Skyhigh® Security Service Edge (SSE)

IPsec Configuration Citrix SD-WAN VPX

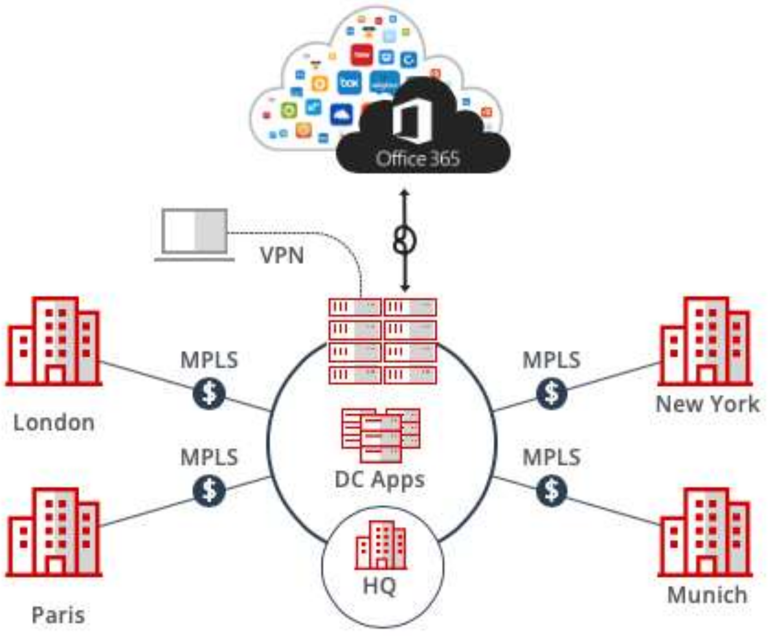
Table of Contents

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.

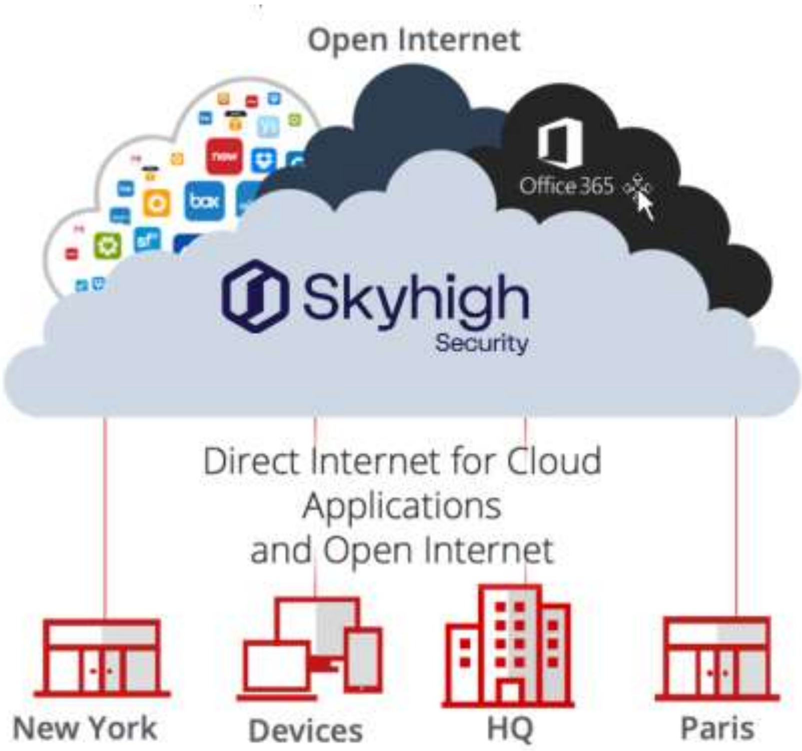
Hub and Spoke Architecture



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 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 Citrix SD-WAN VPX to Skyhigh Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configure IPsec site-to-site with Citrix SD-WAN

When 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 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 the cloud service.

Environment

- Skyhigh Security Service Edge (SSE)
- Citrix SD-WAN

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** – The 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.

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 nslookup command-line tool, as follows:

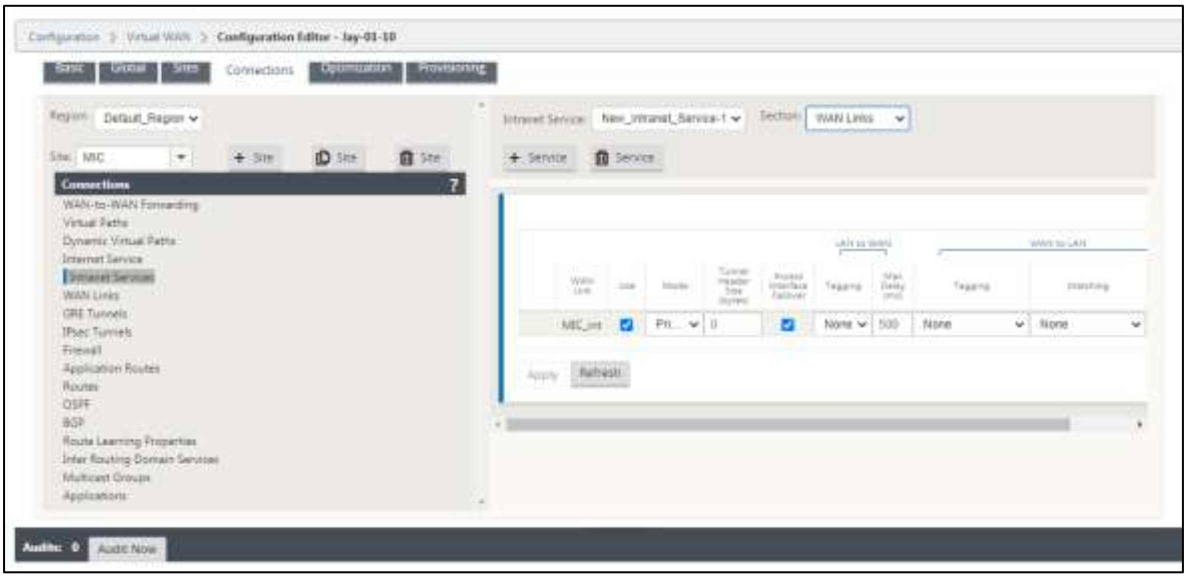
- nslookup 1.network.wgcs.Skyhigh.cloud
- nslookup 2.network.wgcs.Skyhigh.cloud

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 Citrix SD-WAN

To configure IPsec tunnel:

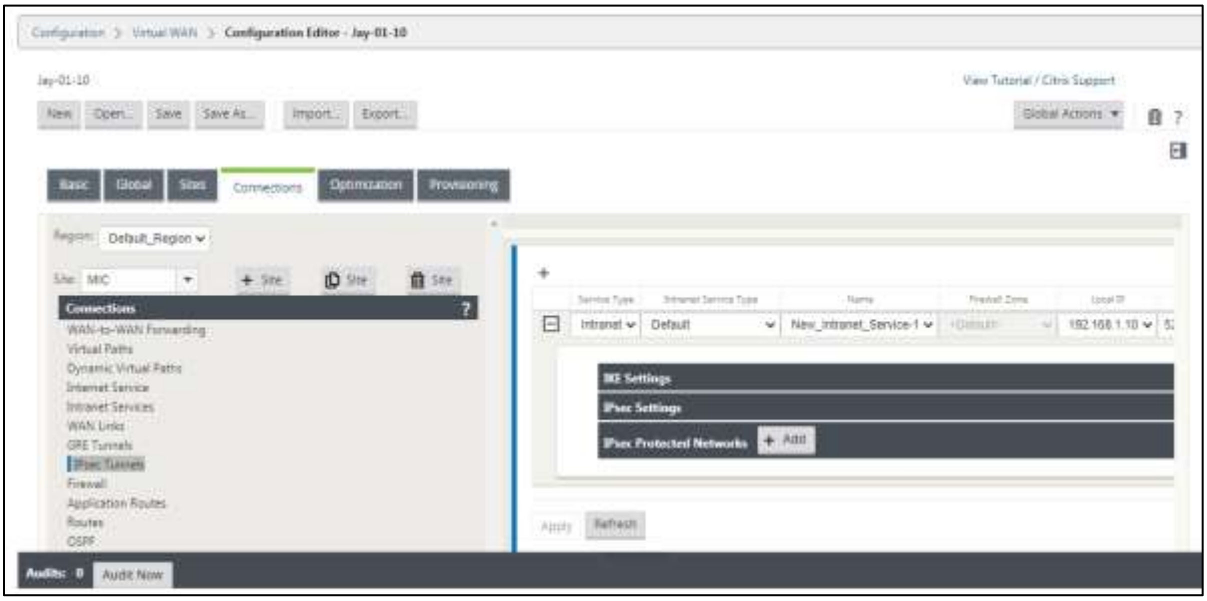
1. In **Configuration Editor**, click **Connections** | **[Site Name]** | **Intranet Services**.



2. Click **Service**.
3. From the **Section** drop-down list, select **Basic Settings**.
4. Select the **Primary Reclaim** check box.
5. From the **Section** drop-down list, select **WAN Links.**
6. Select **Primary** or **Secondary** from **Mode**.
7. Click **Apply** to save your changes.

Configure a basic IPsec Tunnel interface

1. In the **Configuration Editor**, navigate to **Connections** | **[Site Name]** | **IPsec Tunnels**.
2. Select **Service Type** (Intranet).
3. **Select the Local IP available** IP address.
4. **Enter the Peer IP** address of the IPsec tunnel.

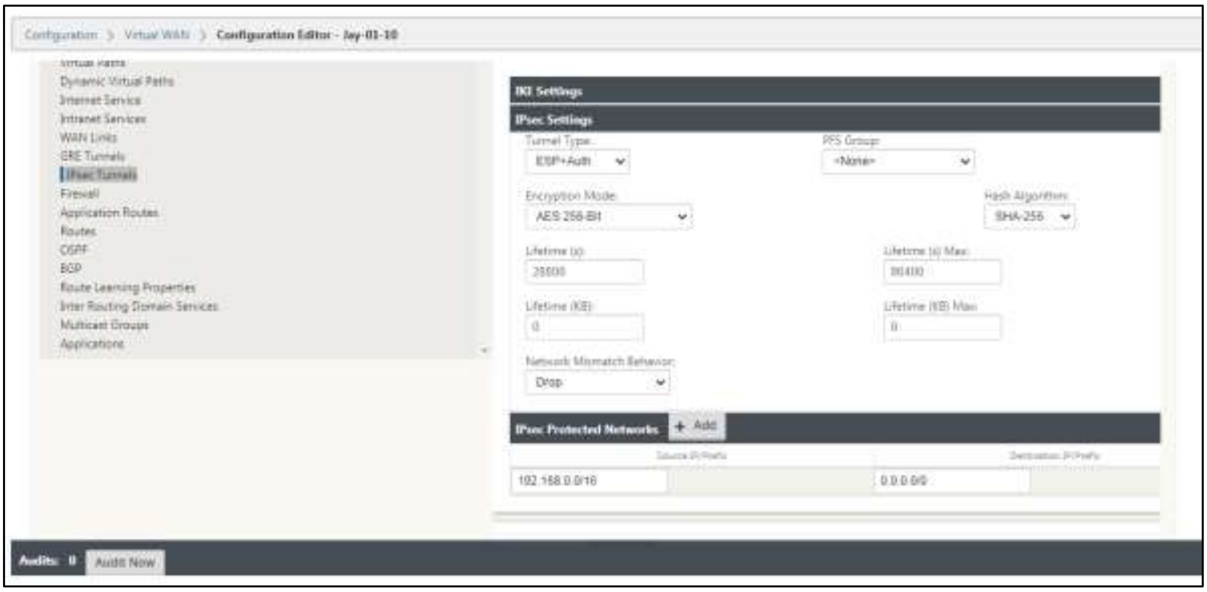


5. Configure **IPsec Settings** by applying the following criteria:

Field	**Description**	**Value**
Local IP	Select the local IP address of the IPsec Tunnel from the drop-down list of available virtual IP addresses configured at this site.	IP address
Peer IP	Enter the peer IP address of the IPsec Tunnel.	IP address
MTU	Enter the **MTU** for fragmenting IKE and IPsec fragments.	1500 (default)
IKE Settings	Select an IKE version from the drop-down list.	IKEv2
Identity	Select an Identity from the drop-down list.	Auto IP Address Manual IP Address User FQDN
Authentication	Select an authentication type from the drop-down list.	Pre-Shared Key: If you are using a pre-shared key, copy and paste it into this field. Click the **Eyeball** icon to view the Pre-Shared Key.

Field	Description	Value
Validate Peer Identity	Select this check box to validate the IKE's peer. If the peer's ID type is not supported, do not enable this feature.	None
DH Group	Select Diffie–Hellman group to use for IKE key generation from the drop-down list.	Group 14 Group 15 Group 16 Group 19 Group 20 Group 21
Hash Algorithm	Select an algorithm from the drop-down list to authenticate IKE messages.	SHA-256
Encryption Mode	Select the **Encryption Mode** for IKE messages from the drop-down list.	AES 256-bit
Lifetime (s)	Enter the preferred duration, in seconds, for an IKE security association to exist.	3600 seconds (default)
Lifetime (s) Max	Enter the maximum preferred duration, in seconds, to allow an IKE security association to exist.	86400 seconds (default)
DPD Timeout (s)	Enter the Dead Peer Detection timeout, in seconds, for VPN connections.	300 seconds (default)

6. Configure IPsec Settings and IPsec Protected Network Settings by applying the following criteria.



Tunnel Type: ESP+Auth
PFS Group: <None>
Encryption Mode: AES 256-Bit
Hash Algorithm: SHA-256
Lifetime (s): 28800
Lifetime (s) Max: 86400
Lifetime (KB): 0
Lifetime (KB) Max: 0
Network Mismatch Behavior: Drop

Source IP/Prefix	Destination IP/Prefix
192.168.0.0/16	0.0.0.0/0

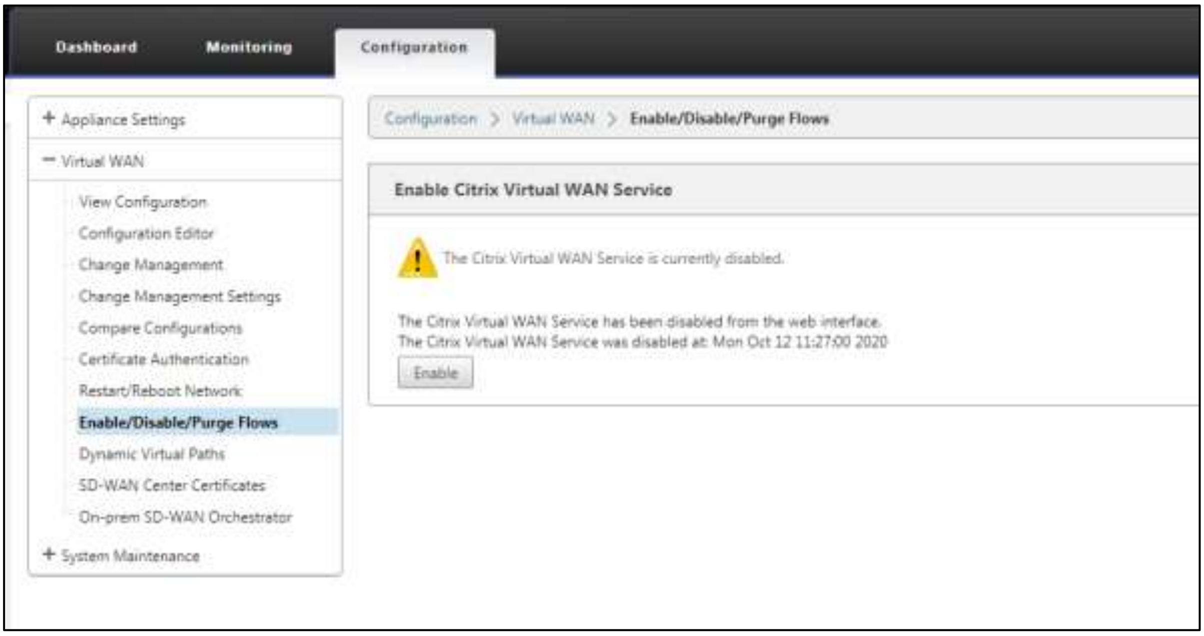
Skyhigh Security

Field	**Description**	**Value (s)**
Tunnel Type	Select the tunnel type from the drop-down list.	ESP+Auth
PFS Group	Select Diffie–Hellman group to use for perfect forward secrecy key generation from the drop-down list.	None
Encryption Mode	Select the encryption mode for IPsec messages from the drop-down list.	AES 256-bit
Lifetime (s)	Enter the amount of time, in seconds, to allow an IPsec security association to exist.	28800 seconds (default)
Lifetime Max (s)	Enter the maximum amount of time, in seconds, to allow an IPsec security association to exist.	86400 seconds (default)
Lifetime (KB)	Enter the amount of data, in kilobytes, for an IPsec security association to exist.	Kilobytes
Lifetime (KB) Max	Enter the maximum amount of data, in kilobytes, to allow an IPsec security association to exist.	Kilobytes
Network Mismatch Behavior	Select an action to take if a packet does not match the IPsec Tunnel's Protected Networks from the drop-down list.	Drop
IPsec Protected Networks: **Source IP/Prefix**	After clicking the Add (+ Add) button, enter the source IP address and Prefix of the network traffic the IPsec Tunnel will protect.	IP address
IPsec Protected Networks: **Destination IP/Prefix**	Enter the destination IP address and prefix of the network traffic the IPsec Tunnel will protect.	IP address

7. Click **Apply** to save your settings.

Enable WAN Service

1. On the **Configuration** tab, click **Virtual WAN | Enable/Disable/Purge Flows**.
2. Click **Enable**.

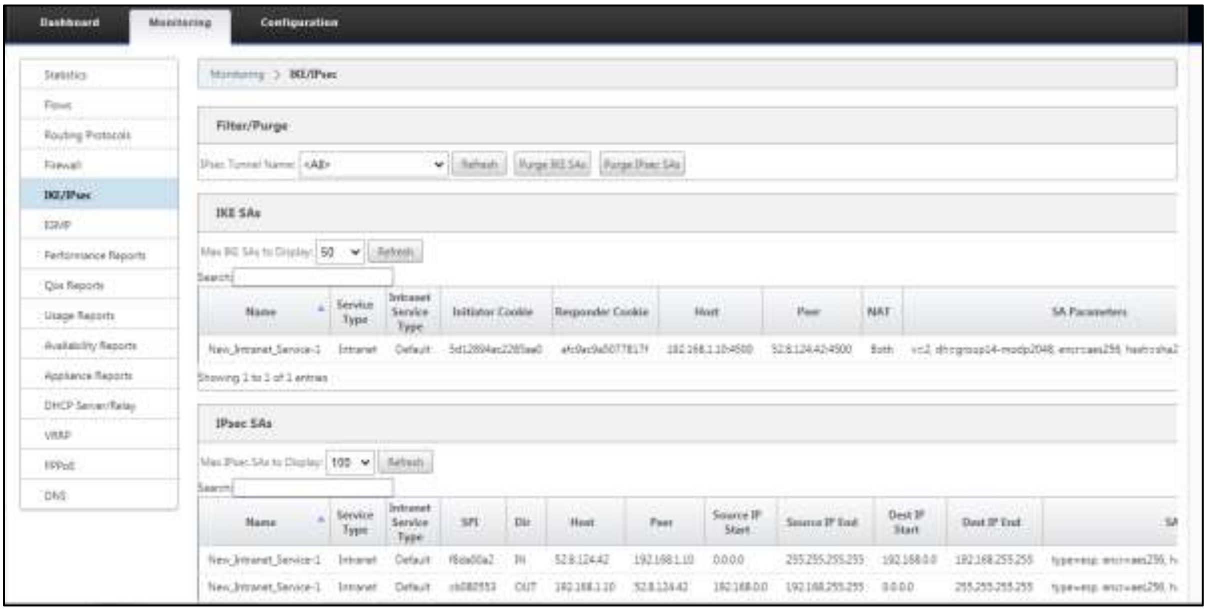

Dashboard
Monitoring
Configuration
+ Appliance Settings
− Virtual WAN
View Configuration
Configuration Editor
Change Management
Change Management Settings
Compare Configurations
Certificate Authentication
Restart/Reboot Network
Enable/Disable/Purge Flows
Dynamic Virtual Paths
SD-WAN Center Certificates
On-prem SD-WAN Orchestrator
+ System Maintenance
Configuration > Virtual WAN > Enable/Disable/Purge Flows
Enable Citrix Virtual WAN Service
Enable

The Citrix Virtual WAN Service is currently disabled.

The Citrix Virtual WAN Service has been disabled from the web interface.
The Citrix Virtual WAN Service was disabled at: Mon Oct 12 11:27:00 2020

Monitor IPsec Tunnels

On the **Monitoring** tab, click **IKE/IPsec** in the SD-WAN appliance GUI to view and monitor IPsec tunnel configuration.



IPsec Tunnel Name: <All>

Max IKE SAs to Display: 50

Name	Service Type	Intranet Service Type	Initiator Cookie	Responder Cookie	Host	Peer	NAT	SA Parameters
New_Intranet_Service-1	Intranet	Default	5d12894ac2285ae0	afc9ac9a5077817f	192.168.1.10:4500	52.8.124.42:4500	Both	v=2, dh=group14-modp2048, encr=aes256, hash=sha2

Showing 1 to 1 of 1 entries

Max IPsec SAs to Display: 100

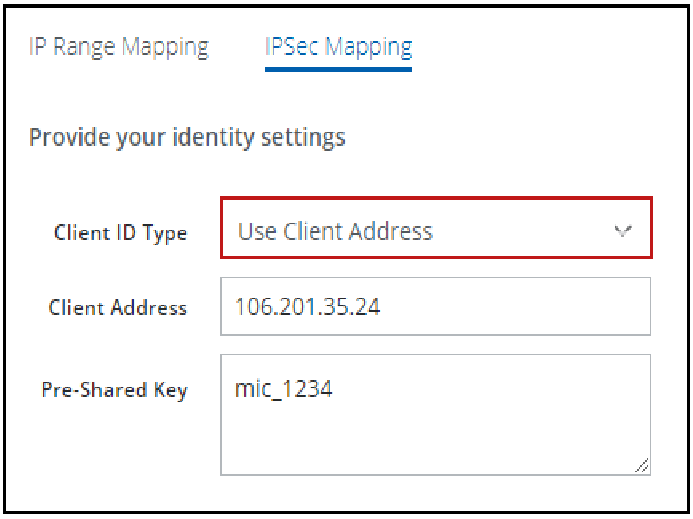
Name	Service Type	Intranet Service Type	SPI	Dir	Host	Peer	Source IP Start	Source IP End	Dest IP Start	Dest IP End	SA
New_Intranet_Service-1	Intranet	Default	f6da00a2	IN	52.8.124.42	192.168.1.10	0.0.0.0	255.255.255.255	192.168.0.0	192.168.255.255	type=esp, encr=aes256, h
New_Intranet_Service-1	Intranet	Default	cb082553	OUT	192.168.1.10	52.8.124.42	192.168.0.0	192.168.255.255	0.0.0.0	255.255.255.255	type=esp, encr=aes256, h

IPsec VPN configuration options

You use one of the following options when configuring IPsec site-to-site authentication in the Citrix SD-WAN 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

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



Provide your identity settings

Client ID Type: Use Client Address

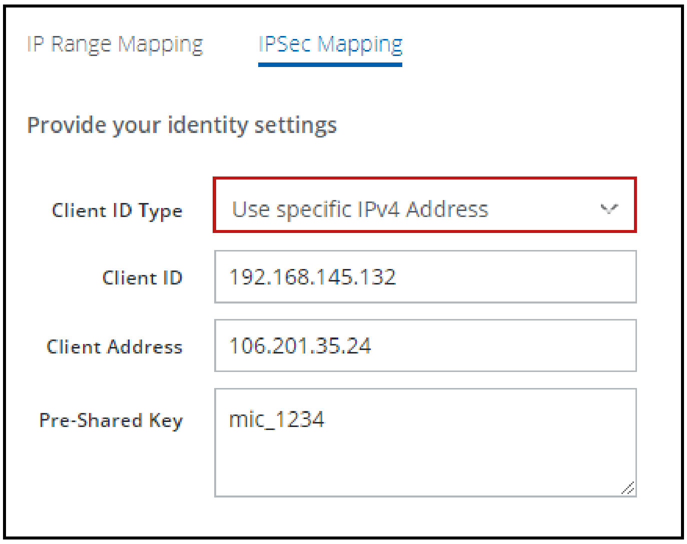
Client Address: 106.201.35.24

Pre-Shared Key: mic_1234

Specific IPv4 address

This screenshot shows how to configure IPsec site-to-site authentication in the Citrix SD-WAN web interface when you select **Specific IPv4 Address** 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 specific IPv4 Address

Client ID: 192.168.145.132

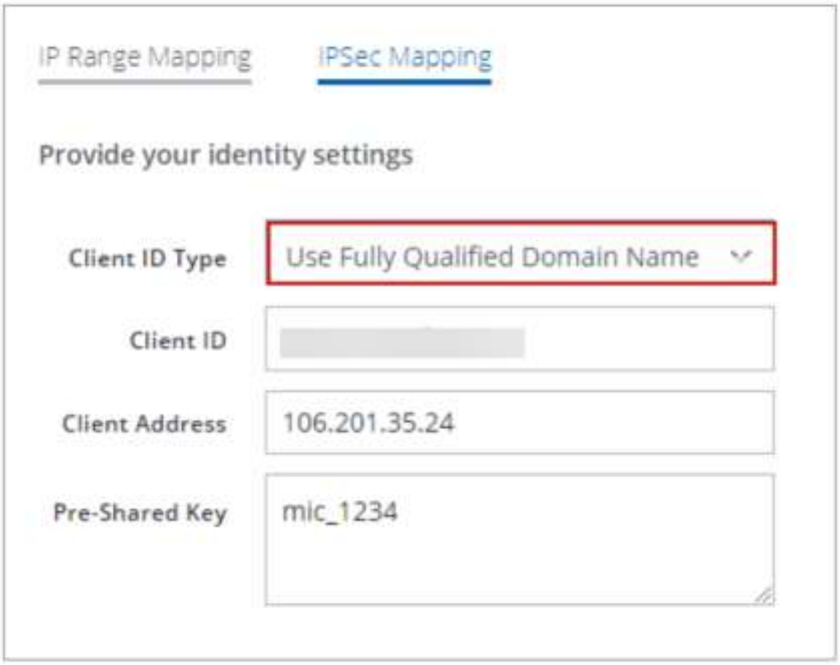
Client Address: 106.201.35.24

Pre-Shared Key: mic_1234

Fully Qualified Domain Name

This screenshot shows how to configure IPsec site-to-site authentication in the Citrix SD-WAN 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: [redacted]

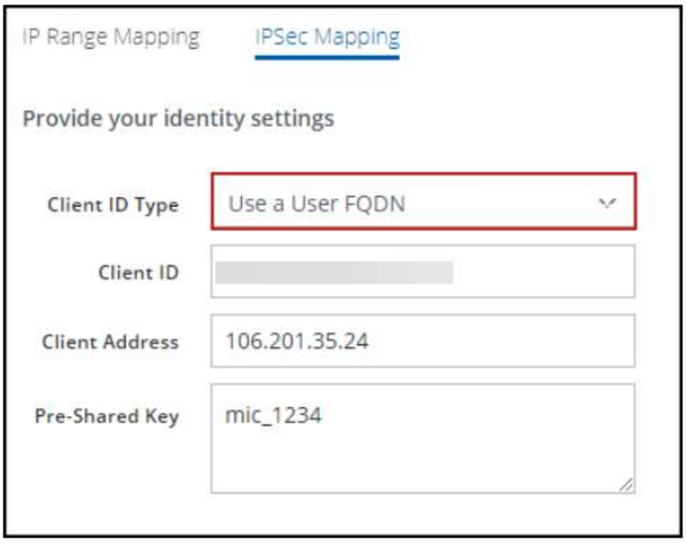
Client Address: 106.201.35.24

Pre-Shared Key: mic_1234

User FQDN

This screenshot shows how to configure IPsec site-to-site authentication in the Citrix SD-WAN 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**.



Provide your identity settings

Client ID Type: Use a User FQDN

Client ID: [redacted]

Client Address: 106.201.35.24

Pre-Shared Key: mic_1234