zscaler™ | aryaka

ZSCALER AND ARYAKA DEPLOYMENT GUIDE

FEBRUARY 2022, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

©2024 Zscaler, Inc. All rights reserved.

©2024 Zscaler, Inc. All rights reserved.

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
ANAP	Aryaka Network Access Point (Ayraka)
CA	Central Authority (Zscaler)
CIDR	Classless Inter-Domain Routing
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IP SLA	Internet Protocol Service Level Agreement
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
MPLS	Multiprotocol Label Switching
PFS	Perfect Forward Secrecy
POPs	Point of Presence
PSK	Pre-Share Key
SLA	Service Level Agreement
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

©2024 Zscaler, Inc. All rights reserved.

Trademark Notice

© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't 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. To learn more, see Zscaler's website.

Aryaka Overview

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, refer to Aryaka's website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Zscaler Resources
- Arkaya Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

©2024 Zscaler, Inc. All rights reserved.

Zscaler and Aryaka Introduction

Overviews of the Zscaler and Aryaka applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

©2024 Zscaler, Inc. All rights reserved.

Aryaka SmartConnect Overview

Aryaka SmartConnect is a turnkey, fully-managed global SD-WAN service that delivers predictable performance for any application, anywhere in the world:

- Deploys in as fast as an hour.
- Leverages a global, software-defined Layer 2 private network with WAN Optimization, using no MPLS.
- Delivers performance acceleration for business-critical applications.
- Provides connectivity to and between multiple cloud platforms.
- Offers 99.99% end-to-end reliability SLA.
- Leverages public internet connectivity for non-critical priority traffic.

Arkaya Resources

The following table contains links to Aryaka support resources.

Name	Definition
Aryaka Documentation	Online documentation for Aryaka products.
Aryaka Contact Us	Online contact information and support resources for Aryaka.

©2024 Zscaler, Inc. All rights reserved.

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 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 guide explains how to configure Aryaka SmartConnect to connect it to the Zscaler cloud, creating a GRE VPN tunnel.

Requirements

The following are required for the Zscaler and Aryaka integration:

- Aryaka SmartConnect service subscription.
- Zscaler Internet Access (ZIA) subscription.

You must contact Zscaler Support to have them provision a location with GRE service as described in **ZIA Configuration**.

The first section of this document outlines the necessary steps on the ZIA Admin Portal and the second section outlines the steps to be performed on Aryaka's SmartConnect platform.

©2024 Zscaler, Inc. All rights reserved.

ZIA Configuration

ZIA configuration must be performed with the help of Zscaler Support. Only Zscaler Support can provision these necessary changes.

1. Contact your Zscaler Account team to have a GRE tunnel provisioned for your account. You must give them information about public IP address of ANAP, and the physical location of your branch office location. 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 ZIA Admin Portal and add your gateway location:
   a. Go to **Administration** > **Location Management**.
   b. Click **Edit** for the new location provided by Zscaler.
   c. Enter the following information:
      - **Name**: Enter a distinctive name.
      - Enter the **Country**, **State/Province**, **Time Zone**.
      - **Public IP Addresses**: Enter the Zscaler virtual IP address.
      - **Proxy Ports**: Use the default.
      - **VPN Credentials**: Select the credentials for the VPN service.
      - Enable **Enforce Authentication**.
4. Click **Save**.

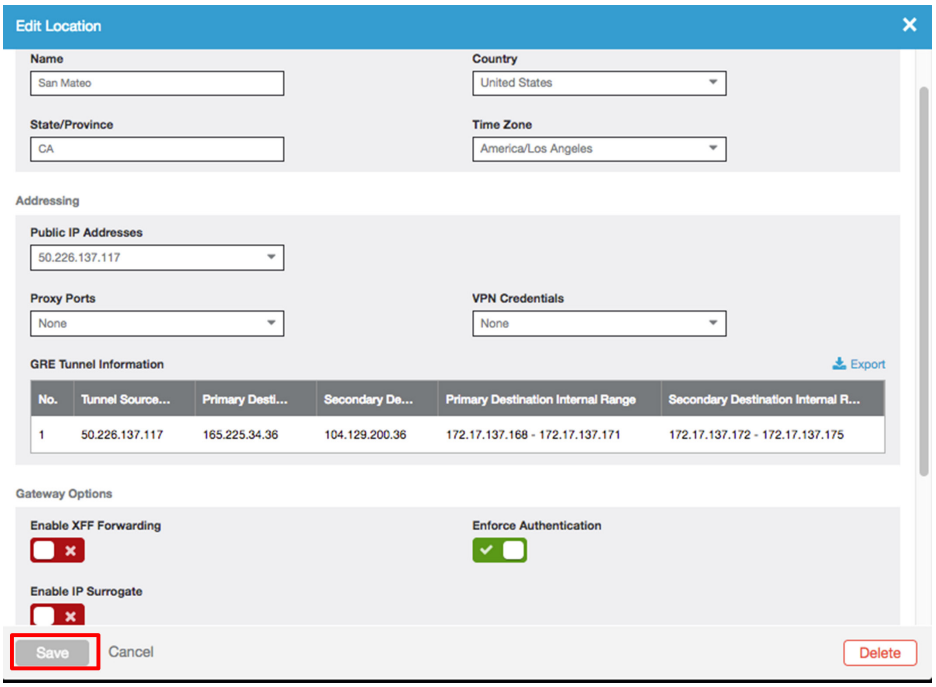

Figure 1. Edit Location

©2024 Zscaler, Inc. All rights reserved.

Activation

After the GRE tunnel provisioning and Location gateway options are configured, you must activate the changes on Zscaler's network.

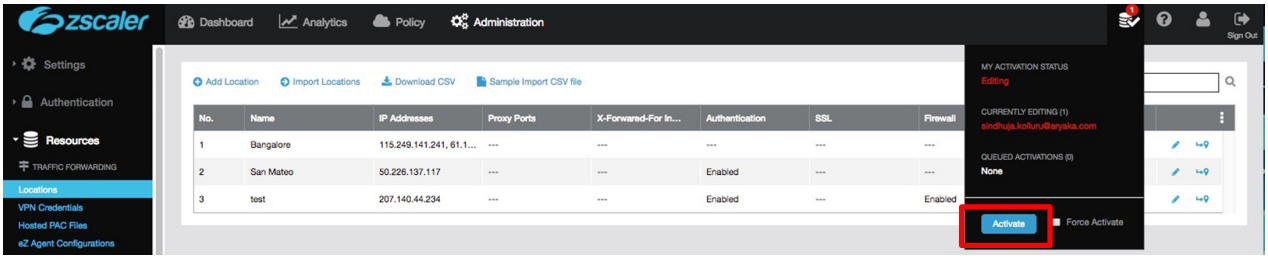

Figure 2. Activate configuration

©2024 Zscaler, Inc. All rights reserved.

MyAryaka Configuration

Aryaka SmartConnect platform allows you to connect to a cloud security service using the Cloud Security Connector feature. Use either the MyAryaka service portal at https://my.aryaka.com or contact Aryaka's Technical support team. The following section lists the steps when using MyAryaka.

Tunnel Set Up

To set up the tunnel:

1. Go to the SmartConnect site on which you want to deploy Zscaler and click **Edit site**.
2. Select **Cloud Security** from the list of **Advanced Settings**.

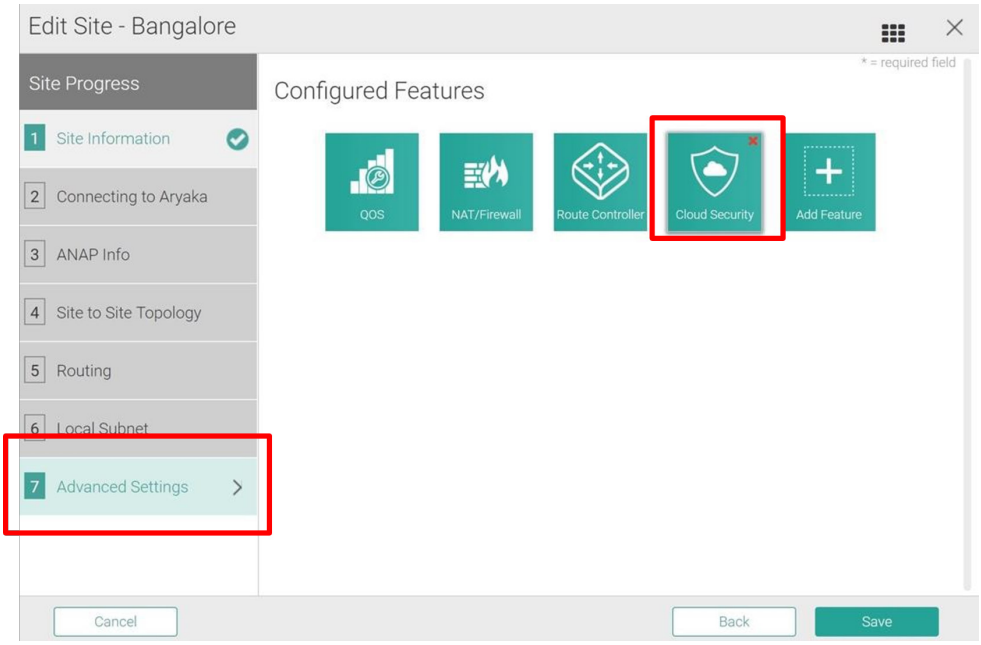

Figure 3. Cloud Security

©2024 Zscaler, Inc. All rights reserved.

3. After you add the Cloud Security Connector feature, you must enter the following details.
   a. **Tunnel Destination**: Enter the primary public destination IP that was assigned by the Zscaler team.
   b. **Ping Source CIDR**: Enter the internal router IP and mask in CIDR format that was assigned by the Zscaler team.
   c. **Ping Destination IP**: Enter the internal ZIA Public Service Edge IP that was assigned by Zscaler. Aryaka uses ICMP probing by default to decide the health of the tunnel.
   d. **Enable IP SLA**: (Optional) The default is **No**. By using HTTP GET in IP SLA, probes are sent towards Zscaler that traverse its full application stack. Zscaler recommends that if you choose to enable IP SLA, do so with the following settings:
      - **HTTP Destination IP**: Set as the internal ZIA Public Service Edge IP provided by Zscaler.
      - **HTTP Get URL**: gateway.<zscaler_cloud>.net/vpntest. To find the zscaler_cloud name, see What Is My Cloud Name for ZIA? (government agencies see What Is My Cloud Name for ZIA?).

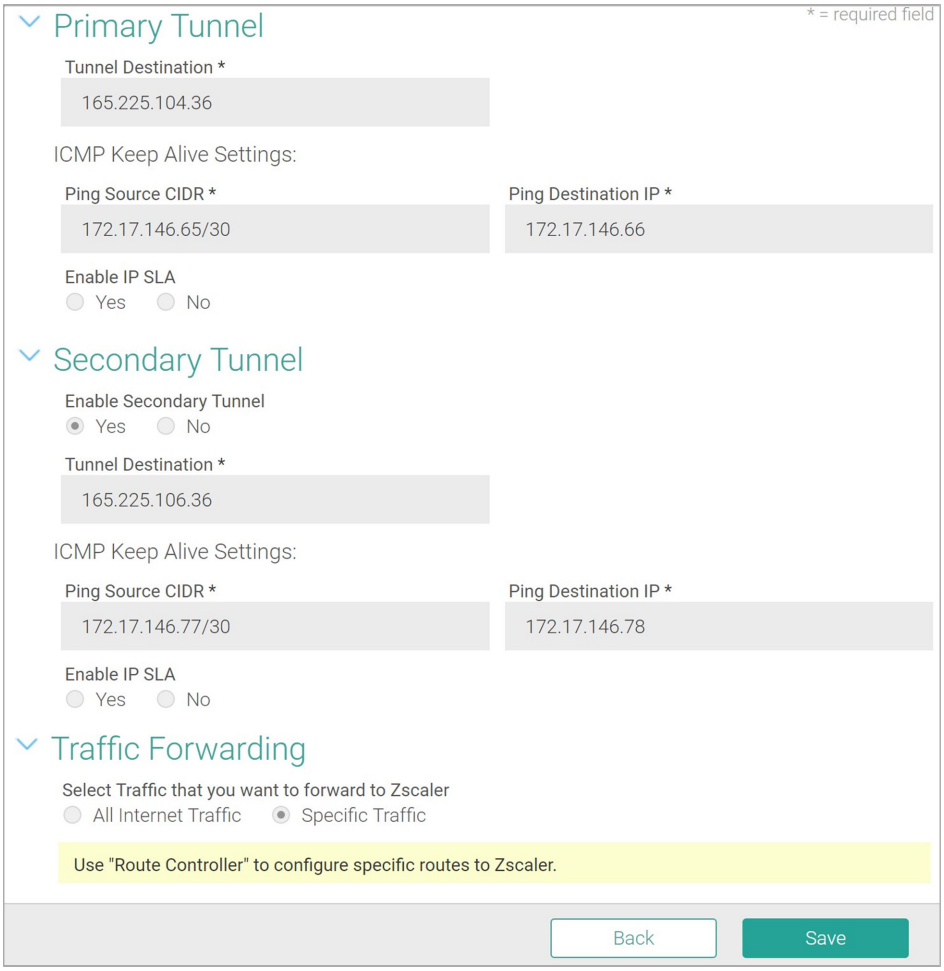

Figure 4. Tunnel Configuration

When service monitoring is down, the primary tunnel will failover to the backup tunnel. When monitoring becomes available again, the service switches back to the primary tunnel. By default, Aryaka drops packets on both tunnel failure and if traffic is destined to private subnet. You can modify these settings in the Advanced mode.

©2024 Zscaler, Inc. All rights reserved.

Traffic Forwarding

With an ANAP in Simple Routed Mode, all traffic that is not destined to the Aryaka POP is routed to the Zscaler Tunnel (Z-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 is inserted into the Route Controller under the Default Routes section for convenience.

If you choose to route only a specific route or routes, you must program the routes in the Router Controller section. Zscaler recommends that you edit Default Routes to control forwarding and not override routes. The override routes take precedence over any Aryaka-destined traffic and can also cause the Site-to-Site traffic to go to Zscaler.

The following figures show a snapshot of the Route Controller feature:

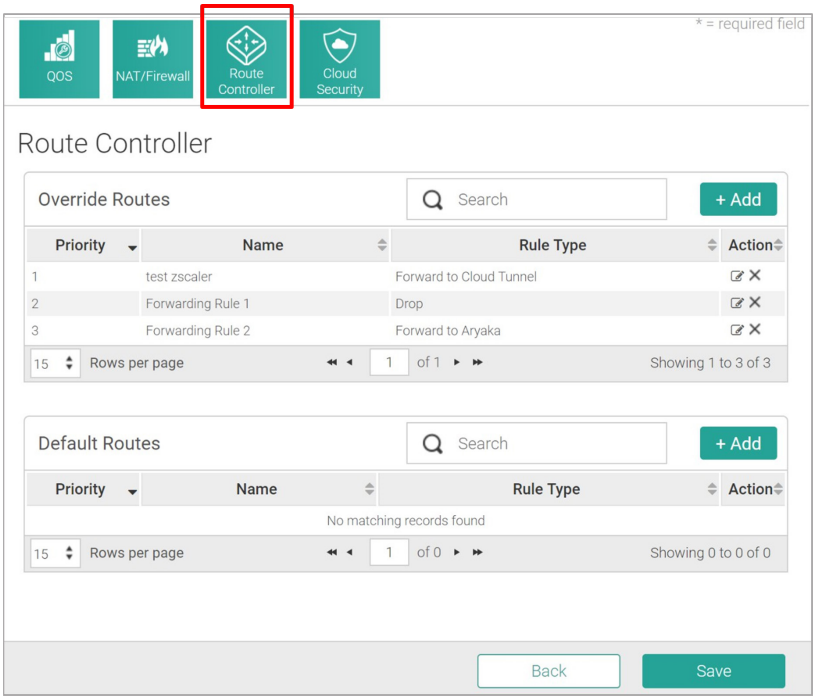

Figure 5. Route Controller

The following figure shows route editing options.

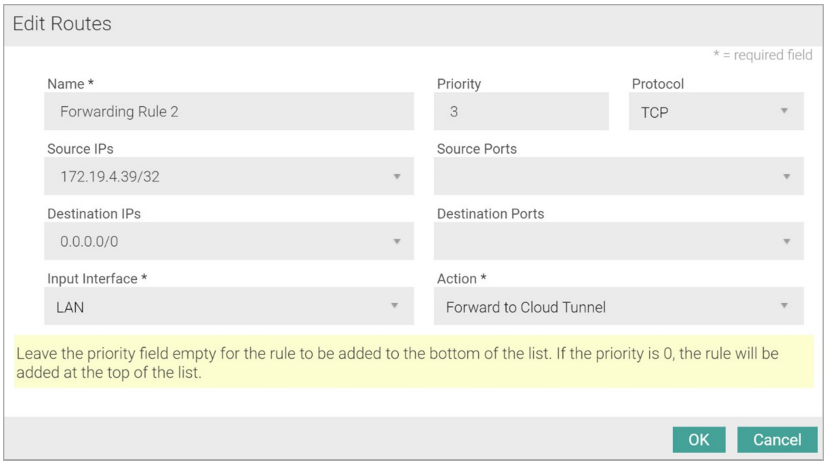

Figure 6. Edit Routes

©2024 Zscaler, Inc. All rights reserved.

MyAryaka Visibility

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

Monitoring Traffic

To monitor Zscaler traffic, go 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 matches Total Internet traffic. The following figure shows a sample graph of traffic data for a site.

Figure 7. Sample traffic graph

©2024 Zscaler, Inc. All rights reserved.

Zscaler Traffic

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

The following figure shows the bi-directional traffic carried by each tunnel and are useful in determining which tunnel is being used to carry traffic.

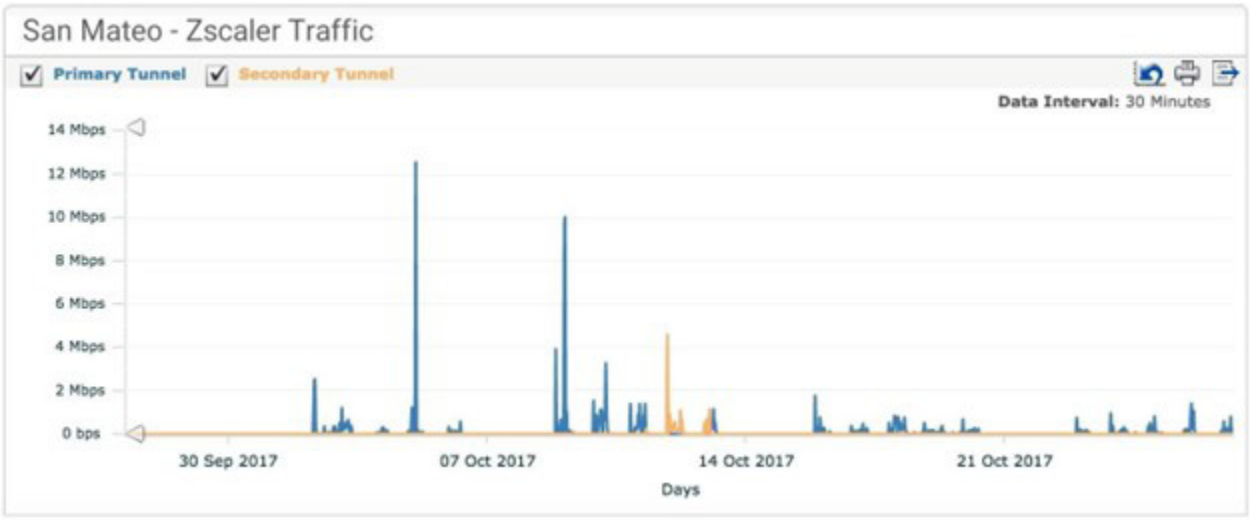

Figure 8. Zscaler traffic

Zscaler Received

The following figure shows all traffic received on the GRE tunnels to Zscaler. This represents all internet traffic inbound to the site from Zscaler.

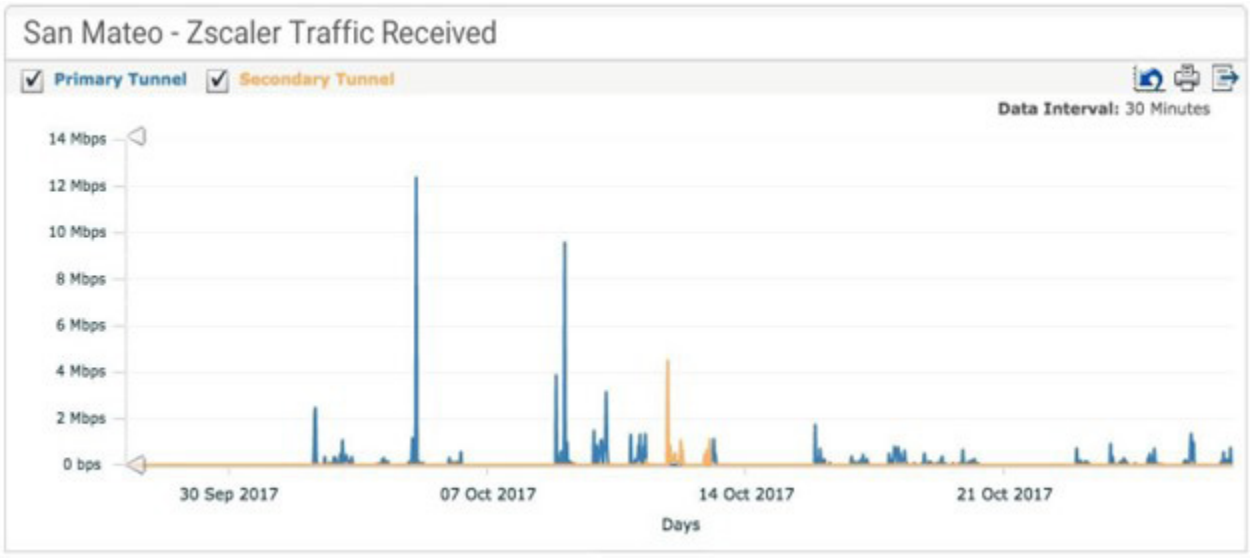

Figure 9. Zscaler traffic received

©2024 Zscaler, Inc. All rights reserved.

Zscaler Transmitted

The following figure shows all traffic that is transmitted on GRE tunnels to Zscaler. This represents all traffic outbound to Zscaler from the site.

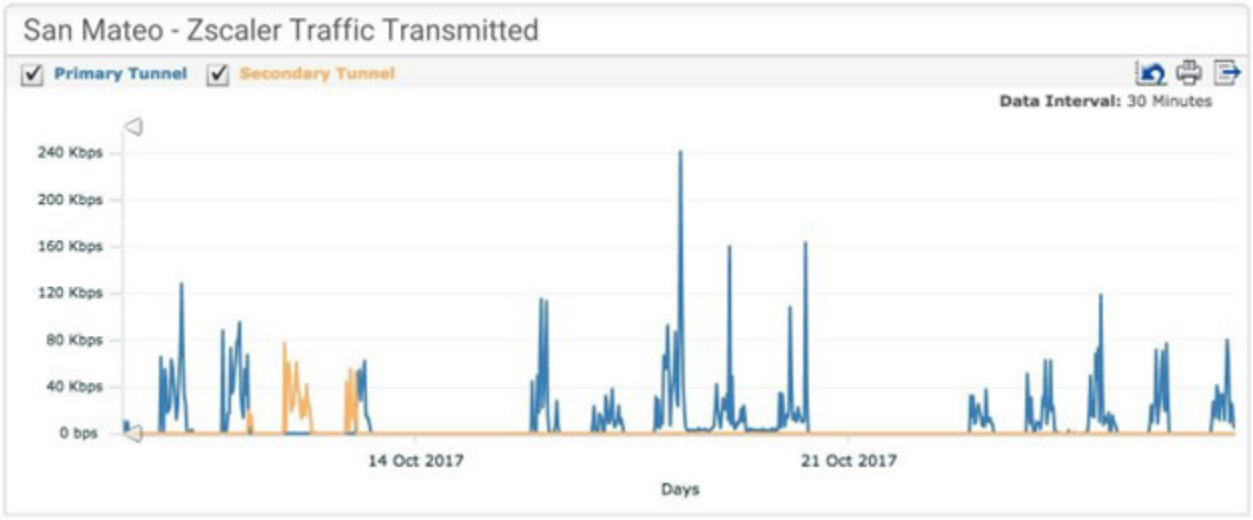

Figure 10. Zscaler traffic transmitted

©2024 Zscaler, Inc. All rights reserved.

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 IP SLA to fetch a file that was configured to be downloaded. This includes DNS resolution time, Connect time, Request time, etc.
- **Fail Count**: This line represents any failures to run IP SLA probe. Failure could be caused by any reason such as connectivity issues, configuration issues, etc.

The following figure depicts a sample Health graph for a site.

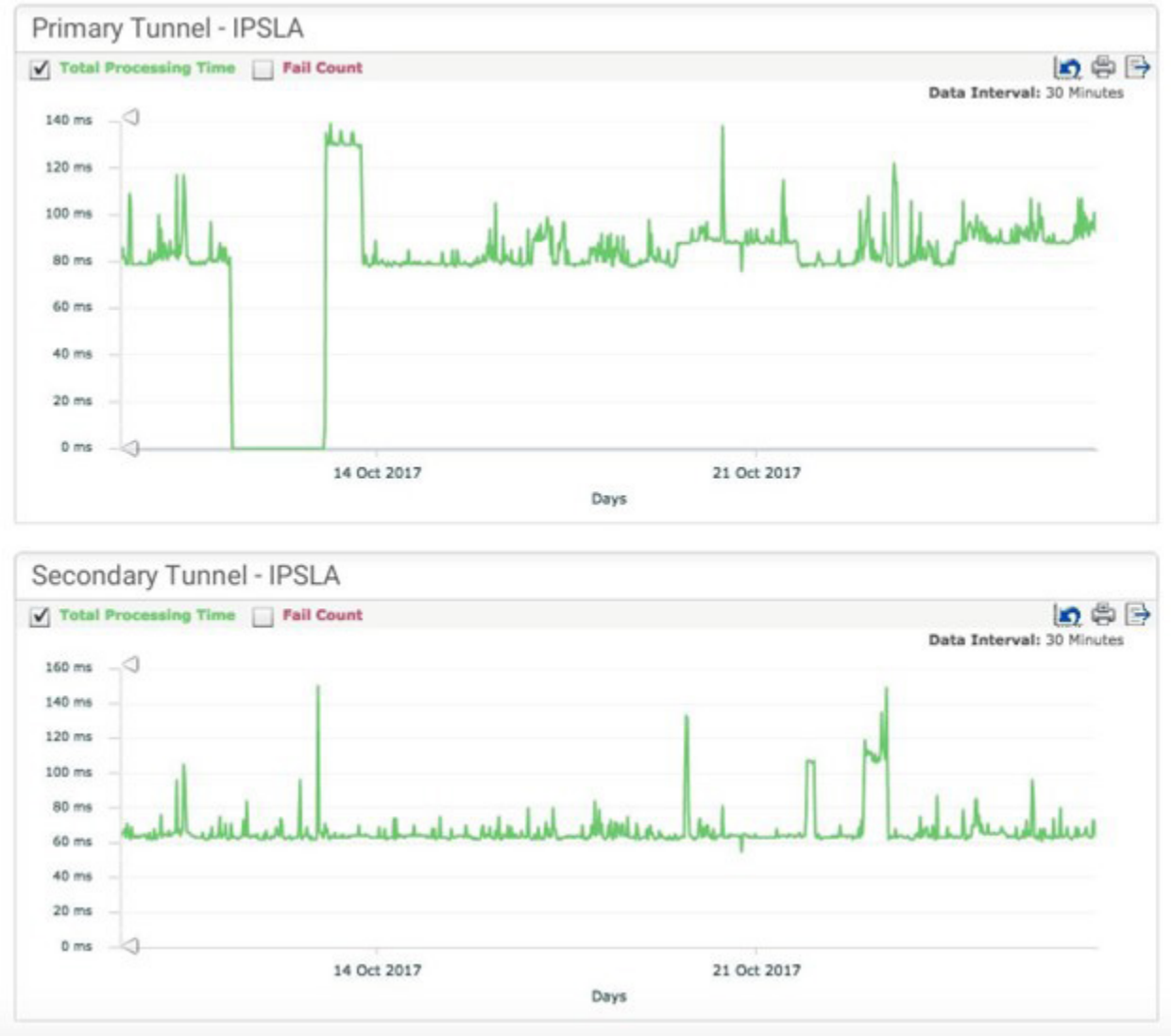

Figure 11. Health graph

©2024 Zscaler, Inc. All rights reserved.

Status

You can determine the status of GRE tunnels by going to the Status Cloud Security Connector. Availability of a GRE tunnel (up/down) is determined using ICMP probing. IP SLA-based probing if configured is used to determine the active state of the tunnel. The following figure 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. Status

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

©2024 Zscaler, Inc. All rights reserved.

Verifying ZIA Configuration

The following describes how to verify the ZIA configuration.

Request Verification Page

Go to https://ip.zscaler.com to validate if you are transiting ZIA. The following figure displays the message when users are not transiting ZIA.

Figure 13. Not transiting ZIA

The following figure shows that you are transiting ZIA.

Figure 14. Transiting ZIA

©2024 Zscaler, Inc. All rights reserved.

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

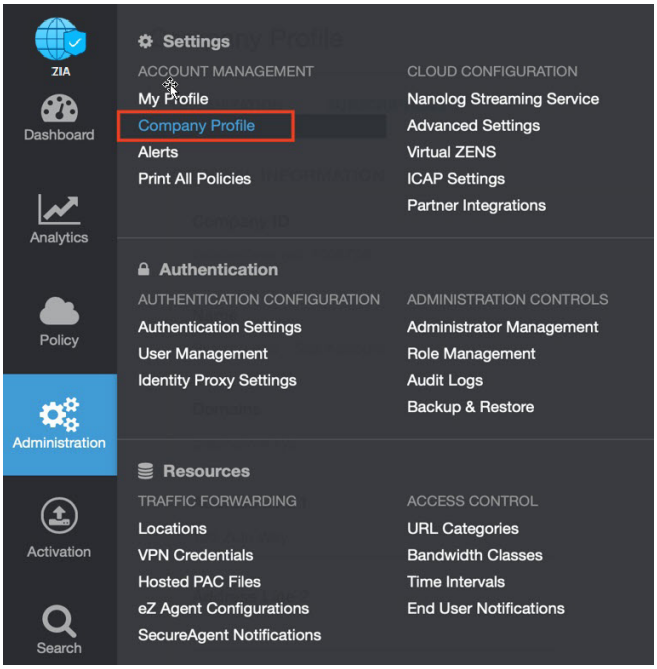

Figure 15. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

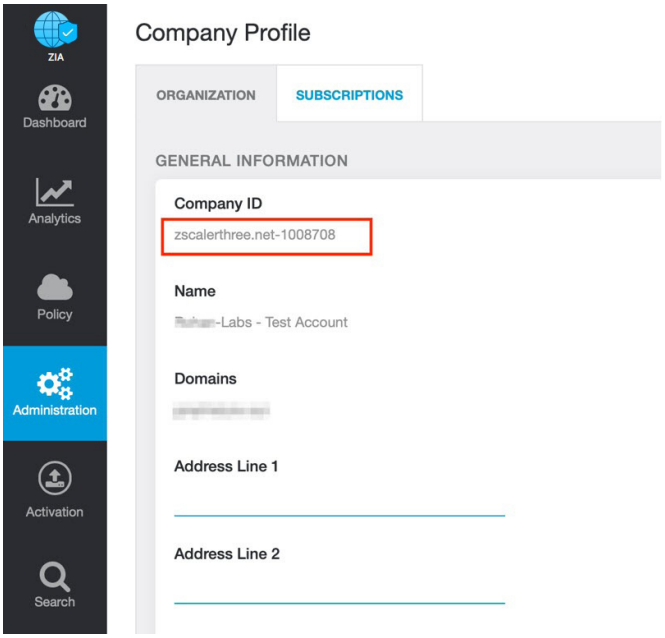

Figure 16. Company ID

©2024 Zscaler, Inc. All rights reserved.

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

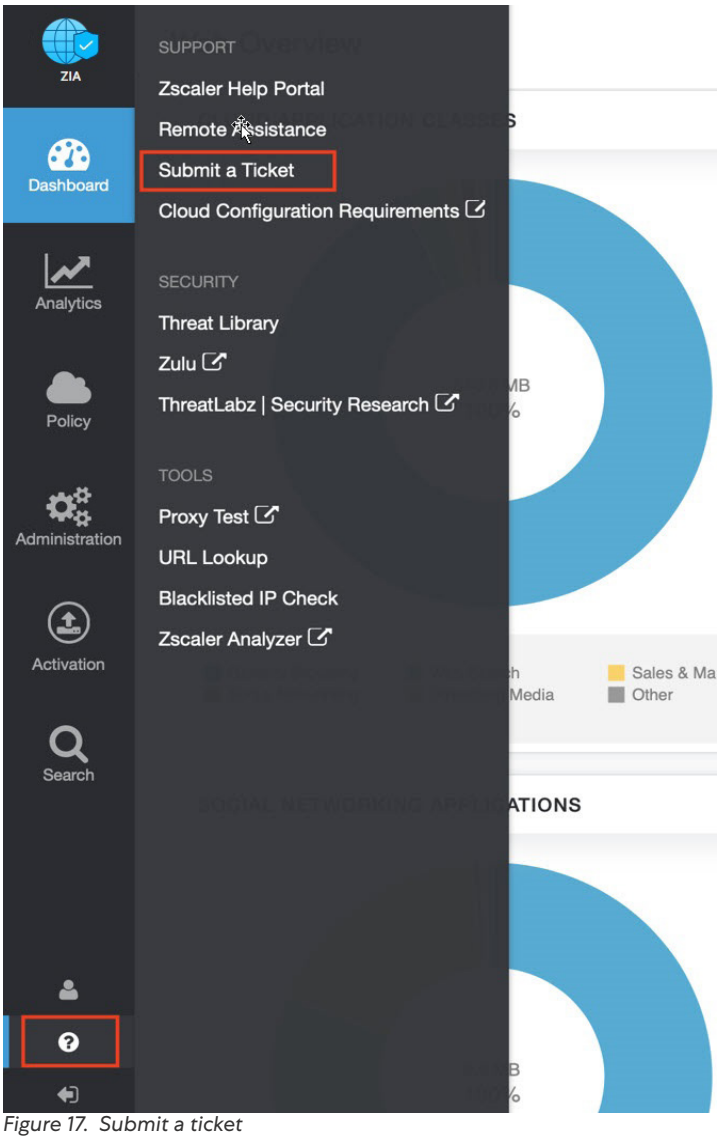

Figure 17. Submit a ticket

©2024 Zscaler, Inc. All rights reserved.