Zscaler-Silver Peak GRE Integration Guide: Manual Mode
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, please send an e-mail to techpubs@silver-peak.com.
- If you have comments or feedback about the interface, please send an e-mail to usability@silver-peak.com.

Silver Peak Access

Silver Peak Support Portal Login
https://www.silver-peak.com/support/customer-login

Silver Peak User Documentation
https://www.silver-peak.com/support/user-documentation

Additional Zscaler information:

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket
Copyright and Trademarks

Silver Peak Zscaler-Silver Peak GRE Integration Guide: Manual Mode

Date: October 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, Suite 100
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support
Contents

Support .......................................................................................................................... ii
Silver Peak Access ....................................................................................................... ii
Additional Zscaler information: .................................................................................. ii
Copyright and Trademarks ............................................................................................ i

About ............................................................................................................................. 1

Before you start .............................................................................................................. 2
Recommendation for GRE traffic originating point ..................................................... 2
Recommendations for number of tunnels ..................................................................... 2
Zscaler Features ............................................................................................................. 2

Use Cases ..................................................................................................................... 4
Use Case: Single ISP Internet Breakout ........................................................................ 5
  Step 1: Request tunnel destination ............................................................................. 5
  Step 2: Deployment .................................................................................................... 5
  Step 3: Setup Internet Breakout Tunnels ................................................................. 6
  Step 4: Business Intent overlays - for Internet Traffic ............................................. 6
  Step 5: Configure IP SLA .......................................................................................... 8
  Monitoring .................................................................................................................. 9
Use Case: Dual ISP Internet Breakout .......................................................................... 10
  Modes of operation ................................................................................................... 10
  Benefits ...................................................................................................................... 11
About

To secure Internet traffic and for direct Internet Breakout from the branch, Silver Peak EdgeConnect supports Internet Breakout tunnels to the Zscaler Secure Web Gateway. This guide is for configuring and monitoring Silver Peak EdgeConnect devices for using the Zscaler Secure Web Gateway. For information on Silver Peak deployment and configuration, see https://www.silver-peak.com/support/user-documentation and for Zscaler documentation, refer to https://support.zscaler.com/hc/en-us/?filter=documentation.

CAUTION: This guide represents the manual configuration of GRE tunnels from EdgeConnect to the Zscaler cloud. Refer to the Zscaler Internet Access section of the Orchestrator Operator's Guide if you want to automate this process.
Before you start

Recommendation for GRE traffic originating point

Zscaler recommends deploying multiple GRE tunnels originating from an internal router behind your edge firewall. Additional information can be found at https://support.zscaler.com/hc/en-us/articles/204928595-GRE-Deployment-Scenarios.

Recommendations for number of tunnels

Zscaler requires customers to build Primary and Backup tunnels from every Internet egress location.

Zscaler Features

Logs help verify that traffic sent to the Zscaler POPs are seen by Zscaler.

Figure 1. Example Zscaler logs

The Zscaler dashboard shows an overview of what is going on:
Figure 2. Example Zscaler dashboard

As an option, configure other Zscaler policies and services. These are outside the scope of this guide.
Use Cases

Use Case: Single ISP Internet Breakout
    Monitoring

Use Case: Dual ISP Internet Breakout
Use Case: Single ISP Internet Breakout

Step 1: Request tunnel destination

- Obtain a support ticket from Zscaler.

Zscaler requires a support ticket to receive the GRE tunnel configuration. Zscaler identifies the tunnel endpoints based on geolocation. You can request alternate locations at the point of contact with Support based on latency and the optimal network path.

Step 2: Deployment

**Figure 3. Logical Deployment of Single ISP Internet Breakout to Zscaler**

**Figure 4. Deployment**

- Within Orchestrator, choose stateful firewall and NAT.
- Optional. Add a new label called Zscaler.
Step 3: Setup Internet Breakout Tunnels

- Within Orchestrator, create Internet Breakout tunnels to the two Zscaler IP’s.

![Figure 5. Internet Breakout Tunnels](image)

**Figure 5. Internet Breakout Tunnels**

a. Choose the interface label for the Zscaler IP from the **Local IP** column. This is the interface used for Internet Breakout per the Deployment page.

b. From **Mode**, choose **gre_ip**.

   NAT is done at the Zscaler end, so no NAT is chosen.

c. From **Peer/Service**, choose Zscaler1 or Zscaler2.

Step 4: Business Intent overlays - for Internet Traffic

For internet breakout to Zscaler, this example uses an overlay called **InternetTraffic** with an ACL called **AllWeb** that defines Web traffic. Any ACL/LAN port/Overlay can be used for Internet Breakout.

- From the **Overlays** list, choose **InternetTraffic**, then apply the **Preferred Policy Order**—Zscaler1, followed by Zscaler2.

  If Zscaler POP1 is unavailable, traffic is sent to Zscaler POP2. Other default actions such as **Break Out locally** or **Backhaul Via Overlay** can also be chosen before the final implicit Drop.
Figure 6. Business Intent Overlays for Internet Traffic
**Figure 7. Business Intent Overlays with Zscaler as Service**

**Step 5: Configure IP SLA**

- From the Orchestrator menu, search for **IP SLA**.

  ICMP based IP SLA can be used to determine if tunnels Zscaler1 or Zscaler2 are down. This helps determine Policy order in the Business Intent Overlays.
Figure 8. IP SLA Configuration

Monitoring

Internet Breakout Tunnels and flows can be seen in the Monitoring and reporting pages, such as Tunnels, Active & Recent Flows, Real-time Charts, and Historical Charts.
Use Case: Dual ISP Internet Breakout

In this case, two tunnels are load-balanced to the same two Points of Presence in the Zscaler cloud. Eg: Comcast and AT&T uplinks to two Zscaler POPs.

![Logical Depiction of Dual ISP Internet Breakout](image)

**Figure 9. Logical Depiction of Dual ISP Internet Breakout**

![Configuring Dual ISP Internet Breakout Tunnels to Zscaler POPs](image)

**Figure 10. Configuring Dual ISP Internet Breakout Tunnels to Zscaler POPs**

**Modes of operation**

Normal mode is to load balance traffic on tunnels ‘to_Zscaler1’ and ‘lb_to_Zscaler1’ to POP1.

- If ISP1 fails, use ‘lb_to_Zscaler1’ to POP1.
- If ISP2 fails, use ‘to_Zscaler1’ to POP1.
- If POP1 fails, load balance using ‘lb_to_Zscaler2’ and ‘to_Zscaler2’.
- If POP2 fails, load balance using ‘lb_to_Zscaler1’ and ‘to_Zscaler1’.

![Diagram of Dual ISP Internet Breakout Deployment](image)

**Figure 11. Dual ISP Internet Breakout Deployment**

IP SLA monitoring must be updated for the new load balancing tunnels. However, the BIO remains the same as the Zscaler Services/POPs don’t change.

**Benefits**

We provide load balancing of Internet Breakout traffic to Zscaler and multiple levels of redundancy when Zscaler POPs fail or when ISPs fail.