aryaka

zscaler™

Aryaka SmartCONNECT with Zscaler

Deployment Guide

Contents

Introduction

Aryaka's Global SD-WAN enables enterprises with fast global connectivity along with accelerated access to mission and business critical applications. Aryaka uses a Global Private Network with built-in optimization and security capabilities that include a multi-layer security approach with a global private core network, fortified security on the POPs , end-to-end encrypted tunnels, and stateful firewalls.

Zscaler adds a layer of advanced security controls needed for web and cloud bound traffic, with an in-line proxy architecture, inspecting traffic (including SSL) to provide identical protection for users wherever they connect, without impacting performance.

- Threat Prevention capabilities include Advanced Threat Protection, Cloud Sandbox, Anti-Virus, and DNS Security.
- Data Protection capabilities include Data Loss Prevention (DLP), Cloud Access Security Broker (CASB) and File Type Controls.
- Access Control capabilities include Next Generation Cloud Firewall, URL Filtering, Bandwidth Control, and DNS Filtering.

The Aryaka Edge device can seamlessly all forward internet and cloud bound traffic directly to the Zscaler cloud and the combined solution does not require additional on-premises hardware, appliances or software.

Together, Aryaka and Zscaler, deliver a best-of-breed SD-WAN and security platform for enterprises accessing mission-critical internally hosted applications as well as those going directly to the Internet for accessing cloud applications.

This Configuration Guide will explain how to configure Aryaka SmartCONNECT to connect it to the Zscaler cloud, creating a GRE VPN tunnel.

Requirements

1. Aryaka SmartCONNECT service subscription.
2. Zscaler Security as a Service platform subscription.

You will also need to contact Zscaler Tech Support to have them provision a location with GRE service in the 'Zscaler configuration' section below. The first section of this document outlines the necessary steps on the Zscaler portal and the second section outlines the steps to be performed on Aryaka's SmartCONNECT platform.

Zscaler Configuration

Zscaler configuration needs to be performed with the help of Zscaler Technical Support. Only Zscaler Support can provision these necessary changes.
1. Contact your Zscaler representative or Customer Support to have a GRE tunnel provisioned for your account. You will need to give them information about public IP address of ANAP and physical location of your branch office location for this.

Note: a GRE tunnel requires a static IP address.

2. Zscaler assigns VIPs (virtual IP addresses) for use as the source and destination addresses inside the tunnel. You need this information to configure Zscaler in Aryaka's MyAryaka portal.

3. Log in to the Zscaler service portal at (shown in Figure 1) https://admin.zscloud.net/ and add your gateway location. Click **Save**.

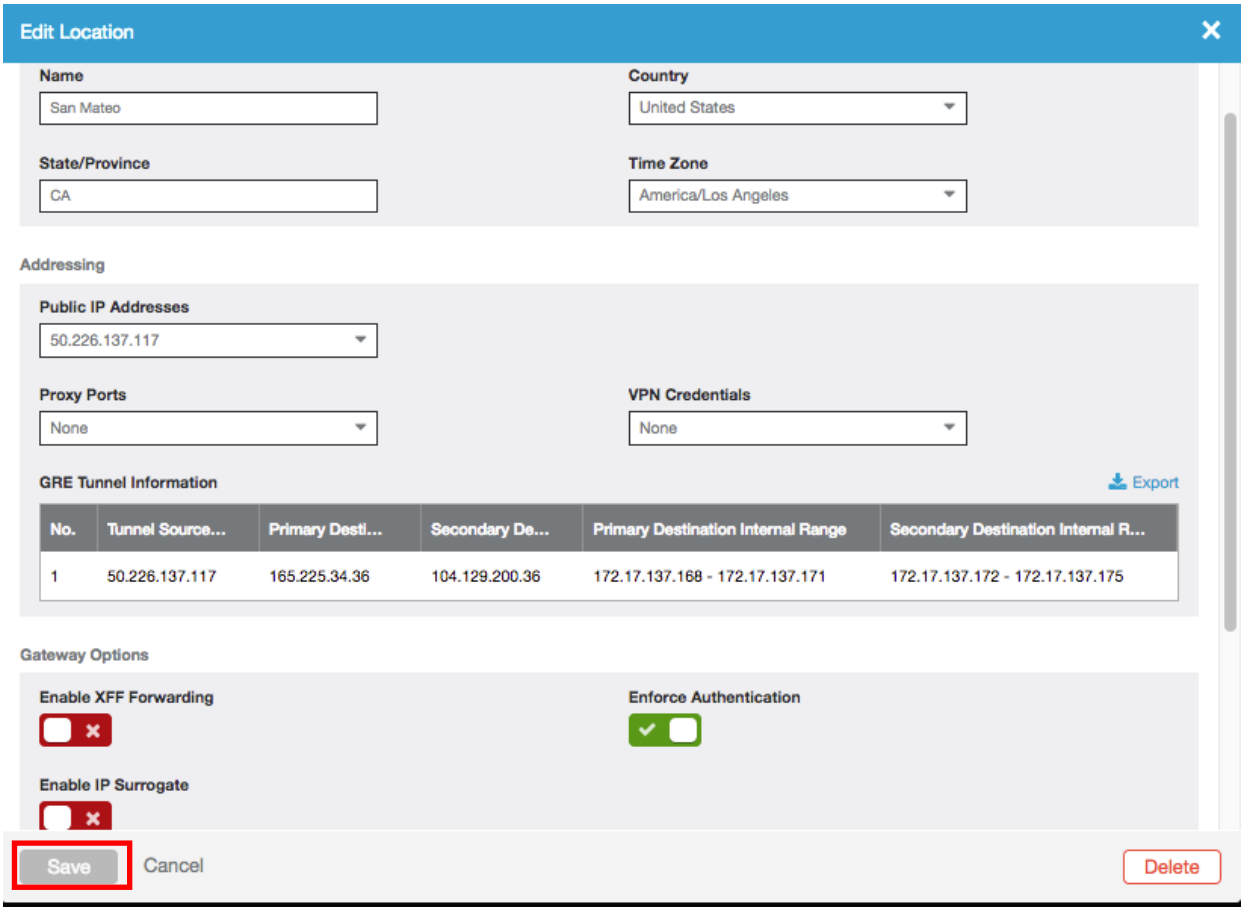

Figure 1

Activation

After the GRE tunnel provisioning & Location steps mentioned above are performed, you need to activate the changes on Zscaler's network.

The location of the **Activate** button is shown in the Figure 2.

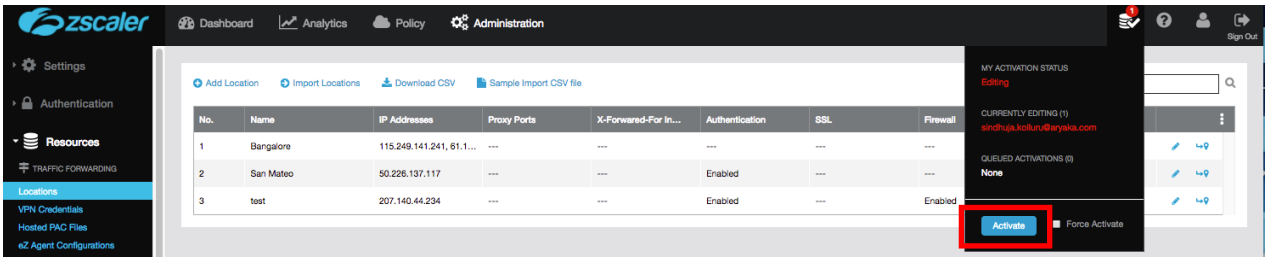

Figure 2

MyAryaka Configuration

Aryaka SmartCONNECT platform allows you to connect to a cloud security service using the Cloud Security Connector feature. Configuration can be done using the MyAryaka service portal at https://my.aryaka.com/ or with the help of Aryaka's Technical support team. The next section lists the steps when the configuration is done using MyAryaka™

Tunnel Setup

1. Navigate to the SmartCONNECT site that you want to deploy Zscaler on, and click Edit site. Select **Cloud Security** from the list of **Advanced Settings**.

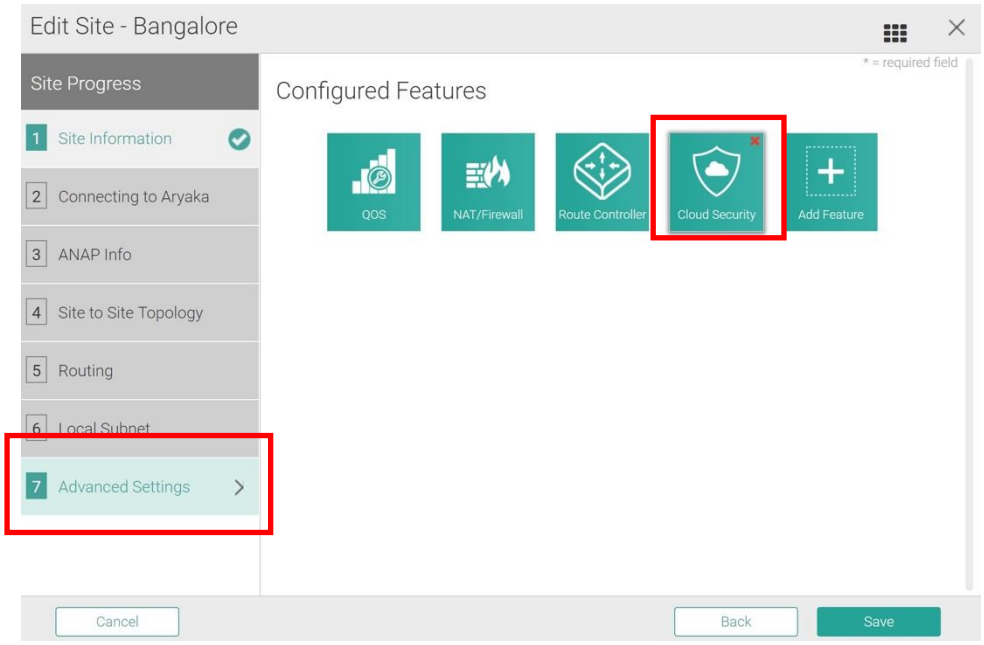

Figure 3

2. Once you add Cloud Security Connector feature, you will be requested to enter details as shown below in Figure 4.

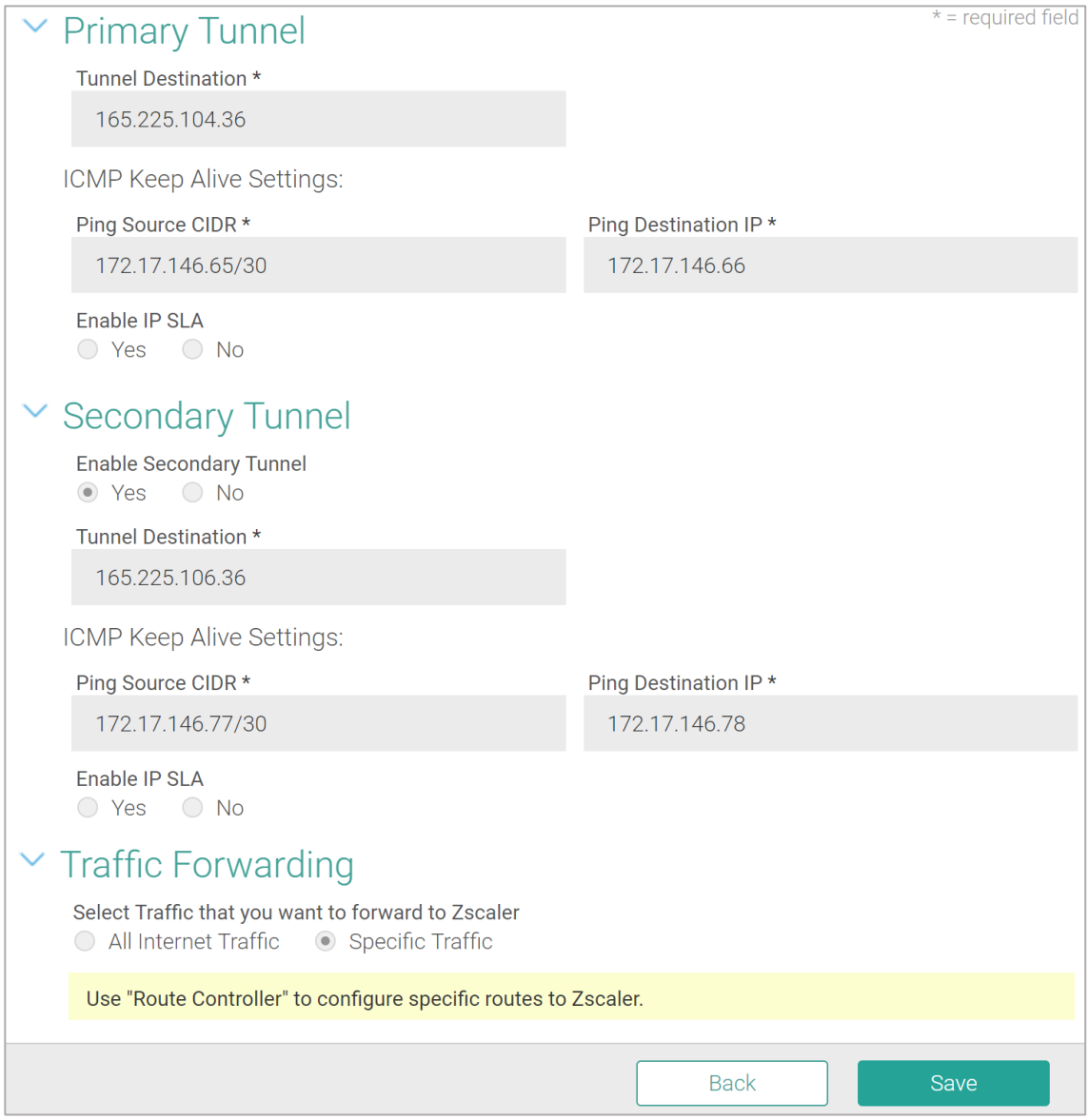

Figure 4

- Tunnel Source – This is the GRE tunnel IP source address and is dependent on ANAP deployment mode.
    - Enter LAN interface IP if ANAP is deployed in Simple Routed Mode
    - Enter M1 or M2 IP addresses if ANAP is deployed in Edge or Inline Routed Mode

- Tunnel Destination – Enter the primary public destination IP that was assigned by the Zscaler team.
- Ping Source CIDR – Enter the Internal Router IP and mask in CIDR format that was assigned by the Zscaler team.
- Ping Destination IP – Enter the Internal ZIA Public Service Edge IP that was assigned by Zscaler

  Aryaka will use ICMP probing by default to decide the health of the tunnel.
- Enable IPSLA – This is optional and is not enabled by default. By using HTTP GET in IPSLA, probes will be sent towards Zscaler that will traverse its full application stack. It is recommended that if you choose to enable IPSLA, do so with the following settings:
- HTTP Destination IP: Set as Internal ZIA Public Service Edge IP provided by Zscaler
- HTTP Get URL: gateway.<zscaler_cloud>.net/vpntest. To find zscaler_cloud name, look here: https://help.zscaler.com/zia/what-my- cloud-name

When service monitoring is down, the primary tunnel will failover to the backup tunnel. When monitoring is once again available, the service will switch back to the primary tunnel. By default, Aryaka will drop packets on both tunnel failure or if traffic is destined to private subnet. These settings can be modified in the *Advanced* mode

Traffic Forwarding

With an ANAP in Simple Routed Mode, all traffic that is not destined to the Aryaka POP will be routed to the Zscaler tunnel. Forwarding of only select traffic requires some form of policy based routing in your upstream firewall/router.

With ANAPs in Edge and Inline routed mode, you can control what traffic gets forwarded to Zscaler. When you choose to forward all traffic to Zscaler, a default rule named 'Forward All to Zscaler' will be inserted into the Route Controller under the "Default Routes" section for convenience.

If you choose to route only a specific route or routes, you will need to program the route(s) in the "Router Controller" section. It is recommended that you edit Default Routes to control forwarding and not override routes. The override routes will take precedence over any Aryaka destined traffic and can also cause the Site-to-Site traffic to go to Zscaler.

Figures 5 and 6 shows a snapshot of Route Controller feature:

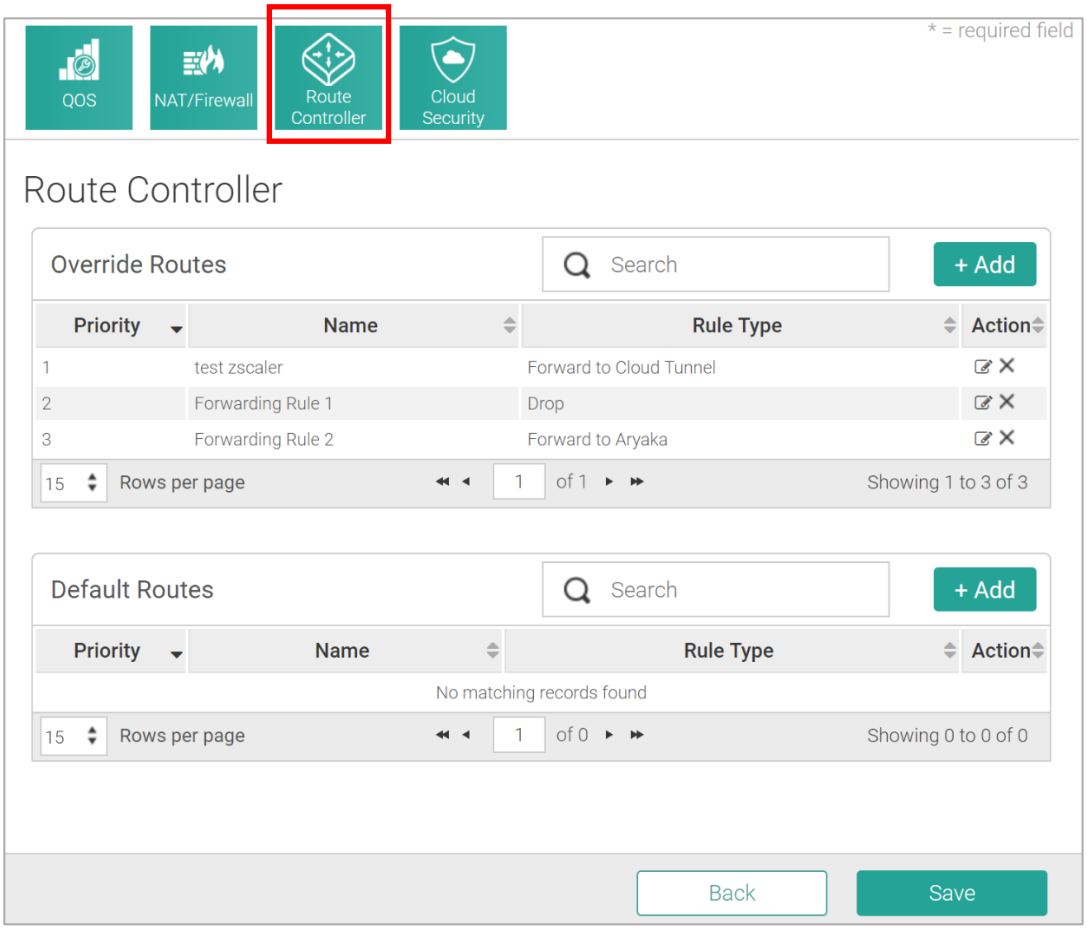

Figure 5

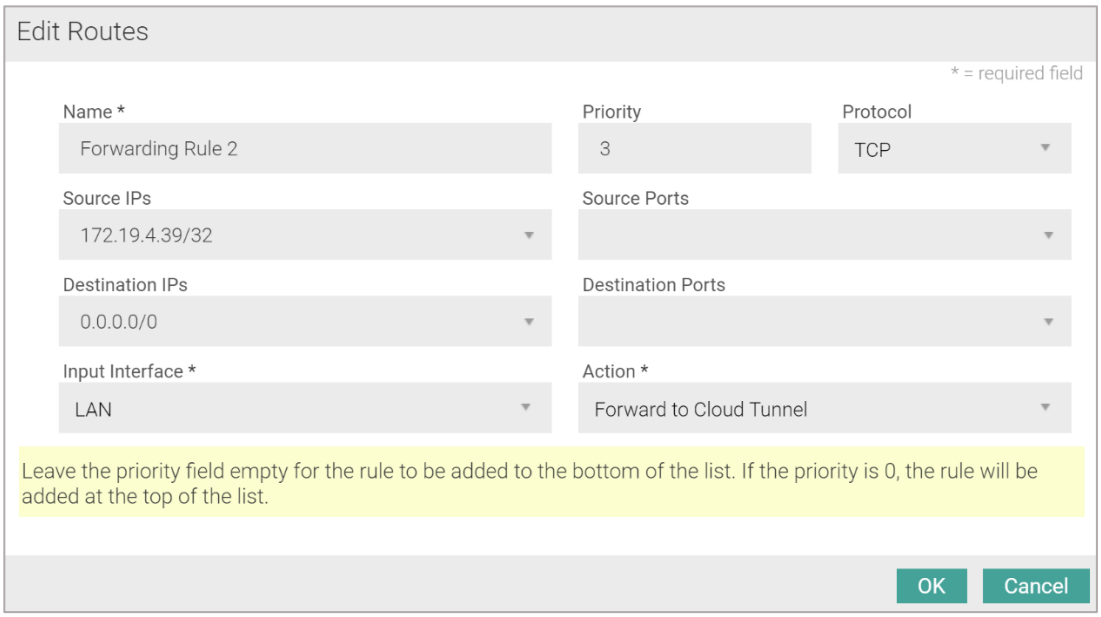

Figure 6

MyAryaka Visibility

You can log in to the MyAryaka™ portal to get complete visibility into all of your traffic routed to Zscaler. You will be able to monitor traffic and health for all of your sites connected to Zscaler via the ANAP.

Monitoring Traffic

To monitor Zscaler traffic, navigate to Cloud Security ConnectorTraffic under the Monitor tab. Select a reference site.

Internet traffic

- Total Internet – All traffic forwarded to the Internet.
- Total Zscaler – All Internet traffic forwarded to Zscaler.
- Total Other – All traffic forwarded to Internet that is not going to Zscaler

The sum of Zscaler Traffic and Other traffic will match Total Internet traffic. Figure 7 is a sample graph showing traffic data for a site.

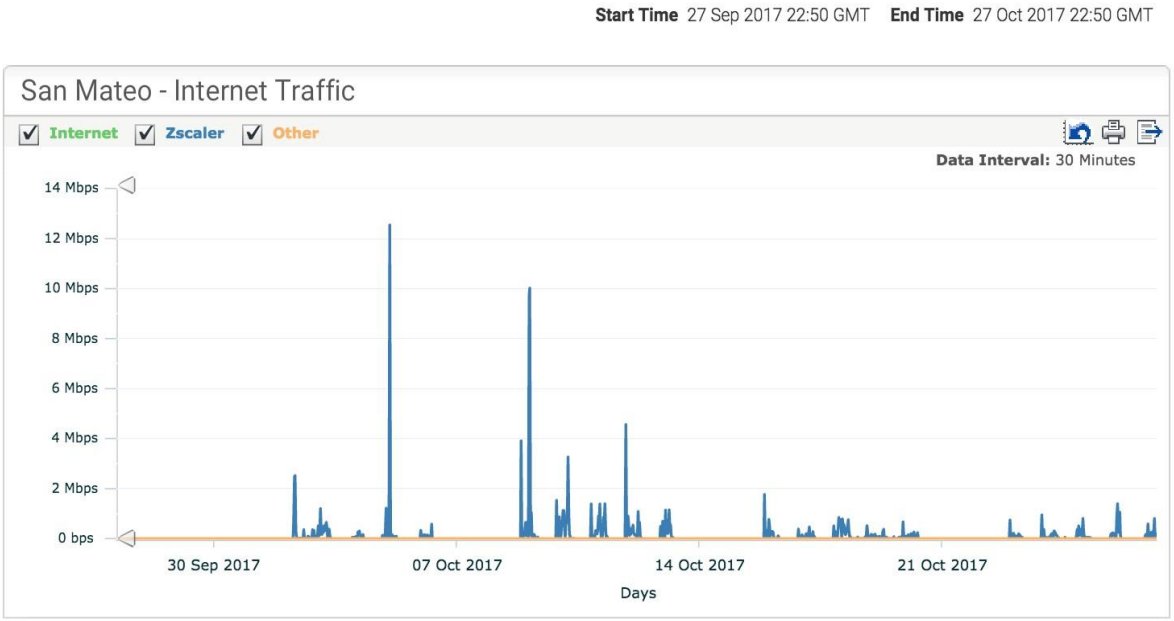

Figure 7

ZScaler Traffic

Zscaler allows redundant tunnels to be configured to their cloud in Active/Standby mode. These graphs provided traffic data that is carried over these tunnels.

Figure 8 shows the bi-directional traffic carried by each tunnel and can be useful in determining which tunnel is being used to carry traffic.

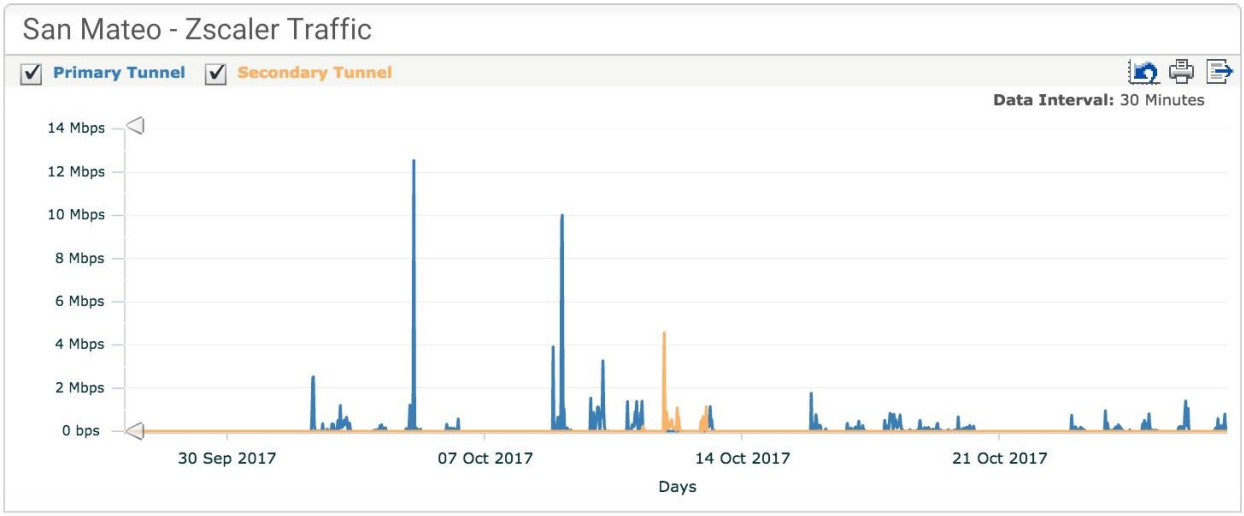

Figure 8

Zscaler Received

Figure 9 shows all traffic received on the GRE tunnels to Zscaler. This represents all Internet traffic inbound to the site from Zscaler.

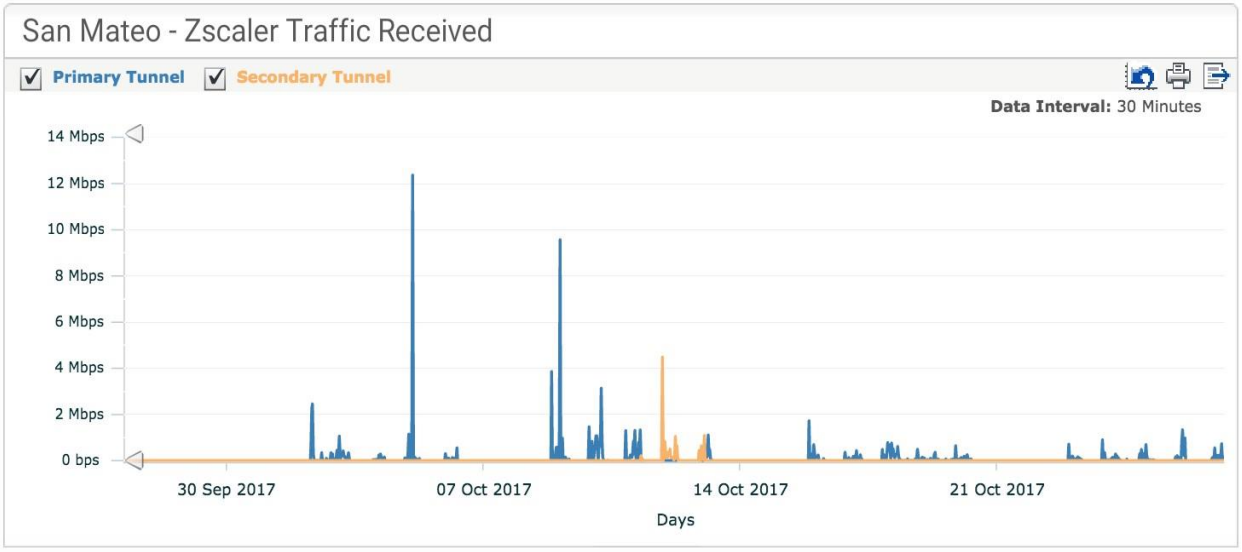

Figure 9

Zscaler Transmitted

Figure 10 shows all traffic that is transmitted on GRE tunnels to Zscaler. This represents all traffic outbound to Zscaler from the site.

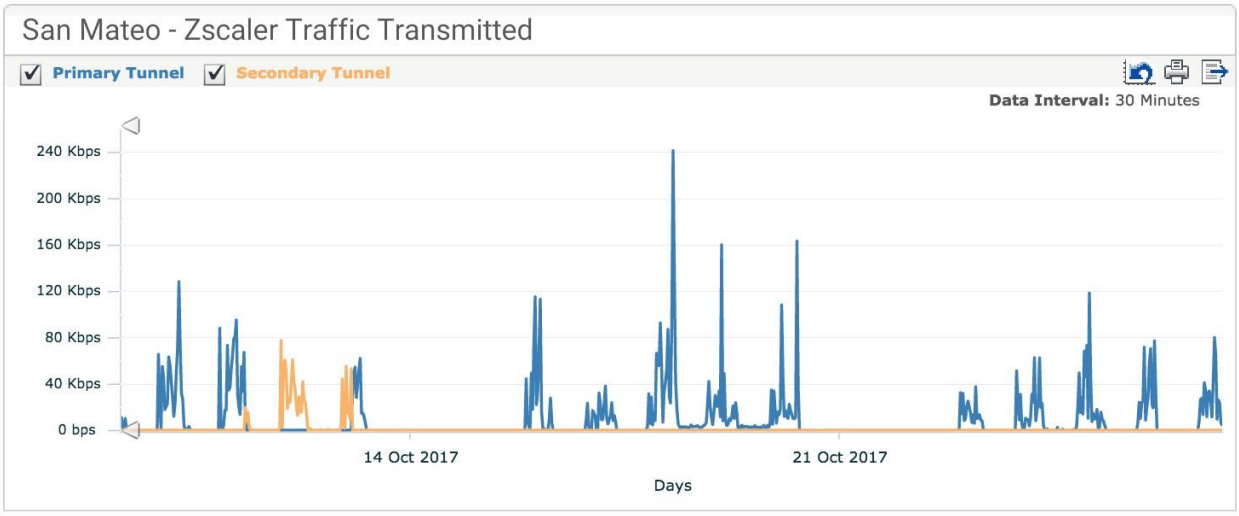

Figure 10

Health

To verify connectivity to Zscaler, navigate to the Cloud Security Connector Health option under the Monitor tab.

The following statistics are displayed to help determine the health of the GRE Tunnels:

Total Processing Time

This line represents the time taken by IPSLA to fetch a file that was configured to be downloaded. This includes DNS resolution time, Connect time, Request time etc.

Fail %

This line represents any failures to run IPSLA probe. Failure could be caused by any reason such as connectivity issues, configuration issues, etc

Figure 11 depicts a sample Health graph for a site.

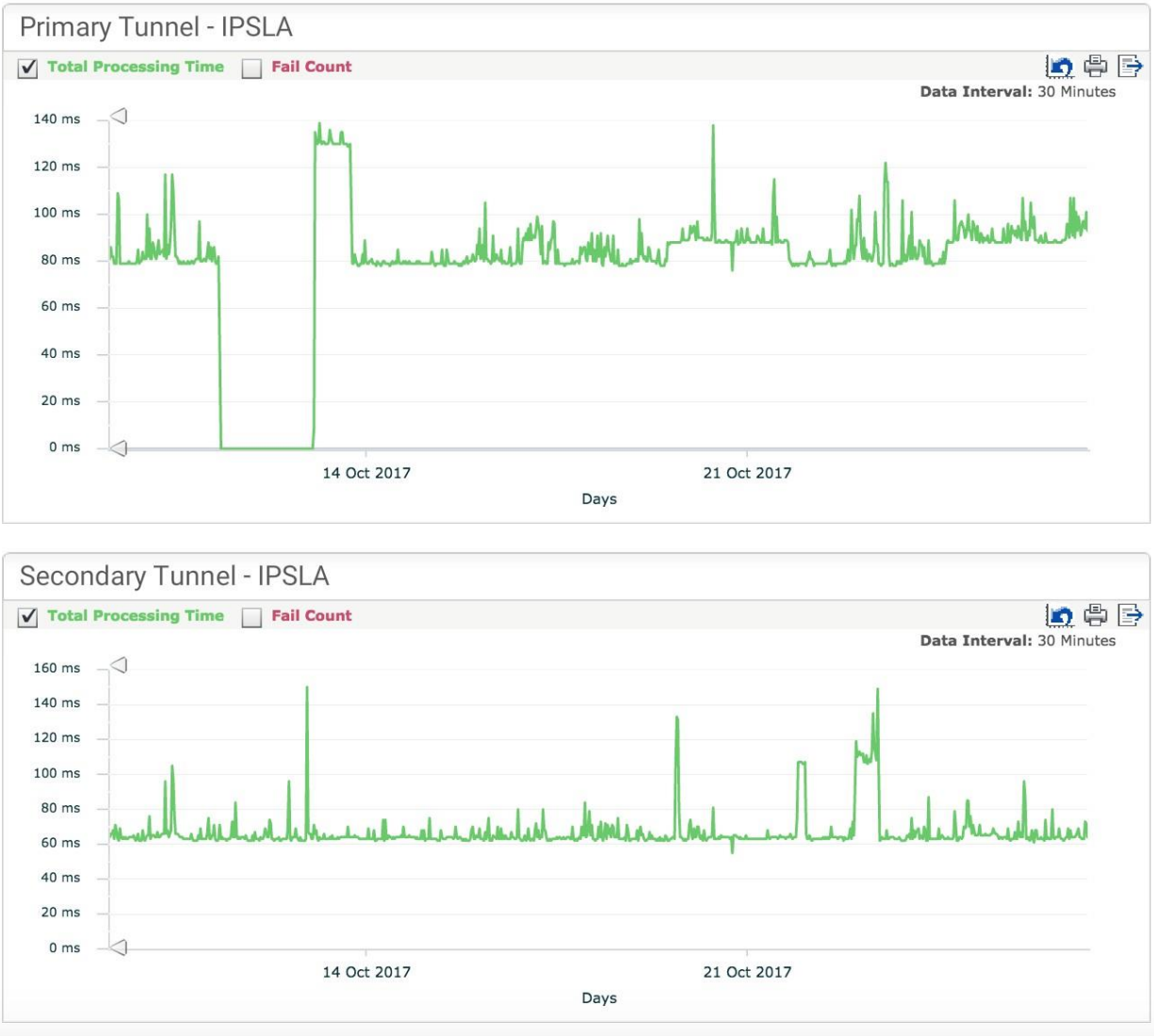

Figure 11

Status

The status of GRE tunnels can be determined by navigating to the Status Cloud Security Connector. Availability of a GRE tunnel (up/down) is determined using ICMP probing. IPSLA based probing if configured is used to determine the active state of the tunnel. Figure 12 provides a snapshot the status of the cloud security connector.

Cloud Security connector - Zscaler Status (Last 5 Mins) Refresh

Site Name	Tunnel Status		Traffic		IPSLA Time	
	Primary	Secondary	Primary	Secondary	Primary	Secondary
San Mateo	Down, Standby	Up, Active	42 KB	174.26 MB	0 ms	77 ms
Bangalore	Up, Active	Down, Standby	0 KB	0 KB	0 ms	0 ms

Figure 12

Alternatively, users can visit http://ip.zscaler.com and verify they are indeed coming through Zscaler.

Verifying ZIA Configuration

Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. Figure 13 displays the message when users are not transiting ZIA.

Figure 13

If you are transiting ZIA, you should see what is presented in Figure 14

Figure 14

About Aryaka

Aryaka offers the only viable SD-WAN solution for global enterprises. Aryaka's global SD-WAN delivers significantly better performance for cloud and on-premises applications — voice, video and data — for enterprise data centers, branch offices and remote/mobile employees anywhere in the world.

Unlike legacy connectivity solutions that take months to deploy, Aryaka's Global SD-WAN can be deployed within days. It is delivered as a service, so IT organizations can consume global networking services the way they would consume SaaS applications like Salesforce and Infrastructure-as-a-Service solutions like Amazon Web Services and Azure.

With more than 700 global enterprise customers, Aryaka is also the largest independent global SD-WAN provider by market share.

To learn more, visit www.aryaka.com.

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, please visit www.zscaler.com.

Additional Resources

Please contact Aryaka support at support@aryaka.com for any additional help.

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

ZIA Test Page:
http://ip.zscaler.com/

Thank You for Considering

For information on other products, services, use cases or customer success, visit www.aryaka.com.

Questions? Email **sales@aryaka.com** or give us a call at **1.877.727.9252.**

Give it a try to experience the benefits for yourself.