GUIDE

McAfee® Unified Cloud Edge

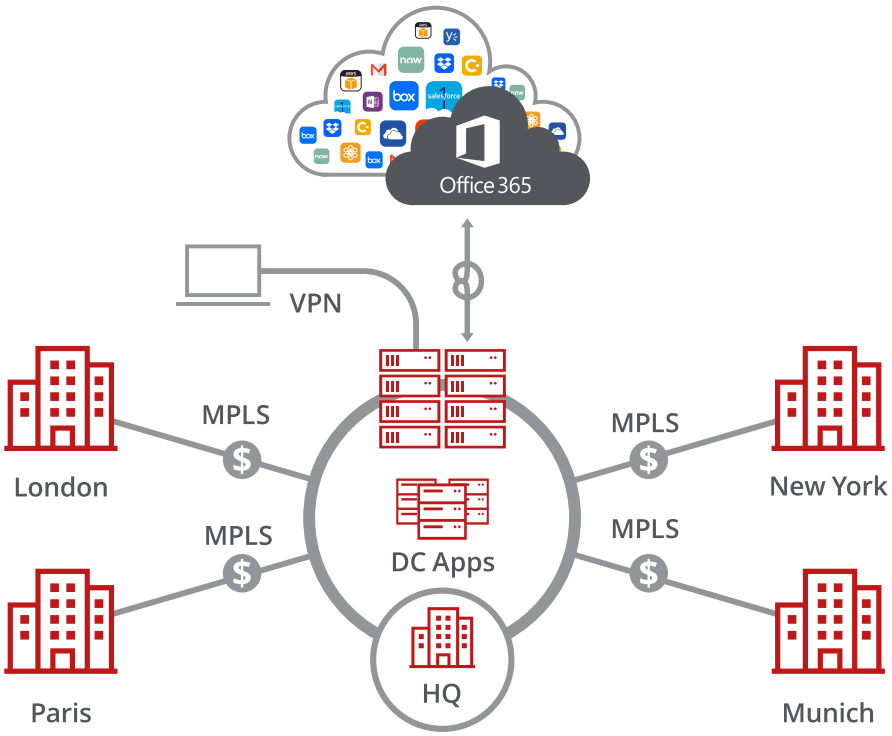
IPSec Configuration Silver Peak EdgeConnect

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 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.

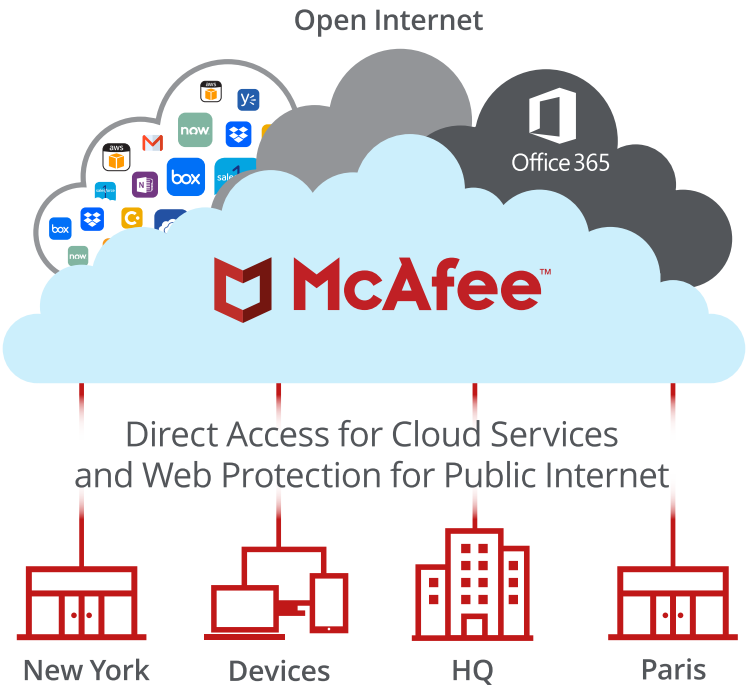
Hub and Spoke Architecture



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

McAfee® Unified Cloud Edge leverages SD-WAN technologies that allow remote offices to securely redirect web traffic to the McAfee® 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 Silver Peak EdgeConnect to McAfee Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configuring IPsec site-to-site with Silver Peak

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 McAfee® Web Gateway Cloud Service (McAfee® WGCS).

IPsec site-to-site overview

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

Environment

- McAfee® MVISION Unified Cloud Edge
- Silver Peak EdgeConnect

Setup includes:

- Configuration of McAfee WGCS using the MVISION Unified Cloud Edge management console
- Configuration of the supported device

For information about configuring McAfee WGCS for IPsec site-to-site, see the McAfee Web Gateway Cloud Service Installation Guide for MVISION Unified Cloud Edge.

Considerations for configuring IPsec site-to-site

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

- **Routing only HTTP and HTTPS traffic** – McAfee 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 McAfee WGCS.
- **Adding SAML authentication** – You can add a SAML configuration to an IPsec site. McAfee 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.mcafee-cloud.com
```

```
nslookup 2.network.wgcs.mcafee-cloud.com
```

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 McAfee WGCS.

Configuring an IPsec VPN tunnel with Silver Peak EdgeConnect

Configure the IPsec VPN tunnel in the Silver Peak EdgeConnect web interface.

Task

1. Log on to the web interface that you use to configure the EdgeConnect device on your remote network.
2. Select **Configuration** | **Tunnels** | **Tunnels** to open the **Tunnels** page.
3. Select **Passthrough** to open the **Passthrough** page.
4. Click the pencil icon to edit the tunnel, then click **Add Tunnel**.
5. Select the **General** tab, then configure these settings:
   - **Alias** – Specify a name for the configuration.
   - **Mode** – Select **IPsec**.
   - **Admin** – Select **Up**.
   - **Local IP** – Provide the public IP address of the EdgeConnect appliance installed on your network.
   - **Remote IP** – Specify the IP address that McAfee WGCS uses for IPsec communications. To find the IP address of the point of presence closest to your device, you can use the nsLook-up command-line tool to query the Global Routing Manager.
   - **NAT** – Select **None**.
   - **Peer/Service** – Leave this field blank.
   - **Auto Max BW Enabled** – Select this setting.
   - **Max BW Kbps** – Leave this field blank.
6. Click **Save** to save the general settings.
7. Select the **IKE** tab, then configure these settings:
   - **Pre-Shared Key** – Provide the same pre-shared key value that you provide when configuring the IPsec location in the MVISION Cloud UI.
   - **Authentication Algorithm** – Select **SHA2** or higher.
   - **Encryption Algorithm** – Select **SHA2-256** or **AES-256**.
   - **Diffie-Hellman Group** – Select 2 or higher.
   - **Lifetime** – Specify **360** for **Mins**.
   - **Dead Peer Detection** – Specify **300** for the **Delay Time** and **5** for the Retry Count.
   - **Local IKE Identifier** – This value must match the **Client ID** that you specify when configuring IPsec in the MVISION Cloud UI. If the **Client ID Type** selected in the MVISION Cloud UI is the **Client Address**, provide the client address for the client ID.
   - **Remote IKE Identifier** – This value must match the value that you provided for the **Remote IP** on the **General** tab.
   - **Phase 1 Mode** – Select **Aggressive**, then select IKE v2 for the IKE Version.

   Note: The selected algorithms and the value of the pre-shared key must match the IPsec configuration in the MVISION Cloud UI. For example, if you select SHA1 for IKE in EdgeConnect, you must also select SHA1 as the authentication algorithm in MVISION Cloud.
8. Click **Save** to save the IKE settings.

9. Select the **IPsec** tab, then configure these settings:
   - **Authentication Algorithm** – Select **SHA2** or higher.
   - **Encryption Algorithm** – Select **SHA2-256** or **AES-256**.
   - **Enable IPsec Anti-replay Window** – Select this setting.
   - **Lifetime** – Specify **360** for **Mins** and **0** for MegaBytes.
   - **Perfect Forward Secrecy Group** – Select **2** or higher.
10. Click **Save**.

The IPsec VPN tunnel is configured on the Silver Peak EdgeConnect side.

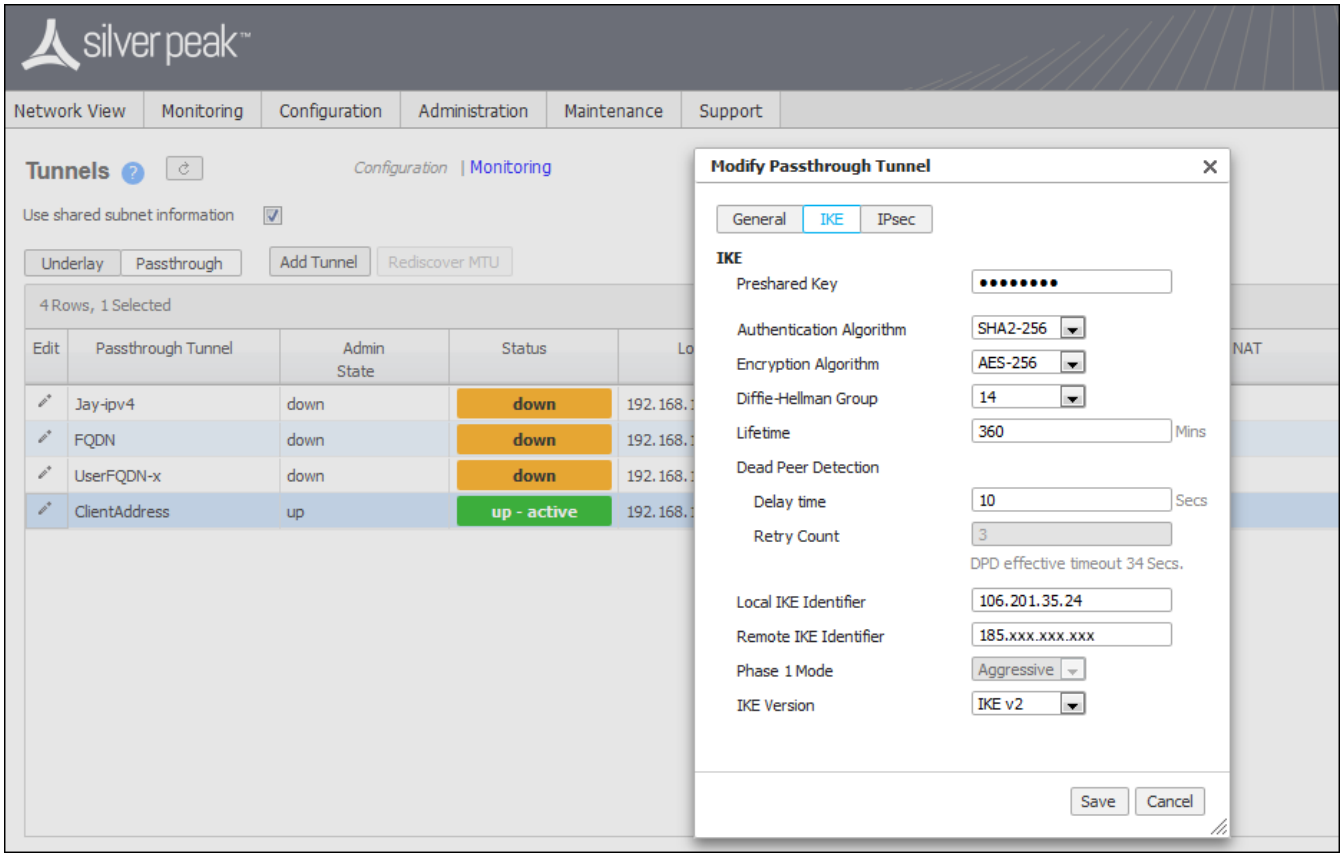
IPsec VPN configuration options

You use one of the following options when configuring IPsec site-to-site authentication in the EdgeConnect web interface. Then you select the same option from the Child ID Type drop-down list when configuring IPsec site-to-site in the MVISION Cloud UI.

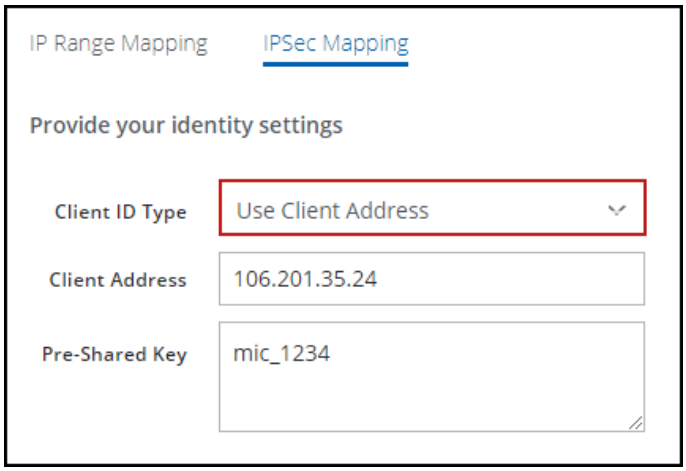
- Client Address
- Specific IPv4 Address
- Fully Qualified Domain Name
- User FQDN

Client Address

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **Client Address** as the **Client ID Type** in the MVISION Cloud UI.

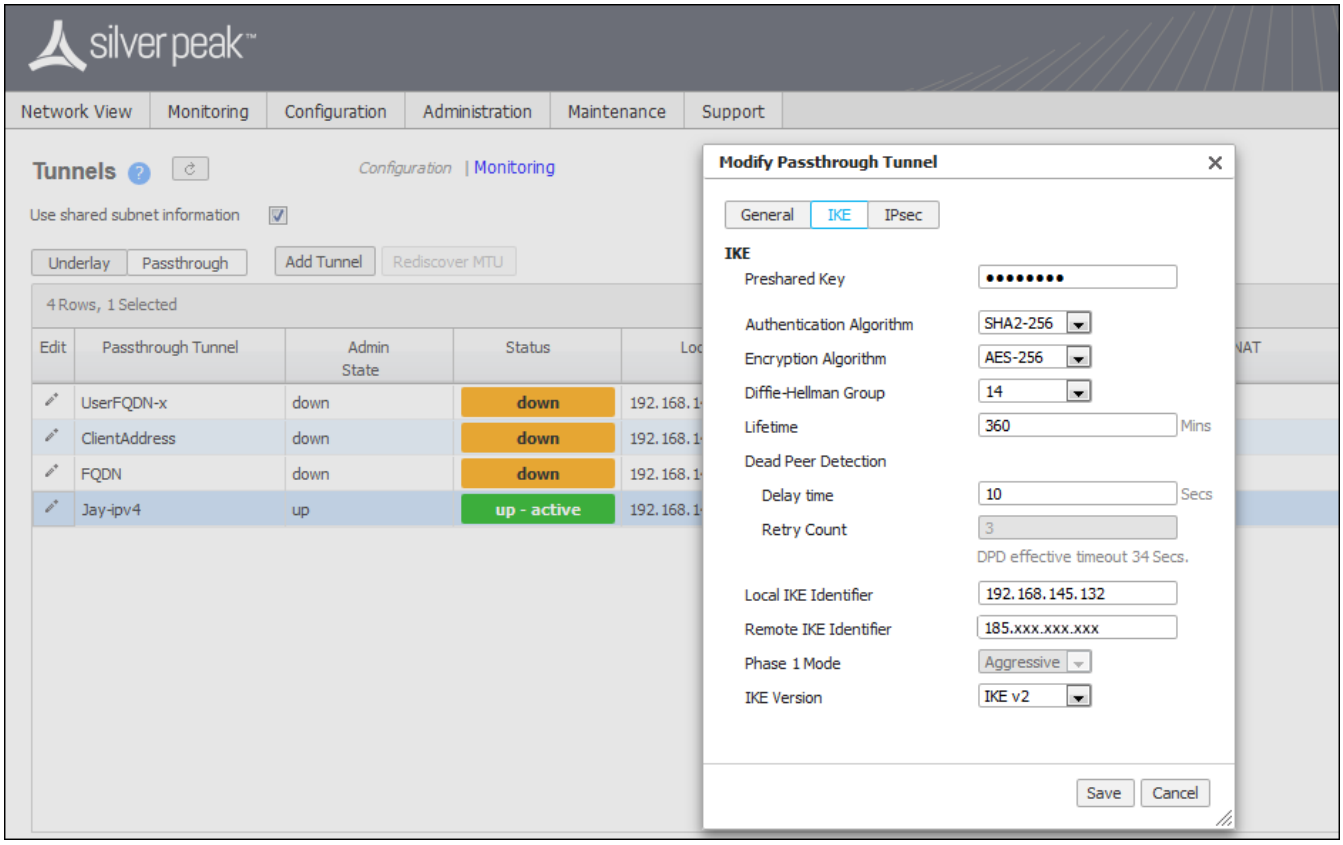


To configure IPsec site-to-site authentication in the MVISION Cloud UI, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

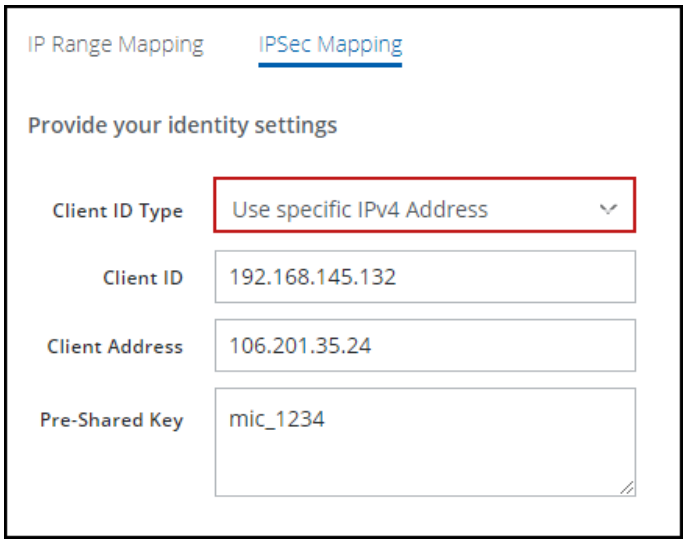


Specific IPv4 Address

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **Specific IPv4 Address** as the **Client ID Type** in the MVISION Cloud UI.

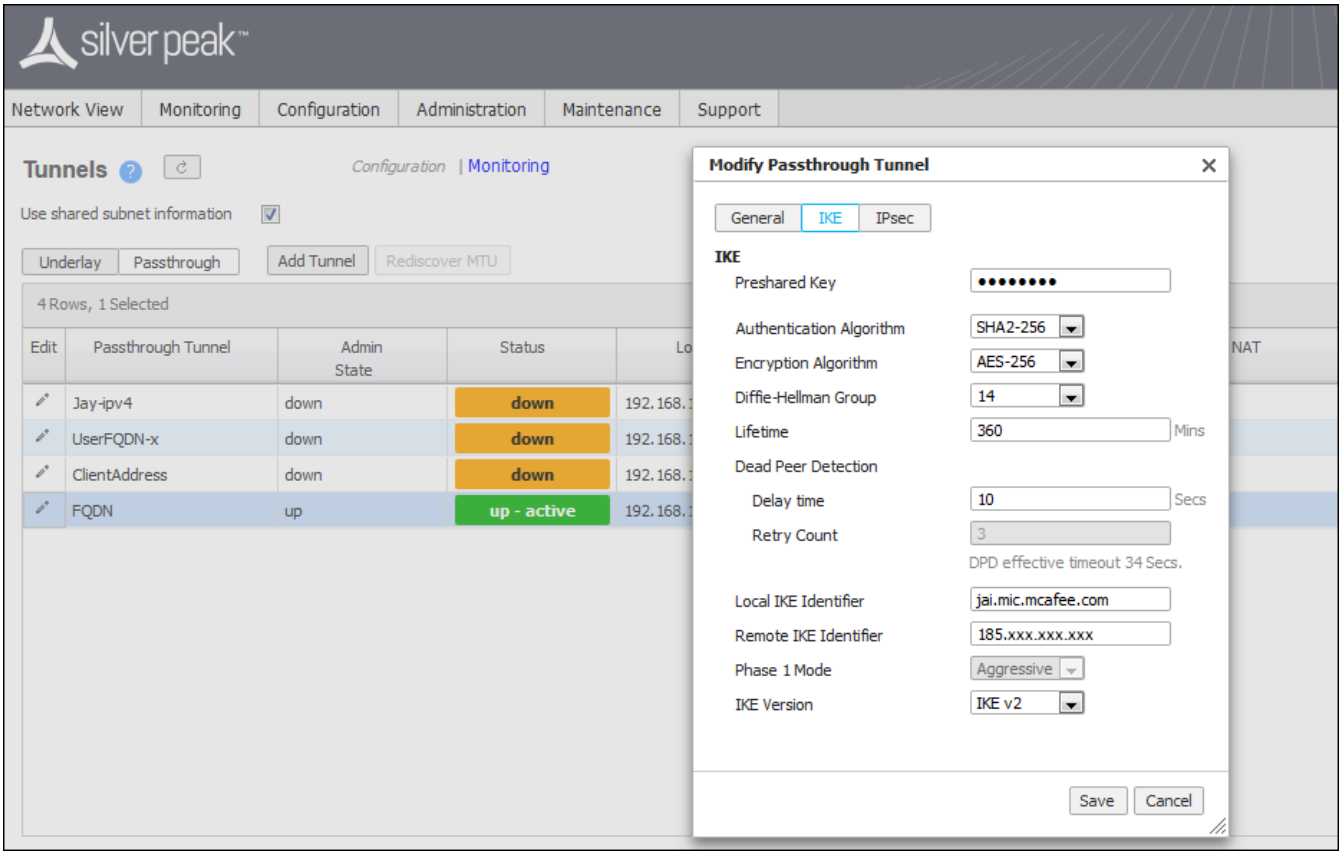


To configure IPsec site-to-site authentication in the MVISION Cloud UI, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

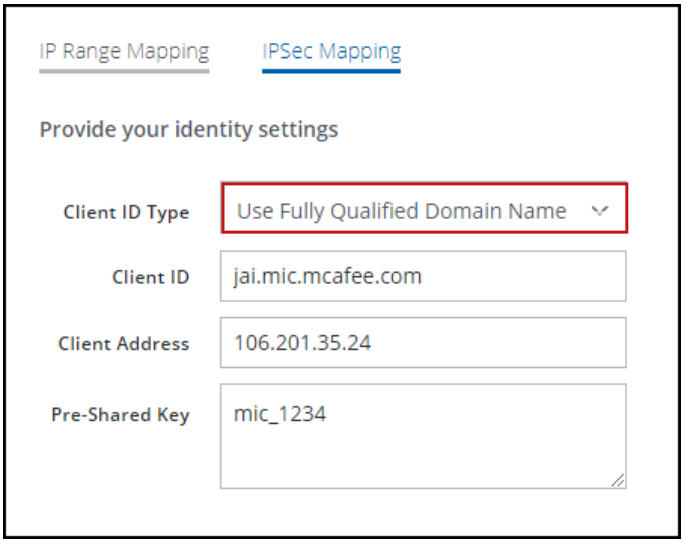


Fully Qualified Domain Name

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **Fully Qualified Domain Name** as the **Client ID Type** in the MVISION Cloud UI.

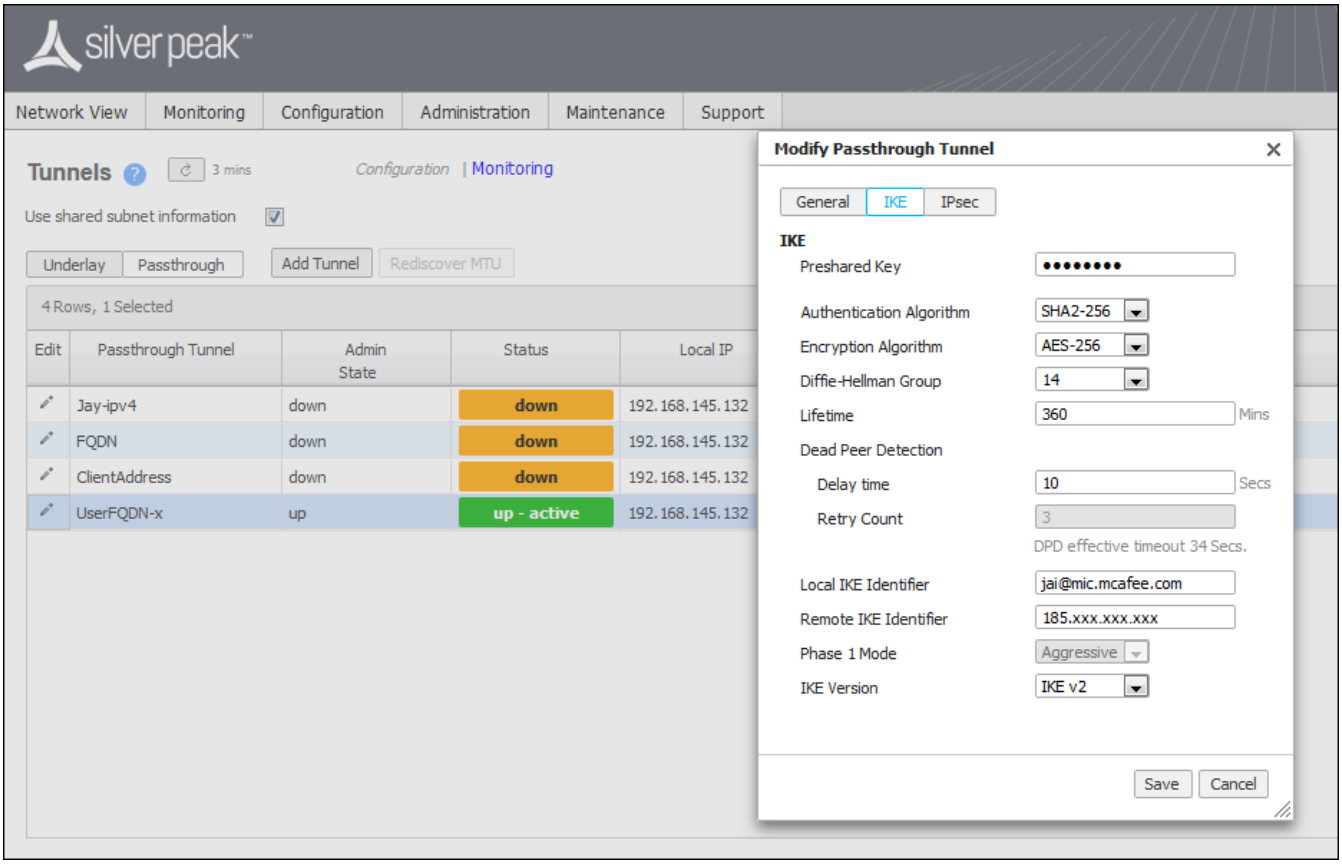


To configure IPsec site-to-site authentication in the MVISION Cloud UI, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

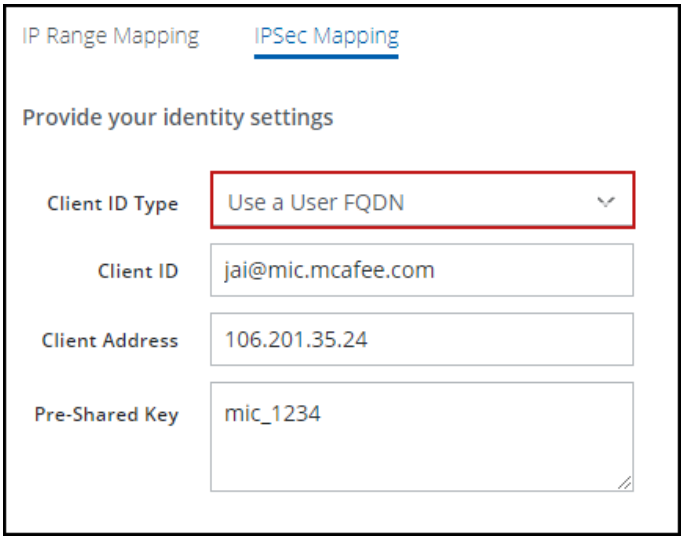


User FQDN

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **User FQDN** as the **Client ID Type** in the MVISION Cloud UI.



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



Configure Business Intent Overlay policies for Silver Peak

To use the IPsec VPN tunnels in a business intent overlay, complete the following steps.

Task

1. From the Silver Peak Orchestrator, select **Configuration: Business Intent Overlay**.
2. Select **Create New**.
3. Select **ACL Policies**, then click **Add Rule**.
4. Click **Edit Match Criteria**, then select **Add port 80, 443**.
5. Click **Save** to return to the previous page.
6. On the Business Intent Overlay page, move the services to the **Preferred Policy Order** section, then move the primary service above the secondary service.
   The primary and secondary services correspond to the primary and secondary IPsec VPN tunnels that you configure. If the primary tunnel is not available, the system sends the web traffic through the secondary tunnel to McAfee WGCS for filtering. If neither tunnel is available, the system drops the web traffic.
7. Click **Save all** to apply the changes.

The business intent overlay policies point to the primary and secondary IPsec VPN tunnels.

McAfee™
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com