



Name : Sherif Saad Abd El-Hafez

Email : -321220233@sha.edu.eg

NTI : – (National Telecommunication
Institute)

Code Group :- DEPI_1_CAI1_ISS8_S1e

Code Coaching :- DEPI_1_CAI1_ISS8_S1e

Phone :- 01208825165

Project Fortinet Cybersecurity Engineer

IPSEC VPN CONFIGURATION

Introduction:

A **VPN (Virtual Private Network)** within a firewall acts as a secure tunnel designed to encrypt and protect data transmission between devices or networks, especially over the internet or other public networks. By integrating VPN capabilities, firewalls enhance security by not only monitoring and controlling traffic but also ensuring that connections remain encrypted and safeguarded against unauthorized access or potential threats. This combination of functionality strengthens the overall security posture of the network.

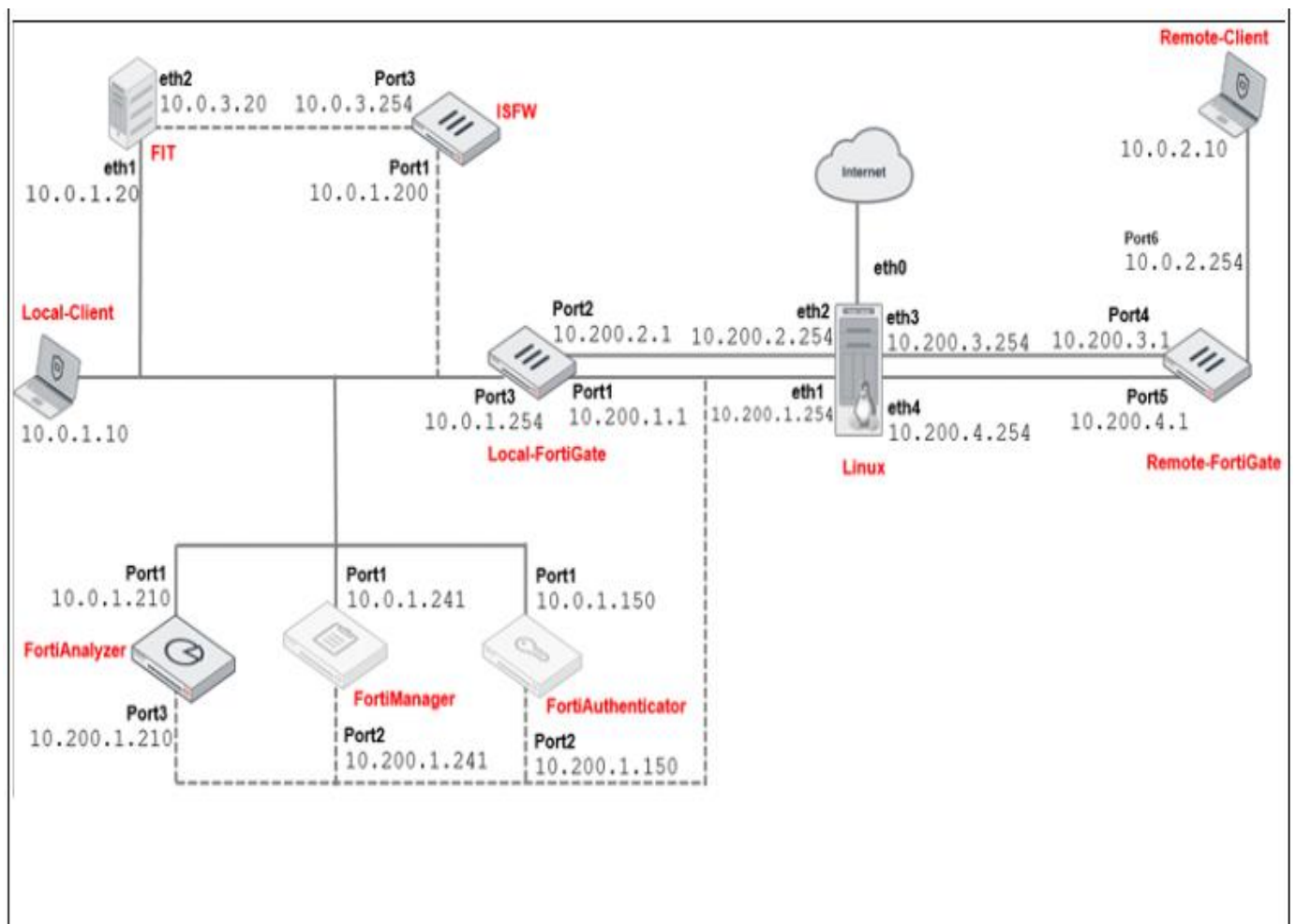
Types of VPN :

1. **Remote Access VPN:**
 - Allows users to connect securely to a private network from any location.
 - Ideal for remote employees accessing company resources.
2. **Site-to-Site VPN:**
 - Connects entire networks (e.g., branch offices and headquarters).
 - Two types: Intranet VPN (within the same organization) and Extranet VPN (with external partners).
3. **SSL VPN:**
 - Provides secure access via a web browser without the need for special software.
 - Suitable for accessing applications securely online.
4. **IPSec VPN:**
 - Secures data through encryption and authentication.
 - Used for safely transmitting data over public networks.
5. **Hybrid VPN:**
 - Combines MPLS performance with VPN encryption.
 - Best for large enterprises needing high speed and security.
6. **Cloud VPN:**
 - Connects users securely to cloud-based applications or services.
 - Perfect for businesses relying on cloud infrastructure.

Objective of the lab

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

Topology :-



Components:

- Local FortiGate
- Remote FortiGate
- Local Client
- Remote Client

Steps :

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

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 `admin`.
2. Click **VPN > IPsec Tunnels**, and then click **Create New > IPsec Tunnel**.
3. Configure the following settings:

New VPN Tunnel

Network

IP Version: IPv4 IPv6

Remote Gateway: Dialup User

Interface: port1

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: Enable Disable Forced

Dead Peer Detection: Disable On Idle On Demand

DPD retry count: 3

DPD retry interval: 60 s

Forward Error Correction: Egress ☐ Ingress ☐

[+ Advanced...](#)

VPN Creation Wizard

1 VPN Setup

Name:

Template type: Site to Site Hub-and-Spoke Remote Access Custom

< Back

Next >

Cancel

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

Authentication

Method
Pre-shared Key

Pre-shared Key
fortinet

IKE

Version
1 2

Mode
Aggressive Main (ID protection)

Peer Options

Accept Types
Specific peer ID

Peer ID
Remote--FortiGate

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	10.0.10.0/24	0.0.0.0/0.0.0.0

New Phase 2

Name
ToRemote

Comments
Comments

Local Address
Subnet 10.0.10.0/24

Remote Address
Subnet 0.0.0.0/0.0.0.0

+ Advanced...

8. Keep the default values for the remaining settings.

9. Click **OK**.

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

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

New Policy

Name

Remote_out

Incoming Interface

port3

Outgoing Interface

ToRemote

Source

LOCAL_SUBNET

+

Destination

REMOTE_SUBNET

+

Schedule

always

Service

ALL

+

Action

ACCEPT

DENY

Inspection Mode

Flow-based

Proxy-based

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

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

Name

Remote_in

Incoming Interface

ToRemote

Outgoing Interface

port3

Source

REMOTE_SUBNET

+

Destination

LOCAL_SUBNET

+

Schedule

always

Service

ALL

+

Action

ACCEPT

DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

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

9. Click **OK**

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Create New

Edit

Delete

Policy Lookup

Search

Q

Export

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
port3 → ToRemote 1								
Remote_out	LOCAL_SUBNET	REMOTE_SUBN...	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
ToRemote → port3 1								
Remote_in	REMOTE_SUBN...	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
Implicit 1								
Implicit Deny	all	all	always	ALL	DENY			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 `admin`.
2. Click **VPN > IPsec Tunnels**, and then click **Create New > IPsec Tunnel**.
3. Configure the following settings

Field	Value
Name	ToLocal
Template type	Custom

Dashboard >
Network >
Policy & Objects >
Security Profiles >
VPN >
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard ☆

VPN Creation Wizard
1 VPN Setup
Name
Template type ☒ Site to Site ☐ Hub-and-Spoke ☐ Remote Access
☒ Custom

Back
Next >
Cancel

4. Click **Next**.

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

Field	Value
Name	ToLocal
Template type	Custom

Dashboard >
Network >
Policy & Objects >
Security Profiles >
VPN >
Overlay Controller VPN
IPsec Tunnels ☆
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication >
System 1 >
Security Fabric >
Log & Report >

New VPN Tunnel
Name
Comments 0/255

Network
IP Version ☒ IPv4 ☐ IPv6
Remote Gateway Static IP Address
IP Address
Interface
Local Gateway ☐
Mode Config ☐
NAT Traversal ☒ Enable ☐ Disable ☐ Forced
Keepalive Frequency
Dead Peer Detection ☐ Disable ☒ On Idle ☐ On Demand
DPD retry count
DPD retry interval s
Forward Error Correction Egress ☐ Ingress ☐
+ Advanced...

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

Dashboard >
 Network >
 Policy & Objects >
 Security Profiles >
 VPN >
 Overlay Controller VPN
 IPsec Tunnels ☆
 IPsec Wizard
 IPsec Tunnel Template
 SSL-VPN Portals
 SSL-VPN Settings
 SSL-VPN Clients
 VPN Location Map
 User & Authentication >

New VPN Tunnel

Authentication

Method

Pre-shared Key

Pre-shared Key

fortinet

IKE

Version

1 2

Mode

Aggressive Main (ID protection)

Peer Options

Accept Types

Any peer ID

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

Field	Value
Local ID	Remote-FortiGate

- Security Profiles >
- VPN** >
- Overlay Controller VPN
- IPsec Tunnels** ☆
- IPsec Wizard
- IPsec Tunnel Template
- SSL-VPN Portals
- SSL-VPN Settings
- SSL-VPN Clients
- VPN Location Map
- User & Authentication >
- System 1 >
- Security Fabric >
- Log & Report >

Phase 1 Proposal

Encryption

DES ▾

Authentication

SHA512 ▾ ✕

Encryption

DES ▾

Authentication

SHA256 ▾ ✕

Encryption

DES ▾

Authentication

MD5 ▾ ✕

Encryption

DES ▾

Authentication

SHA1 ▾ ✕

Encryption

DES ▾

Authentication

SHA384 ▾ ✕

Diffie-Hellman Groups

☐ 32

☐ 31

☐ 30

☐ 29

☐ 28

☐ 27

☐ 21

☐ 20

☐ 19

☐ 18

☐ 17

☐ 16

☐ 15

☒ 14

☒ 5

☐ 2

☐ 1

Key Lifetime (seconds)

87600

Local ID

Remote-FortiGate

XAUTH

Type

Disabled ▾

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:

Local Address: Subnet 10.0.2.0/24

Remote Address: Subnet 10.0.1.0/24

OK Cancel

9. Keep the default values for the remaining settings.

10. Click **OK**.

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

New Static Route

Automatic gateway retrieval ☐

Destination **Subnet** Internet Service
10.0.1.0/24

Interface **ToLocal**

Administrative Distance **1**

Comments Write a comment... 0/255

Status **Enabled** Disabled

Advanced Options

Destination	Gateway IP	Interface	Status	Comments
10.0.1.0/24	10.200.1.1	ToLocal	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

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

New Policy

Name

Local_out

Incoming Interface

port6

Outgoing Interface

ToLocal

Source

REMOTE_SUBNET

Destination

REMOTE_SUBNET

Schedule

always

Service

ALL

Action

ACCEPT

DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

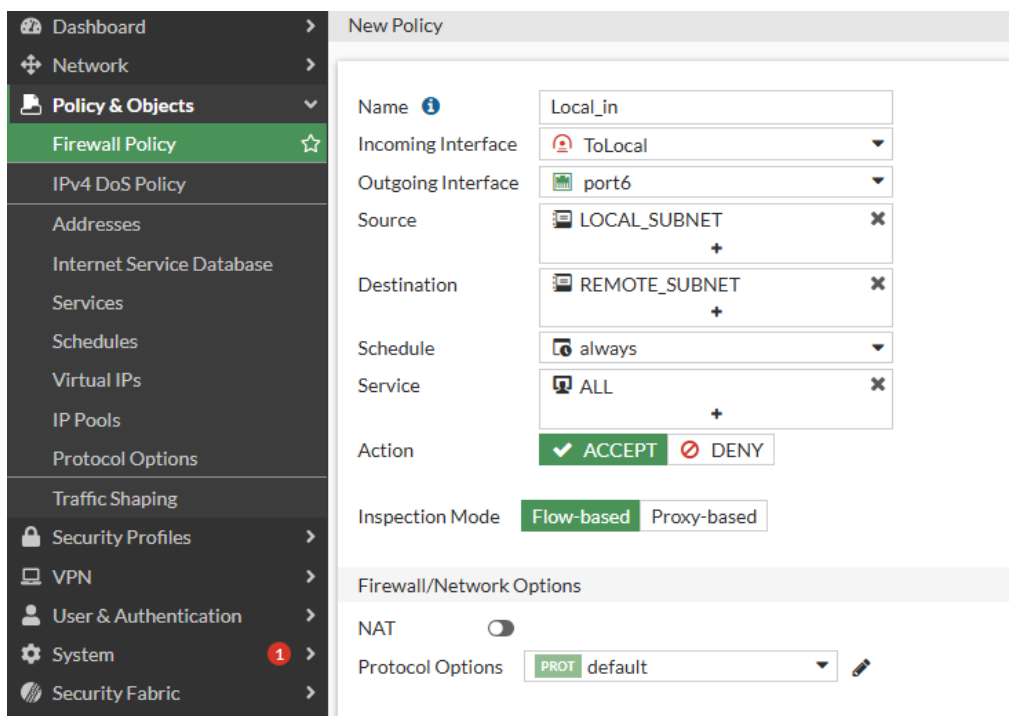
Protocol Options

PRDT default

- 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**.

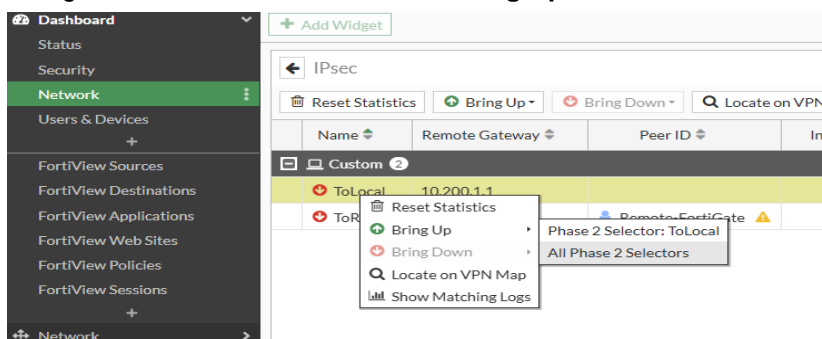
Name	Source	Destination	Schedule	Service	Action	NAT
port6 → port4	port6	port4				
port6 → ToLocal	port6	ToLocal				
Local_out	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled
ToLocal → port6	ToLocal	port6				
Local in	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	ACCEPT	Disabled

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.

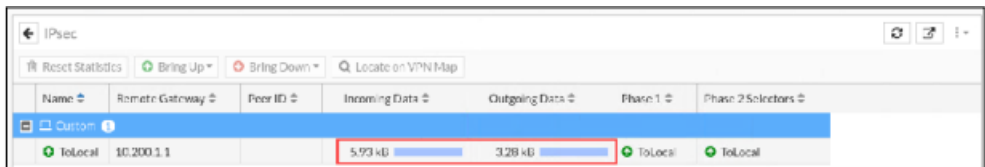


4. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

```
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.



Testing the lab

- 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	to:remote	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
1/2.16.100.0/24	0.0.0.0	port3	0	Connected

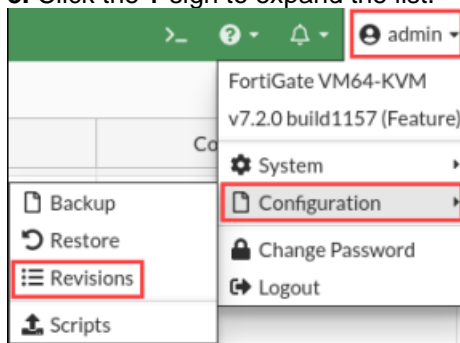
- 9. On the Remote-Client VM, press **Ctrl+C** to stop the ping

2) Configuring a Static IPsec VPN Between Two FortiGate Devices

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.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `admin`.
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
7.2.0 build 1157 15	
38	admin
37	admin
36	admin
35	admin
34	admin
33	admin
32	admin
31	admin
30	admin
29	admin
28	admin
27	admin
26	admin
25	admin
23	admin

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

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 10.200.3.1

Interface: port1

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: **Enable** Disable Forced

Keepalive Frequency: 10

Dead Peer Detection: **On idle** Disable On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

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

Edit Phase 2

Name: ToRemote

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

Dashboard
Network
Interfaces
DNS
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects

Edit Static Route
Automatic gateway retrieval ☐
Destination Internet Service
Interface
Administrative Distance
Comments
Status ☒ Enabled ☐ Disabled
Advanced Options

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
Destination	Subnet 10.0.2.0/24
Interface	ToRemote

Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric

Edit Policy
Name
Incoming Interface
Outgoing Interface
Source
Destination
Schedule
Service
Action ☒ ACCEPT ☐ DENY
Inspection Mode ☒ Flow-based ☐ Proxy-based
Firewall/Network Options
NAT ☐
Protocol Options

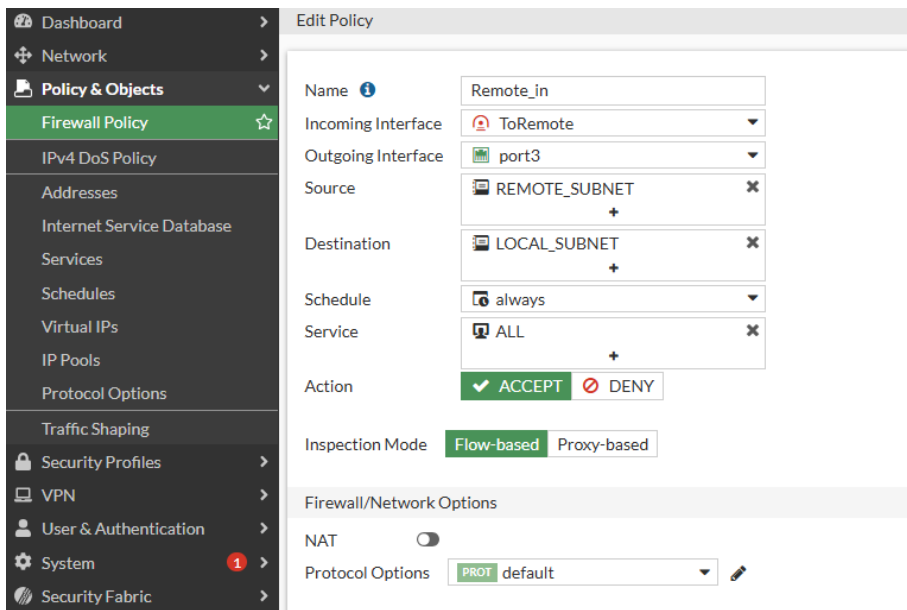
4. In the **Firewall/Network Options** section, disable **NAT**.

5. Click **OK**.

6. Click **Create New** again.

7. Configure the following settings:

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



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

9. Click **OK**.

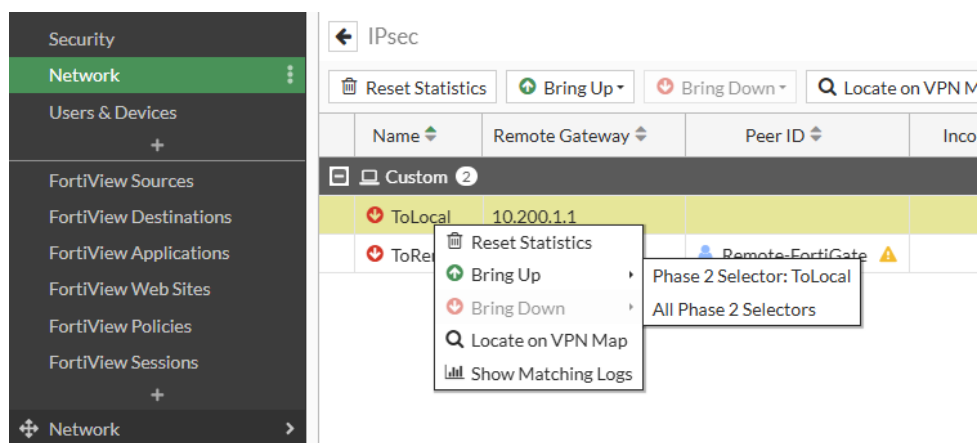
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port3 → ToRemote	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
port6 → ToLocal	LOCAL_SUBNET	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
ToLocal → port6	LOCAL_SUBNET	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
ToRemote → port3	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Remote_in	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Implicit									

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.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selector
ToLocal	10.200.1.1	RemoteFortiGate	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
Tunnel1	10.200.3.1	Remote-FortiGate	7.90 KiB	4.37 KiB	Tunnel1

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

3) Configuring Redundant Static IPsec VPN Tunnels Between Two FortiGate Devices

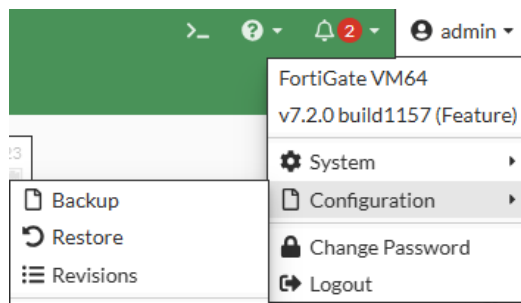
In this exercise, you will configure one more VPN tunnel between Local-FortiGate and Remote-FortiGate for redundancy purposes. You must first restore a configuration file on Remote-FortiGate.

Prerequisites

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

To restore the Remote-FortiGate configuration file

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

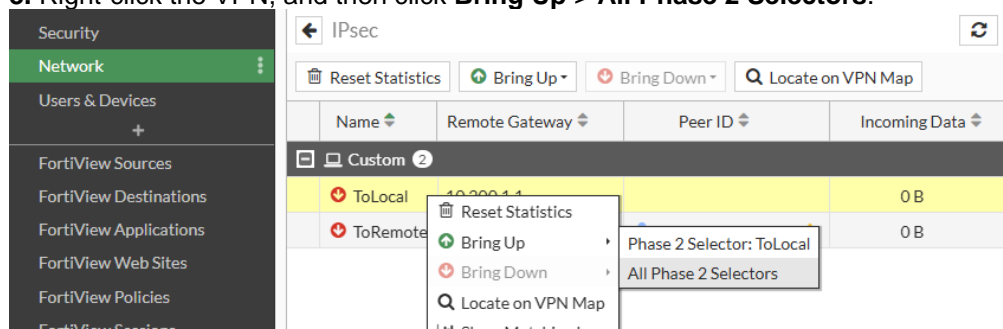
Check the IPsec VPN Tunnel on Local-FortiGate

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

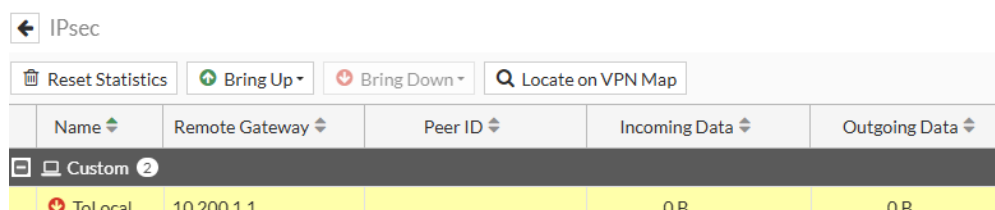
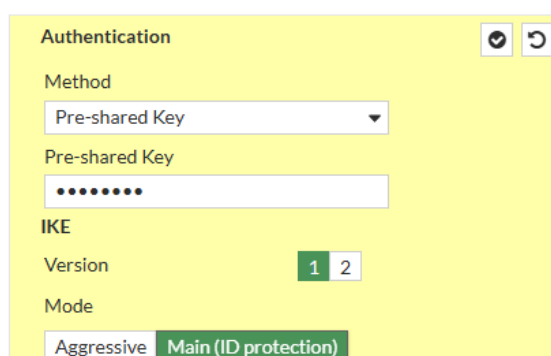
To check the VPN on Local-FortiGate

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.

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.



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 LocalFortiGate 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.

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: 1 2

Mode: Aggressive Main (ID protection)

Peer Options

Accept Types: Any peer ID

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: 1 2

Mode: Aggressive Main (ID protection)

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)

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: 1 2

Mode: Aggressive 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.
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.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
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

Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric

VPN Creation Wizard

1 VPN Setup
2 Authentication
3 Policy & Routing
4 Review Settings

Name
ToRemoteBackup
Template type
Site to Site
Hub-and-Spoke
Remote Access
Custom
NAT configuration
No NAT between sites
This site is behind NAT
The remote site is behind NAT
Remote device type
FortiGate
Cisco

Site to Site - 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

Click **Next**.

Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map

VPN Creation Wizard

1 VPN Setup
2 Authentication
3 Policy & Routing
4 Review Settings

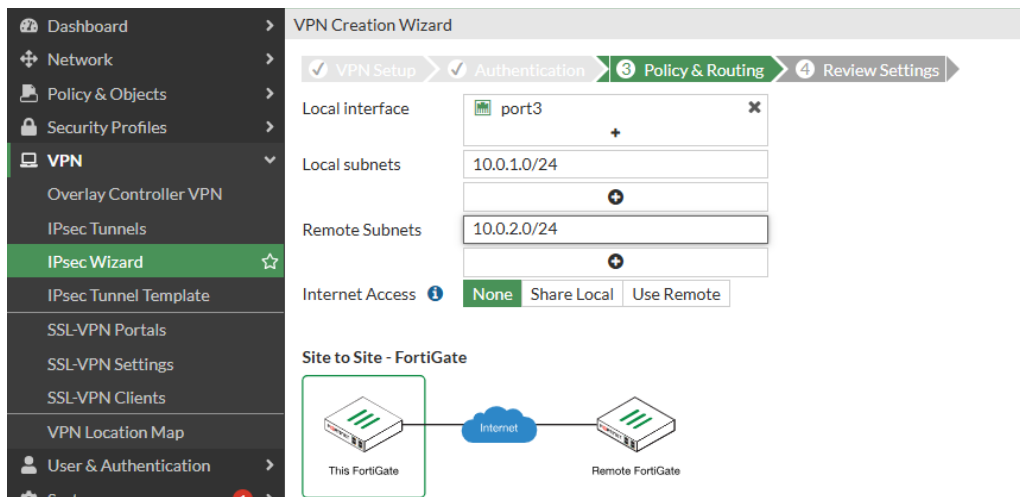
Remote device
IP Address
Dynamic DNS
Remote IP address
10.200.4.1
Outgoing Interface
port2
Authentication method
Pre-shared Key
Signature
Pre-shared key
.....

Site to Site - FortiGate

5. Click **Next**.

6. Configure the following settings:

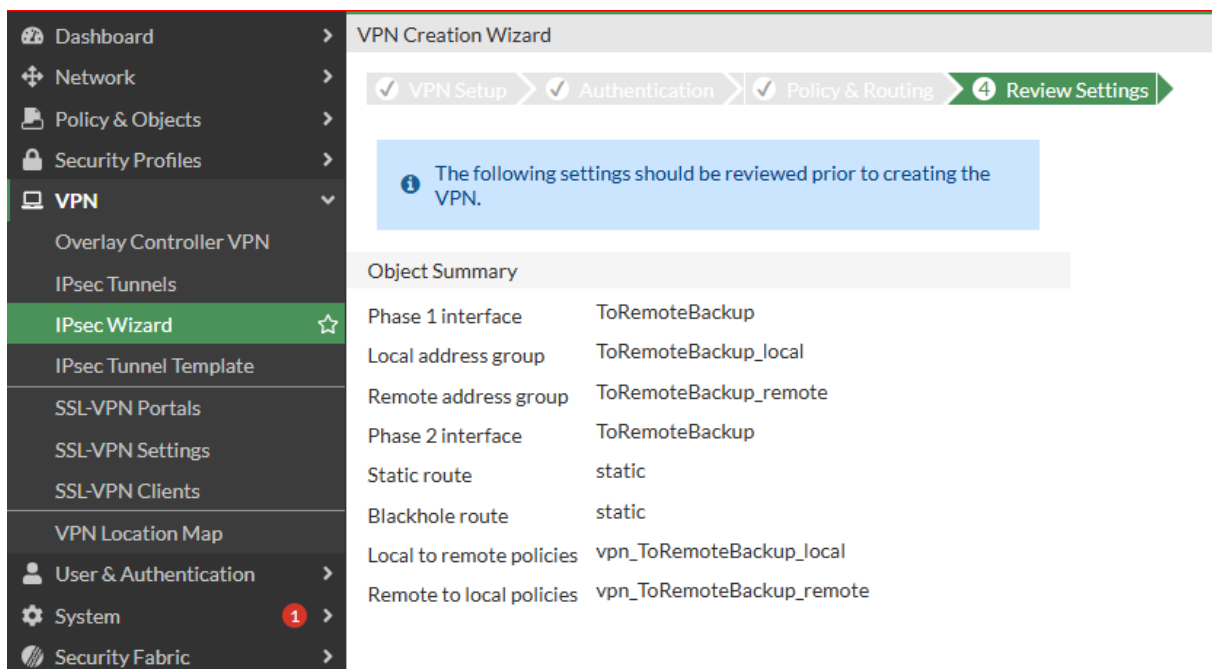
Field	Value
Local interface	port3
Local subnets	10.0.1.0/24
Remote Subnets	10.0.2.0/24
Internet Access	None



7. Click **Next**.

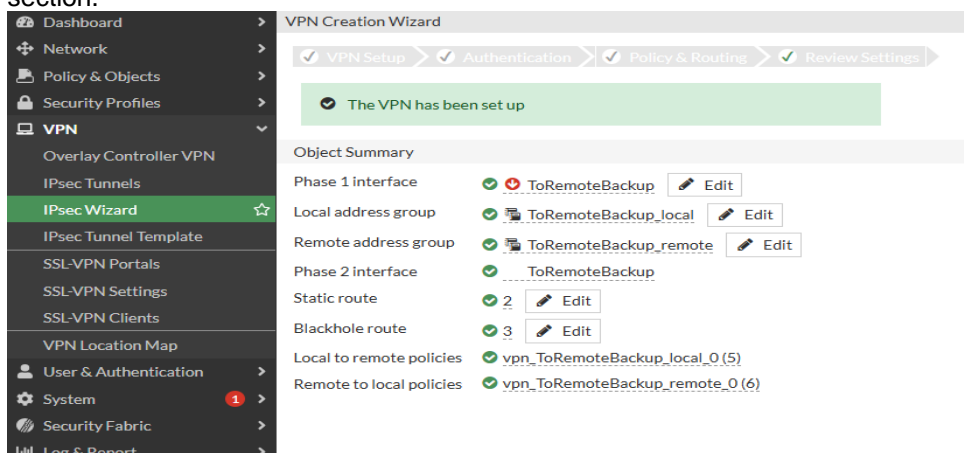
8. Click **Create**.

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.

+ Create New ▾		✎ Edit		✕ Delete		Search		Q	
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.

The screenshot shows the FortiGate GUI with the left sidebar menu expanded to 'VPN > IPsec Tunnels'. The 'ToRemoteBackup' tunnel is selected. The main panel displays the 'Edit VPN Tunnel' configuration for 'ToRemoteBackup'. The configuration includes:

- Tunnel Template:** Site to Site - FortiGate
- Convert To Custom Tunnel:** Button
- Name:** ToRemoteBackup
- Comments:** VPN: ToRemoteBackup (Created by VPN wizard)
- Network:** Remote Gateway: Static IP Address (10.200.4.1), Outgoing Interface: port2
- Authentication:** Authentication Method: Pre-shared Key
- Phase 2 Selectors:** Local Address: ToRemoteBackup_local, Remote Address: 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

FortiGate-VM64	
Dashboard	
Network	
Policy & Objects	
Firewall Policy	
IPv4 DoS Policy	
Addresses	
Internet Service Database	
Services	
Schedules	
Virtual IPs	
IP Pools	
Protocol Options	
Traffic Shaping	
Security Profiles	
VPN	
User & Authentication	
System	
Security Fabric	
Log & Report	

Name	Details
IP Range/Subnet 10	
FABRIC_DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTA...	0.0.0.0/0
LOCAL_SUBNET	0.0.0.0/0
REMOTE_SUBNET	0.0.0.0/0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134....
ToRemote	10.0.1.0/24
ToRemoteBackup_local_su...	10.0.1.0/24
ToRemoteBackup_remote_...	10.0.2.0/24
all	0.0.0.0/0
none	0.0.0.0/32
FQDN 6	
gmail.com	gmail.com
login.microsoft.com	login.microsoft.com
login.microsoftonline.com	login.microsoftonline.com
login.windows.net	login.windows.net
wildcard.dropbox.com	*.dropbox.com

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**.

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Create New

Edit

Delete

Policy Lookup

Search

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port3 → ToRemote									
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
port3 → ToRemoteBackup									
port6 → ToLocal									
ToLocal → port6									
ToRemote → port3									
Remote_in	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
ToRemoteBackup → port3									
Implicit									

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

SD-WAN	ToRemoteBackup_remote	10.200.4.1	ToRemoteBackup	✓ Enabled	VPN: ToRemoteBackup (Create...
Static Routes	ToRemoteBackup_remote		Blackhole	✓ Enabled	VPN: ToRemoteBackup (Create...

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.

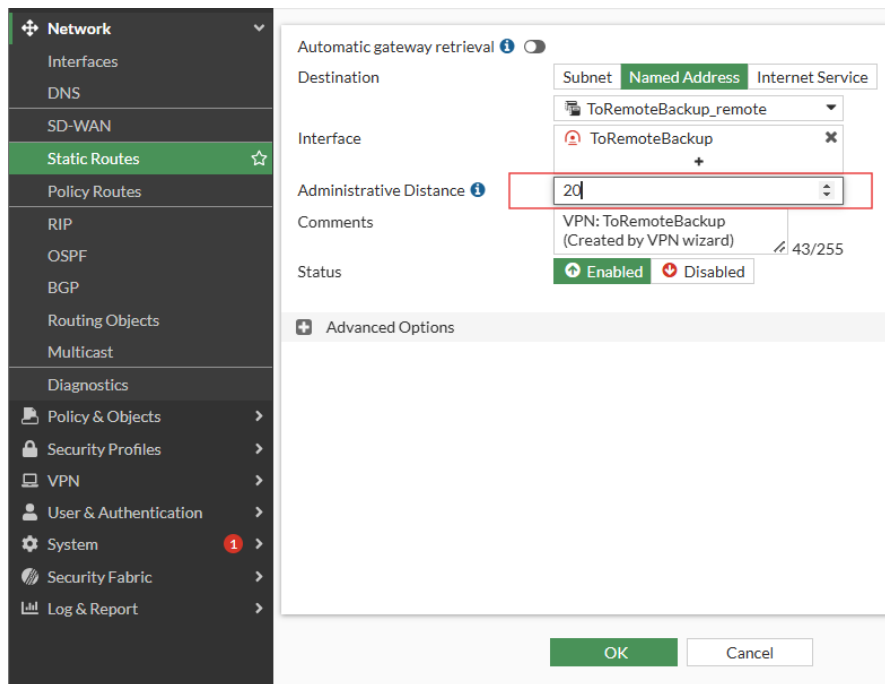
To configure a backup VPN on Local-FortiGate

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

SD-WAN	ToRemoteBackup_remote	10.200.4.1	ToRemoteBackup	✓ Enabled	VPN: ToRemoteBackup (Create...
Static Routes	ToRemoteBackup_remote		Blackhole	✓ Enabled	VPN: ToRemoteBackup (Create...

4. 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

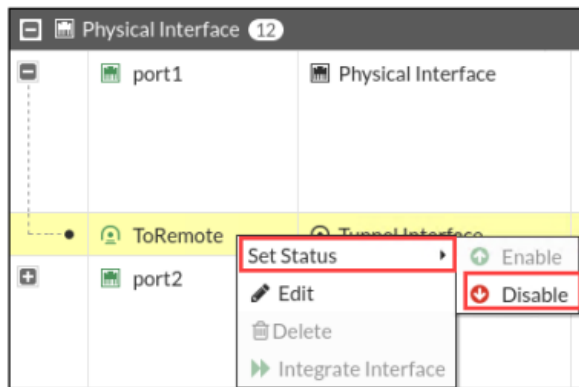
1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to sniff all ICMP traffic to `10.0.2.10` with verbosity 4:
`diagnose sniffer packet any 'icmp and host 10.0.2.10' 4`
3. On the Local-Client VM, open a terminal window, and then run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

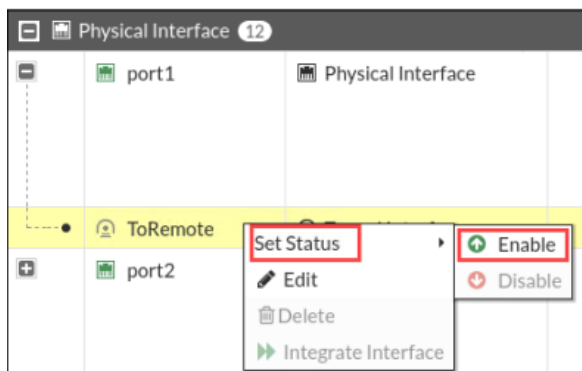
Notice that the **ToRemoteBackup** VPN is being used now.

```
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.