Skyhigh® Security Service Edge (SSE)

IPsec Configuration Cisco Viptela vManage

Table of Contents

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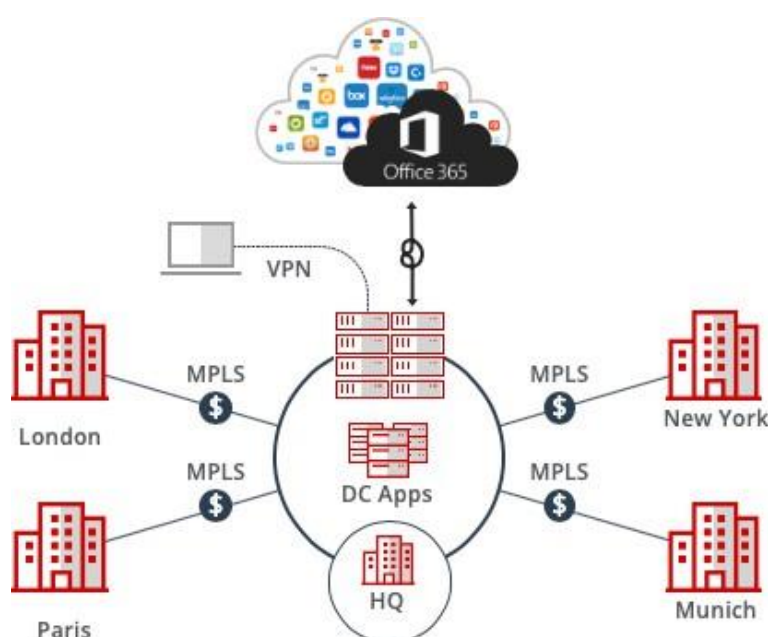
SD-WAN combines traditional WAN technologies, such as MPLS and broadband connections, because it is abstracted from the hardware. Organizations leverage SD-WAN solutions because they provide enhanced capabilities for connectivity, monitoring, and managing network traffic while reducing cost.

Skyhigh Security Service Edge (SSE) 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
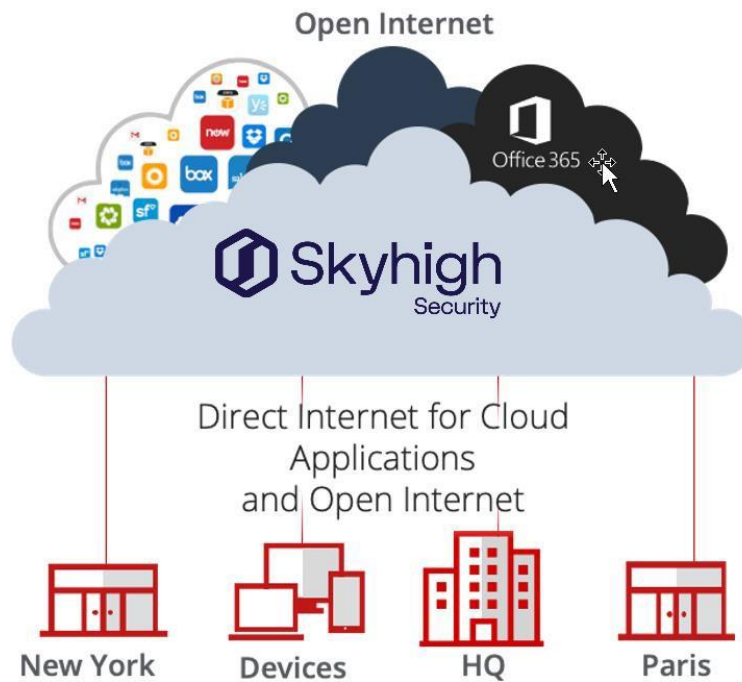
This guide explains how to set up IPsec tunnels from Cisco Viptela vManage to Skyhigh Secure Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configure IPsec site-to-site with Cisco Viptela

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

IPsec site-to-site overview

To secure communications 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 the cloud service.

Environment

- Skyhigh Security Service Edge (SSE)
- Cisco Viptela vManage

Setup includes

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

For information about configuring Skyhigh WGCS for IPsec site-to-site, see the Skyhigh Secure 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 through the VPN tunnel to ports 80 and 443 (HTTP and HTTPS traffic, respectively). 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 multiple remote offices connected to your main office 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 site. Skyhigh WGCS uses SAML to authenticate requests received from the site 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.

Find 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 nslookup 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 Cisco Viptela vManage

Navigate to the Template Screen

1. In vManage NMS, select **Configuration | Templates.**
2. On the **Device** tab, click **Create Template.**
3. From the **Create Template** drop-down list, select **From Feature Template.**
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click the **Service VPN** tab located below the **Description** field or scroll to the **Service VPN** section.
6. Under **Additional VPN Templates**, click **VPN Interface IPsec.**
7. From the **VPN Interface IPsec** drop-down list, select **Create Template.**
   Displays the VPN Interface IPsec template. The top of the form contains fields for naming the template and the bottom fields for defining VPN Interface IPsec parameters.
8. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

# Configure a basic IPsec tunnel interface

To configure an IPsec tunnel to use for IKE sessions:

1. Select the **Basic Configuration** tab, and configure the following parameters:

Note: Parameters marked with an asterisk are required to configure an IPsec tunnel.

Parameter Name	Description
Shutdown	Click **No** to enable the interface.
Interface Name	Enter the name of the IPsec interface, in the format IPsec number. You can enter a value from 1 to 256.
Description	Enter a description of the IPsec interface.
IPv4 Address	Enter the IPv4 address of the IPsec interface, in the format IPv4-prefix/length. The address must be a /30.
Source	Set the source of the IPsec tunnel that is being used for IKE key exchange: • Click **IP Address**—Enter the IPv4 address of the source tunnel interface. This address must be configured in VPN 0. • Click **Interface**—Enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in VPN 0.
Destination: IPsec Destination IP Address/FQDN	Set the destination of the IPsec tunnel that is being used for IKE key exchange. Enter either an IPv4 address or the fully qualified DNS name that points to the destination.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

2. To save the feature template, click **Save**.

Skyhigh Security
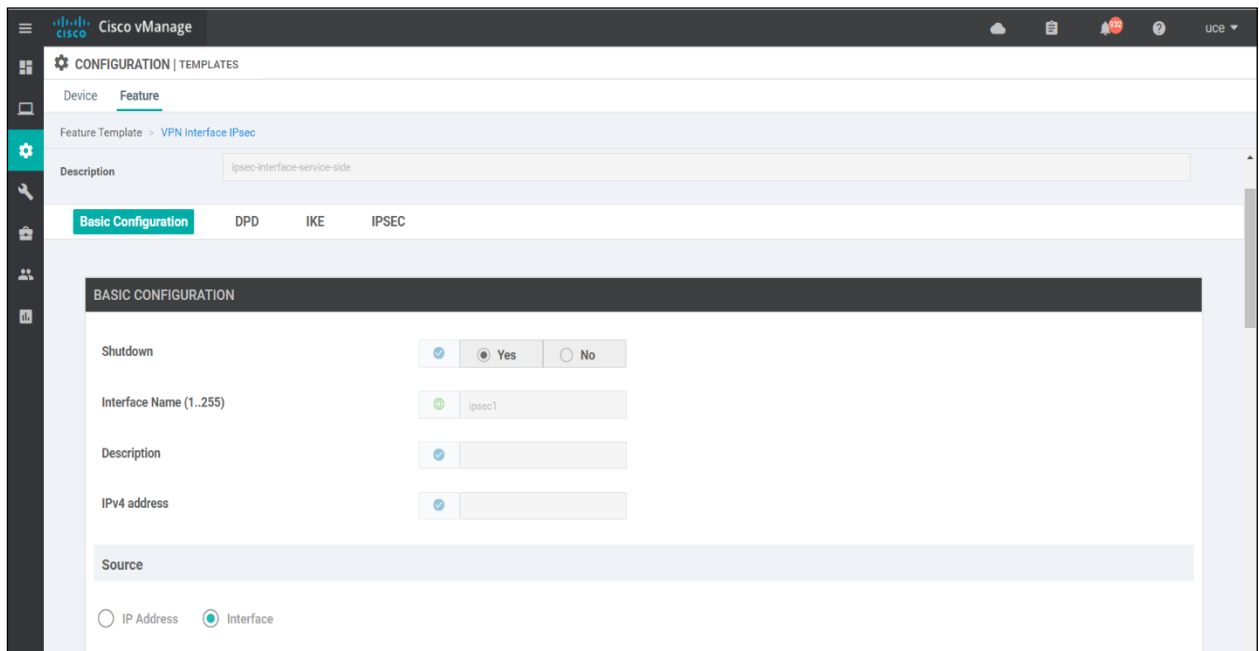
Configure Dead-Peer detection

To configure IKE dead-peer detection, determine whether the connection to an IKE peer is functional and reachable.

1. Select the **DPD** tab, and configure the following parameters:

Parameter Name	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 0 through 65535 seconds (1 hour through 14 days) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer. Range: 0 through 255 Default: 3

2. To save the feature template, click **Save**.

Configure IKE

1. Select the **IKE** tab and configure the following parameters:

- **Authentication and encryption**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity

- **Diffie-Hellman group number**—16
- **Rekeying time interval**—4 hours
- **SA establishment mode**—Main
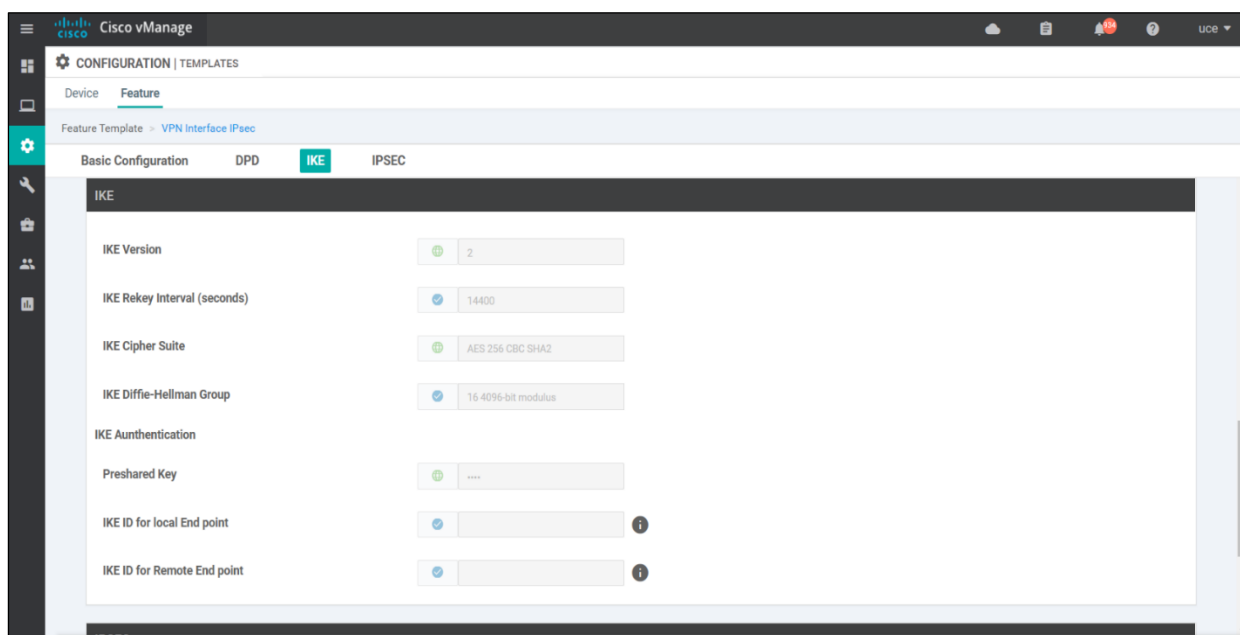
2. Configure the following IKEv2 parameters:

Parameter Name	Description
IKE Version	Select IKEv2
IKE Mode	Specify the IKE SA establishment mode. Values: Aggressive mode, Main mode Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes256-cbc-sha1 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange. Values: 1024-bit modulus, 2048-bit modulus, 3072-bit modulus, 4096-

Parameter Name	Description
	bit modulus Default: 4096-bit modulus
IKE Authentication: Preshared Key	Enter the password that you want to use as preshared key for authentication.
IKE ID for Local End Point	If the remote IKE peer requires a local end point identifier, specify it. Default: Tunnel's source IP address
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's destination IP address

3. To save the feature template, click **Save**.

Configure IPsec tunnel parameters

To configure the IPsec tunnel that carries IKE traffic:

1. Select the **IPsec** tab and configure the following parameters:

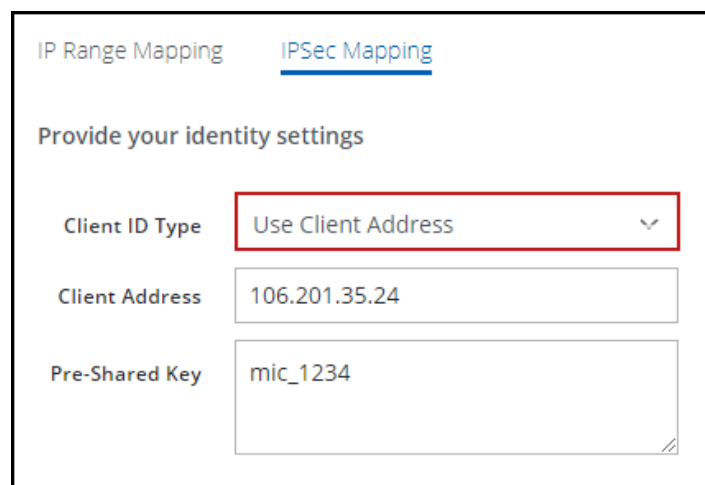| Parameter Name	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 32 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: aes256-cbc-sha1, aes256-gcm, null-sha1 Default: aes256-gcm
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Values: · group-2—Use the 1024-bit Diffie-Hellman prime modulus group. · group-14—Use the 2048-bit Diffie-Hellman prime modulus group. · group-15—Use the 3072-bit Diffie-Hellman prime modulus group. · group-16—Use the 4096-bit Diffie-Hellman prime modulus group. · none—Disable PFS. Default: group-16

IPsec VPN configuration options

You use one of the following options when configuring IPsec site-to-site authentication in the Cisco Viptela vManage web interface. Then you select the same option from the **Client ID Type** drop-down list when configuring IPsec site-to-site in the Skyhigh SSE.

- Client Address
- Specific IPv4 Address
- Fully Qualified Domain Name
- User FQDN

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

Specific IPv4 address

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

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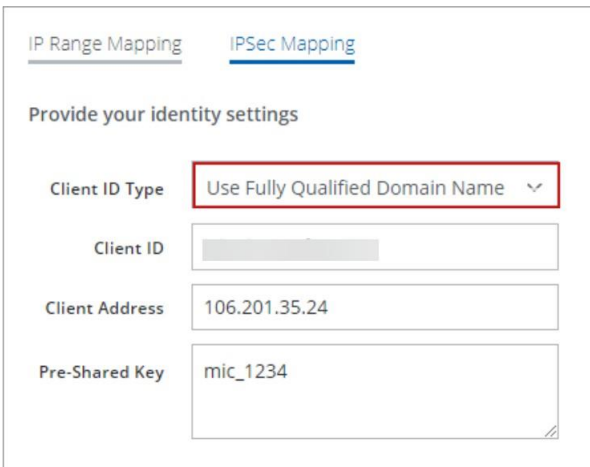
Fully Qualified Domain Name

This screenshot shows how to configure IPsec site-to-site authentication in the Cisco Viptela vManage 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**.
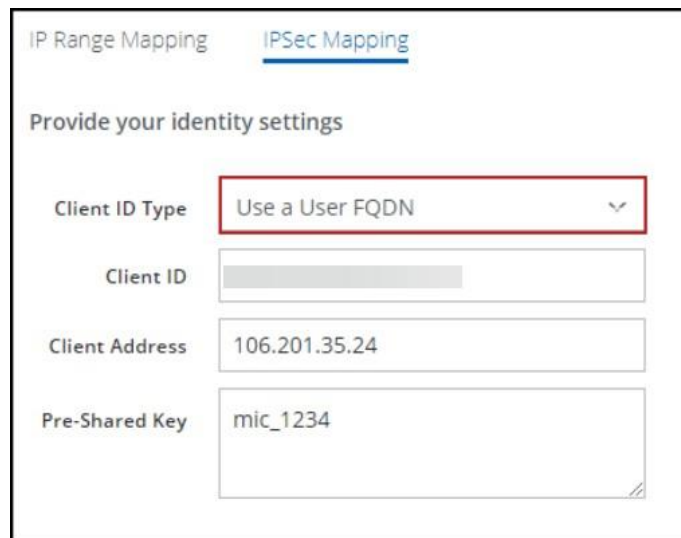
User FQDN

This screenshot shows how to configure IPsec site-to-site authentication in the Cisco Viptela vManage web interface when you select **User FQDN** 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**.