

atmosphere'22 BELGIUM

Aruba Data Center Solutions

Dik van Oeveren, Consulting Systems Engineer

September 2022

Data Center Network Architectures and Use Cases

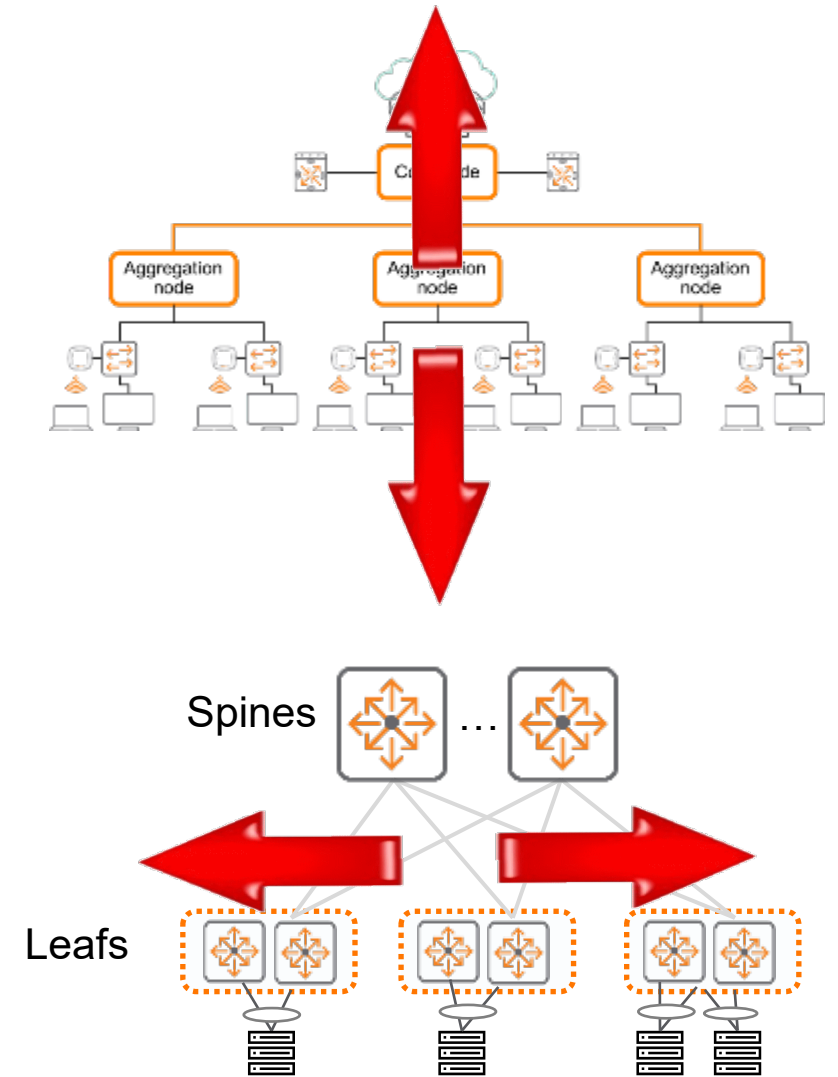
What makes a Data Center Network?

– Local Area Network (LAN) / Campus Networks

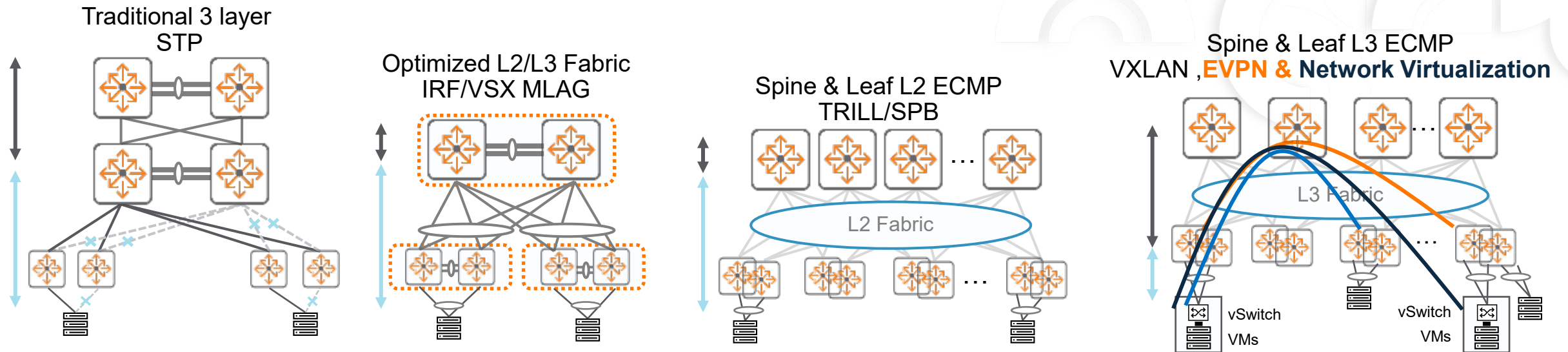
- Same geographical location, building, campus etc.
- Wired and wireless network connects users, IP phones and wireless APs
- Typical features required: POE, 802.1X etc

– Data Center Networks

- Same geographical location (single data center)
- Connects Servers/VMs/Containers, applications, storage, firewalls/ load balancers, etc. – wired connectivity
- Stable, low latency fabrics with high availability / high performance and throughput / density and scale
- Build revenue for business (E-Commerce)!
- Typical features required: VXLAN/EVPN, BGP, OSPF, DCB, etc..
- Focus on improving East - West traffic between racks

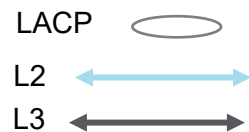


Enterprise Datacenter Network Architecture Evolution

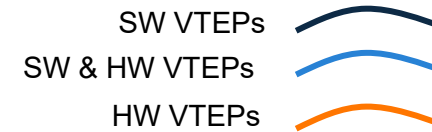


Scalability, Agility, Orchestration

Classic / Underlay



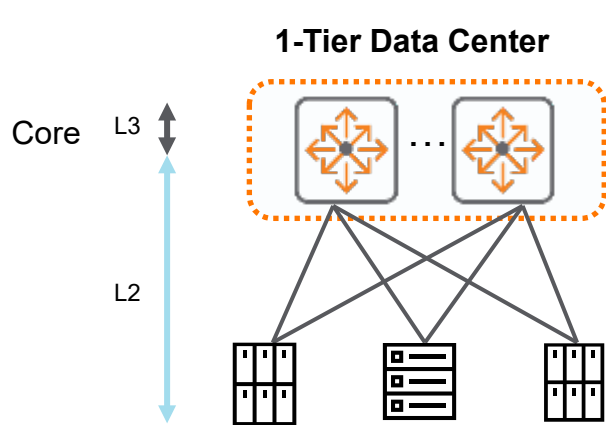
VXLAN Overlay



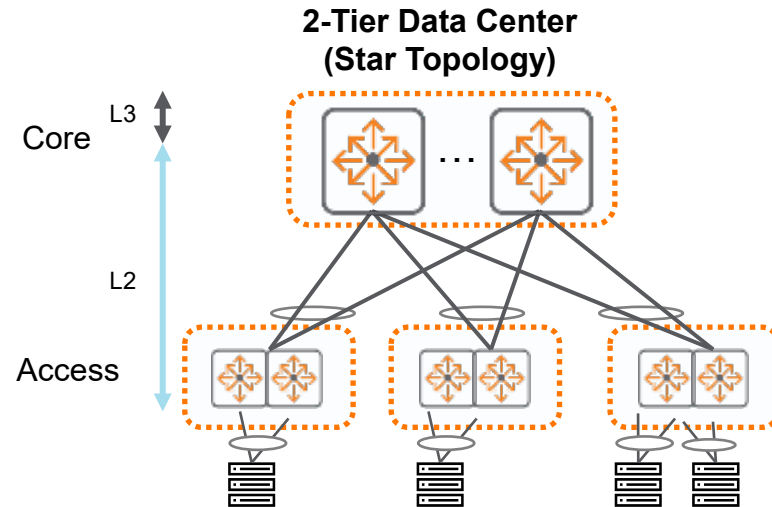
Aruba Data Center Network Reference Architecture Overview

Does Every DC Network Architecture require Spine/Leaf with VXLAN?

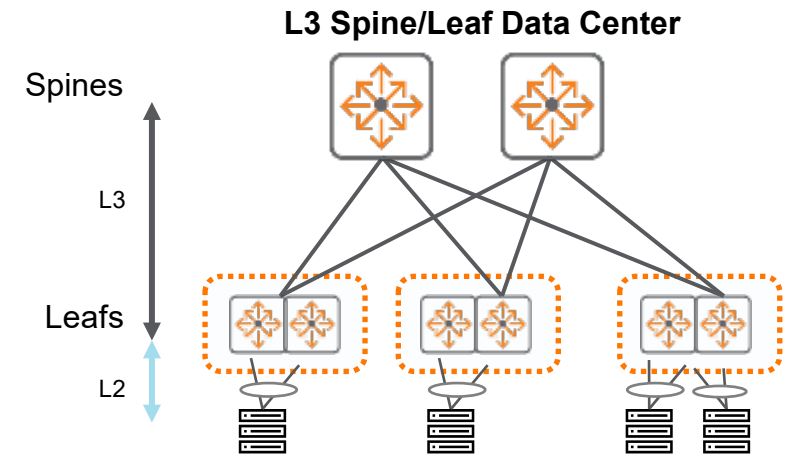
- These are still valid based on customer requirements, they all support HA and network automation



- Supports L2 (e.g. vMotion) /L3 connectivity between racks/servers
- Modular/Fixed port core switches are possible, this will determine how many servers can be connected
- Link aggregation from core to servers provides traffic load sharing and link/switch redundancy

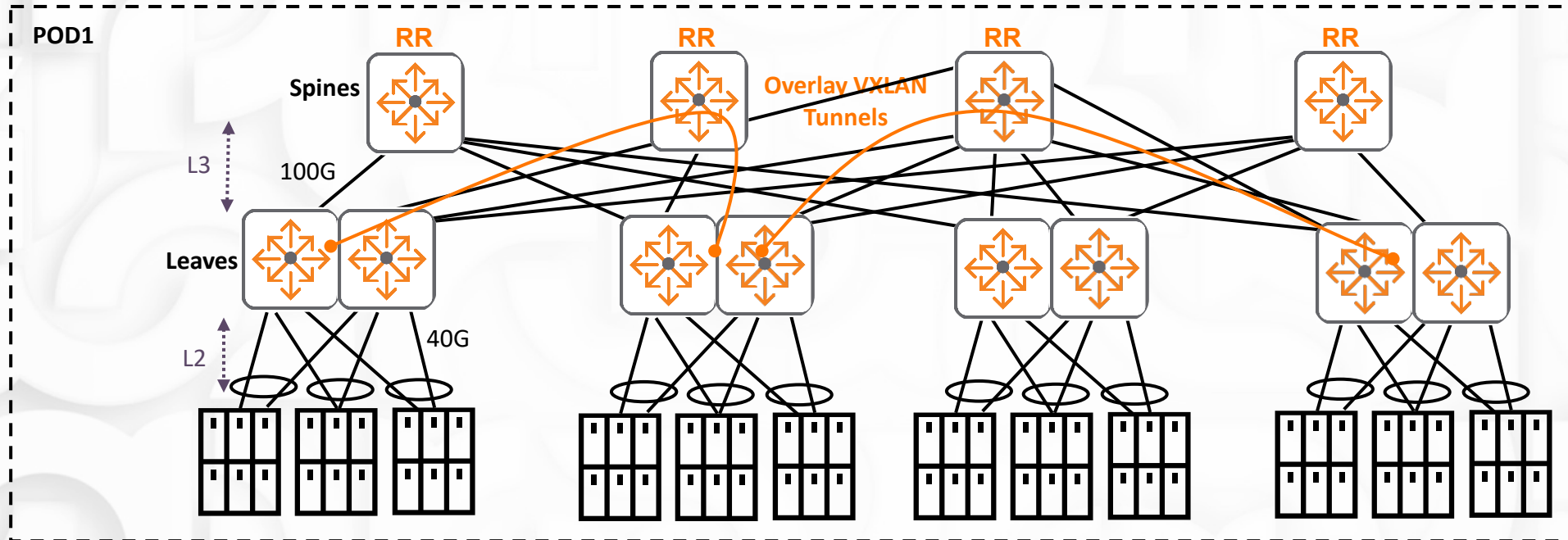


- Supports L2 (e.g. vMotion) /L3 connectivity between racks/servers
- Modular/Fixed port core switches are possible, this will determine how many access switches can be used
- Loop free topology as link aggregation is used between Access/Core for traffic load sharing and link/switch redundancy
- STP enabled as a backup mechanism to prevent loops
- Link aggregation from access to servers provides traffic load sharing and link/switch redundancy



- Supports L3 connectivity between racks/leafs
- Removes STP since an L3 IP fabric is used
- Failure domain contained at L2 leafs
- Modular/Fixed port spines are possible, this will determine how large the fabric can grow
- Link aggregation from leafs to servers provides traffic load sharing and link/switch redundancy

Intra-DC with EVPN VXLAN



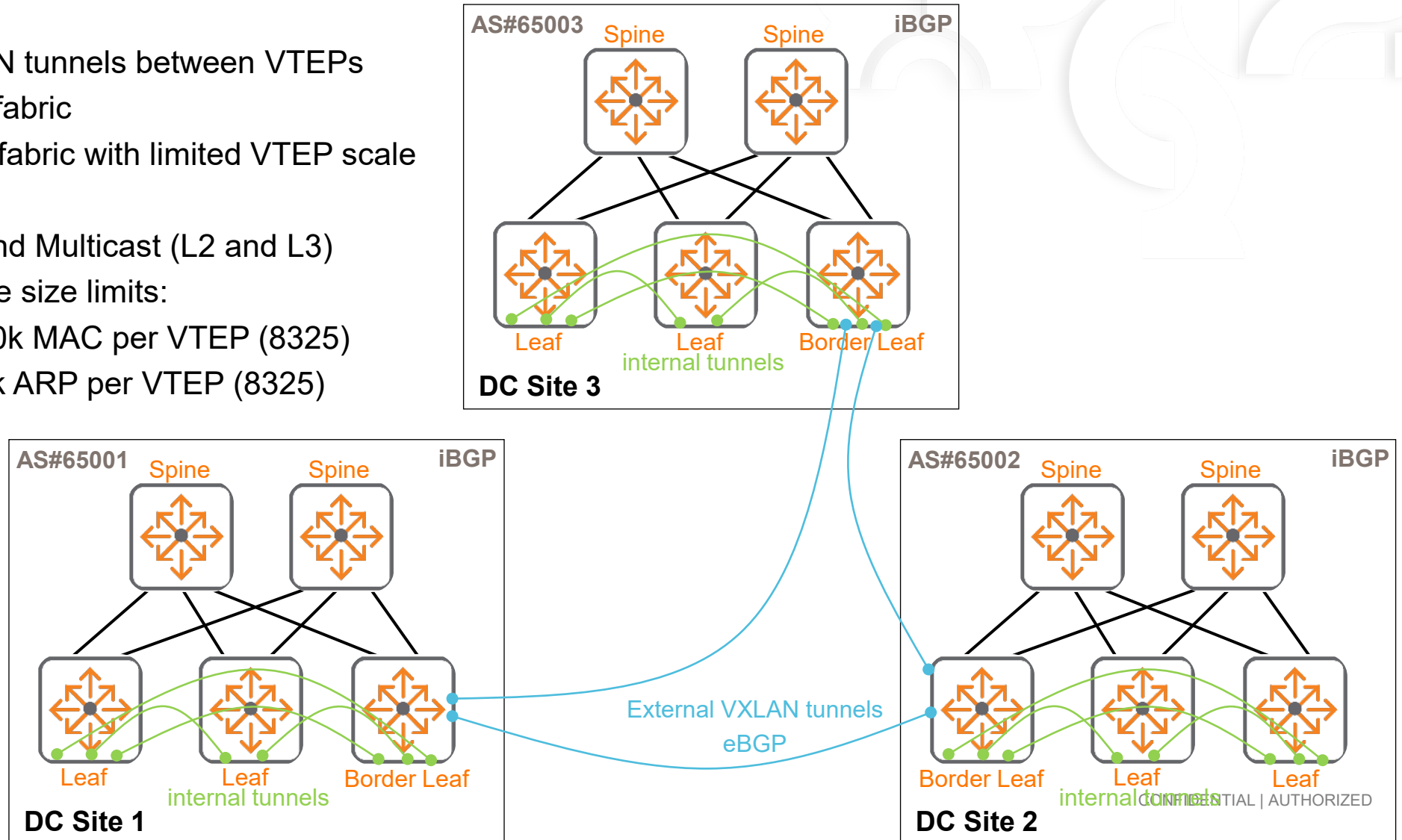
Main drivers:

- Provides both L2/L3 network connectivity and multi-tenancy (beyond 4K VLANs) across racks
- Virtual network agility
- Remove STP from the DC fabric

Data Center Interconnect: Single Fabric (1 AS) multi site

– Recommended for majority of deployments (based on CX 10.10)

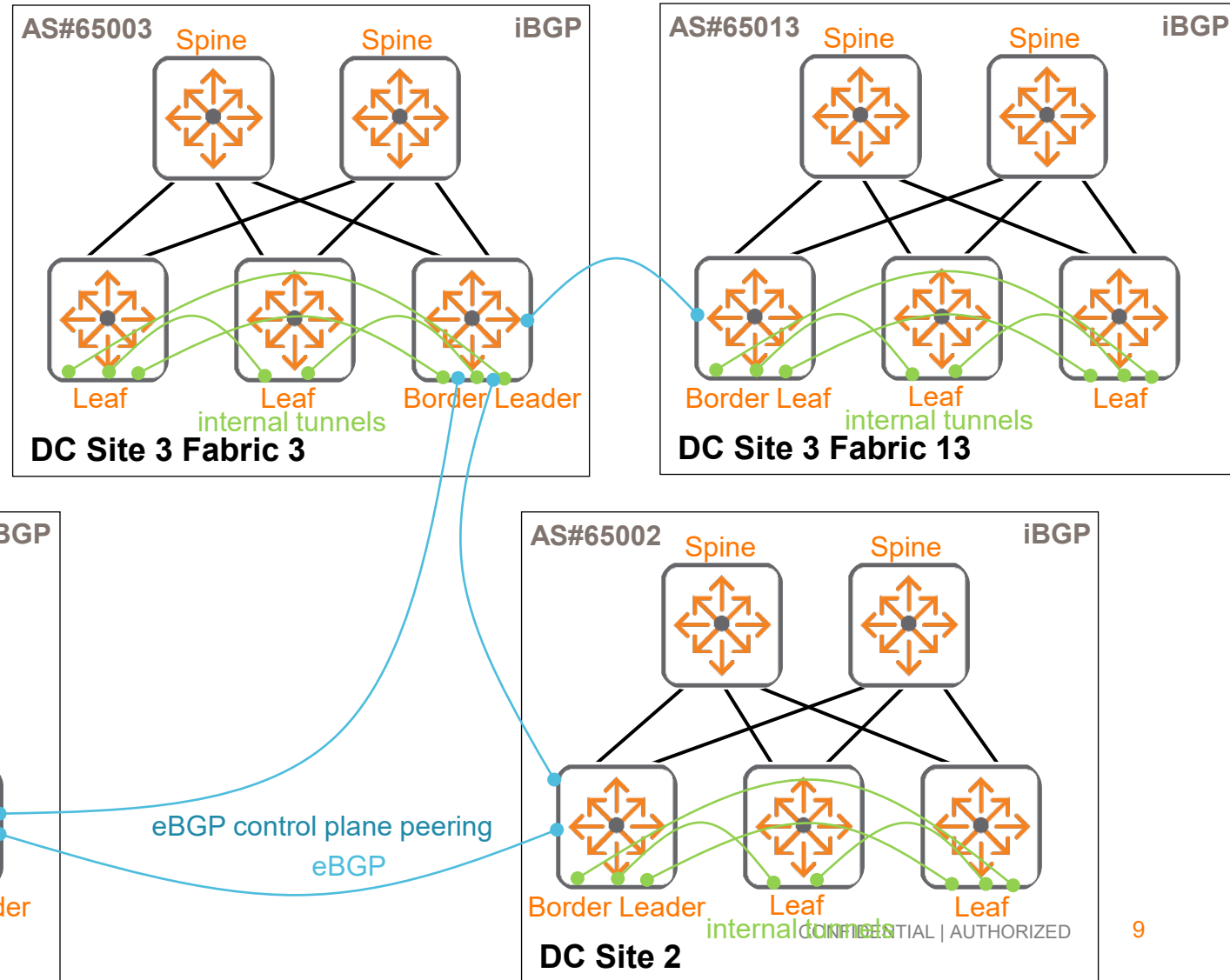
- Full mesh VXLAN tunnels between VTEPs within a VXLAN fabric
- A single VXLAN fabric with limited VTEP scale (256 max.)
- Supports IPv6 and Multicast (L2 and L3)
- Be aware of table size limits:
 - Approx. 100k MAC per VTEP (8325)
 - Approx. 50k ARP per VTEP (8325)



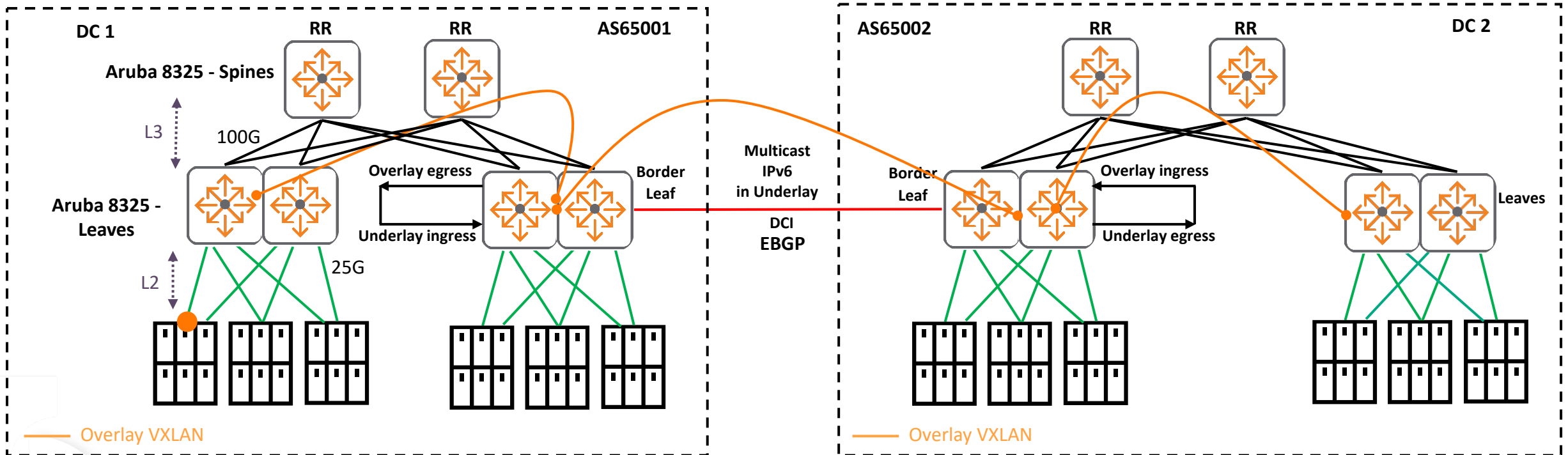
Data Center Interconnect: Multiple Fabric, multiple sites

– If VTEP scale out is required (based on CX 10.10)

- Scales out number of VTEP's (256 per fabric)
- Border leader function avoids BGP full meshing
 - Acts as “proxy” for border leaves
- More complex configuration:
 - Route Maps to define next hop IP
- At this stage, no support for IPv6 and Multicast
 - Requires EVPN route-type 6, 7, 8



Workaround for multi hop multicast/IPv6 in overlay

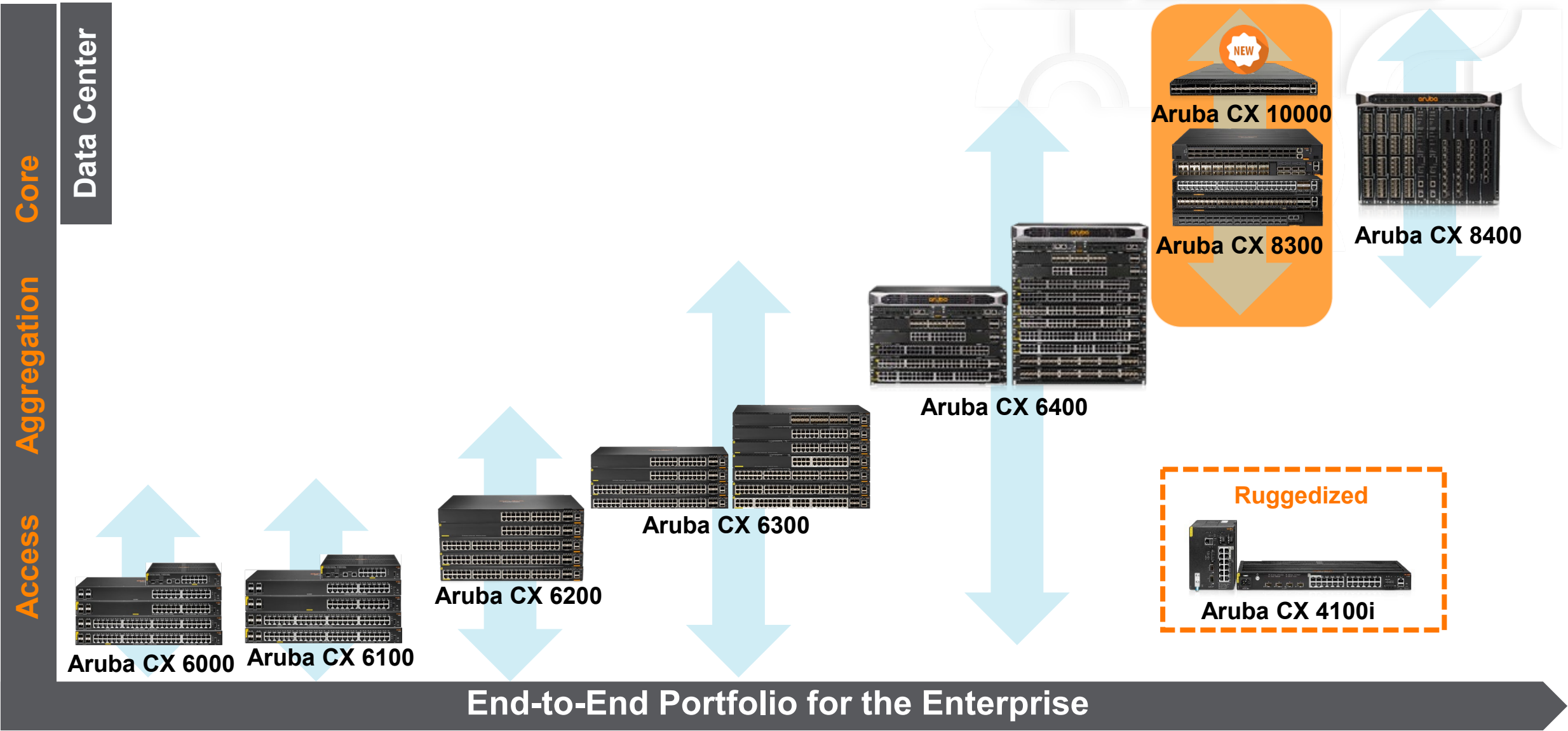


Intra DC overlay multicast/IPv6 is egressed from overlay to underlay network on the border leaf
Inter DC multicast/IPv6 traffic uses the underlay network

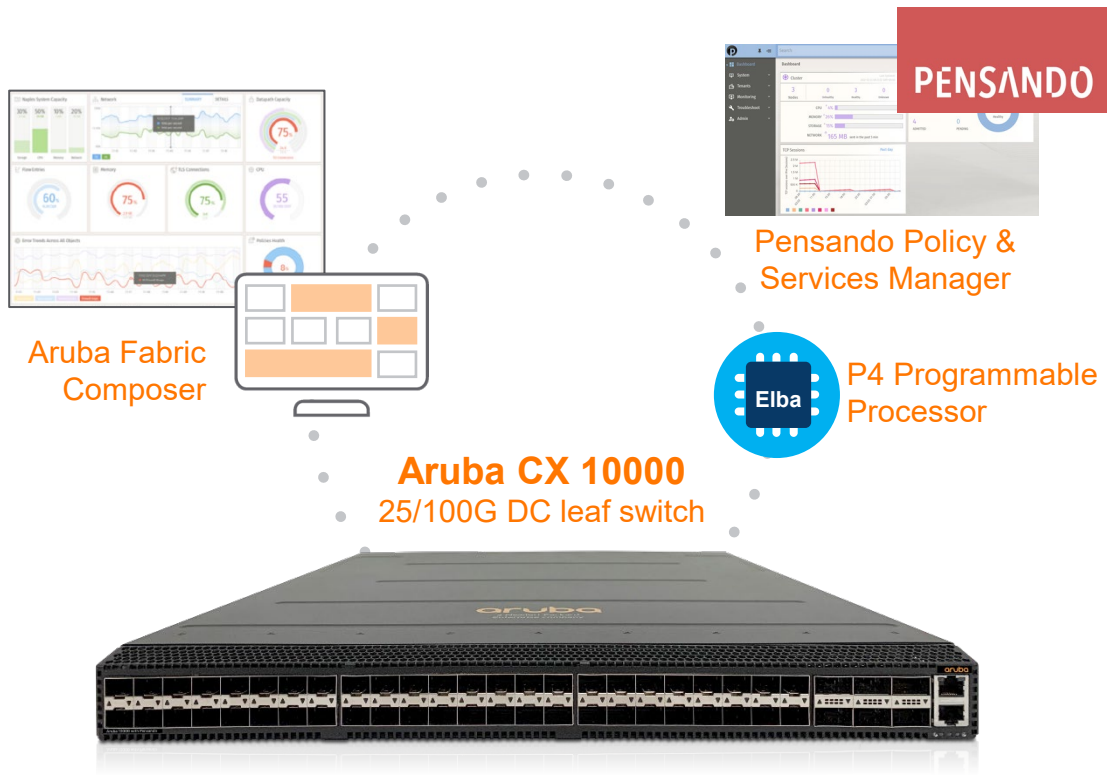
Aruba Data Center Network Switching portfolio



Aruba CX Switching Portfolio



Aruba CX 10000 Distributed Services Switch - Powered by Pensando



—1RU Fixed Switch Form Factor:

- T3 Switching ASIC - 3.2 Tbps, 32MB Buffer (shared)
 - Used for forwarding/routing/other features
- 2 x Pensando Elba (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 Services/Use-Cases:

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

—Platform Management Options:

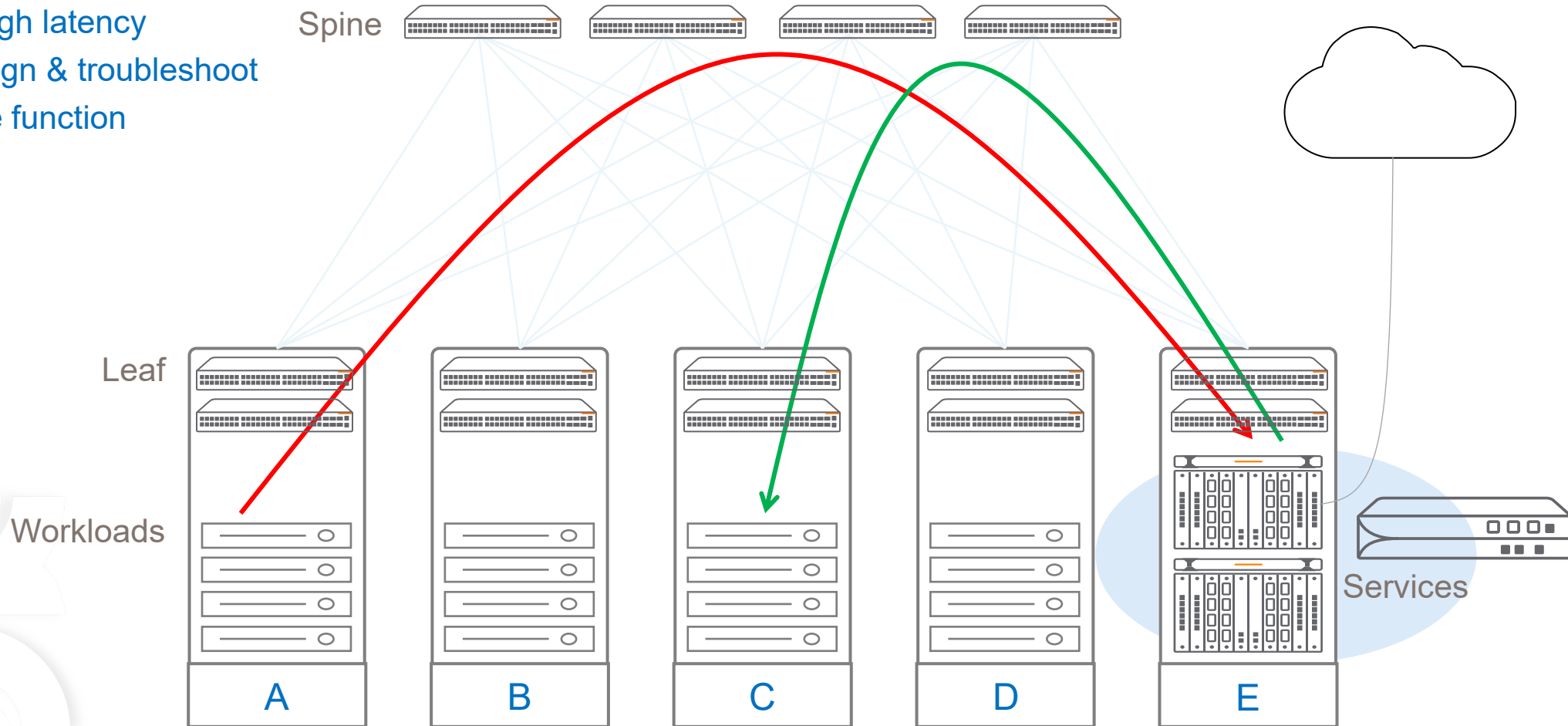
- Aruba AFC & Pensando PSM
- PSM & DevOps Tools (Terraform/Ansible), REST API



Security enforcement today: centralized services architecture

Centralized Services

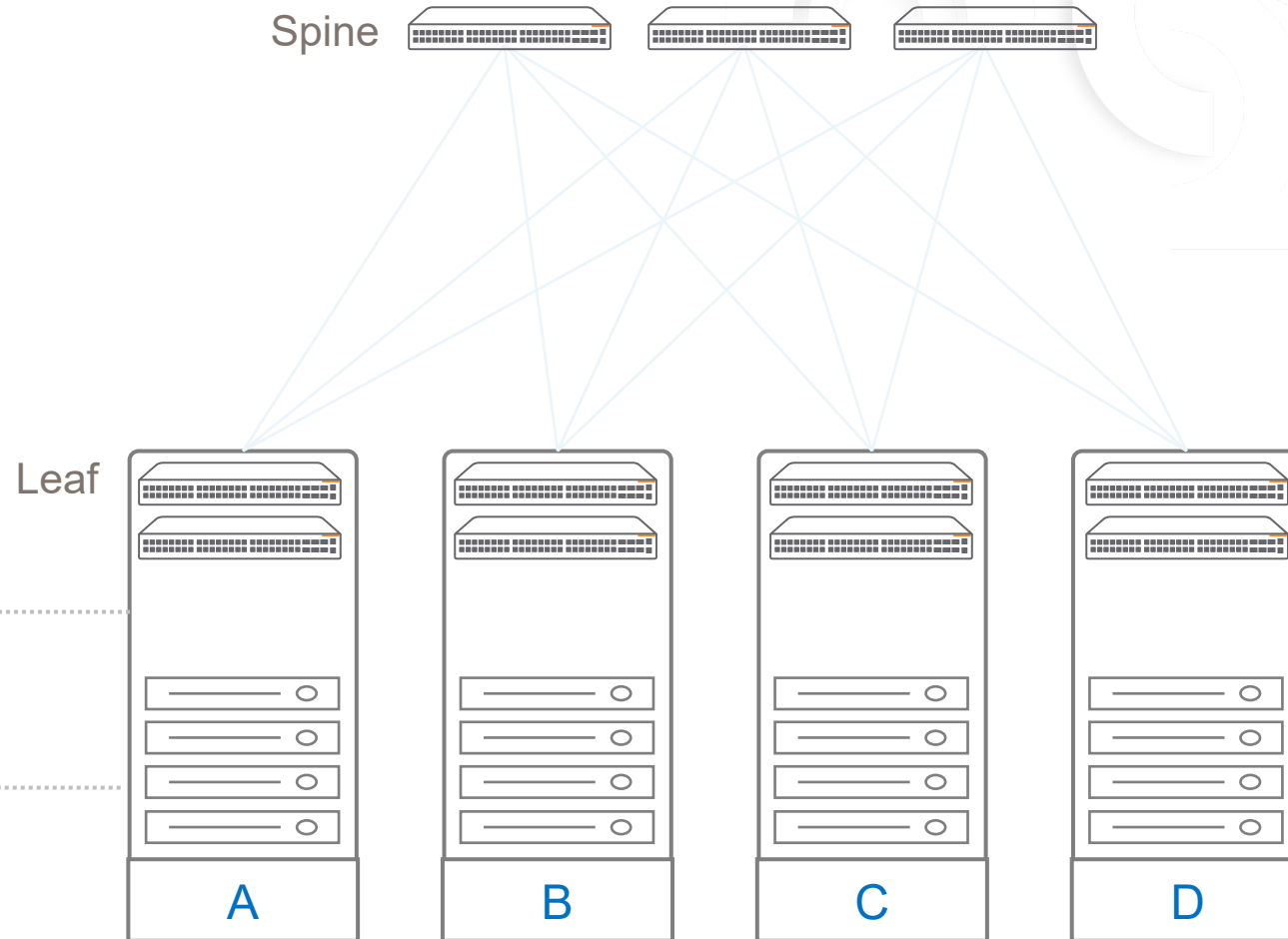
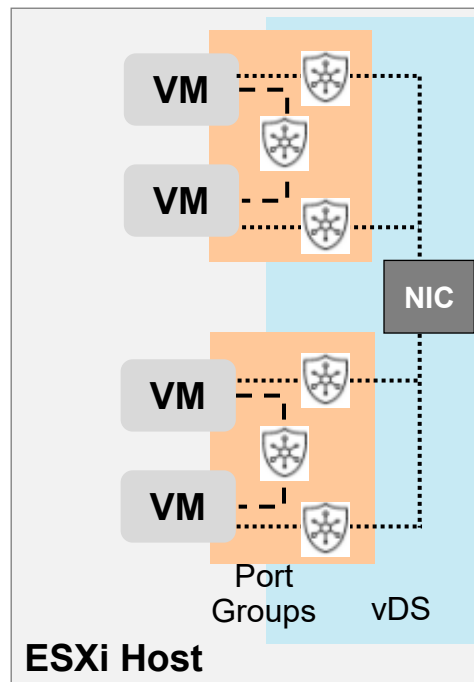
- Waste of bandwidth
- Congestion & high latency
- Complex to design & troubleshoot
- Limited to single function
- Very expensive



Security enforcement today: distributed Services architecture

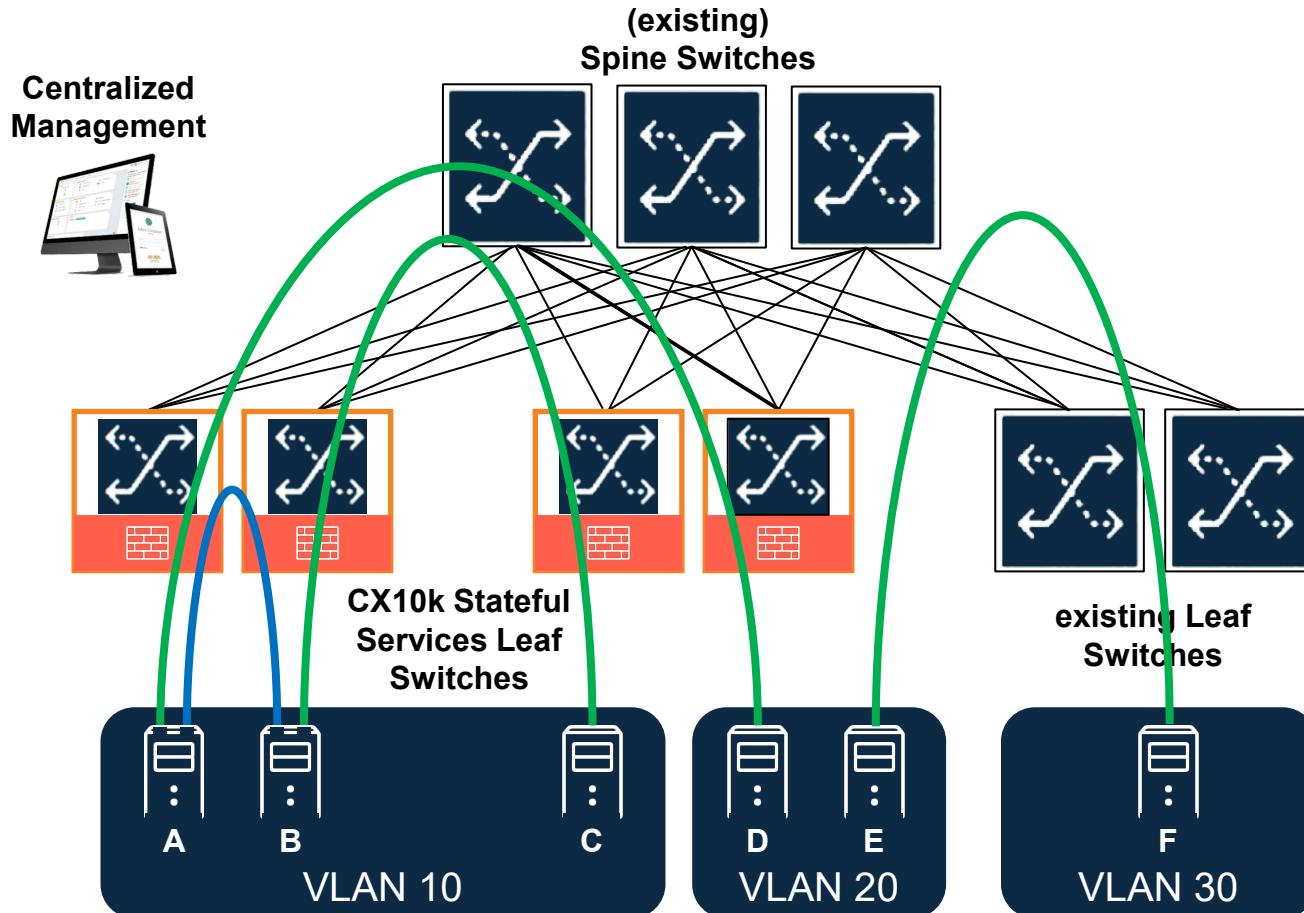
Software based Services

- High resource requirement on host (CPU/Memory)
- Congestion & high latency (ms)
- Complex to design & troubleshoot
- Very expensive (Licenses)



Stateful network firewall

Protect the services inside your Data Center



Secure traffic between two servers through Stateful Firewall:

In the same VLAN

In different VLANs

Both connected any leaf Distributed Services Switch

Where one server is connected to an existing leaf

High performance (800Gbps)

Low latency (4us)

Protect the Unprotected:

Hypervisors (management, storage)

Backup Servers

IP Storage Appliances

Shared Services

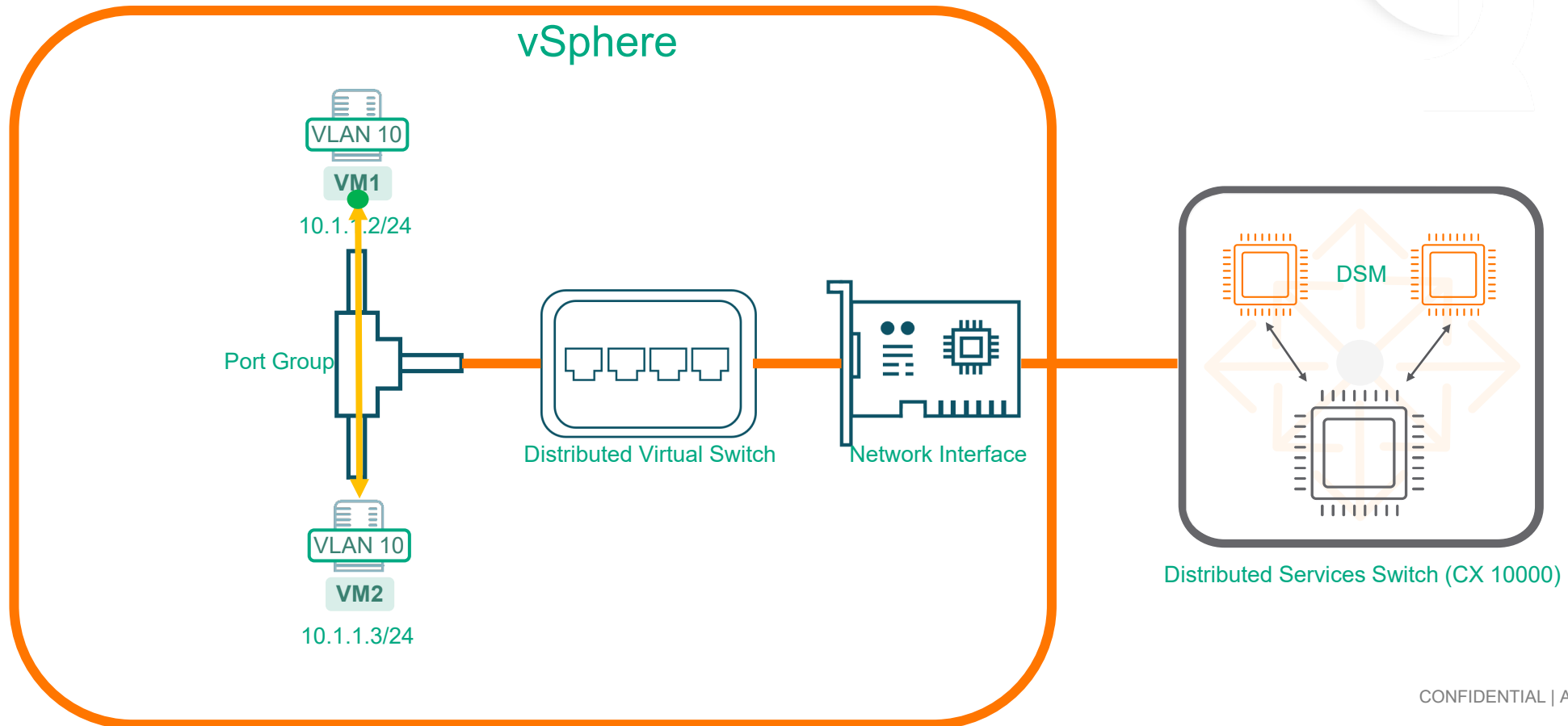
Bare Metal Servers

How does it work: micro segmentation

Traffic inspection for workloads that are on the same network

By default on a vSphere port group traffic within the port group is allowed

How can we create micro segmentation that allows stateful firewalling between workloads that are on the same subnet/VLAN?

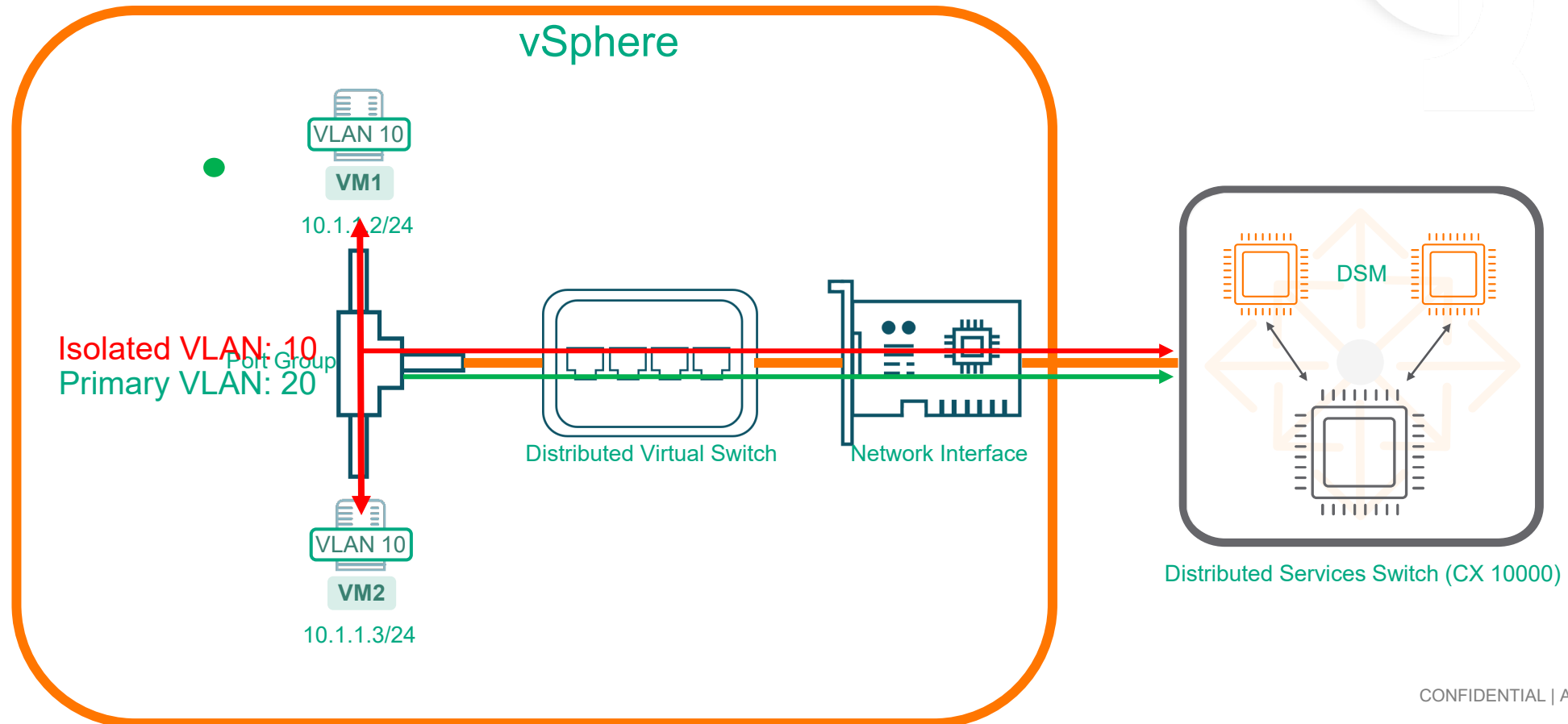


How does it work: micro segmentation

Traffic inspection for workloads that are on the same network

Micro segmentation can be achieved through Private VLAN functionality in vSphere and on Aruba CX switches

The primary VLAN (VLAN 20) is used for egress traffic into the CX 10000. VLAN 10 traffic is also egressed, there is still isolation between hosts

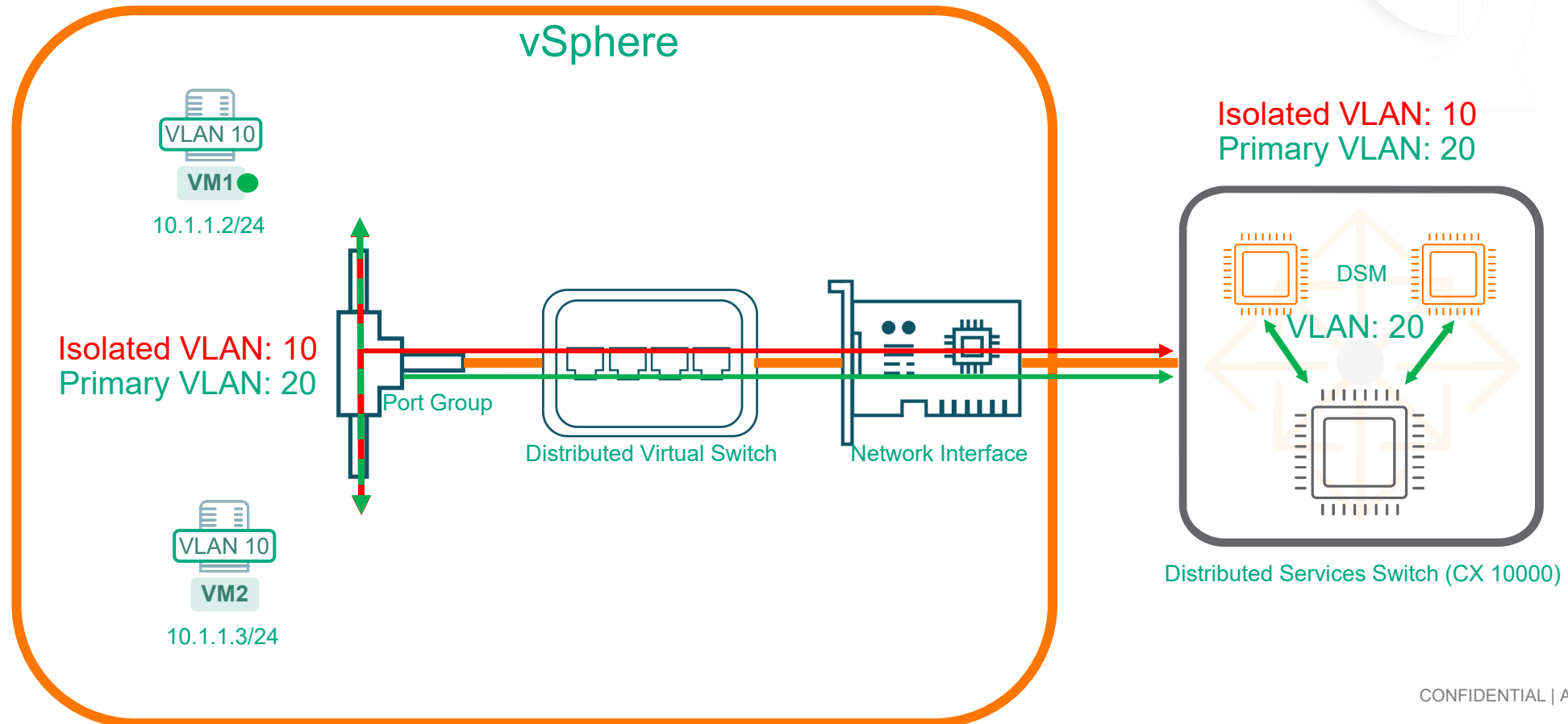


How does it work: micro segmentation

Traffic inspection for workloads that are on the same network

The CX 10000 is also configured for Private VLAN where VLAN 10 is the isolated VLAN and VLAN 20 the primary (promiscuous) VLAN

When a VLAN (Network) exists on the DSM for the primary VLAN (20), traffic is redirected to the DSM for stateful inspection

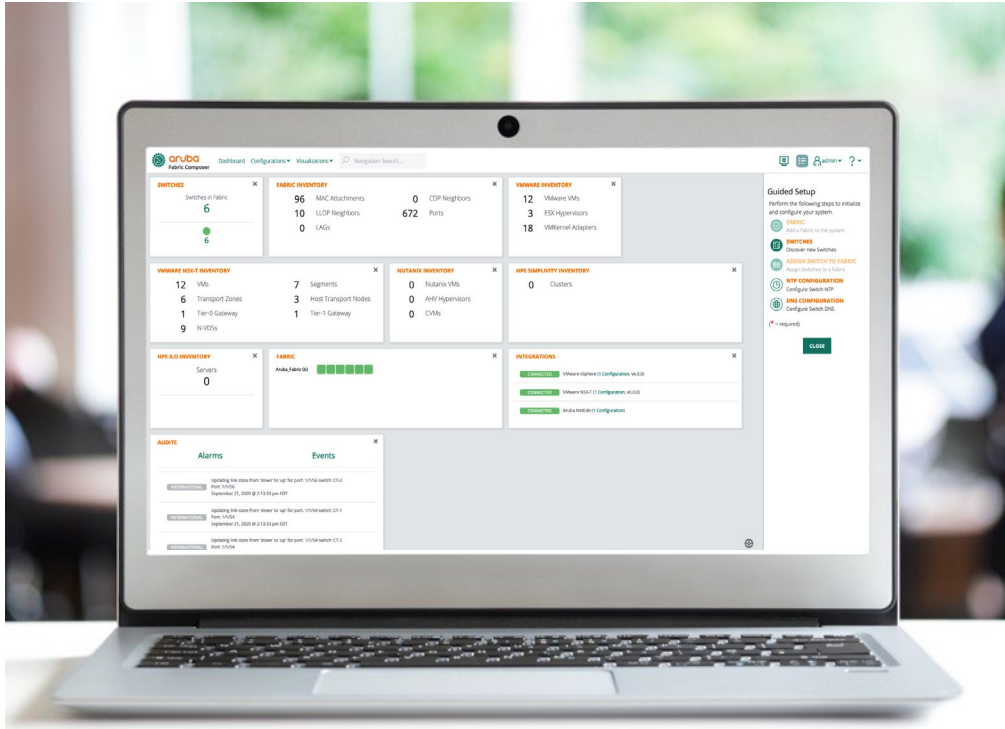


Aruba Data Center Network Orchestration



Aruba Fabric Composer

The on-site data fabric orchestration system



Key Features & Benefits

- Simplified provisioning & orchestration
- Complex workflow automation
- Manage and monitor global network configuration
- Integrate with 3rd party data center orchestration systems
- Integration with HPE Infrastructure hardware and software
- Visualize data center infrastructure
- Automate lifecycle events in the data center
- Holistic troubleshooting of end-to-end network connectivity

Aruba Fabric Composer Delivers 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

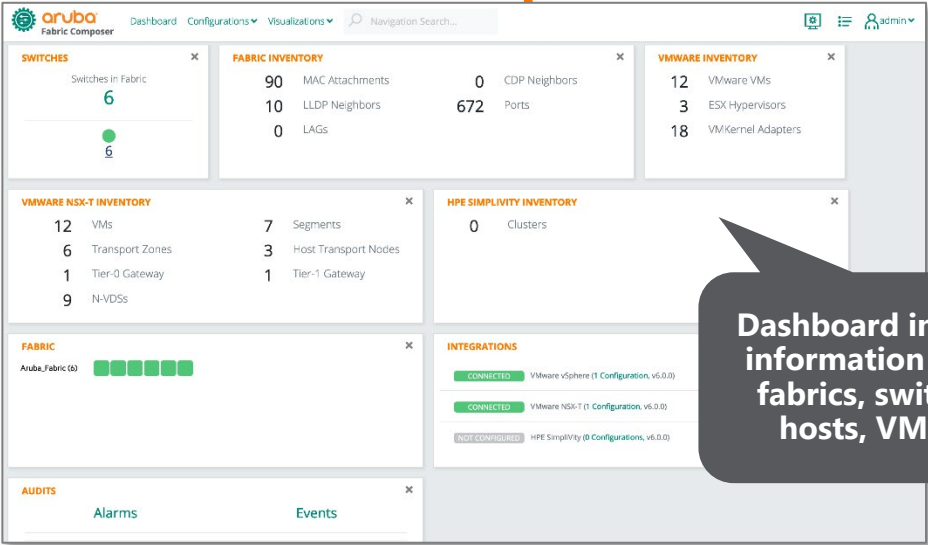


SECURITY AND COMPLIANCE TEAMS

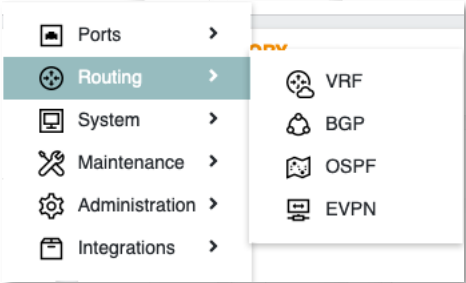
- Centrally managed distributed services to secure critical workloads and data
- Maintain flow-level visibility and control across the estate
- Simplify scale and increase performance
- Reduce costs and increase efficiencies



Aruba Fabric Composer



Dashboards include information about fabrics, switches, hosts, VMs, ...



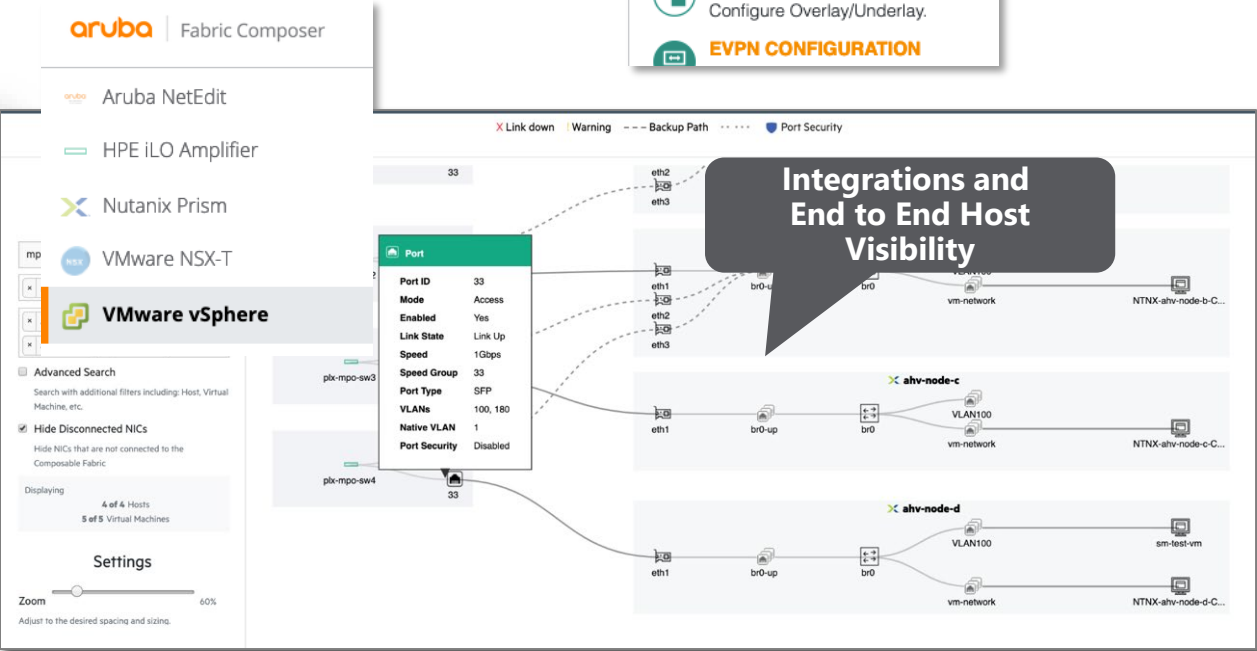
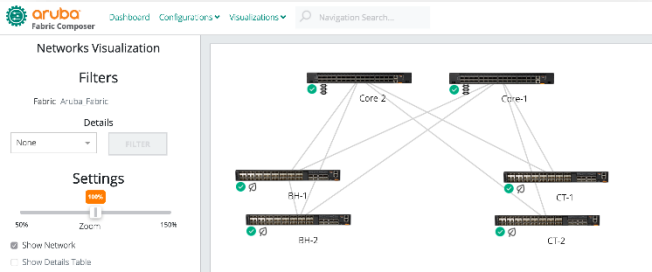
Workflow Automations and Guided Setup

Guided Setup

Perform the following steps to initialize and configure your system.

- FABRIC**
 - Add a Fabric to the system.
- SWITCHES**
 - Discover new Switches.
- ASSIGN SWITCH TO FABRIC**
 - Assign Switches to a Fabric.
- NTP CONFIGURATION**
 - Configure Switch NTP.
- DNS CONFIGURATION**
 - Configure Switch DNS.
- VSX CONFIGURATION**
 - Configure VSX Switch Pairing.
- LEAF SPINE CONFIGURATION**
 - Configure Leaf Spine Connections.
- OVERLAY CONFIGURATION**
 - Configure Overlay/Underlay.
- EVPN CONFIGURATION**

Network and Switch Visualizations



Aruba Fabric Composer: Workflow based orchestration

Create an EVPN (Add)

Configuration / Routing / EVPN

Fabric GVA-Fabric

EVPN

EVPN MULTI SITE

	Name	Switch Name	VLAN	L2VNI	Route Distinguisher	Import Route Targets (ASPL...	Export Route Targets (AS...	
	Enter Name...	Enter Switch Name...	Enter Regex for VLAN...	Enter Regex for L2VNI...	Enter Regex for Route Disting...	Enter Regex for Import Route	Enter Regex for Export	
<input type="checkbox"/>	GVA-EVPN-aruba-10k-1-1201	aruba-10k-1	1201	121201	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-aruba-10k-2-1201	aruba-10k-2	1201	121201	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-aruba-8360-3-1201	aruba-8360-3	1201	121201	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-VSX-Primary-1201	VSX-Primary	1201	121201	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-VSX-Secondary-1201	VSX-Secondary	1201	121201	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-aruba-10k-1-1202	aruba-10k-1	1202	121202	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-aruba-10k-2-1202	aruba-10k-2	1202	121202	auto	auto	auto	
<input type="checkbox"/>	GVA-EVPN-aruba-8360-3-1202	aruba-8360-3	1202	121202	auto	auto	auto	Yes
<input type="checkbox"/>	GVA-EVPN-VSX-Primary-1202	VSX-Primary	1202	121202	auto	auto	auto	Yes
<input type="checkbox"/>	GVA-EVPN-VSX-Secondary-1202	VSX-Secondary	1202	121202	auto	auto	auto	Yes

ACTIONS

Add

Edit

Delete

VLAN

Import Route Targets

Export Route Targets

Redistribute Host Route

Settings

Reapply EVPN

Yes

Yes

Yes



Aruba Fabric Composer: Workflow based orchestration

Create an EVPN (Select switches or apply to the whole fabric)

EVPN(GVA-Fabric)

Introduction

Switches

Name

VNI Mapping

Settings

Summary

Create EVPN instances across the entire Fabric or select specific Switches.

☐ Create EVPN instances across the entire Fabric and all Leaf and Border Leaf Switches contained within it.

Switches *

Select Switches...

GVA-VSX_VSX-Secondary_VSX-Primary (VSX-Primary / VSX-Secondary)

aruba-10k-1

aruba-10k-2

aruba-8360-3

SELECT ALL

(* = Required)

CANCEL

BACK

NEXT



Aruba Fabric Composer: Workflow based orchestration

Create an EVPN (Provide a descriptive name)

EVPN(GVA-Fabric)

Introduction

Switches

Name

VNI Mapping

Settings

Summary

Enter a required Name Prefix and an optional Description.

Name Prefix *

EVPN Customer A

Any non empty string, example: Evpn-mapping

Description

Example: Evpn-mapping Description

(* = Required)

CANCEL

BACK

NEXT



Aruba Fabric Composer: Workflow based orchestration

Create an EVPN (Assign the appropriate VLAN's: VNI)

EVPN(GVA-Fabric)

✓

✓

✓

✓

?

?

Introduction

Switches

Name

VNI Mapping

Settings

Summary

Specify required VLANs and Base L2VNI for generating the VLAN-to-VNI mappings.

VLANs *

1204

A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102.

Base L2VNI *

120000

A number between 0 and 16777214, example 0. Computed VLAN + VNI cannot exceed 16777214.

(* = Required)

CANCEL

BACK

NEXT



Aruba Fabric Composer: Workflow based orchestration

Create an EVPN (Assign the route target type and virtual MAC Addresses)

EVPN(GVA-Fabric)

✓

Introduction

✓

Switches

✓

Name

✓

VNI Mapping

✓

Settings

?

Summary

Set the Virtual MAC Address Range. Select or add a MAC Address Resource Pool or specify a range.

MAC Address Resource Pool *

GVA MAC Address pool (00:00:00:00:06-00:00:00:00:00:ff)

ADD

MAC Address Range

A hyphen-separated range of valid MAC Addresses, example: 02:00:00:00:02:00-02:00:00:00:02:FF

Set the required Route Target Type and associated values. The Route Target Type determines the format of the route targets generated.

Route Target Type *

AUTO

AUTO

ASN:VNI

ASN:VLAN

ASN:NN

(* = Required)

CANCEL

BACK

NEXT

CONFIDENTIAL | AUTHORIZED

28

Aruba Fabric Composer: Workflow based orchestration

Create an EVPN (and..... DEPLOY)

EVPN(GVA-Fabric)

✓

Introduction

✓

Switches

✓

Name

✓

VNI Mapping

✓

Settings

✓

Summary

Fabric

Name Prefix

Description

VLANs

Base L2VNI

Route Target Type

MAC Address Resource Pool

GVA-Fabric

EVPN Customer A

1204

120000

AUTO

GVA MAC Address pool (00:00:00:00:00:06-00:00:00:00:00:ff)

CANCEL

BACK

APPLY

The Pensando Distributed Services Platform



– Policy & Services Manager

- Centralized Lifecycle Management
- Ensures Full-stack Enterprise-grade Security & Policy Compliance
- REST-API integration with existing apps

– Distributed Services

- Software-defined Services
- Inline All-the-time at Wire-speed

– Programmable ASIC

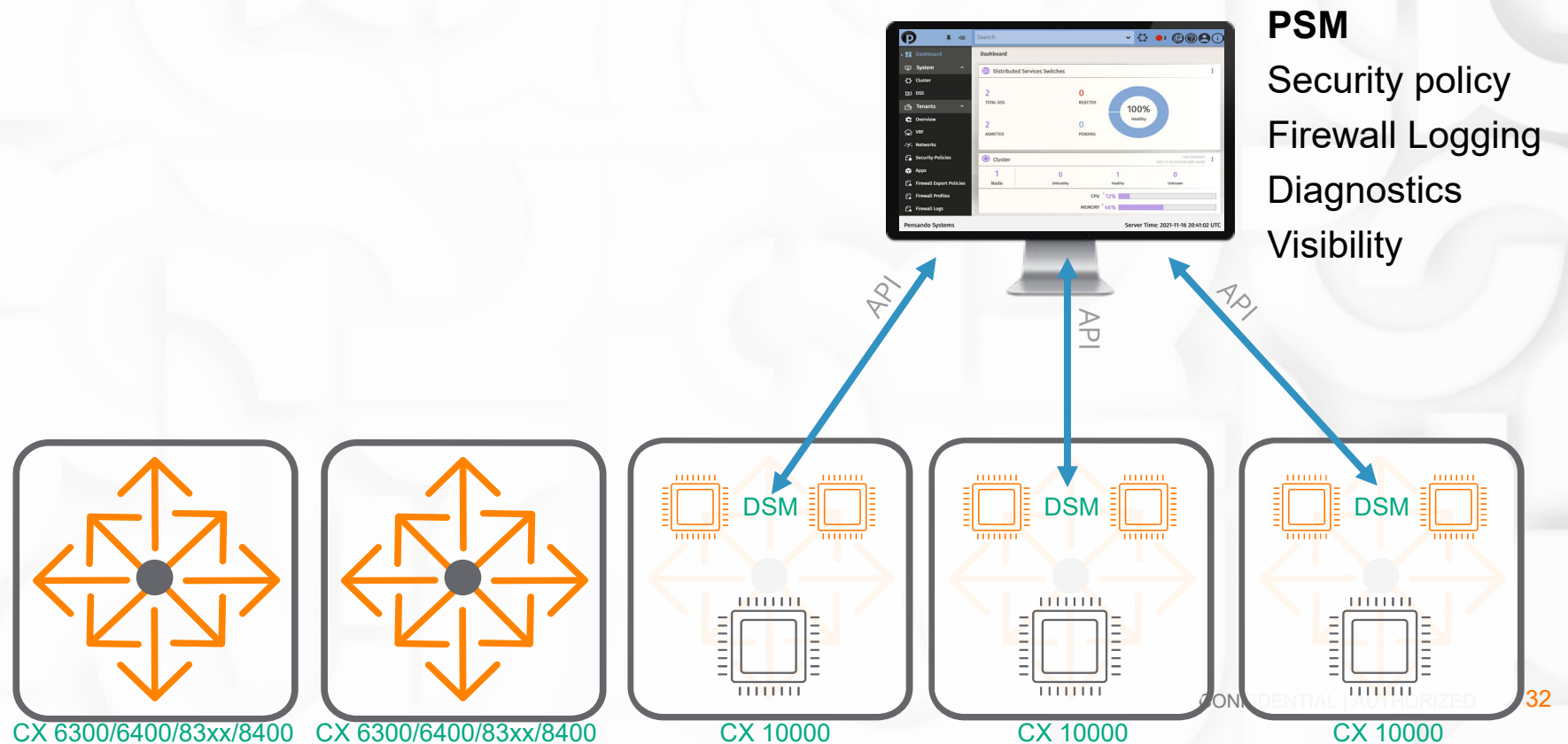
- Form-Factor Agnostic
- Designed for Security
- Low Power/Latency/Jitter
- High Bandwidth & Scale

Pensando Distributed Services Manager 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

Orchestration and management

Pensando Services Manager provides policy enforcement, firewall logging, diagnostics and visibility for the DSM's
Pensando Services Manager does not provide fabric and switch orchestration and management



Orchestration and management

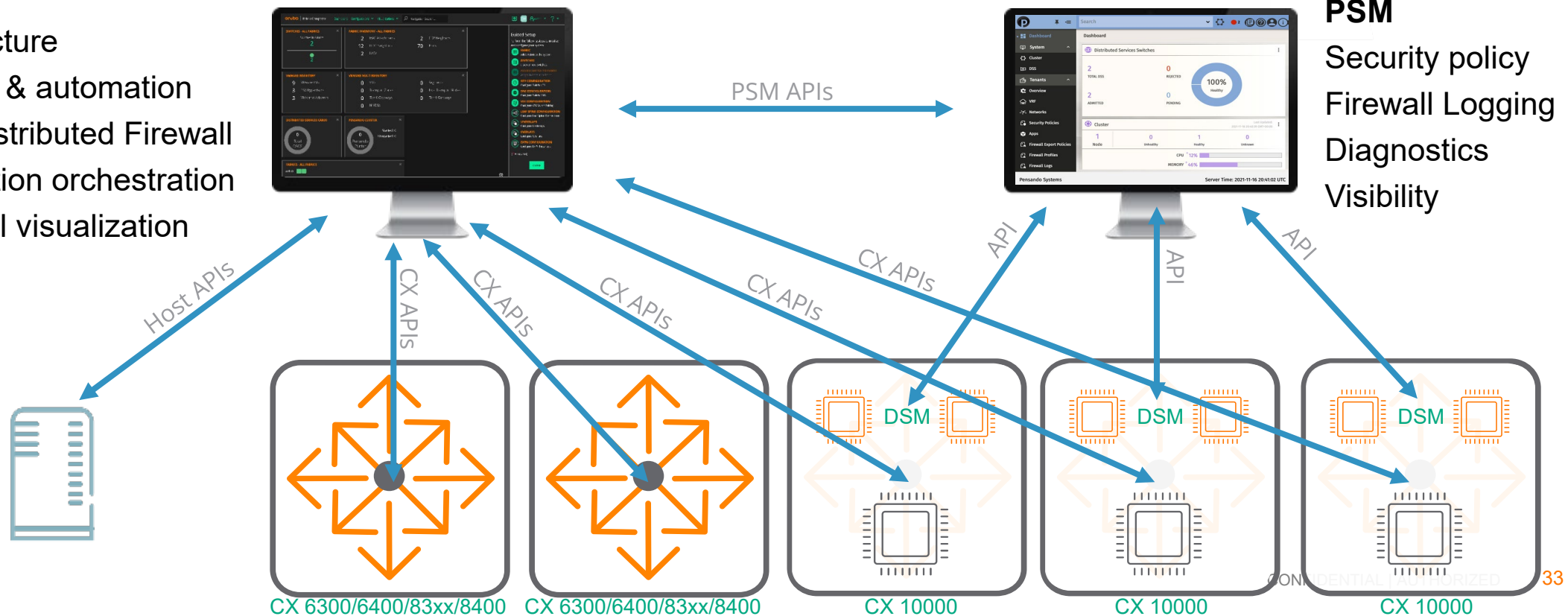
Aruba Fabric Composer provides datacenter orchestration, configuration and management for CX switches
Aruba Fabric Composer allows for security policy management by means of PSM API exchange between AFC and PSM
Aruba Fabric Composer has tight integrations with many third-party solutions (vSphere, Nutanix, Simplivity, iLO, etc)

AFC

Unified infrastructure
Fabric discovery & automation
Policy – ACL, Distributed Firewall
Micro segmentation orchestration
Physical & virtual visualization

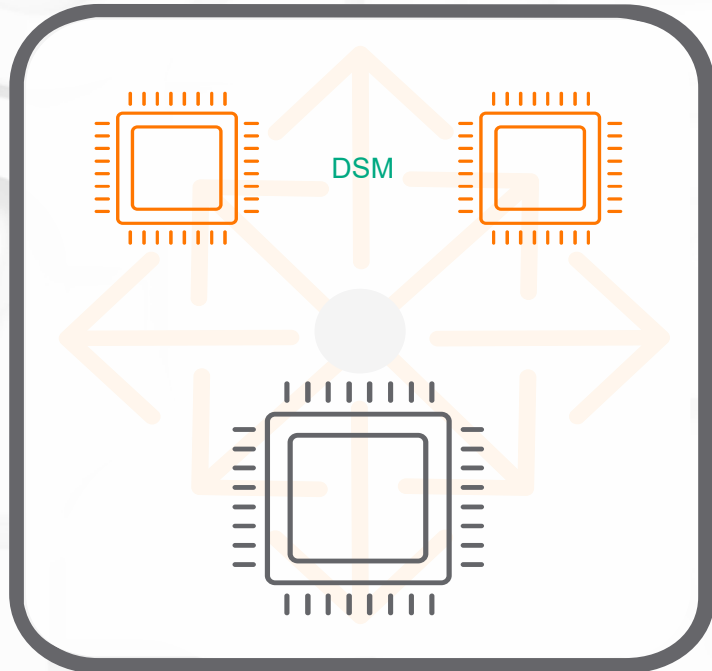
PSM

Security policy
Firewall Logging
Diagnostics
Visibility



Visibility

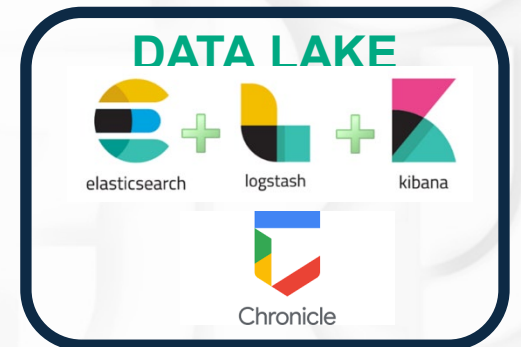
From Operational Visibility to Observability



DSM

NON-SAMPLED

SYSLOG
IPFIX



atmosphere'22

BELGIUM

Thank you

dik.van.oeveren@hpe.com