

# Documentation: Configuring IPsec VPN on FortiGate Devices

## Author

- **Name:** Ammar Ahmed Sayed Mohamed
- **National ID:** 30302162500938
- **Student No:** 21014507
- **Email:** 11410120215020@stud.cu.edu.eg
- **LinkedIn:** [Ammar Ahmed](#)
- **City:** Giza
- **Organization:** NTI

## Overview

This lab guides you through the configuration of site-to-site IPsec VPN tunnels between two FortiGate devices. You'll configure a dial-up VPN and a static VPN to enable secure communication between two networks.

## Objectives

- Configure a site-to-site VPN on FortiGate devices.
- Implement both dial-up and static VPN setups.

## Estimated Completion Time

40 minutes

## Exercise 1: Configuring a Dial-Up IPsec VPN

In this exercise, you will set up a dial-up VPN where **Local-FortiGate** acts as the VPN server and **Remote-FortiGate** as the client.

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

1. Log in to Local-FortiGate.
2. Navigate to **VPN > IPsec Tunnels > Create New**.
3. Configure the following:
  - **Name:** ToRemote
  - **Template Type:** Custom
  - **Remote Gateway:** Dialup User
  - **Interface:** port1
  - **Authentication:** Pre-shared Key ( fortinet )
  - **Accept Types:** Specific Peer ID ( Remote-FortiGate )
4. Define Phase 2 Selectors:
  - **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

addr\_subnet

10.0.1.0/24

Remote Address

addr\_subnet

0.0.0.0/0.0.0.0

Advanced...

💡 **Note:** For scalability, set the remote address to `0.0.0.0/0` to accommodate multiple peers.

## Step 2: Create Firewall Policies on Local-FortiGate

1. Navigate to **Policy & Objects > Firewall Policy > Create New**.
2. Configure **Remote\_out** policy:
  - **Incoming Interface:** `port3`
  - **Outgoing Interface:** `ToRemote`
  - **Source:** `HQ_SUBNET`
  - **Destination:** `BRANCH_SUBNET`
  - **NAT:** Disabled
3. Repeat to configure **Remote\_in**, reversing the traffic flow.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
+ port3 → port1 1							
port3 → ToRemote 1							
2	Remote_out	HQ_SUBNET	BRANCH_SUBNET	always	ALL	ACCEPT	Disabled
ToRemote → port3 1							
3	Remote_in	BRANCH_SUBNET	HQ_SUBNET	always	ALL	ACCEPT	Disabled

## Step 3: Create Phase 1 and Phase 2 on Remote-FortiGate (Dial-Up Client)

1. Log in to Remote-FortiGate.
2. Navigate to **VPN > IPsec Tunnels > Create New**.
3. Configure the following:
  - **Name:** `ToLocal`
  - **Remote Gateway:** Static IP ( `10.200.1.1` )
  - **Authentication:** Pre-shared Key ( `fortinet` )
  - **Local ID:** `Remote-FortiGate`
4. Define Phase 1 Proposal:



ID	Name	Source	Destination	Schedule	Service	Action	NAT
<div> <div>+</div> <div>port6 → port4 1</div> </div>							
<div> <div>-</div> <div>port6 → ToLocal 1</div> </div>							
2	Local_out	4 BRANCH_SUBNET	4 HQ_SUBNET	always	ALL	ACCEPT	Disabled
<div> <div>-</div> <div>ToLocal → port6 1</div> </div>							
3	Local_in	4 HQ_SUBNET	4 BRANCH_SUBNET	always	ALL	ACCEPT	Disabled

## Step 5: Test and Monitor the VPN

- Bring up the tunnel from Remote-FortiGate.

← IPsec

↺ Reset Statistics

⬆ Bring Up

⬇ Bring Down

🔍 Search

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

↺ Reset Statistics

⬆ Bring Up

⬇ Bring Down

🔍 Locate on VPN Map

Phase 2 Selector: ToLocal

All Phase 2 Selectors

← IPsec

🔍 Search

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

- Test connectivity by pinging 10.0.1.10 from 10.0.2.10 .

← IPsec

🔍 Search

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

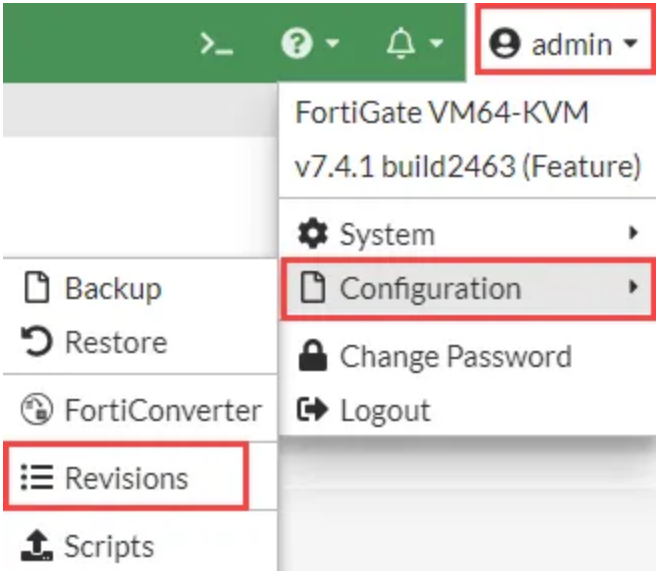
Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.0.2.0/24		ToRemote	15	Static
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

## Exercise 2: Configuring a Static IPsec VPN

In this exercise, you'll configure a static VPN between Local-FortiGate and Remote-FortiGate.

### Step 1: Restore Configuration on Local-FortiGate

- Navigate to **Configuration > Revisions**.



2. Select the revision with the comment `local-ipsec-vpn` , and click **Revert**.

Delete Details Diff Revert Save Changes ⚠			
Config ID	Username	Date	Comments
7.4.1 build 2463 16			
61	admin	2023/10/16 09:27:26	local-SD-WAN
60	admin	2023/10/16 09:21:29	local-dialup
59	admin	2023/10/16 09:08:03	local-app-control
58	admin	2023/10/16 09:04:05	local-av
57	admin	2023/10/16 08:57:55	local-Certificate
56	admin	2023/10/16 08:44:28	routing
55	admin	2023/10/13 11:42:45	local-ha
54	admin	2023/10/13 11:30:48	local-diagnostics
53	admin	2023/10/13 11:21:28	local-SF
52	admin	2023/10/13 11:07:35	local-ipsec-vpn
51	admin	2023/10/13 10:44:02	local-SSL-VPN
50	admin	2023/10/13 10:39:02	local-web-filtering
49	admin	2023/10/13 10:21:09	local-FSSO
48	admin	2023/10/13 10:18:10	local-firewall-authentication
47	admin	2023/10/13 10:12:49	local-firewall-policy
42	admin	2023/10/13 09:29:56	initial

## Step 2: Create Phase 1 and Phase 2 on Local-FortiGate

1. Log in to Local-FortiGate.
2. Navigate to **VPN > IPsec Tunnels > Create New**.
3. Configure:
  - **Name:** `ToRemote`
  - **Remote Gateway:** Static IP ( `10.200.3.1` )
  - **Interface:** `port1`
4. Define Phase 2 Selectors:
  - **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

addr\_subnet

10.0.1.0/24

Remote Address

addr\_subnet

10.0.2.0/24

+ Advanced...

### Step 3: Create a Static Route on Local-FortiGate

1. Navigate to **Network > Static Routes > Create New**.
2. Configure:
- **Destination:** 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...

Status

Enabled

Disabled

+ Advanced Options

OK

Cancel

### Step 4: Create Firewall Policies on Local-FortiGate

1. Create a policy ( Remote\_out ) for traffic from port3 to ToRemote.
2. Right-click Remote\_out, and create a reverse policy ( Remote\_in ).

port3 → ToRemote 1

2

Remote\_out

LOCAL SUBNET

+ Implicit 1

Policy

Filter by Name

Set Status

Copy

Paste

Insert empty policy

Create reverse policy

Show matching logs

Show in FortiView

Edit

Edit in CLI

Delete policy

+ port3 → ToRemote 1						
- ToRemote → port3 1						
3		4 BRANCH_SUBNET	4 HQ_SUBNET	always	ALL	ACCEPT

ID	Name	Source	Destination	Schedule	Service	Action	NAT
+ port3 → port1 1							
- port3 → ToRemote 1							
2	Remote_out	4 HQ_SUBNET	4 BRANCH_SUBNET	always	ALL	ACCEPT	Disabled
- ToRemote → port3 1							
3	Remote_in	4 BRANCH_SUBNET	4 HQ_SUBNET	always	ALL	ACCEPT	Disabled

## Testing the Static VPN

- Verify tunnel status on the Dashboard.

← IPsec

Reset Statistics

Bring Up

Bring Down

Search

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

Reset Statistics

Bring Up

Bring Down

Locate on VPN Map

Phase 2 Selector: ToRemote

All Phase 2 Selectors

← IPsec

Search

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

- Generate traffic to confirm encrypted communication between subnets.

← IPsec

Search

	Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1							
	ToRemote	10.200.3.1	Remote-FortiGate	8.4 kB	8.4 kB	ToRemote	ToRemote

This lab provides foundational knowledge for configuring and managing IPsec VPNs using FortiGate devices. Both dial-up and static VPNs allow secure and scalable connectivity between sites.