Silver Peak

EdgeConnect and Forcepoint Web Security Cloud

Integration Guide

201423-001 Rev A

Table of Contents

Copyright and Trademarks

Silver Peak EdgeConnect and Forcepoint Web Security Cloud Integration Guide

Date: November 2018

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 PeakSilver 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

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 https://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 the Forcepoint Web Security Cloud.

Service chain an EdgeConnect appliance with Forcepoint by setting up interoperable site-to-site IPsec tunnels between the EdgeConnect appliance and Forcepoint. 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 between the services.

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

Set up Forcepoint

Prerequisites

Before setting up site-to-site IPsec tunnels, complete the following tasks.

- ☐ Find the public IP address of your Silver Peak EdgeConnect appliance.
- ☐ Find the MAC address of the source interface of your appliance.
- ☐ Generate a pre-shared key that you use for both Forcepoint and EdgeConnect.

Add an edge device in Forcepoint

1. Sign in to the Forcepoint Web Security Cloud portal with your user credentials.
2. In the main screen, select **Web** > **Network Devices** > **Device Management**.
3. Select the add file button.
4. Select **Add Edge Device**.

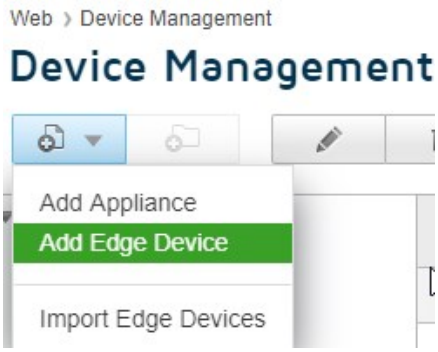

Figure 1: Forcepoint Added Edge Device.

5. In the **Name** field, enter a name for this appliance.
6. From the **Device type** list, select **Other**.
7. In the **Description** field, enter a descriptive text.
8. In the **MAC address** field, enter the MAC address of your appliance. The MAC address is the source interface of your appliance, such as **wan0**.
9. Select **Pre-shared key (PSK)**.
10. In the **Egress IP Address** field, enter the public IP of your Silver Peak appliance.
11. From the **Pre-shared key** list, select **Use your own key** and enter the key name in the blank field.
12. Select **Save**.

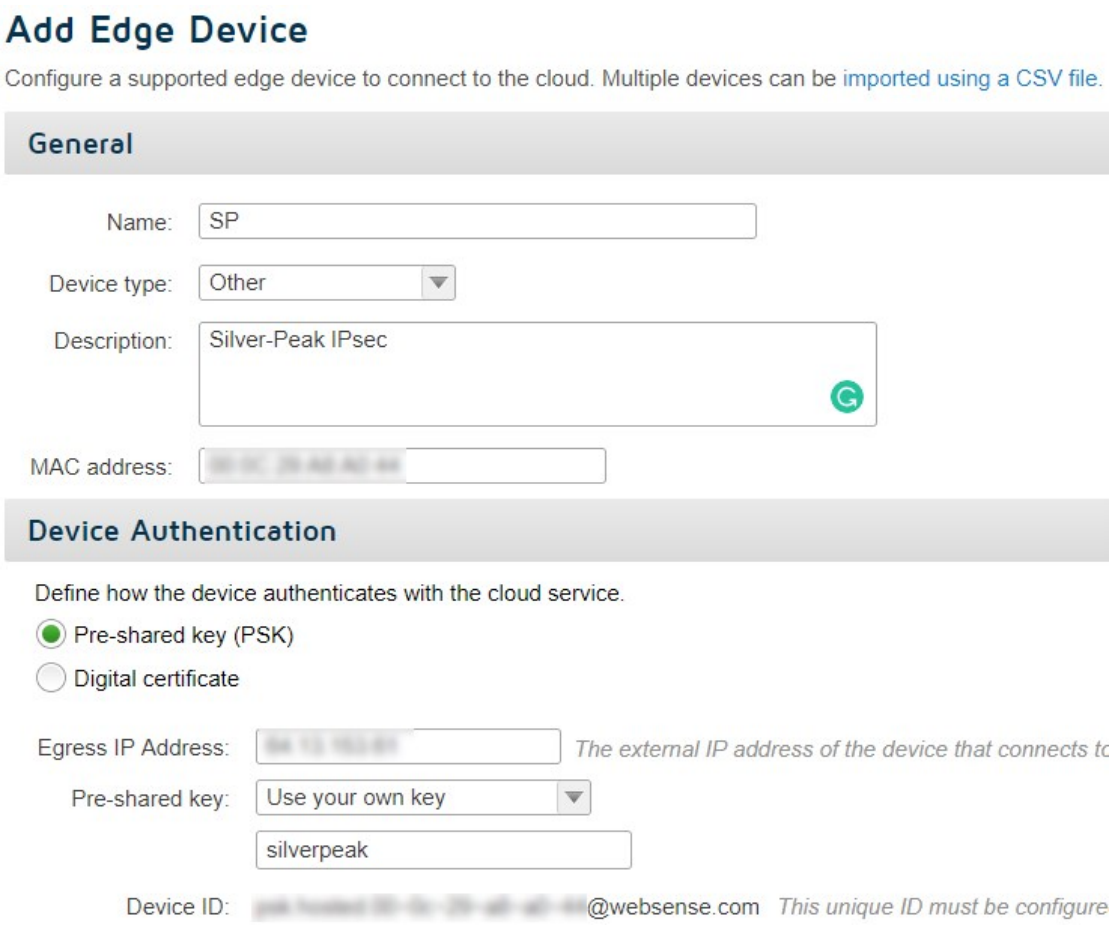

Figure 2: Configure the edge device.

Set up Silver Peak EdgeConnect

Set up IPsec tunneling to connect to the edge device that you added in Forcepoint.

Configure IPsec tunnels

Create an IPsec VPN tunnel to the primary Web Security Service. Complete the following steps to create each tunnel.

1. Sign in to Orchestrator.
2. From the home screen, select **Configuration** >**Tunnels**.

   The Tunnels screen opens.
3. Click the pencil icon next to an EdgeConnect appliance to edit the appliance tunnel.
4. Select the **Passthrough** tab, then select **Add Tunnel**.

   The Add Passthrough Tunnel screen opens.
5. Select the **General** tab.
6. Fill in the following fields.

General	Task
Alias	Enter a name for the alias, such as **Forcepoint**.
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 device IP located in the cloud. Use the EdgeConnect public IP as the local IP.
NAT	Select **none**,
Peer/Service	Select or type Forcepoint.
Auto Max BW Enabled	Select the check box.
Max BW Kbps	Leave this field blank.

7. Select the **IKE** tab.

8. Fill in the following fields.

IKE	Task
Pre-Shared Key	Enter the same pre-shared key that you entered in when added an edge device in Forcepoint.
Authentication Algorithm	Select **SHA1**.
Encryption Algorithm	Select **AES-128**.
Diffie-Hellman Group	Select **5**.
Lifetime	Enter **1440**.
Delay time	Enter a delay time, such as **300**.
Retry Count	Enter **5**.
IKE Identifier	Select **USER_FQDN**. Enter the device ID from the edge device in Forcepoint.
Phase 1 Mode	Select **Main**.

9. Select the **IPsec** tab.

10. Fill in the following fields.

IPsec	Task
Authentication Algorithm	Select **SHA1** or higher.
Encryption Algorithm	Select **AES-128** or higher.
Enable IPsec Anti-replay Window	Select the check box.
Lifetime	In the **Mins** field, enter **480**. In the **Megabytes** field, enter **0**.
Perfect Forward Secrecy Group	Select **disable**.

11. Select **Save**.

    You created an IPsec VPN tunnel to the Forcepoint edge device.

Configure Business Intent Overlay policies

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

1. In Orchestrator, select **Business Intent Overlay**.
2. In the **Internet Traffic** section, select the pencil icon next to **Policies**.
3. In the **Service Name** field, type a name for the Forcepoint peer/service.
4. Select **Add**.
5. Click **Close** to return to the previous screen.
6. From the **Business Intent Overlay** screen, move the Forcepoint service to the **Preferred Policy Order** section.
7. In the **Preferred Policy Order** section, move the Forcepoint service above the other policies.

   NOTE By moving the Forcepoint service to the top of the list, all internet-bound traffic passes through the Forcepoint IPsec tunnel. If the tunnel is down, traffic backhauls via the overlay.

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

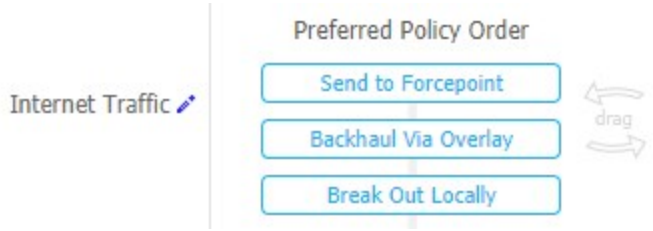

Figure 3: Preferred policy order.

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