

Silver Peak

# EdgeConnect and McAfee Web Gateway Cloud Service

## Integration Guide

# Table of Contents

---

<b>Table of Contents</b> .....	<b>2</b>
<b>Copyright and Trademarks</b> .....	<b>3</b>
<b>Support</b> .....	<b>4</b>
<b>Related Documentation</b> .....	<b>5</b>
<b>About</b> .....	<b>6</b>
Prerequisites .....	7
Set up IPsec tunnels in McAfee .....	8
<b>Deployment scenarios with Silver Peak EdgeConnect</b> .....	<b>9</b>
Active-backup internet breakout .....	10
Configure IPsec tunnels .....	10
Create a secondary IPsec VPN tunnel .....	12
Configure Business Intent Overlay policies .....	12
Active-active internet breakout .....	14
Configure IPsec tunnels .....	14
Create a secondary IPsec VPN tunnel .....	16
Configure Business Intent Overlay policies .....	16
Branch HA, Internet breakout .....	18
Configure branch HA .....	18

# Copyright and Trademarks

Silver Peak EdgeConnect and McAfee Integration Guide

Date: July 2019

Copyright © 2019 Silver Peak Systems, Inc. All rights reserved. Information in this document is subject to change at any time. Use of this documentation is restricted as specified in the End User License Agreement. No part of this documentation can be reproduced, except as noted in the End User License Agreement, in whole or in part, without the written consent of Silver Peak Systems, Inc.

## Trademark Notification

The following are trademarks of Silver Peak Systems, Inc.: Silver Peak Systems™, the Silver Peak logo, Network Memory™, Silver Peak NX-Series™, Silver Peak VX-Series™, Silver Peak VRX-Series™, Silver Peak Silver Peak Unity EdgeConnect™, and Silver Peak Orchestrator™. All trademark rights reserved. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

## Warranties and Disclaimers

THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SILVER PEAK SYSTEMS, INC. ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THIS DOCUMENTATION OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS DOCUMENTATION. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL SILVER PEAK SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENTATION. THIS DOCUMENTATION MAY INCLUDE TECHNICAL OR OTHER INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENTATION. SILVER PEAK SYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENTATION AT ANY TIME.

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](http://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](mailto:techpubs@silver-peak.com).
- If you have comments or feedback about the interface, send an e-mail to [usability@silver-peak.com](mailto: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
<b>Name</b>	Enter a descriptive name for the service data center location
<b>External IP</b>	Enter the Public IP of your EdgeConnect appliance
<b>Local network</b>	Enter the internal subnet of your local network
<b>Preshared key</b>	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 `XXXXXXXXXX` with your customer ID.
  - a. **To find the first closest PoPs:** `nslookup 1.network.cXXXXXXXXXX.saasprotection.com`
  - b. **To find the second closest PoPs:** `nslookup 2.network.cXXXXXXXXXX.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.

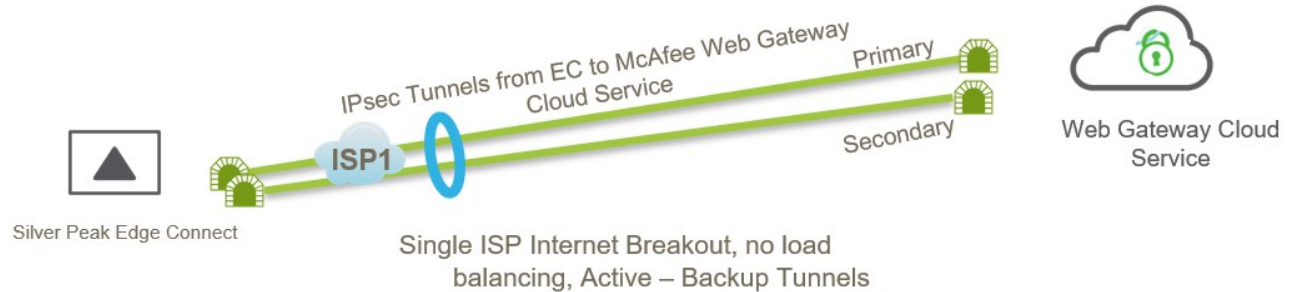


Figure 1: Active-backup mode.

### 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
<b>Alias</b>	Enter a name for the alias.
<b>Mode</b>	Select <b>IPSec</b> .
<b>Admin</b>	Select <b>up</b> .
<b>Local IP</b>	Enter the local IP of the actual appliance located on prem.

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

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

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

**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
<b>Authentication Algorithm</b>	Select <b>SHA1</b> or higher.

<b>Encryption Algorithm</b>	Select <b>SHA2-256</b> or <b>AES-256</b> .
<b>Enable IPsec Anti-replay Window</b>	Enable the check box.
<b>Lifetime</b>	In the <b>Mins</b> field, enter <b>360</b> . In the <b>MegaBytes</b> field, enter <b>0</b> .
<b>Perfect Forward Secrecy Group</b>	Select <b>2</b> 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** 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
<b>Alias</b>	Enter a name for the alias.
<b>Mode</b>	Select <b>IPSec</b> .
<b>Admin</b>	Select <b>up</b> .

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

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

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

**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

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

**VRRP** ⓘ ⌚ 1 min Configuration | Monitoring

Add VRRP

Group ID	Interface ▲	State	Admin	Virtual IP	Advertisement Timer	Priority		Preemption	Authenticat... String	Description	Details
						Configured	State				
100	lan0	master	Up		1	128	128	<input checked="" type="checkbox"/>			ⓘ ✕

Apply Cancel

**VRRP** ⓘ ⌚ 2 mins Configuration | Monitoring

Add VRRP

Group ID	Interface ▲	State	Admin	Virtual IP	Advertisement Timer	Priority		Preemption	Authenticat... String	Description	Details
						Configured	State				
100	lan0	backup	Up		1	12	12	<input checked="" type="checkbox"/>			ⓘ ✕

Apply Cancel

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.

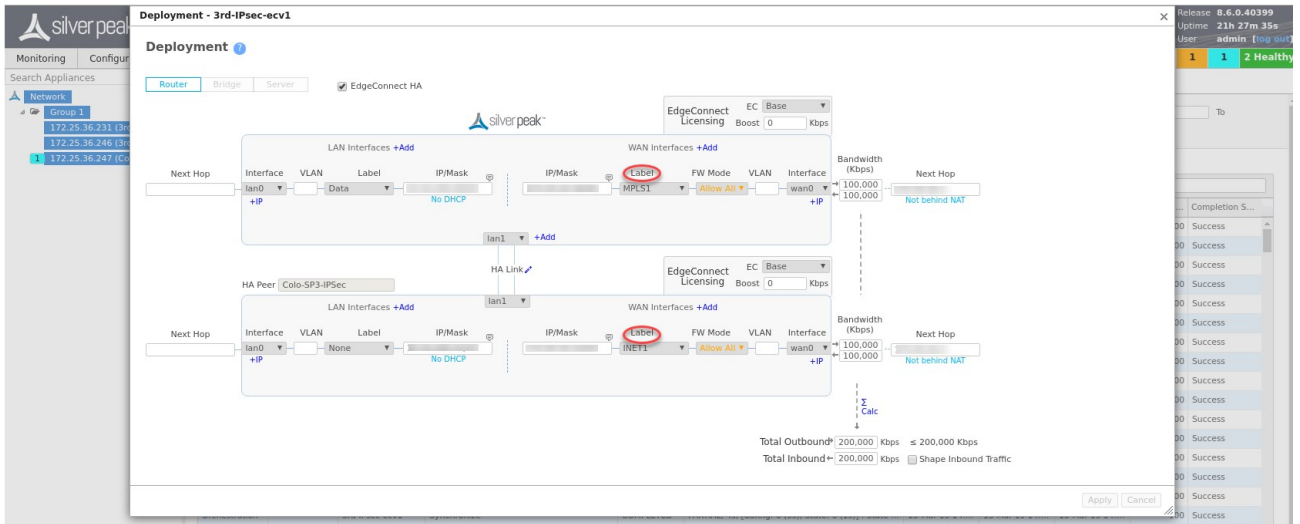


Figure 5: HA configuration.

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.

**Deployment** Configure Interfaces | Routes

Router Bridge Server

LAN Interfaces +Add

Next Hop	Interface	VLAN	Label	IP/Mask
	lan0		Data	No DHCP
	lan1	100	None	No DHCP

WAN Interfaces +Add

IP/Mask	Label	FW Mode	VLAN	Interface	Bandwidth (Kbps)	Next Hop
	MPLS1	Allow All		wan0	100,000	Not behind NAT
	INET1	Allow All	101	lan1	100,000	Not behind NAT

Total Outbound\* 200,000 Kbps ≤ 200,000 Kbps  
 Total Inbound ← 200,000 Kbps  Shape Inbound Traffic

EdgeConnect Licensing EC Base Boost 0 Kbps

**Deployment** Configure Interfaces | Routes

Router Bridge Server

LAN Interfaces +Add

Next Hop	Interface	VLAN	Label	IP/Mask
	lan0		None	No DHCP
	lan1	101	None	No DHCP

WAN Interfaces +Add

IP/Mask	Label	FW Mode	VLAN	Interface	Bandwidth (Kbps)	Next Hop
	MPLS1	Allow All	100	lan1	100,000	Not behind NAT
	INET1	Allow All		wan0	100,000	Not behind NAT

Total Outbound\* 200,000 Kbps ≤ 200,000 Kbps  
 Total Inbound ← 200,000 Kbps  Shape Inbound Traffic

EdgeConnect Licensing EC Base Boost 0 Kbps

Figure 6: Deployment settings.

8. Create the McAfee tunnels on the appliances.

**Tunnels** Configuration | Monitoring

Use shared subnet

Information

Underlay Passthrough Add Tunnel Rediscover MTU

5 Rows, 1 Selected Search

Edit	Passthrough Tunnel	Admin State	Status	Local IP	Remote IP	Mode	NAT	Peer/Service	Auto Max BW	Max BW Kbps (1..200000)	
✓	mcafee_pop1	up	up - active			IPSec	none	Primary_McAfee	<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	Passthrough_MPLS1_ForHA	up	up - active			No Encap	snat		<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	mcafee_pop2_ha	up	up - active			IPSec	none	Secondary_McAfee	<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	Passthrough_MPLS1_McAfee	up	up - active			No Encap	none		<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	Passthrough_INET1_McAfee	up	up - active			No Encap	snat		<input checked="" type="checkbox"/>	100000(Auto)	✕

**Tunnels** Configuration | Monitoring

Use shared subnet

Information

Underlay Passthrough Add Tunnel Rediscover MTU

5 Rows, 1 Selected Search

Edit	Passthrough Tunnel	Admin State	Status	Local IP	Remote IP	Mode	NAT	Peer/Service	Auto Max BW	Max BW Kbps (1..200000)	
✓	mcafee_pop2	up	up - active			IPSec	none	Secondary_McAfee	<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	Passthrough_INET1_ForHA	up	up - active			No Encap	snat		<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	mcafee_pop1_ha	up	up - active			IPSec	none	Primary_McAfee	<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	Passthrough_MPLS1_McAfee	up	up - active			No Encap	snat		<input checked="" type="checkbox"/>	100000(Auto)	✕
✓	Passthrough_INET1_McAfee	up	up - active			No Encap	none		<input checked="" type="checkbox"/>	100000(Auto)	✕

Flows use primary tunnel at first

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