# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Copyright and Trademarks</td>
<td>3</td>
</tr>
<tr>
<td>Support</td>
<td>4</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>5</td>
</tr>
<tr>
<td>About</td>
<td>6</td>
</tr>
<tr>
<td>Set up Forcepoint</td>
<td>7</td>
</tr>
<tr>
<td>Set up Silver Peak EdgeConnect</td>
<td>10</td>
</tr>
</tbody>
</table>

### Set up Forcepoint
- Prerequisites                               | 7    |
- Add an edge device in Forcepoint             | 8    |

### Set up Silver Peak EdgeConnect
- Configure IPsec tunnels                      | 10   |
- Configure Business Intent Overlay policies   | 12   |
Copyright and Trademarks

Silver Peak EdgeConnect and Forcepoint Web Security Cloud Integration Guide

Date: November 2018

Copyright © 2018 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 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](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.

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.
Add Edge Device

Configure a supported edge device to connect to the cloud. Multiple devices can be imported using a CSV file.

**General**

- **Name:** SP
- **Device type:** Other
- **Description:** Silver-Peak IPsec
- **MAC address:**

**Device Authentication**

Define how the device authenticates with the cloud service.

- **Pre-shared key (PSK)**
- **Digital certificate**

- **Egress IP Address:** The external IP address of the device that connects to.
- **Pre-shared key:** Use your own key
  - **silverpeak**
- **Device ID:** This unique ID must be configure

*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.

<table>
<thead>
<tr>
<th>Task</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Enter a name for the alias, such as Forcepoint.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select IPsec.</td>
</tr>
<tr>
<td>Admin</td>
<td>Select up.</td>
</tr>
<tr>
<td>Local IP</td>
<td>Enter your appliance IP, which can be private if the appliance is behind a NAT or public.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>Enter the remote device IP located in the cloud. Use the EdgeConnect public IP as the local IP.</td>
</tr>
<tr>
<td>NAT</td>
<td>Select none.</td>
</tr>
<tr>
<td>Peer/Service</td>
<td>Select or type Forcepoint.</td>
</tr>
<tr>
<td>Auto Max BW Enabled</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>Max BW Kbps</td>
<td>Leave this field blank.</td>
</tr>
</tbody>
</table>
7. Select the IKE tab.
8. Fill in the following fields.

<table>
<thead>
<tr>
<th>IKE</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-Shared Key</strong></td>
<td>Enter the same pre-shared key that you entered in when added an edge device in Forcepoint.</td>
</tr>
<tr>
<td><strong>Authentication Algorithm</strong></td>
<td>Select SHA1.</td>
</tr>
<tr>
<td><strong>Encryption Algorithm</strong></td>
<td>Select AES-128.</td>
</tr>
<tr>
<td><strong>Diffie-Hellman Group</strong></td>
<td>Select 5.</td>
</tr>
<tr>
<td><strong>Lifetime</strong></td>
<td>Enter 1440.</td>
</tr>
<tr>
<td><strong>Delay time</strong></td>
<td>Enter a delay time, such as 300.</td>
</tr>
<tr>
<td><strong>Retry Count</strong></td>
<td>Enter 5.</td>
</tr>
<tr>
<td><strong>IKE Identifier</strong></td>
<td>Select USER_FQDN.</td>
</tr>
<tr>
<td></td>
<td>Enter the device ID from the edge device in Forcepoint.</td>
</tr>
</tbody>
</table>

| **Phase 1 Mode**         | Select Main.                                                        |

9. Select the IPsec tab.
10. Fill in the following fields.

<table>
<thead>
<tr>
<th>IPsec Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Algorithm</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
</tr>
<tr>
<td>Enable IPsec Anti-replay Window</td>
</tr>
<tr>
<td>Lifetime</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Perfect Forward Secrecy Group</td>
</tr>
</tbody>
</table>

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.

![Preferred Policy Order](image)

*Figure 3: Preferred policy order.*

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