

# airheads

## TECH TALK *LIVE*

**aruba**  
a Hewlett Packard  
Enterprise company

## Aruba's Software Defined Branch Services

Mitchell Pompe, Aruba

#ArubaAirheads

# What is SD-WAN vs SD-Branch?

SD-WAN is a subset of SD-Branch

## Software Defined Wide Area Network

SD-WAN makes it easy for IT to control application traffic entering and exiting a branch office across multiple WAN uplinks.

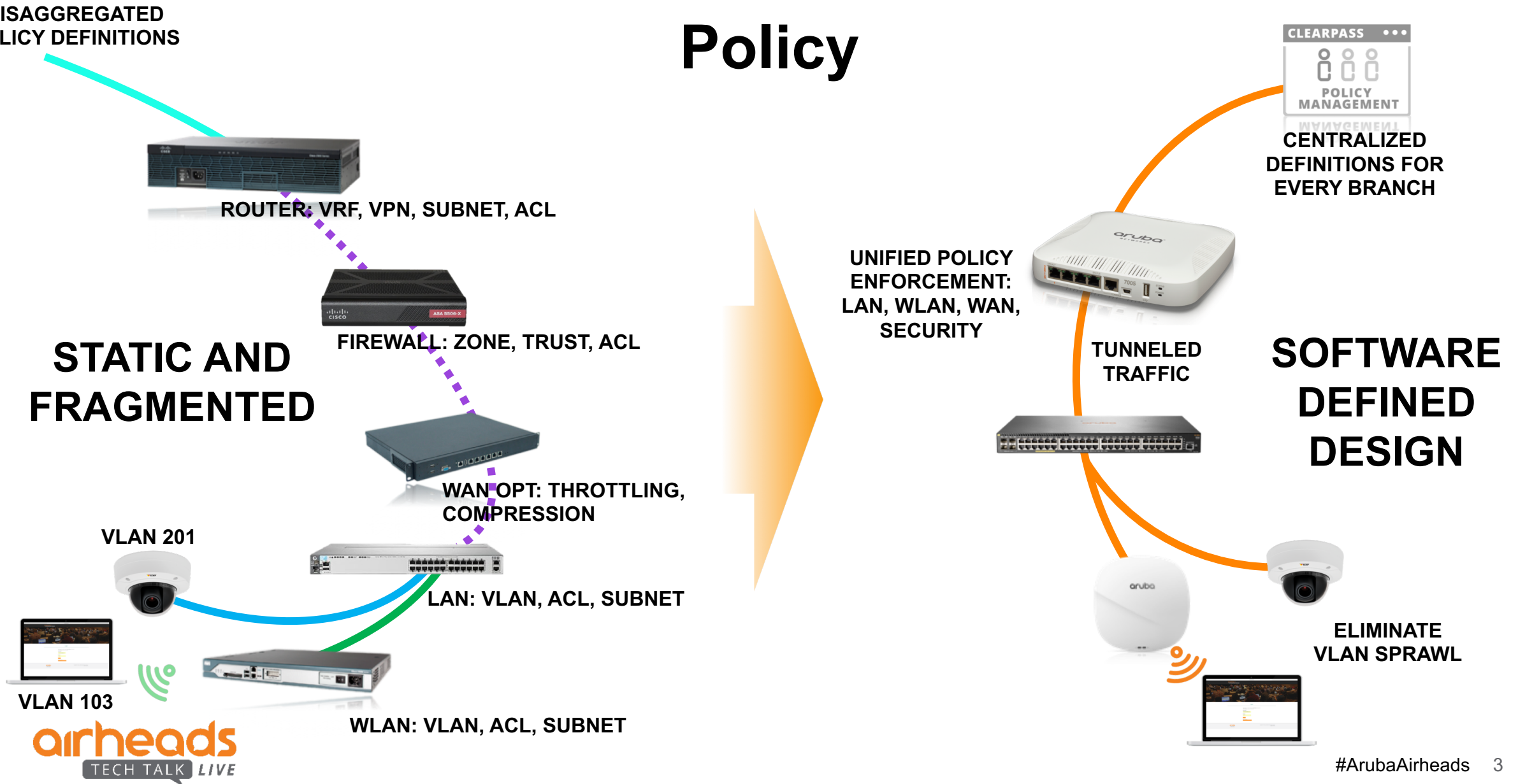
*An optimized WAN experience*

## Aruba's Software Defined Branch

SD-Branch integrates SD-WAN, WLAN, LAN, and security together with common policy and management for simplified branch management

*An optimized end-to-end branch experience*

# Traditional vs SD-Branch



# The Traditional Port

VLAN 100  
ACL 'headless'

VLAN 200  
QoS Policy 'A'

VLAN 300  
ACL 'desktop'

VLAN 400  
ACL 'guest'



# 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

Drive simplicity and fewer boxes in branch solution



## Transport Independency

Own your WAN policy

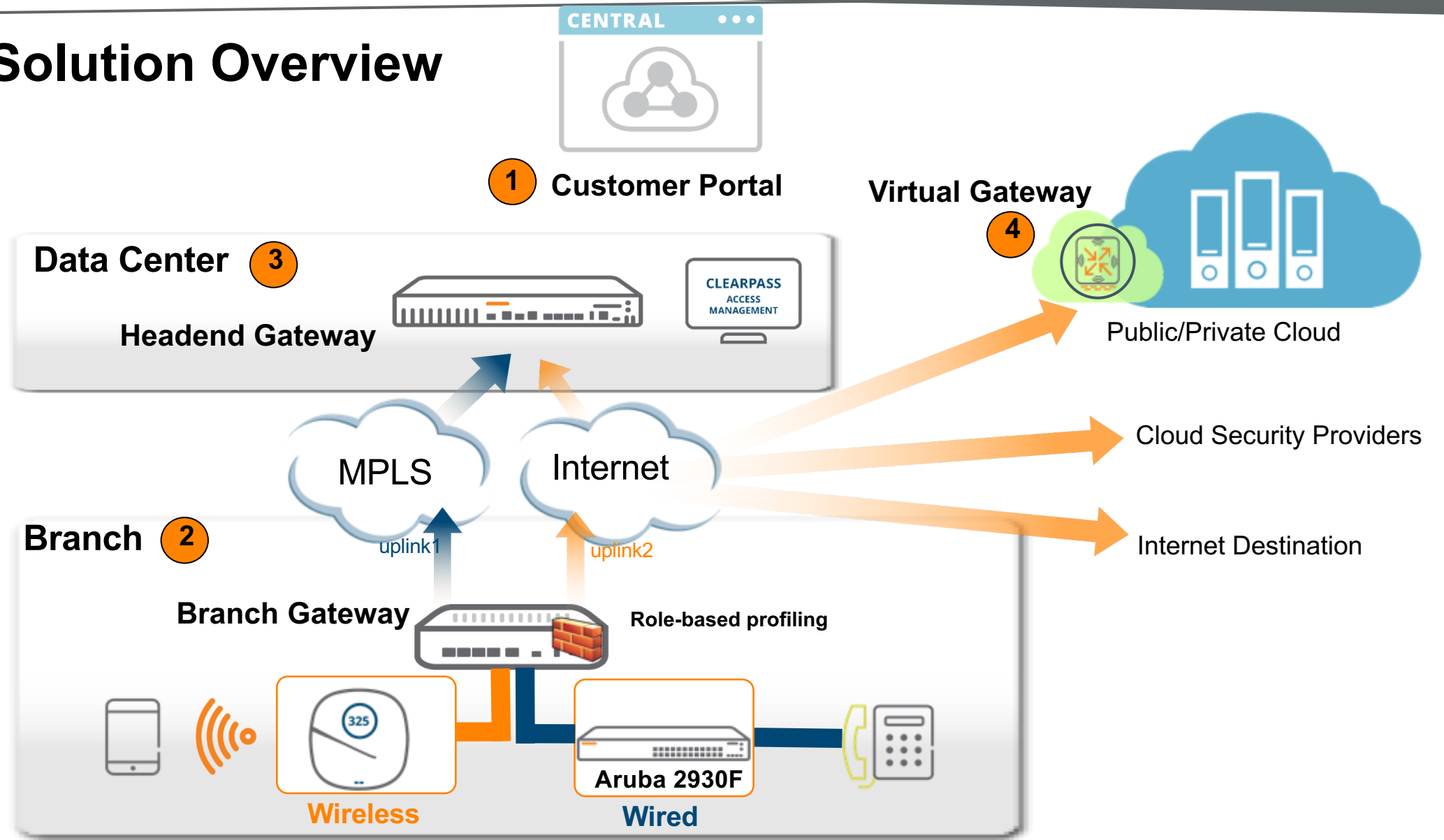


## Common Policy and Management

for Wired, WLAN and WAN



# Aruba Solution Overview



# CLOUD MANAGED 7000 SERIES BRANCH GATEWAYS

## INTEGRATED SD-WAN, LAN, WLAN, AND SECURITY



### ENTERPRISE-CLASS SD-WAN

Up to  
**10X**

Better performance  
than full-stack vendors

- 2.4Gbps of encrypted throughput
- App visibility and analytics
- Web content filtering

Up to  
**5**

WAN ports for  
flexible HA options

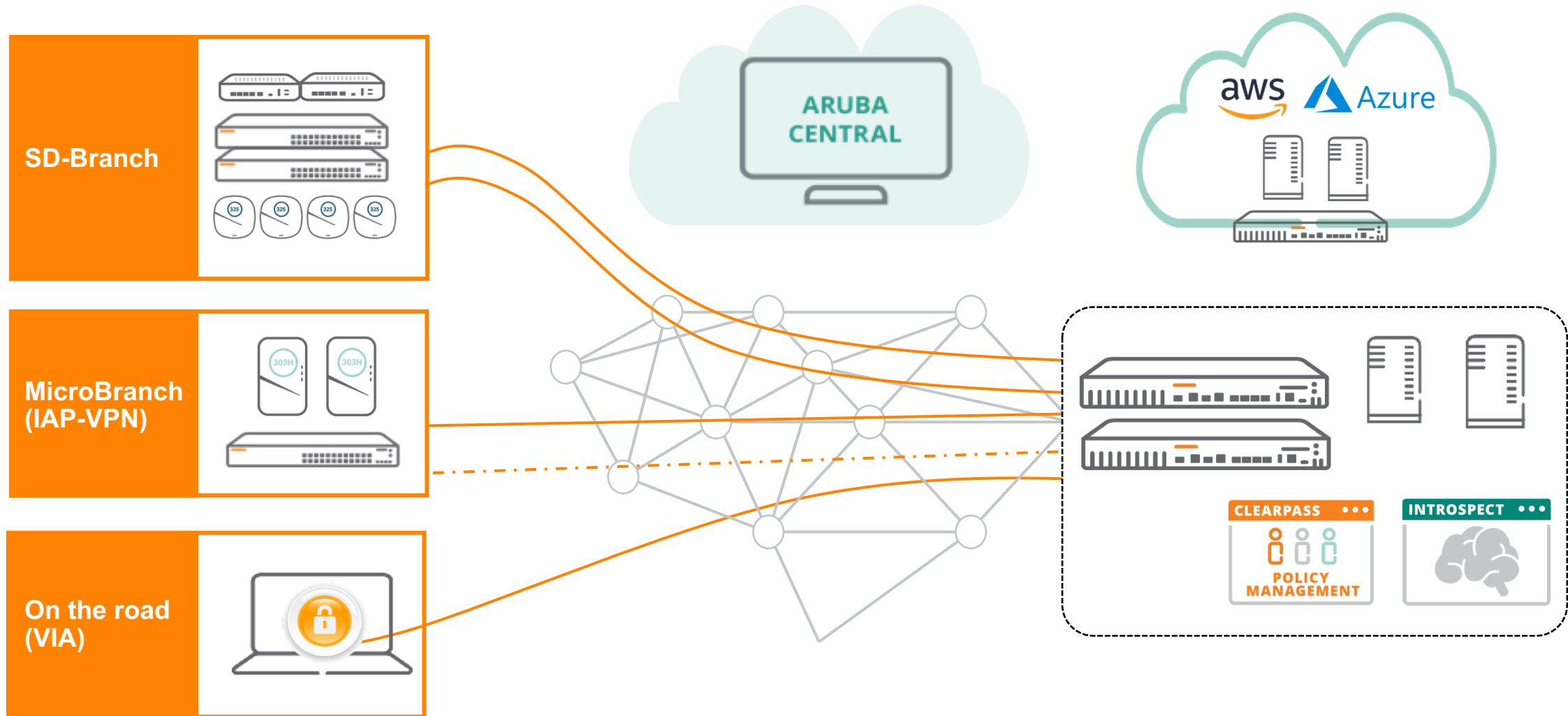
- Dynamic Path Selection, WAN QoS
- Policy-based routing, compression
- Active-Active hardware redundancy

Up to  
**64K**

active firewall sessions

- L4-L7 Firewall CC EAL4+
- Wide area NAC/AAA Survivability
- Crypto Engine (IPsec VPN)

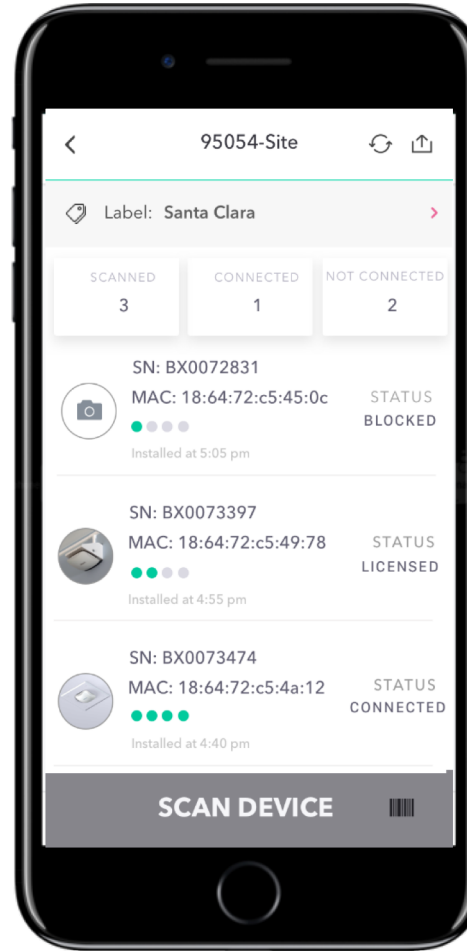
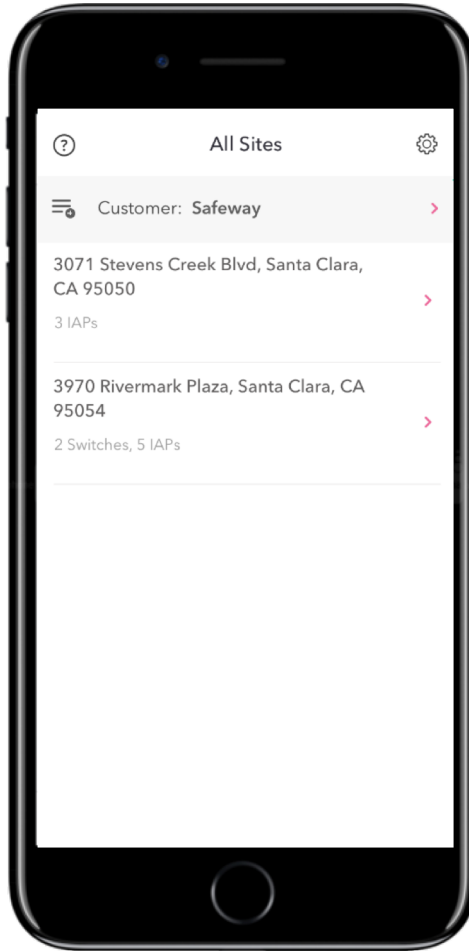
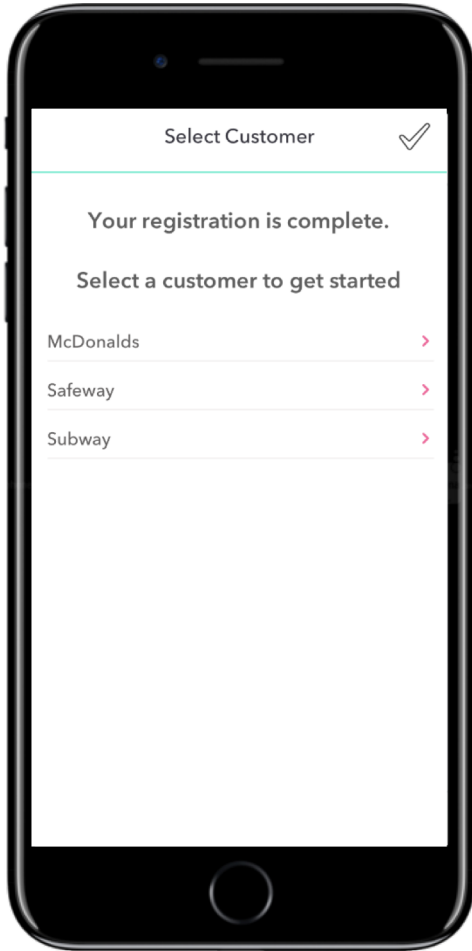
# Aruba Distributed Architectures



# Simplicity at Enterprise Scale

## Aruba Central

# Simple Onboarding



- 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

arubaCentral

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

FILTER GATEWAY MANAGEMENT

home-7008 (1 Total Devices | 0 Down AP)

REFINE FILTER LISTING

sam

GROUPS All Groups (11)

GROUP-samGROUP-sam-7008

GATEWAYS

GROUP-samdesk-7005

GROUP-sam-7008home-7008

GROUP-samJW634A-20:4C:03:...

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

+

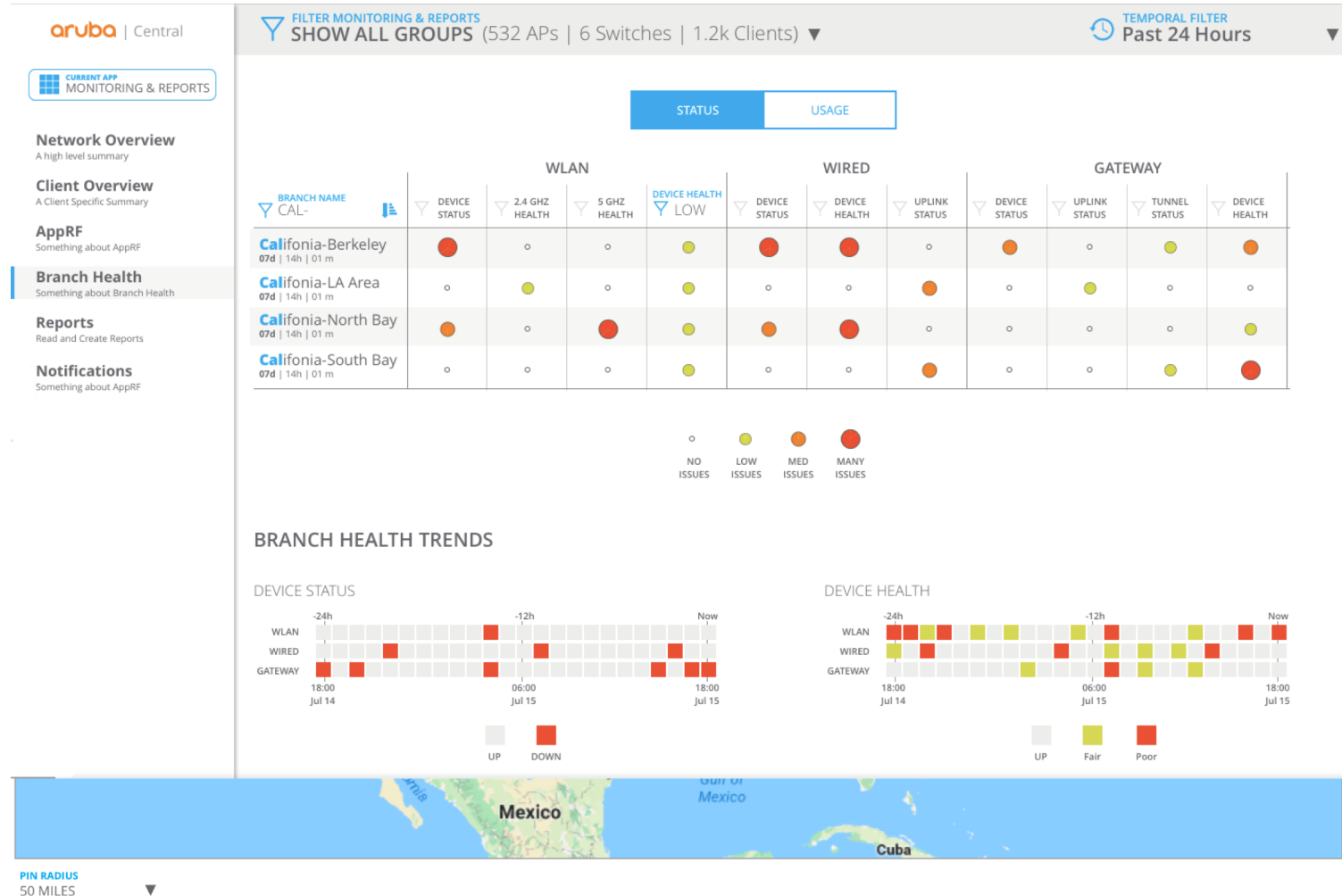
Port Channel

NAME	MEMBERS	PROTOCOL
------	---------	----------

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

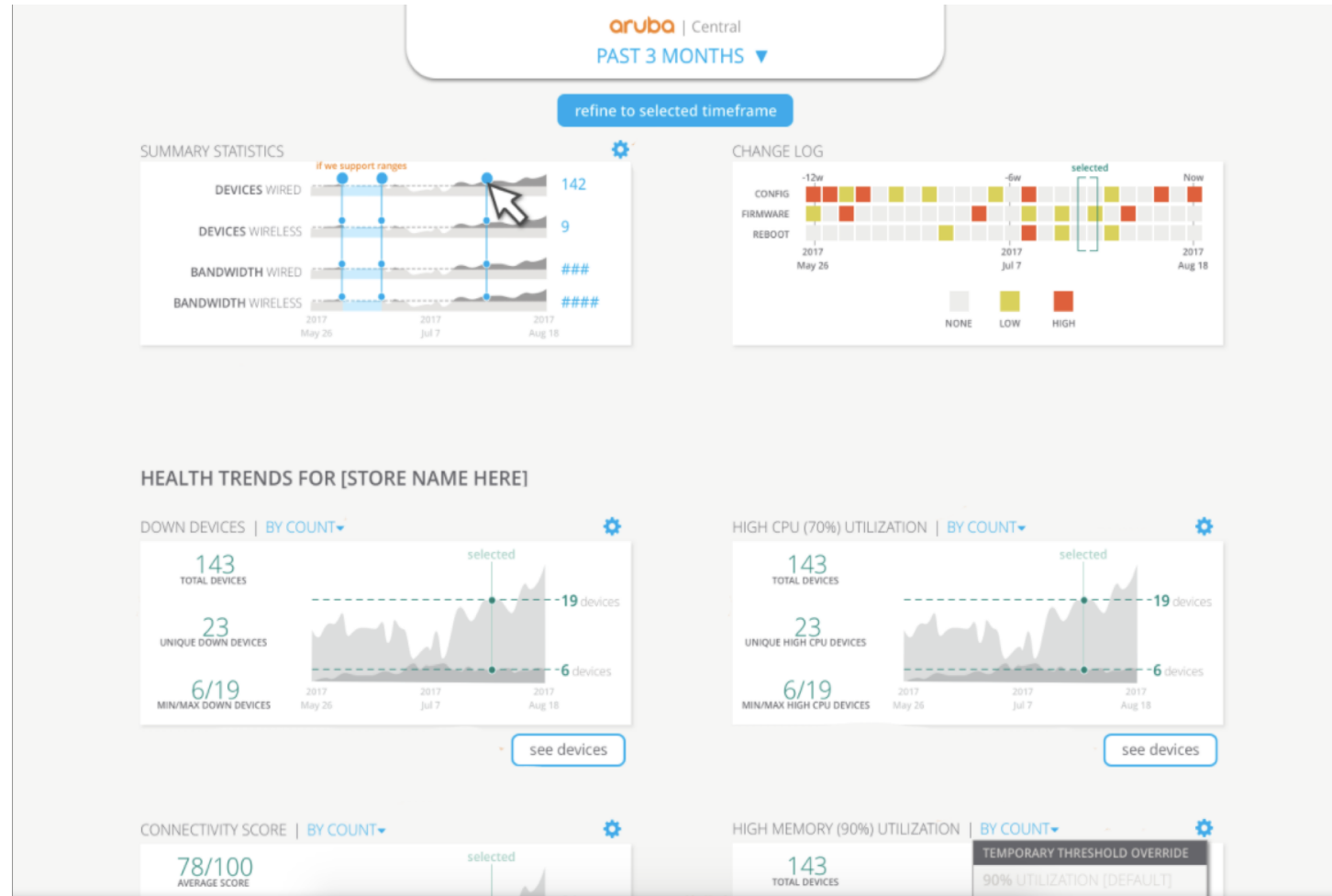
# Health Dashboard

- 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



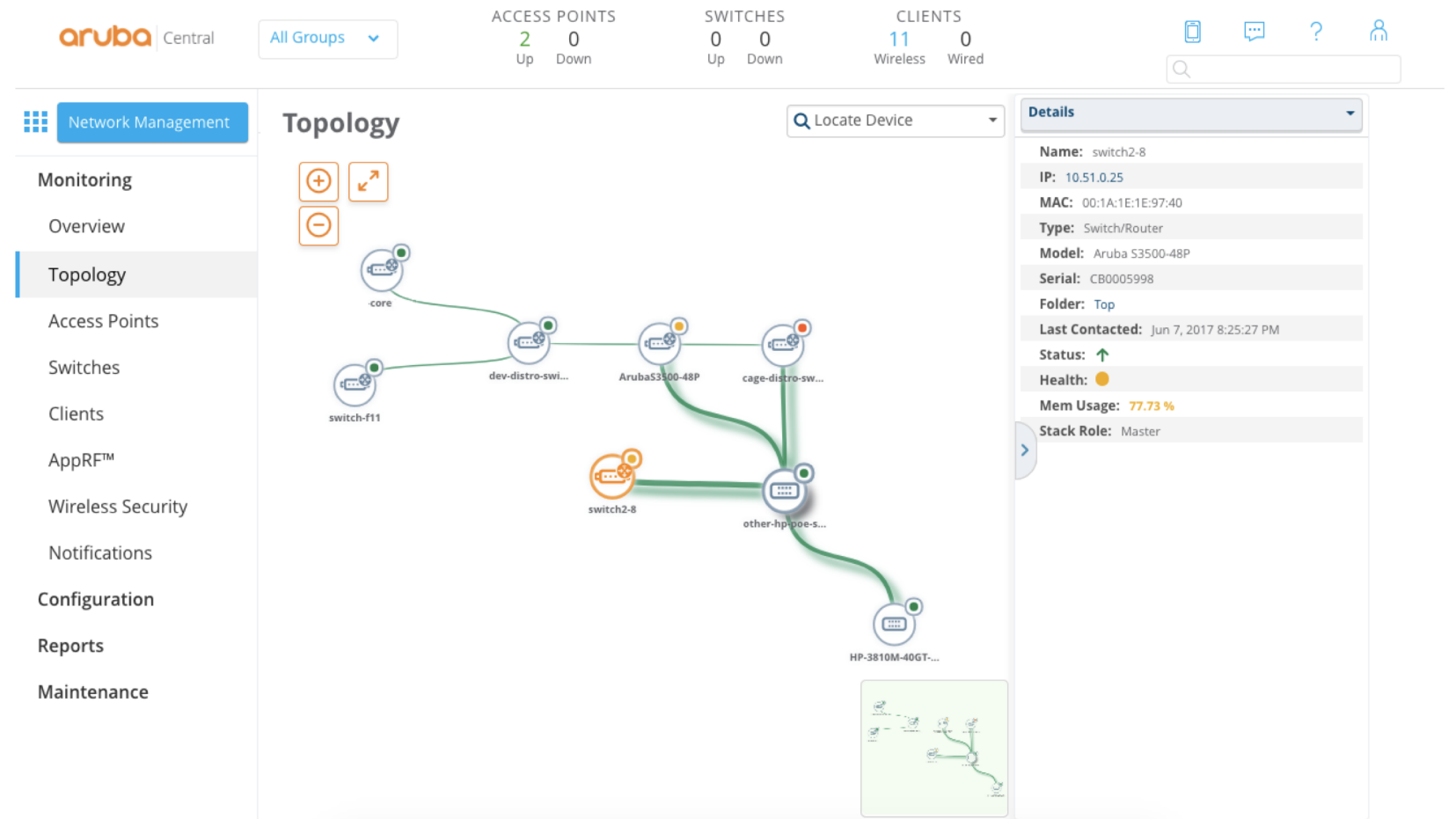
# Site Health Dashboard

- 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

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



## Client View - Complete end-to-end visibility

- Client info
- RF & Health
- Location
- Clarity
- UCC
- Live info
- Packet capture

Clients

20:4c:03:35:3e:8d

GO LIVE

ZAGNKLR008

Connected with good performance

DEVICE HEALTH

100 %

SNR

34 dB

TX RATE

650 Mbps

RX RATE

650 Mbps

CONNECTED TO

AP1

OVERVIEW

CONNECTIVITY


APPLICATIONS

LOCATION

EVENTS

DATA PATH


CLIENT



ZAGNKLR008

CONNECTED


SSID



Cookie Monster

UP


AP



AP1

UP

GATEWAY



MPM-NL-MSL-VPNC

UP

CLIENT INFO

USERNAME

ZAGNKLR008

HOSTNAME

ZAGNKLR008

IP ADDRESS

172.16.1.253

CLIENT TYPE

Wireless

CONNECTED SINCE

Jan 15 2019 08:41:04

DEVICE OS

Unknown

NETWORK INFO

VLAN

1

AP ROLE

Cookie Monster

GATEWAY ROLE

authenticated

AUTH SERVER

--

DHCP SERVER

172.16.1.2

CONNECTION INFO

CHANNEL

36 (80 MHz)

BAND

5 GHz

CLIENT CAPABILITIES

802.11ac

CLIENT MAX SPEED

1.30 Gbps

# More than just monitoring...

## Maintenance

- SW upgrades
- Golden SW image
- Troubleshooting
  - Remote console

## Alerting

- Email Alerts
- Webhooks notifications (HTTP Post)

## Reporting

- WAN inventory
- WAN Transport health
- WAN Policy compliance
- WAN availability
- ...



Aruba ▾

● Mitchell Pompe



🔍 All Threads

Channels



# central

# general

# random

+ Add a channel

Direct Messages



♥ Slackbot

● Mitchell Pompe (you)

+ Invite people

Apps



#central

☆ | 👤 1 | 📎 0 | ✎ Add a topic



🔍 Search



🎁 3 Updates



### Bring your team into Slack

Slack is better with teammates – invite them to start collaborating.

[Add People](#)

Customer ID: 5003025-1402

**CLARITY\_DHCP\_DELAY - severity : Critical**

2019-03-04 05:00:07 UTC

Alert ID:

More Details:

**Aruba Central** APP 7:00 AM

More than 30% of DHCP attempts made in the last 30 minutes was delayed more than 200ms

✕

Customer ID: 5003025-1402

**CLARITY\_DHCP\_DELAY - severity : Critical**

2019-03-04 05:30:07 UTC

Alert ID:

More Details:

**Aruba Central** APP 1:12 PM

SLA DPS Compliance Violations for Customer : 5003025 with Device Serial Number : CP0030539 for Policy Name : Aruba Traffic and Uplink Id : 102

Customer ID: 5003025-20

**DPS\_COMPLIANCE\_ALERT - severity : Critical**

2019-02-27 10:10:03 UTC

Alert ID: AWkubr0GwwyPCYMZiNbX

More Details:

CP0030539



Message #central

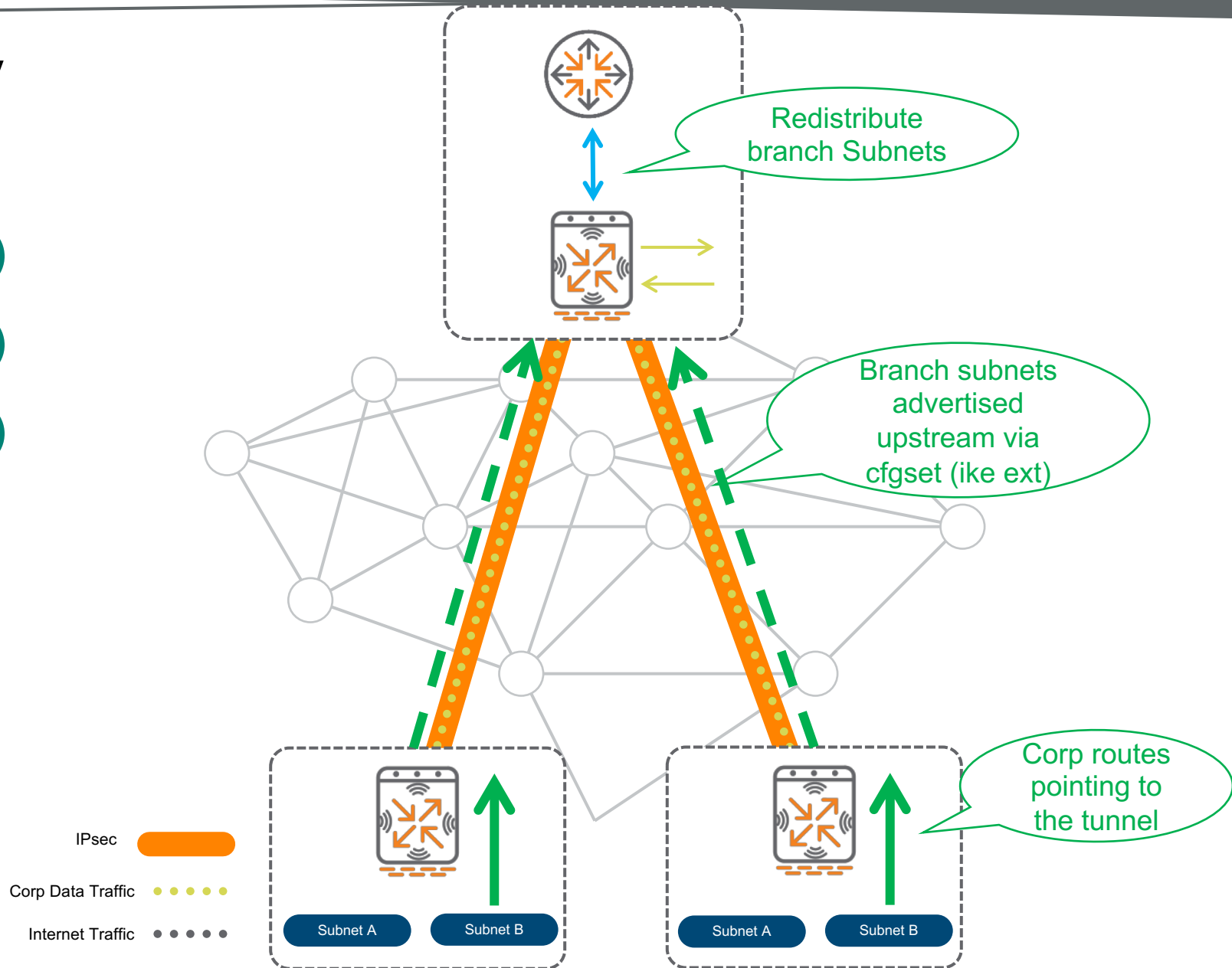


# Transport-Independent WAN

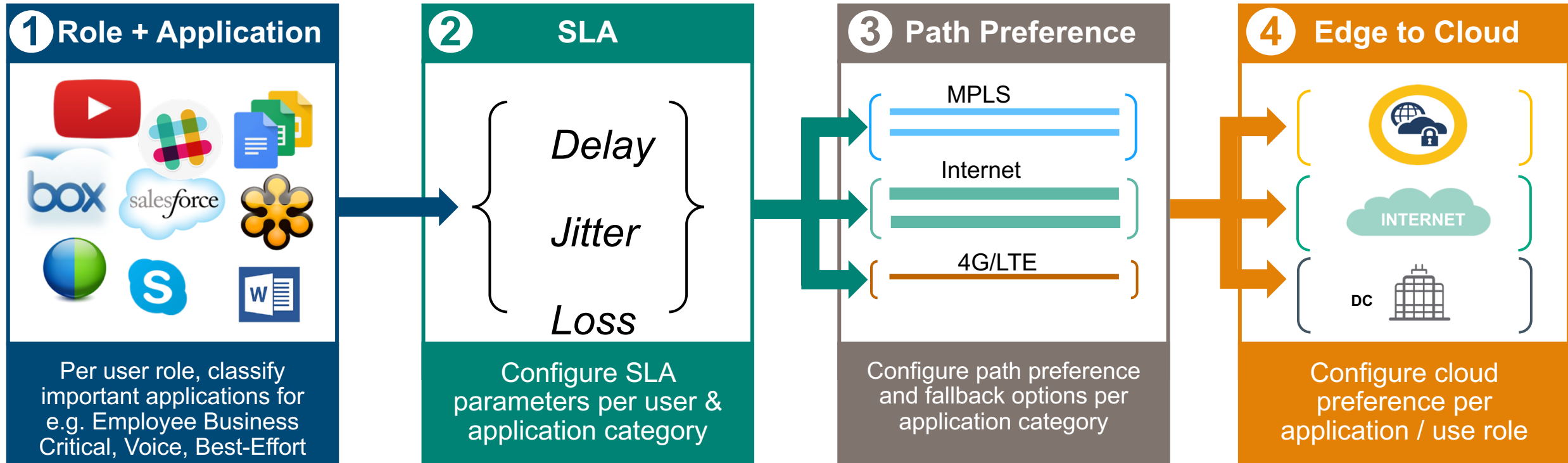
## Aruba SD-WAN

# 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

Demo

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

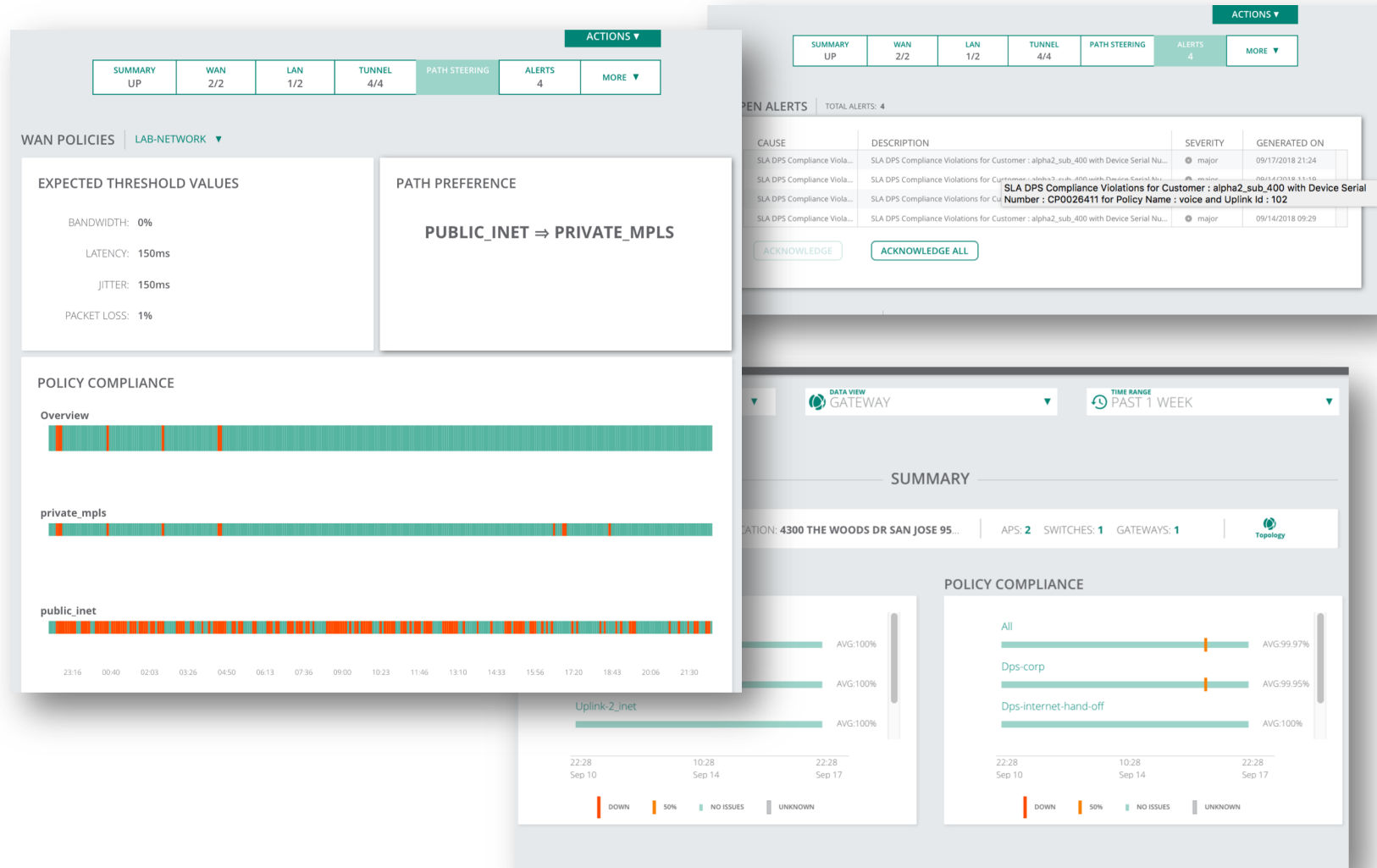
- View compliance per WAN link
- Highlight violations with specific reasons

*Is the policy honoring path preference?*

- View session distribution across active links

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

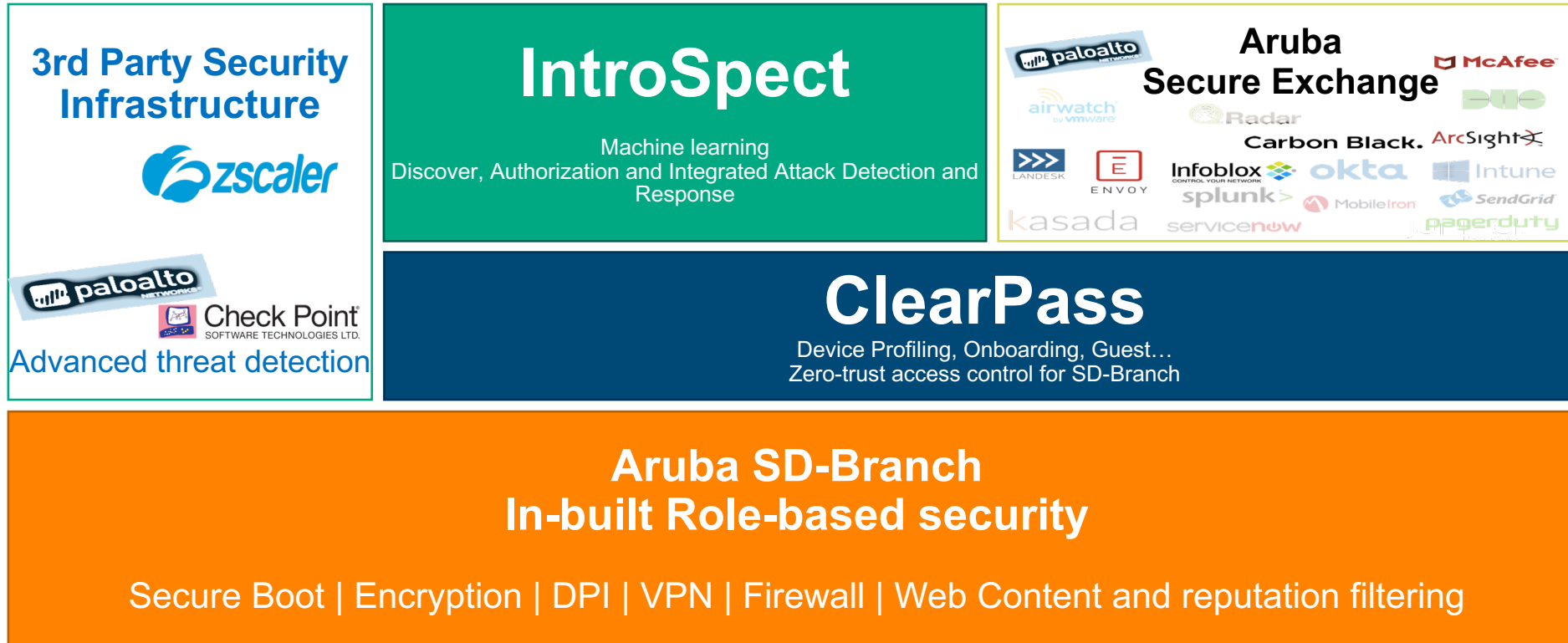
- Quickly identify session movement between WAN links



# Secure-First Branch

End-to-end branch security

# Security Layers



Security Core



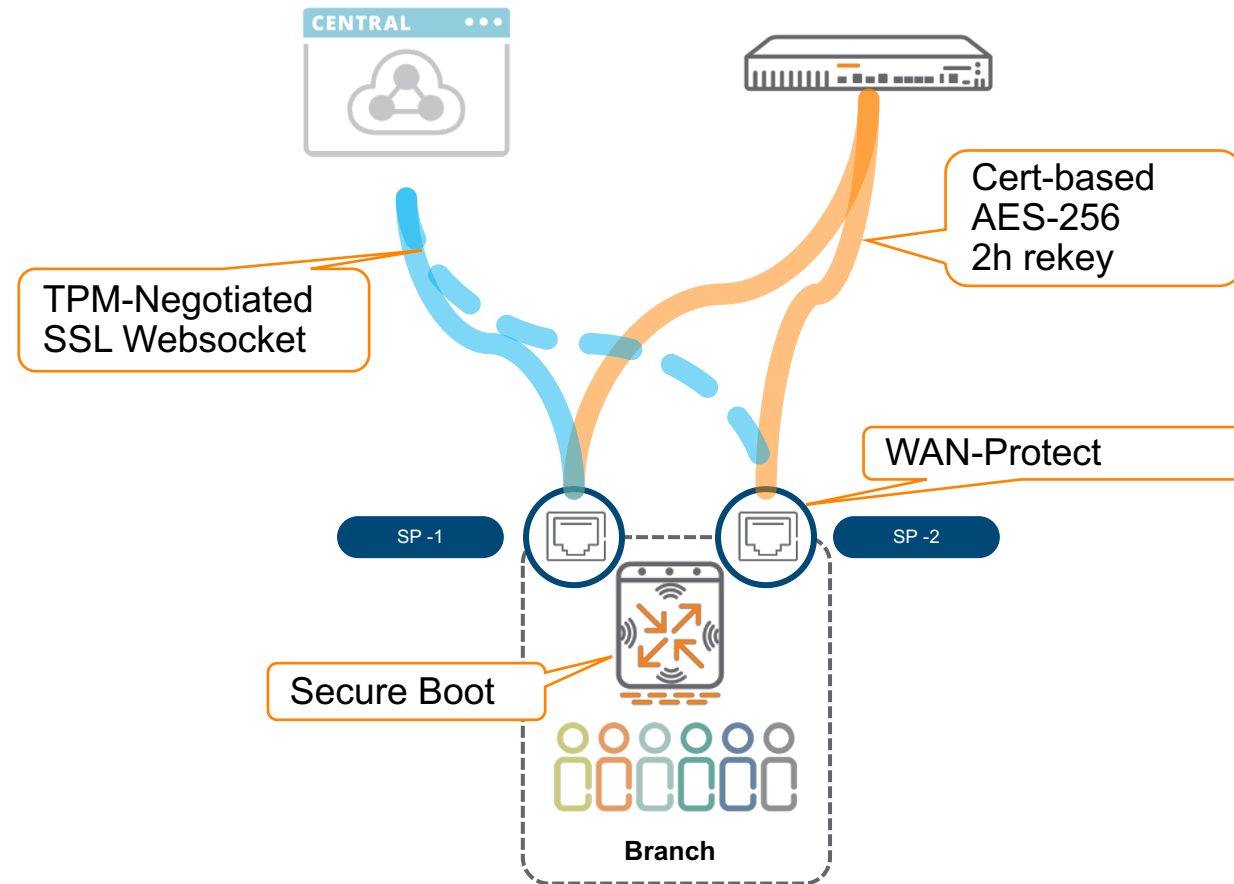
360 Security  
Exchange Program

# Security and hardening

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



Security Core

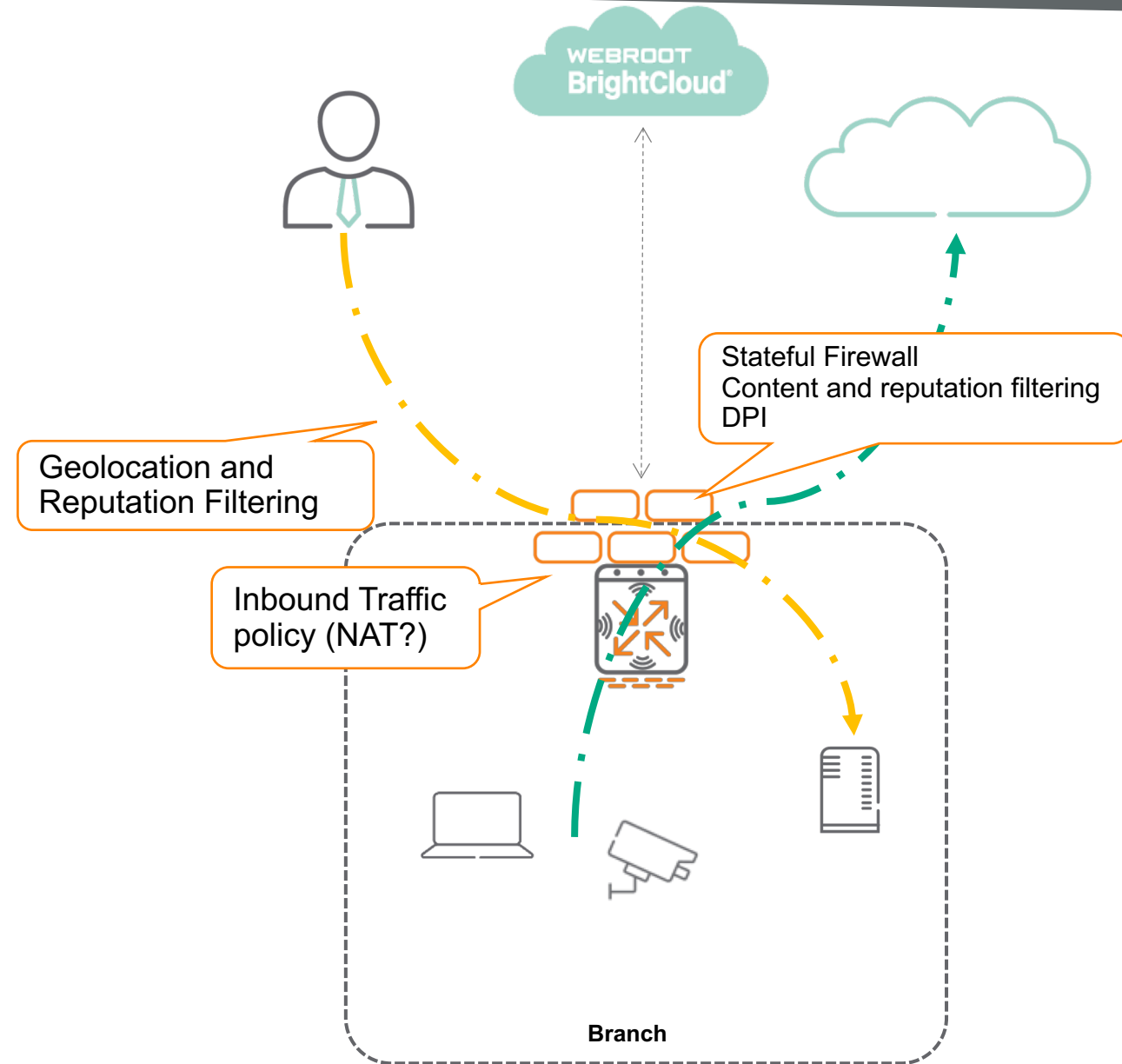


# Branch Firewall

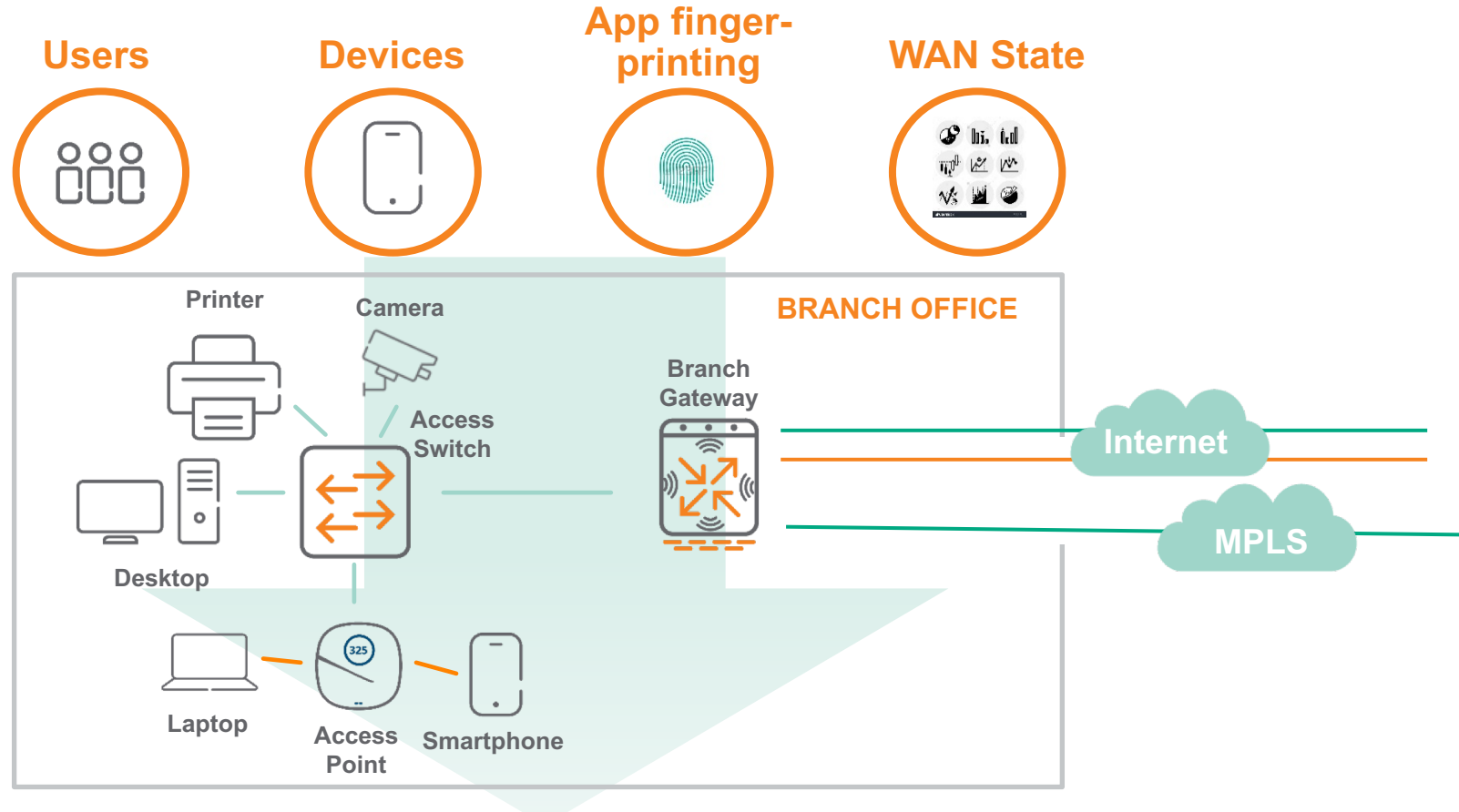
- 1 Inbound firewall policies  
- Apply on WAN interfaces
- 2 Geolocation and reputation filtering  
- Inbound and outbound
- 3 Stateful firewall with ALGs and DPI
- 4 Web Content and Reputation Filtering



Security Core



# Role Based 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

# Making branch security scalable...

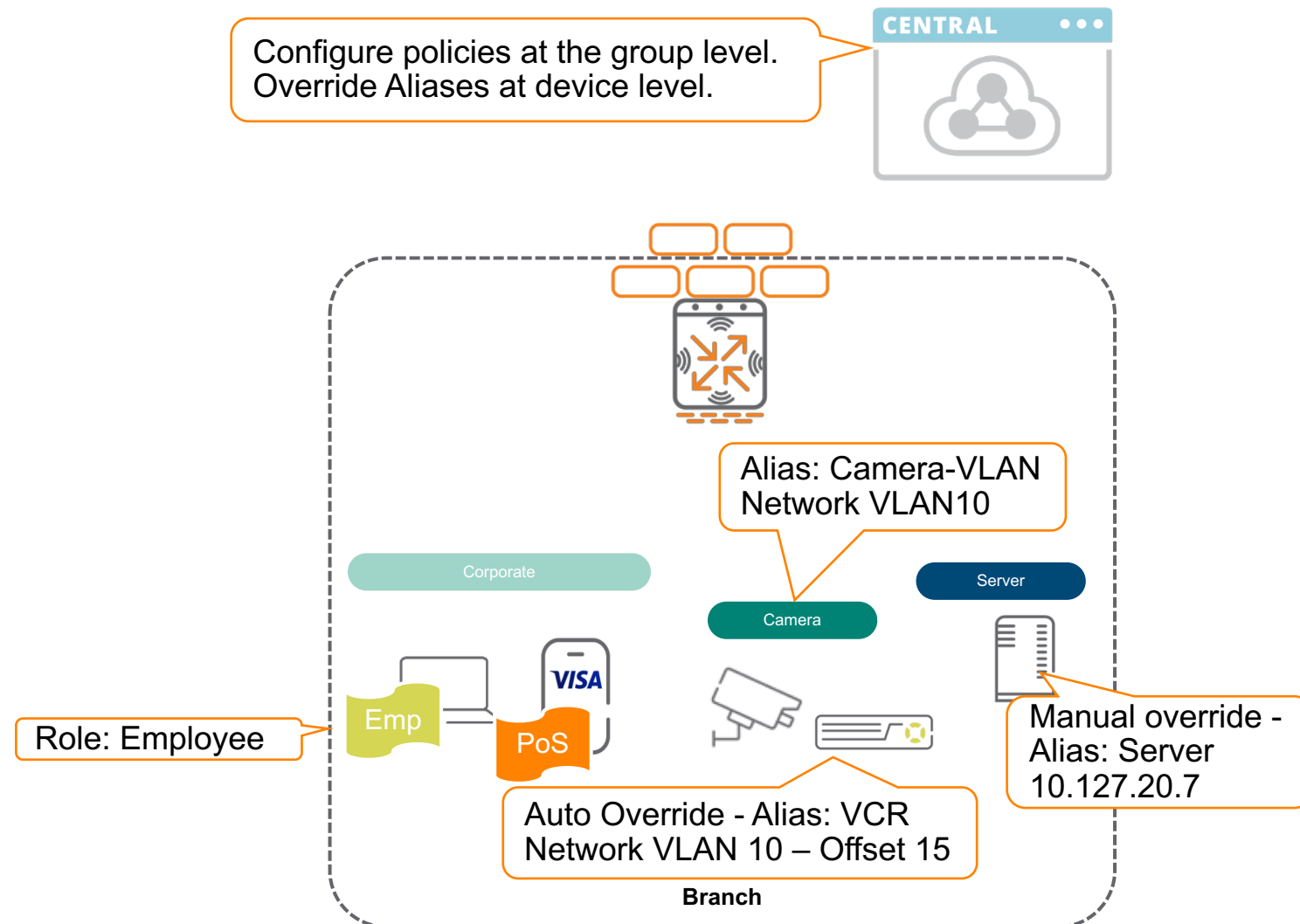
## Group based security policies

- 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



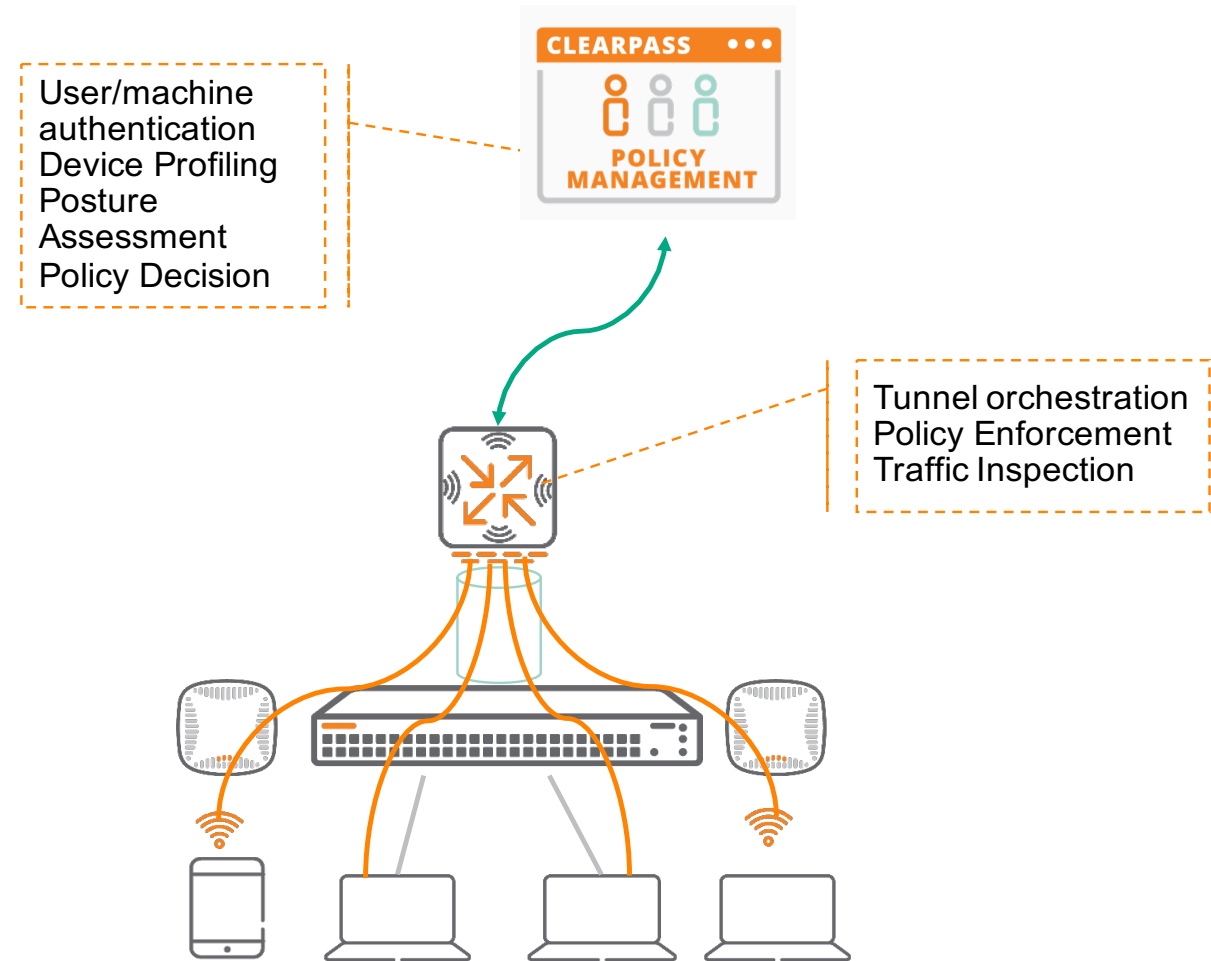
# Consolidated Policy Enforcement Point

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



# User Centric policy demo

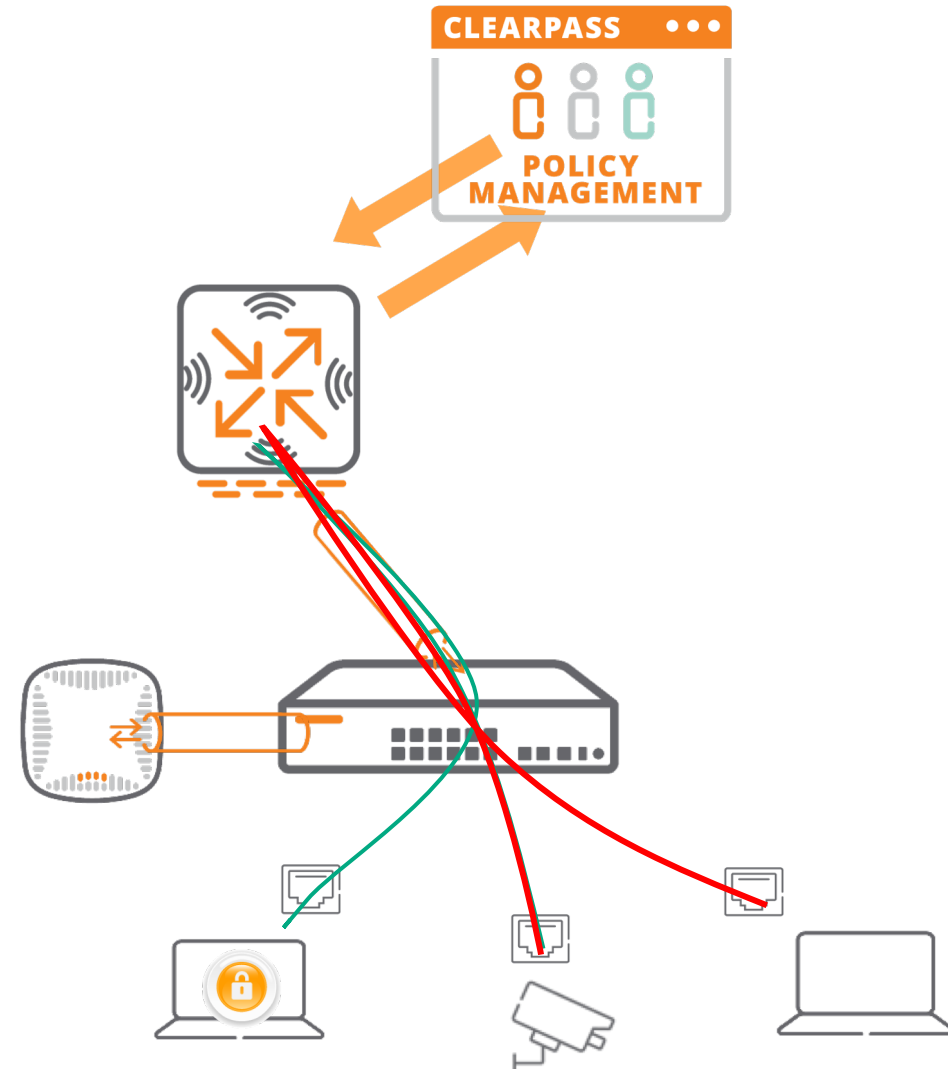
Demo

- 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**  
TECH TALK LIVE



# Wi-Fi Security As of Yesterday: WPA2

- **WPA2 was standardized in 2004**
  - When APs could not do heavy-weight cryptographic work
  - Wi-Fi was a PCMCIA card doing 11g– solely a last hop technology
- **Unforeseen from the horizon of 2004**
  - Captive portals
  - Wi-Fi everywhere! Planes, trains, automobiles, stadiums, the mall, coffee shops...
  - Wi-Fi as an entitlement... and an inducement to sit down, stay, and spend money
  - Rise of app-based services on client devices that rely on Wi-Fi
  - Wi-Fi being used to manage operations of large spaces (cameras, signage, PCI, etc)
- **Tools provided by WPA2 cannot meet current market needs**
  - WPA2-PSK– is flawed, imposes unreasonable requirements on users to address the flaw
  - WPA2-Enterprise– very complicated to provision, fragile, not supported by every device
- **Operators, service providers, enterprises, and users have to “make do”**
  - Tragic results naturally follow



# Enforcing L7+ security policies

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

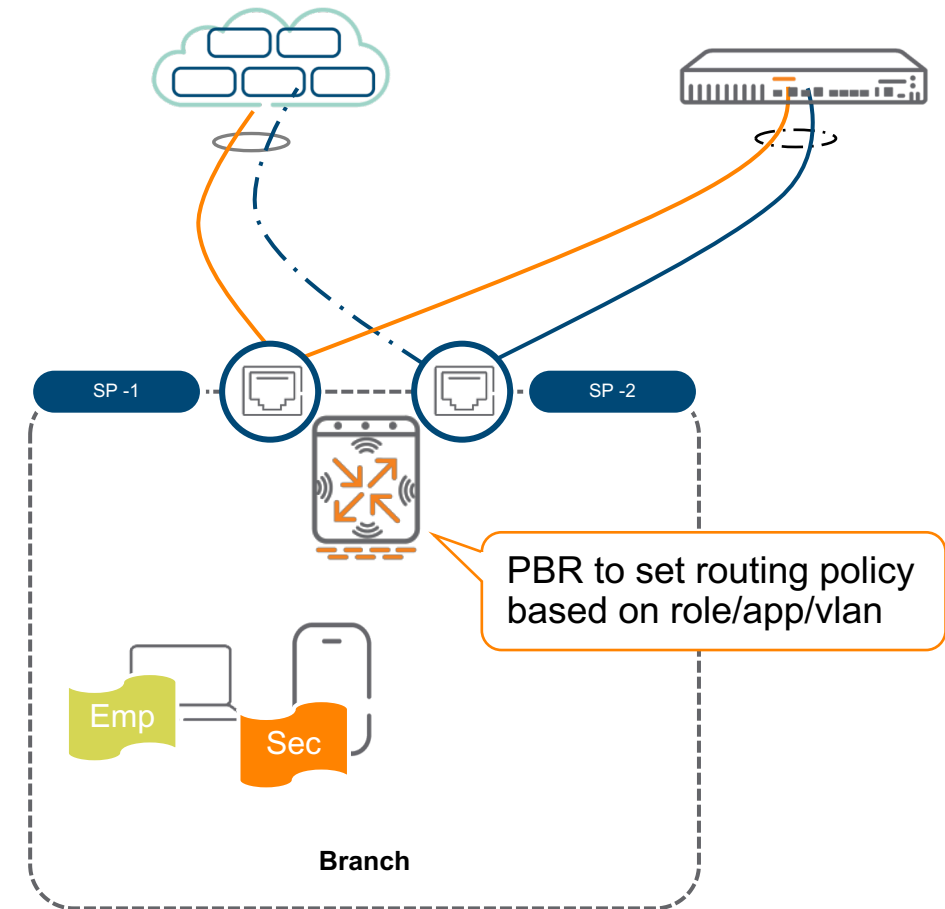
- 1 ClearPass assigns user role
- 2 ClearPass shares role with firewall
- 3 Role includes routing policy to force Internet traffic through Cloud Security
- 4 IDS/DPS/DLP Enforcement



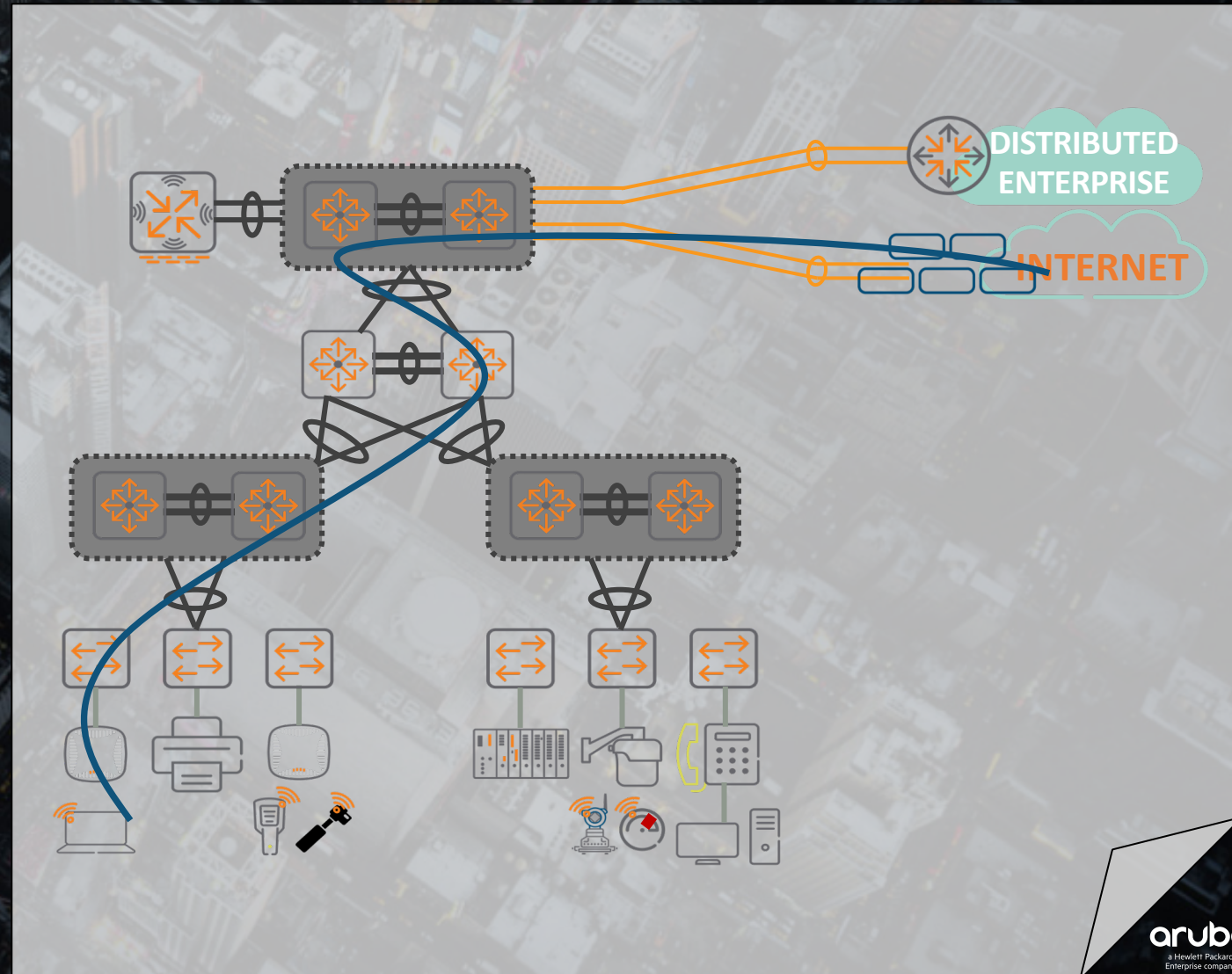
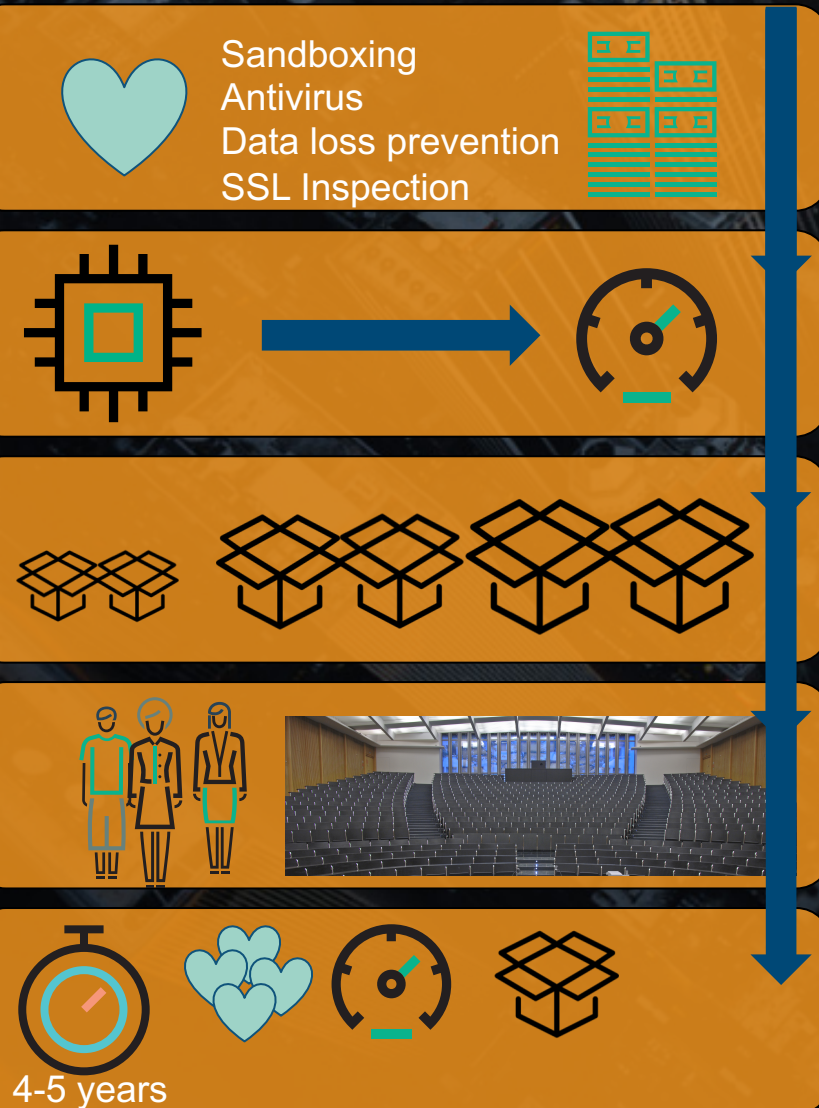
Security Core



360 Security  
Exchange Program



# Why cloud security partnerships



# Beyond Security Enforcement

## UEBA - Introspect integration

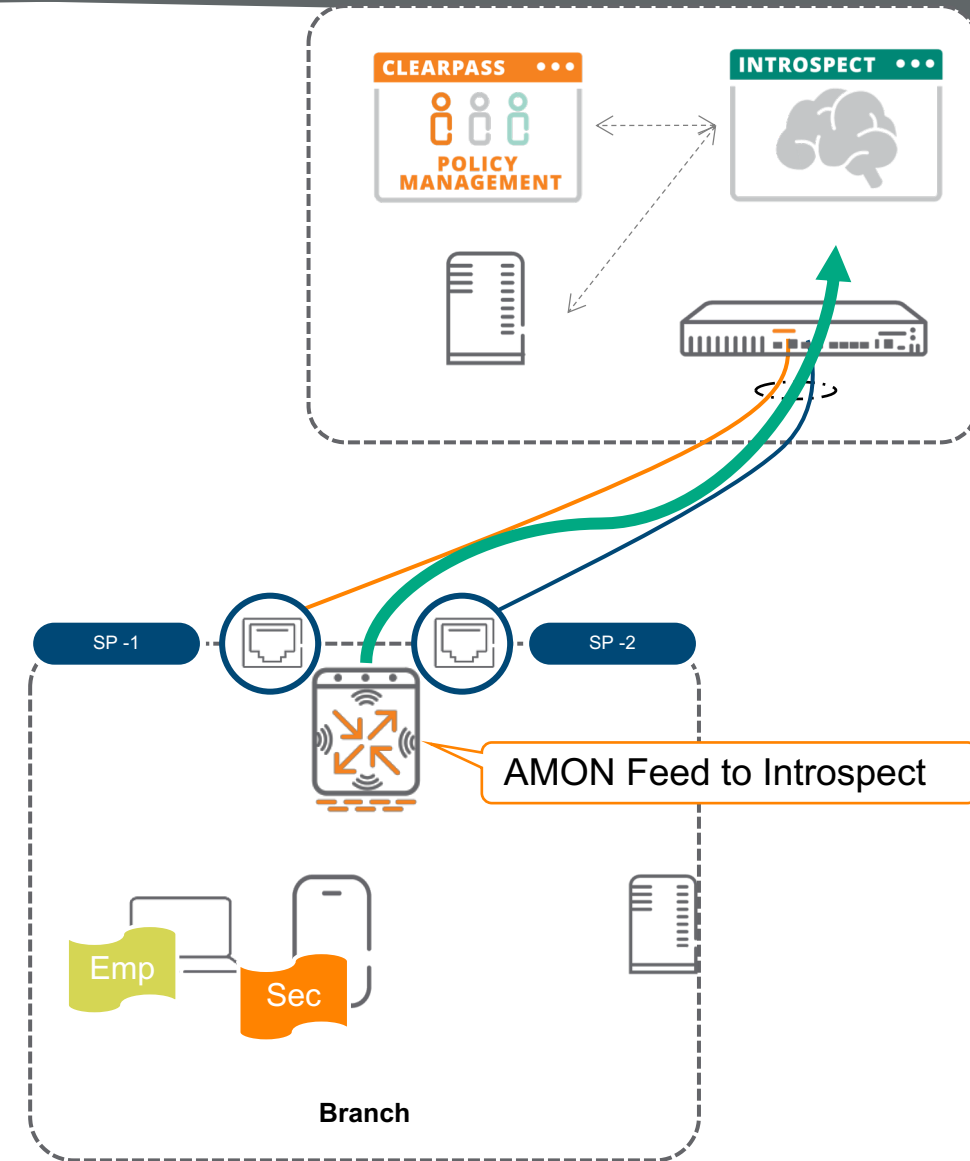
- 1 ClearPass assigns user role
- 2 Introspect integrated with ClearPass and other user services
- 3 GW Sends FW metadata (AMON feed) to Introspect



Security Core



360 Security  
Exchange Program



# Beyond Security Enforcement

## UEBA - Introspect integration

## Walkthrough

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**  
TECH TALK LIVE

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

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 8
- ☐ ms-communicator 4
- ☐ Skype 4
- ☐ Outlook 3
- ☐ HTTP 2
- ☐ Facebook 1
- ☐ Gmail 1
- ☐ iCloud 1
- ☐ ICMP 1

Location 6

- ☐ United States 708
- ☐ Australia 168
- ☐ Internal 57
- ☐ Japan 3
- ☐ Switzerland 2

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

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	1.11.1	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, 71.4	
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	1.11.1	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.cape networks... 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	

# SD-Branch Security



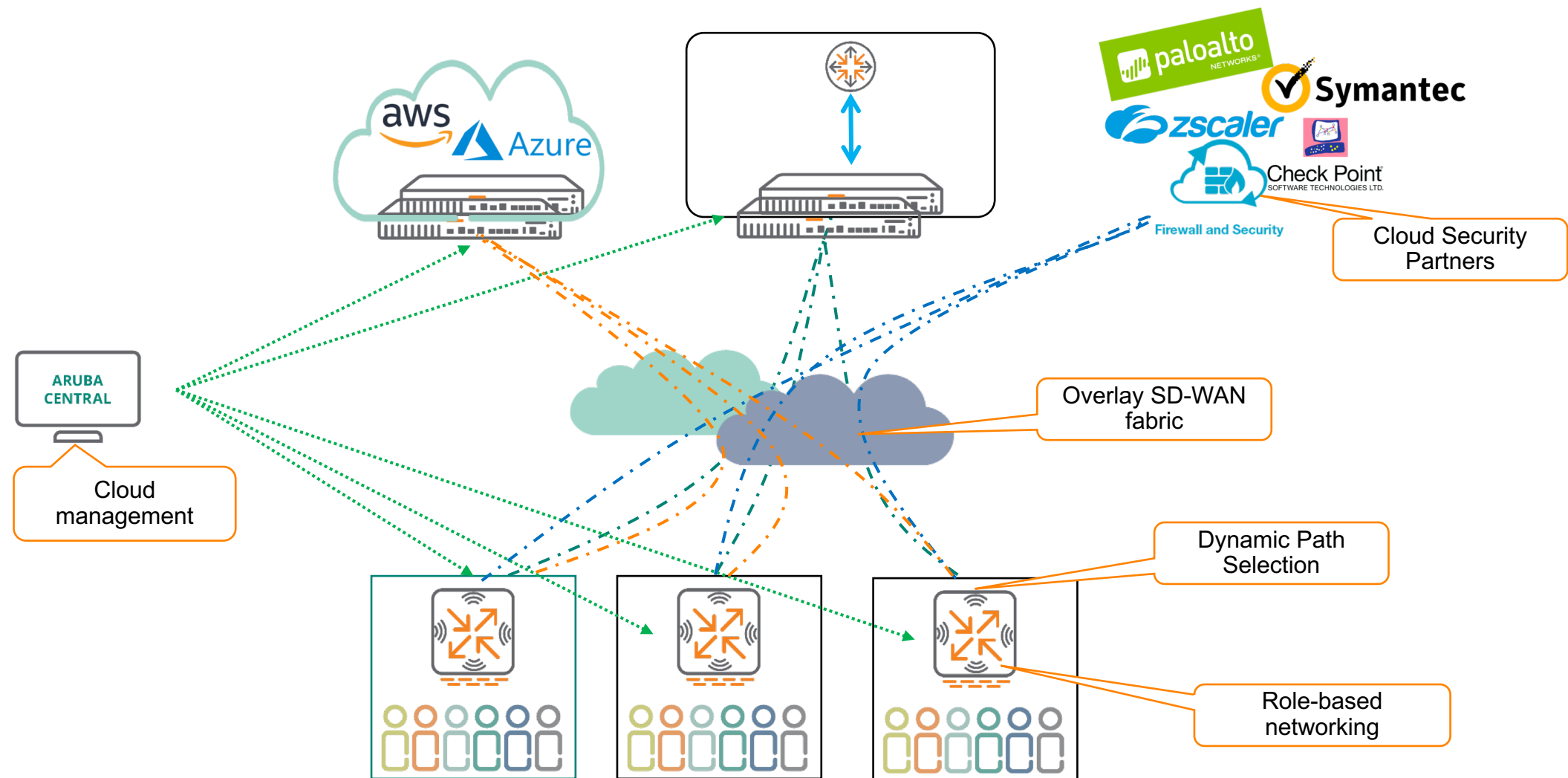
Security Core



360 Security  
Exchange Program

- ✓ Enterprise-grade Hardening
- ✓ Secure management and tunnels
- ✓ Stateful Firewall
- ✓ Deep Packet Inspection
- ✓ Role-Based Access
- ✓ Web Content, Reputation and Geolocation filtering with WebRoot's machine-learning technology
- ✓ Dynamic Segmentation with ArubaOS-SW
- ✓ Advanced Threat Detection with best-of-breed partners
- ✓ User and Entity Behavior Analytics with Introspect
- ✓ ...

# Aruba SD-WAN solution components



# Agenda



## SD-WAN 1.2

Solution components

Reminder...

## Public Cloud

Single VPC/VNET

Multi-VPC

Orchestration

## SD-WAN 1.5

Underlay routing

Tunnel Orchestration

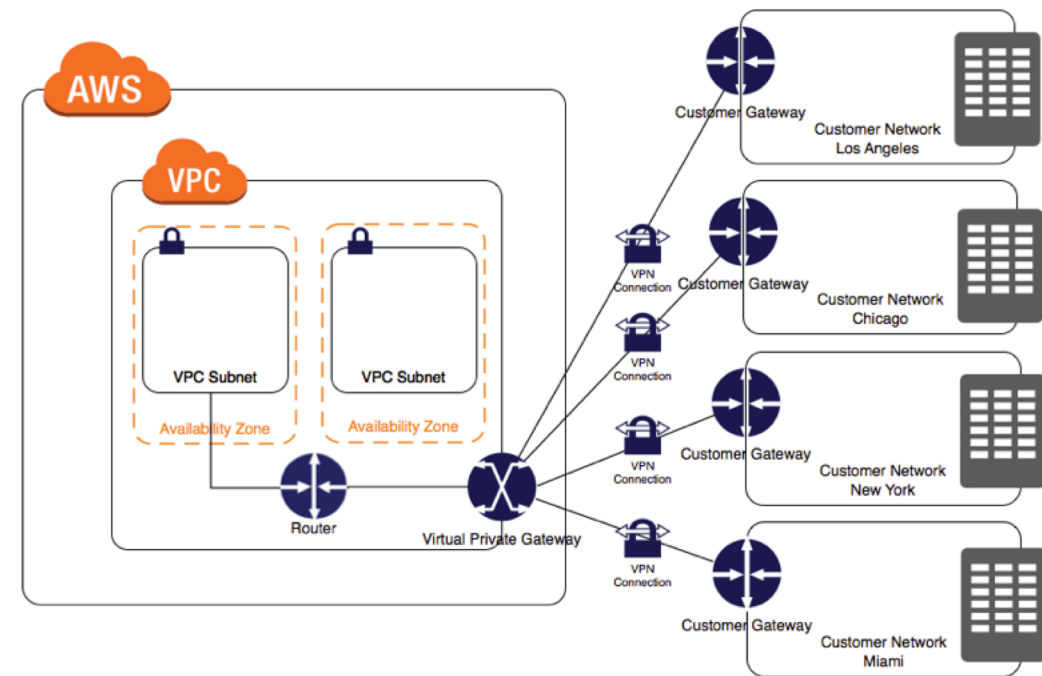
Route Orchestration

Transition

# Branch to Cloud Connectivity

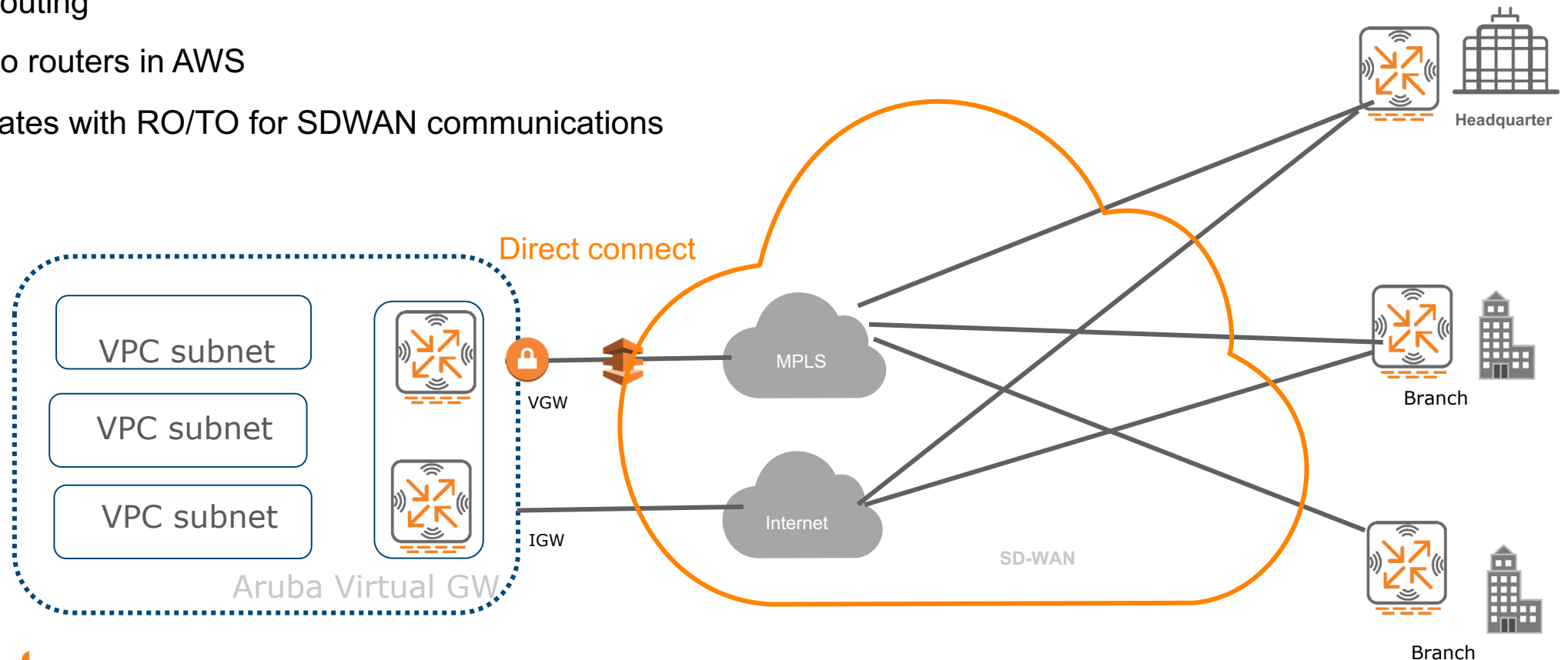
## AWS managed VPN service - Why do we need a vGW?

- Restrictive – 10 VPN connections per VGW, one SA per tunnel
- Charged per hour - \$72 per month for a pair of tunnels
- Hard to manage at Scale, no policy based routing
- Inconsistent architecture for different types – Direct connect underlay and overlay based VPN



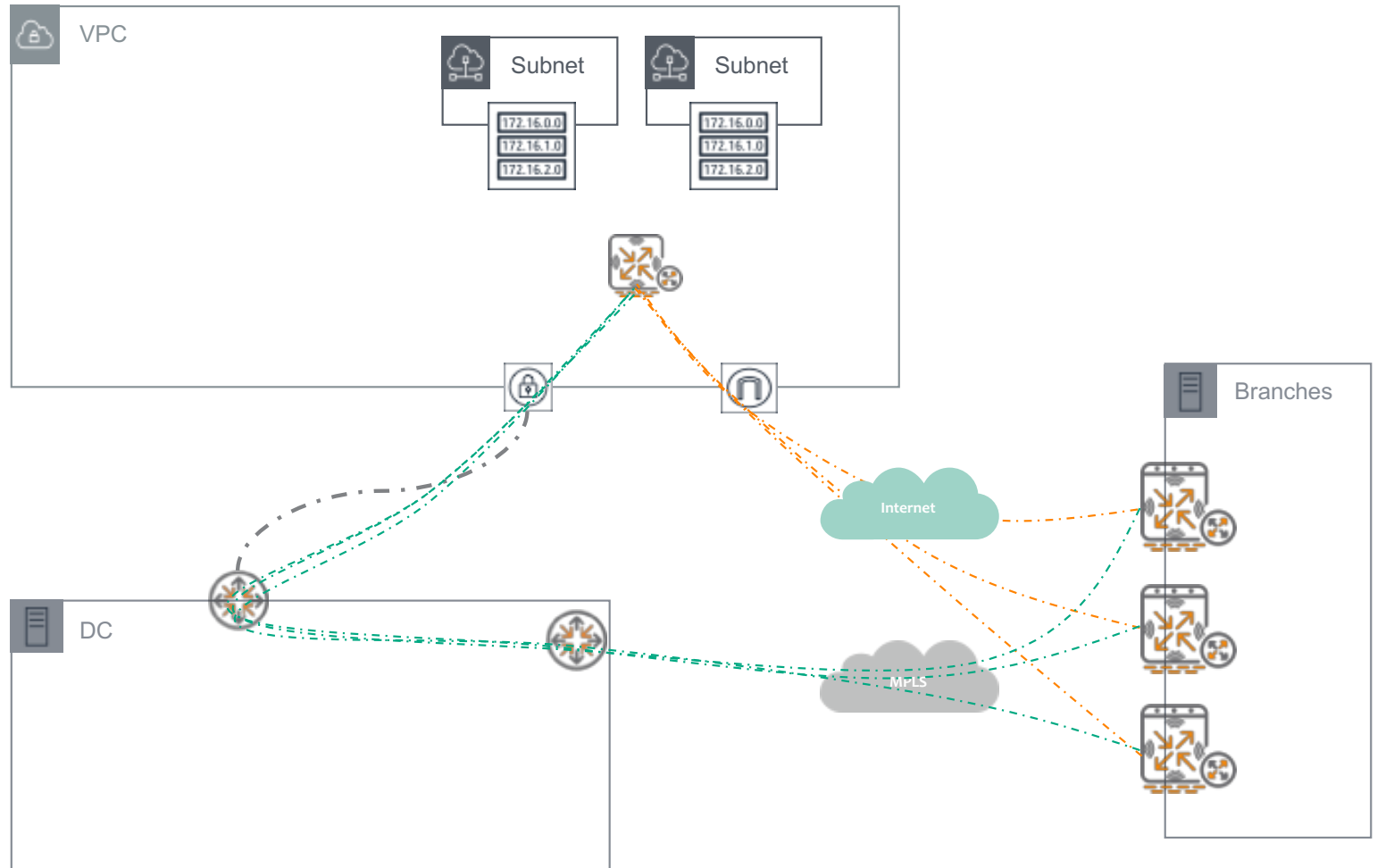
# Aruba Virtual Gateway with Full Orchestration

- Increased VPN scale (1600 tunnels on VGW-500 SKU)
- Supports Reverse Path Pinning – Allowing LB/DPS in the Branch
- Dynamic Routing
  - BGP to routers in AWS
  - Integrates with RO/TO for SDWAN communications



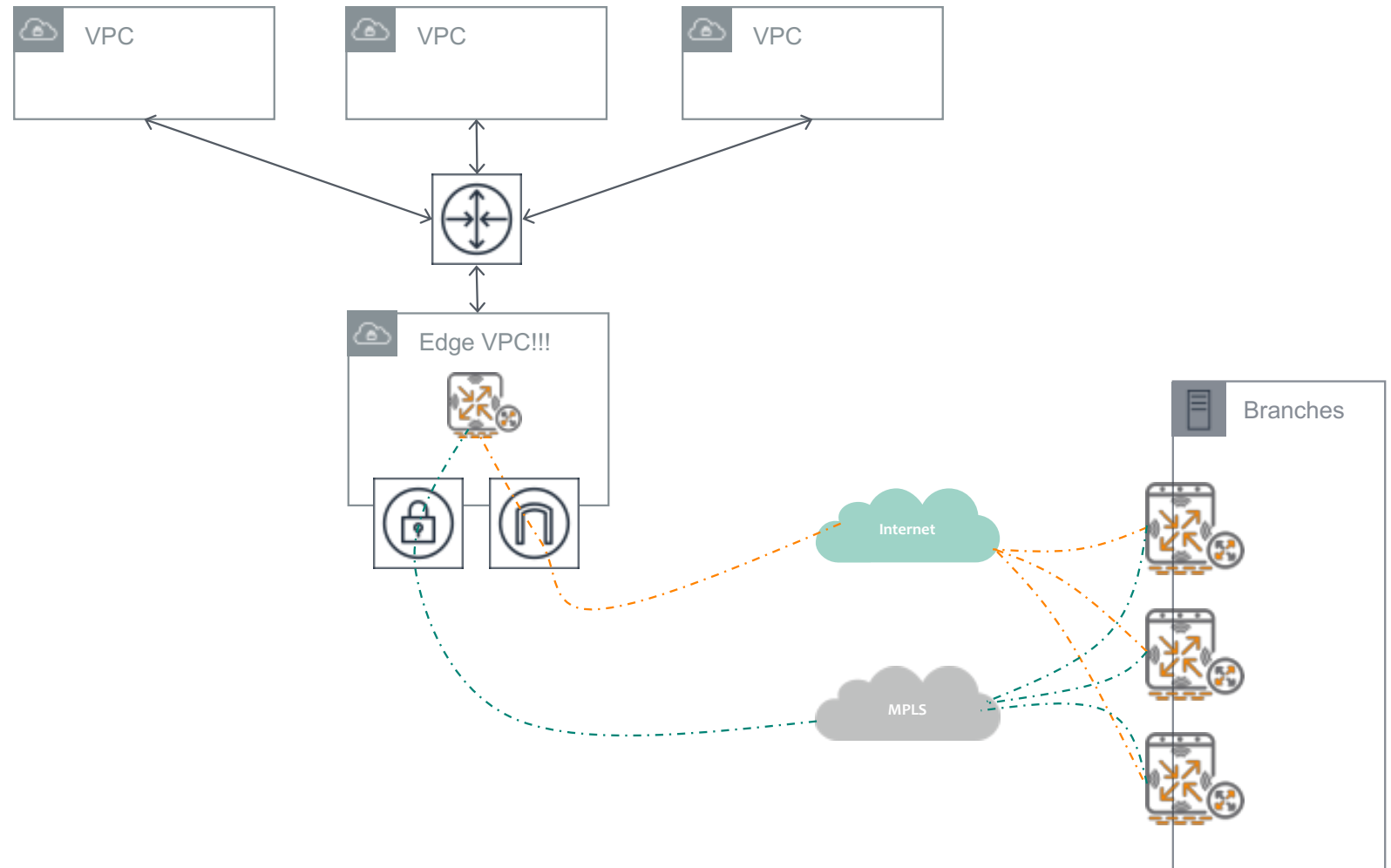
# Networking with single VPC

- **Region:** Oregon
- **VPC:** aruba-sdbranch
- **AZ:** i3 per region
- **Internet GW** – Resource to connect to Internet
- **VPN GW** – Resource to establish DirectConnect with your DC
- Route table attached subnets (same route table can be re-used)
- Elastic IP – Maps a public IP address to an internal resource
- ...
- NAT GW, Peering connections, security groups, encryption keys...



# Networking with multiple VPCs (ii)

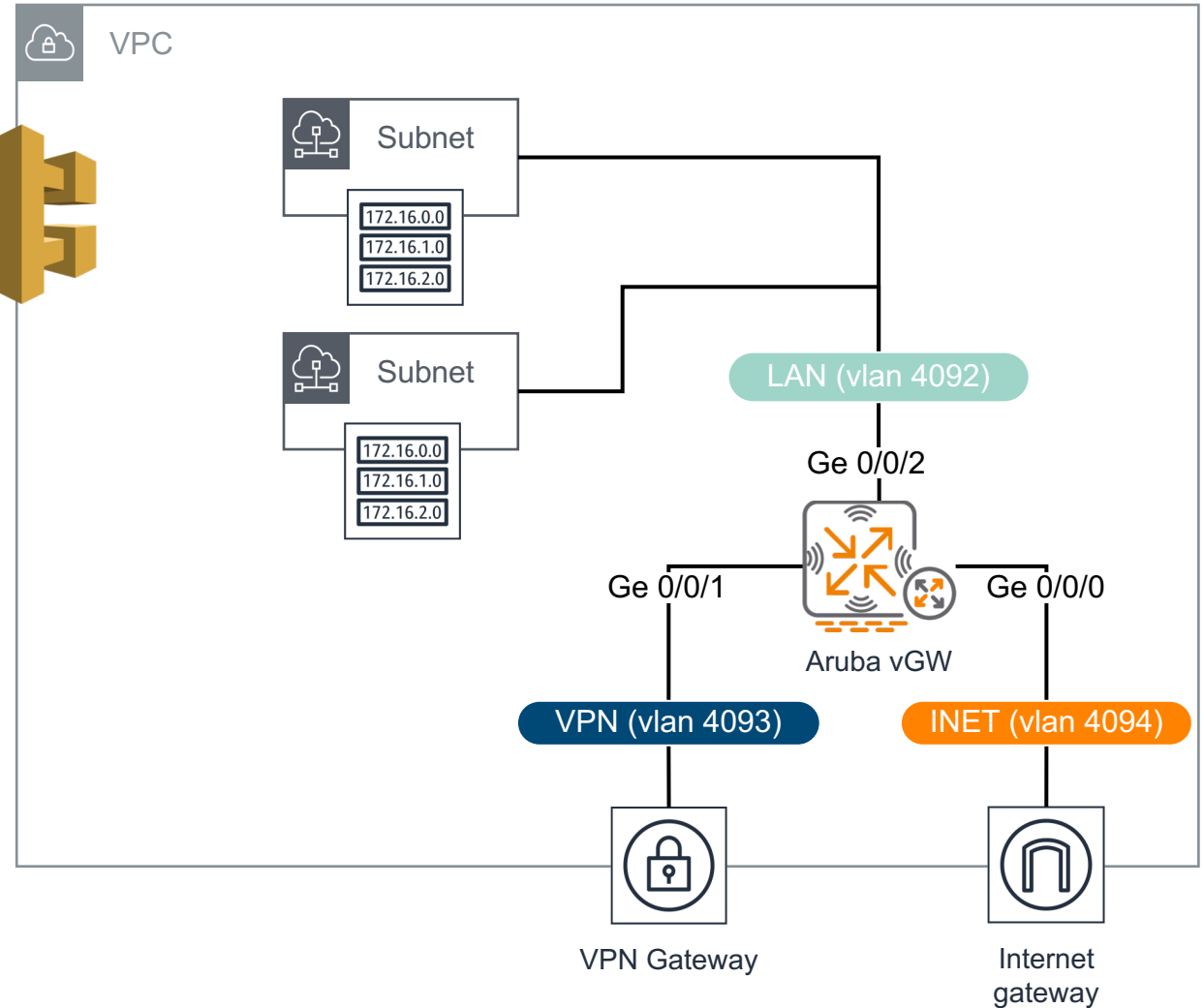
- Region: Oregon
- Transit Gateway: aruba-sdbranch
- Advertise routes via BGP to the Transit Gateway



# Orchestrated vGW bringup



API



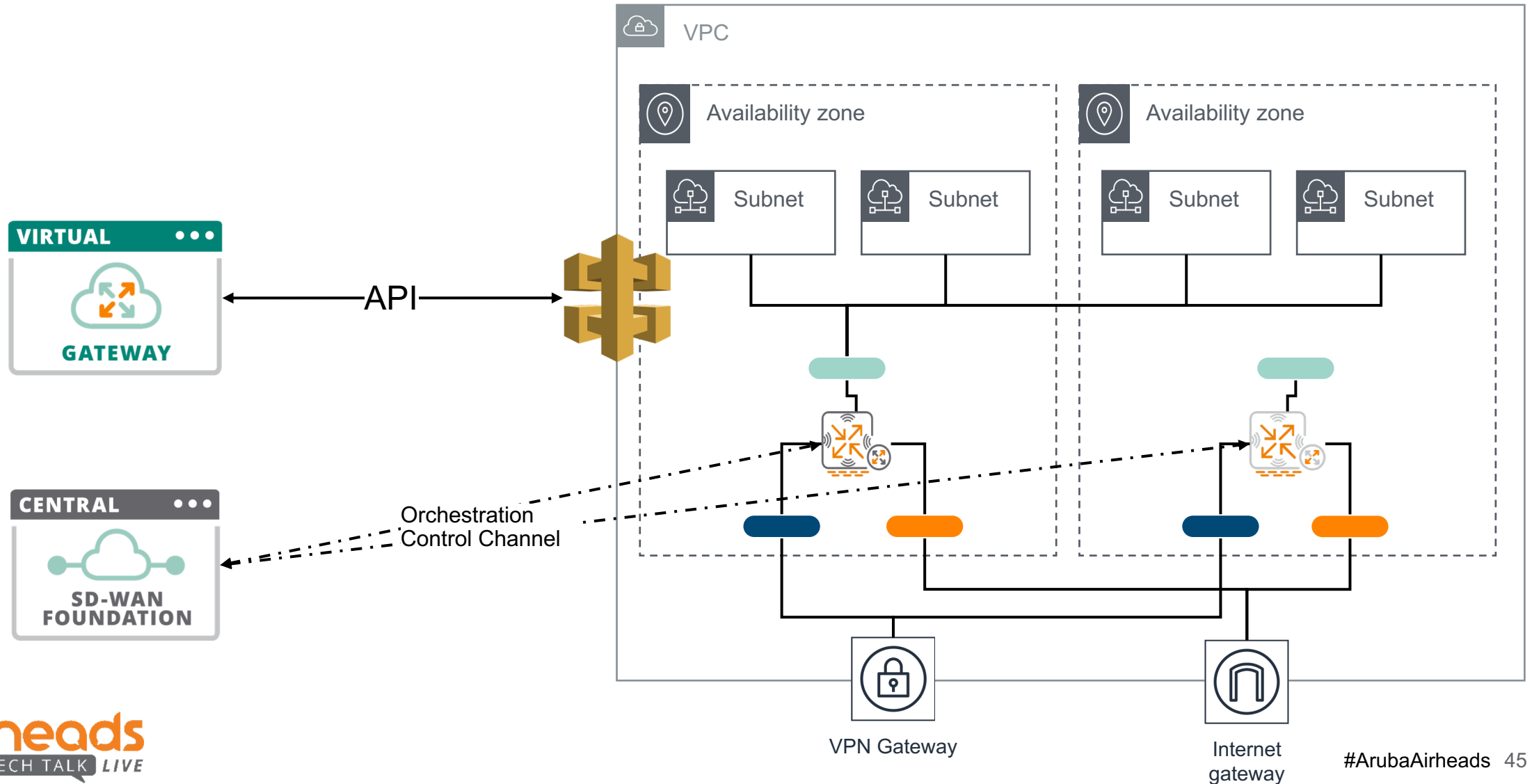
## Needs:

- 3rd party ARN token
- /24 subnet for interconnects (8\* /27s)

## Provides:

- AMI bringup
- 8\* ENIs
- Elastic IP
- Subnet routing table pointing to vGW
- HA (cont...)

# Orchestrated HA





airheads  
TECH TALK LIVE



# Agenda



## SD-WAN 1.2

Solution components

Reminder...

## Public Cloud

Single VPC/VNET

Multi-VPC

Orchestration

## SD-WAN 1.5

Underlay routing

Tunnel Orchestration

Route Orchestration

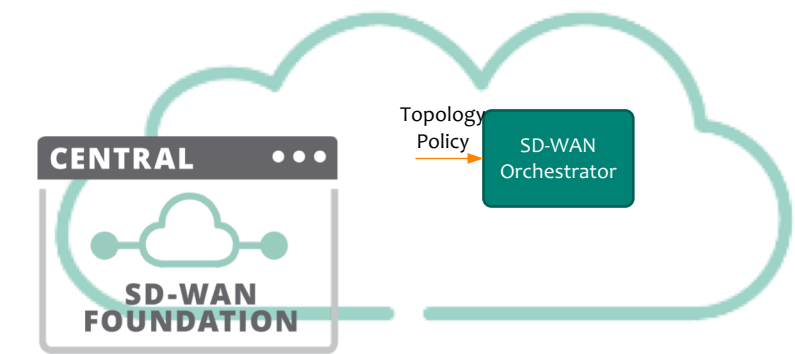
Transition

# SD-WAN Orchestrator

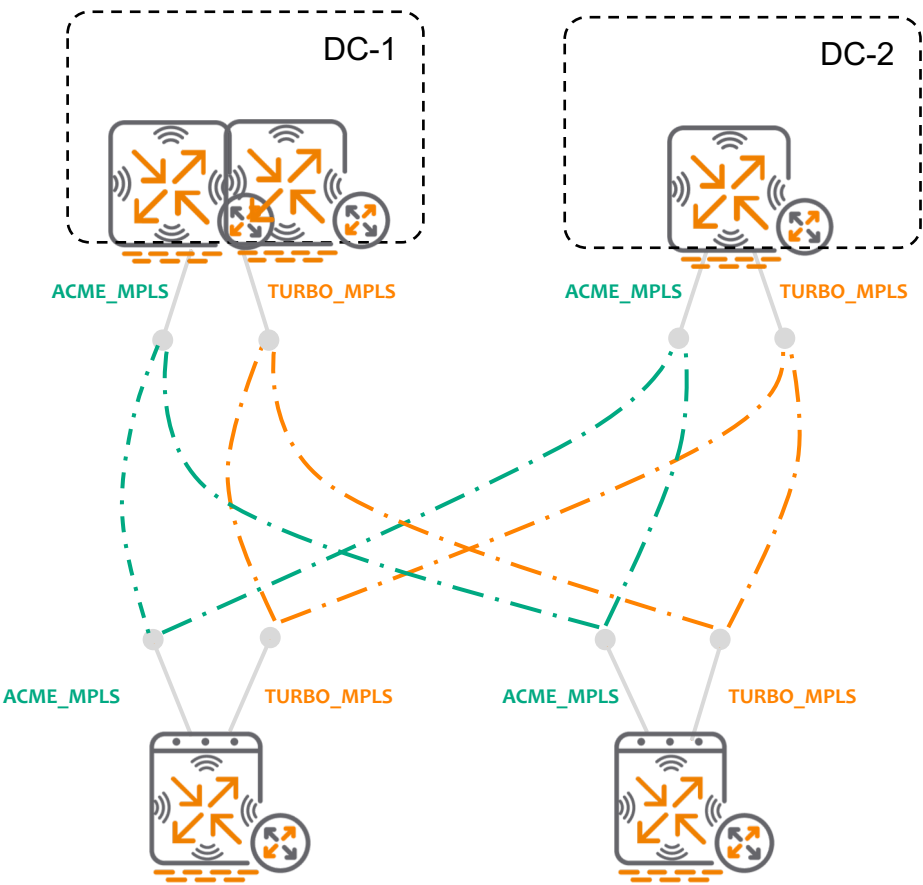
Automatic set-up of overlay tunnels and routes for SD-WAN

# SD-WAN Orchestrator - Overlay Tunnels

Private circuits

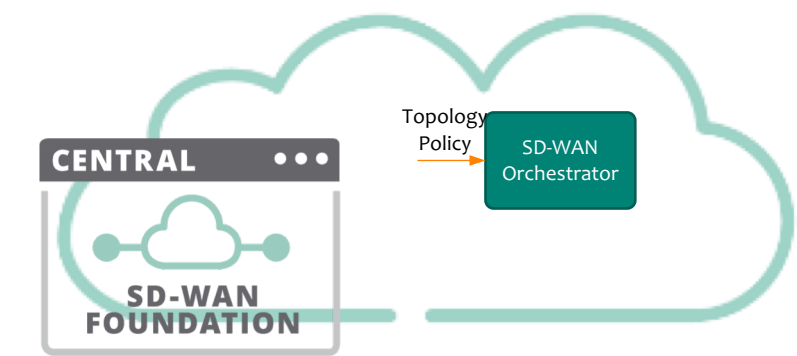


SRC	DST	TYPE	Tag	Cost
BG-1	DC-1-VPNC-1	MPLS	ACME	10
BG-1	DC-1-VPNC-2	MPLS	ACME	20
BG-1	DC-2-VPNC-1	MPLS	TURBO	30
...				

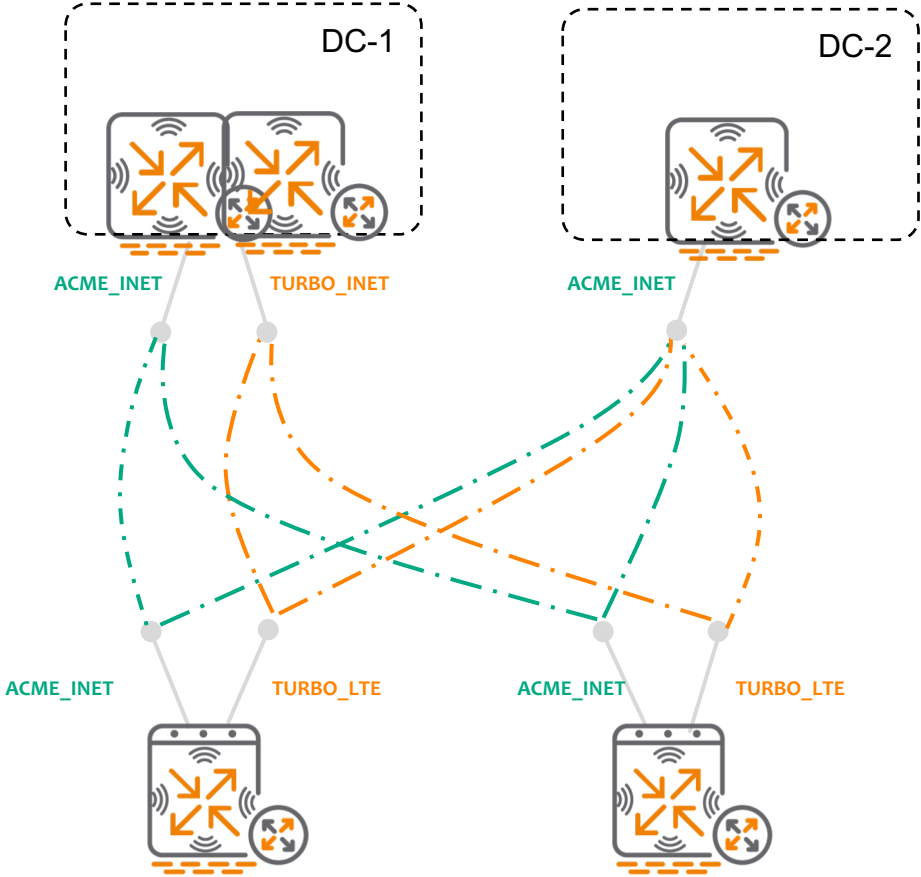


# Overlay Tunnel Orchestrator

## Public circuits



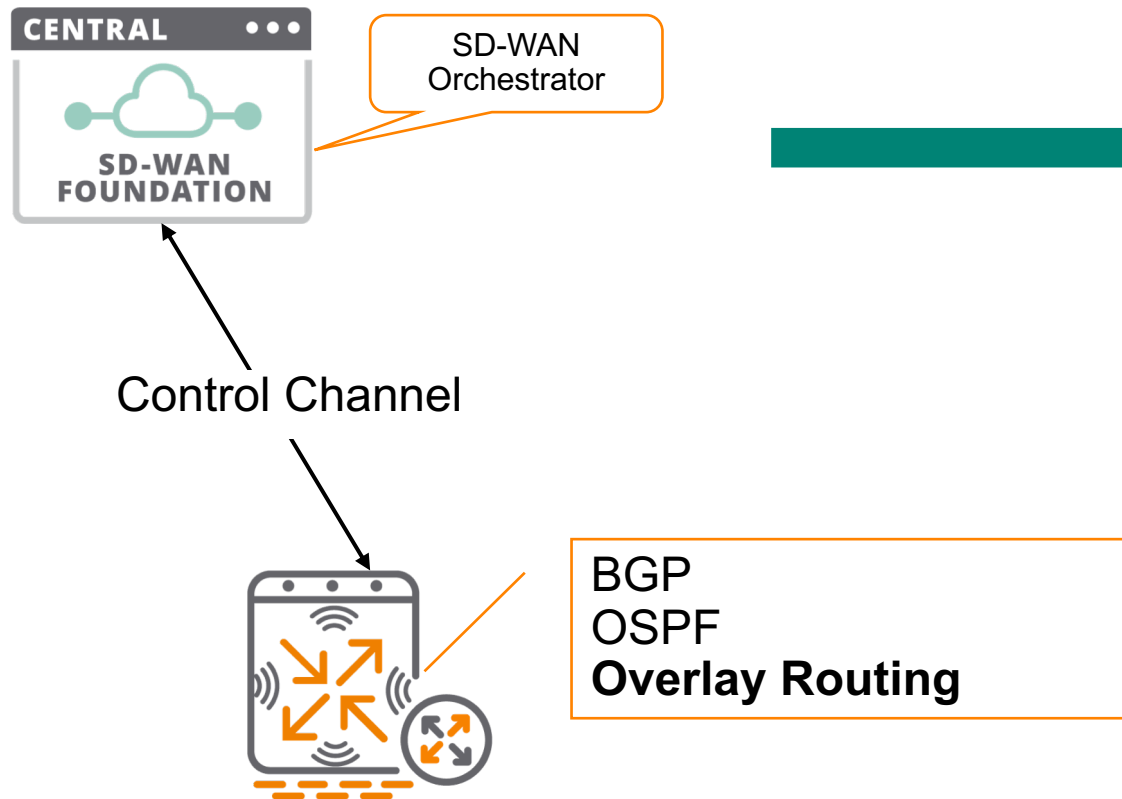
SRC	DST	TYPE	Tag	Cost
BG-1	DC-1-VPNC-1	INET	ACME	10
BG-1	DC-1-VPNC-2	INET	ACME	20
BG-1	DC-2-VPNC-1	INET	TURBO	30
...				



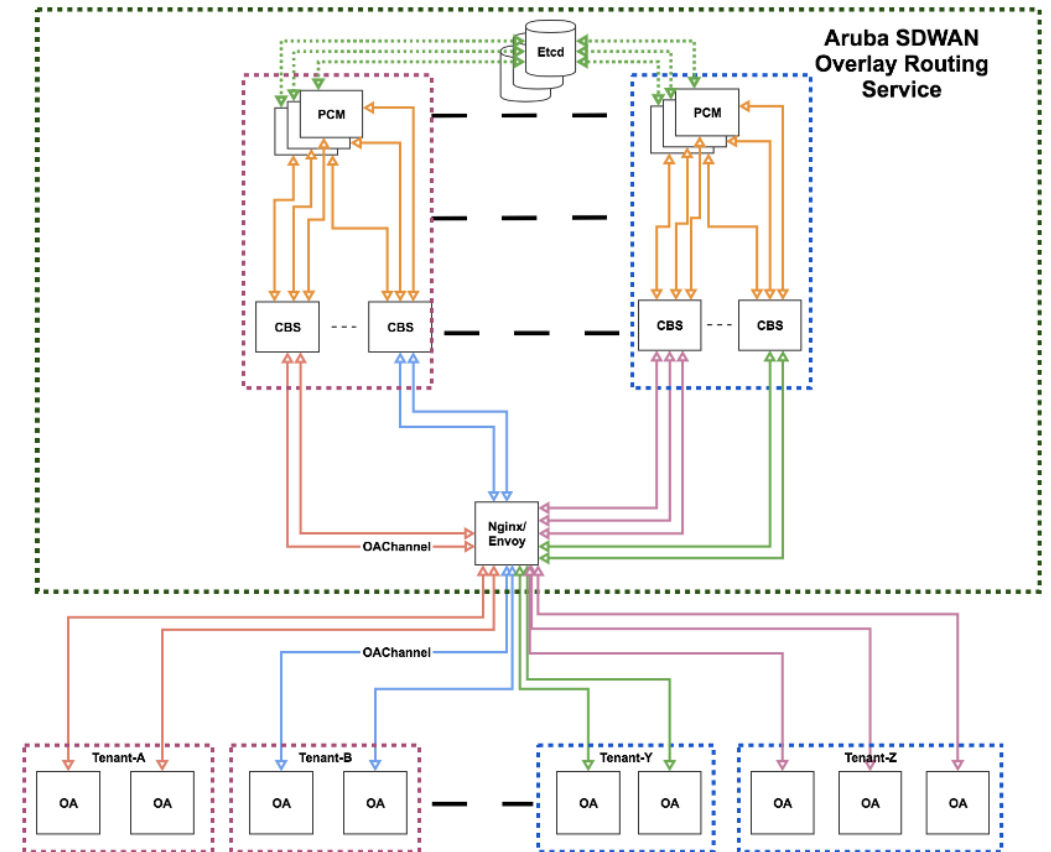
# SD-WAN Orchestrator - Overlay Routing

Building blocks

## Overlay Agent Communication

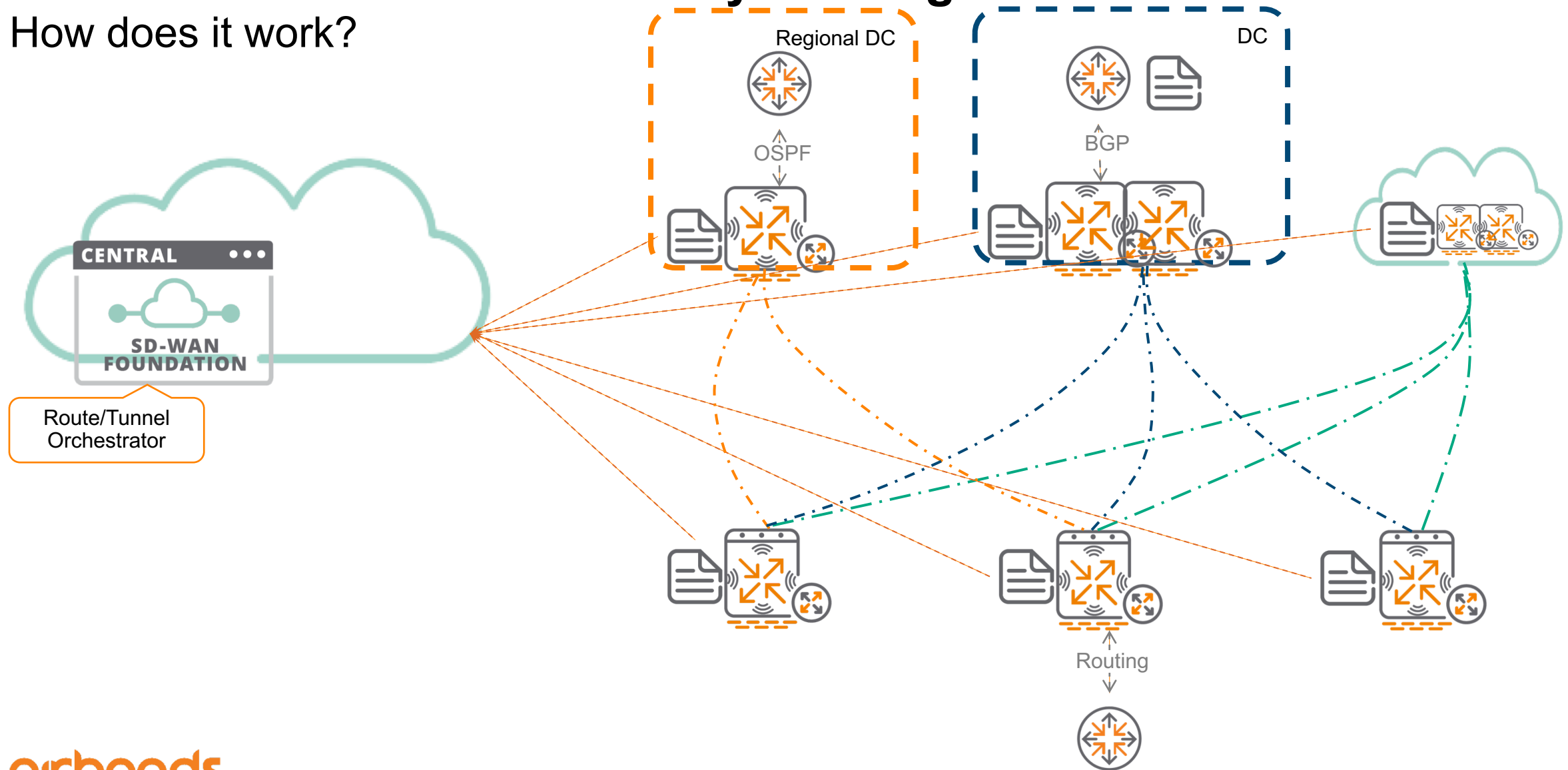


## Orchestration Service Architecture



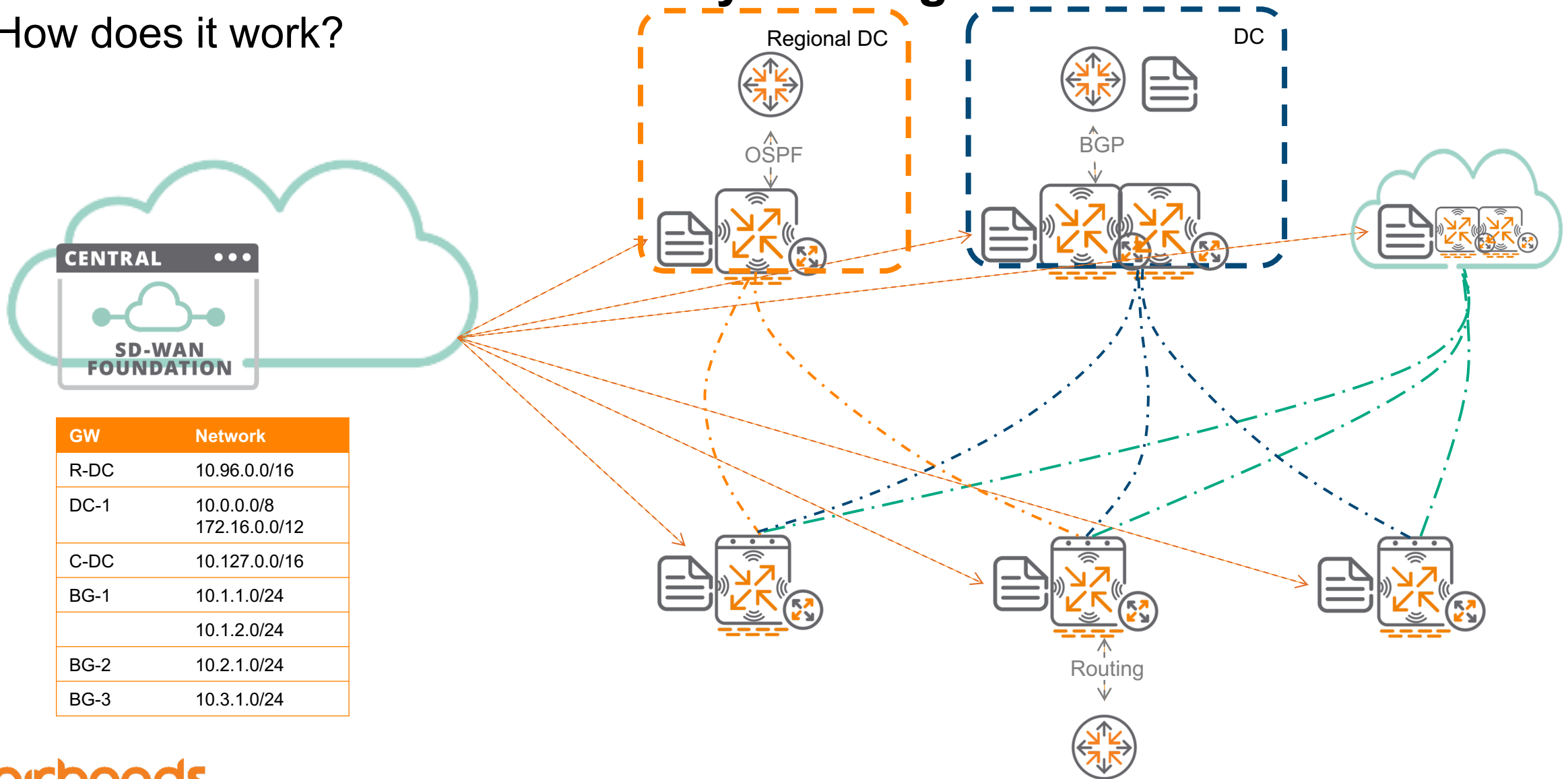
# SD-WAN Orchestrator - Overlay Routing

How does it work?



# SD-WAN Orchestrator - Overlay Routing

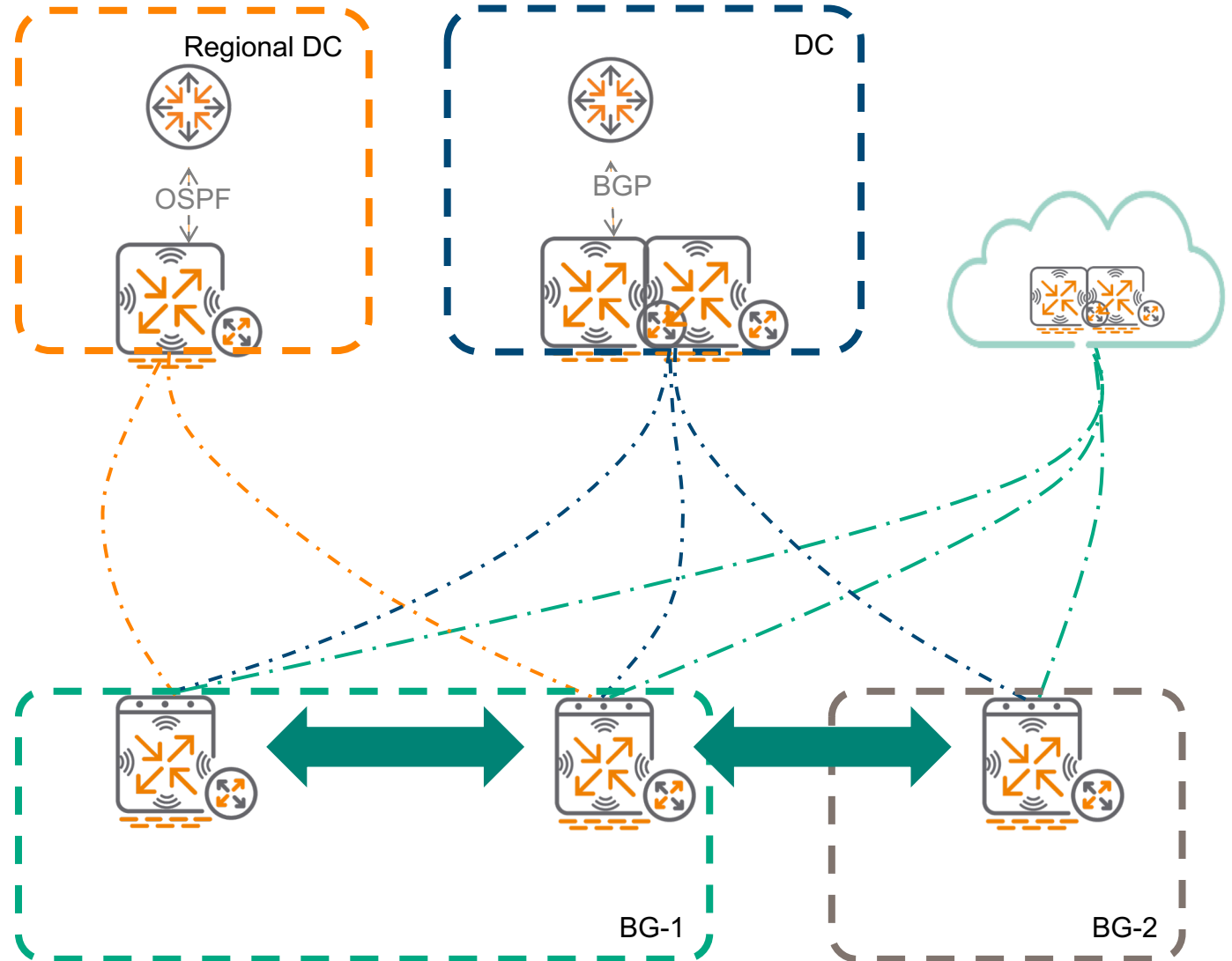
How does it work?



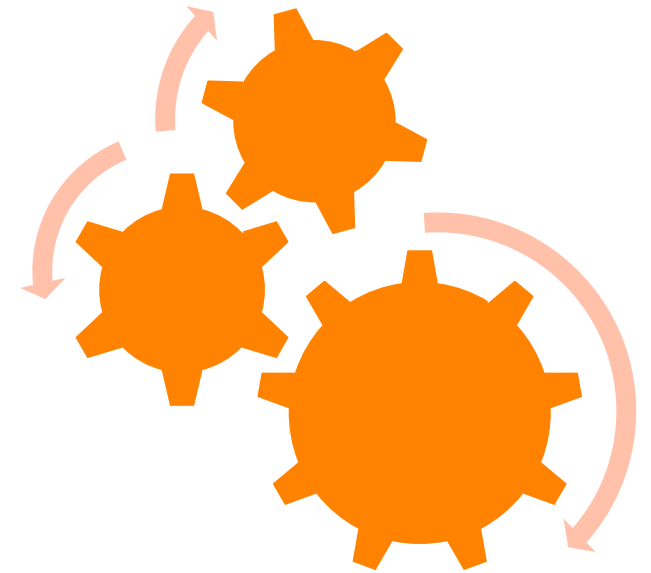
# DC Preference

Which hub for Branch to Branch?

- 1 Regional DC Primary for its region
- 2 Aggregate routes in the DC (recommended anyway)
- 3 Allow Branch 2 branch?

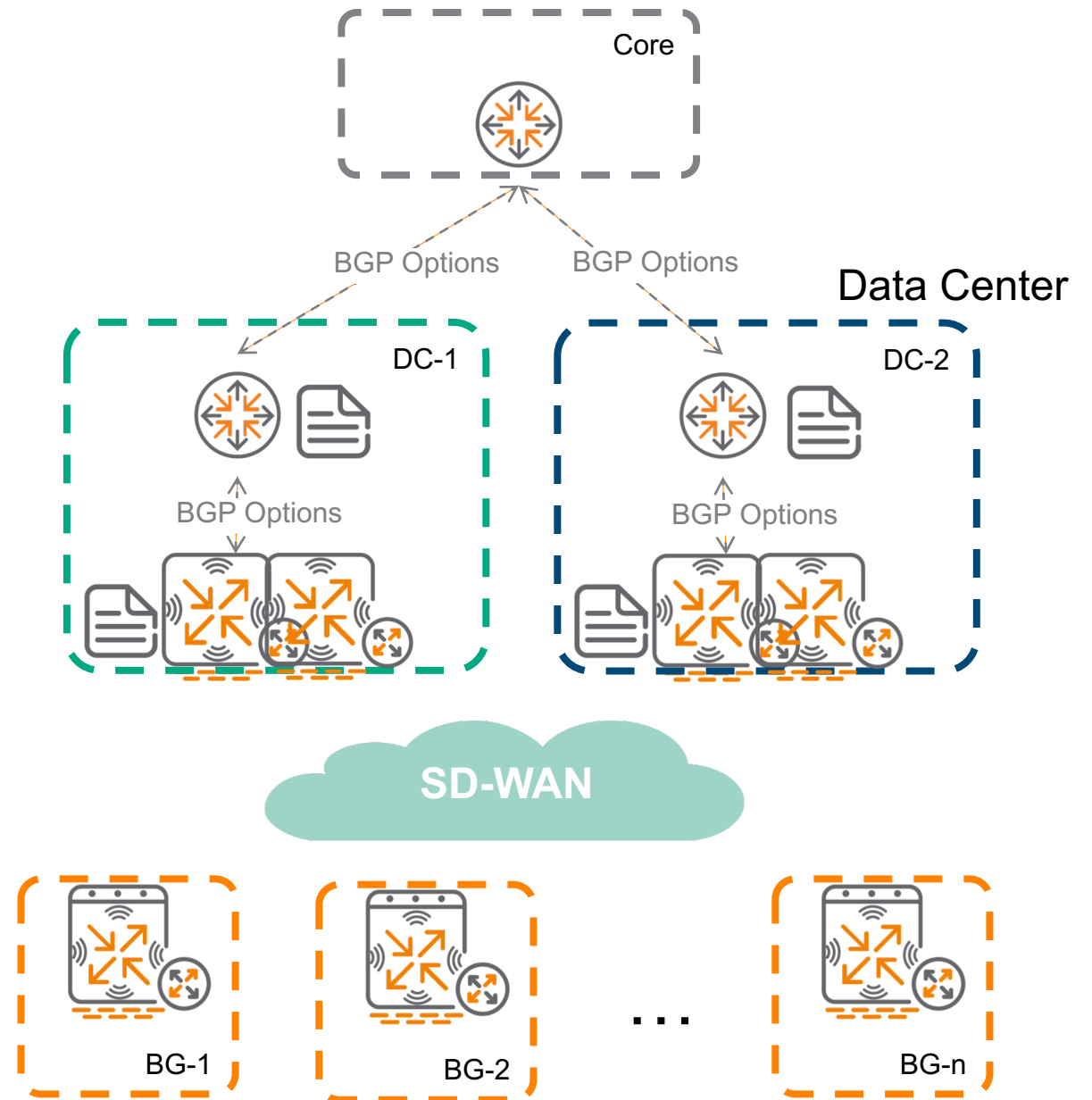


# SD-WAN Orchestrator in action



# Introducing BGP at Headend

- BGP standard features :
  - Local-Pref
  - Auto-Cost (MED)
  - AS-Prep
  - Route Maps
  - Communities
  - eBGP/iBGP



# BGP Standard feature set

- BGP peering – EBGp / IBGP
- Hold/keepalive timers tuning
- Redistributing BGP routes – Overlay, static, OSPF, connected
- Neighbor – route-maps, nexthop-self, allowas-in, ebgp multihop, update source
- Prefix lists for filtering
- Route-maps with match and set conditions

```
router bgp <autonomous-system-number>
```

```
router bgp router-id <router-id>
```

```
router bgp hold <hold-time>
```

```
router bgp keepalive <keepalive-time>
```

```
router bgp redistribute static [ OSPF | Overlay <metric>]
```

```
router bgp network <net-addr> <mask>
```

```
router bgp neighbor <ID><AS>
```

```
    update-source {ip-address }
```

```
    allowas-in
```

```
    ebgp-multihop
```

```
    next-hop-self
```

```
    route-map < route-map name> in | out
```

```
route-map <name> [permit | deny] <seq number>
```

```
    match ip [ address | next-hop] prefix-list <prefix list name>
```

```
    set as-path prepend [<as-number>] | [last-as <number of times to prepend as>]
```

```
    set community <number> | < as:nn> ! Either 4-byte number or 2-byte:2-byte number.
```

```
    set ip next-hop <addr>
```

```
    set local-preference <value>
```

```
    set metric <value>
```

```
    set origin  egp | igp
```

```
ip prefix-list <name> seq <seq no> [permit | deny] <address> <mask>
```

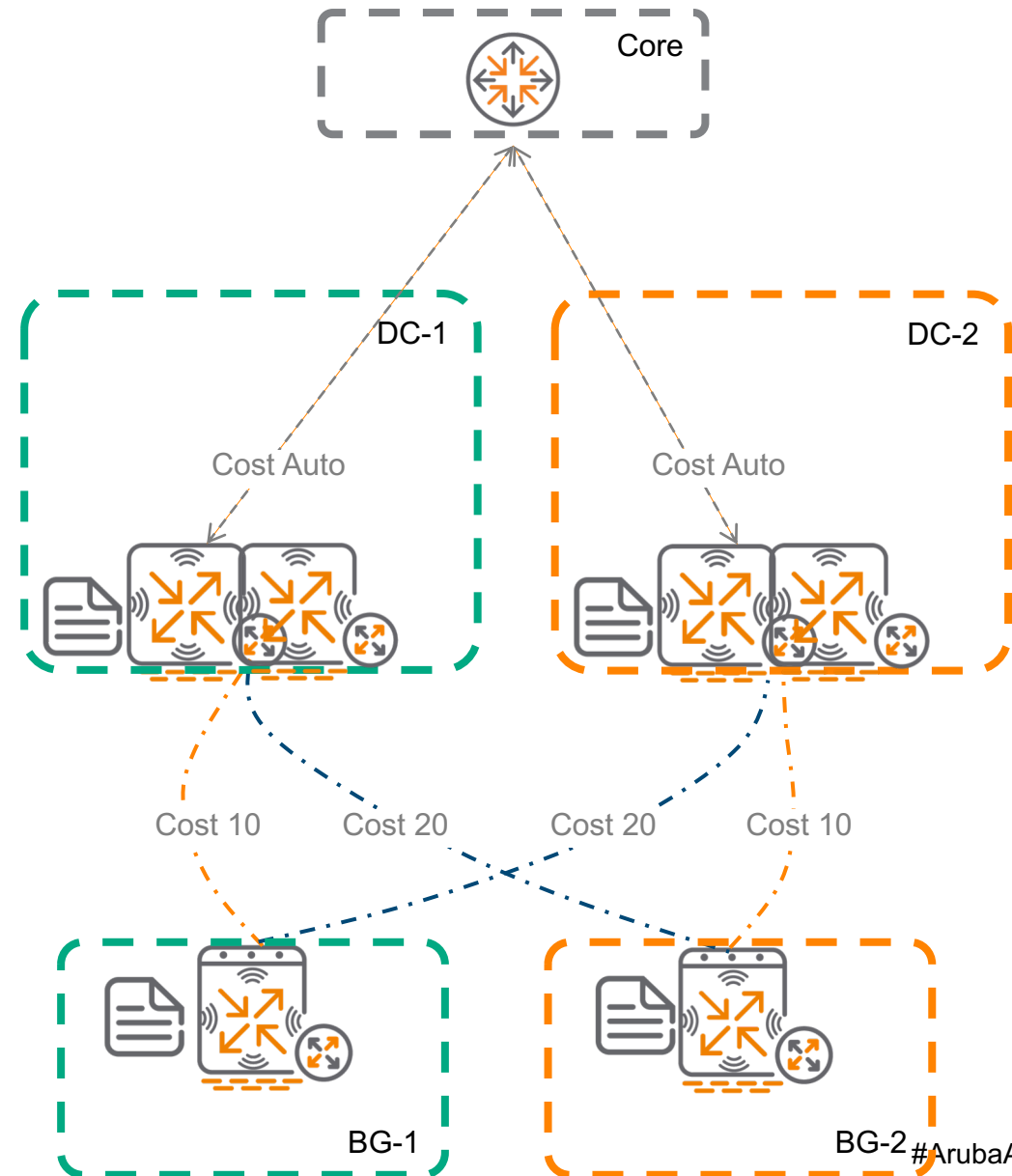
# Multiple Active Hubs

## BGP (i)

- 1 BG-1 Prefers DC-1
- 2 BG-2 Prefers DC-2
- 3 Auto-Propagate cost (MED)

Simplified BGP use-case

- Auto-Cost (MED)
- Local-Pref
- eBGP/iBGP



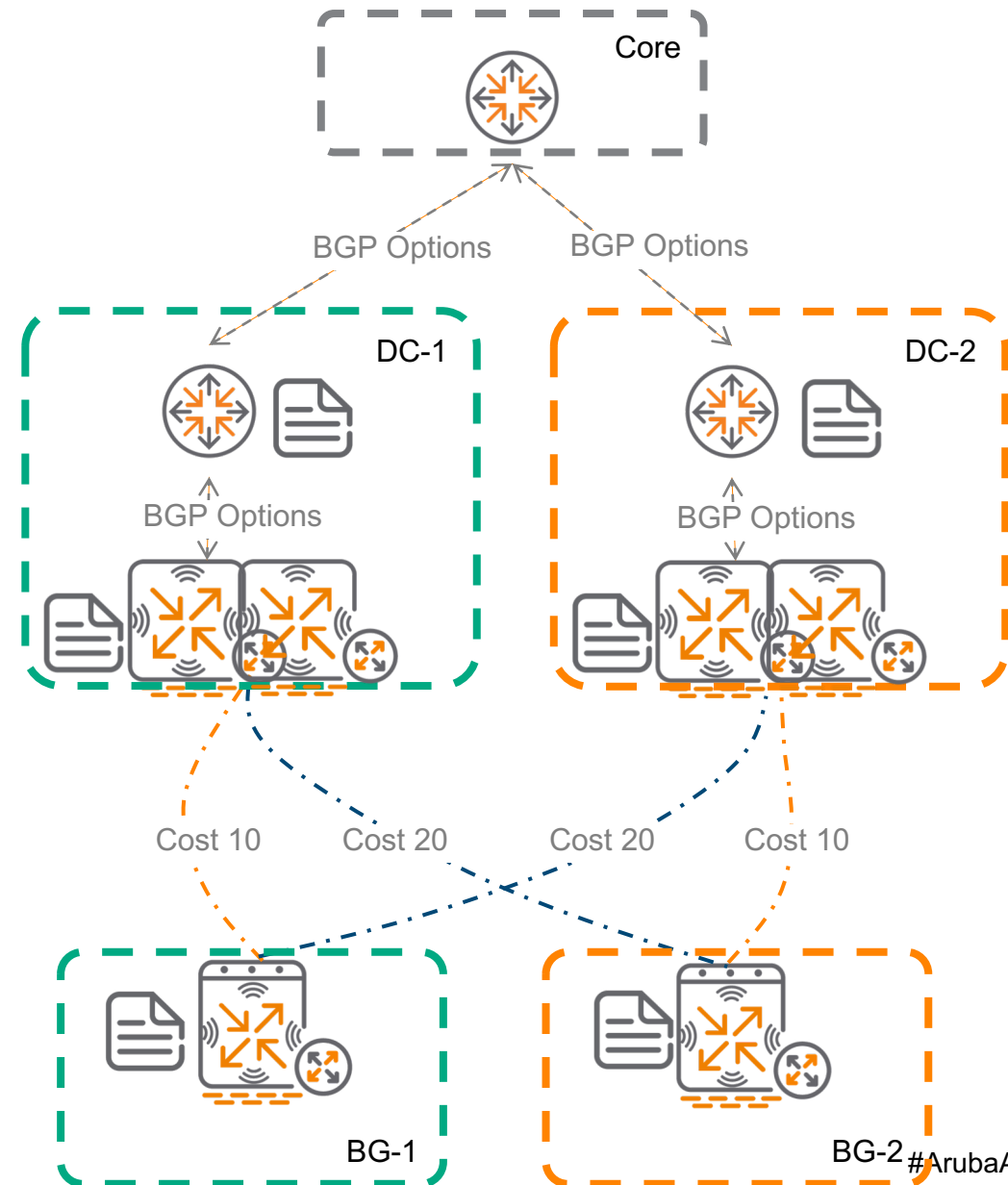
# Multiple Active Hubs

## BGP (ii)

- 1 BG-1 Prefers DC-1
- 2 BG-2 Prefers DC-2
- 3 Route Maps + ASPrep/MED/Community

Standard BGP implementation

- Route-Maps
- MED
- AS-Path prepending
- Local-Pref
- Communities
- eBGP/iBGP



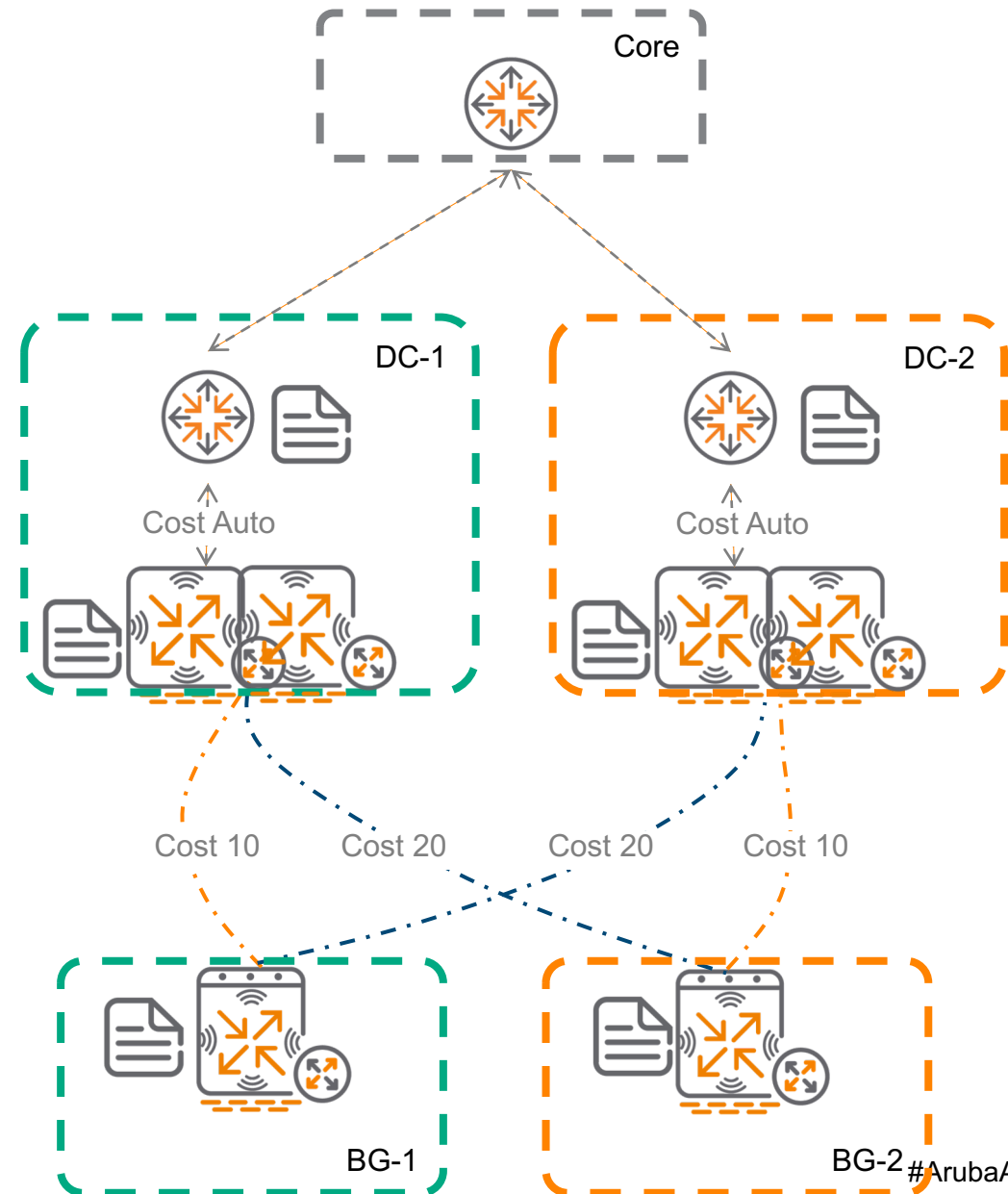
# Multiple Active Hubs

## OSPF

- 1 BG-1 Prefers DC-1
- 2 BG-2 Prefers DC-2
- 3 Auto-Propagate OSPF Cost

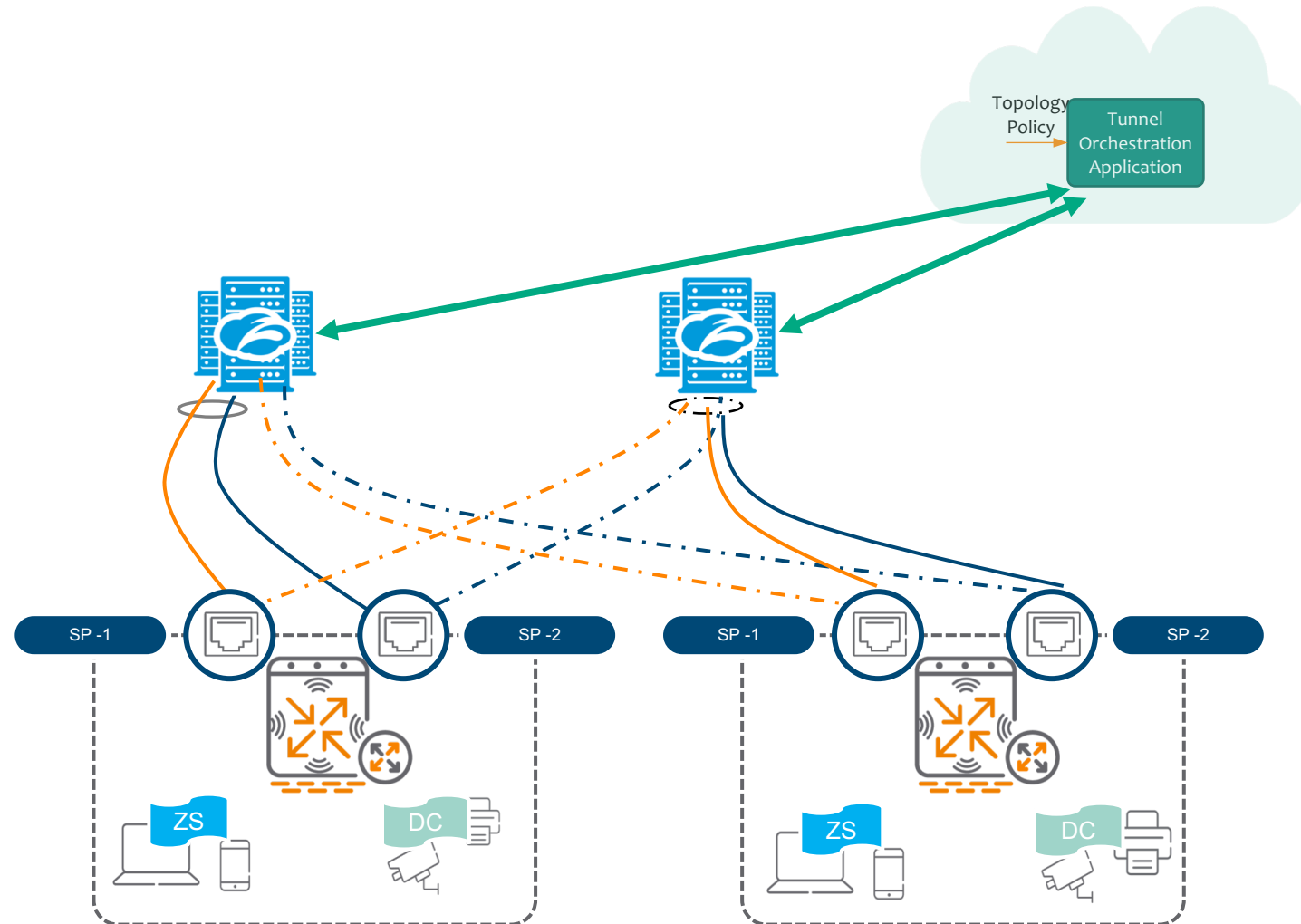
### New in OSPF

- Auto-Cost
- E1/E2 Routes



# Zscaler Orchestrated Integration

- 1 Tunnel Orchestrator gets info about GWs and available ZIA nodes
- 2 Locations/VPN Credentials created in Zscaler
- 3 Tunnel Orchestrator points each GW to the right ZIA node(s) and negotiates local-fqdn and PSK
- 4 PBR send the traffic through the active ZIA tunnel

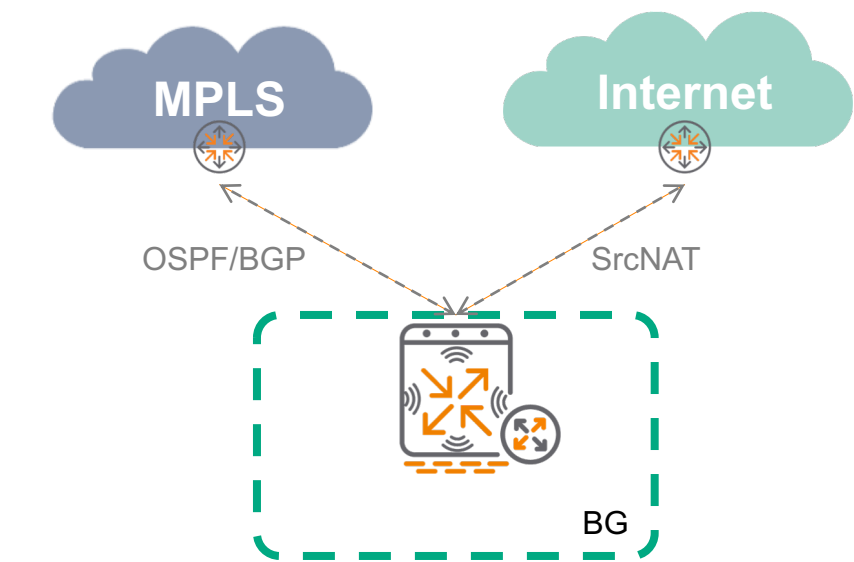


# Underlay only branch

## BGW as Cloud managed Gateway/firewall

Underlay Only!!!

Session view coming in Q2 CY19



SESSIONS SUMMARY

CURRENT ENTRIES

1853

MAX ENTRIES

16383

HIGH WATER MARK

8203

ALLOCATION FAILURES

120

DENIED ENTRIES

162

SESSIONS | LAST UPDATED: 5:45:01 PM

FILTERS

SOURCE IP

DESTINATION IP

APPLICATION / PORT

DESTINATION

FILTERED ENTRIES: 1853

▼ APPLICATION

App 1

▼ SOURCE IP

aa:bb:cc:dd

▼ DESTINATION

aa:bb:cc:dd

▼ PROTOCOL

TCP

▼ SOURCE PORT

0000

▼ APP PORT

0000 (HTTP)

▼ ACTION

Permit

▼ FLAGS

A, S, Y, F, J, O

▼ APPLICATION

App 2

▼ SOURCE IP

aa:bb:cc:dd

▼ DESTINATION

aa:bb:cc:dd

▼ PROTOCOL

TCP

▼ SOURCE PORT

0000

▼ APP PORT

0000 (HTTP)

▼ ACTION

Deny

▼ FLAGS

R, V, A, S, H, T, P, C, M, ...

FIREWALL POLICY

MATCHING NAME (ACL)  
lorem ipsum

MATCHING RULE (ACE)  
lorem ipsum

ACTION  
Permit/Deny

TIME STAMP

START TIME  
lorem ipsum

RECEIVE TIME  
lorem ipsum

WEBCC ATTRIBUTES

WEBCC CATEGORY  
lorem ipsum

WEBCC REPUTATION  
lorem ipsum

APPLICATION

APP CATEGORY  
lorem ipsum

MATCHING PBR ("R")

RACL POLICY NAME  
lorem ipsum

RACL POLICY RULE  
lorem ipsum

HITS  
lorem ipsum

NEXT-HOP INTERFACE/TUNNEL  
lorem ipsum

DYNAMIC PATH SELECTION (DPS)

POLICY NAME  
lorem ipsum

MATCHING POLICY RULE  
lorem ipsum

IS THE LATEST UPDATED POLICY USED?  
lorem ipsum

UPLINK/PATH & COMPLIANCE  
lorem ipsum

CHOSEN UPLINK INTERFACE  
lorem ipsum

CHOSEN UPLINK PATH (TUNNEL)  
lorem ipsum

IS IT PICKING PRIMARY, SECONDARY, TERTIARY PATH?  
lorem ipsum

COMPLIANCE OF THE PATH (OVERLAY & UNDERLAY)  
lorem ipsum

App 3

aa:bb:cc:dd

aa:bb:cc:dd

TCP

0000

0000 (HTTP)

Deny

F, H, T, P, L, G, E, I

App 4

aa:bb:cc:dd

aa:bb:cc:dd

TCP

0000

0000 (HTTP)

Permit

L, C, U, M, J, O, H, Q

App 5

aa:bb:cc:dd

aa:bb:cc:dd

TCP

0000

0000 (HTTP)

Permit

G, E, I, B, M, U, L, E, I, B, ...

App 6

aa:bb:cc:dd

aa:bb:cc:dd

TCP

0000

0000 (HTTP)

Deny

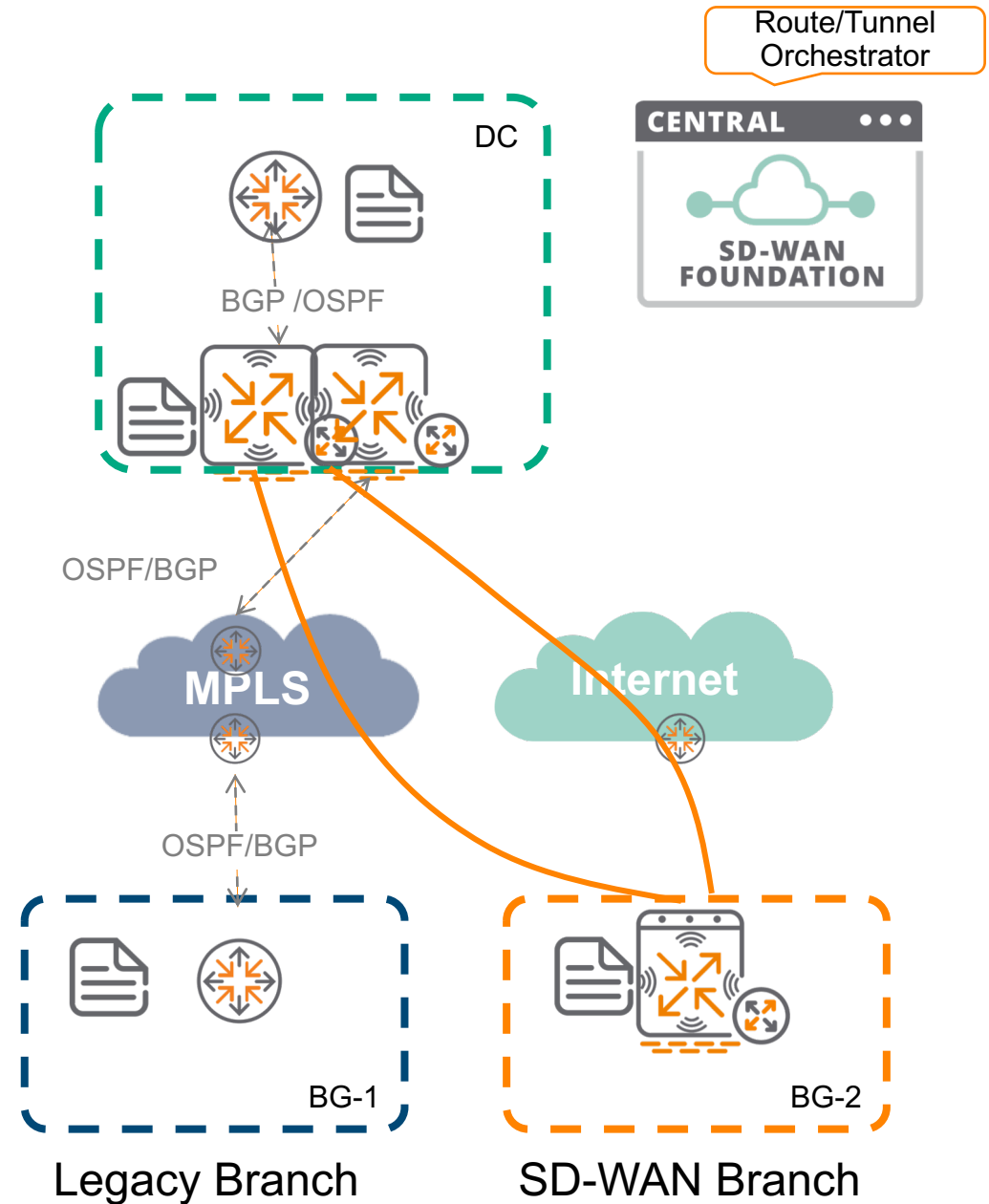
L, G, E, I

# Migration

# Correct Migration

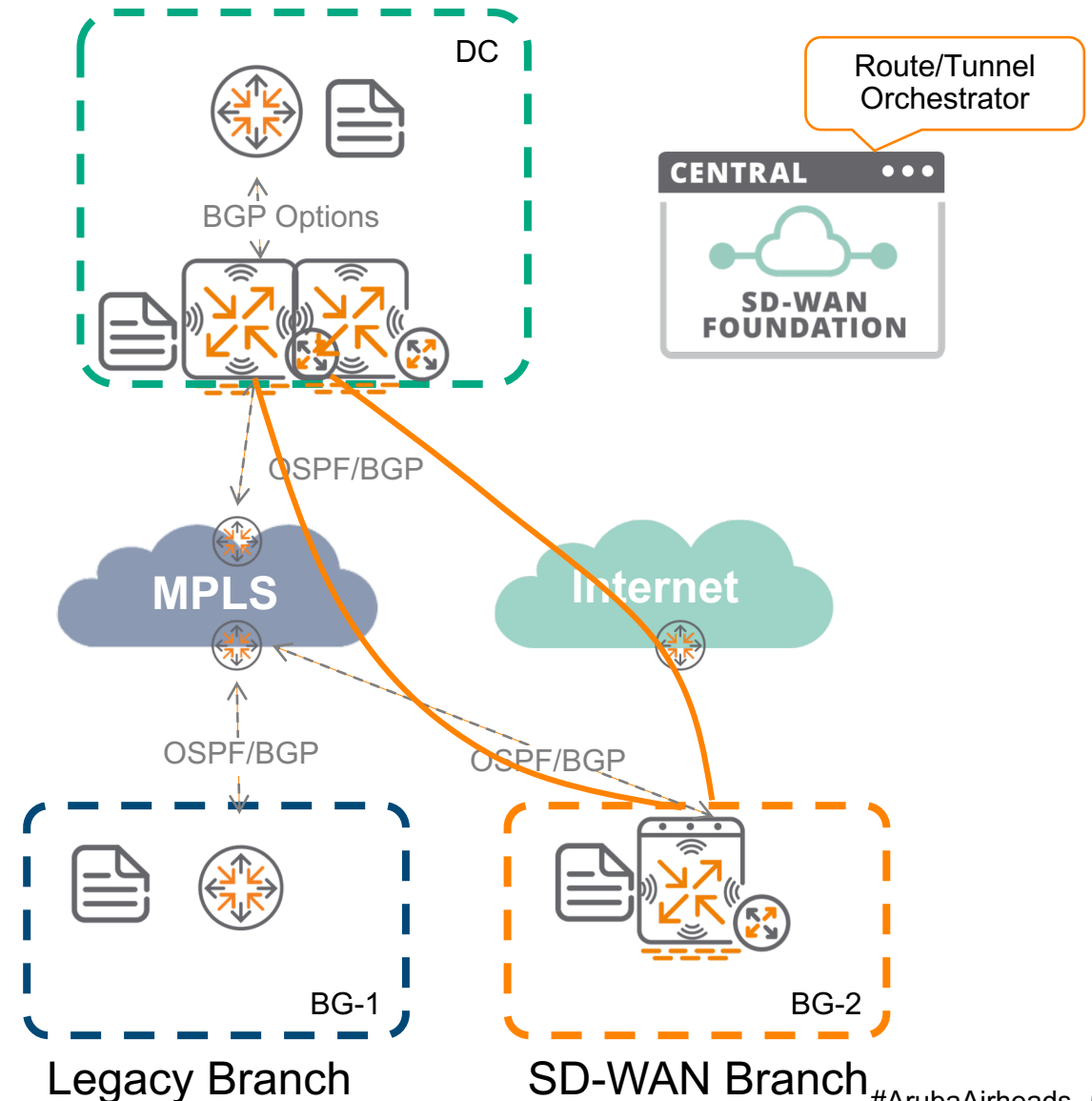
Migrated branches - Overlay

Pending branches - Underlay



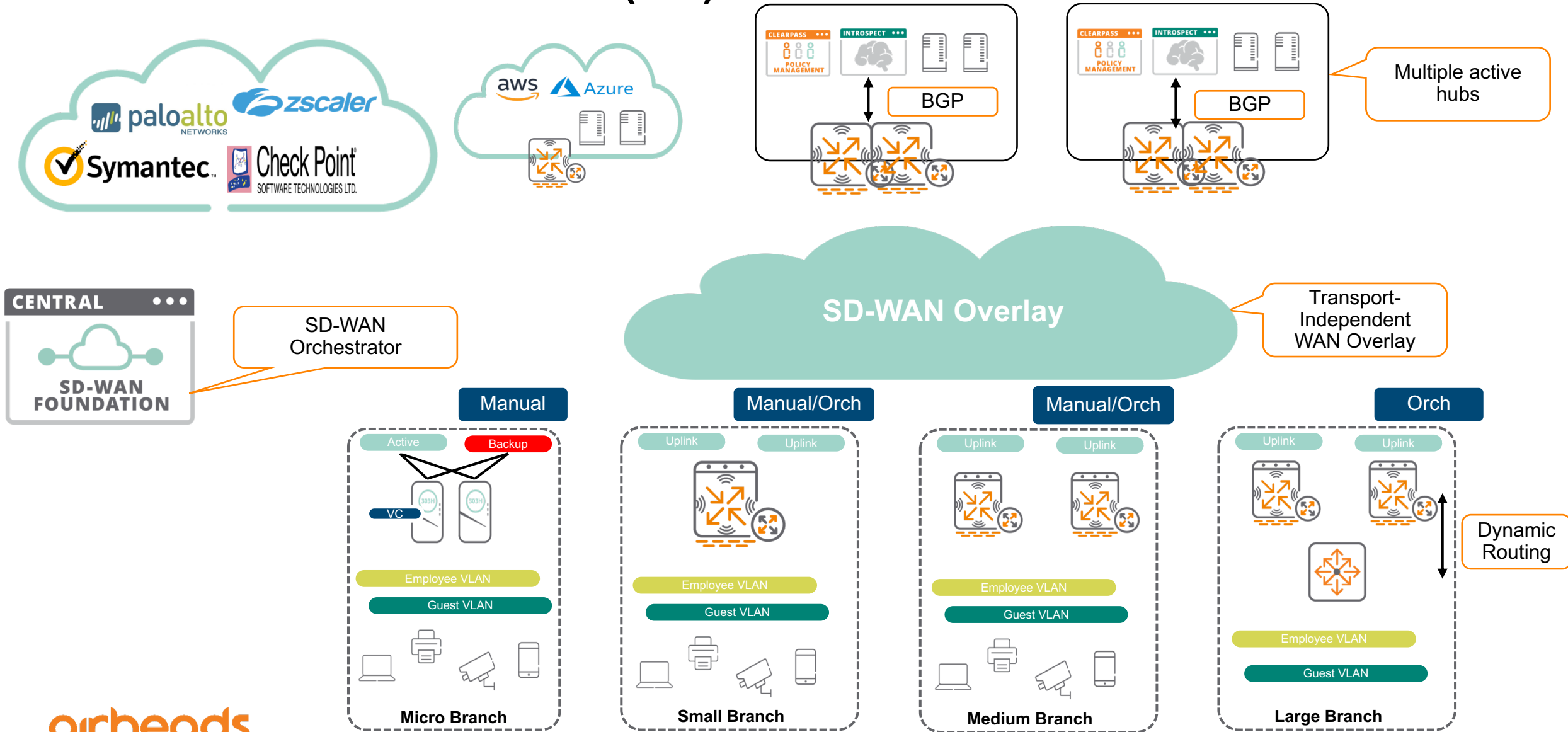
# Underlay + Overlay on Same Gateway

- This is NOT a supported architecture.
- You'll just get into trouble (routing loops). Do not do it
- If you do it, you're on your own.



# Summary...

# SD-Branch Architectures (1.5)



# Questions?

# airheads

TECH TALK *LIVE*

Thank You