aruba
a Hewlett Packard Enterprise company

POLICY BASED ROUTING IN THE BRANCH – ARUBAOS 8.X

11:00 GMT | 12:00 CET | 13:00 GST
OCT 30th, 2018

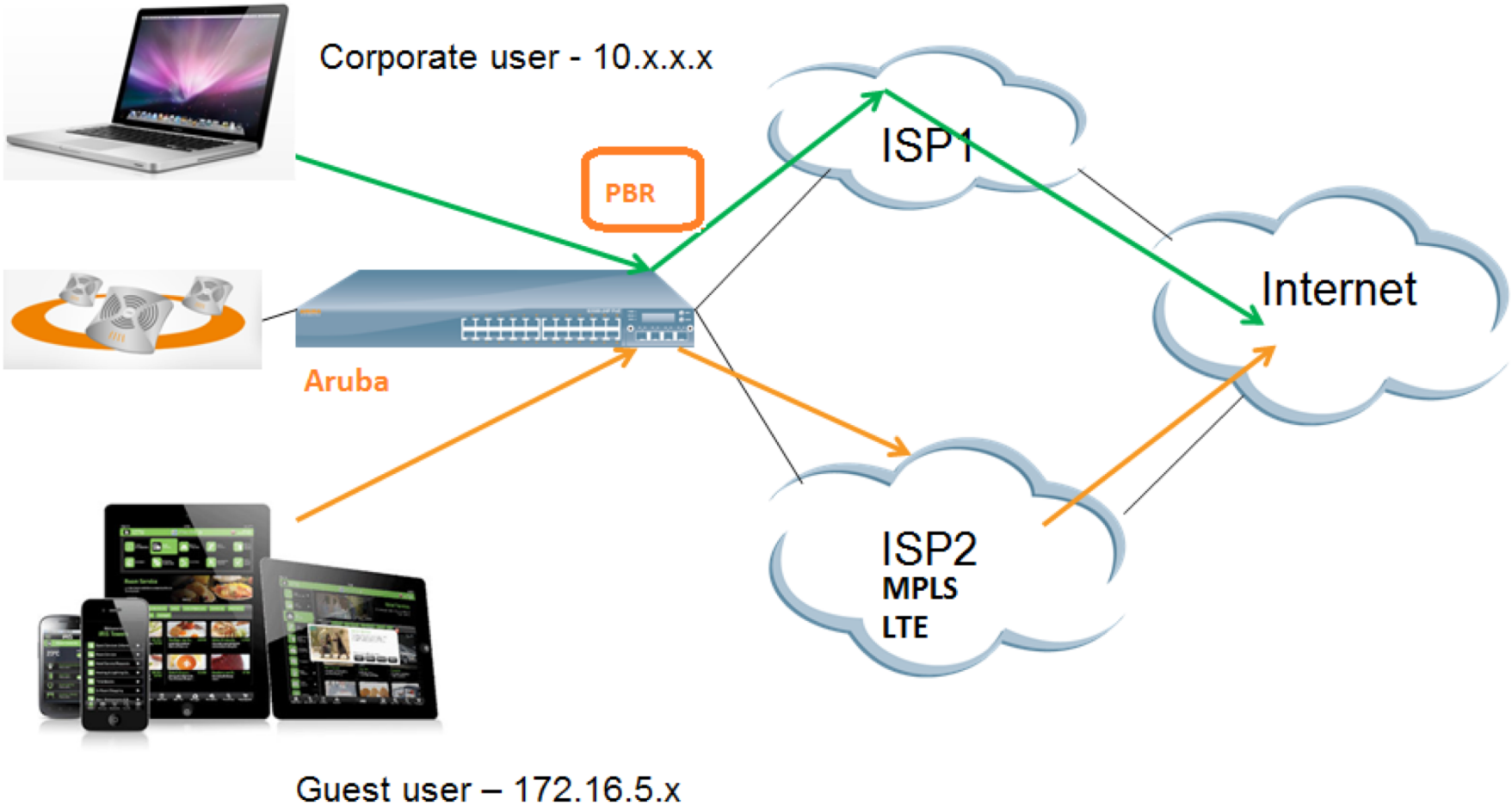
Presenter: Raj Shekhar

AIRHEADS COMMUNITY

Agenda

- **What's Policy Based Routing?**
- **Benefits of PBR**
- **Aruba's implementation of PBR**
- **PBR in the SD-Branch Controller**
- **Troubleshooting**

What is PBR?


Corporate user - 10.x.x.x
PBR
ISP1
Internet
Aruba
ISP2
MPLS
LTE
Guest user – 172.16.5.x

Benifits

- **Traditional routing is based on destination IP.**
- **In PBR Traffic shall be routed based on**
  - Source
  - Destination
  - L4-L7
  - Application or Application Category (AppRF)

PBR can make use of all available uplinks by splitting traffic among them.

- **Elements of PBR**
  - PBR Nexthop
    - Nexthop-List
    - L3 GRE Tunnel / Tunnel Group
    - Site-to-Site VPN Tunnel
    - Forward (regular routing)
  - Route ACL
  - Attach points
    - User-Role
    - L3 VLAN

Configuration

- **Define PBR Nexthop**

  - Nexthop-List

```
(BoC) (config) #ip nexthop-list nhlist
(BoC) (config-nexthop-list)#?
 ip                      Nexthop IP
 no                      Delete Command
 preemptive-failover     Enable/Disable preemptive failover

(BoC) (config-nexthop-list)#ip ?
 A.B.C.D                 Nexthop IP address
 dhcp                    Gateway IP through DHCP
```

Next Hop

- L3 GRE Tunnel / Tunnel-Group
  Existing L3 GRE Tunnel redirect

- Site-to-Site VPN Tunnel
  Traffic can be encrypted and send it across

- Regular Forwarding
  Traffic can be forwarded as usual

- **Define Route ACL to redirect matching traffic to PBR Nexthop**

```
(BoC) (config) #ip access-list route pbr                    ← Local command
(BoC) (config-route-pbr)#any network 10.0.0.0 255.0.0.0 any route ?
ipsec-map               Forward packets to ipsec tunnel
next-hop-list           Forward packets to nexthop list
tunnel                  Forward packets to L3 tunnel
tunnel-group            Forward packets to tunnel group

(BoC) (config-route-pbr)#any network 10.0.0.0 255.0.0.0 any forward ?
position                Filter position. Default is last. 1 is first.
<cr>
```

Attach route ACL to User-Role / L3 VLAN

```
(BoC) (config) #routing-policy-map role authenticated access-list pbr   ← Attaching route ACL to User-Role (Local Command)

(BoC) (config) #interface vlan 101                          ← Attaching route ACL to VLAN (Local Command)
(BoC) (config-subif)#ip access-group pbr in
```

Branch > Smart Config

Profile Management | System | Networking | Routing | VPN | WAN | Summary | Whitelist

Profile A7030

Routing | **PBR**

Nexthop Configuation

Nexthop-list Name	Nexthop-list IPs	Preemptive Failover	Action
nhlist	172.20.42.216 (128)	Enabled	Edit Delete

Add

PBR Rules

Route ACL name pbr Delete

IP Version	Source	Destination	Service/Application	Action
IPv4	any	network 172.21.0.0 255.255.0.0	any	route next-hop-list "nhlist"

Add Delete

Target

PBR Rule Name	Type	Target	Action
pbr	role	authenticated	Edit Delete

Add

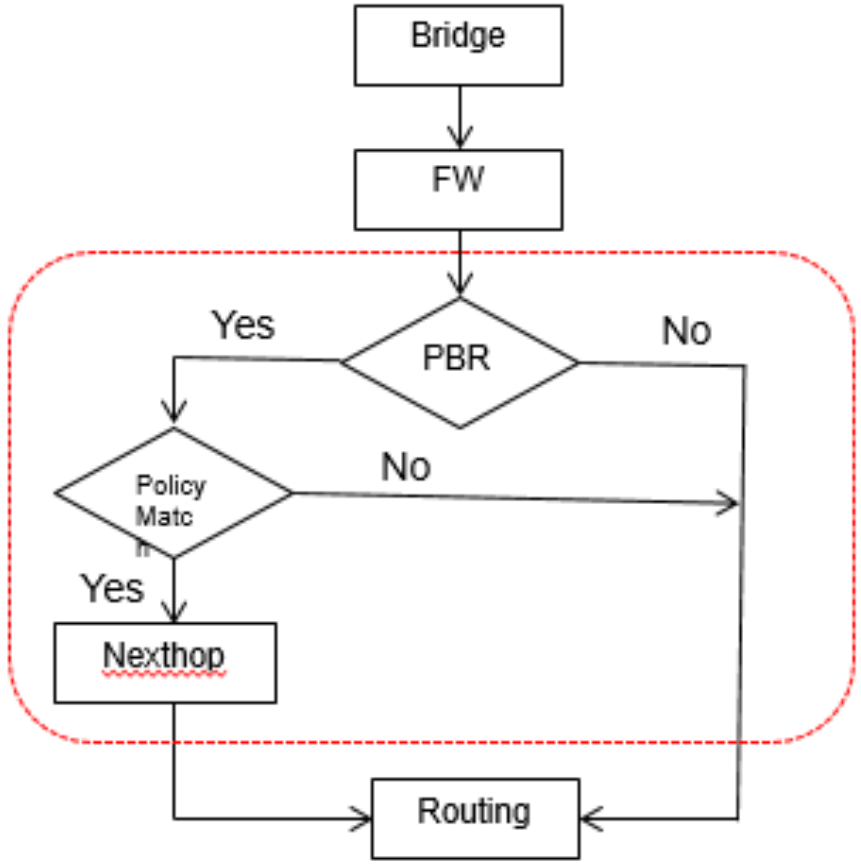
Apply

Commands View Commands

Working

- Once NH-List is attached to Route ACL, active IP for NH-List is selected based on reachability and priority and programmed in Datapath
- Reachability check is done periodically and Active IP is refreshed, if there is any change in reachability or priority.
- Whenever user traffic hits the Route ACL, traffic will be sent to appropriate PBR Nexthop

PBR..



Platform Support

- Supported on 7xxx & MMC platforms
- Supported on MM, MD & Branch Controllers
- PEFNG License
- L4-L7 Based routing requires DPI

```
(BoC) #show ip health-check

IP Health-check Entries

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

Probe IP       Src Interface  State  Probe-Profile  Avg RTT(in ms)

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

172.20.28.238  vlan 4094      Up     default        0

172.20.42.216  --             Up     default        0

(BoC) #show ip nexthop-list

Nexthop-List Entries

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

Nexthop-list Name  Nexthop-list Id  Pr...ive Failover  Active IP      Nexthop IPs(Priority)

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

nhlist             0x4401           Enabled             172.20.42.216   172.20.42.216(128)

(BoC) #show datapath nexthop-list

Datapath Nexthop Table Entries

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

SOS Dest  Active IP      NhIdx  NhVer

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

0x4401    172.20.42.216  1      0x2
```

NH-List ID is populated once it is referenced in Route ACL

```
(7005-236) #show datapath session verbose

Datapath Session Table Entries

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

Flags: F - fast age, S - src NAT, N - dest NAT

       D - deny, R - redirect, Y - no syn

       H - high prio, P - set prio, T - set ToS

       C - client, M - mirror, V - VOIP

       Q - Real-Time Quality analysis

       I - Deep inspect, U - Locally destined

       E - Media Deep Inspect, G - media signal

       r - Route Nexthop

       A - Application Firewall Inspect

Session Index, Route/Cache Index, Agg. Version Number[SIDX SRTI SRCI SRTRCV]

Source IP       Destination IP  Prot SPort DPort  Cntr    Prio ToS Age Destination TAge Packets    Bytes      SIDX     SRTI SRCI     SRTRCV
UsrIdx   UsrVer   AclVer   NhIdx    NhVer    Flags
--------------- --------------- ---- ----- ----- -------- ---- --- --- ----------- ---- ---------  --------- -------- ---- -------- --------
-------- -------- -------- -------- -------- ---------------

172.21.101.2    192.168.5.2     17   63    63     0/0      0    0   14  nexthop 1   e4   0          0          4010     0    0        0
0        0        0        0        0        F

192.168.5.2     172.21.101.2    17   63    63     0/0      0    0   0   nexthop 1   e4   1366796    1342193672 401d     2    9        12
a        21       924      1        2        FCr
```

Key Points to implement

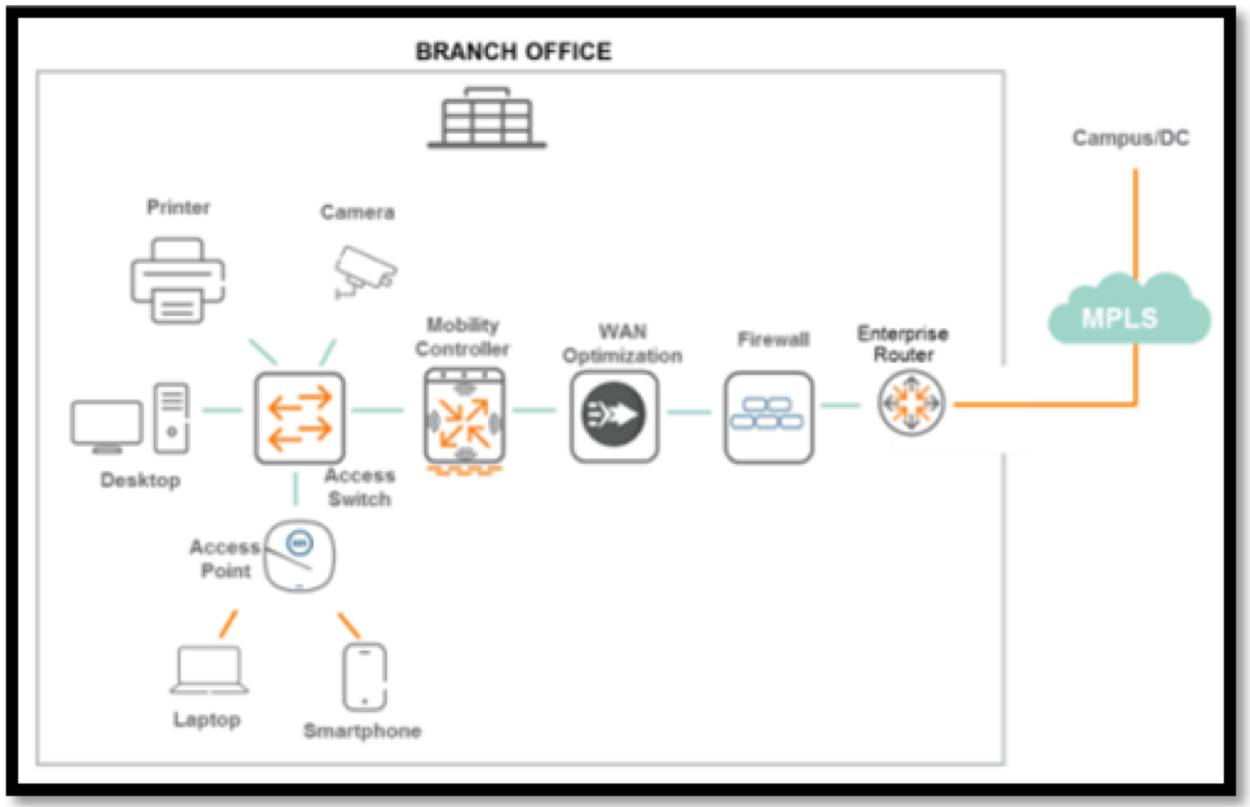
- Next hop IP address must be same as that of the L3 router that is adjacent/directly connected.
- PBR would take precedence over IPsec routing.
- Stateless ACLs have an implicit deny at the end of the ACL. So a permit statement without nexthop/redirect option must be configured to allow traffic that needs to be permitted, but not subjected to policy routing.
- ICMP protocol must be allowed for Health Check Manager to detect next Hop.

SD-WAN Solution

- SD-WAN is an acronym for software-defined networking in a wide area network (WAN).
- An SD-WAN simplifies the management and operation of a WAN by decoupling (separating) the networking hardware from its control mechanism.
- A key application of an SD-WAN is to allow companies to build higher-performance WANs using lower-cost and commercially available Internet access, enabling businesses to partially or wholly replace more expensive private WAN connection technologies such as MPLS.

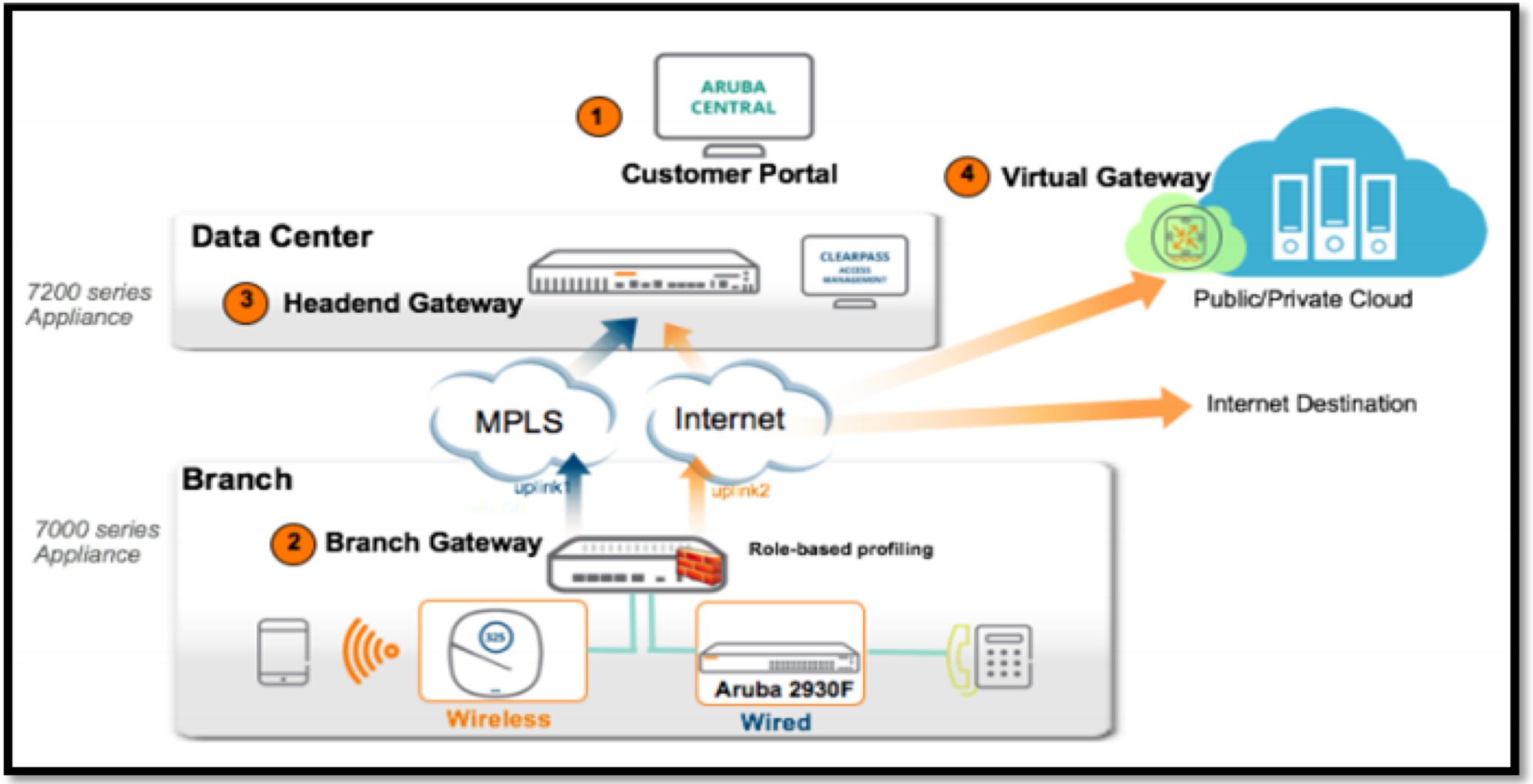
SD-Branch

- However, while SD-WAN solves a real IT problem, it only addresses one of the problems faced when dealing with distributed locations. Organizations often roll out and operate distributed, heterogeneous networks with small, centralized teams. These distributed networks offer many services besides just WAN connectivity. **Branch networks need wired and wireless local area network (LAN), security and policy enforcement, and of course, WAN interconnect.**
- The software defined branch extends the concepts around SD-WAN to all elements in the branch, **delivering a full-stack solution that addresses wired and wireless LAN, security and policy enforcement, and, of course, WAN connectivity.**


BRANCH OFFICE
Printer
Camera
Mobility Controller
WAN Optimization
Firewall
Enterprise Router
Campus/DC
MPLS
Desktop
Access Switch
Access Point
Laptop
Smartphone

What makes the SD-WAN (Key Elements)

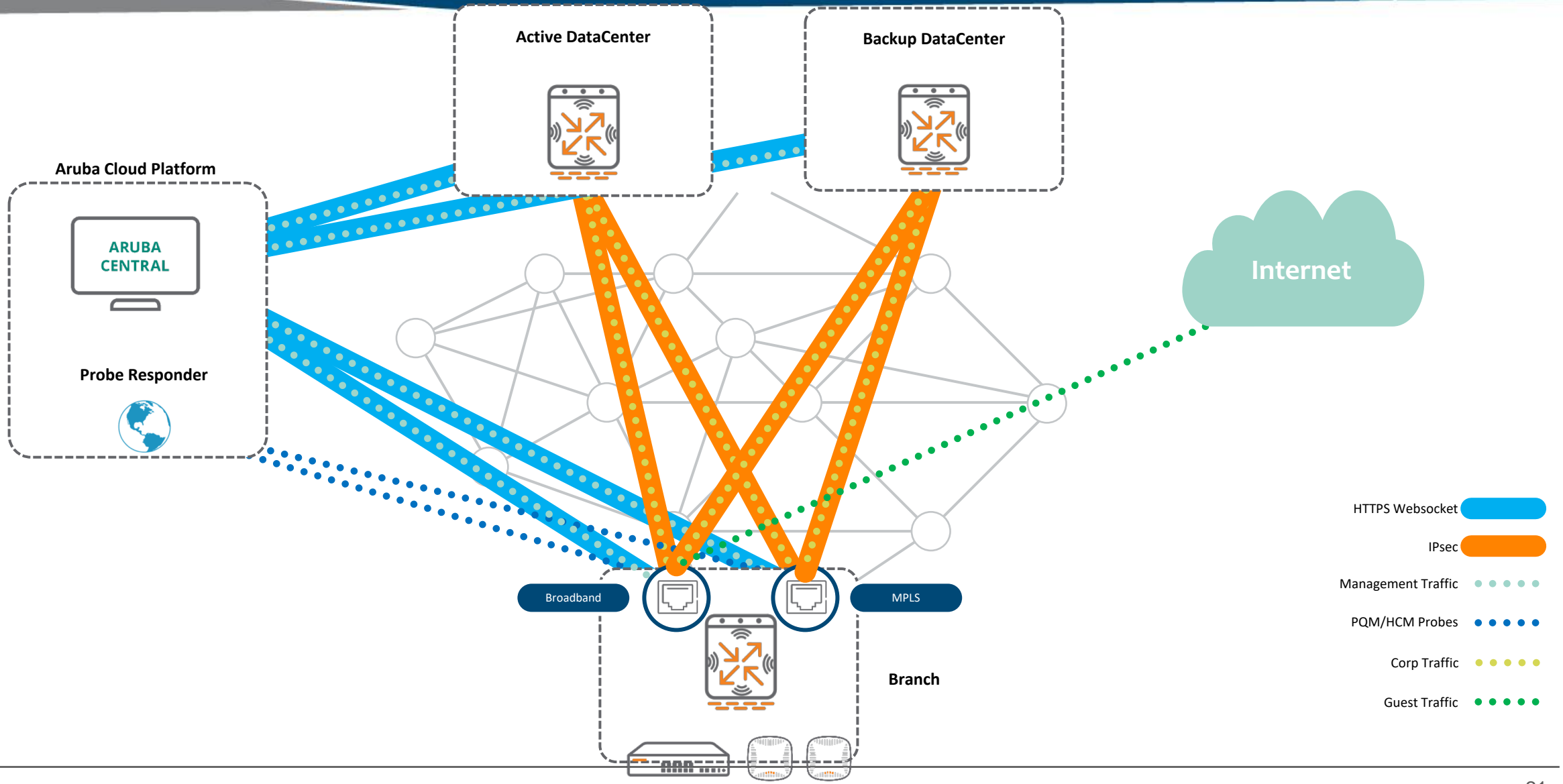
- **Cloud Management –** *Aruba Central*, Aruba's cloud management service, offers a unified point of management and control for all Aruba APs, switches, Branch Gateways, Headend Gateways, and Cloud Gateways.
- **Branch Gateway –** is the appliance at the branch that connects to WAN uplinks and participates as an end-point in the SD-WAN overlay fabric.The branch gateway is a policy enforcement point for wired, wireless, security and WAN policies (including routing).
- **Branch LAN/WLAN –** *Aruba switches and APs* provide wired and wireless networking for users at branch sites.
- **Headend Gateway –** The Headend Gateway acts as a VPN concentrator (VPNC) and runs at the head-end in hub-and-spoke and multi hub-and-spoke topologies; terminating IPsec VPN tunnels and participating in the data center and campus routing scheme.


1
ARUBA CENTRAL
Customer Portal
4
Virtual Gateway
Public/Private Cloud
Data Center
7200 series Appliance
3
Headend Gateway
CLEARPASS
MPLS
Internet
Internet Destination
Branch
7000 series Appliance
uplink1
uplink2
2
Branch Gateway
Role-based profiling
Aruba 2930F
Wireless
Wired

PBR on the Branch controller

- With Aruba Software Defined (SD) Branch solution seeks to simplify WAN connectivity by setting up an encrypted overlay tunnel over the WAN. Hence, tools like PBR becomes more and more critical.
- Its starts after branch is allowed (whitelisted) on Central.
- Once a branch gateway goes through the provisioning process (ideally, ZTP) and has received it's configuration from Central, the branch gateway will attempt to establish IPSec tunnels over every interface to the different hubs we may have. The process is secured by using TPM certificates present in every device.
- The branch gateways will share their subnets with the hubs as part of the negotiation of the IKE tunnels.

SD-Branch Architecture Overview

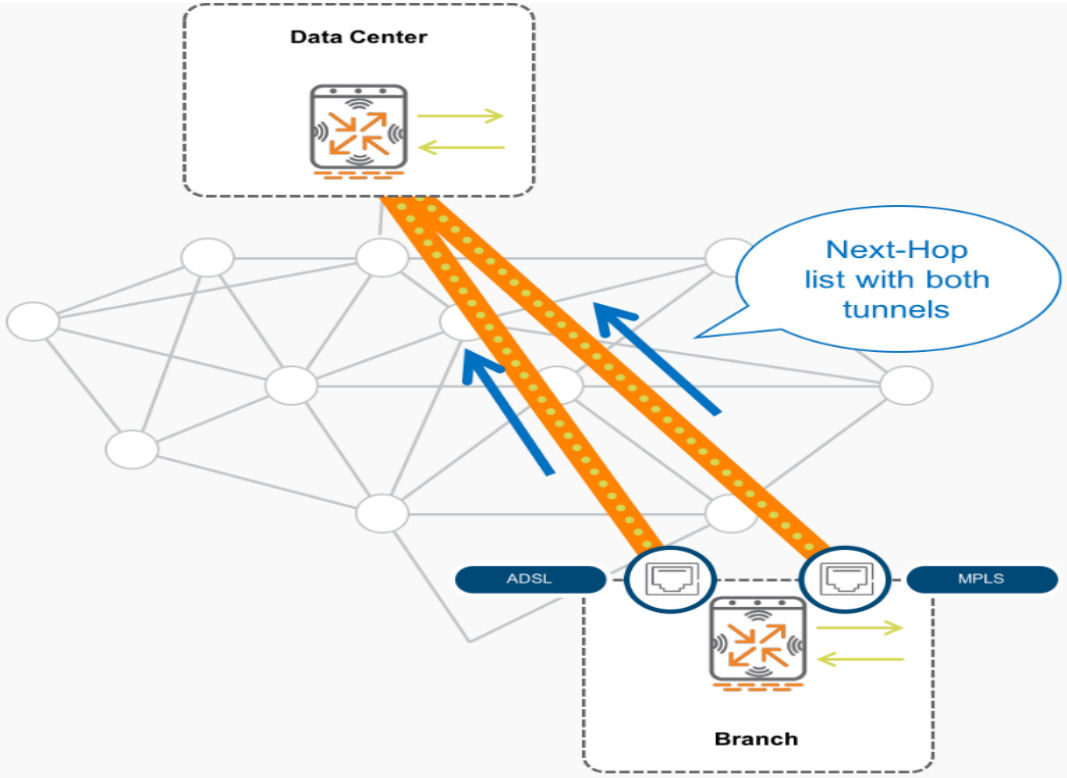


Multiple Links using PBR

There will be situations where we will want all or a subset of devices to be routed in a different way. Some very common use-cases are to force a subset of devices to always go through the DataCenter (i.e., full-tunnel mode) or to always break-out locally. This can be easily handled in Aruba's SD-WAN solution by using PBR (which can be applied on a per-VLAN or per-Role basis).

Only for reference – Config is GUI-based

```
ip nexthop-list full-tunnel
  ipsec-map vpnc1-adsl priority 100
  ipsec-map vpnc1-mpls priority 100
  ipsec-map vpnc2-link1 priority 50
  ipsec-map vpnc2-link2 priority 50
!
Ip access-list route full-tunnel
  alias local-net alias local-net any forward
  any any any route next-hop-list full-tunnel
!
User-role POS
  access-list session POS
  access-list route full-tunnel
```



Full-Tunnel-LB.png - more info

aruba | Central

CURRENT APP
GATEWAY MANAGEMENT

Search Current App
Find devices, clients and networks

Interfaces
Set Interfaces, DHCP, NAT parameters

WAN
Set uplink, path steering policies

VPN
Set IPSec encryption parameters

Routing
Set routing parameters

Security
Set advanced security parameters

System
Manage advanced system settings

High Availability
Set redundancy parameters

Configuration Audit
Review Configuration status

FILTER GATEWAY MANAGEMENT
BRANCH-7008 (2 Total Devices | 0 Down APs | 0 Down SWITCHES | 0 Down

IP Routes | Policy-Based Routing | **NextHop Configuration** | OSPF

NextHop-list name: full-tunnel

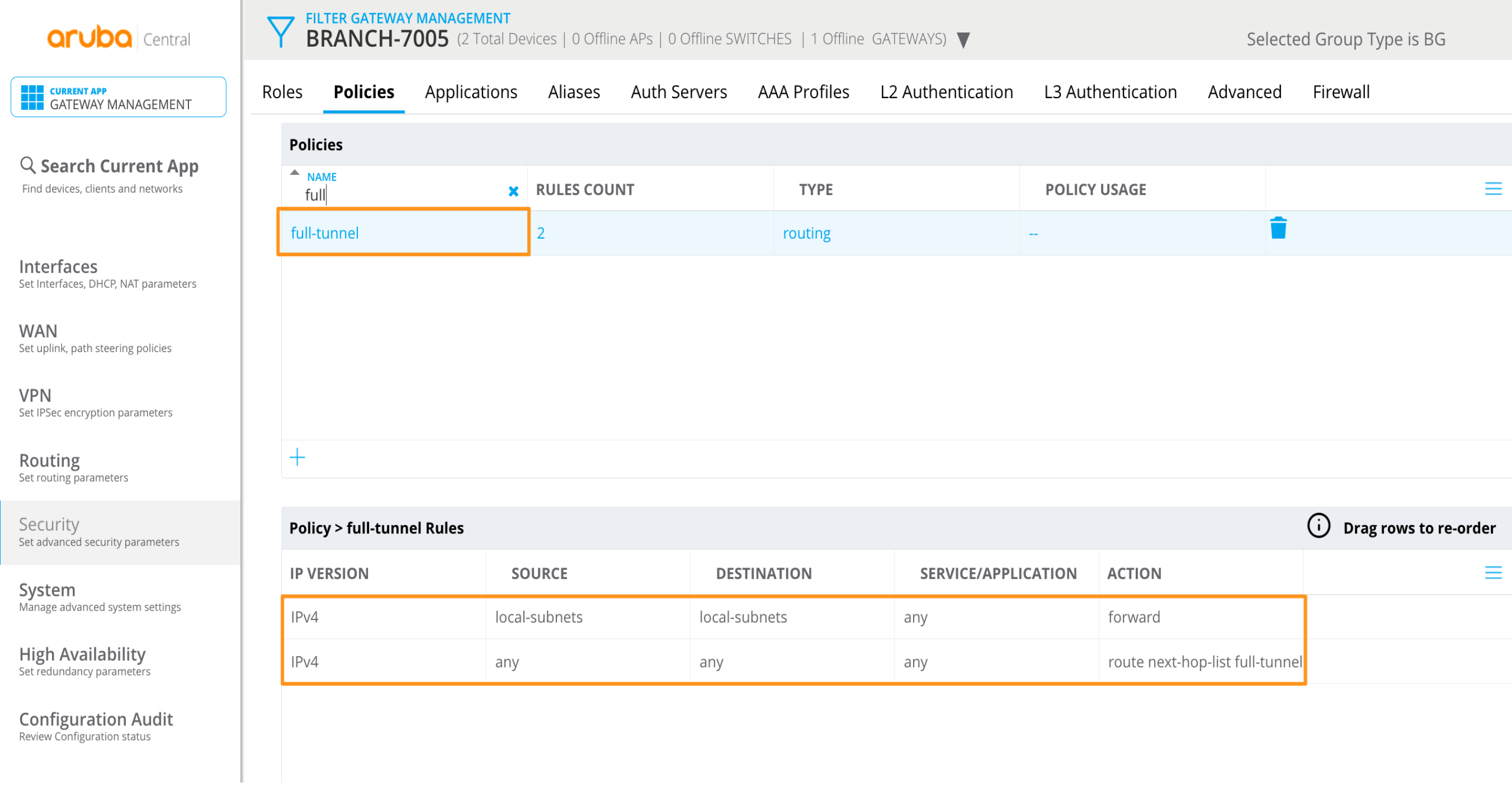
NextHop IP/DHCP:

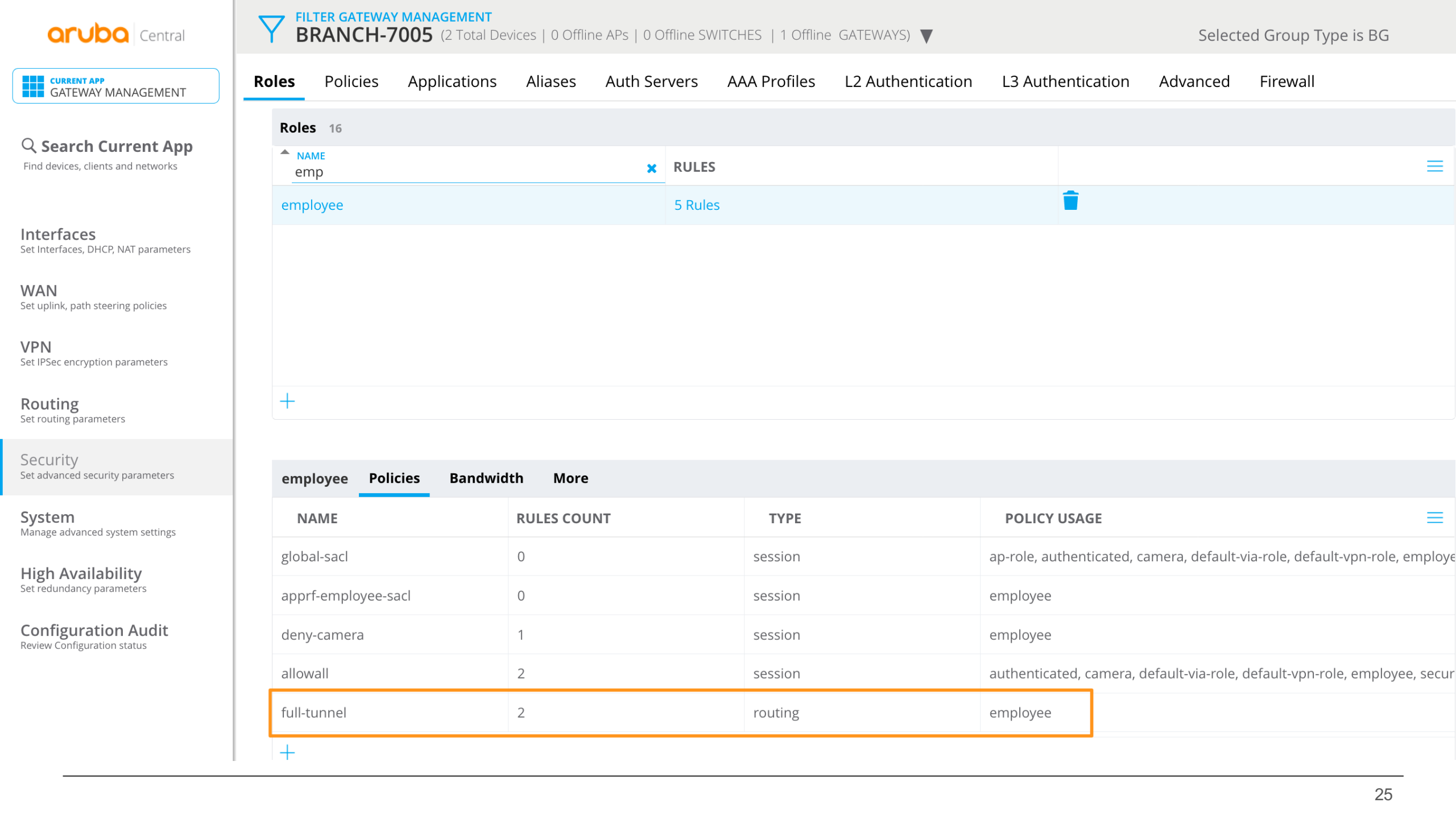
IP/DHCP	PRIORITY

No data to display

IPsec name map:

IPSEC MAP NAME	PRIORITY
data-vpnc-00:1a:1e:03:72:a0-euskaltel_inet	100
data-vpnc-00:1a:1e:03:72:a0-telefonica_mpls	100


aruba Central
CURRENT APP
GATEWAY MANAGEMENT
Search Current App
Find devices, clients and networks
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Set redundancy parameters
Configuration Audit
Review Configuration status
FILTER GATEWAY MANAGEMENT
BRANCH-7005 (2 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 1 Offline GATEWAYS)
Selected Group Type is BG
Roles
Policies
Applications
Aliases
Auth Servers
AAA Profiles
L2 Authentication
L3 Authentication
Advanced
Firewall
Policies
NAME
full
RULES COUNT
TYPE
POLICY USAGE
full-tunnel
2
routing
--
Policy > full-tunnel Rules
Drag rows to re-order
IP VERSION
SOURCE
DESTINATION
SERVICE/APPLICATION
ACTION
IPv4
local-subnets
local-subnets
any
forward
IPv4
any
any
any
route next-hop-list full-tunnel


aruba Central
CURRENT APP
GATEWAY MANAGEMENT
Search Current App
Find devices, clients and networks
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Set redundancy parameters
Configuration Audit
Review Configuration status
FILTER GATEWAY MANAGEMENT
BRANCH-7005 (2 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 1 Offline GATEWAYS)
Selected Group Type is BG
Roles
Policies
Applications
Aliases
Auth Servers
AAA Profiles
L2 Authentication
L3 Authentication
Advanced
Firewall
Roles 16
NAME
emp
RULES
employee
5 Rules
employee
Policies
Bandwidth
More
NAME
RULES COUNT
TYPE
POLICY USAGE
global-sacl
0
session
ap-role, authenticated, camera, default-via-role, default-vpn-role, employe
apprf-employee-sacl
0
session
employee
deny-camera
1
session
employee
allowall
2
session
authenticated, camera, default-via-role, default-vpn-role, employee, secur
full-tunnel
2
routing
employee

What it needs?

In the branches

- Branch Gateway: In this case, the Aruba 7000 series will only act as a branch gateway, NOT as WLAN controller.
- ArubaOS-Switch –
- Instant Access Points

In the datacenters

Headend Gateway - Both the Aruba 7000 series as well as the Aruba 7200 series can act as VPNCs. Once again, they will only act as VPN concentrator (for SD-WAN, VIA and IAP-VPN), but NOT as WLAN controller.

Aruba Central for management and control

show ip nexthop-list [Name] [detail] – List of NH-List configured with Active IP and SOS Dest ID etc

show ip health-check – Reachability status of each IP in NH-List

show ip probe – Health check is done based on probe configuration

show datapath nexthop-list – List of NH-List with SOS Dest ID for each

show crypto ipsec ipsec-map-id - Displays SOS Dest ID for each S2S VPN tunnel

show route-access-list – Lists route ACLs and its user-role mapping

show rights <> – Lists of session ACLs and route ACL attached to a given user-role

show datapath user - Displays the Session ACL and Route ACL of the user

show datapath acl <id> - Displays the session/route ACL and Hit count

show datapath vlan - Displays the route ACL configured on VLAN

Show acl hits – Displays hit count for Session and Route ACL

show datapath session verbose - Displays the session table with PBR specific fields like nhIdx, nhVer

logging level debugging system process fpapps – Logs nexthop failover related info

logging level debugging system process hcm – Logs Health check ping probe related info

aruba
a Hewlett Packard
Enterprise company

THANK YOU !