1 Table of Contents

Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
15 Mar 2024	0.1	Ariya Parsamanesh	Initial creation
17 Mar 2024	0.2	Ariya Parsamanesh	Added the CL2 with authentication

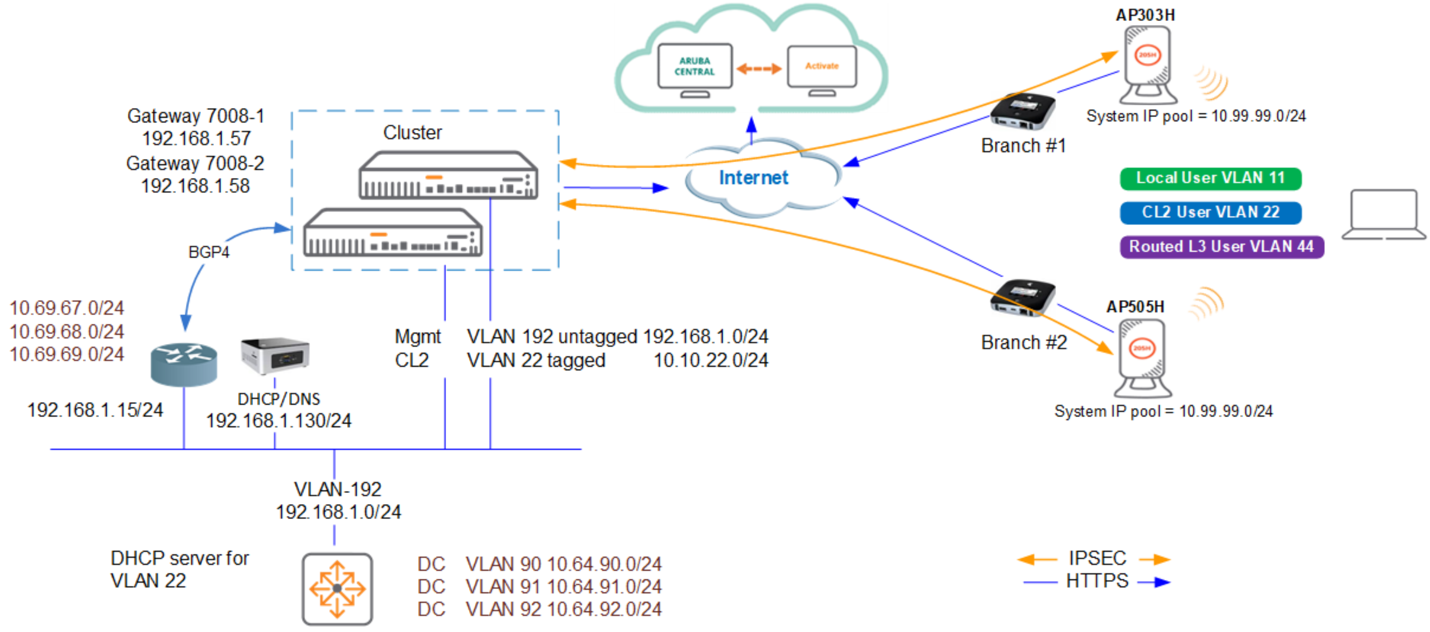
2 Microbranch with AOS10

AOS 10.x enables APs in remote sites to use most of the SD-WAN features and be managed by Aruba Central. For Micro Branch deployments, AOS 10.x currently supports deployment of a single AP as a Micro Branch AP in remote sites. The AOS 10.x enables these APs to form orchestrated IPsec tunnels to the Gateway cluster.

Microbranch APs support

- Orchestrated tunnels and routes (hub & spoke)
- VPNC Clustering
- PBR for local breakout (incl. 1st packet classification)
- Gateway Like WAN Monitoring
- Cloud Security Orchestration (Aruba AXIS, ZScaler, etc)

The topology that we'll be deploying is as shown below.



This is a 5x parts microbranch series. The aim here is to provide the starting point to put together a solution that include the AOS10 APs as microbranch, two VPNCs that are clustered along with Aruba Central to configure and monitor the solution.

- Part1 – Solution overview, basic configuration and testing of VPNC and AOS10 AP
- Part2 – Centralised L2 forwarding mode with authentication and policy-based routing
- Part3 – NATed Layer 3 forwarding mode with centralised authentication proxy
- Part4 – Routed Layer 3 forwarding mode with centralised authentication proxy
- Part5 – Overlay Route Orchestrator, route summarisation, BGP routes redistribution and monitoring

2.1 Things you need

- Two AOS10 APs running 10.4.0.2 or later
- AOS10 VPNCs running 10.4.0.2 or later
- Aruba Central account with eval licenses.
- LAN switch
- Operational Internet link

2.2 IP Addressing

This tables shows the IP addressing, subnets and routes that we'll be using.

	System IP Pool	**Local VLAN (SNAT)**	**Centralised L2**	**Routed L3 (shared Pool)**	**Configured Routes**
	Used for Tunnel-inner-ip	VLAN11	VLAN22	VLAN44	
Microbranch1	10.99.99.7/32	10.11.11.1/24		10.44.44.81/28	
Microbranch2	10.99.99.4/32	10.11.11.1/24		10.44.44.17/28	
DC DHCP server			10.10.22.1/24		
VPNC 1	192.168.1.57/24				
VPNC 2	192.168.1.58/24				
VPNC – static routes					10.64.90.0/24 10.64.91.0/24 10.64.92.0/24
VPNC – BGP routes					10.69.67.0/24 10.69.68.0/24 10.69.69.0/24

3 Microbranch Centralised L2 Configuration

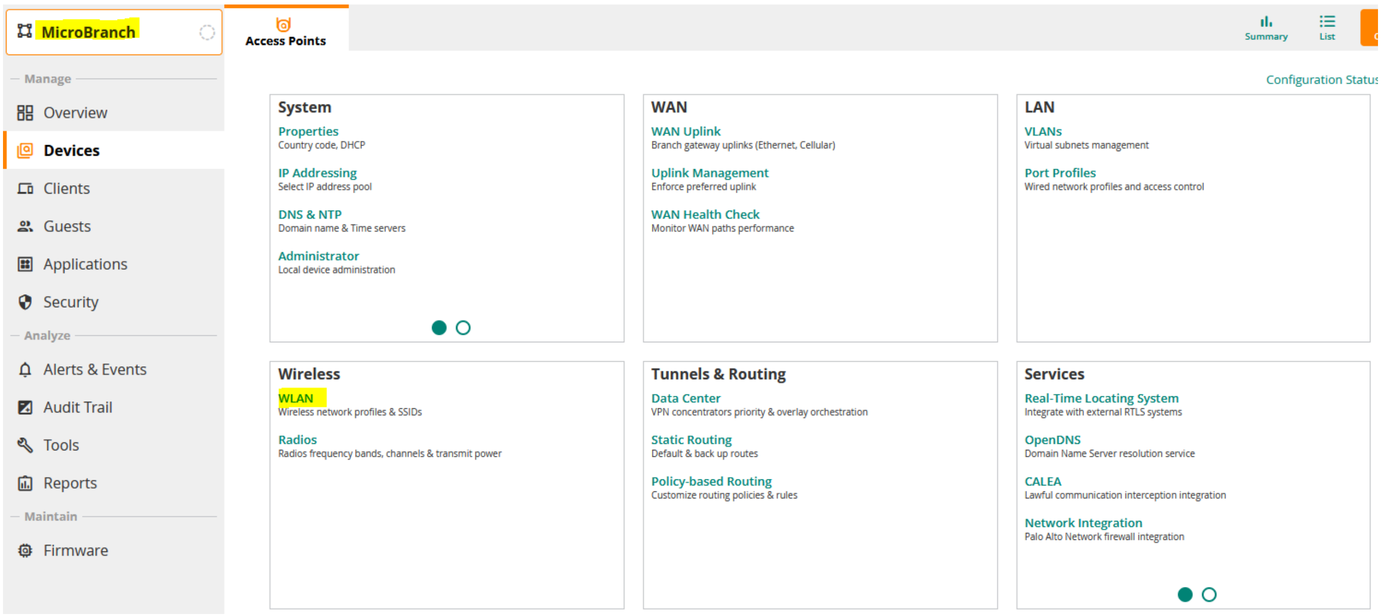
In this section we'll configure the SSID for centralised Layer 2. In this mode

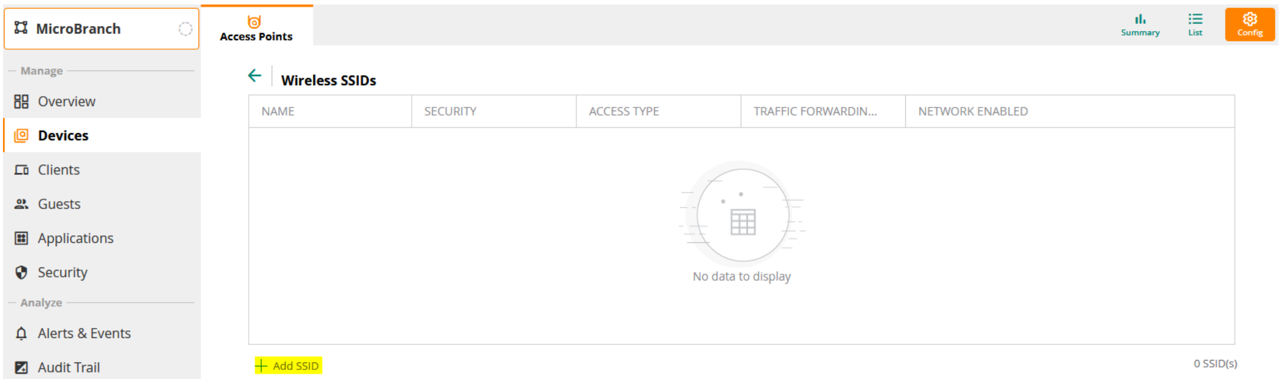
- DHCP service for the VLAN is performed by the DHCP server in the DC.
- The client traffic to DC is sourced with the client's IP address and no NATing is performed
- Other routes in DC needs PBR to be configured for the CL2 client to overwrite the default split tunnelling behaviour
- Client traffic to Internet is done through split tunnel at the AP even though it has a default gateway which is in DC and it will be source NAT with the AP's uplink IP address.

Note that since we have a VPNC cluster the cluster will be the RADIUS proxy for CL2 mode SSID.

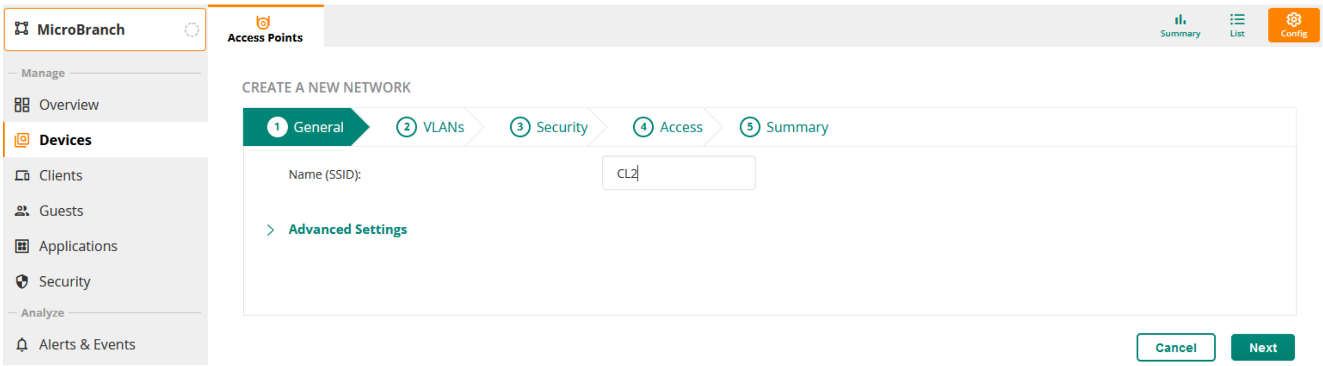
3.1 CL2 WLAN Configuration

From the group level we'll add a CL2 SSID.


MicroBranch
Access Points
Summary
List
Manage
Overview
Devices
Clients
Guests
Applications
Security
Analyze
Alerts & Events
Audit Trail
Tools
Reports
Maintain
Firmware
Configuration Status
System
Properties
Country code, DHCP
IP Addressing
Select IP address pool
DNS & NTP
Domain name & Time servers
Administrator
Local device administration
WAN
WAN Uplink
Branch gateway uplinks (Ethernet, Cellular)
Uplink Management
Enforce preferred uplink
WAN Health Check
Monitor WAN paths performance
LAN
VLANs
Virtual subnets management
Port Profiles
Wired network profiles and access control
Wireless
WLAN
Wireless network profiles & SSIDs
Radios
Radios frequency bands, channels & transmit power
Tunnels & Routing
Data Center
VPN concentrators priority & overlay orchestration
Static Routing
Default & back up routes
Policy-based Routing
Customize routing policies & rules
Services
Real-Time Locating System
Integrate with external RTLS systems
OpenDNS
Domain Name Server resolution service
CALEA
Lawful communication interception integration
Network Integration
Palo Alto Network firewall integration



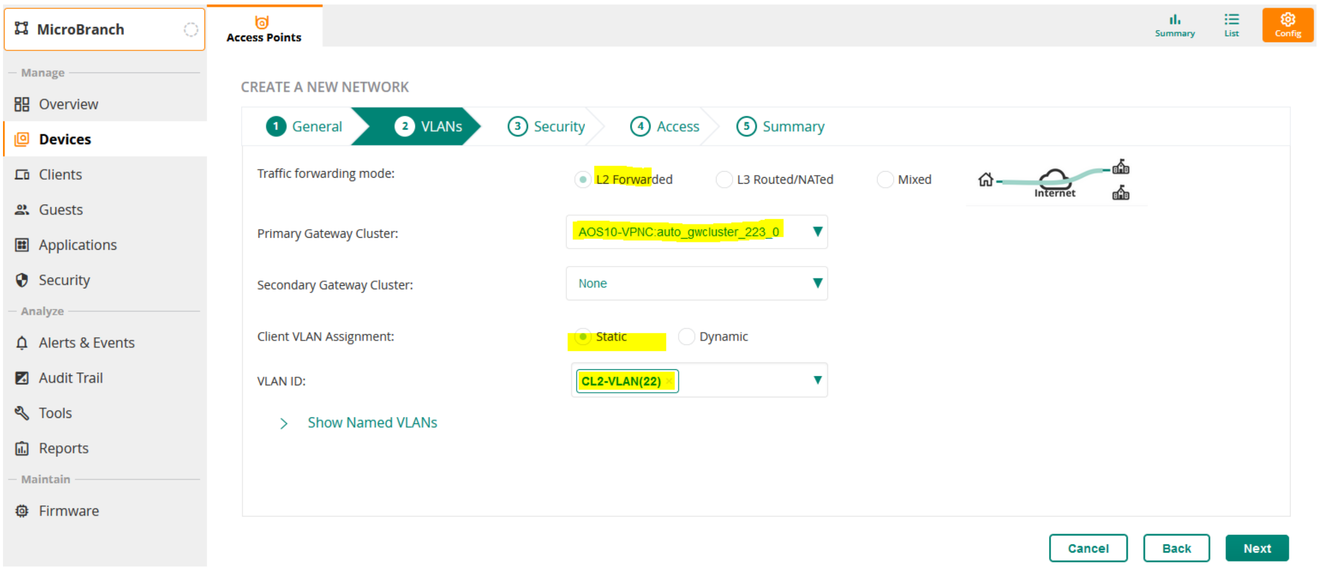
NAME	SECURITY	ACCESS TYPE	TRAFFIC FORWARDIN...	NETWORK ENABLED



CREATE A NEW NETWORK

Name (SSID): CL2

Advanced Settings



CREATE A NEW NETWORK

Traffic forwarding mode: ● L2 Forwarded ○ L3 Routed/NATed ○ Mixed

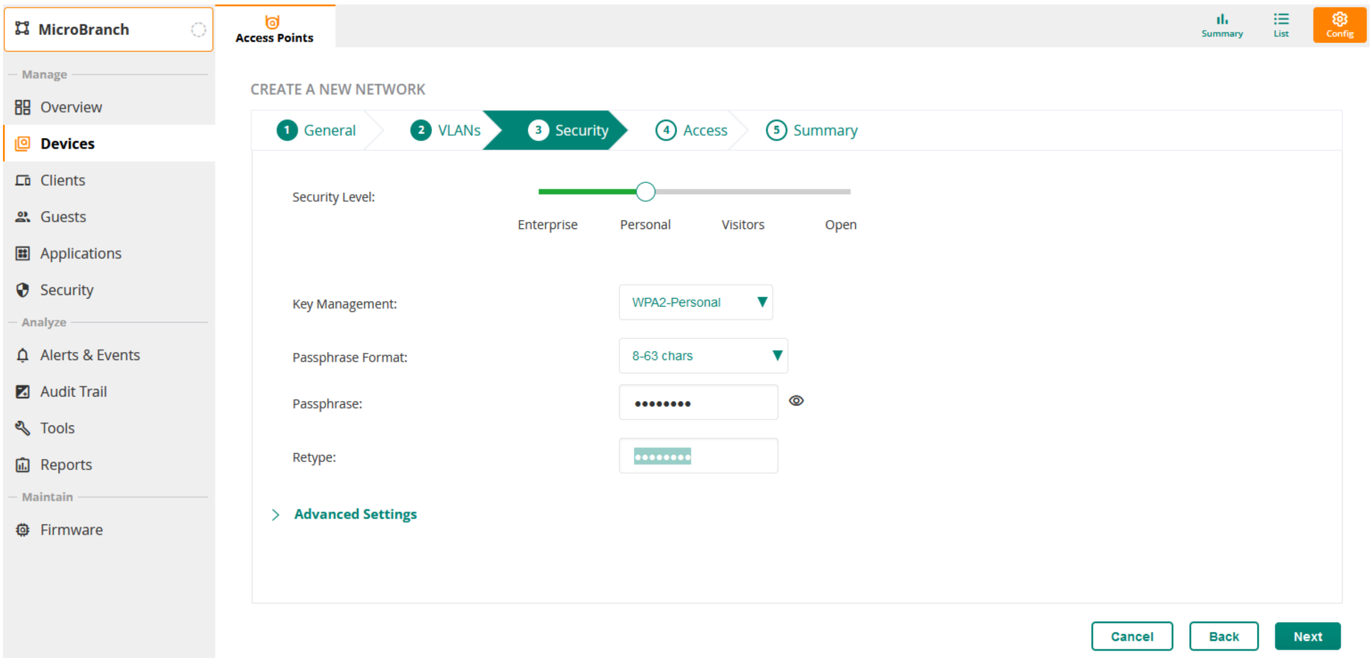
Primary Gateway Cluster: AOS10-VPNC:auto_gwcluster_223_0

Secondary Gateway Cluster: None

Client VLAN Assignment: ● Static ○ Dynamic

VLAN ID: CL2-VLAN(22)

Show Named VLANs



CREATE A NEW NETWORK

Security Level: Enterprise Personal Visitors Open

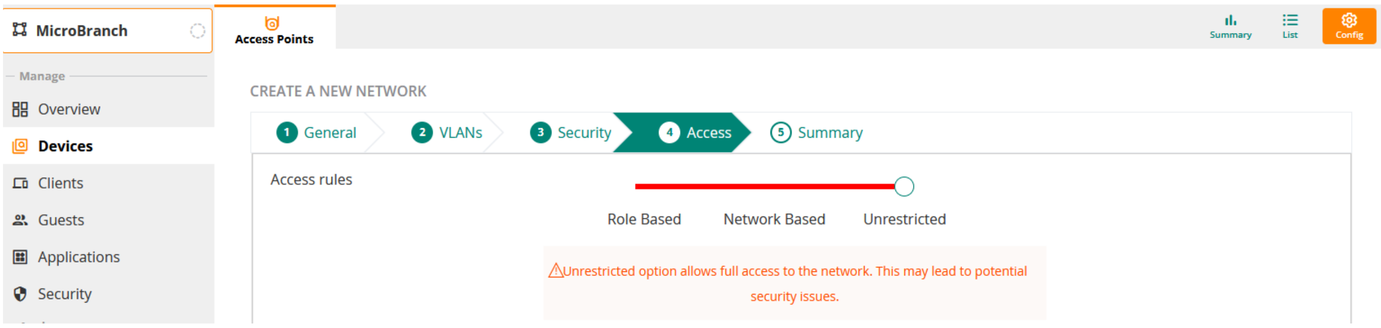
Key Management: WPA2-Personal

Passphrase Format: 8-63 chars

Passphrase: ••••••••

Retype: ••••••••

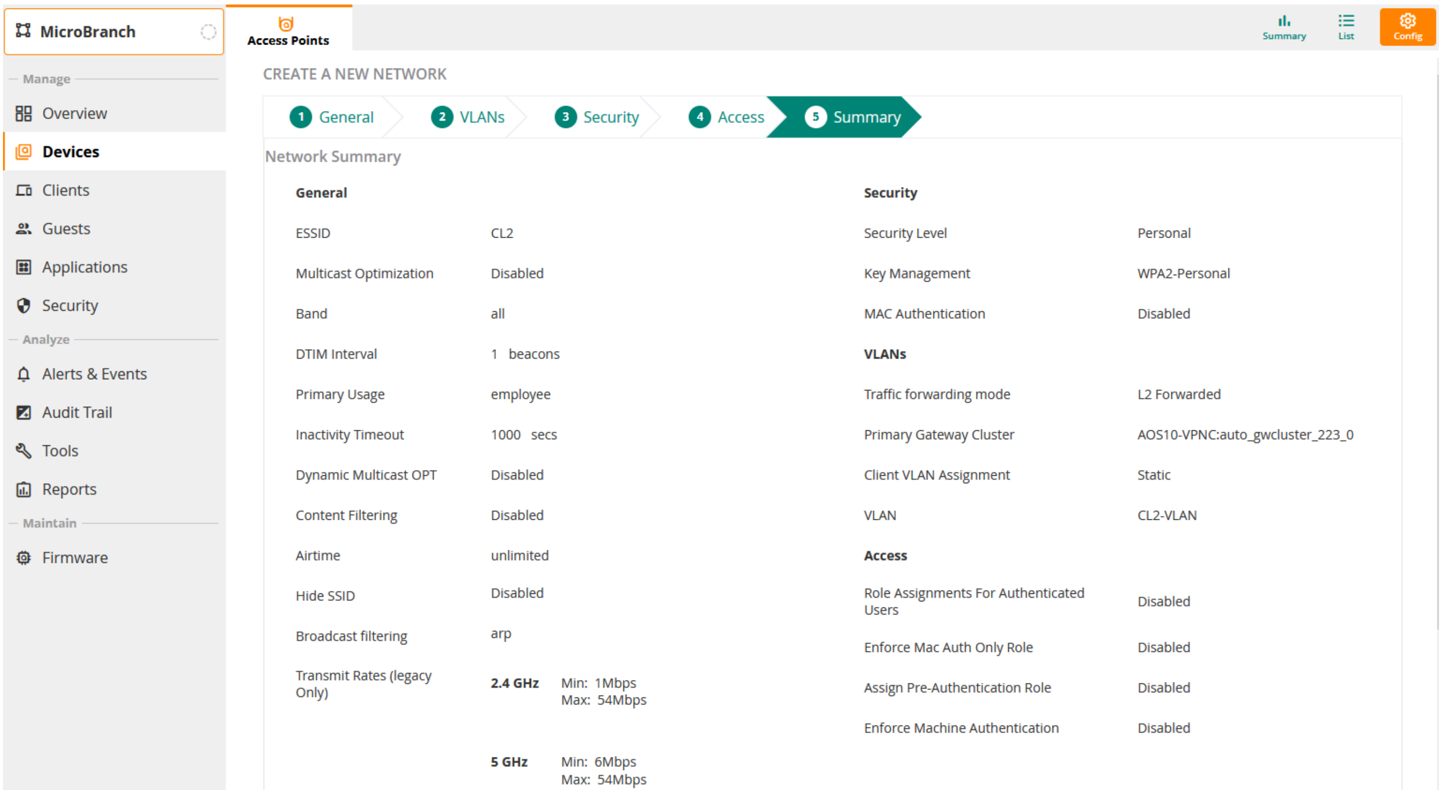
Advanced Settings



CREATE A NEW NETWORK

Access rules: Role Based Network Based Unrestricted

⚠Unrestricted option allows full access to the network. This may lead to potential security issues.

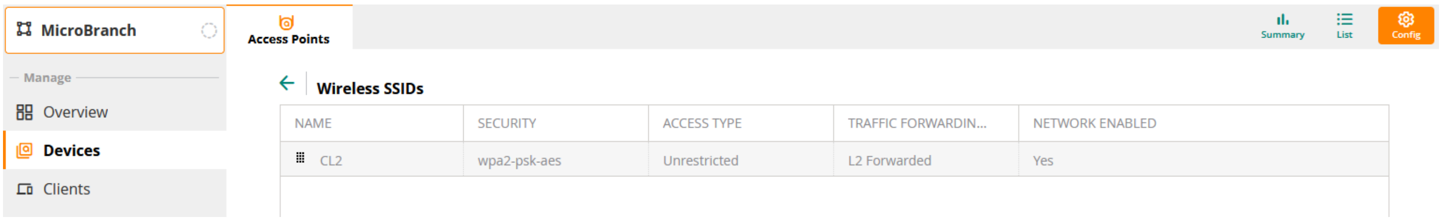


CREATE A NEW NETWORK

Network Summary

General		Security	
ESSID	CL2	Security Level	Personal
Multicast Optimization	Disabled	Key Management	WPA2-Personal
Band	all	MAC Authentication	Disabled
DTIM Interval	1 beacons	**VLANs**	
Primary Usage	employee	Traffic forwarding mode	L2 Forwarded
Inactivity Timeout	1000 secs	Primary Gateway Cluster	AOS10-VPNC:auto_gwcluster_223_0
Dynamic Multicast OPT	Disabled	Client VLAN Assignment	Static
Content Filtering	Disabled	VLAN	CL2-VLAN
Airtime	unlimited	**Access**	
Hide SSID	Disabled	Role Assignments For Authenticated Users	Disabled
Broadcast filtering	arp	Enforce Mac Auth Only Role	Disabled
Transmit Rates (legacy Only)	**2.4 GHz** Min: 1Mbps Max: 54Mbps	Assign Pre-Authentication Role	Disabled
		Enforce Machine Authentication	Disabled
	5 GHz Min: 6Mbps Max: 54Mbps		

Now that we have configured our CL2 SSID, we'll get a client to connect to it.

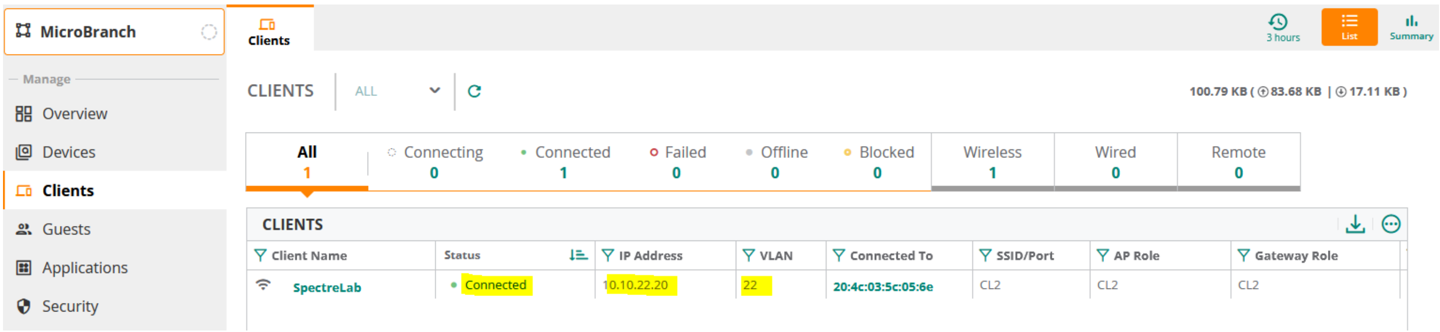


Wireless SSIDs

NAME	SECURITY	ACCESS TYPE	TRAFFIC FORWARDIN...	NETWORK ENABLED
CL2	wpa2-psk-aes	Unrestricted	L2 Forwarded	Yes

3.2 CL2 SSID Testing

We'll get a client to connect to this SSID.



CLIENTS ALL

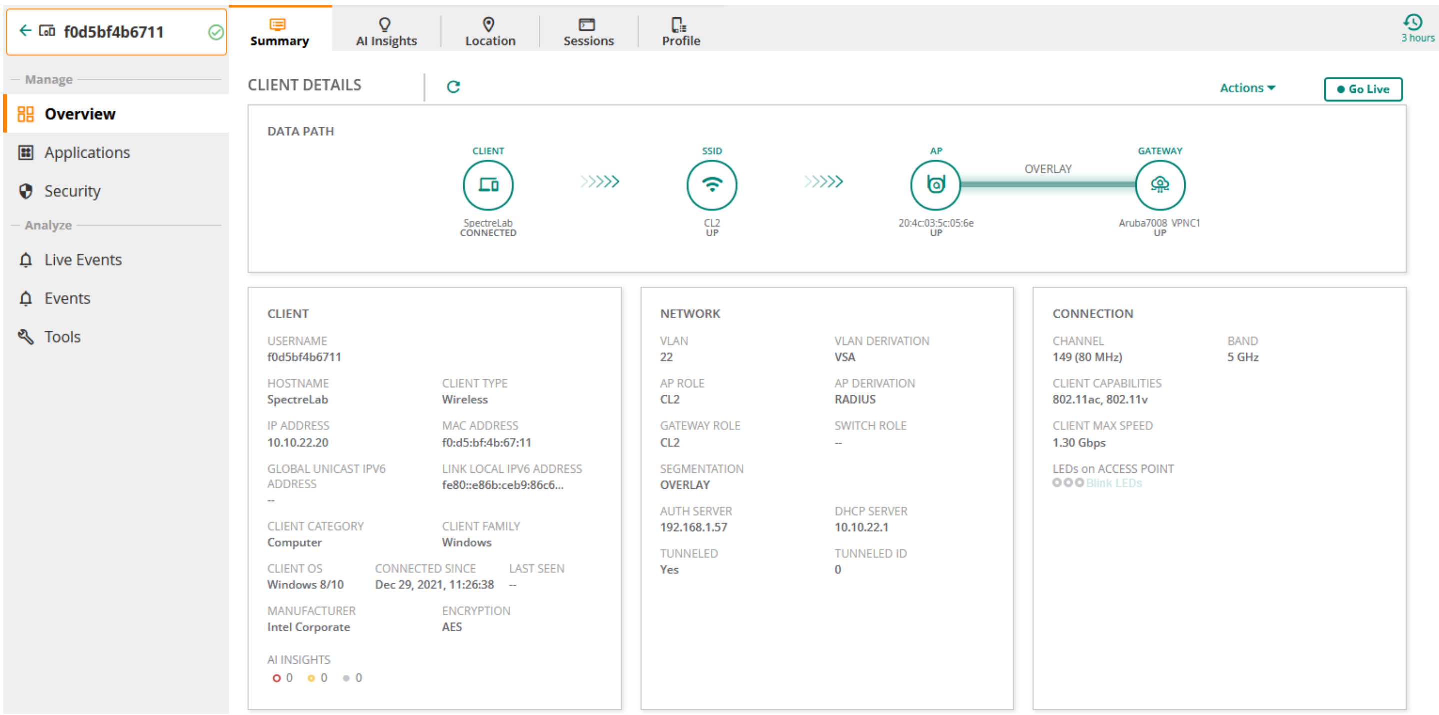
100.79 KB (83.68 KB | 17.11 KB)

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
SpectreLab	Connected	10.10.22.20	22	20:4c:03:5c:05:6e	CL2	CL2	CL2

Once you click on the client's name you get the client details.



CLIENT DETAILS

DATA PATH

SpectreLab CONNECTED → CL2 UP → 20:4c:03:5c:05:6e UP — OVERLAY — Aruba7008_VPNC1 UP

CLIENT

USERNAME f0d5bf4b6711	
HOSTNAME SpectreLab	CLIENT TYPE Wireless
IP ADDRESS 10.10.22.20	MAC ADDRESS f0:d5:bf:4b:67:11
GLOBAL UNICAST IPV6 ADDRESS --	LINK LOCAL IPV6 ADDRESS fe80::e86b:ceb9:86c6...
CLIENT CATEGORY Computer	CLIENT FAMILY Windows
CLIENT OS Windows 8/10	CONNECTED SINCE Dec 29, 2021, 11:26:38
LAST SEEN --	
MANUFACTURER Intel Corporate	ENCRYPTION AES

AI INSIGHTS
○ 0 ● 0 ● 0

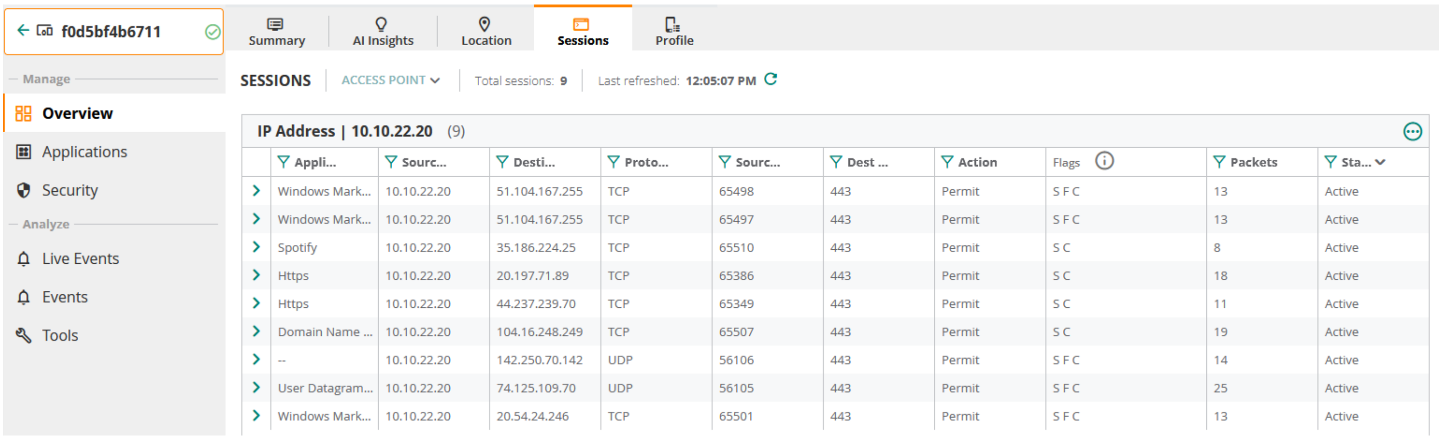
NETWORK

VLAN 22	VLAN DERIVATION VSA
AP ROLE CL2	AP DERIVATION RADIUS
GATEWAY ROLE CL2	SWITCH ROLE --
SEGMENTATION OVERLAY	
AUTH SERVER 192.168.1.57	DHCP SERVER 10.10.22.1
TUNNELED Yes	TUNNELED ID 0

CONNECTION

CHANNEL 149 (80 MHz)	BAND 5 GHz
CLIENT CAPABILITIES 802.11ac, 802.11v	
CLIENT MAX SPEED 1.30 Gbps	
LEDs on ACCESS POINT Blink LEDs	

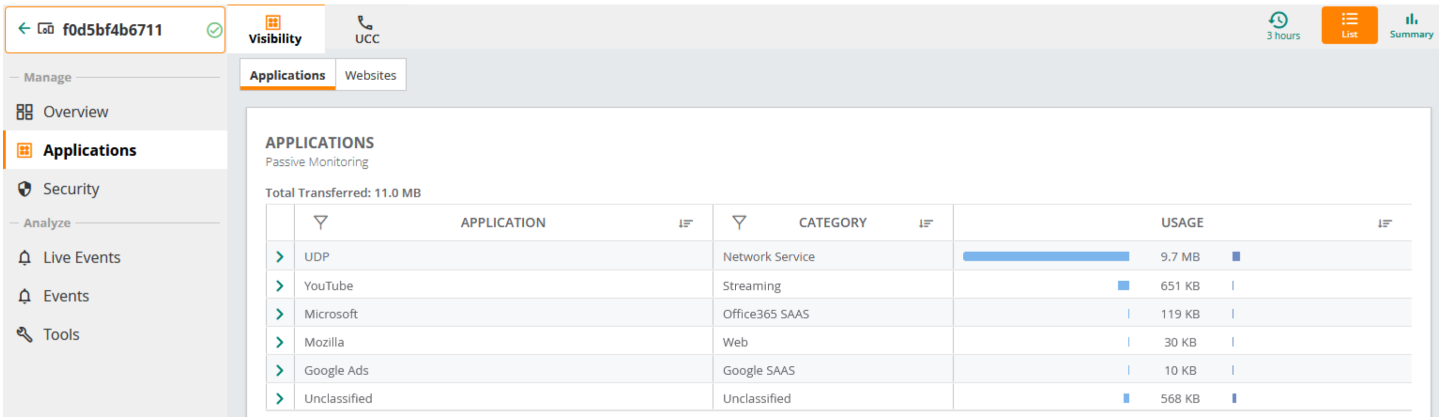
We can also check the sessions and the Applications for this user



SESSIONS | Total sessions: 9 | Last refreshed: 12:05:07 PM

IP Address | 10.10.22.20 (9)

Appli...	Sourc...	Desti...	Proto...	Sourc...	Dest ...	Action	Flags	Packets	Sta...
Windows Mark...	10.10.22.20	51.104.167.255	TCP	65498	443	Permit	S F C	13	Active
Windows Mark...	10.10.22.20	51.104.167.255	TCP	65497	443	Permit	S F C	13	Active
Spotify	10.10.22.20	35.186.224.25	TCP	65510	443	Permit	S C	8	Active
Https	10.10.22.20	20.197.71.89	TCP	65386	443	Permit	S C	18	Active
Https	10.10.22.20	44.237.239.70	TCP	65349	443	Permit	S C	11	Active
Domain Name ...	10.10.22.20	104.16.248.249	TCP	65507	443	Permit	S C	19	Active
--	10.10.22.20	142.250.70.142	UDP	56106	443	Permit	S F C	14	Active
User Datagram...	10.10.22.20	74.125.109.70	UDP	56105	443	Permit	S F C	25	Active
Windows Mark...	10.10.22.20	20.54.24.246	TCP	65501	443	Permit	S F C	13	Active

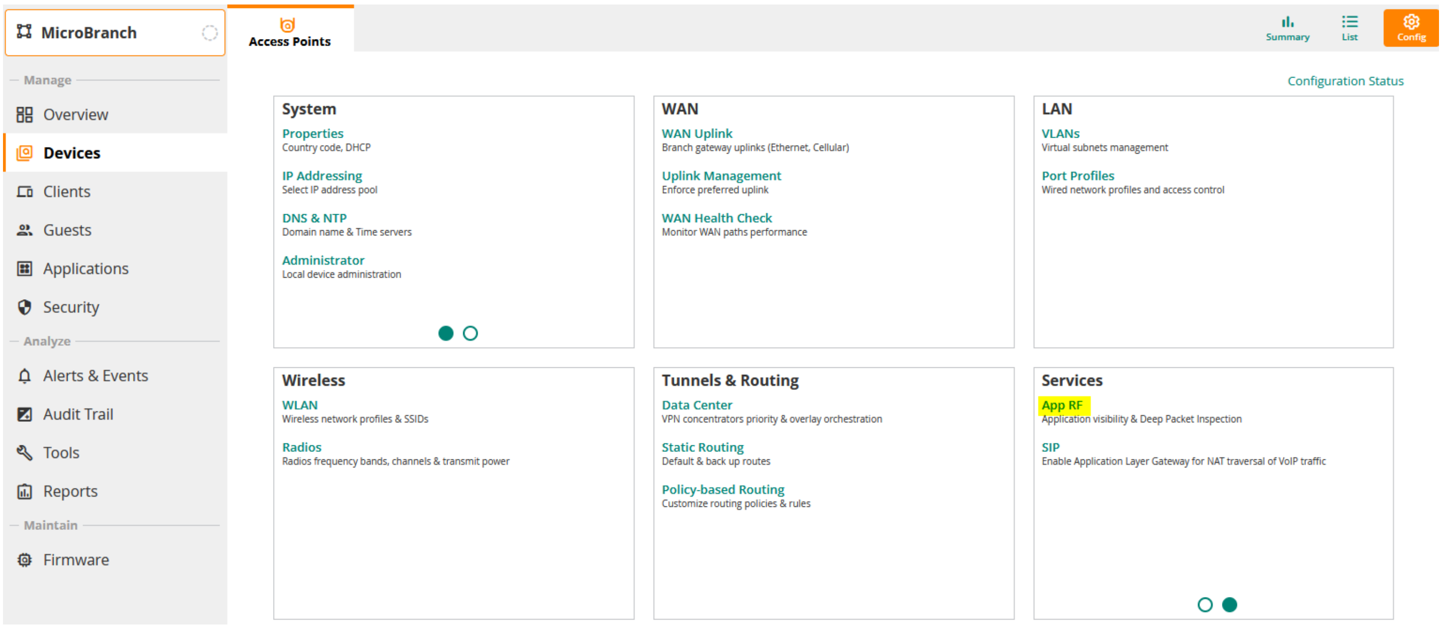


APPLICATIONS
Passive Monitoring

Total Transferred: 11.0 MB

APPLICATION	CATEGORY	USAGE
UDP	Network Service	9.7 MB
YouTube	Streaming	651 KB
Microsoft	Office365 SAAS	119 KB
Mozilla	Web	30 KB
Google Ads	Google SAAS	10 KB
Unclassified	Unclassified	568 KB

Note that for the application to be visible here, you need to enable AppRF.



System

Properties
Country code, DHCP

IP Addressing
Select IP address pool

DNS & NTP
Domain name & Time servers

Administrator
Local device administration

WAN

WAN Uplink
Branch gateway uplinks (Ethernet, Cellular)

Uplink Management
Enforce preferred uplink

WAN Health Check
Monitor WAN paths performance

LAN

VLANs
Virtual subnets management

Port Profiles
Wired network profiles and access control

Wireless

WLAN
Wireless network profiles & SSIDs

Radios
Radios frequency bands, channels & transmit power

Tunnels & Routing

Data Center
VPN concentrators priority & overlay orchestration

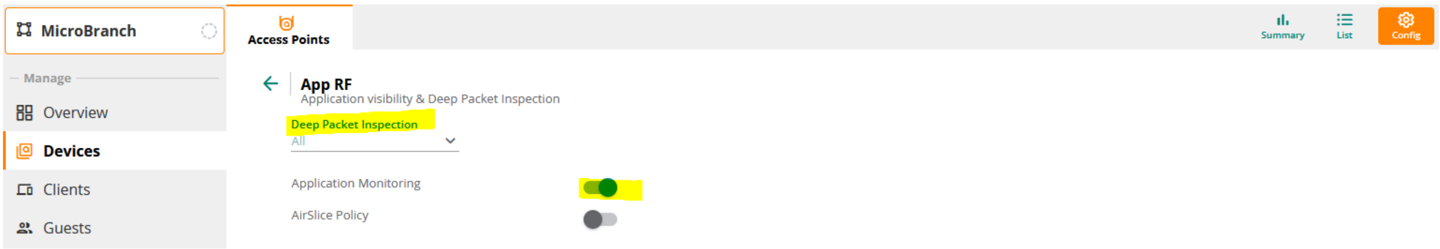
Static Routing
Default & back up routes

Policy-based Routing
Customize routing policies & rules

Services

App RF
Application visibility & Deep Packet Inspection

SIP
Enable Application Layer Gateway for NAT traversal of VoIP traffic



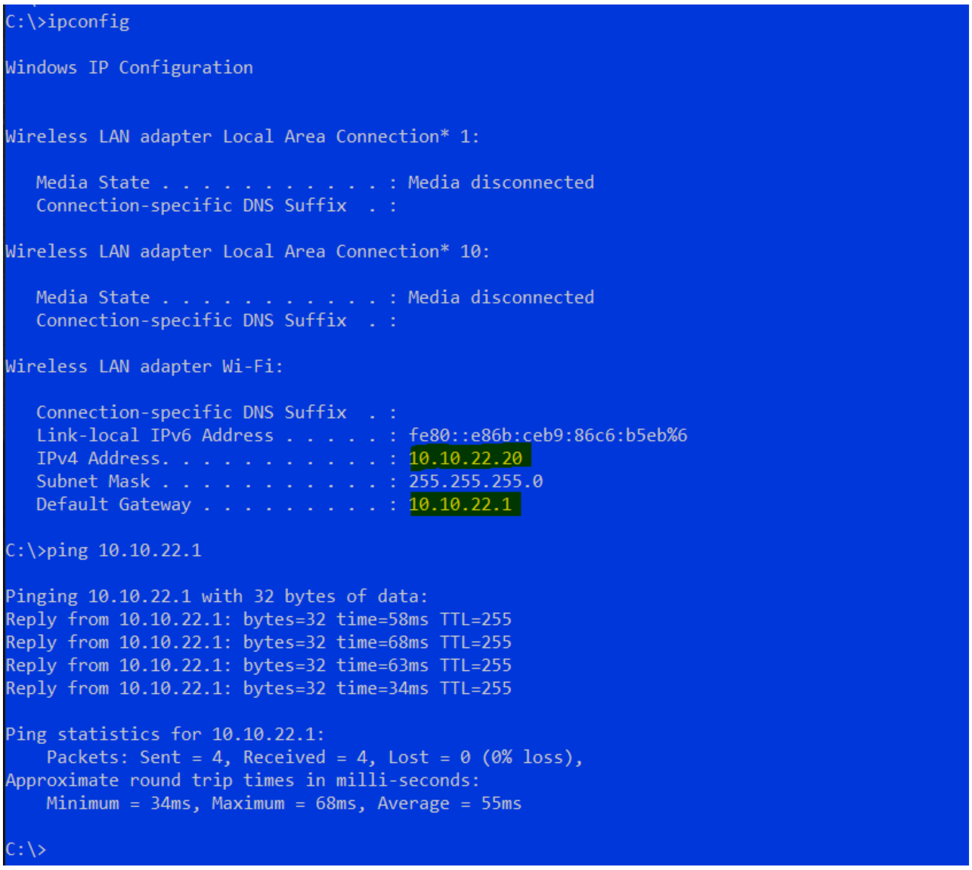
App RF
Application visibility & Deep Packet Inspection

Deep Packet Inspection
All

Application Monitoring ●

AirSlice Policy ○

Here is the IP address info from the client.



```
C:\>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e86b:ceb9:86c6:b5eb%6
   IPv4 Address. . . . . . . . . . . : 10.10.22.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.22.1

C:\>ping 10.10.22.1

Pinging 10.10.22.1 with 32 bytes of data:
Reply from 10.10.22.1: bytes=32 time=58ms TTL=255
Reply from 10.10.22.1: bytes=32 time=68ms TTL=255
Reply from 10.10.22.1: bytes=32 time=63ms TTL=255
Reply from 10.10.22.1: bytes=32 time=34ms TTL=255

Ping statistics for 10.10.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 68ms, Average = 55ms

C:\>
```

Note that we can successfully ping the default gateway 10.10.22.1 but as stated before the AP performs split tunnel for any other traffic that is not on 10.10.22.0/24 and hence it uses the AP's default route. Hence, we cannot ping any of the DC routes like 10.64.90.0/24, 10.64.91.0/24 and 10.64.92.0/24

Here is the number of CLI commands that you can run on the AP.

```
20:4c:03:5c:05:6e# sh clients

Client List
-----------
Name          IP Address   MAC Address        OS      ESSID  Access Point       Channel
Type  Role  IPv6 Address                 Signal    Speed (mbps)
----          ----------   -----------        --      -----  ------------       -------
----  ----  ------------                 ------    ------------
f0d5bf4b6711  10.10.22.20  f0:d5:bf:4b:67:11  Win 10  CL2    20:4c:03:5c:05:6e  149E
AC    CL2   fe80::e86b:ceb9:86c6:b5eb  67(good)  866(good)
Number of Clients   :1
Info timestamp      :11663
20:4c:03:5c:05:6e#
```

```
20:4c:03:5c:05:6e# sh datapath session
Datapath Session Table Entries

------------------------------

Flags: A - Application Firewall Inspect
       C - client, D - deny, E - Media Deep Inspect
       F - fast age, G - media signal, H - high prio
       I - Deep inspect, L - ALG session, M - mirror, N - dest NAT
       O - Session is programmed through SDN/Openflow controller
       P - set prio, R - redirect, S - src NAT,
       T - set ToS, U - Locally destined, V - VOIP
       X - Http/https redirect for dpi denied session
       Y - no syn
       a - rtp analysis, h - Https redirect error page
       i - in offload flow, m - media mon
       p - Session is marked as permanent
       s - media signal
       d - DPI cache hit
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor, t - time based, i - in flow
Flow Offload Blacklist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel

Source IP         Destination IP  Prot SPort Dport Cntr Prio ToS Age Destination TAge Packets Bytes Flags
Offload flags
----------------  --------------  ---- ----- ----- ---- ---- --- --- ----------- ---- ------- ----- ------ --
10.10.22.20       204.79.197.203  6    49222 443   0    0    0   1   dev27       30   12      109f  SCi
10.10.22.20       10.10.22.1      1    51    2048  0    0    0   0   dev27       14   1       3c    FCI
10.10.22.20       10.10.22.1      1    50    2048  0    0    0   0   dev27       19   1       3c    FCI
10.10.22.20       10.10.22.1      1    49    2048  0    0    0   1   dev27       1e   1       3c    FCI
10.10.22.20       10.10.22.1      1    48    2048  0    0    0   1   dev27       23   1       3c    FCI
10.10.22.20       74.125.109.42   17   65317 443   0    0    0   1   dev27       1d   2f      e95   FSCi
10.10.22.20       44.237.239.70   6    65349 443   0    0    0   12  dev27       3864 14      a28   SCi
10.10.22.20       20.54.24.246    6    49220 443   0    0    0   6   dev27       1e2  c       704   SCi
10.10.22.1        10.10.22.20     1    49    0     0    0    56  1   dev27       1e   1       3c    FI
10.10.22.1        10.10.22.20     1    48    0     0    0    56  1   dev27       23   1       3c    FI
10.10.22.1        10.10.22.20     1    51    0     0    0    56  1   dev27       14   1       3c    FI
10.10.22.1        10.10.22.20     1    50    0     0    0    56  1   dev27       19   1       3c    FI
10.10.22.20       104.16.248.249  6    65507 443   0    0    0   1   dev27       2759 41d     1df6d SCi
10.10.22.20       142.250.70.142  17   56106 443   0    0    0   0   dev27       2d   8       8c5   FSCi
10.10.22.20       1.1.1.1         17   50409 53    0    0    0   0   dev27       31   2       72    FSCIAd E
10.10.22.20       20.197.71.89    6    49174 443   0    0    0   56  dev27       1b47 f       d50   Sci

20:4c:03:5c:05:6e#
```

Here the traffic is getting source NATed for all except the one that is bound for 10.10.22.0/24

Remember we have 3x datacentre VLANs (10.64.90.0/24, 10.64.91.0/24 and 10.64.92.0/24) when I try to ping 10.64.90.1 from the client that is connected to CL2 SSID, the ping fails. You can use this command to check if the traffic is going through the IPSEC tunnel or is AP split tunnelling it.

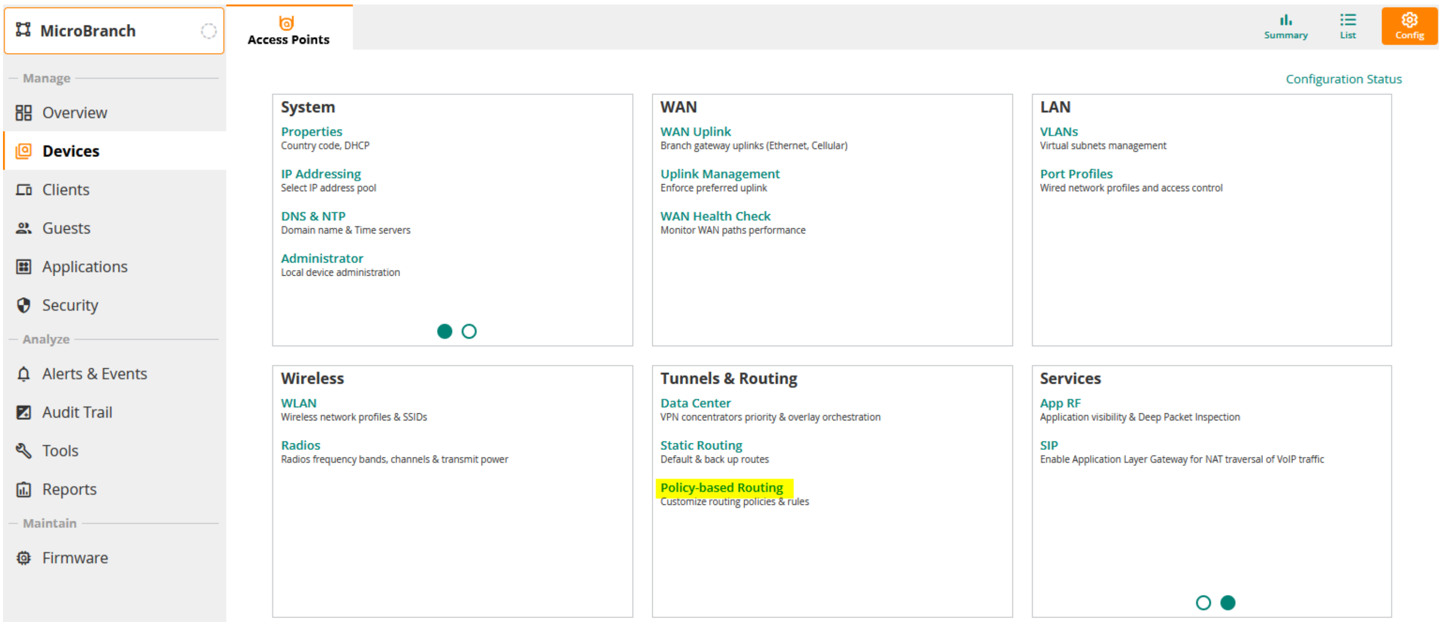
```
20:4c:03:5c:05:6e# sh datapath route
Route Table Entries
-------------------
Flags: L - Local, P - Permanent,  T - Tunnel, Y - Dirty, I - IPsec, M - Mobile, A - ARP,
D - Drop, U - Use Default Gateway, G - PPPoE/3G/4G Gateway

       IP              Mask            Gateway        Cost  VLAN  Flags
---------------  ---------------  ---------------  ----  ----  -----
```

```
0.0.0.0          0.0.0.0          192.168.2.1        0  4092
169.254.0.0      255.255.0.0      169.254.1.1        0  4092  LP
172.31.98.0      255.255.254.0    172.31.98.1        0  3333  D
192.168.2.0      255.255.255.0    192.168.2.50       0  4092  LP

Route Cache Entries
-------------------
Flags: L - local, P - Permanent,  T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop, G
- 3G/4G

       IP               MAC              VLAN      Flags      TunIdx
---------------  -----------------  -----------  ---------  ------
1.1.1.1          B0:B9:8A:A6:CA:3A         4092
10.64.90.1       B0:B9:8A:A6:CA:3A         4092
192.168.1.57     00:00:00:00:00:00  tunnel   26  PT               1
192.168.2.1      B0:B9:8A:A6:CA:3A         4092  A
10.99.99.1       20:4C:03:5C:05:6E         4092  LP
192.168.2.50     20:4C:03:5C:05:6E         4092  LP
20.197.71.89     B0:B9:8A:A6:CA:3A         4092
142.250.70.142   B0:B9:8A:A6:CA:3A         4092
10.10.22.20      F0:D5:BF:4B:67:11           22
172.31.98.1      20:4C:03:5C:05:6E         3333  LP
74.125.109.42    B0:B9:8A:A6:CA:3A         4092
169.254.1.1      20:4C:03:5C:05:6E         4092  LP
184.85.81.146    B0:B9:8A:A6:CA:3A         4092
20:4c:03:5c:05:6e#
```

In the above output we see that the traffic is using VLAN 4092 which is the AP's uplink VLAN.

3.3 Policy Based Routing

Here we'll configure a Policy Based Routing (PBR) so that the CL2 user can reach the data centre routes. As always, we'll start from the group level for the microbranch AP.



System
Properties
Country code, DHCP
IP Addressing
Select IP address pool
DNS & NTP
Domain name & Time servers
Administrator
Local device administration

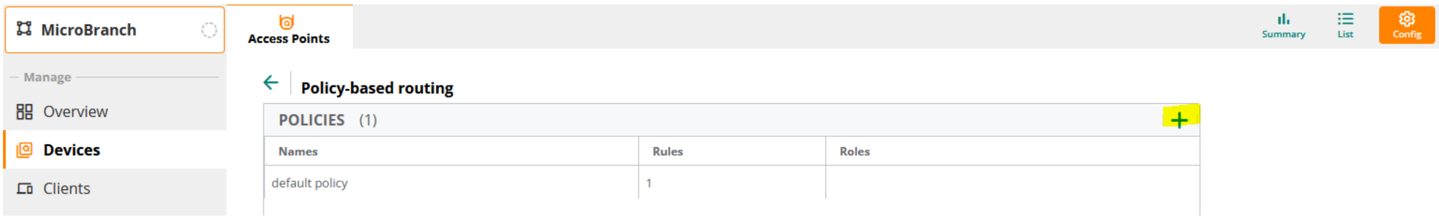
WAN
WAN Uplink
Branch gateway uplinks (Ethernet, Cellular)
Uplink Management
Enforce preferred uplink
WAN Health Check
Monitor WAN paths performance

LAN
VLANs
Virtual subnets management
Port Profiles
Wired network profiles and access control

Wireless
WLAN
Wireless network profiles & SSIDs
Radios
Radios frequency bands, channels & transmit power

Tunnels & Routing
Data Center
VPN concentrators priority & overlay orchestration
Static Routing
Default & back up routes
Policy-based Routing
Customize routing policies & rules

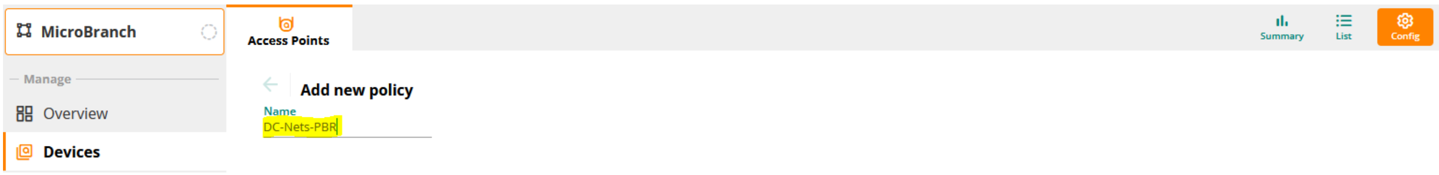
Services
App RF
Application visibility & Deep Packet Inspection
SIP
Enable Application Layer Gateway for NAT traversal of VoIP traffic



Policy-based routing

POLICIES (1)

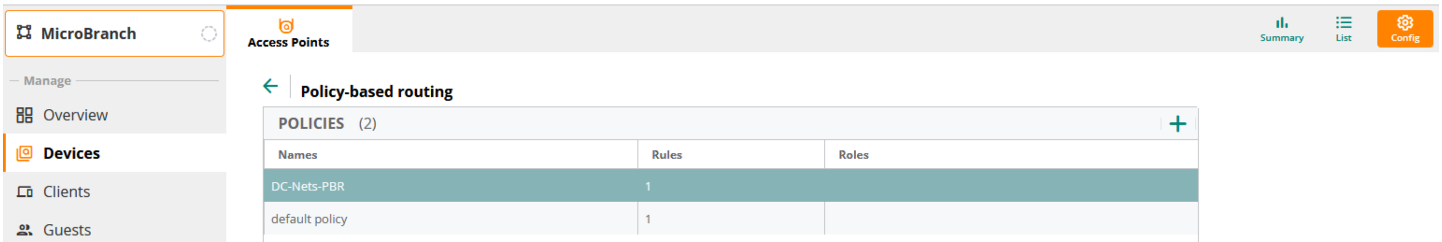
Names	Rules	Roles
default policy	1	



Add new policy

Name
DC-Nets-PBR

Now we’ll edit this new PBR policy.

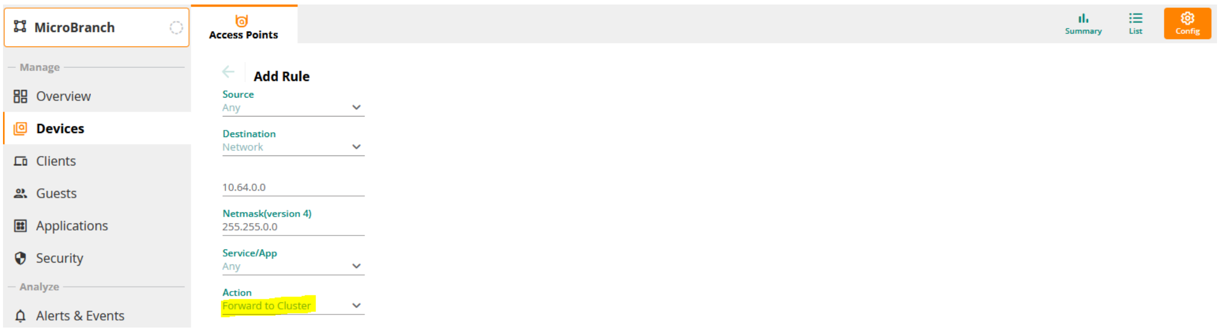


Policy-based routing

POLICIES (2)

Names	Rules	Roles
DC-Nets-PBR	1	
default policy	1	

Note that we have 3x DC networks namely 10.64.90.0/24, 10.64.91.0/24 and 10.64.92.0/24



Add Rule

Source
Any

Destination
Network

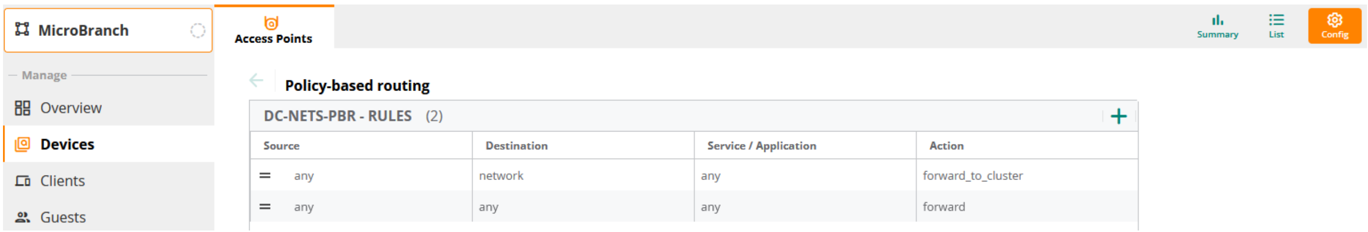
10.64.0.0

Netmask(version 4)
255.255.0.0

Service/App
Any

Action
Forward to Cluster

So, once we have saved it,

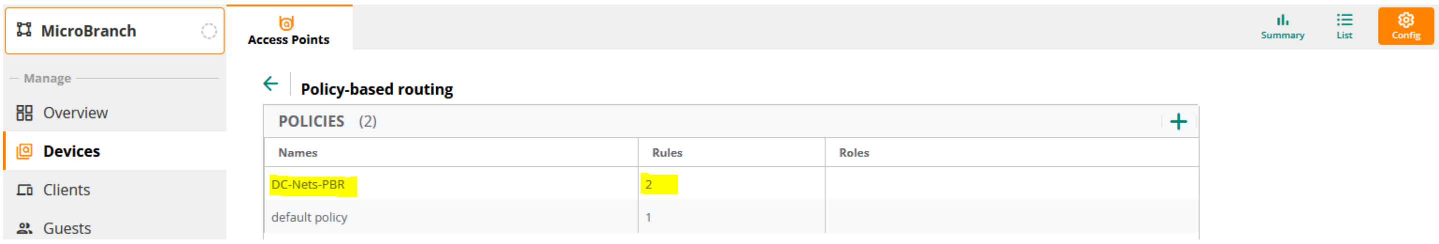


Policy-based routing

DC-NETS-PBR - RULES (2)

Source	Destination	Service / Application	Action
any	network	any	forward_to_cluster
any	any	any	forward

So now we have 2x rules in our PBR policy

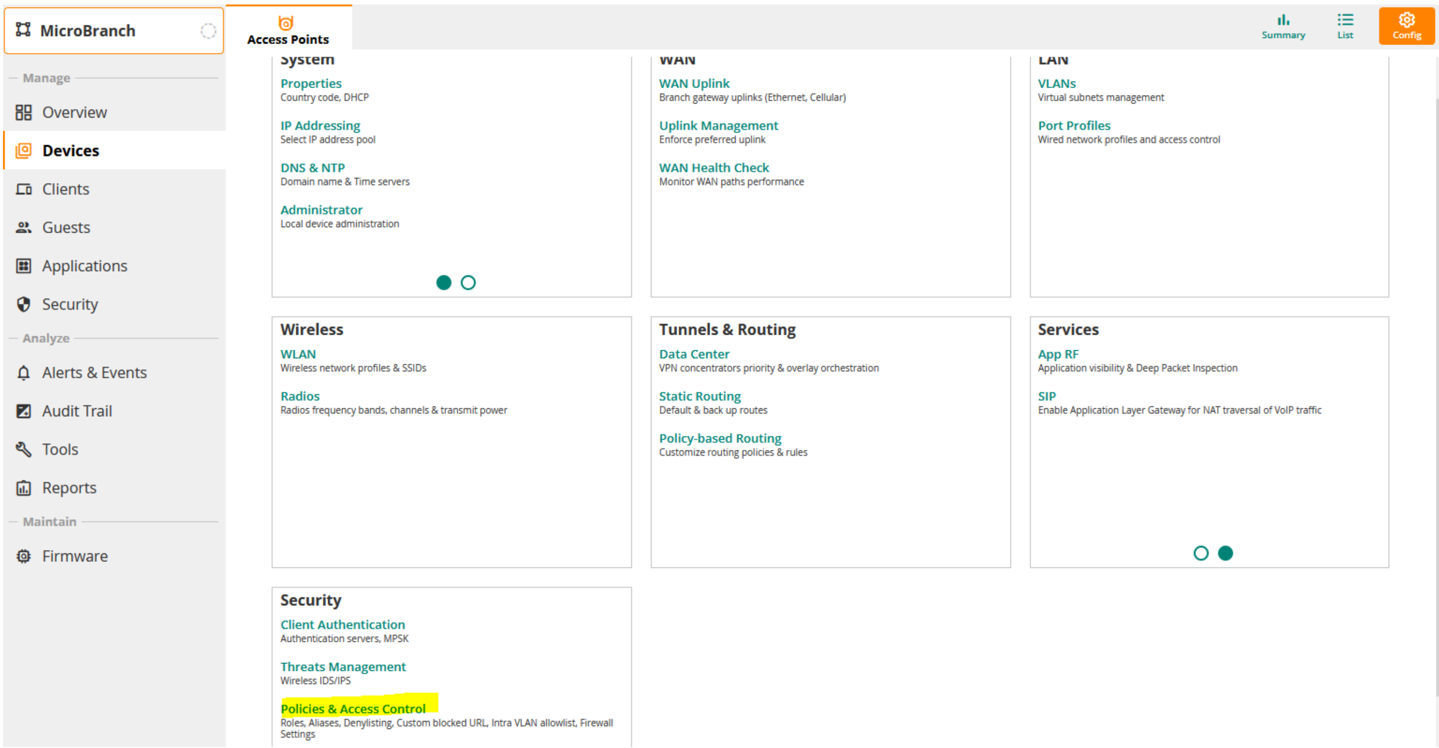


Policy-based routing

POLICIES (2)

Names	Rules	Roles
DC-Nets-PBR	2	
default policy	1	

We should now apply this to the user role.



System
Properties
Country code, DHCP
IP Addressing
Select IP address pool
DNS & NTP
Domain name & Time servers
Administrator
Local device administration

WAN
WAN Uplink
Branch gateway uplinks (Ethernet, Cellular)
Uplink Management
Enforce preferred uplink
WAN Health Check
Monitor WAN paths performance

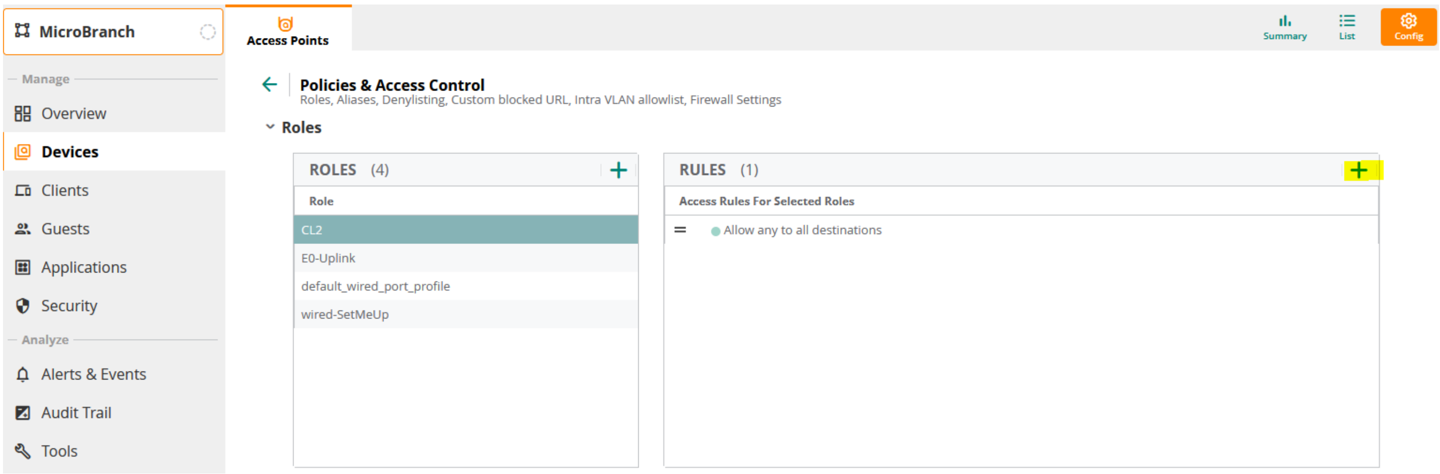
LAN
VLANs
Virtual subnets management
Port Profiles
Wired network profiles and access control

Wireless
WLAN
Wireless network profiles & SSIDs
Radios
Radios frequency bands, channels & transmit power

Tunnels & Routing
Data Center
VPN concentrators priority & overlay orchestration
Static Routing
Default & back up routes
Policy-based Routing
Customize routing policies & rules

Services
App RF
Application visibility & Deep Packet Inspection
SIP
Enable Application Layer Gateway for NAT traversal of VoIP traffic

Security
Client Authentication
Authentication servers, MPSK
Threats Management
Wireless IDS/IPS
Policies & Access Control
Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings



Policies & Access Control
Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings

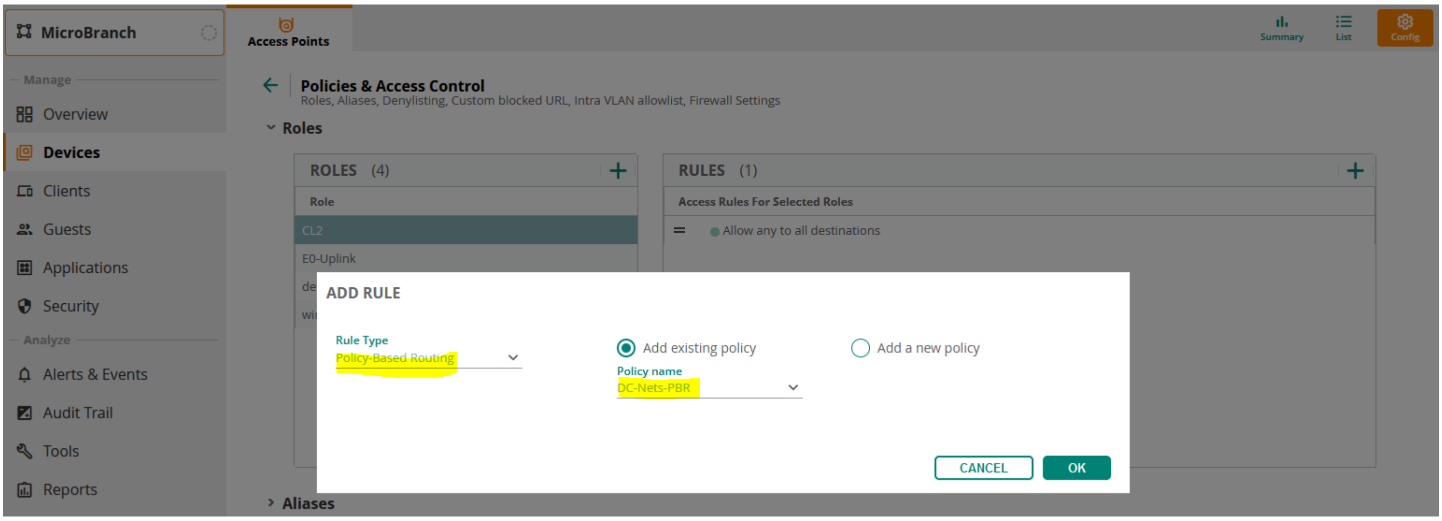
Roles

ROLES (4)

Role
CL2
E0-Uplink
default_wired_port_profile
wired-SetMeUp

RULES (1)

Access Rules For Selected Roles
= ● Allow any to all destinations



Policies & Access Control
Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings

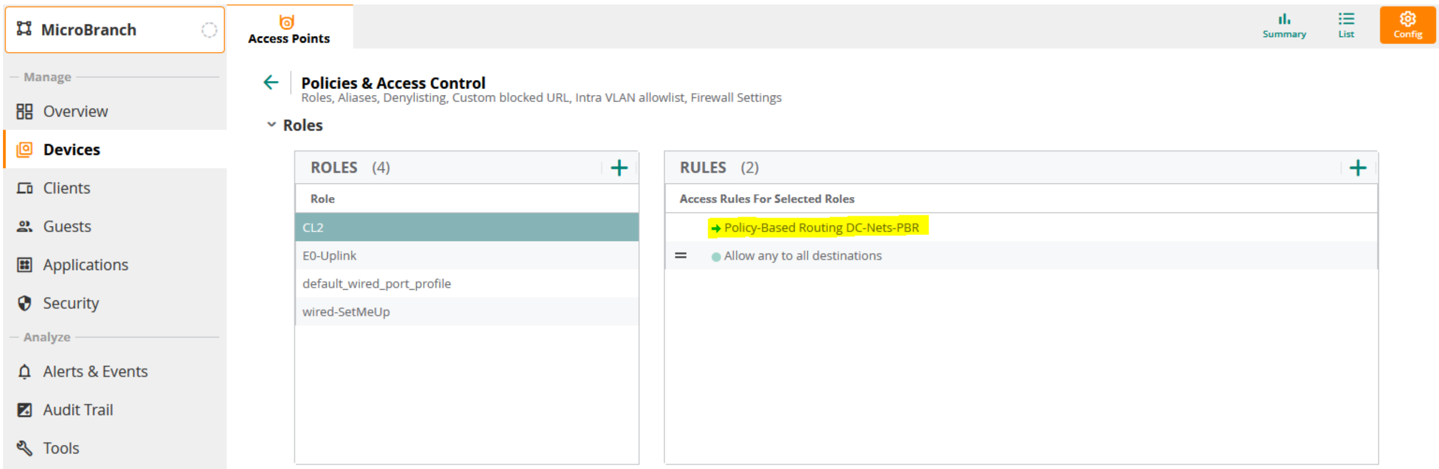
ADD RULE

Rule Type: Policy-Based Routing

● Add existing policy ○ Add a new policy

Policy name: DC-Nets-PBR

Once we save it, it gets displayed as a rule for CL2 user role.



Policies & Access Control
Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings

Roles

ROLES (4)

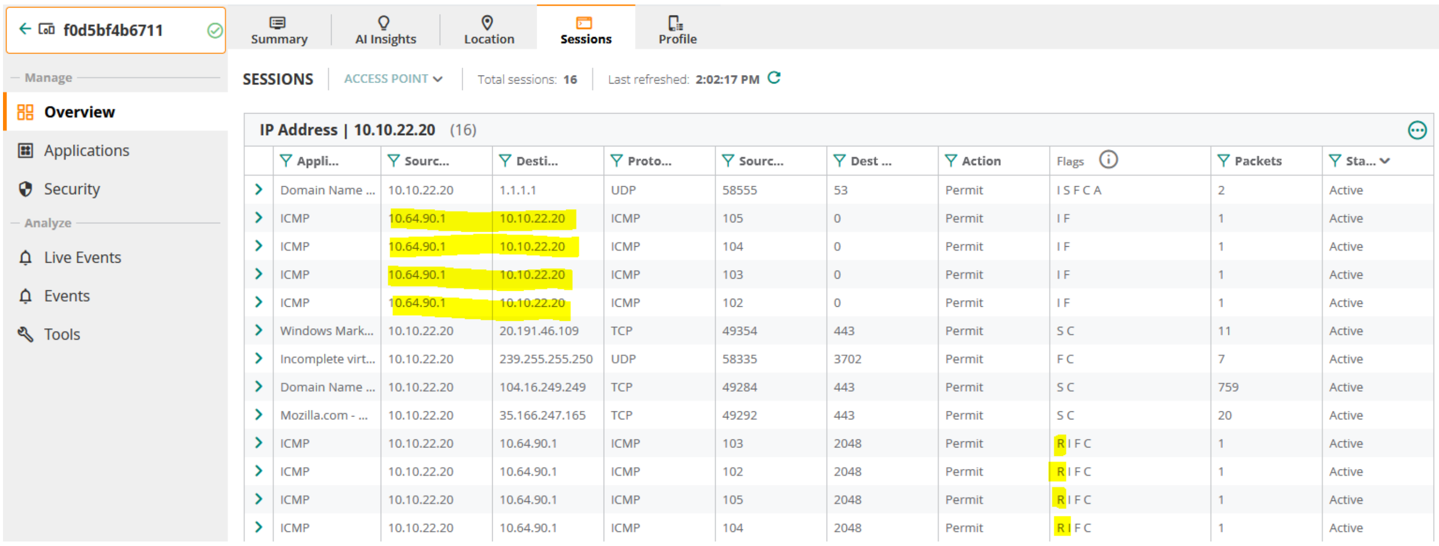
Role
CL2
E0-Uplink
default_wired_port_profile
wired-SetMeUp

RULES (2)

Access Rules For Selected Roles
Policy-Based Routing DC-Nets-PBR
Allow any to all destinations

Now we need to disconnect the CL2 user and reconnect it for the new policy to get applied and will ping 10.64.90.1

The ping is successful this time as we can see it in the session table. Note the "R" flag that means the traffic is redirected.



SESSIONS | ACCESS POINT | Total sessions: 16 | Last refreshed: 2:02:17 PM

IP Address | 10.10.22.20 (16)

Appli...	Sourc...	Desti...	Proto...	Sourc...	Dest ...	Action	Flags	Packets	Sta...
Domain Name ...	10.10.22.20	1.1.1.1	UDP	58555	53	Permit	I S F C A	2	Active
ICMP	10.64.90.1	10.10.22.20	ICMP	105	0	Permit	I F	1	Active
ICMP	10.64.90.1	10.10.22.20	ICMP	104	0	Permit	I F	1	Active
ICMP	10.64.90.1	10.10.22.20	ICMP	103	0	Permit	I F	1	Active
ICMP	10.64.90.1	10.10.22.20	ICMP	102	0	Permit	I F	1	Active
Windows Mark...	10.10.22.20	20.191.46.109	TCP	49354	443	Permit	S C	11	Active
Incomplete virt...	10.10.22.20	239.255.255.250	UDP	58335	3702	Permit	F C	7	Active
Domain Name ...	10.10.22.20	104.16.249.249	TCP	49284	443	Permit	S C	759	Active
Mozilla.com - ...	10.10.22.20	35.166.247.165	TCP	49292	443	Permit	S C	20	Active
ICMP	10.10.22.20	10.64.90.1	ICMP	103	2048	Permit	R I F C	1	Active
ICMP	10.10.22.20	10.64.90.1	ICMP	102	2048	Permit	R I F C	1	Active
ICMP	10.10.22.20	10.64.90.1	ICMP	105	2048	Permit	R I F C	1	Active
ICMP	10.10.22.20	10.64.90.1	ICMP	104	2048	Permit	R I F C	1	Active

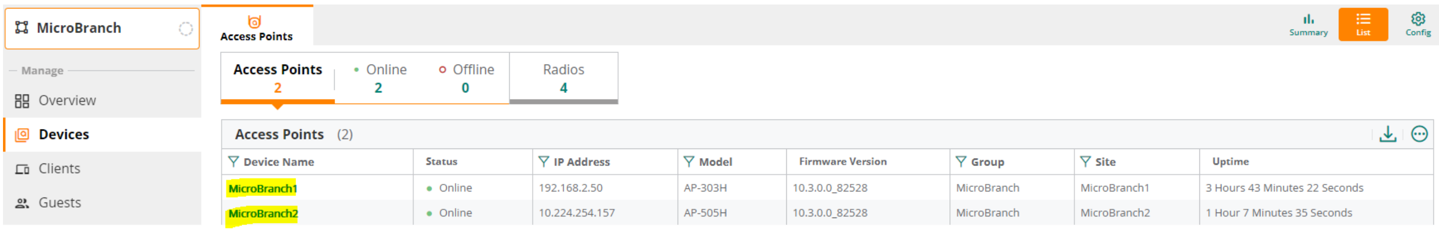
Also checking the datapath session command on the AP.

```
20:4c:03:5c:05:6e# sh datapath session   | incl 10.64
10.64.90.1         10.10.22.20     1    97     0      0     0    56   0    cluster     4     1       3c     FI
10.64.90.1         10.10.22.20     1    96     0      0     0    56   0    cluster     9     1       3c     FI
10.64.90.1         10.10.22.20     1    95     0      0     0    56   0    cluster     e     1       3c     FI
10.64.90.1         10.10.22.20     1    94     0      0     0    56   0    cluster     13    1       3c     FI
10.10.22.20        10.64.90.1      1    97     2048   0     0    0    0    cluster     4     1       3c     FRCI
10.10.22.20        10.64.90.1      1    96     2048   0     0    0    0    cluster     9     1       3c     FRCI
10.10.22.20        10.64.90.1      1    95     2048   0     0    0    0    cluster     e     1       3c     FRCI
10.10.22.20        10.64.90.1      1    94     2048   0     0    0    0    cluster     13    1       3c     FRCI
20:4c:03:5c:05:6e#
```

3.4 Adding Another Microbranch AP

Here we'll add the second microbranch AP, using the same process we described earlier and upgrade it to AOS10.5.1.0

The new AP-505H is then added to same microbranch group. I have renamed the APs to Microbranch 1 and 2



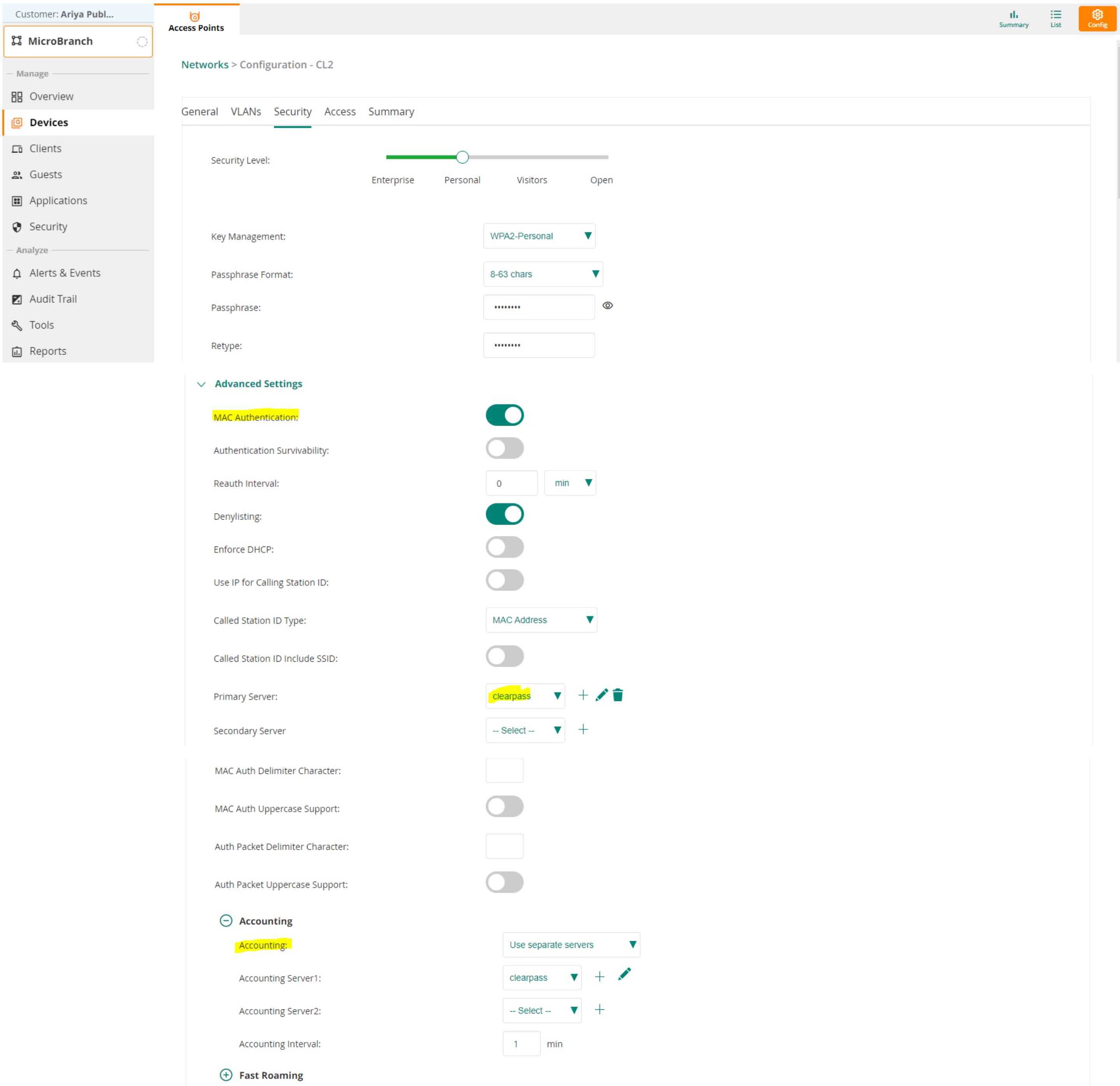
Access Points 2 | Online 2 | Offline 0 | Radios 4

Access Points (2)

Device Name	Status	IP Address	Model	Firmware Version	Group	Site	Uptime
MicroBranch1	Online	192.168.2.50	AP-303H	10.3.0.0_82528	MicroBranch	MicroBranch1	3 Hours 43 Minutes 22 Seconds
MicroBranch2	Online	10.224.254.157	AP-505H	10.3.0.0_82528	MicroBranch	MicroBranch2	1 Hour 7 Minutes 35 Seconds

3.5 CL2 With Authentication

Here we have added a MAC auth to our PSK based SSID just to demonstrate what happens during the authentication process.



Networks > Configuration - CL2

Security Level: Enterprise Personal Visitors Open

Key Management: WPA2-Personal

Passphrase Format: 8-63 chars

Passphrase: ••••••••

Retype: ••••••••

Advanced Settings

MAC Authentication:

Authentication Survivability:

Reauth Interval: 0 min

Denylisting:

Enforce DHCP:

Use IP for Calling Station ID:

Called Station ID Type: MAC Address

Called Station ID Include SSID:

Primary Server: clearpass

Secondary Server -- Select --

MAC Auth Delimiter Character:

MAC Auth Uppercase Support:

Auth Packet Delimiter Character:

Auth Packet Uppercase Support:

Accounting

Accounting: Use separate servers

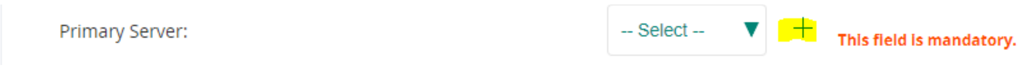
Accounting Server1: clearpass

Accounting Server2: -- Select --

Accounting Interval: 1 min

Fast Roaming

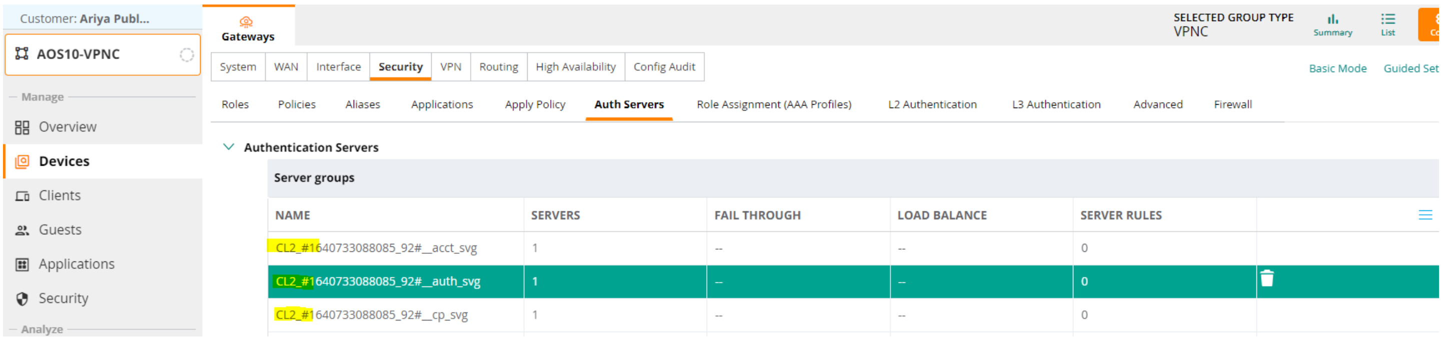
You should note that you need to create the authentication server from within the above workflow.



Primary Server: -- Select -- This field is mandatory.

You can also configure the auth servers in VPNCs and then select it from the above workflow.

Once you save the above modification and you have saved it then all that info gets sets sent to VPNCs.

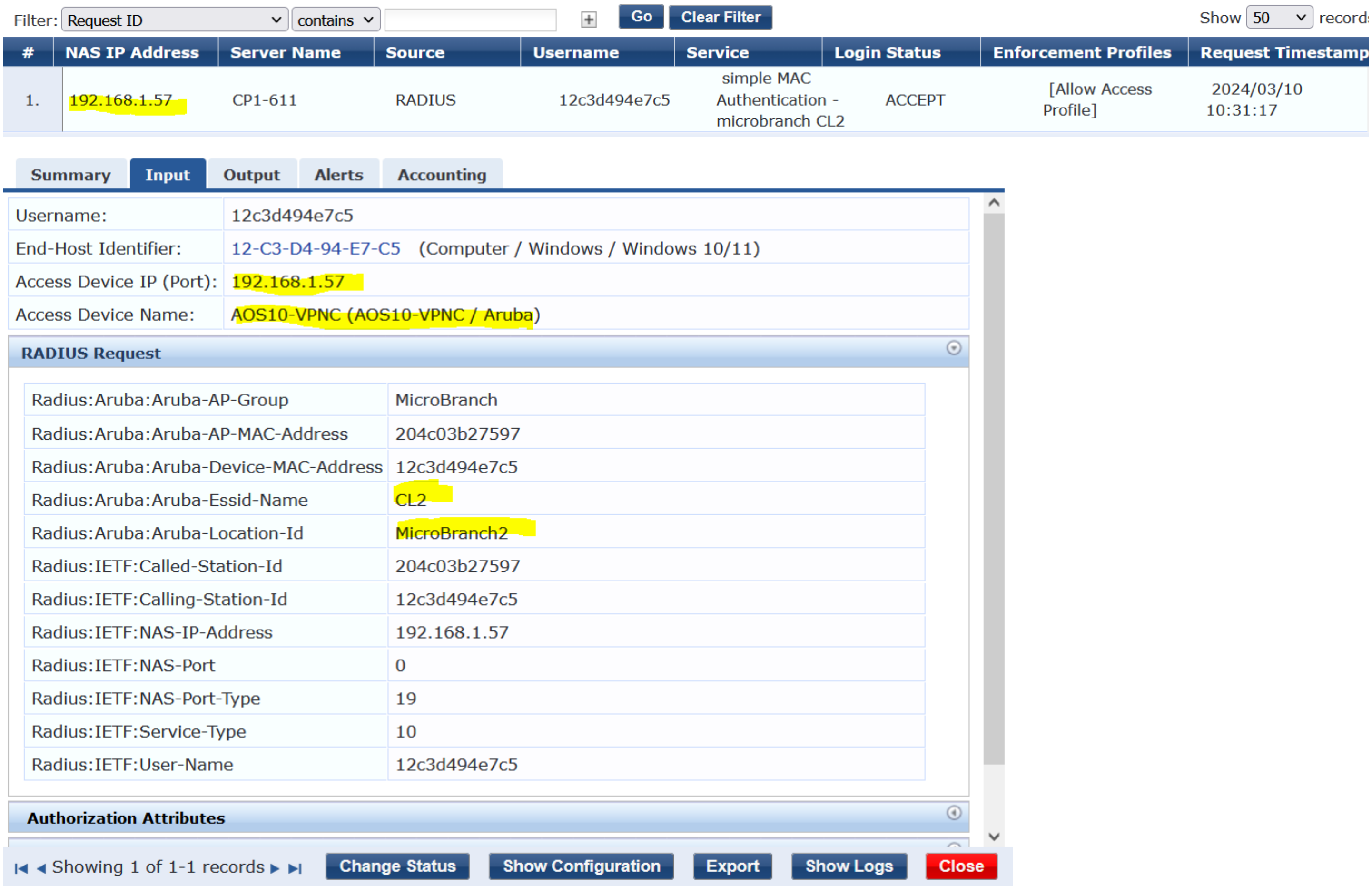


Authentication Servers

Server groups

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
CL2_#1640733088085_92#__acct_svg	1	--	--	0
CL2_#1640733088085_92#__auth_svg	1	--	--	0
CL2_#1640733088085_92#__cp_svg	1	--	--	0

Once that is done, we get a user to connect back to CL2 SSID from microbranch2.



#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.57	CP1-611	RADIUS	12c3d494e7c5	simple MAC Authentication - microbranch CL2	ACCEPT	[Allow Access Profile]	2024/03/10 10:31:17

Username:	12c3d494e7c5
End-Host Identifier:	12-C3-D4-94-E7-C5 (Computer / Windows / Windows 10/11)
Access Device IP (Port):	192.168.1.57
Access Device Name:	AOS10-VPNC (AOS10-VPNC / Aruba)

RADIUS Request

Radius:Aruba:Aruba-AP-Group	MicroBranch
Radius:Aruba:Aruba-AP-MAC-Address	204c03b27597
Radius:Aruba:Aruba-Device-MAC-Address	12c3d494e7c5
Radius:Aruba:Aruba-Essid-Name	CL2
Radius:Aruba:Aruba-Location-Id	MicroBranch2
Radius:IETF:Called-Station-Id	204c03b27597
Radius:IETF:Calling-Station-Id	12c3d494e7c5
Radius:IETF:NAS-IP-Address	192.168.1.57
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	10
Radius:IETF:User-Name	12c3d494e7c5

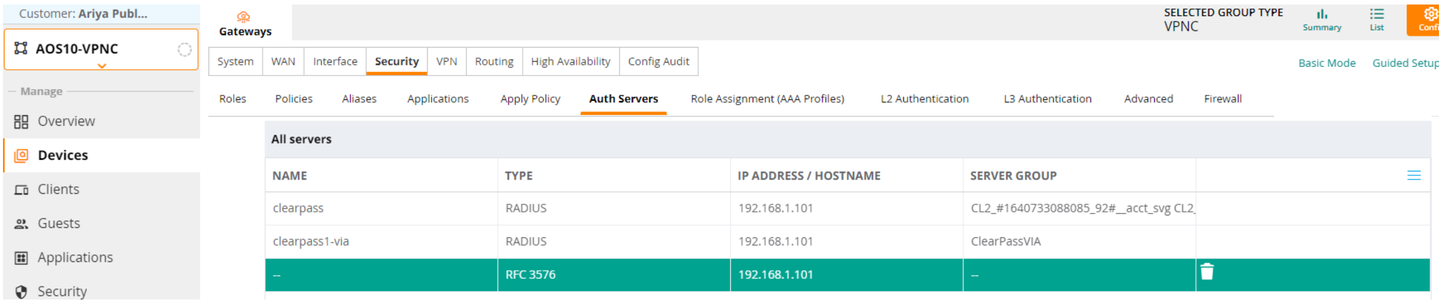
Authorization Attributes

Note that the AP is named as MicroBranch2 which was previously configured and that the SSID name “CL2” is proxied by the VPNC.

```
(Aruba7008_VPNC1) #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
Connected To      Roaming   Essid/Bssid/Phy              Profile                      Forward
mode   Type   Host Name   User Type
----------   ------------    ------      ----      ----------  ----   --------   -----
-------------  -------   ---------------            -------                  ------------
----  ---------  ---------
```

```
10.10.22.33  12:c3:d4:94:e7:c5  12c3d494e7c5  CL2        00:00:05     MAC              N/A
Wireless  CL2/20:4c:03:b2:75:97/N/A  CL2_#1640733088085_92#_  dtunnel
WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
(Aruba7008_VPNC1) #
```

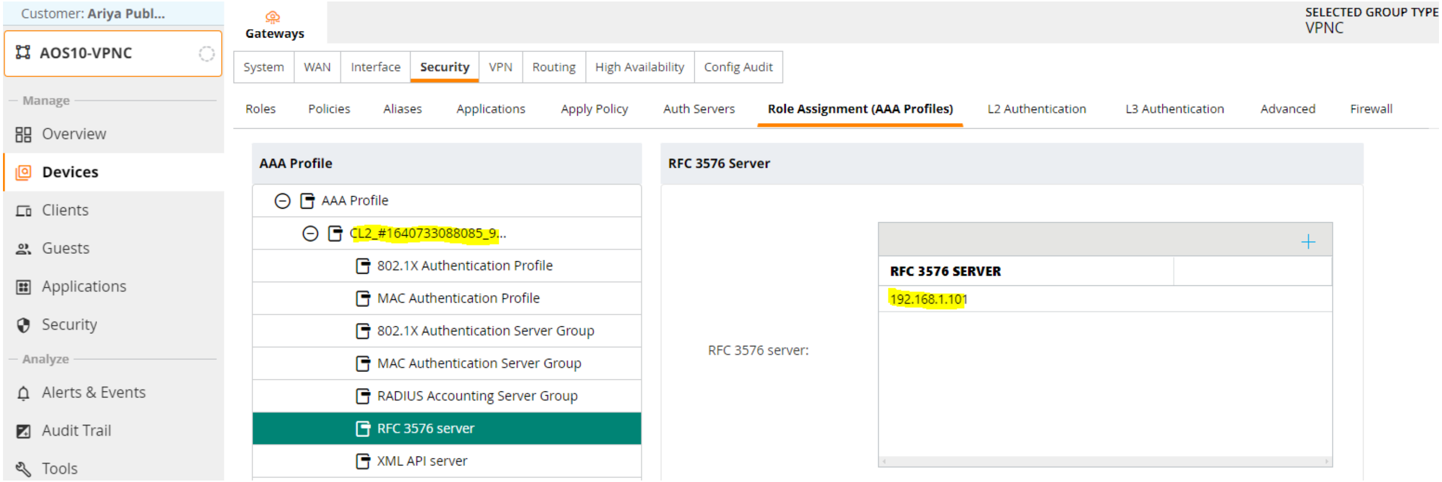
One thing that does not get pushed to VPNCs when you create the auth server from microbranch is the RFC3576 which you need to configure in VPNC group. This is used for CoA



All servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
clearpass	RADIUS	192.168.1.101	CL2_#1640733088085_92#__acct_svg CL2_
clearpass1-via	RADIUS	192.168.1.101	ClearPassVIA
--	RFC 3576	192.168.1.101	--

And then reference it in the role assignment for CL2 as shown below.



AAA Profile

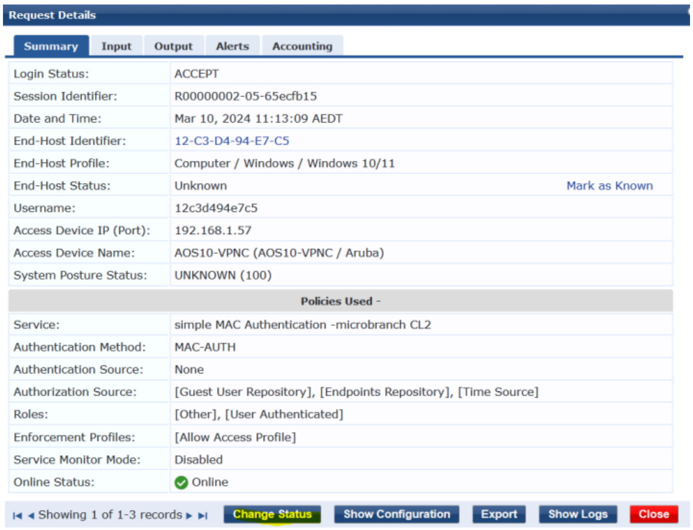
- AAA Profile
  - CL2_#1640733088085_9...
    - 802.1X Authentication Profile
    - MAC Authentication Profile
    - 802.1X Authentication Server Group
    - MAC Authentication Server Group
    - RADIUS Accounting Server Group
    - RFC 3576 server
    - XML API server

RFC 3576 Server

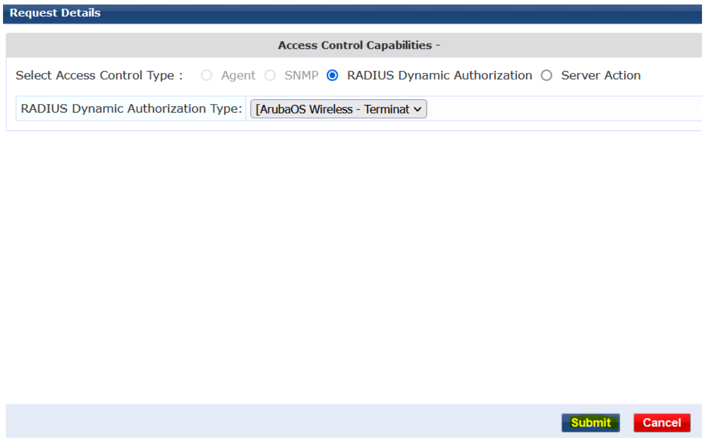
RFC 3576 server:

RFC 3576 SERVER
192.168.1.101

Now with this configuration in place, ClearPass can send CoA to VPNCs. This is one quick way to test it.


Request Details

Login Status:	ACCEPT
Session Identifier:	R00000002-05-65ecfb15
Date and Time:	Mar 10, 2024 11:13:09 AEDT
End-Host Identifier:	12-C3-D4-94-E7-C5
End-Host Profile:	Computer / Windows / Windows 10/11
End-Host Status:	Unknown Mark as Known
Username:	12c3d494e7c5
Access Device IP (Port):	192.168.1.57
Access Device Name:	AOS10-VPNC (AOS10-VPNC / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	simple MAC Authentication -microbranch CL2
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Online


Request Details

Access Control Capabilities -

Select Access Control Type : ○ Agent ○ SNMP ● RADIUS Dynamic Authorization ○ Server Action

RADIUS Dynamic Authorization Type: [ArubaOS Wireless - Terminat ⌄]

This is the end of this part.