



Skyhigh® Security Service Edge (SSE)

IPSec Configuration Fortinet FortiGate

Table of Contents

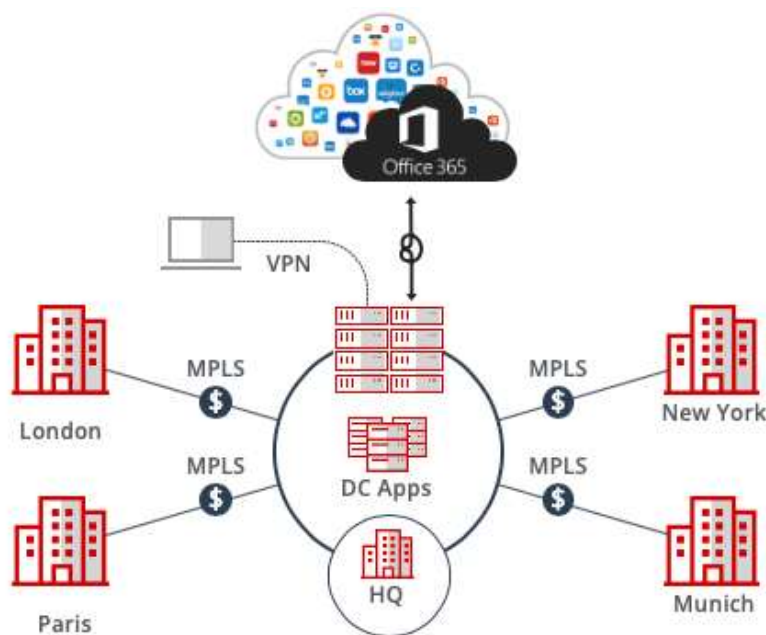
<u>INTRODUCTION TO SD-WAN ARCHITECTURE</u>	<u>3</u>
HUB AND SPOKE ARCHITECTURE	3
<u>DIRECT TO CLOUD</u>	<u>4</u>
<u>CONFIGURING IPSEC SITE-TO-SITE WITH FORTINET FORTIGATE</u>	<u>5</u>
IPSEC SITE-TO-SITE OVERVIEW	5
ENVIRONMENT	5
SETUP INCLUDES	5
CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE	5
FINDING THE BEST AVAILABLE POINTS OF PRESENCE	6
<u>CONFIGURE AN IPSEC VPN TUNNEL WITH FORTIGATE</u>	<u>7</u>
CREATE AN IPSEC VPN TUNNEL WITH FORTIGATE	7
CONFIGURE THE IPSEC VPN TUNNEL FOR FORTIGATE	8
SPECIFIC IPV4 ADDRESS	9
FULLY QUALIFIED DOMAIN NAME	10
USER FQDN	11
<u>VIEW THE STATUS OF THE TUNNEL CONFIGURED WITH FORTIGATE</u>	<u>12</u>
FORTIGATE 64D STATIC AND POLICY ROUTES	12
CREATE A STATIC ROUTE FOR FORTIGATE 64D.....	12
<u>CREATE A POLICY ROUTE FOR FORTIGATE.....</u>	<u>13</u>
CONFIGURE THE POLICY ROUTE FOR FORTIGATE.....	13

Introduction to SD-WAN Architecture

A Software-Defined Wide Area Network (SD-WAN) is a virtual WAN architecture that simplifies the connectivity, management, and operation of a traditional WAN.

As more companies shift to cloud applications, the result is a higher demand for bandwidth and direct internet connections to remote locations. Traditional MPLS networks are secure and stable, but expensive, and often fall victim to backhauling via the traditional hub and spoke architecture, where data is routed back through a central data center and out again to remote offices and users.

Hub and Spoke Architecture



SD-WAN combines traditional WAN technologies, such as MPLS and broadband connections, because it is abstracted from the hardware. Organizations leverage SD-WAN solutions because they provide enhanced capabilities for connectivity, monitoring, and managing network traffic while reducing cost.

Skyhigh Security Service Edge leverages SD-WAN technologies that allow remote offices to securely redirect web traffic to the Skyhigh Secure Web Gateway Cloud Service, where it is filtered according to your organization's web policy.

Direct to Cloud



This guide explains how to set up IPsec tunnels from Fortinet FortiGate to Skyhigh Secure Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configuring IPsec site-to-site with Fortinet FortiGate

If your organization uses one of the supported third-party SD-WAN devices to secure a remote office, you can use the IPsec protocol to secure communications between this site and Skyhigh Web Gateway Cloud Service (Skyhigh WGCS).

IPsec site-to-site overview

To secure communications between a remote site and Skyhigh WGCS using IPsec site to site authentication, you create an IPsec VPN tunnel between the supported SD-WAN device and cloud service.

Environment

- Skyhigh Security Service Edge (SSE)
- Fortinet FortiGate

Setup includes

- Configuration of Skyhigh WGCS using the Skyhigh Security Service Edge management console.
- Configuration of supported device.

For information about configuring Skyhigh WGCS for IPsec site to site, see the Skyhigh Web Gateway Cloud Service Guide.

Considerations for configuring IPsec site-to-site

Before configuring IPsec site-to-site authentication, review the following considerations.

- **Routing only HTTP and HTTPS traffic:** Skyhigh WGCS only handles IPsec traffic directed to ports 80 and 443 (HTTP and HTTPS traffic, respectively) through the VPN tunnel. Configure your device to route only HTTP and HTTPS traffic through the VPN tunnel.
- **Configuring two IPsec VPN tunnels:** Best practice is to configure a primary and secondary VPN tunnel. The primary tunnel is connected to the best available point of presence (POP), while the secondary tunnel is connected to the second-best point of presence. This practice ensures continuous IPsec support in case one point of presence is not available.
- **Using an IPsec VPN tunnel to connect remote sites:** If you have one or more remote sites that are connected to your network by VPN, you can protect traffic and improve network latency by creating a VPN tunnel between each site and Skyhigh WGCS.
- **Adding SAML authentication** — You can add a SAML configuration to an IPsec location. Skyhigh WGCS uses SAML to authenticate requests received from the location through the IPsec tunnel.

- **Using a NAT device:** If your IPsec device is located behind a NAT device and the outgoing interface has a private IP address, set the **Local ID** attribute to your public IP address.

Finding the best available points of presence

To find the point of presence closest to the device that you are configuring for IPsec authentication, you query the Global Routing Manager (GRM). The GRM is a DNS service that routes traffic to the best available point of presence.

From the network where your device is installed, run the n:lookup command-line tool, as follows:

- nslookup 1.network.wgcs.skyhigh.cloud
- nslookup 2.network.wgcs.skyhigh.cloud

In response to these commands, the GRM returns the IP addresses of the best and second-best points of presence, respectively, based on the network location of your device. You need these values when configuring the primary and secondary IPsec VPN tunnels in your device and in Skyhigh WGCS.

Configure an IPsec VPN tunnel with FortiGate

Configure the IPsec VPN tunnel in the Fortinet FortiGate web interface.

1. Create a VPN tunnel.
2. Configure the VPN tunnel.
3. View the status of the VPN tunnel.

Create an IPsec VPN tunnel with FortiGate

Create an IPsec VPN tunnel between the FortiGate device on the remote network and Skyhigh WGCS.

1. Log on to the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **VPN | IPsec | Tunnels**, then click **Create New**. The **VPN Creation Wizard** opens to the **VPN Setup** step.
3. In the **Name** field, specify a name for the VPN tunnel that you are configuring.
4. From the Template options, select **Site to Site • Fortigate**, then Click **Next**.
5. Configure the Authentication settings:
 - **Remote Gateway** – Specify the IP address that Skyhigh WGCS uses for IPsec communications. IPsec communications are sent from your network to this address.
 - **Note:** To find the IP address of the point of presence closest to your device, use the nslookup command-line tool to query the Global Routing Manager.
 - **Outgoing Interface**– From this drop-down list, select the outgoing interface of the FortiGate device. **Example:** Port 1
 - **Authentication Method** – Select **Pre-shared Key**.
 - **Pre-shared Key**– Specify the value of the key that you define and share with Skyhigh WGCS. This setting matches the Pre-Shared Key value that you specify when configuring the VPN tunnel in Skyhigh SSE.
 - **Local ID** – Specify IP address [This must match with Client ID]
6. Click **Next**.
7. Configure the **Policy & Routing** settings:
 - **Local Interface** – From the drop-down list, select the local interface of the FortiGate device.
 - **Local Subnets** – Specify the internal IP address of your network in IPv4 format using CIDR notation with a network size range of 16–32 bits. IPsec communications are sent from Skyhigh WGCS to this address. This setting matches the Local Network value that you specify when configuring the VPN tunnel in Skyhigh WGCS.
 - **Remote Subnets** – Specify the range of requested IP addresses that are sent through the VPN tunnel to Skyhigh WGCS. To make sure that all traffic is sent to Skyhigh WGCS through the tunnel, specify this value: 0.0.0.0/0.
8. Choose **Remote** as internet.
9. Click **Create**.

The VPN Creation Wizard displays this message: The VPN has been set up.

Configure the IPsec VPN tunnel for FortiGate

Configure the IPsec VPN tunnel using the values that Skyhigh SSE supports.

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **VPN | IPsec | Tunnels**.
3. Select the tunnel you created, then click **Edit**.
4. Click **Convert to Custom Tunnel**.
5. Under the **Authentication** heading, set the **IKE Version** to 2.
6. Under the **Phase 1 Proposal** heading:
 - a) Remove the two 3DES entries from the list.
 - b) Verify that Group 5 is selected.
7. Under the Phase 2 Selectors heading, verify that the **Local Address** and **Remote Address** settings are correct.
8. To open the **Phase 2 Proposal** settings, click Advanced, then:
 - a) Remove the two **3DES** entries from the list.
 - b) Verify that **Group 5** is selected.
9. Click **OK**.

IPsec VPN configuration options

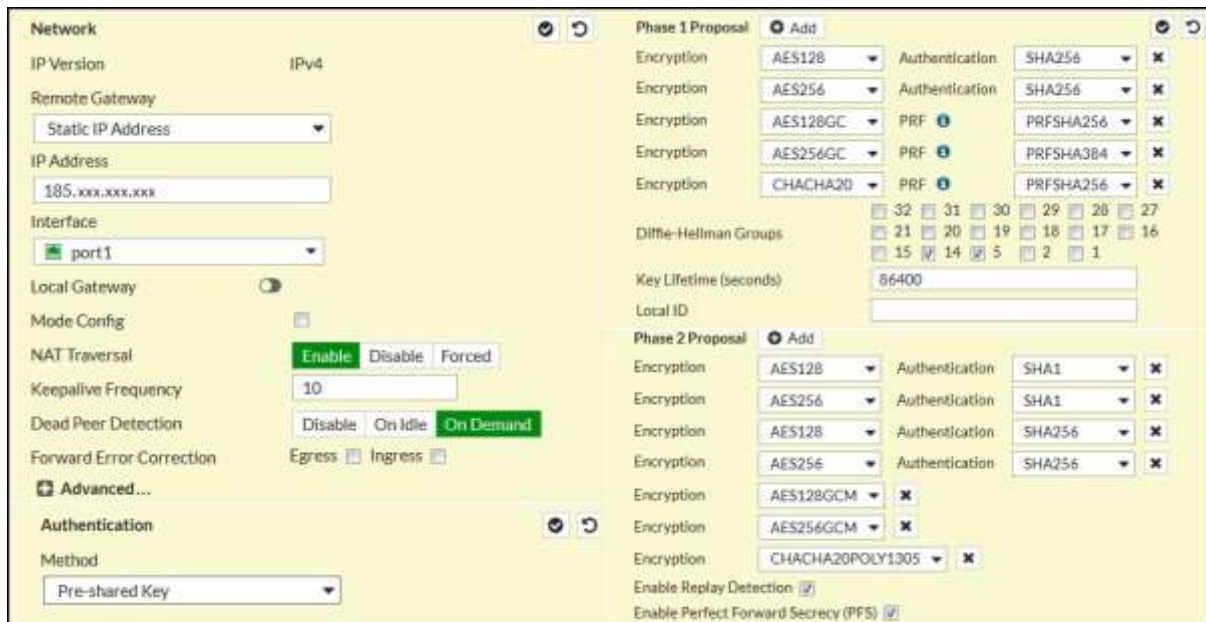
There are three different ways we can configure on the FortiGate side and equal UCE snapshots are mentioned below. For information about configuring Skyhigh WGCS, see the WGCS Skyhigh SSE Installation Guide.

- Specific IPv4 Address
- Fully qualified Domain Name
- User FQDN

Specific IPv4 Address

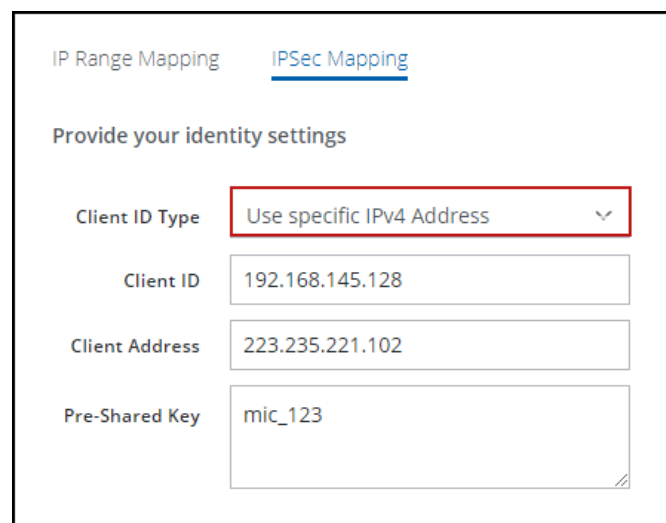
This screenshot shows how to configure IPsec site-to-site authentication in the FortiGate web interface when you select **Specific IPv4 Address** as the **Client ID** Type in the Skyhigh SSE.

Note: When using this option to configure FortiGate, make sure to leave the **Local ID** field empty.



The screenshot displays the FortiGate web interface for IPsec configuration. The 'Network' tab is selected, showing the 'Static IP Address' for the Remote Gateway and 'port1' for the Interface. The 'Authentication' section shows 'Pre-shared Key' as the Method. The 'Phase 1 Proposal' and 'Phase 2 Proposal' sections show various encryption and authentication options.

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.



The screenshot shows the Skyhigh SSE IPsec Mapping configuration page. The 'IPSec Mapping' tab is active. The 'Client ID Type' is set to 'Use specific IPv4 Address'. The 'Client ID' is 192.168.145.128, the 'Client Address' is 223.235.221.102, and the 'Pre-Shared Key' is mic_123.

Fully Qualified Domain Name

This screenshot shows how to configure IPsec site-to-site authentication in the FortiGate web interface when you select **Fully Qualified Domain Name** as the **Client ID Type** in the Skyhigh SSE.

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

IP Range Mapping IPsec Mapping

Provide your identity settings

Client ID Type Use Fully Qualified Domain Name ▾

Client ID johnson@skyhigh.com

Client Address 223.235.221.102

Pre-Shared Key mic_123

User FQDN

This screenshot shows how to configure IPsec site-to-site authentication in the FortiGate web interface when you select **User FQDN** as the **Client ID Type** in the Skyhigh SSE.

The screenshot displays the FortiGate web interface for IPsec configuration. The 'Network' tab is selected, showing settings for the IPsec tunnel. Key configurations include:

- IP Version:** IPv4
- Remote Gateway:** Static IP Address
- IP Address:** 185.xxx.xxx.xxx
- Interface:** port1
- Local Gateway:** Disabled
- Mode Config:** Disabled
- NAT Traversal:** Enabled
- Keepalive Frequency:** 10
- Dead Peer Detection:** On Demand
- Forward Error Correction:** Egress
- Authentication:** Pre-shared Key
- Phase 1 Proposal:** AES128, AES256, AES128GC, AES256GC, CHACHA20
- Phase 2 Proposal:** AES128, AES256, AES128GCM, AES256GCM, CHACHA20POLY1305

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

The screenshot shows the 'IPSec Mapping' configuration page in the Skyhigh SSE. The 'Client ID Type' is set to 'Use a User FQDN', and the 'Client ID' field is highlighted with a red box. Other fields include 'Client Address' (223.235.221.102) and 'Pre-Shared Key' (mic_123).

View the status of the tunnel configured with FortiGate

To verify that the IPsec VPN tunnel with FortiGate is correctly configured, view the status of the tunnel.

1. Open the web interface that you use to configure the FortiGate device on your network.
2. Select **VPN | Monitor | IPsec Monitor**.
3. In the table, locate the VPN tunnel in the **Name** column.

In the **Status** column, a green icon and up arrow show that the VPN tunnel is configured correctly.

FortiGate 64D static and policy routes

Complete these tasks to create and configure the static and policy routes for FortiGate.

1. Create a static route for FortiGate.
2. Create a policy route for FortiGate.
3. Configure the policy route for FortiGate.

Create a static route for FortiGate 64D

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **Network | Static Routes**, then click **Create New**.
3. Configure these settings:
 - **Destination** – Specify the IP address that Skyhigh WGCS uses for IPsec communications. This setting matches the Remote Gateway value that you configure when creating the VPN tunnel in the FortiGate interface. To find the IP address of the point of presence closest to your device, use the nslookup command-line tool to query the Global Routing Manager.
 - **Gateway** – Specify the FortiGate outbound IP address. This setting matches the External IP value that you specify when configuring the VPN tunnel in Skyhigh WGCS.
4. Expand the **Advanced Options**, then specify a value for the **Priority** setting. Review these considerations:
 - The static route with the lowest priority value has the highest priority.
 - Specify a value that is greater than the priority configured for the default static route, so that the default static route always has a higher priority.
 - When configuring static routes for multiple VPN tunnels, the routes can have the same priority value.
5. Click **OK**.

Create a policy route for FortiGate

The FortiGate device uses the policy route to determine whether TCP packets are directed through the VPN tunnel or to the Internet.

- **TCP packets going to ports 80 and 443** – Using the static route, the device directs these packets through the VPN tunnel.
- **All other packets** – Using the default static route, the device directs these packets to the Internet.

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **Network | Policy Routes**, then click **Create New**.
3. Under **If incoming traffic matches**, configure these settings:
 - **Protocol** – Select **TCP**.
 - **Incoming interface** – From the drop-down list, select **internal**.
 - **Source address | mask** – Specify the internal IP address of your network in IPv4 format using CIDR notation with a network size range of 16–32 bits. IPsec communications are sent from Skyhigh WGCS to this address. This setting matches the Local Network value that you specify when configuring the VPN tunnel in Skyhigh WGCS.
 - **Destination address | mask** – Specify the range of requested IP addresses that are sent through the policy route to Skyhigh WGCS. To ensure that all traffic is sent to Skyhigh WGCS through this route, specify this value: 0.0.0.0/0.
4. Under **Then**, configure these settings:
 - **Action** – Select **Enable Forward Traffic**.
 - **Gateway address** – Specify the outgoing interface of the FortiGate device.
5. Click **OK**.

Configure the policy route for FortiGate

Configure the policy route so that the FortiGate device only routes TCP packets going to ports 80 and 443 (HTTP and HTTPS traffic, respectively) through the IPsec VPN tunnel.

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **Policy & Objects | IPv4 Policy**.
3. Select the policy route that you created, then click **Edit**.
4. From the **Service** drop-down list: Under **Web Access**, select **HTTP**.
5. Click the **Add** icon, then under **Web Access**, select **HTTPS**.
6. Click **OK**.

Trellix, FireEye, and McAfee Security are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Other names and brands are the property of these companies or may be claimed as the property of others.
Copyright © 2022 Musarubra US LLC.