

Aruba CX 10000: Enabling a New Distributed Services Architecture

Steve Baker

– Technical Marketing Engineer

Steve Bartlett

– Technical Marketing Engineer

Toby Makepeace

– Pensando Systems Engineer



Agenda

1

Overview

2

Details

3

Pensando Distributed Services Platform

4

Aruba DSS + Aruba Fabric Composer + PSM

5

Policy Flows

6

Demo

7

Additional Resources

The background features a solid red circle in the top-left corner and a large, dark blue shape with a white dotted pattern that occupies the right and bottom portions of the frame.

Overview

Modern Data Center Security Requirements

See Everything



Complete visibility of users, devices, applications, workloads and processes

Reduce the Attack Surface



Prevent attackers from moving laterally east-west with micro-segmentation and application whitelisting

Stop the Breach



Quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations

Aruba - Value across the data center



INFRASTRUCTURE & NETWORK TEAM

- Simplify scale and growth
- Rapid and error-free fabric deployments
- Streamline deployments to deliver higher value to business owners
- Enhance visibility and control with simplified API integrations



SERVER ADMINS, VM / APPLICATION OWNERS

- Remove bottlenecks and boost performance
- Deploy and scale without the need for specialized skills
- Provision resources in real-time, without opening a Network ticket
- Orchestrate virtualized and bare-metal resources



SECURITY AND COMPLIANCE TEAMS

- Centrally managed distributed services to secure critical workloads and data
- Maintain flow-level visibility and control across the estate
- Simplify scale and increase performance
- Reduce costs and increase efficiencies

NEW Switching Category = Distributed Services Switch

Aruba CX Routing and Switching



Pensando L4-L7 Stateful Software Services



FIREWALL



DDoS



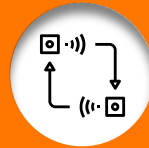
ENCRYPTION



NAT



LOAD BALANCER



FLOW LOGGING

Not in first release

aruba +

PENSANDO



Trident-3 ASIC

48 x SFP28 / 6 x 100G

Aruba CX 10000

DSM = Distributed Services Module

End-to-End Enterprise Switching Portfolio

Access - Aggregation - Core - DC/Cloud



Aruba CX 6100
Aruba CX 6000



Aruba CX 6200



Aruba CX 6300



Aruba CX 6400



Aruba CX 10000



Aruba CX 8300



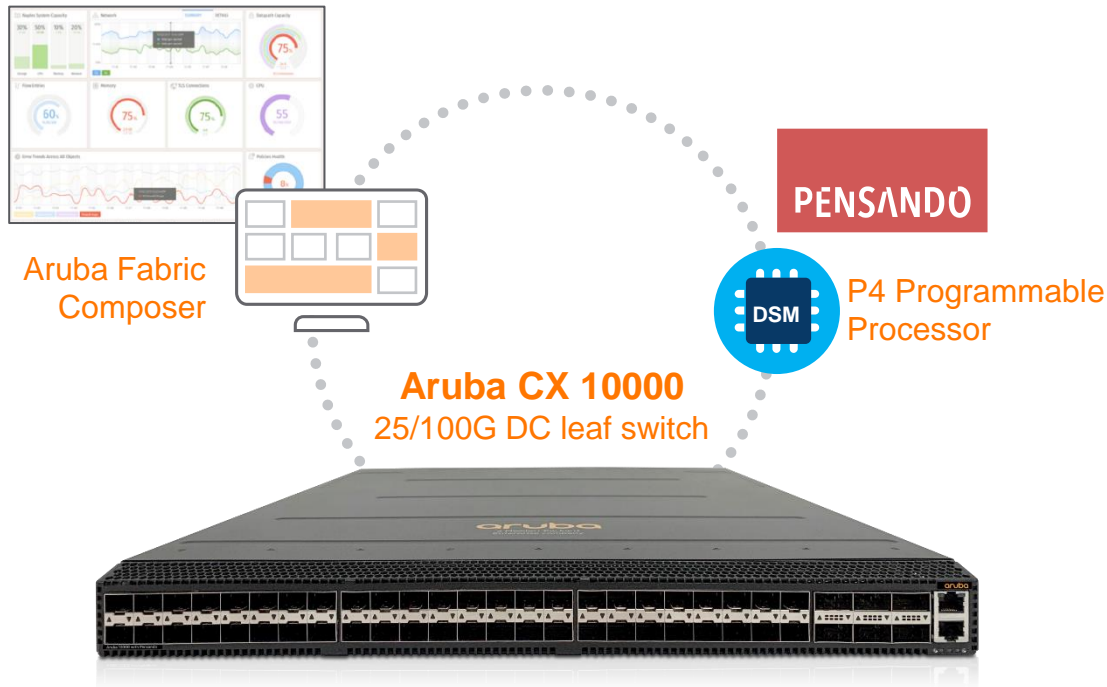
Aruba CX 8400



Ruggedized
Aruba CX 4100i

Price / performance, use case flexibility, form factor

Aruba CX 10000 Distributed Services Switch



- SW: AOS-CX 10.09, Pensando 1.18.1
- SA/GA: December 6, 2021

1RU Fixed Switch Form Factor:

- T3 Switching ASIC - 3.2 Tbps, 32MB Buffer (shared)
 - **Used for forwarding/routing/other features**
- 2 x Pensando DSM (7nm) Programmable Processor
 - **Used for smart stateful services (all forwarding performed by T3)**
- 2 x Redundant Power Supplies (N+1)
- AOS-CX Network OS, full protocol stack support

Port Configuration:

- 48 x 1/10G/25G SFP28, 6 x 100G QSFP
- 1 x 1G RJ45 management, 1 x RJ45 console port, 1 x USB

Phase 1 Planned Services/Use-Cases:

- East-West DC Segmentation (Distributed Firewall & DDoS)
- Micro segmentation
- Observability (Packet Capture, Flow Logging/Statistics)

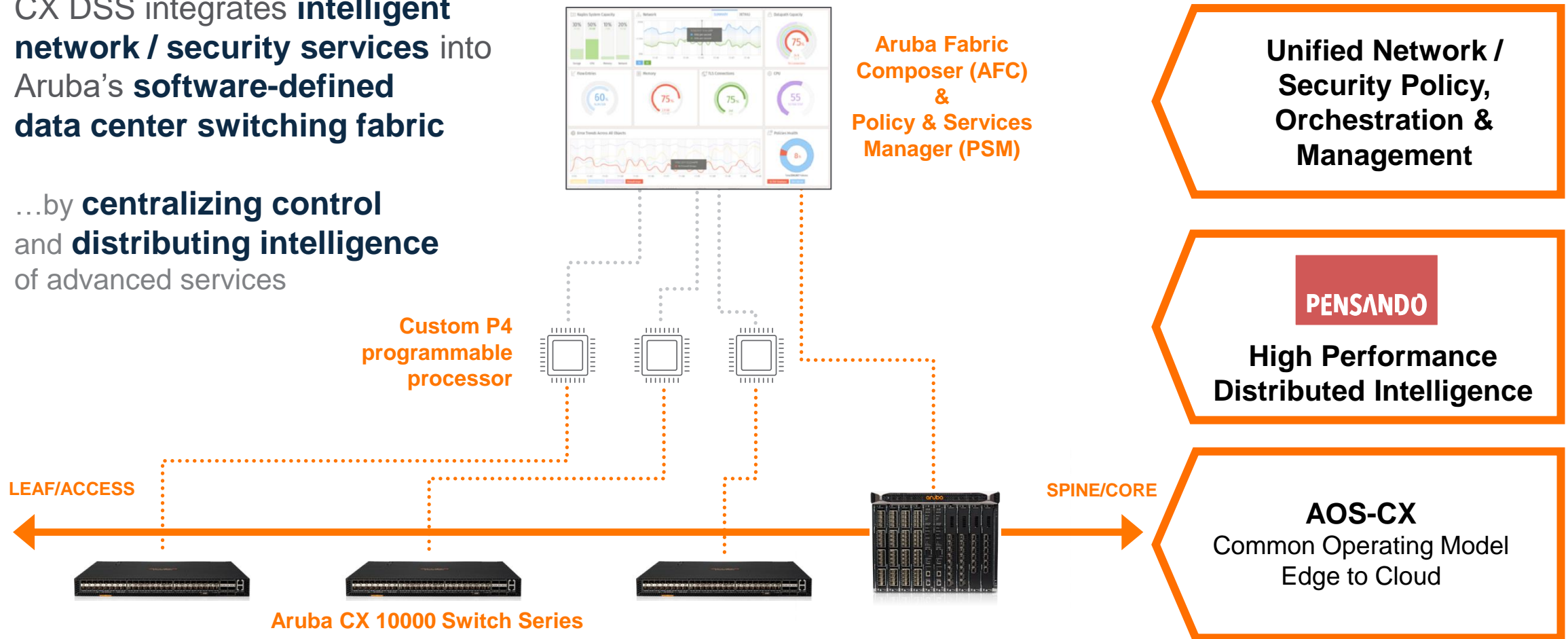
Platform Management Options:

- Aruba AFC & Pensando PSM
- PSM & DevOps Tools (Terraform/Ansible), REST-API

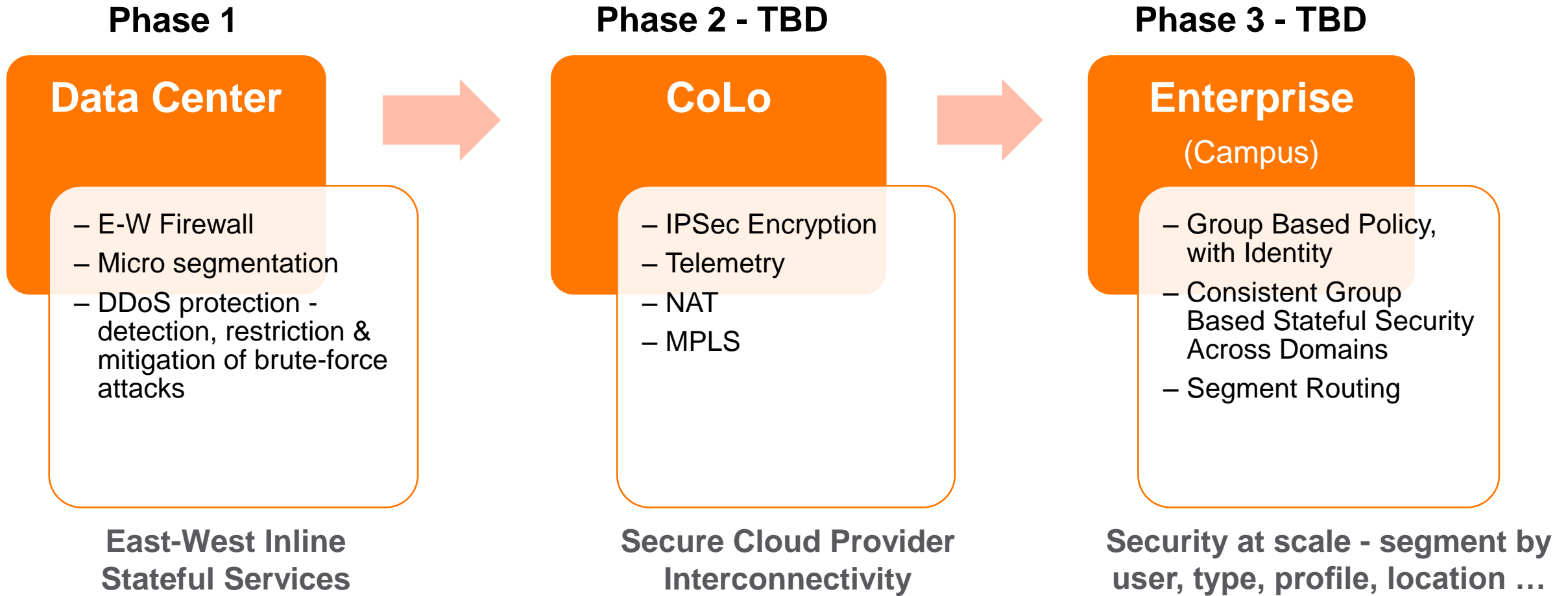
Delivering Advanced Services Closer To The Network-server Edge

CX DSS integrates **intelligent network / security services** into Aruba's **software-defined data center switching fabric**

...by **centralizing control** and **distributing intelligence** of advanced services



Aruba CX 10000 Roadmap

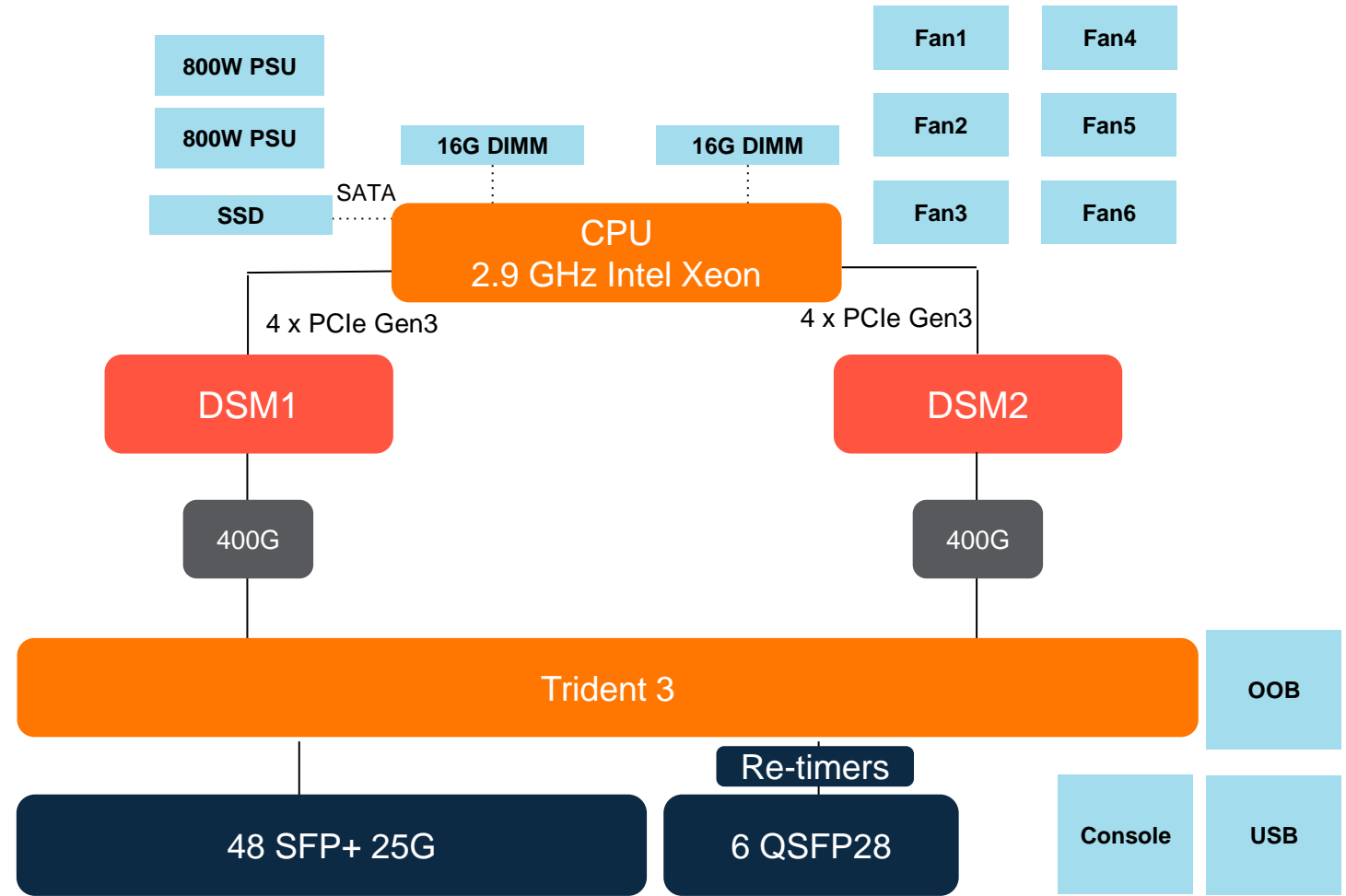


The background features a solid red circle in the upper-left corner. A large, dark blue shape, resembling a stylized 'L' or a corner, occupies the right and bottom portions of the frame. This blue shape is filled with a fine, light blue dot pattern.

Details

Architecture Overview

- 48 x 25G (SFP+) and 6 x 100G (QSFP28) ports
- Broadcom TD3 ASIC used for forwarding and other features.
- Pensando DSM ASICs used for smart stateful services.
- All forwarding is performed by TD3, DSM only delivers stateful services.
- Each DSM has 400G connection to TD3
 - These are 4x100G links, part of internal LAG 521 and 522.
 - Internal links are not visible in regular CX-OS commands.
 - Hashing algorithm RTAG7 uses L3/L4 information to LB packets on internal links.
- DSM shell access from x86 space is via int_mnic PCIe interface.
 - via CX-OS shell or diag CLI

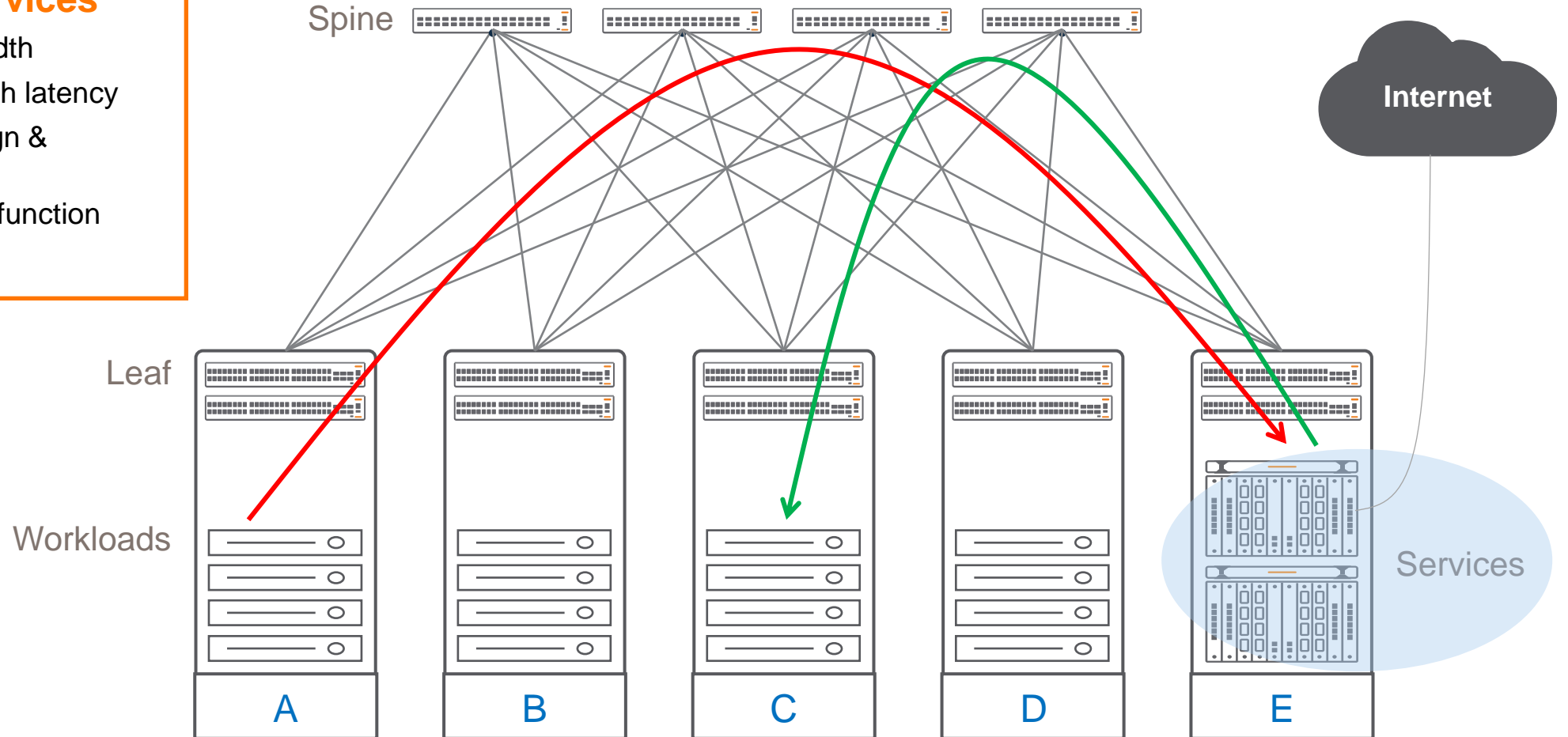


High Performance Data Center Fabrics

Centralized Services Architecture

Centralized Services

- Waste of bandwidth
- Congestion & high latency
- Complex to design & troubleshoot
- Limited to single function
- Very expensive



High Performance Data Center Fabrics

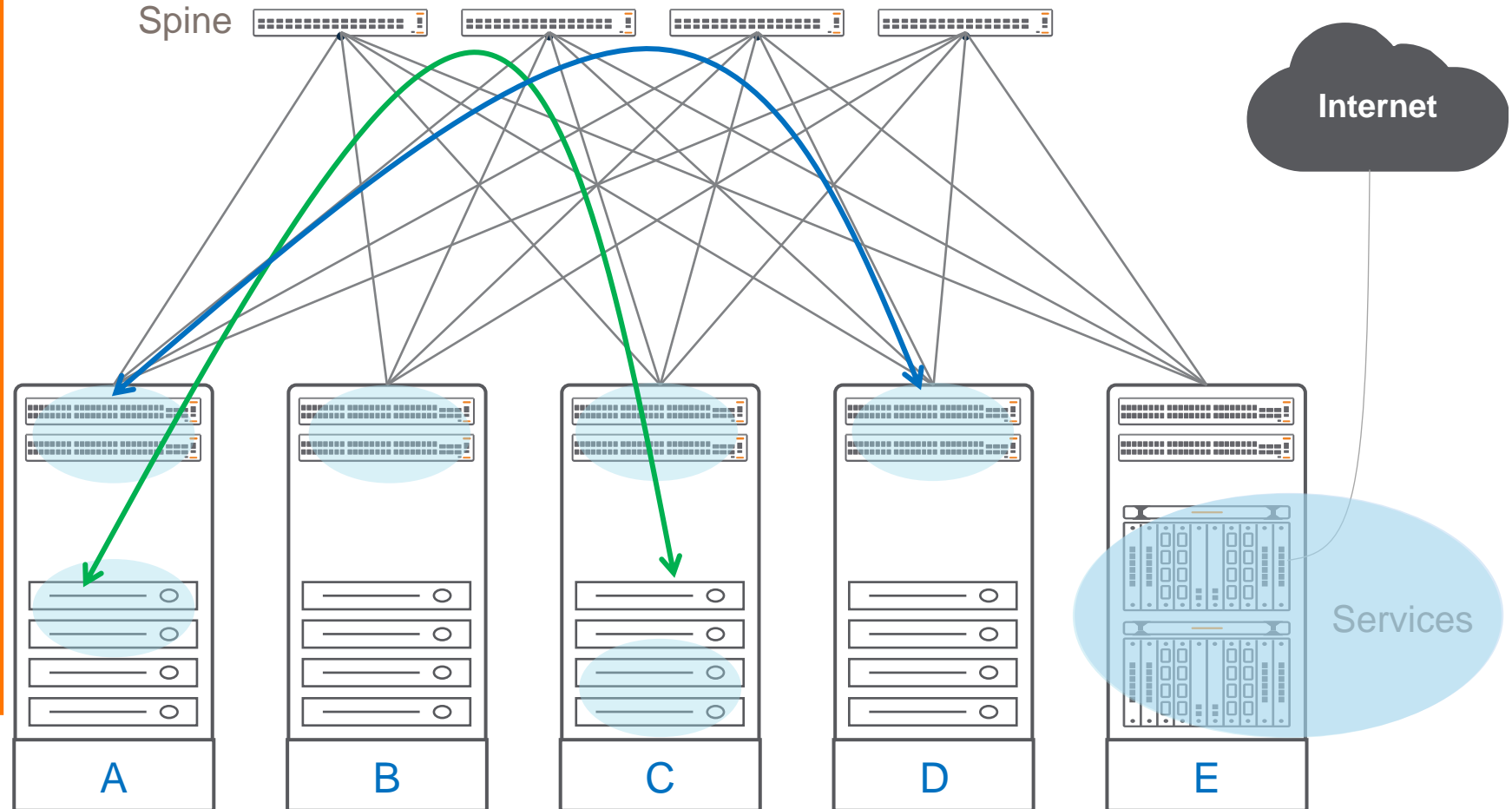
Distributed Services Architecture

Stateful FW Secures Traffic Between Servers:

- In the same VLAN
- In different VLANs
- Both connected to same or different Distributed Services Switch
- Where one server is connected to an existing Leaf

Protect the Unprotected

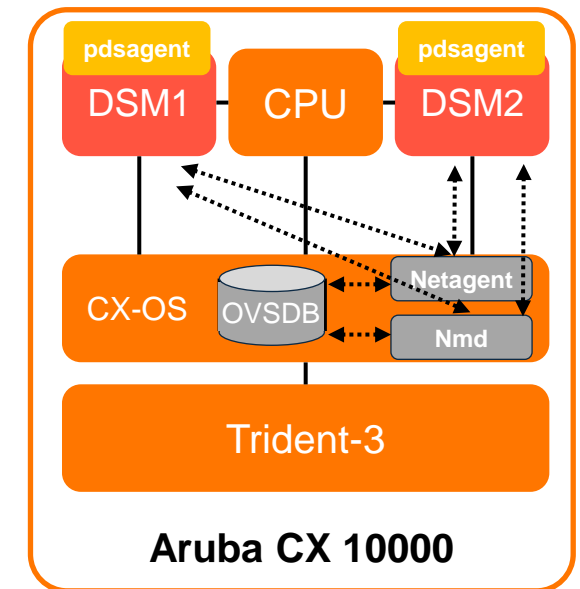
- Hypervisors (mgmt, storage)
- Backup Servers
- IP Storage Appliances
- Shared Services
- Bare Metal Servers



Architecture Overview

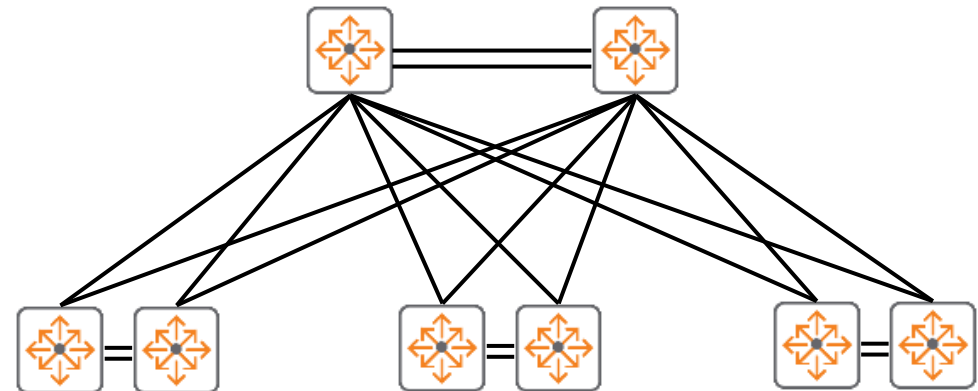
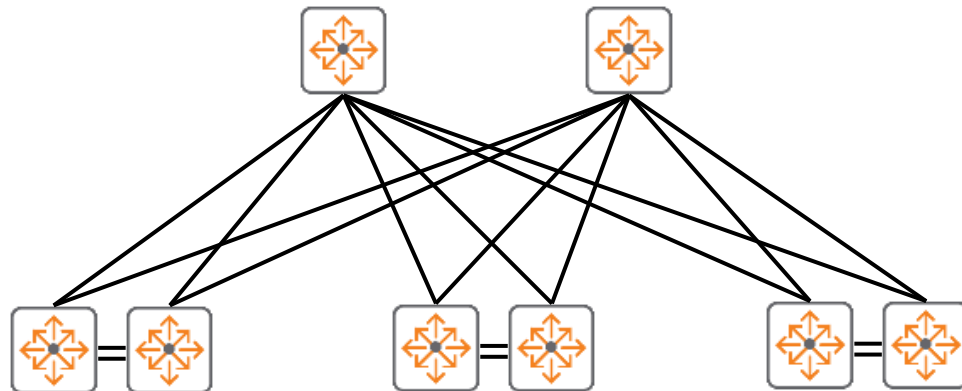
Control Plane

- Two Pensando agents run in CX-OS on x86
 - nmd → handles registration to PSM & sends heartbeats to PSM
 - netagent → manages configuration pull from PSM and keeps DSM configuration in sync
- pdsagent runs on ARM cores in DSM ASIC and is responsible for:
 - ASIC initialization
 - Processing gRPC APIs
 - P4 table management
 - Monitoring ASIC interrupts, temperature, logging etc
- nmd and netagent communicate with pdsagent running on both DSM ASICs.
- netagent programs ovssdb. switchd registers for these notifications and program TD3 ASIC, to redirect traffic to DSM.
- netagent manages how VLANs are mapped to DSM 1 or DSM2
 - L2 VLANs → VLAN ID is input for hash
 - VLAN w/SVI → PSM VRF UUID is input for hash



Overview of supported topologies

- The supported topologies for Phase1 are VxLAN leaf or L2 Core/Distribution/Access
- Switch ports are classified into the following categories:
 - Front panel ports, connected to the hosts/workloads (default)
 - Uplink/Fabric ports, connected to the spine nodes (configuration driven)
 - Smart/Service ports, connected to DSM in the box
 - Out of band management port(s) - this traffic will not hit DSM
 - ISL ports - this traffic will not hit DSM (except flow-sync)
- Traffic redirection to DSM is supported only for IPv4 traffic (unicast/unknown unicast).



- Traffic from/to DSM is sent with QinQ tag (L3VNI case)

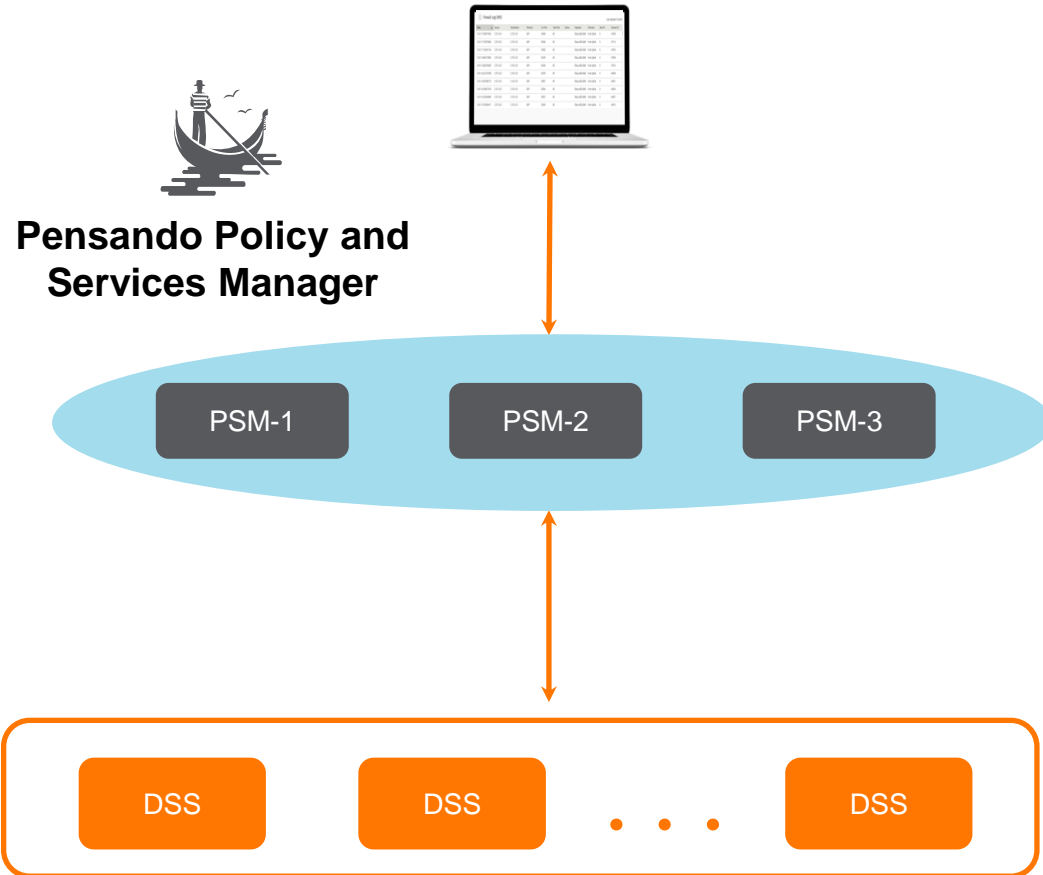
Inner tag represents front panel port or internal identifier used for fabric ports.

Outer tag represents pre-routed VLAN for packet ingressing front panel ports and post-routed VLAN for packets ingressing on the fabric ports



The Pensando Distributed Services Platform

PSM Functions



Management and Security

High Availability, Certificate Management, TLS Communication, Authn/Authz

Policy & Configuration

Declarative Intent, Distribution, Status Reporting
Configuration Backup, Restore

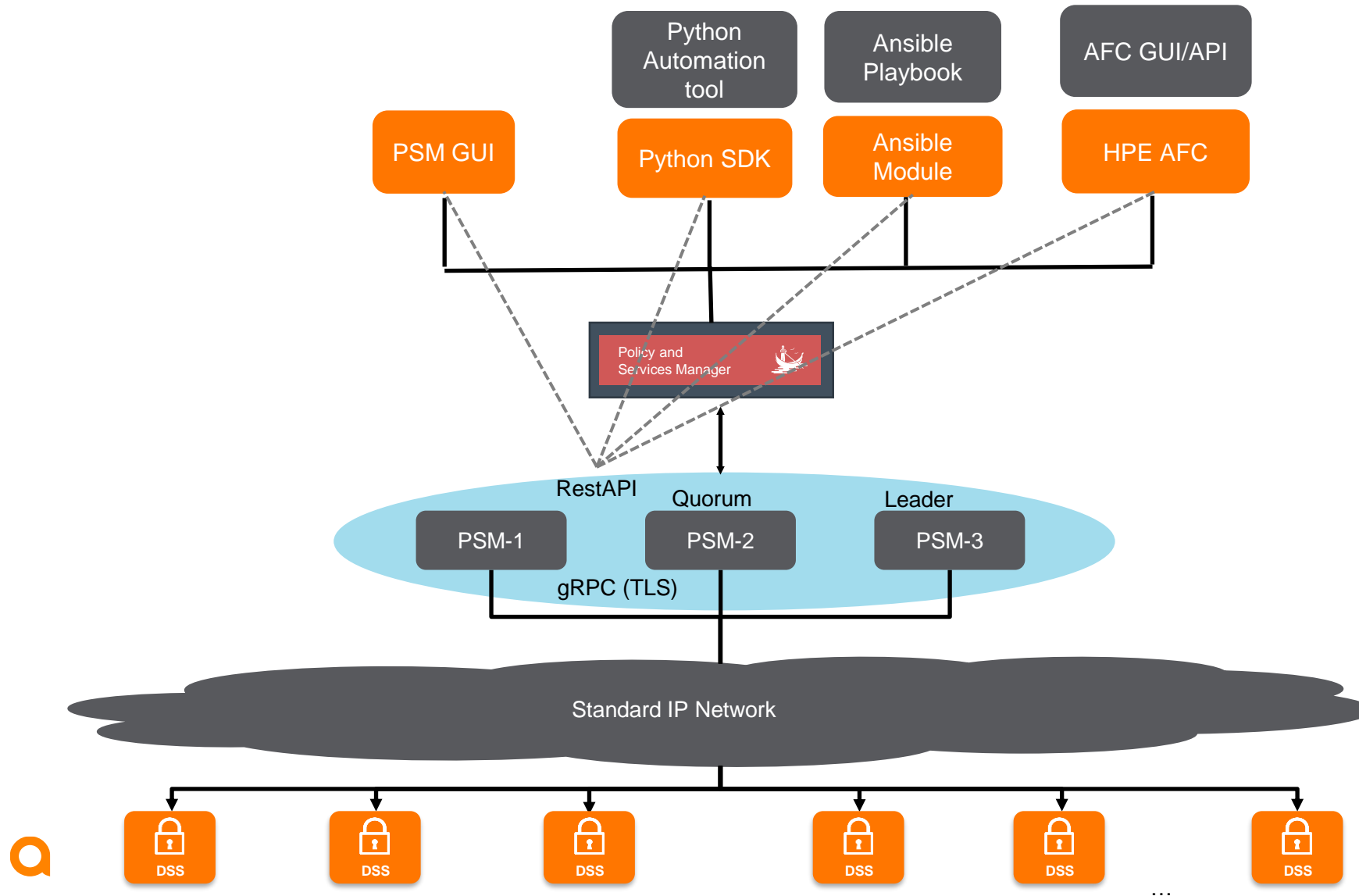
Observability and Analytics

Health Monitoring, Metrics Aggregation
Flow Logs, Object Relationships, Impact analysis

Operations

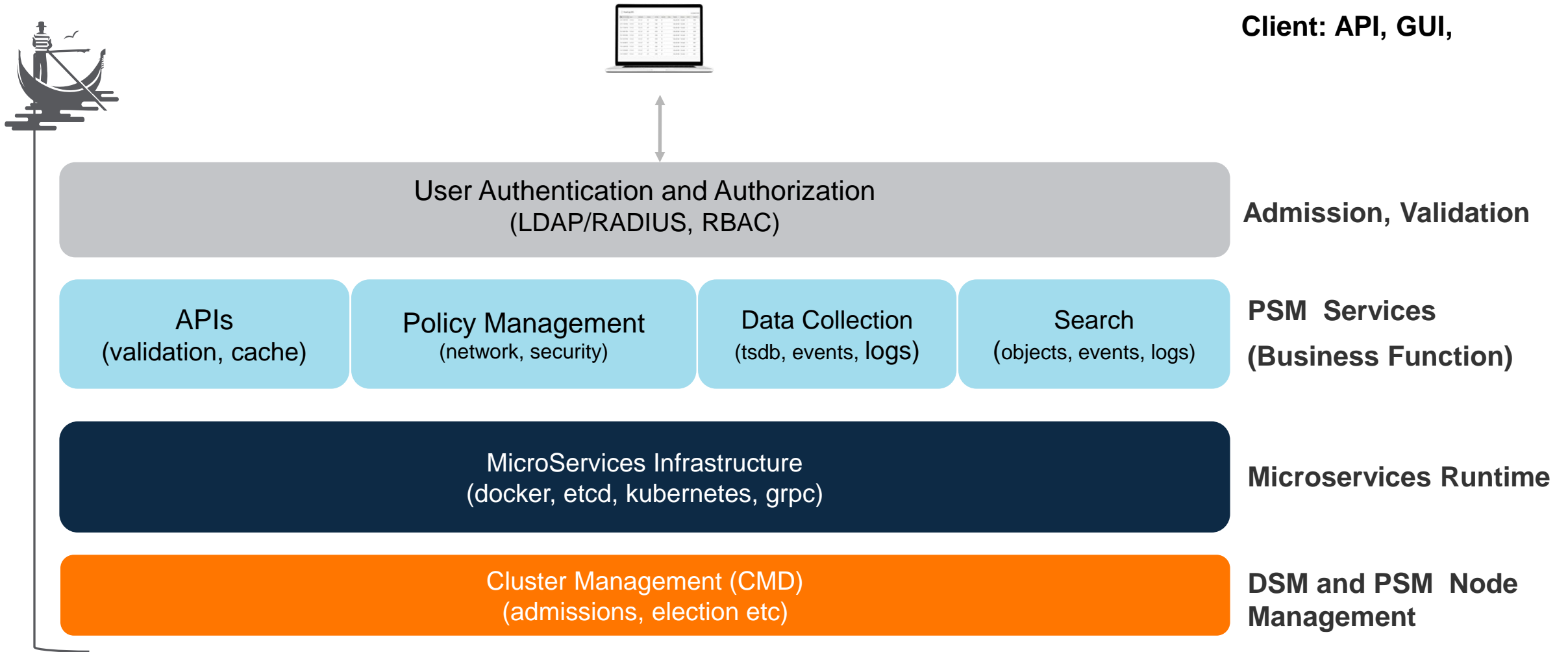
Events, Alerts, Troubleshooting, Search, Configuration Lookup, API Watchers

Central Firewall Policy Management with PSM



- Central location for policy creation with distributed enforcement
- Security policy are automatically distributed to CX 10000 where it is needed
- Automatic policy distribution with fabric expansion or configuration changes
- Flexible way and multiple tools to create security policy

Architectural Layers in PSM



PSM Operations

- Cluster Creation
 - Create PSM Cluster
- DSS Admission
 - Discovery, Commission and Decommission
- Events
 - System generated, immutable record
- Alerts
 - User defined conditions
 - Events/object status/stats based
 - Can be in Open/Acknowledged or Resolved state
 - Syslog Export
- Tech Support
 - Logs and Internal data for offline analysis
- Search
 - All objects, events, logs
- Rollout Service
 - Upgrade PSM
- Metrics Service
 - Distributed time series database
 - Available via APIs

Stateful Network Firewall vs Stateless ACL

Metrics	Stateful Firewall	Stateless ACL
Security Posture	High	Low
Flow visibility	Yes	No
Automatically allow return traffic in secure manner	Yes. Simplify policy configuration	No. Need to explicitly create rules for both directions
Protect client application	Yes.	No.
Scalability	High	Low
Policy flexibility	High	Low



Aruba DSS + Aruba Fabric Composer + PSM

Aruba Fabric Composer Orchestration to Speed Delivery

Orchestration and Automation for Aruba Data Center fabrics. Build DC fabrics with API driven super wizards.

Provision in minutes vs. hours. Create leaf-spine networks with OSPF underlay, and BGP based EVPN overlay.

Holistic policy synchronization for Aruba CX and DSS Switches/Pensando PSM.

Eco-System aware integrations enable visualization and monitoring of attached hypervisors, VMs and Host networking environment.

Automates away everyday networking tasks, including provisioning of VLANs and LAGs on Top of Rack.

Simplified troubleshooting thanks to a deep insight into end-to-end connectivity.

Powerful Integrations Help IT Admins Automate Network Configuration



vmware®

iLO Amplifier Pack

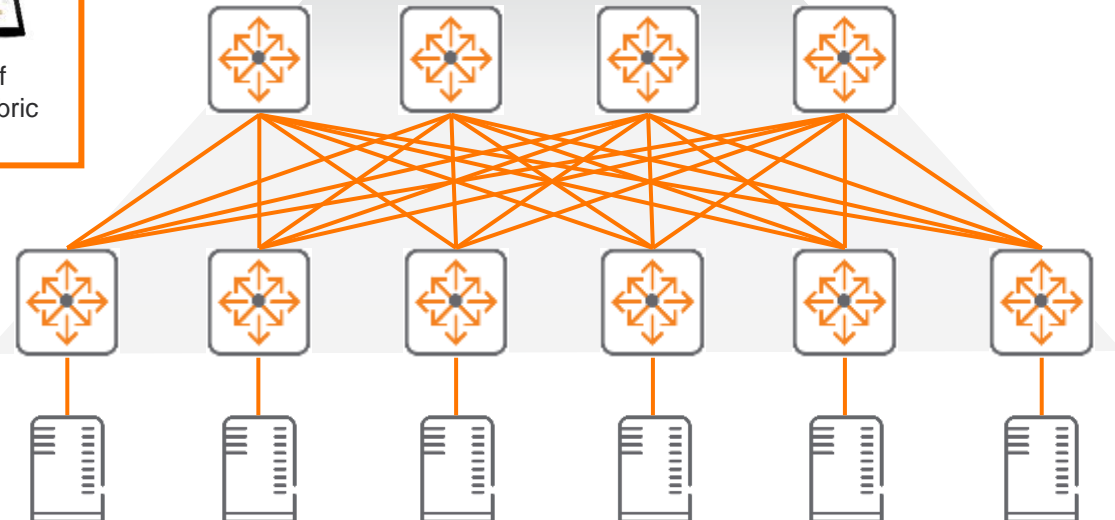
NUTANIX

Hewlett Packard
Enterprise
SimpliVity

Aruba NetEdit

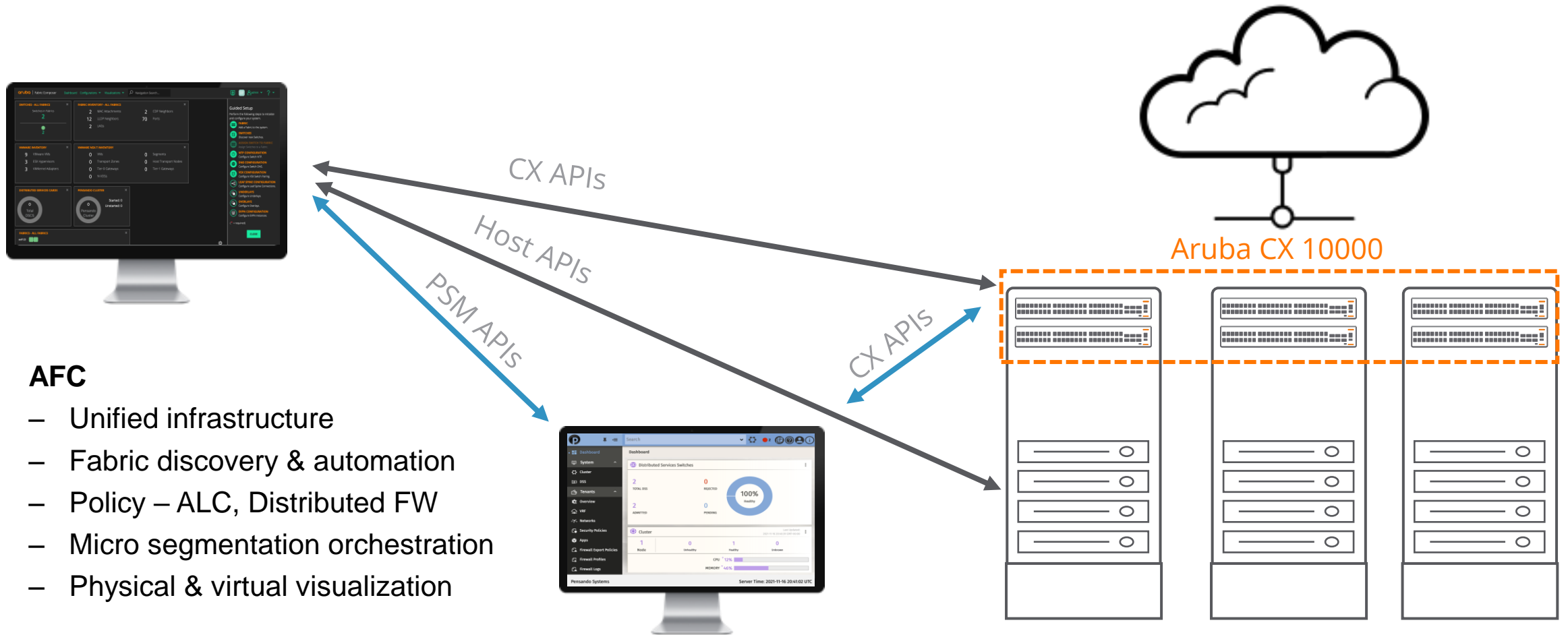


Single Point of
Integration to Fabric
Infrastructure



Aruba CX Switch Series: CX 6300 (OOB), CX 8325, CX 8360, CX 8400, CX 10000

Unified Services & Security Policy



AFC

- Unified infrastructure
- Fabric discovery & automation
- Policy – ALC, Distributed FW
- Micro segmentation orchestration
- Physical & virtual visualization

PSM

- Security policy
- FW Logs
- Diagnostics

Aruba Fabric Composer Dashboard

Dashboard View

Includes information about fabrics, switches, hosts, VMs, and Security

Workflow Automations and Guided Setup

Point and click GUI streamlines and automates away complexity

aruba | Fabric Composer

Dashboard

Configurations

Visualizations

Navigation Search

SWITCHES

Switches in Fabric

6

6

VMWARE NSX-T INVENTORY

12 VMs

6 Transport Zones

1 Tier-0 Gateway

8 N-VDSs

FABRIC

fabric01 (6)

Ports

Routing

System

Maintenance

Administration

Integrations

Policy

Policy Groups

Policies

Rules

Service Groups

Applications

Service Qualifiers

VMWARE INVENTORY

12 VMware VMs

3 ESX Hypervisors

18 VMKernel Adapters

VMWARE INVENTORY

Nutanix VMs

AHV Hypervisors

VMs

HPE ILO INVENTORY

Servers

5

HEALTHY 4

WARNING 1

INTEGRATIONS

CONNECTED VMware vSphere (1 Configuration, v6.0.0)

CONNECTED VMware NSX-T (1 Configuration, v6.0.0)

CONNECTED HPE ILO Amplifier (1 Configuration, v6.0.0)

admin

?

NETWORK

DISTRIBUTED SERVICES

Network Setup

Perform the following steps to initialize and configure your system.

SWITCHES Discover new Switches.

FABRIC Add a Fabric to the system.

Assign Switch To Fabric.

NTP CONFIGURATION Configure Switch NTP.

DNS CONFIGURATION Configure Switch DNS.

VSX CONFIGURATION Configure VSX Switch Pairing.

L3 LEAF-SPINE CONFIGURATION Configure L3 Leaf-Spine Connections.

L2 LEAF-SPINE CONFIGURATION Configure L2 Leaf-Spine Connections.

UNDERLAYS Configure Underlays.

OVERLAYS Configure Overlays.

Distributed Services Setup

Perform the following steps to initialize and configure distributed services.

PENSANDO PSM Configure the Distributed Services Manager

PSM/SWITCH ASSOCIATION Distributed Services Switch Assignment

CONFIGURE VRF Synchronize VRFs with Pensando

CONFIGURE NETWORKS Configure Networks for Selected VRF

CONFIGURE POLICY Configure Policies.

Network and Switch Visualization

Hosts, MAC, Neighbors, Switch inventory, health status

API level integrations with various environments

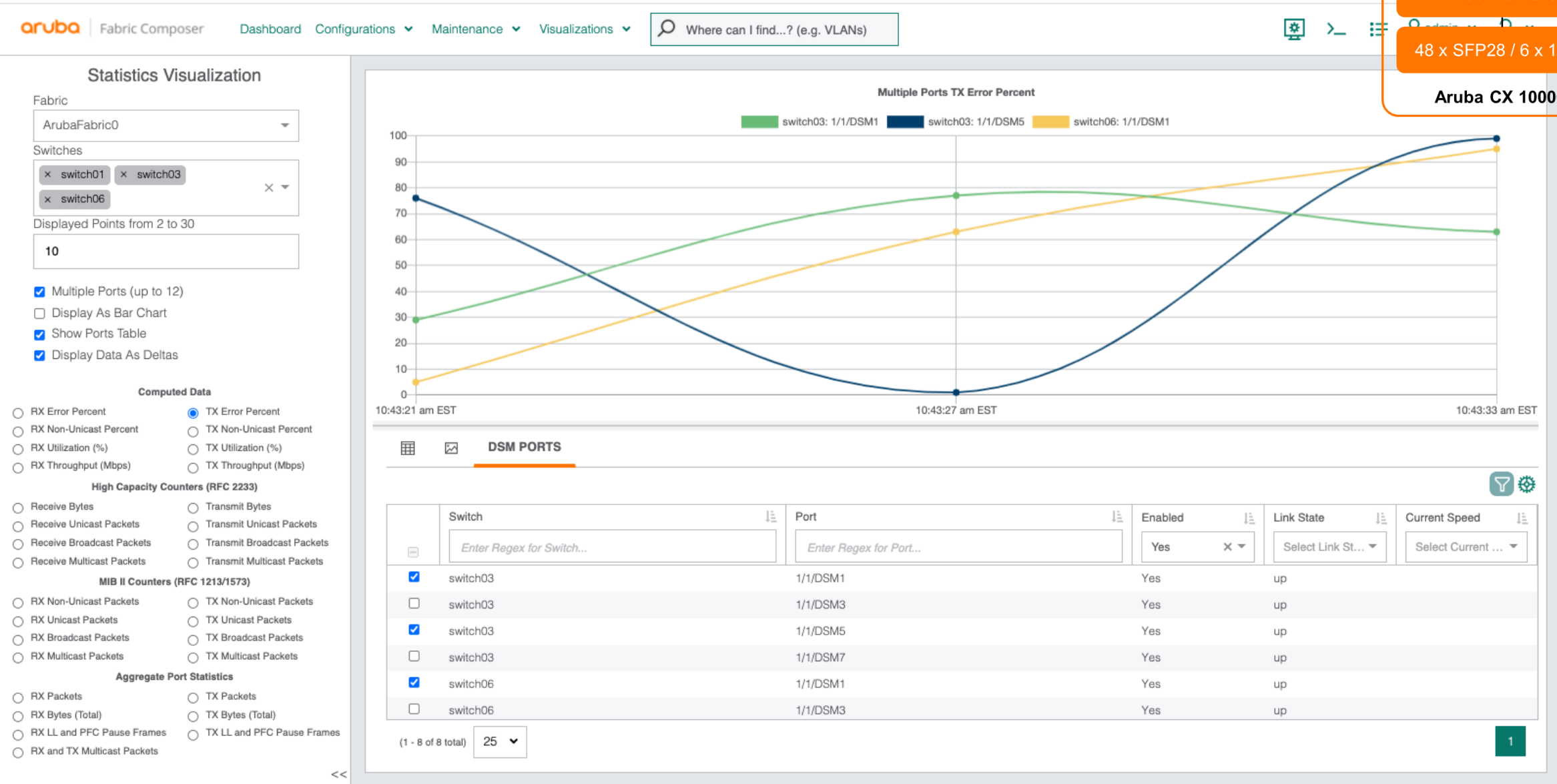
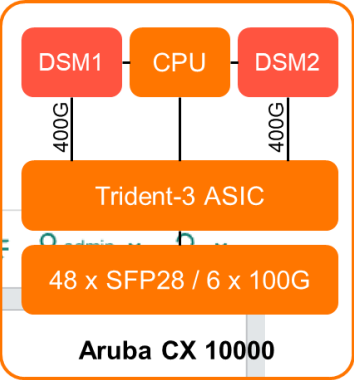
Including HPE, Aruba, VMware vSphere, ESX, NSX and Nutanix



Aruba Fabric Composer 6.2 – Key Features

- AFC 6.2 functionality provided to support Distributed Services Architecture and the Aruba CX 10000 solution.
- The Solution allows to create a new market for Aruba DCN by combining Aruba switching technology with Pensando SmartNIC, all centrally managed by AFC.
- Customers want a single-pane-of-glass orchestration in datacenters.
- Expand Fabric Composer footprint and provide micro-segmentation capability.
- Support for Aruba CX 10000 Distributed Services Switch
- Pensando PSM (T) Integration
- Pensando Policy orchestration
- Aruba AOS-CX ACLs orchestration
- Orchestration of PVLAN based micro-segmentation on vSphere
- Base PVLAN management/automation on CX platforms
- Improved telemetry capabilities for AOS CX
- Live telemetry for DSS/DSM
- Firewall logging configuration
- Network Visualizations overhaul
- Switch configuration snapshot and rollback
- Live VSX upgrade from AFC
- Switch CLI support

DSM Ports Telemetry

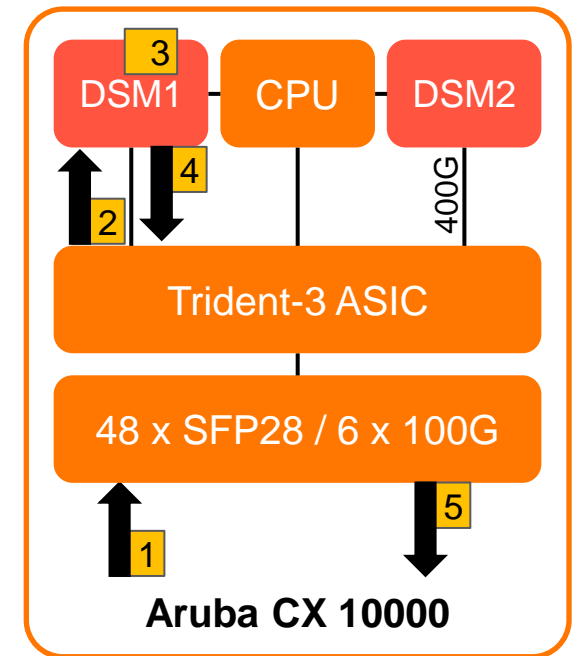


The background features a solid red circle in the top-left corner and a large, dark blue shape with a white dotted pattern that occupies the right and bottom portions of the frame.

Policy Flows

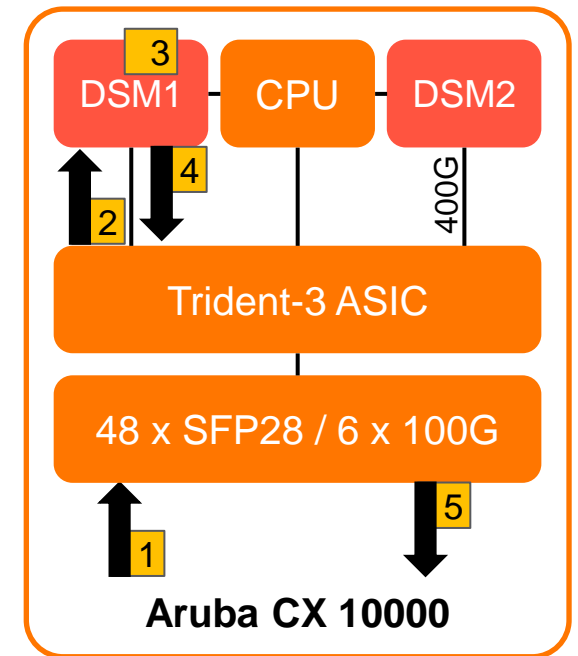
Packet Flow - Front Panel to Fabric (VxLAN)

1. Native IPv4 packet ingress to front panel port.
2. Based on programmed FP rules, TD3 will send packet to an DSM with QinQ tag
3. Packet is sent with inner VLAN as front panel port identifier (for LAG, internal identifier is used for inner VLAN) and outer VLAN as incoming dot1q tag.
 1. DSM identifies this is traffic from front panel since inner VLAN is not 2048 and packet is QinQ tagged, and applies egress policy.
4. DSM sends back QinQ packet to TD3
 1. Packet is sent with inner VLAN as front panel port identifier (for LAG, internal identifier is used for inner VLAN) and outer VLAN as incoming dot1q tag.
5. TD3 performs VxLAN encap and forwarding decision and sends packet out fabric port.
 1. Inner VLAN is used for source pruning (unknown unicast) and is not part of the VxLAN encap packet sent from TD3.



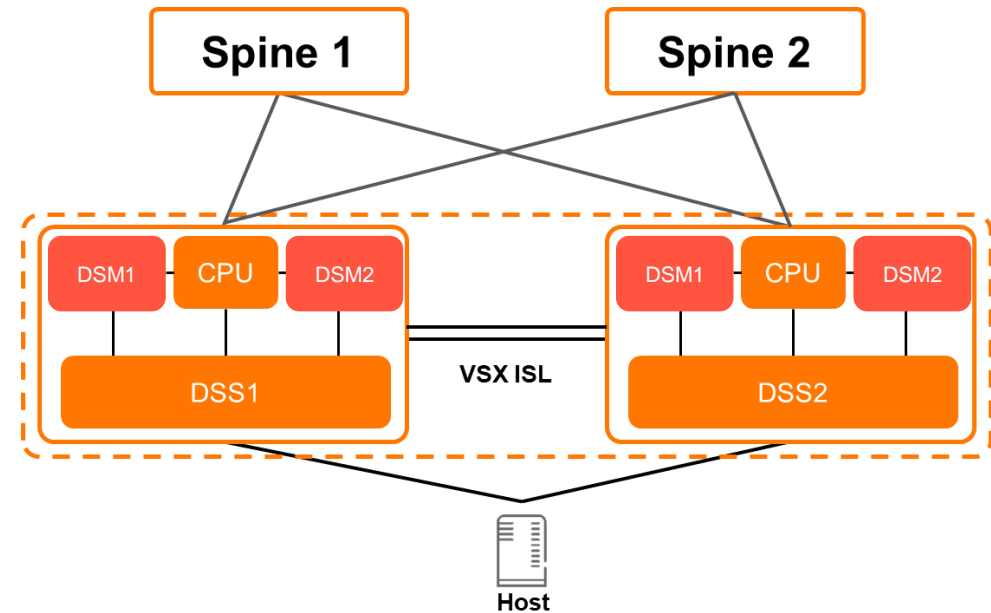
Packet Flow - Fabric to Front Panel (VxLAN)

1. VxLAN packet ingress to switch.
2. TD3 decaps packet and DSM will perform policy evaluation post decap
 1. For L2VNI case, packet is sent with inner VLAN = 2048 and outer VLAN equals VLAN mapped to VNI.
 2. For L3VNI case, packet is sent with a single tag (no QinQ) and the VLAN tag is the destination VLAN for the decap, post-routed packet.
3. DSM identifies this is traffic from fabric based on either inner VLAN of 2048 or single tag packet and applies ingress policy.
4. DSM sends back QinQ.
 1. For L2VNI and L3VNI case, inner VLAN of 2048 is used. Outer VLAN is the same as step 2.
5. Native packet is forwarded in the BD to the appropriate port.

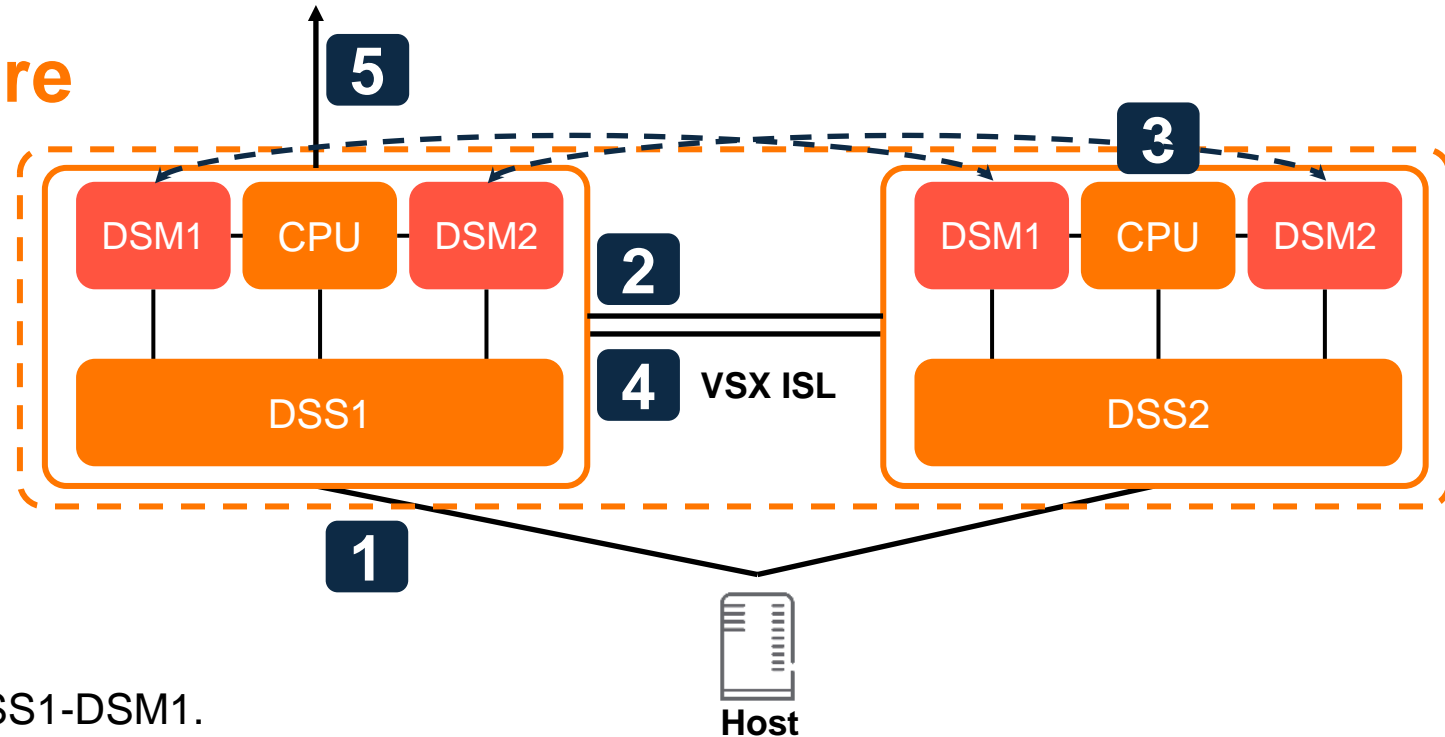


VSX Overview

- In VSX environment, flow-table between the VSX peers have to be synced.
- This is to avoid the following problems:
 - Asymmetric traffic: In VSX scenario, there is a possibility of forward/reverse packets arriving at different CX 10000.
 - In that case both CX 10000 need to be sync w.r.t. flow-table since policies can be different in both directions.
 - Packet flow can shift from one CX 10000 to another due to routing hash change in Spine.
 - Due to this, traffic disruption may happen due to incorrect policy evaluation.
 - FIN and RST will be seen by only one CX 10000 hence there will be a mismatch in the idle timeouts used.
 - Due to this one CX 10000 may age “Flow Entries” faster than the other if state specific timeouts are in use.
 - Similarly due to the traffic pattern in the Flow (eg. UDP flow that has mostly unidirectional traffic) also one CX 10000 may age “Flow Entries” faster than the other
 - Symmetric traffic: Even in a Symmetric traffic scenario, if one of the CX 10000 go down the other node needs to have the flow-table info in order not to cause traffic disruption.



Flow-Sync Procedure



1. Packet from the host reaches DSS1-DSM1.
2. The DSS1-DSM1 device that has seen the first packet (Flow miss), is evaluated for policy but the flow-installation/pkt forwarding/drop is not done yet. It sends the packet, encapsulated in another packet (UDP 11362/VLAN 4094) to the DSS2-DSM1.
3. The DSS2-DSM1 that has received the encapsulated packet, punts it to VPP which will look into the inner packet instead of the outer packet. Policy-eval is done and flow-entry is programmed on P4 pipeline.
4. DSS2-DSM1 sends the packet back to DSS1-DSM1 after installation of the flow.
5. DSS1-DSM1 receives the packet back, sends it back to the SW and installs flow to the P4 pipeline and forwards/drops the packet based on the policy evaluation (done previously).

1. In case of TCP, The FIN packet is also sent from DSS1-DSM1 to DSS2-DSM1 to kick-off the close timers.

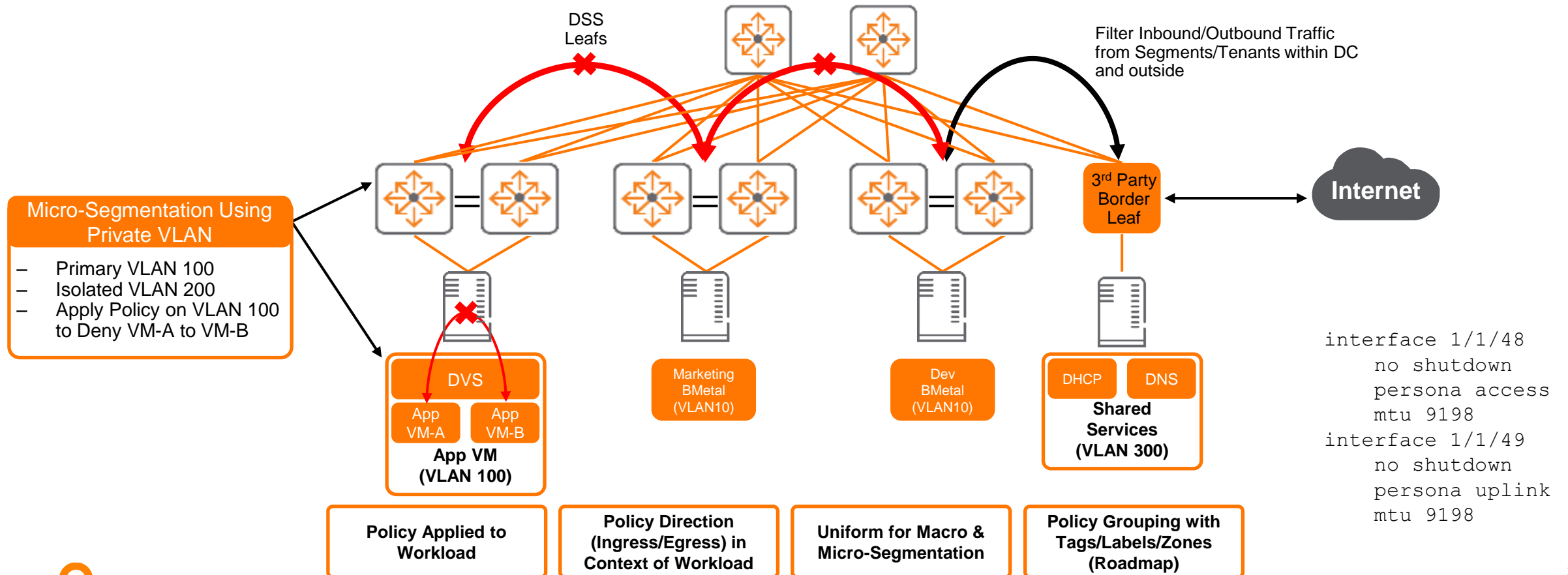
Policy Flow Overview

PSM
Centralized
Policy Orchestration



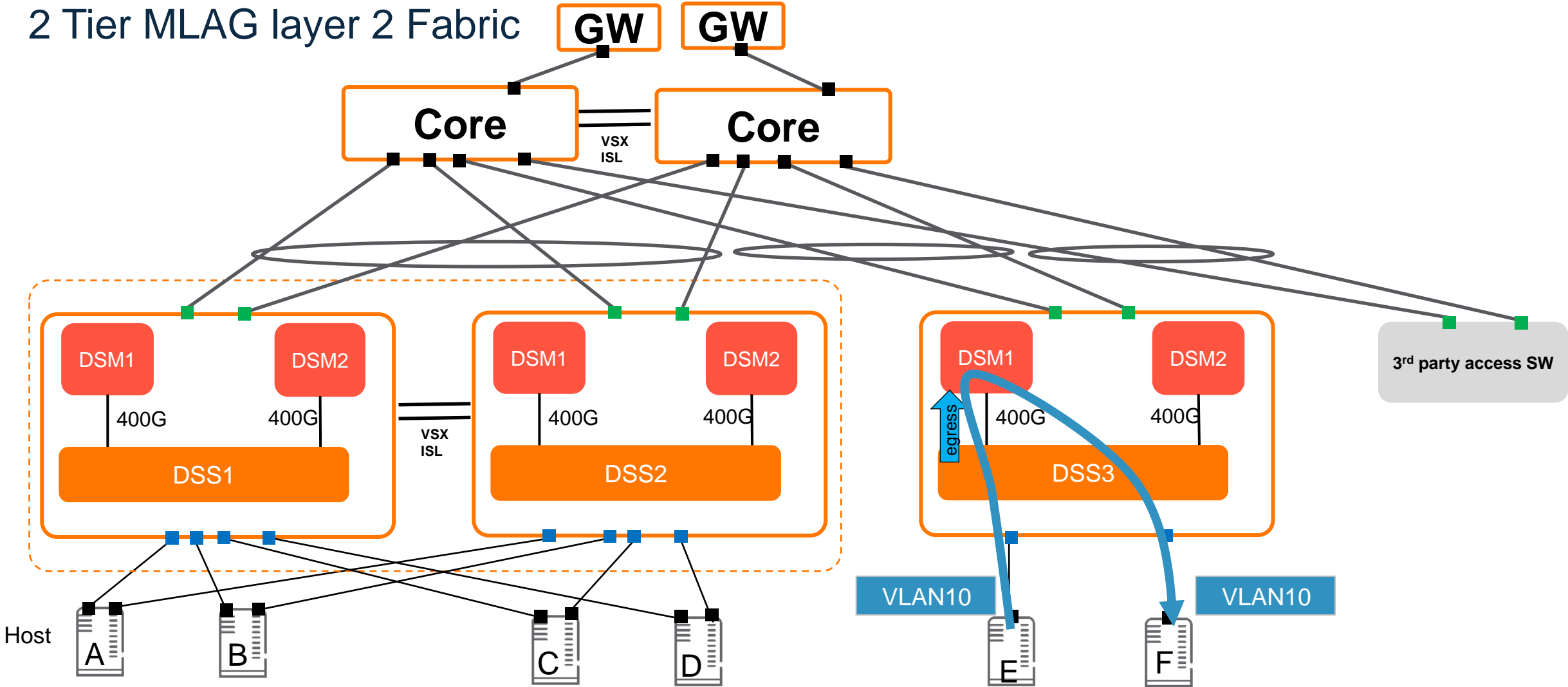
Direction definition

- Egress: Workload is sending traffic
- Ingress: Workload is consuming traffic
- Personae CLI config option on a port is used to set the appropriate policy:
 - All traffic leaving the workload/host and entering the switch from host facing ports is subject to **“access”** personae
 - All traffic destined to the workload/host and entering the switch from fabric facing ports is subject to **“uplink”** personae



Intra subnet – single DSS

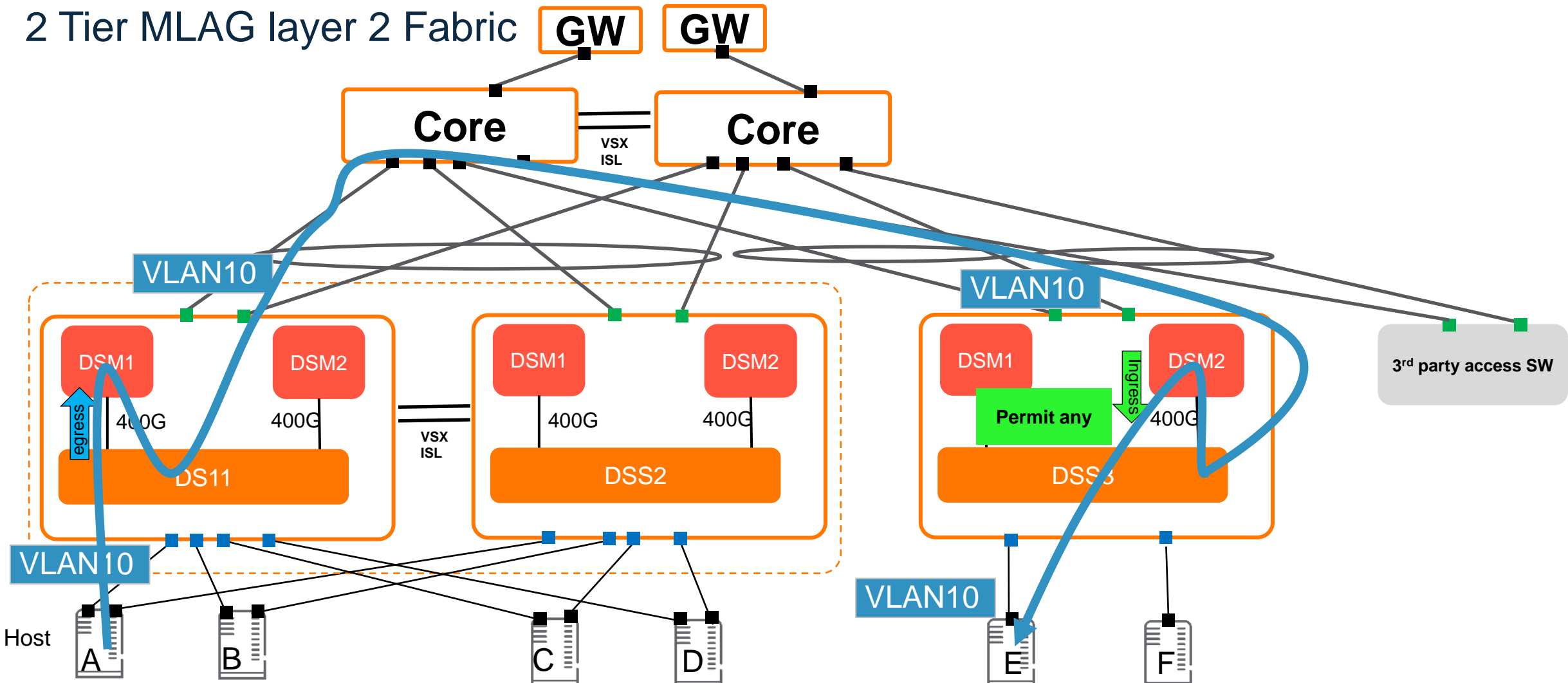
2 Tier MLAG layer 2 Fabric



Name	VRF	VLAN	FW Logging	Ingress Policy	Egress Policy
v10	test1	10	Enabled		Test

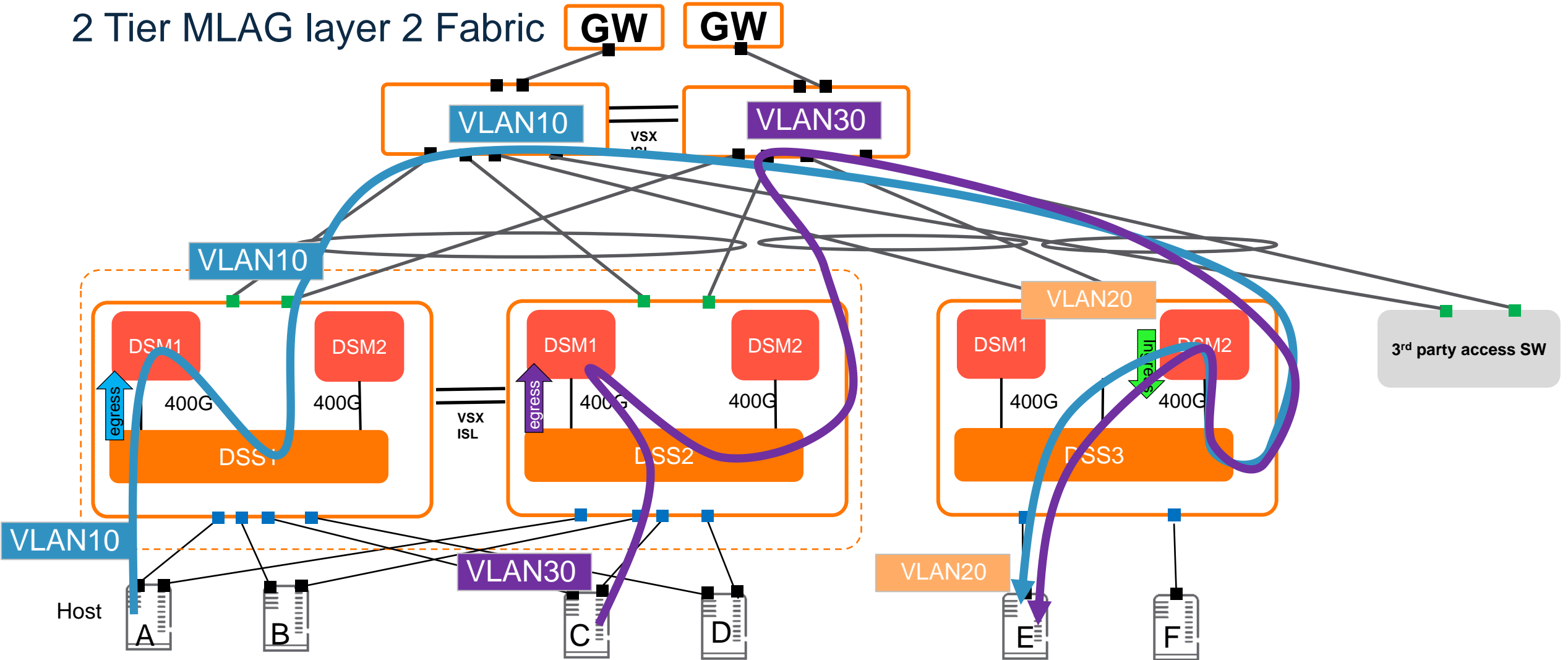
Intra subnet – different DSS

2 Tier MLAG layer 2 Fabric



<input type="checkbox"/>	Name	VRF	VLAN	FW Logging	Ingress Policy	Egress Policy	Modification Time
<input type="checkbox"/>	v10	test1	10	Enabled	permit-any	Test	2021-09-27 17:52:42 GMT+00:00

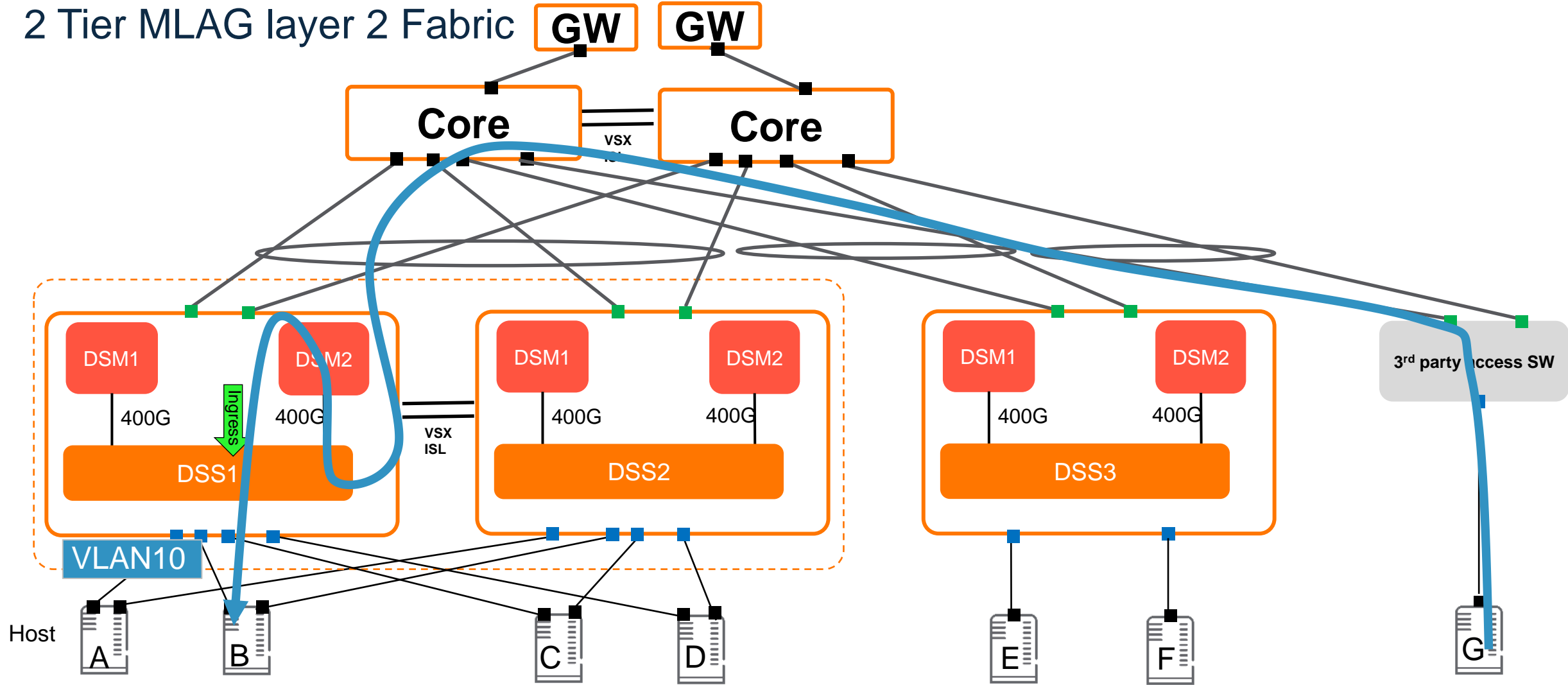
Inter subnet – different DSS



Name	VRF	VLAN	FW Logging	Ingress Policy	Egress Policy
v10	test1	10	Enabled	permit-any	Test
v20	test1	20	Disabled	permit-any	Test
v30	test1	30	Disabled	permit-any	Test

3rd party access switch – Host G to B

2 Tier MLAG layer 2 Fabric

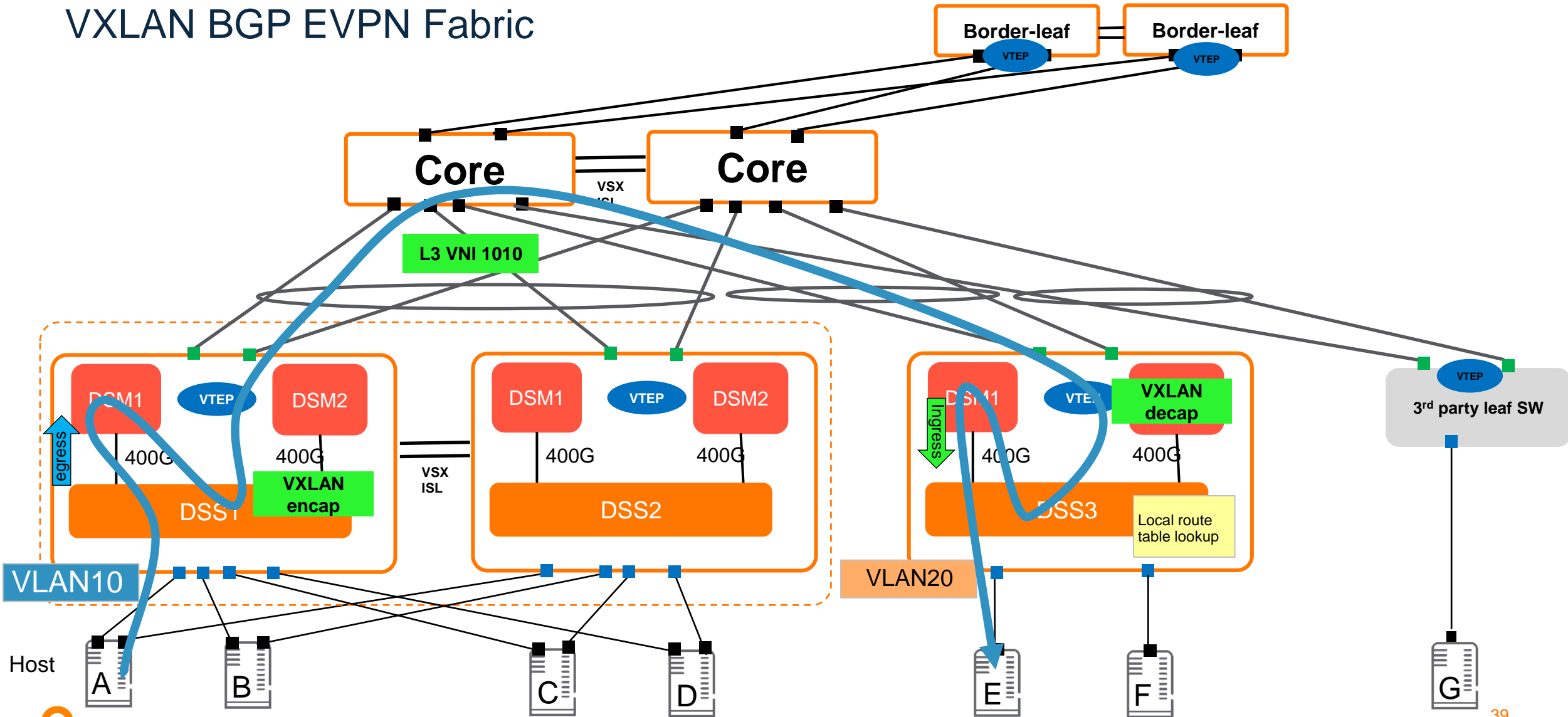


Name	VRF	VLAN	FW Logging	Ingress Policy	Egress Policy
v10	test1	10	Enabled	Test	Test



L3 VNI VXLAN Switching

VXLAN BGP EVPN Fabric



The background features a solid red circle in the top-left corner and a large, dark blue shape with a white dotted pattern that occupies the right and bottom portions of the frame.

Demo

Demo - Policy building blocks - AFC

Aruba Fabric Composer 6.2

AFC can apply policy to the distributed FW (Layer4) or apply ACLs (Layer 2 & Layer 3)

A policy is made of a number of building blocks

- Service Qualifiers

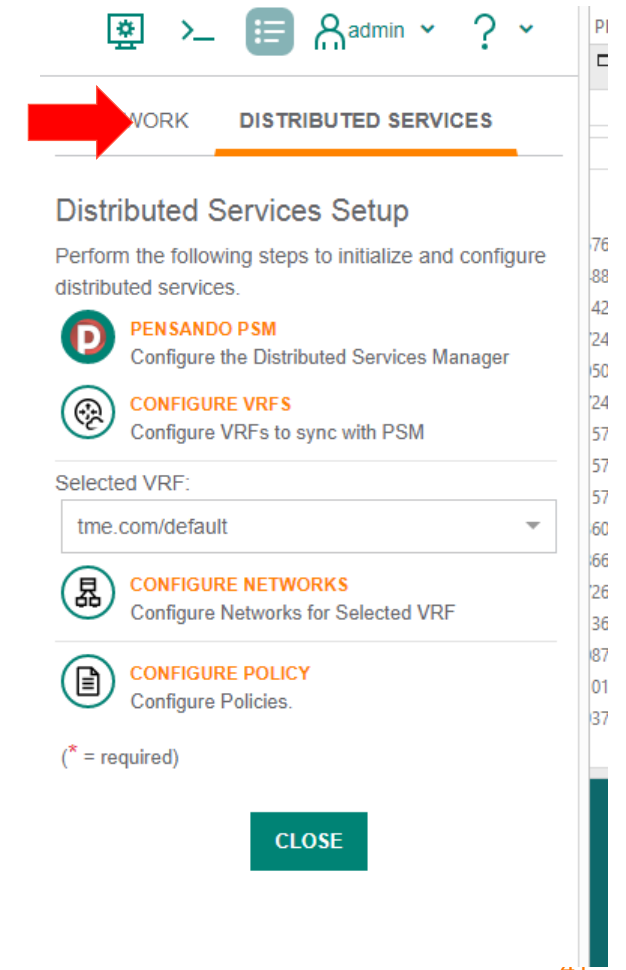
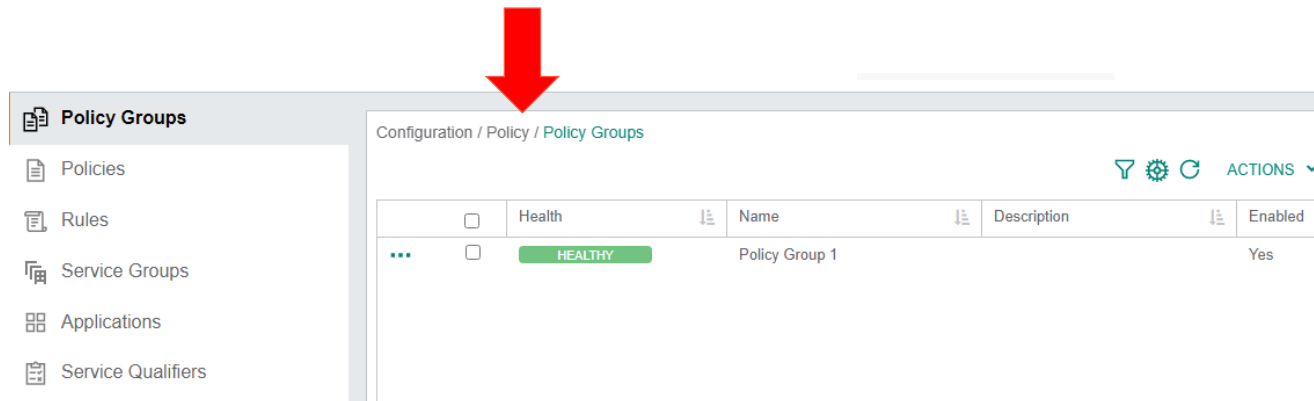
- Applications *(will be greyed out as part of the initial release)*

- Service Groups *(will be changed to Groups as part of the initial release)*

- Rules

Intent for policies can also be grouped together and applied as a policy group

Configuration and application is via the Configuration / Policy tab or via the 'Distributed Services' guided set-up tab



Demo

Policy building blocks – Service Qualifiers

Service port numbers: UDP, TCP, ICMP etc

Some (considerable amount) service qualifiers are pre-populated

Administrators can create their own service qualifier groups

Today grouped ports/ranges are not supported in the first release

Service qualifiers

Configuration / Policy / Service Qualifiers

ACTIONS

<input type="checkbox"/>	Name	Type	VLANs	Ethertype
<input type="checkbox"/>	all	Layer 3		
<input type="checkbox"/>	all_tcp	Layer 3		
<input type="checkbox"/>	all_udp	Layer 3		
<input type="checkbox"/>	bgp	Layer 3		
<input type="checkbox"/>	cim server	Layer 3		
<input type="checkbox"/>	cim_server	Layer 3		
<input type="checkbox"/>	cim_server	Layer 3		
<input type="checkbox"/>	cim_server_tcp	Layer 3		
<input type="checkbox"/>	cim_server_udp	Layer 3		
<input type="checkbox"/>	dce_rpc_tcp	Layer 3		
<input type="checkbox"/>	dce_rpc_udp	Layer 3		
<input type="checkbox"/>	dhcp_client	Layer 3		
<input type="checkbox"/>	dhcp_server	Layer 3		
<input type="checkbox"/>	dhcp6	Layer 3		
<input type="checkbox"/>	dhcp6	Layer 3		
<input type="checkbox"/>	dns	Layer 3		
<input type="checkbox"/>	dns_sec_tcp	Layer 3		

Demo

Policy building blocks – Applications

The intent is for multiple 'Service qualifiers to be grouped and given an 'Application' label'

Applications

An application label can be aligned to an IT system application, support access role or a specific function aligned to a service qualifier or group of service qualifiers

Configuration / Policy / Applications

	<input type="checkbox"/>	Name	Service Qualifiers	Rules
...	<input type="checkbox"/>	app2	ftp_control, ftp_data, ftps_control_tcp, ftps_data_udp	rule4
...	<input type="checkbox"/>	icmp	icmp	rule-3
...	<input type="checkbox"/>	'Applications' – Feature is now a roadmap item and no definitive decision yet made on feature function		





Demo

Policy building blocks – Service Groups

Service-Groups

Service groups are a way of identifying endpoints by VM name, VM tag MAC or IP address and grouping together to as a service group and then apply to a 'rule'

You cannot mix service group type, for example if Service-Group1 is grouping device end points by IP address, you will need to create another service group to group end points with VM names

Configuration / Policy / Service Groups								
<div>   ACTIONS </div>								
<input type="checkbox"/>	Name	Type	IPv4 Addresses	MAC Addresses	Rules			
<input type="checkbox"/>	Service-Group1	Layer 3	10.1.1.1 10.1.1.12/32			Layer 3 – via VM tag, VM name or ip address		
<input type="checkbox"/>	Service-Group2	Layer 2		FF:FF:FF:FF:FF:FF 50:00:00:00:00:02 : FF:FF:FF:FF:FF:FF		Layer 2 – via MAC address & mask		

Demo

Policy building blocks – Rules

If you create a rule it can be at layer 2 or layer 3 (not both – FW rules @ Layer3+)

A rule is either providing a permit statement or deny statement

Rules can also leverage ‘service groups’ as well as ‘service qualifiers’

Configuration / Policy / Rules

Filter, Settings, Refresh, ACTIONS

	<input type="checkbox"/>	Name	Type	Action	Source Service Groups
...	<input type="checkbox"/>	rule4	Layer 3	Allow	
...	<input type="checkbox"/>	rule-general	Layer 3	Allow	Service-Group1
...	<input type="checkbox"/>	rule-2	Layer 3	Allow	

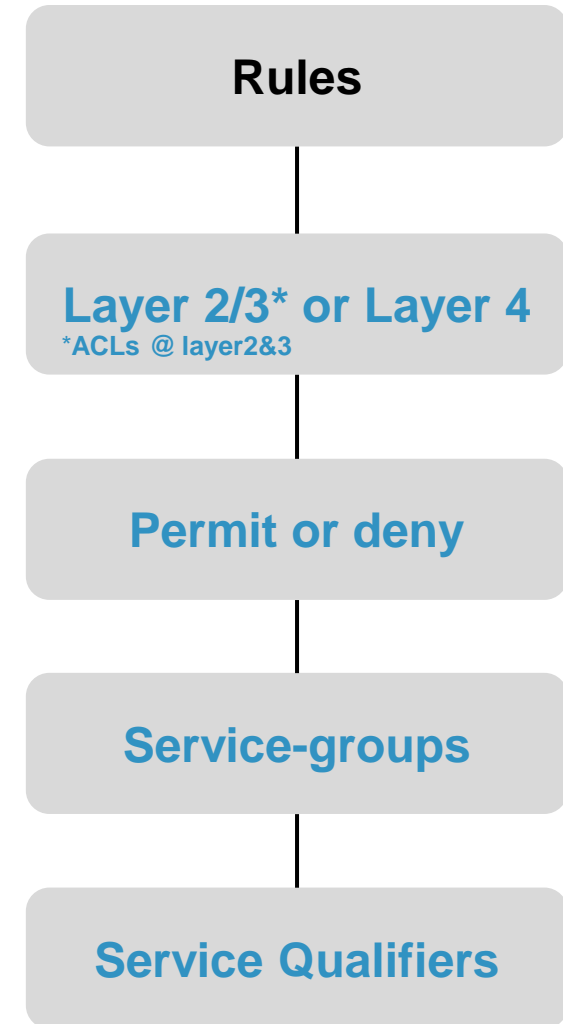
Rule -- rule-2

NAME ACTION SERVICE GROUPS APPLICATIONS AND SERVICE QUALIFIERS SUMMARY

Select or add either Applications or Service Qualifiers.

Applications: sql dbase [x] [ADD]

Service Qualifiers: Select... [ADD]



Policy building blocks – Policies

AFC Policies can leverage the Distributed FW or apply L2 & L3 ACLs

Each will leverage configured rules comprising of the various building blocks of 'service qualifiers' & 'Service groups

Enforcers will vary depending on policy deployment – with the distributed FW, the policy will be applied to VLAN(s) and will be 'fabric' wide.

Configuration / Policy / Policies

1 selected

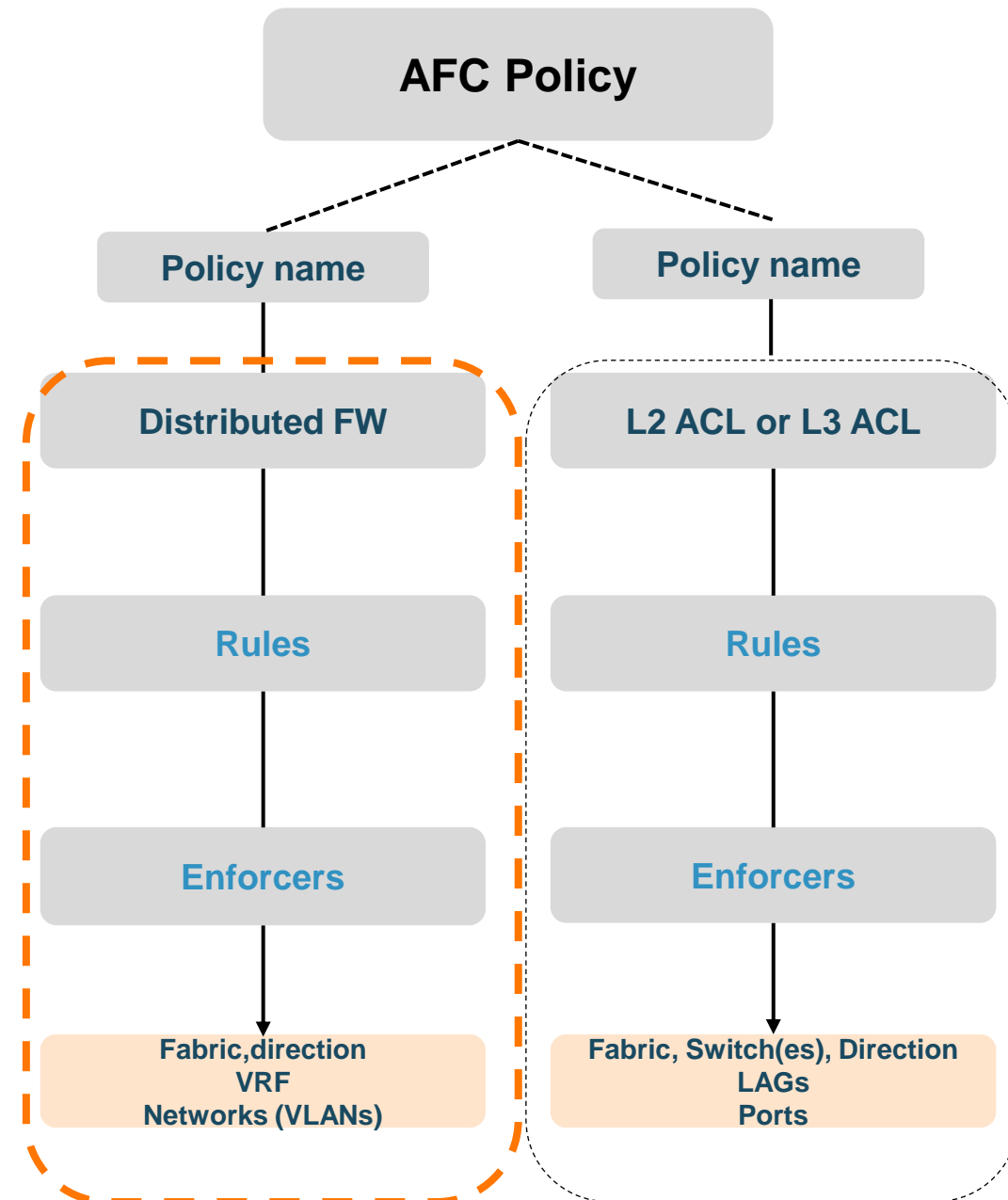
Health	Name	Enabled	Type
HEALTHY	sql-access-admin	Yes	Distributed Firewall

Policy -- sql-access-admin

NAME SETTINGS RULES ENFORCERS SUMMARY

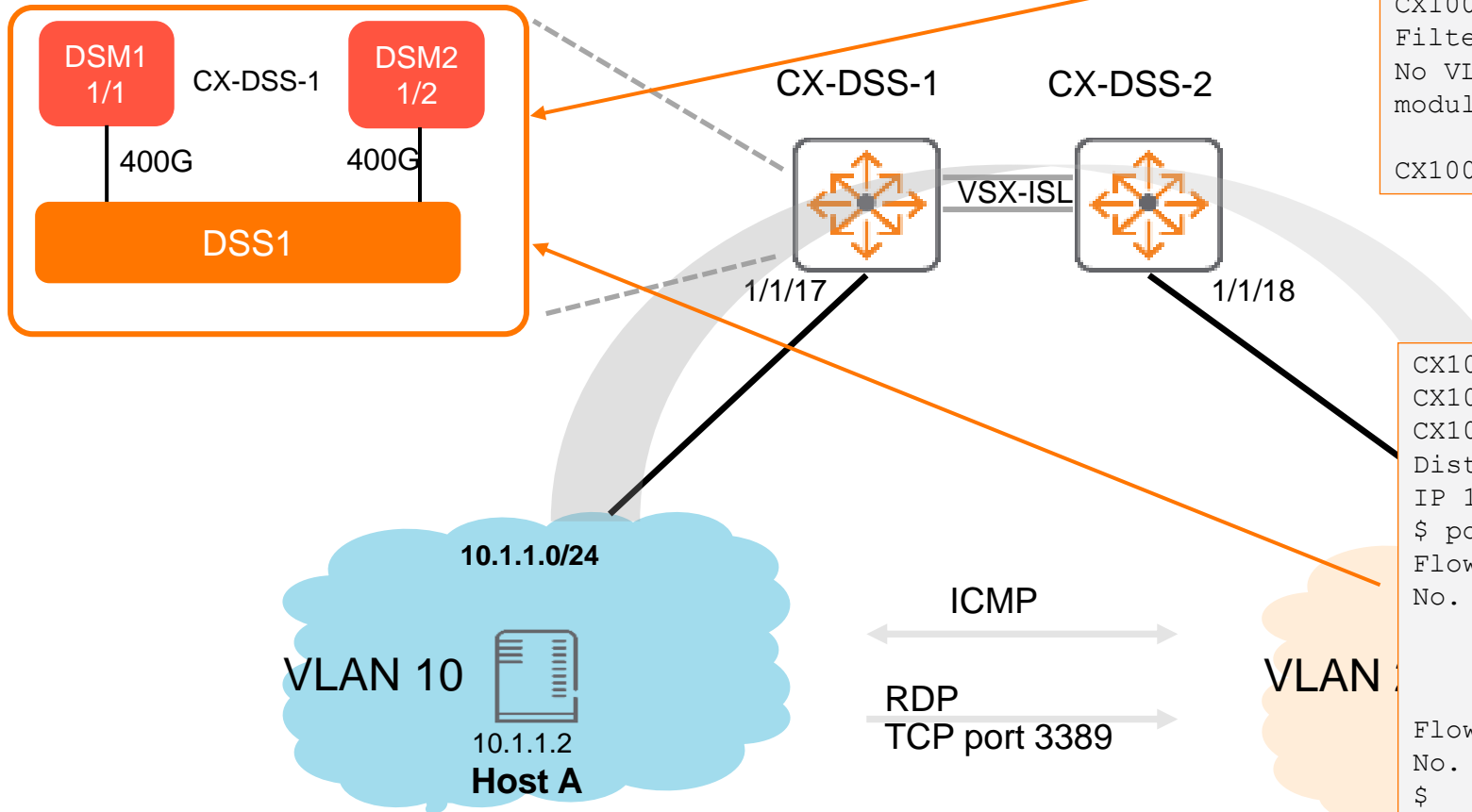
Set one or more Rules on the Policy.

Index	Name	Type	Action	Source Service Gr
1	rule-2	Layer 3	Allow	
2	rule-3	Layer 3	Drop	
3	rule4	Layer 3	Allow	



Demo topology

Traffic bypassing FW



VLAN 10 redirection

```
CX10000-R1RU33-SW1# sh dsm 1/1 red
Filter information
No VLAN redirect configured to Distributed Services
module

CX10000-R1RU33-SW1# sh dsm 1/2 red
Filter information
No VLAN redirect configured to Distributed Services
module

CX10000-R1RU33-SW1#
```

Flow table – example DSM 1/1

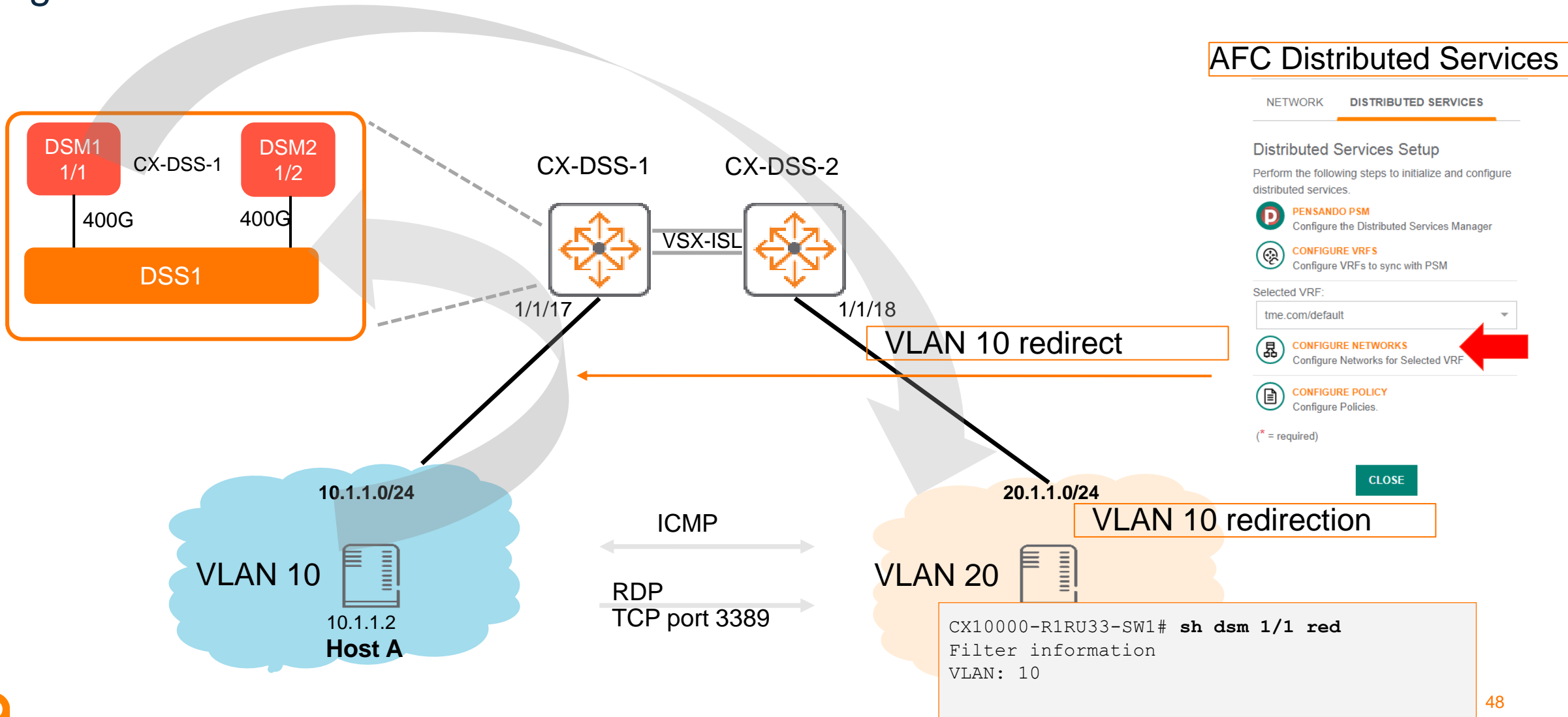
```
CX10000-R1RU33-SW1# conf t
CX10000-R1RU33-SW1(config)# diagnostics
CX10000-R1RU33-SW1(config)# diag dsm 1/1
Distributed Services module 1/1 is ready
IP 169.254.13.1
$ pdsctl show flow
Flow-table-0
No. of flows: 0
```

There are seven flow tables – abbreviated for brevity

```
Flow-table-7
No. of flows: 0
$
```

Demo topology

Egress VLAN 10 traffic redirected on SW DSS1- DSM

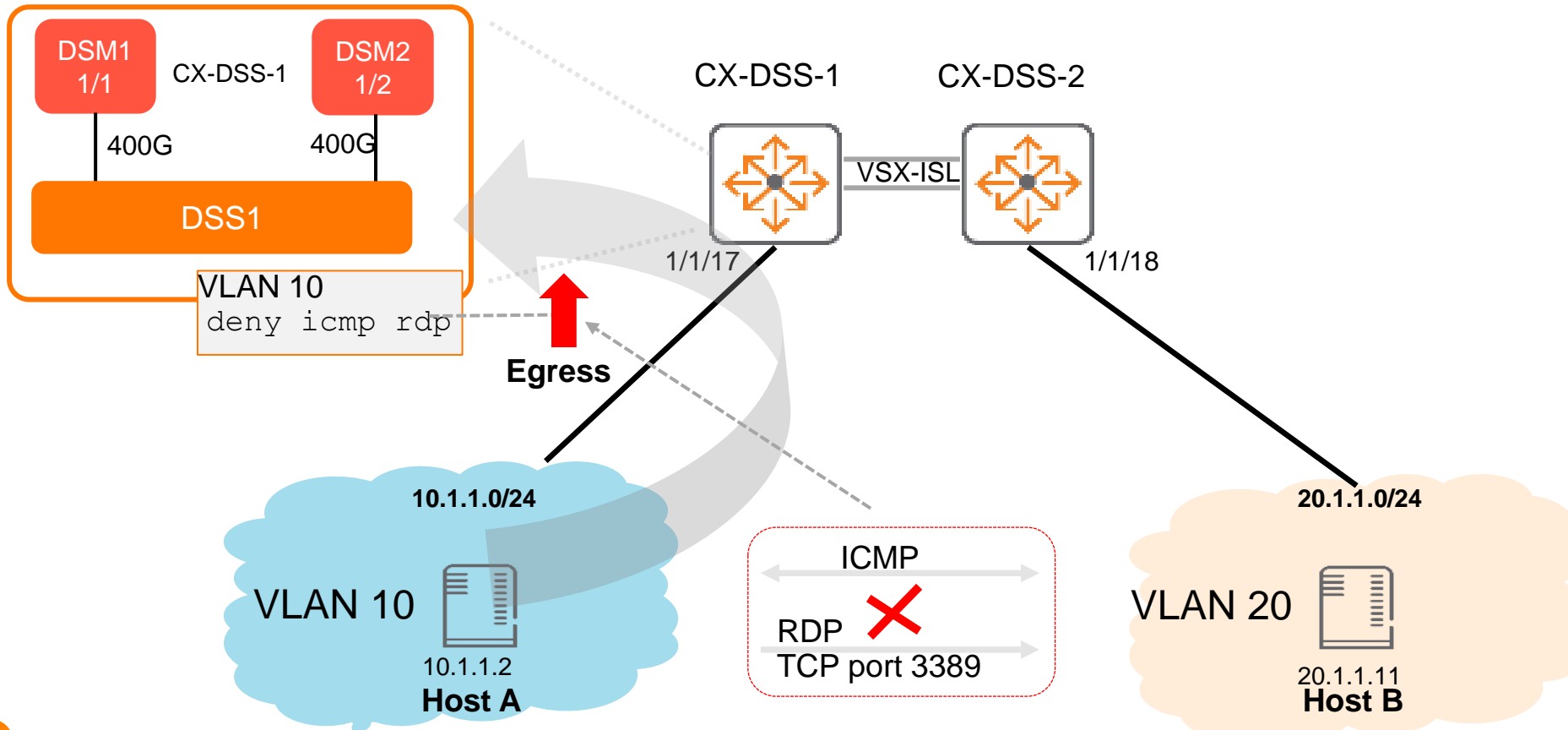


Demo topology - Demo

Egress VLAN 10 traffic redirected to DSS1 DSM – with a policy

VLAN 10 egress policy

10.1.1.2	src port	59012	20.1.1.11	dest port	3389	TCP	Deny - outbound flow
20.1.1.11	src port	3389	10.1.1.2	dest port	59012	TCP	Deny - return flow



CLI commands

```
CX10000-R1RU33-SW1# sh psm
```

Policy and Services Manager Information

```
Operational Status : admitted
Access Source      : cli
VRF                : mgmt
Host IP            : 10.10.10.150
CX10000-R1RU33-SW1#
```

```
CX10000-R1RU33-SW1# sh dsm 1/1
```

```
Distributed Services module 1/1 is ready
Description: DSS-48x25G-6x100G
Full Description:
Serial number: FSJ2128004A
Product number: DSS-4825-6100
MAC Address: 04:90:81:00:36:b6
```

```
CX10000-R1RU33-SW1# sh dsm 1/1 redirect
Filter information
VLAN: 10
```

```
CX10000-R1RU33-SW1# sh dsm 1/1
interface  Interface information
redirect   Show redirected vlans
statistics DSC interface statistics
vsx-peer   Displays VSX peer switch
information
<cr>
```

```
CX10000-R1RU33-SW1# conf t
CX10000-R1RU33-SW1(config)# diagnostics
CX10000-R1RU33-SW1(config)# diag dsm 1/1
Distributed Services module 1/1 is ready
IP 169.254.13.1
$ pdsctl show flow
Flow-table-0
No. of flows: 0
```

There are seven flow tables – abbreviated for brevity

```
Flow-table-7
No. of flows: 0
$
```

```
$ pdsctl show flow
Legend
Handle      : Session Handle
Role        : I (Initiator), R (Responder)
Direction   : U (From Uplink), H (From Host)
BdId        : Bridge Domain ID or subnet ID
SIP          : Source IP address
Sport       : Source port for TCP/UDP
Id           : ICMP identifier
DIP          : Destination IP address
Dport       : Destination port for TCP/UDP
TyCo        : ICMP type and code
Proto       : IP Protocol
Action      : A (Allow), D (Drop), P (Pending evaluation)
```

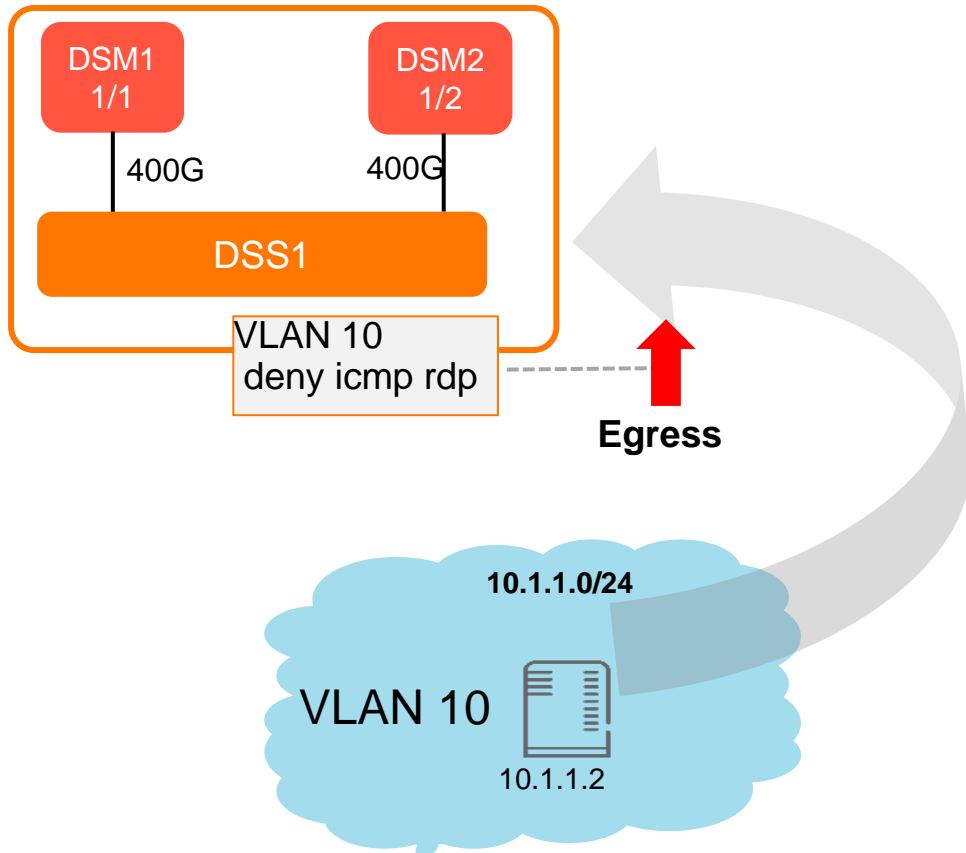
Demo topology

Egress VLAN 10 traffic redirected to DSS1- DSM with Policy (deny)

Sample Flow table – example DSM 1/1

Handle	Role/Dir	BdId	SIP	Sport Id	DIP	Dport TyCo	Proto
Flow-table-0							
No. of flows: 0							
Flow-table-1							
2097231	I/H	1	10.1.1.2	3	20.1.1.11	2048	ICMP D
2097231	R/U	1	20.1.1.11	3	10.1.1.2	0	ICMP D
No. of flows: 2							
Flow-table-2							
4194366	I/H	1	10.1.1.2	62621	15.234.147.195	53	UDP A
4194366	R/U	1	15.234.147.195	53	10.1.1.2	62621	UDP A
4194376	I/H	1	10.1.1.2	59012	20.1.1.11	3389	TCP D
4194376	R/U	1	20.1.1.11	3389	10.1.1.2	59012	TCP D
No. of flows: 4							
Flow-table-3							
6291610	I/H	1	10.1.1.2	49924	15.234.147.195	53	UDP A
6291610	R/U	1	15.234.147.195	53	10.1.1.2	49924	UDP A

Troubleshooting – Policy not behaving as stated



– troubleshooting flow

1. Check PSM and DSC switch integration and connectivity & integration from AFC to the PSM

2. Check the appropriate VLAN redirected to the DSM modules

3. Verify FW policies are being correctly applied, correct policy direction ,ports, VLAN and policy sequence

4. Is the flow already present in the flow table?
Session may need to be restarted

5. Is the flow hitting the flow table ?

6. Check host connectivity to switch

Caveats and configuration notes

Policy change from deny to permit (and vice versa) will require a new flow to be seen if the flow already exists in the flow table

Flow table use source/destination UDP /TCP ports to match against destination rule to permit or deny a flow

A policy (whether permit/deny ingress/egress) will automatically permit or deny the return flow as defined in the policy rules

For every rule in the policy, validate the following:-

- There should be only be a single 'Qualifier' per rule
- The 'Qualifier' in the rule should only have a single entry

Removing a network (VLAN) in the DSC network panel from AFC will automatically remove all flows from the flow table for that VLAN (decoupling VLAN redirect)

UDP (& ICMP) packet flows inactivity timeout from the flow table is 90 seconds

TCP packet flows inactivity timeout from the flow table is 3600 seconds (1hr)

Where no policy is applied, the default is allow all, where a policy is named the default is a implicit deny all.

The background features a solid red circle in the upper-left corner and a large, dark blue shape with a white dotted pattern that occupies the right and bottom portions of the frame.

Additional Resources

Ordering Information

SKU Includes Platform &
Perpetual Software RTU

Aruba CX 10000



CX-OS



Pensando Services

PSM, Stateful firewall, DDoS, telemetry



AFC Automation (Optional Add-On)

Orderability Enabled Dec CY'21

Product SKU	Description
-------------	-------------

R8P13A	Aruba CX 10000-48Y6C FB6F2PS Bundle
--------	-------------------------------------

R8P14A	Aruba CX 10000-48Y6C BF6F2PS Bundle
--------	-------------------------------------

R8R51A	Aruba CX 10000 FB AC PSU
--------	--------------------------

R8R52A	Aruba CX 10000 BF AC PSU
--------	--------------------------

R8R53A	Aruba CX 10000 FB Fan
--------	-----------------------

R8R54A	Aruba CX 10000 BF Fan
--------	-----------------------

R8R55A	Aruba CX 10000 1U 2p Rack Mount Kit
--------	-------------------------------------

R8R56A	Aruba CX 10000 1U 4p Rack Mount Kit
--------	-------------------------------------

Pensando Policy Services Manager (PSM) is bundled with the Aruba CX 10000 switch and will be available on ASP for Customer downloads



Aruba Services Offers for CX 10000

Service Level Options	Details
Foundation Care Services	NBD Exchange
	4 Hour Exchange
	NBD Onsite
	4 Hour Onsite
	6 Hour Call to Repair
	TAC-Only
	Hardware-Only
HTS Professional Services	Aruba CX 10000 w/Pensando QuickStart Service



HPE Network Services for Pensando

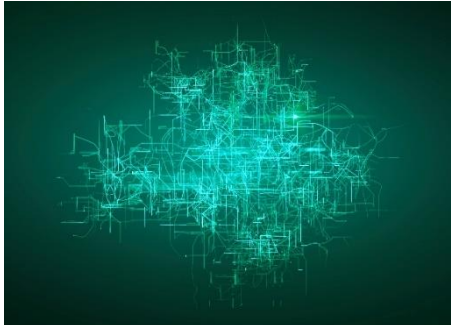
Pointnext



Advise

Guide customers on what they have (pain points) and what their future state looks like

Build a roadmap that will help them realize the full value of Pensando



Assess

Interview based discovery of current state for telemetry and networking

Add on (future): DC infrastructure, security, apps, DevOps, DevSecOps, skills, economic analysis



Design

Network telemetry, functions and security rules migration to Pensando

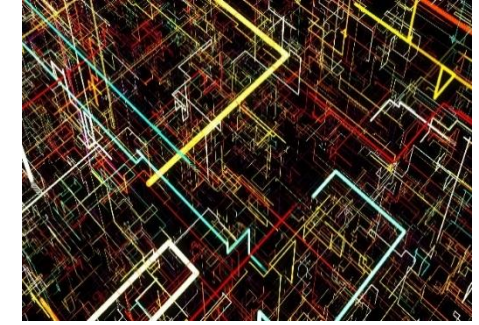
Multi-cloud: integration design, distributed FWs, micro-segmentation, multi-DC, automation



Integrate

Implementation of the Pensando solution and integration with existing datacenter infrastructure

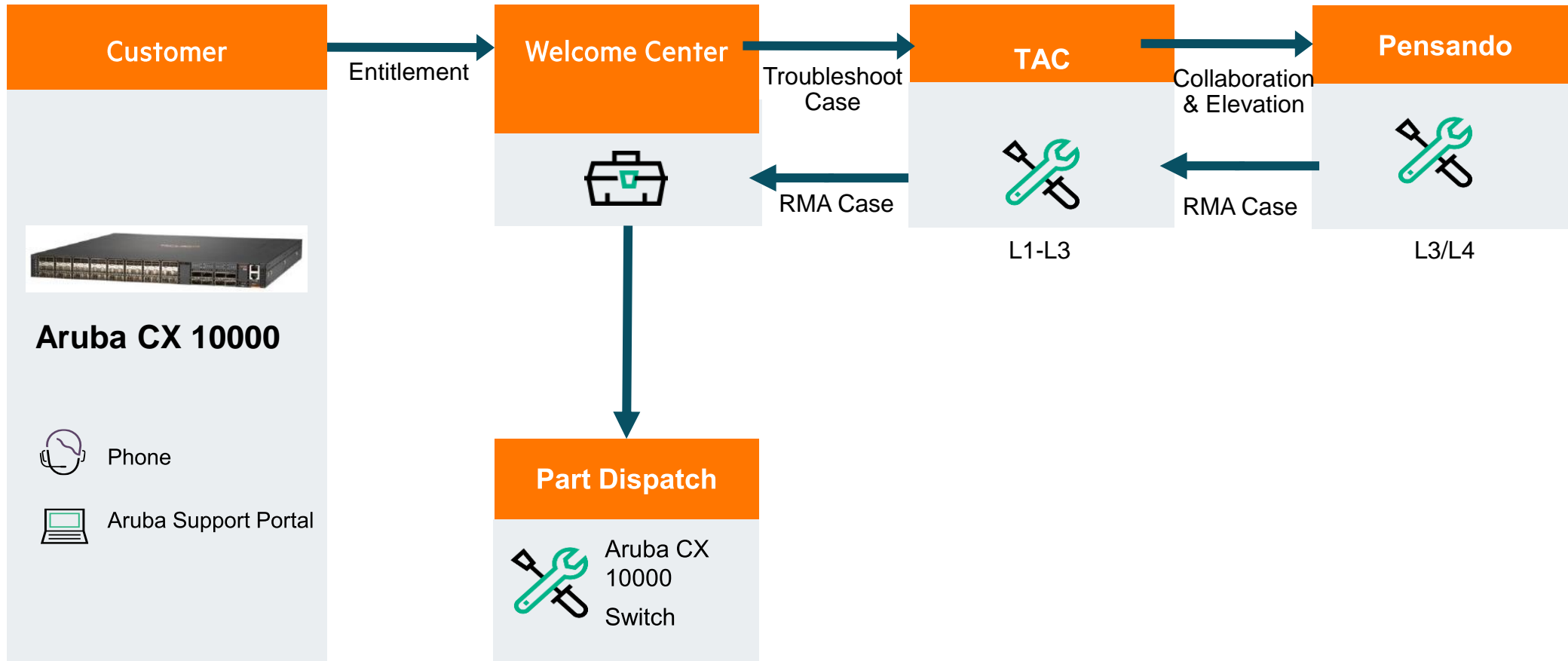
As-built verification testing and handover training



Optimize

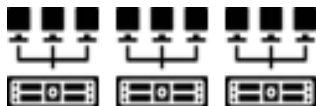
Enhanced exploitation of Pensando features to optimize telemetry, network and security services

Support Call Flows – Aruba CX 10000



TCO Comparison Data Center Security

Every CX 10000 Includes Firewall, Zero-trust



Network and Security Services	Centralized Appliances	Distributed Agents	Distributed Services Switch
25/100G ToR Switch	\$36,000	\$36,000	Aruba CX 10000
Firewall Appliance	\$386,000	\$0	\$44,995
Software Agents	\$0	\$250/year per license	Included – All network and stateful security services Each CX pair = 800G FW
3 Year TCO (70% discount)	\$2,705,040	\$3,373,560	\$864,000

Assumptions:

of total servers: 1,000
of servers per rack: 32
of network ports per server: 2
of TOR switches needed: 64
Bandwidth per rack: 400Gbps
E-W vs N-S BW: 75% vs 25%

Firewall model: Fortigate 4200F
Firewall throughput: 800Gbps
of Firewalls needed: 12

of VMs per server: 10
of total license needed: 10,000

~70%
1/3 of the TCO
w/Optimized
Service delivery



Qualifying Questions to Get Started



- Data Center modernization, application, cloud initiatives?
- IT refresh / upgrade – higher performing compute, storage ➡ network (CX 25/100G)
- HPE Compute, SimpliVity, VMware, Nutanix HCI ➡ software-defined automation (AFC)
- Struggling to manage/scale heavily segmented multi-tenant DC environments ➡ (AFC, VXLAN/EVPN)
- East-West firewall, Micro-Segmentation, extending Zero Trust enterprise ➡ DSS
- Traditional Firewall appliance sprawl - frustration with the high cost/complexity of HW FW, Agents ➡ DSS
- HPE and Aruba FULL STACK IT solutions delivers more value / competitive differentiation

Thank You