Silver Peak

EdgeConnect and Check Point Network Security as a Service

Integration Guide

201487-001 Rev A
# Table of Contents

**Table of Contents** .......................................................... 2

**Copyright and Trademarks** ............................................... 3

**About this guide** .......................................................... 4
  What is Check Point Network Security as a Service? .................. 5
  Registering a new account ................................................ 6

**Creating a site at the Check Point Infinity portal** .................. 7
  Protecting sites using GRE tunnels ..................................... 7
  Configuring your SD-WAN router to route traffic through Check Point Network Security as a Service ............................................. 11

**Setting up Silver Peak EdgeConnect** .................................. 14
  Setting up a single GRE tunnel .......................................... 15
  Configuring a deployment profile ....................................... 15
  Configuring Business Intent Overlay policies .......................... 16
  Applying the overlay to the appliance .................................. 17
  Setting up pass-through tunnels ........................................ 18
  Checking your route policies ............................................ 19
  Monitoring the traffic flow .............................................. 19
  Setting up an active-active configuration .............................. 21
  Configuring a deployment profile ....................................... 21
  Configuring Business Intent Overlay policies ........................ 22
  Applying the overlay to the appliance .................................. 23
  Setting up pass-through tunnels ........................................ 24
  Checking your route policies ............................................ 25
  Confirming the flow behavior ........................................... 25
  Setting up an active-standby configuration ............................ 27
  Configuring a deployment profile ....................................... 27
  Configuring Business Intent Overlay policies ........................ 28
  Applying the overlay to the appliance .................................. 29
  Setting up pass-through tunnels ........................................ 30
  Checking your route policies ............................................ 31
  Monitoring the traffic flow .............................................. 31
  Confirming the flow behavior ........................................... 32

**Monitoring cybersecurity events using the Check Point Infinity portal** .................................................. 33

**Support** ......................................................................... 36

**Related Documentation** .................................................. 37
Copyright and Trademarks

Silver Peak EdgeConnect and Check Point Network Security as a Service Integration Guide

Date: March 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 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

Copyright © 2019 by Silver Peak Systems, Inc. All rights reserved
About this guide

This guide describes how to set up GRE tunnels and service chain traffic from a Silver Peak® EdgeConnect™ appliance to the Check Point Network Security as a Service by completing four major steps.

1. Create a site using the Check Point Infinity portal.
2. Add the Check Point tunnels to the Silver Peak Business Intent Overlay policy.
3. Monitor end-to-end traffic using Silver Peak flow monitoring.
4. Monitor cybersecurity events using the Check Point Infinity portal.
What is Check Point Network Security as a Service?

Check Point Network Security as a Service is a cloud security platform that provides Check Point threat prevention and access control for branch offices. You can connect your existing routing equipment or SD-WAN device to the Network Security as a Service without additional dedicated hardware.

Network Security as a Service is a full software-as-a-service model that eliminates the need for maintenance from the user.

The Check Point security product line includes the following features.

- Prevent known attacks using reputation services, signatures, and bot communication prevention.
- Prevent unknown attacks using cloud-based sandboxing.
- An access control policy that includes content awareness, HTTPS inspection, and application control.
- A web-based management system for security events and log monitoring, as well as policy and site configuration.
Registering a new account

If you don't have an account to access the Check Point Infinity portal, you can register for one at https://portal.checkpoint.com/register/cloudguardnsaas. Follow the steps on the screen to complete your registration.

**NOTE** On the main screen, make sure Network Security As A Service displays on the screen and the NETWORK icon is highlighted in pink. This indicates that you're creating the correct Check Point account.

**NOTE** Using Check Point Network Security as a Service depends on your purchased software license. For more information about licensing, contact your Check Point sales representative or check for updates on the Check Point user community page.

![Create Account Form]

*Figure 1: Registering a new account for Network Security as a Service.*
Creating a site at the Check Point Infinity portal

Protecting sites using GRE tunnels

Complete the followings steps.

   The NETWORK SECURITY AS A SERVICE screen opens.
   **NOTE** If you don’t see the correct screen, select the application switcher icon at the top-left corner, then select **Network Security as a Service**.

2. From the left side of the screen, select **SITES**.
   The Sites screen opens.
Figure 3: Creating a Check Point site.

3. Select the + button to create a new site.

   The CREATE NEW SITE screen opens.

   A site represents your branch office that uses a Silver Peak EdgeConnect appliance.

4. In the Site Name field, enter a name for the site location.

5. In the Location of the cloud service field, select a location that is near your site.

   Check Point Network Security as a Service inspects traffic from your branch office to the internet with a cloud service that’s in one of these locations. To ensure best performance, select the location of the cloud service that is closest to the location of your site. For some countries, such as those in South America or the Middle East, the best choice for the location of the cloud service might be a strong cross-country internet link.

6. In the Comments field, enter an optional description of the site.

7. Select Next to set up router details.
8. From the **Tunnel Type** list, select a tunnel type setting. Because this guide explains how to protect sites with GRE tunnels, select **GRE**.

9. In the **External IP** field, enter the IP address of your branch office site. This IP address must be static and accessible from the internet.

![Figure 4: Configuring the router details.](image)

10. Select **Next** to set up internal subnets.

11. From the Internal Subnets screen, enter the IP addresses and subnets of your internal networks in the branch office site.

    Check Point Network Security as a Service applies the cybersecurity features on any traffic coming from these network addresses.
Figure 5: Configuring the site internal subnets.

12. Select **Next** to confirm that Check Point is creating the site.

13. Select **Finish And Create Site**.

    Check Point might take a few minutes to create the site.
**Figure 6: Confirming the site creation.**

Configuring your SD-WAN router to route traffic through Check Point Network Security as a Service

Complete the following steps.

1. From the card that represents your site, select the menu icon represented by three dots.
2. Select **View Instructions**.

![View Instructions](image)

*Figure 7: Viewing the site instructions.*

3. View the tunnel addresses, the tunnel failover functionality, and the traffic routes by viewing the instructions.

The instructions contain the following.

- The IP address and destinations for each of the two GRE tunnels.
- The fail over or fail open options for the tunnels.
- The access routes to route traffic from the internal networks to the Check Point service. The routes and networks are protected by Check Point Network Security as a Service.
Figure 8: Check Point sites.
Setting up Silver Peak EdgeConnect

To secure internet traffic and for direct internet breakout from the branch, Silver Peak supports internet pass-through tunnels to Check Point Network Security as a Service. You can set up EdgeConnect appliances with the following use cases.

- Configure EdgeConnect with a single GRE tunnel.
- Configure EdgeConnect with a two tunnel active-active setup.
- Configure EdgeConnect with a two tunnel active-standby setup.

**NOTE** Use Silver Peak EdgeConnect version 8.1.9.0 or later and Silver Peak Orchestator version 8.5.0 or later.
Setting up a single GRE tunnel

This section describes how to set up a single GRE tunnel to send traffic to and from Check Point.

Configuring a deployment profile

Use deployment profiles to standardize your deployments, configuring the LAN interfaces and WAN interfaces of your GRE tunnel.

1. In the Orchestrator main screen, right click the EdgeConnect appliance that you want to add GRE tunnels.
2. Select Deployment.
   The Deployment screen opens.
3. In the Deployment screen, create your LAN interfaces and WAN interfaces. In this example, the deployment profile has lan0, lan1, wan0, and wan1.
4. From the FW Mode list, select your preferred firewall mode.
5. Set the bandwidth and next hop IP addresses.
6. Select Apply.

![Deployment Screen](image)

Figure 9: Logical deployment of a single GRE tunnel to Check Point.
Configuring Business Intent Overlay policies

A business intent overlay (BIO) specifies how traffic with particular characteristics are handled within the network. For GRE tunnels to Check Point, this example uses an overlay called **GRE** with an overlay ACL called **InternetTraffic** that defines the web traffic.

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

1. In the Orchestrator main screen, select **Business Intent Overlay**.
   
   The Business Intent Overlay screen opens.

2. From the **Overlays** list, choose **GRE** or the overlay of your choice.

3. In the **Internet Traffic** section, select the pencil icon next to **Policies**.

4. In the **Service Name** field, add a new service object that represents the Check Point peer/service. Enter a name that describes the Check Point service such as "Check Point Cloud."

5. Select **Add**.

6. Select **Close** to return to the previous screen.

7. From the Business Intent Overlay screen, move the Check Point service to the **Preferred Policy Order** section.

8. In the **Preferred Policy Order** section, move the Check Point service above the other policies.

   **NOTE** By moving the Check Point service to the top of the list, all internet-bound traffic passes through the Check Point GRE tunnel. If the tunnel is down, the traffic backhauls by using the overlay.
9. Select **Save all** to apply all changes.

![Business Intent Overlays](image.png)

**Figure 10: Business Intent Overlays for internet traffic.**

You configured business intent overlay policies that point to the GRE tunnel.

### Applying the overlay to the appliance

For the BIO to take effect, apply the overlay to the appliance.

1. In the left tree section, select the appliances to apply the overlay.
2. Select the **Add** check box for the GRE overlay.
3. Select **Apply**.
Figure 11: Applying the overlay.

Setting up pass-through tunnels

Create pass-through tunnels to service chain traffic to and from Silver Peak and Check Point.

1. In the Orchestrator main screen, select **Configuration > Tunnels**.
   The Tunnels screen opens.
2. Select the **Passthrough** tab.
3. Select the pencil icon next to the appliance name to edit the appliance tunnel.
   A new screen opens.
4. Select the **Passthrough** tab.
5. Select **Add Tunnel**.
6. In the **Alias** field, enter a name for the pass-through tunnel.
7. From the **Mode** list, select **GRE**.
8. From the **Admin** list, select **up**.
9. In the **Local IP** field, enter the IP address of the Silver Peak EdgeConnect appliance.
10. In the **Remote IP** field, enter the IP address of the Check Point tunnel displayed in the Check Point Infinity portal under Site Instructions.
11. From the **NAT** list, select **none**.
12. In the **Peer/Service** field, enter the name of the service that you created in the Business Intent Overlay.
13. For **Auto Max BW Enabled**, select the check box.
14. Select **Save**.
Checking your route policies

A BIO automates the creation of route policies, and generally determines to which destination a packet is routed. Route policy settings are used for exceptions to the BIO configuration.

1. In the Orchestrator main screen, select **Configuration > Route Policies**.
2. View your route policy to make sure your tunnels are set up correctly.

**Figure 13: Route policies.**

Monitoring the traffic flow

After you set up GRE tunnels, examine the traffic behavior.

1. In the Orchestrator main screen, select **Monitoring > Active & Recent Flows**.
2. Monitor the traffic flows in the flows table.
Figure 14: Monitoring flows.
Setting up an active-active configuration

This section describes how to set up a two tunnel active-active configuration to send traffic to and from Check Point.

Configuring a deployment profile

Use deployment profiles to standardize your deployments, configuring the LAN interfaces and WAN interfaces of your GRE tunnels.

1. In the Orchestrator main screen, right click the EdgeConnect appliance that you want to add GRE tunnels.
2. Select Deployment.
   The Deployment screen opens.
3. In the Deployment screen, create your LAN interfaces and WAN interfaces. In this example, the deployment profile has lan0, lan1, wan0, and wan1.
4. From the FW Mode list, select your preferred firewall mode.
5. Set the bandwidth and next hop IP addresses.
6. Select Apply.

![Deployment](image)

Figure 15: Logical deployment of two GRE tunnels to Check Point.
Configuring Business Intent Overlay policies

A business intent overlay (BIO) specifies how traffic with particular characteristics are handled within the network. In an active-active configuration, create a single service that points to the two Check Point GRE tunnels in the BIO screen.

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

1. In the Orchestrator main screen, select Business Intent Overlay.
   The Business Intent Overlay screen opens.
2. From the Overlays list, choose GRE or the overlay of your choice.
3. In the Internet Traffic section, select the pencil icon next to Policies.
4. In the Service Name field, add a new service object that represents the Check Point peer/service. Enter a name that describes the Check Point service such as "Check Point Cloud."
5. Select Add.
6. Select Close to return to the previous screen.
7. From the Business Intent Overlay screen, move the Check Point service to the Preferred Policy Order section.
8. In the Preferred Policy Order section, move the Check Point service above the other policies.

   **NOTE** By moving the Check Point service to the top of the list, all internet-bound traffic passes through the Check Point GRE tunnel. If the tunnel is down, the traffic backhauls by using the overlay.
9. Select **Save all** to apply all changes.

Figure 16: Business Intent Overlays for internet traffic.

You configured business intent overlay policies that point to the GRE tunnel.

**Applying the overlay to the appliance**

For the BIO to take effect, apply the overlay to the appliance.

1. In the left tree section, select the appliances to apply the overlay.
2. Select the **Add** check box for the GRE overlay.
3. Select **Apply**.
Figure 17: Applying the overlay.

Setting up pass-through tunnels

Create two pass-through tunnels to service chain traffic to and from Silver Peak and Check Point.

1. In the Orchestrator main screen, select Configuration > Tunnels.
   The Tunnels screen opens.
2. Select the Passthrough tab.
3. Select the pencil icon next to the appliance name to edit the appliance tunnel.
   A new screen opens.
4. Select the Passthrough tab.
5. Select Add Tunnel.
6. In the Alias field, enter a name for the pass-through tunnel, such as to_Checkpoint.
7. From the Mode list, select GRE.
8. From the Admin list, select up.
9. In the Local IP field, enter the IP address of the Silver Peak EdgeConnect appliance.
10. In the Remote IP field, enter the IP address of the Check Point tunnel displayed in the Check Point Infinity portal under Site Instructions.
11. From the NAT list, select none.
12. In the Peer/Service field, enter the name of the service that you created in the Business Intent Overlay.
13. For Auto Max BW Enabled, select the check box.
14. Select Save.
15. Create a second tunnel by repeating steps 5 through 14. Give the second tunnel an alias name, such as to_Checkpoint_2.

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>up</th>
<th>up_active</th>
<th>IP Address 1</th>
<th>IP Address 2</th>
<th>GRE</th>
<th>none</th>
<th>Checkpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>to_Checkpoint</td>
<td>up</td>
<td></td>
<td>172.17.33.54</td>
<td>172.17.33.14</td>
<td>GRE</td>
<td>none</td>
<td>Checkpoint</td>
</tr>
<tr>
<td>to_Checkpoint_2</td>
<td>up</td>
<td></td>
<td>172.17.33.88</td>
<td>172.17.33.22</td>
<td>GRE</td>
<td>none</td>
<td>Checkpoint</td>
</tr>
</tbody>
</table>

Figure 18: Passthrough tunnels.

Checking your route policies

A BIO automates the creation of route policies, and generally determines to which destination a packet is routed. Route policy settings are used for exceptions to the BIO configuration.

1. In the Orchestrator main screen, select **Configuration > Route Policies**.
2. View your route policy to make sure your tunnels are set up correctly.

Route Policies

<table>
<thead>
<tr>
<th>Rule</th>
<th>Appliance</th>
<th>Action</th>
<th>Priority</th>
<th>Match Criteria</th>
<th>Set Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>map</td>
<td>20000</td>
<td>ACL Overlay_GRE</td>
<td>Destination (Overlay) GRE Fallback drop</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>map</td>
<td>65000</td>
<td>Match Everything</td>
<td>Destination: auto optimized, path default, fallback pass-through</td>
</tr>
</tbody>
</table>

Figure 19: Route policies.

Confirming the flow behavior

Confirm that the flows are behaving correctly.

1. Send four flows to the internet. Confirm that two flows go through the first Check Point tunnel. Confirm that the other two flows go through the second Check Point tunnel.

Figure 20: Example of four traffic flows to the internet.
2. Turn off the active Check Point tunnel. Confirm that all traffic goes through the second Check Point.

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Application</th>
<th>Location</th>
<th>Address Map</th>
<th>SP1</th>
<th>Port1</th>
<th>SP2</th>
<th>Port2</th>
<th>DIP</th>
<th>Inbound Bytes</th>
<th>Outbound Bytes</th>
<th>Outbound Tunnel1</th>
<th>Outbound Tunnel2</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd-Phase-0</td>
<td>Soma</td>
<td>San Francisco</td>
<td>Amazon.com</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>to_Checkpoint_2</td>
<td>to_Checkpoint_2</td>
<td>32h</td>
</tr>
<tr>
<td>3rd-Phase-0</td>
<td>Soma</td>
<td>San Francisco</td>
<td>Verizon Inc.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>to_Checkpoint_2</td>
<td>to_Checkpoint_2</td>
<td>32h</td>
</tr>
<tr>
<td>3rd-Phase-0</td>
<td>Soma</td>
<td>San Francisco</td>
<td>Mountain View</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>to_Checkpoint_2</td>
<td>to_Checkpoint_2</td>
<td>32h</td>
</tr>
</tbody>
</table>

Figure 21: Example of the traffic behavior after turning off the first tunnel.

1. Turn on the active Check Point tunnel. Confirm that traffic load balances between the two tunnels.

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Application</th>
<th>Location</th>
<th>Address Map</th>
<th>SP1</th>
<th>Port1</th>
<th>SP2</th>
<th>Port2</th>
<th>DIP</th>
<th>Inbound Bytes</th>
<th>Outbound Bytes</th>
<th>Outbound Tunnel1</th>
<th>Outbound Tunnel2</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd-Phase-0</td>
<td>Soma</td>
<td>San Francisco</td>
<td>Amazon.com</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>to_Checkpoint_2</td>
<td>to_Checkpoint_2</td>
<td>32h</td>
</tr>
<tr>
<td>3rd-Phase-0</td>
<td>Soma</td>
<td>San Francisco</td>
<td>Verizon Inc.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>to_Checkpoint_2</td>
<td>to_Checkpoint_2</td>
<td>32h</td>
</tr>
<tr>
<td>3rd-Phase-0</td>
<td>Soma</td>
<td>San Francisco</td>
<td>Mountain View</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>to_Checkpoint_2</td>
<td>to_Checkpoint_2</td>
<td>32h</td>
</tr>
</tbody>
</table>

Figure 22: Example of the traffic behavior after turning on the first tunnel.
Setting up an active-standby configuration

This section describes how to set up a two tunnel active-standby configuration to send traffic to and from Check Point.

Configuring a deployment profile

Use deployment profiles to standardize your deployments, configuring the LAN interfaces and WAN interfaces of your GRE tunnels.

1. In the Orchestrator main screen, right click the EdgeConnect appliance that you want to add GRE tunnels.
2. Select Deployment.
   The Deployment screen opens.
3. In the Deployment screen, create your LAN interfaces and WAN interfaces. In this example, the deployment profile has lan0, lan1, wan0, and wan1.
4. From the FW Mode list, select your preferred firewall mode.
5. Set the bandwidth and next hop IP addresses.
6. Select Apply.

Figure 23: Logical deployment of two GRE tunnels to Check Point.
Configuring Business Intent Overlay policies

A business intent overlay (BIO) specifies how traffic with particular characteristics are handled within the network. In an active-active configuration, create two services that point to the Check Point GRE tunnels Checkpoint and Checkpoint_2 in the BIO screen.

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

1. In the Orchestrator main screen, select Business Intent Overlay.
The Business Intent Overlay screen opens.
2. From the Overlays list, choose GRE or the overlay of your choice.
3. In the Internet Traffic section, select the pencil icon next to Policies.
4. In the Service Name field, add a new service object that represents the Check Point peer/service. Enter a name that describes the Check Point service such as "Check Point Cloud."
5. Select Add.
6. Select Close to return to the previous screen.
7. From the Business Intent Overlay screen, move the Check Point service to the Preferred Policy Order section.
8. In the Preferred Policy Order section, add the Check Point services, one below the other.

**NOTE** By moving the Check Point service to the top of the list, all internet-bound traffic passes through the Check Point GRE tunnel. If the tunnel is down, the traffic backhauls by using the overlay.
9. Select Save all to apply all changes.

Figure 24: Business Intent Overlays for internet traffic.

You configured business intent overlay policies that point to the GRE tunnel.

Applying the overlay to the appliance

For the BIO to take effect, apply the overlay to the appliance.

1. In the left tree section, select the appliances to apply the overlay.
2. Select the Add check box for the GRE overlay.
3. Select Apply.
Figure 25: Applying the overlay.

Setting up pass-through tunnels

Create two pass-through tunnels to service chain traffic to and from Silver Peak and Check Point.

1. In the Orchestrator main screen, select **Configuration > Tunnels**.
   The Tunnels screen opens.
2. Select the **Passthrough** tab.
3. Select the pencil icon next to the appliance name to edit the appliance tunnel.
   A new screen opens.
4. Select the **Passthrough** tab.
5. Select **Add Tunnel**.
6. In the **Alias** field, enter a name for the pass-through tunnel, such as **to_Chaspoint**.
7. From the **Mode** list, select **GRE**.
8. From the **Admin** list, select **up**.
9. In the **Local IP** field, enter the IP address of the Silver Peak EdgeConnect appliance.
10. In the **Remote IP** field, enter the IP address of the Check Point tunnel displayed in the Check Point Infinity portal under Site Instructions.
11. From the **NAT** list, select **none**.
12. In the **Peer/Service** field, enter the name of the service that you created in the Business Intent Overlay.
13. For **Auto Max BW Enabled**, select the check box.
14. Select **Save**.
15. Create a second tunnel by repeating steps 5 through 14. Use the service name **Checkpoint_2** and the alias name **to_Checkpoint_2**.

![Figure 26: Passthrough tunnels.](image)

**Checking your route policies**

A BIO automates the creation of route policies, and generally determines to which destination a packet is routed. Route policy settings are used for exceptions to the BIO configuration.

1. In the Orchestrator main screen, select **Configuration > Route Policies**.
2. View your route policy to make sure your tunnels are set up correctly.

**Figure 27: Route policies.**

**Monitoring the traffic flow**

After you set up GRE tunnels, examine the traffic behavior.

1. In the Orchestrator main screen, select **Monitoring > Active & Recent Flows**.
2. Monitor the traffic flows in the flows table.

![Figure 28: Monitoring flows.](image)
Confirming the flow behavior

Confirm that the flows are behaving correctly.

1. Send four flows to the internet. Confirm that all flows go through the active Check Point tunnel.

```
<table>
<thead>
<tr>
<th>Host Name</th>
<th>Application</th>
<th>Location</th>
<th>Address Map</th>
<th>SP1</th>
<th>Port1</th>
<th>Port2</th>
<th>Detail</th>
<th>Inbound Bytes</th>
<th>Outbound Bytes</th>
<th>Outbound Tunnel</th>
<th>Inbound Tunnel</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>San</td>
<td>Francisco</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>San</td>
<td>Francisco</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
</tbody>
</table>
```

*Figure 29: Example of four traffic flows to the internet.*

2. Turn off the active Check Point tunnel. Confirm that all traffic goes through the standby tunnel.

```
<table>
<thead>
<tr>
<th>Host Name</th>
<th>Application</th>
<th>Location</th>
<th>Address Map</th>
<th>SP1</th>
<th>Port1</th>
<th>Port2</th>
<th>Detail</th>
<th>Inbound Bytes</th>
<th>Outbound Bytes</th>
<th>Outbound Tunnel</th>
<th>Inbound Tunnel</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>San</td>
<td>Francisco</td>
<td>6</td>
<td></td>
<td></td>
<td>1</td>
<td>25</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>San</td>
<td>Francisco</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>6</td>
<td></td>
<td></td>
<td>1</td>
<td>15</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
</tbody>
</table>
```

*Figure 30: Example of the traffic behavior after turning off the active tunnel.*

3. Turn on the active Check Point tunnel. Confirm that traffic goes through the active tunnel.

```
<table>
<thead>
<tr>
<th>Host Name</th>
<th>Application</th>
<th>Location</th>
<th>Address Map</th>
<th>SP1</th>
<th>Port1</th>
<th>Port2</th>
<th>Detail</th>
<th>Inbound Bytes</th>
<th>Outbound Bytes</th>
<th>Outbound Tunnel</th>
<th>Inbound Tunnel</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>25</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>Mountain</td>
<td>View</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>75</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
<tr>
<td>3rd_Plane</td>
<td>comp</td>
<td>San</td>
<td>Francisco</td>
<td>8</td>
<td></td>
<td></td>
<td>1</td>
<td>25</td>
<td>15</td>
<td>tc_Checkpoint</td>
<td>tc_Checkpoint</td>
<td>2h 16h</td>
</tr>
</tbody>
</table>
```

*Figure 31: Example of the traffic behavior after turning on the active tunnel.*
Monitoring cybersecurity events using the Check Point Infinity portal

Using the Check Point Infinity portal, you can monitor which attacks were prevented by the Check Point cybersecurity features.


The NETWORK SECURITY AS A SERVICE screen opens.

NOTE If you don’t see the correct screen, select the application switcher icon at the top-left corner, then select Network Security as a Service.

![Changing applications in the Check Point Infinity portal.](image)

*Figure 32: Changing applications in the Check Point Infinity portal.*
2. From the left side of the screen, select **LOGS**.

---

**Figure 33: Check Point Logs screen.**

3. Select the **Cyber Attack View** tab to view attacks that were prevented by Check Point.

4. Select the **Access Control** tab to view malicious applications that were prevented by Check Point, as well as the total consumed traffic and visibility of the applications that the end users accessed the most.

5. Select the **Application and URL Filtering** tab to generate a real-time report of your branch office cybersecurity status. You can export this report as a PDF file by selecting the menu at the top-right of the screen.

6. From the left side of the screen, select **POLICY** to view and change your security policy for access control, threat prevention, and HTTPS inspection.
Figure 34: Check Point Policy screen.

**WARNING**  The changes to the security policies are not applied until you select Install Policy.
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 Silver Peak user documentation is available at [https://www.silver-peak.com](https://www.silver-peak.com).