

Hewlett Packard
Enterprise

HPE **aruba**
networking

Aruba CX 10000

Firewall mit Switch oder Switch mit Firewall?



Max Schmidt - Systems Engineer, AMD

AMD
PENSANDO

Disclaimer and Attributions

The information contained herein is for informational purposes only and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale. GD-18

©2023 Advanced Micro Devices, Inc. All rights reserved. AMD, the AMD Arrow logo, AMD Instinct, EPYC, Pensando, Alveo, Versal, Infinity Fabric, ROCm, and combinations thereof are trademarks of Advanced Micro Devices, Inc. PCIe is a registered trademark of PCI-SIG Corporation. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

How to explain what the CX10k is

Stateful Services for Switched and Routed Network Traffic

It's a duck



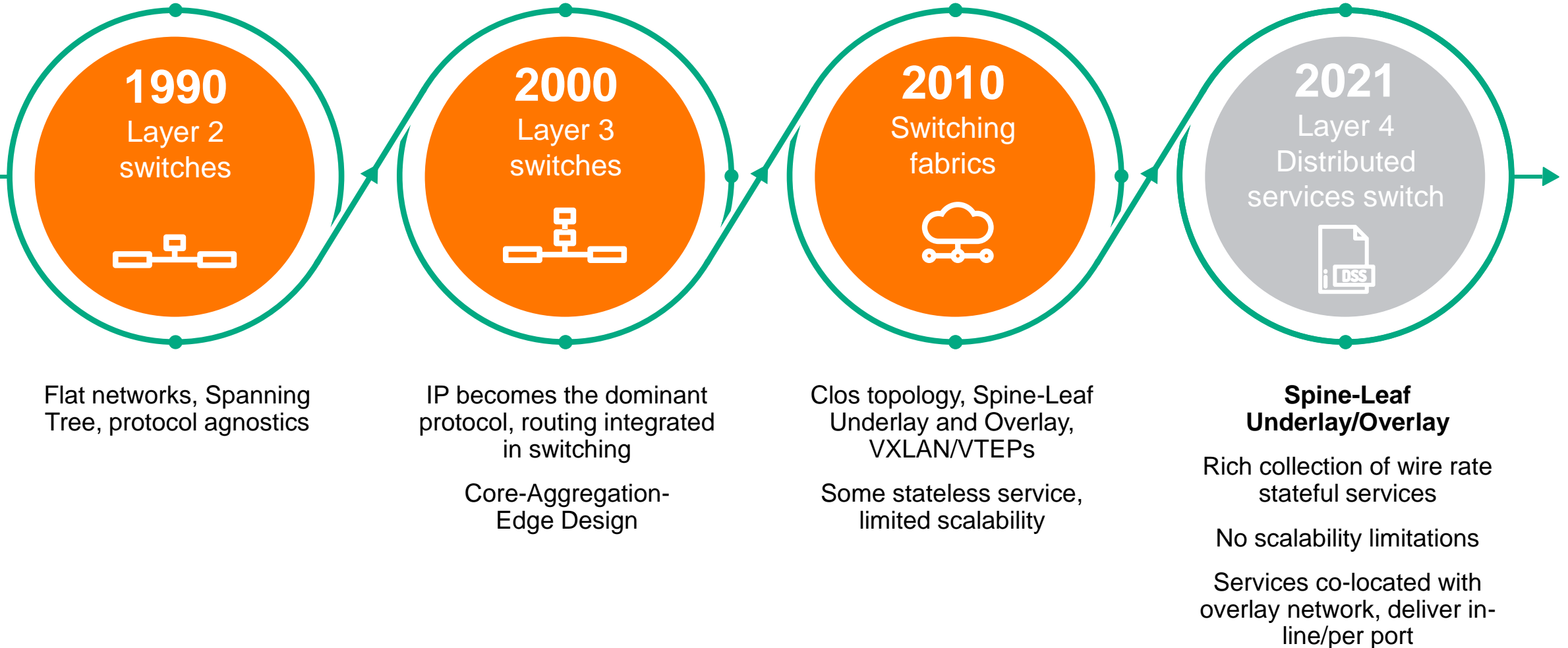
It's a rabbit

It's a Switch with a
built-in Firewall



It's a Firewall with a
built-in Switch

NEXT GEN HIGH PERFORMANCE DATA CENTER FABRICS



Stateful Fabrics with Aruba CX10000

Distributed Services Switch: L2/L3/L4

1. **Seamless Integration/Migration in L2/L3 Mode**
2. **Security build into the Fabric – simple, lower cost Segmentation & Encryption**
3. **Full Visibility, know what's going on**
4. **Higher Degree of Network Automation**

The diagram illustrates the Aruba CX Routing and Switching architecture. At the top, an orange banner reads "ARUBA CX ROUTING AND SWITCHING". Below this, a grey box titled "L4-L7 Stateful Software Services" contains five icons representing different services: E-W FIREWALL (a shield with a flame), DDoS (a document with a red 'X'), ENCRYPTION (a padlock), NAT (two arrows pointing in opposite directions), and TELEMETRY (a network diagram with a signal icon). To the right of the diagram is a photograph of the physical Aruba CX switch, a black rack-mountable device with multiple ports. Above the switch is the "HPE aruba networking" logo, with "Powered by AMD PENSANDO" written below it.

Unified services switching platform
Broadcom T3, with 2 Pensando DPU (7nm)

Aruba AOS-CX and Orchestration (AFC)
Full protocol stack, centrally managed at scale

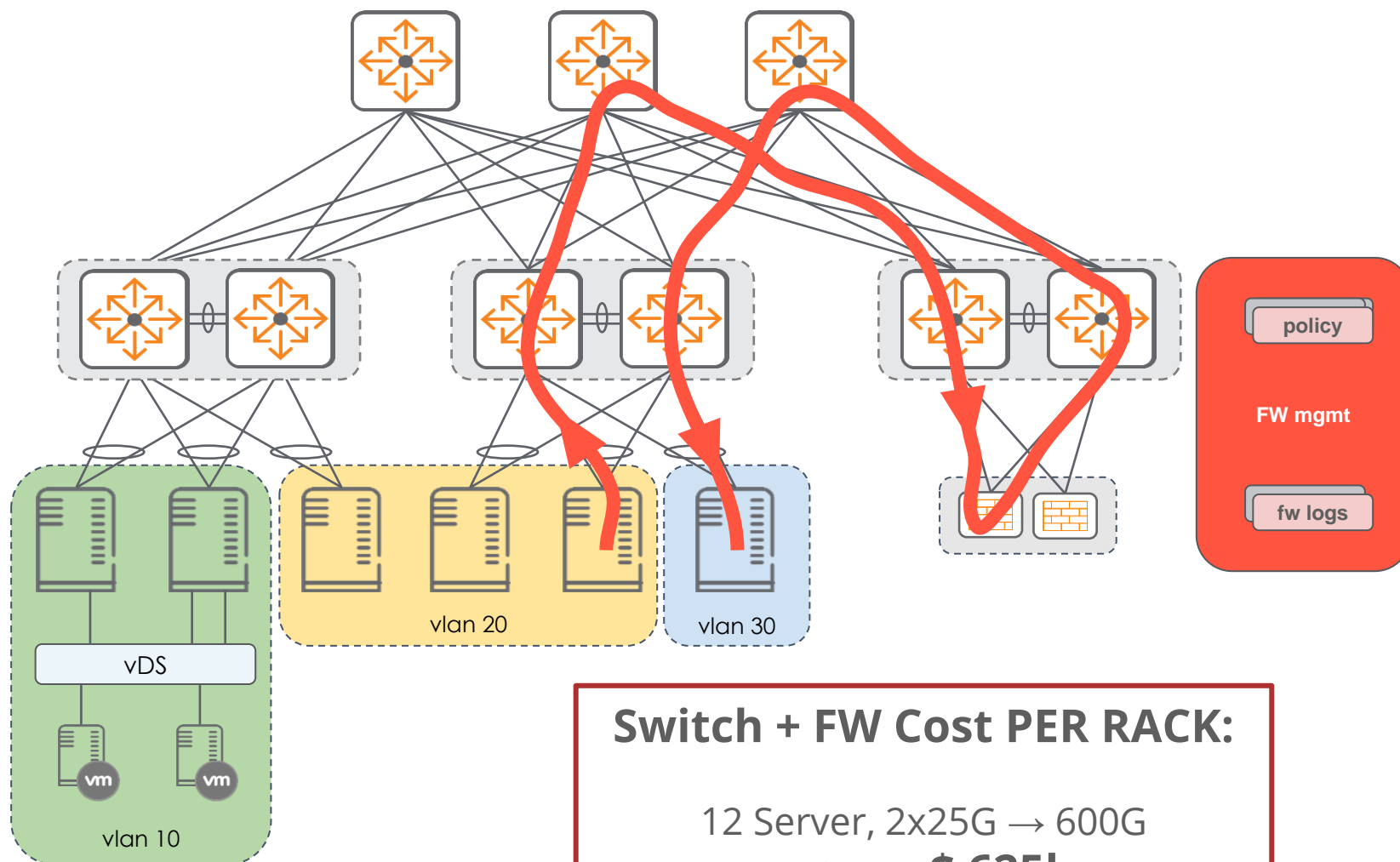
Services with Scale and Performance
Stateful firewall, DDoS, encryption, NAT

Orders of magnitude (100x) policy scale
beyond traditional switch platforms

**100x Scale, 10x Performance,
35% of TCO**

Current Data Center (Micro)-Segmentation Challenges

Centralized Services Architecture



Switch + FW Cost PER RACK:

12 Server, 2x25G → 600G
= appr \$ 625k
 (2x \$300k FW + 2x \$12k ToR)

Centralized Stateful Firewall Services

- managed from a **single Management Instance**
- provide seamless failover
- **collects firewall logs**

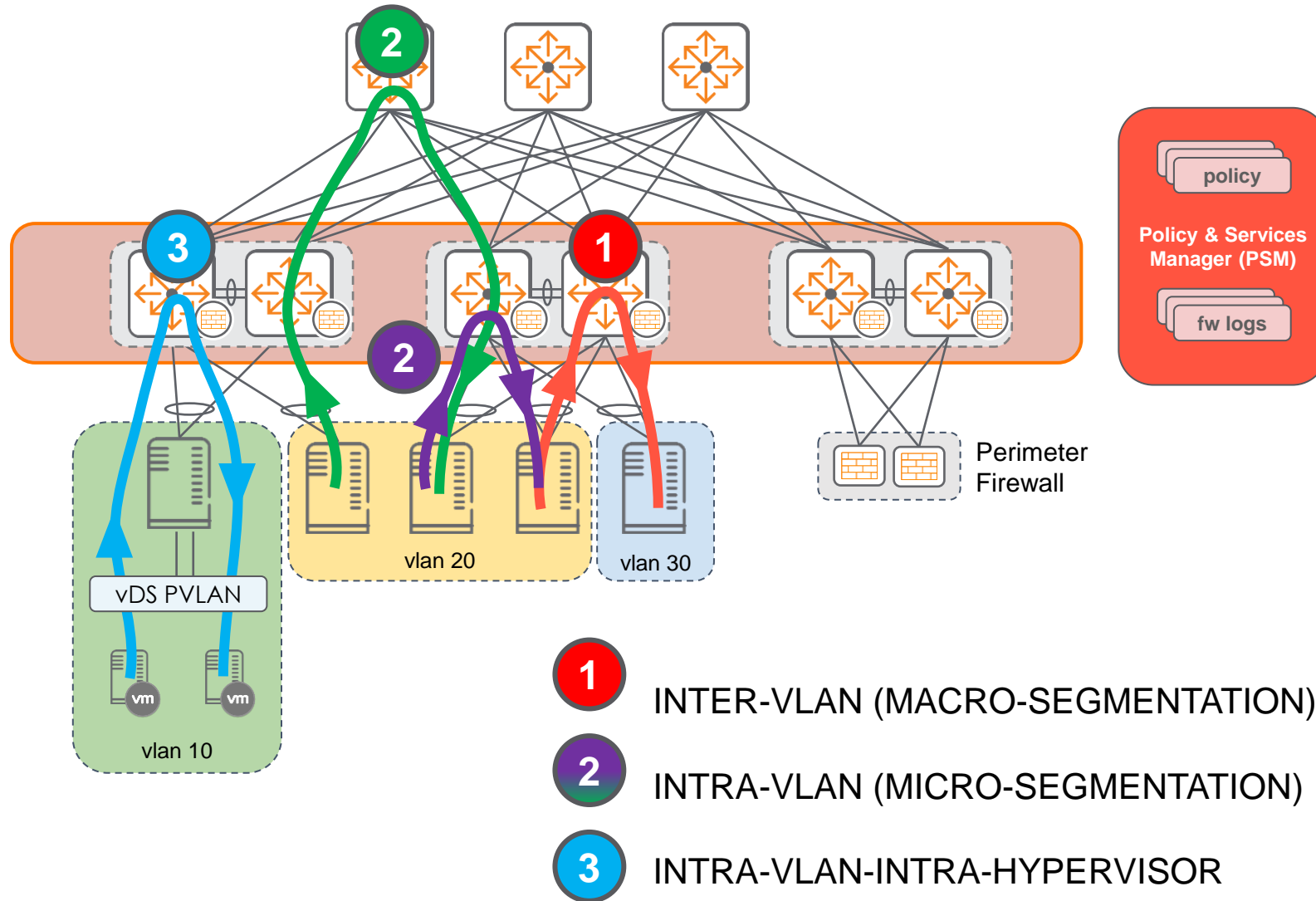
Requires a Network Design that supports the functionality

- Firewall provide Default Gateway functionality on the Network to **route the traffic through the Firewall**
- **IP Addressing Scheme** needs to reflect the separation for the stateful policy enforcement
- Application Tiers **stretch multiple Firewalling Zones**

Redirect to Firewall

- Increases **Latency**
- Consumes Network **Bandwidth**
- Adds **Complexity**

Distributed Services Architecture



Distributed Stateful Services

- are provided in path, **without redirection** to a centralized appliance
- Programmable ASICs provide **hardware offloading** capabilities AND flexibility for different Use Cases

The Policy & Services Manager (PSM)

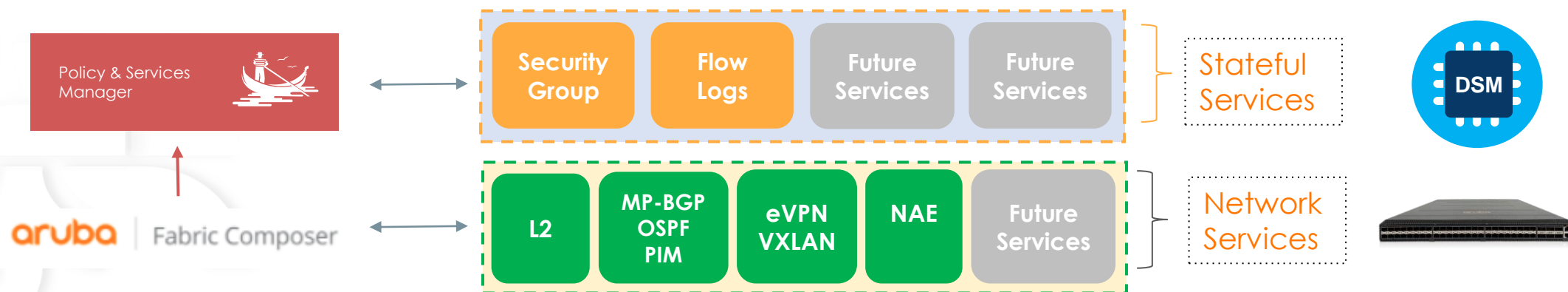
- provides **centralized management** of policies and services
- **distributes the configuration** to all stateful services switches
- **collects fw logs**, alarms, telemetry and statistics
- **integrates in Ecosystems**

CX10K Architecture



CX 10000 Architecture Overview

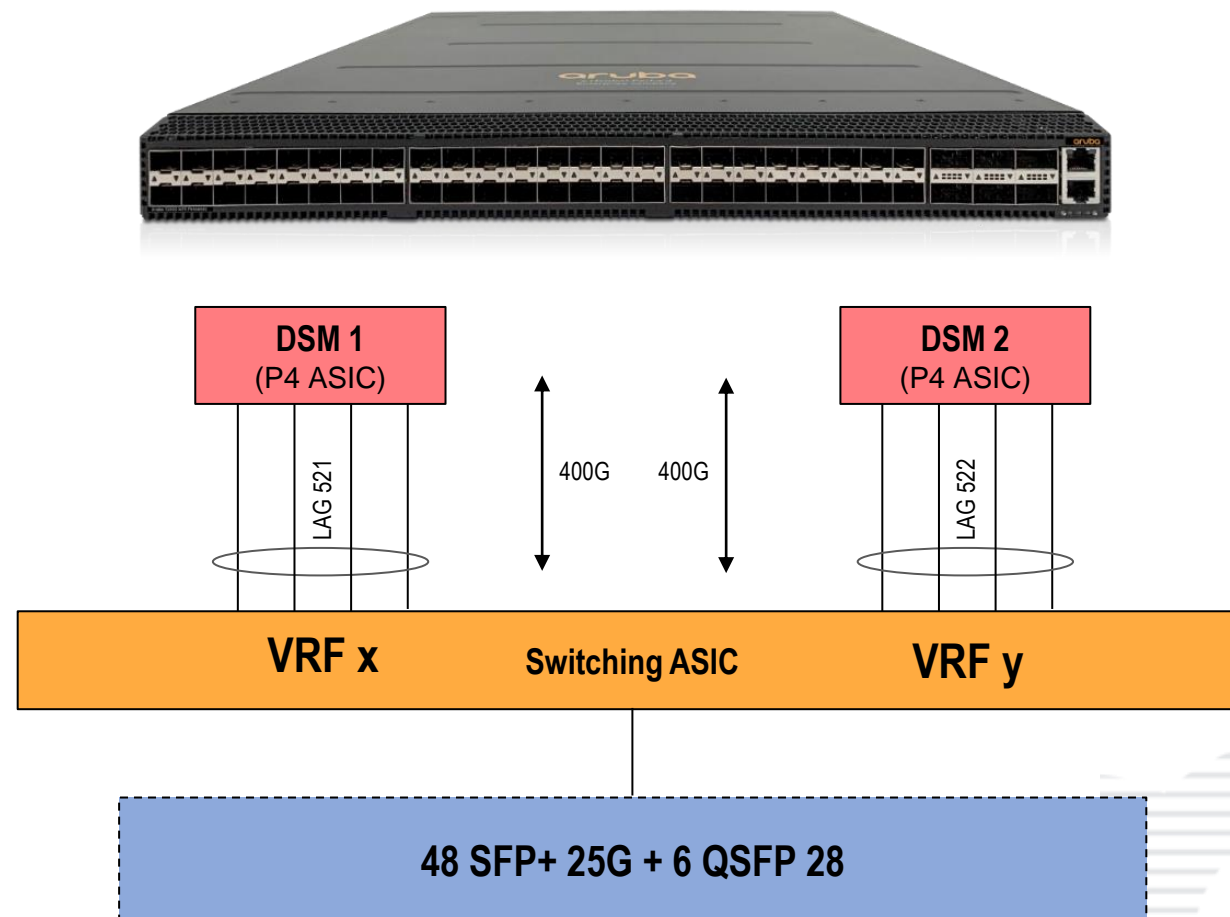
- L2/L3 Networking including Underlay/Overlay configured via AOS-CX CLI, REST API, AFC or Python.
 - All L2/L3 Networking features are performed by Trident 3 ASIC.
- Stateful features including Stateful L4 Firewall, Flow Logs configured via PSM GUI, PSM API, PSM Python or AFC (with PSM integration)
 - Traffic is not redirected for Stateful Evaluation unless the configuration is present on PSM, and VLAN/VRF exists in AOS-CX.
 - Stateful features cannot be configured from AOS-CX CLI.



Distributed Services Switch – High-Level Architecture

Each DSM has 400G connection to TD3

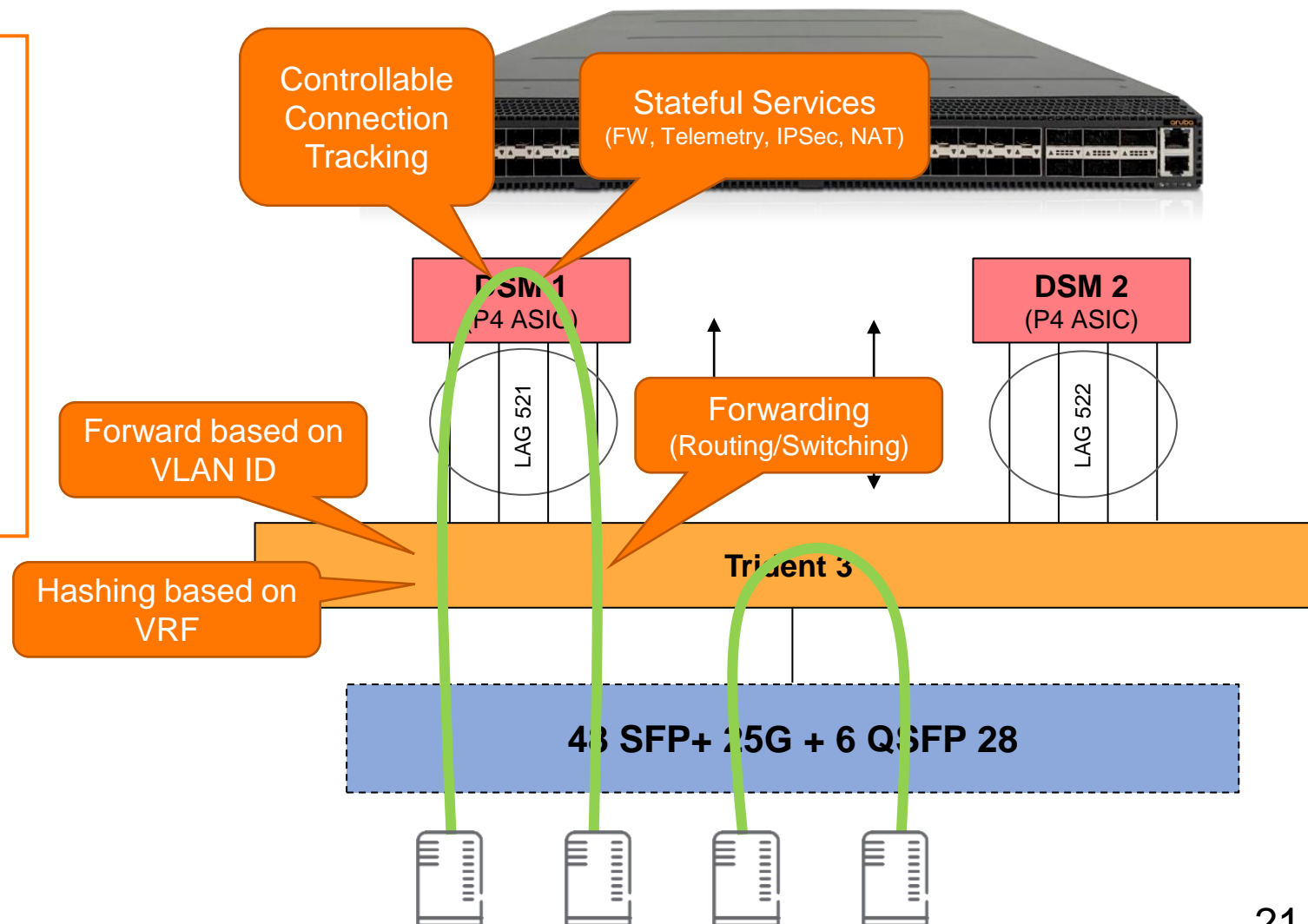
- These are 4x100G links, part of internal LAG 521 and 522.
- Hashing algorithm uses L3/L4 information to LB packets on internal links.
- Internal links are not visible in regular CX-OS commands.



Distributed Services Switch – High-Level Architecture

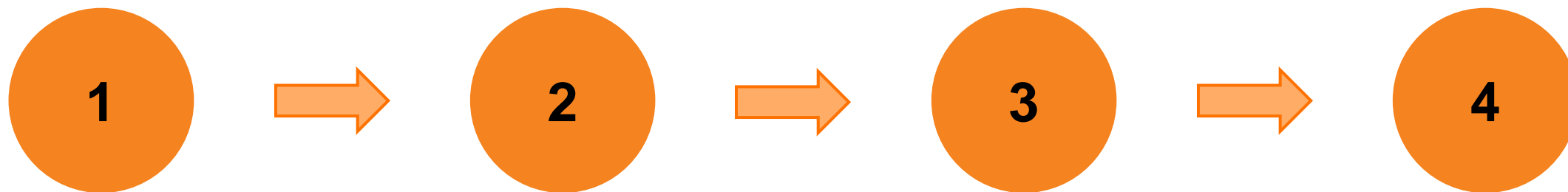
Each DSM has 400G connection to TD3

- These are 4x100G links, part of internal LAG 521 and 522.
- Hashing algorithm uses L3/L4 information to LB packets on internal links.
- Internal links are not visible in regular CX-OS commands.



Migration Path

Step-by-Step to a more secure DC environment



Network Lifecycle

Replace existing network
or
enhance existing network

Leverage DSM for Visibility

Leverage the Visibility for Policy
Creation and Troubleshooting

Introduce Macro Segmentation

Enable the created Policy,
leverage FW logging
capabilities for compliance

Introduce Micro Segmentation

Move from Macro
Segmentation to Micro
Segmentation

Demo



Use Cases

Configurations & how customers will deploy the CX10K in their networks

1



VXLAN Leaf

CX10000 with Active Gateway as a Leaf in a VXLAN fabric

- **VXLAN EVPN Fabric**
 - **Server Leaf**
 - **Border Leaf/Gateway**

2



Layer 3 Switch

Switch is configured as Default Gateway for local attached Servers

- **L3 Fabrics**
- **Collapsed Core (for Servers)**
- **Remote Data Room**

3



Layer 2 Switch

CX10000 for L2 VLANs Gateway is on Core or central Firewall

- **2-/3-Tier DC Network**
- **Sub-Leaf/Secure Interconnect**

Configurations & how customers will deploy the CX10K in their networks

4



IPSec* / NAT*

Switch is configured as Edge Gateway for IPSec and / or NAT

- **IPSec Gateway/Aggregation**
- **Data Center Interconnect**
- **Various NAT Scenarios**

***Requires Premium license**



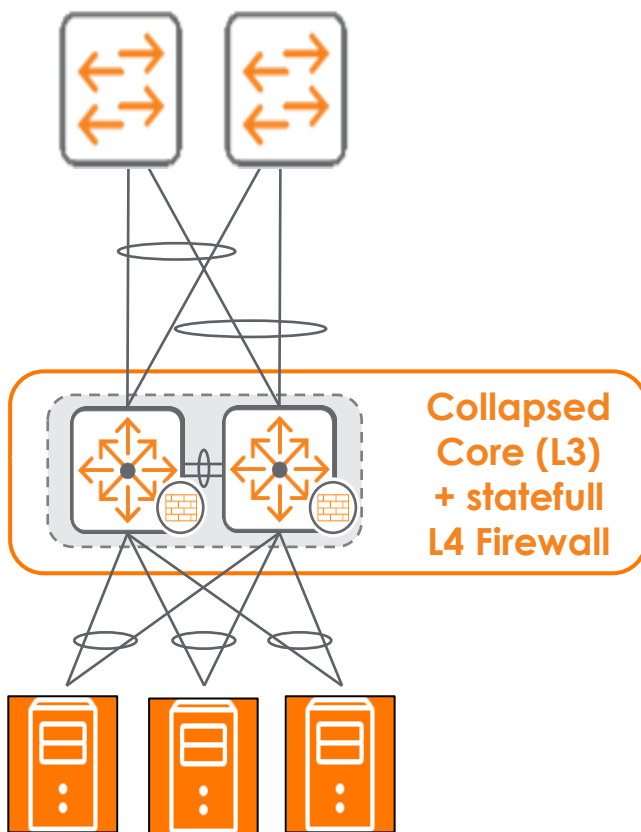
Customer Examples

MANUFACTURING CUSTOMER

IT/OT Segmentation

Outline

- HQ'd in Germany
- 50 Production Facilities globally (Europe, America, APJ, China)
- 11.000 Employees
- \$1.8Bn annual Revenue
- Network and Security Redesign
- SDWAN and SASE Readiness
- IT/OT Segmentation

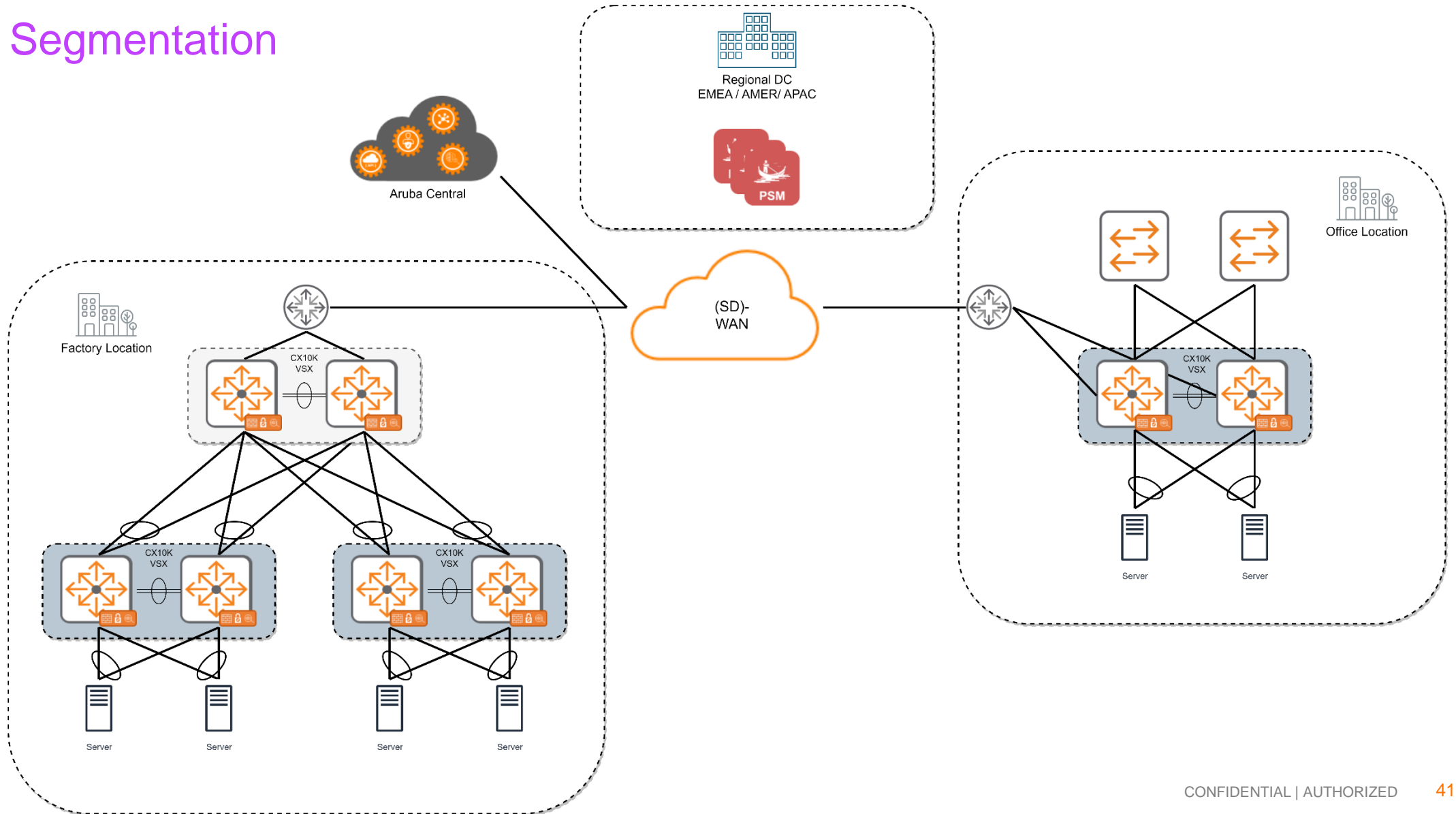


Business Outcome

- Reduced internal Firewalls at all sites.
- Dramatic Capex reduction
- Reduced Security Opex
- True Micro-Segmentation
- Visibility
- Simplified the architecture

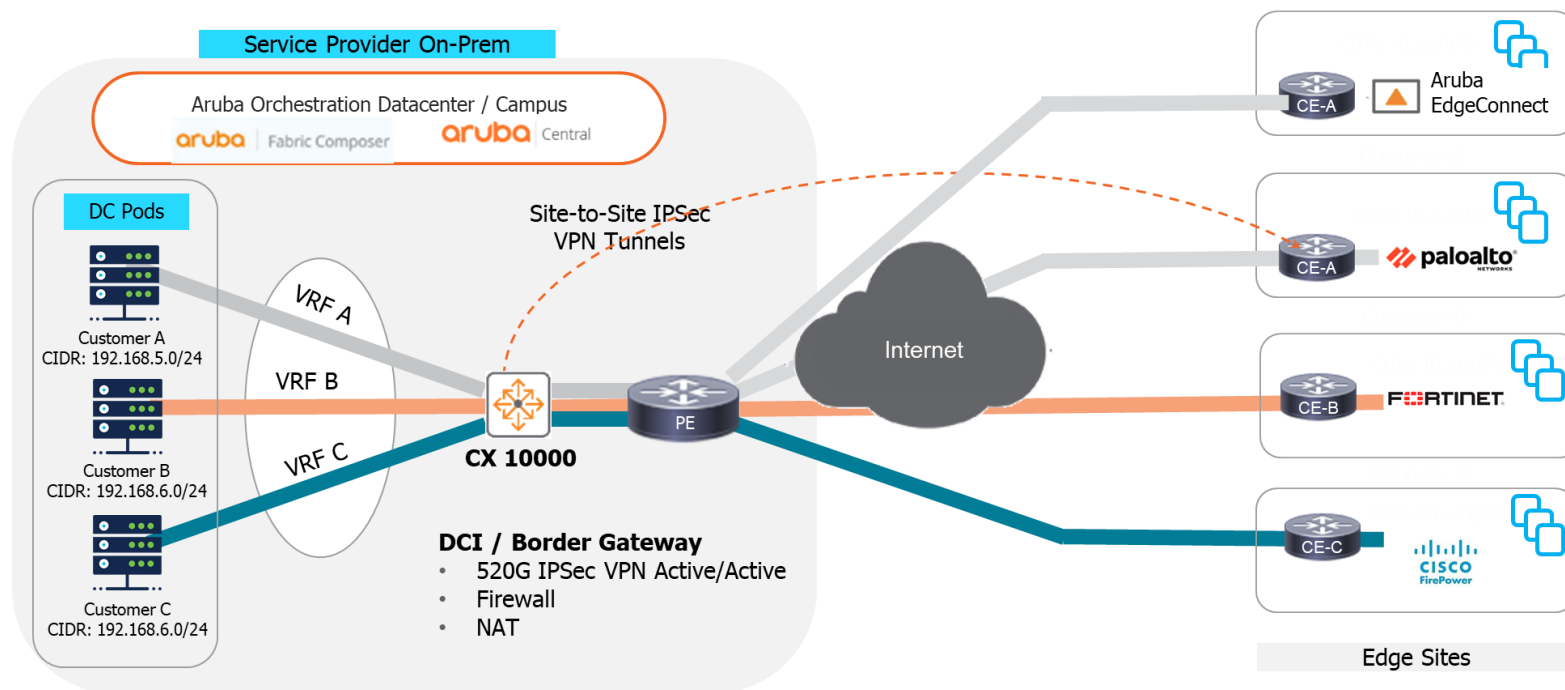
MANUFACTURING CUSTOMER cont.

IT/OT Segmentation



DXC Network Services

DXC Secure Network Fabric Co-Developed with Hewlett Packard Enterprise and AMD



Business Outcome

- Up to 30% reduction in DC Connectivity Cost
- >60% in time reduction in time to onboard/migrate customer workloads
- >70% increase in workload security posture within DC
- Up to 30% increase in telemetry Data visibility with >50% reduced efforts
- Up to 83% reduction in DC Network Security Infrastructure footprint



Thank You!