# ZSCALER AND EXTREME NETWORKS DEPLOYMENT GUIDE

OCTOBER 2023, VERSION 1.1

BUSINESS DEVELOPMENT GUIDE

# Contents



 

 

# 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 |
|---|---|
| CA | Central Authority (Zscaler) |
| 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) |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol Security (RFC2411) |
| PFS | Perfect Forward Secrecy |
| PSE | Public Service Edge |
| PSK | Pre-Shared Key |
| SSL | Secure Socket Layer (RFC6101) |
| TLS | Transport Layer Security |
| VDI | Virtual Desktop Infrastructure |
| WSG | Web Security Gateway |
| XFF | X-Forwarded-For (RFC7239) |
| ZBF | Zone-Based Firewall |
| ZCP | Zscaler Cloud Protection (Zscaler) |
| ZDX | Zscaler Digital Experience (Zscaler) |
| ZIA | Zscaler Internet Access (Zscaler) |
| ZPA | Zscaler Private Access (Zscaler) |

 

# 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.

## Extreme Networks Overview

Extreme Networks (NASDAQ: EXTR) is committed to making networking effortless—advancing how we live, work, and share. Over 50,000 customers in 80+ countries trust Extreme's end-to-end, cloud-driven networking solutions and rely on its top-rated services and support to accelerate digital transformation efforts and deliver progress like never before. To learn more, refer to the Extreme Networks 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
- Extreme Networks Resources
- Appendix A: Requesting Zscaler Support

## Software Versions

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

## Prerequisites

This guide provides GUI examples for configuring ZIA and ExtremeCloud SD-WAN. All examples in this guide presume that the reader has a basic comprehension of IP networking. All examples in this guide explain how to provision new services with Zscaler and with ExtremeCloud SD-WAN. The prerequisites to use this guide are:

- ZIA
  - A working instance of ZIA (any cloud)
  - Administrator login credentials
- ExtremeCloud SD-WAN Portal
  - A working tenant on the ExtremeCloud SD-WAN Portal, with administrator login credentials
  - One or more ExtremeCloud SD-WAN appliances online and working

 

## 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.

 

# Zscaler and Extreme Networks Introduction

Overviews of the Zscaler and Extreme Networks 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. |

 

## ExtremeCloud SD-WAN Overview

ExtremeCloud SD-WAN helps you become an Infinite Enterprise, enabling your employees, customers, and partners access to applications regardless of location while removing complexity from the network.

ExtremeCloud SD-WAN unifies networking and security operations through simple-to-use management seamlessly integrated into ExtremeCloud. With ExtremeCloud SD-WAN, you can securely connect your sites—branch, campus, data center—to each other and the cloud while optimizing application performance.

ExtremeCloud SD-WAN is an all-inclusive subscription-based solution, providing:

- Superior economics: Reduce total cost of ownership (TCO).
- Unified management for your wired, wireless, and SD-WAN network and secure networking to protect users and applications.
- Exceptional application performance.
- Continuous support to help you achieve strategic goals and targeted business outcomes.

## Extreme Networks Resources

The following table contains links to Extreme Networks support resources.

| Name | Definition |
|---|---|
| Extreme Networks Product Documentation | Online help for Extreme Networks products. |
| Extreme Networks Support | Online support requests for Extreme Networks. |
| Extreme Networks Community | Online community for Extreme Networks products. |

 

# About This Guide

This guide explains how to configure ZIA and ExtremeCloud SD-WAN to secure traffic from a branch site equipped with an SD-WAN appliance to the internet by redirecting traffic to ZIA Public Service Edges via IPSec IKEv2 VPN tunnels.

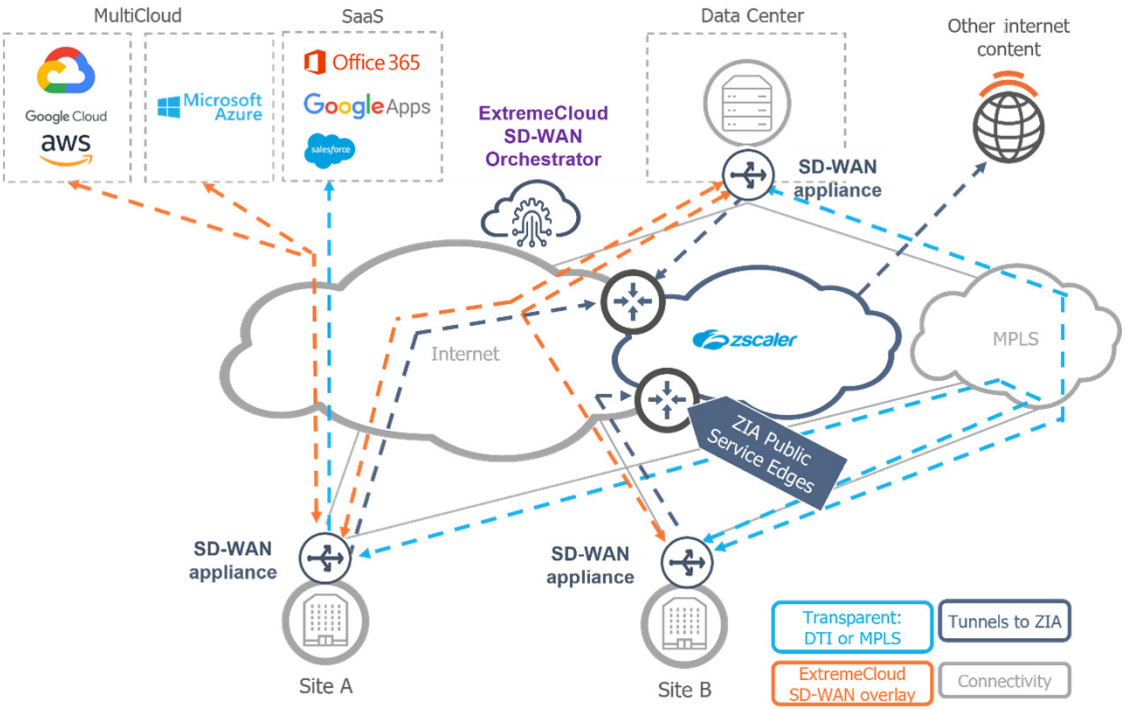


*Figure 1. ZIA and ExtremeCloud SD-WAN*

## Topology

This guide uses a simplified topology that includes:

- A site with internet access and an SD-WAN appliance in Router mode deployed between the LAN hosts and the internet customer premises equipment (CPE).
- SD-WAN appliance policy-based IPSec IKEv2 VPN tunnels to a pair of ZIA Public Service Edges.

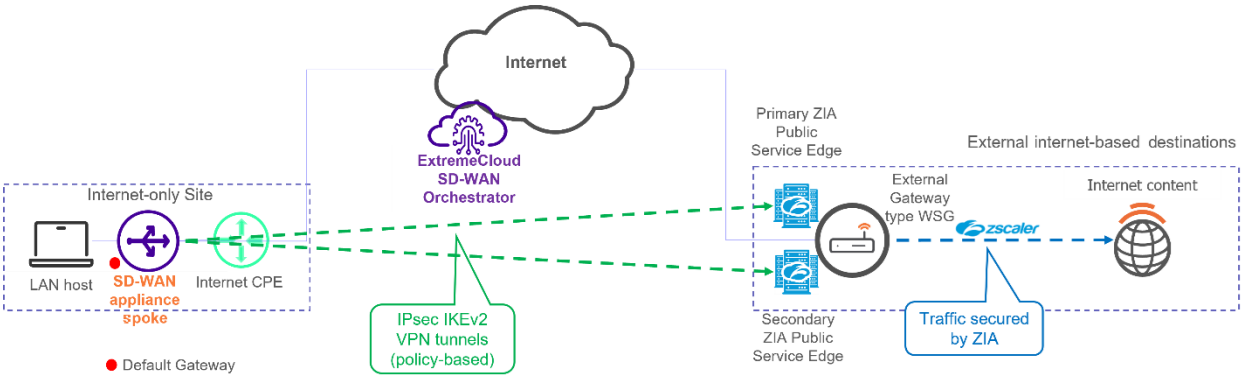


*Figure 2. Test topology*

 

# Configuring ZIA

This section demonstrates all the steps required to configure IPSec VPN tunnels from a branch site to ZIA, which include:

- Creating a VPN credential
- Configuring a location
- Locating the Zscaler data centers

All procedures require you to be logged in to the ZIA Admin Portal as a user with administrator permissions.

## Creating a VPN Credential

Log in to the ZIA Admin Portal as an administrator.

### FQDN-based VPN Credential

Define a VPN credential for the IKE negation process in ZIA. The VPN credential is required to create a Location:

1. Go to **Administration** > **Resources** > **VPN Credentials**.

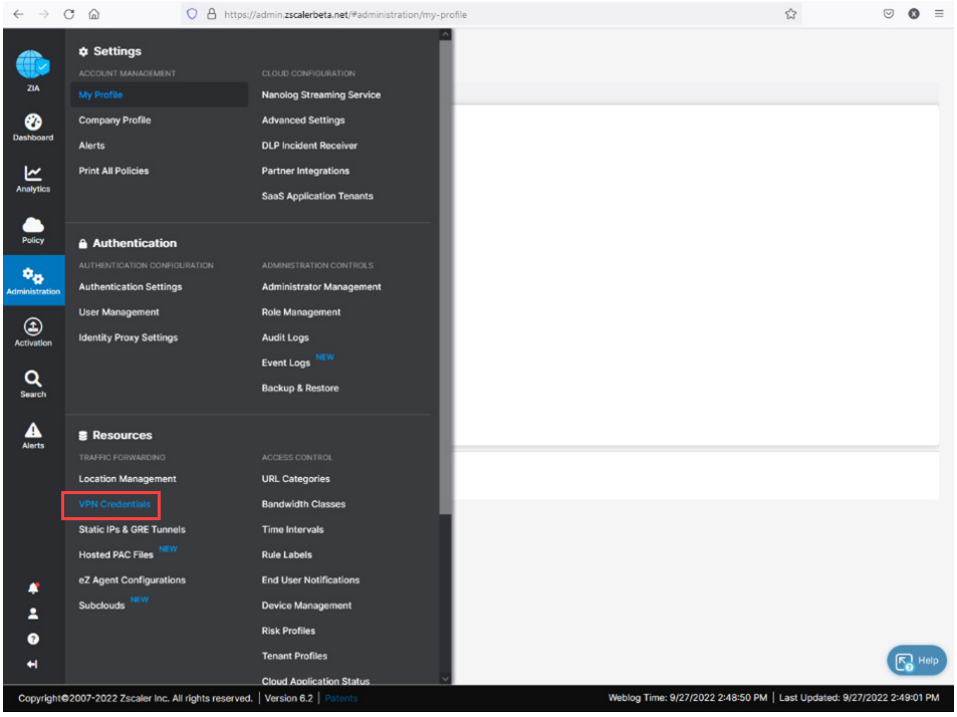


*Figure 3. VPN Credentials*

2. Click **Add VPN Credential**.

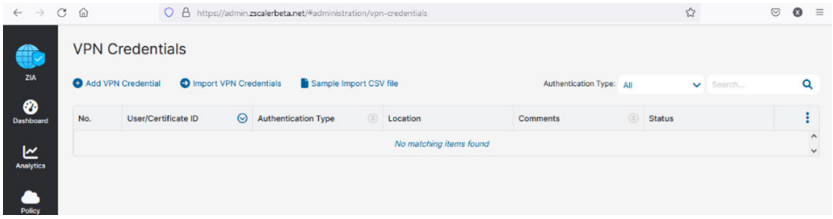


*Figure 4. Add VPN Credential*

3. Complete the following fields to add the VPN credential:
   a. In the **Authentication Type** field, select **FQDN**.
   b. In the **User ID** field, enter a unique user ID.
   c. In the **New Pre-Shared Key** and **Confirm New Pre-Shared Key** fields, enter the key.
   d. Select **Save**.

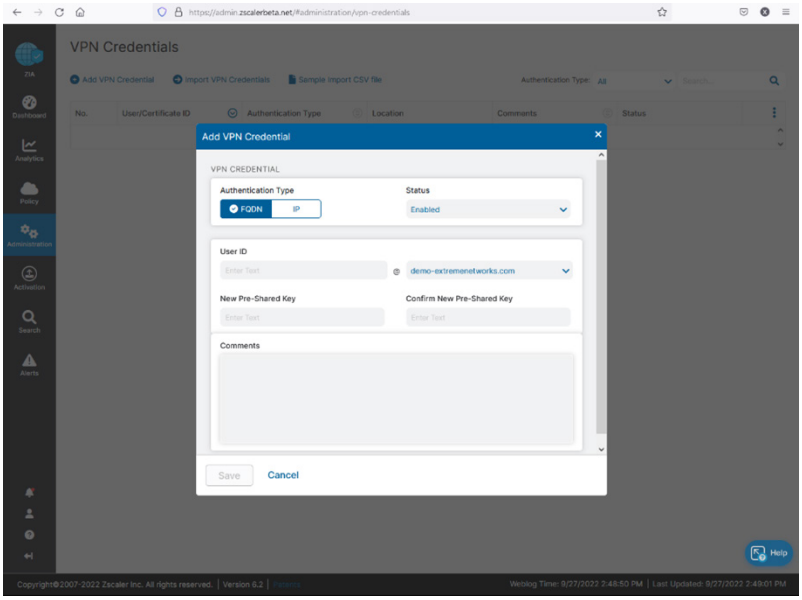


*Figure 5. Define the VPN credential*

The new VPN credential is displayed on the VPN Credentials page.

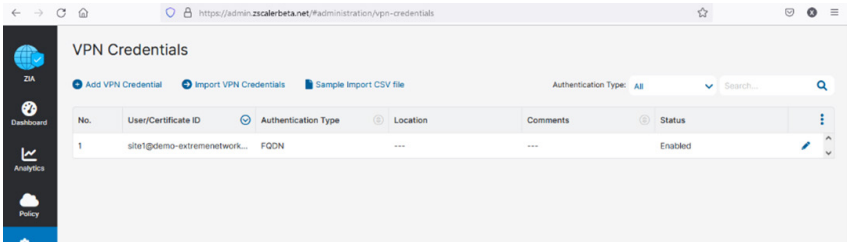


*Figure 6. VPN credential created*

 

## Configuring a Location

Next, create a location representing a physical site in ZIA:

1. Go to **Administration** > **Resources** > **Location Management**.

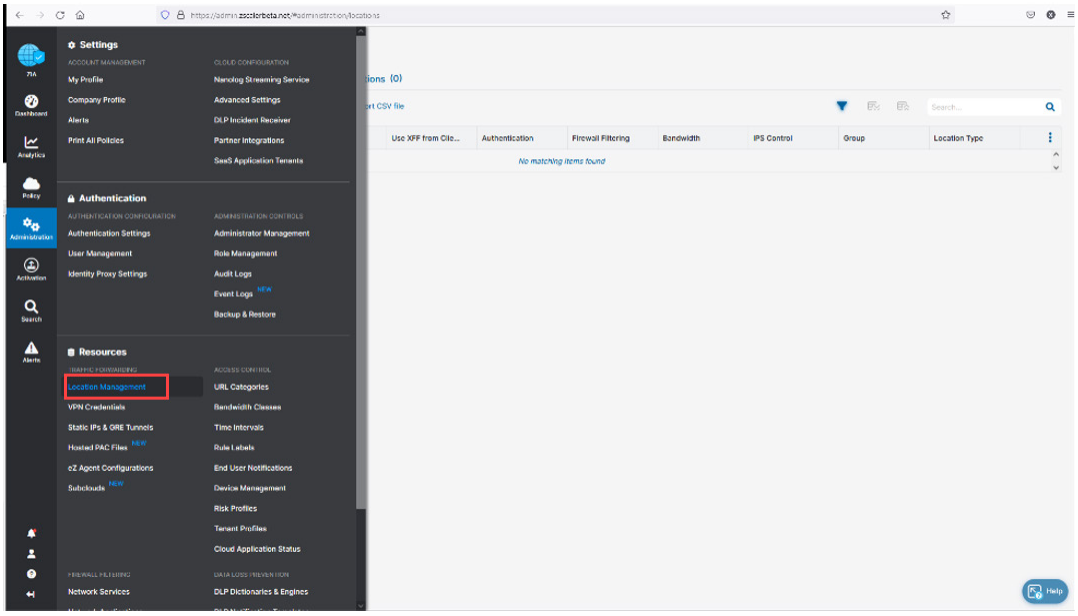


*Figure 7. Location Management*

2. Click **Add Location**.

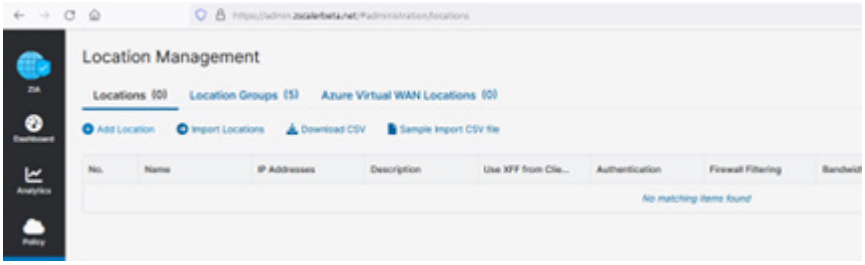


*Figure 8. Add Location*

 

3. Define the new **Location**:
   a. Enter the location **Name** (use the same name as the site name in the ExtremeCloud SD-WAN Portal).
   b. Select the **Country**.
   c. Enter the **City/State/Province** info.
   d. Select the **Time Zone**.
   e. Select the **Manual Location Groups** or select the **Exclude from Manual Location Groups** option. To learn more, see About Location Groups (government agencies, see About Location Groups).
   f. Select the **Location Type**.
   g. (Optional) Enter a **Description** of the location.
   h. In the **Static IP Addresses** and **GRE Tunnels** field, select **None**.
   i. In the **VPN Credentials** field, select the FQDN you defined in Create an FQDN-based VPN Credential.
   j. Define the **Gateway Options**.
   k. Select **Save**.

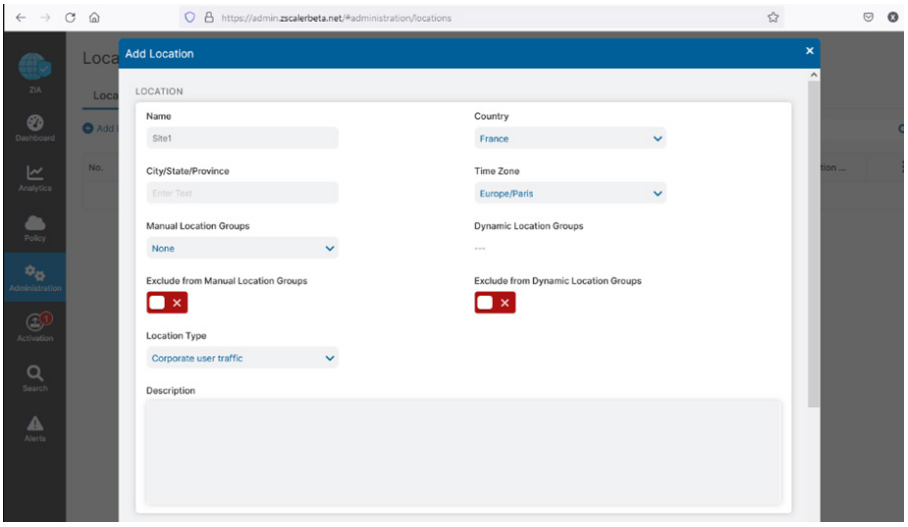


*Figure 9. Add Location (first part)*

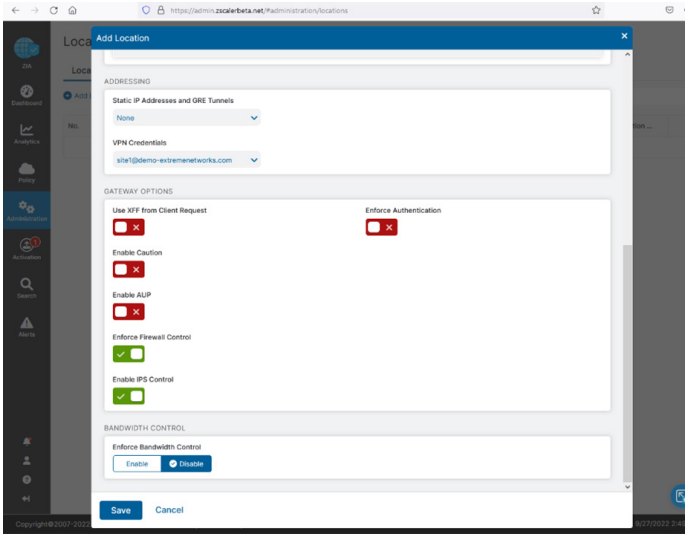


*Figure 10. Define Location (second part)*

 

The new location is displayed on the Location Management page.

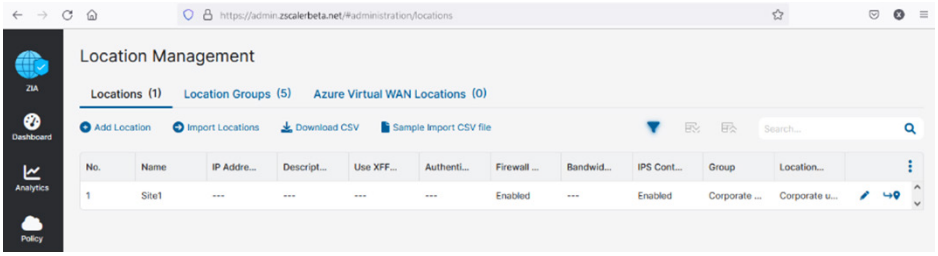


*Figure 11. Location created*

## Configure Sub-Locations

To perform this optional step, see the following ZIA documents:

- Understanding Sub-Locations (government agencies, Understanding Sub-Locations).
- Configuring Sub-Locations (government agencies, Configuring Sub-Locations).

## Activate the Configuration Changes

After you create the VPN credential and the location, activate the changes, which are queued.

Go to **Administration** > **Activate**.

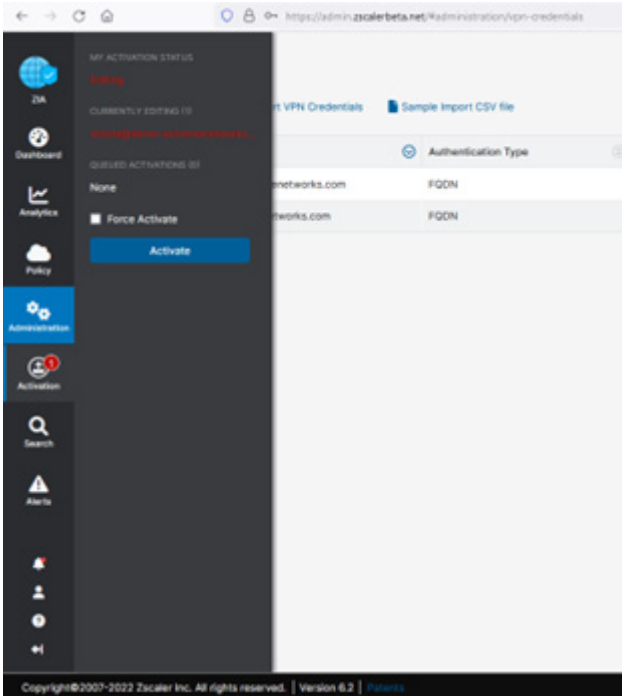


*Figure 12. Activate queued changes*

The configuration of ZIA is complete.

 

## Configuration for Sites with Redundancy

A different configuration is needed in each of the following scenarios:

- Several WAN interfaces of the same SD-WAN appliance (several ISPs) must connect to ZIA.
- Several WAN interfaces of different SD-WAN appliances on the same site (hardware redundancy) must connect to ZIA.

Review the following considerations that apply to the configuration in the ZIA Admin Portal:

- Only one Location object is needed to represent the whole site. See Configuring a Location.
- If a FQDN-based VPN credential is considered, then only one VPN credential is needed for all the WAN interfaces of this site. See FQDN-based VPN Credential.

 

# Configuring XD SD-WAN

This section demonstrates the steps for configuring ExtremeCloud SD-WAN to set up IPSec VPN tunnels from a branch site to ZIA:

- Defining an External Gateway of type WSG.
- Setting up tunnels to the External Gateway.

For all procedures, you must log in to ExtremeCloud SD-WAN Portal as a user with permissions in the Network section.

## Locating the Zscaler Data Centers

To locate the Zscaler data centers:

1. Log in to ExtremeCloud SD-WAN Main Menu with a user that has permissions in the Network section.
2. Before properly configuring ExtremeCloud SD-WAN, identify the ZIA Public Service Edges that are the most relevant to the site.

For more information, see Locating the Host Names and IP Addresses for ZIA Public Service Edges (government agencies, see Locating the Host Names and IP Addresses for ZIA Public Service Edges).

As a result, two VPN host names are selected and the corresponding IP addresses are looked up.

For this guide, locations Frankfurt IV and Washington DC are selected after looking at the URL (government agencies, see looking at the URL).

The corresponding VPN host names and their IP addresses are:

- fra4-vpn.zscalerbeta.net (165.225.72.38)
- was1-vpn.zscalerbeta.net (104.129.194.38)

Regular Location | Regional Surcharge | Multi-cluster VIP | Auto Geo Proximity Enabled | Not Ready for Use | No New Provisioning

| Location | IP Address (CIDR Notation) | Proxy Hostname | GRE Virtual IP | SVPN Virtual IP | VPN Host Name | Notes |
|---|---|---|---|---|---|---|
| EMEA | Copy IPs | | | | | |
| Frankfurt IV | 165.225.72.0/22 | fra4.sme.zscalerbeta.net | 165.225.72.38 | | fra4-vpn.zscalerbeta.net | |
| Americas | Copy IPs | | | | | |
| San Francisco IV | 199.168.148.0/23 | sunnyvale1.sme.zscalerbeta.net | 199.168.148.131 | | sunnyvale1-vpn.zscalerbeta.net | |
| | 2605:4300:1211::/48 | | | | | Not Ready for Use |
| | 2605:4300:1212::/48 | | | | | Not Ready for Use |
| | 2605:4300:1214::/48 | | | | | Not Ready for Use |
| | 2605:4300:1213::/48 | | | | | Not Ready for Use |
| Washington DC | 104.129.194.0/23 | was1.sme.zscalerbeta.net | 104.129.194.38 | | was1-vpn.zscalerbeta.net | |

*Figure 13. Select ZIA Public Service Edges from ExtremeCloud SD-WAN*

 

## Defining an External Gateway

Define an external Secure Web Gateway. In this procedure, the policy-based VPN IPSec tunnels are set up to the endpoints (hostnames) that you identified when you located the Zscaler data centers.

1. In the ExtremeCloud SD-WAN Main Menu, go to **Settings** > **Policy Configuration** and select **View all** in the **Security** panel.

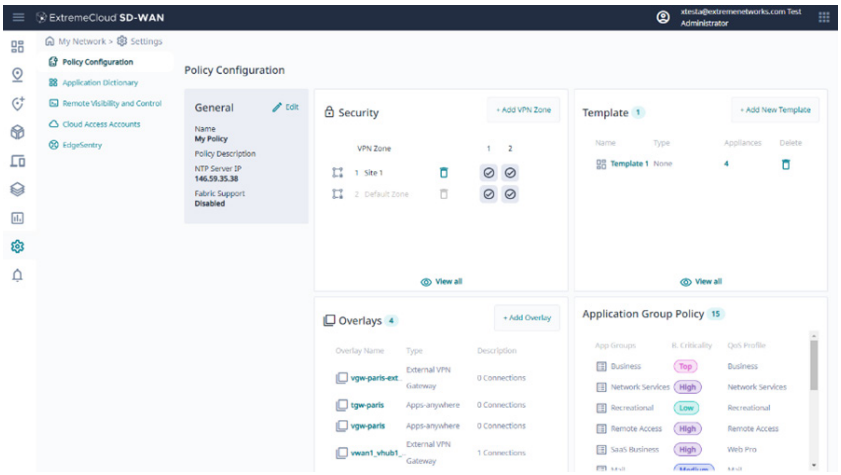


*Figure 14. Go to Security Configuration*

2. Select the **Secure Web Gateway** tab and click **Add External SWG**.

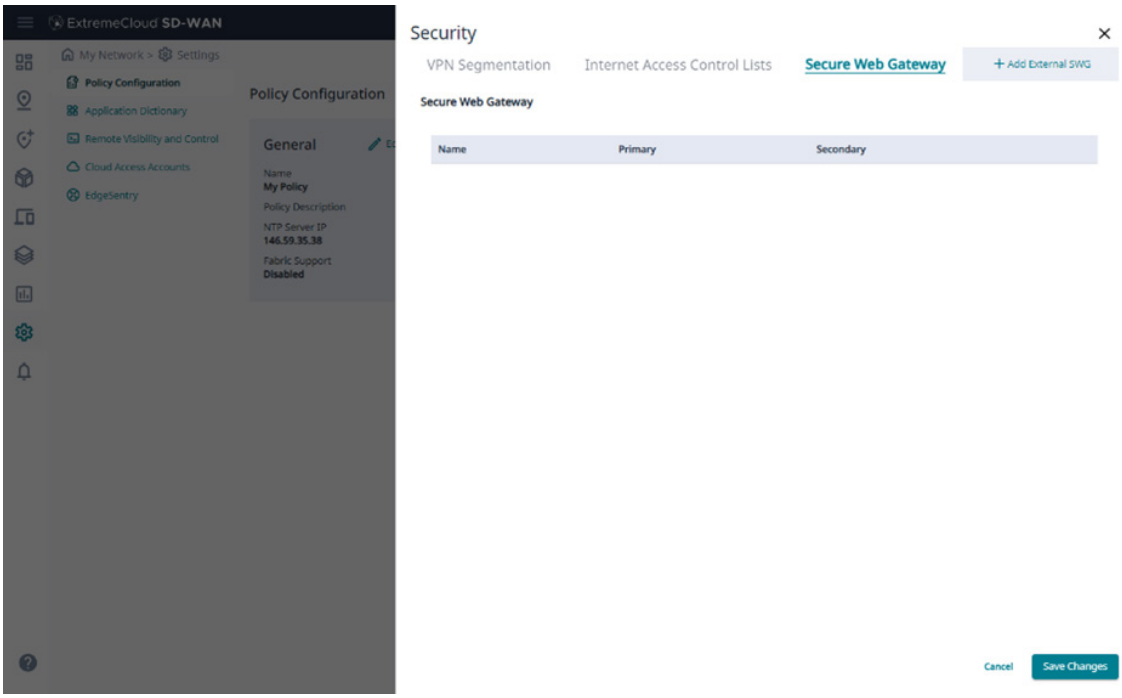


*Figure 15. Add External SWG*

 

3. Define the **New External SWG**:
   a. In the **Name** field, enter a descriptive name for the gateway.
   b. In the two **Public IP Address** fields, enter the IP addresses you identified when you located the Zscaler data centers.
   c. For the parameters in the IKE policy and IPSec policy sections, select values that are supported by ZIA. Zscaler recommends the values shown in the following image. For more information, see Understanding IPSec VPNS (government agencies, see Understanding IPSec VPNS).
   d. In the **MTU** field, enter `1400`.
   e. In the **Default Pre-Shared Key** field, enter the same pre-shared key that you entered when you defined the VPN credential. For more information, see FQDN-based VPN Credential.
   f. Click **Save Changes**.

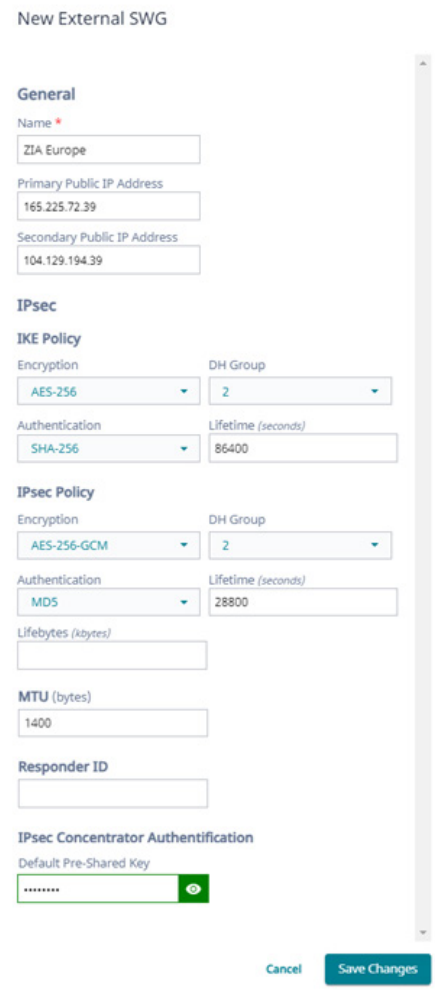


*Figure 16. Define External Gateway*

 

The new gateway is displayed in the list of Secure Web Gateways.

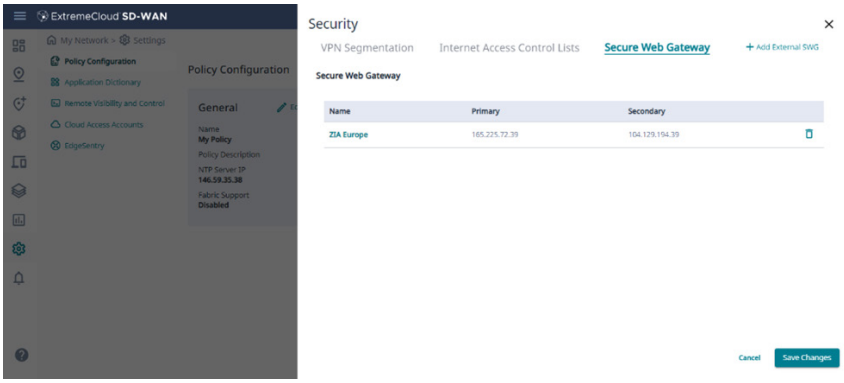


*Figure 17. External Secure Web Gateway created*

## One External Gateway Used by Multiple Sites

You can define an External Gateway in ExtremeCloud SD-WAN and use it multiple times if several SD-WAN appliances (and sites) must connect to the same pair of ZIA Public Service Edges (VPN host names).

The typical case is a pair of VPN host names identified as relevant for a geographic region, with multiple sites (and appliances) in this region. One External Gateway is then defined (using the IP addresses of the pair of VPN host names) in ExtremeCloud SD-WAN and used multiple times as the destination for tunnels from the several sites of that region.

- If the VPN credentials of the ZIA Location objects corresponding to these sites share the same Pre-Shared Key, then this Pre-Shared Key is set on the External Gateway and skipped when defining the tunnels.
- If the VPN credentials of the ZIA Location objects have different Pre-Shared Keys, then there is no need to define it on the External Gateway. Instead, the Pre-Shared Keys are set while defining the tunnels.

To learn more, see Validating, Supervising, and Troubleshooting.

 

## Setting Up Tunnels to the External Gateway

Define the tunnels to the previously created External Gateway.

1. In the ExtremeCloud SD-WAN Main Menu, go to **Network** > **Configuration** and update the targeted **SD-WAN Appliance**.

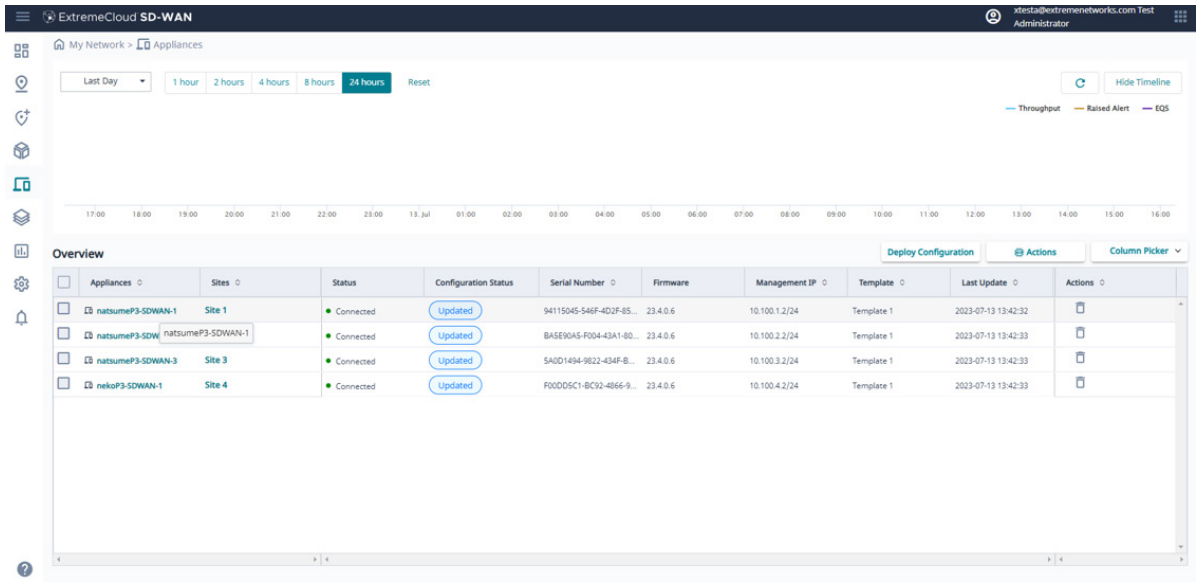


*Figure 18. Go to Appliances*

2. On the page of the selected appliance, click **Edit Configuration**.

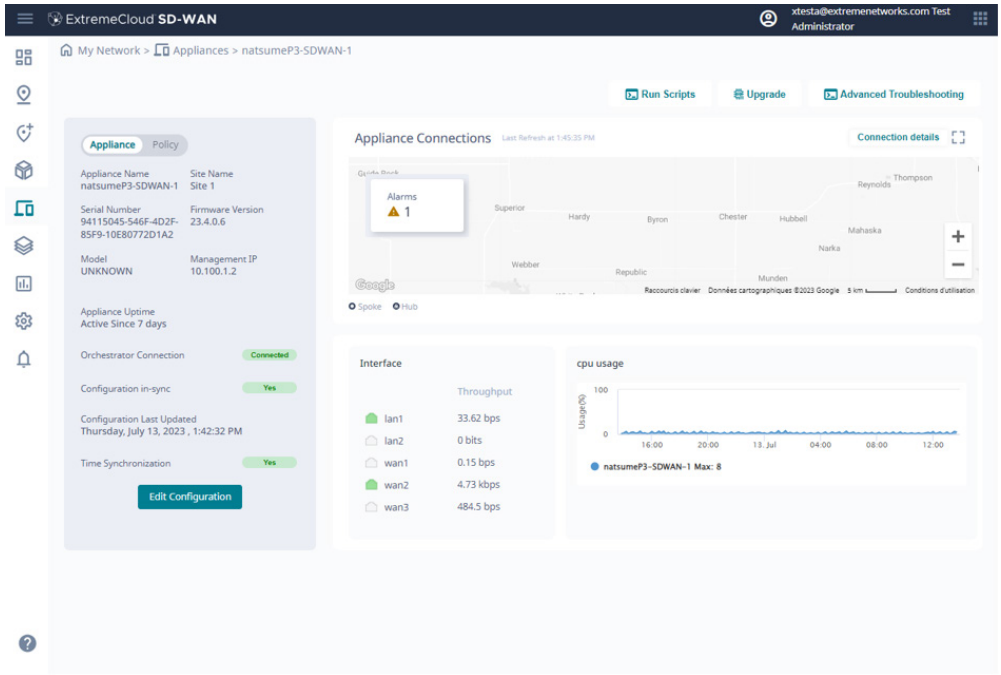


*Figure 19. Edit appliance configuration*

3. Select the **WAN** tab, display the WAN interface that you want to connect to ZIA, and go to the **Security Gateway** panel.

 

4. In the **Security Gateway** panel, select the external SWG you created.

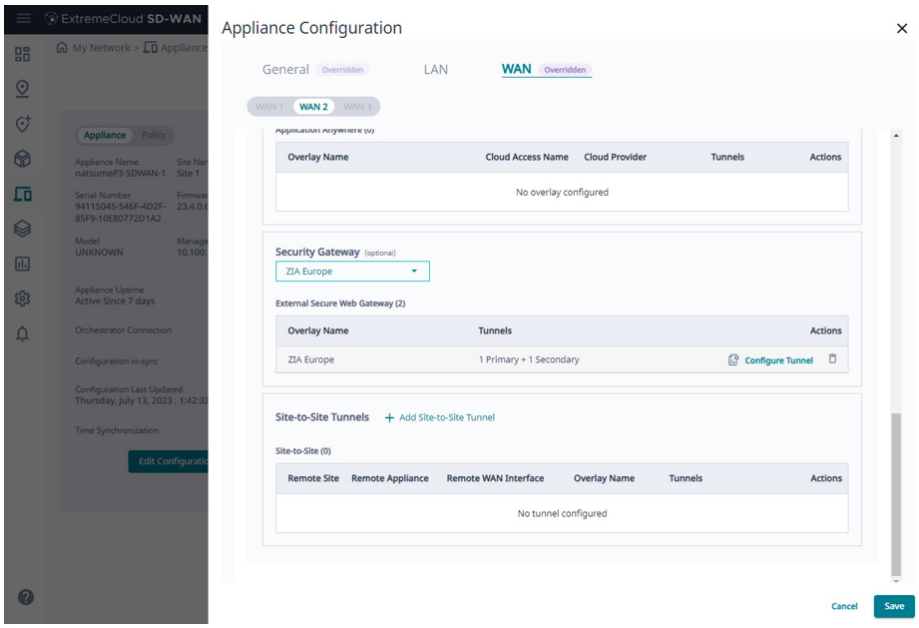


*Figure 20. Select the external SWG*

5. On the selected external SWG, click **Configure Tunnel** and define the details for the tunnels.
   a. In the **Initiator ID** field, enter the FQDN from the FQDN-based VPN Credential.
   b. For the **PSK** field, consider the items in One External Gateway Used by Multiple Sites. If the pre-shared key for the external gateway is the same as the key for the VPN credential, then leave the field blank. If the pre-shared key is different for the sites that use the gateway, then enter the pre-shared key here.
   c. Leave the **Inside Local IP** and **Inside Remote IP** blank. These fields do not apply to this procedure.

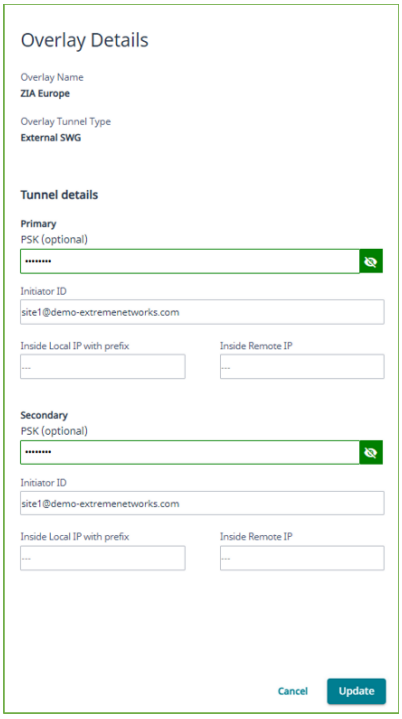


*Figure 21. Define Initiator ID and PSK*

 

6. Click **Update** to commit the changes.
7. Return to the **Appliance Configuration**, and select **Deploy Configuration**. The SD-WAN appliance receives the information to set up tunnels to ZIA.

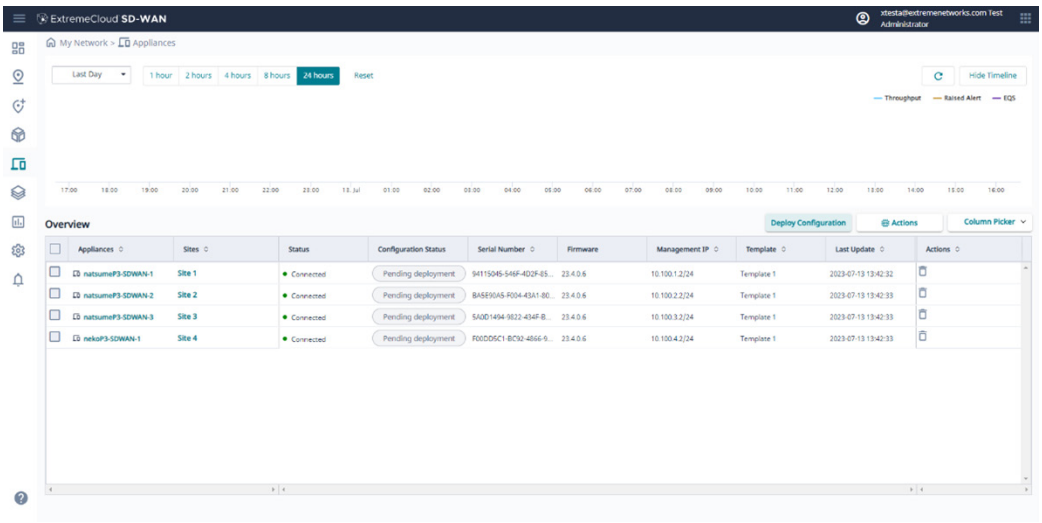


*Figure 22. Deploy Configuration*

 

## Configuring Internet Access Control Lists to Forward Traffic to ZIA

Take the following steps to ensure that the zone-based firewall correctly forwards internet traffic.

The Zone-Based Firewall might already be configured with several VPN zones, application sets, and internet policies. Your configuration steps depend on this pre-existing information. This procedure references a simple use case in which all internet traffic from a site is sent through ZIA Public Service Edges. Many other scenarios are possible, including (but not limited to) the following:

- Some users have internet traffic protected through ZIA and others are denied internet access.
- A Direct-to-Internet policy is applied to some applications sets (which is often recommended by business SaaS providers), and a WSG policy is applied to the rest of the internet.

1. In the ExtremeCloud SD-WAN Main Menu, go to **Settings** > **Policy Configuration** and select **View all** in the **Security** panel.
2. In the **VPN Segmentation** tab, select **Add VPN Zone**.

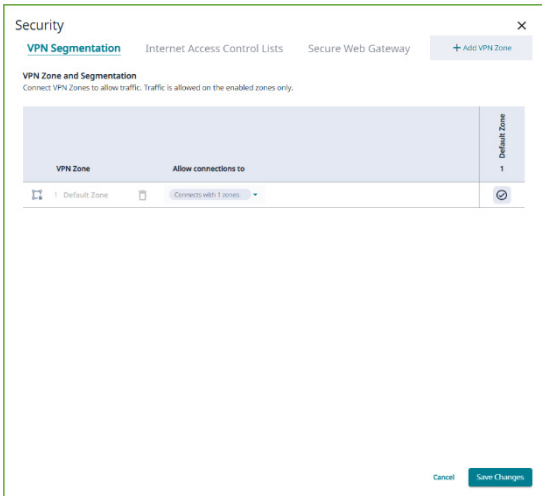


*Figure 23. Add VPN Zone*

 

3. Define a zone that corresponds to the entire site:
   a. In the **Name** field, enter a descriptive name for the zone.
   b. Set the **Priority** accordingly.
   c. Select the site from the **Sites** drop-down menu.
   d. Add all the site subnets.

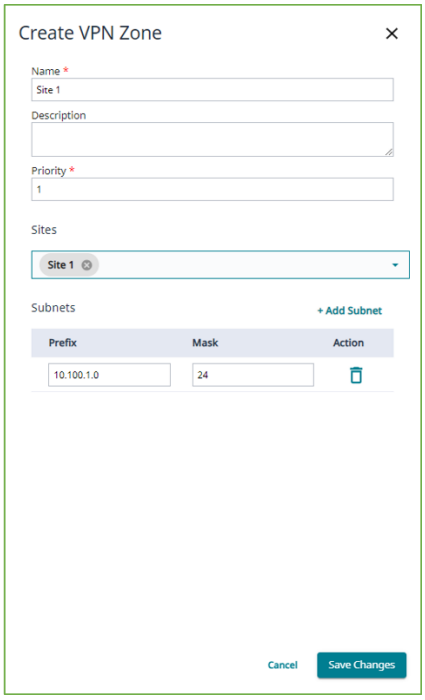


*Figure 24. Define the new zone*

4. Select **Save Changes** to commit the definition. The new zone is now visible in the **VPN Segmentation** tab.
5. Select the **Internet Access Control Lists** tab, where the new zone is also visible, including a default policy. In this example, the policy is **DENY**.

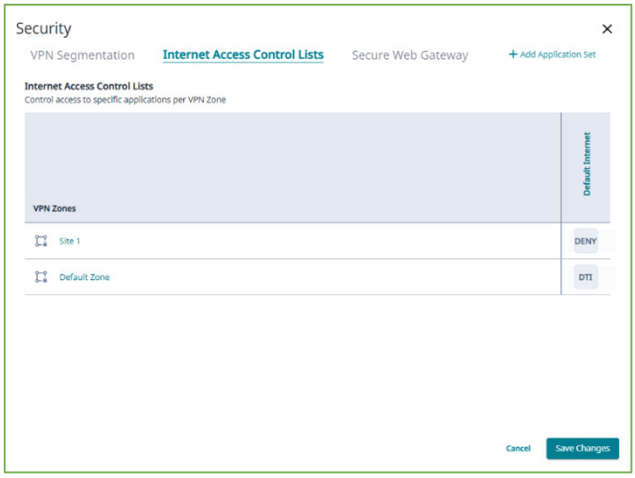


*Figure 25. New VPN zone and its default policy*

 

6. Select the default policy and choose **Secure Web Gateway** from the list.

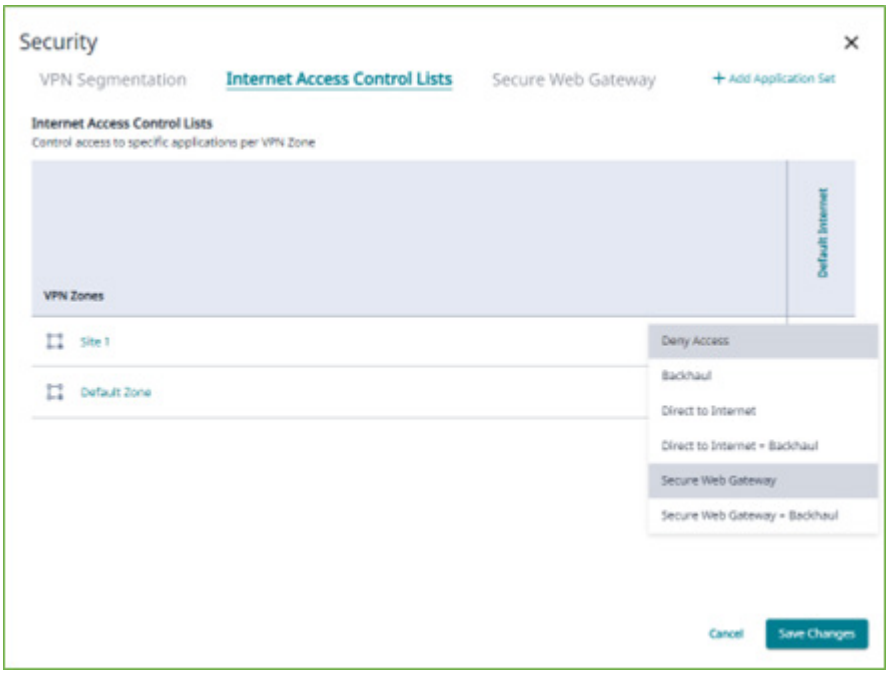


*Figure 26. Internet access policies*

Site 1 now shows as an SWG.

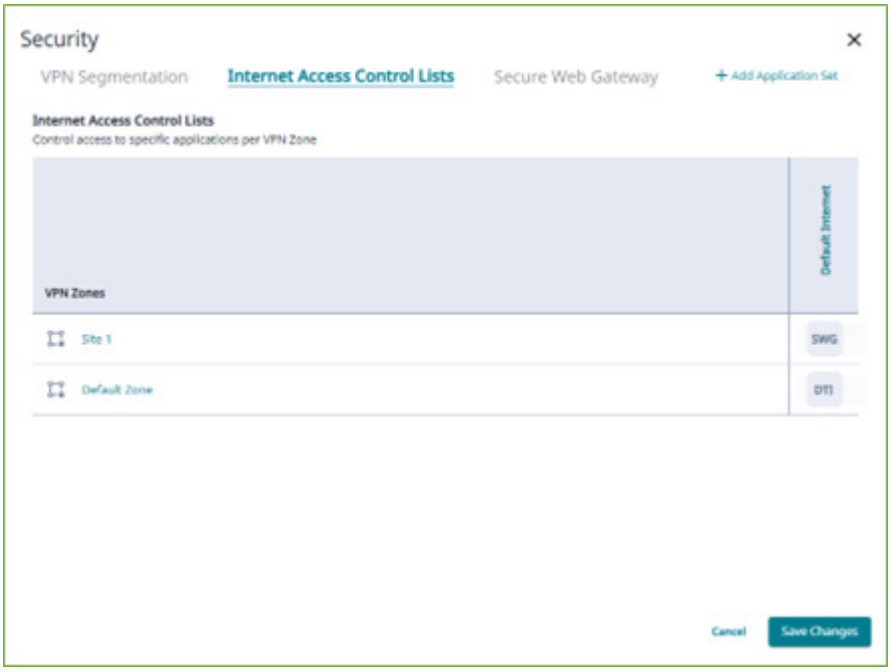


*Figure 27. Internet access policies*

All traffic from this site to the internet now travels through the tunnels that you defined. The configuration of ExtremeCloud SD-WAN is complete.

 

# Validating, Supervising, and Troubleshooting

After the configuration is completed in the ZIA Admin Portal and in ExtremeCloud SD-WAN Orchestrator, user internet traffic from the site is protected by ZIA.

Seen from the internet, the site's public IP address is from a Zscaler data center.

Accessing http://ip.zscaler.com from hosts located on the LAN side of the SD-WAN appliance returns information on the Zscaler data center being used.

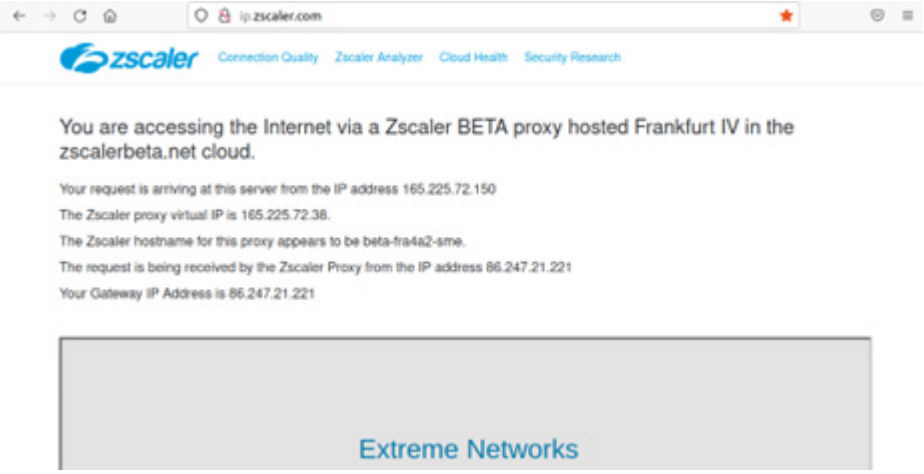


*Figure 28. Zscaler data center used*

## Supervising the Tunnels to ZIA

The ZIA Admin Portal and ExtremeCloud SD-WAN Orchestrator provide tools to obtain a status on the tunnels and insight on their use.

### In ZIA Admin Portal

You can supervise tunnels between the SD-WAN appliance and ZIA Public Service Edges in the ZIA Admin Portal.

1. Go to **Analytics** > **Insights** > **Tunnel Insights**.

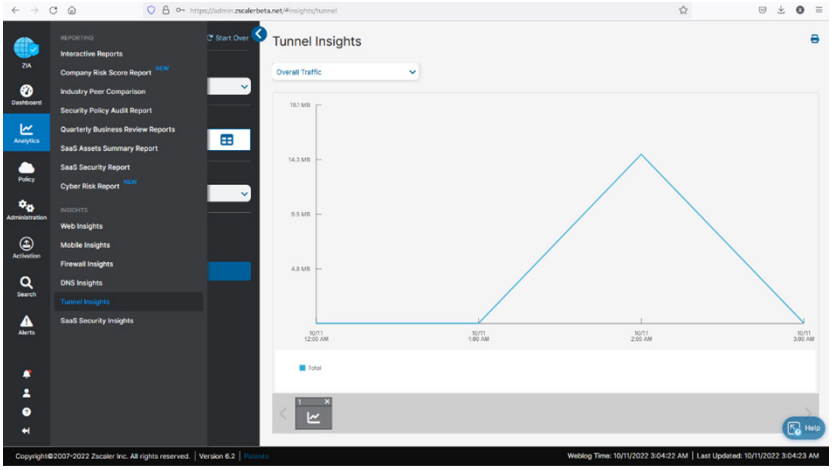


*Figure 29. Tunnel Insights*

 

2. Select the **Insights** tab. The page offers several ways to filter and present data.
3. In the following example, review the amount of traffic sent to ZIA Public Service Edges, per **Location** and over the current month.

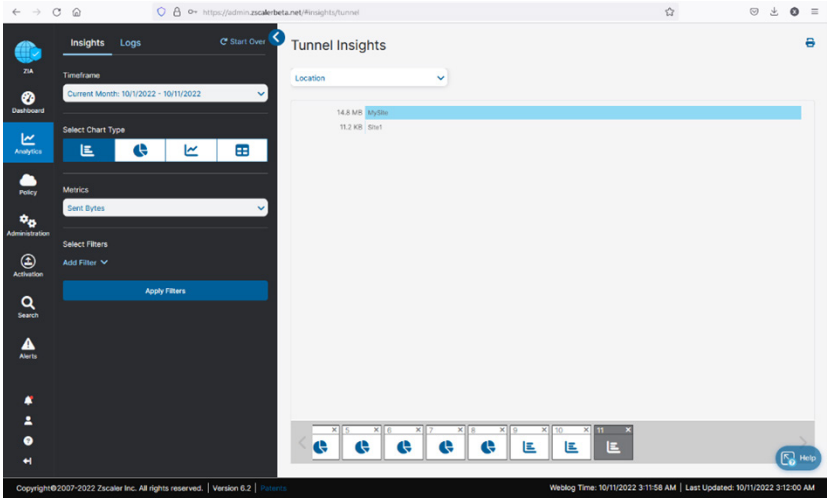


*Figure 30. Tunnel Insights page*

## In ExtremeCloud SD-WAN Orchestrator

ExtremeCloud SD-WAN Orchestrator provides a map and a page dedicated to the supervision of all tunnels.

1. In the ExtremeCloud SD-WAN Main Menu, go to **Appliances** and select the appliance.
2. Look at the map displayed in the appliance page, the various connections of this appliance are displayed. The defined external gateway is represented by a shield icon and its name. A line represents a connection (i.e., the two tunnels to the primary and secondary destinations). A dashed line between the appliance and the external gateway indicates that the connection is down (both tunnels down).

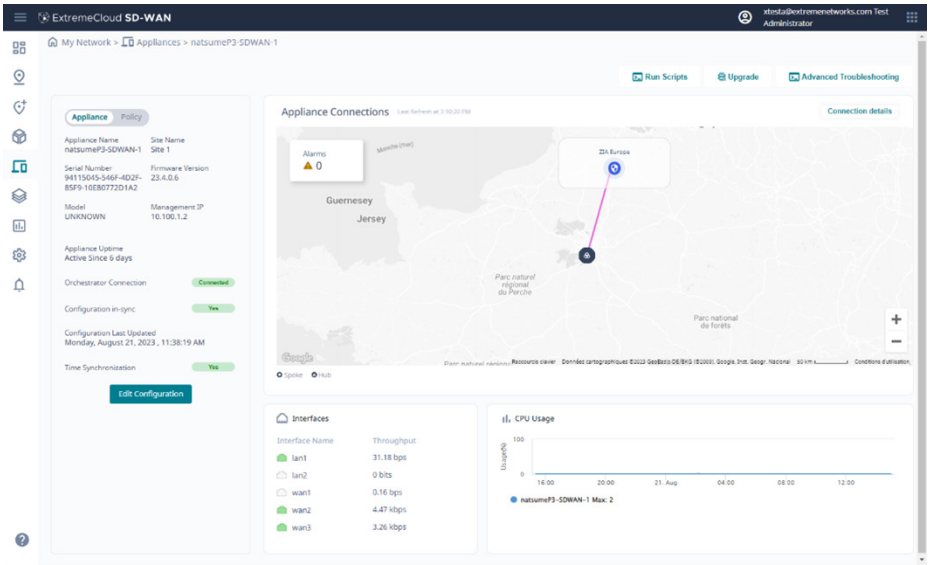


*Figure 31. Map of appliance connections*

3. Select **Connection Details** for details on all the appliance connections. In the displayed table, you can identify the tunnels to ZIA by looking at:
   - The type of the tunnel (**Type** column), which is **Secure Web Gateway**.
   - The external SWG name (**Overlay** column), which is the name given when you completed the steps in Defining an External Gateway.

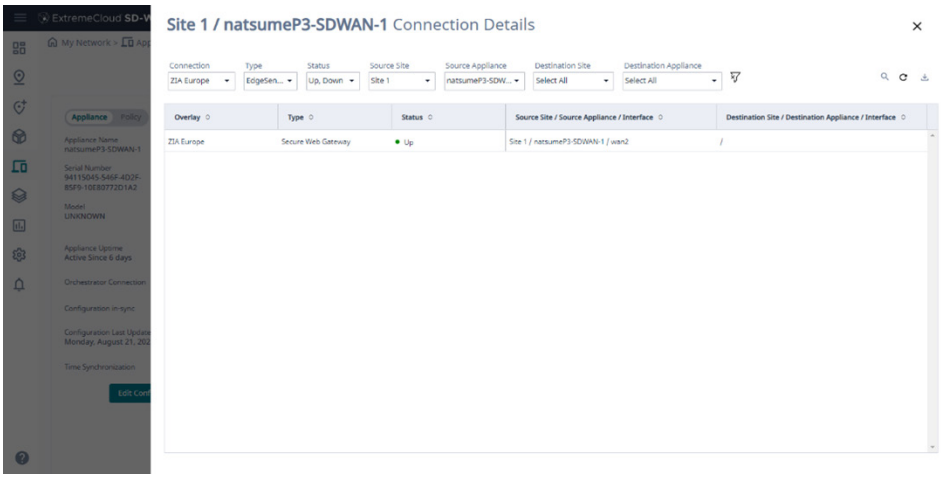


*Figure 32. Connection Details*

Only one entry is presented in this table for one pair of tunnels to the external gateway (primary and secondary destinations). The status is Up if at least one of the two tunnels is up.

 

# Troubleshooting the Tunnels to ZIA

ZIA allows you to troubleshoot tunnels to Zscaler if issues occur.

## In ZIA Admin Portal

On the ZIA Insights Logs page, review or retrieve states and events related to the tunnels between the appliances and ZIA.

1. Go to **Analytics** > **Insights** > **Tunnel Insights**.
2. Select the **Logs** tab.
3. Select a time frame and apply filters to narrow the search. Results are displayed on the page or downloaded as a .csv.
4. Review the following example, which shows all the tunnel events from a particular source IP address that occurred during the current month.

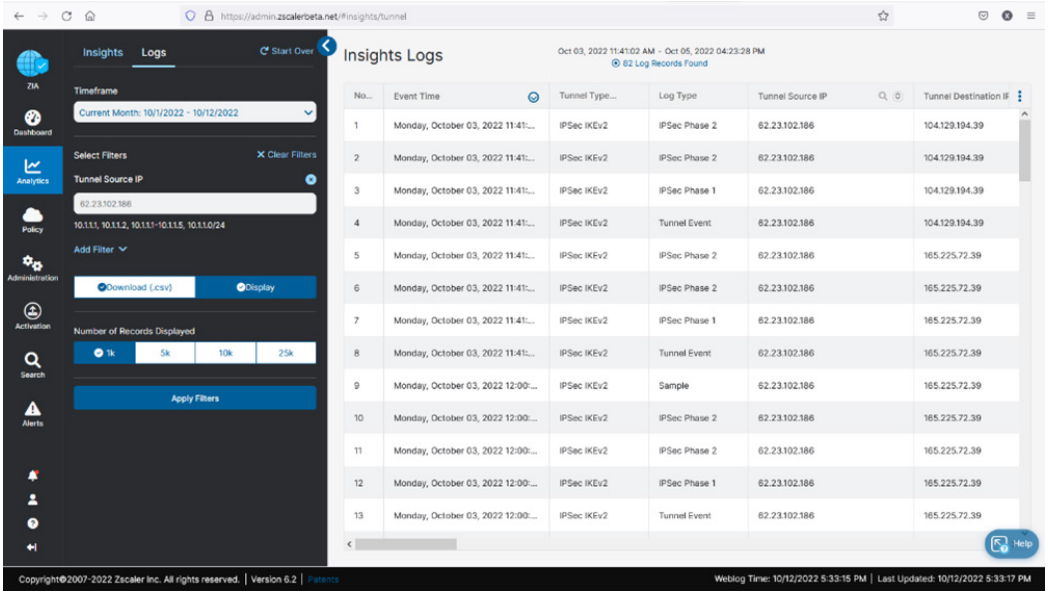


*Figure 33. Tunnel Insights Logs in the ZIA Admin Portal*

 

## In ExtremeCloud SD-WAN Orchestrator

To configure ExtremeCloud SD-WAN Orchestrator:

1. In the ExtremeCloud SD-WAN Main Menu, go to **Appliances** and select the appliance.
2. Select **Advanced Troubleshooting**.
3. In the troubleshooting page, go to **Tunnels** > **IPSec**.

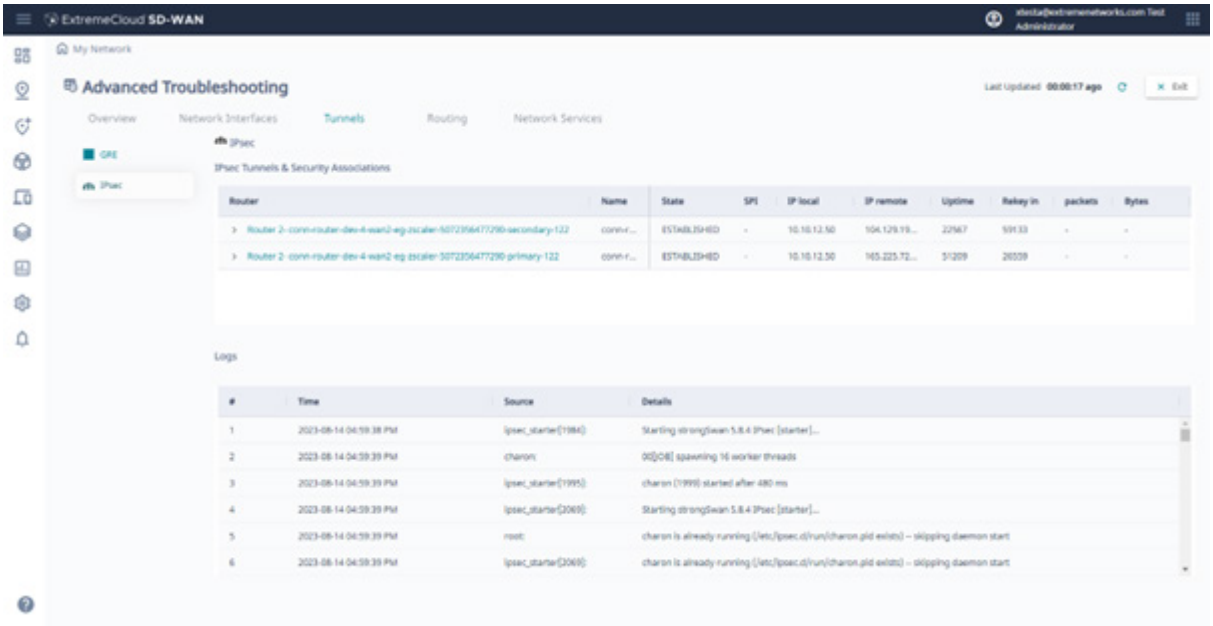


*Figure 34. IPSec tunnel troubleshooting*

IPSec tunnels and their security associations are listed in the first table, and provide the state and a few metrics. This table displays all IPSec tunnels handled by the appliance. You can identify the tunnels to ZIA by looking at the IP addresses (**IP remote** column).

Logs are displayed in the second table and provide information if the tunnels are not successfully established.

 

# 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**.

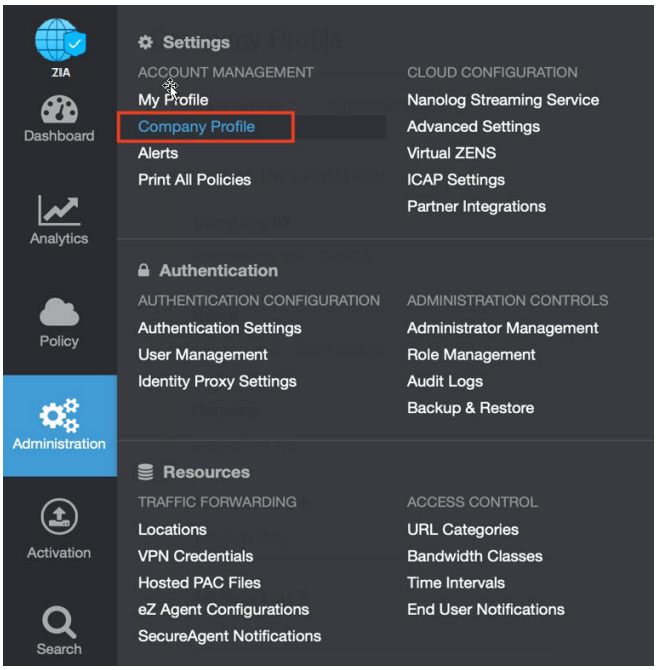


*Figure 35. Collecting details to open support case with Zscaler TAC*

2. Copy your Company ID.

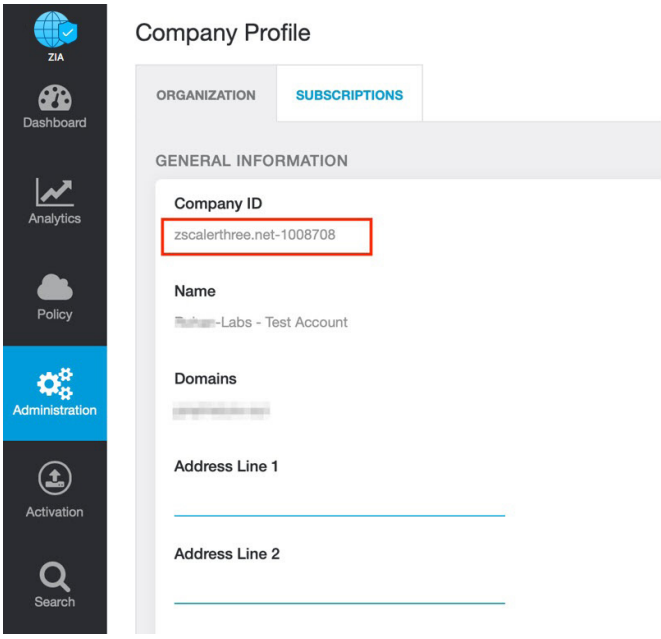


*Figure 36. Company ID*

 

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

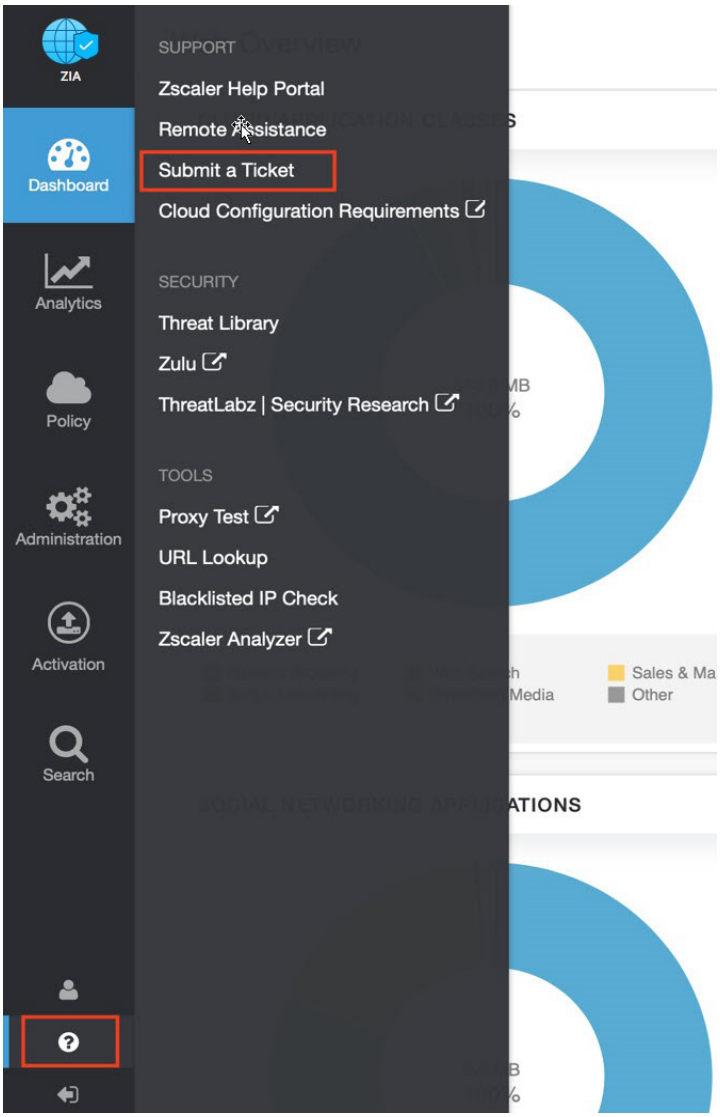


*Figure 37. Submit a ticket*

 