ZSCALER AND ARUBA EDGECONNECT SD-BRANCH DEPLOYMENT GUIDE

JULY 2019, VERSION 2.0

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
BGW	Branch Gateway (Aruba)
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DPD	Dead Peer Detection (RFC 3706)
DPS	Dynamic Path Selection
ESP	Edge Services Platform
GRE	Generic Routing Encapsulation (RFC2890)
FQDN	Fully Qualified Domain Name
IKEv2	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
LAN	Local Area Network
MPLS	Multi-Label Switching Protocl
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SLA	Service Level Agreement
SSL	Secure Socket Layer (RFC6101)
TPM	Trusted Platform Module
VDI	Virtual Device Interface
vGW	Virtual Gateway
VPN	Virtual Private Network
VPNC	Virtual Private Network Consortium
WAN	Wide Area Network
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

About This Document

The following sections describe the organizations referenced in 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. For more information, see Zscaler's website or follow Zscaler on Twitter @zscaler.

Aruba Overview

Aruba, a Hewlett Packard Enterprise company, is the global leader in secure, intelligent edge-to-cloud networking solutions that use AI to automate the network, while harnessing data to drive powerful business outcomes. With Aruba Edge Services Platform (ESP) and as-a-service options as part of the HPE GreenLake family, Aruba takes a cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments, covering all aspects of wired, wireless LAN, and wide area networking (WAN).

To learn more, see Aruba's website. For real-time news updates, follow Twitter and Facebook at @VisitAruba.

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:

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

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.

Zscaler and Aruba Introduction

The following sections describe the applications referenced in this deployment guide.

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, SaaS Security, and Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
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.

Aruba EdgeConnect SD-Branch Overview

Software-Defined WAN (SD-WAN) technology is the answer to growing bandwidth demands and tightening budget considerations. New solutions offer simplified WAN operations and reduced operational costs for those managing public and private WAN connections, and those shifting toward cloud-based services altogether.

Aruba EdgeConnect SD-Branch is designed for optimizing routing decisions and improving visibility across the LAN and WAN edge. Full Layer 7 application awareness combines with unique in-branch visibility based on end-user roles, device type, and location context to make the Aruba EdgeConnect SD-Branch solution ideal for distributed enterprises.

Aruba Resources

The following table contains links to Aruba support resources.

Name	Definition
Aruba Technical Documentation	Help documentation for Aruba products.
Aruba Airheads Community	Online help forum for Aruba solutions.

Security in Aruba SD-Branch

Security is an integral part of the Aruba SD-Branch solution. The security of the Aruba SD-Branch solution is built in layers, from the hardening of the operating system to the integration with best-of-breed security partners.

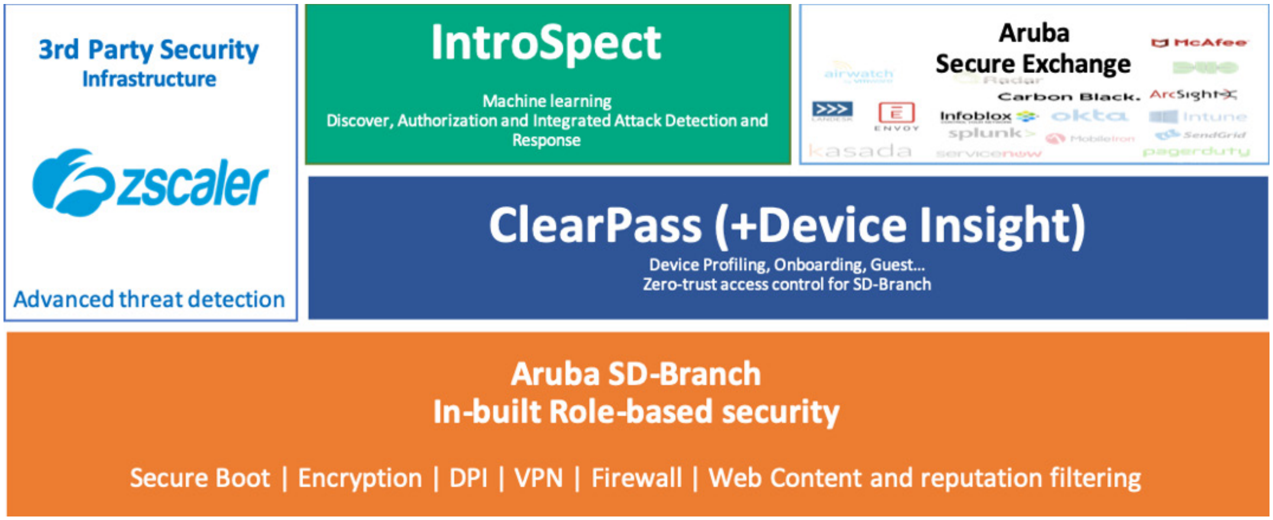

3rd Party Security
Infrastructure
zscaler
Advanced threat detection
IntroSpect
Machine learning
Discover, Authorization and Integrated Attack Detection and Response
Aruba
Secure Exchange
McAfee
airwatch
Radar
Carbon Black.
ArcSight
LANDESK
ENVOY
Infoblox
okta
Intune
splunk>
MobileIron
SendGrid
kasada
servicenow
pagerduty
ClearPass (+Device Insight)
Device Profiling, Onboarding, Guest...
Zero-trust access control for SD-Branch
Aruba SD-Branch
In-built Role-based security
Secure Boot | Encryption | DPI | VPN | Firewall | Web Content and reputation filtering

Figure 1. Aruba SD-Branch security layers

Security Layers

The Aruba Gateways use the ArubaOS platform as the operating system. This includes:

- Secure boot: TPM signed software image. Heavily restricting communications until the gateway has received its configuration from Aruba Central.
- Secure Zero Touch Provisioning: Leveraging the TPM loaded in the Aruba gateways to secure communications with Aruba Central.
- AES 256 encryption: For all branch-hub tunnels.
- Aruba Role-based stateful firewall: With support for scalable configuration using firewall aliases, ALGs, and role-based policies.
- Deep Packet Inspection: Module with capacity to identify close to 3,200 applications.
- Web content and reputation filtering: Using WebRoot's machine learning technology to classify content, reputation, and geolocation for billions of URLs.

The Aruba SD-Branch solution integrates with ClearPass or other Authentication, Authorization, Accounting (AAA) servers to form a policy-driven branch. This model dynamically assigns policies based on users and devices, as opposed to the traditional way of assigning these policies manually based on ports, VLANs, and IP addresses. This policy-driven branch is enhanced by leveraging integrations with the 140+ partners in the 360 Security Exchange program. It can be pushed even further by integrating with Aruba Introspect for User Entity and Behavioral Analytics (UEBA).

Lastly, the Aruba SD-Branch solution integrates with third-party security infrastructure partners. With these integrations, the Aruba SD-Branch architecture seeks to offer enterprise-grade advanced threat protection in a scalable manner. With this in mind, the integration with Zscaler provides a scalable solution for advanced threat protection in branch networks.

ZIA Integration Overview

It is common in networking architecture today to tunnel traffic between a HQ and branches over either MPLS or dedicated encrypted VPN links. As more services are cloud-based, and more information is available on the internet, it makes less sense to tunnel traffic back to a central point before reaching its endpoint.

Breaking out traffic locally from the branches (as opposed to an on-premises appliance in the data center) allows traffic to reach its destination faster and use bandwidth more efficiently. However, allowing traffic directly between devices in the branch and the internet can introduce security risks.

To secure this traffic, the Aruba Branch Gateway (BGW) can redirect selected traffic through a cloud-based security platform such as the ZIA service. This enables services like advanced threat protection or DLP (for more information, see Zscaler Help Portal) without the need to increase the footprint in branch locations.

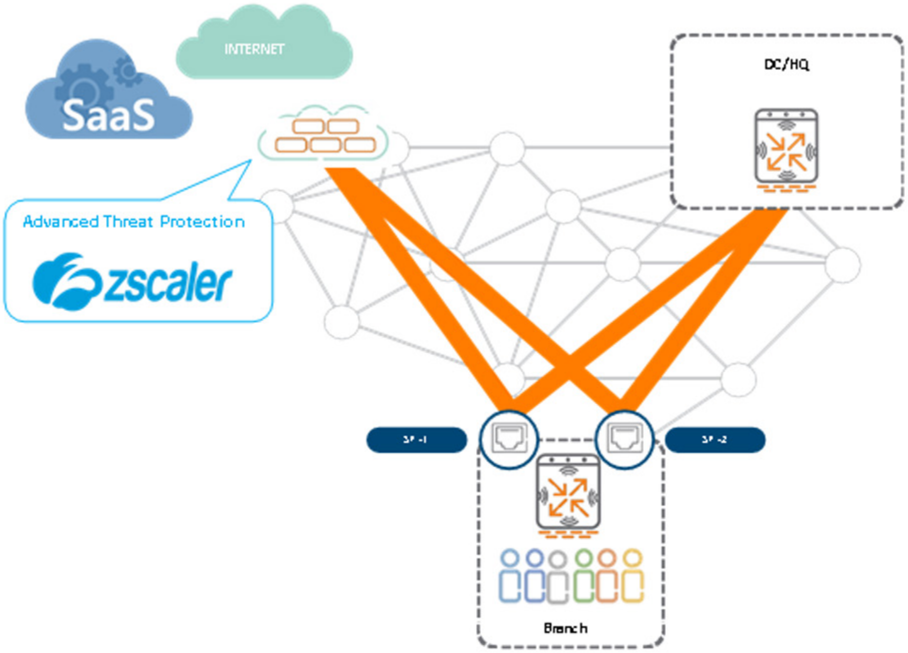


Figure 2. Aruba SD-Branch integration with Zscaler Cloud security infrastructure

Tunnel Establishment

Zscaler delivers a next-generation security architecture built from the ground up for performance and scalability. It is a three-tiered platform with differentiated control plane (Zscaler Central Authority), data plane (Zscaler Public Service Edge) and logging/statistics plane (Zscaler Nanolog Servers). It is distributed across more than 150 data centers on 6 continents, which means that users are always a short hop away from their applications.

ZIA is a secure internet and web gateway delivered as a service from the cloud. To integrate with this service, the SD-WAN solution needs to establish tunnels with the nearest ZIA Public Service Edge to send internet-bound traffic through them.

Both Aruba and the ZIA service support establishing communications through IPSec or GRE tunnels. The drawback of using GRE, however, is that tunnels can't traverse NAT boundaries, which are very common in branch environment. For this reason, this deployment guide focuses on the implementation based on IPSec tunnels.

Tunnel Details

The tunnels between the BGW and the ZIA Public or Private Service Edges use IPSec with null encryption. Traffic traverses NAT boundaries and leverages IKEv2 for authentication, while at the same time limiting the overhead. To bring up the tunnels, you must set up accounts in Zscaler for the Aruba BGWs and have them authenticate themselves. Such tunnels can be established manually or by using the SD-WAN Orchestrator service available in the Aruba SD-Branch solution.

The following table is a summary of the tunnel characteristics.

Feature	Phase 1	Phase 2
Encryption	AES-128	Null
Integrity	HMAC-SHA1-96	MD5
Authentication	FQDN & PSK	N/A
Key Exchange Method	Diffie-Hellman	Diffie-Hellman
Diffie-Hellman Group	2	2
NAT-Transversal	Enabled	N/A
Dead Peer Detection (DPD)	Enabled	
Perfect Forward Secrecy (PFS)	N/A	Disabled
Maximum Transmission Unit (MTU)	N/A	1460 Bytes
Maximum Segment Size (MSS)	N/A	1388 Bytes
VPN Type	N/A	Policy-based VPN

Tunnel Orchestration

Aruba BGWs can bring up tunnels to the ZIA service manually. This requires creating “locations” (as well as unique VPN credentials) in the ZIA service for each branch site. It also requires configuring the Aruba SD-WAN BGWs to bring up tunnels to the nearest ZIA Public Service Edges for traffic. Manually bringing up tunnels can be a very labor-intensive task.

This function is automated in the Aruba SD-Branch solution by SD-WAN Orchestrator. The Aruba SD-WAN Orchestrator is a cloud-native, multi-tenant control plane that is included as part of Aruba Central to automate SD-WAN deployments. The benefit of the SD-WAN Orchestrator is that WAN links are automatically discovered, and tunnels and routes are orchestrated based on business and topological needs, such as mapping data centers to branch offices (for more information, see the **Aruba SD-WAN documentation**).

In the context of the Zscaler integration, the SD-WAN Orchestrator has the role of negotiating the tunnel establishment between BGW and the nearest ZIA Public Service Edge. It does so by executing the following steps:

1. Bind Aruba BGWs with the nearest ZIA Public Service Edge: The Orchestrator queries the ZIA service for the nearest Public Service Edge for each SD-WAN Gateway based on the public IP address from which every branch is seen.
2. Create locations in ZIA: The SD-WAN Orchestrator creates the locations for all BGWs in the selected groups through the ZIA APIs. Unique VPN credentials are also created for each BGW.
3. Orchestrate tunnels: The SD-WAN Orchestrator instructs each BGW to establish tunnels with the nearest ZIA Public Service Edge using the credentials negotiated in step 2.

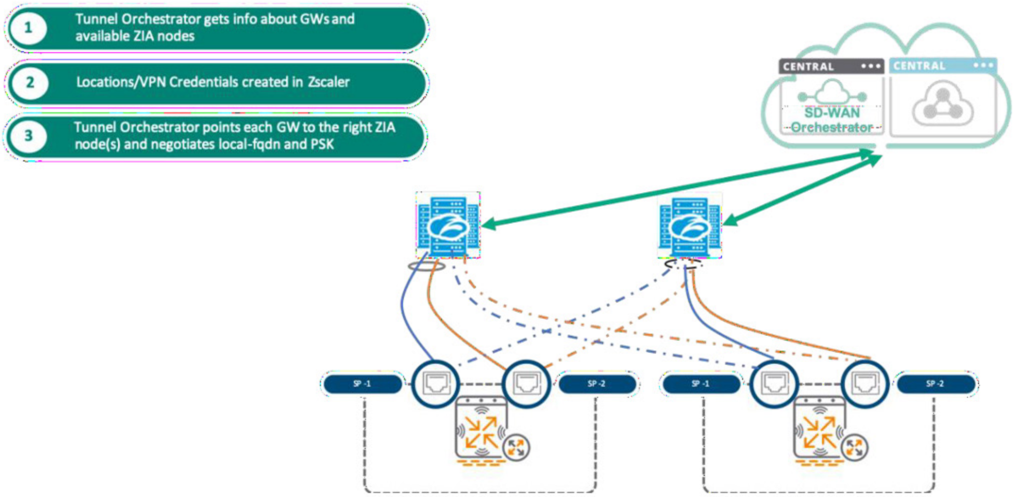

1 Tunnel Orchestrator gets info about GWs and available ZIA nodes
2 Locations/VPN Credentials created in Zscaler
3 Tunnel Orchestrator points each GW to the right ZIA node(s) and negotiates local-fqdn and PSK
CENTRAL
CENTRAL
SD-WAN Orchestrator
SP -1
SP -2
SP -1
SP -2

Figure 3. Orchestrated tunnels

Policy-Based Routing

After the tunnels are established, make sure the relevant traffic is sent through these tunnels. The Aruba SD-Branch solution uses policy-based routing (or role-based routing) to determine which traffic flows are sent through the ZIA service.

Consider the following parameters when determining traffic types to be sent through the ZIA service:

- VLAN/User Role: Policy-based routing policies can be applied to roles or VLANs.
- Stateful Firewall attributes: Protocol, Source/destination address, source/destination port.
- FQDN: ArubaOS supports creating netservices based on FQDN, which can be used to build policy-based routing policies.

The following figure illustrates how Aruba Gateways selectively redirect traffic to ZIA. In this example, cameras are full-tunneled to the data center (DC), the guest is sent directly to the internet, and employees/IoT are sent to the internet through the ZIA service (with the exception of specific well-known SaaS applications).

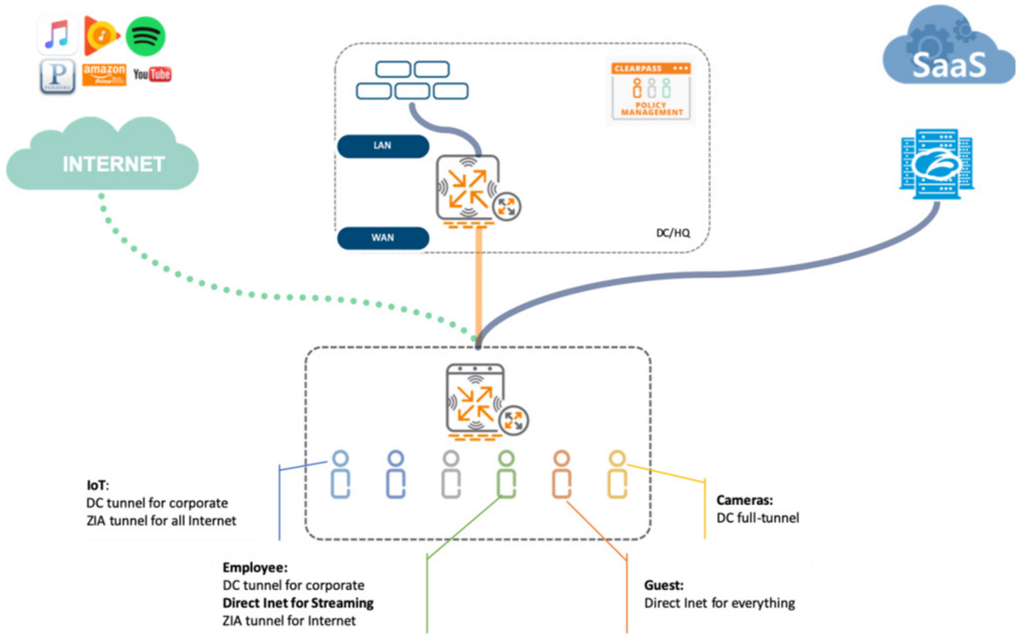


Figure 4. Role-based routing policies

Reference Architectures

The integration of Aruba SD-WAN and ZIA allows for a wide variety of scenarios. This section describes the most common scenarios, which are validated by the Aruba Solution Test team.

Branch Gateways to ZIA

Aruba BGWs establish tunnels to one or several ZIA Public Service Edges (which can be in different regions, as shown in the following figure) to secure user traffic going to public cloud services or to the internet. This provides high availability. The solution supports manually setting the destination ZIA Public Service Edge for each BGW. It uses the SD-WAN Orchestrator to learn the closest ZIA Public Service Edge for each branch and automatically establishing the tunnels to it.

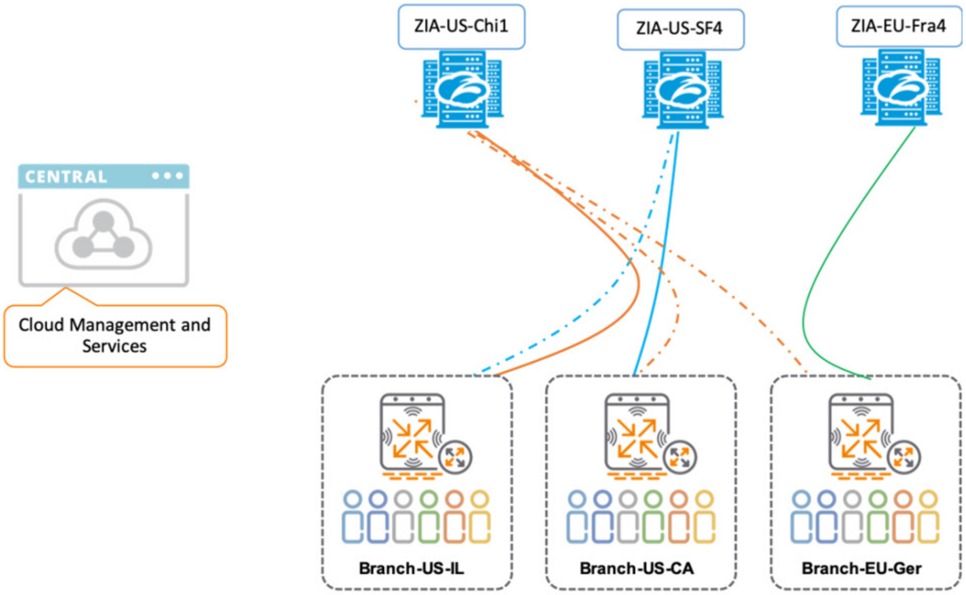


Figure 5. Tunnel to nearest ZIA Public Service Edge

Uplink Load-Balancing and DPS

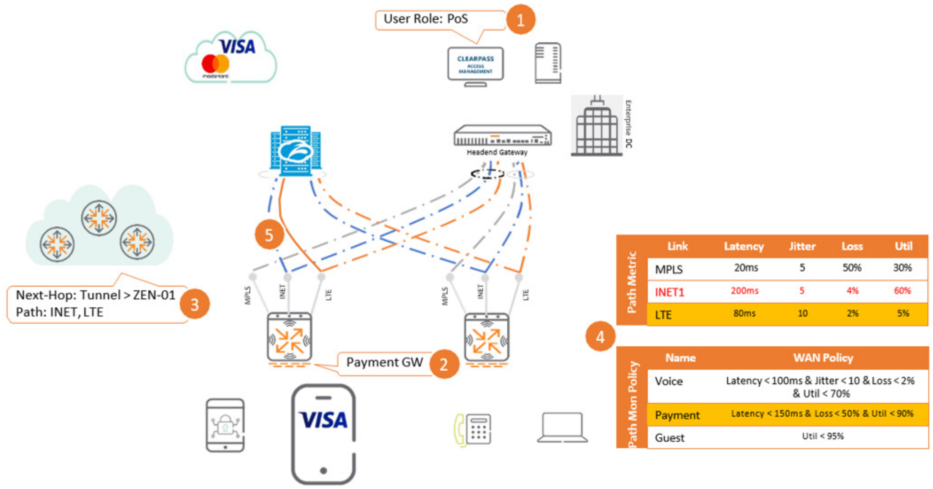
Aruba BGWs supports uplink load-balancing. All traffic that enters ZIA through a tunnel is guaranteed to return (egress) through the same tunnel. The ZIA architecture prevents any chance of asymmetrical routing when parallel tunnels are established. The BGW sets up a tunnel from every WAN interface.

Moreover, the Aruba BGW is capable of selecting the WAN circuit to be used by each traffic flow based on rich policies such as the ones built for policy-based routing. The routing engine (global routing table or policy-based routing) provides a set of next-hops, and the dynamic path selection (DPS) engine selects the optimal path. On top of that, the BGW can monitor the different WAN circuits to steer traffic to the optimal path based on SLAs set for each application.

See the following example workflow:

1. Aruba ClearPass (or another RADIUS server) assigns the role **PoS** to the device.
2. The firewall classifies the session as **Payment**.
3. The routing for a PoS device using a payment app states that the next-hop is a certain ZIA Public Service Edge, and the paths are, for example, INET and LTE.
4. Because the traffic is classified as Payment, it's handled by the DPS policy Payment. This policy has INET as the preferred path, as well as an SLA that must be met.

5. If the measured values for INET meet the SLA for the Payment policy, the session goes through the tunnel established using the INET uplink. If at any point the measured SLA for INET drops, the BGW steers the session to any other active tunnel that meets the SLA. If no circuit meets the SLA, the system chooses the one that deviates the least from the configured SLA.



Path Metric	Link	Latency	Jitter	Loss	Util
	MPLS	20ms	5	50%	30%
	INET1	200ms	5	4%	60%
	LTE	80ms	10	2%	5%

Path Mon Policy	Name	WAN Policy
	Voice	Latency < 100ms & Jitter < 10 & Loss < 2% & Util < 70%
	Payment	Latency < 150ms & Loss < 50% & Util < 90%
	Guest	Util < 95%

Figure 6. Dynamic path steering

Headend Gateway to ZIA

If branch traffic is aggregated at a local hub and then routed to the internet or other corporate resources, Aruba VPNCs can set up tunnels to the nearest ZIA Public Service Edge to have branch traffic go through additional security validations.

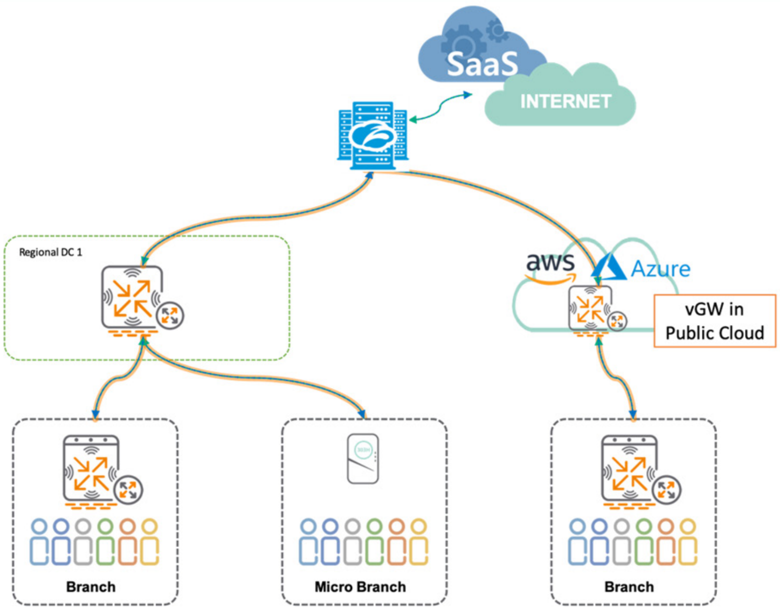


Figure 7. Tunnels from regional data centers

Both hardware as well as virtual Headend Gateways (virtual gateways in private instances of a public cloud) are supported in this model.

Redundancy of ZIA Public Service Edge

As shown in the previous section, the load-balancing and DPS mechanisms would take care of WAN circuit redundancy. However, that might not be sufficient in the unlikely event that a ZIA Public Service Edge becomes unavailable. In that case, the Aruba SD-Branch integration with Zscaler makes use of the DPD protocol to ensure the traffic doesn't get blackholed.

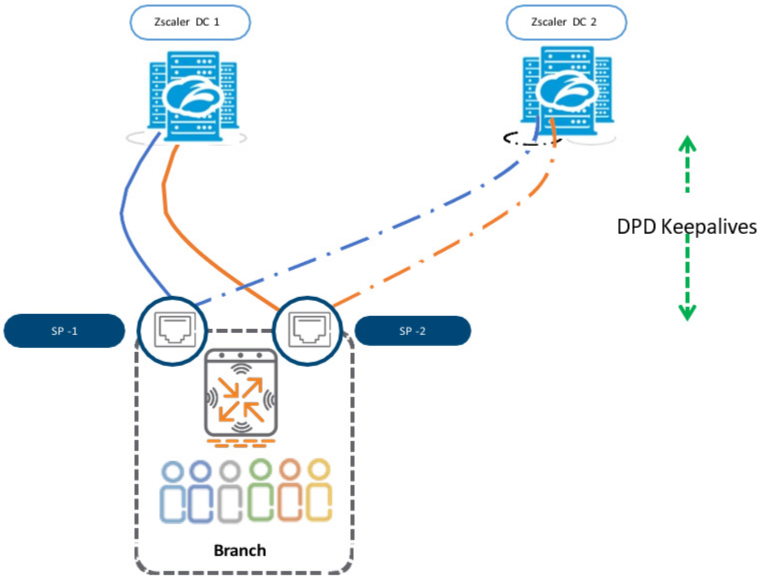


Figure 8. ZIA Public Service Edge redundancy

Tunnels to redundant ZIA Public Service Edges are supported for both topologies displayed: BGWs to ZIA and Headend Gateways to ZIA.

Branch Gateway Redundancy

When redundancy is required inside the branch, SD-WAN gateways can share uplink interfaces with their high availability pairs. This is done by establishing a virtual uplink through the LAN to share such interfaces. The result is that each BGW has physical uplinks as well as virtual uplinks.

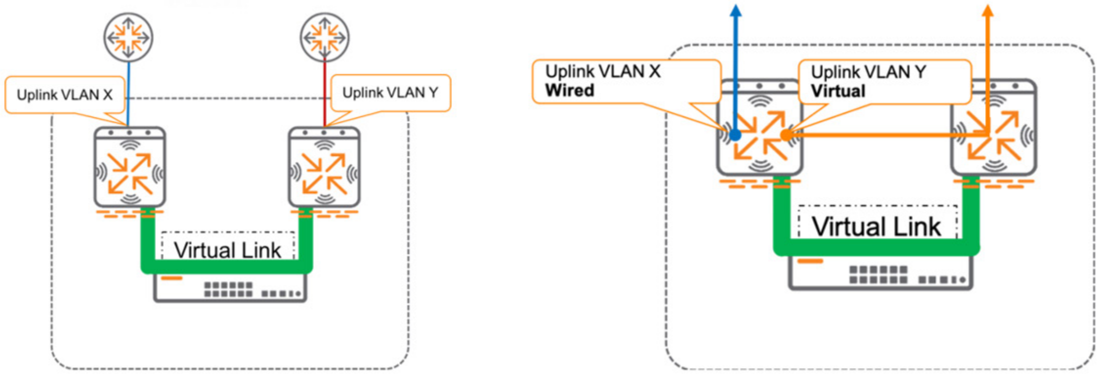


Figure 9. Branch high availability

In this scenario, each BGW establishes tunnels to the ZIA service through all uplink interfaces (physical and virtual). Both BGWs are defined in ZIA as a single location and use the same VPN credentials, or as two locations with different credentials for each BGW. Both operating modes are supported.

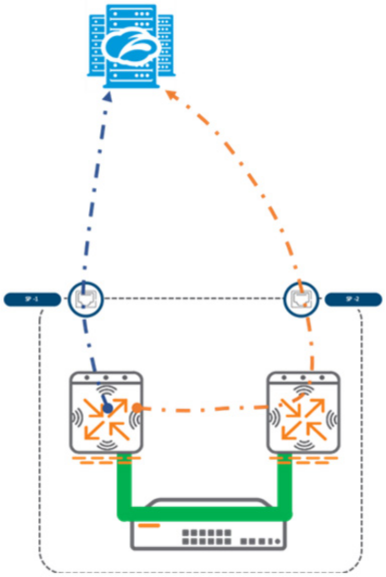


Figure 10. ZIA tunnels with branch high availability

Configuration Workflows

The following section describes how to configure workflows for the Zscaler and Aruba integration.

Tunnel Establishment

You can manually configure the Aruba and ZIA integration, or you can leverage the SD-WAN Orchestrator to streamline the process of creating locations, VPN credentials, and BGW tunnels in the ZIA service.

Orchestrated Tunnel Establishment

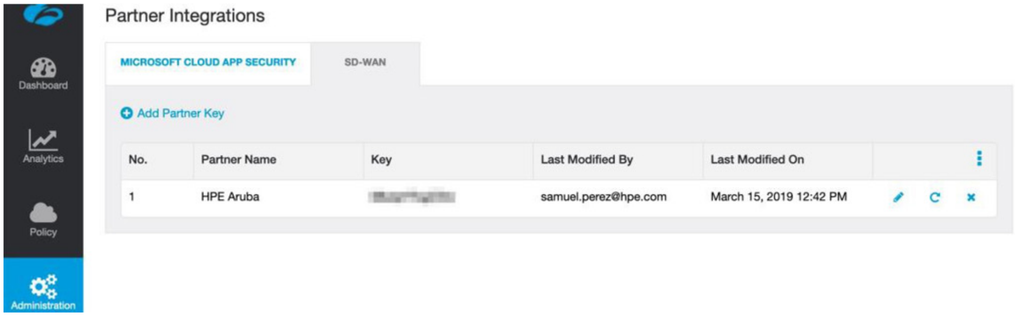
The integration between Aruba SD-Branch and the ZIA service can make use of the SD-WAN Orchestrator to automate large distributed deployments.

Configuring ZIA for API access

ZIA Admin Portal's automated workflow doesn't need to create locations or VPN credentials because the SD- WAN Orchestrator does this through the API. The SD-WAN Orchestrator needs partner access to communicate through the API.

To add a partner key for Aruba SD-Branch:

1. Log in to the ZIA Admin Portal.
2. Click **Administration** > **Partner Integrations** > **SD-WAN**.
3. Click **Add Partner Key**.

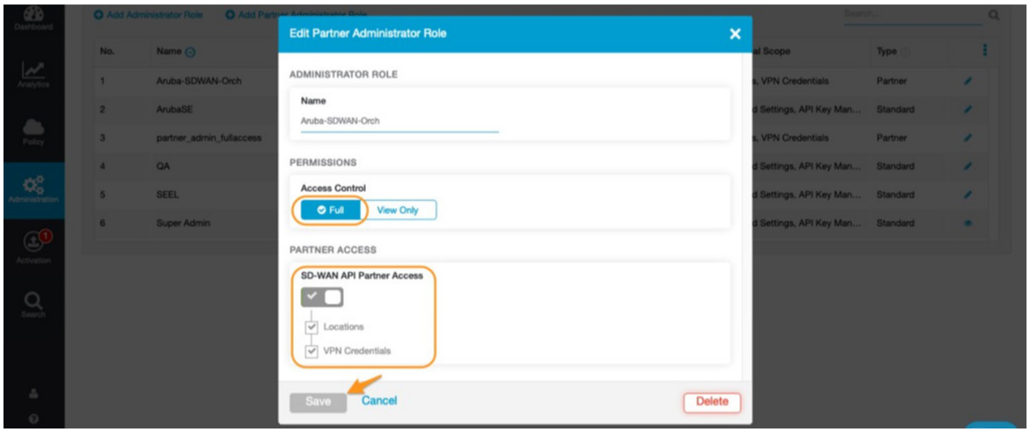


Partner Integrations

No.	Partner Name	Key	Last Modified By	Last Modified On
1	HPE Aruba	[redacted]	samuel.perez@hpe.com	March 15, 2019 12:42 PM

Figure 11. Create Partner API Key

4. In **Administration** > **Role Management**, create a Partner Administrator Role to provide credentials for the API access.



No.	Name	…al Scope	Type
1	Aruba-SDWAN-Orch	…, VPN Credentials	Partner
2	ArubaSE	…d Settings, API Key Man...	Standard
3	partner_admin_fullaccess	…, VPN Credentials	Partner
4	QA	…d Settings, API Key Man...	Standard
5	SEEL	…d Settings, API Key Man...	Standard
6	Super Admin	…d Settings, API Key Man...	Standard

Edit Partner Administrator Role

ADMINISTRATOR ROLE

Name: Aruba-SDWAN-Orch

PERMISSIONS

Access Control: [✓ Full] View Only

PARTNER ACCESS

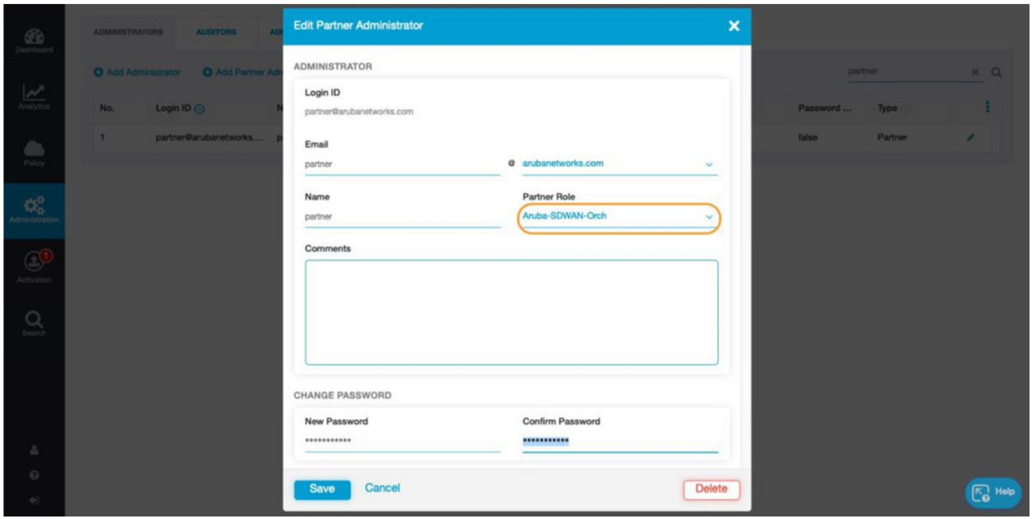
SD-WAN API Partner Access ✓

☑ Locations

☑ VPN Credentials

Figure 12. Create Partner Role

5. Go to **Administration** > **Administrator Management**, then create a partner account for the SD-WAN Orchestrator.



No.	Login ID	Password ...	Type
1	partner@arubanetworks....	false	Partner

Edit Partner Administrator

ADMINISTRATOR

Login ID: partner@arubanetworks.com

Email: partner @ arubanetworks.com

Name: partner

Partner Role: Aruba-SDWAN-Orch

Comments:

CHANGE PASSWORD

New Password: ••••••••••••

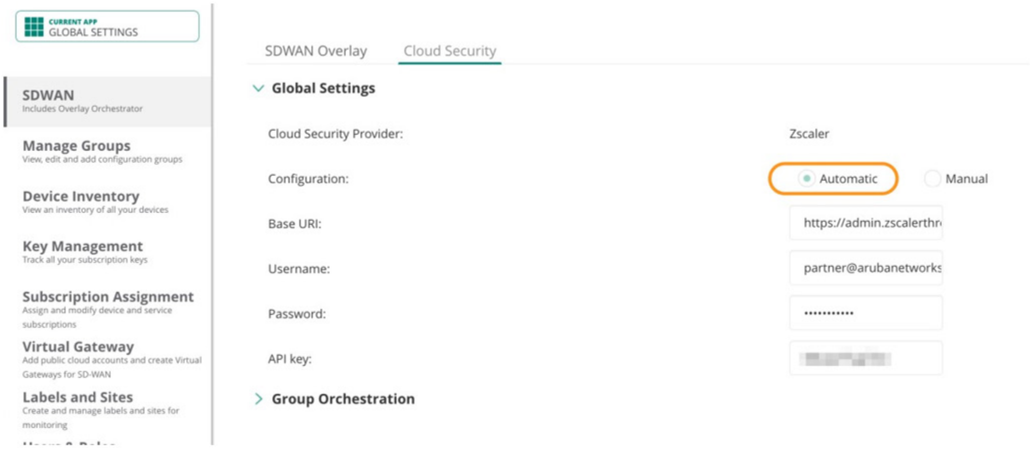
Confirm Password: ••••••••••••

Figure 13. Create partner account

Configuring Aruba SD-WAN for Orchestrated Tunnels

To enable orchestration of tunnels:

1. Navigate to **Global Settings** > **SDWAN** > **Cloud Security**.
2. Enter the partner credentials and API Key for the SD-WAN Orchestrator to communicate to the ZIA service.


CURRENT APP
GLOBAL SETTINGS
SDWAN
Includes Overlay Orchestrator
Manage Groups
View, edit and add configuration groups
Device Inventory
View an inventory of all your devices
Key Management
Track all your subscription keys
Subscription Assignment
Assign and modify device and service subscriptions
Virtual Gateway
Add public cloud accounts and create Virtual Gateways for SD-WAN
Labels and Sites
Create and manage labels and sites for monitoring
SDWAN Overlay
Cloud Security
Group Orchestration

Global Settings

Cloud Security Provider: Zscaler

Configuration: ● Automatic ○ Manual

Base URI: https://admin.zscalerthr

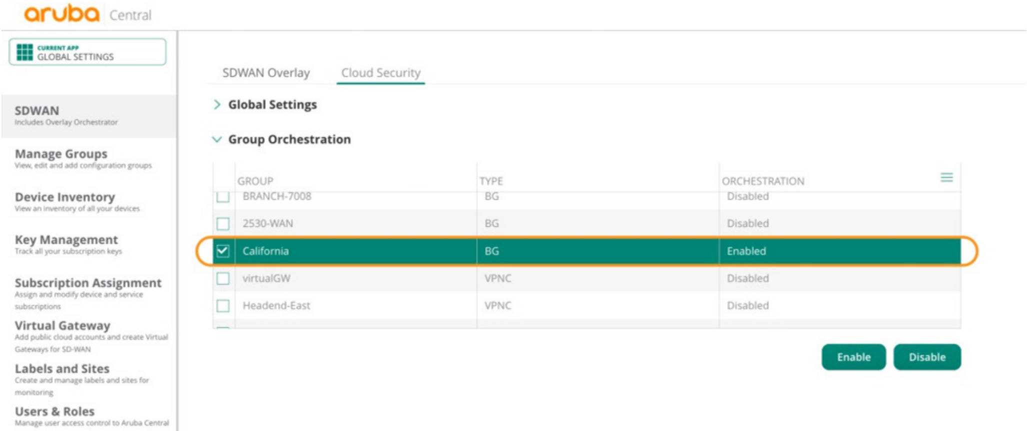
Username: partner@arubanetworks

Password: •••••••••••

API key: [redacted]

Figure 14. Enable automatic establishment of tunnels to ZIA service

3. Then, select the Gateway groups that establish tunnels to the ZIA service.


aruba Central
CURRENT APP
GLOBAL SETTINGS
SDWAN
Includes Overlay Orchestrator
Manage Groups
View, edit and add configuration groups
Device Inventory
View an inventory of all your devices
Key Management
Track all your subscription keys
Subscription Assignment
Assign and modify device and service subscriptions
Virtual Gateway
Add public cloud accounts and create Virtual Gateways for SD-WAN
Labels and Sites
Create and manage labels and sites for monitoring
Users & Roles
Manage user access control to Aruba Central
SDWAN Overlay
Cloud Security
Global Settings
Group Orchestration
Enable
Disable

	GROUP	TYPE	ORCHESTRATION
□	BRANCH-7008	BG	Disabled
□	2530-WAN	BG	Disabled
☑	California	BG	Enabled
□	virtualGW	VPNC	Disabled
□	Headend-East	VPNC	Disabled

Figure 15. Select groups to tunnel to ZIA

4. Enable the Orchestrated Zscaler integration in Aruba Central. After enabling the integration, the SD-WAN Orchestrator instructs the Gateways to establish tunnels to all ZIA Public Service Edge from all public WAN interfaces.

INET, MetroE, and LTE are considered public, while MPLS is considered private.

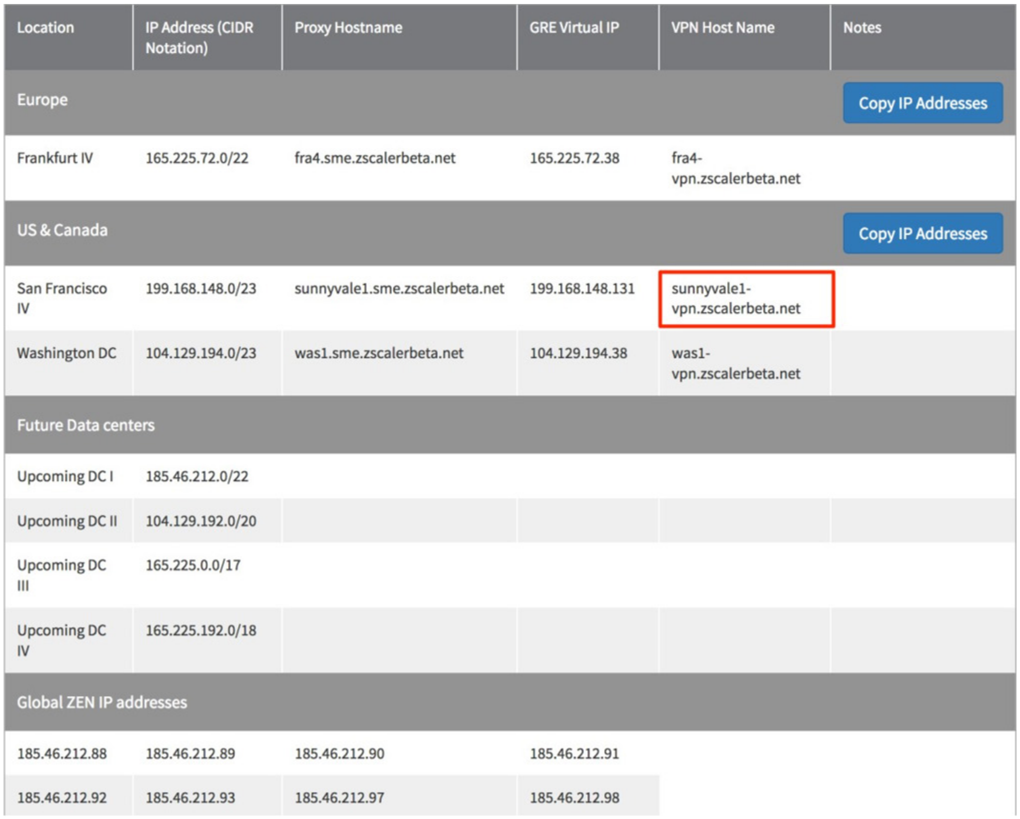
The minimum ArubaOS version required for the Zscaler Orchestrated tunnels is 8.4.0.0-1.0.6.0.

Manual Tunnel Establishment

As described in the overview, the integration with ZIA requires configurations on both the ZIA Admin Portal and in Aruba Central. The following configuration steps are streamlined because the ZIA service always sends return traffic through the traffic originating the session (removing the need for routing exchanges).

Pre-Requisites

Before configuring ZIA, locate the FQDN of the ZIA instance. For more information, see [Zscaler's support documentation](#).



Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	VPN Host Name	Notes
Europe					Copy IP Addresses
Frankfurt IV	165.225.72.0/22	fra4.sme.zscalerbeta.net	165.225.72.38	fra4-vpn.zscalerbeta.net	
US & Canada					Copy IP Addresses
San Francisco IV	199.168.148.0/23	sunnyvale1.sme.zscalerbeta.net	199.168.148.131	sunnyvale1-vpn.zscalerbeta.net	
Washington DC	104.129.194.0/23	was1.sme.zscalerbeta.net	104.129.194.38	was1-vpn.zscalerbeta.net	
Future Data centers					
Upcoming DC I	185.46.212.0/22				
Upcoming DC II	104.129.192.0/20				
Upcoming DC III	165.225.0.0/17				
Upcoming DC IV	165.225.192.0/18				
Global ZEN IP addresses					
185.46.212.88	185.46.212.89	185.46.212.90	185.46.212.91		
185.46.212.92	185.46.212.93	185.46.212.97	185.46.212.98		

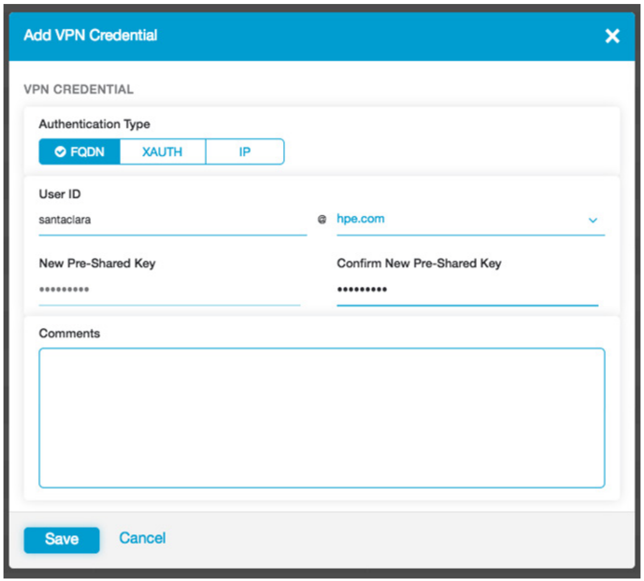
Figure 16. Locate Zscaler Public Service Edges

Configuring ZIA

Configure the ZIA service to receive VPN tunnels from Aruba Gateways. As described previously, these are IPSec tunnels that use IKEv2 credentials to uniquely identify each BGW. Assign each BGW a location and the corresponding VPN credentials in the ZIA Admin Portal.

To configure the ZIA service:

1. Log in to the ZIA Admin Portal.
2. Navigate to **Administration** > **Resources** > **VPN-Credentials**.
3. Click **Add VPN Credential**.
4. Select **FQDN** and type the User ID and Pre-Shared Key for a given location (or set of locations).
5. Click **Save**.



Authentication Type: FQDN (selected) | XAUTH | IP

User ID: santaclara @ hpe.com

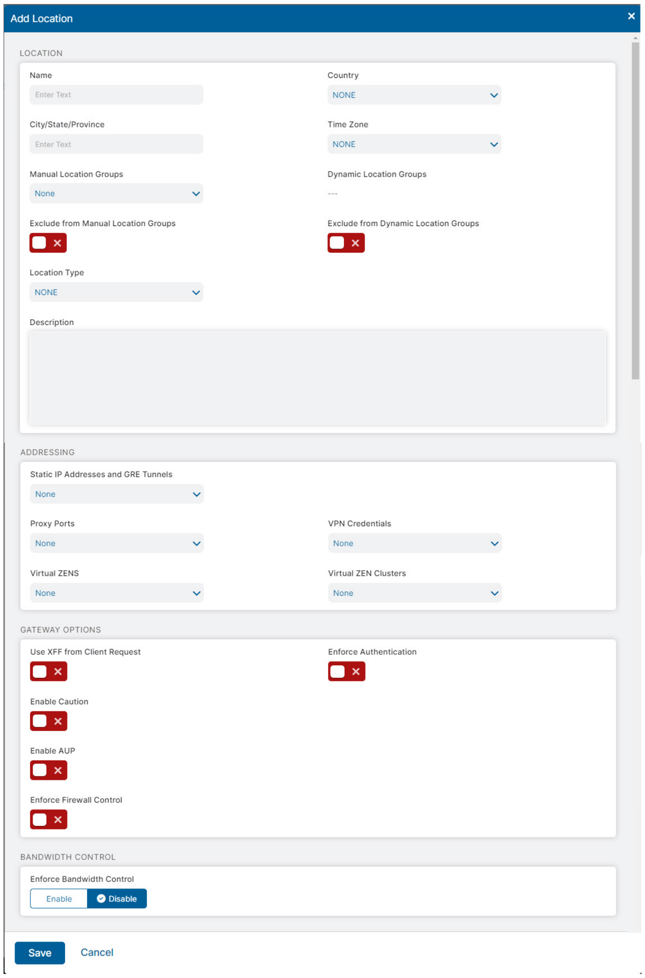
New Pre-Shared Key: •••••••••

Confirm New Pre-Shared Key: •••••••••

Figure 17. Create VPN Credential

After the credential is set, set up a location. The location identifies a specific site or a specific group of sites.

1. Navigate to **Administration** > **Resources** > **Locations**.
2. Choose **Add Location**.
3. Add the name, address, and time zone.
4. Select the previously created VPN credentials.
5. Click **Save**.



Add Location ×

LOCATION

Name: Enter Text

Country: NONE

City/State/Province: Enter Text

Time Zone: NONE

Manual Location Groups: None

Dynamic Location Groups: ---

Exclude from Manual Location Groups: ✕

Exclude from Dynamic Location Groups: ✕

Location Type: NONE

Description:

ADDRESSING

Static IP Addresses and GRE Tunnels: None

Proxy Ports: None

VPN Credentials: None

Virtual ZENS: None

Virtual ZEN Clusters: None

GATEWAY OPTIONS

Use XFF from Client Request: ✕

Enforce Authentication: ✕

Enable Caution: ✕

Enable AUP: ✕

Enforce Firewall Control: ✕

BANDWIDTH CONTROL

Enforce Bandwidth Control: Enable [✓ Disable]

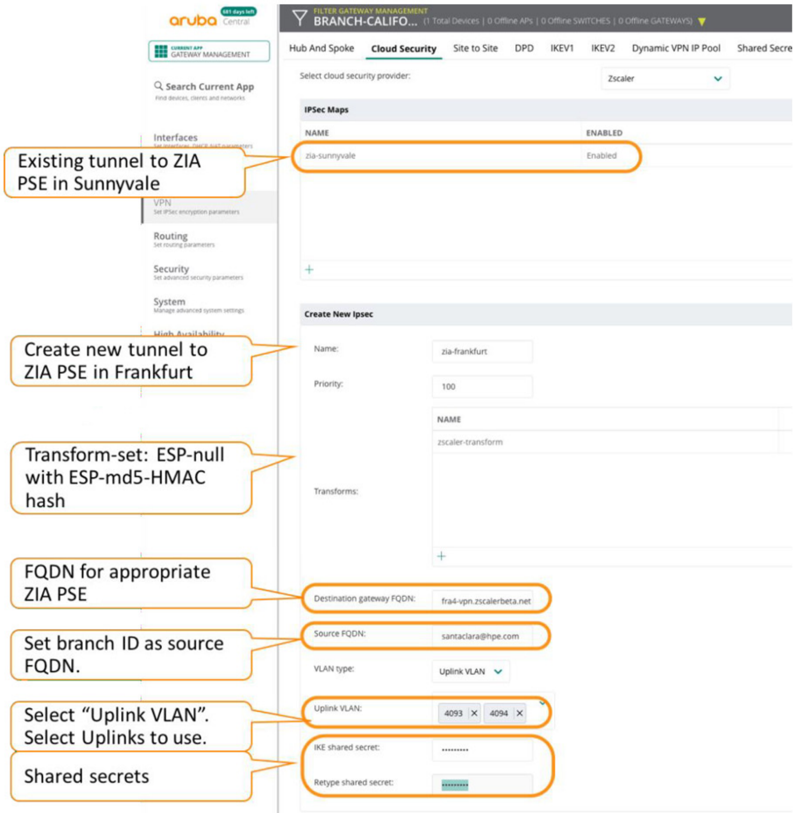
Save Cancel

Figure 18. Add Location

Configuring Aruba Gateways to Manually Establish Tunnels to ZIA

The Aruba BGW sets up tunnels to ZIA through every WAN interface. On the **VPN** > **Cloud Security** page in Aruba Central, configure the following parameters:

- **Name**: Enter the Administrative name for the tunnel.
- **Priority**: Type the Admin ID for the tunnel.
- **Transform**: Set ESP-null encryption with ESP-md5-HMAC hash.
- **Destination Gateway FQDN**: Set the FQDN for the BGW.
- **Source FQDN**: Set the user ID created in ZIA (santaclara@hpe.com in the example).
- **Uplink VLAN/VLAN**: When tunneling from a BGW, select the **Uplink VLAN(s)** used to bring up tunnels to ZIA. In the case of VPNCs, select the VLAN from which the tunnels are initiated.
- **IKE Shared Secret**: Set the same value created in the Zscaler configuration.


aruba Central
681 days left
CURRENT APP GATEWAY MANAGEMENT
Search Current App
Find devices, clients and networks
Interfaces
Set interfaces, DHCP, NAT parameters
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
FILTER GATEWAY MANAGEMENT
BRANCH-CALIFO... (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)
Hub And Spoke
Cloud Security
Site to Site
DPD
IKEV1
IKEV2
Dynamic VPN IP Pool
Shared Secre

Select cloud security provider: Zscaler

IPSec Maps

NAME	ENABLED
zia-sunnyvale	Enabled

Create New Ipsec

Name: zia-frankfurt

Priority: 100

Transforms:

NAME
zscaler-transform

Destination gateway FQDN: fra4-vpn.zscalerbeta.net

Source FQDN: santaclara@hpe.com

VLAN type: Uplink VLAN

Uplink VLAN: 4093 ✕ 4094 ✕

IKE shared secret: •••••••••

Retype shared secret: •••••••••

Existing tunnel to ZIA PSE in Sunnyvale

Create new tunnel to ZIA PSE in Frankfurt

Transform-set: ESP-null with ESP-md5-HMAC hash

FQDN for appropriate ZIA PSE

Set branch ID as source FQDN.

Select “Uplink VLAN”. Select Uplinks to use.

Shared secrets

Figure 19. Cloud security configuration

In the unlikely event that a Zscaler data center is unresponsive, Aruba sets up tunnels to different ZIA Public Service Edges and handles failover as part of the policy-based routing policy, as described in the Reference Architectures section.

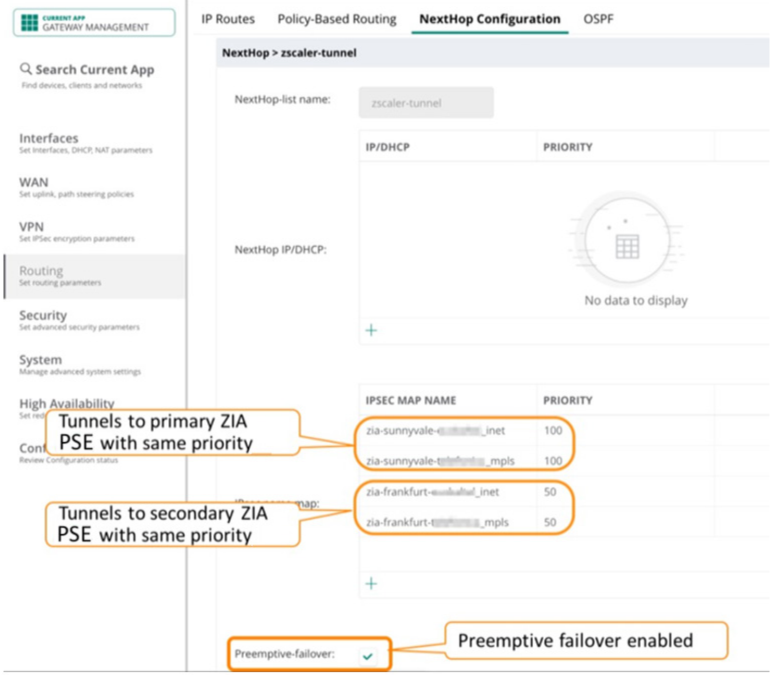
Policy-Based Routing

After you establish the tunnels between the BGWs and the ZIA services (regardless of whether this is done manually or using the orchestrated workflow), the next step is selecting the traffic to send through the ZIA service. This is done by leveraging the policy-based routing capabilities in the Aruba BGWs.

Create a Next-Hop List with the Tunnels

The BGWs establish tunnels with ZIA through all active uplinks. You must organize the tunnels in a next-hop-list so they are used by the routing policies.

1. Go to **Routing** > **Next Hop Configuration**.
2. Create a **Next Hop list**.
3. Add an IPSec map for Site-to-Site IPSec tunnels under **IPSec maps**.
   - Use the same priority for several paths from the same BGW.
   - Use different priorities for different Zscaler data centers.
4. Enable **Preemptive failover**.


CURRENT APP
GATEWAY MANAGEMENT
Search Current App
Find devices, clients and networks
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Conf
Review Configuration status
IP Routes
Policy-Based Routing
NextHop Configuration
OSPF
No data to display

NextHop > zscaler-tunnel

NextHop-list name: zscaler-tunnel

NextHop IP/DHCP:

IP/DHCP	PRIORITY

IPSEC MAP NAME	PRIORITY
zia-sunnyvale-[redacted]_inet	100
zia-sunnyvale-[redacted]_mpls	100
zia-frankfurt-[redacted]_inet	50
zia-frankfurt-[redacted]_mpls	50

Preemptive-failover: ✓

Tunnels to primary ZIA PSE with same priority

Tunnels to secondary ZIA PSE with same priority

Preemptive failover enabled

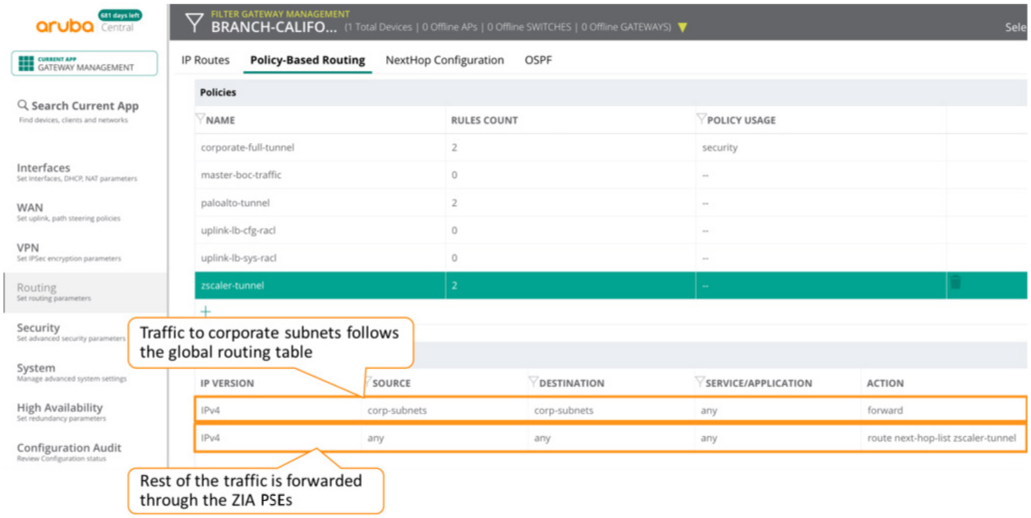
Figure 20. Add IPSec maps to next hop

In the case of the orchestrated mode, assign a higher priority to the primary tunnels. Assign the same priority to all tunnels to a given ZIA Public Service Edge.

Add Next-Hop to a Routing Policy

After the next-hop list with the tunnels to the ZIA is created, add it to a routing policy in the Routing > Policy- Based Routing.

In the following image, you can see that the next-hop-list, zscaler-tunnel, created in the previous section is added to the zscaler-tunnel policy. The policy sends all traffic to corporate subnets (an alias representing 10.0.0.0/8 and 172.16.0.0/12) through the regular path, and sends the rest of the traffic through the ZIA Public Service Edges.


aruba Central
681 days left
CURRENT APP GATEWAY MANAGEMENT
Search Current App
Find devices, clients and networks
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Set redundancy parameters
Configuration Audit
Review Configuration status
FILTER GATEWAY MANAGEMENT
BRANCH-CALIFO... (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)
Sele
IP Routes
Policy-Based Routing
NextHop Configuration
OSPF
Policies

NAME	RULES COUNT	POLICY USAGE
corporate-full-tunnel	2	security
master-boc-traffic	0	--
paloalto-tunnel	2	--
uplink-lb-cfg-racl	0	--
uplink-lb-sys-racl	0	--
zscaler-tunnel	2	--

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION
IPv4	corp-subnets	corp-subnets	any	forward
IPv4	any	any	any	route next-hop-list zscaler-tunnel

Traffic to corporate subnets follows the global routing table

Rest of the traffic is forwarded through the ZIA PSEs

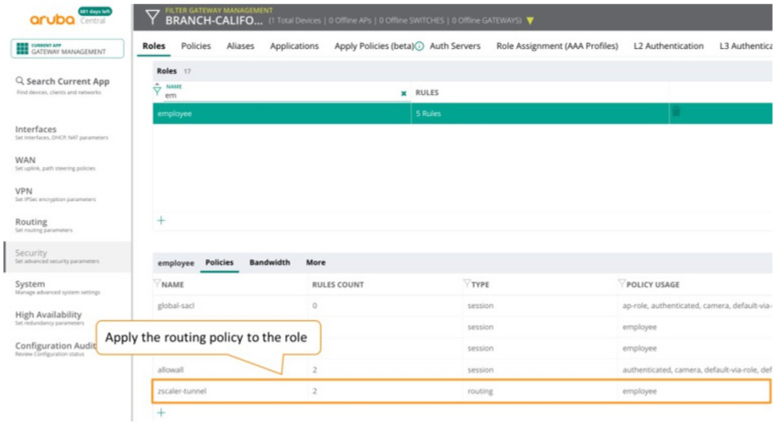
Figure 21. Routing policies

Apply Routing Policy

After creating the routing policy, apply the policy to the relevant traffic.

In the case of BGWs, apply the policies to the roles or VLANs of the devices that are sent through the ZIA service:

1. To apply the policy to a VLAN, go to **Security** > **Apply Policies** and select the policy from the drop-down menu next to each VLAN.
2. To apply the policy to a role, go to **Security** > **Roles** and edit the role that you want to send through ZIA by adding a routing policy.


aruba Central
681 days left
CURRENT APP GATEWAY MANAGEMENT
Search Current App
Find devices, clients and networks
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Set redundancy parameters
Configuration Audit
Review Configuration status
FILTER GATEWAY MANAGEMENT
BRANCH-CALIFO... (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)
Roles
Policies
Aliases
Applications
Apply Policies (beta)
Auth Servers
Role Assignment (AAA Profiles)
L2 Authentication
L3 Authentica
Roles 17
employee
Policies
Bandwidth
More

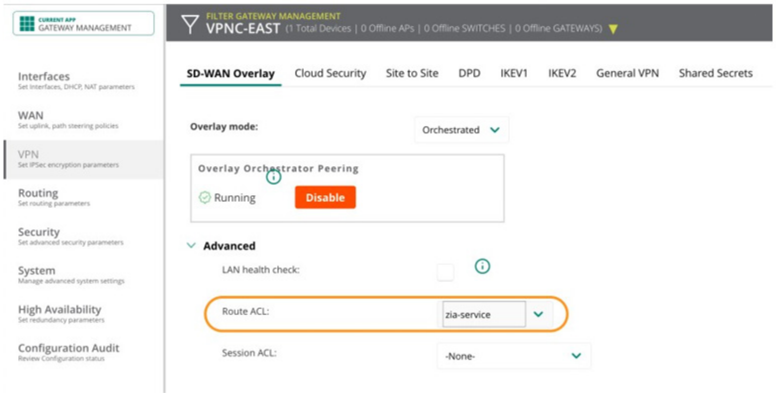
NAME em	RULES
employee	5 Rules

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated, camera, default-via-
		session	employee
		session	employee
allowall	2	session	authenticated, camera, default-via-role, def
zscaler-tunnel	2	routing	employee

Apply the routing policy to the role

Figure 22. Apply routing policy

In the case of VPNCs, the routing policy is normally applied to the incoming SD-WAN traffic. Navigate to **VPN** > **SDWAN Overlay** > **Advanced**.


CURRENT APP
GATEWAY MANAGEMENT
FILTER GATEWAY MANAGEMENT
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Set redundancy parameters
Configuration Audit
Review Configuration status
SD-WAN Overlay
Cloud Security
Site to Site
DPD
IKEV1
IKEV2
General VPN
Shared Secrets
Disable

VPNC-EAST (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

Overlay mode: Orchestrated

Overlay Orchestrator Peering

Running

Advanced

LAN health check: □

Route ACL: zia-service

Session ACL: -None-

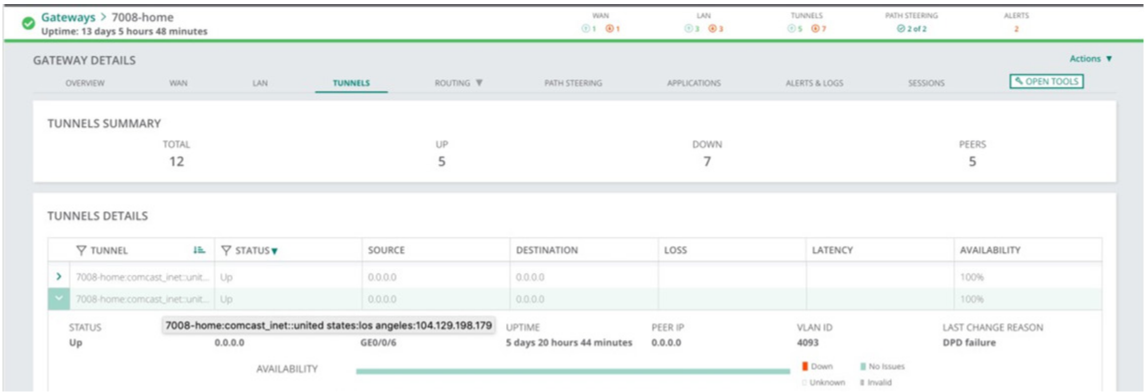
Figure 23. Apply routing policy to incoming SD-WAN overlay

Verification Steps

The following sections cover verifying Zscaler and Aruba configurations.

Aruba Central

You can verify the tunnel state from Aruba Central. Navigate to **Gateways** > **Tunnels** in the monitoring dashboard.



Gateways > 7008-home
Uptime: 13 days 5 hours 48 minutes

WAN	LAN	TUNNELS	PATH STEERING	ALERTS
1 1	3 3	5 7	2 of 2	2

GATEWAY DETAILS

TUNNELS SUMMARY

TOTAL	UP	DOWN	PEERS
12	5	7	5

TUNNELS DETAILS

	TUNNEL	STATUS	SOURCE	DESTINATION	LOSS	LATENCY	AVAILABILITY
›	7008-home:comcast_inet::unit...	Up	0.0.0.0	0.0.0.0			100%
˅	7008-home:comcast_inet::unit...	Up	0.0.0.0	0.0.0.0			100%

7008-home:comcast_inet::united states:los angeles:104.129.198.179

STATUS			UPTIME	PEER IP	VLAN ID	LAST CHANGE REASON
Up	0.0.0.0	GE0/0/6	5 days 20 hours 44 minutes	0.0.0.0	4093	DPD failure

AVAILABILITY

Figure 24. Monitoring tunnels to ZIA Public Service Edge

You can also verify the tunnel state through the site topology view.

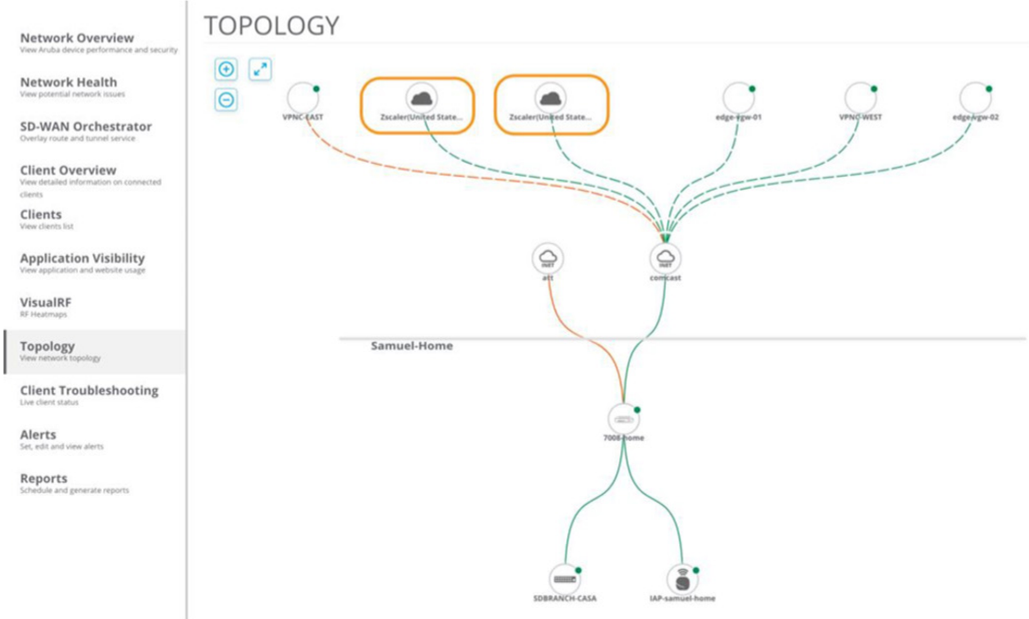
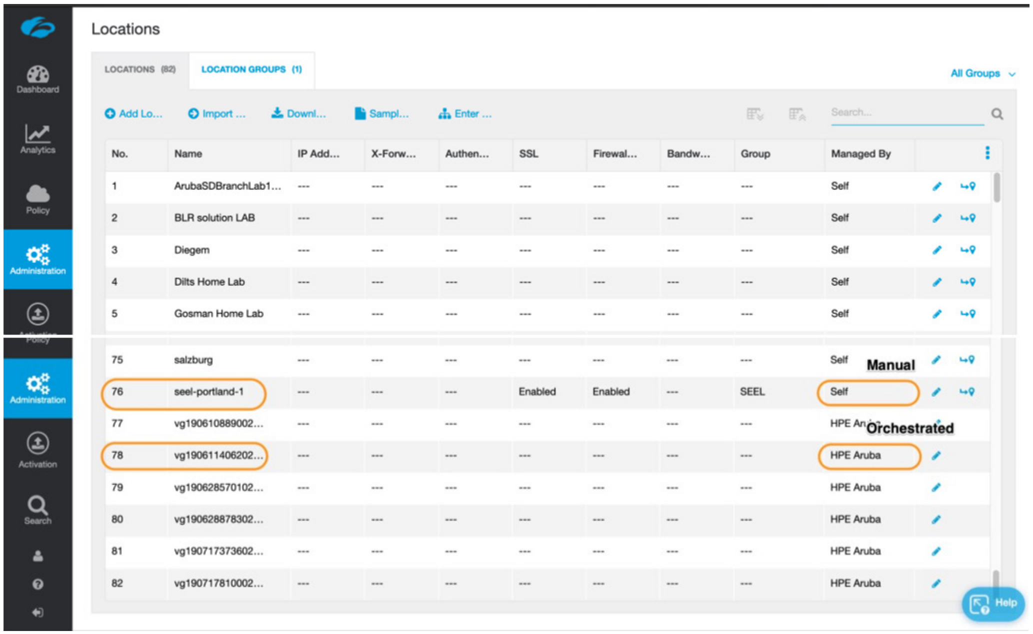


Figure 25. Tunnels to ZIA in Topology View

ZIA Admin Portal

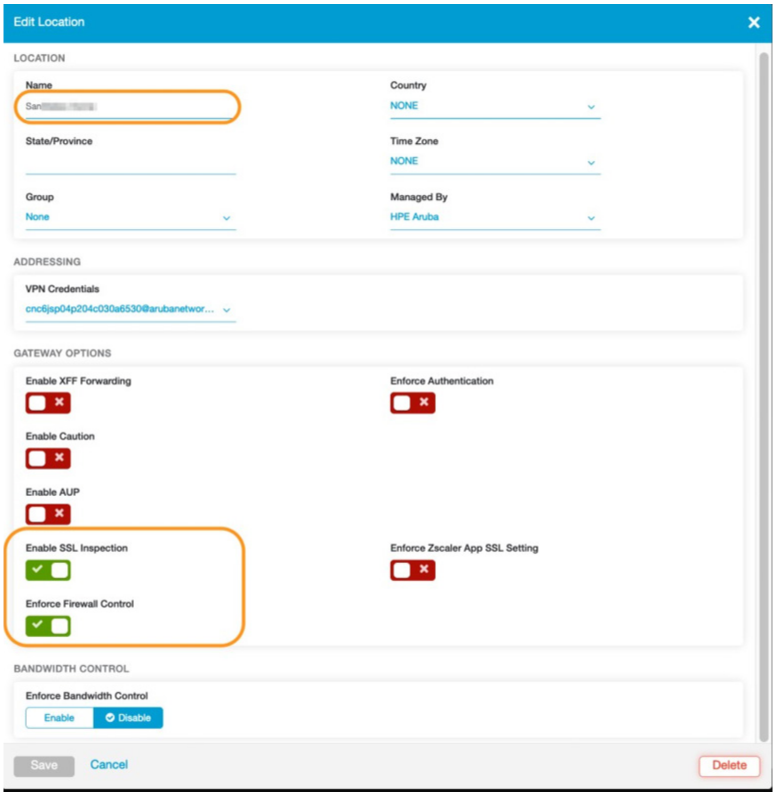
For orchestrated tunnels, it's important to verify that the API has created the necessary locations in the ZIA service (this may take a few minutes if the ZIA service API is overloaded). Manually created sites are displayed as Self, and orchestrated sites as HPE Aruba.



No.	Name	IP Add...	X-Forw...	Authen...	SSL	Firewal...	Bandw...	Group	Managed By
1	ArubaSDBranchLab1...	---	---	---	---	---	---	---	Self
2	BLR solution LAB	---	---	---	---	---	---	---	Self
3	Diegem	---	---	---	---	---	---	---	Self
4	Dilts Home Lab	---	---	---	---	---	---	---	Self
5	Gosman Home Lab	---	---	---	---	---	---	---	Self
75	salzburg	---	---	---	---	---	---	---	Self
76	seel-portland-1	---	---	---	Enabled	Enabled	---	SEEL	Self
77	vg190610889002...	---	---	---	---	---	---	---	HPE Ar
78	vg190611406202...	---	---	---	---	---	---	---	HPE Aruba
79	vg190628570102...	---	---	---	---	---	---	---	HPE Aruba
80	vg190628878302...	---	---	---	---	---	---	---	HPE Aruba
81	vg190717373602...	---	---	---	---	---	---	---	HPE Aruba
82	vg190717810002...	---	---	---	---	---	---	---	HPE Aruba

Figure 26. ZIA locations

After these locations (with the corresponding VPN credentials) are created, they can be edited at any time to enable additional security services or to provide a more easily recognizable name.


Edit Location

LOCATION

Name: San[redacted]

Country: NONE

State/Province:

Time Zone: NONE

Group: None

Managed By: HPE Aruba

ADDRESSING

VPN Credentials: cnc6jsp04p204c030a6530@arubanetwor...

GATEWAY OPTIONS

Enable XFF Forwarding: ✗

Enforce Authentication: ✗

Enable Caution: ✗

Enable AUP: ✗

Enable SSL Inspection: ✓

Enforce Zscaler App SSL Setting: ✗

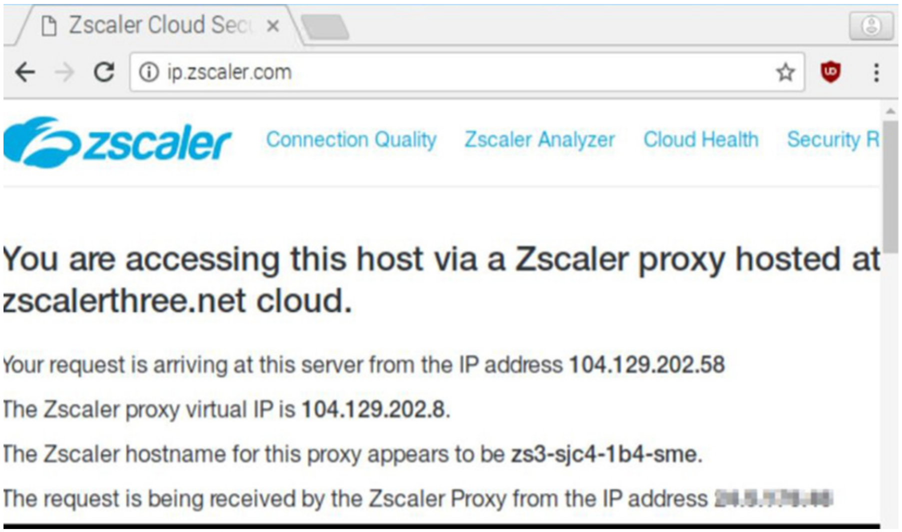
Enforce Firewall Control: ✓

BANDWIDTH CONTROL

Enforce Bandwidth Control: Enable [✓ Disable]

Figure 27. Edit location

The client device can also connect to https://ip.zscaler.com. This page is displayed if the client is browsing the internet through the ZIA service and verifies which node that the traffic is coming from.



You are accessing this host via a Zscaler proxy hosted at zscalerthree.net cloud.

Your request is arriving at this server from the IP address **104.129.202.58**

The Zscaler proxy virtual IP is **104.129.202.8**.

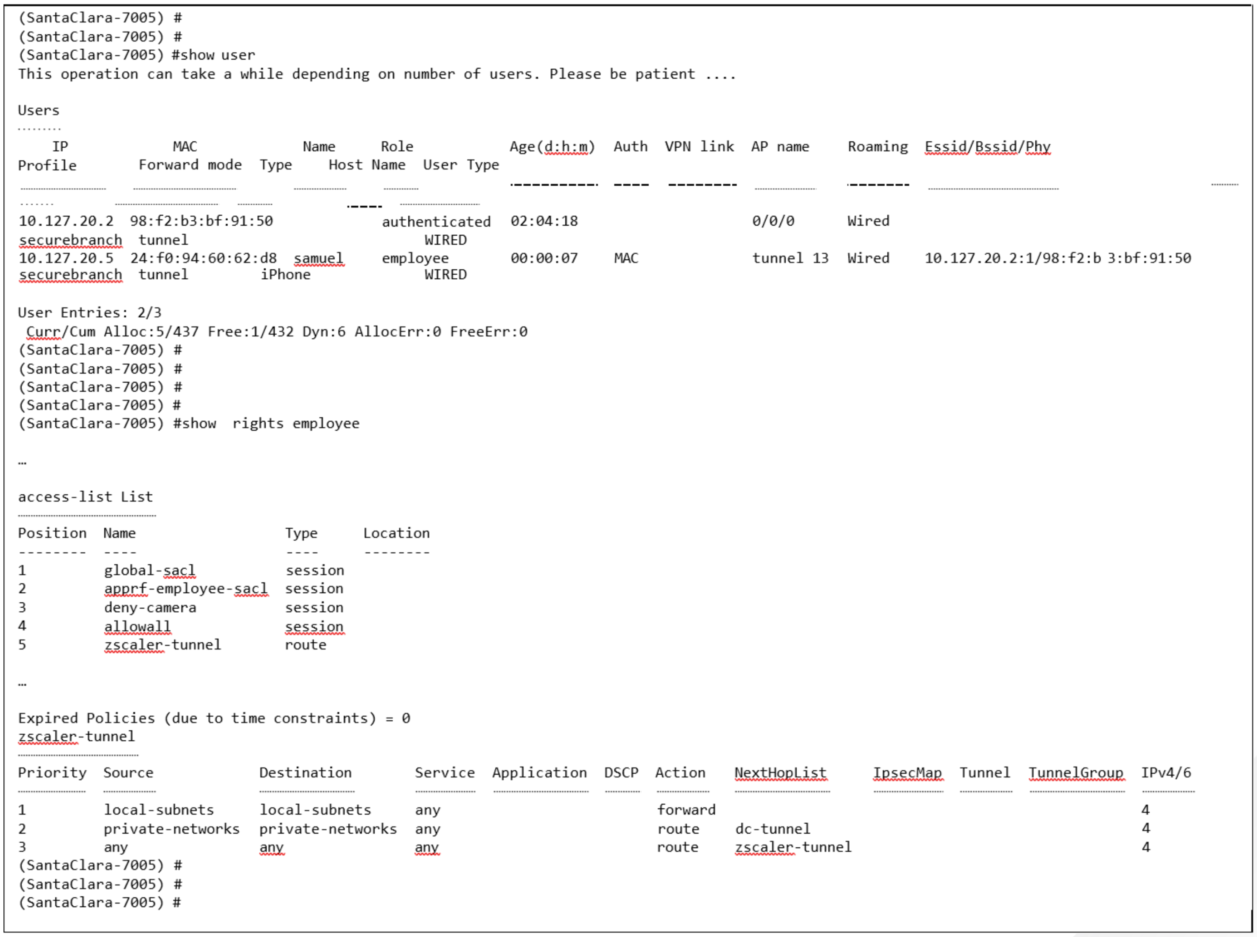
The Zscaler hostname for this proxy appears to be **zs3-sjc4-1b4-sme.**

The request is being received by the Zscaler Proxy from the IP address [redacted]

Figure 28. Zscaler verification page

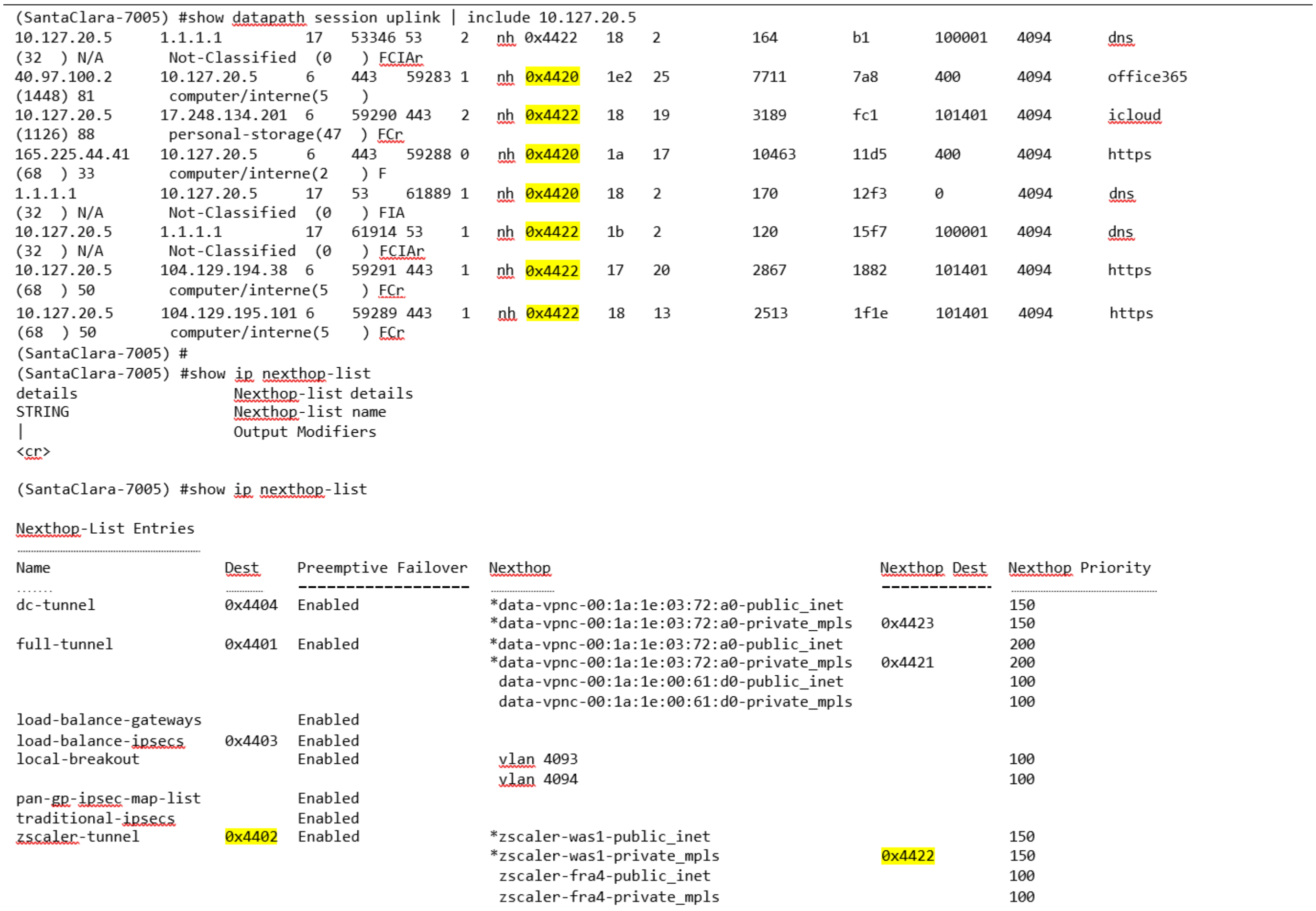
Aruba Gateways

You can test further by connecting to the Gateway's CLI either via SSH or through the remote console provided in Aruba Central. The Gateway shows how the device is in a role (employee) that has a routing policy associated.



```
(SantaClara-7005) #
(SantaClara-7005) #
(SantaClara-7005) #show user
This operation can take a while depending on number of users. Please be patient ....

Users
.........
    IP           MAC           Name    Role         Age(d:h:m)  Auth  VPN link  AP name    Roaming  Essid/Bssid/Phy
Profile      Forward mode  Type    Host Name  User Type
                                                    ----------  ----  --------             -------
.......                                      ----
10.127.20.2  98:f2:b3:bf:91:50          authenticated  02:04:18                 0/0/0      Wired
securebranch  tunnel                            WIRED
10.127.20.5  24:f0:94:60:62:d8  samuel  employee       00:00:07     MAC         tunnel 13  Wired    10.127.20.2:1/98:f2:b 3:bf:91:50
securebranch  tunnel       iPhone               WIRED

User Entries: 2/3
 Curr/Cum Alloc:5/437 Free:1/432 Dyn:6 AllocErr:0 FreeErr:0
(SantaClara-7005) #
(SantaClara-7005) #
(SantaClara-7005) #
(SantaClara-7005) #
(SantaClara-7005) #show  rights employee

…

access-list List
................
Position  Name                  Type     Location
--------  ----                  ----     --------
1         global-sacl           session
2         apprf-employee-sacl   session
3         deny-camera           session
4         allowall              session
5         zscaler-tunnel        route

…

Expired Policies (due to time constraints) = 0
zscaler-tunnel
..............
Priority  Source             Destination      Service  Application  DSCP  Action   NextHopList     IpsecMap  Tunnel  TunnelGroup  IPv4/6
1         local-subnets      local-subnets    any                          forward                                                4
2         private-networks   private-networks any                          route    dc-tunnel                                     4
3         any                any              any                          route    zscaler-tunnel                                4
(SantaClara-7005) #
(SantaClara-7005) #
(SantaClara-7005) #
```

The Gateway also shows how the device is going to public destinations (and returning from them) through ZIA.



```
(SantaClara-7005) #show datapath session uplink | include 10.127.20.5
10.127.20.5     1.1.1.1         17   53346 53    2   nh 0x4422   18   2          164        b1       100001   4094      dns
(32  ) N/A       Not-Classified  (0    ) FCIAr
40.97.100.2     10.127.20.5     6    443   59283 1   nh 0x4420   1e2  25         7711       7a8      400      4094      office365
(1448) 81        computer/interne(5    )
10.127.20.5     17.248.134.201  6    59290 443   2   nh 0x4422   18   19         3189       fc1      101401   4094      icloud
(1126) 88        personal-storage(47  ) FCr
165.225.44.41   10.127.20.5     6    443   59288 0   nh 0x4420   1a   17         10463      11d5     400      4094      https
(68  ) 33        computer/interne(2    ) F
1.1.1.1         10.127.20.5     17   53    61889 1   nh 0x4420   18   2          170        12f3     0        4094      dns
(32  ) N/A       Not-Classified  (0    ) FIA
10.127.20.5     1.1.1.1         17   61914 53    1   nh 0x4422   1b   2          120        15f7     100001   4094      dns
(32  ) N/A       Not-Classified  (0    ) FCIAr
10.127.20.5     104.129.194.38  6    59291 443   1   nh 0x4422   17   20         2867       1882     101401   4094      https
(68  ) 50        computer/interne(5    ) FCr
10.127.20.5     104.129.195.101 6    59289 443   1   nh 0x4422   18   13         2513       1f1e     101401   4094      https
(68  ) 50        computer/interne(5    ) FCr
(SantaClara-7005) #
(SantaClara-7005) #show ip nexthop-list
details                  Nexthop-list details
STRING                   Nexthop-list name
|                        Output Modifiers
<cr>

(SantaClara-7005) #show ip nexthop-list

Nexthop-List Entries
--------------------

Name                   Dest    Preemptive Failover  Nexthop                                     Nexthop Dest  Nexthop Priority
----                   ----    -------------------  -------                                     ------------  ----------------
dc-tunnel              0x4404  Enabled              *data-vpnc-00:1a:1e:03:72:a0-public_inet                  150
                                                    *data-vpnc-00:1a:1e:03:72:a0-private_mpls   0x4423        150
full-tunnel            0x4401  Enabled              *data-vpnc-00:1a:1e:03:72:a0-public_inet                  200
                                                    *data-vpnc-00:1a:1e:03:72:a0-private_mpls   0x4421        200
                                                     data-vpnc-00:1a:1e:00:61:d0-public_inet                  100
                                                     data-vpnc-00:1a:1e:00:61:d0-private_mpls                 100

load-balance-gateways          Enabled
load-balance-ipsecs    0x4403  Enabled
local-breakout                 Enabled               vlan 4093                                                100
                                                     vlan 4094                                                100

pan-gp-ipsec-map-list          Enabled
traditional-ipsecs             Enabled
zscaler-tunnel         0x4402  Enabled              *zscaler-was1-public_inet                                 150
                                                    *zscaler-was1-private_mpls                  0x4422        150
                                                     zscaler-fra4-public_inet                                 100
                                                     zscaler-fra4-private_mpls                                100
```

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support, select **Administration** > **Settings** > **Company Profile**.

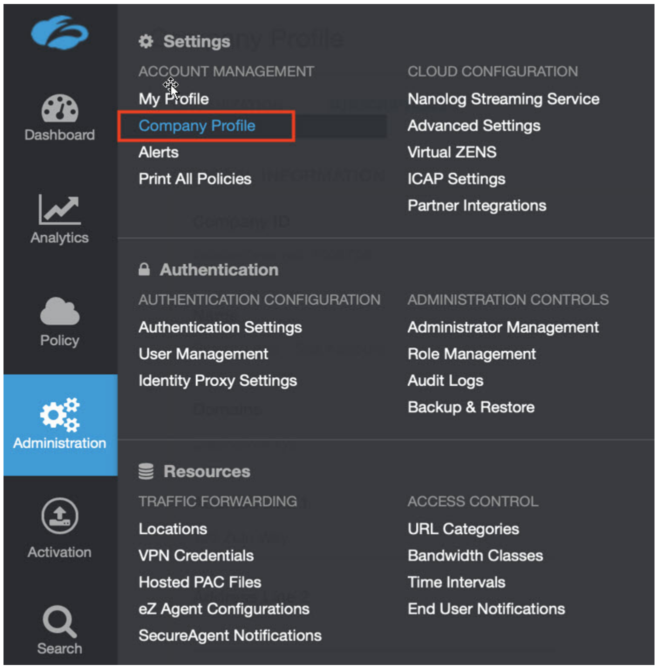
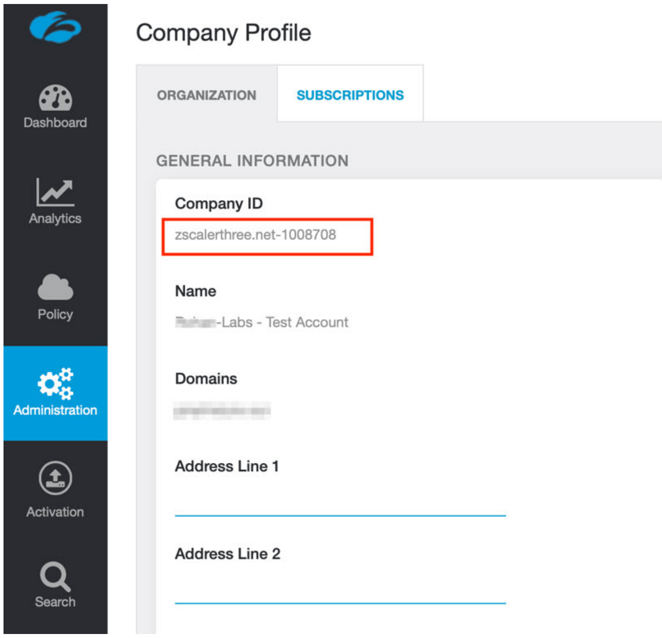


Figure 29. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 30. Company ID

Enter Support Section

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

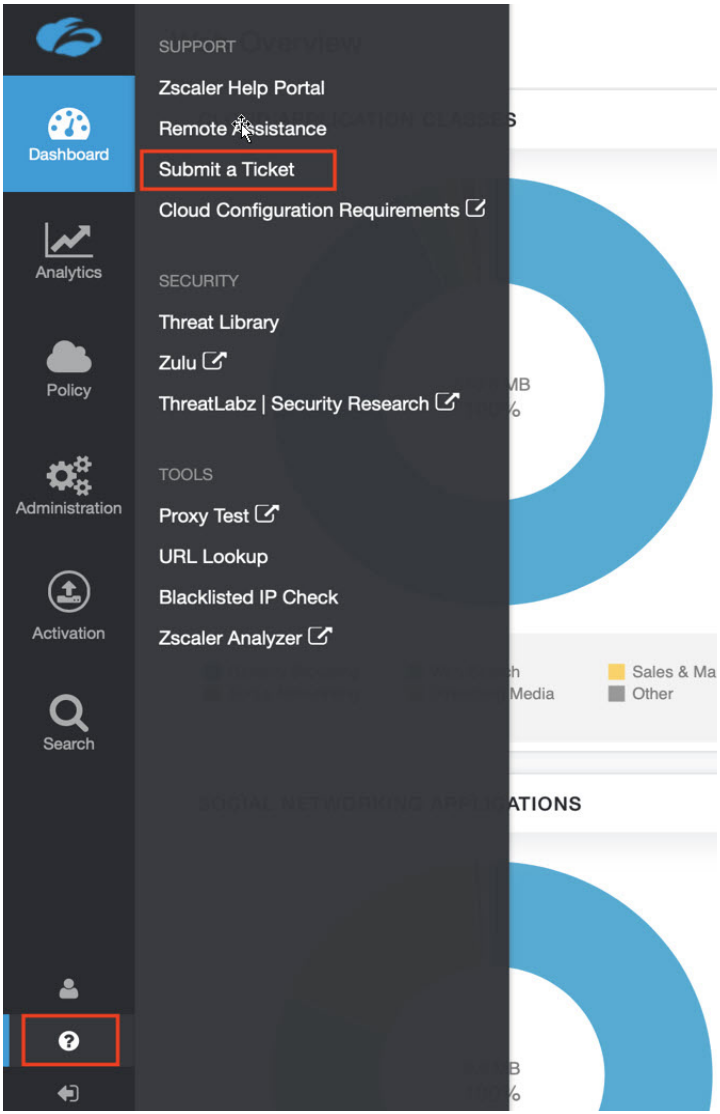


Figure 31. Submit a Ticket