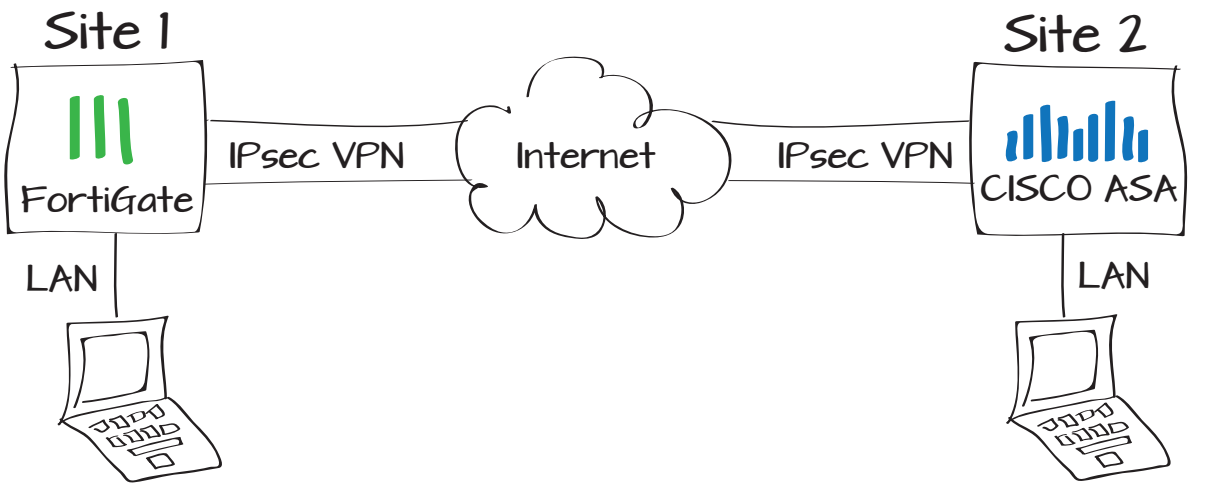
# Configuring IPsec VPN with a FortiGate and a Cisco ASA

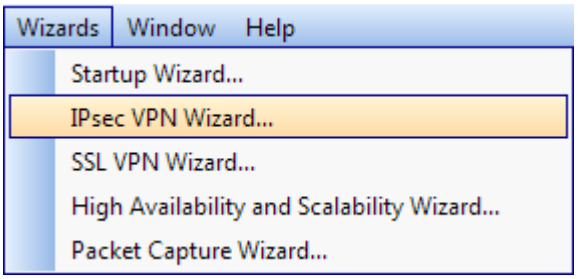
The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is behind a Cisco ASA. Using FortiOS 5.0 and Cisco ASDM 6.4, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, 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

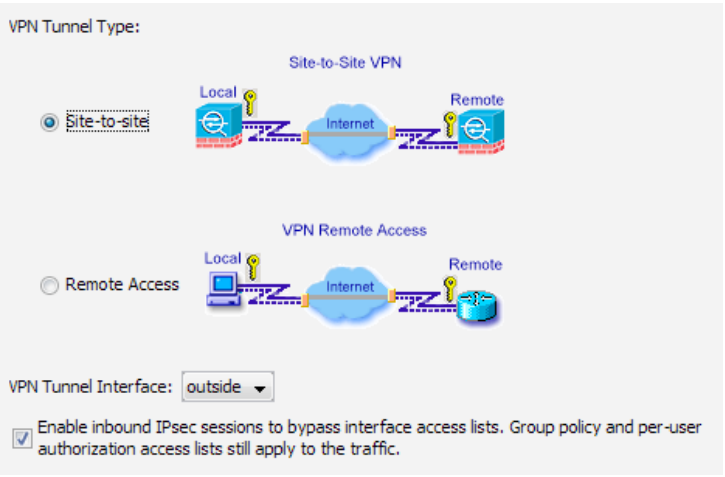


# Configuring the Cisco device using the IPsec VPN Wizard

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



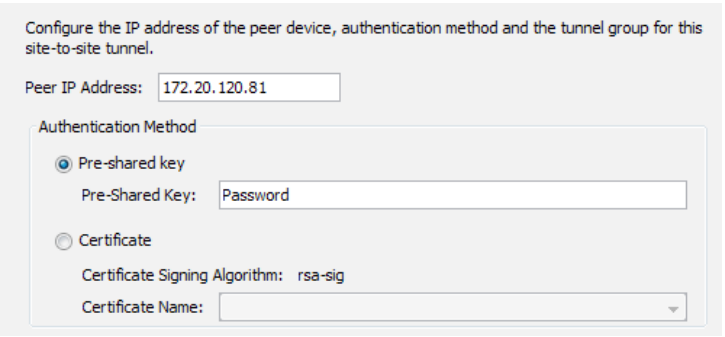

From the options that appear, select **Site-to-site**, with the **VPN Tunnel Interface** set to **outside**, then click **Next**.




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**.



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.

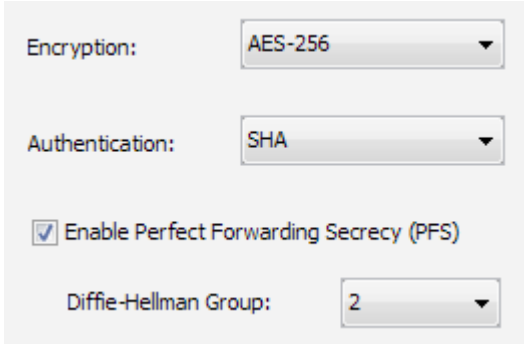
Configure Phase 1 with **AES-256 Encryption** and **SHA Authentication**.

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

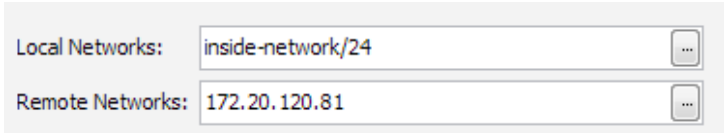

Configure Phase 1 with **AES-256 Encryption** and **SHA Authentication**.

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

Click **Next**.

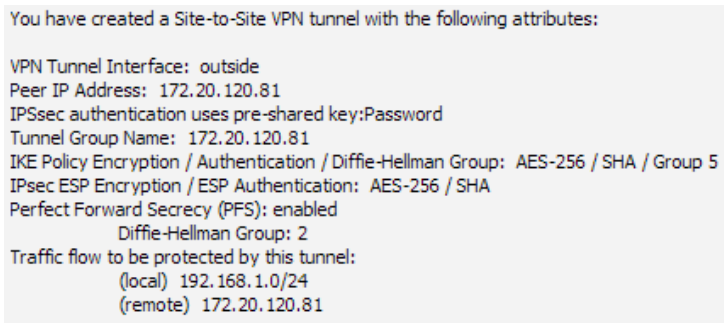



Set the **Local Network** and **Remote Network**.




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.



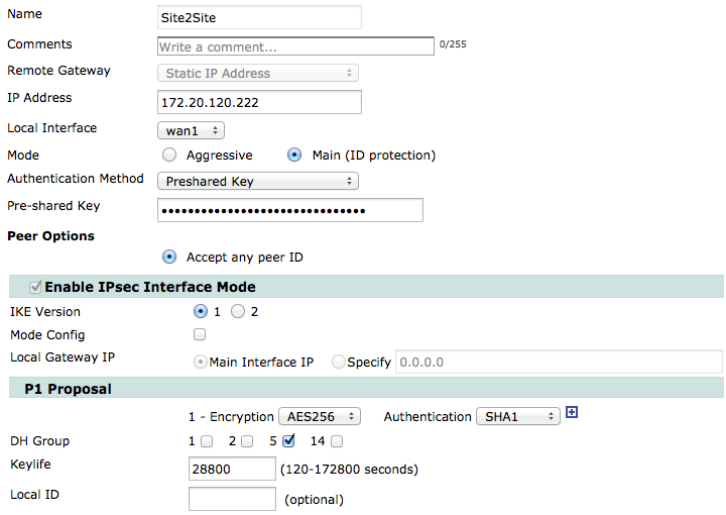
# Configuring the FortiGate tunnel phases

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.

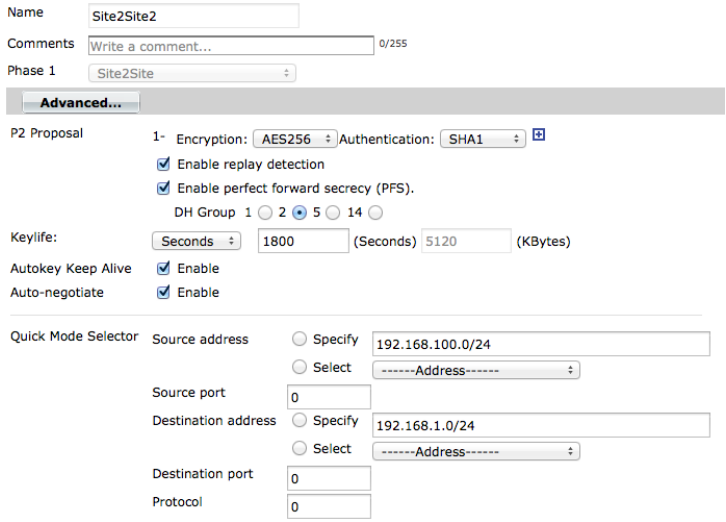
Configure this phase to match the encryption settings configured on the Cisco device and click **OK**.




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.



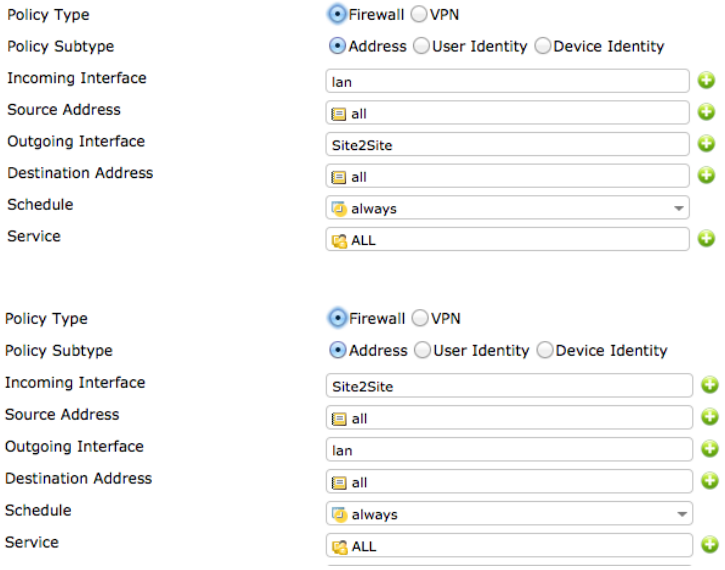
## Configuring the FortiGate policies

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.




## 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**.

# 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 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 | Bring Down | 0 B | 2169 B | 2570 seconds |

Refresh  Download Raw Log

| # | 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 | | |