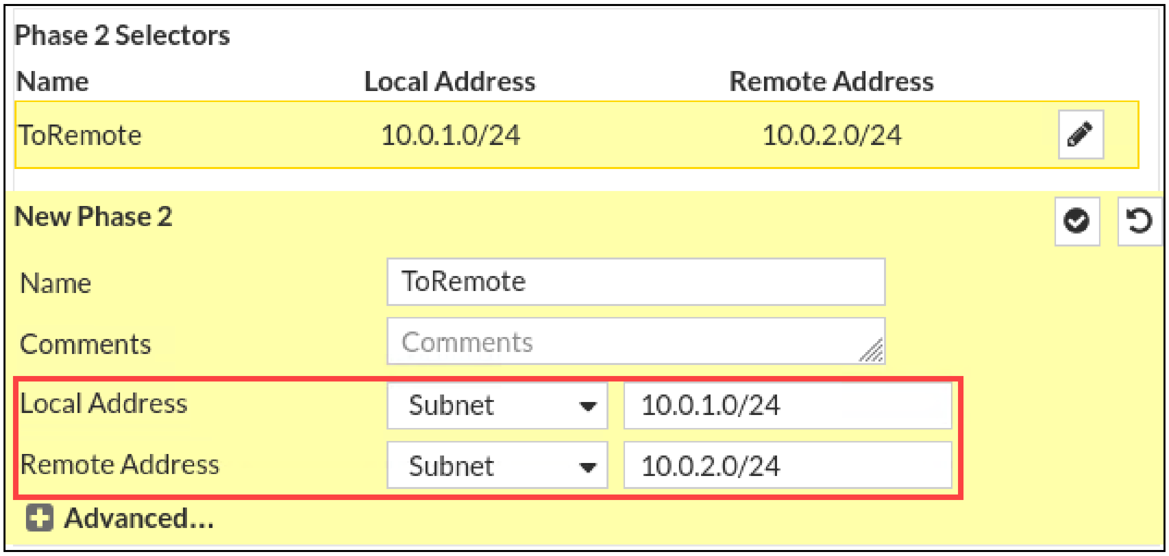
Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Interface	port1
Dead Peer Detection	On Idle

6. In the **Authentication** section, configure the following settings:

Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Mode	Aggressive
Accept Types	Any peer ID

7. In the **Phase 2 Selectors** section, configure the following settings:

Field	Value
Local Address	10.0.1.0/24
Remote Address	10.0.2.0/24



Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	10.0.1.0/24	10.0.2.0/24

New Phase 2

Name: ToRemote

Comments: Comments

Local Address: Subnet 10.0.1.0/24

Remote Address: Subnet 10.0.2.0/24

8. Keep the default values for the remaining settings.
9. Click **OK**.

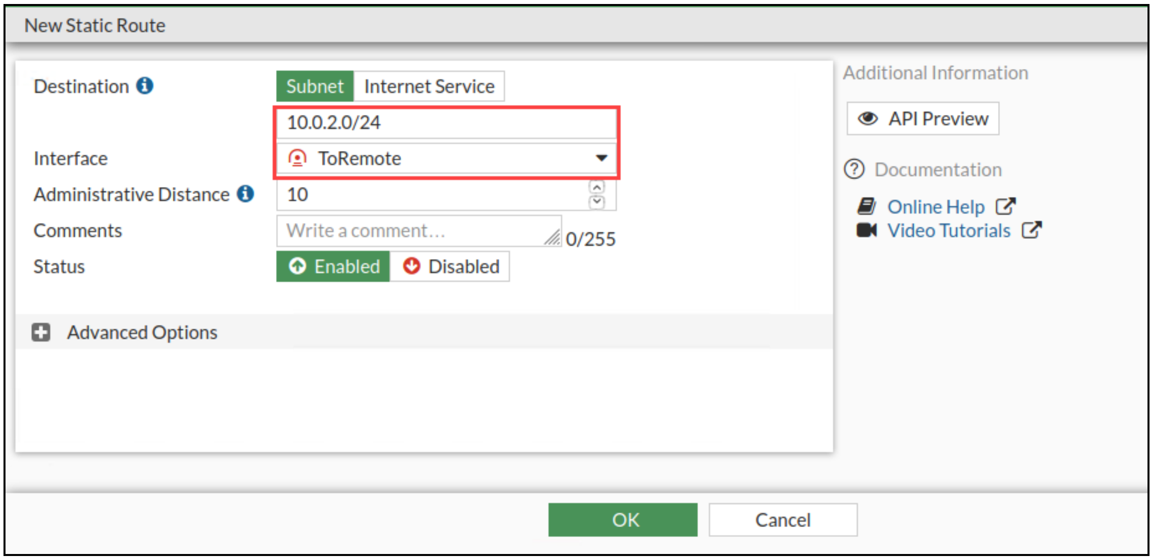
Create a Static Route for VPN Traffic on Local-FortiGate

You will create one static route on Local-FortiGate.

To create a static route for VPN traffic on Local-FortiGate

1. On the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Destination	Subnet 10.0.2.0/24
Interface	ToRemote



New Static Route

Destination: Subnet | Internet Service
10.0.2.0/24
Interface: ToRemote
Administrative Distance: 10
Comments: Write a comment... 0/255
Status: Enabled | Disabled

4. Click **OK**.

Create Firewall Policies for VPN Traffic on Local-FortiGate

You will create two firewall policies between **port3** and **ToRemote**—one for each traffic direction.

To create firewall policies for VPN traffic

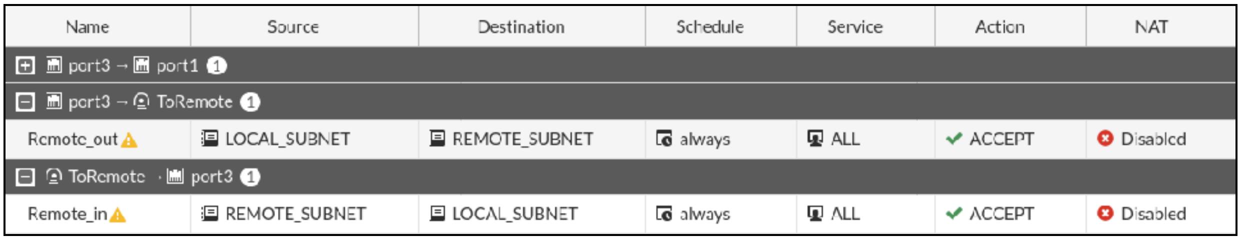
1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Remote_out
Incoming Interface	port3
Outgoing Interface	ToRemote
Source	LOCAL_SUBNET
Destination	REMOTE_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. Click **OK**.
6. Click **Create New** again.
7. Configure the following settings:

Field	Value
Name	Remote_in
Incoming Interface	ToRemote
Outgoing Interface	port3
Source	REMOTE_SUBNET
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

8. In the **Firewall/Network Options** section, disable **NAT**.
9. Click **OK**.



Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port3 → port1 1						
⊟ port3 → ToRemote 1						
Remote_out ⚠	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled
⊟ ToRemote → port3 1						
Remote_in ⚠	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	Disabled

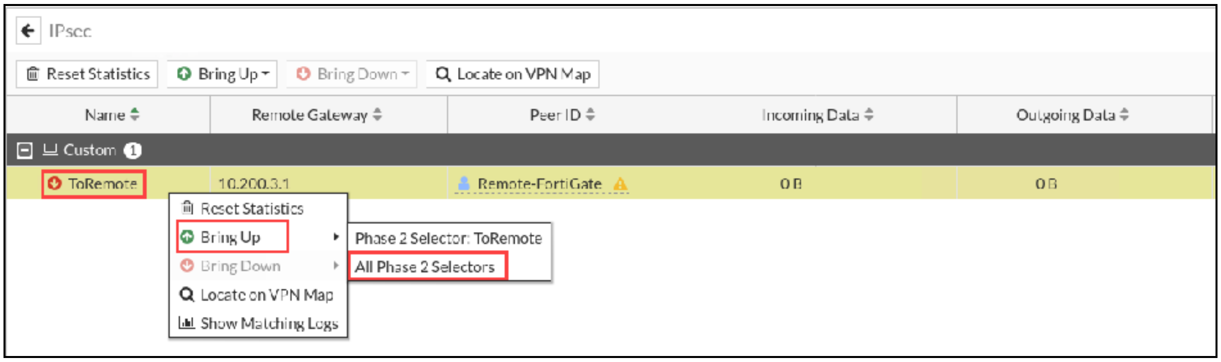
Test and Monitor the VPN

You will test the VPN and monitor its status.

To test the VPN

1. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
2. Click the **+** sign beside **Custom** to expand the custom VPN tunnel section.

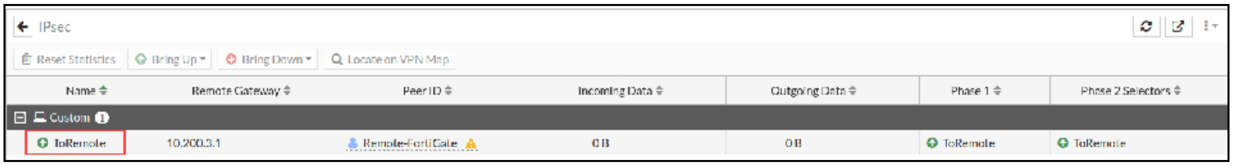
   Notice that the **ToRemote** VPN is currently down.
3. Right-click the VPN, and then click **Bring Up** > **All Phase 2 Selectors**.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
ToRemote	10.200.3.1	Remote-FortiGate	0 B	0 B

4. In the top-right corner, click the refresh button to refresh the widget information.

   The **Name** column of the VPN now contains a green up arrow, which indicates that the tunnel is up.



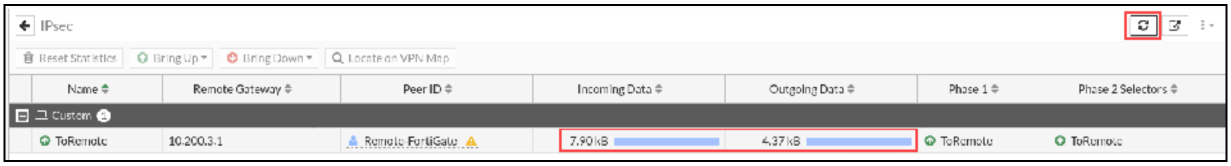
Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
ToRemote	10.200.3.1	Remote-FortiGate	0 B	0 B	ToRemote	ToRemote

5. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

```
ping 10.0.1.10
```

   The ping should work.
6. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
7. In the upper-right corner, click the refresh button multiple times to refresh the widget information.

   You will notice that the counters for **Incoming Data** and **Outgoing Data** increase over time. This indicates that the traffic between `10.0.1.10` and `10.0.2.10` is being encrypted successfully and routed through the tunnel.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
ToRemote	10.200.3.1	Remote-FortiGate	7.90 kB	4.37 kB	ToRemote	ToRemote

8. On the Remote-Client VM, press `Ctrl`+`C` to stop the ping.

Exercise 3: Configuring Redundant Static IPsec VPN Tunnels Between Two FortiGate Devices

In this exercise, you will configure one more VPN tunnel between Local-FortiGate and Remote-FortiGate for redundancy purposes. You must first restore a configuration file on Remote-FortiGate.

Prerequisites

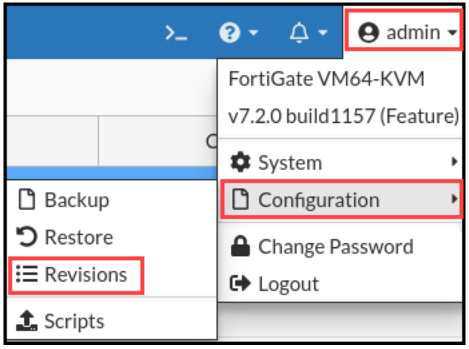
Before beginning this exercise, you must restore a configuration file on Remote-FortiGate.

Make sure that you restore the correct configuration on Remote-FortiGate, using the following steps. Failure to restore the correct configuration on Remote-FortiGate will prevent you from doing the lab exercise.

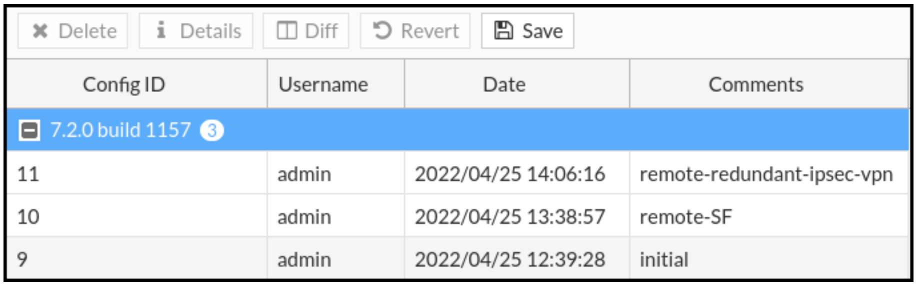
After you load the configurations, Remote-FortiGate will be preconfigured for VPN redundancy. This exercise provides instructions to review the configuration for Remote-FortiGate.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **remote-redundant-ipsec-vpn**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 (3)			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

5. Click **OK** to reboot.

Check the IPsec VPN Tunnel on Local-FortiGate

You just restored a configuration file to Remote-FortiGate. You will now check the status of the **ToRemote** VPN on Local-FortiGate.

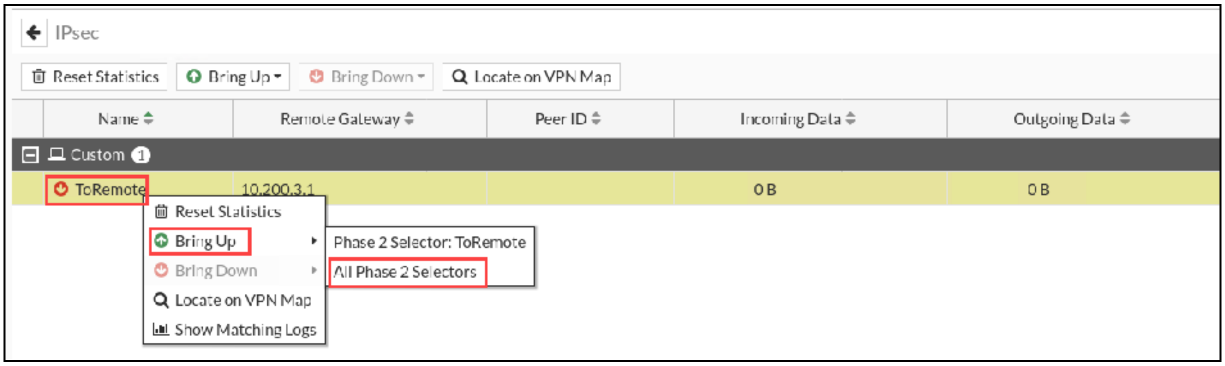
To check the VPN on Local-FortiGate

1. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
2. Click the **+** sign beside **Custom** to expand the custom VPN tunnel section.

   Notice that the **ToRemote** VPN is currently down.

If the **ToRemote** VPN still appears up, wait a few more seconds, and then press `Ctrl+R` to refresh the page. The tunnel will be brought down automatically by dead peer detection (DPD) approximately 60 seconds after the configuration is restored on Remote-FortiGate.

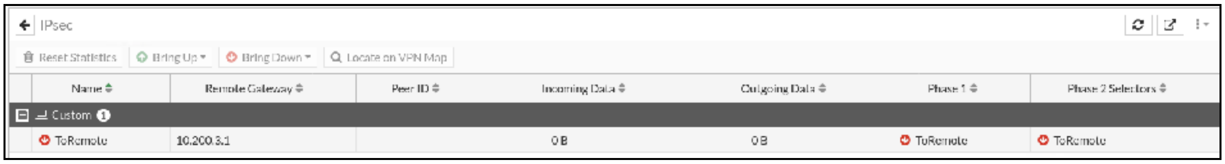
3. Right-click the VPN, and then click **Bring Up** > **All Phase 2 Selectors**.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
Custom 1				
ToRemote	10.200.3.1		0 B	0 B

4. In the upper-right corner, click the refresh button to refresh the widget information.

   The **Name** column of the VPN shows a red down arrow, indicating that the tunnel is still down.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToRemote	10.200.3.1		0 B	0 B	ToRemote	ToRemote

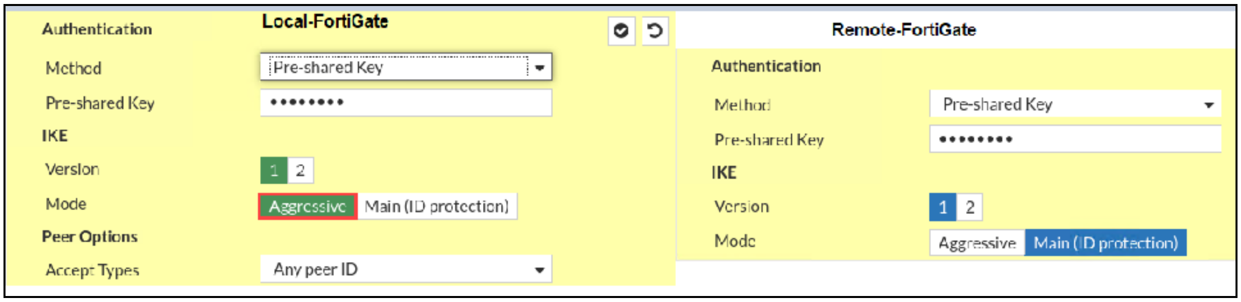
After you restore the configuration on Remote-FortiGate, the configuration for the tunnel on Remote-FortiGate no longer mirrors the configuration on Local-FortiGate, which is why the tunnel does not come up this time. You will fix this in the next procedure.

Review the VPN Configuration on Both FortiGate Devices

Phase 1 and phase 2 settings on both peers are no longer a mirror of each other. You will review the VPN configuration on each FortiGate and identify the differences. After that, you will apply the changes to the Local-FortiGate configuration so it mirrors the configuration on Remote-FortiGate.

To review the VPN configuration on both FortiGate devices

1. On the Local-FortiGate GUI, click **VPN** > **IPsec Tunnels**, and then double-click **ToRemote** to review the tunnel settings.
2. On the Remote-FortiGate GUI, click **VPN** > **IPsec Tunnels**, and then double-click **ToLocal** to review the tunnel settings.
3. Compare the settings in the **Authentication** section on each FortiGate.



Local-FortiGate

Authentication
Method: Pre-shared Key
Pre-shared Key: ••••••••
IKE
Version: 1 2
Mode: Aggressive | Main (ID protection)
Peer Options
Accept Types: Any peer ID

Remote-FortiGate

Authentication
Method: Pre-shared Key
Pre-shared Key: ••••••••
IKE
Version: 1 2
Mode: Aggressive | Main (ID protection)

Stop and think!

What are the differences in the VPN configuration between the two FortiGate devices?

Authentication

- Local-FortiGate uses aggressive mode for IKE, while Remote-FortiGate uses main mode.

To change the VPN configuration on Local-FortiGate

1. On the Local-FortiGate GUI, click **VPN** > **IPsec Tunnels**, and then double-click **ToRemote** to edit the tunnel settings.
2. Click the **Authentication** section, and then configure the following setting:

Field	Value
Mode	Main (ID protection)

3. Click **OK**.

Test and Monitor the VPN

Now that you fixed the VPN configuration on Local-FortiGate, you will test the VPN. Instead of bringing up the tunnel manually, you will generate traffic to bring the tunnel up.

To test the VPN

1. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

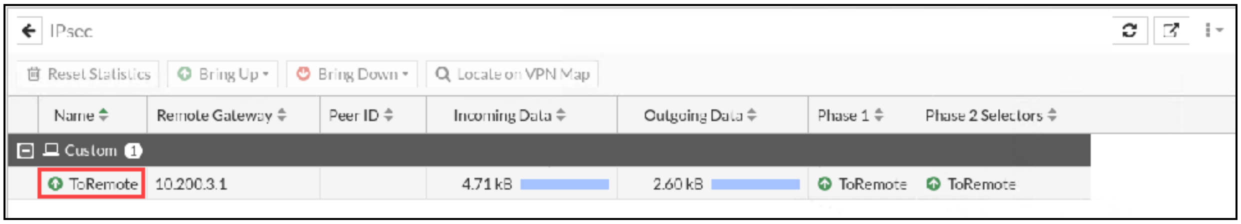
   ```
   ping 10.0.1.10
   ```

   The ping should work.

The first few pings will fail while FortiGate negotiates and establishes the VPN.

2. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
3. Click the **+** sign beside **Custom** to expand the custom VPN tunnel section.

   Notice that the **ToRemote** VPN is currently up.



IPsec

Reset Statistics | Bring Up | Bring Down | Locate on VPN Map

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToRemote	10.200.3.1		4.71 kB	2.60 kB	ToRemote	ToRemote

4. On the Remote-Client VM, press `Ctrl`+`C` to stop the ping.

Create a Backup VPN Tunnel Using the IPsec Wizard

You will configure a backup VPN tunnel on Local-FortiGate, named **ToRemoteBackup**, for redundancy purposes. To configure the new tunnel, you will use the IPsec wizard. On the Remote-FortiGate, the backup VPN tunnel was preconfigured and named **ToLocalBackup**.

To create a VPN using the IPsec wizard

1. On the Local-FortiGate GUI, click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
2. Configure the following settings:

Field	Value
Name	ToRemoteBackup
Template type	Site to Site
NAT configuration	No NAT between sites
Remote device type	FortiGate

3. Click **Next**.
4. Configure the following settings:

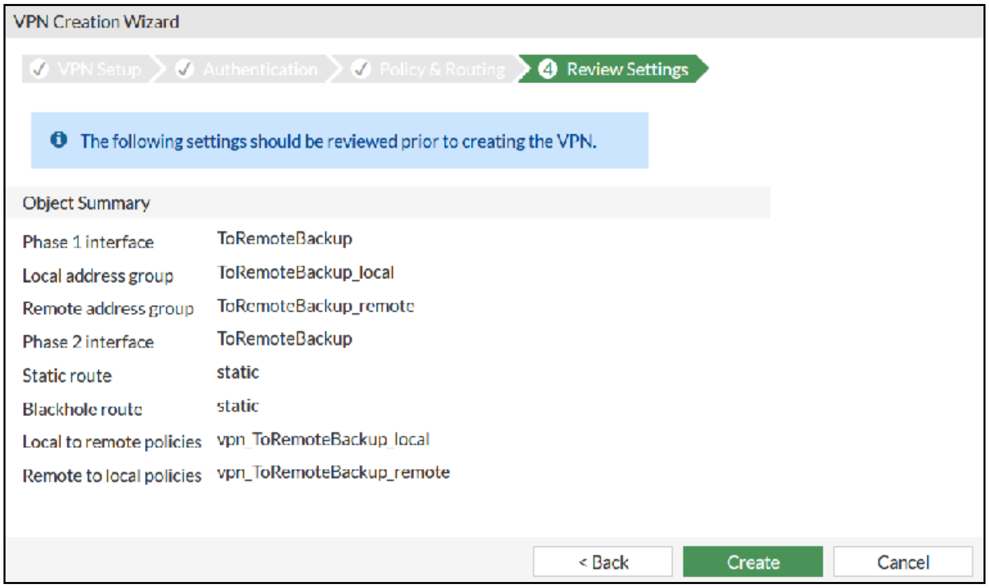
Field	Value
Remote device	IP Address
Remote IP address	10.200.4.1
Outgoing Interface	port2
Authentication method	Pre-shared Key
Pre-shared key	fortinet

5. Click **Next**.
6. Configure the following settings:

Field	Value
Local interface	port3
Local subnets	10.0.1.0/24
Remote Subnets	10.0.2.0/24
Internet Access	None

7. Click **Next**.
8. Click **Create**.

   You should see the following screen:



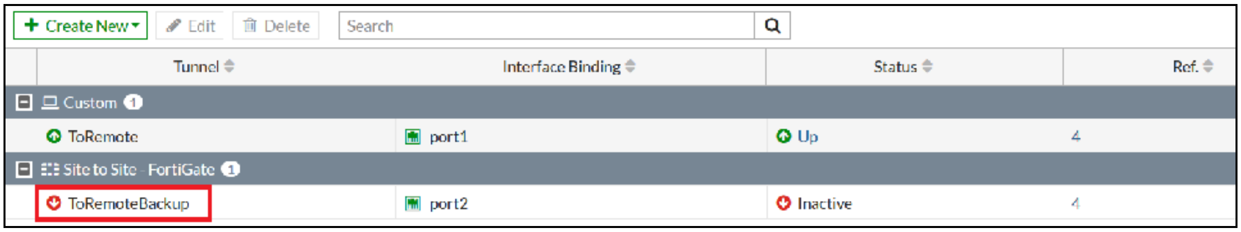
The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	ToRemoteBackup
Local address group	ToRemoteBackup_local
Remote address group	ToRemoteBackup_remote
Phase 2 interface	ToRemoteBackup
Static route	static
Blackhole route	static
Local to remote policies	vpn_ToRemoteBackup_local
Remote to local policies	vpn_ToRemoteBackup_remote

9. Click **Create** to create the new VPN tunnel.
10. Click **Show Tunnel List**, and then click the **+** sign beside **Site to Site - FortiGate** to expand the VPN tunnel section.

    You will see the VPN you just created.



Tunnel	Interface Binding	Status	Ref.
Custom 1			
ToRemote	port1	Up	4
Site to Site - FortiGate 1			
ToRemoteBackup	port2	Inactive	4

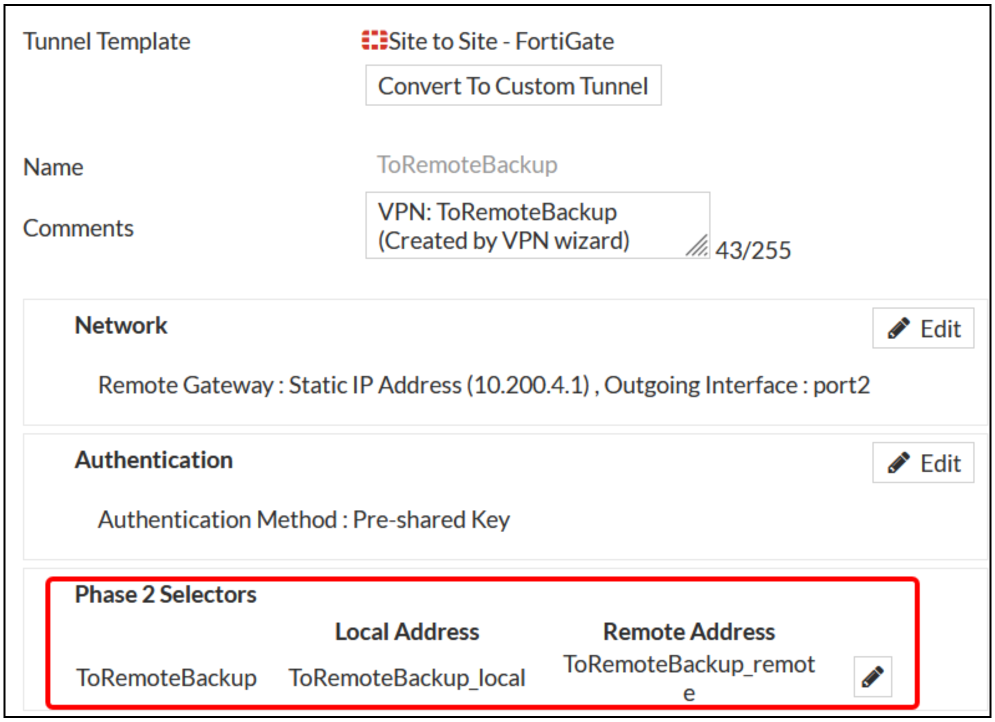
Review the Objects the IPsec Wizard Created

You will review the objects that the IPsec wizard created.

To review the objects the IPsec wizard created

1. On the Local-FortiGate GUI, click **VPN** > **IPsec Tunnels**, and then double-click **ToRemoteBackup** to review the tunnel settings.

   Notice the quick mode selectors that the wizard configured for you.



Tunnel Template: Site to Site - FortiGate

Name: ToRemoteBackup

Comments: VPN: ToRemoteBackup (Created by VPN wizard) 43/255

Network

Remote Gateway : Static IP Address (10.200.4.1) , Outgoing Interface : port2

Authentication

Authentication Method : Pre-shared Key

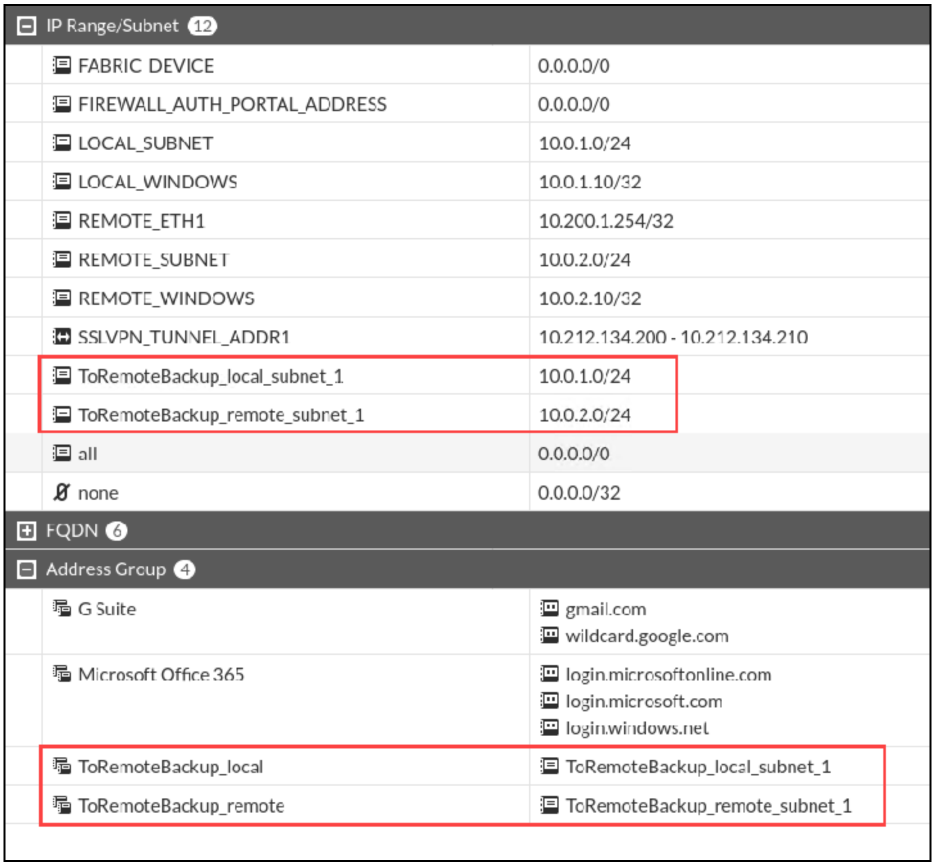
Phase 2 Selectors

	Local Address	Remote Address
ToRemoteBackup	ToRemoteBackup_local	ToRemoteBackup_remote

2. Click **Cancel**.
3. Click **Policy & Objects** > **Addresses**, and then click the **+** icon to expand **Address Group**.

   Observe the following new firewall address objects:

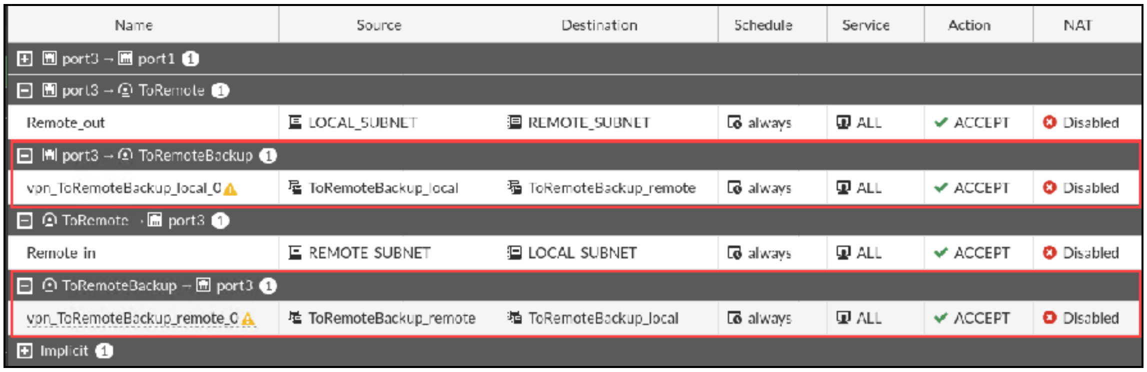
   - **ToRemoteBackup_local_subnet_1**, a member of the **ToRemoteBackup_local** address group
   - **ToRemoteBackup_remote_subnet_1**, a member of the **ToRemoteBackup_remote** address group



IP Range/Subnet 12	
FABRIC DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
LOCAL_SUBNET	10.0.1.0/24
LOCAL_WINDOWS	10.0.1.10/32
REMOTE_ETH1	10.200.1.254/32
REMOTE_SUBNET	10.0.2.0/24
REMOTE_WINDOWS	10.0.2.10/32
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
ToRemoteBackup_local_subnet_1	10.0.1.0/24
ToRemoteBackup_remote_subnet_1	10.0.2.0/24
all	0.0.0.0/0
none	0.0.0.0/32
FQDN 6	
Address Group 4	
G Suite	gmail.com wildcard.google.com
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net
ToRemoteBackup_local	ToRemoteBackup_local_subnet_1
ToRemoteBackup_remote	ToRemoteBackup_remote_subnet_1

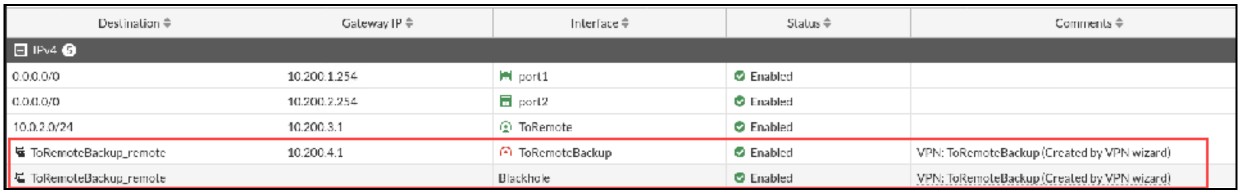
4. Click **Policy & Objects** > **Firewall Policy**.

   Observe the two new firewall policies: one from **port3** to **ToRemoteBackup** and another from **ToRemoteBackup** to **port3**. You will see that the **Action** in both cases is **ACCEPT**.



Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1						
port3 → ToRemote 1						
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled
port3 → ToRemoteBackup 1						
vpn_ToRemoteBackup_local_0 ⚠	ToRemoteBackup_local	ToRemoteBackup_remote	always	ALL	✓ ACCEPT	Disabled
ToRemote → port3 1						
Remote in	REMOTE SUBNET	LOCAL SUBNET	always	ALL	✓ ACCEPT	Disabled
ToRemoteBackup → port3 1						
vpn_ToRemoteBackup_remote_0 ⚠	ToRemoteBackup_remote	ToRemoteBackup_local	always	ALL	✓ ACCEPT	Disabled
Implicit 1						

5. Click **Network** > **Static Routes**, and then view the static route the wizard added.



Destination	Gateway IP	Interface	Status	Comments
IPv4 5				
0.0.0.0/0	10.200.1.254	port1	Enabled	
0.0.0.0/0	10.200.2.254	port2	Enabled	
10.0.2.0/24	10.200.3.1	ToRemote	Enabled	
ToRemoteBackup_remote	10.200.4.1	ToRemoteBackup	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)
ToRemoteBackup_remote		Blackhole	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)

Stop and think!

Why did the IPsec wizard add a second route using the blackhole interface?

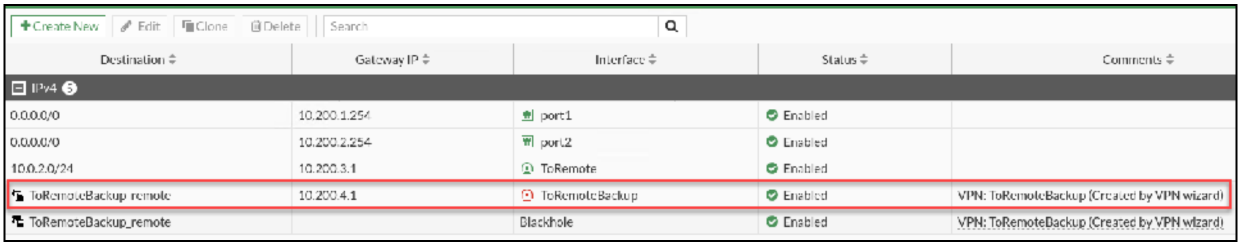
FortiGate drops all packets routed to the blackhole interface. The IPsec wizard added two static routes: one to the IPsec virtual interface, with a distance of 10, and one to the blackhole interface, with a distance of 254. The route with the lowest distance, the one to the IPsec virtual interface, takes precedence. However, if the VPN is down, the route to the blackhole interface becomes active, even though it was originally the route with the higher distance. So, traffic destined to the VPN is now routed to the blackhole interface and dropped. The route to the blackhole interface prevents FortiGate from sending VPN traffic to the default route while the VPN is down. The route to the blackhole interface also prevents FortiGate from creating unnecessary sessions in the session table.

Adjust Routing for the Backup VPN Tunnel on Local-FortiGate

You will increase the administrative distance of the static route the IPsec wizard created for the **ToRemoteBackup** VPN, so the tunnel is only used when the **ToRemote** VPN is down.

To configure a backup VPN on Local-FortiGate

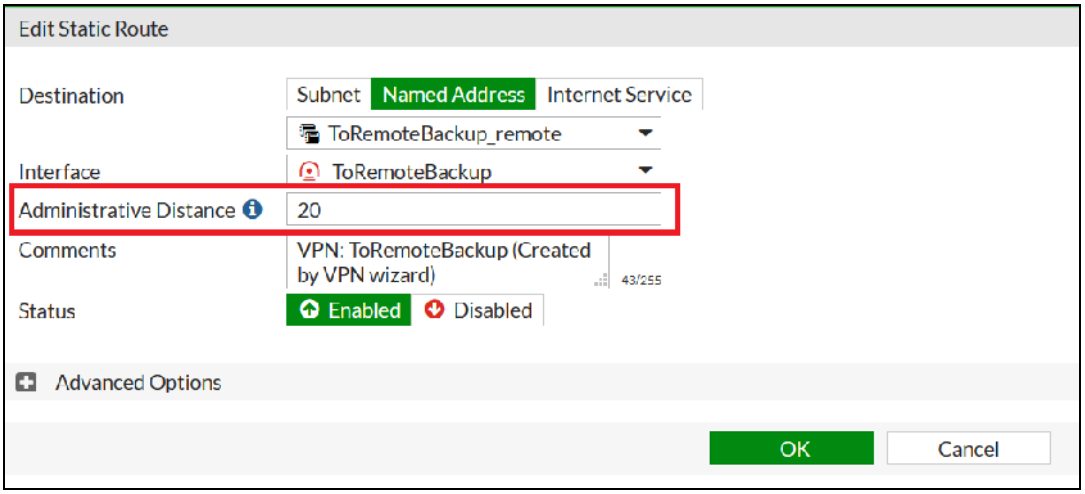
1. On the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Double-click the static route created for **ToRemoteBackup** to edit the settings.



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.200.1.254	port1	Enabled	
0.0.0.0/0	10.200.2.254	port2	Enabled	
10.0.2.0/24	10.200.3.1	ToRemote	Enabled	
ToRemoteBackup_remote	10.200.4.1	ToRemoteBackup	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)
ToRemoteBackup_remote		Blackhole	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)

3. Configure the following setting:

Field	Value
Administrative Distance	20



Edit Static Route

Destination: Subnet | **Named Address** | Internet Service

ToRemoteBackup_remote

Interface: ToRemoteBackup

Administrative Distance: 20

Comments: VPN: ToRemoteBackup (Created by VPN wizard) 43/255

Status: **Enabled** | Disabled

4. Click **OK**.

Review the Backup VPN Configuration on Remote-FortiGate

For the purpose of this lab, the backup VPN configuration on Remote-FortiGate was preconfigured for you. The configuration also includes a zone to reduce the number of firewall policies needed for the redundant VPNs. You will review this configuration.

To review the Remote-FortiGate configuration

1. On the Remote-FortiGate GUI, click **VPN** > **IPsec Tunnels**, and then double-click **ToLocalBackup** to review the tunnel settings.
2. Click **Network** > **Static Routes**, and then view **ToLocalBackup** to review the static route for the backup VPN.
3. Click **Network** > **Interfaces**, and then expand the **Zone** section to view the **VPN** zone details to review the interface zone.
4. Click **Policy & Objects** > **Firewall Policy**, and then view the **Local_out** and **Local_in** policies to review the firewall policies for VPN traffic on Remote-FortiGate.

Test VPN Redundancy

You will test the VPN failover. You will use the sniffer tool to monitor which VPN tunnel the traffic is using.

To test VPN redundancy

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to sniff all ICMP traffic to `10.0.2.10` with verbosity `4`:

```
diagnose sniffer packet any 'icmp and host 10.0.2.10' 4
```

3. On the Local-Client VM, open a terminal window, and then run a continuous ping to Remote-Client, using the following command:

```
ping 10.0.2.10
```

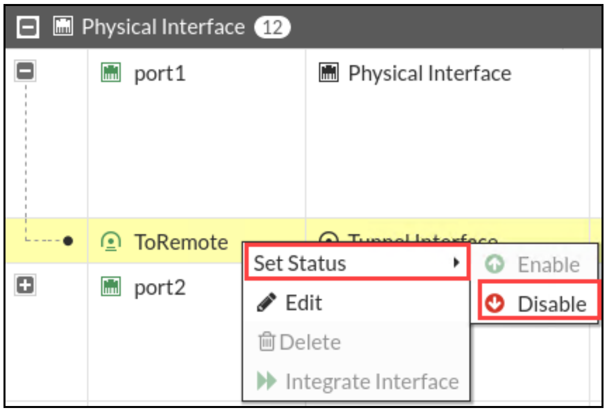
4. Return to the Local-FortiGate CLI session, and then view the sniffer output.

   It shows that Local-FortiGate is routing the packets through the `ToRemote` VPN.

```
28.040086 port3 in 10.0.1.10 -> 10.0.2.10: icmp: echo request
28.040107 ToRemote out 10.0.1.10 -> 10.0.2.10: icmp: echo request
28.041188 ToRemote in 10.0.2.10 -> 10.0.1.10: icmp: echo reply
28.041196 port3 out 10.0.2.10 -> 10.0.1.10: icmp: echo reply
```

Now, you will simulate a failure in the **ToRemote** VPN, and observe how FortiGate starts using the secondary **ToRemoteBackup** VPN.

5. On the Local-FortiGate GUI, click **Network** > **Interfaces**.
6. Click the **+** sign beside **port1** to view the subinterfaces using port1.
7. Right-click **ToRemote**, and then click **Set Status** > **Disable** to disable the VPN interface.



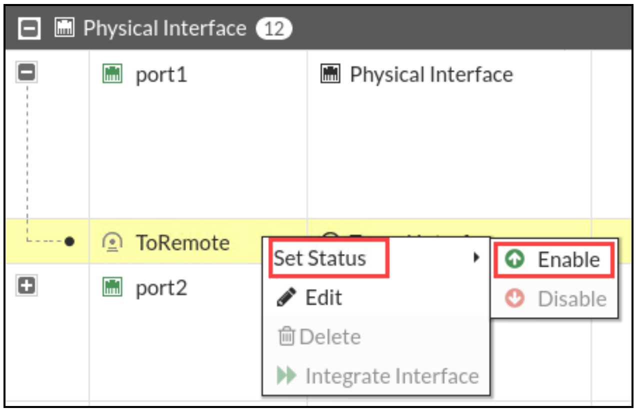
ToRemote is now grayed out.

8. Wait about a minute for DPD to detect the failure in **ToRemote**, and as a result, for FortiGate to reroute the traffic through **ToRemoteBackup**.
9. Return to the Local-FortiGate CLI session, and then view the sniffer output again.

   Notice that the `ToRemoteBackup` VPN is being used now.

```
546.352063 port3 in 10.0.1.10 -> 10.0.2.10: icmp: echo request
546.352090 ToRemoteBackup out 10.0.1.10 -> 10.0.2.10: icmp: echo request
546.353546 ToRemoteBackup in 10.0.2.10 -> 10.0.1.10: icmp: echo reply
546.353560 port3 out 10.0.2.10 -> 10.0.1.10: icmp: echo reply
```

10. On the Local-FortiGate GUI, click **Network** > **Interfaces**.
11. Click the **+** sign beside **port1** to view the subinterfaces using port1.
12. Right-click **ToRemote**, and then click **Set Status** > **Enable** to re-enable the VPN interface.



ToRemote is no longer grayed out.

13. Return to the Local-FortiGate CLI session, and then view the sniffer output again.

Notice that the `ToRemote` VPN is being used again.

```
589.622935 port3 in 10.0.1.10 -> 10.0.2.10: icmp: echo request
589.622948 ToRemote out 10.0.1.10 -> 10.0.2.10: icmp: echo request
589.624057 ToRemote in 10.0.2.10 -> 10.0.1.10: icmp: echo reply
589.624072 port3 out 10.0.2.10 -> 10.0.1.10: icmp: echo reply
```

14. Press `Ctrl`+`C` to stop the ping.

15. Close the Local-FortiGate CLI window.

Lab 7: High Availability

In this lab, you will examine how to set up a FortiGate Clustering Protocol (FGCP) high availability (HA) cluster of FortiGate devices. You will explore active-active HA mode and observe FortiGate HA behavior. You will also perform an HA failover and use diagnostic commands to observe the election of a new primary device in the cluster. Finally, you will configure management ports on FortiGate devices to reach each FortiGate individually for management purposes.

Objectives

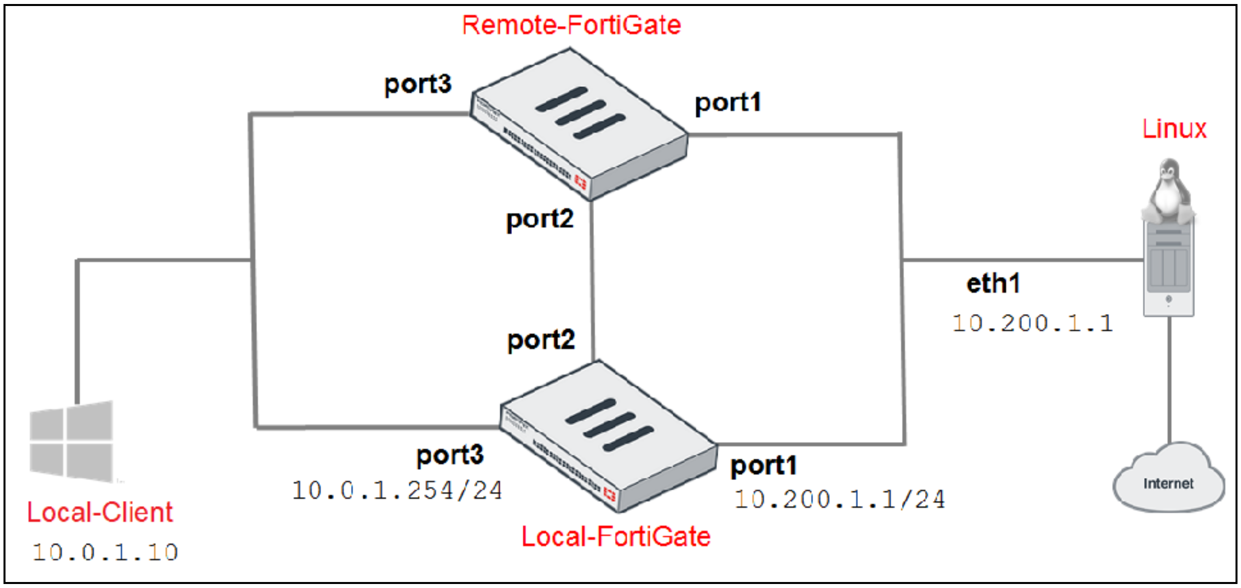
- Set up an HA cluster using FortiGate devices
- Observe HA synchronization and interpret diagnostic output
- Perform an HA failover
- Manage individual cluster members by configuring a reserved management interface

Time to Complete

Estimated: 40 minutes

Lab HA Topology

After you upload the required configurations to each FortiGate, the logical topology will change to the following:



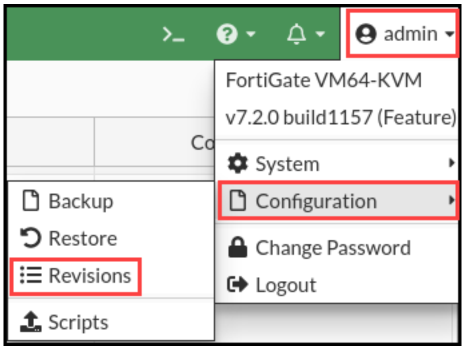
Prerequisites

Before beginning this lab, you must restore a configuration file to Local-FortiGate and Remote-FortiGate.

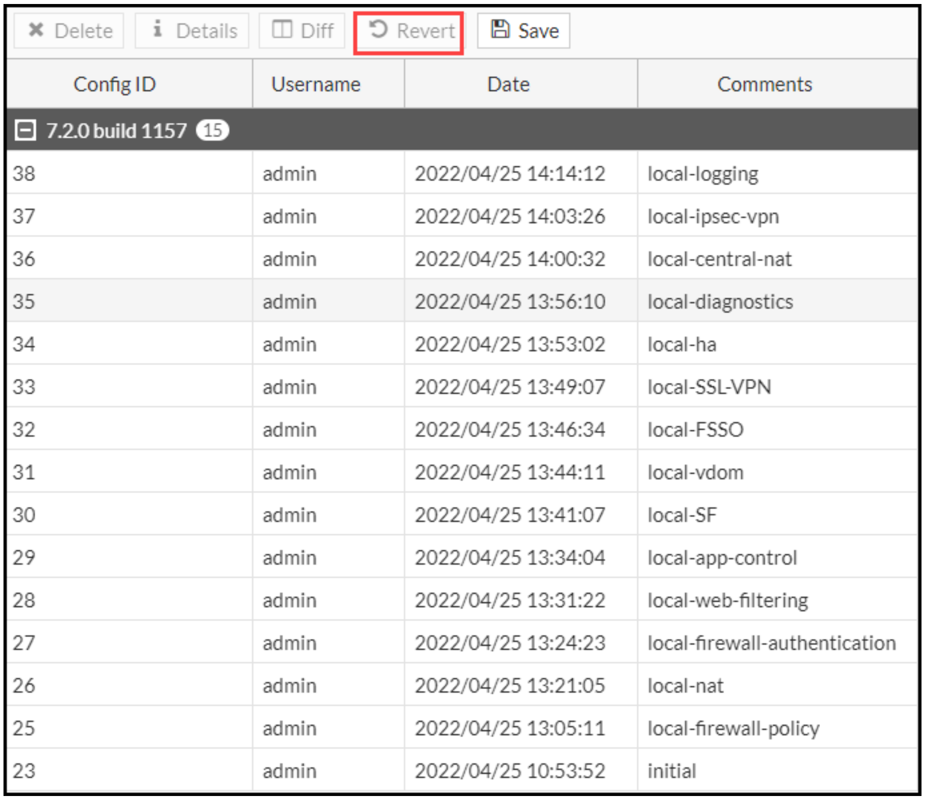
> You *must* restore the configuration to Local-FortiGate *first*, and then to Remote-FortiGate.
>
> If you restore the configuration to Remote-FortiGate first, it will produce unintended results and may prevent you from doing the lab exercises.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **local-ha**, and then click **Revert**.

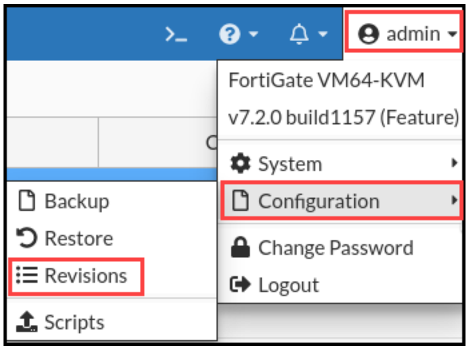


Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

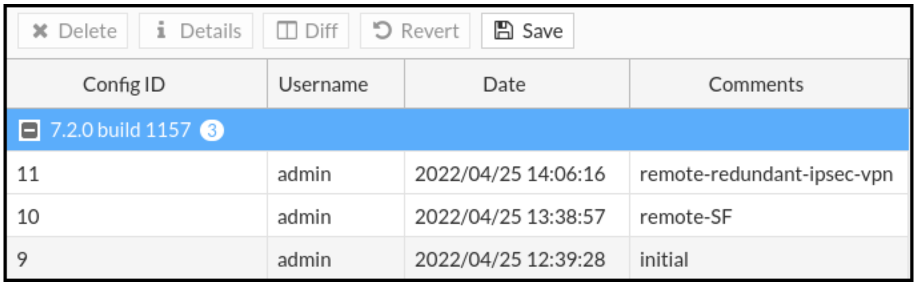
5. Click **OK** to reboot.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
⊟ 7.2.0 build 1157 3			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

5. Click **OK** to reboot.

Exercise 1: Configuring HA

FortiGate HA uses FGCP, which uses a heartbeat link for HA-related communications to discover other FortiGate devices in the same HA group, elect a primary device, synchronize configuration, and detect failed devices in an HA cluster.

In this exercise, you will examine how to configure HA settings on both FortiGate devices. You will observe the HA synchronization status, and use `diagnose` commands to verify that the configuration is in sync on both FortiGate devices.

Unless instructed otherwise, always use the console connection of Local-FortiGate and Remote-FortiGate to access the CLI. This ensures that you can access the CLI of the device regardless of the HA role.

Configure HA Settings on Local-FortiGate

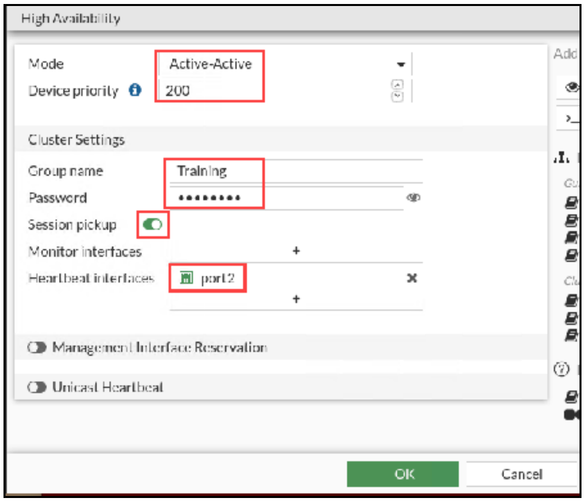
You will configure HA-related settings using the Local-FortiGate GUI.

To configure HA settings on Local-FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **System** > **HA**, and then configure the following HA settings:

Field	Value
Mode	Active-Active
Device priority	200
Group name	Training
Password	Fortinet **Tip**: Click **Change**, and then type the password.
Session pickup	<enable>
Monitor interfaces	Click **X** to remove any ports that are selected.
Heartbeat interfaces	Click **X** to remove port4, and then select port2.

The configuration should look like the following example:



High Availability

Mode: Active-Active

Device priority: 200

Cluster Settings

Group name: Training

Password: ••••••••

Session pickup: ●

Monitor interfaces

Heartbeat interfaces: port2

Management Interface Reservation

Unicast Heartbeat

3. Click **OK**.

Configure HA Settings on Remote-FortiGate

You will configure HA-related settings on Remote-FortiGate, using the console.

To configure HA settings on Remote-FortiGate

1. Connect to the Remote-FortiGate CLI, and then log in with the username `admin` and password `password`.
2. Enter the following commands:

```
config system ha
   set group-name Training
   set mode a-a
   set password Fortinet
   set hbdev port2 0
   set session-pickup enable
   set override disable
   set priority 100
end
```

Observe and Verify the HA Synchronization Status

Now that you have configured HA on both FortiGate devices, you will verify that HA is established and that the configurations are fully synchronized.

The checksums for all cluster members must match for the FortiGate devices to be synchronized.

To observe and verify the HA synchronization status

1. On the Remote-FortiGate CLI, you should see the debug messages about the HA synchronization process.

   These messages sometimes display useful status change information.

2. Wait 4–5 minutes for the FortiGate devices to synchronize.

   After the FortiGate devices are synchronized, the Remote-FortiGate device logs out all admin users.

```
secondary succeeded to sync external files with primary
secondary starts to sync with primary
logout all admin users
```

3. When prompted, log back in to the Remote-FortiGate CLI with the username `admin` and password `password`.
4. To check the HA synchronization status, enter the following command:
   ```
   diagnose sys ha checksum show
   ```
5. On the Local-FortiGate CLI, enter the following command to check the HA synchronization status:
   ```
   diagnose sys ha checksum show
   ```
6. Compare the output from both FortiGate devices.

   If both FortiGate devices are synchronized, the checksums match.
7. Alternatively, you can run the following CLI command on any member to view the checksums of all members:
   ```
   diagnose sys ha checksum cluster
   ```

Verify FortiGate Roles in an HA Cluster

After the checksums of both FortiGate devices match, you will verify the cluster member roles to confirm the primary and secondary devices.

To verify FortiGate roles in an HA cluster

1. On both the Local-FortiGate CLI and Remote-FortiGate CLI, enter the following command to verify that the HA cluster is established:
   ```
   get system status
   ```
2. On both FortiGate devices, view the `Current HA mode` line, and then write down the device serial number (`Serial-Number`).

   Notice that Local-FortiGate is `a-a primary` and Remote-FortiGate is `a-a secondary`.

> **Stop and think!**
>
> Why was Local-FortiGate elected as the primary?
>
> In the primary election process, the first criterion checked is the number of connected monitored ports. Because you didn't configure monitored ports, then the next criterion is checked.
>
> Because you disabled the override setting, then the next criterion checked is HA uptime. Because you enabled HA on both devices about the same time, then the HA uptime difference is less than five minutes, and therefore, the next criterion, priority, is checked.
>
> Local-FortiGate has a priority of 200, which is greater than Remote-FortiGate, which has a priority of 100. The result is that Local-FortiGate is elected primary.

3. On the Local-FortiGate CLI , enter the following command to confirm the reason for the primary election:
   ```
   get system ha status
   ```
4. In the output, look for the `Primary selected using` section to identify the reason for the latest primary election event.

Your output should look similar to the following example:

```
Primary selected using:
    <2022/04/22 09:03:55> vcluster-1: FGVM010000064692 is selected as the primary because its
 override priority is larger than peer member FGVM010000065036.
```

The output confirms that Local-FortiGate was elected primary because of its higher priority.

If you see that the election reason is a higher uptime, then that is probably because you rebooted one of the members, and as a result, the HA uptime of that device was reset. The reboot then caused the HA uptime difference to be more than five minutes.

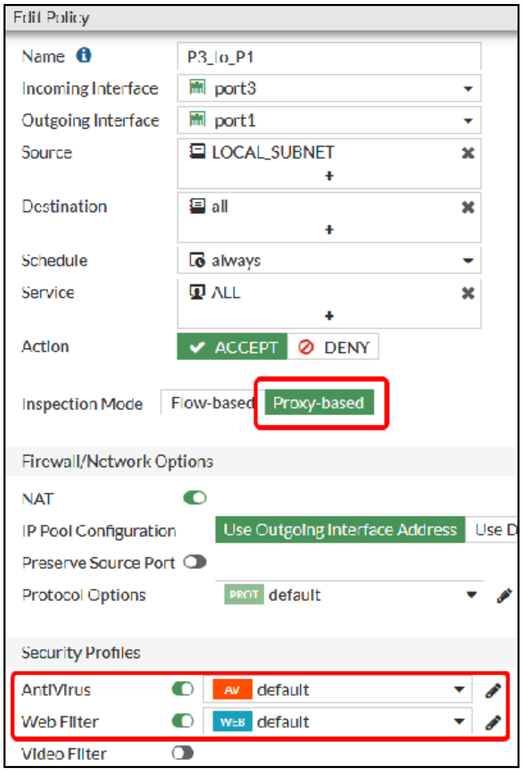
Verify Firewall Policy Configuration

By default, a FortiGate HA active-active cluster load balances only sessions that are subject to proxy inspection. For this reason, you will verify that the matching firewall policy is configured to perform proxy inspection.

To verify firewall policy configuration

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the firewall policy named **P3_to_P1** to view its settings.

   Your page should look similar to the following example:



Edit Policy

Name: P3_to_P1
Incoming Interface: port3
Outgoing Interface: port1
Source: LOCAL_SUBNET
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY
Inspection Mode: Flow-based | Proxy-based

Firewall/Network Options
NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use D
Preserve Source Port: ○
Protocol Options: PROT default

Security Profiles
AntiVirus: ● AV default
Web Filter: ● WEB default
Video Filter: ○

The firewall policy **P3_to_P1** has been preconfigured for you. The firewall policy matches the internet traffic that you will generate in the next task, and is configured to perform antivirus and web filtering proxy-based inspection on the matching traffic. This way, the primary FortiGate will distribute some of the matching sessions to the secondary FortiGate.

3. Click **Cancel**.

View Session Statistics

You will view session statistics.

To view session statistics

1. On the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:
    - https://docs.fortinet.com
    - www.yahoo.com
    - www.bbc.com
2. On both the Local-FortiGate CLI and Remote-FortiGate CLI, enter the following command:

```
get system session status
```

The *primary* FortiGate handles more sessions than the *secondary* FortiGate. This is because the primary handles:

- Cluster management traffic (local-in and local-out connections)
- Non-TCP firewall traffic
- TCP firewall traffic that is not subject to proxy-based inspection or any inspection
- TCP firewall traffic that is subject to proxy-based inspection and that isn't distributed to the secondary

Exercise 2: Triggering an HA Failover

You set up an HA cluster. In this exercise, you will examine how to trigger an HA failover, and observe the renegotiation among devices to elect a new primary device and redistribute the sessions.

Unless instructed otherwise, always use the console connection of Local-FortiGate and Remote-FortiGate to access the CLI. This ensures that you can access the device CLI regardless of the HA role.

Trigger a Failover by Rebooting the Primary FortiGate

You will reboot the primary FortiGate in the cluster to trigger a failover.

Take the Expert Challenge!

1. On the Local-Client VM, complete the following:
   - Play a long video (more than 5 minutes long) on https://www.youtube.com.
   - Run a continuous ping to IP address `4.2.2.2`.
2. On the Local-FortiGate CLI, reboot Local-FortiGate.

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

After you have performed these steps, see Triggering an HA Failover on page 108.

To trigger a failover by rebooting the primary FortiGate

1. On the Local-Client VM, open a browser, and then visit the following URL:
   https://www.youtube.com
2. Play a long video (more than 5 minutes long).
3. While the video is playing, open a terminal, and then run a continuous ping to a public IP address:
   ```
   ping 4.2.2.2
   ```
4. To trigger a failover, on the Local-FortiGate CLI, enter the following command to reboot Local-FortiGate:
   ```
   execute reboot
   ```
5. Press `Y` to confirm that you want to reboot Local-FortiGate.

Verify the HA Failover and FortiGate Roles

You will verify the HA failover, and check the roles of FortiGate in an HA cluster.

To verify the HA failover and FortiGate roles

1. On the Local-Client VM, check the terminal and video that you started earlier.

   Because of the failover, Remote-FortiGate is now the primary processor of traffic. Your ping and video should still be running.

2. Press `Ctrl+C` to stop the ping.
3. To verify that Remote-FortiGate is acting as the primary device in the HA cluster, on the Remote-FortiGate CLI, enter the following command:

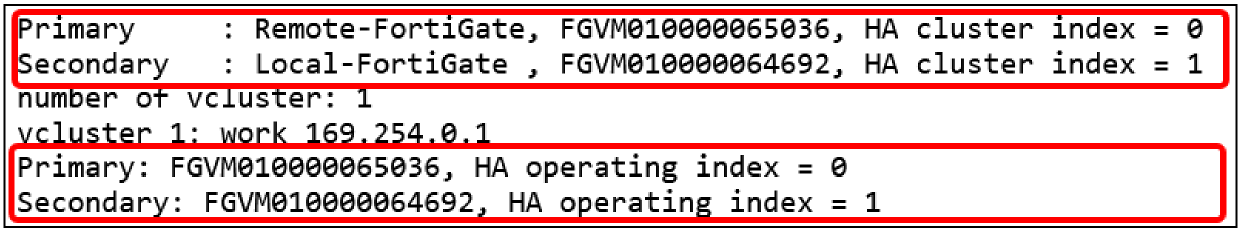
   ```
   get system status
   ```

> **Stop and think!**
>
> When Local-FortiGate finishes rebooting and rejoins the cluster, does it rejoin as the *secondary* device, or resume its initial role of *primary* device?

4. To see the status of all cluster members, enter the following command on any FortiGate in the cluster:

   ```
   get system ha status
   ```

   You should see that *Local-FortiGate* rejoins the cluster as a *secondary* device. It lost its role as the primary device.



```
Primary     : Remote-FortiGate, FGVM010000065036, HA cluster index = 0
Secondary   : Local-FortiGate , FGVM010000064692, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FGVM010000065036, HA operating index = 0
Secondary: FGVM010000064692, HA operating index = 1
```

The output of `get system ha status` has been cut to fit this page.

Local-FortiGate becomes the *secondary* device in the cluster because it has a lower HA uptime than Local-Remote. In addition, the HA uptime difference between the members is more than 5 minutes.

Trigger an HA Failover by Resetting the HA Uptime

You will trigger a failover by resetting the HA uptime on the current primary FortiGate—which should be Remote-FortiGate—and then you will verify the role of Remote-FortiGate in the HA cluster.

To trigger an HA failover by resetting the HA uptime on FortiGate

1. On the Remote-FortiGate CLI console, enter the following command:

   ```
   diagnose sys ha reset-uptime
   ```

After you reset the HA uptime on Remote-FortiGate, Local-FortiGate becomes the member with the highest HA uptime. Because the HA uptime difference between the members is more than five minutes, then Local-FortiGate is elected as the new primary.

Remote-FortiGate now has the *secondary* role in the cluster.

2. On the Remote-FortiGate CLI, enter the following command to verify this:

```
get system status
```

Observe HA Leave and Join Messages Using Diagnostic Commands

The HA synchronization process is responsible for FGCP packets that communicate cluster status and build the cluster. You will use real-time diagnostic commands to observe this process.

To observe HA failover using diagnostic commands

1. On the Local-FortiGate CLI, enter the following commands:

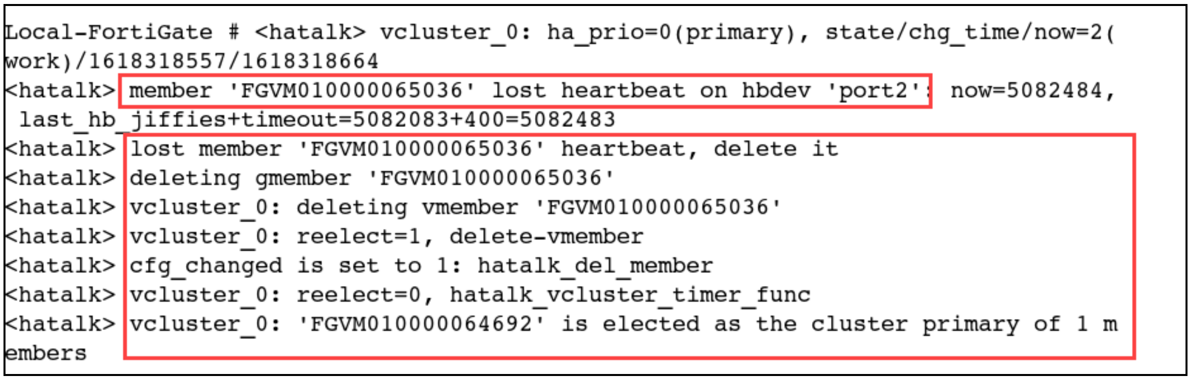
```
diagnose debug enable
diagnose debug application hatalk 0
diagnose debug application hatalk 255
```

The `diagnose debug application hatalk 0` command stops the debug. You will use this command later.

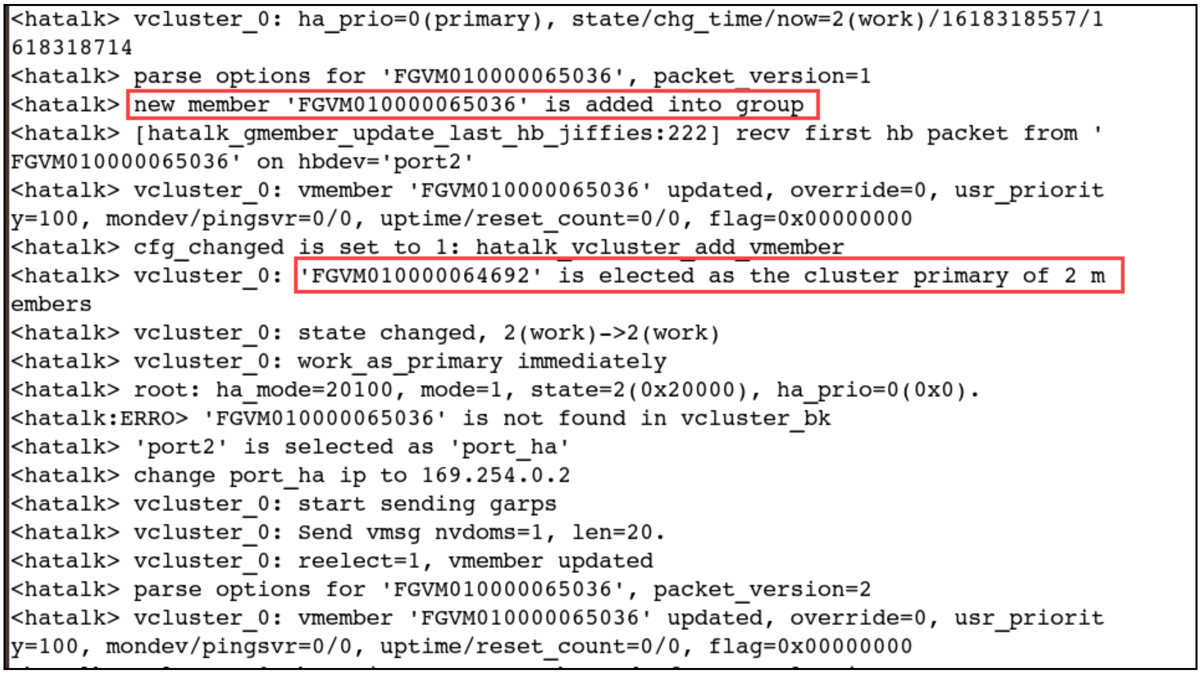
2. On the Remote-FortiGate CLI, enter the following command to reboot Remote-FortiGate:

```
execute reboot
```

3. Press `Y` to confirm that you want to reboot Remote-FortiGate.
4. On the Local-FortiGate CLI, view the output while the secondary device reboots and starts communicating with the cluster.



```
Local-FortiGate # <hatalk> vcluster_0: ha_prio=0(primary), state/chg_time/now=2(
work)/1618318557/1618318664
<hatalk> member 'FGVM010000065036' lost heartbeat on hbdev 'port2', now=5082484,
 last_hb_jiffies+timeout=5082083+400=5082483
<hatalk> lost member 'FGVM010000065036' heartbeat, delete it
<hatalk> deleting gmember 'FGVM010000065036'
<hatalk> vcluster_0: deleting vmember 'FGVM010000065036'
<hatalk> vcluster_0: reelect=1, delete-vmember
<hatalk> cfg_changed is set to 1: hatalk_del_member
<hatalk> vcluster_0: reelect=0, hatalk_vcluster_timer_func
<hatalk> vcluster_0: 'FGVM010000064692' is elected as the cluster primary of 1 m
embers
```



```
<hatalk> vcluster_0: ha_prio=0(primary), state/chg_time/now=2(work)/1618318557/1
618318714
<hatalk> parse options for 'FGVM010000065036', packet_version=1
<hatalk> new member 'FGVM010000065036' is added into group
<hatalk> [hatalk_gmember_update_last_hb_jiffies:222] recv first hb packet from '
FGVM010000065036' on hbdev='port2'
<hatalk> vcluster_0: vmember 'FGVM010000065036' updated, override=0, usr_priorit
y=100, mondev/pingsvr=0/0, uptime/reset_count=0/0, flag=0x00000000
<hatalk> cfg_changed is set to 1: hatalk_vcluster_add_vmember
<hatalk> vcluster_0: 'FGVM010000064692' is elected as the cluster primary of 2 m
embers
<hatalk> vcluster_0: state changed, 2(work)->2(work)
<hatalk> vcluster_0: work_as_primary immediately
<hatalk> root: ha_mode=20100, mode=1, state=2(0x20000), ha_prio=0(0x0).
<hatalk:ERRO> 'FGVM010000065036' is not found in vcluster_bk
<hatalk> 'port2' is selected as 'port_ha'
<hatalk> change port_ha ip to 169.254.0.2
<hatalk> vcluster_0: start sending garps
<hatalk> vcluster_0: Send vmsg nvdoms=1, len=20.
<hatalk> vcluster_0: reelect=1, vmember updated
<hatalk> parse options for 'FGVM010000065036', packet_version=2
<hatalk> vcluster_0: vmember 'FGVM010000065036' updated, override=0, usr_priorit
y=100, mondev/pingsvr=0/0, uptime/reset_count=0/0, flag=0x00000000
```

The output shows that the current primary FortiGate is sending heartbeat packets and trying to synchronize its configuration with the configuration of the secondary FortiGate.

5. To stop the debug output on Local-FortiGate, press the up arrow key twice, select the second-last command (in this case, `diagnose debug application hatalk 0`), and then press `Enter`.

Exercise 3: Configuring the HA Management Interface

In this exercise, you will examine how to configure a spare interface in the cluster as a reserved HA management interface. This allows both FortiGate devices to be reachable for management purposes regardless of the member role.

If a reserved HA management interface is not configured, your cluster management connections are handled by the primary FortiGate. However, you can access the CLI of the secondary FortiGate from the primary FortiGate CLI, or by using the secondary console connection.

You can also configure an in-band HA management interface, which is an alternative to the reserved HA management interface, and does *not* require reserving an interface that is only for management access.

Unless instructed otherwise, always use the console connection of Local-FortiGate and Remote-FortiGate to access the CLI. This ensures that you can access the device CLI regardless of the HA role.

Access the Secondary FortiGate CLI Through the Primary FortiGate CLI

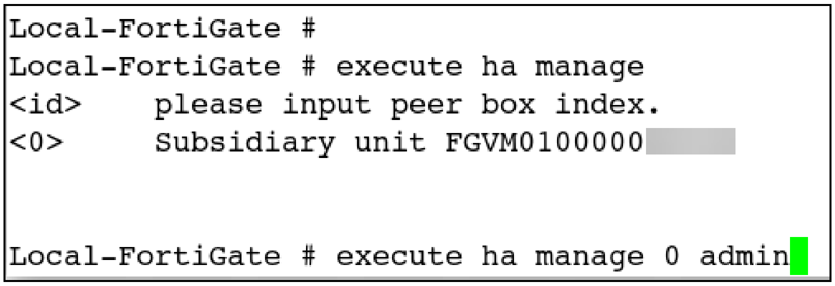
You will connect to the secondary FortiGate CLI through the primary FortiGate CLI.

To access the secondary FortiGate CLI through the primary FortiGate CLI

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to access the secondary FortiGate CLI through the primary FortiGate heartbeat interface:

   ```
   execute ha manage <id> admin
   ```

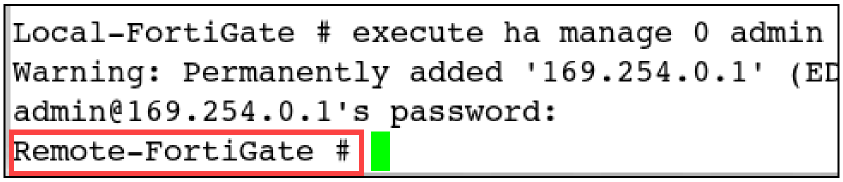
Use `?` to list the values for `<id>`.



```
Local-FortiGate #
Local-FortiGate # execute ha manage
<id>    please input peer box index.
<0>     Subsidiary unit FGVM0100000[redacted]


Local-FortiGate # execute ha manage 0 admin
```

3. When prompted, enter the password `password` to log in to Remote-FortiGate.



```
Local-FortiGate # execute ha manage 0 admin
Warning: Permanently added '169.254.0.1' (ED
admin@169.254.0.1's password:
Remote-FortiGate #
```

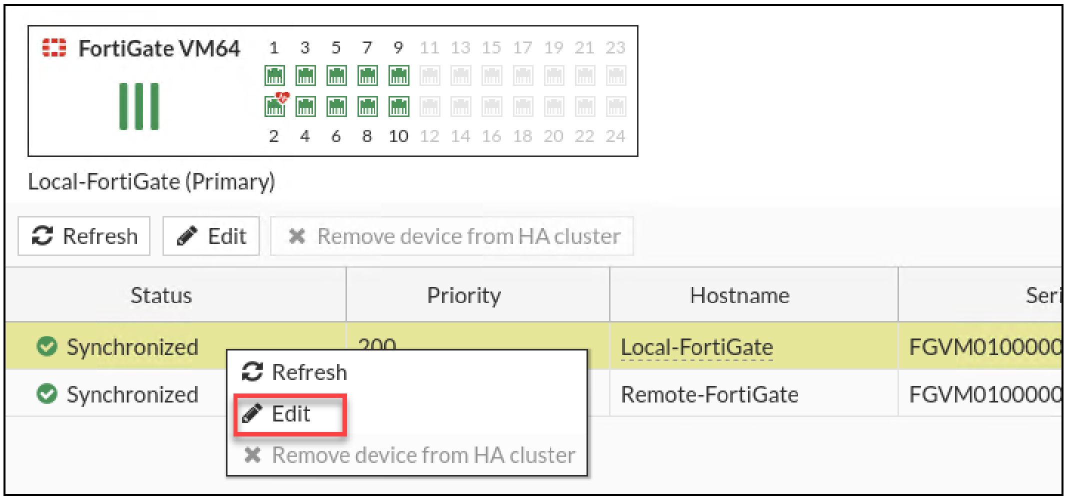
4. Enter the following command to get the status of the secondary FortiGate:
   `get system status`
5. View the `Current HA mode` line.
   You will notice that Remote-FortiGate is `a-a secondary`.
6. Enter the following command to return to the Local-FortiGate CLI:
   `exit`

Set Up a Reserved HA Management Interface

You will use an unused interface on the FortiGate devices in an HA cluster to configure a reserved HA management interface and a unique IP address on each member. This way, you can access each member directly regardless of its role.

To set up a reserved HA management interface

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. Click **System** > **HA**.
3. Right-click **Local-FortiGate**, and then click **Edit**.



Status	Priority	Hostname	Seri
✓ Synchronized	200	Local-FortiGate	FGVM0100000
✓ Synchronized		Remote-FortiGate	FGVM0100000

4. Enable **Management Interface Reservation**, and then in the **Interface** field, select **port7**.
5. Click **OK**.

port7 connects to the same LAN segment as port3.

Configure and Access the Primary FortiGate Using the Reserved HA Management Interface

You will configure and verify access to the primary FortiGate using the reserved HA management interface.

To configure and verify access to the primary FortiGate using the reserved HA management interface

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to configure port7:

```
config system interface
   edit port7
   set ip 10.0.1.253/24
   set allowaccess ping ssh snmp http
end
```

Even though this address overlaps with port3, which is not allowed by default (FortiGate does not allow overlapped subnets by default), it is allowed here because the routing entries for the reserved HA management interface are excluded from the routing table.

3. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.253` (note the IP address) with the username `admin` and password `password`.

   This verifies connectivity to port7.

Configure and Access the Secondary FortiGate Using the Reserved HA Management Interface

You will configure and verify access to the secondary FortiGate using the reserved HA management interface.

Take the Expert Challenge!

1. On the Remote-FortiGate CLI, complete the following:
   - Verify that the reserved HA management interface was synchronized with the secondary device.

     ```
     show system ha
     ```

   - Verify that **port7** has no configuration, and then configure **port7 IP/Netmask** as `10.0.1.252/24` with the same `allowaccess` configured for Local-FortiGate **port7**.
2. On the Local-Client VM, log in to the Remote-FortiGate GUI (`admin`/`password`) using the port7 IP address to verify connectivity.

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

After the configuration is ready, see Configuring the HA Management Interface on page 112.

To configure and verify access to the secondary FortiGate using the management interface

1. On the Remote-FortiGate CLI, enter the following command to verify that the reserved HA management interface was synchronized with the secondary device:

   ```
   show system ha
   ```

   Look for `ha-mgmt-status` and `config ha-mgmt-interfaces`. These should already be set.
2. Enter the following command to verify that port7 has no configuration:

   ```
   show system interface port7
   ```

3. Configure port7, using the following commands:

   ```
   config system interface
      edit port7
         set ip 10.0.1.252/24
         set allowaccess ping ssh snmp http
      next
   end
   ```

4. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.0.1.252` (note the IP address) with the username `admin` and password `password`.

   This will verify connectivity to port7.

   Each device in the cluster now has its own management IP address for monitoring purposes.

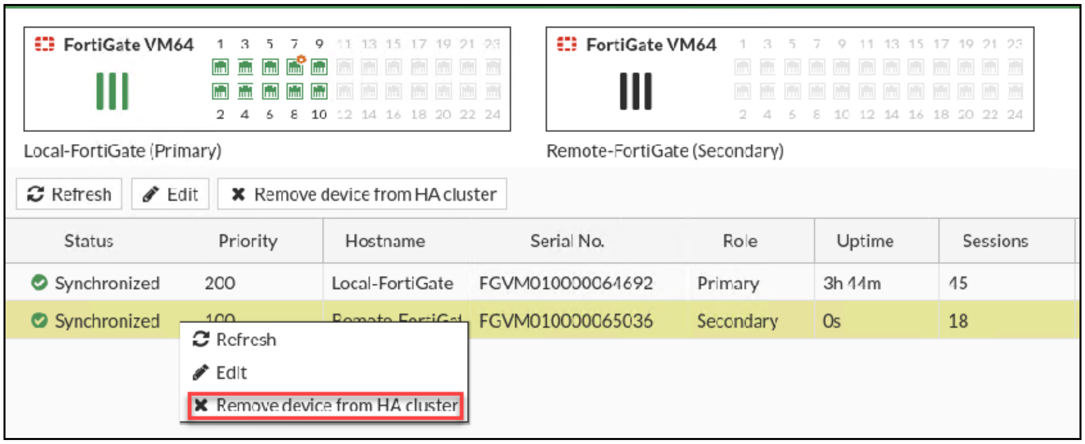
Disconnect Remote-FortiGate From the Cluster

You will disconnect Remote-FortiGate from the cluster. Remote-FortiGate will prompt you to configure an IP address on any port on Remote-FortiGate so that you can access it after the disconnection.

To disconnect Remote-FortiGate from the cluster

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.

2. Click **System** > **HA**.
3. Right-click **Remote-FortiGate**, and then click **Remove device from HA cluster**.


FortiGate VM64
Local-FortiGate (Primary)
FortiGate VM64
Remote-FortiGate (Secondary)
Refresh
Edit
Remove device from HA cluster
Refresh
Edit
Remove device from HA cluster

Status	Priority	Hostname	Serial No.	Role	Uptime	Sessions
Synchronized	200	Local-FortiGate	FGVM010000064692	Primary	3h 14m	15
Synchronized	100	Remote-FortiGat	FGVM010000065036	Secondary	0s	18

4. When prompted, configure the following settings:

Field	Value
Interface	port3
IP/Netmask	10.0.1.251/24

5. Click **OK**.

   This removes the FortiGate from the HA cluster.

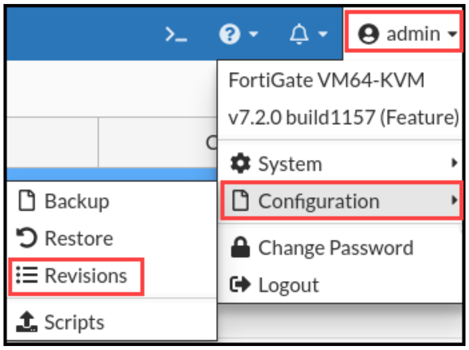
Restore the Remote-FortiGate Configuration

You will restore the Remote-FortiGate configuration, so that you can use Remote-FortiGate in the next labs.

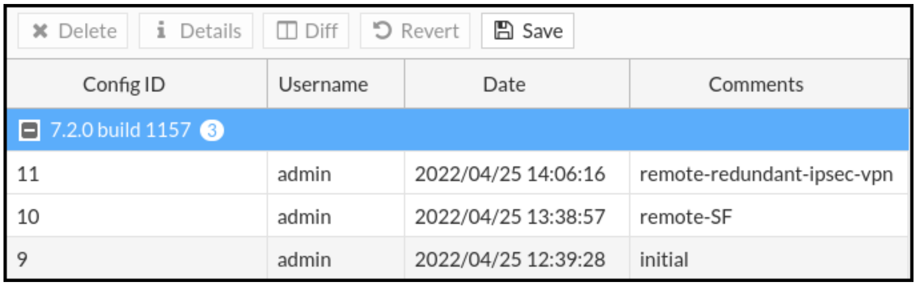
Failure to perform these steps will prevent you from doing the next exercises.

To restore the Remote-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.0.1.251` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 3			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

5. Click **OK** to reboot.

Failure to perform these steps will prevent you from doing the next exercises.

Lab 8: Diagnostics Performance

In this lab, you will run diagnostic commands to learn about the current status of FortiGate. You will also use the sniffer and debug flow tools to troubleshoot and fix a connectivity problem.

Objectives

- Identify normal behavior for your network
- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers
- Diagnose connectivity problems using the debug flow
- Diagnose resource problems, such as high CPU or memory usage

Time to Complete

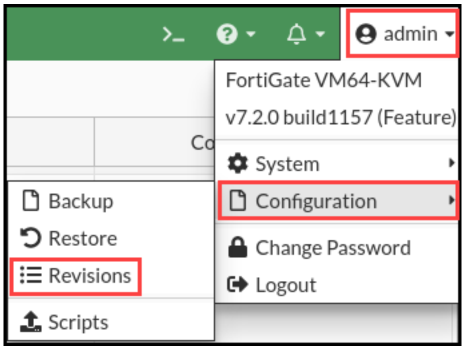
Estimated: 30 minutes

Prerequisites

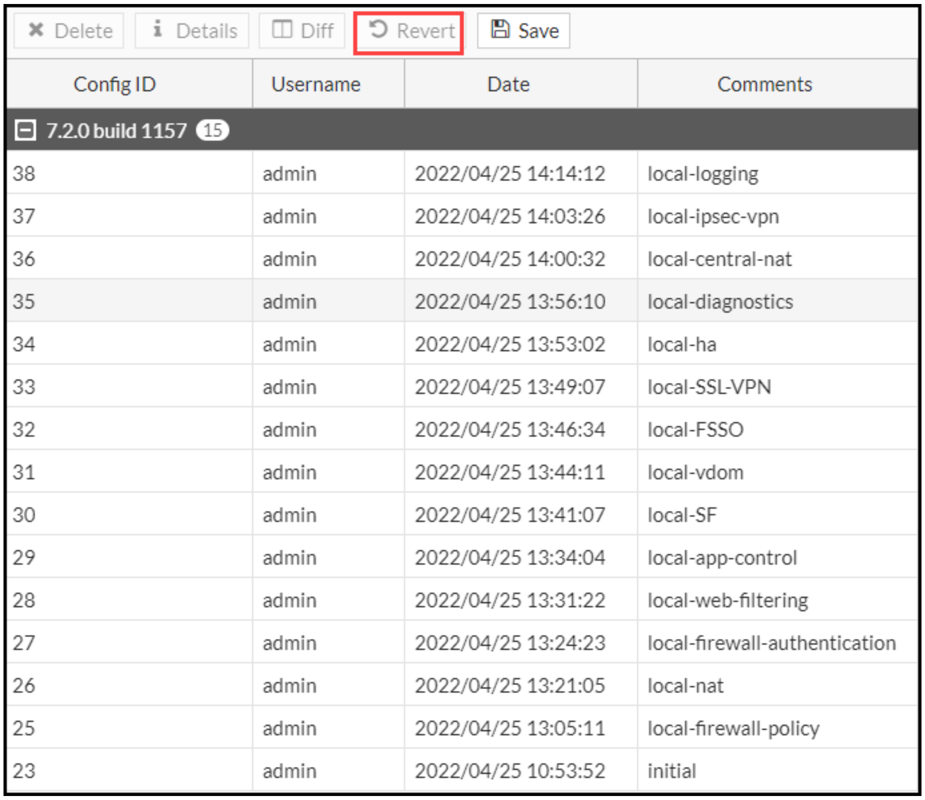
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the Local-FortiGate configuration file

1. On the Local-FortiGate GUI, log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-diagnostics**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Determining What Is Happening Now

In this exercise, you will use CLI commands to get information about FortiGate, such as traffic volume, CPU usage, memory usage, and the ARP table.

Run Diagnostic Commands

You will run some diagnostic commands and take note of some of the information displayed.

To run diagnostic commands

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Find the following information and write down your answers in the space provided—refer to the list of commands that follows to get the answers:

Field	Value
Firmware branch point	
Current HA mode	
Hostname	
CPU utilization	
Memory utilization	
Average network usage	
Average session setup rate	
Negotiated speed and duplex mode for interface port1	
MTU for port1	
MAC address for the IP address 10.200.1.254	
Name of the process consuming the most CPU (if any)	
Name of the process consuming the most memory	

Enter the following CLI commands to find the information requested above:

```
get system status
get system performance status
get hardware nic port1
get system arp
diagnose sys top 1
```

(Press `Shift`+`P` to order the processes by CPU usage, `Shift`+`M` to order them by memory usage, or `Q` to stop.)

3. Close the Local-FortiGate CLI session.

Exercise 2: Troubleshooting a Connectivity Problem

In this exercise, you will use the sniffer and debug flow to troubleshoot a network connectivity problem.

Identify the Problem

As you will see in this procedure, there is a network connectivity problem between the Local-Client VM and the Linux server.

To identify the problem

1. On the Local-Client VM, open a terminal window.
2. Start a continuous ping to the Linux server (IP address `10.200.1.254`):

   ```
   ping 10.200.1.254
   ```

   The ping is failing. You will use the sniffer and debug flow tools on Local-FortiGate to find out why.
3. Do not close the terminal window—keep the ping running.

Use the Sniffer

Take the Expert Challenge!

Now that you understand what the problem is, try to fix it without looking at the FortiGate configuration. Use the built-in sniffer and debug flow tools to troubleshoot the problem.

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

After you complete the challenge, see Troubleshooting a Connectivity Problem on page 122.

You will start troubleshooting by sniffing the ICMP traffic going to the Linux server.

To use the sniffer

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to sniff the ICMP traffic to `10.200.1.254`:

   ```
   diagnose sniffer packet any "icmp and host 10.200.1.254" 4
   ```

3. Observe the output.

   ```
   interfaces=[any]
   filters=[icmp and host 10.200.1.254]
   5.439019 port3 in 10.0.1.10 -> 10.200.1.254: icmp: echo request
   10.442347 port3 in 10.0.1.10 -> 10.200.1.254: icmp: echo request
   ```

```
15.444343 port3 in 10.0.1.10 -> 10.200.1.254: icmp: echo request
20.545397 port3 in 10.0.1.10 -> 10.200.1.254: icmp: echo request
```

The packets are arriving on FortiGate, but FortiGate is not routing them.

4. Press `Ctrl+C` to stop the sniffer.

Use the Debug Flow Tool

You will run the debug flow tool to get information about why the packets are being dropped.

To use the debug flow tool

1. On the Local-FortiGate CLI session, enter the following commands. You will configure the debug flow filter to capture all ICMP traffic to and from the `10.200.1.254` IP address.

   ```
   diagnose debug flow filter clear
   diagnose debug flow filter proto 1
   diagnose debug flow filter addr 10.200.1.254
   diagnose debug enable
   diagnose debug flow trace start 3
   ```

   The output should be similar to the following example. FortiGate receives the ICMP packet from `10.0.1.10` to `10.200.1.254` from `port3`.

   ```
   id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet
       (proto=1, 10.0.1.10:1->10.200.1.254:2048) from port3. type=8, code=0, id=1,
       seq=33."
   ```

   It creates a new session.

   ```
   id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new
       session-00000340"
   ```

   It finds a route for the destination `10.200.1.254` through `port1`.

   ```
   id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route:
       flag=04000000 gw-10.200.1.254 via port1"
   ```

   It drops the packet. The debug flow shows the error message.

   ```
   id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy
       check (policy 0)"
   ```

   The `Denied by forward policy check` message indicates that the traffic is denied by a firewall policy. It could be either a denied policy explicitly configured by the administrator, or the implicit denied policy for traffic that does not match a configured policy.

   The `policy 0` indicates that the traffic was denied by the default implicit policy. If the traffic was blocked by an explicitly configured policy, its policy ID number would be indicated in this output, instead of `0`.

Fix the Problem

Now that you found the cause of the problem, you will fix the problem.

To fix the problem

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Look at the firewall policies.

   The **Full_Access** firewall policy does not allow ICMP traffic (only HTTP)—this is why FortiGate is dropping the ping packets.
4. Edit the **Full_Access** firewall policy.
5. Change the service from **HTTP** to **ALL**.
6. Click **OK**.

Test the Fix

You will test to confirm that the configuration change fixed the problem.

To test the fix

1. On the Local-Client VM, check the terminal window to see if the continuous ping is working now.
2. Press `Ctrl`+`C` to stop the ping, but leave the terminal open.
3. On the Local-FortiGate CLI session where you are running debug commands, clear all the ICMP sessions from the session table, using the following commands:

```
diagnose sys session filter clear
diagnose sys session filter proto 1
diagnose sys session clear
```

4. Start the debug flow again, using the following commands:

```
diagnose debug flow filter clear
diagnose debug flow filter proto 1
diagnose debug flow filter addr 10.200.1.254
diagnose debug enable
diagnose debug flow trace start 3
```

   There should not be any output yet, because the ping is not running.
5. Return to the terminal window, and then start the ping again.

```
ping 10.200.1.254
```

6. Check the debug flow output.

   It is a bit different now. The error message is not displayed and you can see a few new logs.

   Traffic is allowed by the firewall policy with the ID 1.

```
id=20085 trace_id=4 func=fw_forward_handler line=737 msg="Allowed by Policy-1: SNAT"
```

   FortiGate applies source NAT (SNAT).

```
id=20085 trace_id=4 func=__ip_session_run_tuple line=3164 msg="SNAT 10.0.1.10-
    >10.200.1.1:62464"
```

   Additionally, you can see the debug flow logs from the return (ping reply) packets.

```
id=20085 trace_id=5 func=print_pkt_detail line=5363 msg="vd-root received a packet
    (proto=1, 10.200.1.254:62464->10.200.1.1:0) from port1. type=0, code=0, id=62464,
    seq=83."
id=20085 trace_id=5 func=resolve_ip_tuple_fast line=5438 msg="Find an existing
    session, id-000003f2, reply direction"
id=20085 trace_id=5 func=__ip_session_run_tuple line=3178 msg="DNAT 10.200.1.1:0-
    >10.0.1.10:1"
id=20085 trace_id=5 func=vf_ip_route_input_common line=2583 msg="find a route:
    flag=04000000 gw-10.0.1.10 via port3"
```

The procedure in this exercise describes what you should usually do when troubleshooting connectivity problems on FortiGate. Sniff the traffic first to check that the packets are arriving on FortiGate and that FortiGate is routing them correctly. If the sniffer shows that the traffic is being dropped by FortiGate, use the debug flow tool to find out why.

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.