Silver Peak

EdgeConnect and Symantec Web Security Service

Integration Guide

201413-001 Rev A

Table of Contents

Copyright and Trademarks

Silver Peak EdgeConnect and Symantec Integration Guide

Date: August 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 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 two Symantec Web Security Services (WSS) to enable advanced security inspection.

Service chain an EdgeConnect appliance with WSS by setting up interoperable site-to-site IPsec tunnels between the appliance and WSS. 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 two devices.

Set up Symantec Web Security Service

Prerequisites

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

- ☐ Find the IP address for your gateway as the destination for your primary IPsec VPN tunnel and another as the destination for your secondary IPsec VPN tunnel.
- ☐ Find the public IP address of your gateway to the Symantec Web Security Service.

Find the public IP address of your gateway

For your gateway, select an IP address as the destination of your primary IPsec VPN tunnel and another IP as the destination for your secondary IPsec VPN tunnel. Use these IP addresses when creating tunnels to Symantec.

1. Go to the Reference: Web Security Service Data Center Ingress IPs section of the Symantec website.
2. Find your geographical location and IP addresses. Choose one IP as the primary and another as a backup.

   You are now ready to set up the Symantec Web Security Service (WSS).

Set up IPsec tunnels in Symantec

Set up an IPsec tunnel to a Symantec Web Security Service by adding VPN credentials and link the credentials to a location.

1. Sign in to the Symantec Web Security Service website.

   The home screen opens.

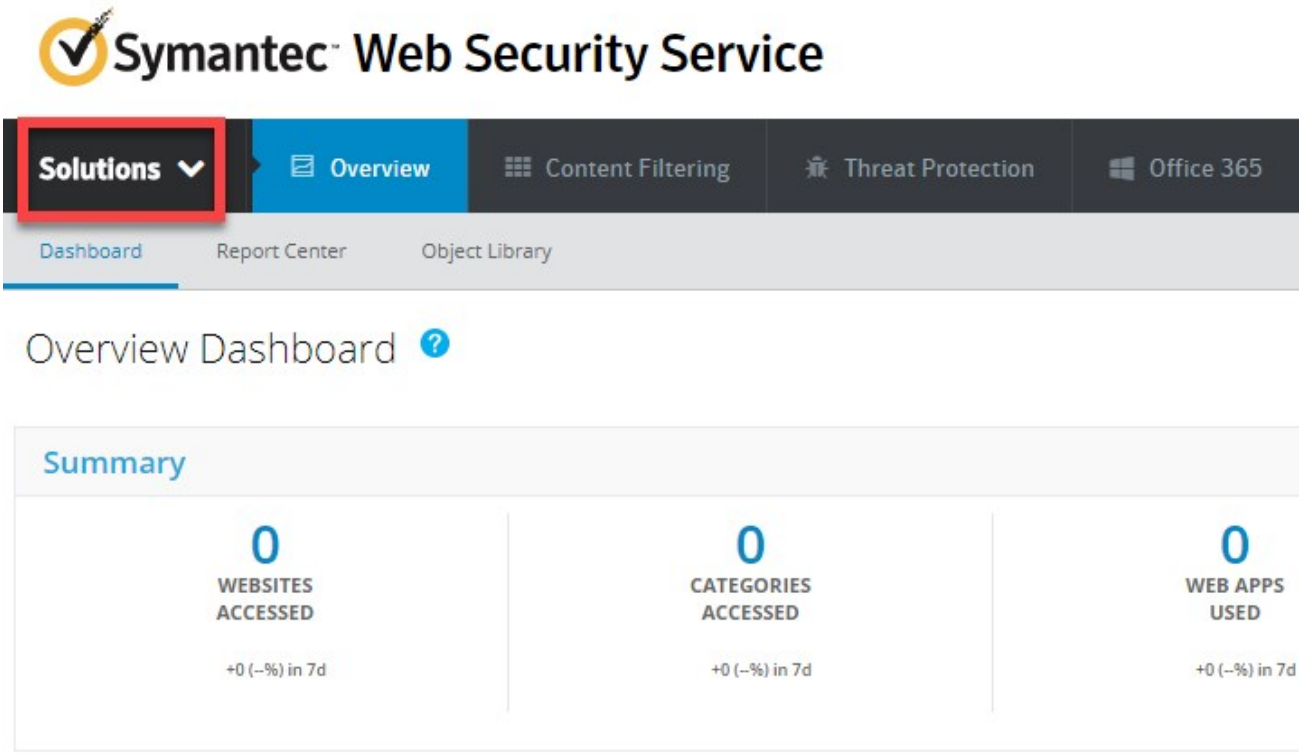

   Figure 1: Symantec Web Security Service home screen.

2. From the **Solutions** drop down list, select **Service**.

   The Locations screen opens.

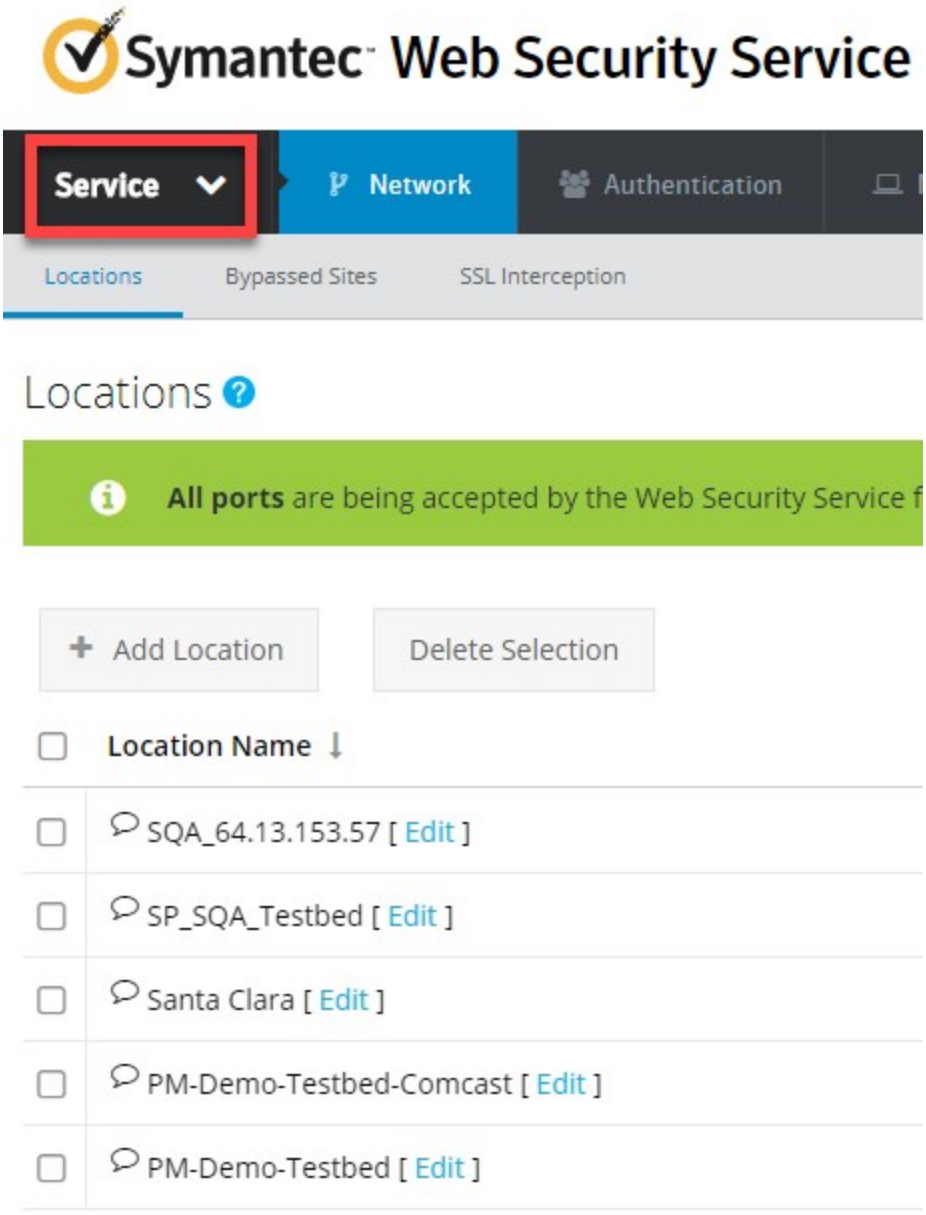

Figure 2: Symantec Web Security Service locations.

3. Select **+ Add Locations**.

   The Add Location screen opens.

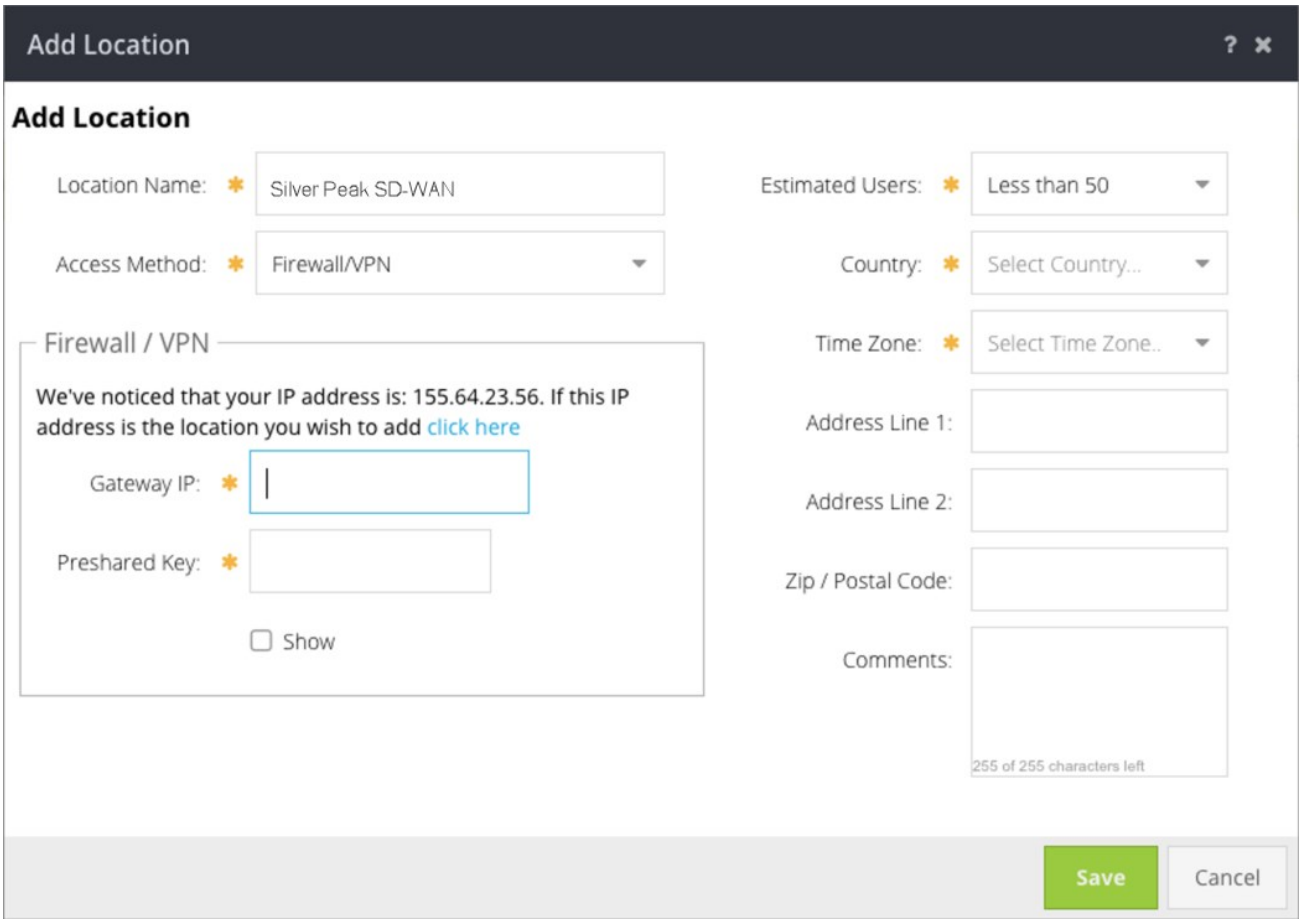

Figure 3: Add locations.

4. Add a new location for each service data center that you want to onboard.

   NOTE The configuration uses IPSec v1 and PSK to establish a tunnel.

Add location	Task
Location Name	Enter a descriptive name for the service data center location.
Access Method	From the list, select **Firewall/VPN** .
Estimated Users	From the list, select the estimated number of users, taking into account the number of users from all remote locations that might use this service center.
Country	Select the country of the service data center.
Time Zone	Select the time zone of the service data center.
Gateway IP	Enter the public IP of the third party IPsec endpoint in the service center data center.

Preshared Key	Enter the pre-shared key used for this service center data center.
Comments	Enter an optional descriptive comment.

NOTE The configuration uses IPsec version 1 and PSK to establish tunnels.

5. Select **Save**.

   You can now create your IPSec tunnels in Silver Peak Orchestrator to Symantec Web Security Service.

Deployment scenarios with Silver Peak EdgeConnect

Silver Peak supports two ways to configure and deploy an EdgeConnect appliance with Symantec.

- Active-backup internet breakout
- Active-active internet breakout

NOTE Use Silver Peak EdgeConnect version 8.1.8.0 or later and Silver Peak Orchestrator version 8.4.0 or later.

Active-backup internet breakout

In this scenario, active-backup tunnels load-balance the traffic to Symantec Web Security Service.

Figure 4: Active-backup mode.

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** >**Tunnels**.

   The Tunnels screen opens.
3. Click the pencil icon to edit the 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.
Mode	Select **IPsec**. **IPsec UDP** is reserved for EdgeConnect-to-EdgeConnect tunnels.

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 WSS device IP located in the cloud. Use EdgeConnect's public IP as the local IP.
NAT	Select **none**.
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 when creating the VPN credential in Symantec Web Security Service.
Authentication Algorithm	Select **SHA1** or higher.
Encryption Algorithm	Select **AES-256**.
Diffie-Hellman Group	Select **14** or higher.
Lifetime	Enter **480**.
IKE Identifier	Select **IP ADDRESS**.
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-256**.
Lifetime	In the **Mins** field, enter **60**. In the **Megabytes** field, enter **0**.
Perfect Forward Secrecy Group	Select **14** or higher.

11. Select **Save**.

    You created an IPsec VPN tunnel to the primary Web Security Service.

Create a second 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. However, make sure the public IP address and service name of the secondary tunnel are different from the ones you used for the primary tunnel.

NOTE The algorithms and the pre-shared key must match the WSS. For example, if you select **SHA1** for IKE, the authentication algorithm in WSS should also be **SHA1**.

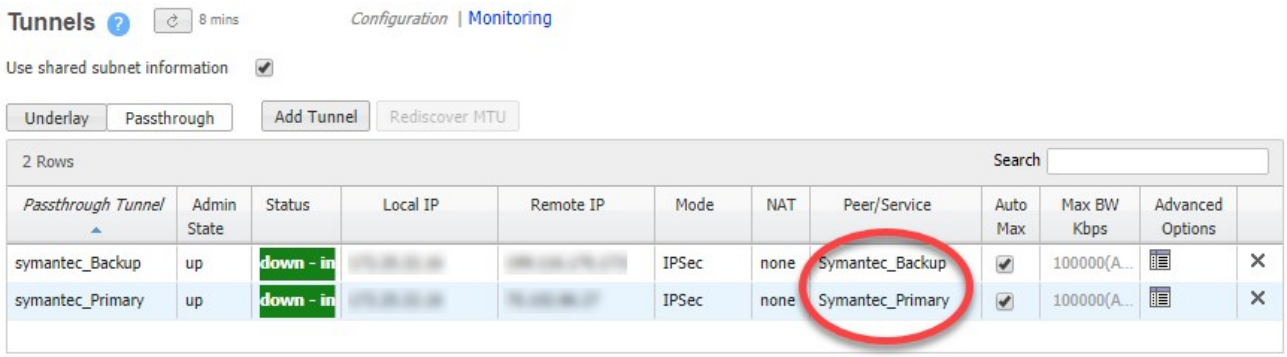

Figure 5: Silver Peak tunnel configuration with active-active mode.

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. Select **Policies**.
3. In the **Service Name** field, type a name for a peer/service. In this example, the first peer/service is **Symantec_Primary**.
4. Select **Add**.
5. In the **Service Name** field, type a name for a second peer/service. In this example, the second peer/service is **Symantec_Backup**.
6. Select **Add**.

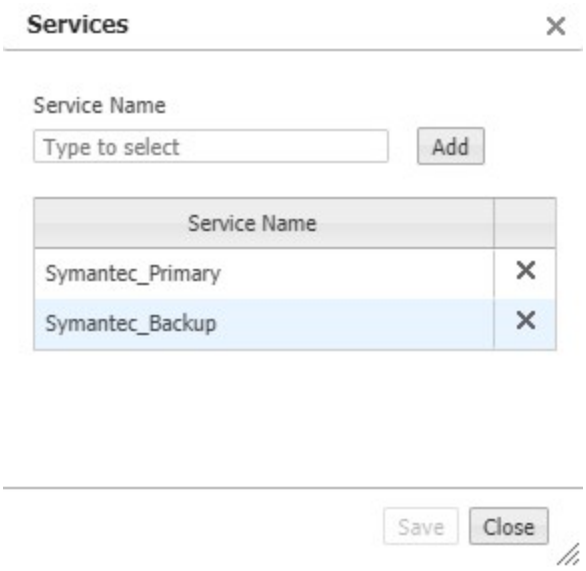

Figure 6: Services.

7. Click **Close** to return to the previous screen.
8. From the **Business Intent Overlay** screen, move the services to the **Preferred Policy Order** section.
9. In the **Preferred Policy Order** section, move the primary service above the secondary service.

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

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

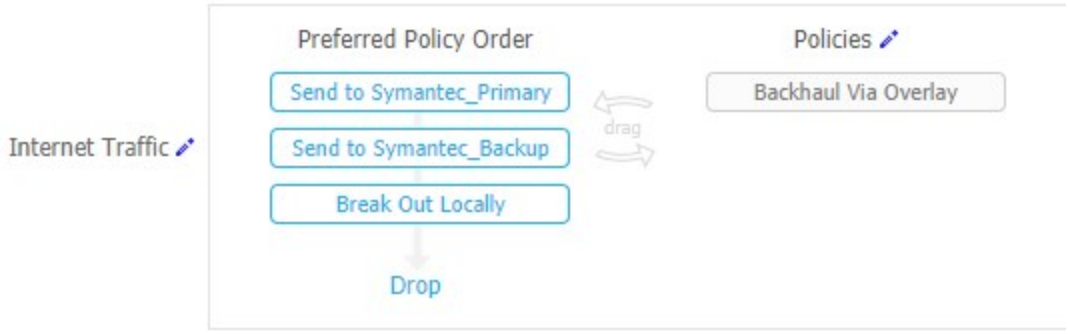

Figure 7: Preferred policy order.

You 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 Symantec Web Security Service.

Figure 8: Active-active mode.

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** >**Tunnels**.

   The Tunnels screen opens.
3. Click the pencil icon to edit the 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.
Mode	Select **IPsec**. **IPsec UDP** is reserved for EdgeConnect-to-EdgeConnect tunnels.

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 WSS device IP located in the cloud.
NAT	Select **none**.
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 when creating the VPN credential in Symantec Web Security Service.
Authentication Algorithm	Select **SHA1** or higher.
Encryption Algorithm	Select **AES-256**.
Diffie-Hellman Group	Select **14** or higher.
Lifetime	Enter **480**.
Dead Peer Detection	For **Delay time**, enter **300**. For **Retry Count**, enter **3**.
IKE Identifier	Leave this option blank.
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-256**.
Lifetime	In the **Mins** field, enter **60**. In the **Megabytes** field, enter **0**.
Perfect Forward Secrecy Group	Select **14** or higher.

Select **Save**.

You created an IPsec VPN tunnel to the primary Web Security Service.

Create a second 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. However, make sure the public IP address and service name of the secondary tunnel are different from the ones you used for the primary tunnel.

NOTE The algorithms and the pre-shared key must match the WSS. For example, if you select **SHA1** for IKE, the authentication algorithm in WSS should also be **SHA1**.

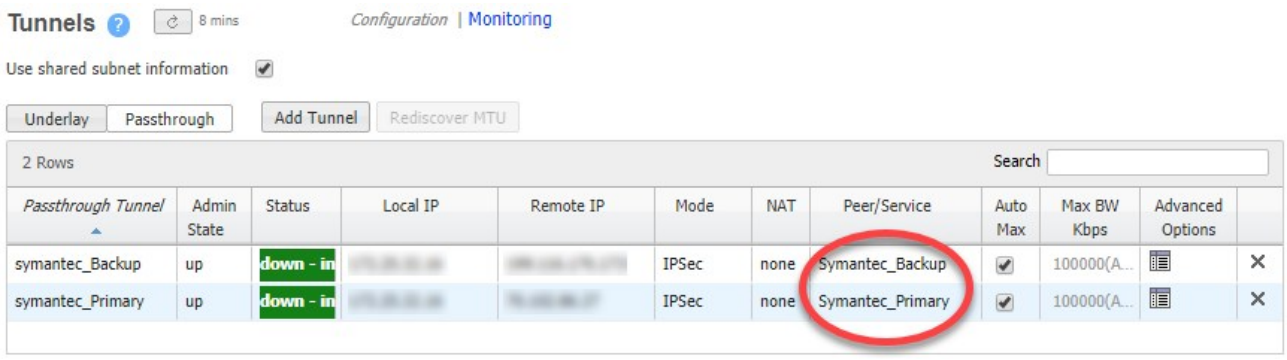

Figure 9: Silver Peak tunnel configuration with active-active mode.

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. Select **Policies**.
3. In the **Service Name** field, type a name for a peer/service. In this example, the first peer/service is **Symantec_Primary**.
4. Select **Add**.
5. In the **Service Name** field, type a name for a second peer/service. In this example, the second peer/service is **Symantec_Backup**.
6. Select **Add**.

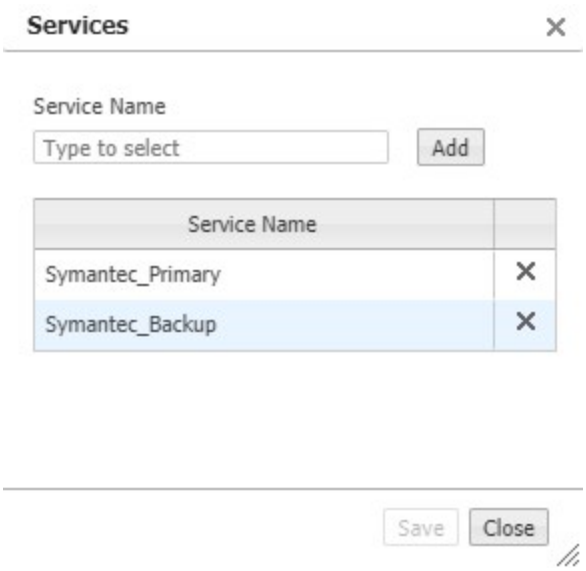

Figure 10: Services.

7. Click **Close** to return to the previous screen.
8. From the **Business Intent Overlay** screen, move the services to the **Preferred Policy Order** section.
9. In the **Preferred Policy Order** section, move the primary service above the secondary service.

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

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

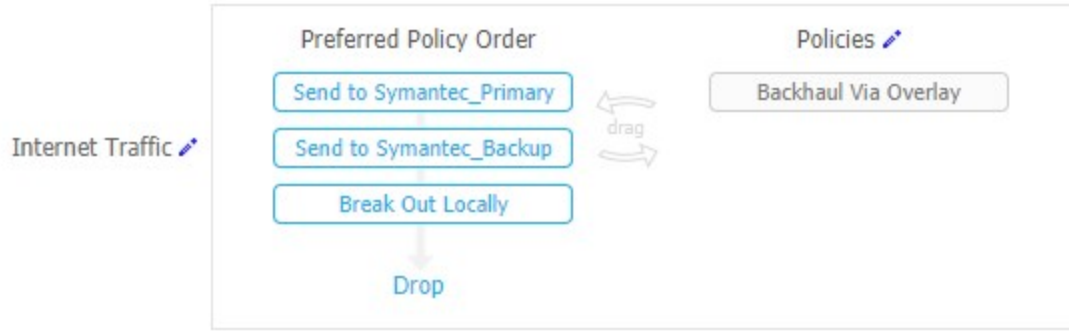

Figure 11: Preferred policy order.

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

Configure load balancing

Configure load balancing

To load balance the configuration, use the same peer/service name for both Symantec tunnels. As a result, EdgeConnect load balances the traffic between both tunnels per flow load balance.

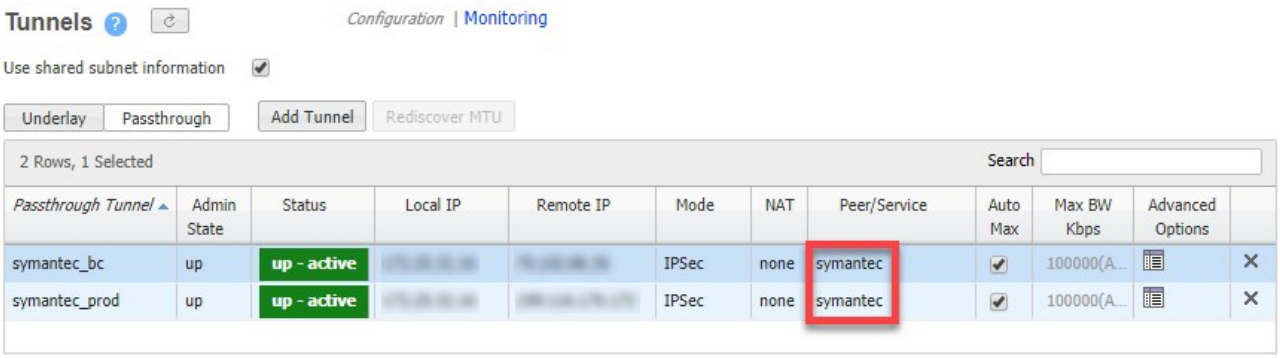

Figure 12: Load balanced tunnels.

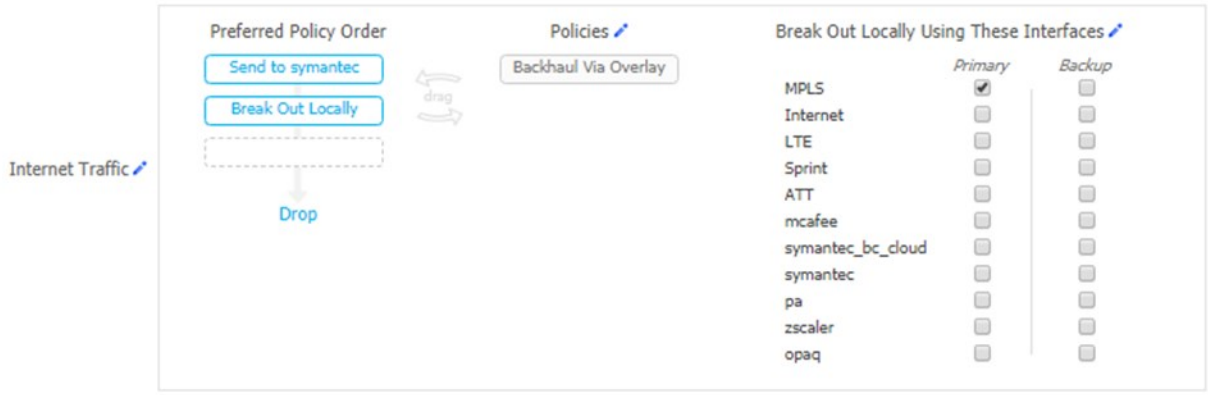

Figure 13: Preferred policy order for load-balanced tunnels.