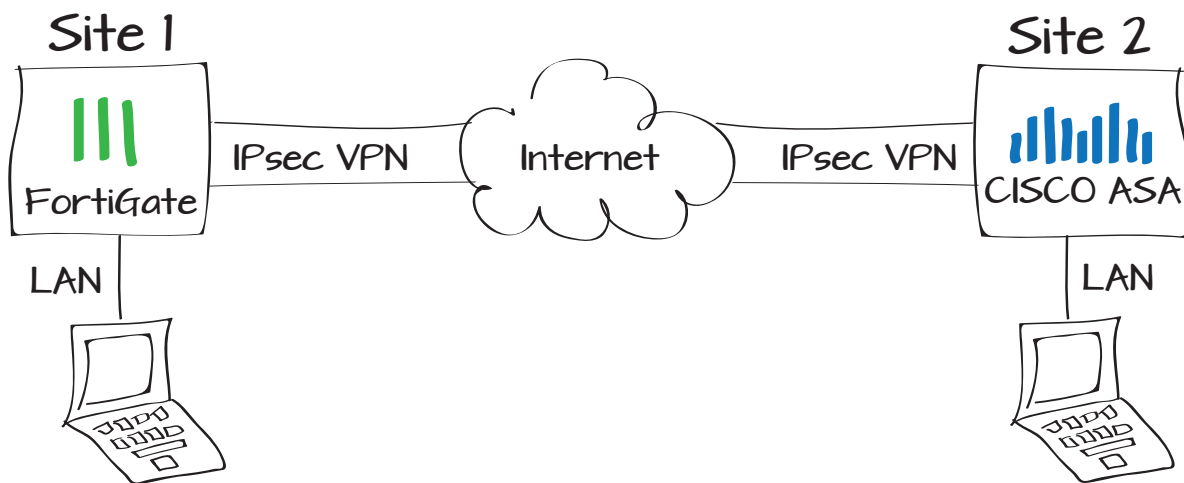


# Configuring IPsec VPN with a FortiGate and a Cisco ASA

The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is behind a Cisco ASA. Using FortiOS 5.0 and Cisco ASDM 6.4, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied. The procedure assumes that both devices are configured with appropriate internal and external interfaces.

1. Configuring the Cisco device using the IPsec VPN Wizard
2. Configuring the FortiGate tunnel phases
3. Configuring the FortiGate policies
4. Configuring the static route in the FortiGate
5. Results



## Configuring the Cisco device using the IPsec VPN Wizard

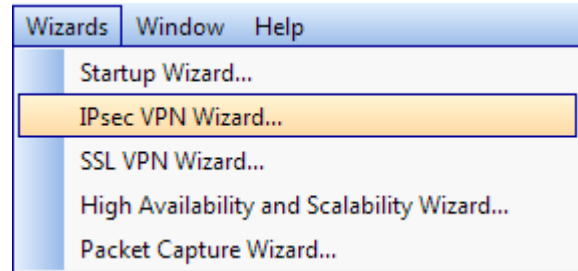
In the Cisco ASDM, under the **Wizard** menu, select **IPsec VPN Wizard**.

From the options that appear, select **Site-to-site**, with the **VPN Tunnel Interface** set to **outside**, then click **Next**.

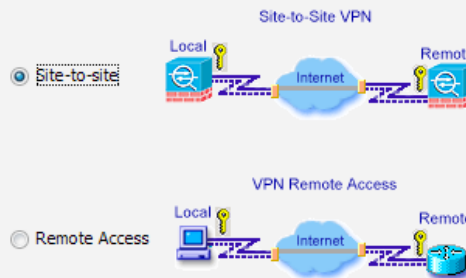
In the **Peer IP Address** field, enter the IP address of the FortiGate unit through which the SSL VPN traffic will flow.

Under **Authentication Method**, enter a secure **Pre-Shared Key**. You will use the same key when configuring the FortiGate tunnel phases. Choose something more secure than “Password”.

When you are satisfied, click **Next**.



VPN Tunnel Type:



VPN Tunnel Interface:

Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel.

Peer IP Address:

Authentication Method

Pre-shared key

Pre-Shared Key:

Certificate

Certificate Signing Algorithm:

Certificate Name:

The next steps in the IPsec VPN Wizard is to establish the tunnel phases 1 and 2.



The encryption settings established here must match the encryption settings configured later in the FortiGate.

Configure Phase 1 with **AES-256 Encryption** and **SHA Authentication**.

Set the **Diffie-Hellman Group** to **5**.

Configure Phase 1 with **AES-256 Encryption** and **SHA Authentication**.

Enable **PFS** and set the **Diffie-Hellman Group** to **2**.

Click **Next**.

Set the **Local Network** and **Remote Network**.

Click **Next** and review the configuration before you click **Finish**.

The tunnel configuration on the Cisco ASA is complete. Now you must configure the FortiGate with similar settings, except for the remote gateway.

Encryption: AES-256

Authentication: SHA

Diffie-Hellman Group: 5

Encryption: AES-256

Authentication: SHA

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 2

Local Networks: inside-network/24

Remote Networks: 172.20.120.81

You have created a Site-to-Site VPN tunnel with the following attributes:

VPN Tunnel Interface: outside  
Peer IP Address: 172.20.120.81  
IPsec authentication uses pre-shared key:Password  
Tunnel Group Name: 172.20.120.81  
IKE Policy Encryption / Authentication / Diffie-Hellman Group: AES-256 / SHA / Group 5  
IPsec ESP Encryption / ESP Authentication: AES-256 / SHA  
Perfect Forward Secrecy (PFS): enabled  
Diffie-Hellman Group: 2  
Traffic flow to be protected by this tunnel:  
(local) 192.168.1.0/24  
(remote) 172.20.120.81

# Configuring the FortiGate tunnel phases

In the FortiOS GUI, navigate to **VPN > IPsec > Auto Key (IKE)** and select **Create Phase 1**.

Name the tunnel, statically assign the **IP Address** of the remote gateway, and set the **Local Interface** to **wan1**.

Select **Preshared Key** for **Authentication Method** and enter the same preshared key you chose when configuring the Cisco IPsec VPN Wizard.

Configure this phase to match the encryption settings configured on the Cisco device and click **OK**.

Select **Create Phase 2**.

Identify Phase 1, which you just configured, and ensure that the encryption settings match the Phase 2 encryption settings configured on the Cisco device.

Optionally, under **Quick Mode Selector**, specify the **Source address** and **Destination address** at the endpoints of the tunnel.

The screenshot displays the FortiGate configuration interface for IPsec VPN phases. The top section is for Phase 1 configuration, and the bottom section is for Phase 2 configuration.

**Phase 1 Configuration:**

- Name: Site2Site
- Comments: Write a comment... (0/255)
- Remote Gateway: Static IP Address
- IP Address: 172.20.120.222
- Local Interface: wan1
- Mode:  Aggressive  Main (ID protection)
- Authentication Method: Preshared Key
- Pre-shared Key: [Redacted]
- Peer Options:  Accept any peer ID
- Enable IPsec Interface Mode
- IKE Version:  1  2
- Mode Config:
- Local Gateway IP:  Main Interface IP  Specify (0.0.0.0)
- P1 Proposal:**
  - 1 - Encryption: AES256 Authentication: SHA1
  - DH Group:  1  2  5  14
  - Keylife: 28800 (120-172800 seconds)
  - Local ID: [Redacted] (optional)

**Phase 2 Configuration:**

- Name: Site2Site2
- Comments: Write a comment... (0/255)
- Phase 1: Site2Site
- Advanced...**
  - P2 Proposal: 1- Encryption: AES256 Authentication: SHA1
  - Enable replay detection
  - Enable perfect forward secrecy (PFS).
  - DH Group:  1  2  5  14
  - Keylife: Seconds: 1800 (Seconds) 5120 (KBytes)
  - Autokey Keep Alive:  Enable
  - Auto-negotiate:  Enable
- Quick Mode Selector:**
  - Source address:  Specify 192.168.100.0/24  Select -----Address-----
  - Source port: 0
  - Destination address:  Specify 192.168.1.0/24  Select -----Address-----
  - Destination port: 0
  - Protocol: 0

## Configuring the FortiGate policies

Navigate to **Policy > Policy > Policy** and create firewall policies that allow inbound and outbound traffic over the tunnel.

In the first (outbound) policy, set the **Incoming Interface** to **lan** and set the **Source Address** to **all**.

Set the **Outgoing Interface** to the tunnel interface and set the **Destination Address** to **all**. Configure the **Schedule** and **Service** as desired.

Create the second (inbound) policy to allow traffic to flow in the opposite direction, and configure the **Schedule** and **Service** as desired.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	lan <span>+</span>
Source Address	all <span>+</span>
Outgoing Interface	Site2Site <span>+</span>
Destination Address	all <span>+</span>
Schedule	always <span>+</span>
Service	ALL <span>+</span>

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	Site2Site <span>+</span>
Source Address	all <span>+</span>
Outgoing Interface	lan <span>+</span>
Destination Address	all <span>+</span>
Schedule	always <span>+</span>
Service	ALL <span>+</span>

## Configuring the static route in the FortiGate

Navigate to **Router > Static > Static Routes** and select **Create New**.

Create a static route with the **Destination IP/Mask** matching the address of the Cisco local network (by default, 192.168.1.0).

Under **Device**, select the site-to-site tunnel, and click **OK**.

Destination IP/Mask	192.168.1.0/255.255.255.0
Device	Site2Site <span>▾</span>
Distance	10 (1-255, Default=10)
Priority	0 (0-4294967295)
Comments	Write a comment... <span>0/255</span>

## Results

The tunnel should now be active. On the FortiGate, verify that the tunnel is 'up' by navigating to **VPN > Monitor > IPsec Monitor**.

The IPsec Monitor table will indicate the source and destination DNS addresses, and the status of the tunnel (up or down) and its uptime.

For more detailed tunnel information, go to **Log & Report > Event Log > VPN** and view the table.

Select the tunnel entry in the table to view the information in greater detail.

Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source
Site2Site	Static IP or Dynamic DNS	172.20.120.222	0		888	192.168.100.0/24
Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime		
192.168.1.0/24	<span style="color: green;">Bring Down</span>	0 B	2169 B	2570 seconds		

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
1	14:38:17		negotiate	success	negotiate IPsec phase 2	Site2Site
2	14:38:17		negotiate	success	progress IPsec phase 2	Site2Site
3	14:38:17		install_sa		install IPsec SA	Site2Site
4	14:38:17		negotiate	success	progress IPsec phase 2	Site2Site
5	14:09:46		negotiate	success	negotiate IPsec phase 2	Site2Site
6	14:09:46		negotiate	success	progress IPsec phase 2	Site2Site
7	14:09:46		tunnel-up		IPsec connection status change	Site2Site
8	14:09:46		phase2-up		IPsec phase 2 status change	Site2Site
9	14:09:46		install_sa		install IPsec SA	Site2Site
10	14:09:46		negotiate	success	progress IPsec phase 2	Site2Site
11	14:09:46		negotiate	success	progress IPsec phase 1	Site2Site
12	14:09:46		negotiate	success	progress IPsec phase 1	Site2Site

Action	negotiate	Cookies	c2a44adda34edfff/a3945a75a39f2f2f
Date/Time	14:38:17 (1384353497)	ESP Auth	HMAC_SHA1
ESP Transform	ESP_AES	Group	N/A
IPsec Local IP	172.20.120.81	IPsec Remote IP	172.20.120.222
Level	notice	Local Port	500
Log ID	37122	Message	negotiate IPsec phase 2
Outgoing Interface	wan1	Remote Port	500
Role	responder	Status	success
Sub Type	vpn	Timestamp	Wed Nov 13 14:38:17 2013
User	N/A	VPN Tunnel	Site2Site
Virtual Domain	root	XAUTH Group	N/A
XAUTH User	N/A		