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

Trademark Notification

Warranties and Disclaimers

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

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

h*ttps://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

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.

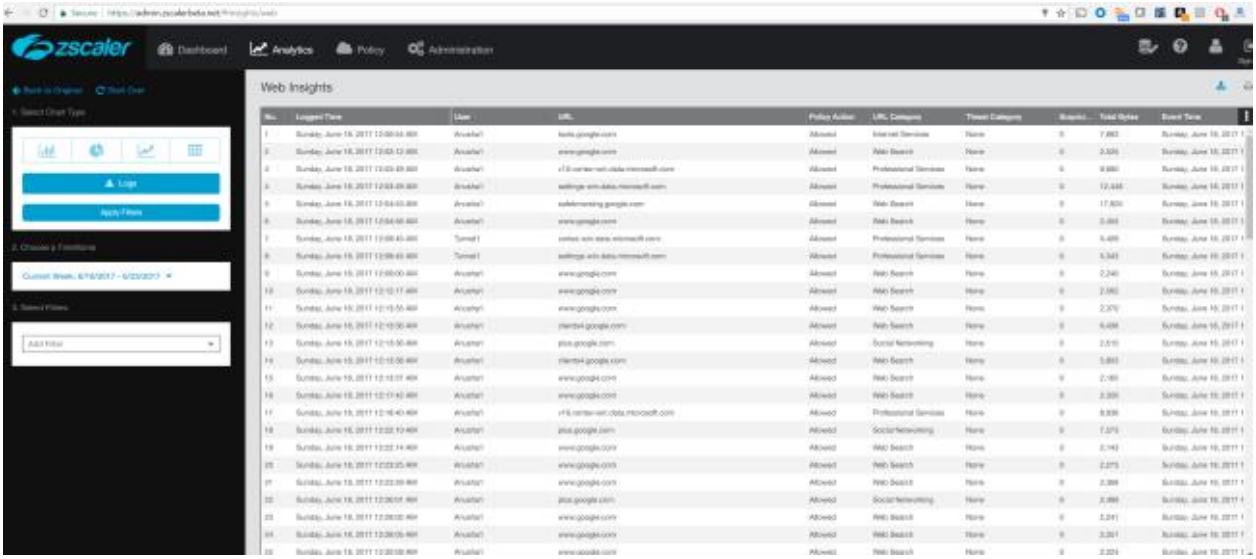

Figure 1. Example Zscaler logs

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

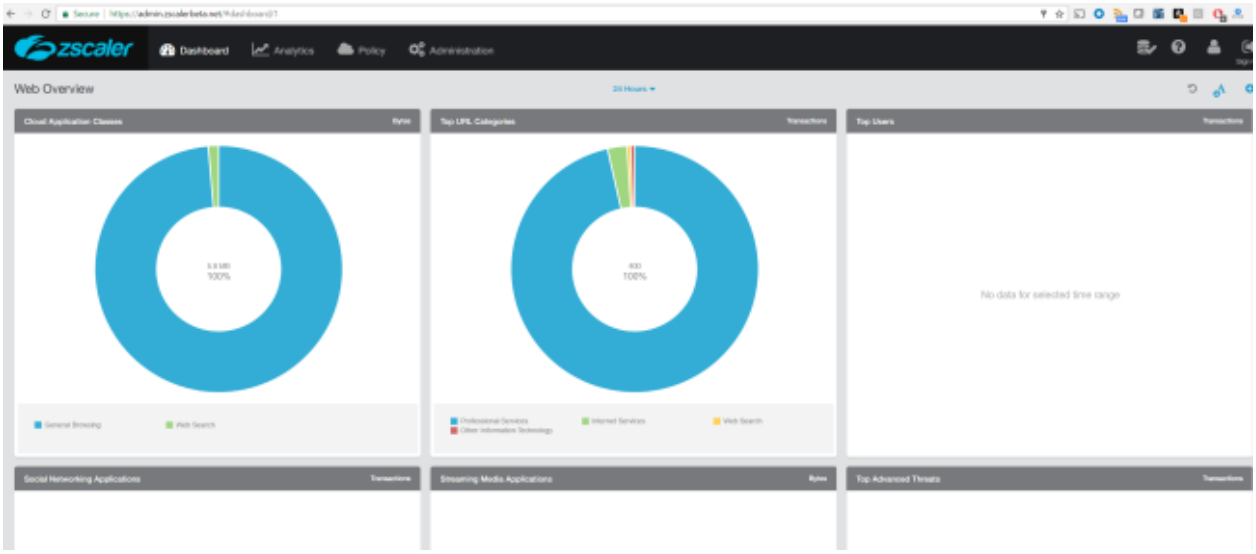

Figure 2. Example Zscaler dashboard

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

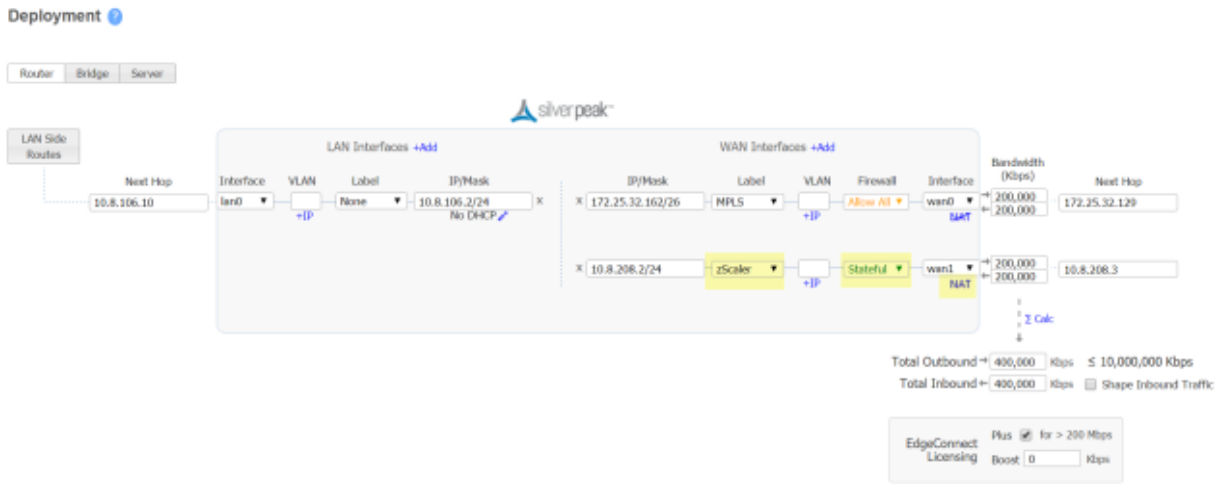

Figure 4. Deployment

- 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.

Figure 5. Internet Breakout Tunnels

A. Choose interface label for the Zscaler IP as **Local IP**. This is the interface used for Internet Breakout as per the Deployment page.

B. Choose **Mode** gre_ip.

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

C. 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.

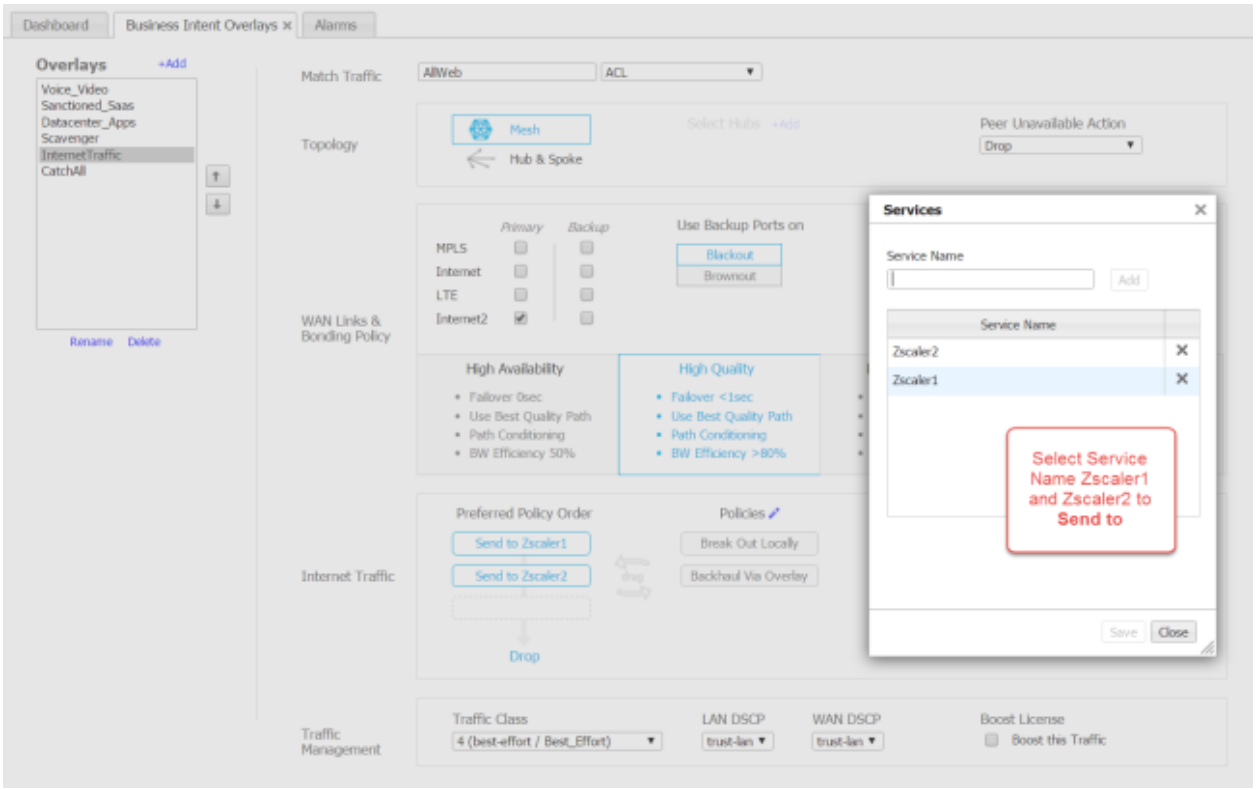

Figure 6. Business Intent Overlays for Internet Traffic

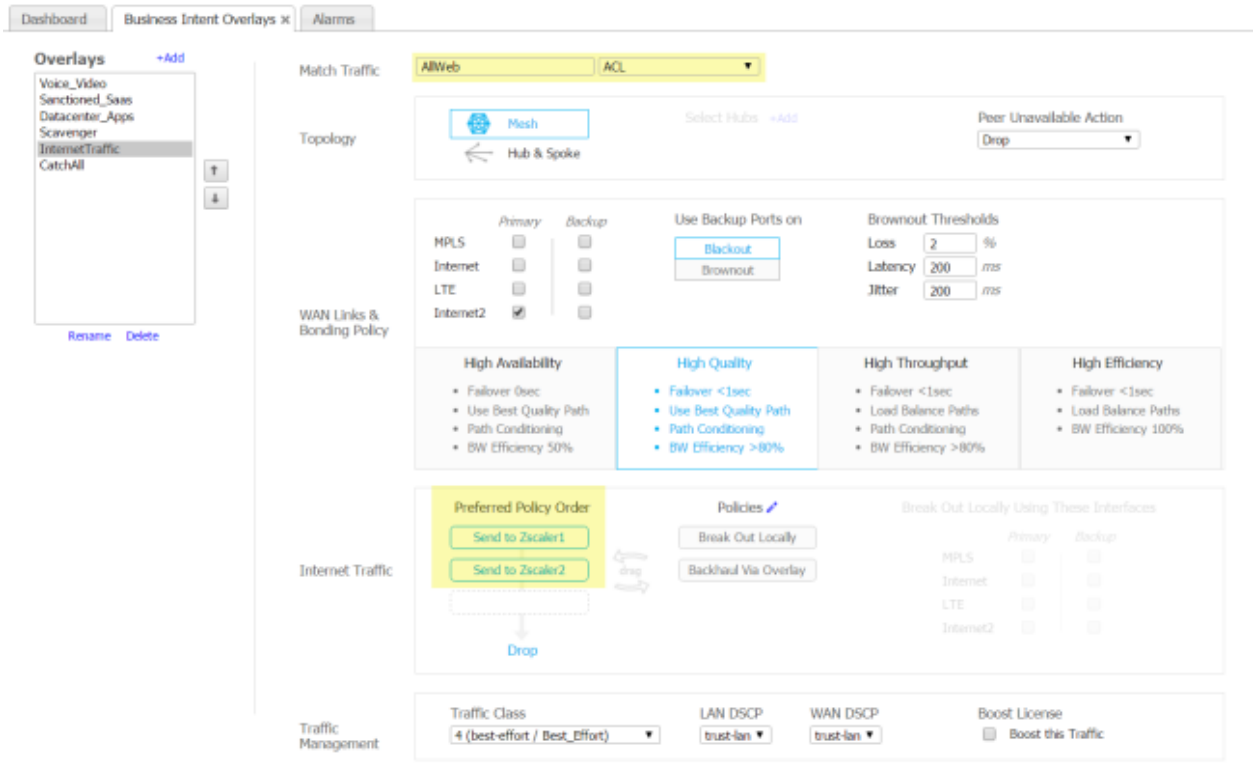

Figure 7. Business Intent Overlays with Zscaler as Service

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.

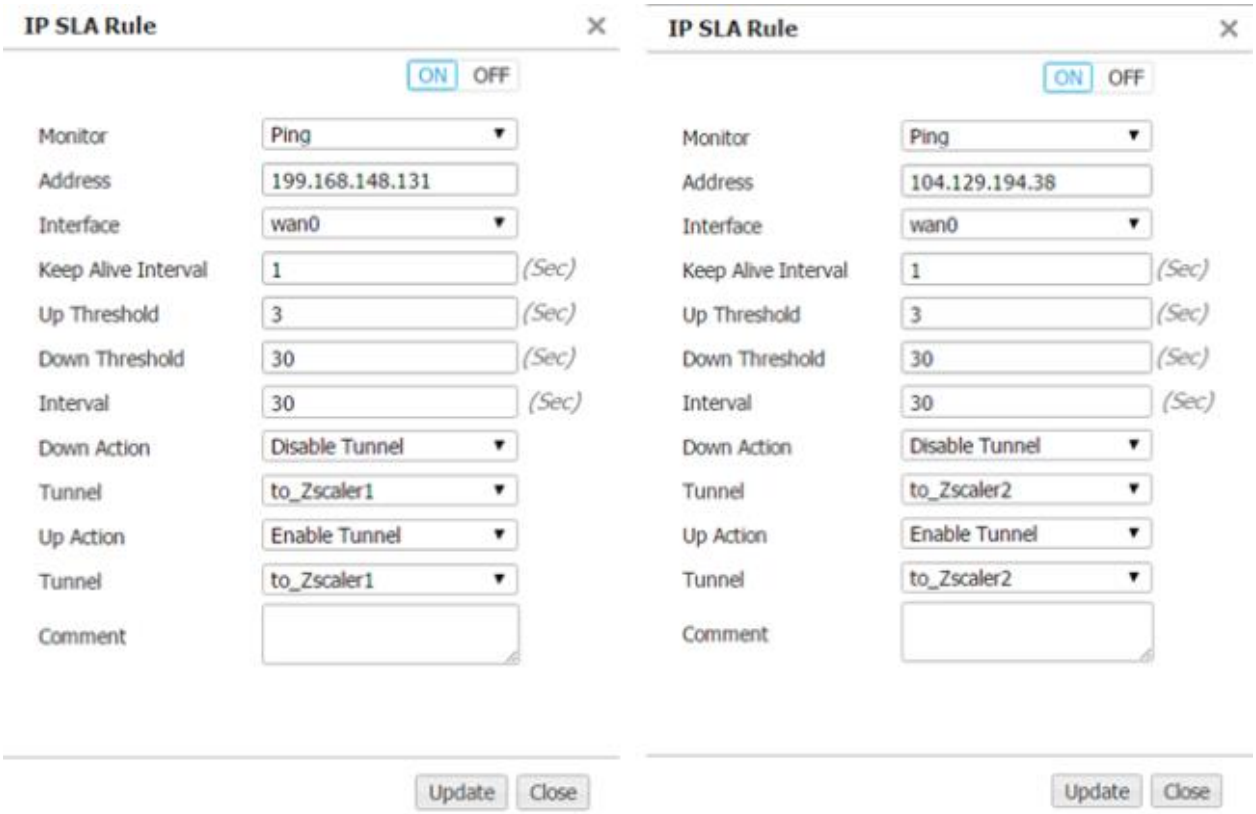

Figure 8. IP SLA Configuration

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.

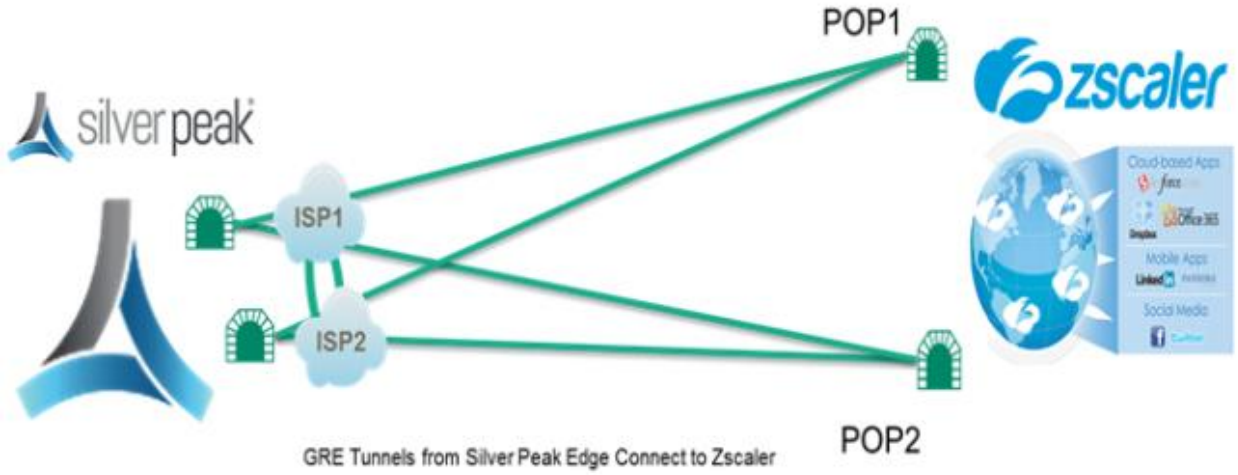

Figure 9. Logical Depiction of Dual ISP Internet Breakout

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’.

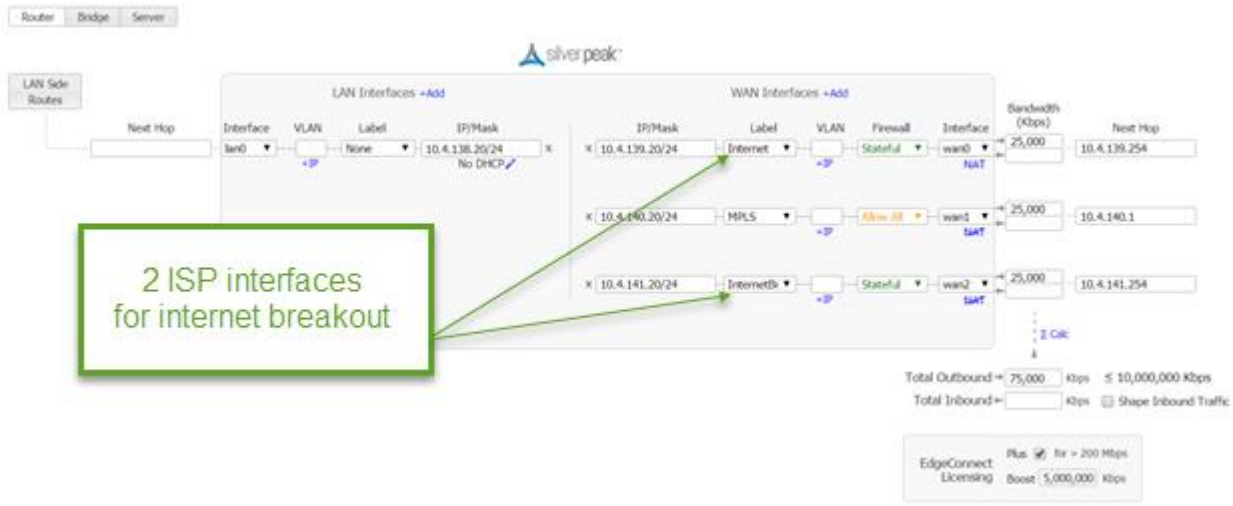

Figure 11. Dual ISP Internet Breakout Deployment

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