

Silver Peak

# Zscaler Deployment Guide

Revised June 23, 2017

BEST PRACTICES FOR DEPLOYING ZSCALER SERVICE CHAINING WITH  
SILVER PEAK EDGECONNECT

# Copyright and Trademarks

Silver Peak Zscaler Deployment Guide Best Practices

Date: January 2017

Copyright © 2017 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 Peak Silver 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>

## 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](http://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](mailto:techpubs@silver-peak.com).
- If you have comments or feedback about the interface, please send an e-mail to [usability@silver-peak.com](mailto: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>

# Contents

<b>Copyright and Trademarks .....</b>	<b>2</b>
<b>Support.....</b>	<b>4</b>
Silver Peak Access .....	4
Additional Zscaler information: .....	5
<b>Introduction .....</b>	<b>1</b>
<b>Before you start .....</b>	<b>2</b>
Recommendation for GRE traffic originating point .....	2
Recommendations for number of tunnels.....	2
Some Zscaler Features.....	2
<b>Use Case: Single ISP Internet Breakout.....</b>	<b>4</b>
Step 1: Request tunnel destination .....	4
Step 2: Deployment .....	4
Step 3: Setup Internet Breakout Tunnels .....	5
Step 4: Business Intent overlays – for Internet Traffic ...	5
Step 5: Configure IP SLA.....	7
<b>Monitoring .....</b>	<b>8</b>
<b>Use Case: Dual ISP Internet Breakout.....</b>	<b>9</b>
Modes of operation .....	9
Benefits.....	10
<b>Use Case: Backhauled Internet Breakout .....</b>	<b>11</b>

# Introduction

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>.

# Before you start

## Recommendation for GRE traffic originating point

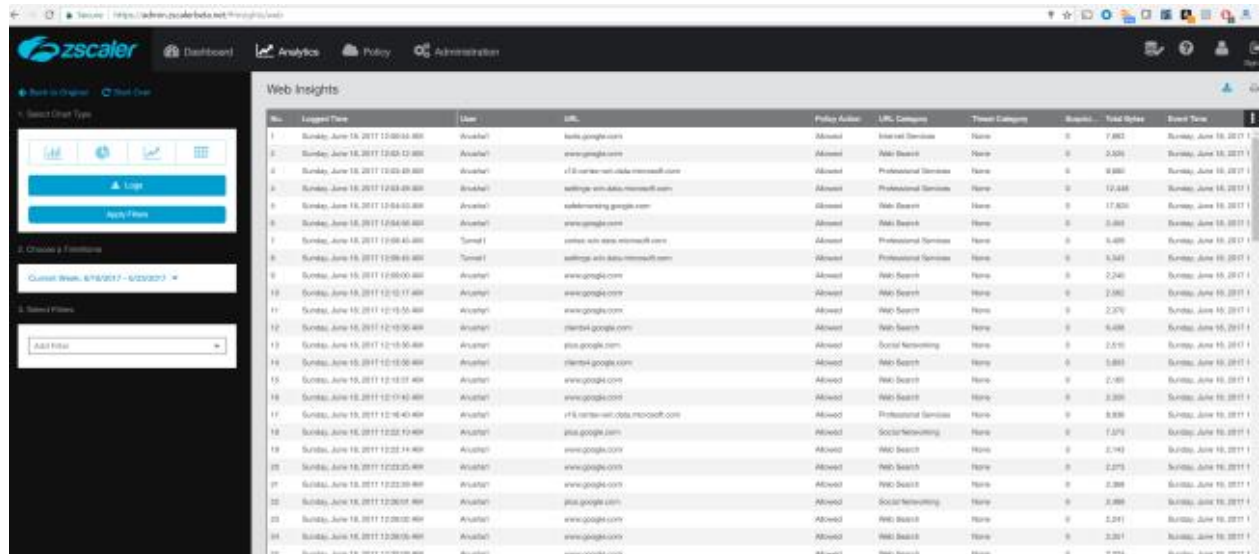
Zscaler recommends deploying multiple GRE tunnels originating from an internal router behind your edge firewall. Additional information can be found at <https://support.zscaler.com/hc/en-us/articles/204928595-GRE-Deployment-Scenarios>

## Recommendations for number of tunnels

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

## Some Zscaler Features

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

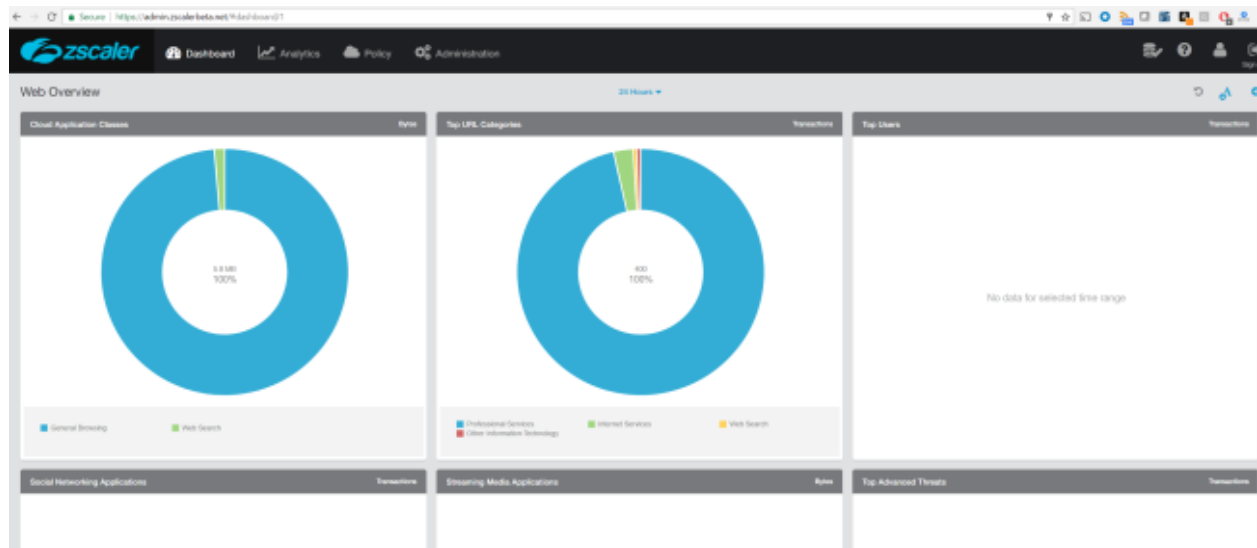


No.	Loggen Time	User	URL	Policy Action	URL Category	Threat Category	Block...	Total Bytes	Event Time
1	Sunday, June 18, 2017 12:00:00.000	Anonymous	beta.google.com	Allowed	Internet Services	None	0	7,882	Sunday, June 18, 2017 12:00:00.000
2	Sunday, June 18, 2017 12:00:12.000	Anonymous	www.google.com	Allowed	Web Search	None	0	5,526	Sunday, June 18, 2017 12:00:12.000
3	Sunday, June 18, 2017 12:00:20.000	Anonymous	v18-metastatic-beta-microsoft.com	Allowed	Professional Services	None	0	9,880	Sunday, June 18, 2017 12:00:20.000
4	Sunday, June 18, 2017 12:00:28.000	Anonymous	settings-wws-beta-microsoft.com	Allowed	Professional Services	None	0	12,448	Sunday, June 18, 2017 12:00:28.000
5	Sunday, June 18, 2017 12:00:36.000	Anonymous	ads-adserving.google.com	Allowed	Web Search	None	0	17,826	Sunday, June 18, 2017 12:00:36.000
6	Sunday, June 18, 2017 12:00:44.000	Anonymous	www.google.com	Allowed	Web Search	None	0	3,400	Sunday, June 18, 2017 12:00:44.000
7	Sunday, June 18, 2017 12:00:52.000	Torrel I	www.win-wws-beta-microsoft.com	Allowed	Professional Services	None	0	6,420	Sunday, June 18, 2017 12:00:52.000
8	Sunday, June 18, 2017 12:00:59.000	Torrel I	settings-wws-beta-microsoft.com	Allowed	Professional Services	None	0	5,340	Sunday, June 18, 2017 12:00:59.000
9	Sunday, June 18, 2017 12:01:07.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,240	Sunday, June 18, 2017 12:01:07.000
10	Sunday, June 18, 2017 12:01:15.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,580	Sunday, June 18, 2017 12:01:15.000
11	Sunday, June 18, 2017 12:01:23.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,370	Sunday, June 18, 2017 12:01:23.000
12	Sunday, June 18, 2017 12:01:31.000	Anonymous	identical.google.com	Allowed	Web Search	None	0	6,488	Sunday, June 18, 2017 12:01:31.000
13	Sunday, June 18, 2017 12:01:39.000	Anonymous	plus.google.com	Allowed	Social Networking	None	0	2,510	Sunday, June 18, 2017 12:01:39.000
14	Sunday, June 18, 2017 12:01:47.000	Anonymous	identical.google.com	Allowed	Web Search	None	0	5,880	Sunday, June 18, 2017 12:01:47.000
15	Sunday, June 18, 2017 12:01:55.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,300	Sunday, June 18, 2017 12:01:55.000
16	Sunday, June 18, 2017 12:02:03.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,300	Sunday, June 18, 2017 12:02:03.000
17	Sunday, June 18, 2017 12:02:11.000	Anonymous	v18-metastatic-beta-microsoft.com	Allowed	Professional Services	None	0	8,926	Sunday, June 18, 2017 12:02:11.000
18	Sunday, June 18, 2017 12:02:19.000	Anonymous	plus.google.com	Allowed	Social Networking	None	0	1,370	Sunday, June 18, 2017 12:02:19.000
19	Sunday, June 18, 2017 12:02:27.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,140	Sunday, June 18, 2017 12:02:27.000
20	Sunday, June 18, 2017 12:02:35.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,270	Sunday, June 18, 2017 12:02:35.000
21	Sunday, June 18, 2017 12:02:43.000	Anonymous	www.google.com	Allowed	Web Search	None	0	3,388	Sunday, June 18, 2017 12:02:43.000
22	Sunday, June 18, 2017 12:02:51.000	Anonymous	plus.google.com	Allowed	Social Networking	None	0	3,988	Sunday, June 18, 2017 12:02:51.000
23	Sunday, June 18, 2017 12:02:59.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,210	Sunday, June 18, 2017 12:02:59.000
24	Sunday, June 18, 2017 12:03:07.000	Anonymous	www.google.com	Allowed	Web Search	None	0	3,200	Sunday, June 18, 2017 12:03:07.000
25	Sunday, June 18, 2017 12:03:15.000	Anonymous	www.google.com	Allowed	Web Search	None	0	2,220	Sunday, June 18, 2017 12:03:15.000

Figure 1. Example Zscaler logs



The Zscaler dashboard gives you a quick overview of what is going on.



*Figure 2. Example Zscaler dashboard*

You can optionally configure other Zscaler policies/services. They are outside the scope of this guide.

# Use Case: Single ISP Internet Breakout

## Step 1: Request tunnel destination

- Obtain a support ticket.

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

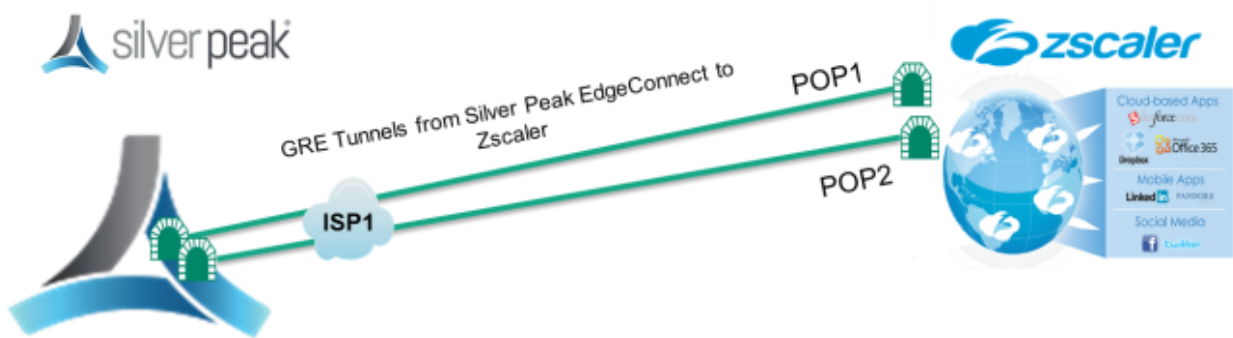


Figure 3. Logical Deployment of Single ISP Internet Breakout to Zscaler

Deployment

Router Bridge Server

LAN Side Routes

LAN Interfaces +Add				WAN Interfaces +Add						
Interface	VLAN	Label	IP/Mask	IP/Mask	Label	VLAN	Firewall	Interface	Bandwidth (Kbps)	Next Hop
lan0		None	10.8.106.2/24 No DHCP	172.25.32.162/26	MPLS		Allow All	wan0	200,000 200,000	172.25.32.129
				10.8.208.2/24	zScaler		Stateful	wan1	200,000 200,000	10.8.208.3

Total Outbound: 400,000 Kbps ≤ 10,000,000 Kbps  
 Total Inbound: 400,000 Kbps  Shape Inbound Traffic

EdgeConnect Licensing Boost:  for > 200 Mbps  
 Boost: 0 Kbps

Figure 4. Deployment

- Choose **stateful** firewall and NAT.

- Optional. Add a new label called **Zscaler**.

### Step 3: Setup Internet Breakout Tunnels

- Create Internet Breakout tunnels to the two Zscaler IP's.

4 Rows	Search																																							
<table border="1"> <thead> <tr> <th>Overlay</th> <th>Underlay</th> <th>Passthrough</th> </tr> </thead> <tbody> <tr> <td>Geneva</td> <td>Zscaler1</td> <td>10.8.208.2</td> </tr> <tr> <td>Geneva</td> <td>Zscaler2</td> <td>10.8.208.2</td> </tr> </tbody> </table>	Overlay	Underlay	Passthrough	Geneva	Zscaler1	10.8.208.2	Geneva	Zscaler2	10.8.208.2	<table border="1"> <thead> <tr> <th>Edit</th> <th>Appliance</th> <th>Passthrough Tunnel</th> <th>Local IP</th> <th>Remote IP</th> <th>Mode</th> <th>Max BW Un...</th> <th>NAT</th> <th>Peer</th> <th>Max BW Kbps</th> </tr> </thead> <tbody> <tr> <td></td> <td>Geneva</td> <td>Zscaler1</td> <td>10.8.208.2</td> <td>199.168.148.131</td> <td>gre_ip</td> <td>☑</td> <td>none</td> <td>Zscaler1</td> <td>400000</td> </tr> <tr> <td></td> <td>Geneva</td> <td>Zscaler2</td> <td>10.8.208.2</td> <td>104.129.194.38</td> <td>gre_ip</td> <td>☑</td> <td>none</td> <td>Zscaler2</td> <td>400000</td> </tr> </tbody> </table>	Edit	Appliance	Passthrough Tunnel	Local IP	Remote IP	Mode	Max BW Un...	NAT	Peer	Max BW Kbps		Geneva	Zscaler1	10.8.208.2	199.168.148.131	gre_ip	☑	none	Zscaler1	400000		Geneva	Zscaler2	10.8.208.2	104.129.194.38	gre_ip	☑	none	Zscaler2	400000
Overlay	Underlay	Passthrough																																						
Geneva	Zscaler1	10.8.208.2																																						
Geneva	Zscaler2	10.8.208.2																																						
Edit	Appliance	Passthrough Tunnel	Local IP	Remote IP	Mode	Max BW Un...	NAT	Peer	Max BW Kbps																															
	Geneva	Zscaler1	10.8.208.2	199.168.148.131	gre_ip	☑	none	Zscaler1	400000																															
	Geneva	Zscaler2	10.8.208.2	104.129.194.38	gre_ip	☑	none	Zscaler2	400000																															

Figure 5. Internet Breakout Tunnels

- Choose interface label for the Zscaler IP as **Local IP**. This is the interface used for Internet Breakout as per the Deployment page.
- Choose **Mode** `gre_ip`.  
NAT is done at the Zscaler end, so no NAT is chosen.
- Choose **Peer/Service** Name to be Zscaler1, 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.

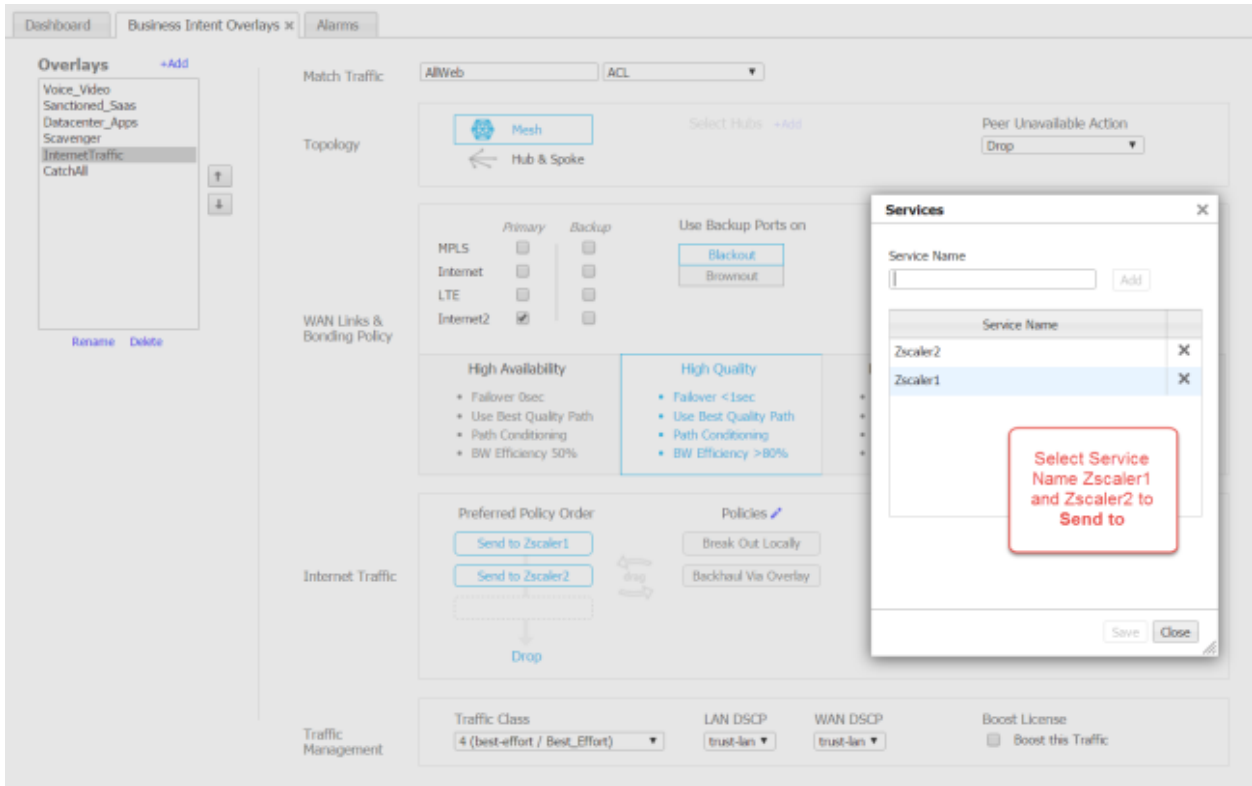


Figure 6. Business Intent Overlays for Internet Traffic

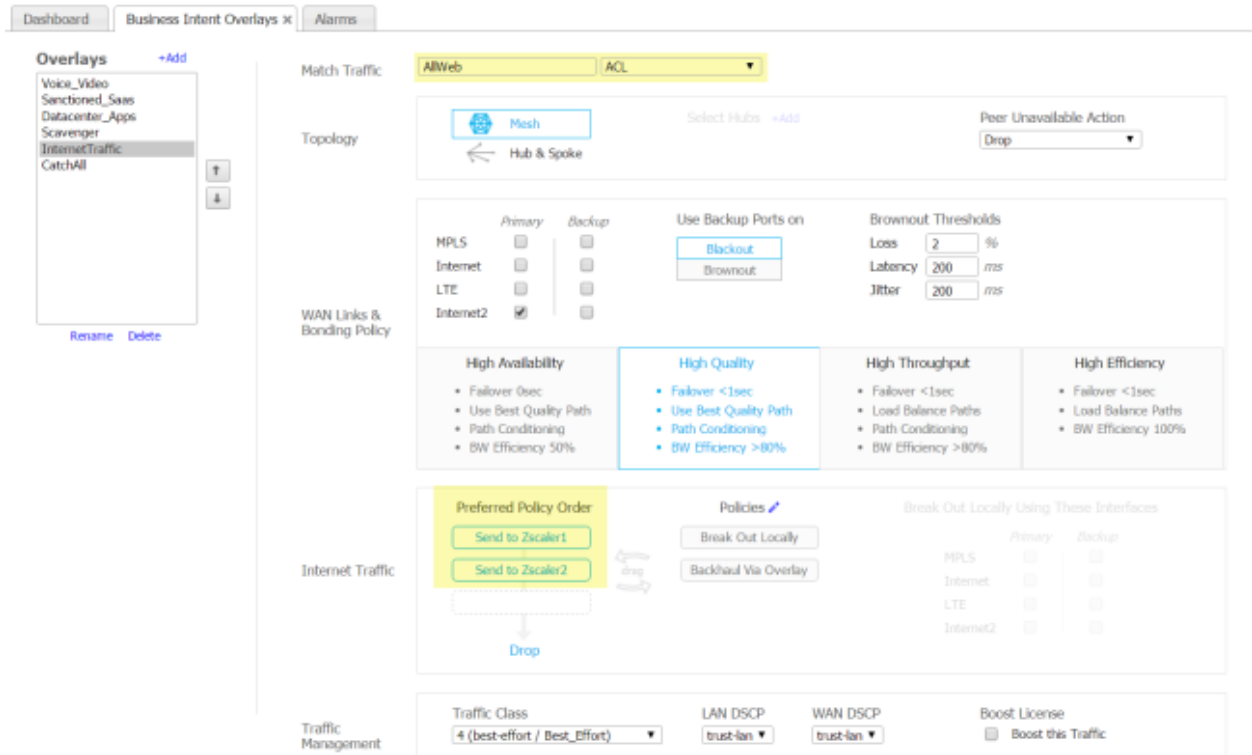


Figure 7. Business Intent Overlays with Zscaler as Service

## 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.

**IP SLA Rule** ×

ON OFF

Monitor:

Address:

Interface:

Keep Alive Interval:  (Sec)

Up Threshold:  (Sec)

Down Threshold:  (Sec)

Interval:  (Sec)

Down Action:

Tunnel:

Up Action:

Tunnel:

Comment:

Update Close

**IP SLA Rule** ×

ON OFF

Monitor:

Address:

Interface:

Keep Alive Interval:  (Sec)

Up Threshold:  (Sec)

Down Threshold:  (Sec)

Interval:  (Sec)

Down Action:

Tunnel:

Up Action:

Tunnel:

Comment:

Update Close

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.

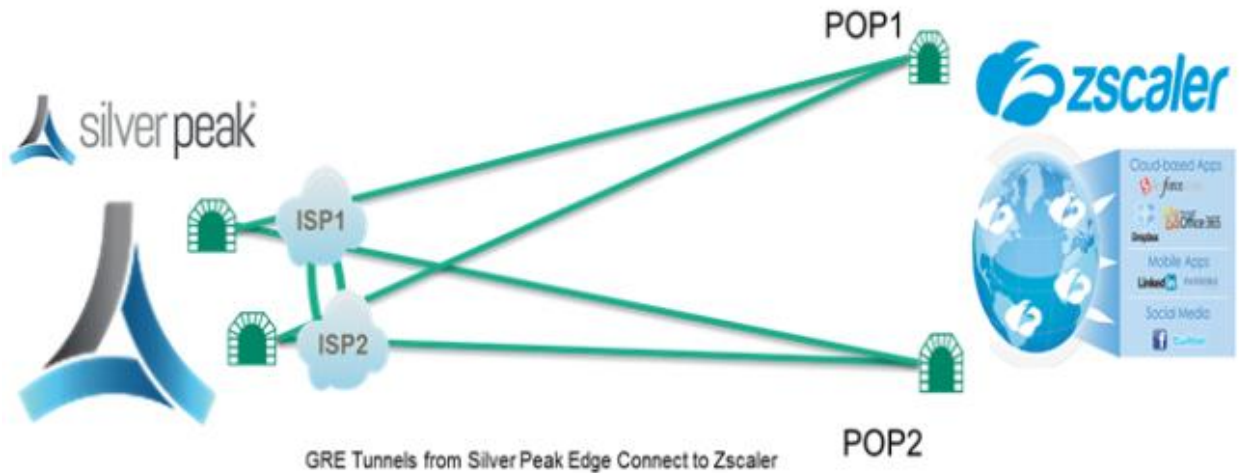


Figure 9. Logical Depiction of Dual ISP Internet Breakout

Tunnels Search

Overlay Underlay Passthrough

Edit	Appliance	Passthrough Tunnel	Local IP	Remote IP	Mode	Max BW Un.	NAT	Peer/Service	Max BW Kbps
✓	San Francisco	to_Zscaler2	104.139.20	104.129.194.38	gre_ip	✓	none	Zscaler2	75000
✓	San Francisco	to_Zscaler1	104.139.20	199.168.148.131	gre_ip	✓	none	Zscaler1	75000
✓	San Francisco	lb_to_Zscaler2	104.141.20	104.129.194.38	gre_ip	✓	none	Zscaler2	75000
✓	San Francisco	lb_to_Zscaler1	104.141.20	199.168.148.131	gre_ip	✓	none	Zscaler1	75000

ISP 1

ISP 2

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'.

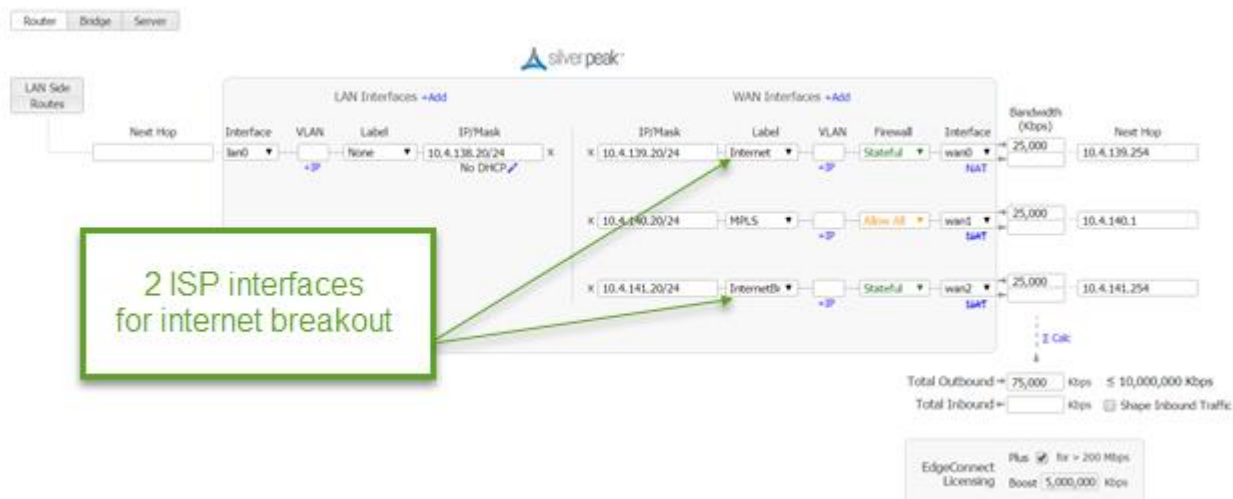


Figure 11. Dual ISP Internet Breakout Deployment

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.



# Use Case: Backhauled Internet Breakout

Content forthcoming