AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

Aruba SD-Branch

John Schaap
john.schaap@hpe.com

26 October 2018

#ArubaAirheads

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

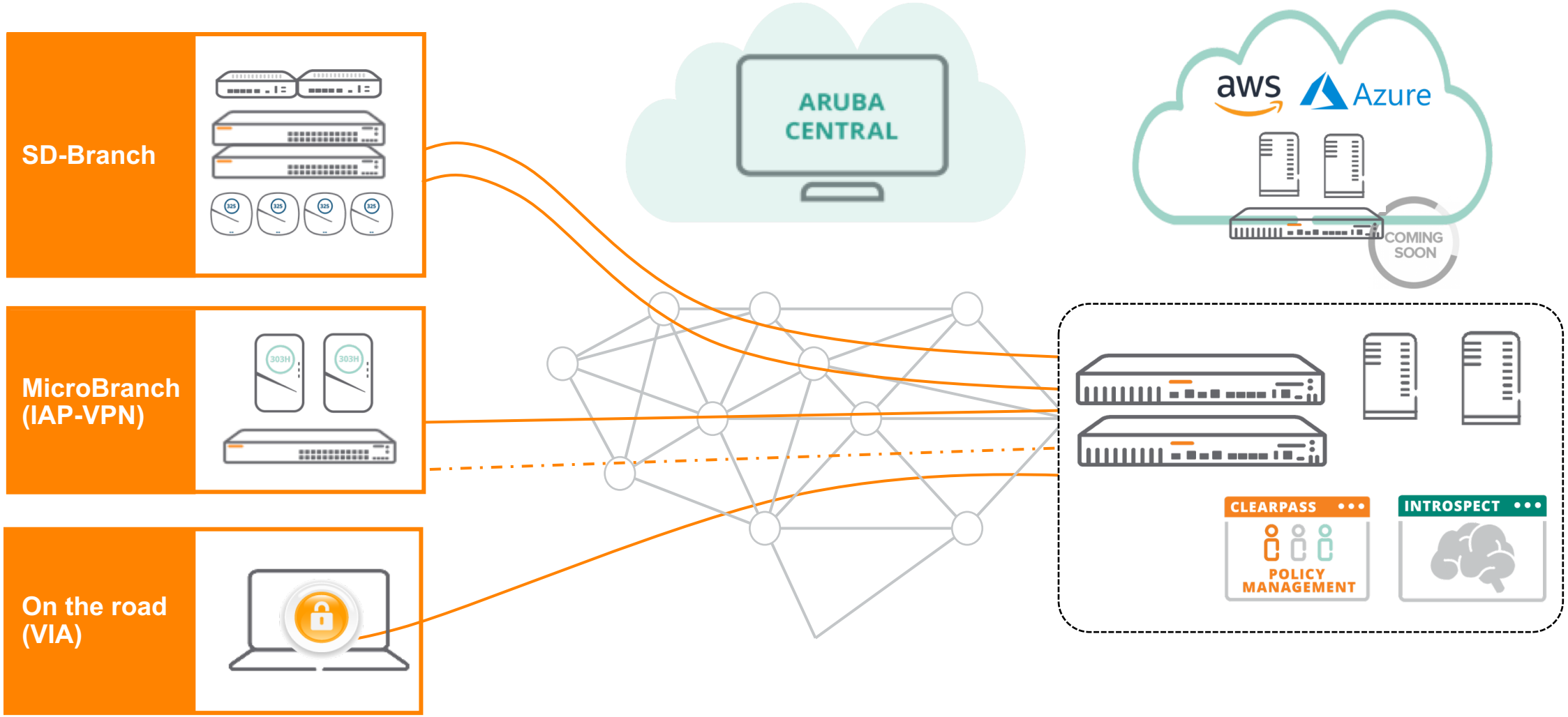
Goal: Solve the Branch problem, not just the WAN

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

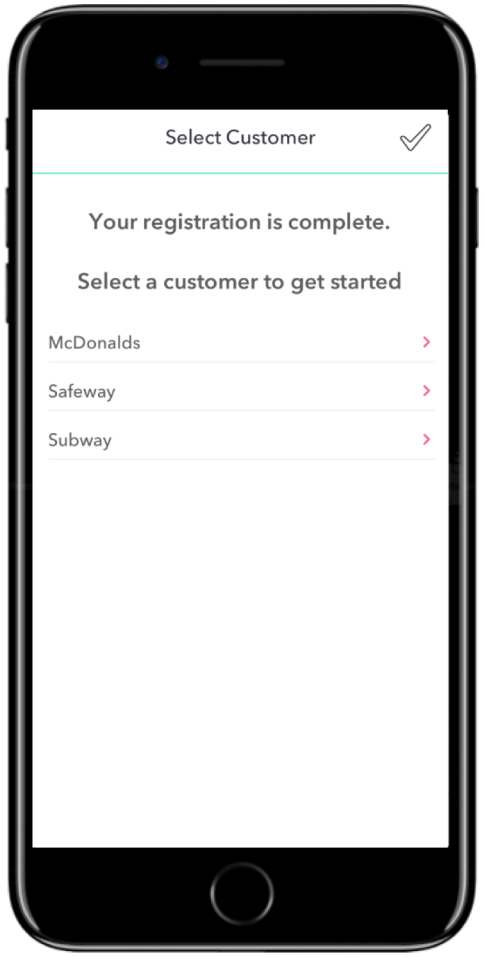
PRESENCE ANALYTICS

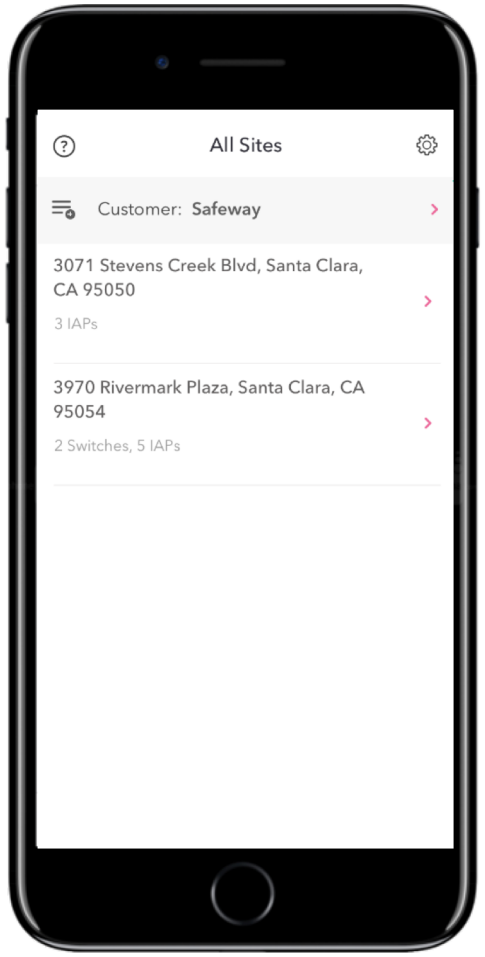
SD-WAN

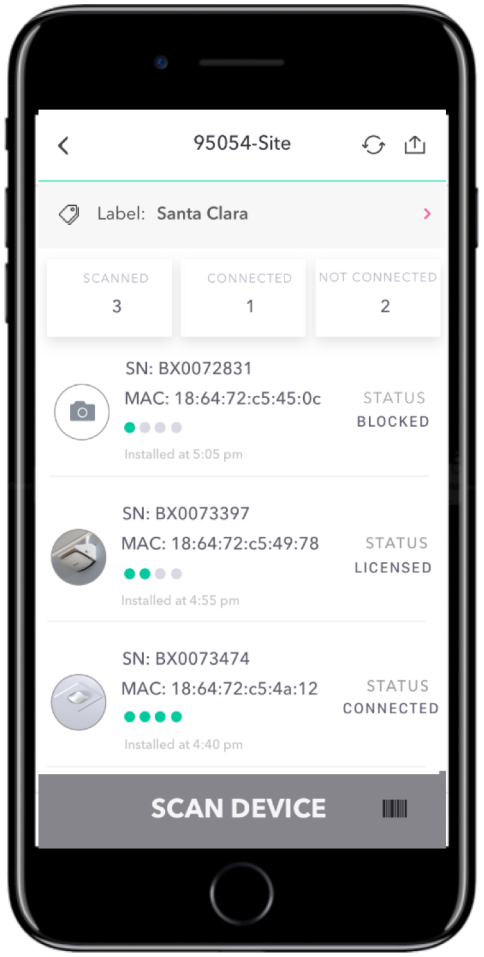
SECURITY

Simple Onboarding

Demo



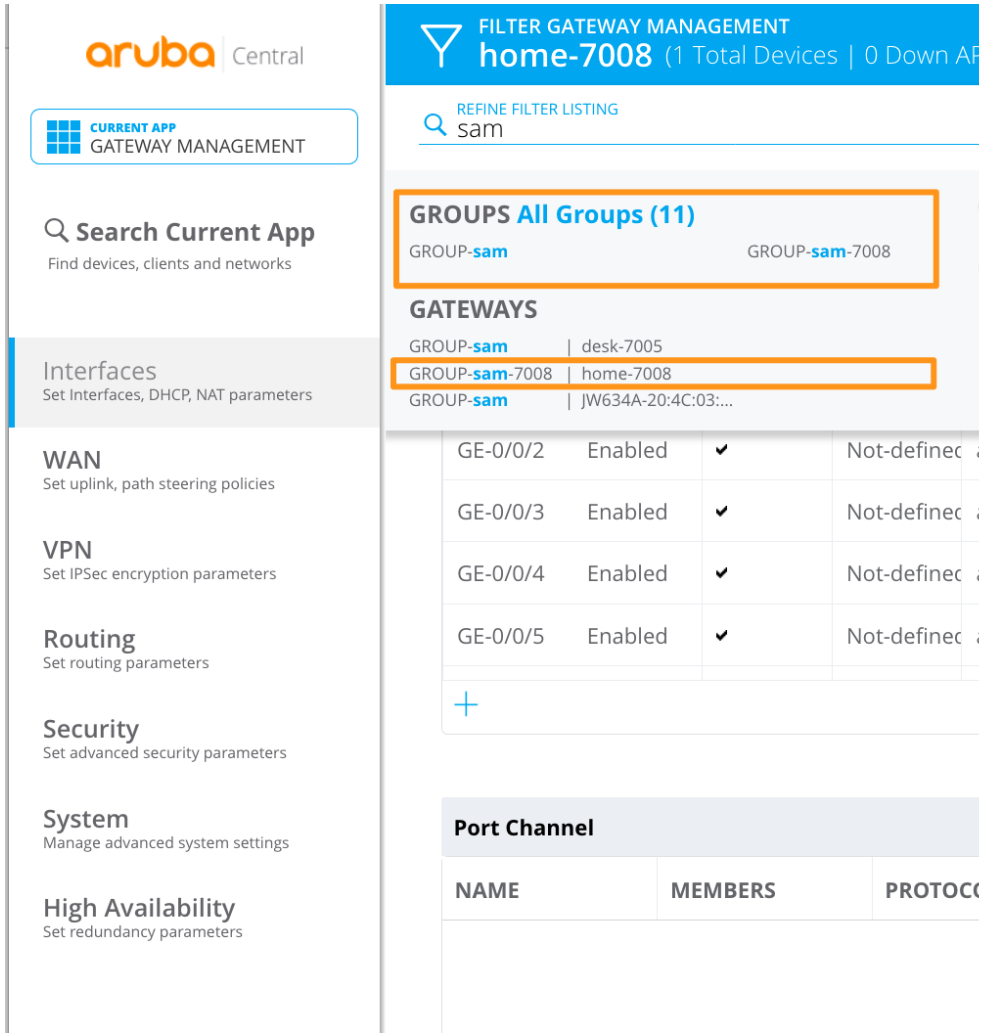




- Installer selects site and scans devices
- Installer gets status of device on boarding
- Admin gains central visibility into onboarding
- Site awareness seeded into onboarding
- Configuration group pushed as part of onboarding

Hierarchical Management

Walkthrough



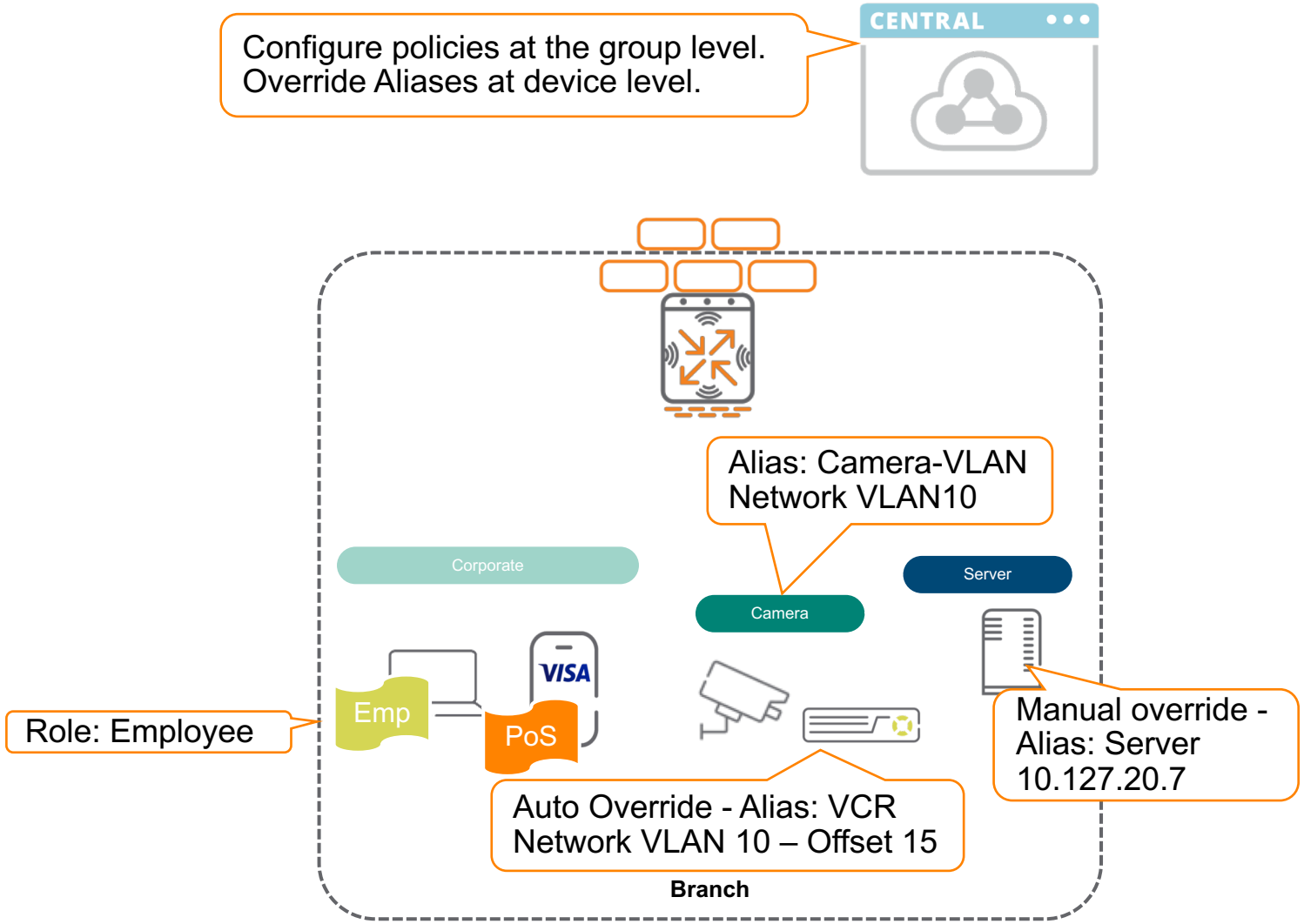
1. Apply configurations on a group basis
2. Overrides on a per-device basis (bulk-edit possible)
3. Monitoring based on sites/labels

Making branch security scalable…

Group based security policies

Walkthrough

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…



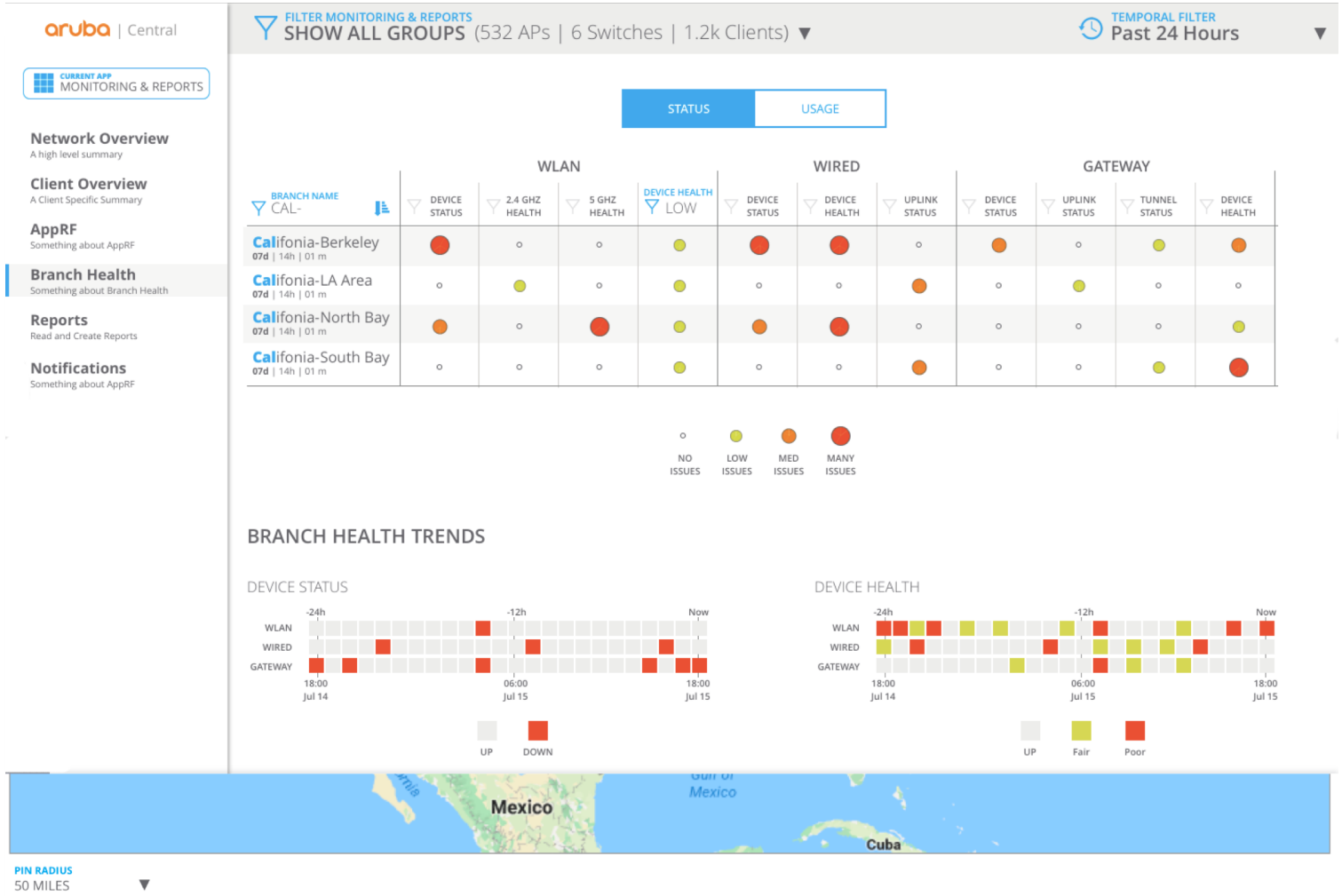
Security Core

AIRHEADS meetup

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

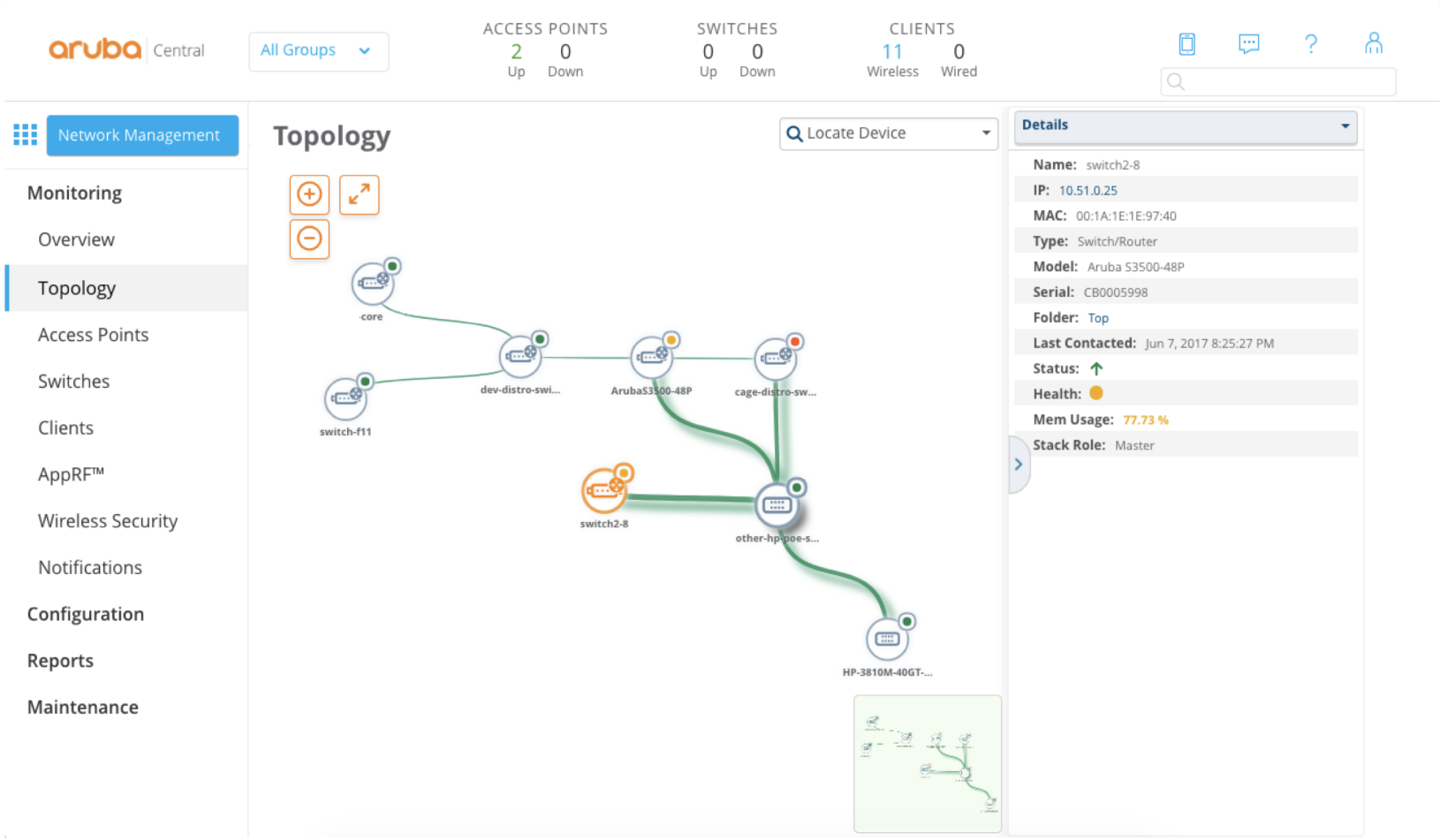
- System Health Indicators
  - Devices Disconnected
  - CPU Utilization
  - Memory Utilization
- RF Health Indicators
  - Channel Utilization (5/2.4Ghz)
  - Noise Floor (5/2.4Ghz)
- Client Health Indicators
  - Client Health Score
  - Connectivity Health Score
- WAN Health Indicators
  - Policy compliance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

AIRHEADS meetup

Topology View

Walkthrough

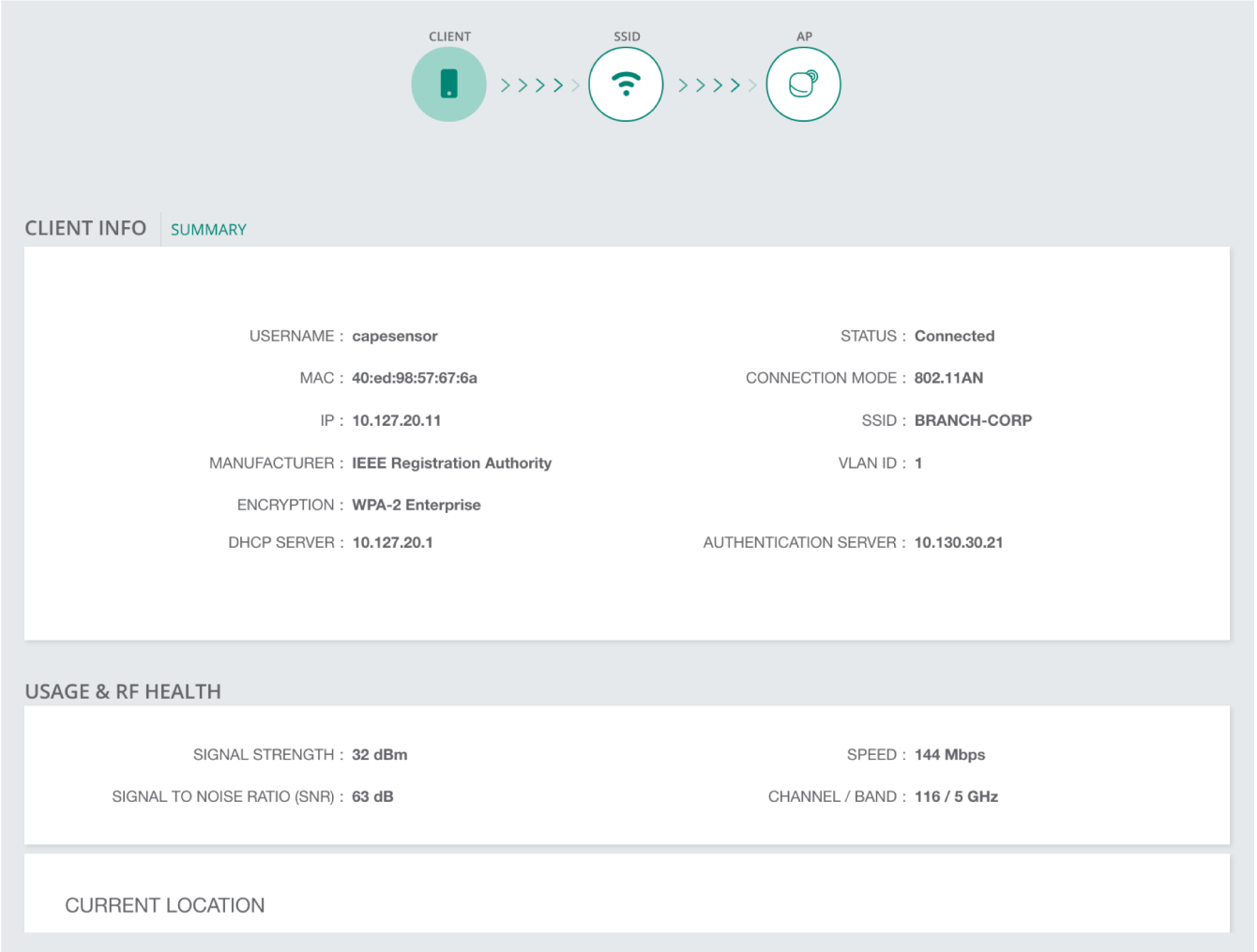
- Tree and Planetary View
- Health status
- Hover info
- VLAN Overlays



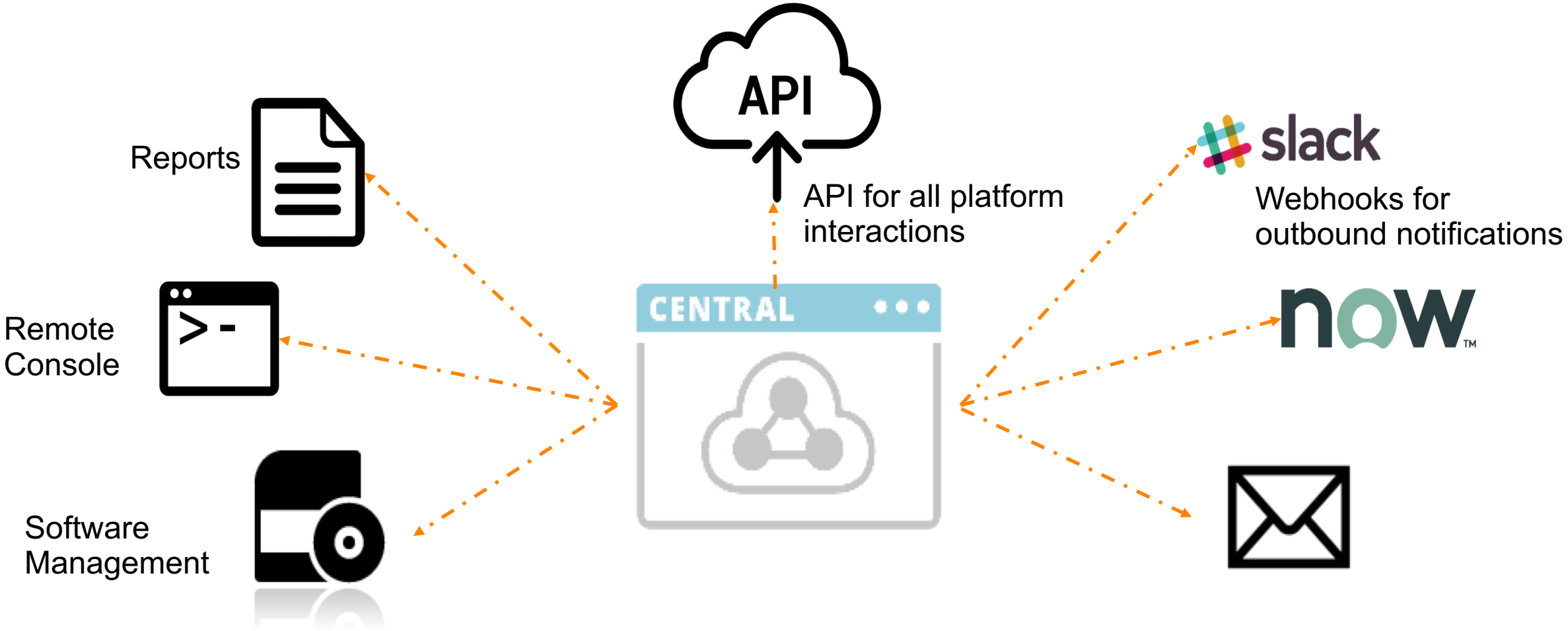
Client View

Walkthrough

- Complete end-to-end visibility:
  - Client info
  - RF & Health
  - Location
  - Clarity
  - UCC
  - …



More than just monitoring…



Goal: Solve the Branch problem, not just the WAN

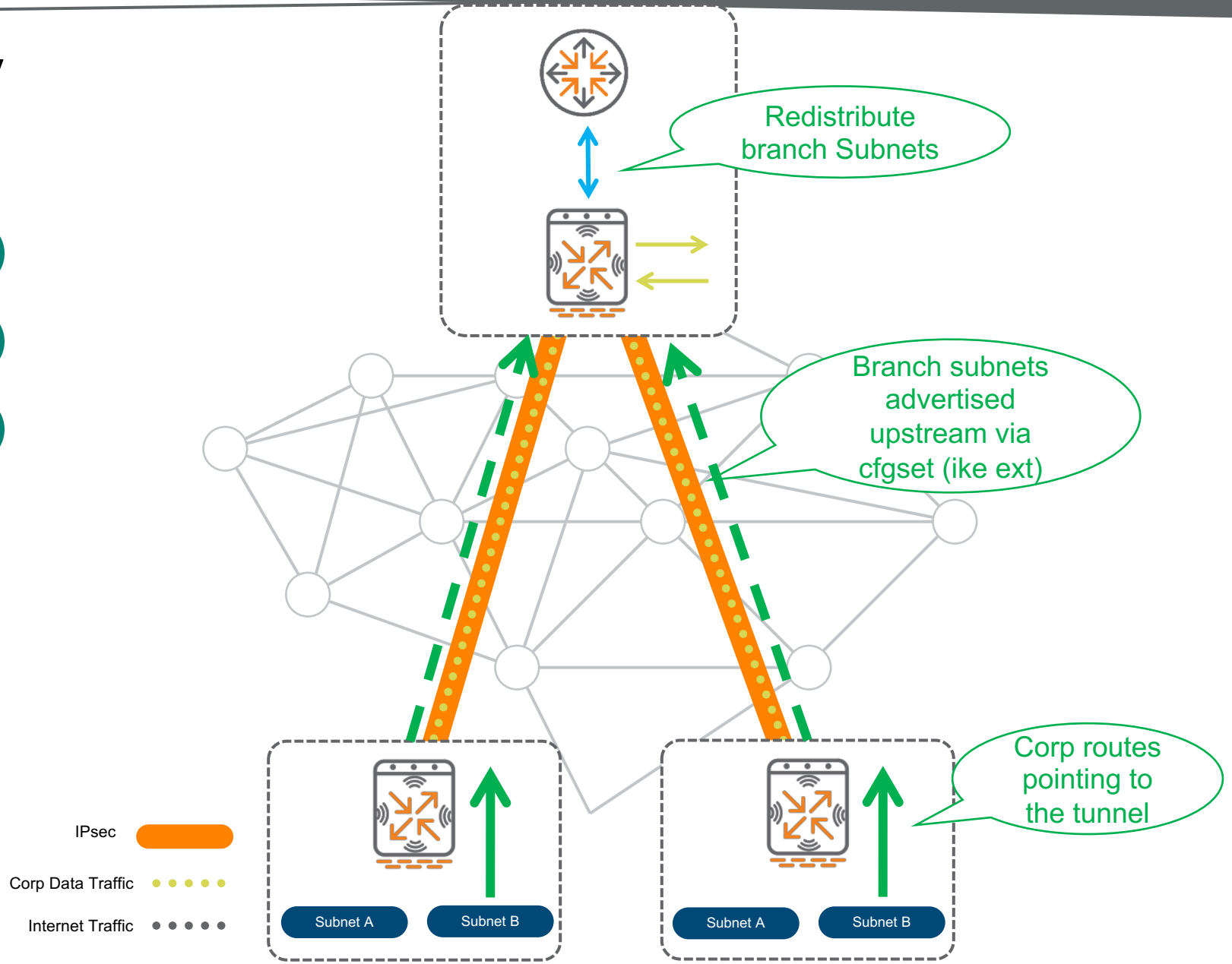
Simple (at Enterprise scale)
Drive simplicity and fewer boxes in branch solution

Transport Independency
Own your WAN policy

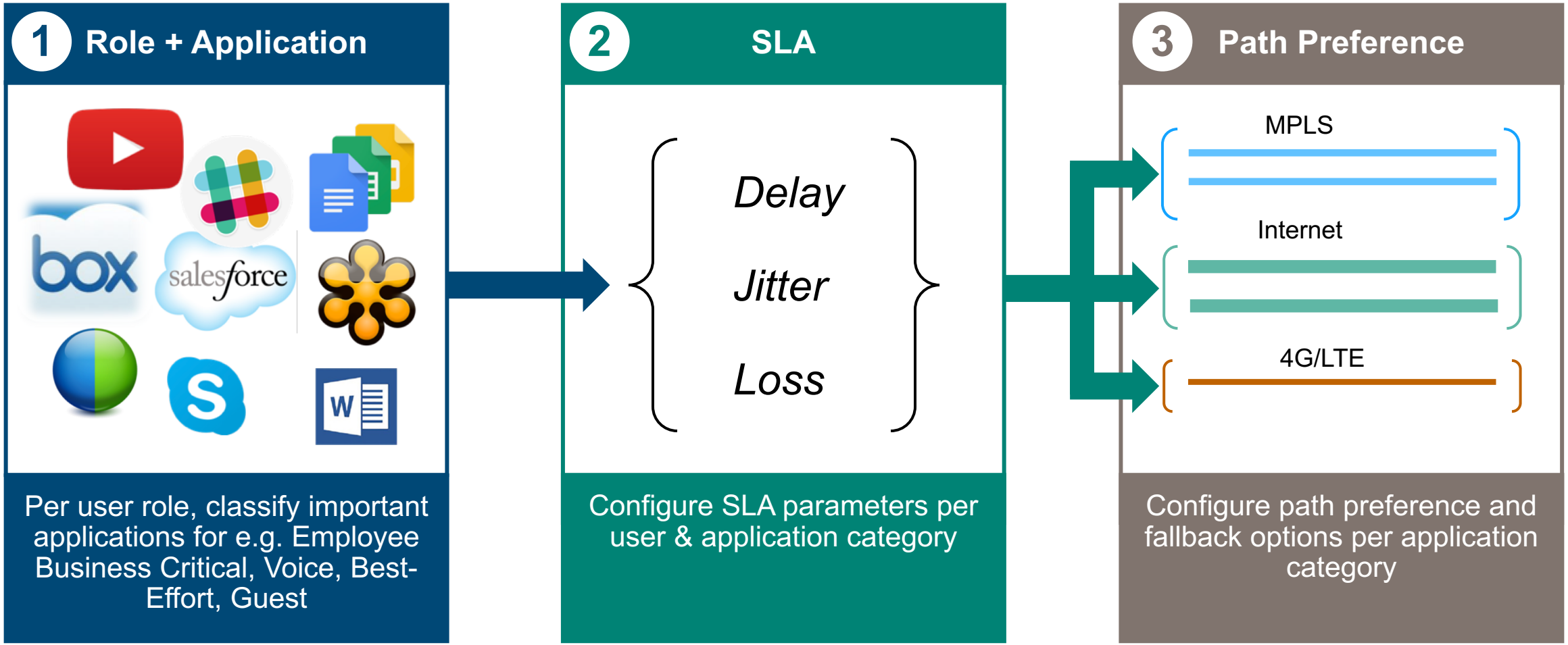
Common Policy and Management
for Wired, WLAN and WAN

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: 10.1.1.1

Protocol: ICMP UDP

Probe interval: 1 sec.

Bursts per probe: 30

3 Configure path preference parameters

WAN Path Selection for Employee Mission Critical Policy

Direct to Internet

Primary path: MPLS1, MPLS2

Secondary path: All INET All LTE

Last resort path: -- None --

Dynamic Path Steering

Demo

Is the WAN link compliant to the application SLA?

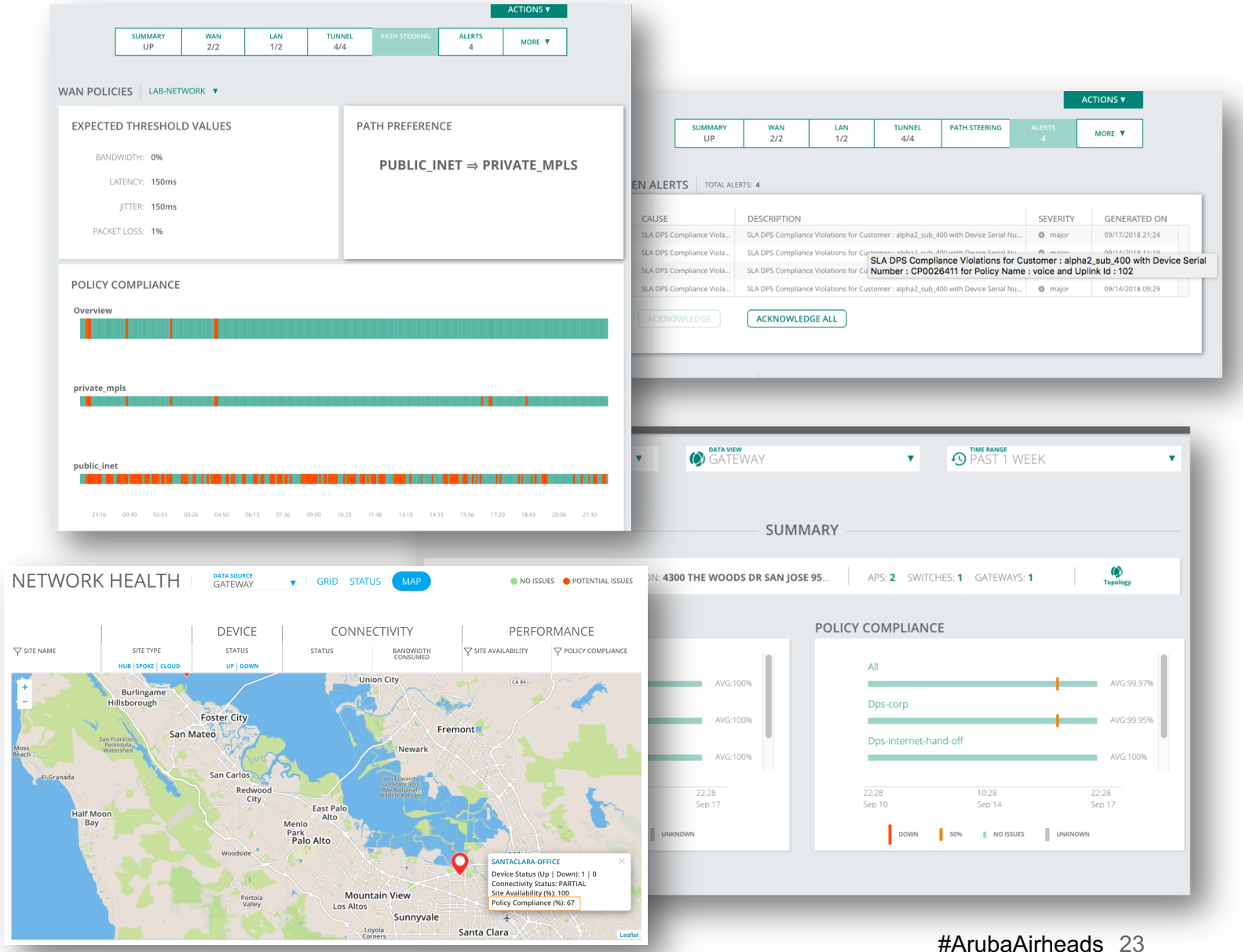
- **View compliance per WAN link**
- **Highlight violations with specific reasons**

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**



AIRHEADS meetup

Goal: Solve the Branch problem, not just the WAN

Simple (at Enterprise scale)
Drive simplicity and fewer boxes in branch solution

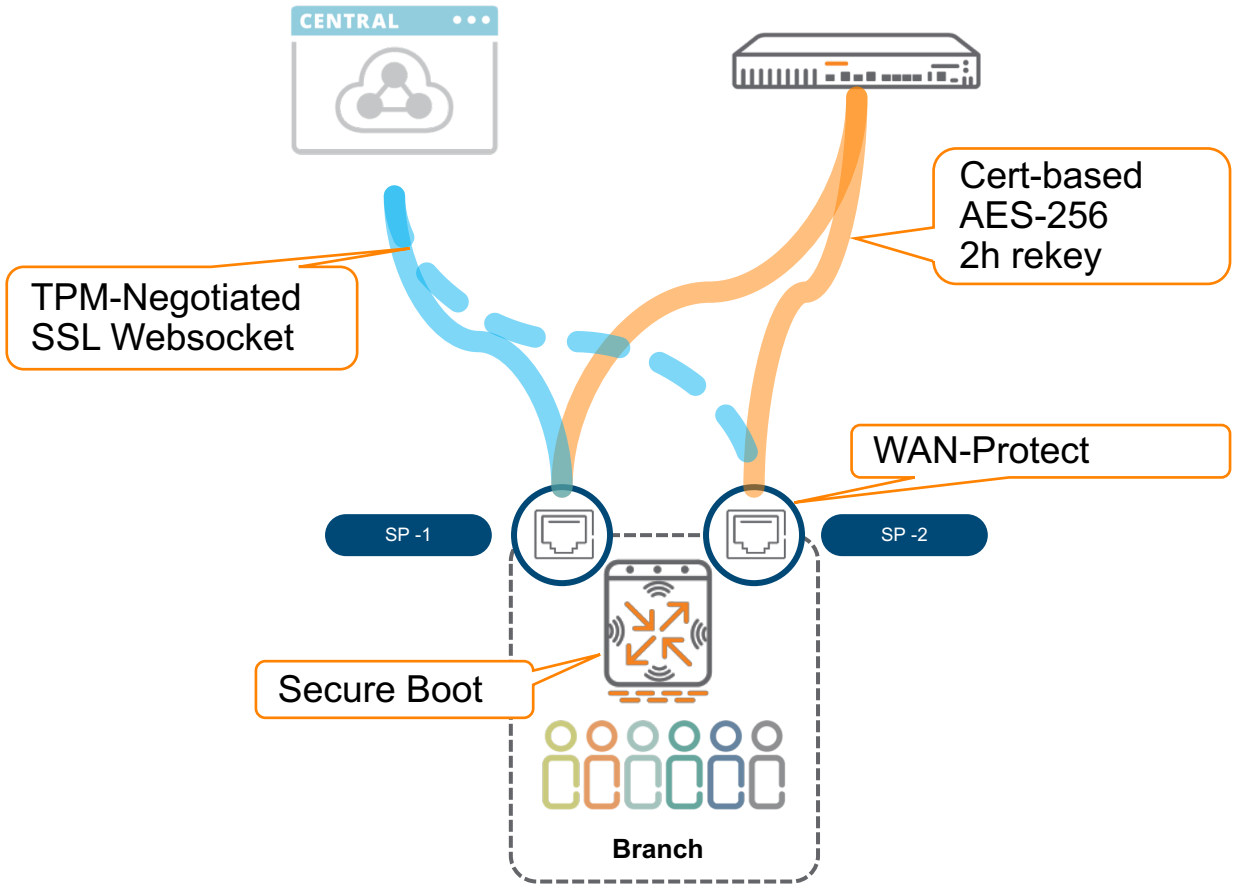
Transport Independency
Own your WAN policy

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



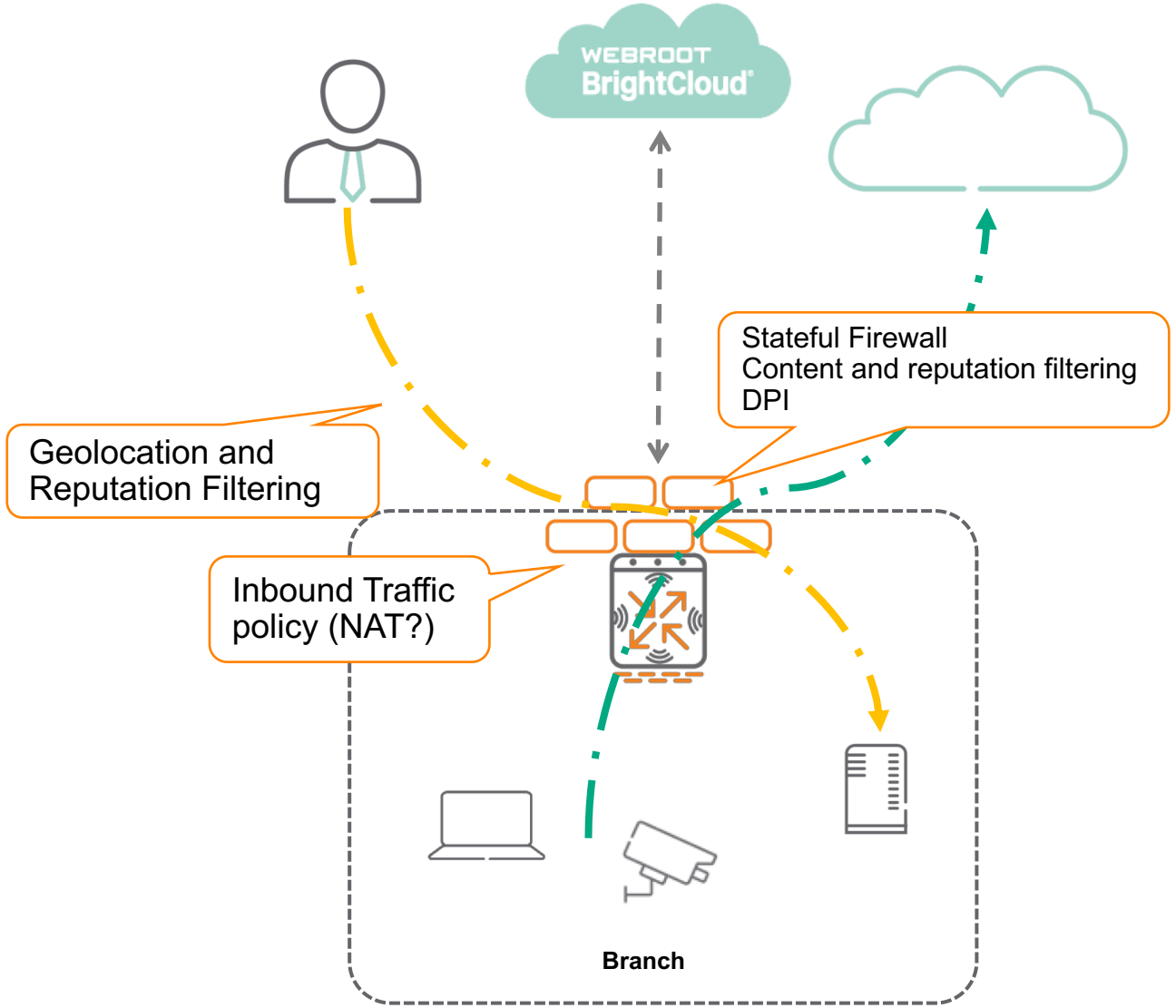
Security Core

AIRHEADS meetup

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



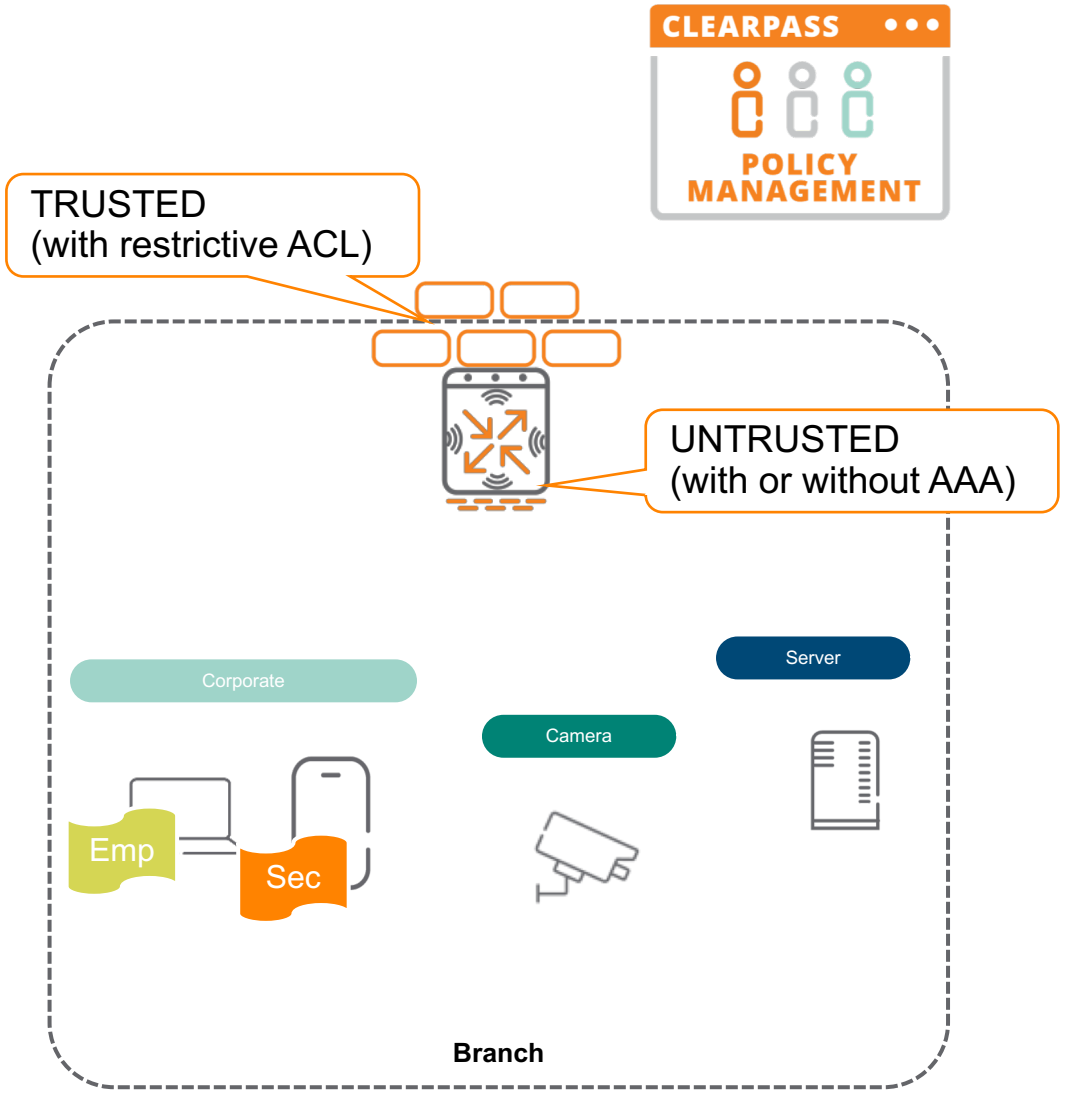
Security Core

AIRHEADS meetup

Role-based Security

Backup

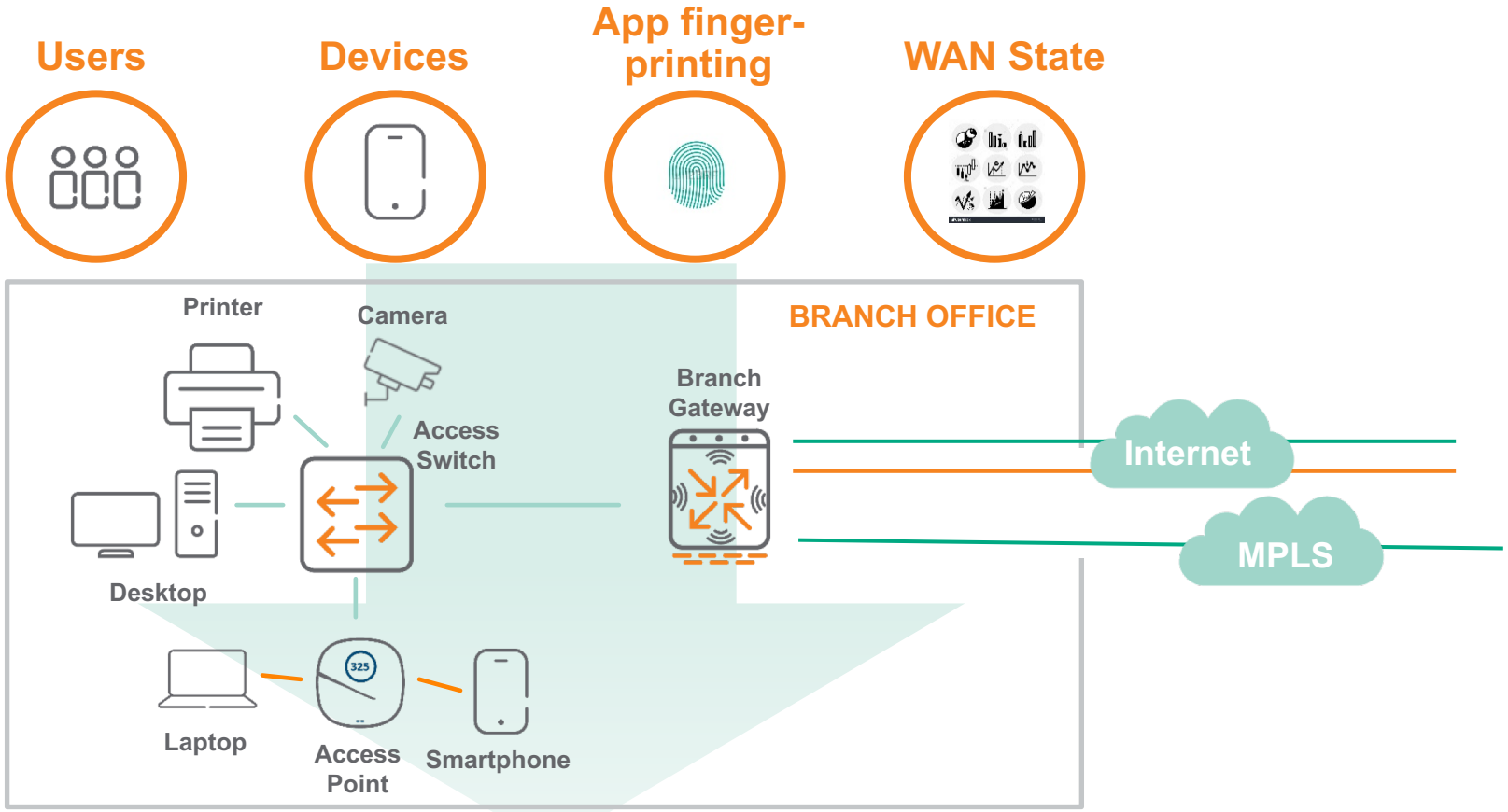
1. ALWAYS set WAN ports to TRUSTED
2. LAN ports should be set to UNTRUSTED
3. Apply AAA profiles to branch VLANs
4. (optional) Set AAA-based enforcement



Security Core

AIRHEADS meetup

Role Based Polices for LAN, Security, WAN

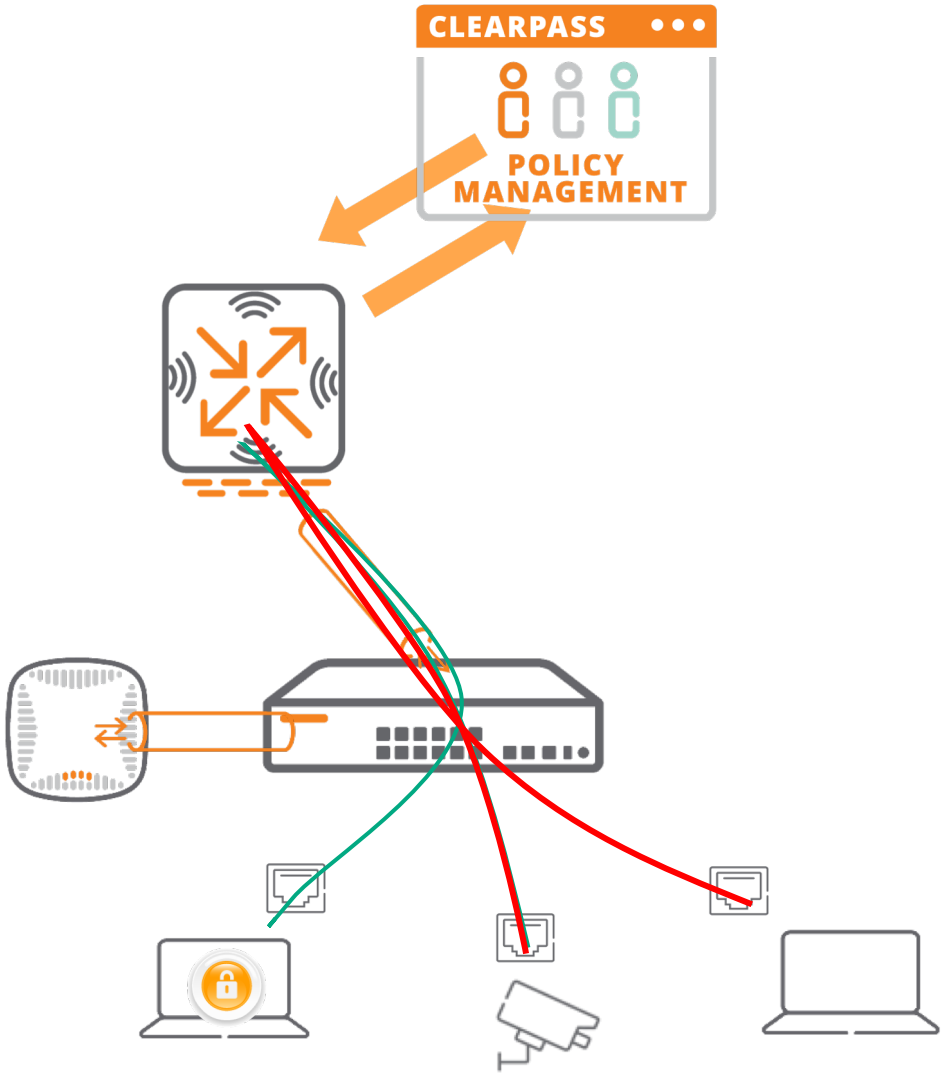


LAN Policies	Security Policies	WAN Policies
WLAN and wired switching policies applied per role. E.g.: Guest SSID, QoS for PCI traffic	Firewall and WebCC policies applied per role. E.g.: WebCC for Guest, PCI traffic isolation	Path steering policies applied per role. E.g.: Guest to Internet, PCI traffic 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



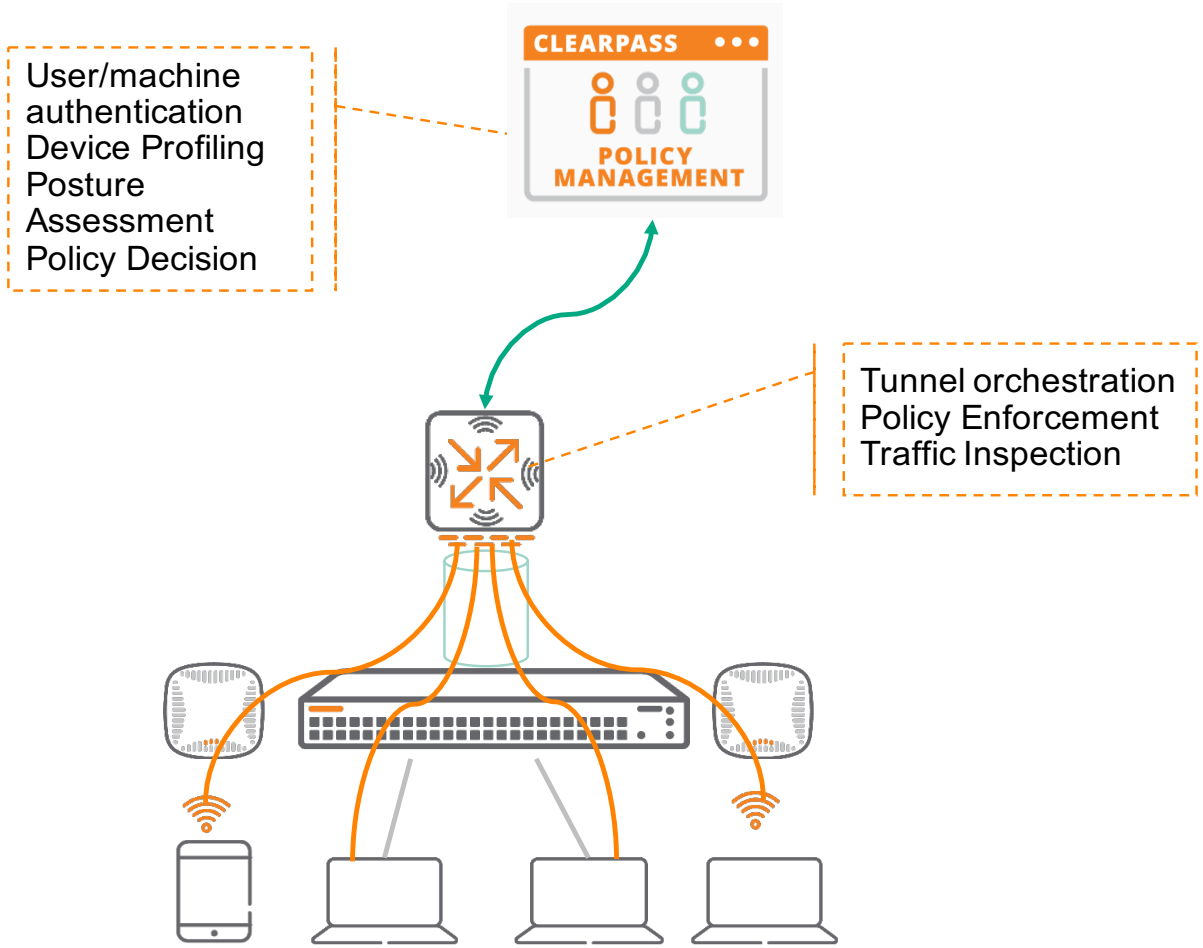
Security Core

AIRHEADS meetup

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

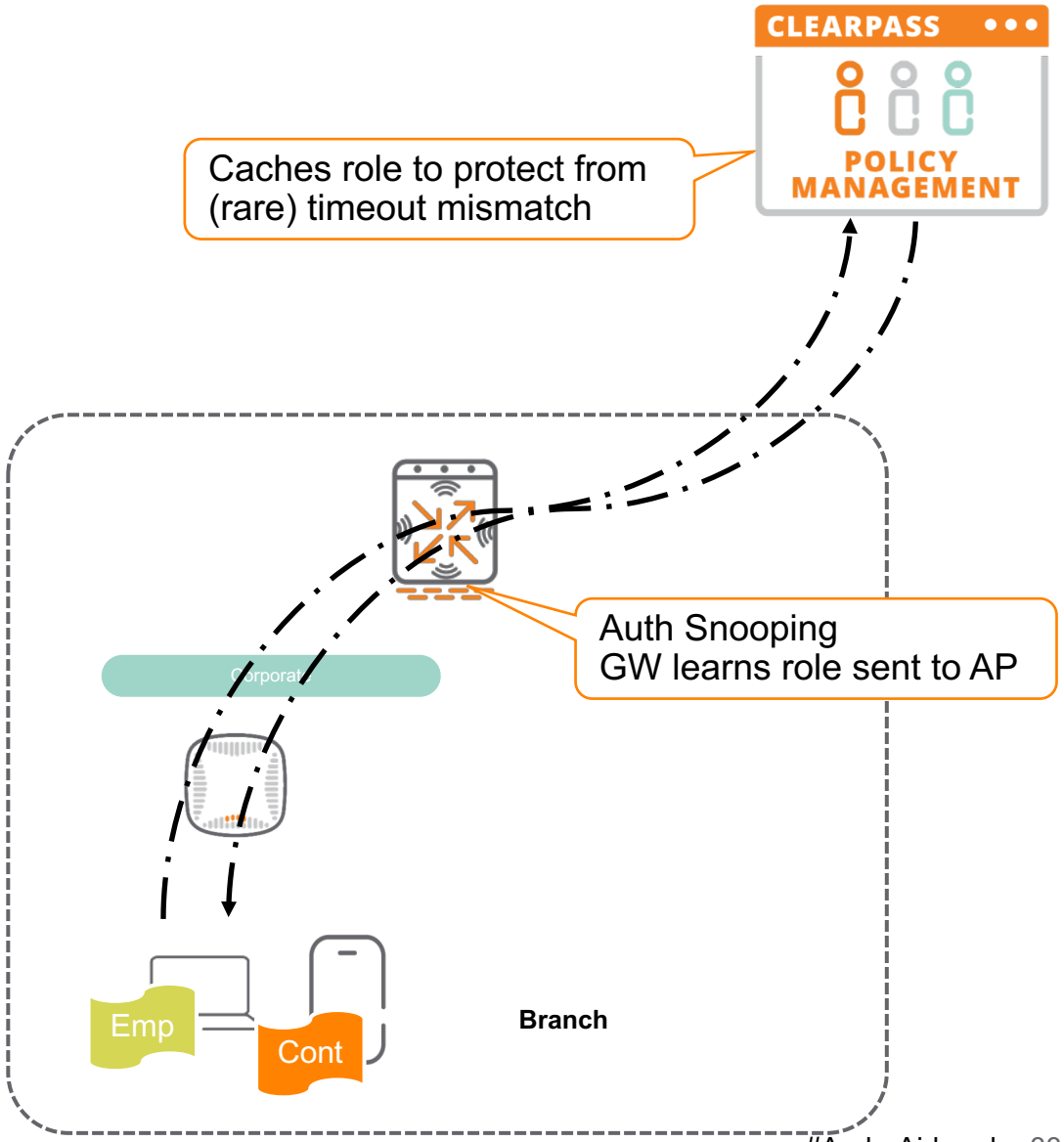
AIRHEADS meetup

Authentication Snooping (stateful-dot1X)

Learning roles from other authentications

Backup

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

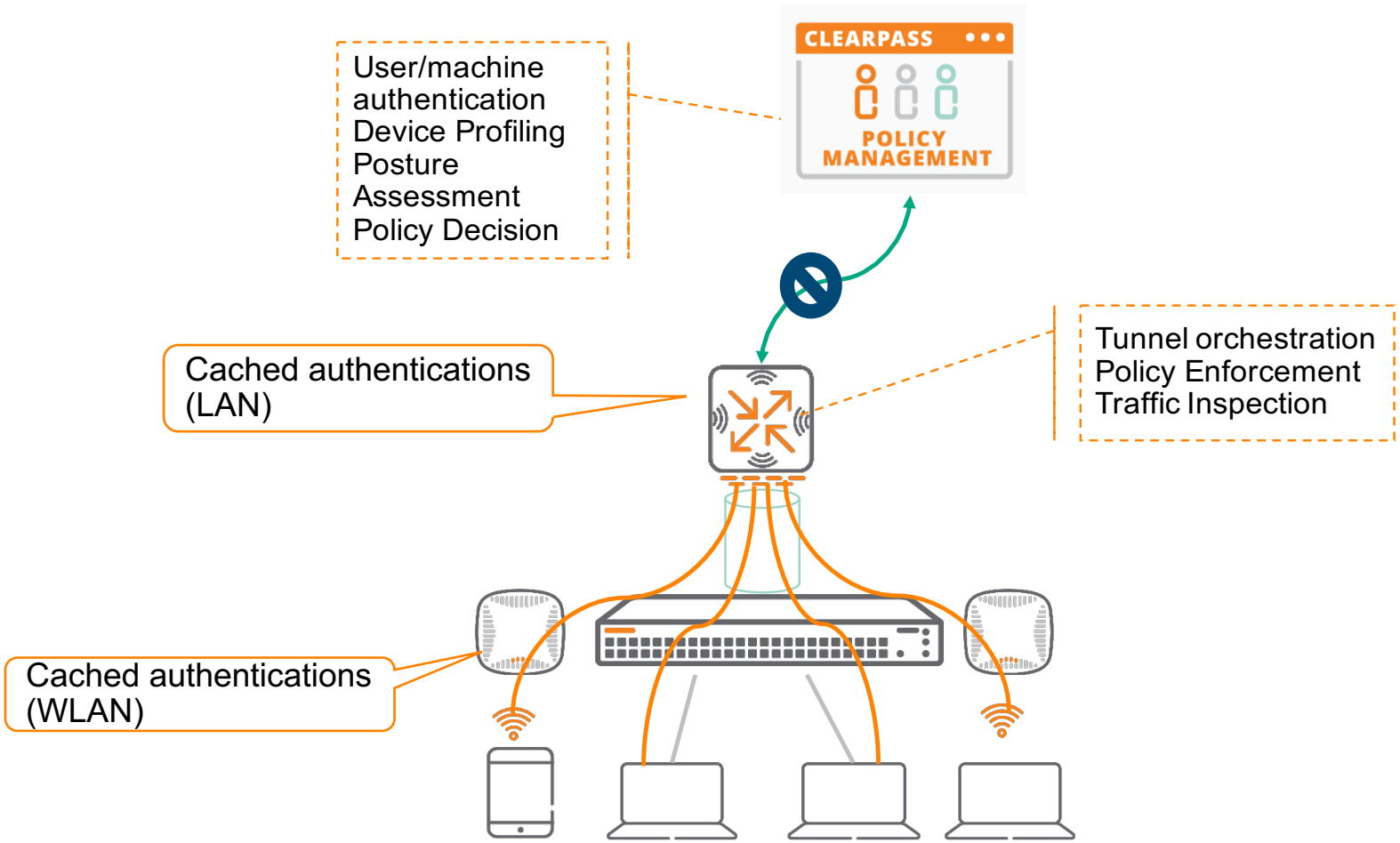
AIRHEADS meetup

Backup

AAA survivability

Controlling the risk…

1. Gateway Caches MAC/EAP-TLS
2. IAP Caches PEAP/EAP-TLS

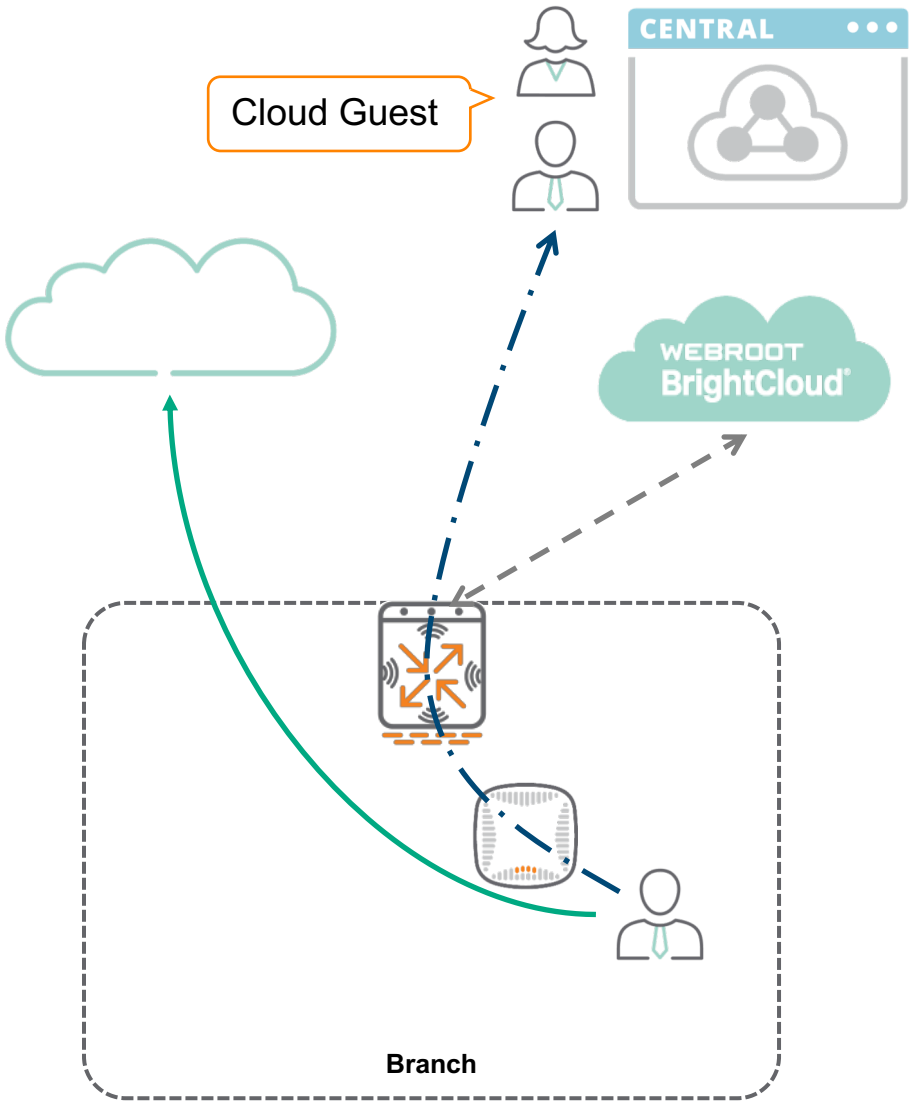


Enforcing L7+ security policies

Guest Access + WebCC

Backup

1. Guest access registration via Central (or ClearPass Guest)
2. Role-based WebCC and reputatlon policy



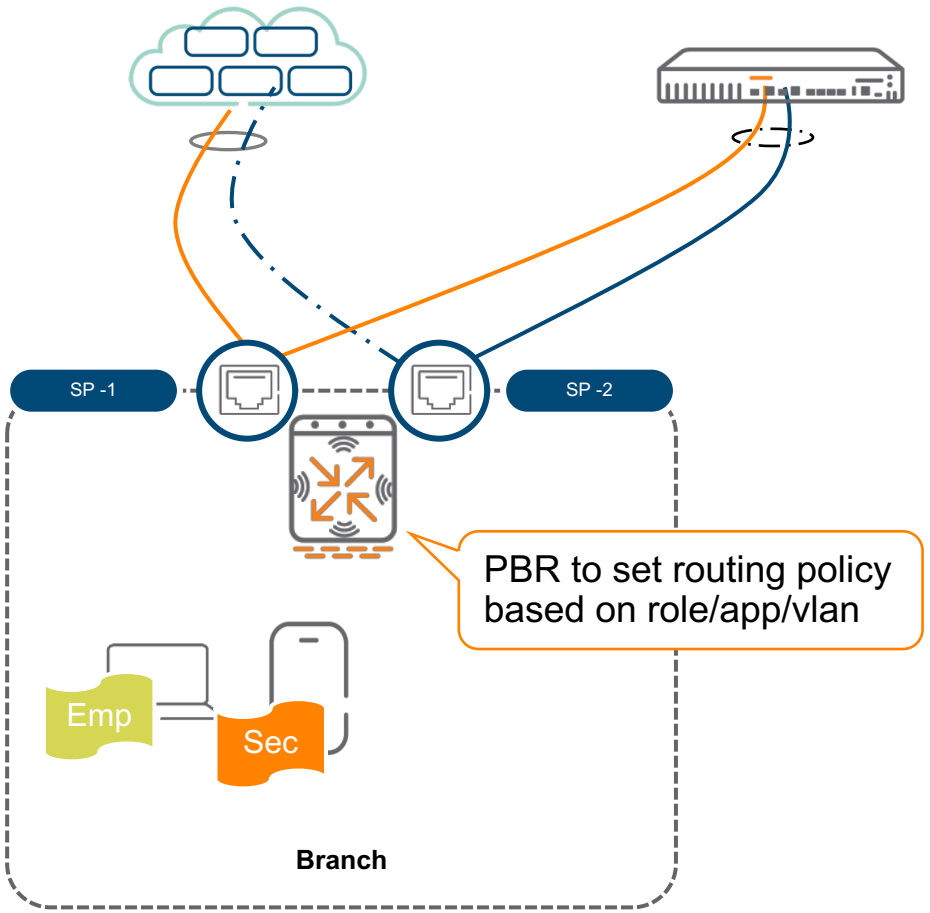
Security Core

AIRHEADS meetup

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

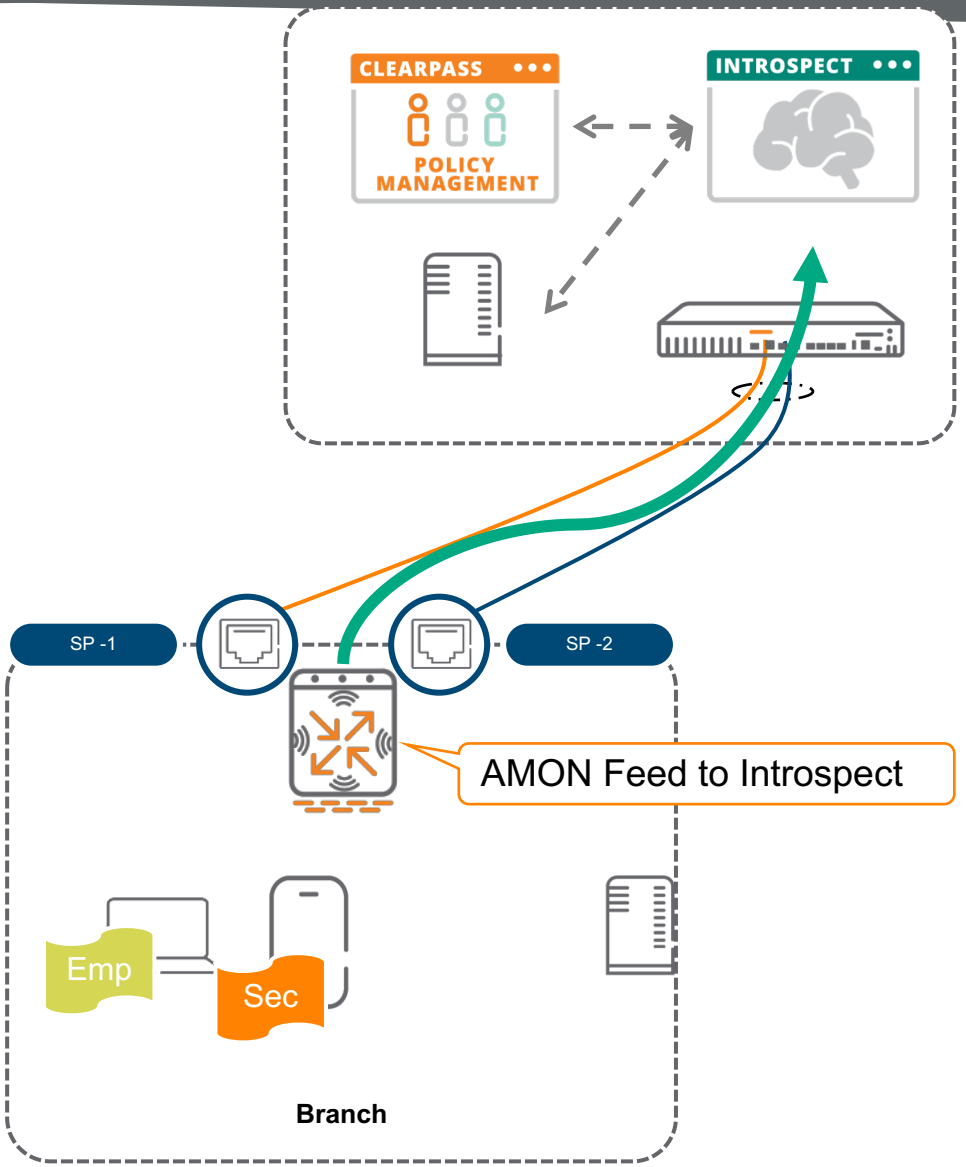
360 Security Exchange Program

AIRHEADS meetup

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

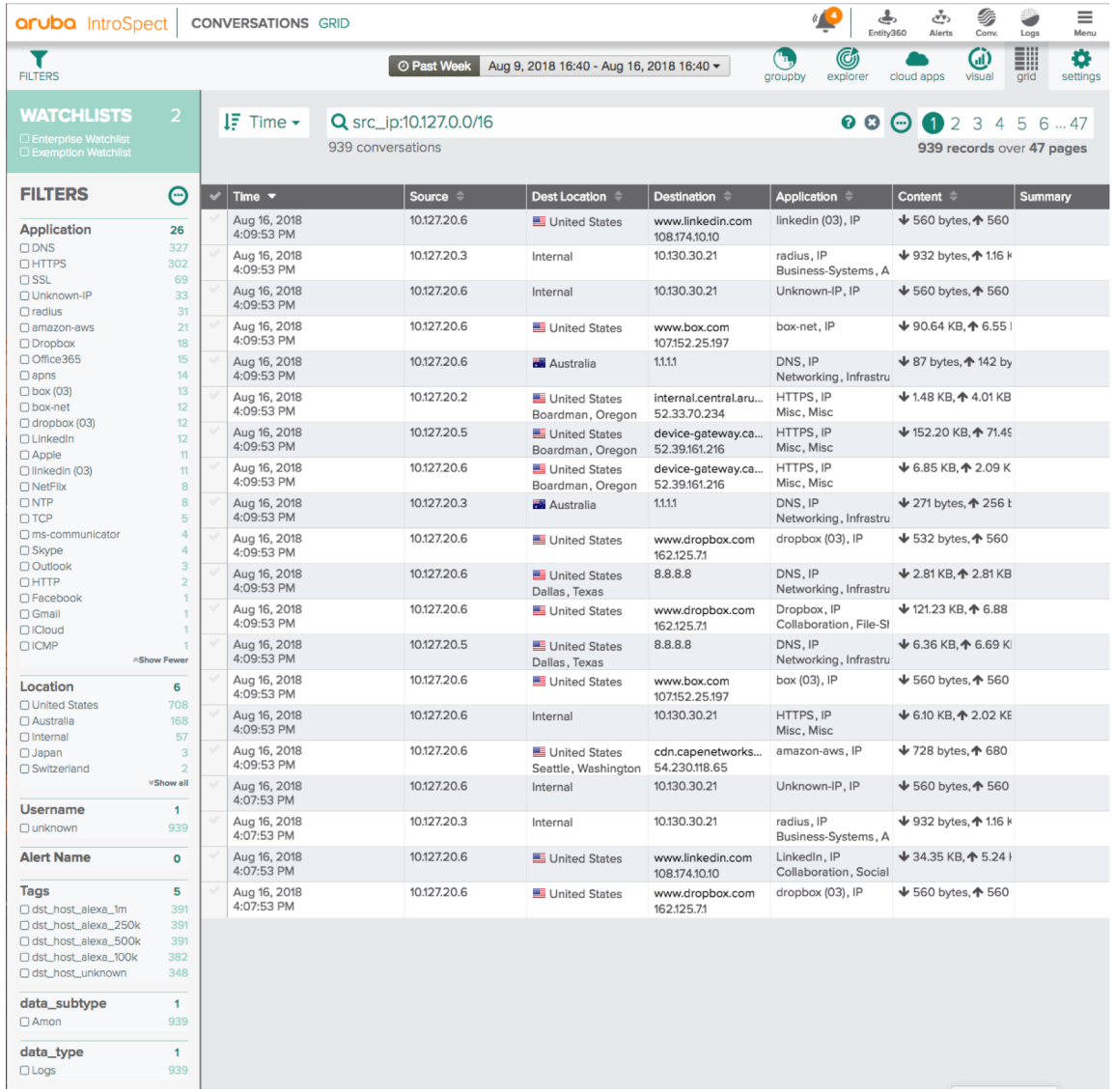
360 Security Exchange Program

AIRHEADS meetup

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

AIRHEADS meetup

Security Layers

3rd Party Security Infrastructure

zscaler

paloalto

Check Point SOFTWARE TECHNOLOGIES LTD.

Advanced threat detection

IntroSpect

Machine learning
Discover, Authorization and Integrated Attack Detection and Response

Aruba Secure Exchange

paloalto, McAfee, airwatch by vmware, Radar, Duo, Carbon Black., ArcSight, LANDESK, ENVOY, Infoblox, okta, Intune, splunk, MobileIron, SendGrid, kasada, servicenow, pagerduty

ClearPass

Device Profiling, Onboarding, Guest…
Zero-trust access control for SD-Branch

Aruba SD-Branch
In-built Role-based security

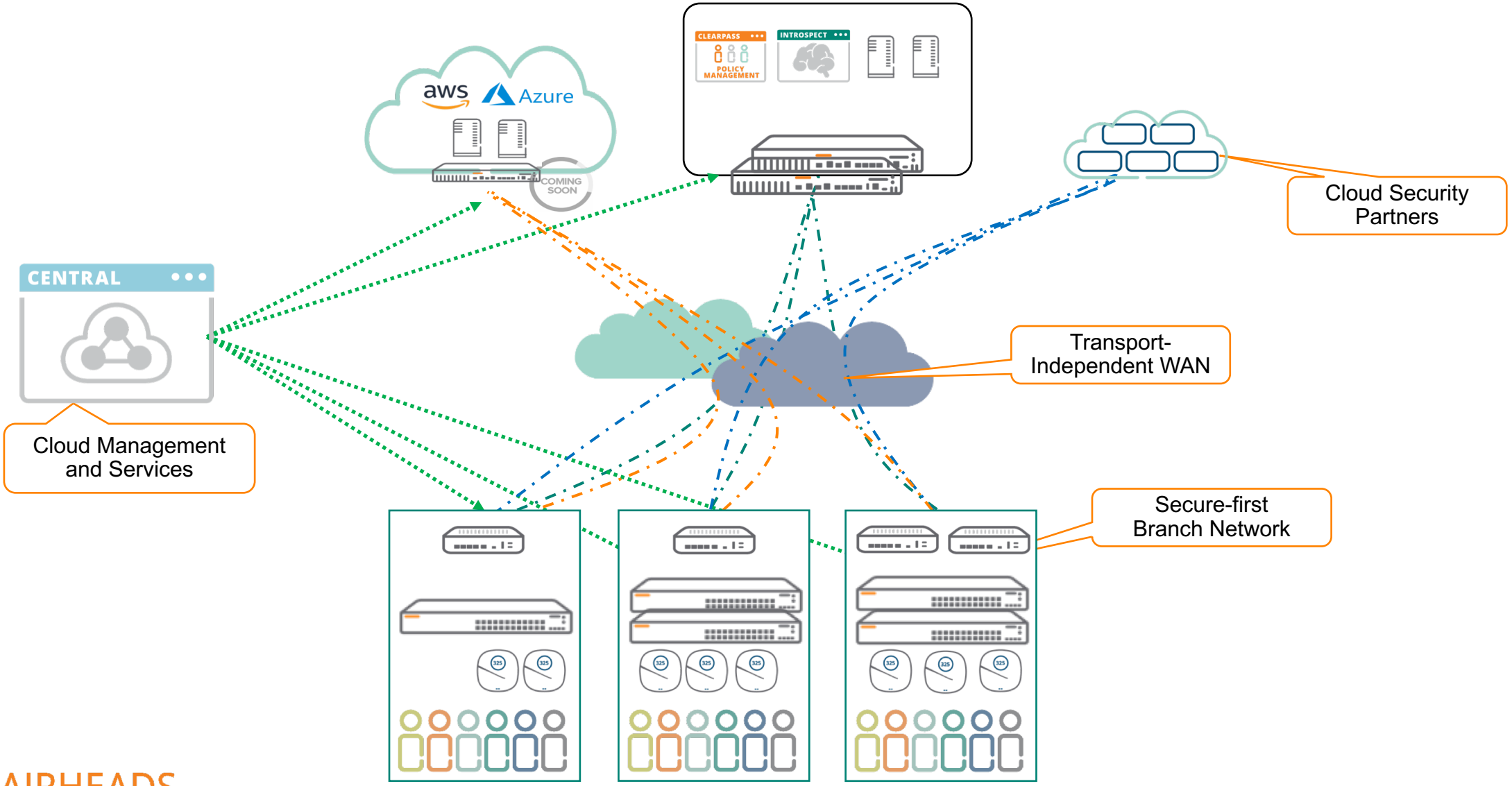
Secure Boot | Encryption | DPI | VPN | Firewall | Web Content and reputation filtering

Security Core

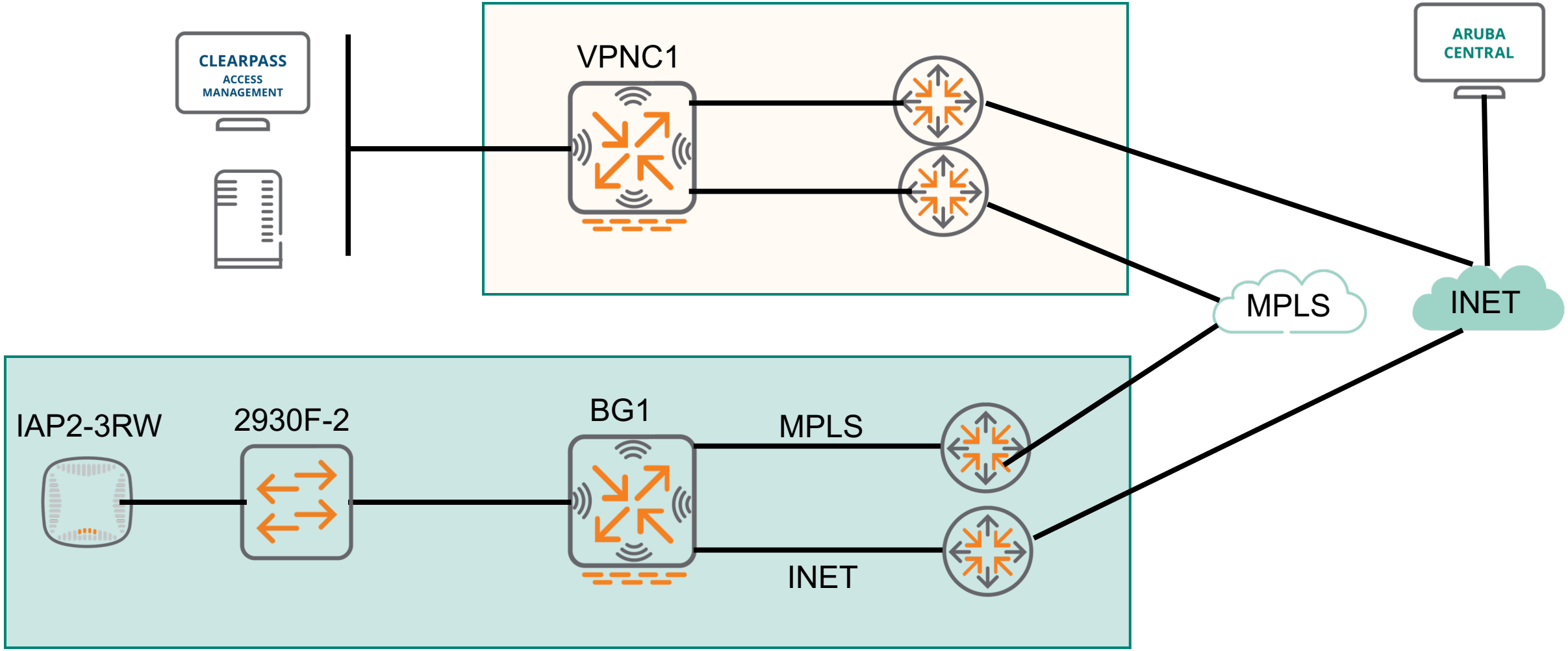
360 Security Exchange Program

AIRHEADS meetup

Aruba SD-Branch solution



Demo


CLEARPASS
ACCESS
MANAGEMENT
VPNC1
ARUBA
CENTRAL
MPLS
INET
IAP2-3RW
2930F-2
BG1
MPLS
INET

aruba
a Hewlett Packard Enterprise company

AIRHEADS meetup

Thank You