



Skyhigh® Security Service Edge(SSE)

IPsec Configuration with Versa



Table of Contents

CONFIGURING IPSEC SITE-TO-SITE WITH VERSA.....	3
IPSEC SITE-TO-SITE OVERVIEW	3
ENVIRONMENT.....	3
SETUP INCLUDES.....	3
CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE	3
FINDING THE BEST AVAILABLE POINTS OF PRESENCE	4
TEMPLATE CREATION	5
IPSEC VPN CONFIGURATION OPTIONS.....	9
CLIENT ADDRESS	10
FULLY QUALIFIED DOMAIN NAME	11
USER FQDN	11

Configuring IPsec site-to-site with Versa

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 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)
- Versa Director

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.

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.

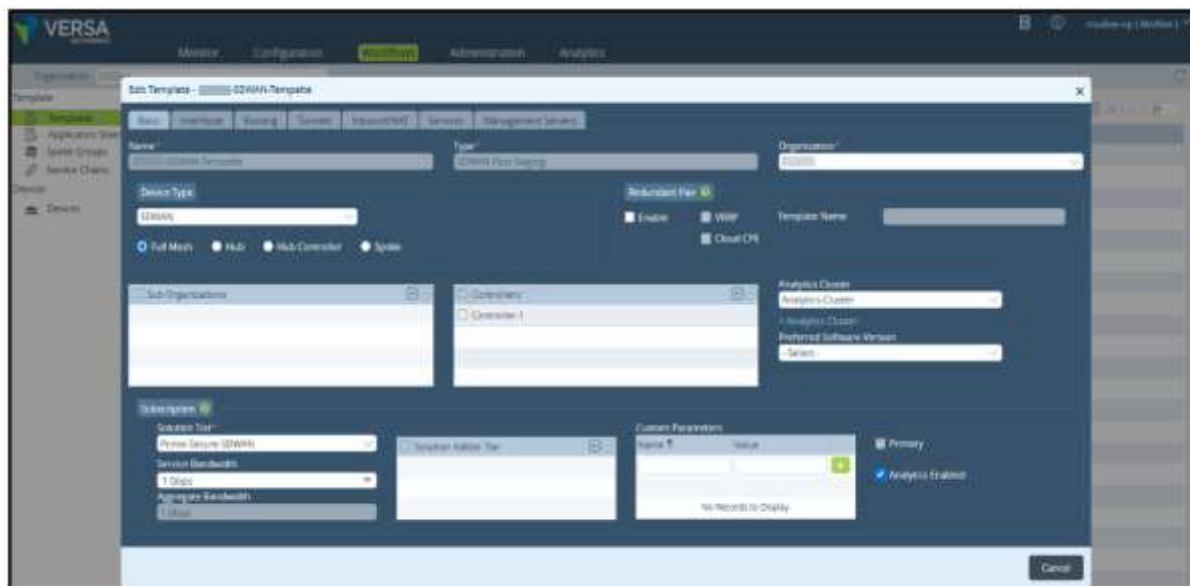
From the network where your device is installed, run the nslookup command-line tool, as follows:

- 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.

Template Creation

1. In the Versa Director interface, select **Workflows | Templates**.



2. Create your LAN interfaces.



3. Select **Management Servers**, then click **Create**. The template is created successfully.

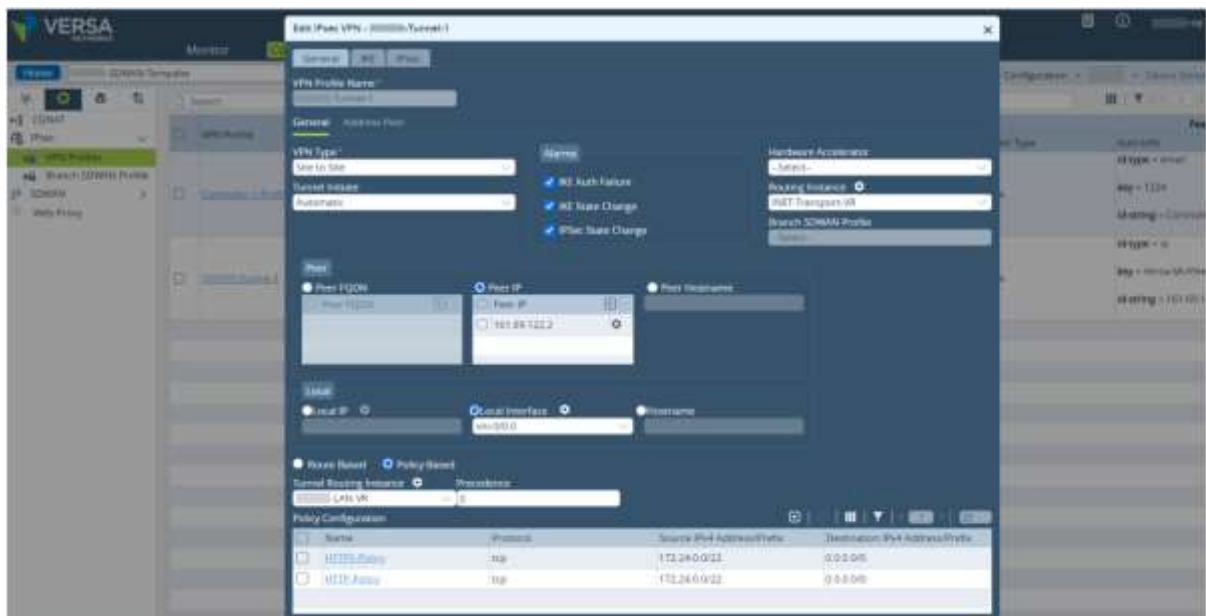
4. Add **Device** and complete the device deployment settings, including the serial number.

The screenshot shows the 'Add Device' dialog box in the VERSA Workflows interface. The dialog has tabs for 'Basic', 'Location Information', 'Turnout Information', 'Device/Service Template', and 'Raw Data'. The 'Basic' tab is active, showing fields for 'Name' (set to 'SDWAN'), 'Global Device ID' (set to '158'), 'Organization' (set to 'SDWAN'), 'Deployment Type' (set to 'CPE-SANMESH Device'), 'Serial Number' (set to '15800000000000000000'), 'Device Group' (set to 'SDWAN-ES'), 'Admin Contact Information' (with 'Email' and 'Phone Number' fields), and 'Subscription' (with 'Service Bandwidth' and 'Aggregation Bandwidth' fields). A 'Cancel' button is at the bottom right.

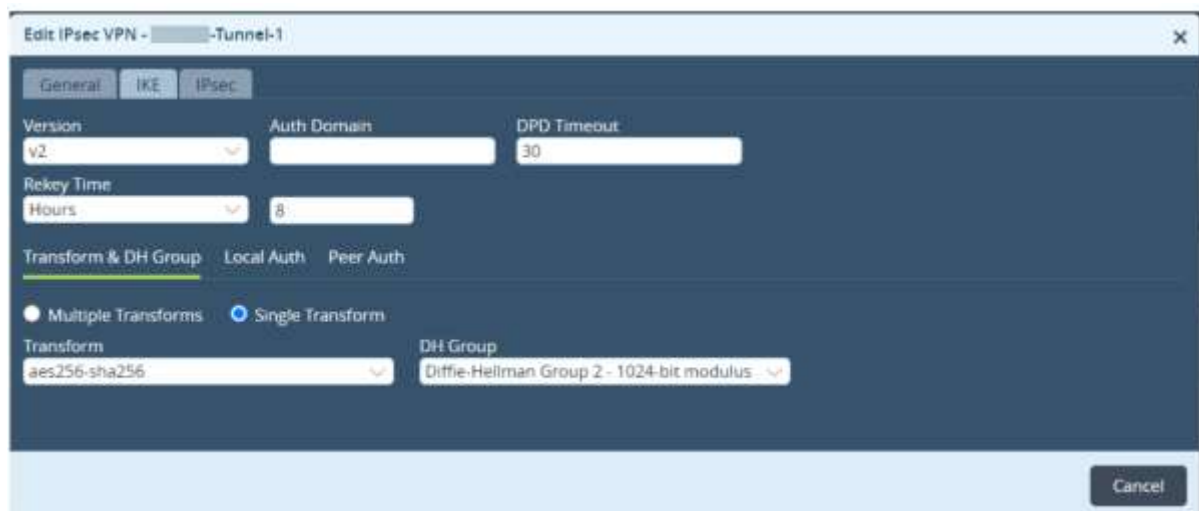
5. **Add/Edit** Application Steering and Deploy.

The screenshot shows the 'Add/Edit Application Steering and Deploy' page in the VERSA Workflows interface. The page is divided into four main sections: 'Real Time' (with 'Real-time Forwarding' and 'Audio Video Forwarding' options), 'Business Critical' (with 'Business Critical Forwarding' and 'Business Critical Forwarding' options), 'Default' (with 'Default Forwarding' and 'Default Forwarding' options), and 'Low Priority' (with 'Low Priority Forwarding' and 'Low Priority Forwarding' options). Each section contains a list of applications with checkboxes for selection. The 'Real Time' section includes 'Voice' and 'Audio Video Forwarding'. The 'Business Critical' section includes 'XDR App', 'Business App', and 'Web App'. The 'Default' section includes 'Google App', 'CloudFront App', and 'Software Update'. The 'Low Priority' section includes 'Advertising', 'Gaming', and 'P2P'. A 'Add Traffic Category' button is at the top right.

6. **Configure VPN Profile.** Select **Configuration | Services | IPsec | VPN Profiles**, then click **+ Add General Profile**.



7. Select **IKE**, then configure **Version v2**.



9. Select **Local Auth**, then configure the settings.

The screenshot shows the 'Edit IPsec VPN - Tunnel-1' dialog box with the 'Local Auth' tab selected. The 'General' tab is also visible. The 'Version' is set to 'v2', 'Auth Domain' is empty, and 'DPD Timeout' is '30'. 'Rekey Time' is set to '8' hours. The 'Transform & DH Group' is 'Local Auth'. The 'Authentication Type' is 'PSK', 'Shared Key' is '(\$v_Tunnel-1_Local_auth_)', 'Identity Type' is 'IP', and 'Identity' is '(\$v_Tunnel-1_Local_auth_)'. A 'Cancel' button is at the bottom right.

10. Select **Peer Auth**, then configure the settings.

- **Authentication Type:** PSK
- **Shared Key:** This value must match pre-shared key that you configure in Skyhigh SSE.
- **Identity Type:** IP/EMAIL/FQDN
- **Identity:** IP address of the best or second-best available PoP returned by the nslookup tool.

Note: The selected algorithms and the value of the pre-shared key must match the IPsec configuration in the Skyhigh SSE. For example, if you select SHA1 for IKE in Versa Director, you must also select SHA1 as the authentication algorithm in Skyhigh SSE.

The screenshot shows the 'Edit IPsec VPN - Tunnel-1' dialog box with the 'Peer Auth' tab selected. The 'General' tab is also visible. The 'Version' is set to 'v2', 'Auth Domain' is empty, and 'DPD Timeout' is '30'. 'Rekey Time' is set to '8' hours. The 'Transform & DH Group' is 'Peer Auth'. The 'Authentication Type' is 'PSK', 'Shared Key' is 'Versa-123', 'Identity Type' is 'IP', and 'Identity' is '161.69.122.2'. A 'Cancel' button is at the bottom right.

11. Select **IPsec**, then configure the settings.

The screenshot shows the 'Edit IPsec VPN' configuration window for 'Tunnel-1'. The 'IPsec' tab is selected. The configuration includes the following settings:

- Mode:** Tunnel
- Anti Replay:** enable
- Fragmentation:** pre-fragmentation
- Force-NAT-T Configuration:** Disable
- Keep Alive Timeout:** 10
- IPsec Rekey Time:** Hours, 8
- IPsec Rekey Volume:** MB
- Transform:** Multiple Transforms (selected), Single Transform
- Transform:** esp-aes256-sha256
- Perfect Forward Secrecy Group:** No PFS

A 'Cancel' button is located at the bottom right of the window.

IPsec VPN configuration options

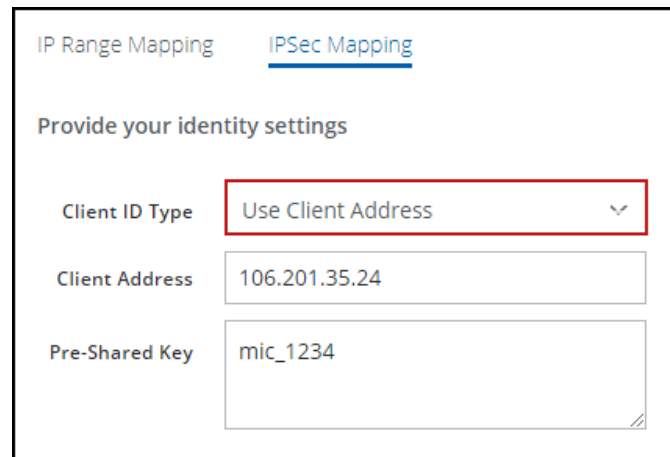
You use one of the following options when configuring IPsec site-to-site authentication in the Versa Director web interface. Then select the same option from the **Child ID Type** drop-down list when configuring IPsec site-to-site in the Skyhigh SSE.

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

Note: To view IPsec configuration in the Skyhigh SSE, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

Client Address

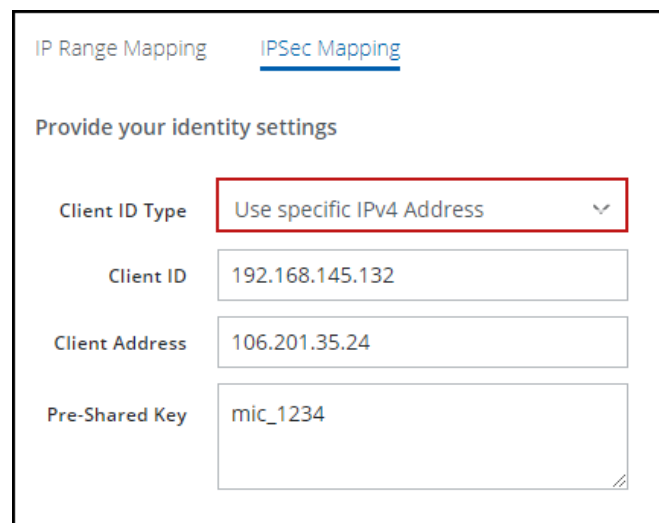
When you configure IPsec in the Versa Director interface using the **Client Address** option, match the values configured in the Skyhigh SSE.



The screenshot shows the 'IPsec Mapping' tab in the Versa Director interface. Under the heading 'Provide your identity settings', the 'Client ID Type' dropdown is set to 'Use Client Address' (highlighted with a red box). The 'Client Address' field contains the value '106.201.35.24', and the 'Pre-Shared Key' field contains 'mic_1234'.

Specific IPv4 Address

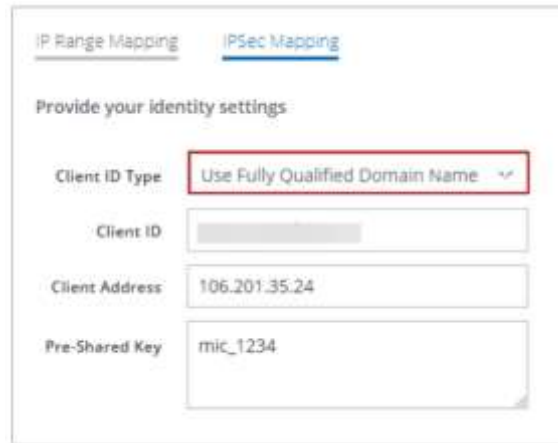
When you configure IPsec in the Versa Director interface using the **Specific IPv4 Address** option, match the values configured in the Skyhigh SSE.



The screenshot shows the 'IPsec Mapping' tab in the Versa Director interface. Under the heading 'Provide your identity settings', the 'Client ID Type' dropdown is set to 'Use specific IPv4 Address' (highlighted with a red box). The 'Client ID' field contains the value '192.168.145.132', the 'Client Address' field contains '106.201.35.24', and the 'Pre-Shared Key' field contains 'mic_1234'.

Fully Qualified Domain Name

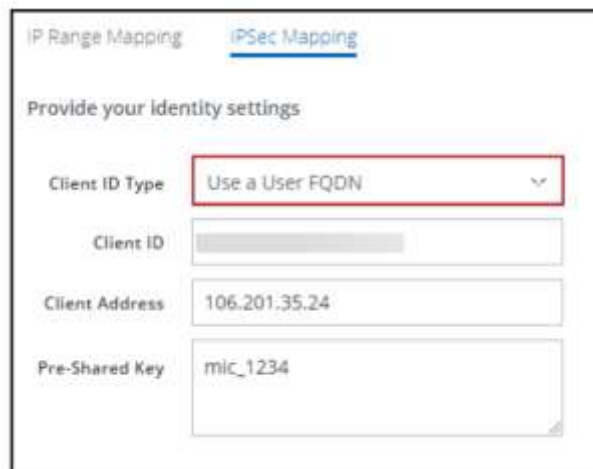
When you configure IPsec in the Versa Director interface using the **Fully Qualified Domain Name** option, match the values configured in the Skyhigh SSE.



The screenshot shows the 'IPsec Mapping' tab in the Versa Director interface. Under the heading 'Provide your identity settings', there are four fields: 'Client ID Type' (a dropdown menu with 'Use Fully Qualified Domain Name' selected and highlighted by a red box), 'Client ID' (an empty text box), 'Client Address' (a text box containing '106.201.35.24'), and 'Pre-Shared Key' (a text box containing 'mic_1234').

User FQDN

When you configure IPsec in the Versa Director interface using the **User FQDN** option, match the values configured in the Skyhigh SSE.



The screenshot shows the 'IPsec Mapping' tab in the Versa Director interface. Under the heading 'Provide your identity settings', there are four fields: 'Client ID Type' (a dropdown menu with 'Use a User FQDN' selected and highlighted by a red box), 'Client ID' (an empty text box), 'Client Address' (a text box containing '106.201.35.24'), and 'Pre-Shared Key' (a text box containing 'mic_1234').

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.