

# Aruba SD-Branch

John Schaap  
[john.schaap@hpe.com](mailto:john.schaap@hpe.com)

26 October 2018

# Challenges with Current Distributed Architectures

## LAN Side Challenges

- Complexity caused by increasing number of devices, VLAN proliferation
- End points going mobile
- Poor visibility into clients/devices
- Lack of authentication of clients/devices
- Lack of common policy for users connecting to network via wired or wireless



## WAN Side Challenges

- Limited capacity & long setup times for MPLS
- Lack of control and visibility into WAN traffic
- Complex management of the WAN and routing policy
- More SaaS traffic (O365, Box, SFDC, ...) directed over Internet.
- Lack security measures and control to safeguard the network

## Operational Challenges

- Multiple management platforms, Multiple operating models, Multiple vendors, Policy is distributed

# Goal: Solve the Branch problem, not just the WAN



## Simple (at Enterprise scale)

Drive simplicity and fewer boxes in branch solution



## Transport Independency

Own your WAN policy

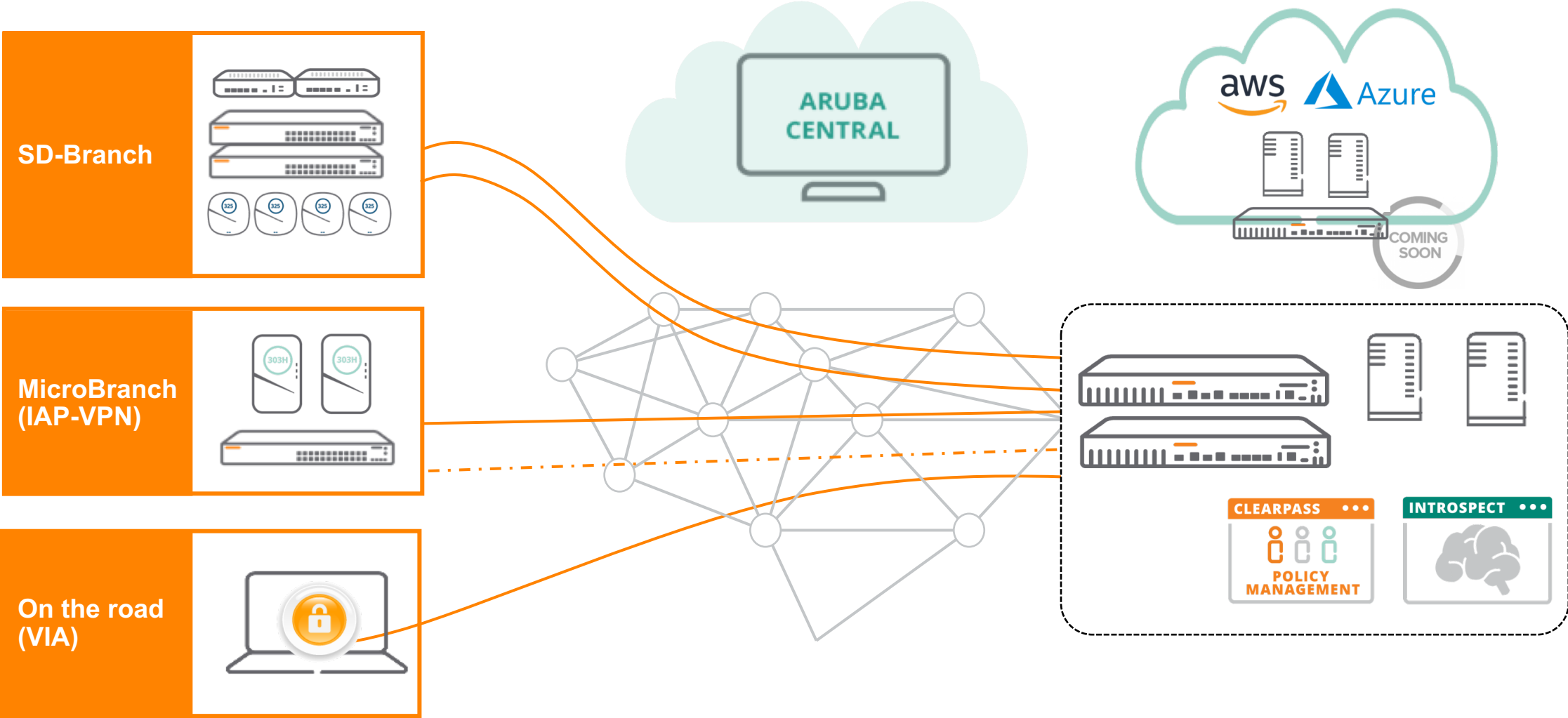


## Common Policy and Management

for Wired, WLAN and WAN



# Aruba Distributed Architectures





# Goal: Solve the Branch problem, not just the WAN



## Simple (at Enterprise scale)

Drive simplicity and fewer boxes in branch solution



## Transport Independency

Own your WAN policy



## Common Policy and Management

for Wired, WLAN and WAN

# Software driven branch networks

## CLOUD MANAGEMENT



## NETWORK INFRASTRUCTURE



INSTANT ACCESS POINTS



ARUBA-OS SWITCHES



BRANCH GATEWAY

## SERVICES

GUEST WI-FI



NETWORK ANALYTICS



PRESENCE ANALYTICS



SD-WAN

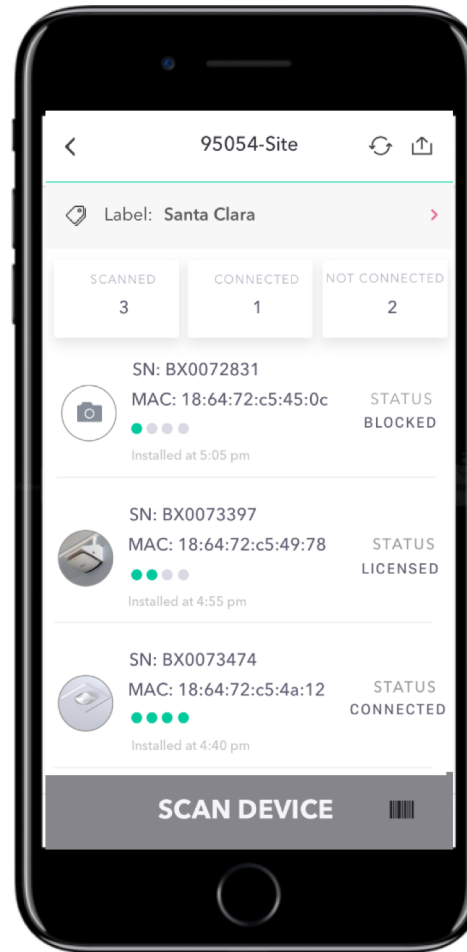
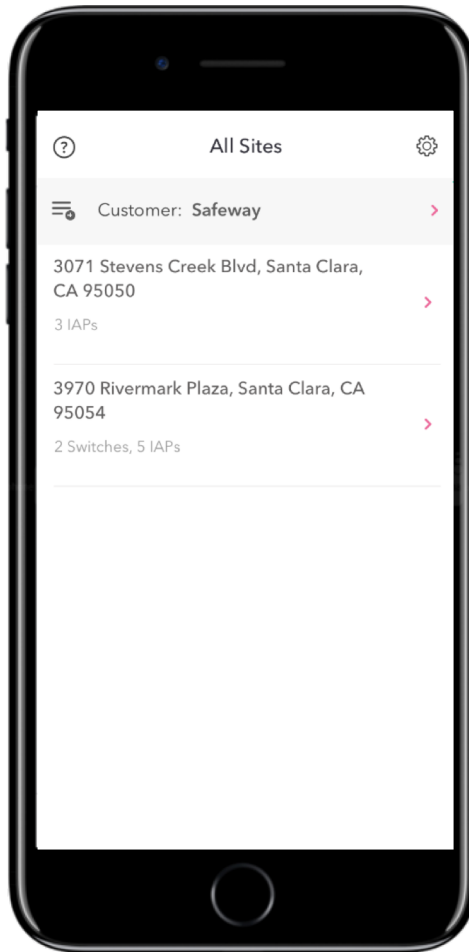
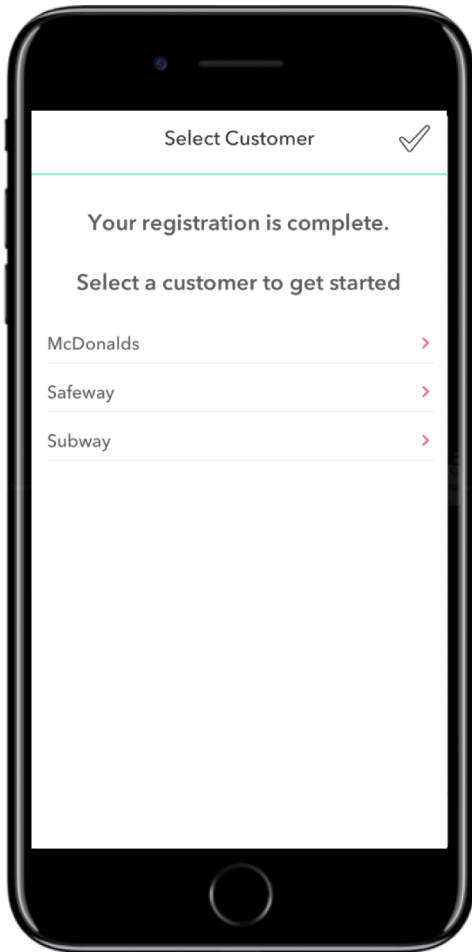


SECURITY



# Simple Onboarding

Demo



- Installer selects site and scans devices
- Installer gets status of device on boarding
- Admin gains central visibility into onboarding
- Site awareness seeded into onboarding
- Configuration group pushed as part of onboarding

# Hierarchical Management

## Walkthrough

The screenshot displays the Aruba Central Gateway Management interface. On the left, a sidebar contains navigation links: **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), and **High Availability** (Set redundancy parameters). The main content area is titled **FILTER GATEWAY MANAGEMENT home-7008** (1 Total Devices | 0 Down AP). Below this is a **REFINE FILTER LISTING** search bar with the text 'sam'. A section titled **GROUPS All Groups (11)** shows **GROUP-sam** and **GROUP-sam-7008**. The **GATEWAYS** section lists **GROUP-sam** with sub-items **desk-7005**, **GROUP-sam-7008** (highlighted with an orange box), and **JW634A-20:4C:03:...**. Below the gateways is a table with columns **NAME**, **MEMBERS**, and **PROTOCOL**. The table contains four rows of gateway information, all with 'Enabled' status and 'Not-defined' protocol. A **Port Channel** section is visible at the bottom.

NAME	MEMBERS	PROTOCOL
GE-0/0/2	Enabled	Not-defined
GE-0/0/3	Enabled	Not-defined
GE-0/0/4	Enabled	Not-defined
GE-0/0/5	Enabled	Not-defined

1

Apply configurations on a group basis

2

Overrides on a per-device basis (bulk-edit possible)

3

Monitoring based on sites/labels



# Making branch security scalable...

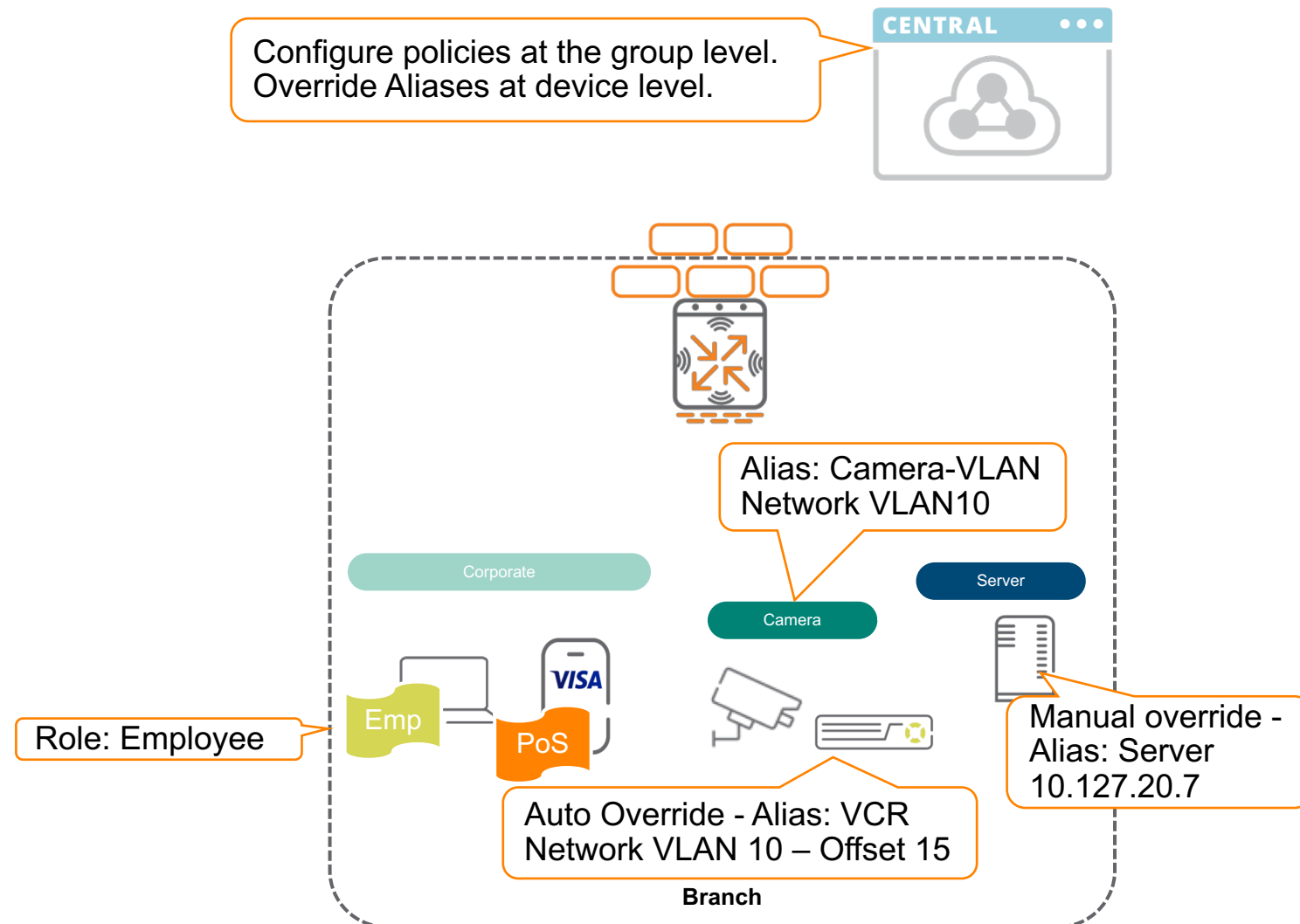
## Group based security policies

- 1 Manual override:  
Set alias at group, define it at device
- 2 Automatic override:  
Set VLAN + offset (or the whole VLAN)
- 3 Role based policies:  
From role A to role B...



Security Core

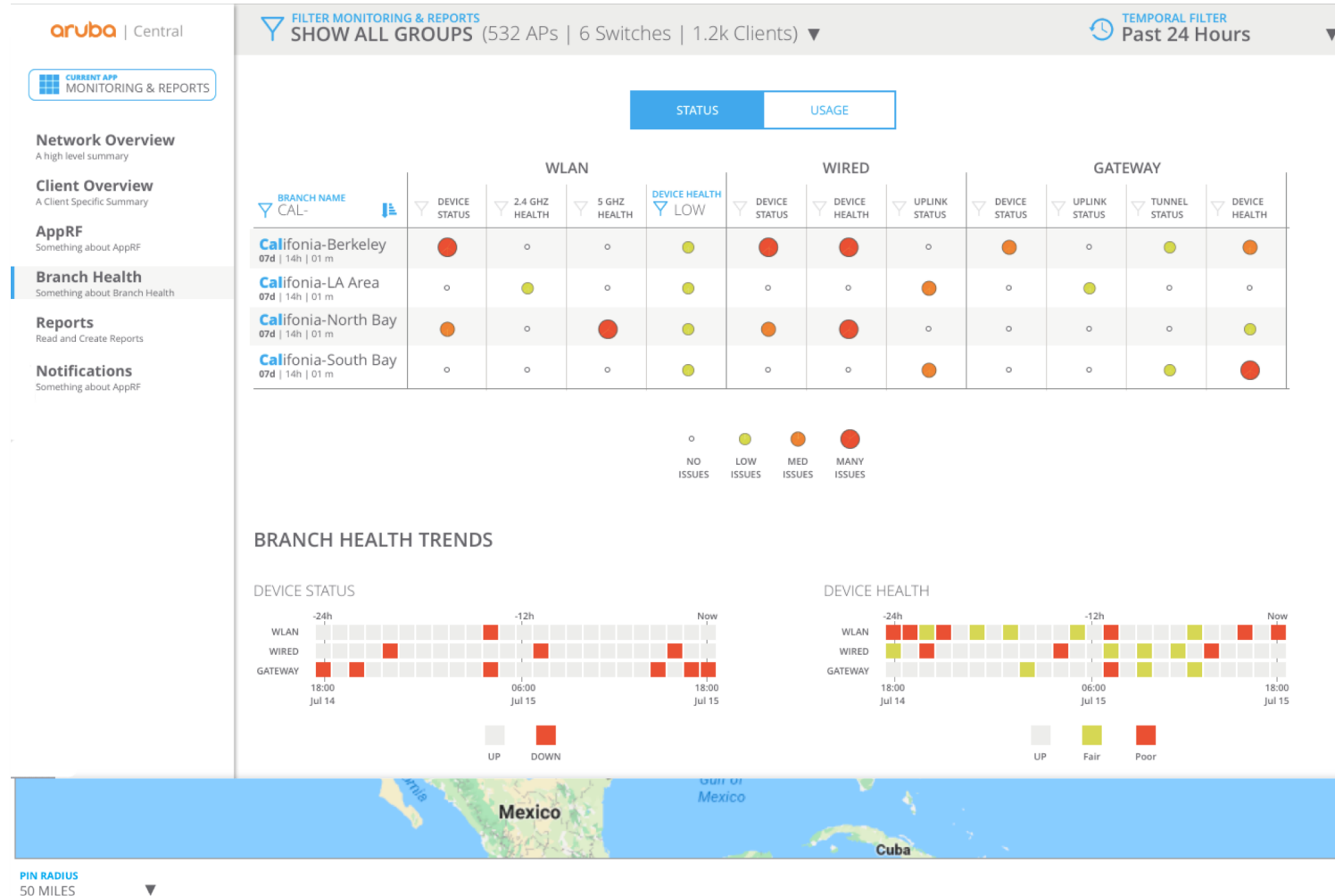
## Walkthrough



# Health Dashboard

## Walkthrough

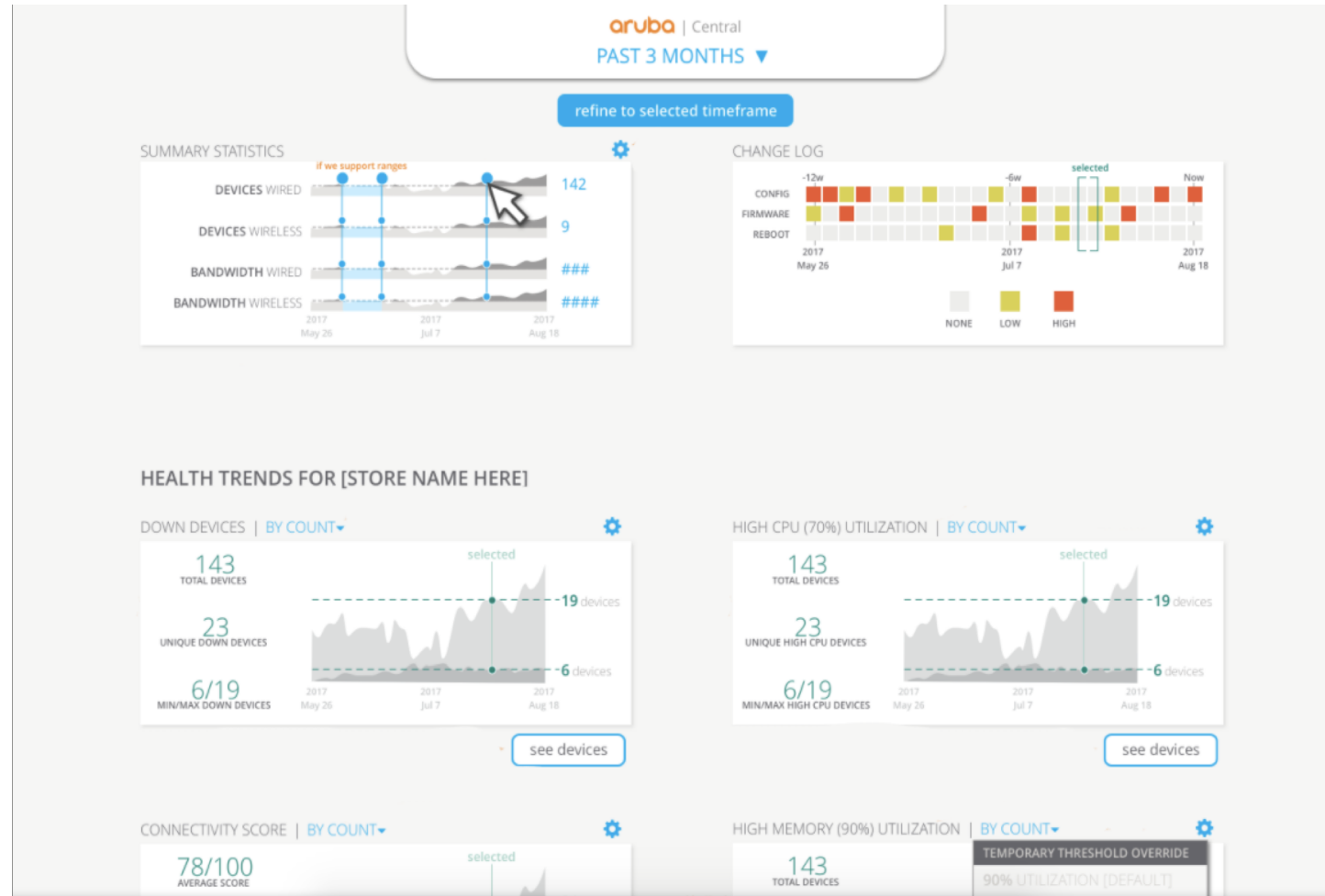
- Monitoring via two approaches
  - Metrics and stats that are passively collected
  - Metrics and stats that are actively collected from synthetic transactions
- Results Delivered in Three Ways
  - Via APIs and API based notifications
  - Via exportable reports
  - Via the Central Dashboards



# Site Health Dashboard

## Walkthrough

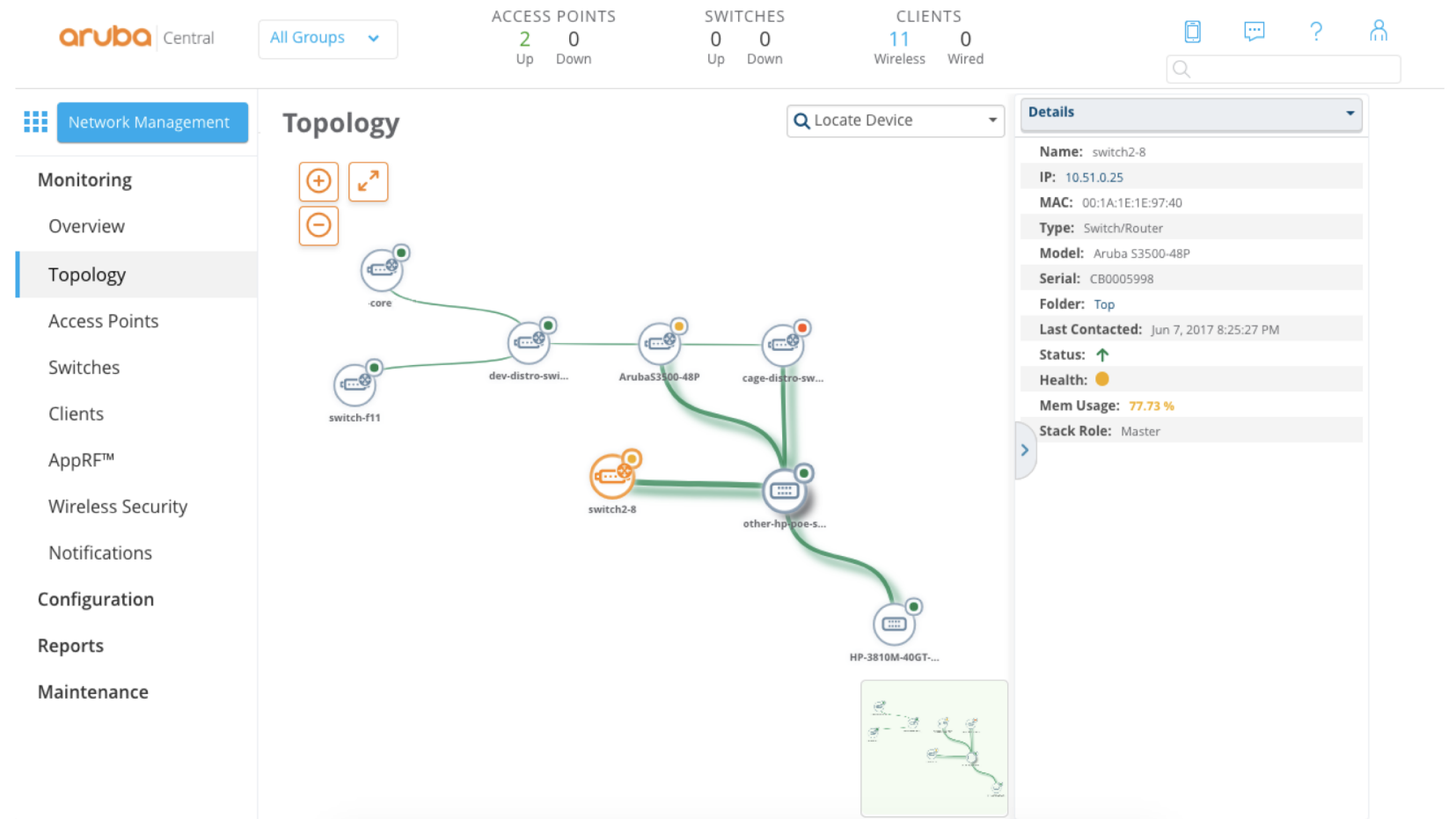
- System Health Indicators
  - Devices Disconnected
  - CPU Utilization
  - Memory Utilization
- RF Health Indicators
  - Channel Utilization (5/2.4Ghz)
  - Noise Floor (5/2.4Ghz)
- Client Health Indicators
  - Client Health Score
  - Connectivity Health Score
- WAN Health Indicators
  - Policy compliance
  - WAN usage



# Topology View

## Walkthrough

- Tree and Planetary View
- Health status
- Hover info
- VLAN Overlays






# Client View

## Walkthrough

- Complete end-to-end visibility:

- Client info
- RF & Health
- Location
- Clarity
- UCC
- ...



CLIENT >>>> SSID >>>> AP

CLIENT INFO | SUMMARY

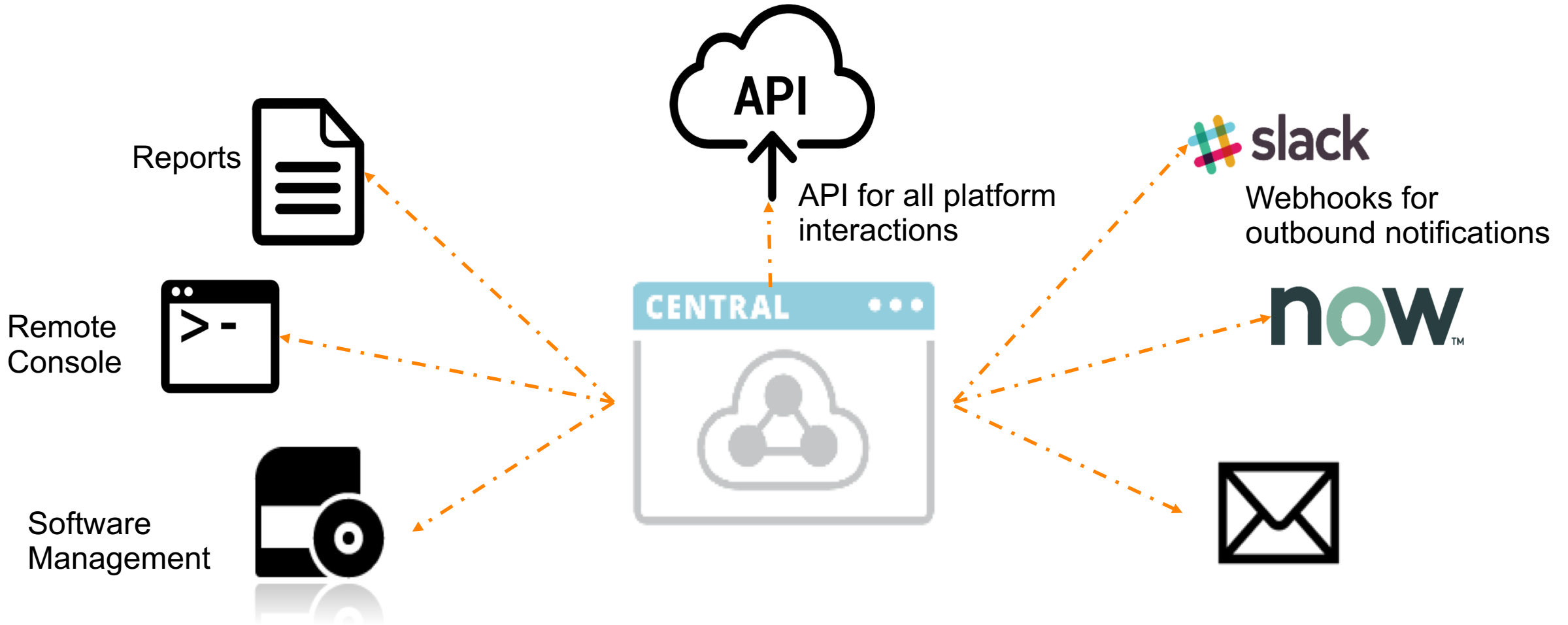
USERNAME : capesensor	STATUS : Connected
MAC : 40:ed:98:57:67:6a	CONNECTION MODE : 802.11AN
IP : 10.127.20.11	SSID : BRANCH-CORP
MANUFACTURER : IEEE Registration Authority	VLAN ID : 1
ENCRYPTION : WPA-2 Enterprise	AUTHENTICATION SERVER : 10.130.30.21
DHCP SERVER : 10.127.20.1	

USAGE & RF HEALTH

SIGNAL STRENGTH : 32 dBm	SPEED : 144 Mbps
SIGNAL TO NOISE RATIO (SNR) : 63 dB	CHANNEL / BAND : 116 / 5 GHz

CURRENT LOCATION

# More than just monitoring...



# Goal: Solve the Branch problem, not just the WAN



## Simple (at Enterprise scale)

Drive simplicity and fewer boxes in branch solution



## Transport Independency

Own your WAN policy

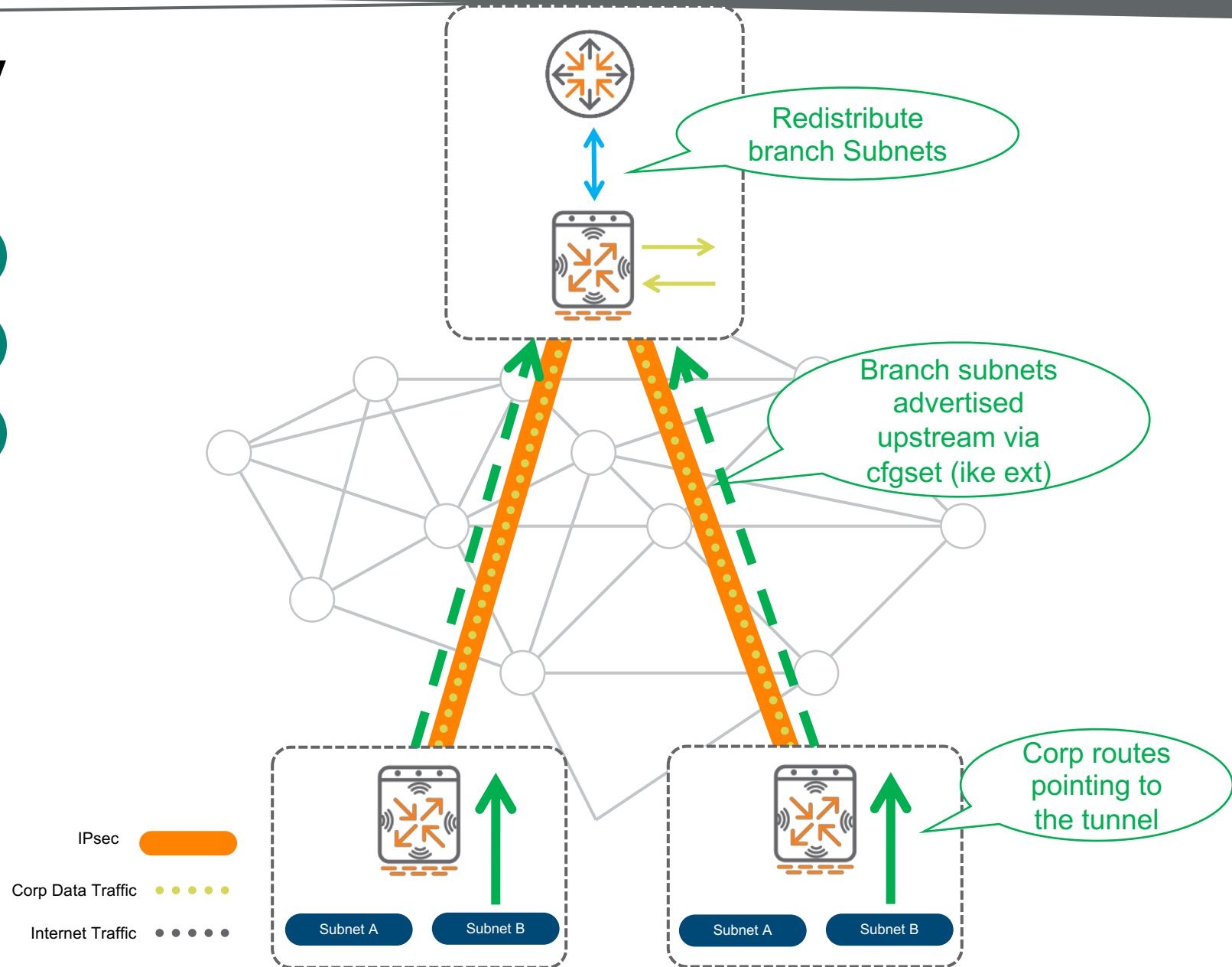


## Common Policy and Management

for Wired, WLAN and WAN

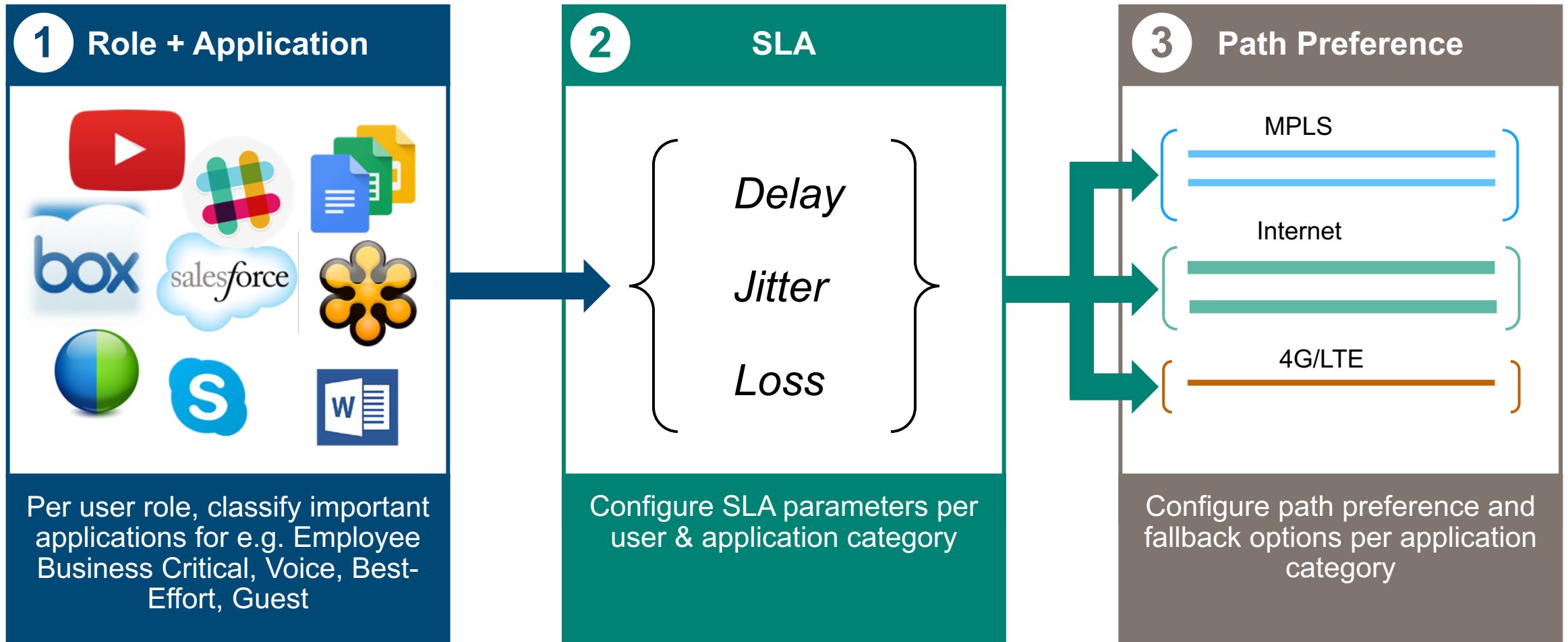
# Setting up the overlay

- 1 Establish VPN tunnels
- 2 Advertise branch routes
- 3 Start sending traffic





# Dynamic Path Selection/Steering





# What does a DPS Policy look like?

## Walkthrough

### 1 Specify 'Interesting' Traffic

#### Traffic Specification Rules for Employee Mission Critical Policy

SOURCE	DESTINATION	APPLICATION	
Employee	Any	Workday	 
Employee	20.20.20.0/24	Exchange	
Employee	30.30.30.0/24	TCP Port 22	



### 2 Choose SLA parameters to measure WAN performance

#### Select SLA for Employee Mission Critical Policy

NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	UTILIZATION (%)
Highly Available	150	150	1	20
Best for Internet	100	100	5	80
Best for Voice	50	25	5	80



#### Probe Options for Highly Available SLA

Destination IP:

Protocol: ☒ ICMP ☐ UDP


Probe interval:  sec.

Bursts per probe:


### 3 Configure path preference parameters

#### WAN Path Selection for Employee Mission Critical Policy

☐ Direct to Internet

Primary path:  

Secondary path:  

Last resort path:  

# Dynamic Path Steering

*Is the WAN link compliant to the application SLA?*

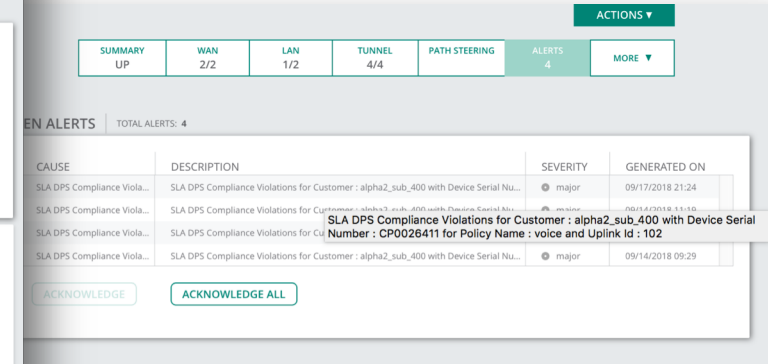
- View compliance per WAN link
- Highlight violations with specific reasons

*Is the policy honoring path preference?*

- View session distribution across active links

*Is DPS kicking in when there are WAN link SLA violations?*

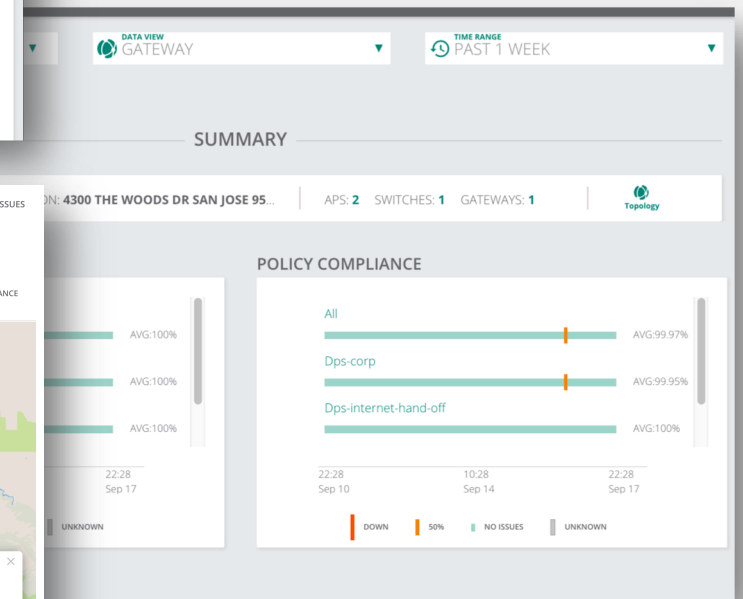
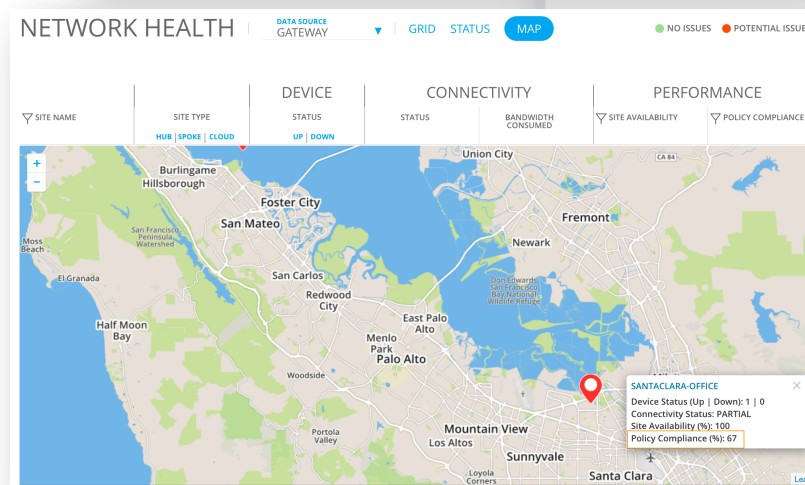
- Quickly identify session movement between WAN links



CAUSE	DESCRIPTION	SEVERITY	GENERATED ON
SLA DPS Compliance Viola...	SLA DPS Compliance Violations for Customer : alpha2_sub_400 with Device Serial Nu...	major	09/17/2018 21:24
SLA DPS Compliance Viola...	SLA DPS Compliance Violations for Customer : alpha2_sub_400 with Device Serial Nu...	major	09/14/2018 11:19
SLA DPS Compliance Viola...	SLA DPS Compliance Violations for Customer : alpha2_sub_400 with Device Serial Nu...	major	09/14/2018 09:29

Number : CP0026411 for Policy Name : voice and Uplink id : 102

Buttons: ACKNOWLEDGE, ACKNOWLEDGE ALL



# Goal: Solve the Branch problem, not just the WAN



## Simple (at Enterprise scale)

Drive simplicity and fewer boxes in branch solution



## Transport Independency

Own your WAN policy



## Common Policy and Management

for Wired, WLAN and WAN



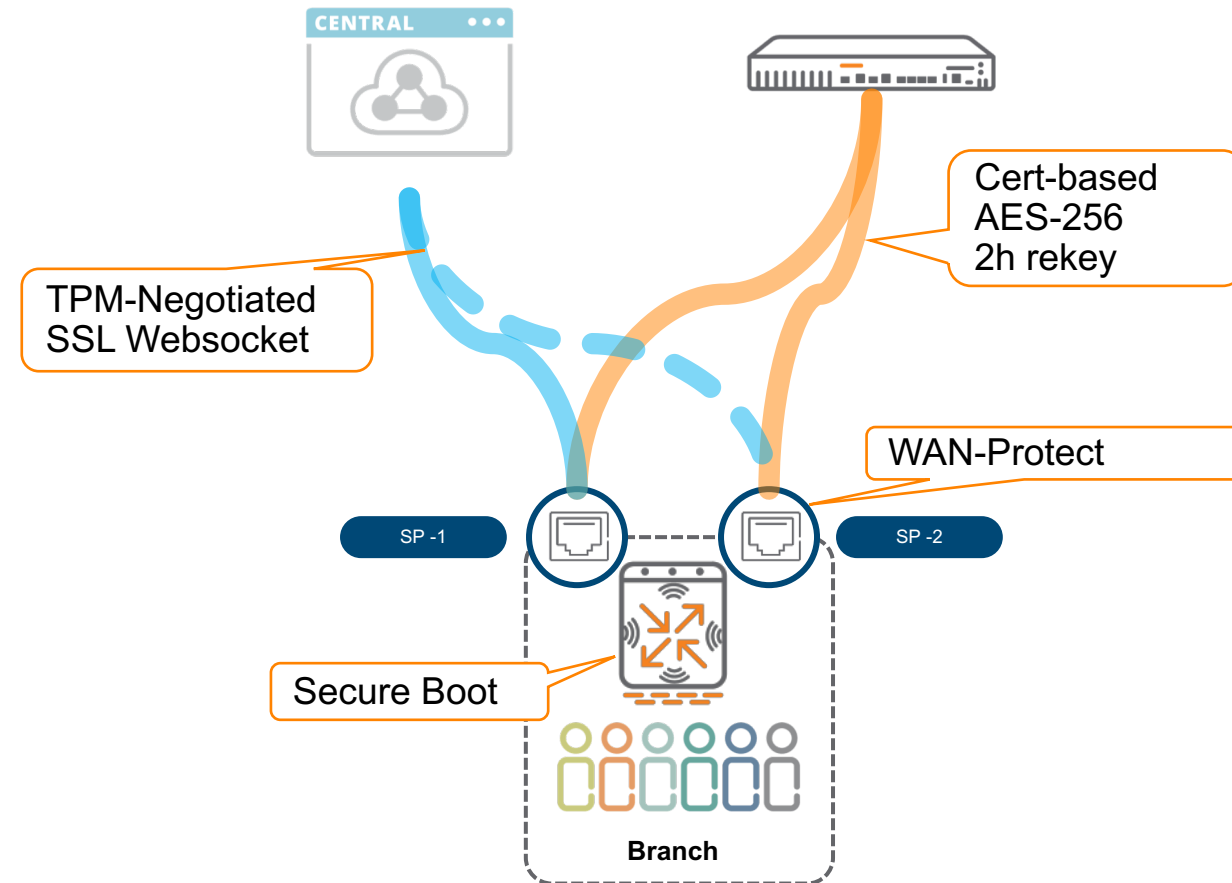
# Security and hardening

Backup

- 1 Secure Boot
- 2 WAN-Protect ACL
- 3 TPM-Negotiated mgmt websocket
- 4 Cert-based AES256 encryption



Security Core



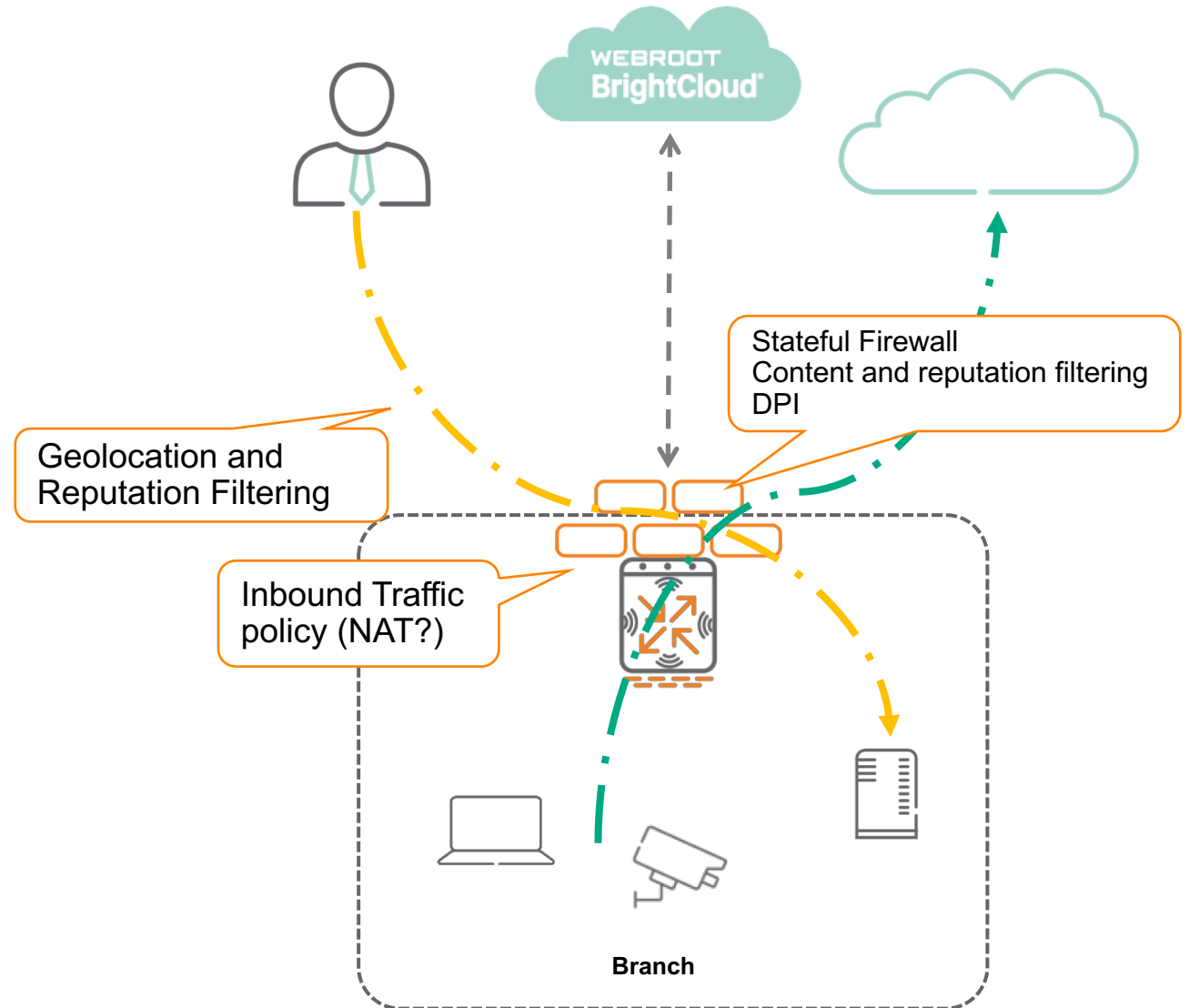
# Branch Firewall

Backup

- 1 Inbound firewall policies  
- Apply on WAN interfaces
- 2 Geolocation and reputation filtering  
- Inbound and outbound
- 3 Stateful firewall with ALGs and DPI
- 4 Web Content and Reputation Filtering



Security Core

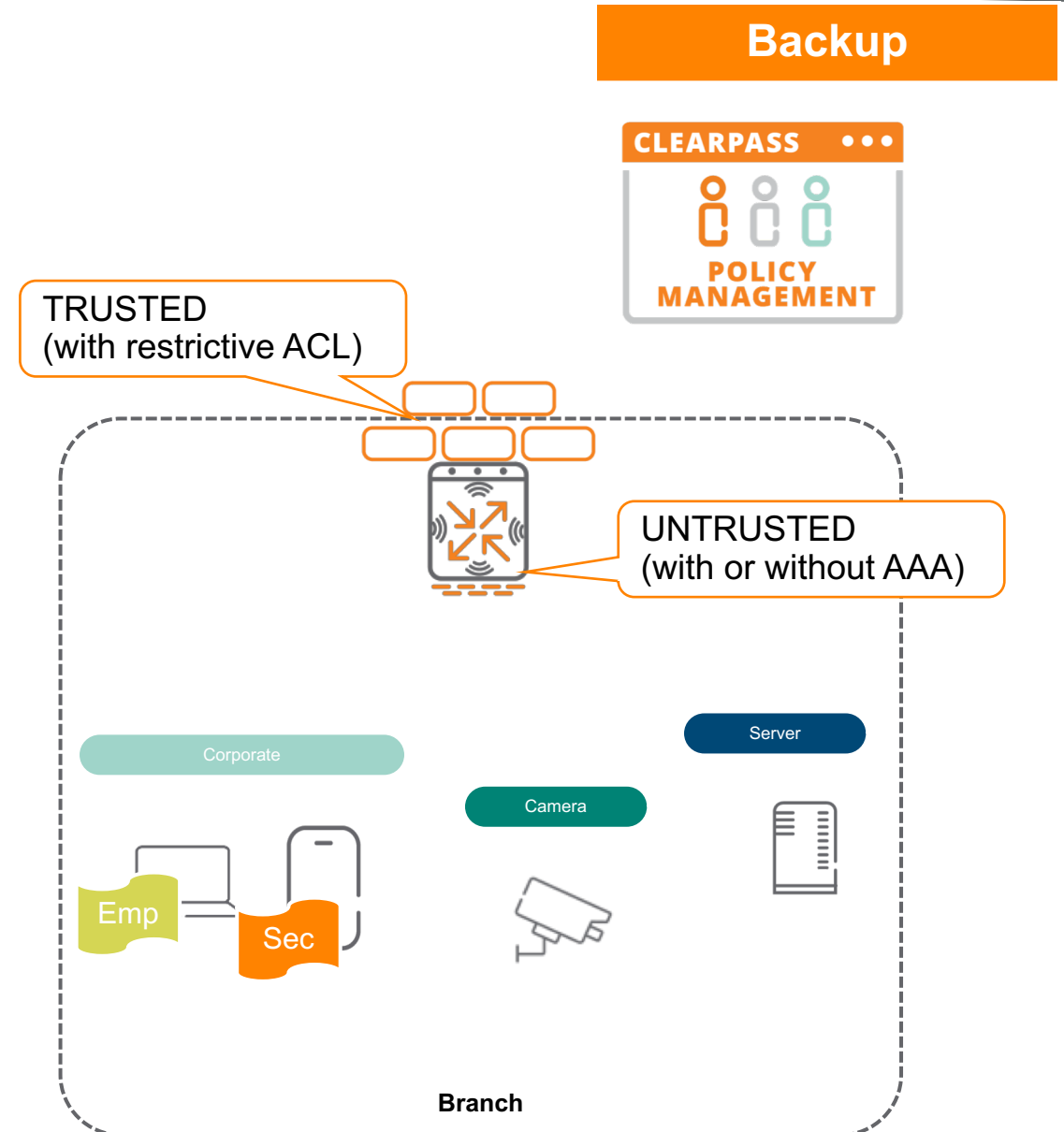


# Role-based Security

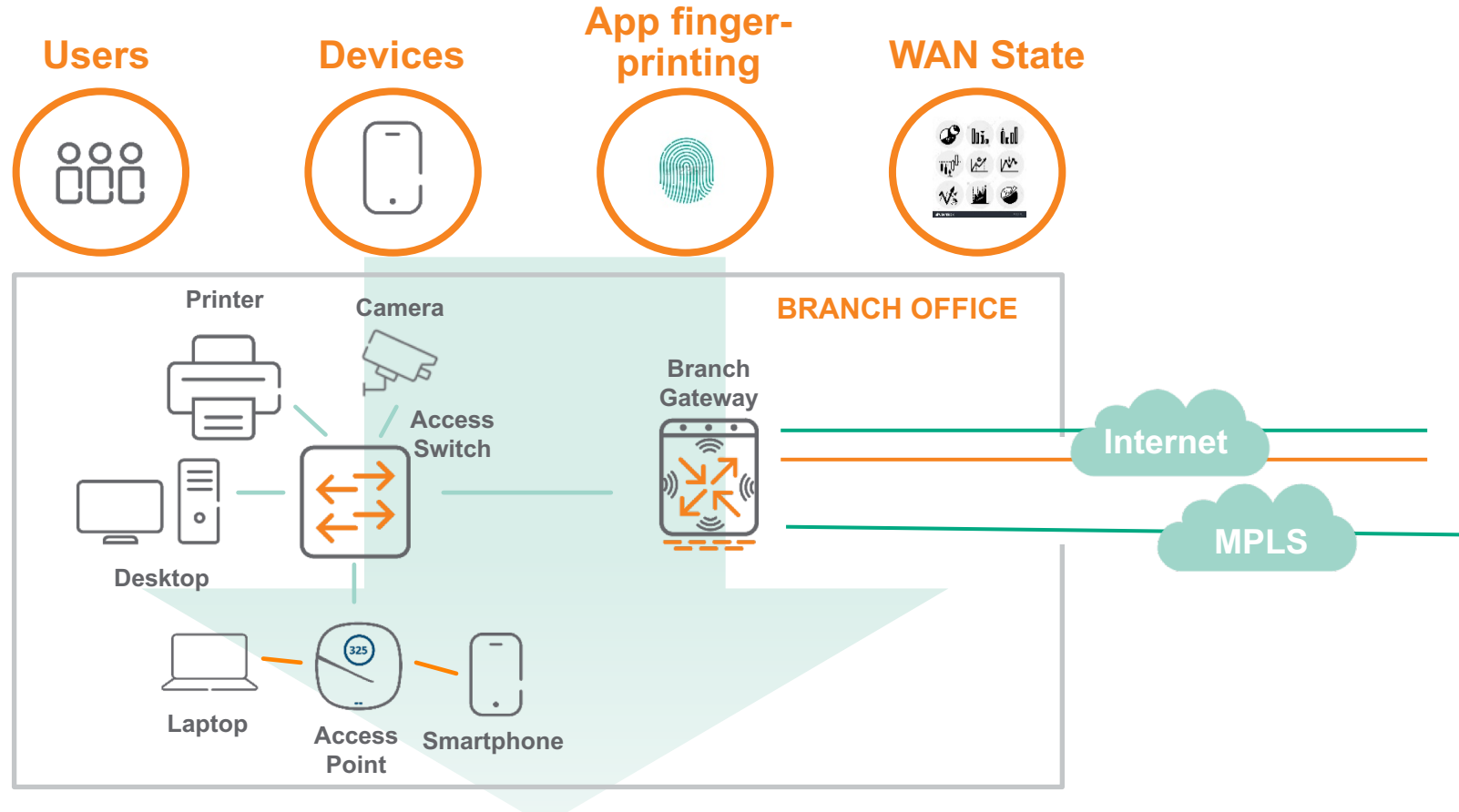
- 1 ALWAYS set WAN ports to TRUSTED
- 2 LAN ports should be set to UNTRUSTED
- 3 Apply AAA profiles to branch VLANs
- 4 (optional) Set AAA-based enforcement



Security Core



# Role Based Policies for LAN, Security, WAN



## LAN Policies

WLAN and wired switching policies applied per role.  
E.g.: Guest SSID, QoS for PCI traffic

## Security Policies

Firewall and WebCC policies applied per role.  
E.g.: WebCC for Guest, PCI traffic isolation

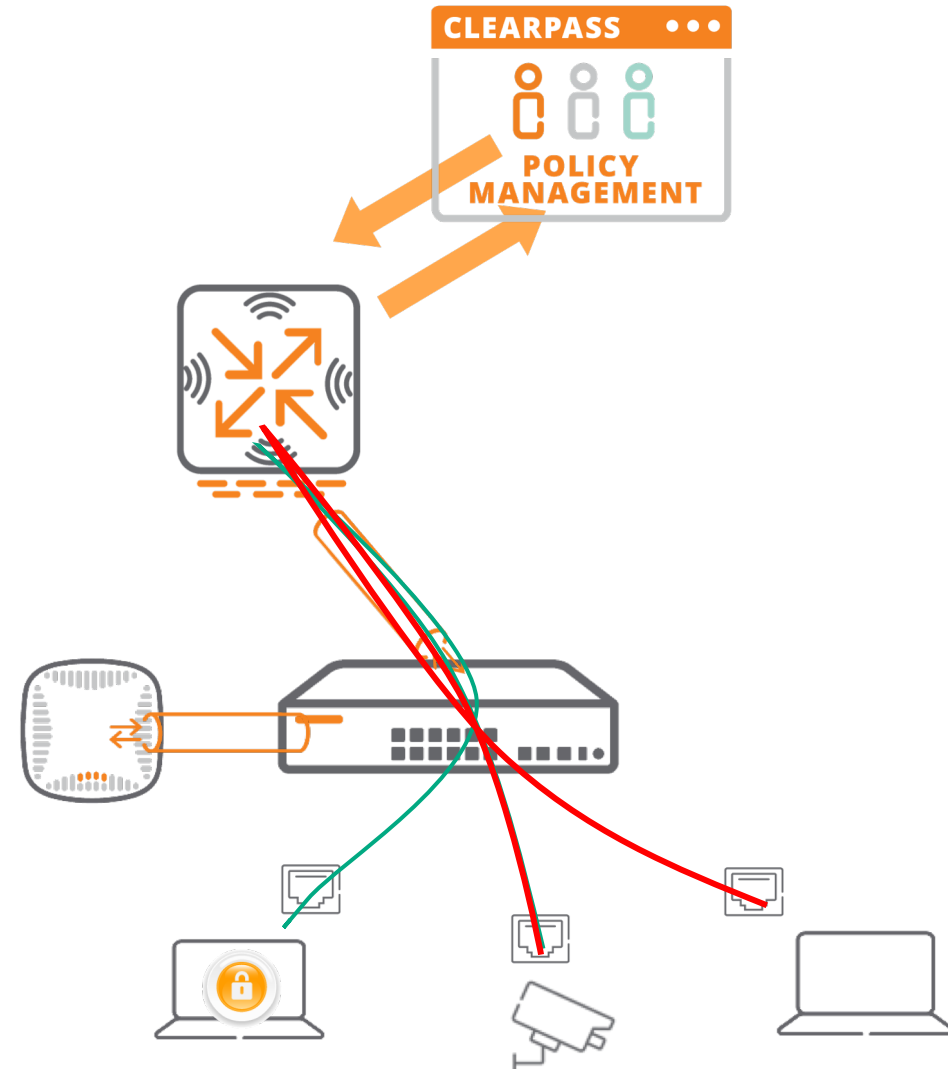
## WAN Policies

Path steering policies applied per role.  
E.g.: Guest to Internet, PCI traffic to MPLS

# User Centric policy demo

Demo

- 1 Switch establishes Tunnel
- 2 APs detected via device-profile. Port override
- 3 Devices profiled and classified by ClearPass
- 4 Roles snooped by GW
- 5 All traffic goes through the firewall > Micro-Segmentation



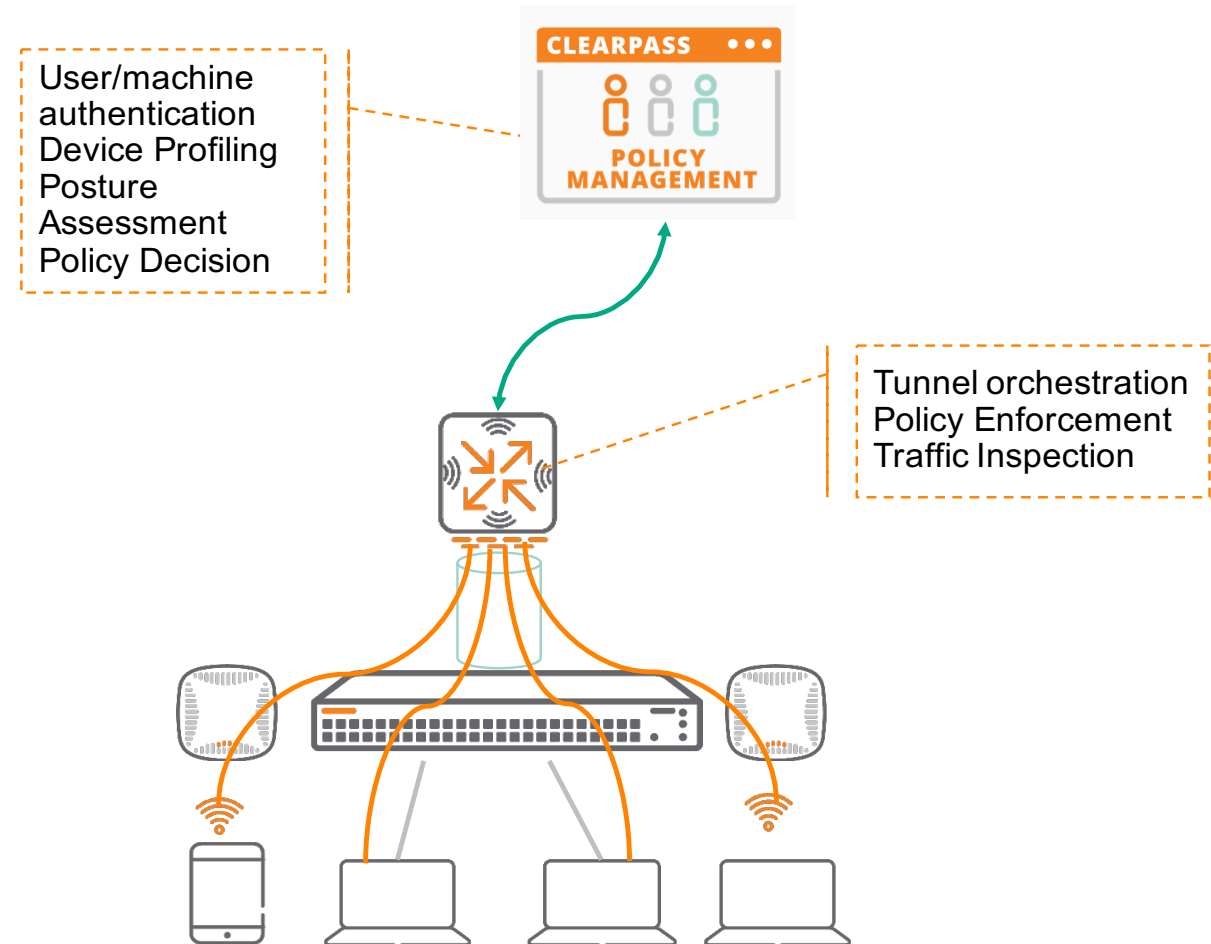
# Consolidated Policy Enforcement Point

## Dynamic Segmentation applied to the branch

- 1 All ports tunneled to GW
- 2 APs detected via device-profile. Set trunk
- 3 Tunneled traffic always UNTRUSTED
- 4 GW becomes branch security enforcement point
- 5 Intra-VLAN traffic now goes through firewall > Dynamic Segmentation!



Security Core



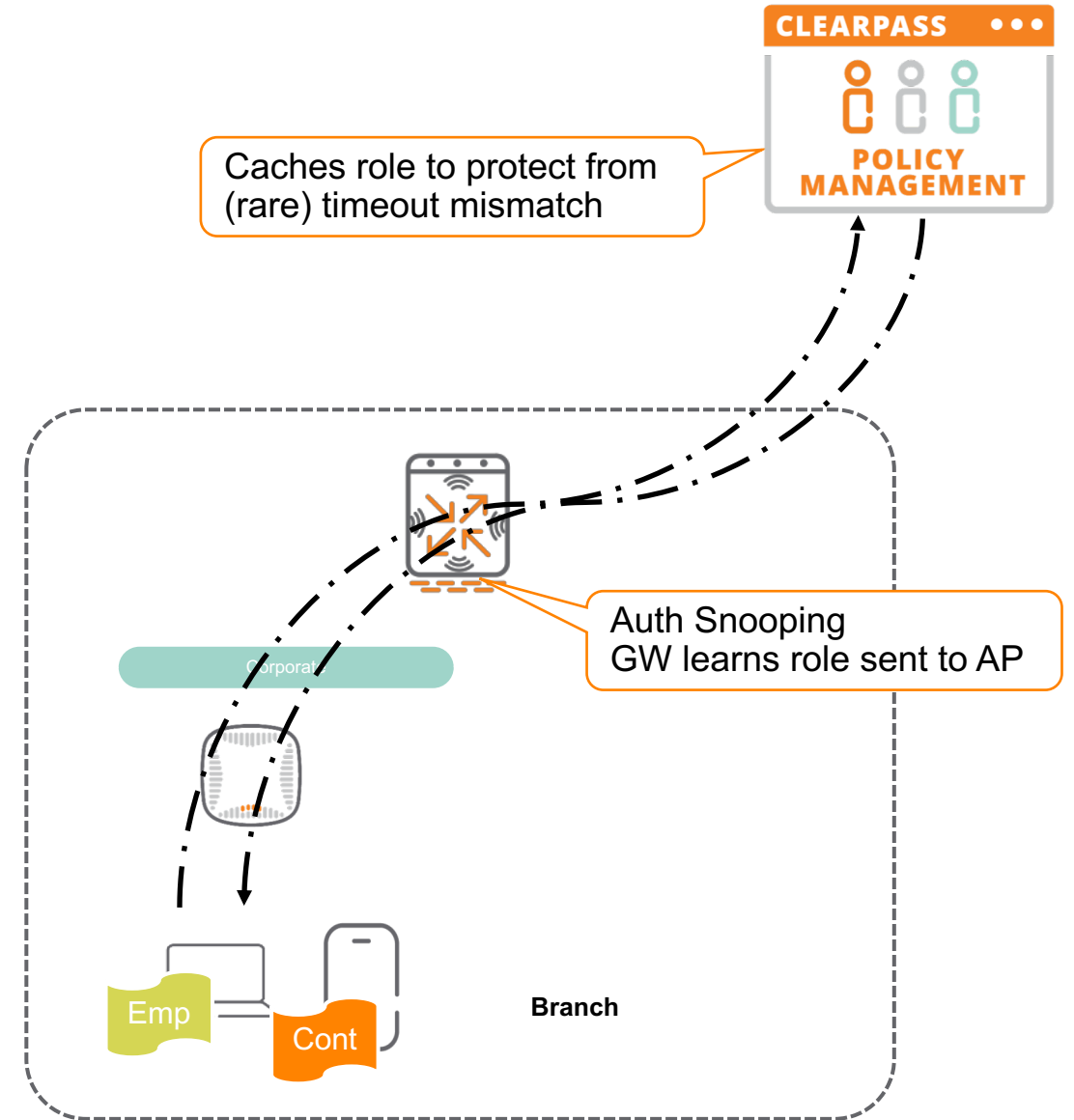
# Authentication Snooping (stateful-dot1X)

Learning roles from other authentications

- 1 AP in "logon" role and Stateful dot1X enabled
- 2 Dot1X auth from AP to AAA Server
- 3 AAA Srv responds with user-role/filter-ID (if ClearPass) also binds role to MAC
- 4 GW Snoops Authentication to learn role
- 5 If GW session expires but dot1X doesn't – MAC auth
- 6 ClearPass responds with cached role



Security Core



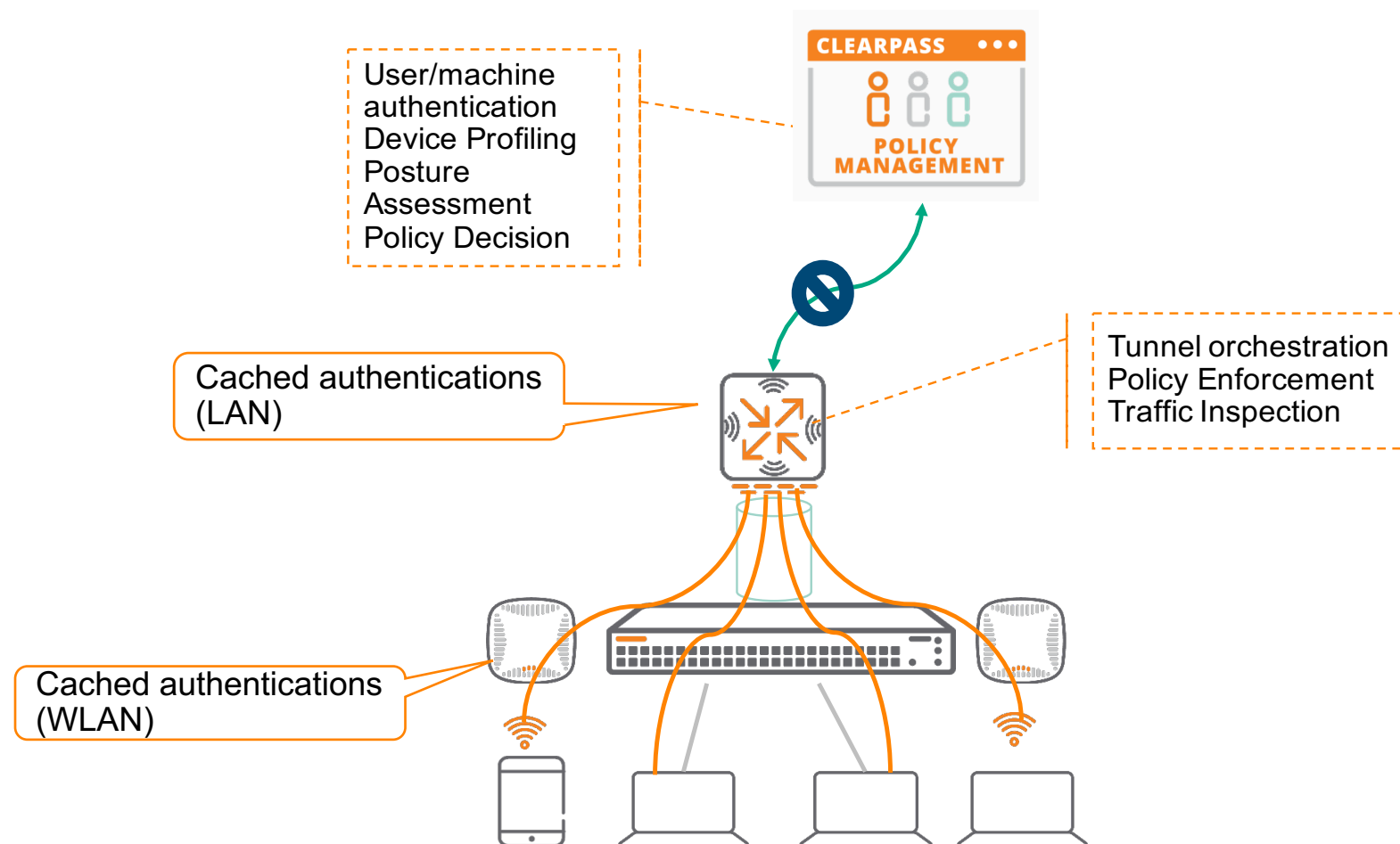


# AAA survivability

## Controlling the risk...

1 Gateway Caches MAC/EAP-TLS

2 IAP Caches PEAP/EAP-TLS



# Guest Access + WebCC

- 1

## Guest access registration via Central (or ClearPass Guest)

2

## Role-based WebCC and reputatlon policy



## Cloud Guest

CENTRAL

**WEBROOT**  
**BrightCloud®**

## Branch

# Enforcing L7+ security policies

Advanced threat detection (Checkpoint / Palo Alto GPCS / Zscaler)

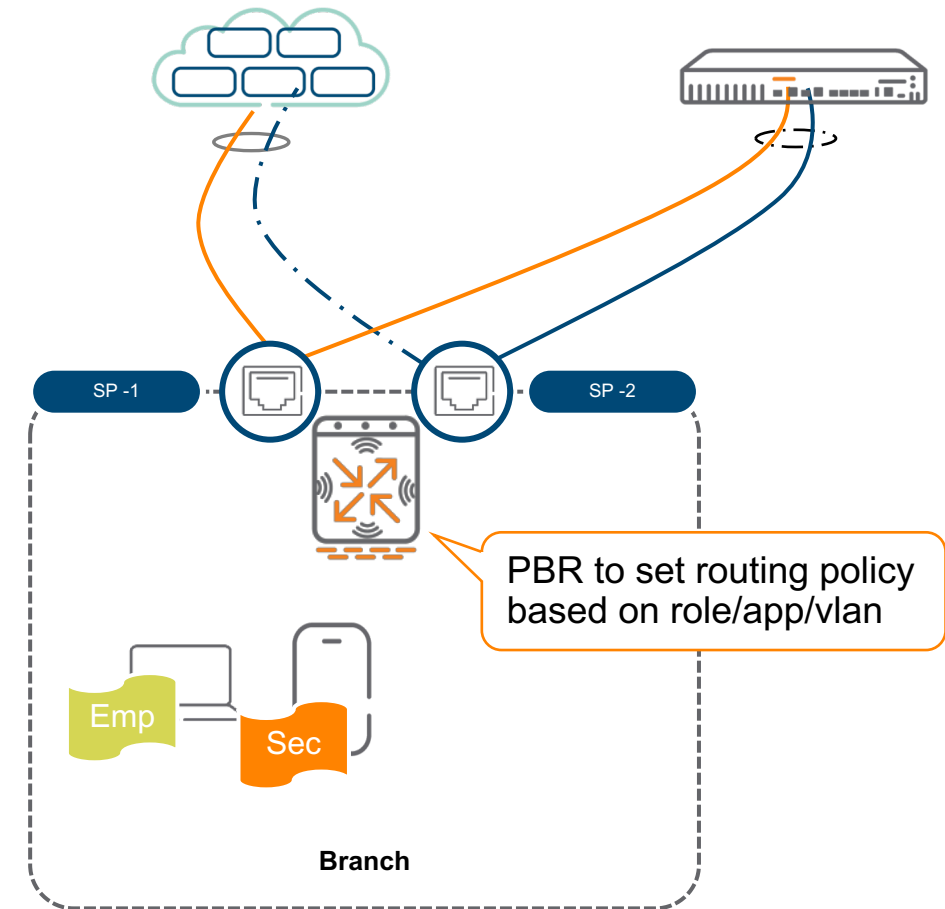
- 1 ClearPass assigns user role
- 2 ClearPass shares role with firewall
- 3 Role includes routing policy to force Internet traffic through Cloud Security



Security Core



360 Security  
Exchange Program



# Beyond Security Enforcement

## UEBA - Introspect integration

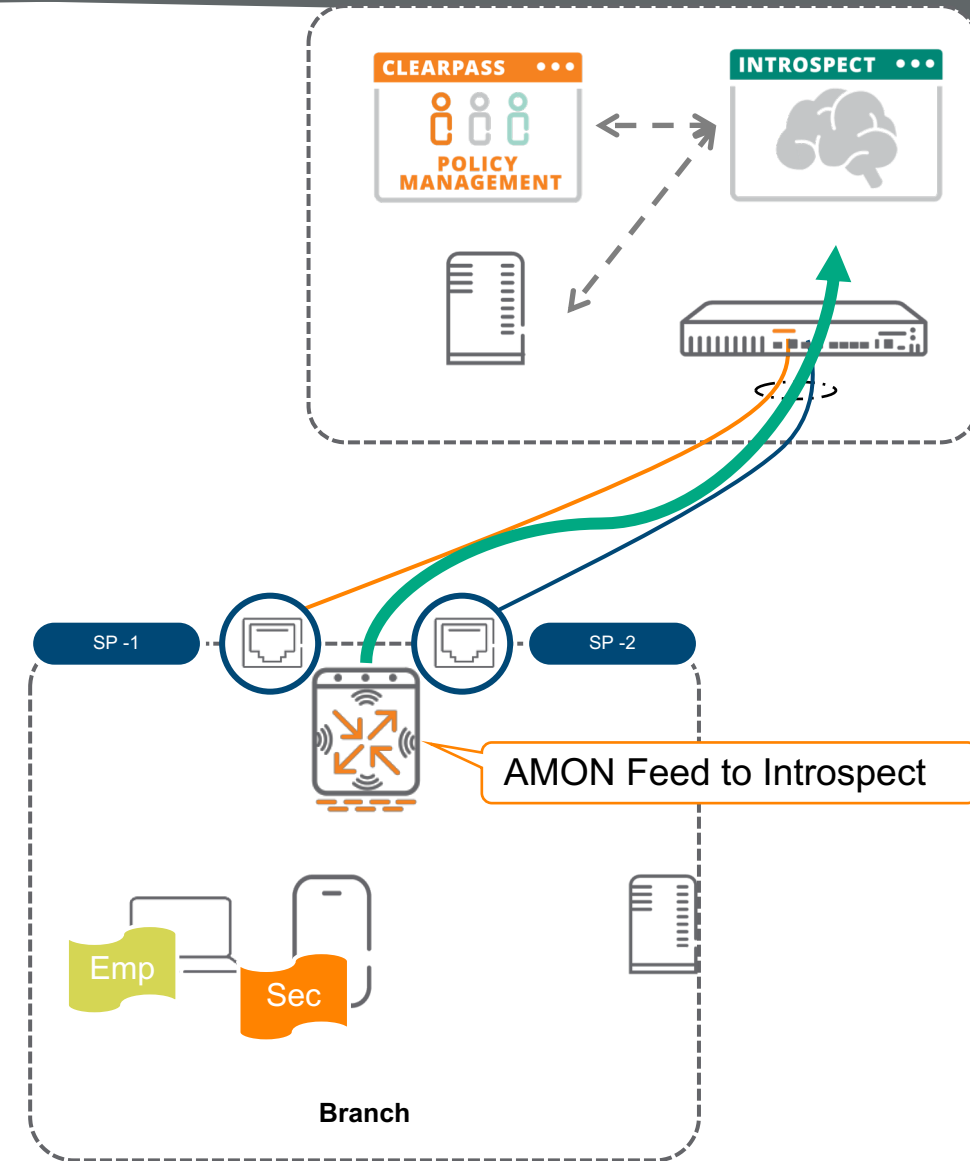
- 1 ClearPass assigns user role
- 2 Introspect integrated with ClearPass and other user services
- 3 GW Sends FW metadata (AMON feed) to Introspect



Security Core



360 Security  
Exchange Program



# Beyond Security Enforcement

## UEBA - Introspect integration

1 ClearPass assigns user role

2 Introspect integrated with ClearPass and other user services

3 GW Sends FW metadata (AMON feed) to Introspect



Security Core



360 Security  
Exchange Program



aruba Introspect CONVERSATIONS GRID

Past Week Aug 9, 2018 16:40 - Aug 16, 2018 16:40

groupby explorer cloud apps visual grid settings

WATCHLISTS 2

Enterprise Watchlist

Exemption Watchlist

Time src\_ip:10.127.0.0/16

939 conversations

939 records over 47 pages

Time	Source	Dest Location	Destination	Application	Content	Summary
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States	www.linkedin.com 108.174.10.10	linkedin (03), IP	560 bytes, 560	
Aug 16, 2018 4:09:53 PM	10.127.20.3	Internal	10.130.30.21	radius, IP Business-Systems, A	932 bytes, 1.16 k	
Aug 16, 2018 4:09:53 PM	10.127.20.6	Internal	10.130.30.21	Unknown-IP, IP	560 bytes, 560	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States	www.box.com 107.152.25.197	box-net, IP	90.64 KB, 6.55 i	
Aug 16, 2018 4:09:53 PM	10.127.20.6	Australia	1.1.1.1	DNS, IP Networking, Infrastru	87 bytes, 142 by	
Aug 16, 2018 4:09:53 PM	10.127.20.2	United States Boardman, Oregon	internal.central.aru... 52.33.70.234	HTTPS, IP Misc, Misc	1.48 KB, 4.01 KB	
Aug 16, 2018 4:09:53 PM	10.127.20.5	United States Boardman, Oregon	device-gateway.ca... 52.39.161.216	HTTPS, IP Misc, Misc	152.20 KB, 71.45	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States Boardman, Oregon	device-gateway.ca... 52.39.161.216	HTTPS, IP Misc, Misc	6.85 KB, 2.09 K	
Aug 16, 2018 4:09:53 PM	10.127.20.3	Australia	1.1.1.1	DNS, IP Networking, Infrastru	271 bytes, 256 t	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States	www.dropbox.com 162.125.71	dropbox (03), IP	532 bytes, 560	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States Dallas, Texas	8.8.8.8	DNS, IP Networking, Infrastru	2.81 KB, 2.81 KB	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States	www.dropbox.com 162.125.71	Dropbox, IP Collaboration, File-Si	121.23 KB, 6.88	
Aug 16, 2018 4:09:53 PM	10.127.20.5	United States Dallas, Texas	8.8.8.8	DNS, IP Networking, Infrastru	6.36 KB, 6.69 Ki	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States	www.box.com 107.152.25.197	box (03), IP	560 bytes, 560	
Aug 16, 2018 4:09:53 PM	10.127.20.6	Internal	10.130.30.21	HTTPS, IP Misc, Misc	6.10 KB, 2.02 KE	
Aug 16, 2018 4:09:53 PM	10.127.20.6	United States Seattle, Washington	cdn.capenetworks... 54.230.118.65	amazon-aws, IP	728 bytes, 680	
Aug 16, 2018 4:07:53 PM	10.127.20.6	Internal	10.130.30.21	Unknown-IP, IP	560 bytes, 560	
Aug 16, 2018 4:07:53 PM	10.127.20.3	Internal	10.130.30.21	radius, IP Business-Systems, A	932 bytes, 1.16 k	
Aug 16, 2018 4:07:53 PM	10.127.20.6	United States	www.linkedin.com 108.174.10.10	LinkedIn, IP Collaboration, Social	34.35 KB, 5.24 i	
Aug 16, 2018 4:07:53 PM	10.127.20.6	United States	www.dropbox.com 162.125.71	dropbox (03), IP	560 bytes, 560	

FILTERS

Application 26

DNS 327

HTTPS 302

SSL 69

Unknown-IP 33

radius 31

amazon-aws 21

Dropbox 18

Office365 15

apns 14

box (03) 13

box-net 12

dropbox (03) 12

LinkedIn 12

Apple 11

linkedin (03) 11

NetFlix 8

TCP 5

NTP 4

Skype 4

Outlook 3

HTTP 2

Facebook 1

Gmail 1

iCloud 1

ICMP 1

Show Fewer

Location 6

United States 708

Australia 168

Internal 57

Japan 3

Switzerland 2

Show all

Username 1

unknown 939

Alert Name 0

Tags 5

dst\_host\_alexa\_1m 391

dst\_host\_alexa\_250k 391

dst\_host\_alexa\_500k 391

dst\_host\_alexa\_100k 382

dst\_host\_unknown 348

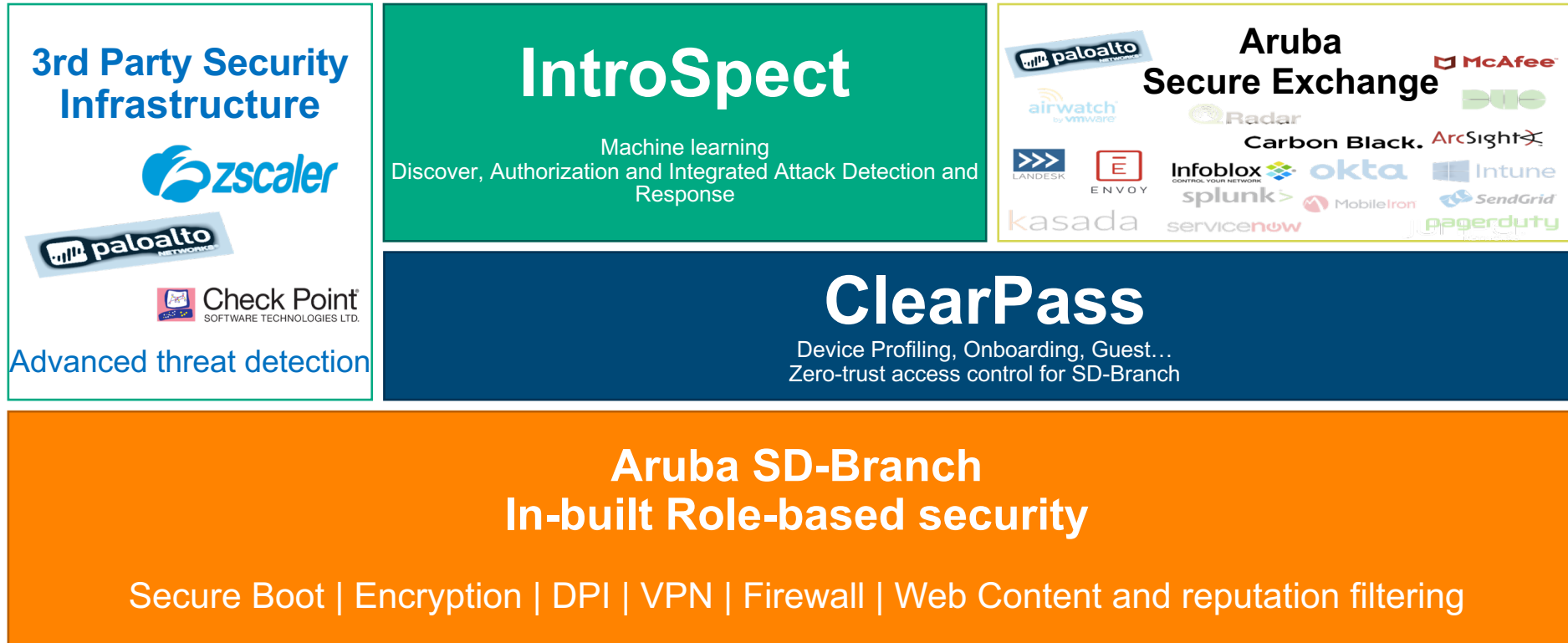
data\_subtype 1

Amon 939

data\_type 1

Logs 939

# Security Layers

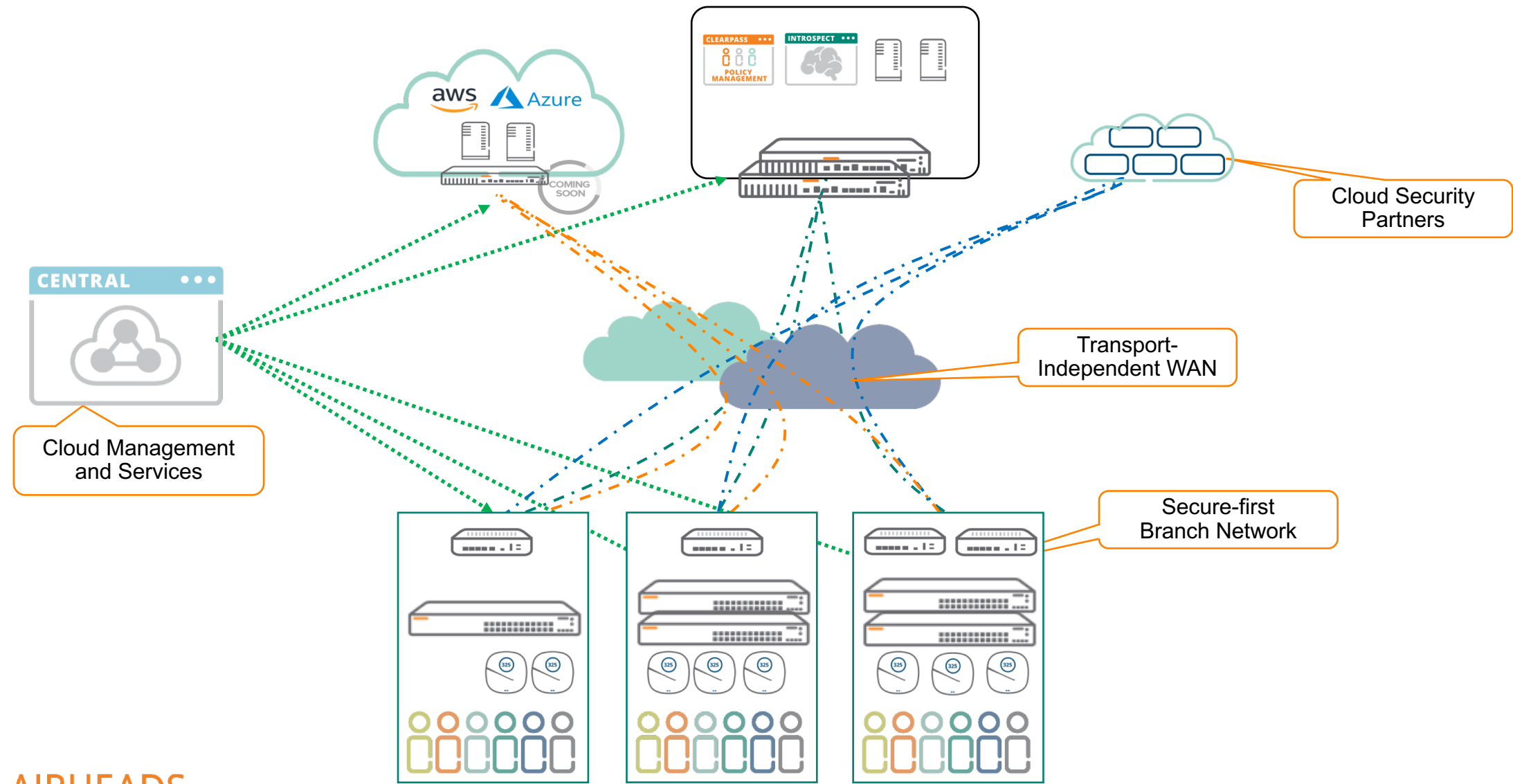


Security Core

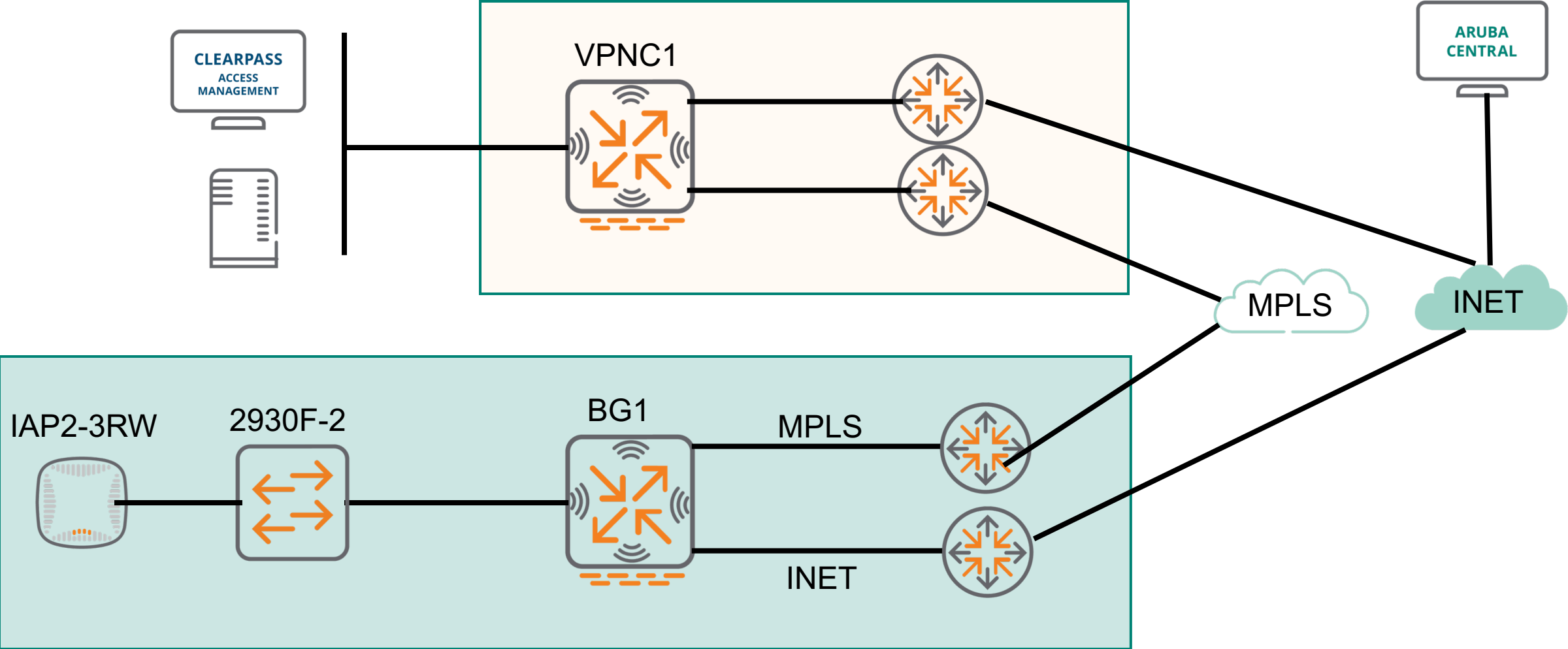


360 Security  
Exchange Program

# Aruba SD-Branch solution



# Demo







# AIRHEADS

meetup

**Thank You**