Contents

1 Microbranch and Zscaler Integration 2

1.1 Before You Start 2

1.2 Zscaler Configuration........ 2

1.3 Aruba Central Configuration 4

1.4 Integration Verification 7

1.5 Policy Based Routing Configuration 10

1.6 User Testing 11

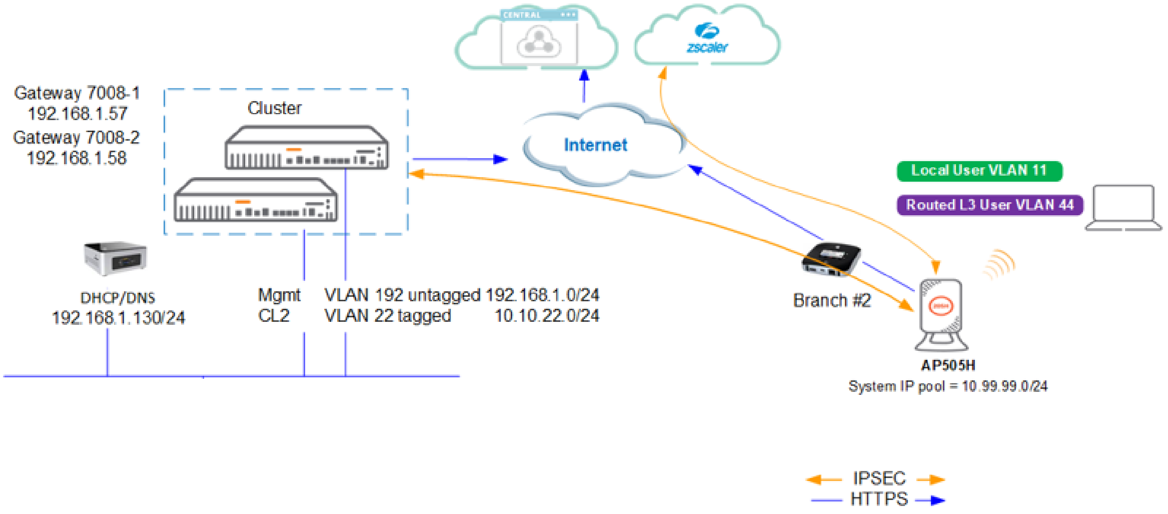
Revision History

DATE	VERSION	EDITOR	CHANGES
10 May 2024	0.1	Ariya Parsamanesh	Initial creation
30 Jun 2024	0.2	Ariya Parsamanesh	Added User Testing section

1 Microbranch and Zscaler Integration

The Microbranch (MB) solution can be seamlessly integrated with leading cloud security providers such as Zscaler through the Aruba Central "Cloud Connect" service. This integration facilitates the establishment of a secure connection between the Microbranch AP and one or multiple cloud-hosted enforcement control points. Specifically, in the case of Zscaler, this connection is established with Zscaler Internet Access (ZIA) Public Service Edges.

ZIA is basically an Internet onramp, which will be the next hop to the Internet bound traffic from MB. Aruba Central cloud connect service automatically orchestrates IPSEC tunnels and gets MB to connect to ZIA Public Service Edges. These IPSEC tunnels use Internet Key Exchange (IKE) protocol which provides the ability to traverse NAT boundaries and leverage IKEv2 for authentication, while at the same time limiting the overhead.



1.1 Before You Start

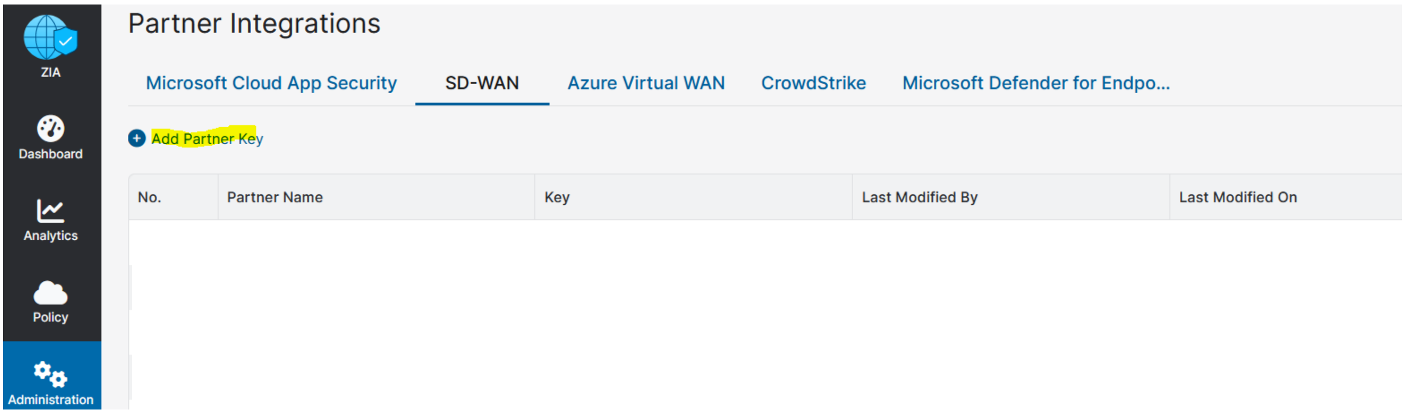
I am assuming you have a working Microbranch setup which means the MB access point is

- added and subscribed with Advance AP foundation license in Aruba Central
- configured and part of the AOS10 microbranch group.
- Running the latest firmware in AOS 10.5.x.x or 10.6.x.x series.

1.2 Zscaler Configuration

You need to login to the Zscaler cloud portal https://admin.zscalerthree.net/ to enable API integration between it and Aruba Central. For the API integration between the two we need an API key and user credentials.

First, we need to configure Zscaler for API access by going to Administration >> Partner Integrations >> SD-WAN and add a Partner key.



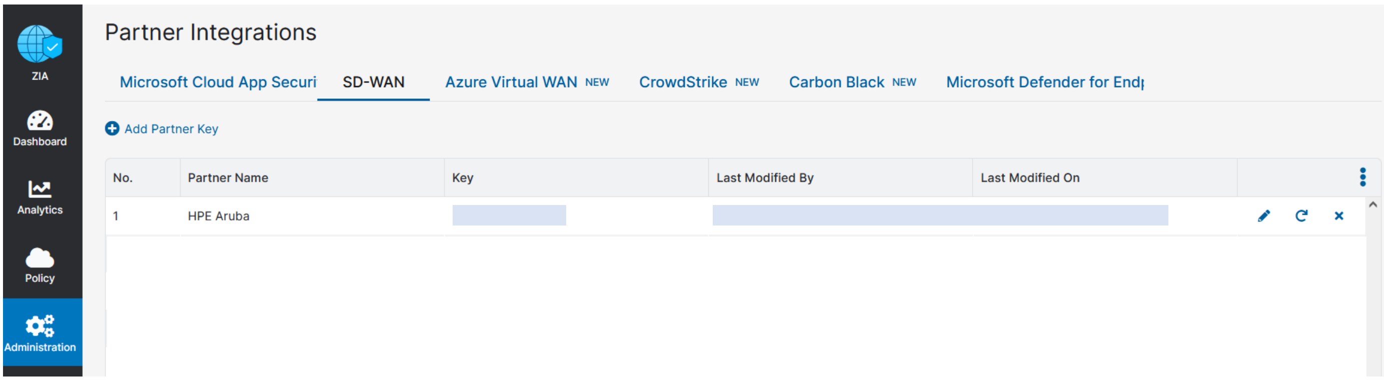
Partner Integrations

Microsoft Cloud App Security | SD-WAN | Azure Virtual WAN | CrowdStrike | Microsoft Defender for Endpo...

Add Partner Key

No.	Partner Name	Key	Last Modified By	Last Modified On

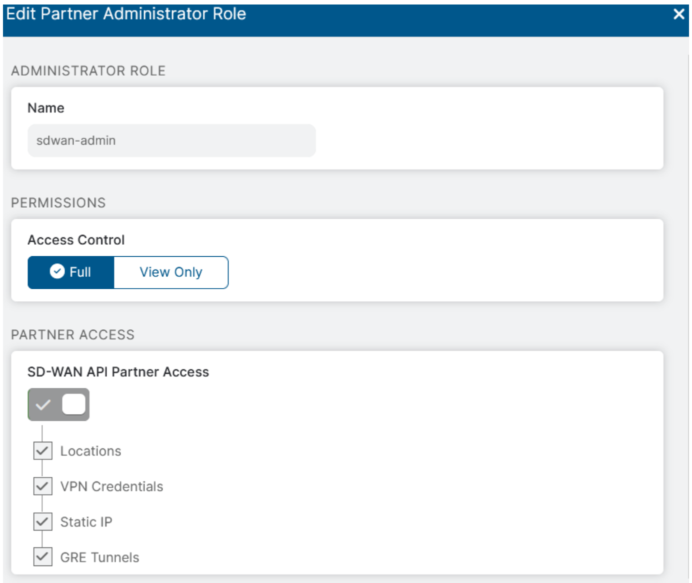
Select the HPE Partner name for the SD-WAN Type and when you are finished, you should get the API key.



Partner Integrations

No.	Partner Name	Key	Last Modified By	Last Modified On
1	HPE Aruba	[redacted]	[redacted]	[redacted]

Next, for the user credentials to be used with the API key, we'll create Partner Administrator Role by going to Administration >> Role Management and creating one. Ensure your login role has access to Locations, VPN Credentials, Static IP and GRE Tunnels. In my case the sdwan-admin role has that access.



Edit Partner Administrator Role

ADMINISTRATOR ROLE

Name: sdwan-admin

PERMISSIONS

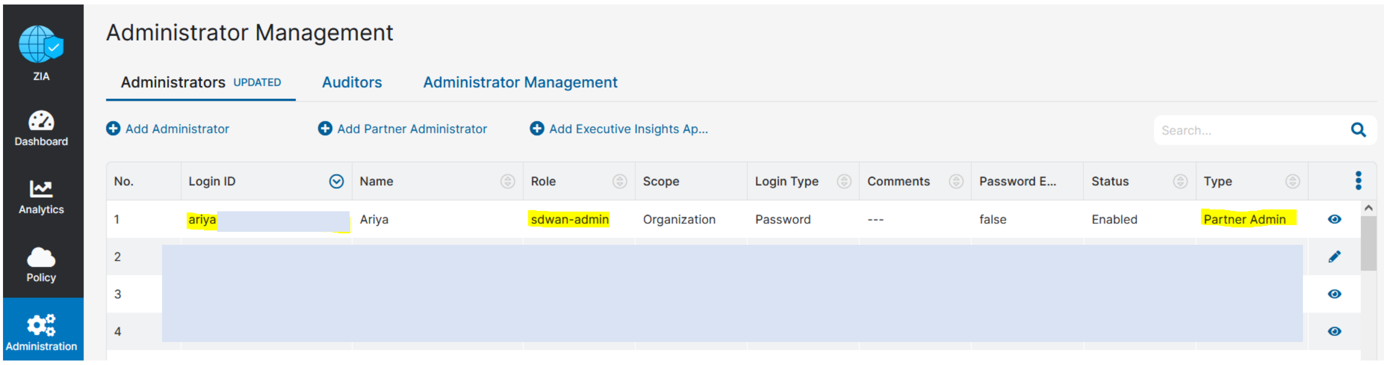
Access Control: [✓ Full] View Only

PARTNER ACCESS

SD-WAN API Partner Access: ✓

- ☑ Locations
- ☑ VPN Credentials
- ☑ Static IP
- ☑ GRE Tunnels

In my case the sdwan-admin role has that access, and finally assign this admin-role to the admin user credential.



Administrator Management

No.	Login ID	Name	Role	Scope	Login Type	Comments	Password E...	Status	Type
1	ariya [redacted]	Ariya	sdwan-admin	Organization	Password	---	false	Enabled	Partner Admin
2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

use this login credentials along with the Key from (Administration >Partner integration) to configure the Zscaler account in Aruba Central.

1.3 Aruba Central Configuration

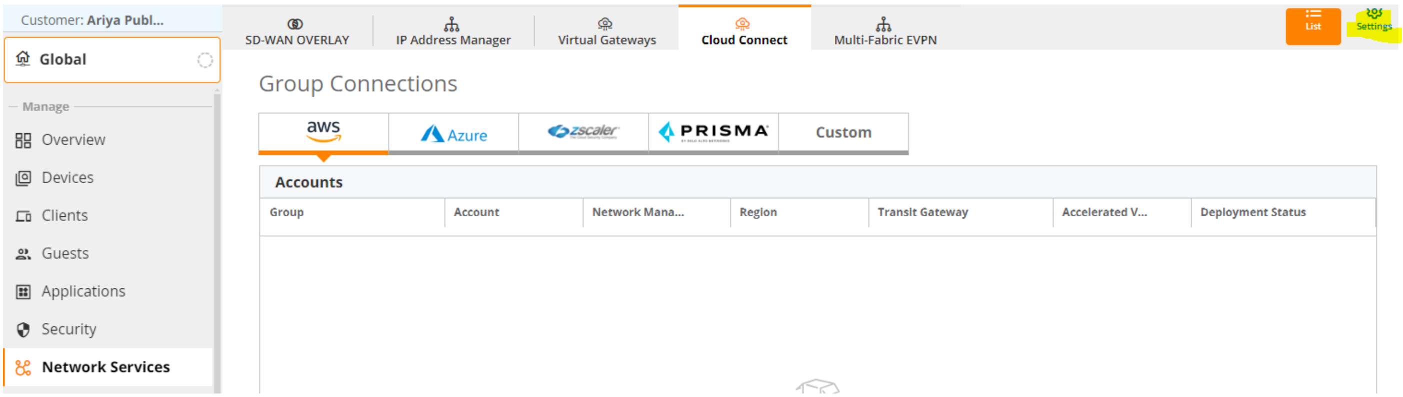
There are a few things you need to note before starting.

- Zscaler integration through Cloud Connect service for Microbranch APs requires firmware AOS 10.3.x
- Microbranch APs require an Advanced AP license for Zscaler integration through Cloud Connect service.

The main tasks are

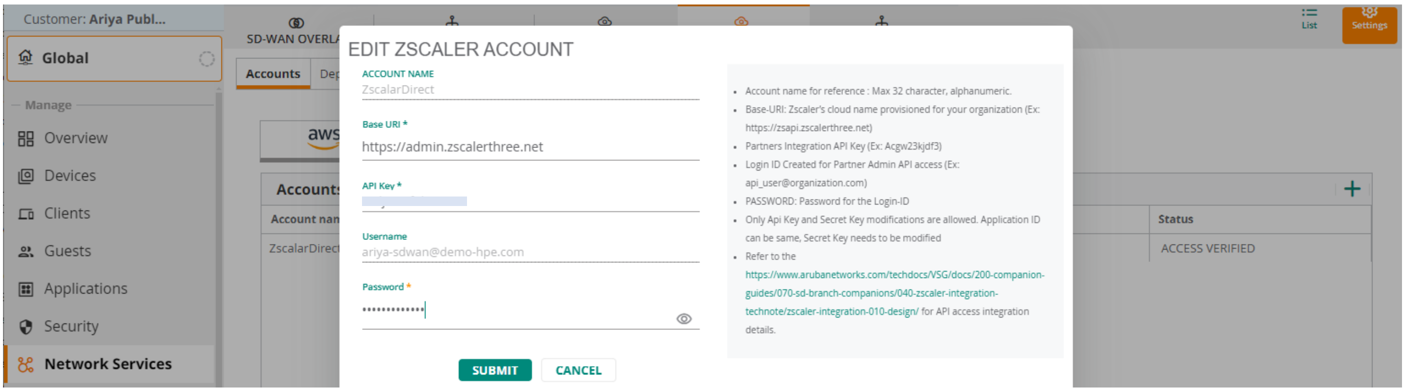
1. Adding a Cloud Provider Account in Aruba Central
2. Enabling Orchestrating Zscaler tunnels to select groups.

Here we'll start with adding the Zscaler account in Aruba Central, by going selecting Network Services and clicking on the Cloud Services tab and then the setting icon.



Group	Account	Network Mana...	Region	Transit Gateway	Accelerated V...	Deployment Status

Select the Zscaler tab and add the new account.



EDIT ZSCALER ACCOUNT

ACCOUNT NAME: ZscalarDirect

Base URI *: https://admin.zscalerthree.net

API Key *: [redacted]

Username: ariya-sdwan@demo-hpe.com

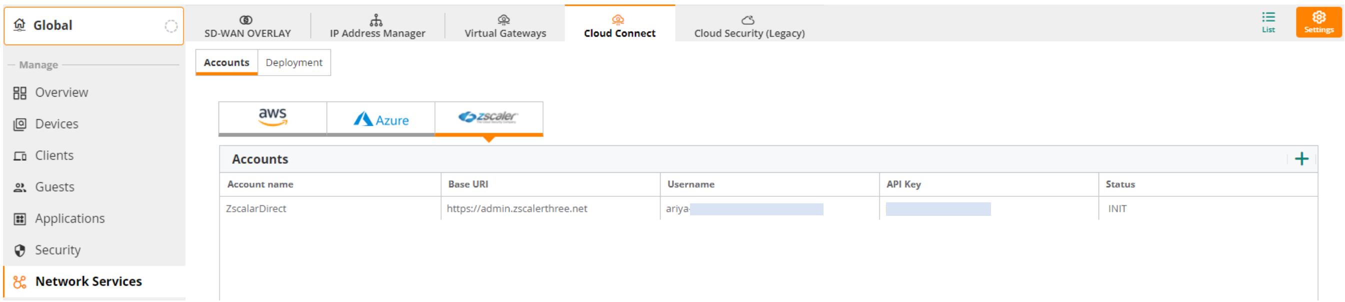
Password *: ••••••••••••••

- Account name for reference : Max 32 character, alphanumeric.
- Base-URI: Zscaler's cloud name provisioned for your organization (Ex: https://zsapi.zscalerthree.net)
- Partners Integration API Key (Ex: Acgw23kjdf3)
- Login ID Created for Partner Admin API access (Ex: api_user@organization.com)
- PASSWORD: Password for the Login-ID
- Only Api Key and Secret Key modifications are allowed. Application ID can be same, Secret Key needs to be modified
- Refer to the https://www.arubanetworks.com/techdocs/VSG/docs/200-companion-guides/070-sd-branch-companions/040-zscaler-integration-technote/zscaler-integration-010-design/ for API access integration details.

Here is the side note that is displayed when you are adding/editing the Zscaler account.

- Account name for reference : Max 32 character, alphanumeric.
- Base-URI: Zscaler's cloud name provisioned for your organization (Ex: https://zsapi.zscalerthree.net)
- Partners Integration API Key (Ex: Acgw23kjdf3)
- Login ID Created for Partner Admin API access (Ex: api_user@organization.com)
- PASSWORD: Password for the Login-ID
- Only Api Key and Secret Key modifications are allowed. Application ID can be same, Secret Key needs to be modified.
- Refer to the https://www.arubanetworks.com/techdocs/VSG/docs/200-companion-guides/070-sd-branch-companions/040-zscaler-integration-technote/zscaler-integration-010-design/ for API access integration details.

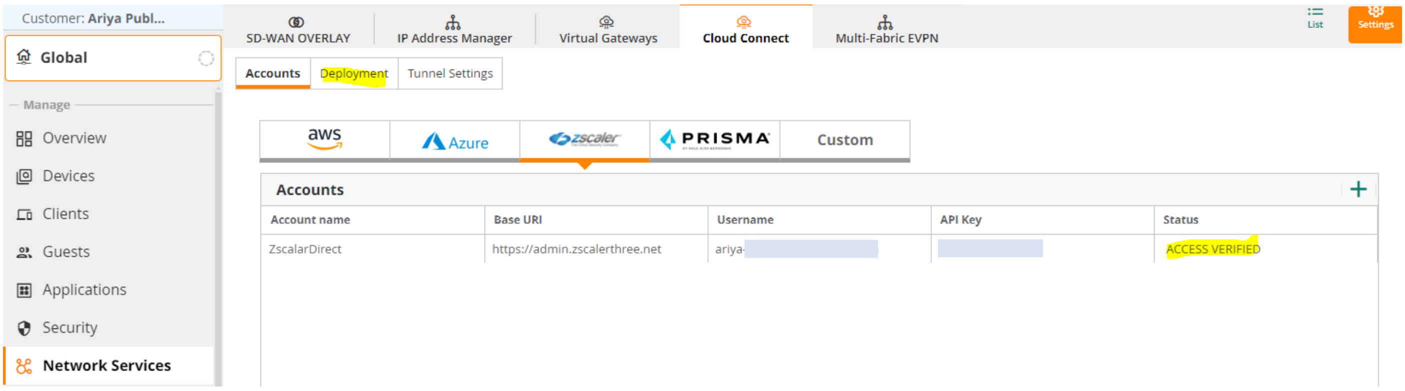
Once you save it you get this display with status being INIT.



Accounts

Account name	Base URI	Username	API Key	Status
ZscalarDirect	https://admin.zscalerthree.net	ariya-[redacted]	[redacted]	INIT

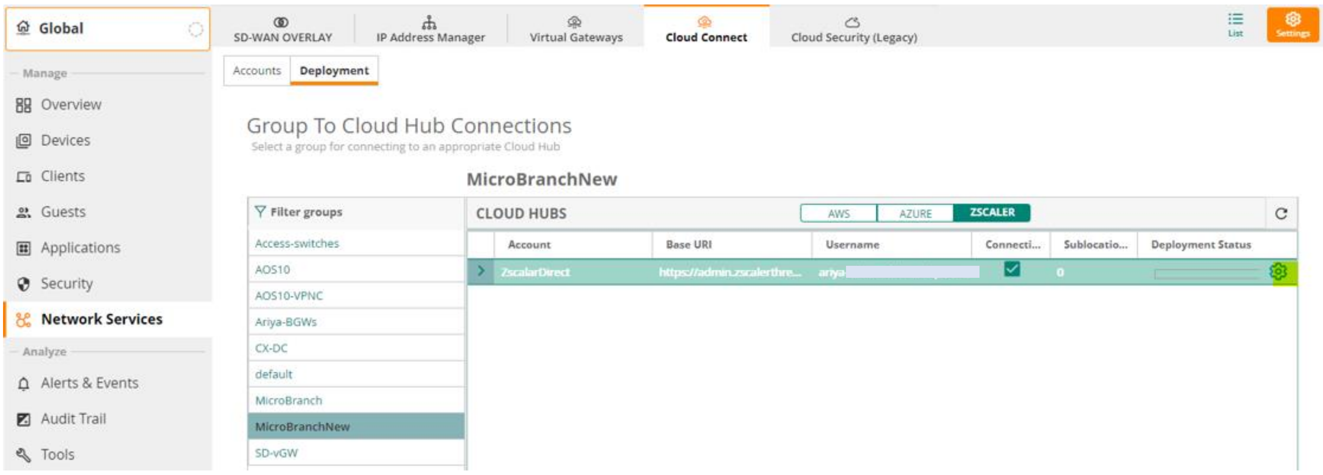
This might take few minutes, be patient.



Accounts

Account name	Base URI	Username	API Key	Status
ZscalarDirect	https://admin.zscalerthree.net	ariya-[redacted]	[redacted]	ACCESS VERIFIED

Now that the account status is "Access Verified", we click on the "Deployment" tab and choose the group that you want to associate the Zscaler account with, in my case it's the microbranch group.



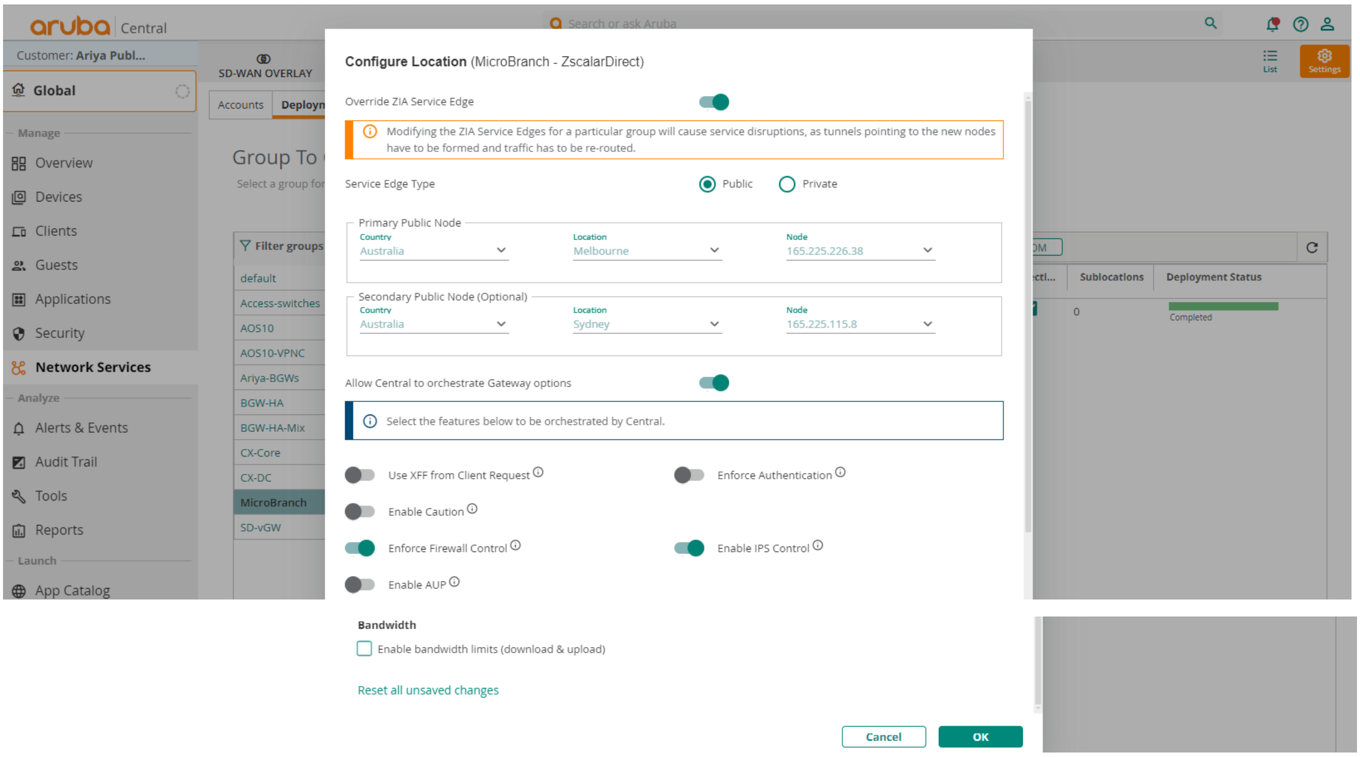
Group To Cloud Hub Connections

Select a group for connecting to an appropriate Cloud Hub

MicroBranchNew

CLOUD HUBS

Account	Base URI	Username	Connecti...	Sublocatio...	Deployment Status
ZscalarDirect	https://admin.zscalerthre...	ariya[redacted]	☑	0	



Configure Location (MicroBranch - ZscalarDirect)

Override ZIA Service Edge ●

ⓘ Modifying the ZIA Service Edges for a particular group will cause service disruptions, as tunnels pointing to the new nodes have to be formed and traffic has to be re-routed.

Service Edge Type ● Public ○ Private

Primary Public Node

Country	Location	Node
Australia	Melbourne	165.225.226.38

Secondary Public Node (Optional)

Country	Location	Node
Australia	Sydney	165.225.115.8

Allow Central to orchestrate Gateway options ●

ⓘ Select the features below to be orchestrated by Central.

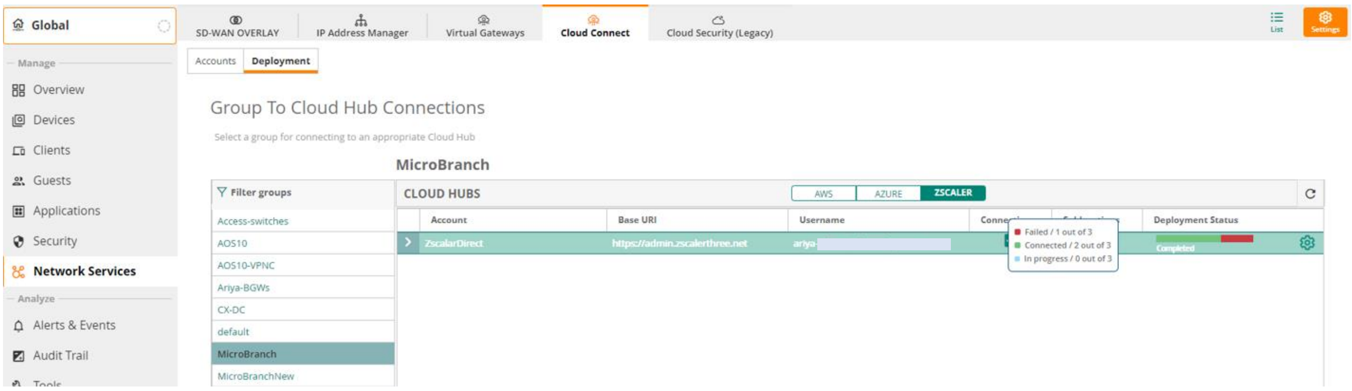
- Use XFF from Client Request ⓘ — off
- Enforce Authentication ⓘ — off
- Enable Caution ⓘ — off
- Enforce Firewall Control ⓘ — on
- Enable IPS Control ⓘ — on
- Enable AUP ⓘ — off

Bandwidth

□ Enable bandwidth limits (download & upload)

Reset all unsaved changes

You then need to select Preview at the bottom of the page and Submit.



Group To Cloud Hub Connections

Select a group for connecting to an appropriate Cloud Hub

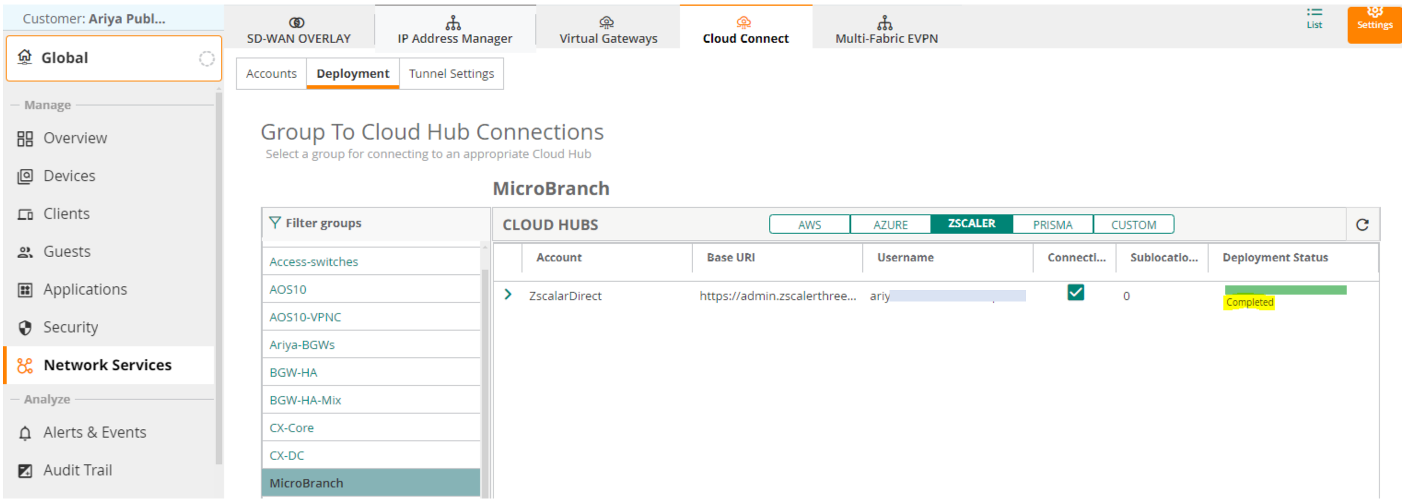
MicroBranch

CLOUD HUBS

Account	Base URI	Username	Conne...	Sublocations	Deployment Status
ZscalarDirect	https://admin.zscalerthree.net	ariya-[redacted]			Completed

- Failed / 1 out of 3
- Connected / 2 out of 3
- In progress / 0 out of 3

This will take a few minutes.



Group To Cloud Hub Connections

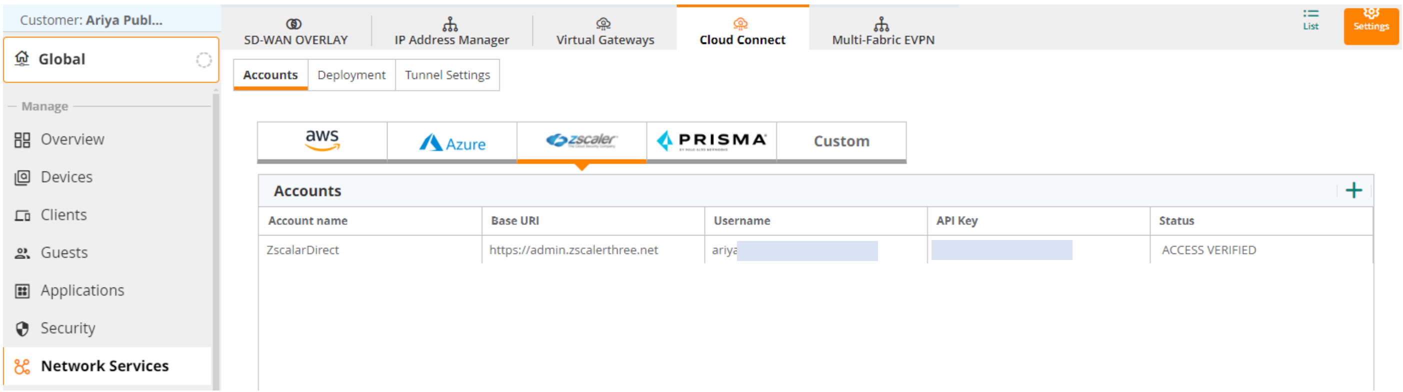
Select a group for connecting to an appropriate Cloud Hub

MicroBranch

CLOUD HUBS

Account	Base URI	Username	Connecti...	Sublocatio...	Deployment Status
ZscalarDirect	https://admin.zscalerthree...	ariy[redacted]	☑	0	Completed

Once this is done, you can see it under accounts as shown below.



Accounts

Account name	Base URI	Username	API Key	Status
ZscalarDirect	https://admin.zscalerthree.net	ariya[redacted]	[redacted]	ACCESS VERIFIED

1.4 Integration Verification

At this point the devices (in my case APs) in that group which you have just setup Zscaler orchestration for, should have by now established the IPSEC tunnels.

The WebUI will take some time, but for now use the CLI to verify, remember that ZIA tunnels will use ISAKMP.

```
MicroBranch2# sh crypto-local isakmp key

ISAKMP KEY
----------
IP/FQDN            KEY                                                        HEX
-------            ---                                                        ---
165.225.115.8/32   57fb1df199583b2d803<strings removed>444199161880b27191becb  N
165.225.226.38/32  6719bf025333adsdsds<strings removed>595810be92b8f457a6dsds  N
Total ISAKMP KEY Count: 2

MicroBranch2#
```

```
MicroBranch2# sh crypto isakmp dpd

IPSEC MAP DPD STATS
-------------------
MAP NAME                                    PEER IP         REQUEST SENT  REQUEST RESENT  REPLY
RECVD  REQUEST RECVD  REPLY SENT  PEER_DEAD
--------                                    -------         ------------  --------------  -----
zs-init-zscalardirect-primary-lte-uplink    165.225.226.38  0             0               0
0              0           0
zs-init-zscalardirect-primary-e0-uplink     165.225.226.38  230           0               230
0              0           0
zs-init-zscalardirect-secondary-e0-uplink   165.225.115.8   229           0               229
0              0           0
zs-init-zscalardirect-secondary-lte-uplink  165.225.115.8   0             0               0
0              0           0
Total IPSEC MAP Count: 4

MicroBranch2#
```

Note that microbranch APs use Overlay Agent Protocol (OAP) to connect to Aruba Central Route/Tunnel orchestrator to get the all the information about routing and tunnels that needs to be established.

```
MicroBranch2# sh l3d oap tunnels

L3D OAP Tunnel Table
---------------------
Peer MAC           Map Name                                         Map Id   State    GenId
Pair UUID
--------           --------                                         ------   -----    -----
---------
20:4c:03:0a:b9:e0  gw-ipsecmap-20:4c:03:0a:b9:e0-e0-uplink          0x50001  Up       119768693
019cbfdf-a087-4b72-b1ab-0612c0de2a69
                   zs-init-zscalardirect-primary-e0-uplink          0x50003  Up       119768694
276a6d41-b41c-4676-8bd2-f3e2cbc2036e
```

```
                   zs-init-zscalardirect-secondary-e0-uplink        0x50004  Up       119768695
6d4017ef-94c1-4aaf-8957-703ee72c0bb4

MicroBranch2#
```

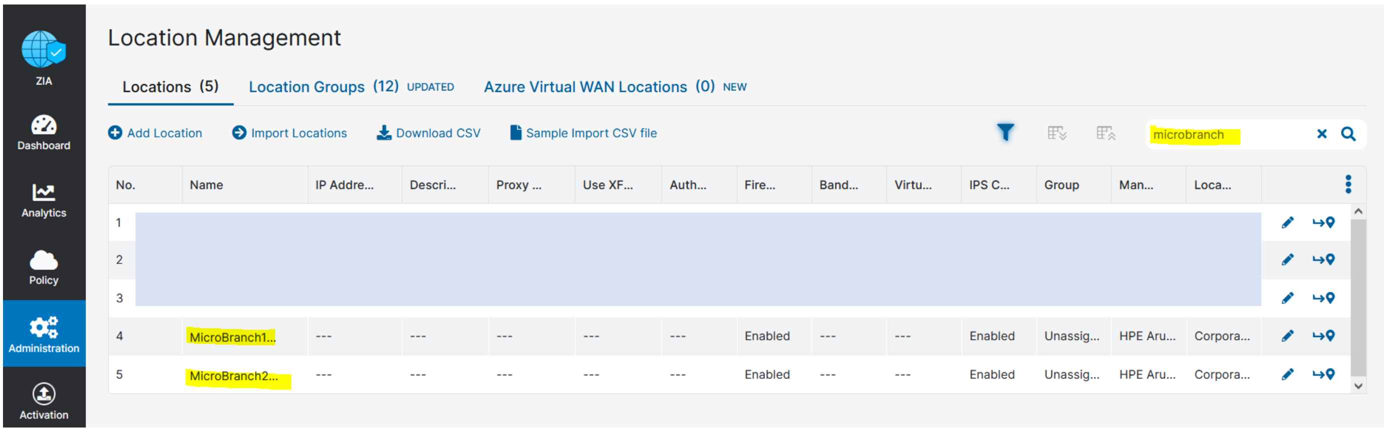
Next, we'll check the IPSEC stats.

```
MicroBranch2# sh crypto ipsec stats

IPSEC STATS
-----------
MAP NAME                                    IP ADDR         DEVNAME  TX/RX PACKETS  TX/RX BYTES
TX/RX DROPS  TX/RX ERRORS
--------                                    -------         -------  -------------  -----------
gw-ipsecmap-20:4c:03:0a:b9:e0-e0-uplink     194.223.11.109  tun0     33402/31319
3732456/3418448   0/0         0/0
gw-ipsecmap-20:4c:03:0a:b9:e0-lte-uplink    194.223.11.109           0/0            0/0
0/0          0/0
zs-init-zscalardirect-primary-e0-uplink     165.225.226.38  tun1     18750/36423
1714608/37751975  0/0         0/0
zs-init-zscalardirect-secondary-e0-uplink   165.225.115.8   tun2     0/0            0/0
0/0          0/0
zs-init-zscalardirect-secondary-lte-uplink  165.225.115.8            0/0            0/0
0/0          0/0
zs-init-zscalardirect-primary-lte-uplink    165.225.226.38           0/0            0/0
0/0          0/0
Total IPSEC Count: 6

MicroBranch2#
```

Finally you can also use the following command to see more details about the tunnels that are established from the AP.

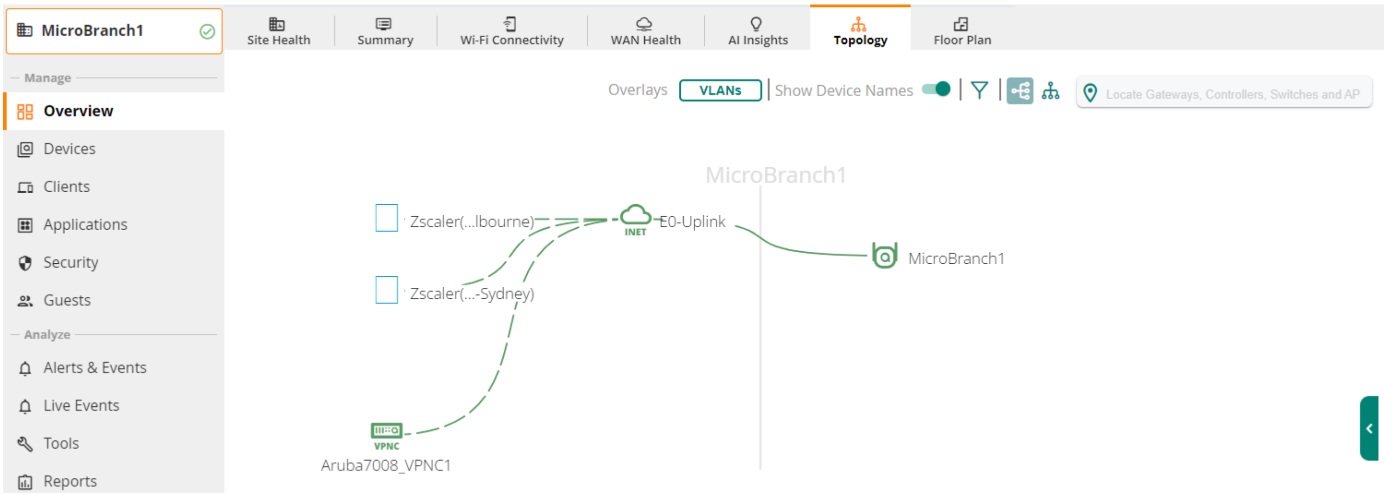
```
MicroBranch2# sh ata endpoint status

ATA Endpoint Status
-------------------
UUID                                  IP ADDR         STATE               TUN DEV  TUN
SPI(OUT/IN)     LINK TAG    VALID TIME(s)  TUNNEL TYPE  GRE VLANs      HBT(Jiff/Missed/Sent/Rcv)
INNER IP    UP TIME(s)
----                                  --------        -----               --------  ---------------
-    --------    -------------  -----------  ---------      -------------------------  ---------
60fbe82a-19a7-4ecb-8eff-34a6fd946127  203.214.83.128  SM_STATE_CONNECTED  tun0
af5b0800/c5f9e000  E0-Uplink   124970         GREoIPSec    1,22,192,4094  4993/0/4618/4618
10.99.99.4  2024-04-11 10:06:11
aea605cf-7d2e-486a-941a-c64394938471  203.214.83.128  SM_STATE_INIT
96bd8100/2e4a900   LTE-Uplink  129567         GREoIPSec    1,22,192,4094  0/0/0/0
10.99.99.4  1970-01-01 11:00:00
f9c5cc3b-c3ce-44a6-af73-e4e0f229aab6  165.225.226.38  SM_STATE_CONNECTED  tun1
30d3f7f0/2ce43b00  E0-Uplink   24182          IPSEC        NULL           0/0/0/0
10.99.99.4  2024-04-11 10:06:20
49437d16-d6f2-4676-b4ad-1cc2b5af8e70  165.225.115.8   SM_STATE_INIT                0/0
LTE-Uplink  -4993          IPSEC         NULL           0/0/0/0                   N/A
1970-01-01 11:00:00
62e670ed-c134-4859-bc42-d1cbebc0019a  165.225.115.8   SM_STATE_CONNECTED  tun2
1524b377/4da09e00  E0-Uplink   24203          IPSEC        NULL           0/0/0/0
10.99.99.4  2024-04-11 10:06:40
29b6476c-b9b3-42ee-8bea-964dd27fffef  165.225.226.38  SM_STATE_INIT                0/0
LTE-Uplink  -4993          IPSEC         NULL           0/0/0/0                   N/A
1970-01-01 11:00:00
Total Endpoints Count: 6

MicroBranch2#
```

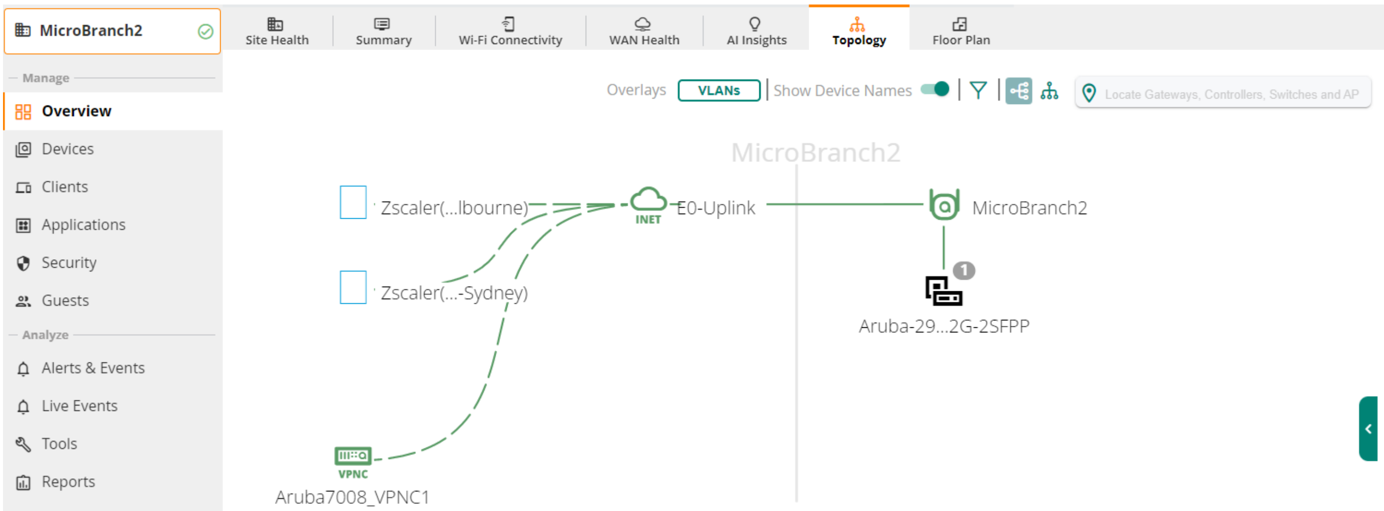
You should be able to see the new location in Zscaler portal as well. You need to search for the Aruba Central group name that you enabled for Zscaler orchestration.



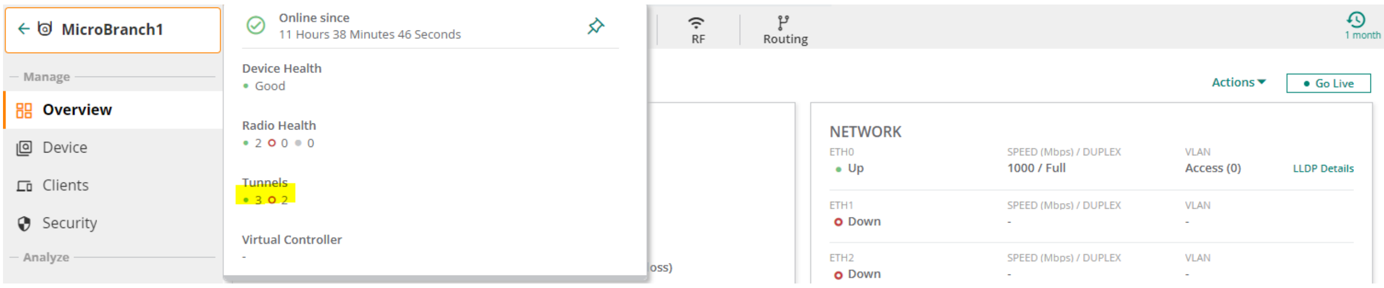
No.	Name	IP Addre...	Descri...	Proxy ...	Use XF...	Auth...	Fire...	Band...	Virtu...	IPS C...	Group	Man...	Loca...
1	[redacted]												
2													
3													
4	MicroBranch1...	---	---	---	---	---	Enabled	---	---	Enabled	Unassig...	HPE Aru...	Corpora...
5	MicroBranch2...	---	---	---	---	---	Enabled	---	---	Enabled	Unassig...	HPE Aru...	Corpora...

After some time you should be able to the Zscaler tunnels in corresponding Site topology view





You should also be able to see the tunnels as well.



Online since
11 Hours 38 Minutes 46 Seconds

Device Health
● Good

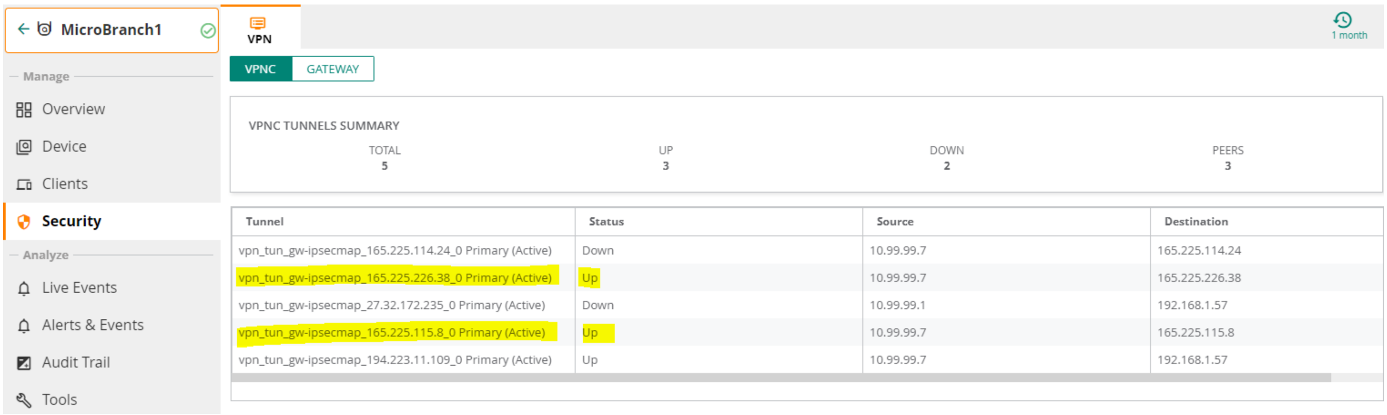
Radio Health
● 2 ○ 0 ● 0

Tunnels
● 3 ○ 2

Virtual Controller
-

NETWORK

ETH0 ● Up	SPEED (Mbps) / DUPLEX 1000 / Full	VLAN Access (0)
ETH1 ○ Down	SPEED (Mbps) / DUPLEX -	VLAN -
ETH2 ○ Down	SPEED (Mbps) / DUPLEX -	VLAN -



VPNC TUNNELS SUMMARY

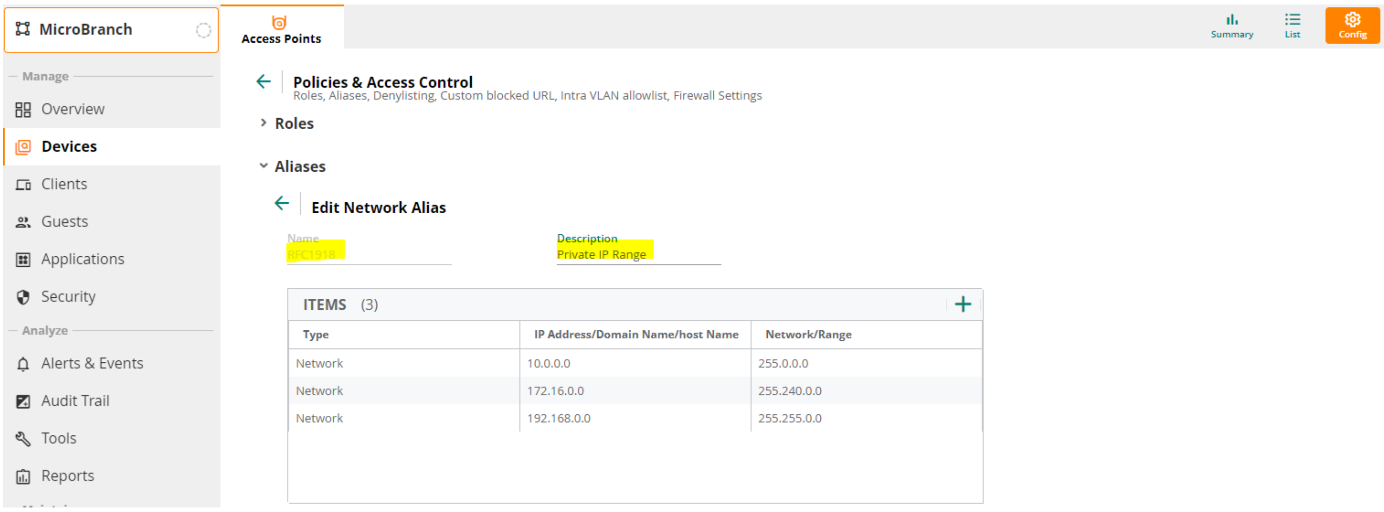
TOTAL	UP	DOWN	PEERS
5	3	2	3

Tunnel	Status	Source	Destination
vpn_tun_gw-ipsecmap_165.225.114.24_0 Primary (Active)	Down	10.99.99.7	165.225.114.24
vpn_tun_gw-ipsecmap_165.225.226.38_0 Primary (Active)	Up	10.99.99.7	165.225.226.38
vpn_tun_gw-ipsecmap_27.32.172.235_0 Primary (Active)	Down	10.99.99.1	192.168.1.57
vpn_tun_gw-ipsecmap_165.225.115.8_0 Primary (Active)	Up	10.99.99.7	165.225.115.8
vpn_tun_gw-ipsecmap_194.223.11.109_0 Primary (Active)	Up	10.99.99.7	192.168.1.57

1.5 Policy Based Routing Configuration

You need to configure a Policy Based Routing (PBR) and then associate it with a user role, in order to redirect some traffic to ZIA tunnels. Here we want the Internet traffic to be policy routed through the ZIA tunnels.

1. Create a RFC1918 alias to group all the private IP subnets.



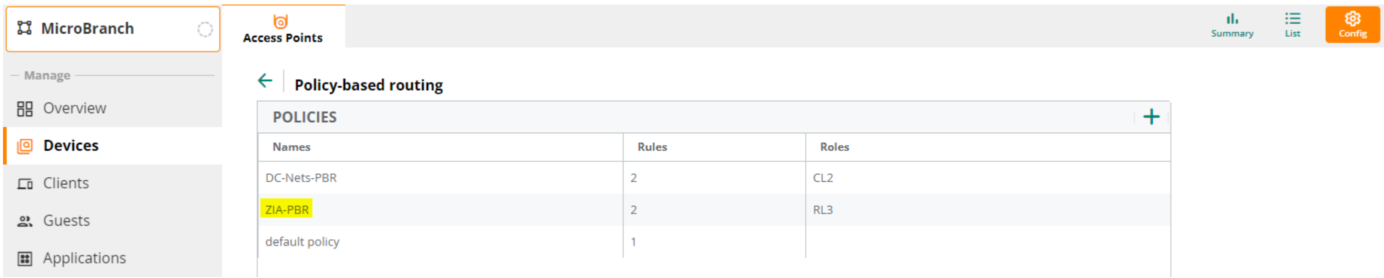
Name: RFC1918

Description: Private IP Range

ITEMS (3)

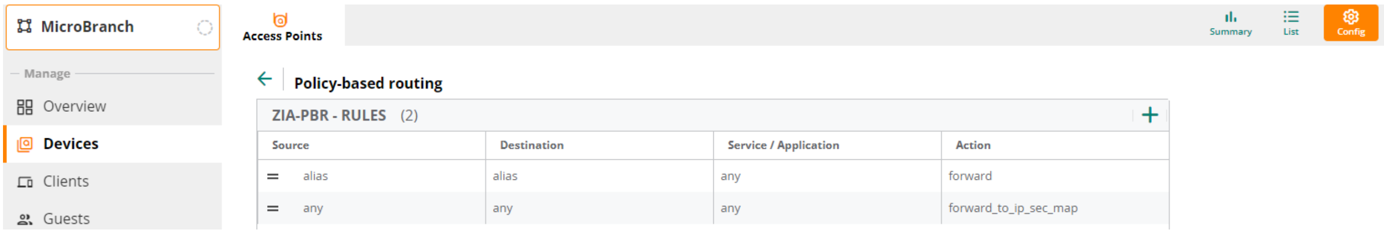
Type	IP Address/Domain Name/host Name	Network/Range
Network	10.0.0.0	255.0.0.0
Network	172.16.0.0	255.240.0.0
Network	192.168.0.0	255.255.0.0

2. Create a PBR policy.



POLICIES

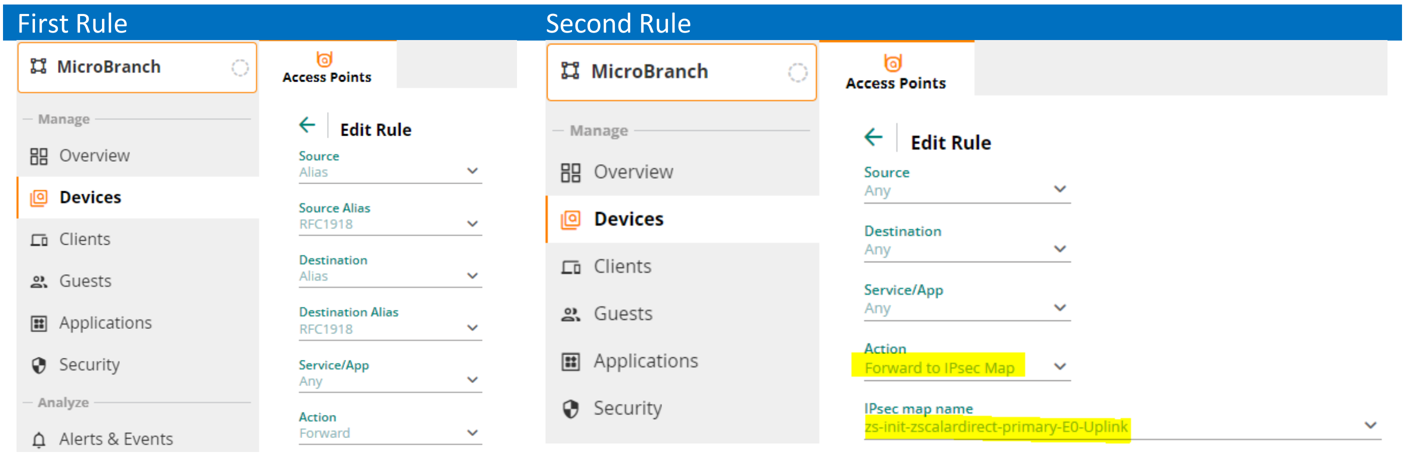
Names	Rules	Roles
DC-Nets-PBR	2	CL2
ZIA-PBR	2	RL3
default policy	1	



ZIA-PBR - RULES (2)

Source	Destination	Service / Application	Action
alias	alias	any	forward
any	any	any	forward_to_ip_sec_map

The rules are as follows.



First Rule

Edit Rule

Source: Alias

Source Alias: RFC1918

Destination: Alias

Destination Alias: RFC1918

Service/App: Any

Action: Forward

Second Rule

Edit Rule

Source: Any

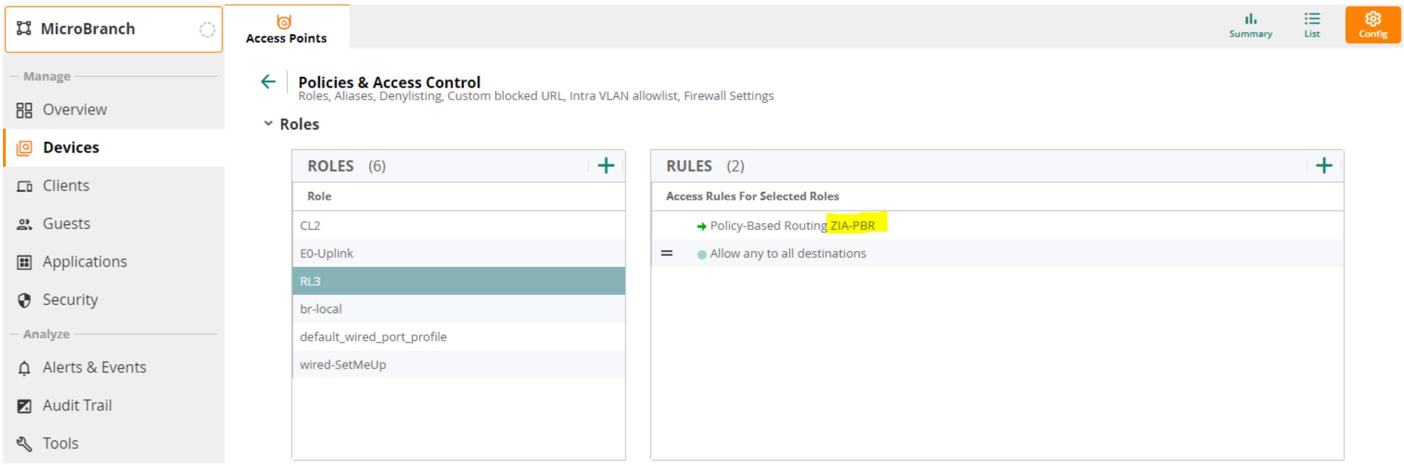
Destination: Any

Service/App: Any

Action: Forward to IPsec Map

IPsec map name: zs-init-zscalardirect-primary-E0-Uplink

3. Associate the PBR policy with a user role.



Policies & Access Control

Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings

Roles

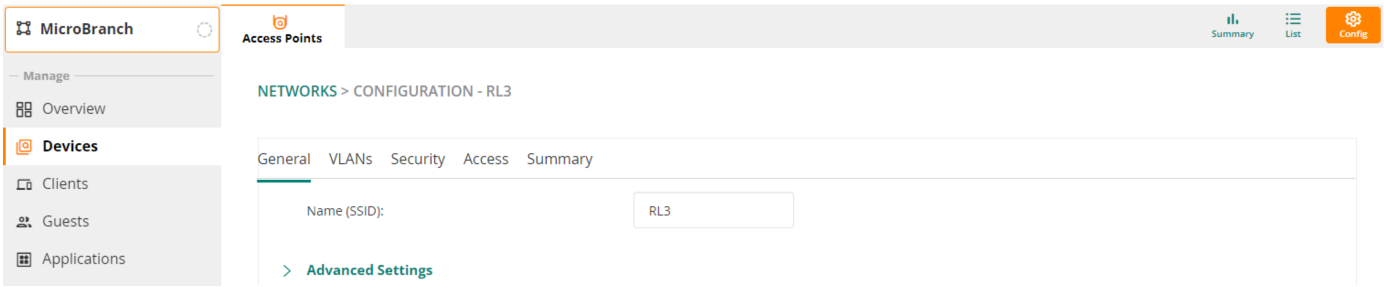
ROLES (6)
Role
CL2
E0-Uplink
RL3
br-local
default_wired_port_profile
wired-SetMeUp

RULES (2)
Access Rules For Selected Roles
Policy-Based Routing ZIA-PBR
Allow any to all destinations

Alternatively, you could also use NextHop list instead. This is where you add all the IPSEC tunnels to the NextHop list so we can then use it in our PBR. NextHop list makes it easier for cases where you have 2 or more IPSEC tunnels that we can forward traffic. In our case we have 2x IPSEC tunnels for each of the uplinks (eth0 and LTE). You can check my technote on microbranch and Aruba SSE integration, where I use NextHop list.

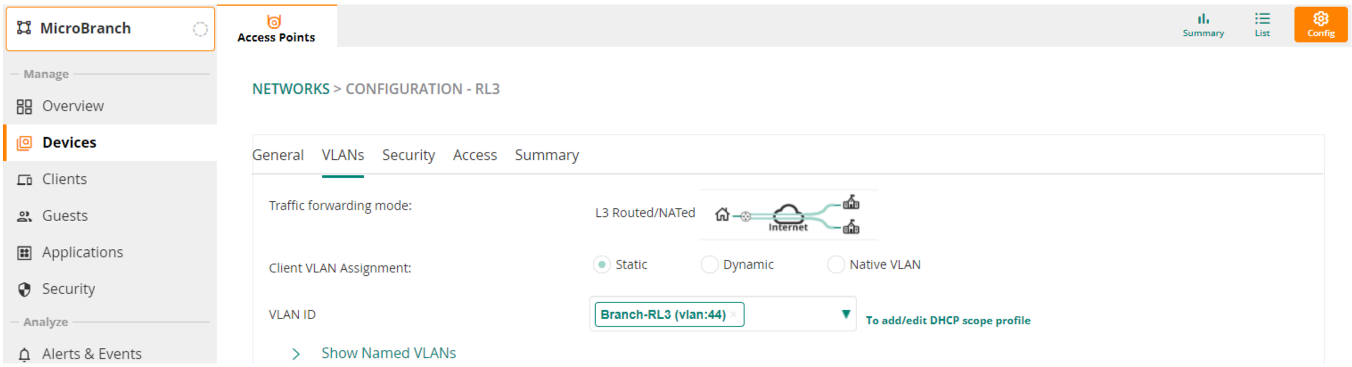
1.6 User Testing

Here we have configured a RL3 SSID which has a default user role of RL3



NETWORKS > CONFIGURATION - RL3

Name (SSID): RL3



NETWORKS > CONFIGURATION - RL3

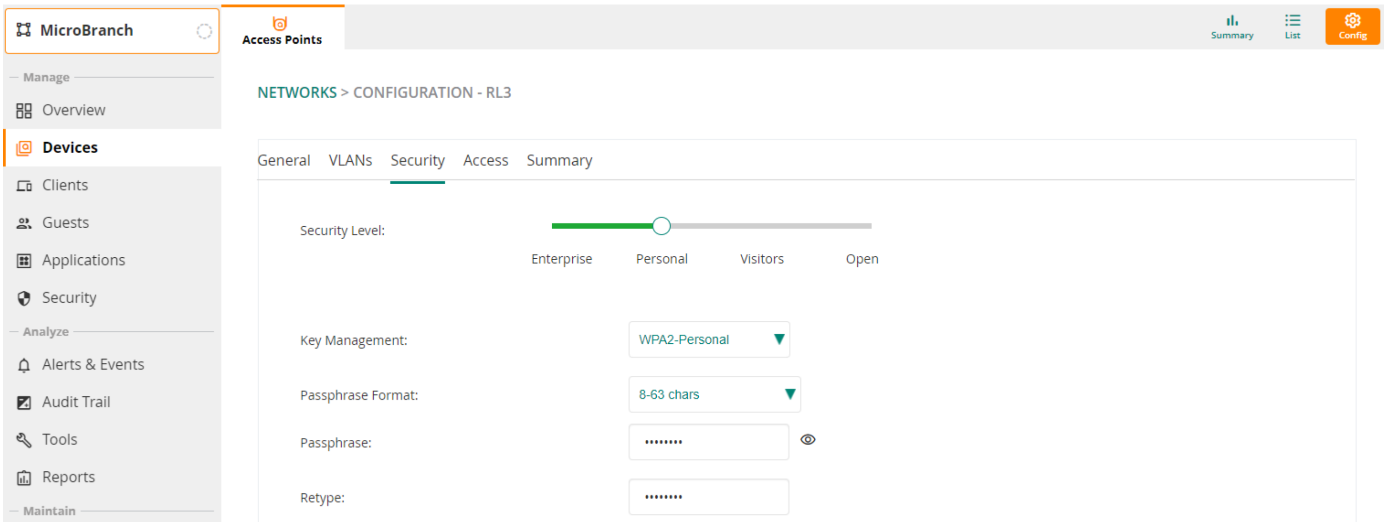
Traffic forwarding mode: L3 Routed/NATed

Client VLAN Assignment: ● Static ○ Dynamic ○ Native VLAN

VLAN ID: Branch-RL3 (vlan:44)

To add/edit DHCP scope profile

> Show Named VLANs



NETWORKS > CONFIGURATION - RL3

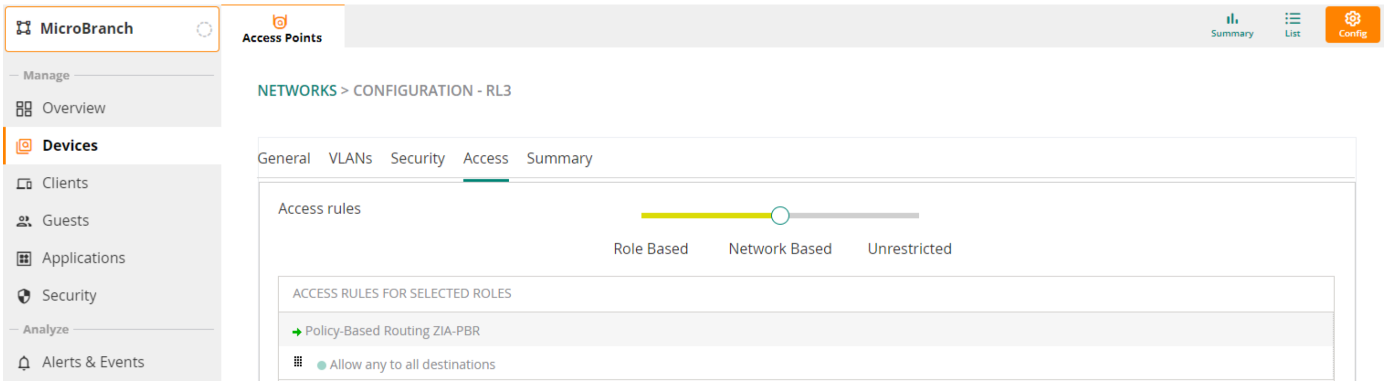
Security Level: Enterprise — **Personal** — Visitors — Open

Key Management: WPA2-Personal

Passphrase Format: 8-63 chars

Passphrase: ••••••••

Retype: ••••••••



NETWORKS > CONFIGURATION - RL3

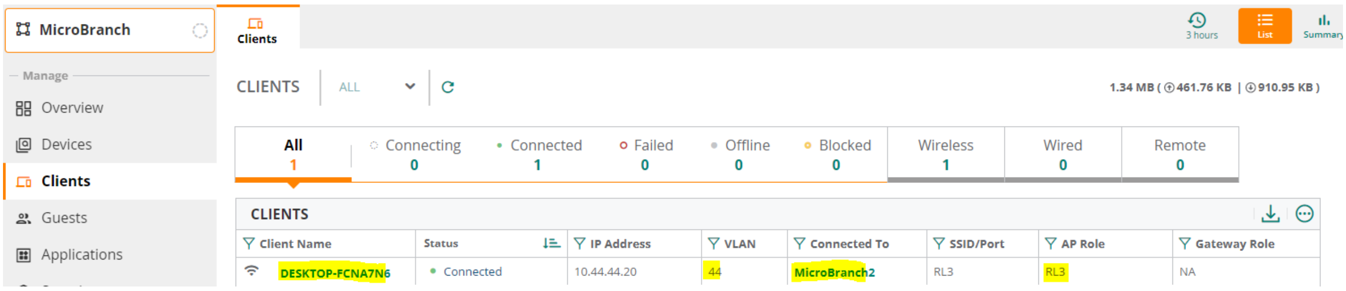
Access rules: Role Based — **Network Based** — Unrestricted

ACCESS RULES FOR SELECTED ROLES

→ Policy-Based Routing ZIA-PBR

● Allow any to all destinations

We will start testing by connecting to RL3 SSID.



CLIENTS ALL

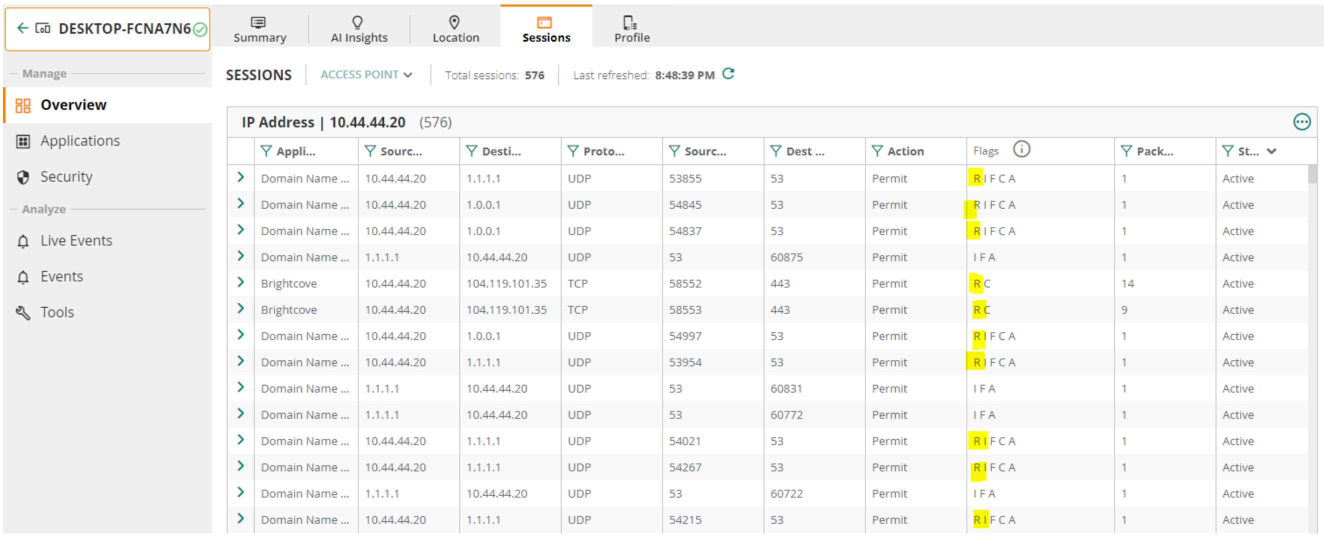
1.34 MB (461.76 KB | 910.95 KB)

All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
1	0	1	0	0	0	1	0	0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
DESKTOP-FCNA7N6	Connected	10.44.44.20	44	MicroBranch2	RL3	RL3	NA

And browse the Internet to generate some traffic to match with our PBR rules. Next, we'll check the sessions table.

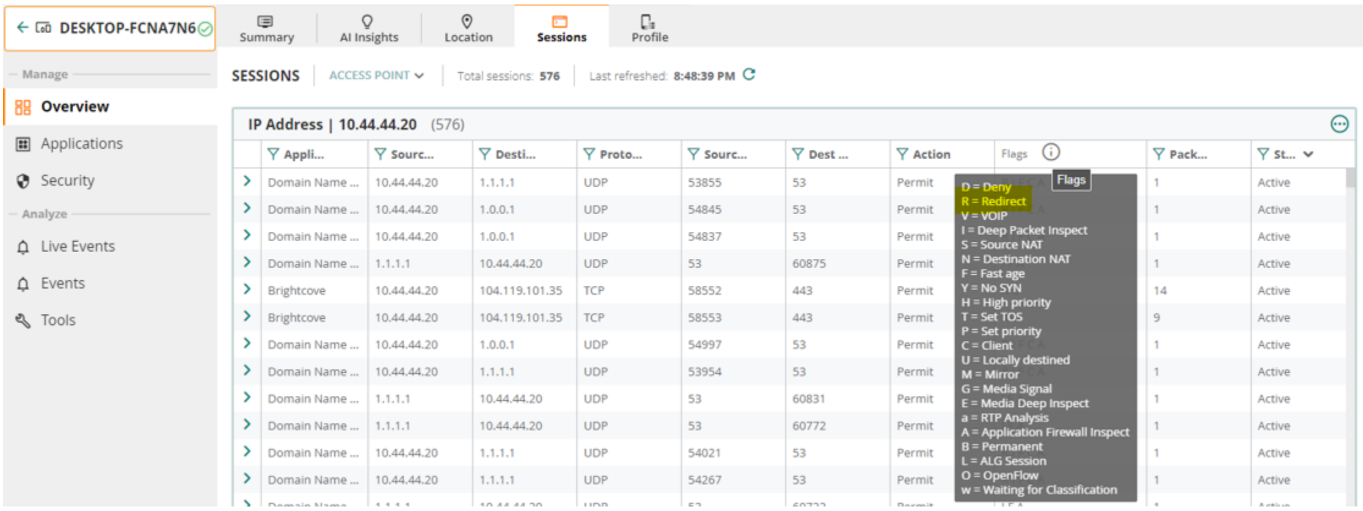


SESSIONS | ACCESS POINT | Total sessions: **576** | Last refreshed: **8:48:39 PM**

IP Address | 10.44.44.20 (576)

Appli...	Sourc...	Desti...	Proto...	Sourc...	Dest ...	Action	Flags	Pack...	St...
Domain Name ...	10.44.44.20	1.1.1.1	UDP	53855	53	Permit	R I F C A	1	Active
Domain Name ...	10.44.44.20	1.0.0.1	UDP	54845	53	Permit	R I F C A	1	Active
Domain Name ...	10.44.44.20	1.0.0.1	UDP	54837	53	Permit	R I F C A	1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60875	Permit	I F A	1	Active
Brightcove	10.44.44.20	104.119.101.35	TCP	58552	443	Permit	R C	14	Active
Brightcove	10.44.44.20	104.119.101.35	TCP	58553	443	Permit	R C	9	Active
Domain Name ...	10.44.44.20	1.0.0.1	UDP	54997	53	Permit	R I F C A	1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	53954	53	Permit	R I F C A	1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60831	Permit	I F A	1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60772	Permit	I F A	1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	54021	53	Permit	R I F C A	1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	54267	53	Permit	R I F C A	1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60722	Permit	I F A	1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	54215	53	Permit	R I F C A	1	Active

Look for the R flag which indicates redirection.



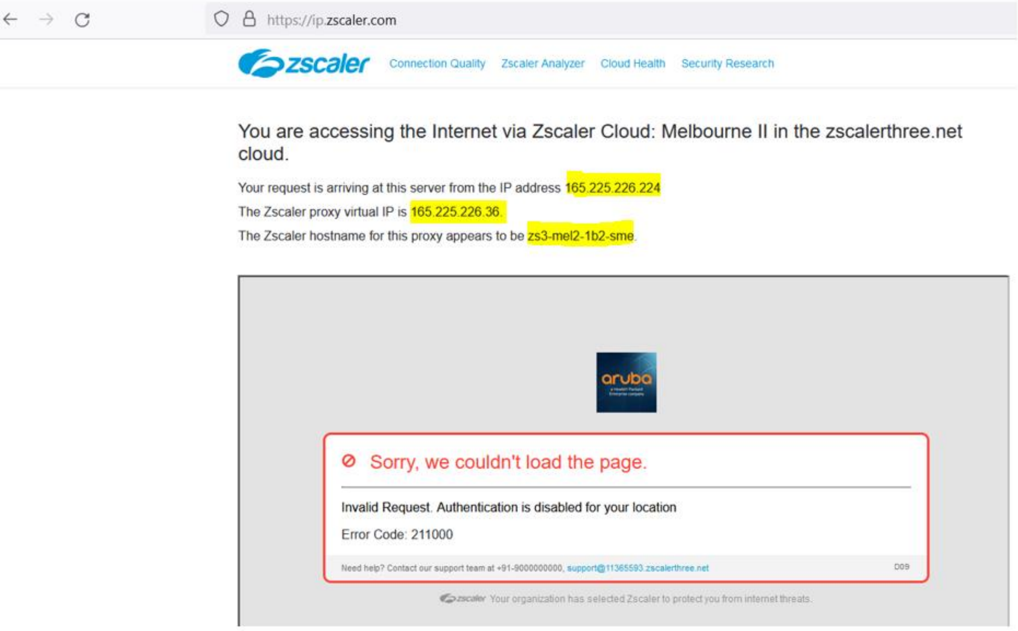
SESSIONS | ACCESS POINT | Total sessions: **576** | Last refreshed: **8:48:39 PM**

IP Address | 10.44.44.20 (576)

Appli...	Sourc...	Desti...	Proto...	Sourc...	Dest ...	Action	Flags	Pack...	St...
Domain Name ...	10.44.44.20	1.1.1.1	UDP	53855	53	Permit		1	Active
Domain Name ...	10.44.44.20	1.0.0.1	UDP	54845	53	Permit		1	Active
Domain Name ...	10.44.44.20	1.0.0.1	UDP	54837	53	Permit		1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60875	Permit		1	Active
Brightcove	10.44.44.20	104.119.101.35	TCP	58552	443	Permit		14	Active
Brightcove	10.44.44.20	104.119.101.35	TCP	58553	443	Permit		9	Active
Domain Name ...	10.44.44.20	1.0.0.1	UDP	54997	53	Permit		1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	53954	53	Permit		1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60831	Permit		1	Active
Domain Name ...	1.1.1.1	10.44.44.20	UDP	53	60772	Permit		1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	54021	53	Permit		1	Active
Domain Name ...	10.44.44.20	1.1.1.1	UDP	54267	53	Permit		1	Active

D = Deny
R = Redirect
V = VOIP
I = Deep Packet Inspect
S = Source NAT
N = Destination NAT
F = Fast age
Y = No SYN
H = High priority
T = Set TOS
P = Set priority
C = Client
U = Locally destined
M = Mirror
G = Media Signal
E = Media Deep Inspect
a = RTP Analysis
A = Application Firewall Inspect
B = Permanent
L = ALG Session
O = OpenFlow
w = Waiting for Classification

Finally from the client laptop you can browse to ip.zscaler.com and get the following information that shows the traffic is going through ZIA service.



You are accessing the Internet via Zscaler Cloud: Melbourne II in the zscalerthree.net cloud.

Your request is arriving at this server from the IP address 165.225.226.224

The Zscaler proxy virtual IP is 165.225.226.36.

The Zscaler hostname for this proxy appears to be zs3-mel2-1b2-sme.

Sorry, we couldn't load the page.

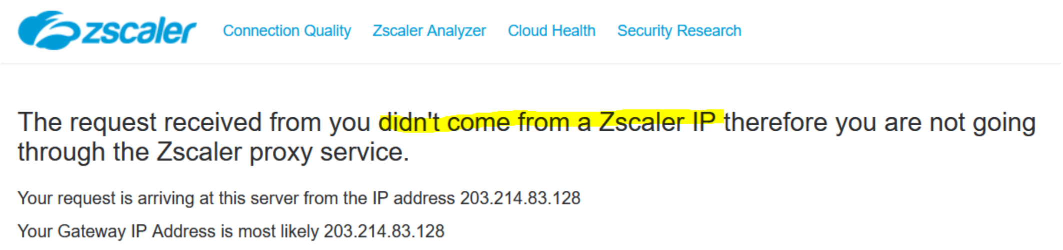
Invalid Request. Authentication is disabled for your location

Error Code: 211000

Need help? Contact our support team at +91-9000000000, support@11365593.zscalerthree.net D09

zscaler Your organization has selected Zscaler to protect you from internet threats.

Note that normally when you browse to ip.zscaler.com, from anywhere else you get this message that shows the request did not come from the Zscaler IP.



The request received from you didn't come from a Zscaler IP therefore you are not going through the Zscaler proxy service.

Your request is arriving at this server from the IP address 203.214.83.128

Your Gateway IP Address is most likely 203.214.83.128