DWF-GEN-4 - Introduction to Aruba SD-WAN Branch solution

Marius Venter
EMEA WIN Team
Consulting Systems Engineer

ABSTRACT

Join this session if you want to understand what ARUBA is delivering in the connected Branch and how you can leverage product today to deliver Branch WAN solutions. This session will look into the phases of how you can migrate of the typical CPE routing to a new age SDBRANCH solution today. This session will also address future looking statements as well as address management strategies.

Agenda:

1) What
2) Why
3) Where
4) When
5) How

Emergence of SD-WAN

Branches still Complex, Expensive and Slow

- Lacks automation, central management
- Endpoints going mobile and untrusted
- Increasing branch traffic to/from Internet destinations
- VPN links expensive, long set-up times, may need multiple providers across multiple geographies
- Internet links “good enough” for most applications

SD-WAN

- The use of software technologies to simplify the problem of interconnecting branches to the enterprise
- Benefits: Faster turn up, higher reliability, lower cost, simpler management

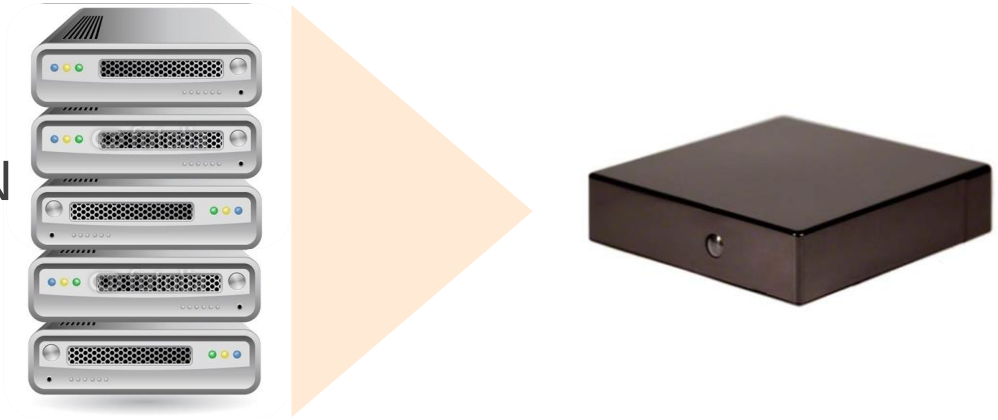
Solve the Branch problem, not just the WAN problem ….

- The Branch needs at least 5 sets of services:
  - WLAN
  - Wired Switching
  - Policy Enforcement & Services
  - WAN Interconnect
  - Basic Firewall
- Provide a simple solution offering all services, must involve same or fewer boxes in the branch
- Common Policy and Management for campus and branch, wired and wireless
- Multiple deployment models: On premises, public cloud, private cloud, managed service offering
- Multiple purchasing models: Perpetual, Subscription

“Branch-in-a-Box”

ALL IN ONE BLACK BOX

Consolidate as many services into a single box for LAN, WLAN and WAN services



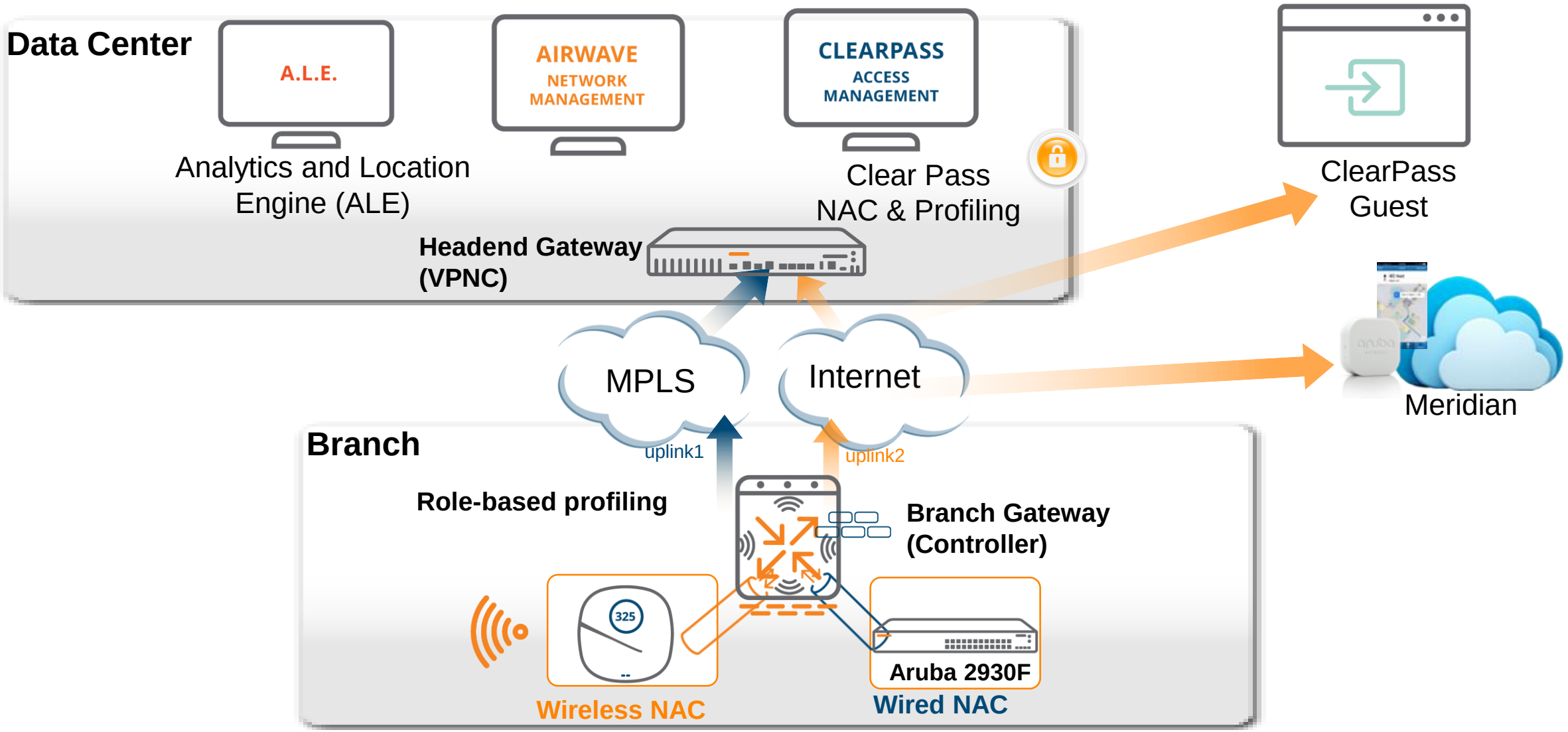
SECURITY

Segmentation for compliance

SIMPLICITY

Zero-touch deployment and ease of use

Solution Components



Flexible Branch Deployment Options

Micro Branch with RAPs

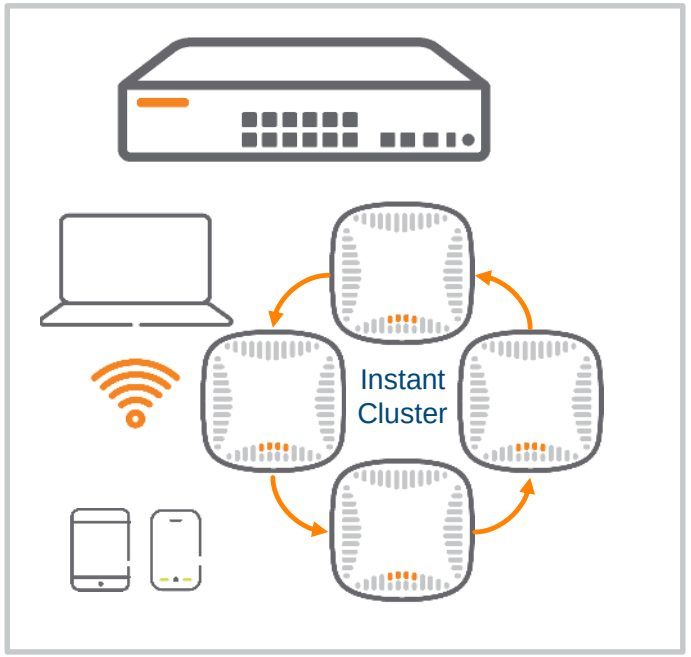
Basic WAN

RAP connected to WAN uplink

100,000s Branches Deployed

Small to Mid Branch with IAPs

Basic WAN

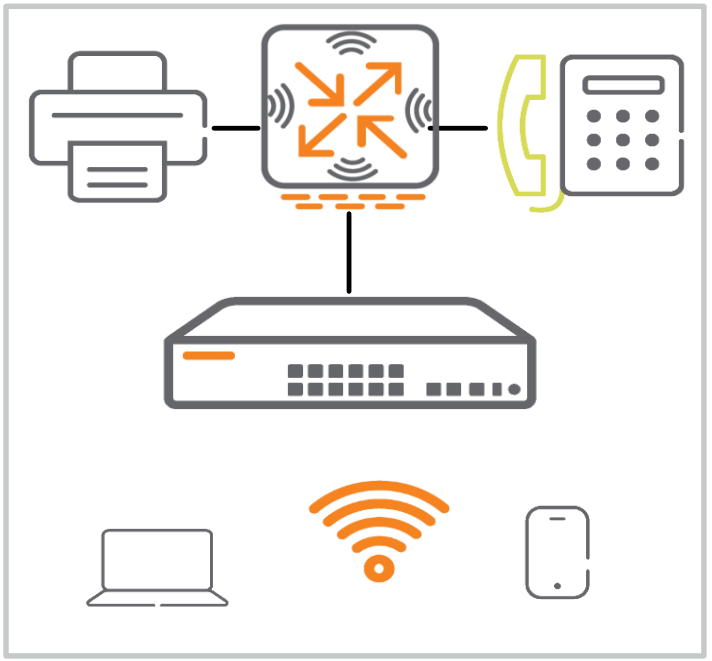


Instant AP cluster connected to a 2930F switch

10,000s Branches Deployed

Large to Mid Branch with Gateway

Advanced WAN



7000 series Branch Controller connected to WAN uplinks, with 2930F and AP's

1000s of Branches Deployed

Enterprise Class, One Network and Policy Management Platform

SD-WAN Solution Building Blocks

Ease of Provisioning & Management

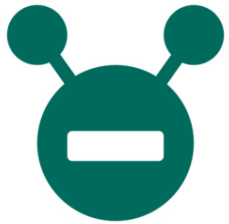
Secure ZTP, Central Management (Cloud)

Dynamic Path Steering

Policy aware application routing, Performance Routing

Secure Overlay

IPsec VPN tunnels, Mesh

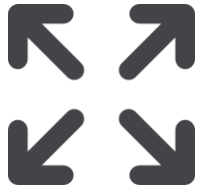


Secure Branch

Firewall, Web CC

App Visibility

DPI, WAN links, AppRF

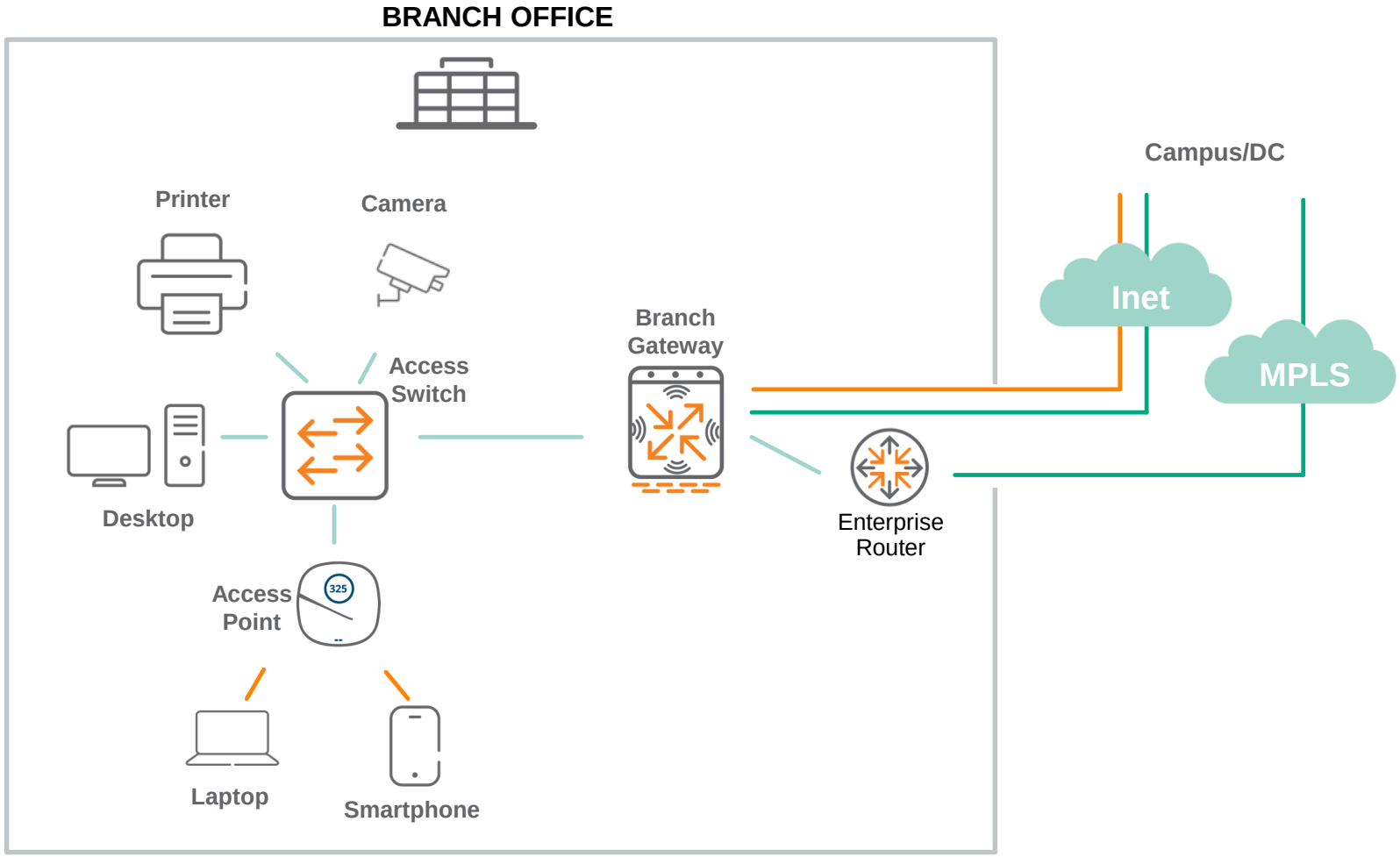


Deployment Flexibility

Multiple WAN uplinks, Routing, Segmentation

Branch 2.0 Architecture

Phase 1: Branch simplification – Managed Branch

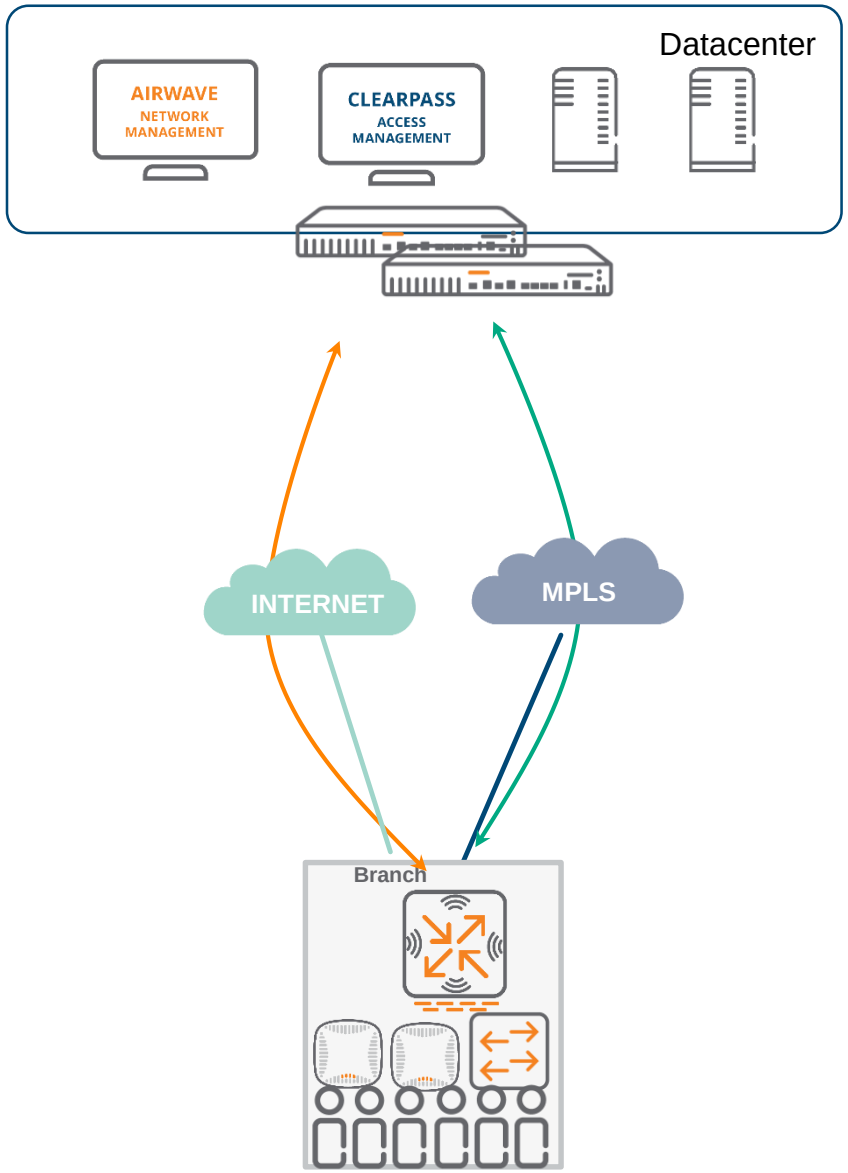


Managed Branch

- Collapse WAN, WLAN/LAN services into Branch Gateway
- Central Branch Management, including WAN and LAN
- Offer Firewall, Security, SD-WAN capabilities, basic Compression
- Augment cost-effective and higher bandwidth Broadband links
- Context-aware application routing to intelligently steer traffic

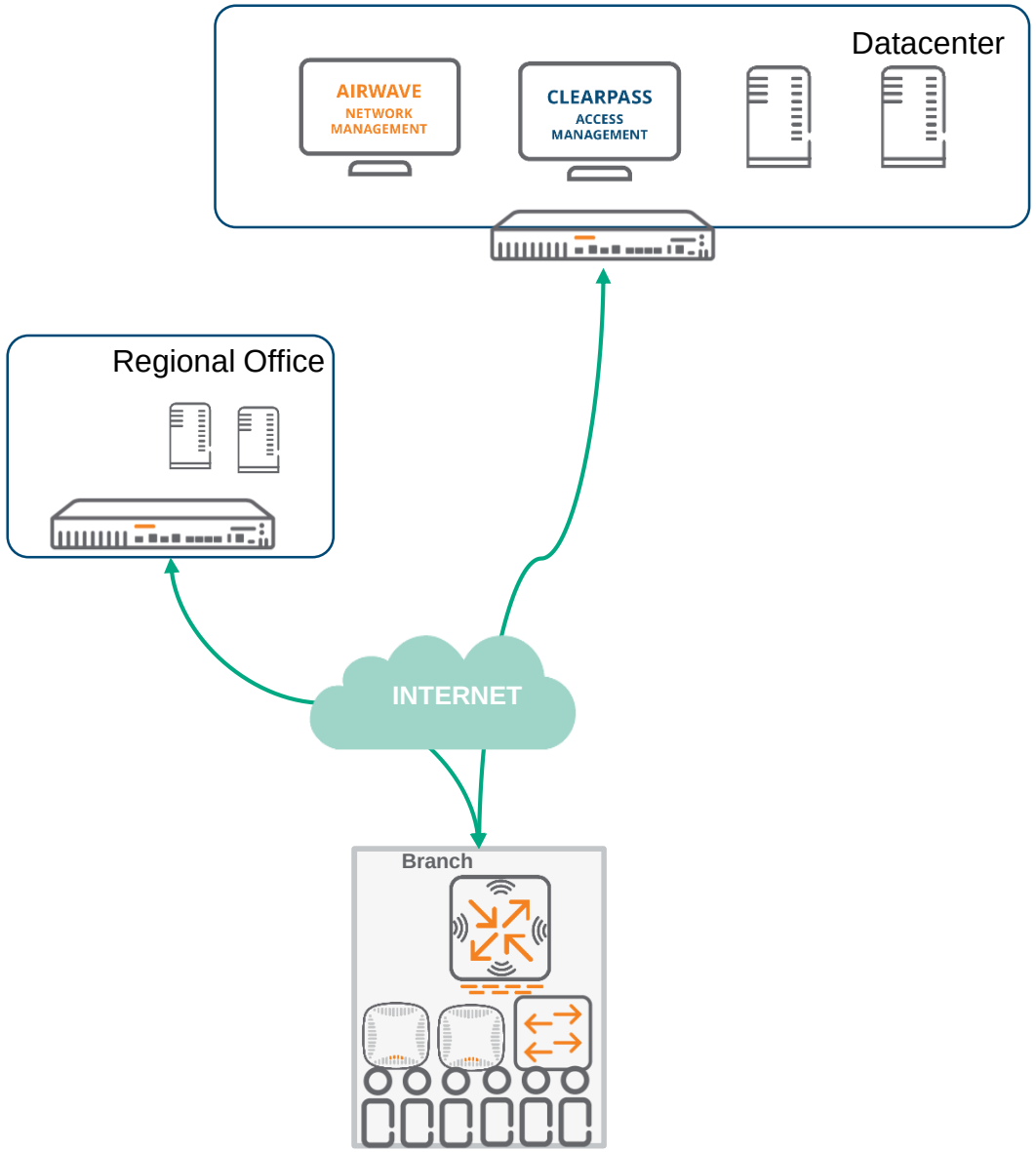
Smart WAN

- ✓ WAN Optimization
  - ✓ WAN Compression
  - ✓ Role based routing
- ✓ **Public line as backup of MPLS**



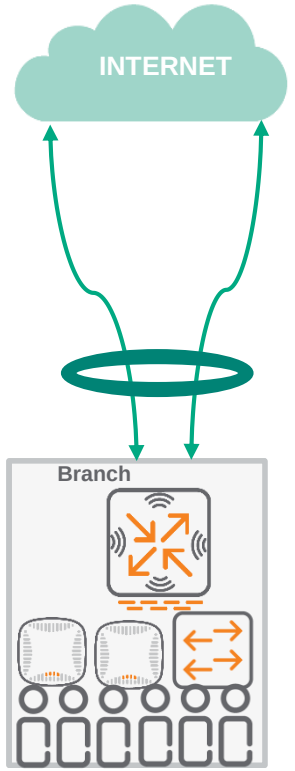
Smart WAN

- ✓ WAN Optimization
  - ✓ WAN Compression
  - ✓ Role based routing
- ✓ Public line as backup of MPLS
- ✓ **Automatic tunnels with regional offices/datacenters**



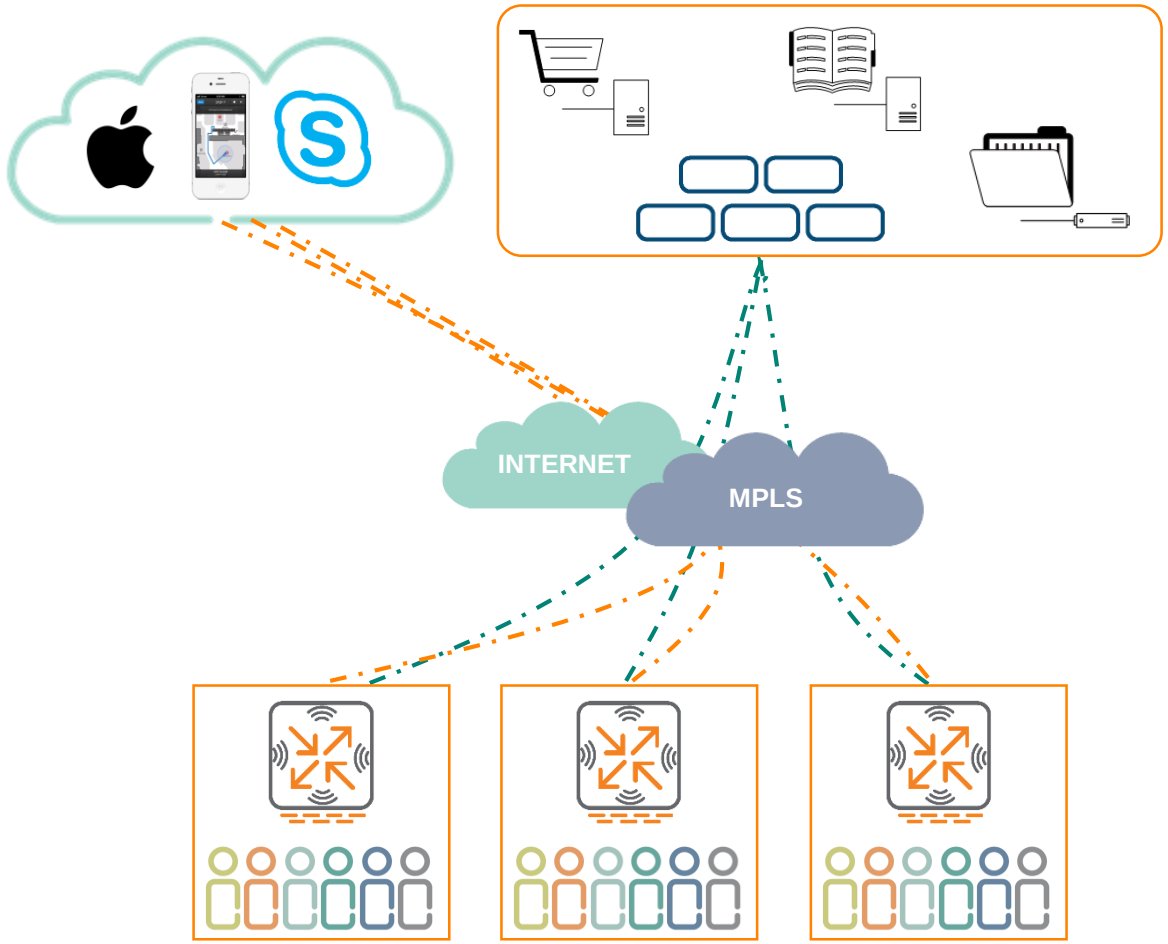
Smart WAN

- ✓ WAN Optimization
  - ✓ WAN Compression
  - ✓ Role based routing
- ✓ Public line as backup of MPLS
- ✓ Automatic tunnels with regional offices/datacenters
- ✓ **Line load balancing**



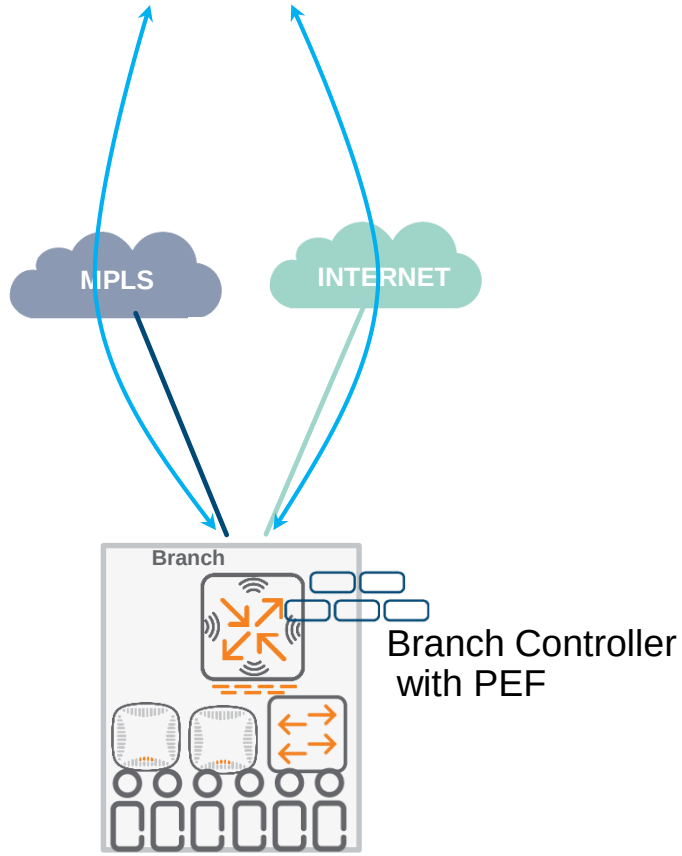
Smart WAN

- ✓ WAN Optimization
  - ✓ WAN Compression
  - ✓ Role based routing
- ✓ Public line as backup of MPLS
- ✓ Automatic tunnels with regional offices/datacenters
- ✓ Line load balancing
- ✓ **User-Centric Security and routing**

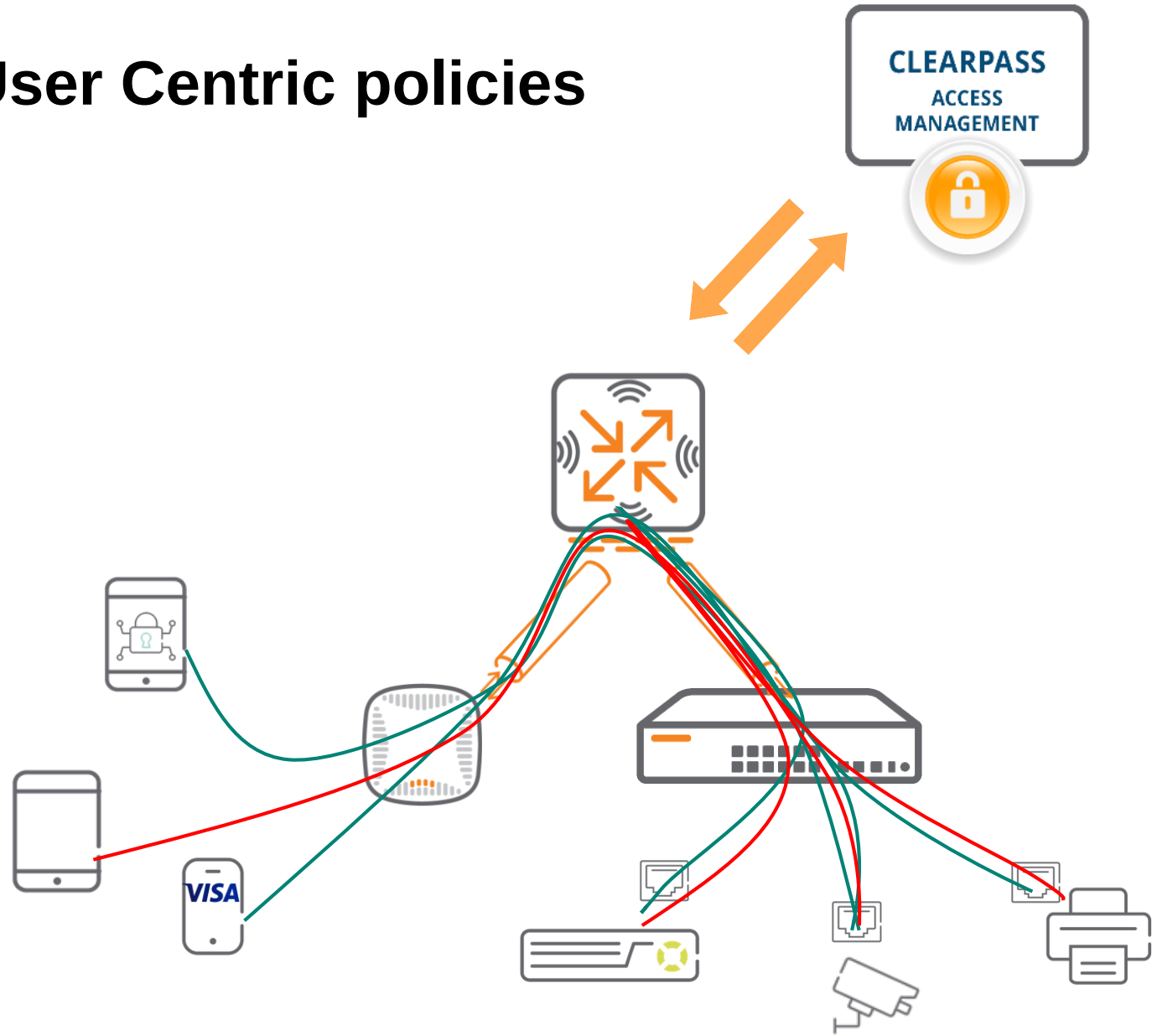


Branch Gateway becomes a Policy Enforcement point

- Device Fingerprinting
- Role Assignment based of Device ownership, VLAN, Policy
- Application Identification
- Application of QOS policies, per role, per application
- Policy definition for Web traffic based of IP Reputation, Geo or Web Category
- Context-Aware Routing and Application Path Steering

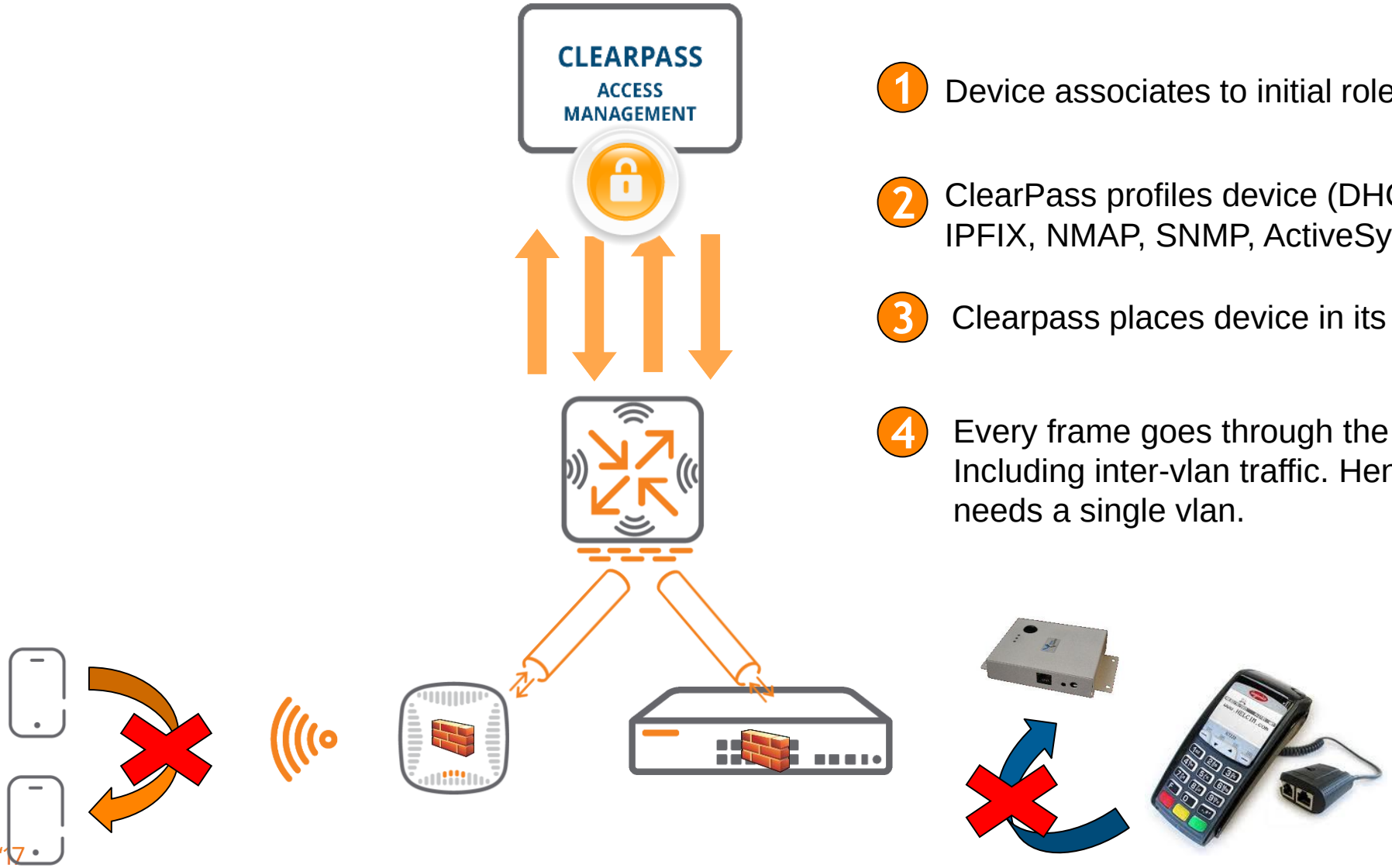


User Centric policies



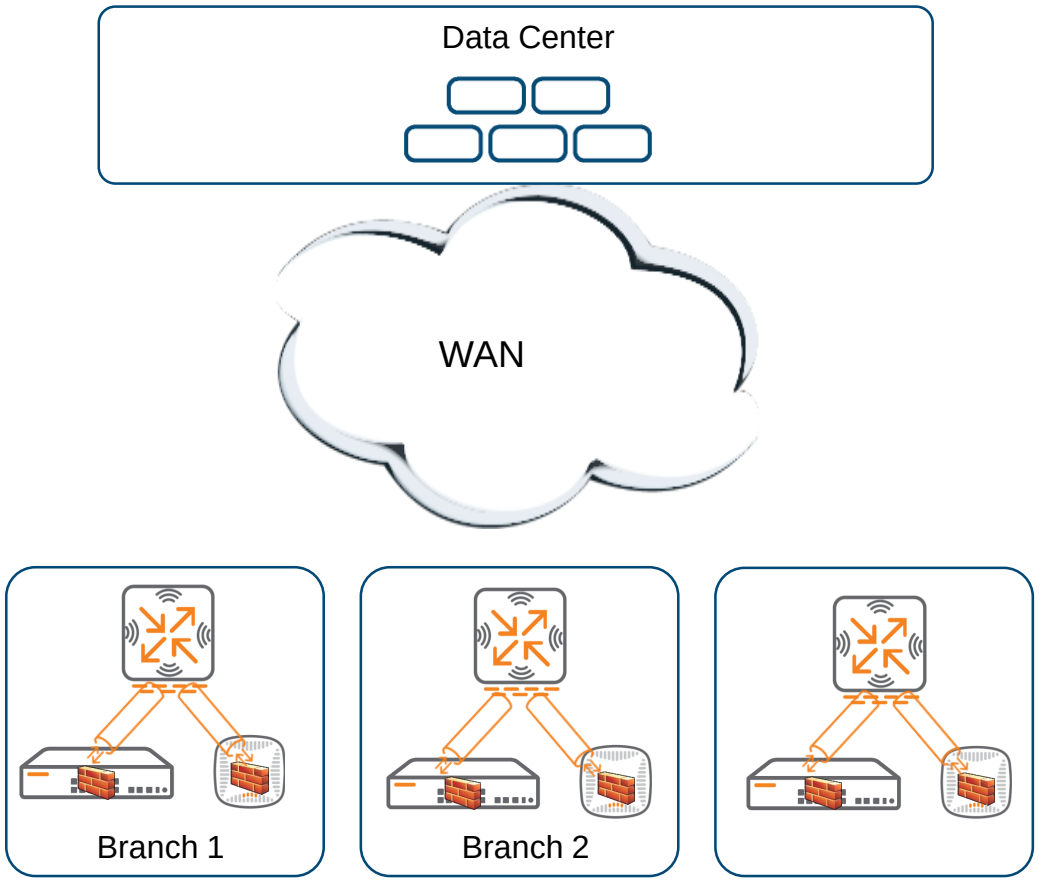
1. Device associates to initial role
2. ClearPass profiles device (DHCP, IF-MAP, IPFIX, NMAP, SNMP, ActiveSync…)
3. Clearpass places device in its role
4. Every frame goes through the firewall. Including inter-vlan traffic. Hence, only needs a single vlan.

Classify User and Devices into Roles



1. Device associates to initial role
2. ClearPass profiles device (DHCP, IF-MAP, IPFIX, NMAP, SNMP, ActiveSync…)
3. Clearpass places device in its role
4. Every frame goes through the firewall. Including inter-vlan traffic. Hence, only needs a single vlan.

Apply LAN, WAN Policy based on Roles

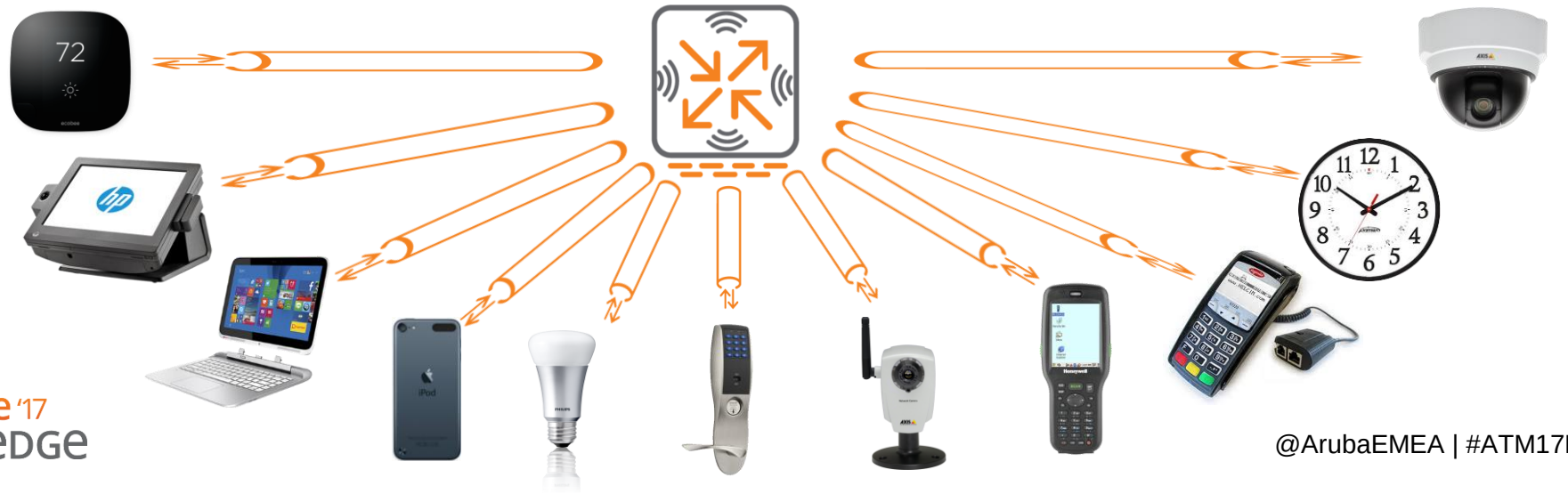


Aruba Branch Controllers in each location with switches working in tunneled-node configuration.

- All LAN/WLAN/WAN security policies enforced in the controller
- Role based access for granular policy enforcement without vlan explosion
- Role based routing for simplified routing and isolation of non-corporate networks (ie. guest WLANs)

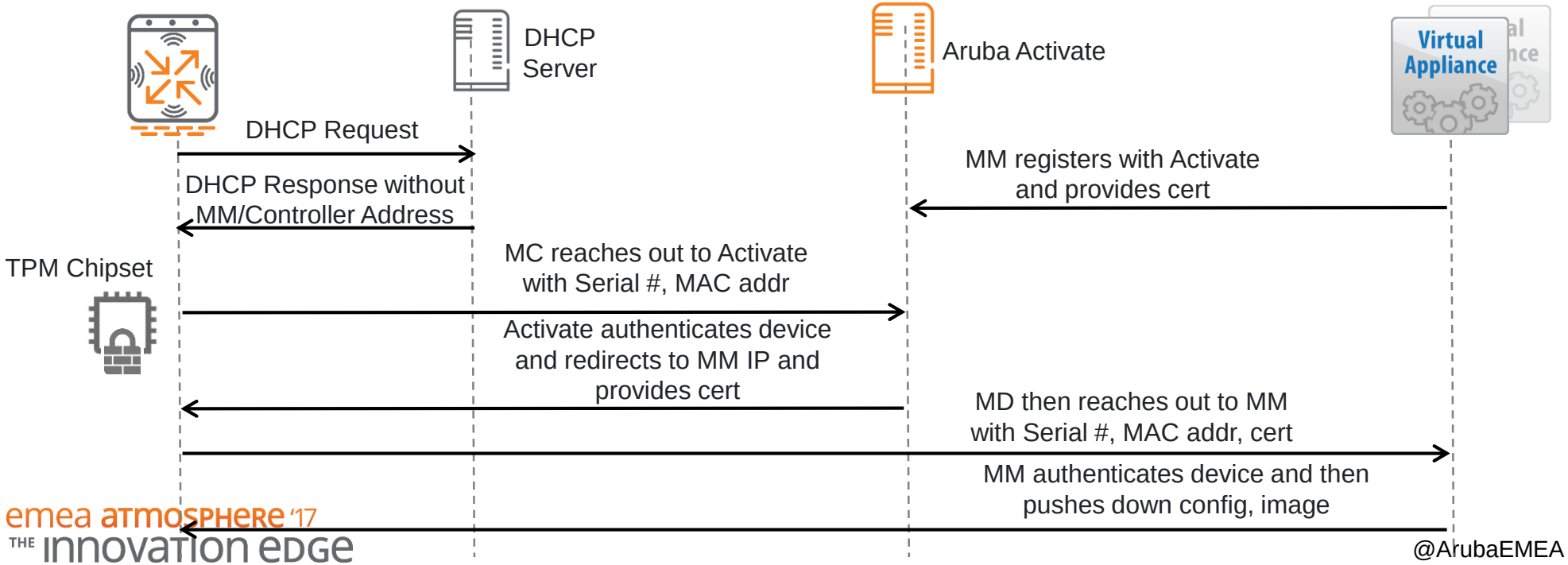
User centric design advantages

Traditional access	Role based access
Intra-vlan communication is allowed	Policy denies intra-vlan communication
VLAN is assigned only once (manually)	Continuous profiling
VLAN assigned based on physical port	Role assigned based on AAA & Profiling
New services requires new VLAN deployment	Faster new services deployment (ZTP)
Ports are default-open, accidental access is possible	All ports are secured



ZTP for secure and fast new branch deployment

Complete Trust	Zero Touch	Scale
Secure Onboarding with embedded TPM chip on all Aruba devices	Ease of use, Zero touch to provision remote Branch	Create Bulk Policy Template to push to Branches



Deep Application Visibility with AppRF

Incorporates Next-Generation Deep Packet Inspection technology

- Uses advanced techniques for application ID, significantly more accurate than old-school signature approaches
- Over 2600+ Applications

Operates at user role level to provide application control

- Block application
- QoS application at L2 or L3
- Bandwidth contracts (uncommitted for v1)

Secure Overlay with IPSec VPN

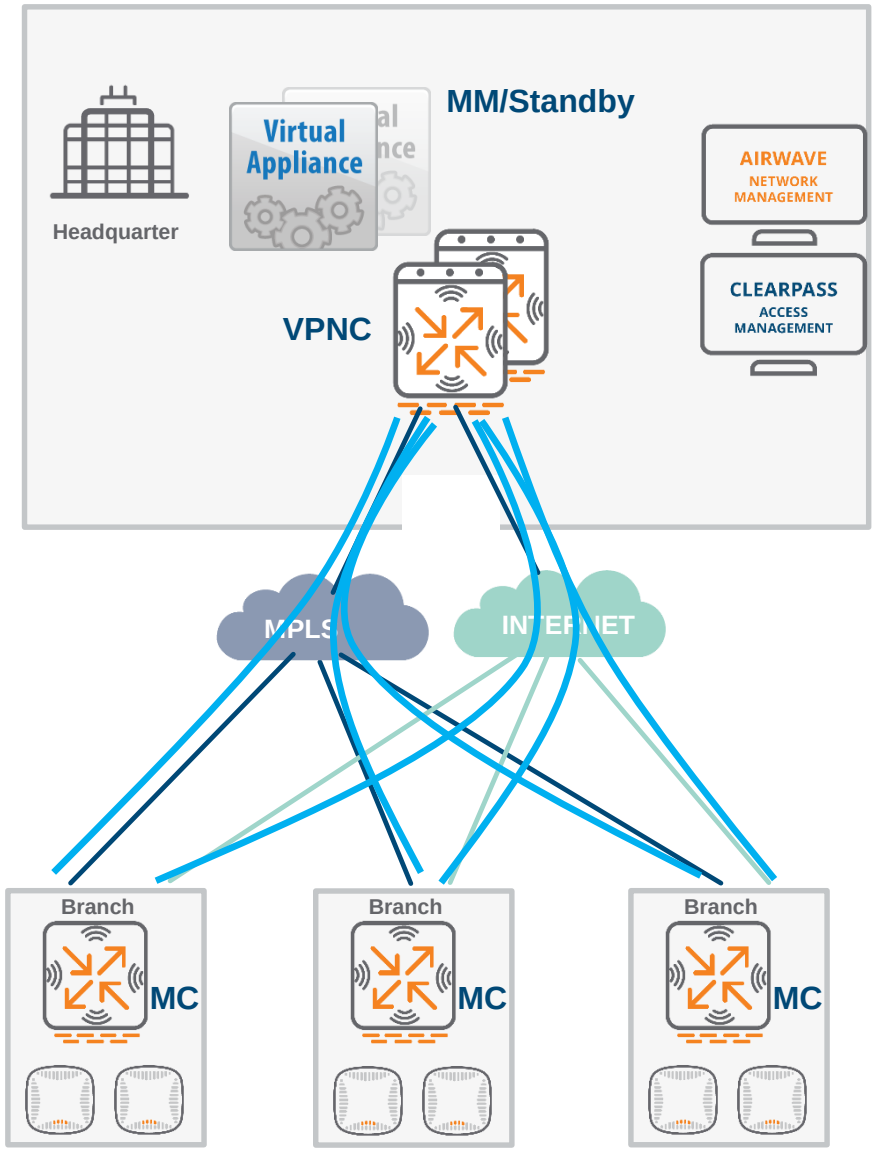
Secure Overlay setup over any access - MPLS or Internet (Cable, DSL, 4G)

Certified Strong Encryption like FIPS

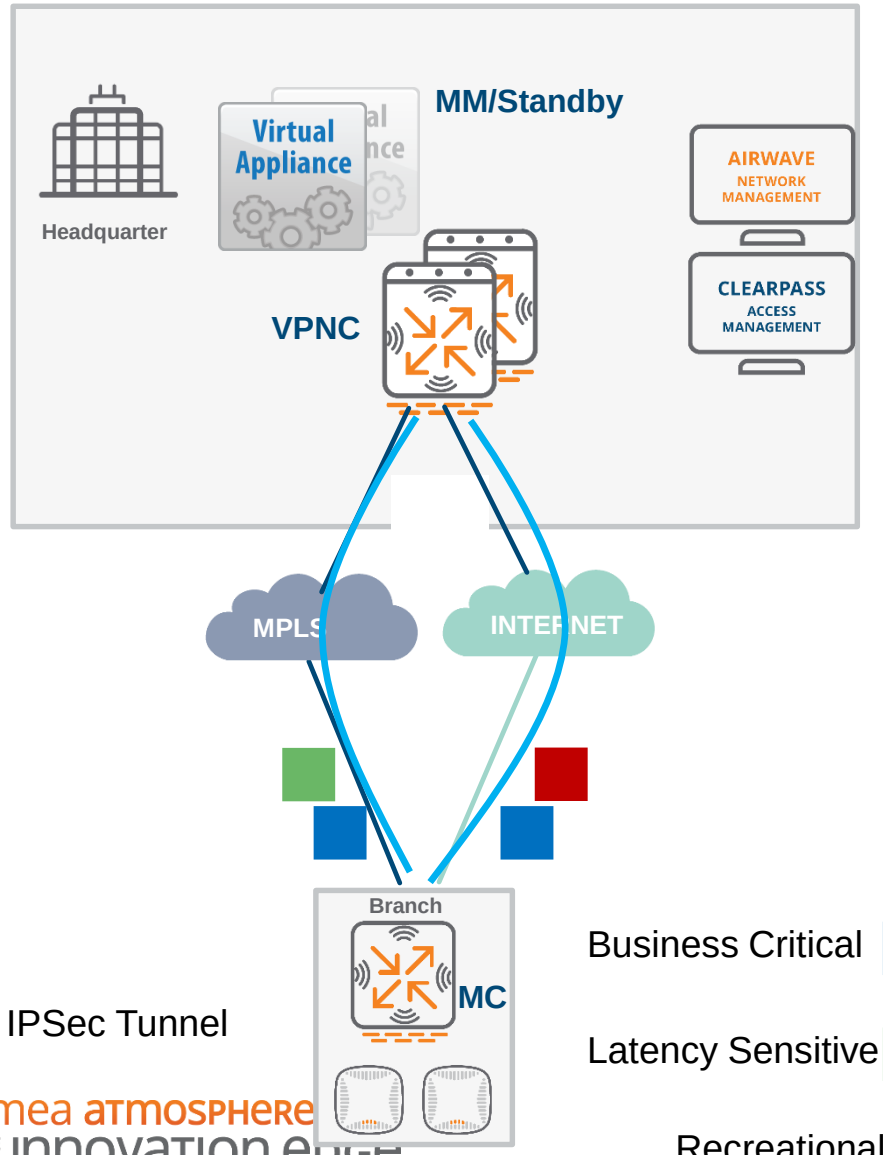
PSK or PKI based VPN setup

Routing overlay with OSPF and Static Routing

Zero Hub configuration when newer Spokes are added*



Context-Aware Path Selection



Policy based Path selection based of

- Applications
- Roles, VLANs

Global Load Balancing based of:

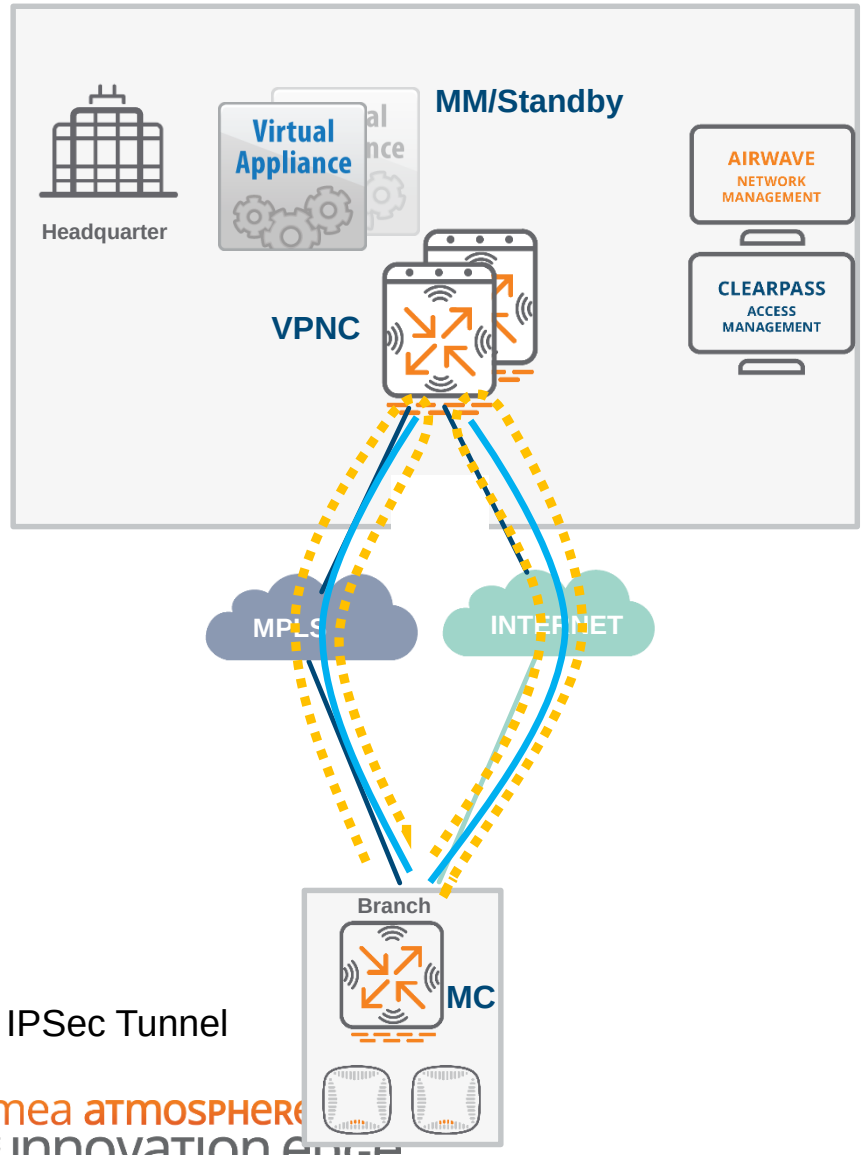
- Round robin (default)
- Hash
- Session count
- Uplink utilization

Uplinks can be configured Active-Active or Active-Backup

Added WAN Compression capability

Business Critical	Office 365 SAP
Latency Sensitive	Lync/SfB Video
Recreational	Youtube

WAN Health Check



Uplink performance measured across WAN

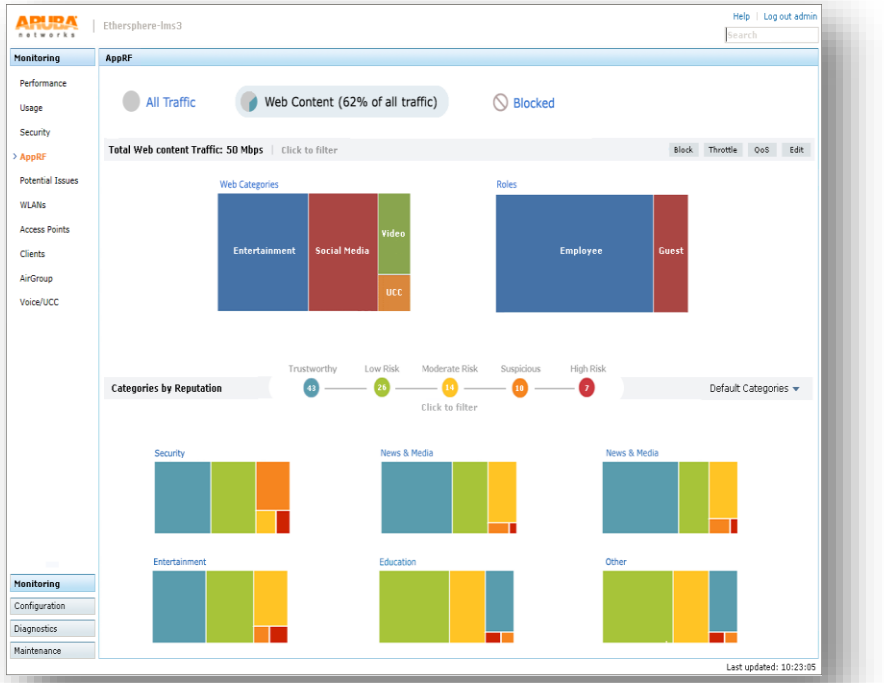
- Delay/Latency
- Packet Loss, Throughput
- Jitter, MOS

Threshold can be set for Media Mode for

- Delay
- Packet Loss, Throughput
- Jitter, MOS

Uplink Health check could be measured with IP or FQDN

Web Content Classification & Reputation



Incorporates Webroot's cloud based machine learning technology to classify

- Over 2.5K URLs per minute
- 1.5M classifications per day
- With a reported false positive rate of less than 0.2%
- Auto-classifiers classify sites into 83 categories and classification is supported for 40+ languages
- Reputation scores are based on categories related to internet security like Malware, phishing, spyware, span, botnet

Operates at user role level

- Block based on category, threat level
- QoS

IP Reputation

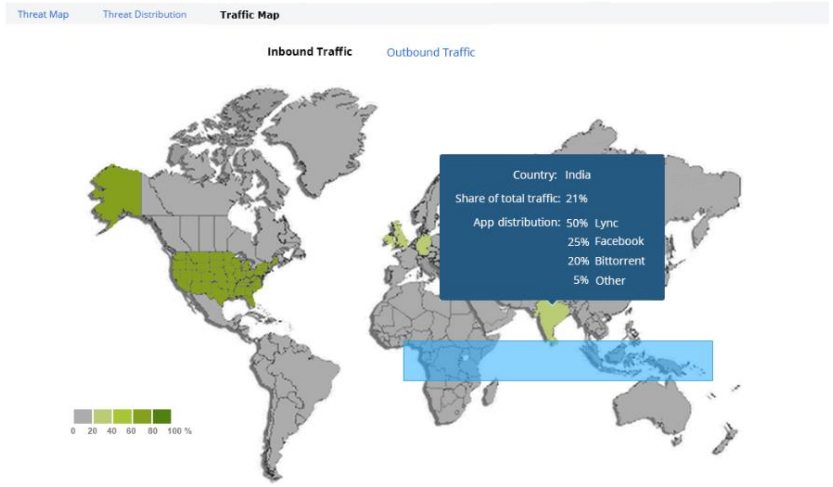
Incorporates Webroot's cloud based machine learning technology to classify

- Monitors **3.7B IPs** (all public IPv4 addresses) using real endpoints and honeypots, sensor network
- Identifies millions of malicious IPs that it monitors closely (**typically 7M to 12M**)
- IP threat types detected - Spam Sources, Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxies, and Mobile Threats
- IP reputation broken into 5 different categories

Operates at a global level

- Block based on per-controller basis

Geo-location Filtering



Ability to associate source/destination IP addresses with location

Leverages Webroot's cloud based service that has geo-location database

- IP ranges can be tied with countries
- Controller has a cache of half a million IP addresses
- Periodic updates

Apply policies to permit/drop inbound/outbound communication with certain countries

Branch Controller Portfolio





Features	7005	7008	7010	7024	7030
AP License	16	16	32	32	64
User count	1K	1K	2K	2K	4K
Firewall throughput	2Gbps	2Gbps	4Gbps	4Gbps	8Gbps
Encryption throughput	1.2Gbps	1.2Gbps	2.4Gbps	2.4Gbps	2.4Gbps
GE ports	4	8	16	24	8
PoE support	Can be PoE powered	Can power 8 ports	12 ports can provide PoE	24 ports can provide PoE	No
SFP/SFP+			2 SFP	2 SFP+	8 Combo ports
Fanless	Yes	Yes	No	No	No

Headend/ VPN Concentrator Portfolio

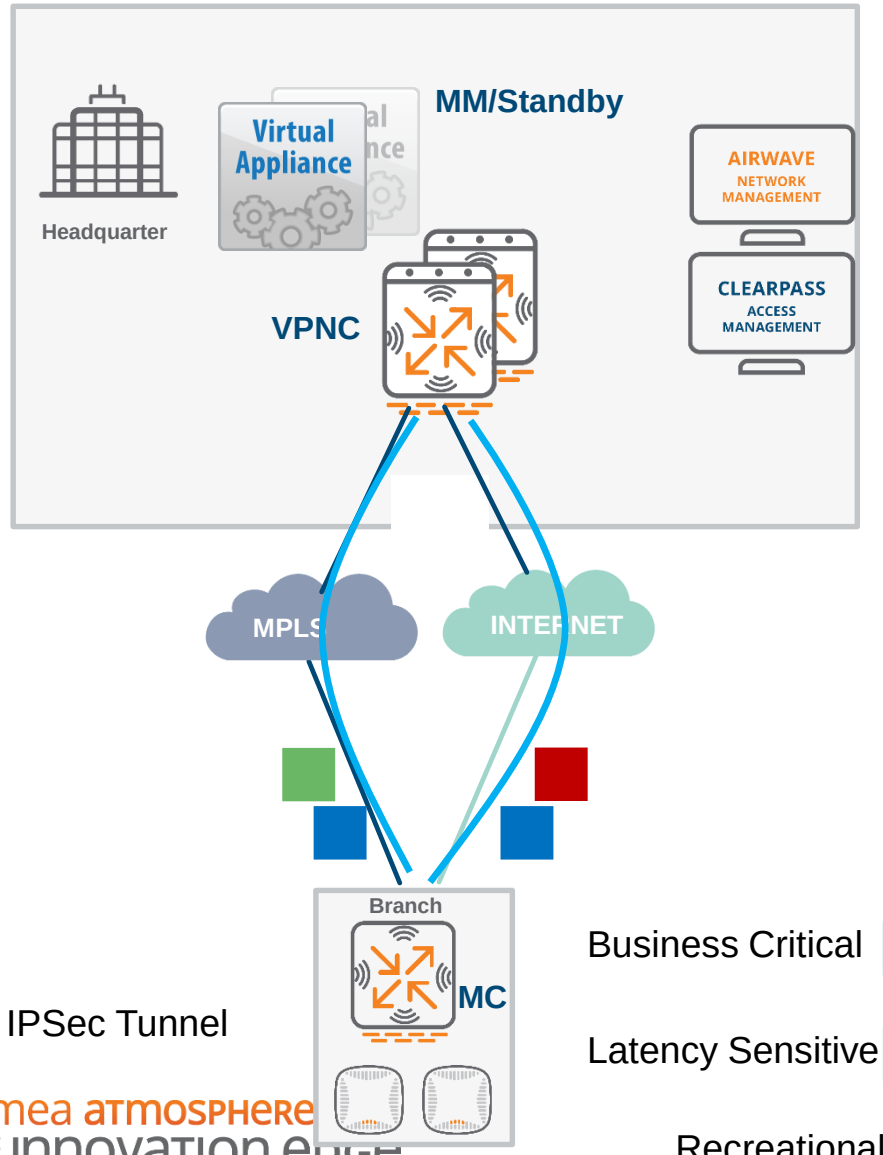



Features	7205	7210	7220	7240
AP License	256	512	1024	2048
User count	8192	16384	24576	32768
Concurrent IPSec Tunnels	4096	16384	24576	32768
Encryption throughput	4.5Gbps	5.9Gbps	20Gbps	30Gbps
Firewall throughput	12Gbps	20Gbps	40Gbps	40Gbps
GE ports	4 (1G Combo)	2 (1G Combo)	2 (1G Combo)	2 (1G Combo)
SFP/SFP+	2 10G SFP+	4 10G SFP+	4 10G SFP+	4 10G SFP+
Redundant Power Supply/Fan	No	Yes	Yes	Yes

Thank you

Roadmap…

Context-Aware Path Selection



Policy based Path selection based of

- Applications
- Roles, VLANs

Global Load Balancing based of:

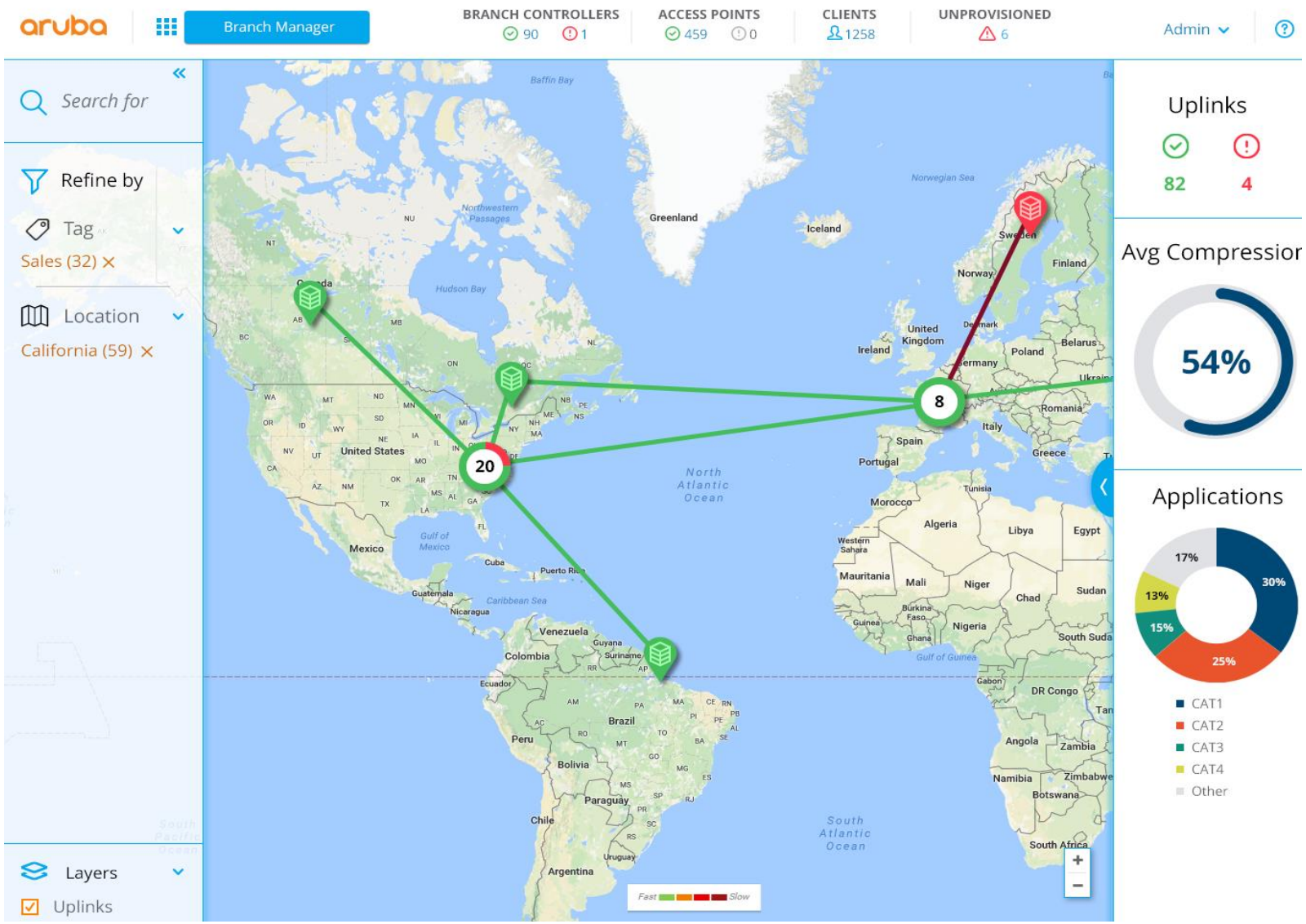
- Round robin (default)
- Hash
- Session count
- Uplink utilization

Uplinks can be configured Active-Active or Active-Backup

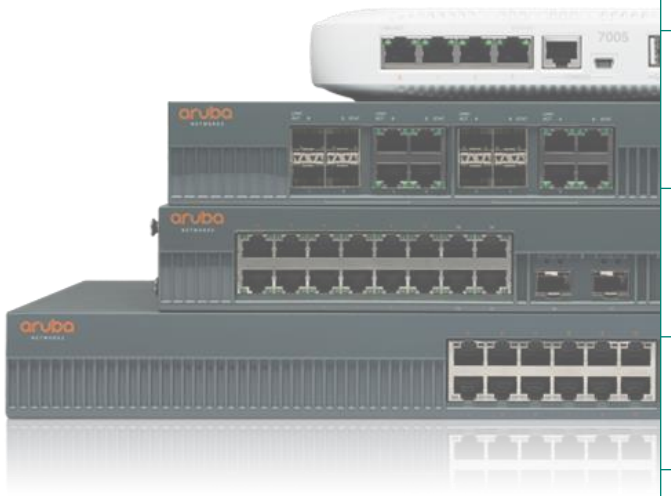
Added WAN Compression capability

SD-Branch


Carrier
1:20 PM
100%
Onboard
Site Address
2885, Lakeside Drive, Santa Clara, CA-94045
SN: CNCGHMJMYH
MAC: 34:FC:B9:C0:A8:D6
IAP-205-US
SN: CNCFHMQFCV
MAC: A8:FC:B9:C0:A8:D6
IAP-305-US
SN: CNCFHMQFCV
MAC: 34:FC:B9:C0:A8:D6
IAP-305-US
Add Device


aruba
Branch Manager
BRANCH CONTROLLERS
90
1
ACCESS POINTS
459
0
CLIENTS
1258
UNPROVISIONED
6
Admin
Search for
Refine by
Tag
Sales (32)
Location
California (59)
Layers
Uplinks
Uplinks
82
4
Avg Compressior
54%
Applications
30%
25%
15%
13%
17%
CAT1
CAT2
CAT3
CAT4
Other
20
8
United States
Mexico
Greenland
Iceland
Sweden
Norway
Finland
United Kingdom
Ireland
Germany
Poland
Belarus
Spain
Portugal
Italy
Romania
Greece
Morocco
Algeria
Libya
Egypt
Tunisia
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Venezuela
Colombia
Brazil
Peru
Bolivia
Paraguay
Chile
Argentina
Angola
Zambia
Namibia
Botswana
Zimbabwe
South Africa
DR Congo
Fast
Slow

Comparing the 7000 Series Models



	7005	7008	7010	7024	7030
AP licenses	16	16	32	32	64
Auto-negotiating 10/100/1K BASE-T ports	4	8	16	24	8
Power Budget/ Consumption	--/16.6W	100W/ 126W	/190W	400W/ 450W	--/55W
Firewall throughput	2Gbps	2Gbps	4Gbps	4Gbps	8Gbps
USB 2.0	Yes; 1	Yes; 2	Yes; 2	Yes; 1	Yes; 1
Fanless	Yes	Yes	No	No	No

Aruba 7000 Series Mobility Controllers for Branch – 7005, 7008, 7010, 7024, 7030

innovation 2016 award
WINNER
Cloud Security Solution

CRN Tech Innovators Awards 2015

- Rapidly deploy to any location with zero touch
- Optimize and secure branch while reducing cost
- Unified policy infrastructure for LAN, Security and WAN

Capabilities

Zero touch provisioning	Context based firewall
WAN opt. (compression)	3rd party integration
WAN survivability	WAN Loadbalancing
WAN health checks	High performance
Secure, wired access	4G/LTE smart backup
Policy-based WAN routing	Resilient

Aruba 7000 Series Performance & Capacity

PERFORMANCE AND CAPACITY					
Features	**7005**	**7008**	**7010**	**7024**	**7030**
Maximum campus AP licenses	16	16	32	32	64
Maximum remote AP licenses	16	16	32	32	64
Maximum concurrent users/devices	1,024	1,024	2,048	2,048	4,096
Maximum VLANs	4,094	4,094	4,094	4,094	4,094
Active firewall sessions	16,384	16,384	32,768	32,768	65,536
Concurrent GRE tunnels	256	256	512	512	1,024
Concurrent IPsec sessions	512	512	1,024	1,024	2,048
Mobility Access Switch tunneled-node ports	512	512	1,024	1,024	2,048
Firewall throughput	2 Gbps	2 Gbps	4 Gbps	4 Gbps	8 Gbps
Encrypted throughput (3DES, AES-CBC)	1.2 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps	2.4 Gbps
Encrypted throughput (AES-CCM)	1.6 Gbps	1.6 Gbps	3.4 Gbps	3.4 Gbps	4.0 Gbps

Aruba 7000 Interfaces

INTERFACES AND INDICATORS					
Features	**7005**	**7008**	**7010**	**7024**	**7030**
Form factor/footprint	Compact	Compact	1 rack unit	1 rack unit	1 rack unit
Auto-negotiating 10/100/1000BASE-T	4	8	16	24	8 (combo)
Gigabit Ethernet ports (GBIC or SFP)	N/A	N/A	2 SFP	2 SFP+	8 (combo)
USB 2.0	Yes (1)	Yes (2)	Yes (2)	Yes (1)	Yes (1)
Management/status LEDs	Yes	Yes	Yes	Yes	Yes
LINK/ACT and status LEDs	No	No	No	Yes	Yes
LCD panel and navigation buttons	No	No	Yes	Yes	Yes
Console port	Yes (micro USB/RJ-45)	Yes (micro USB/RJ-45)	Yes (micro USB/RJ-45)	Yes (micro USB/RJ-45)	Yes (micro USB/RJ-45)
Out-of-band management port	No	No	Yes	Yes	Yes

Aruba 7000 Physical Characteristics

PHYSICAL					
	7005	**7008**	**7010**	**7024**	**7030**
Dimensions (H x W x D)	4.1 cm x 20 cm x 20 cm (1.6" x 7.9" x 7.9")	4.2 cm x 20.32 cm x 20.32 cm (1.65" x 8.0" x 8.0")	4.42 cm x 31.75 cm x 33.7 cm (1.74" x 12.75" x 13.3")	4.37 cm x 44.2 cm x 31.3 cm (1.72" x 17.4" x 12.32")	4.4 cm x 30.5 cm x 21.1 cm (1.7" x 12" x 8.3")
Weight	0.92 kg (2.03 lbs)	1.0 kg (2.2 lbs)	3.4 kg (7.5 lbs)	5.127 kg (11.3 lbs)	2.06 kg (4.54 lbs)
MTBF (hours, @ 25C)	323,896	300,000	232,843	311,901	390,679

aruba
a Hewlett Packard Enterprise company

emea atmosphere '17

THE innovation edge