Silver Peak

EdgeConnect and McAfee Web Gateway Cloud Service

Integration Guide

201551-001 Rev A

Table of Contents

Copyright and Trademarks

Silver Peak EdgeConnect and McAfee Integration Guide

Date: July 2019

Trademark Notification

Warranties and Disclaimers

Silver Peak Systems, Inc.
2860 De La Cruz Boulevard
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support

Support

For product and technical support, contact Silver Peak Systems at either of the following:

1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com/support

We're dedicated to continually improving the usability of our products and documentation.

- If you have suggestions or feedback for our documentation, send an e-mail to techpubs@silver-peak.com.
- If you have comments or feedback about the interface, send an e-mail to usability@silver-peak.com.

Related Documentation

- **Release Notes** provide information on new software features, system bugs, and software compatibility.
- All user documentation is available at http://www.silver-peak.com.

About

This guide explains how to set up IPsec tunnels and service chain traffic from a Silver Peak EdgeConnect appliance to McAfee Web Gateway Cloud Service to enable advanced security inspection.

Service chain an EdgeConnect appliance with McAfee Web Gateway Cloud Service by setting up interoperable site-to-site IPsec tunnels between the appliance and McAfee's cloud service. Part of the integration process is making sure that the IKE and IPsec algorithms are compatible and that tunnels, policies, and routing can be set up properly.

Prerequisites

Before setting up site-to-site IPsec tunnels, you must have the following:

- ☐ The public IP address of your appliance
- ☐ IP address for the gateway as the destination for your primary and secondary IPsec tunnel

NOTE Use Silver Peak EdgeConnect version 8.1.9.0 or later and Silver Peak Orchestrator version 8.5.0 or later.

Set up IPsec tunnels in McAfee

Set up an IPsec tunnel to a McAfee by adding VPN credentials and link the credentials to a location.

1. Sign in to the McAfee ePolicy Orchestrator Cloud website.

   The home screen opens.

2. From the top left corner of the home screen, expand the menu and select **Authentication Settings**.

   The Authentication screen opens.

3. Across to the right of the **IPsec Site-to-Site Settings**, you will see three consecutive dots. Click on the dots to access the **New Location** option.

   The Detail dialog appears on the right of the screen.

4. Enter the following settings, as shown in the table.

Settings	Description
Name	Enter a descriptive name for the service data center location
External IP	Enter the Pubic IP of your EdgeConnect appliance
Local network	Enter the internal subnet of your local network
Preshared key	Enter the pre-shared key.

5. Determine where you'll be redirecting traffic by finding the closest PoPs.

   You will need to find the IP addresses of the closest Web Gateway Cloud Service points of presence (PoPs) to your location. Be sure to perform the nslookups from the environment where the IPsec tunnel will be configured.

   1. Perform a DNS lookup using the following commands, replacing `XXXXXXXXX` with your customer ID.

      a. **To find the first closest PoPs**: `nslookup 1.network.cXXXXXXXXX.saasprotection.com`

      b. **To find the second closest PoPs**: `nslookup 2.network.cXXXXXXXXX.saasprotection.com`

   2. Once you found the first and second closest PoPs, make a note of the IP addresses for later steps.

   You can now create your IPsec tunnels on the appliance.

Deployment scenarios with Silver Peak EdgeConnect

Silver Peak supports three ways to configure and deploy an EdgeConnect appliance with McAfee.

- Active-backup internet breakout
- Active-active internet breakout
- Branch HA, Internet breakout

Active-backup internet breakout

In this scenario, active-backup tunnels send traffic between the appliance and McAfee Web Gateway Cloud Service.

Figure 1: Active-backup mode.

Configure IPsec tunnels

1. Sign in to the Silver Peak Orchestrator.
2. Select **Configuration**: **Tunnels**:**Tunnels**.

   The Tunnels screen opens.
3. Select **Passthrough**.

   The Passthrough screen opens.
4. Click the pencil icon to edit the tunnel.
5. Select **Add Tunnel**.
6. Select **General**.
7. Fill in the following fields.

General	Task
Alias	Enter a name for the alias.
Mode	Select **IPSec**.
Admin	Select **up**.
Local IP	Enter the local IP of the actual appliance located on prem.

Remote IP	Enter the remote IP located in the cloud. Use the EdgeConnect appliance public IP as the local IP.
NAT	Select **None**.
Peer/Service	
Auto Max BW Enabled	Enable the check box.
Max BW Kbps	Leave this field blank.

8. Click **Save**.
9. Select the **IKE** tab.
10. Fill in the following fields.

IPsec	Task
Pre-Shared Key	Enter the same pre-shared key that you entered when creating the VPN credential on the McAfee ePolicy Orchestrator Cloud website.
Authentication Algorithm	Select **SHA1** or higher.
Encryption Algorithm	Select **SHA2-256** or **AES-256**.
Diffie-Hellman Group	Select **2** or higher.
Lifetime	In the **Mins** field, enter **360**.
Dead Peer Detection	For **Delay time**, enter **300**. For **Retry Count**, enter **5**.
IKE Identifier	Select **IP ADDRESS**.
Phase 1 Mode	Select **Main**.

NOTE The algorithms and the preshared key must match the ePolicy Orchestrator Cloud. For example, if you select **SHA1** for IKE, the authentication algorithm in ePolicy Orchestrator Cloud should also be **SHA1**.

11. Click **Save.**
12. Select the **IPsec** tab.
13. Fill in the following fields.

IPsec	Task
Authentication Algorithm	Select **SHA1** or higher.

Encryption Algorithm	Select **SHA2-256** or **AES-256**.
Enable IPsec Anti-replay Window	Enable the check box.
Lifetime	In the **Mins** field, enter **360**. In the MegaBytes field, enter **0**.
Perfect Forward Secrecy Group	Select **2** or higher.

14. Click **Save**.

    You created an IPsec VPN tunnel to the primary ePolicy Orchestrator Cloud.

Create a secondary IPsec VPN tunnel

1. Select the **Passthrough** tab.
2. Select **Add Tunnels**.
3. Create a secondary tunnel by entering a different peer/service name and public IP address for the secondary IPSec tunnel than the one used for the primary tunnel.

You are now ready to configure business intent overlays.

Configure Business Intent Overlay policies

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

1. From the Silver Peak Orchestrator, select **Configuration**: **Business Intent Overlay**.
2. Select **Policies**.
3. In the **Service Name** field, type a name for your peer/service.
4. Click **Close** to return to the previous screen.
5. From the **Business Intent Overlay** screen, move the services to the **Preferred Policy Order** section.
6. In the **Preferred Policy Order** section, move the primary service above the secondary service.

   By moving the primary service to the top of the list, all internet-bound traffic passes through the **McAfee_Primary** tunnel. If the primary tunnel is down, traffic then passes through the **McAfee_Backup** tunnel. If both tunnels are down, the system drops the traffic.

7. Select **Save all** all to apply all changes.

You have configured business intent overlay policies that point to the IPsec VPN tunnels.

Active-active internet breakout

In this scenario, active-active tunnels load-balance the traffic to McAfee Web Gateway Cloud Service

Use the same peer/service name for both McAfee tunnels. When tunnels use identical names, the EdgeConnect load balances the traffic between both tunnels.

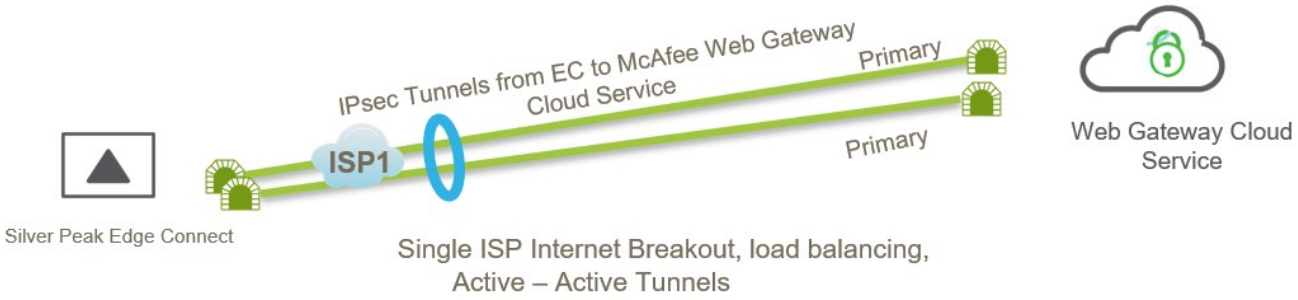


Figure 2: Active-active mode.

Configure IPsec tunnels

1. Sign in to the Silver Peak Orchestrator.
2. Select **Configuration**: **Tunnels**:**Tunnels**.

   The Tunnels screen opens.
3. Select **Passthrough**.

   The Passthrough screen opens.
4. Click the pencil icon to edit the tunnel.
5. Select **Add Tunnel**.
6. Select **General**.
7. Fill in the following fields.

General	Task
Alias	Enter a name for the alias.
Mode	Select **IPSec**.
Admin	Select **up**.

Local IP	Enter your appliance IP, which can be private if the appliance is behind a NAT or public.
Remote IP	Enter the remote IP located in the cloud. Use the EdgeConnect appliance public IP as the local IP.
NAT	Select **None**.
Peer/Service	
Auto Max BW Enabled	Enable the check box.
Max BW Kbps	Leave this field blank.

8. Click **Save**.
9. Select the **IKE** tab.
10. Fill in the following fields.

IPsec	Task
Pre-Shared Key	Enter the same pre-shared key that you entered when creating the VPN credential on the McAfee ePolicy Orchestrator Cloud website.
Authentication Algorithm	Select **SHA1** or higher.
Encryption Algorithm	Select **AES-128**.
Diffie-Hellman Group	Select **2** or higher.
Lifetime	In the **Mins** field, enter **360**.
Dead Peer Detection	For **Delay time**, enter **300**. For **Retry Count**, enter **5**.
IKE Identifier	Select **IP ADDRESS**.
Phase 1 Mode	Select **Main**.

NOTE The algorithms and the preshared key must match the ePolicy Orchestrator Cloud. For example, if you select **SHA1** for IKE, the authentication algorithm in ePolicy Orchestrator Cloud should also be **SHA1**.

11. Click **Save.**
12. Select the **IPsec** tab.
13. Fill in the following fields.

IPsec	Task

Authentication Algorithm	Select **SHA1** or higher.
Encryption Algorithm	Select **AES-128**.
Enable IPsec Anti-replay Window	Enable the check box.
Lifetime	In the **Mins** field, enter **360**. In the MegaBytes field, enter **0**.
Perfect Forward Secrecy Group	Select **2** or higher.

14. Click **Save**.

    You created an IPsec VPN tunnel to the primary ePolicy Orchestrator Cloud.

Create a secondary IPsec VPN tunnel

1. Select the **Passthrough** tab.
2. Select **Add Tunnels**.
3. Create a secondary tunnel by entering the same values that you used for the first tunnel. The peer/service name for the secondary IPSec tunnel must be identical to the primary one. However, make sure the pubic IP address of the secondary tunnel is different from the one you used for the primary tunnel.

You are now ready to configure business intent overlays.

Configure Business Intent Overlay policies

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

1. From the Silver Peak Orchestrator, select **Configuration**: **Business Intent Overlay**.
2. Select **Policies**.
3. In the **Service Name** field, type a name for your peer/service.

   The name must match with the peer/service name you created earlier in step 3 from the Active-active internet breakout section.

4. Click **Close** to return to the previous screen.
5. From the **Business Intent Overlay** screen, move the services to the **Preferred Policy Order** section.

6. In the **Preferred Policy Order** section, move the primary service above the secondary service.
7. Select **Save all** all to apply all changes.

You have configured business intent overlay policies that point to the IPsec VPN tunnels.

Branch HA, Internet breakout

In this scenario, extra device redundancy is provided by Silver Peak branch HA.

Figure 3: Branch HA mode.

Configure branch HA

1. From the Silver Peak Orchestrator, navigate to **Configuration: VRRP**.
2. Configure VRRP on both appliances--one as the master and the other as backup.

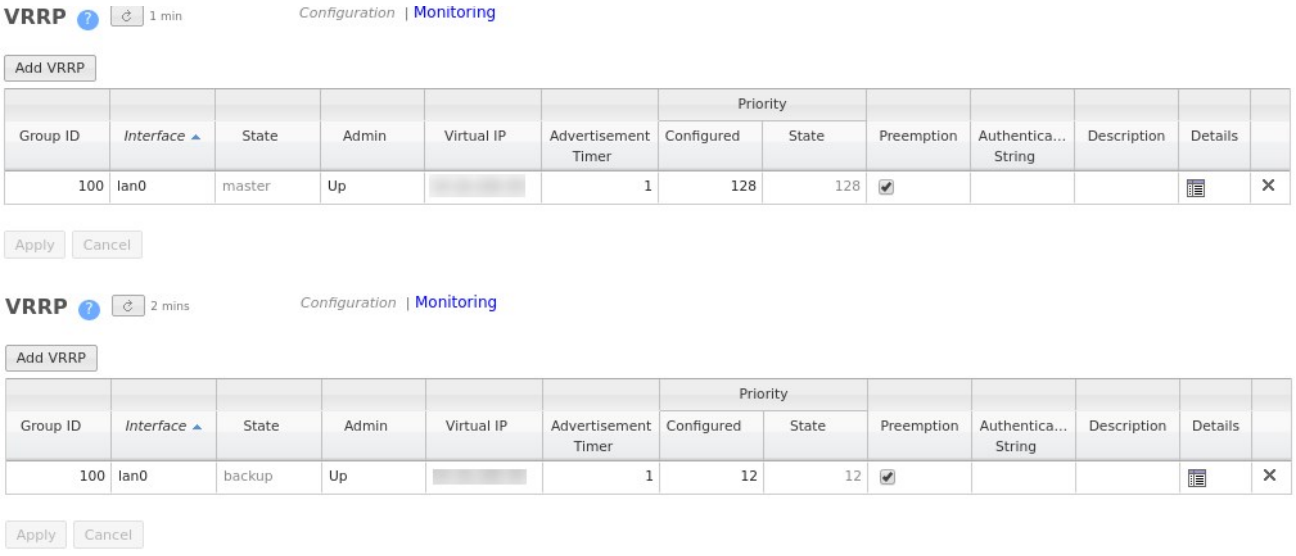


Figure 4: VRRP example

3. To configure HA, right-click on one of the appliances from the left panel to expand the menu, and click **Deployment**.

   The Deployment dialog pop-up appears.

4. Select the check box **EdgeConnect HA**.
5. Select another appliance from the HA Peer drop-down list.
6. Select the interface which binds the two appliances. WAN0 from different appliances, as shown in the example below, should be assigned with difference labels.

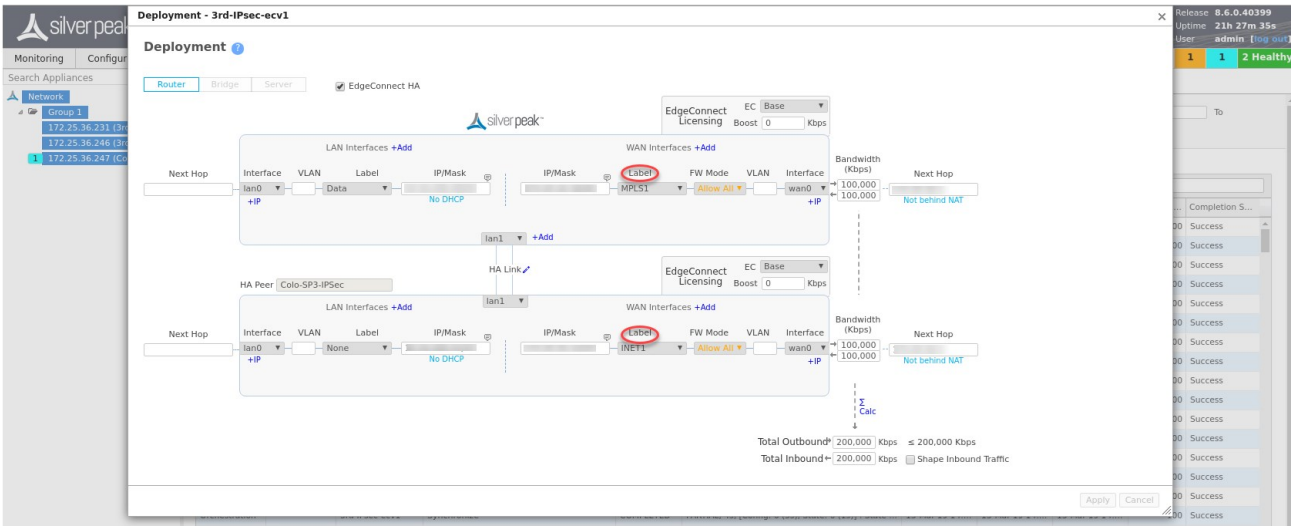


Figure 5: HA configuration.

7. Apply the changes.

NOTE Deployment settings on the appliances should be displayed, as in the example below. The interfaces with VLAN are for HA use.

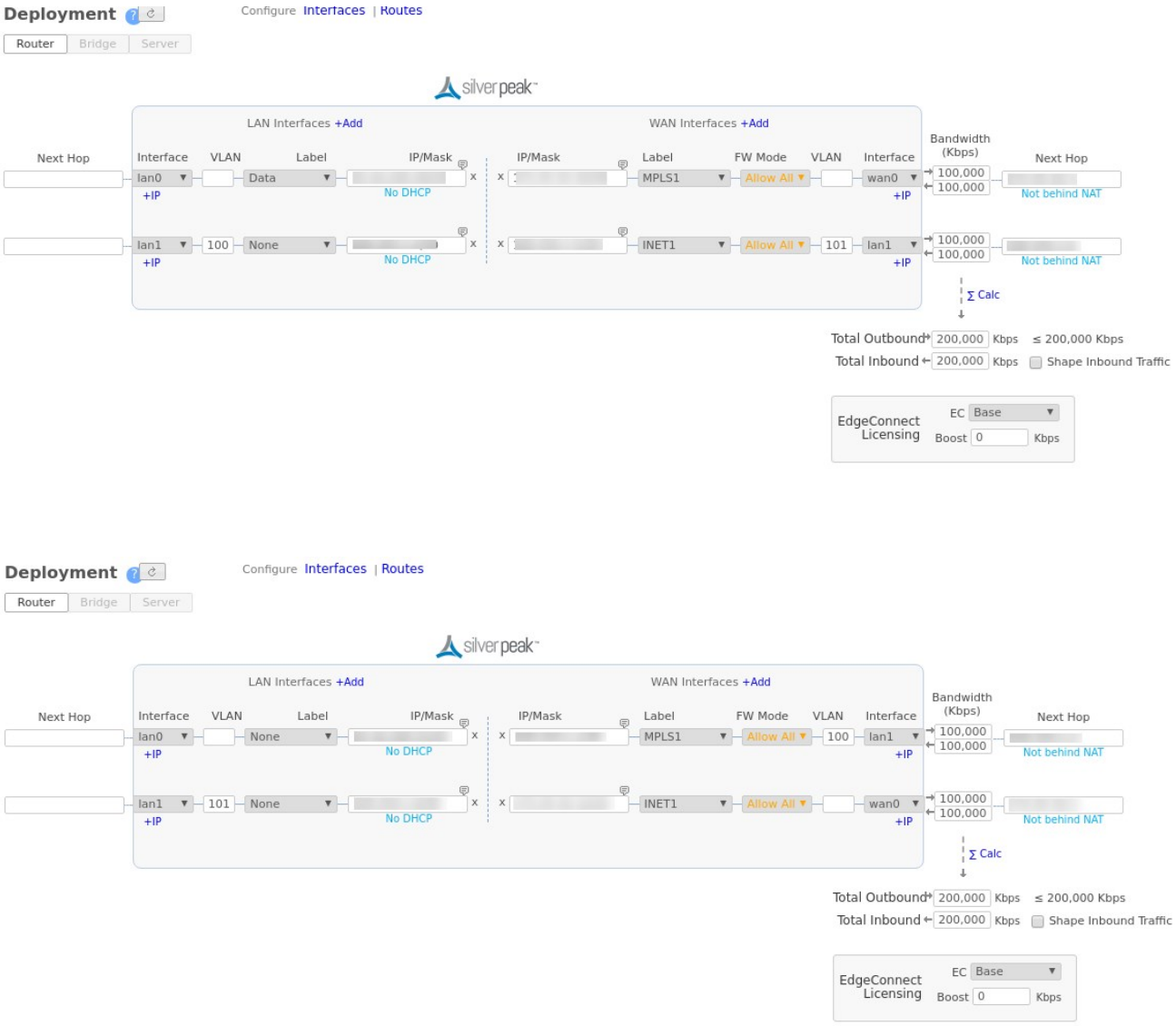
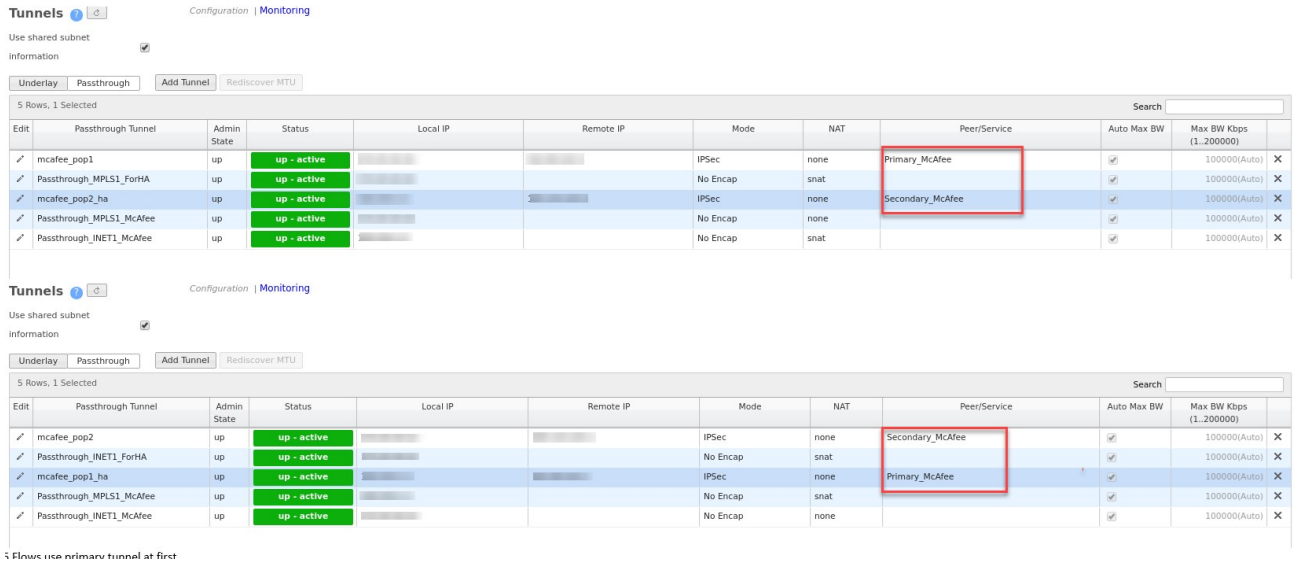


Figure 6: Deployment settings.

8. Create the McAfee tunnels on the appliances.



Flows will use the primary tunnel, and if that tunnel goes down, the flows will fail over to the secondary tunnel.