Copyright Information
Copyright © 2019 Hewlett Packard Enterprise Development LP.

Open Source Code
This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA
# Contents

Revision History ................................................................. 4  
Introduction—Security in Aruba SD-Branch ............................... 5  
  Security layers .................................................................. 6  
ZIA Integration Overview .................................................... 7  
  Tunnel establishment.......................................................... 8  
  Policy-Based Routing ......................................................... 10  
Reference Architectures ....................................................... 11  
  Branch Gateways to ZIA..................................................... 11  
  Headend Gateway (VPNC) to ZIA ....................................... 13  
  Redundancy of ZIA nodes .................................................. 14  
  Branch Gateway Redundancy ............................................. 15  
Configuration Workflows ..................................................... 16  
  Tunnel establishment......................................................... 16  
  Policy-Based Routing ......................................................... 23  
Verification Steps ............................................................... 26
1 Revision History
The following table lists the revisions of this document:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>2019-07-25</td>
<td>Samuel Pérez Buñuel</td>
<td>Added Orchestrated workflow and reference architectures</td>
</tr>
<tr>
<td>1.1</td>
<td>2018-10-18</td>
<td>Samuel Pérez Buñuel</td>
<td>Updated configuration screenshots</td>
</tr>
<tr>
<td>1.0</td>
<td>2018-07-17</td>
<td>Samuel Pérez Buñuel</td>
<td>Initial version</td>
</tr>
</tbody>
</table>

*Table 1 - Revision history*

Note:

ZIA Public Service Edge was previously known as "Zscaler Enforcement Node" or "ZEN". This document may still reference ZEN in some text or pictures.
2 Introduction — Security in Aruba SD-Branch

Security is an integral part of the Aruba SD-Branch solution. First and foremost, because the solution is built from the ground up to be completely policy-driven (or, in Aruba terms, role-based). Secondly, because of the fact that in most cases branches will be directly exposed to the Internet, which will require very robust hardening policies. And lastly, due to the firm belief that “best-of-breed” security should also be built around branch networks.

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.

![Figure 1 - SD-Branch Security Layers](image-url)
2.1 Security layers

First of all, the Aruba Gateways use ArubaOS, which is a tightly hardened 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 3200 applications.
- **Web content and reputation filtering**: using WebRoot's machine learning technology to classify content, reputation, and geolocation for billions of URLs.

Secondly, the Aruba SD-Branch solution can integrate with ClearPass (or other AAA servers) to form a true 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 can be enhanced by leveraging integrations with the 140+ partners in the 360 Secure exchange program. And it can be pushed even further by integrating with Aruba Introspect for User Entity and Behavioral Analytics (UEBA).

Lastly, the Aruba SD-Branch solution can integrate with best-of-breed 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’s Security as a Service offering, provides an extremely simple and scalable solution for advanced threat protection in branch networks.
3 ZIA Integration Overview

A common network architecture today is to tunnel traffic between a HQ and branches over either MPLS or dedicated encrypted VPN links. As more and 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 may 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 Zscaler Internet Access (ZIA) service. This enables best-of-breed security, with services like advanced threat protection or Data Loss Prevention (detailed information can be found in the Zscaler documentation) without the need to increase the footprint in branch locations.

Figure 2 — SD-Branch integration with Zscaler Cloud Security Infrastructure
3.1 Tunnel establishment

The Zscaler security as a service suite is delivered by 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 Enforcement Nodes) and logging/statistics plane (Zscaler Nanolog Servers). It is distributed across more than 100 data centers on 6 continents, which means that users are always a short hop away from their applications (source: Zscaler).

Zscaler Internet Access is a secure Internet and web gateway delivered as a service from the cloud. To integrate with this service, all the SD-WAN solution needs to do is establish tunnels with the nearest ZIA node(s) to send Internet-bound traffic through them (source: Zscaler).

Both Aruba as well as the ZIA service support establishing communications through IPSec or GRE tunnels. The drawback of using GRE, however, is that tunnels won’t be able to traverse NAT boundaries, very common in branch environment. For this reason, this Technical Note will focus on the implementation based on IPSec tunnels.

3.1.1 Tunnel Details

The tunnels between the Aruba Branch Gateway and the ZIA Public Service Edge* (ZENs) use IPSec with null encryption. This provides the ability to traverse NAT boundaries and leverage IKEv2 for authentication, while at the same time limiting the overhead. All that would be required to bring up the tunnels is to set up accounts in Zscaler for the Branch Gateways and have them authenticate themselves using them. Such tunnels can be established manually or by using the SD-WAN Orchestrator service available in the Aruba SD-Branch solution.

A summary of the tunnel characteristics is provided in the following table:

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

*July 2020: ZIA Public Service Edge is the new name for what was previously known as “Zscaler Enforcement Node” or ZEN. The remainder of the document will use the new short form of ZEN.
3.1.2 Tunnel Orchestration

Aruba Gateways can be configured to 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 Gateways to bring up tunnels to the nearest ZEN* nodes to send the traffic through them. In the case of large-scale deployments this 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 (more information can be found in 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 Gateways and the nearest Zscaler Public Service Edge node. Performed by executing

1. **Bind Aruba Gateways with the nearest ZEN* nodes.** The Orchestrator queries the ZIA service for the nearest node(s) 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 Gateways in the selected groups through the ZIA APIs. Unique VPN credentials are also created for each Gateway.

3. **Orchestrate tunnels.** The SD-WAN Orchestrator instructs each Gateway to establish tunnels with the nearest Zscaler Public Service Edge nodes using the credentials negotiated in step 2.

*July 2020. ZIA Public Service Edge is the new name for what was previously known as “Zscaler Enforcement Node” or ZEN. The remainder of this document will use the old short form of ZEN.*
3.2 Policy-Based Routing

Once the tunnels are established, the next step would be to 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 to be sent through the ZIA service.

The following parameters can be taken into consideration when determining traffic types to be sent through the ZIA service:

- **VLAN/User Role**: PBR 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 PBR policies.

The following figure illustrates how Aruba Gateways selectively redirect traffic to ZIA; In this example, cameras are full-tunneled to the DC, 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*
4 Reference Architectures

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

4.1 Branch Gateways to ZIA

Aruba BGWs can establish tunnels to one or several Zscaler Public Service Edge nodes (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, thus providing high availability. The solution supports manually setting the destination Zscaler Public Service Edge node for each BGW. It also provides the possibility of using the SD-WAN Orchestrator learn the closest node for each branch and automatically establish the tunnels to it.

![Tunnel to Nearest Node Diagram](image)

*Figure 5 - Tunnel to Nearest Node*
4.1.1 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 Branch Gateway would simply set up a tunnel from every WAN interface.

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

An example workflow would look like this:

- ClearPass (or another RADIUS server) assigns the role "PoS" to the device
- The firewall classifies the session as “Payment”.
- The routing for a PoS device using a “Payment” app states that the next-hop is a certain ZIA node, and the paths are, for example: INET and LTE
- Because the traffic is classified as "Payment", it's handled by the DPS policy "Payment". This policy has INET as preferred path, as well as an SLA that has to be met.
- If the measured values for INET meet the SLA for the “Payment” policy the session goes through the tunnel that’s established using the INET uplink. If at any point in time the measured SLA for INET drops, the Gateway will steer it to any other active tunnel that’s meeting the SLA. If no circuit meets the SLA, the system will choose the one that deviates the least from the configured SLA.

![Figure 6 - Dynamic path steering](image-url)
4.2 Headend Gateway (VPNC) to ZIA

It often happens that branch traffic is aggregated at a local hub and then routed to the Internet or to other corporate resources. This case is especially common when using private WAN networks. In such scenarios, Aruba VPNCs can set up tunnels to the nearest Zscaler Public Service Edge node to have branch traffic go through additional security validations.

Both hardware as well as virtual (vGWs in private instances of Public Cloud) headend Gateways are supported in this model.
4.3 Redundancy of ZIA Public Service Edge Nodes

As shown in the section above, the load-balancing and Dynamic Path Selection mechanisms would take care of WAN circuit redundancy. However, that may not be sufficient in the unlikely event that a ZEN node would become unavailable. In order to address that, the Aruba SD-Branch integration with Zscaler makes use of the Dead Peer Detection (DPD) protocol to ensure the traffic doesn’t get blackholed.

Figure 8 - Zscaler Public Service Edge redundancy

Tunnels to redundant ZIA nodes are supported for both topologies displayed above; Branch Gateways to ZIA and Headend Gateways to ZIA.
4.4 Branch Gateway Redundancy

When redundancy is required inside the branch, SD-WAN Gateways can share uplink interfaces with their HA pairs. This is done by establishing a virtual uplink through the LAN to share such interfaces. The result, as shown in the image below, is that each Branch Gateway would have “physical” uplinks as well as “virtual” uplinks.

![Figure 9 - Branch HA](image)

In a scenario like this, each Branch Gateway establishes tunnels to the ZIA service through all uplink interfaces (physical and virtual). Both BGWs can be defined in ZIA as a single “Location” and use the same VPN credentials, or as 2 “Locations” with different credentials for each Gateway. Both operating modes are supported.

![Figure 10 - ZIA tunnels with Branch HA](image)
5 Configuration Workflows

5.1 Tunnel establishment

The integration between Aruba and ZIA can be manually configured or it can leverage the SD-WAN Orchestrator to streamline the process of creating “Locations” and VPN credentials in the ZIA service, as well as bringing up the tunnels in the BGWs.

5.1.1 Orchestrated Tunnel Establishment

As mentioned above, the integration between Aruba SD-Branch and the ZIA service can make use of the SD-WAN Orchestrator to automate large distributed deployments. The following configuration steps should be followed:

5.1.1.1 Configuring ZIA for API access

No “Locations” or VPN credentials have to be created in the Zscaler portal in the automated workflow, as the SD-WAN Orchestrator does this through the API. For that to happen, the SD-WAN Orchestrator will need “partner” access to communicate through the API.

To add a partner key for Aruba SD-Branch, complete the following steps:

1. Log in to the Zscaler admin portal.
2. Click Administration > Partner Integrations > SD-WAN in the Partner Integrations page in the ZIA portal.

Click Add Partner Key. Create a Partner Key.

![Figure 11 - Create Partner API Key](image-url)
3. Create a **Partner Administrator Role** to provide credentials for the API access. This is done from Administration > Role Management:

![Figure 12 - Create Partner Role](image)

4. Create a partner account for the SD-WAN Orchestrator. This can be done from Administration > Administrator Management:

![Figure 13 - Create partner account](image)
5.1.1.2 Configuring Aruba SD-WAN for Orchestrated Tunnels

1. To enable orchestration of tunnels, enter the partner credentials and API Key for the SD-WAN Orchestrator to communicate to the ZIA service. This can be configured from **Global Settings > SDWAN > Cloud Security**.

   ![Enable Automatic establishment of tunnels to ZIA service](image)

   Figure 14 – Enable Automatic establishment of tunnels to ZIA service

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

   ![Select Groups to tunnel to ZIA](image)

   Figure 15 - Select Groups to tunnel to ZIA

After you enable the Orchestrated Zscaler integration in Aruba Central, the SD-WAN Orchestrator will instruct the Gateways to establish tunnels to all ZIA nodes 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.
5.1.2 Manual Tunnel Establishment

As described in the overview, the integration with ZIA will require configurations on both the Zscaler admin portal as well as in Aruba Central. These configuration steps, however, will be greatly streamlined by the fact that the ZIA service always sends return traffic through the traffic originating the session (removing the need for routing exchanges).

5.1.2.1 Pre-requisites

The first step before configuring ZIA is to locate the FQDN of the ZIA instance that will be used. For more information, see the documentation at: https://support.zscaler.com/hc/en-us/articles/211692786-How-do-I-locate-the-ZEN-IP-addresses-for-my-IPsec-VPN-tunnels.

<table>
<thead>
<tr>
<th>Location</th>
<th>IP Address (CIDR Notation)</th>
<th>Proxy Hostname</th>
<th>GRE Virtual IP</th>
<th>VPN Host Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frankfurt IV</td>
<td>165.225.72.0/22</td>
<td>fra4.sme.zscalerbeta.net</td>
<td>165.225.72.38</td>
<td>fra4-vpn.zscalerbeta.net</td>
<td></td>
</tr>
<tr>
<td>US &amp; Canada</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>San Francisco IV</td>
<td>199.168.148.0/23</td>
<td>sunnyvale1.sme.zscalerbeta.net</td>
<td>199.168.148.131</td>
<td>sunnyvale1-vpn.zscalerbeta.net</td>
<td></td>
</tr>
<tr>
<td>Washington DC</td>
<td>104.128.194.0/23</td>
<td>was1.sme.zscalerbeta.net</td>
<td>104.128.194.38</td>
<td>was1-vpn.zscalerbeta.net</td>
<td></td>
</tr>
<tr>
<td>Future Data centers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upcoming DC I</td>
<td>185.46.212.0/22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upcoming DC II</td>
<td>104.120.192.0/20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upcoming DC III</td>
<td>165.225.0.0/17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upcoming DC IV</td>
<td>165.225.192.0/18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global ZEN IP addresses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>185.46.212.88</td>
<td>185.46.212.89</td>
<td>185.46.212.90</td>
<td>185.46.212.91</td>
<td></td>
</tr>
<tr>
<td></td>
<td>185.46.212.92</td>
<td>185.46.212.93</td>
<td>185.46.212.97</td>
<td>185.46.212.98</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 16 - Locate Zscaler Public Service Edge nodes*
5.1.2.2 Configuring ZIA

The first step would be to configure the ZIA service to receive VPN tunnels from Aruba Gateways. As described above, these would be IPSec tunnels using IKEv2 credentials to uniquely identify each Gateway. Each Gateway would therefore have to be assigned a “Location” in the Zscaler admin portal, as well as the corresponding VPN credentials.

To configure ZIA service:

1. Log in to the Zscaler portal.
2. Navigate to Administration > Resources > VPN-Credentials. Click Add VPN Credential. Once there, select FQDN and type the UserID and password to be used for a given location (or set of locations).

![Figure 17 - Create VPN Credential](image-url)
Once the credential is set the next step would be to set up a “Location”. This location can be used to identify a certain site or a group of sites.

1. Navigate to Administration > Resources > Locations.
2. Choose Add Location. Add name, address, and time zone.
3. Select the previously created VPN credentials. Why are the credentials associated to the location?

![Edit Location](image)

**Figure 18 - Edit location**

### 5.1.2.3 Configuring Aruba Gateways to Manually establish tunnels to ZIA

As explained in the overview section, the Aruba Branch Gateway would set up tunnels to ZIA through every WAN interface. This is configured from **VPN > Cloud Security** page in Aruba Central. Once there, configure the following parameters:

- **Name** — administrative name for the tunnel
- **Priority** — Admin ID for the tunnel.
- **Transform** — Set ESP-null encryption with ESP-md5-HMAC hash
- **Destination Gateway FQDN** — Set the FQDN for the Zscaler Public Service Edge nodes.
- **Source FQDN** — Set the user ID created in ZIA (santaclara@hpe.com in the example above).
- **Uplink VLAN/VLAN** — When tunneling from a Branch Gateway, select the Uplink VLAN(s) to be used to bring up tunnels to ZIA. In the case of VPNCs, simply select the VLAN from which the tunnels will be initiated.
- **IKE Shared Secret** — Set the same value created in the Zscaler configuration
Figure 19 - Cloud Security configuration

In the case of VPNCs, instead of “Uplink VLAN” simply select the VLAN from which tunnels to the ZIA service would be initiated.

In the unlikely event that a Zscaler datacenter may go down, the solution is capable of setting up tunnels to different ZIA Public Service Edge node and handle failover as part of the PBR policy, as described in the Reference Architectures section.
5.2 Policy-Based Routing

Once the tunnels between the BGWs and the ZIA service are established (regardless of whether this is done manually or using the orchestrated workflow), the only remaining step would be to select which traffic is to be sent through the ZIA service. This is done by leveraging the PBR capabilities in the Aruba BGWs.

5.2.1.1 Create a Next-Hop List with the Tunnels

The Branch Gateways will establish tunnels with ZIA through all active uplinks. The next step would then be to organize the tunnels in a “next-hop-list” so they can be used by the routing policies. This can be done by going to Routing > Next Hop Configuration.

1. Create a Next Hop list.
2. Add an IPsec map for Site-to-Site” IPSec tunnels under IPSec maps
3. Use the same priority for several paths from the same Gateway
4. Use different priorities for different Zscaler datacenters.
5. Ensure that Preemptive failover is enabled.

![Figure 20 - Add IPSec maps to Next Hop](image)

In the case of the orchestrated mode, ensure that you assign a higher priority to the “primary” tunnels. The same priority should be assigned to all tunnels to a given node.
5.2.1.2 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 example below, the policy is sending all the traffic to corporate subnets (an alias representing 10.0.0.0/8 and 172.16.0.0/12) through the regular path, and it’s sending the rest of the traffic through the ZIA Public Service Edge nodes.
5.2.1.3 Apply Routing Policy

After the routing policy is created, the last step would be to apply it to the relevant traffic.

In the case of Branch Gateways, these policies would be applied to the roles or VLANs where we have the devices that have to be sent through the ZIA service:

- To apply the policy to a VLAN, go to Security > Apply Policies and select the policy from the dropdown next to each VLAN.
- To apply the policy to a role, go to Security > Roles” and edit the role you want to send through ZIA by adding a routing policy (routing policies always come at the end).

In the case of VPNCs, the routing policy would normally be applied to the incoming SD-WAN traffic. This can be configured in the VPN > SDWAN Overlay > Advanced section.
6 Verification Steps

6.1 Aruba Central

The state of the tunnels can easily be verified from the interface of Aruba Central. This can be checked from the Tunnels tab in the Gateway monitoring dashboard.

Figure 24 - Monitoring tunnels to ZEN nodes

It can also be verified through the site topology view.

Figure 25 - Tunnels to ZIA in Topology View
6.2 Zscaler Admin portal

In the case of 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 will be displayed as “Self”, and orchestrated sites as "HPE Aruba".

![ZIA locations](image)

*Figure 26 - ZIA locations*
It’s important to note that, once 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](image)

*Figure 27 - Edit Location*
As a last verification, the client device can connect to https://ip.zscaler.com. This page shows if the client is browsing the Internet through a the ZIA service and from which node the traffic is coming from.

Figure 28 – Zscaler verification Page
6.3 Aruba Gateways

Further testing can be done to 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) #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>Name</th>
<th>Role</th>
<th>Age(d:h:m)</th>
<th>Auth</th>
<th>VPN link</th>
<th>AP name</th>
<th>Roaming</th>
<th>Essid/Bssid/Phy</th>
<th>Profile</th>
<th>Forward mode</th>
<th>Type</th>
<th>Host Name</th>
<th>User Type</th>
</tr>
</thead>
</table>
| 10.127.20.2  | 98:f2:b3:bf:91:50 | authenticated | 02:04:18 | 0/0/0 | Wired
| securebranch | tunnel         | WIRED    | securebranch  | tunnel | IWRED |

User Entries: 2/3

(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 any forward 164 b1 100001 4094 dns
2 private-networks private-networks any any route 7711 7a8 400 4094 office365
global-sacl route 3189 fc1 101401 4094 icloud
3 any any any any route 10463 11d5 400 4094 https
4 any any any any route 1867 12f3 170 4094 dns
5 any any any any route 0 4094

(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
10.127.20.5 1126 88 1a 17 10463 11d5 400 4094 office365
10.127.20.5 124 64 170 12f3 0 4094 dns
10.127.20.5 1865 41 1867 12f3 170 4094 dns
10.127.20.5 1865 41 128 15f7 150101 4094 dns
```

(SantaClara-7005) #
10.127.20.5 104.129.195.101 6 59289 443 1 nh 0x4422 18 13 2513 1fel 101401 4094 https
(SantaClara-7005) # show ip nexthop-list
details Nexthop-list details
STRING Nexthop-list name |
<cr>
(SantaClara-7005) # show ip nexthop-list

Next-hop-List Entries
---------------------
<table>
<thead>
<tr>
<th>Name</th>
<th>Dest</th>
<th>Preemptive Failover</th>
<th>Nexthop</th>
<th>Nexthop Dest</th>
<th>Nexthop Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>dc-tunnel</td>
<td>0x4404</td>
<td>Enabled</td>
<td>*data-vpnc::00:1a:1e:03:72:a0-public_inet</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*data-vpnc::00:1a:1e:03:72:a0-private_mpls 0x4423</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>full-tunnel</td>
<td>0x4401</td>
<td>Enabled</td>
<td>*data-vpnc::00:1a:1e:03:72:a0-public_inet</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*data-vpnc::00:1a:1e:03:72:a0-private_mpls 0x4421</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>data-vpnc::00:1a:1e:00:61:d0-public_inet</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>data-vpnc::00:1a:1e:00:61:d0-private_mpls</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>load-balance-gateways</td>
<td>Enabled</td>
<td></td>
<td>vlan 4093</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>load-balance-ipsecs</td>
<td>0x4403</td>
<td>Enabled</td>
<td>vlan 4094</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>local-breakout</td>
<td>Enabled</td>
<td></td>
<td>vlan 4004</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>pan-gp-ipsec-map-list</td>
<td>Enabled</td>
<td></td>
<td>vlan 4093</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>traditional-ipsecs</td>
<td>Enabled</td>
<td></td>
<td>vlan 4094</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>zscaler-tunnel</td>
<td>0x4402</td>
<td>Enabled</td>
<td>*zscaler-was1-public_inet</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*zscaler-was1-private_mpls 0x4422</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>zscaler-fra4-public_inet</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>zscaler-fra4-private_mpls</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
7 Reference

Aruba SD-Branch Fundamentals Guide:


Mid-Size Deployment Guide:


Aruba SD-Branch Online Documentation:

- https://www.arubanetworks.com/seamless-sd-wan-orchestration/

Zscaler Tools/Documentation:

- https://www.zscaler.com/products/cloud-architecture-security-as-a-service
- Zcaler Getting Started: https://help.zscaler.com/zia/getting-started
- Zcaler Knowledge Base: https://support.zscaler.com/hc/en-us/?filter=documentation
- Zcaler Tools: https://www.zscaler.com/tools
- Zcaler Training and Certification: https://www.zscaler.com/resources/training-certification-overview
- Zcaler Submit a Ticket: https://help.zscaler.com/submit-ticket
- ZIA Test Page: http://ip.zscaler.com/