وزارة الاتصالات
وتكنولوجيا المعلومات

رواد مصر الرقمية

PROJECT 2

IPSEC VPN CONFIGURATION

Name: Ahmed Abdallah Ahmed

Project: IPsec VPN Configuration

In this project, 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

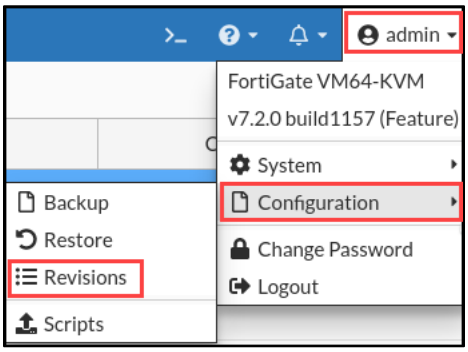
Prerequisites

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

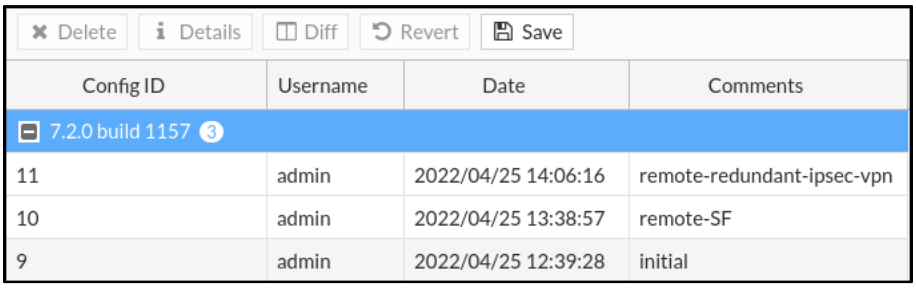
Make sure that you restore the correct configuration on each FortiGate, using the following steps. Failure to restore the correct configuration on each FortiGate will prevent you from doing the lab exercises.

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**.



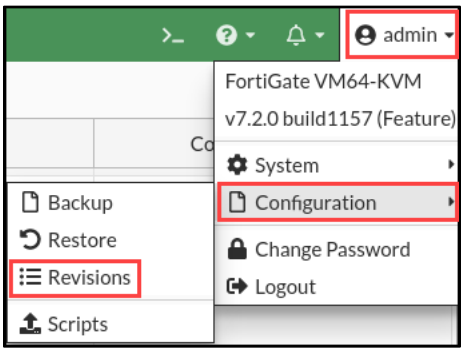
3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



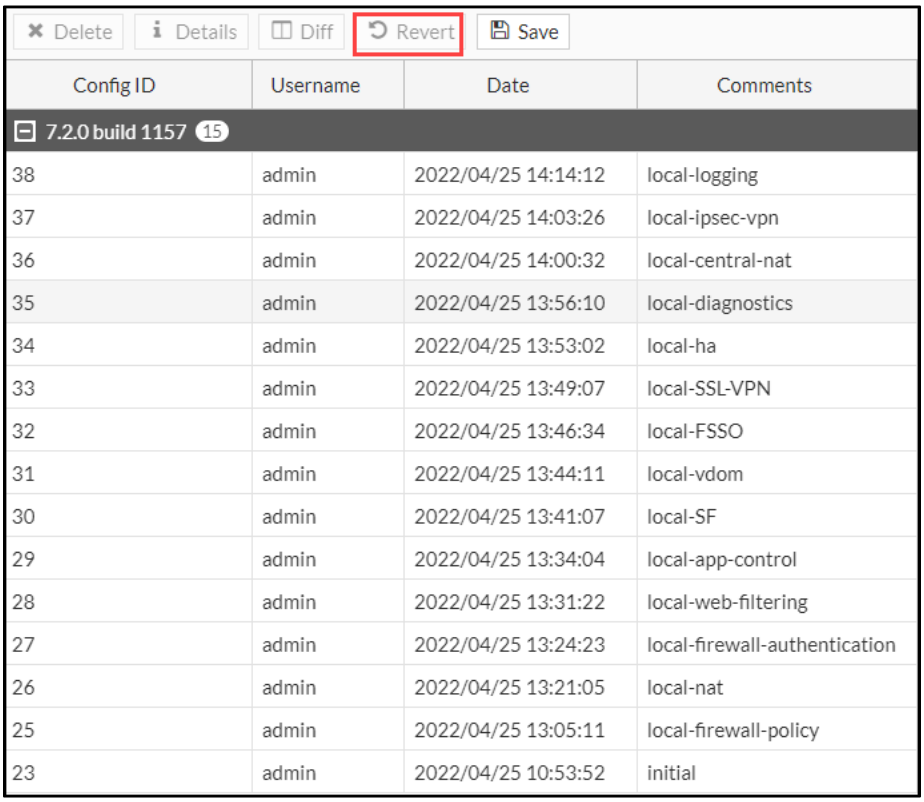
5. Click **OK** to reboot.

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**.



Delete | Details | Diff | Revert | Save

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 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

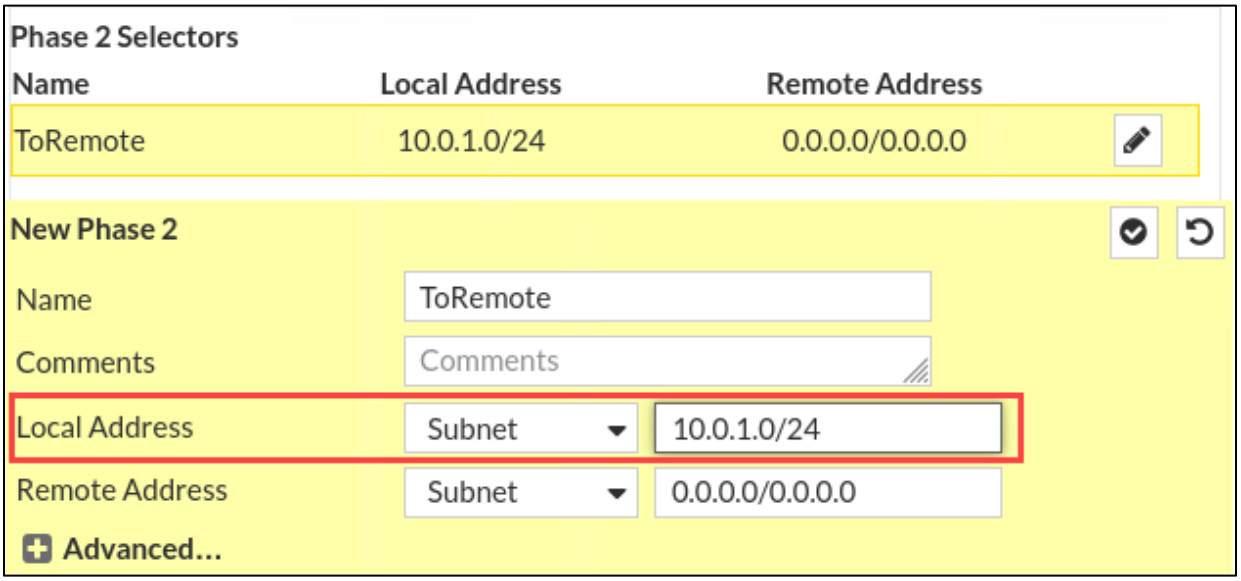
6. In the **Authentication** section, configure the following settings:

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



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

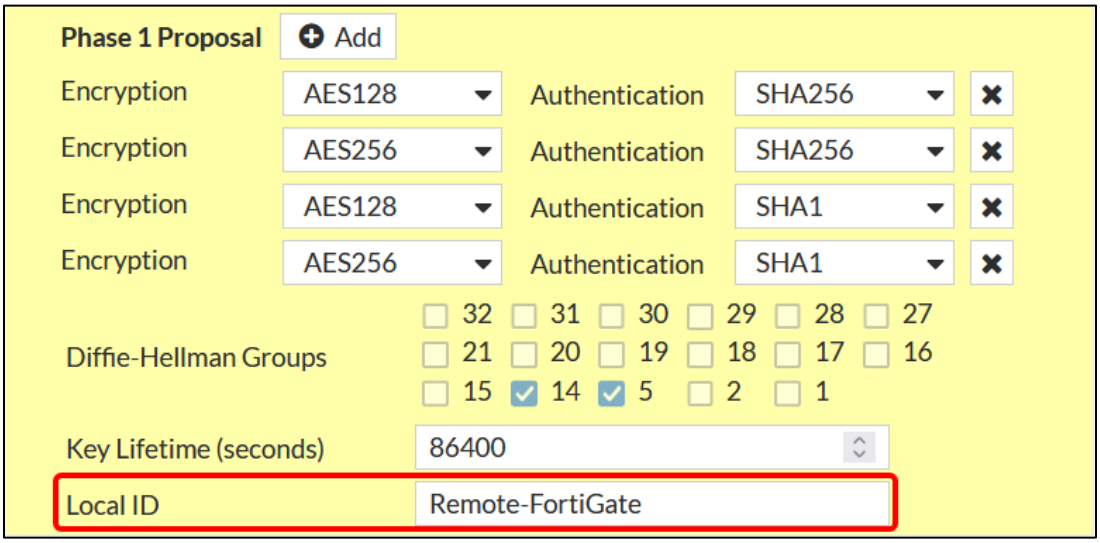
6. In the **Authentication** section, configure the following settings:

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:

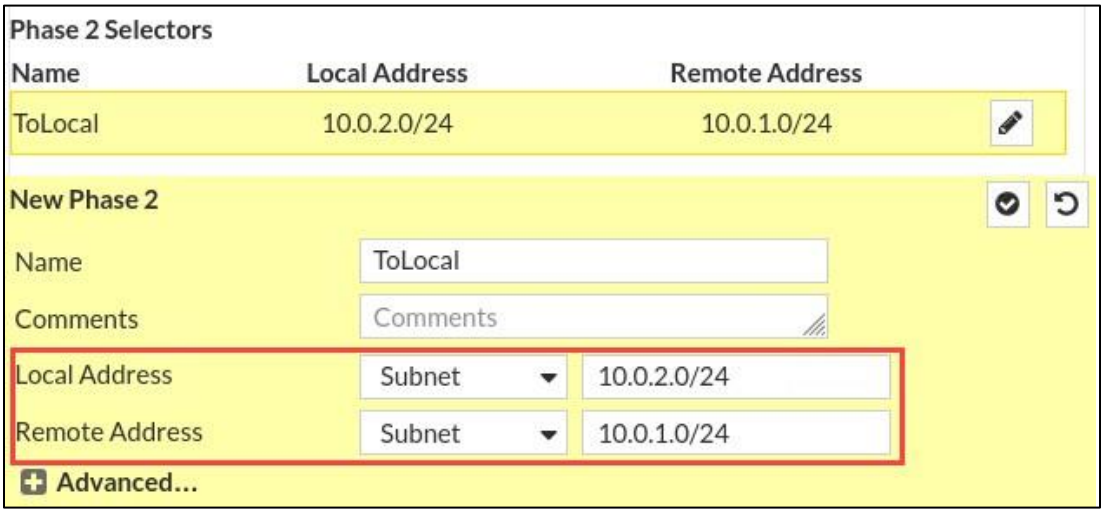
Field	Value
Local ID	Remote-FortiGate



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



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.

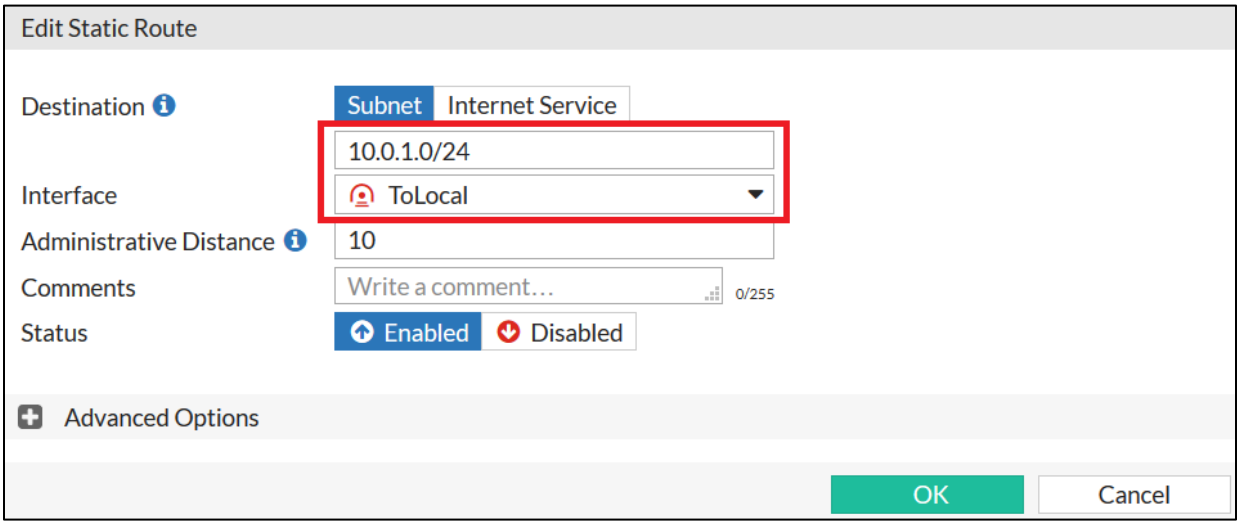
Create a Static Route for VPN Traffic on Remote-FortiGate (Dial-Up Client)

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



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:

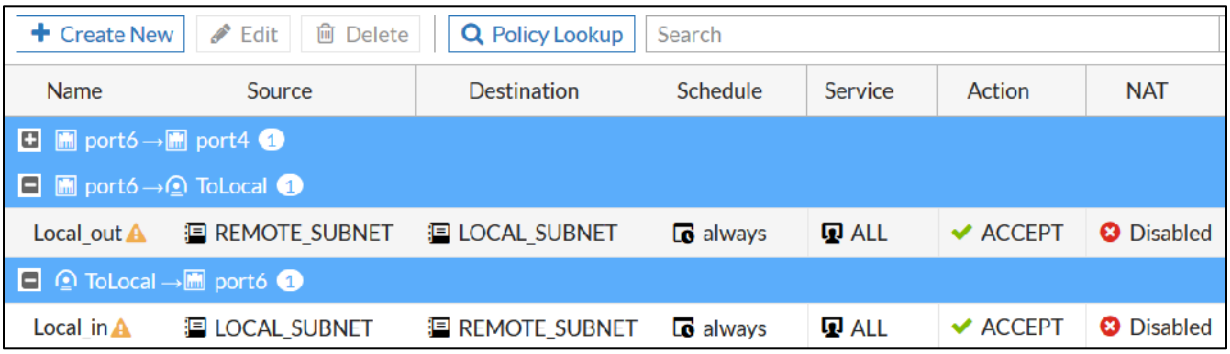
Field	Value
Name	Local_out
Incoming Interface	port6
Outgoing Interface	ToLocal
Source	REMOTE_SUBNET
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

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**.

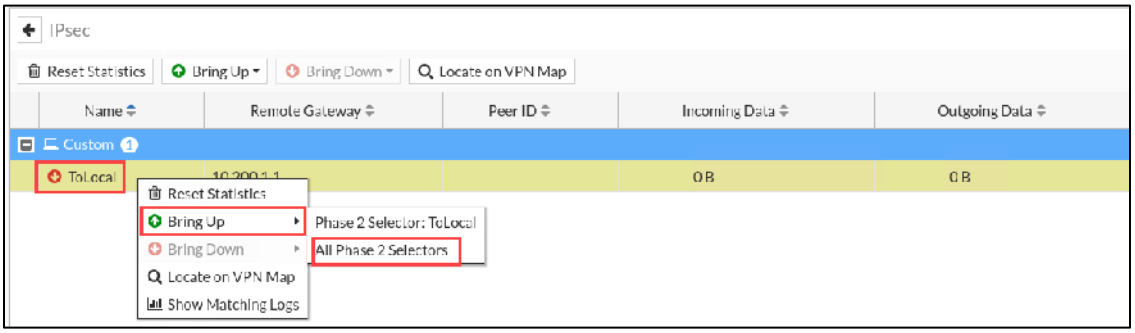


Test and Monitor the VPN

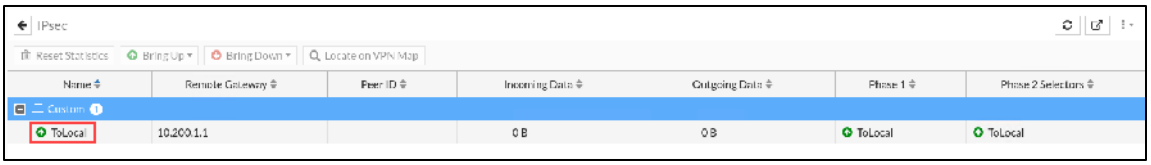
Now that you configured the VPN on both FortiGate devices, you will test the VPN.

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.



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.



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.

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

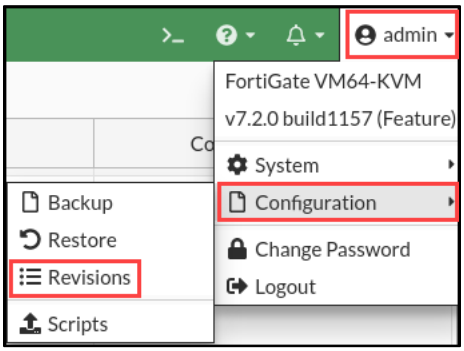
In this exercise, you will configure a static VPN between Local-FortiGate and Remote-FortiGate. You will also configure a static route on Local-FortiGate for VPN traffic.

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

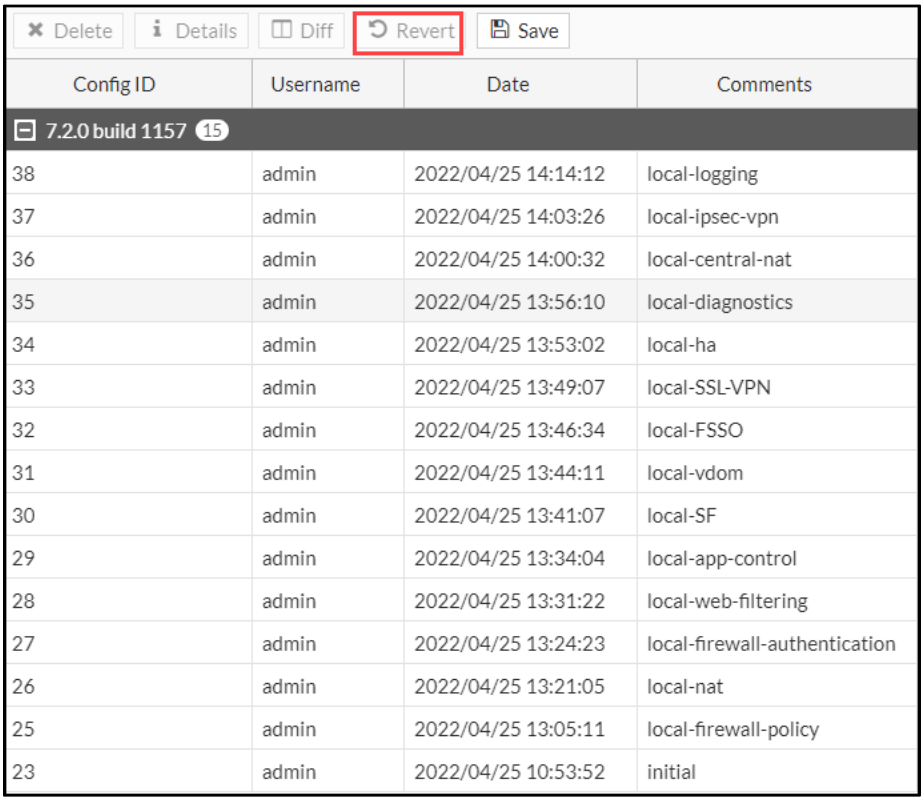
Make sure that you restore the correct configuration on Local-FortiGate, using the following steps. Failure to restore the correct configuration on Local-FortiGate will prevent you from doing the lab exercise.

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**.



Delete | Details | Diff | Revert | Save

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:

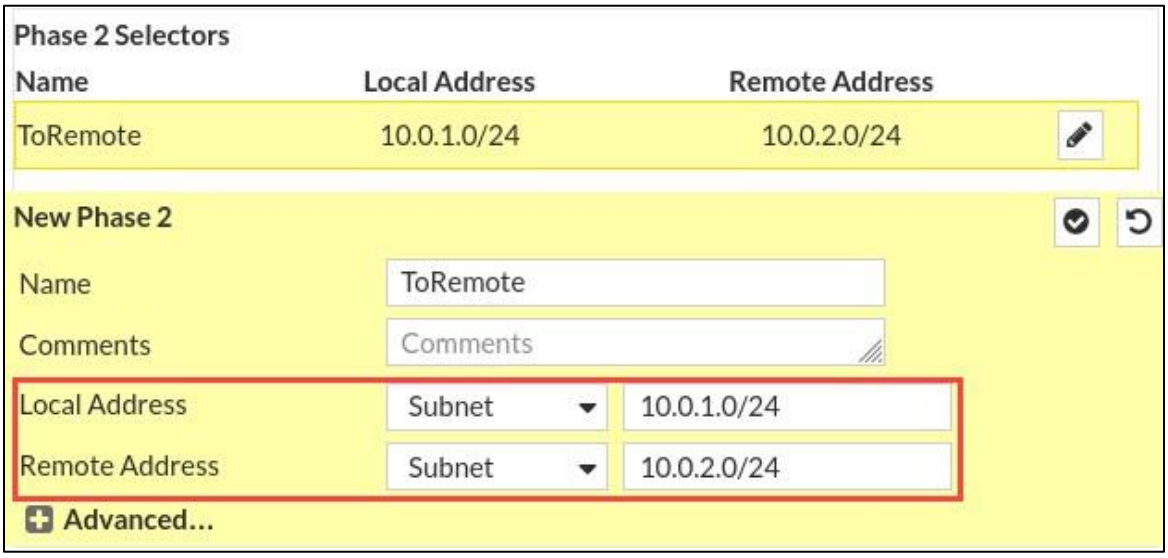
Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Interface	port1
Dead Peer Detection	On Idle

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



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

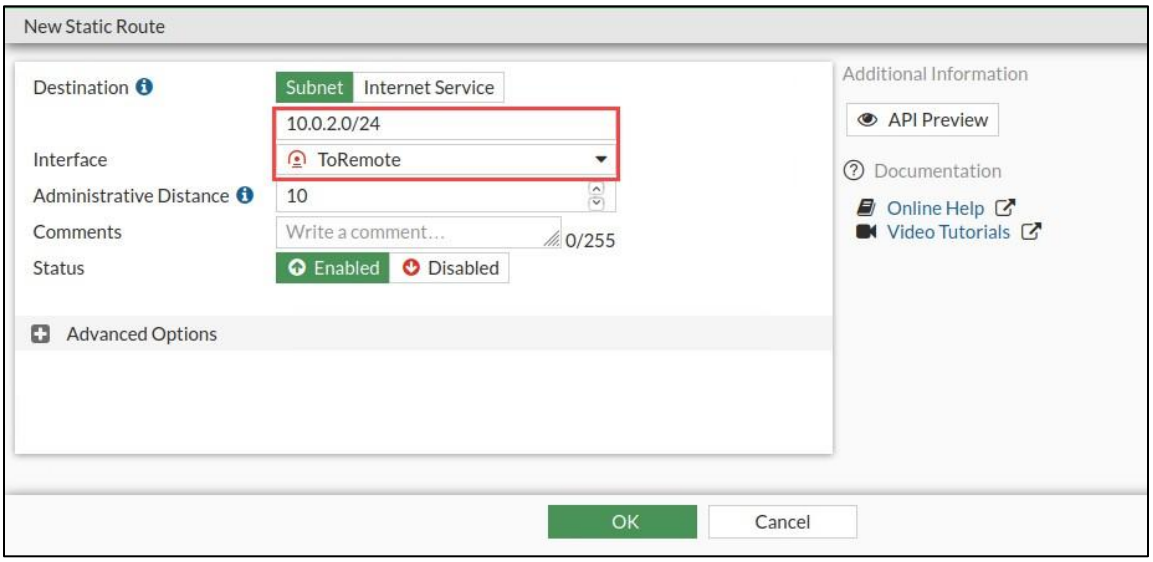
Create a Static Route for VPN Traffic on Local-FortiGate

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



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

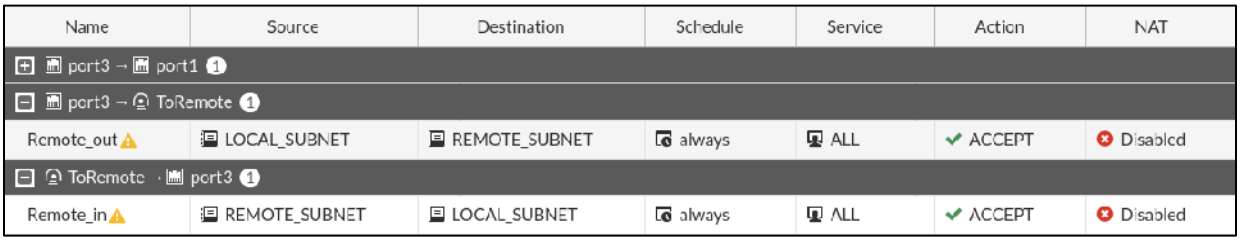
1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**.
3. Configure the following settings:

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

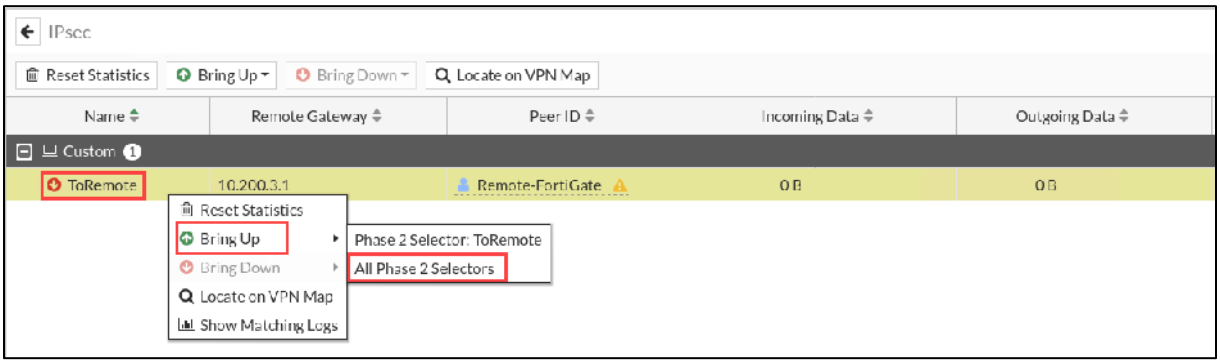
Test and Monitor the VPN

You will test the VPN and monitor its status.

To test the VPN

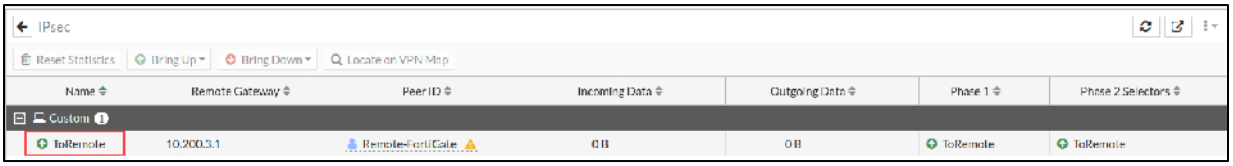
1. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
2. Click the **+** sign beside **Custom** to expand the custom VPN tunnel section.

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



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.

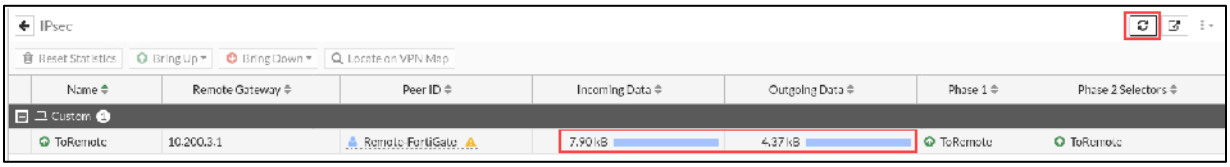


5. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

   ```
   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.



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

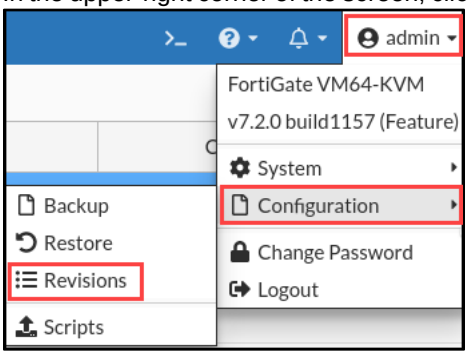
Before beginning this exercise, you must restore a configuration file on Remote-FortiGate.

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.

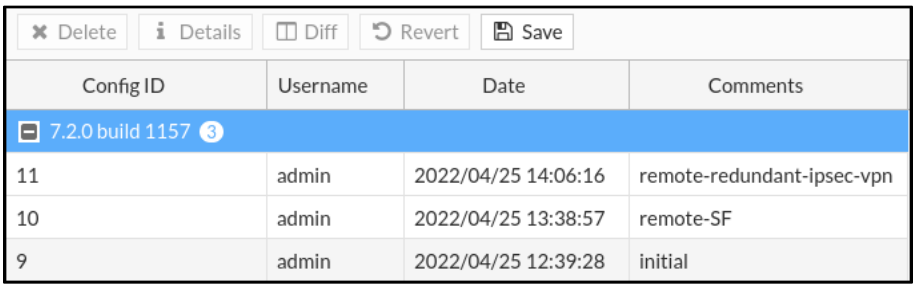
After you load the configurations, Remote-FortiGate will be preconfigured for VPN redundancy. This exercise provides instructions to review the configuration for Remote-FortiGate.

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**.



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.

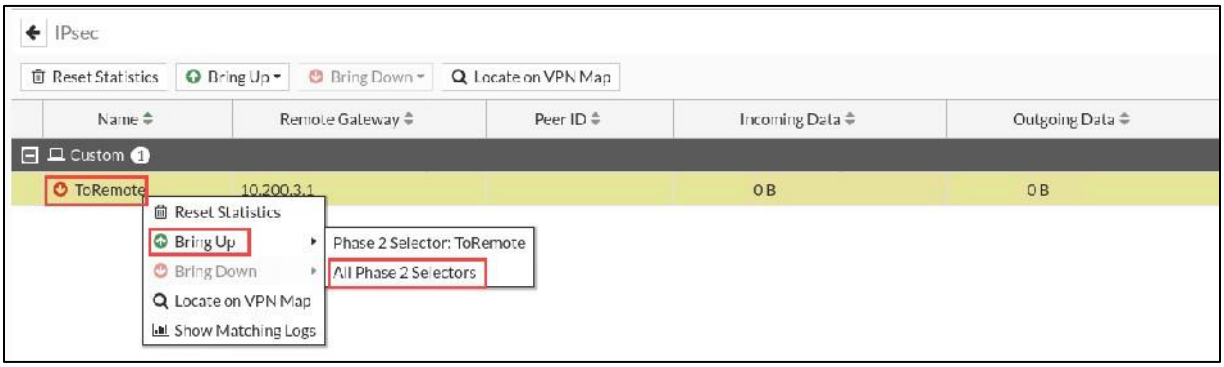
To check the VPN on Local-FortiGate

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.

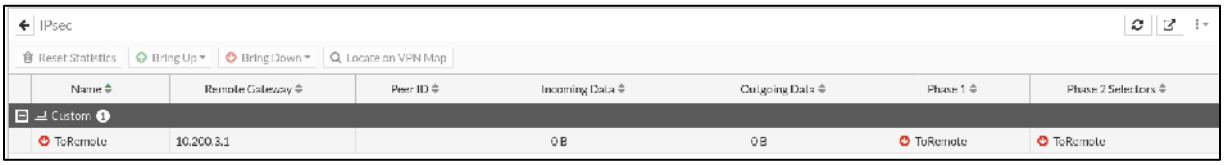
If the **ToRemote** VPN still appears up, wait a few more seconds, and then press `Ctrl+R` to refresh the page. The tunnel will be brought down automatically by dead peer detection (DPD) approximately 60 seconds after the configuration is restored on Remote-FortiGate.

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



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.



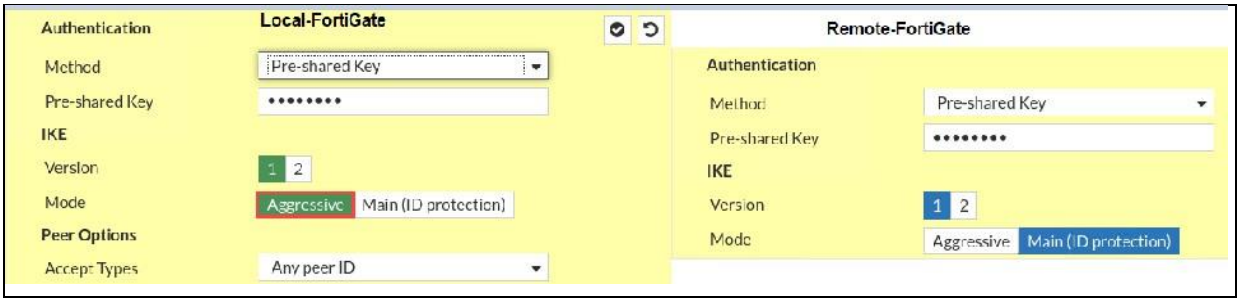
After you restore the configuration on Remote-FortiGate, the configuration for the tunnel on Remote-FortiGate no longer mirrors the configuration on Local-FortiGate, which is why the tunnel does not come up this time. You will fix this in the next procedure.

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.



> **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.

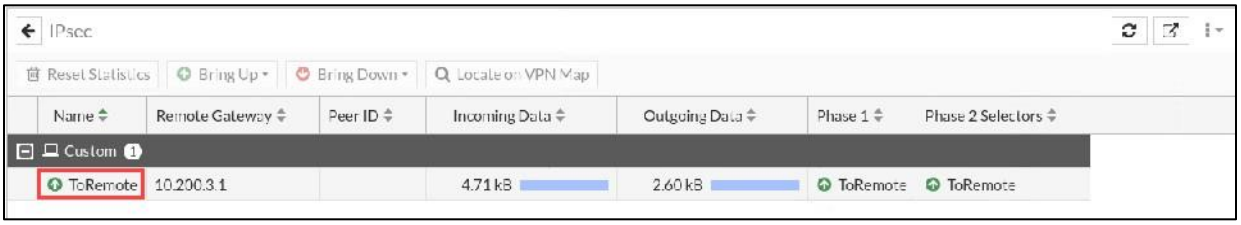
To test the VPN

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.



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:

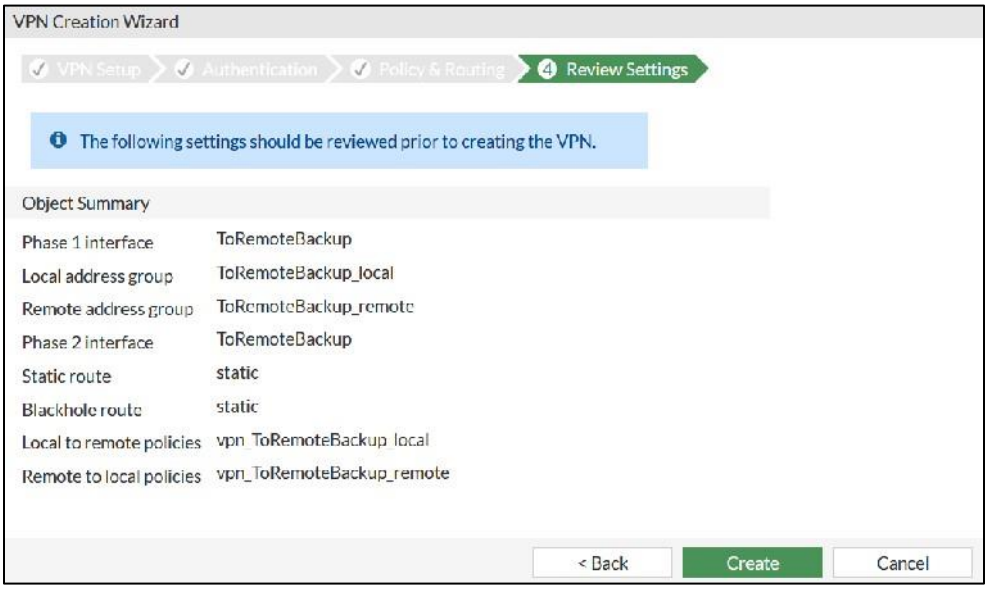
Field	Value
Remote device	IP Address
Remote IP address	10.200.4.1
Outgoing Interface	port2
Authentication method	Pre-shared Key
Pre-shared key	fortinet

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

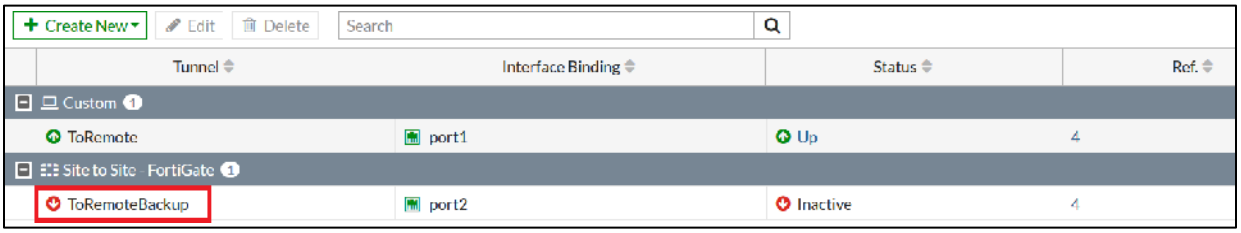
7. Click **Next**.
8. Click **Create**.

   You should see the following screen:



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.



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.

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 6				
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?

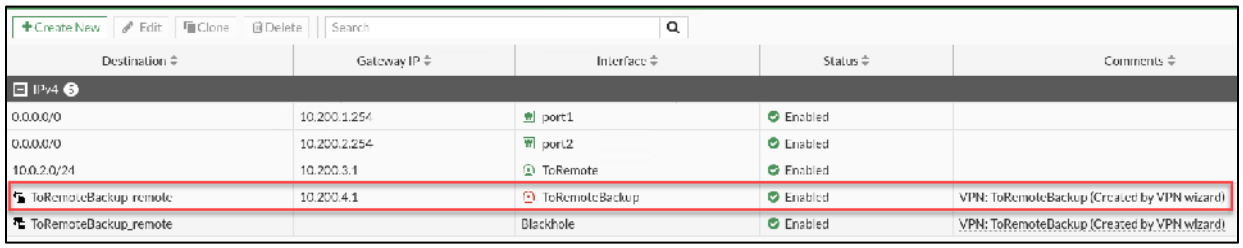
FortiGate drops all packets routed to the blackhole interface. The IPsec wizard added two static routes: one to the IPsec virtual interface, with a distance of 10, and one to the blackhole interface, with a distance of 254. The route with the lowest distance, the one to the IPsec virtual interface, takes 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.

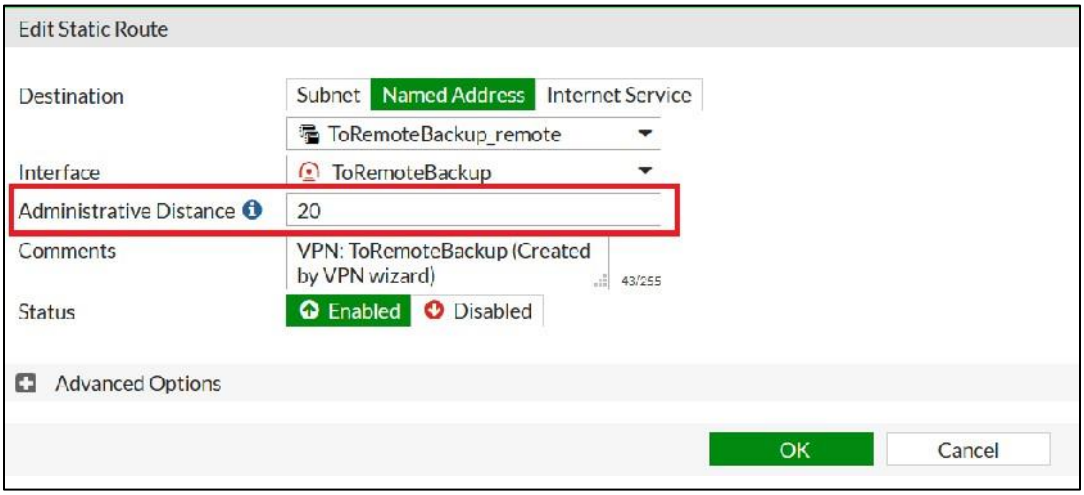
To configure a backup VPN on Local-FortiGate

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



3. Configure the following setting:

Field	Value
Administrative Distance	20



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

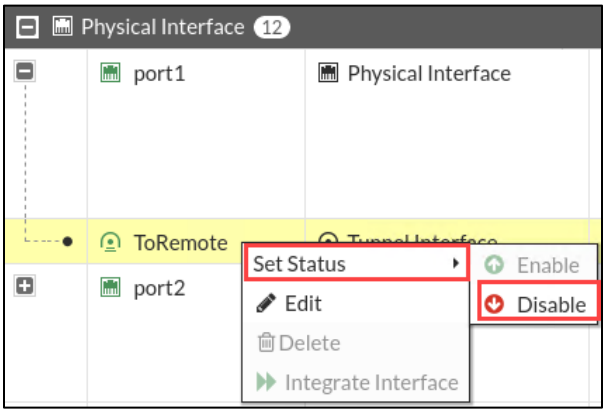
1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to sniff all ICMP traffic to `10.0.2.10` with verbosity `4`:
   ```
   diagnose sniffer packet any 'icmp and host 10.0.2.10' 4
   ```
3. On the Local-Client VM, open a terminal window, 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.



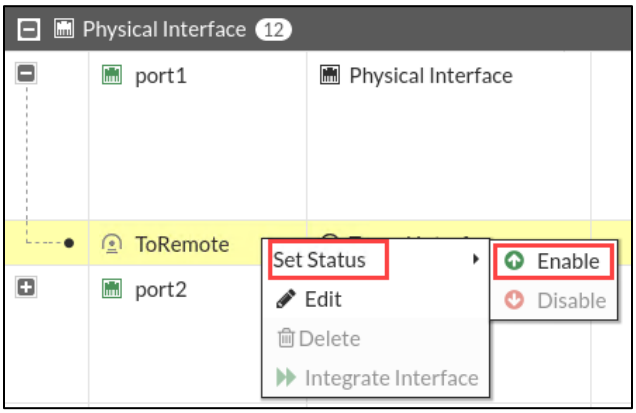
ToRemote is now grayed out.

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.