

Hewlett Packard
Enterprise

Security-first AI-powered Networking Company

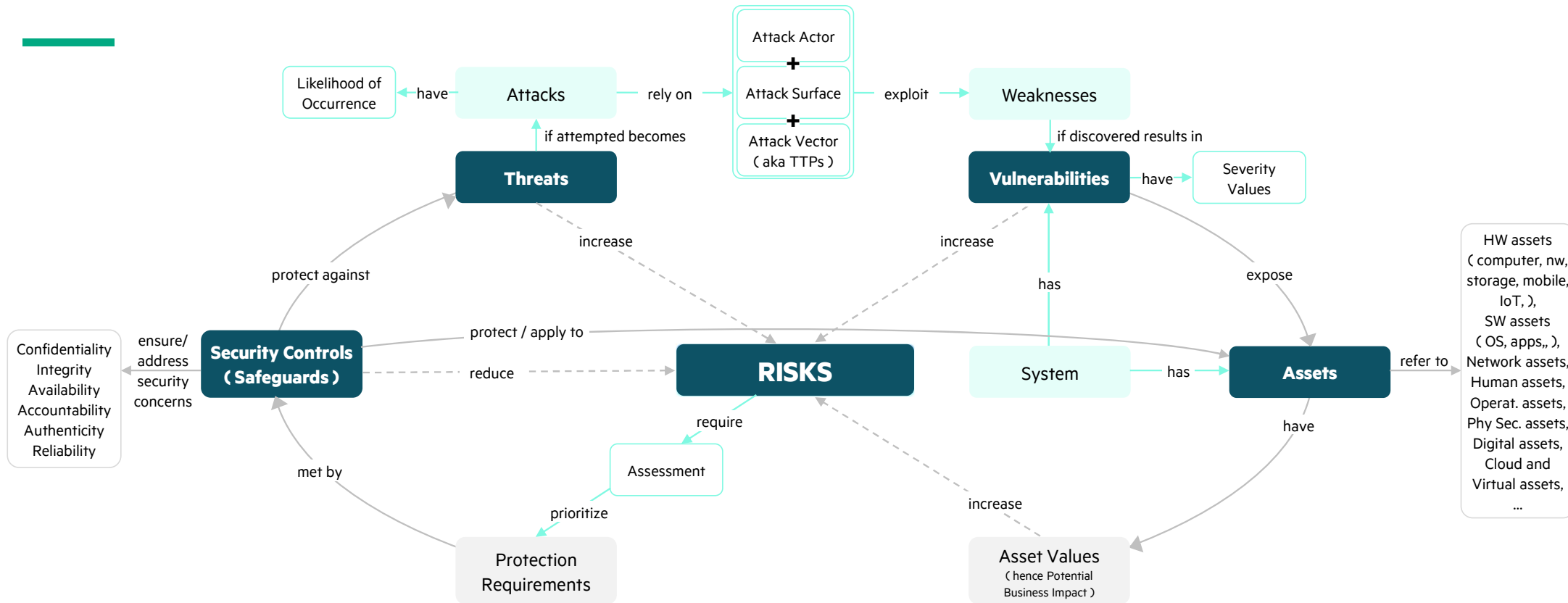
Edge

Paulo Rio

Network and Security Consultant

January 30th, 2025

Security is about Risk ^[2]



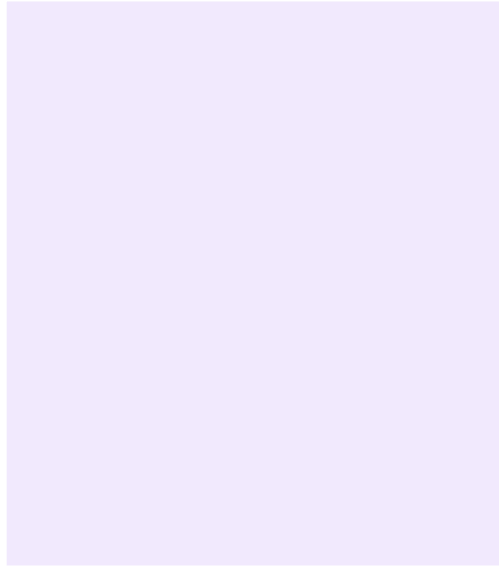
Impact / Consequences of an Attack

RISK = Likelihood of an Attack * Value of the Asset * Severity of the Vulnerability

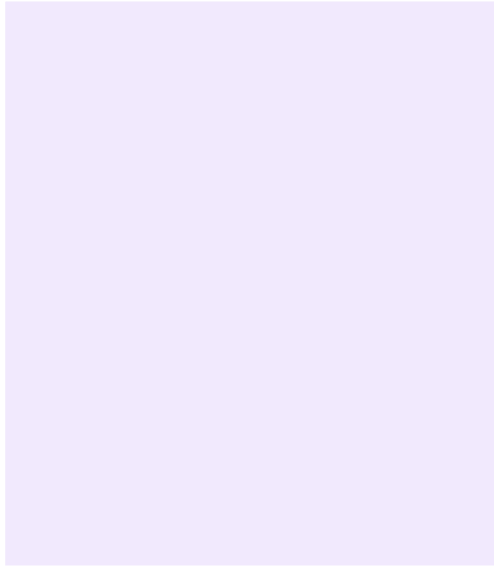
Source: ISO/IEC TR 13335-1:1996

HB231:2000 Information Security Risk Management Guidelines, Standards Australia

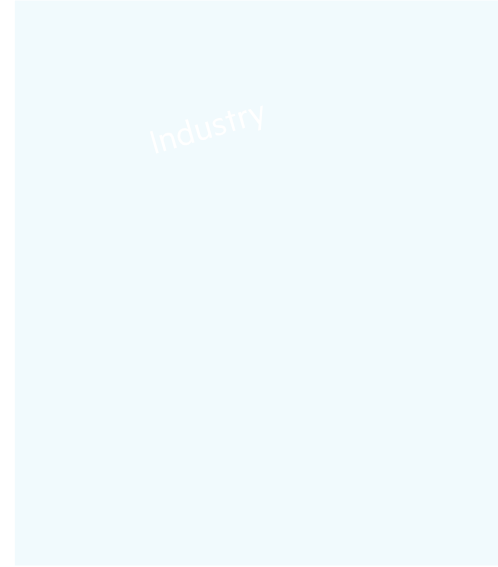
Who said this ?



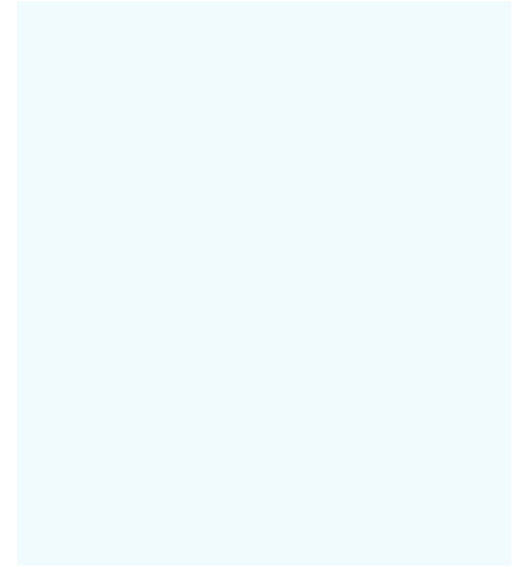
“Trust but Verify”



**“The reward of a thing well
done is to have done it”**



“Trust and don’t Verify”



**“Never Trust,
Always Verify”**



In the past it was **“Trust but Verify”**... In IT it was “Trust and don’t Verify” !!!
_____ now we have **“Never trust, always verify”** i.e. Zero Trust Strategy



“Trust but Verify”

Ronald Reagan
(*“doveryáy, no proveryáy”*)

Intermediate-Range Nuclear Forces Treaty, on 8 December 1987



“The reward of a thing well done is to have done it”

Mikail Gorbachev
(Ralph Waldo Emerson)

https://en.wikipedia.org/wiki/Trust,_but_verify



“Trust and don’t Verify”

The entire industry !...

The perimeter-based approach

<https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security>



**“Never Trust,
Always Verify”**

John Kindervag, Forrester
(Zero Trust Strategy)

The ZT NW Arch, on 11 Nov 2010

What is Zero Trust ?

Principle: **Never Trust, Always Verify**
(No device, user or network segment is inherently trustworthy and thus should be treated as a potential threat).

3 core requirements:

Identity & Authentication

Restricted Access

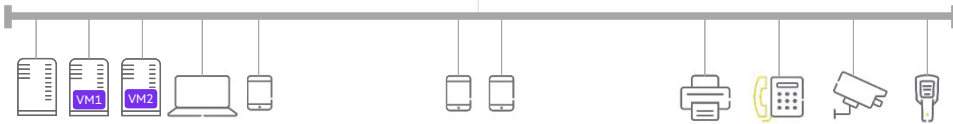
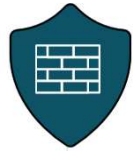
Continual Adaptive Access

Why Design For Zero Trust?

- 1 Takes a more holistic approach
- 2 Design for internal and external threats
- 3 Not reliant on traditional perimeter security
- 4 Limits exposure to vulnerable devices
- 5 Limits network access to 'least privilege'

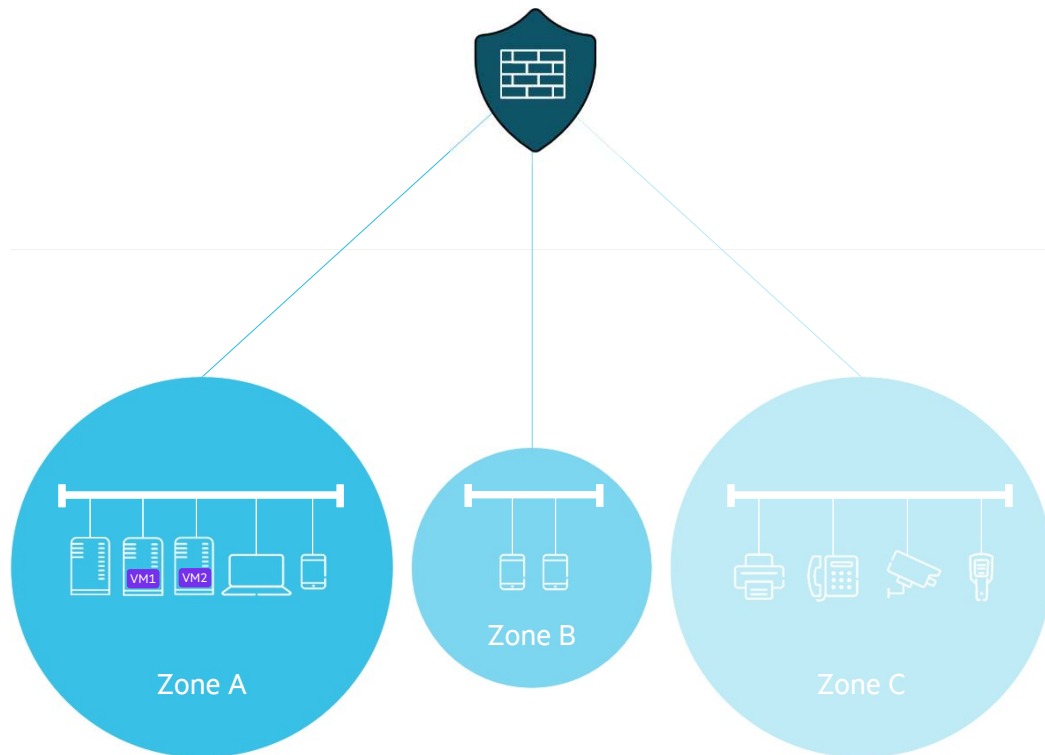
Macro vs Micro-segmentation

No segmentation



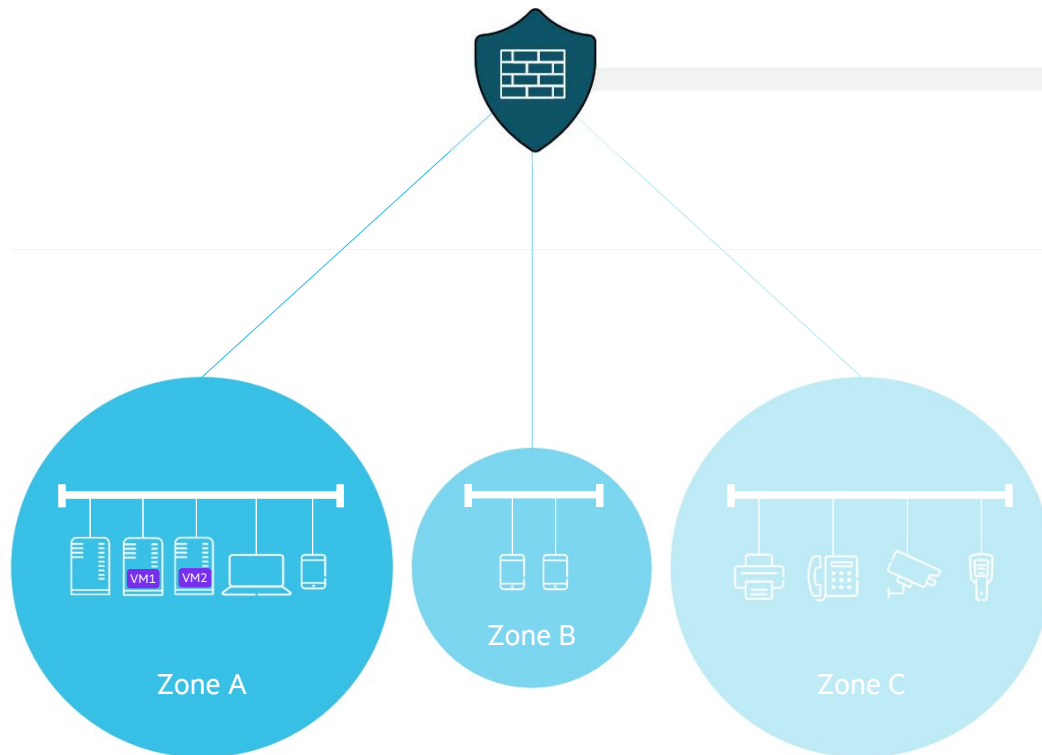
Macro vs Micro-segmentation

Macro-segmentation

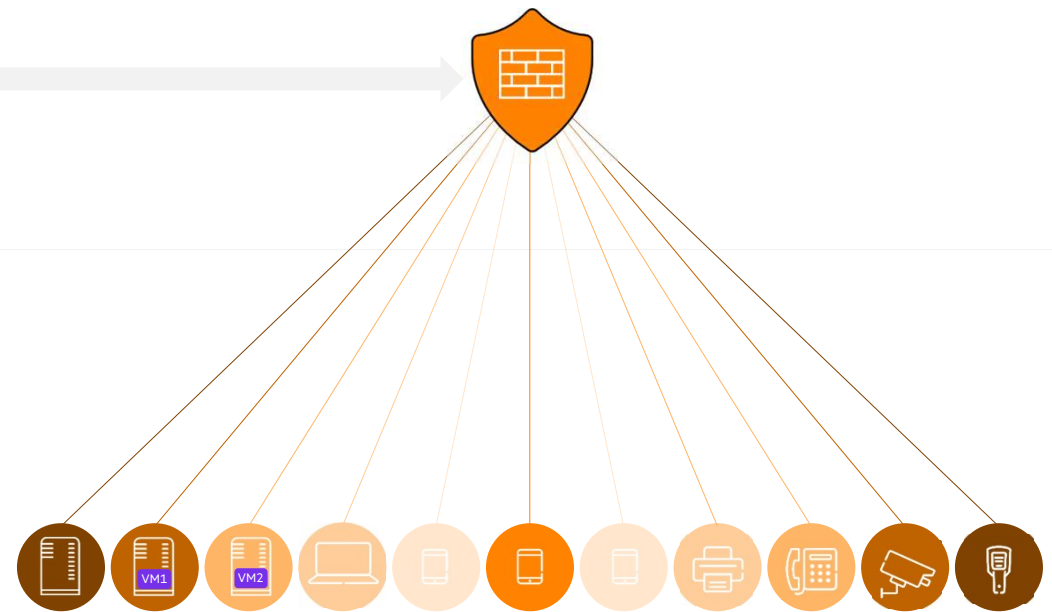


Macro vs Micro-segmentation

Macro-segmentation

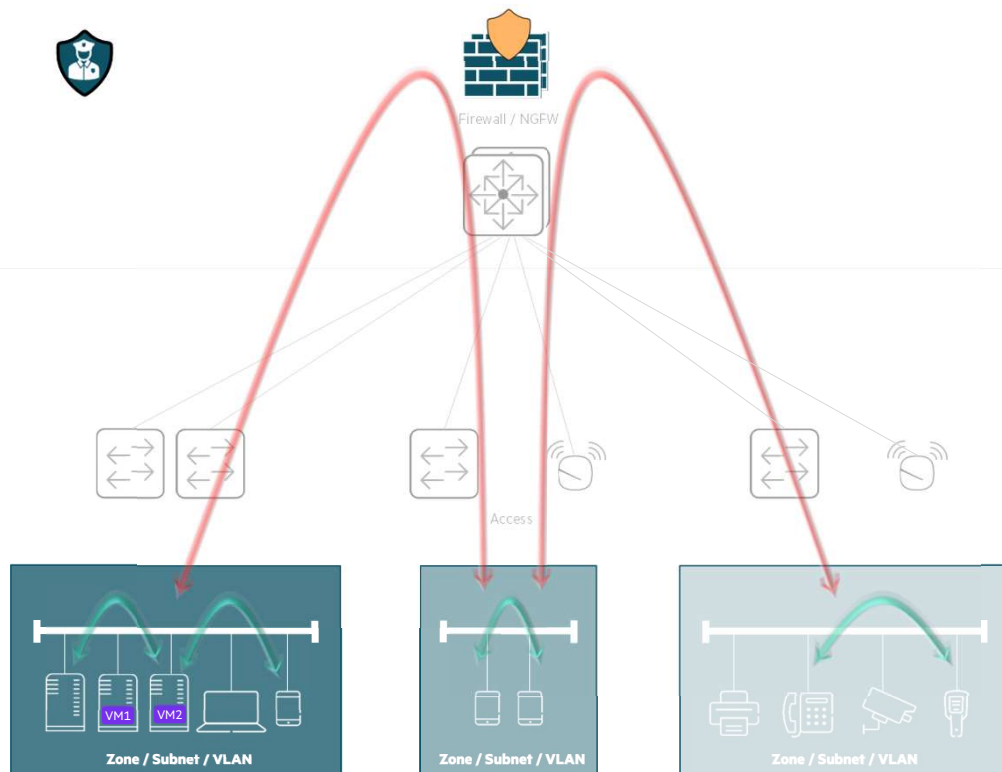


Micro-segmentation

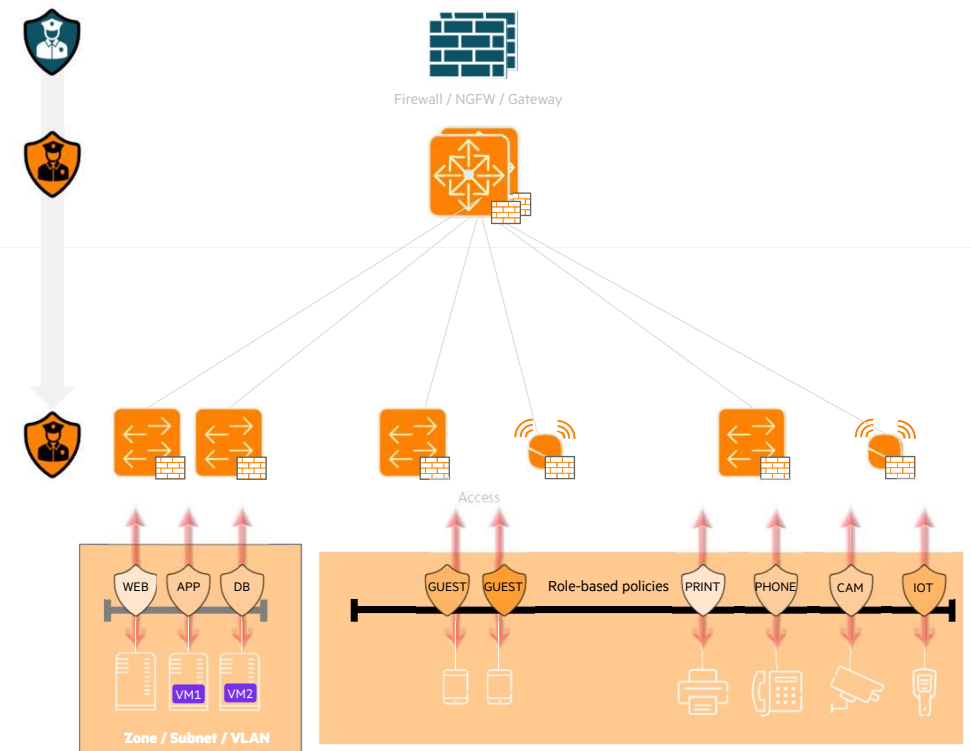


Macro vs Micro-segmentation

Macro-segmentation



Micro-segmentation



↓ Attack Surfaces

↓ Lateral Movement

↑ Threat Protection

EU NIS2 Directive - security of (N)etwork and (I)nformation (S)ystems

Article 21 Cybersecurity risk-management measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

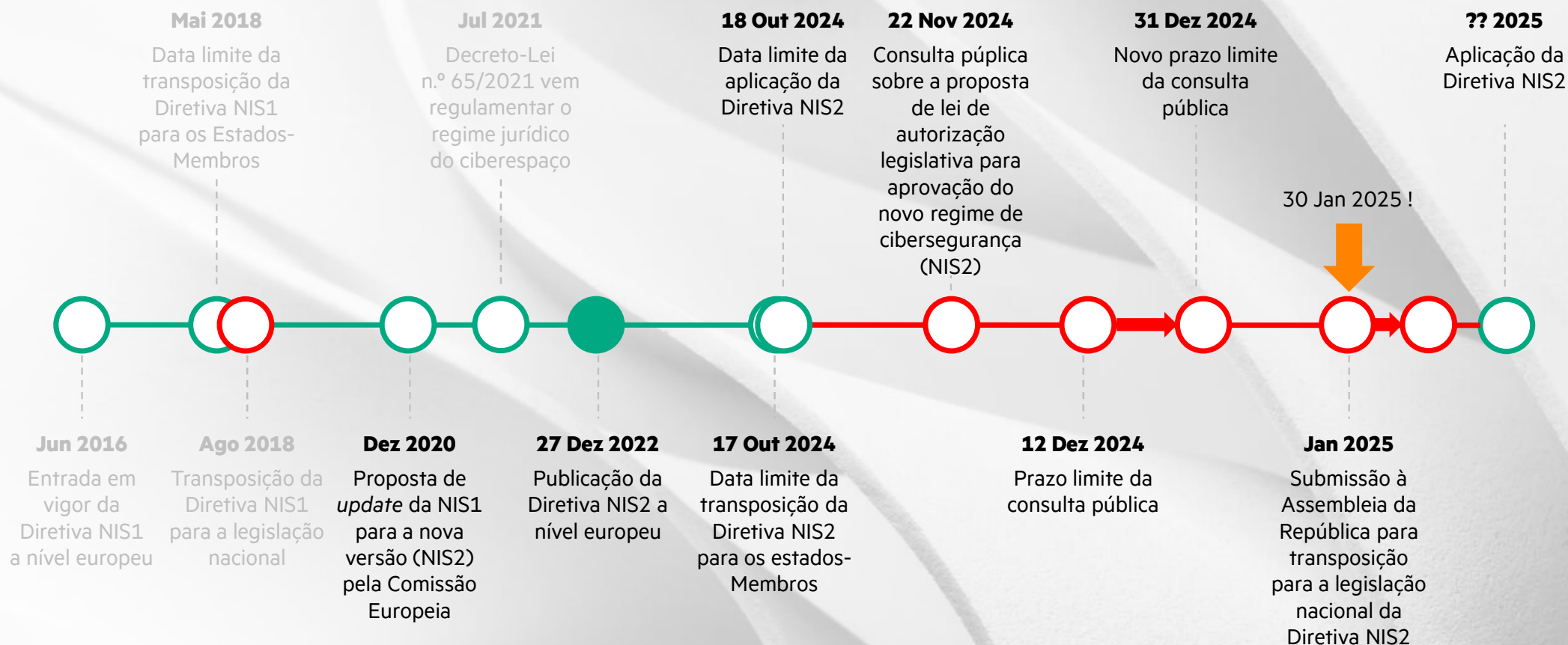
- (a) policies on risk analysis and information system security;
- (b) incident handling;
- (c) business continuity, such as backup management and disaster recovery, and crisis management;
- (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- (e) security in network and information systems acquisition, handling and disclosure;
- (f) policies and procedures to assess the effectiveness of cyber security measures;
- (g) basic cyber hygiene practices and cybersecurity training;
- (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- (i) human resources security, access control policies and asset management;
- (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

(89) Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.



Diretiva de Segurança das Redes e da Informação - SRI 2 (NIS2 Directive)

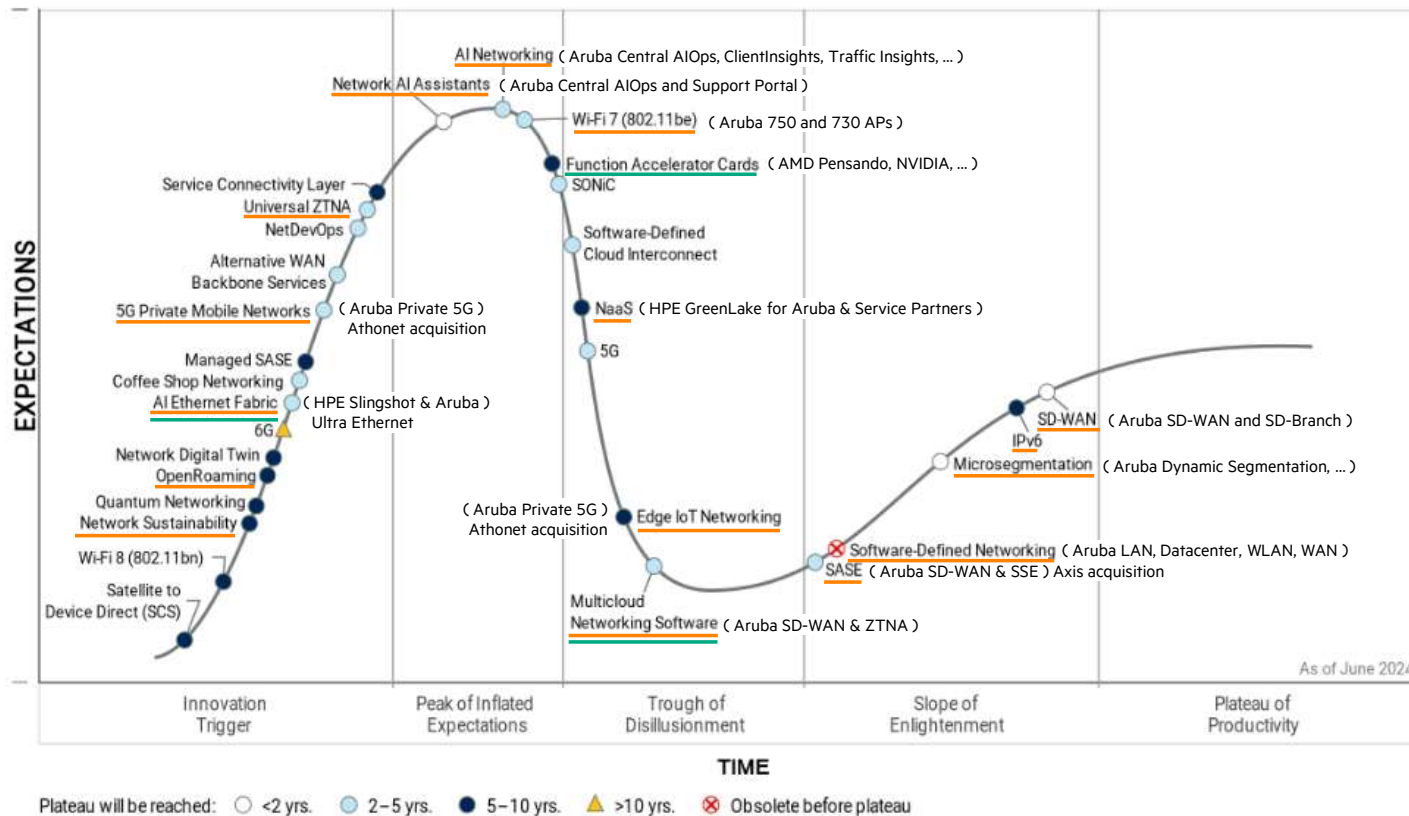
Transposição para a lei portuguesa da Diretiva (UE) 2022/2555 (SRI2)



<https://digital.gov.pt/noticias/novo-regime-juridico-de-ciberseguranca-em-consulta-publica>
<https://www.mgts.pt/pt/conhecimento/legal-alerts/Legal-Alert-Diretiva-SRI2-NIS2/25677/>
https://www.rtp.pt/noticias/economia/consulta-publica-do-novo-regime-de-ciberseguranca-recebe-149-contributos_n1624990

Gartner Hype Cycle Enterprise Networking, 2024

Hype Cycle for Enterprise Networking, 2024

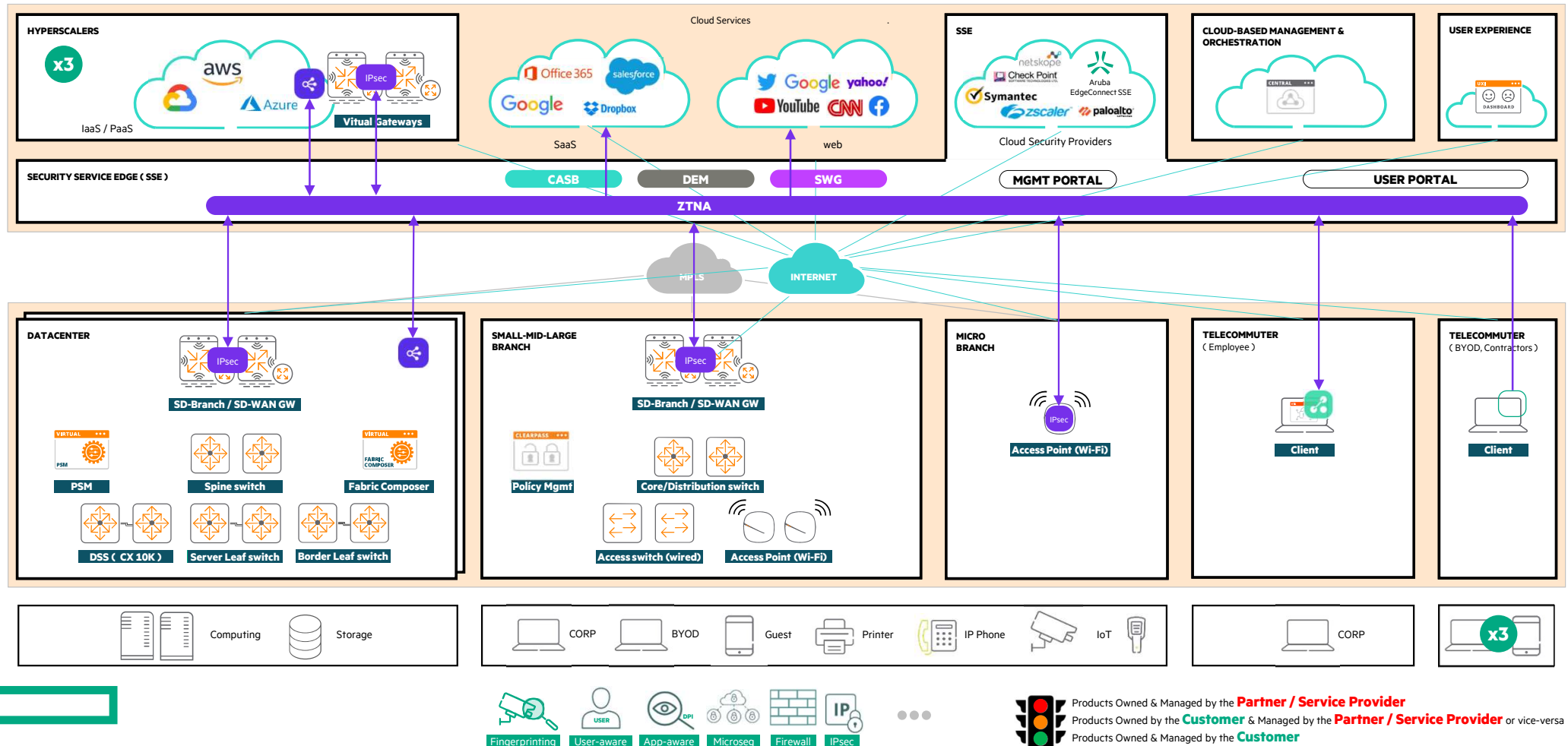


<https://www.gartner.com/en/documents/5500595>

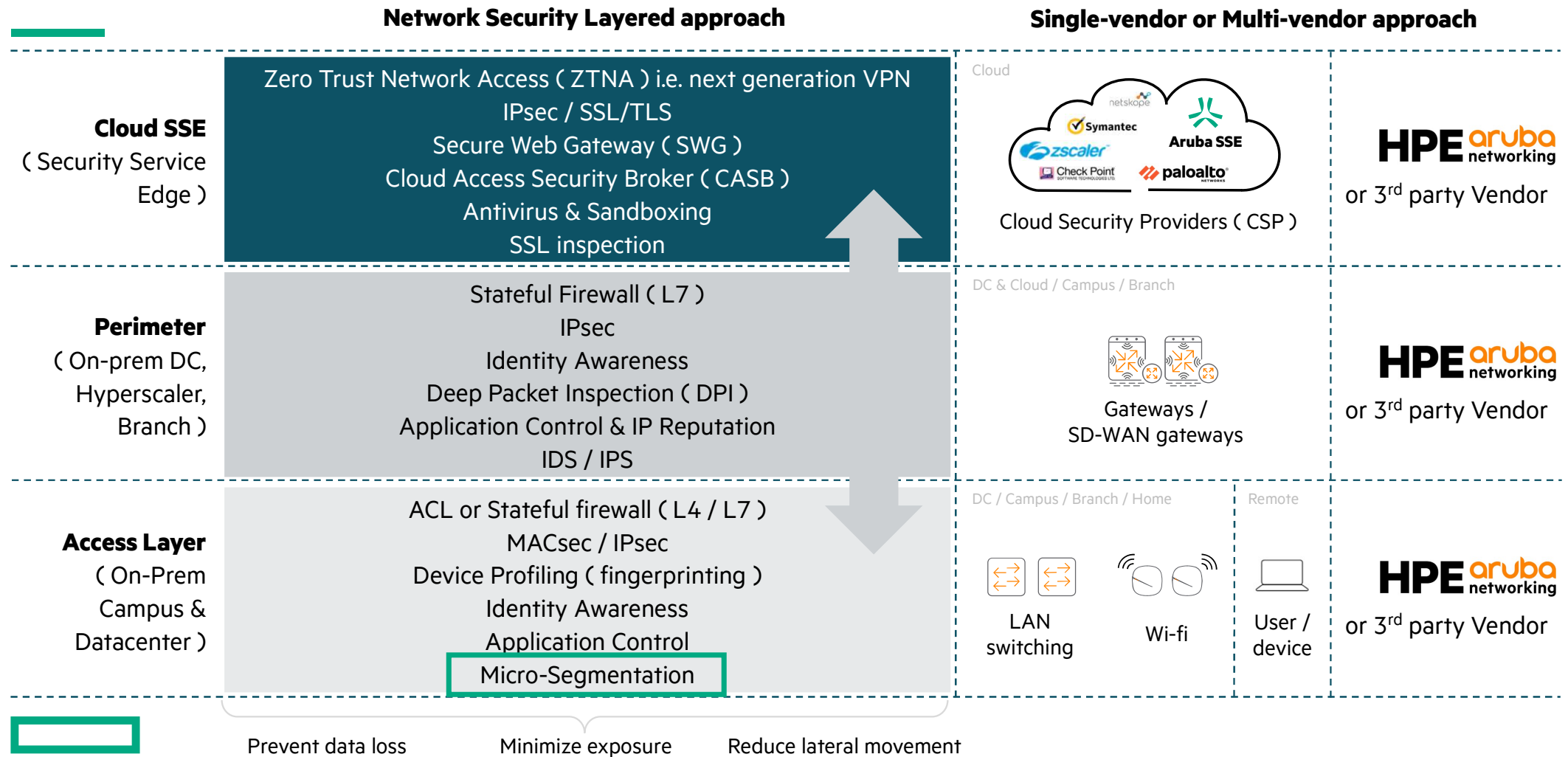
Network Edge Reference Architecture

In the not-too-distant future !...

“Old” Megatrends: Big data, Cloud, Mobility, Security
“New” Megatrends: Hyper-automation, AI, Cybersecurity-Mesh



Zero Trust Security, Architecture Models and Capabilities



Micro-Segmentation in the Campus



Zero Trust Strategy

NIST CSF

Technology Controls

User	Device	Network	Application	Data
Identify	Endpoint	connection	Resource	Information
Identify	Protect	Detect	Respond	Recover
AAA User-aware	Microseg Fingerprint	Firewall / ACL DPI	IPsec Web filtering	Telemetry IDS / IPS

CHALLENGES:

✓ Adopting **IoT**

✓ Adopting **Mobility**

⚠ Innovative **Threats**

PROTECTION GOALS:

↓ Attack Surfaces

↓ Lateral Movement

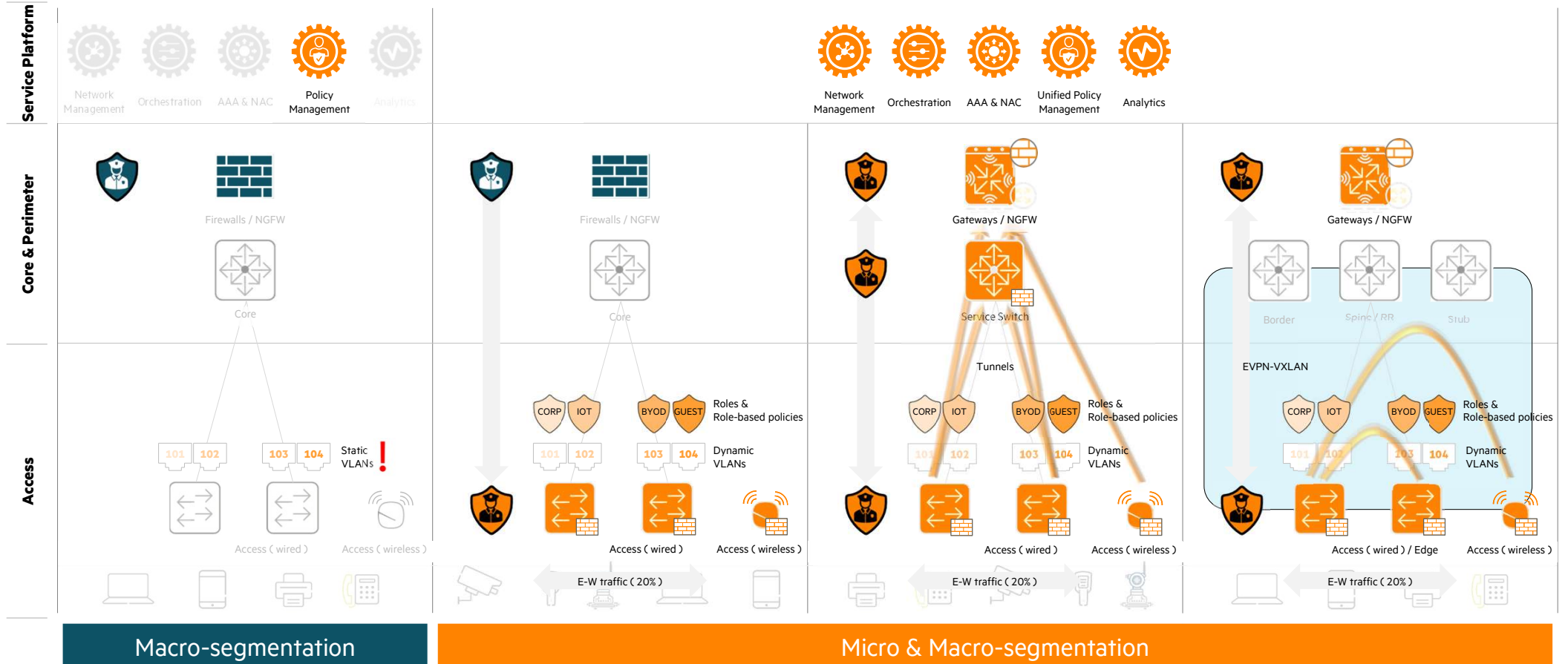
↑ Threat Protection

Centralized VLAN-based

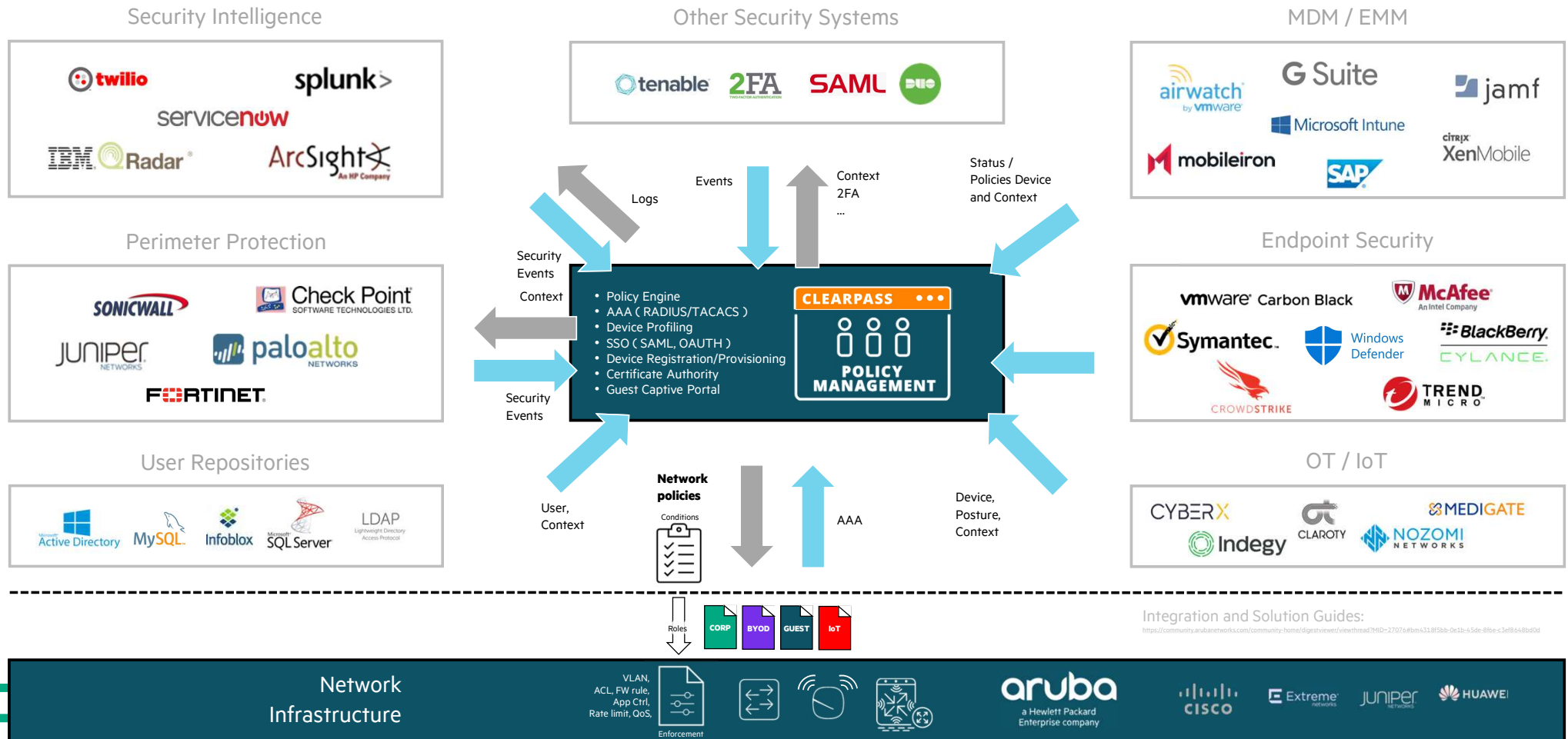
Role-based (port access)

Centralized Role-based

Distributed Role-based



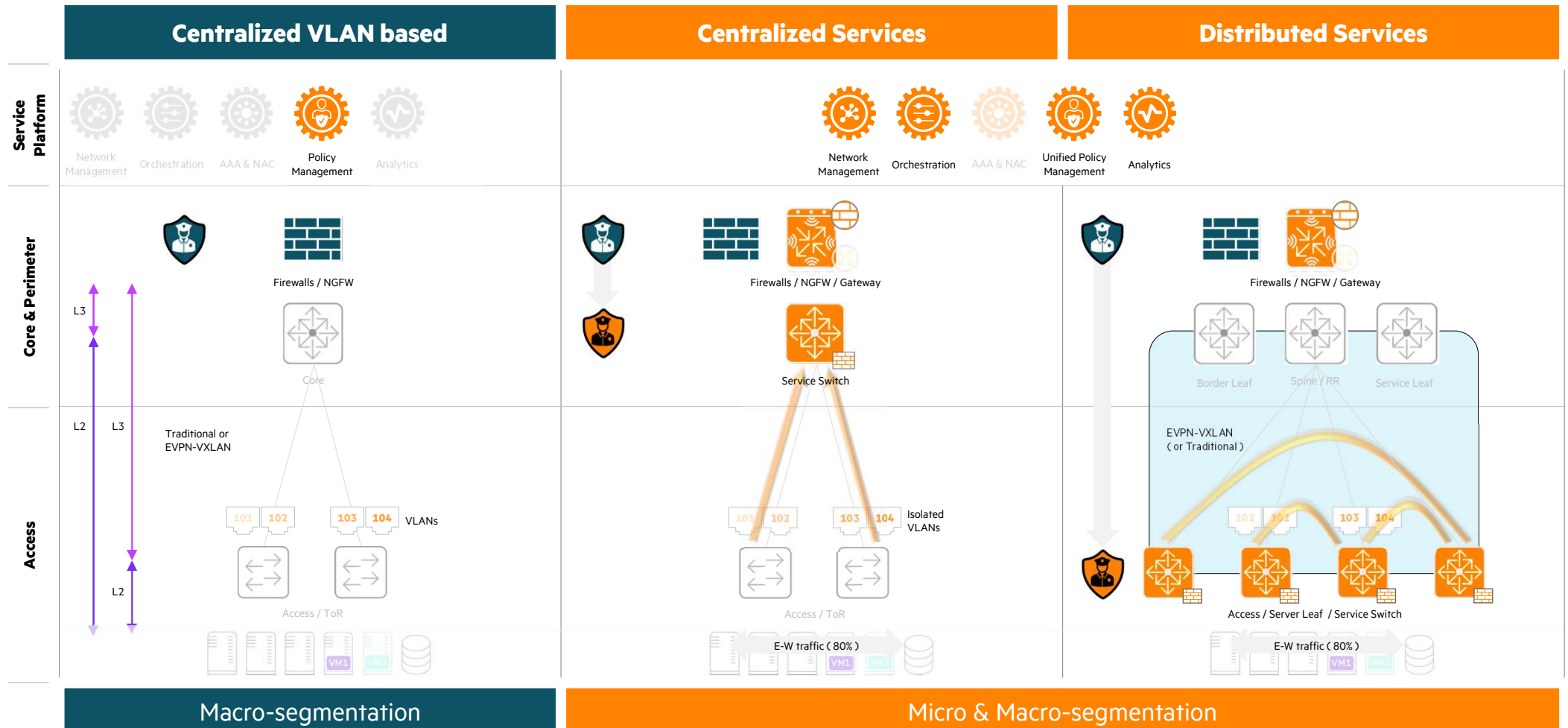
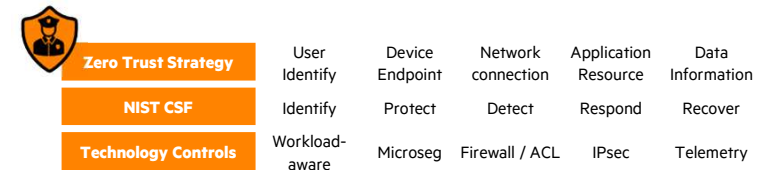
Aruba ClearPass Policy Manager (Policy, Orchestration, AAA, Visibility)



Micro-Segmentation in the Data Center

CHALLENGES: Adopting **Virtualization** Eliminating **Complexity** Innovative **Threats**

GOALS: Attack Surfaces Lateral Movement Threat Protection



UNIQUE !



FIREWALL



DDoS



TELEMETRY



NAT



ENCRYPT



SLB (Roadmap)



Aruba CX 10000 Distributed Services Switch



Aruba CX 10000 and Policy & Services Manager (PSM)

Configuring Security Policies with PSM (Administration View)

The image displays the Aruba Policy & Services Manager (PSM) Administration View, showing the configuration of Network Security Policies and the resulting Firewall Logs.

Network Security Policies:

- Policy Name: blockCMP
- Associated Networks (Ingress Policy): Network1202
- Associated Networks (Egress Policy): Network1202, Network1201

Firewall Logs:

Search filters: DSS: [], Source: [], Port: [], Action: deny, Protocol: [], Dest: [], Policy Name: blockCMP, VLAN: [].

Max Records: 5000, Count Relation: 0.5, Sort: Query by newest logs, VRF: GVA-VRF, Post hour: [].

Firewall Logs (6):

Creation Time	Reporter	Security Policy	Source	Destination	Protocol	Src Port	Dest Port	Action	Session ID	Session Action	Packets Sent	Packets Received	Bytes Sent	Bytes Received	VLAN	Rule Name
2022-09-03 08:03:03 GMT+00:00	Switch Name: aruba1201-1 DSS: 030-0403-8100-5800 MAC: 0400-8100-5800	blockCMP	10.6.202.110	10.6.201.101	icmp	2	2048	Deny	524301	flow_create					1202	blockCMP
2022-09-03 08:04:42 GMT+00:00	Switch Name: aruba1201-2 DSS: 030-0403-8100-5800 MAC: 0400-8100-5800	blockCMP	10.6.201.101	10.6.201.102	icmp	3	2048	Deny	2621558	flow_create					1201	blockCMP
2022-09-03 08:04:15 GMT+00:00	Switch Name: aruba1201-1 DSS: 030-0403-8100-5800 MAC: 0400-8100-5800	blockCMP	10.6.201.102	10.6.201.101	icmp	17	2048	Deny	524317	flow_delete	0		954		1201	blockCMP
2022-09-03 08:04:15 GMT+00:00	Switch Name: aruba1201-3 DSS: 030-0403-8100-5800 MAC: 0400-8100-5800	blockCMP	10.6.201.102	10.6.202.105	icmp	18	2048	Deny	2097388	flow_delete	6		636		1201	blockCMP
2022-09-03 08:03:11 GMT+00:00	Switch Name: aruba1201-1 DSS: 030-0403-8100-5800 MAC: 0400-8100-5800	blockCMP	10.6.201.102	10.6.202.105	icmp	18	2048	Deny	2097388	flow_create					1201	blockCMP
2022-09-03 08:03:05 GMT+00:00	Switch Name: aruba1201-1 DSS: 030-0403-8100-5800 MAC: 0400-8100-5800	blockCMP	10.6.201.102	10.6.201.101	icmp	17	2048	Deny	524317	flow_create					1201	blockCMP

Network Security Policies Configuration:

- VRF: pod1
- Source: 4 items selected
- Destination: DNS
- Select source VLANs: 6 items selected
- Select destination VLANs: 8.8.8.8, 10.29.5.7
- Port: 53

Network Diagram:

The diagram shows a network topology with various nodes and connections. A callout box highlights the configuration for the DNS service:

- Source IP: 10.29.194.11
- Protocol: udp
- Target IP: 10.29.5.7:53

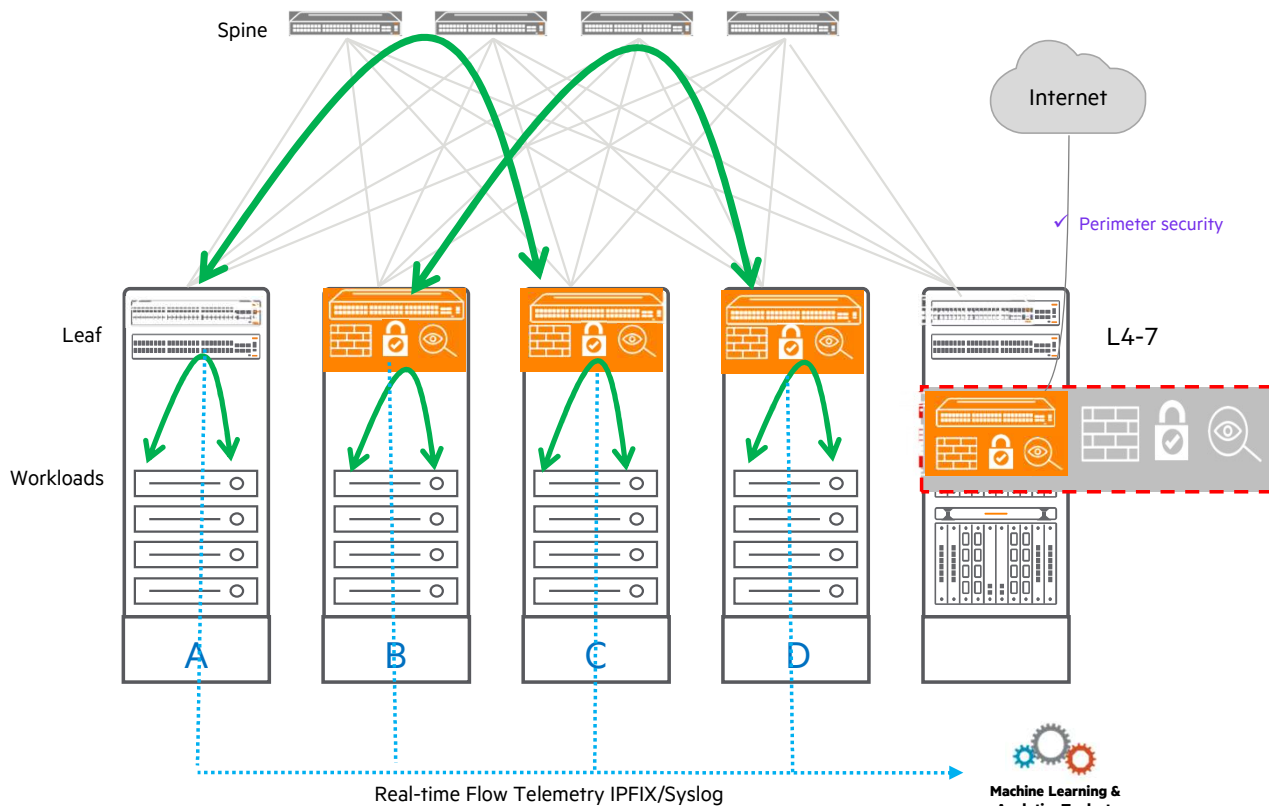
Actions:

- + Add Flows to Policy
- + Add Flows to Group

Distributed Services Architecture

Software Defined Distributed Security

With 4th Generation we offer a new and better way:



Distributed Intelligence Advantage

- Integrated 1.6Tb stateful F/W at every TOR pair
- Improved traffic flows & performance
- Reduced complexity
- Scale services as you add racks
- Pervasive Security – Everywhere for any workload
- Both Macro & Micro Segmentation support
- Centralized management via AFC
- Real-time Telemetry improves existing toolsets
- Significantly reduced costs

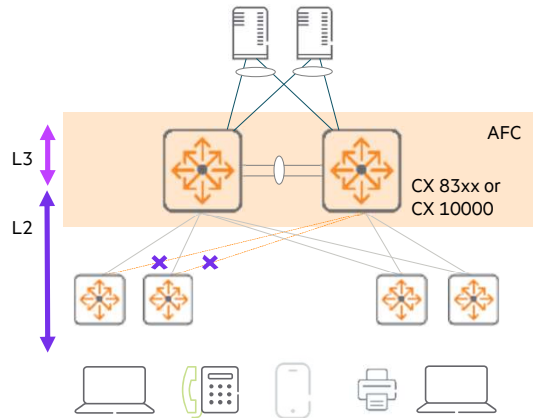
Note: Perimeter Security solution stays in place

*“100 times the scale at 10 times the performance
of our nearest competitor and at one-third the
TCO.”*

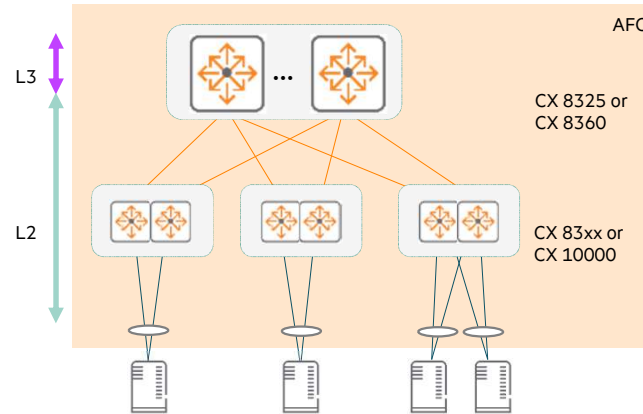
– John Chambers

Most common Datacenter Network architectures

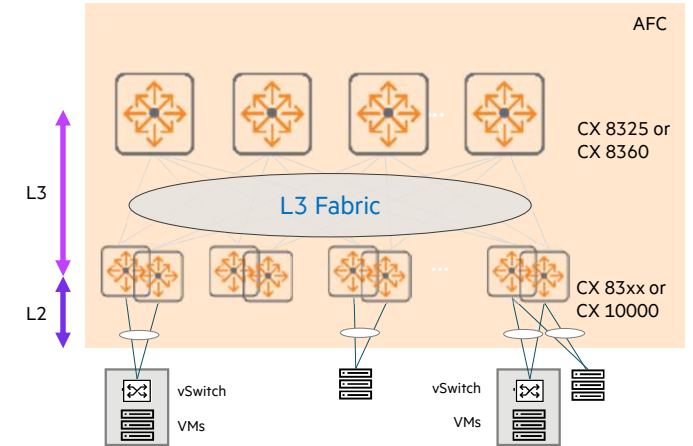
1.1 Traditional Collapsed Core/Agg (1-Tier) (STP / VSX MCLAG)



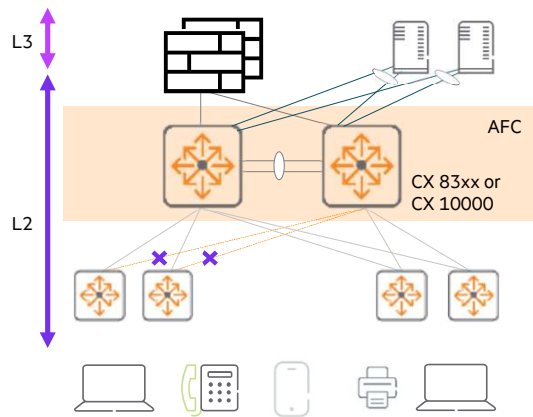
2. Traditional L2/L3 Fabric (2-Tier) (VSX MLAG)



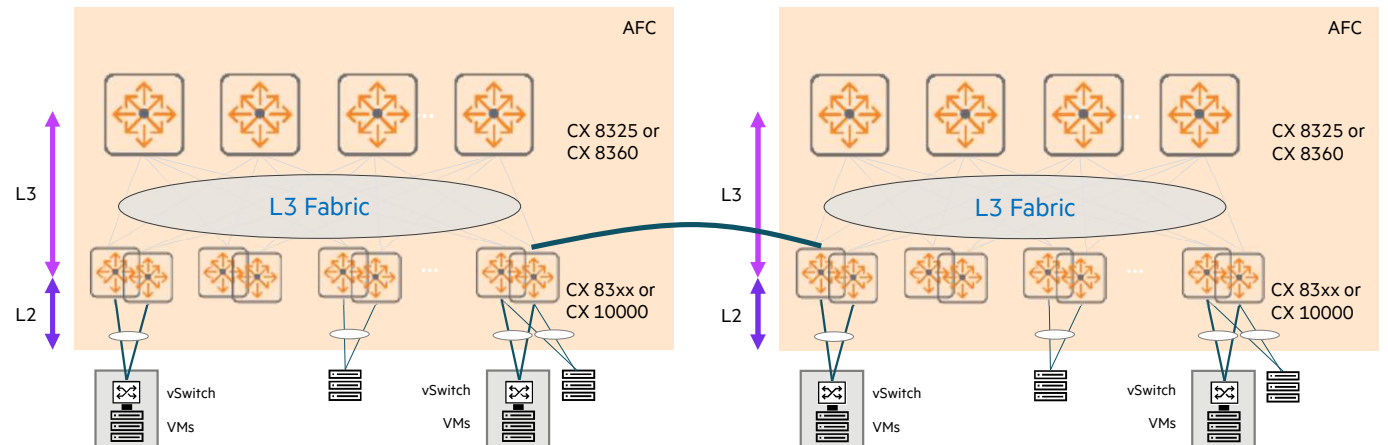
3. Spine & Leaf, EVPN, Single Fabric, Single DC (2-Tier) (VXLAN, EVPN & Network Virtualization)



1.2 Traditional Collapsed Core/Agg (1-Tier) (STP / VSX MCLAG)

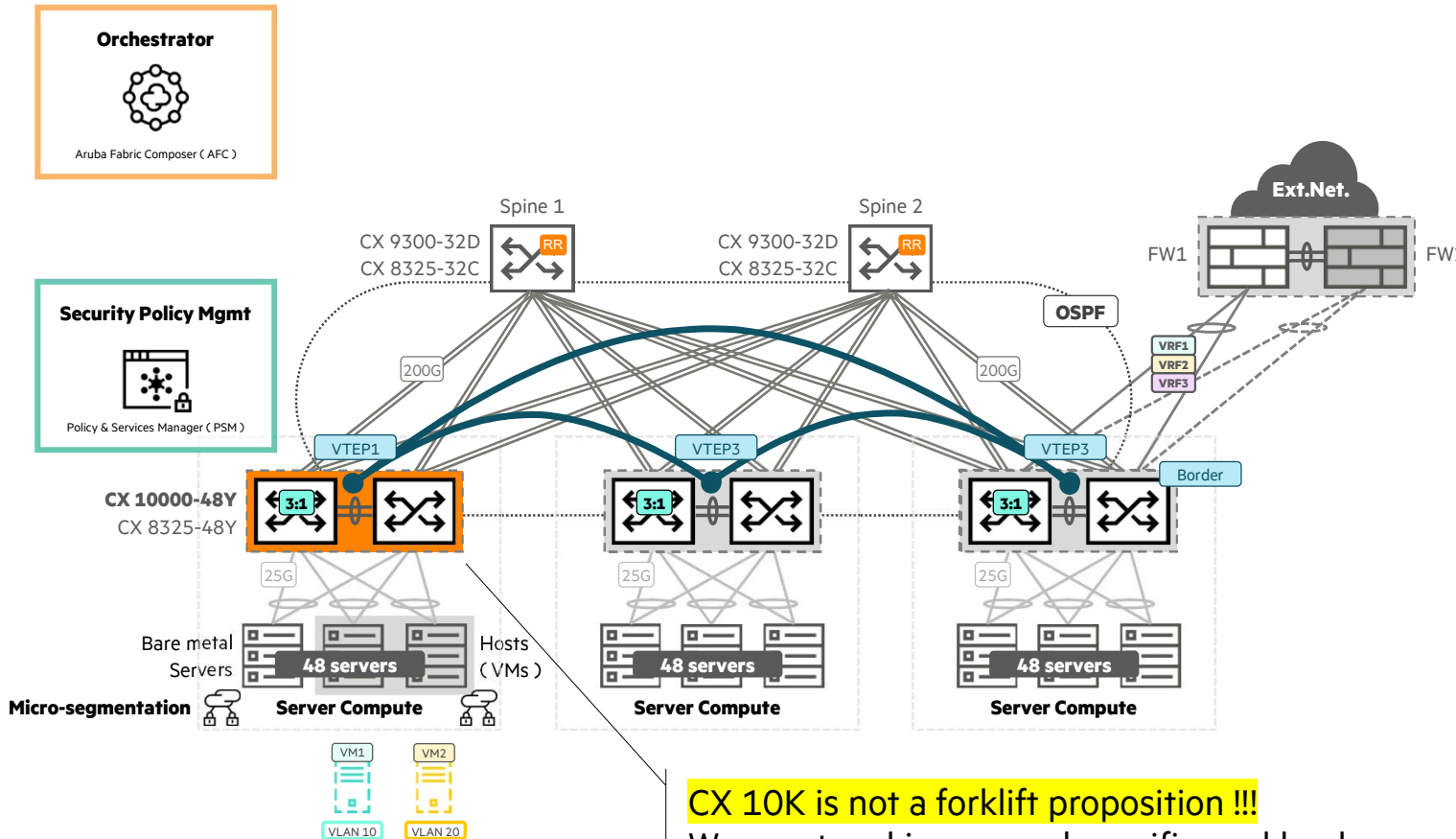


4. Spine & Leaf, EVPN, Single/Multi Fabric, Multi DCs (2-Tier) (VXLAN, EVPN & Network Virtualization)



Datacenter Networking Architecture (Securing Servers and VM workloads)

Traditional L2 or EVPN-VXLAN > Single-Site > Single-POD > L3 > Spine-Leaf Architecture



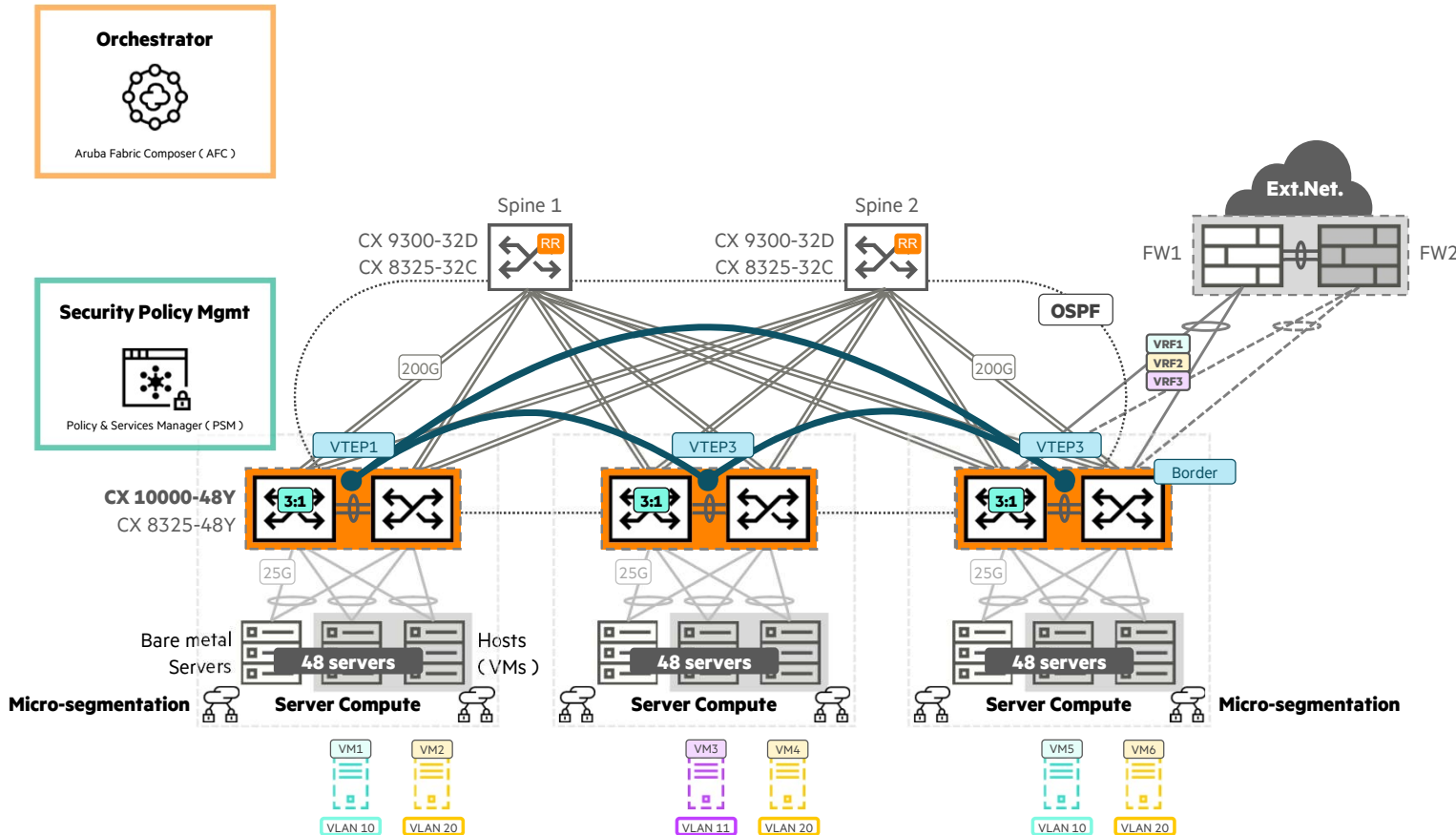
Underlay – 2 spine-leaf links

Features	Scenario EVPN-SS-SP-SL
Leaf VTEP	8325/8360/9300/10000
Spine	8325/8400/9300
Nb. of Spines	2
VSX ISL	4x 100G (possibly 2x100G)
Leaf switch uplinks	4x 100G ROP
Oversubscription ratio	10G NIC: 480G downlink/8325 480/400 => 1.2:1 (48 servers/rack) 25G NIC: 1200G downlink/8325 1200/400 => 3:1 (48 servers/rack) 100G NIC: 2400G downlink/8325 2400/400 => 6:1 (24 servers/rack) 100G NIC: 9600G downlink/9300 9600/1600 => 6:1 (ISL 4x400G) (96 servers/rack-group, spine=9300)
Nb. of racks	- Spine: 8325-32C => 8 racks - Spine: 8400-48C => 12 racks - Spine: 9300-32D => 32 racks

FEXIBLE deployment - Same OS without sacrificing features / capabilities !

Datacenter Networking Architecture (Securing Servers and VM workloads)

Traditional L2 or EVPN-VXLAN > Single-Site > Single-POD > L3 > Spine-Leaf Architecture



Underlay – 2 spine-leaf links

Features	Scenario EVPN-SS-SP-SL
Leaf VTEP	8325/8360/9300/10000
Spine	8325/8400/9300
Nb. of Spines	2
VSX ISL	4x 100G (possibly 2x100G)
Leaf switch uplinks	4x 100G ROP
Oversubscription ratio	10G NIC: 480G downlink/8325 480/400 => 1.2:1 (48 servers/rack) 25G NIC: 1200G downlink/8325 1200/400 => 3:1 (48 servers/rack) 100G NIC: 2400G downlink/8325 2400/400 => 6:1 (24 servers/rack) 100G NIC: 9600G downlink/9300 9600/1600 => 6:1 (ISL 4x400G) (96 servers/rack-group, spine=9300)
Nb. of racks	- Spine: 8325-32C => 8 racks - Spine: 8400-48C => 12 racks - Spine: 9300-32D => 32 racks

FEXIBLE deployment - Same OS without sacrificing features / capabilities !

Collapsed Core (Securing the Campus and DC)

Traditional > L2 > Two-tier Architecture (L3 core / L2 access) and Core with Statefull firewall

