Link Oregon

SPONSORED LIGHTNING TALK

Campus Segmentation Strategies

ARISTA

Speaker:
Joe Lentz, Service Engineer

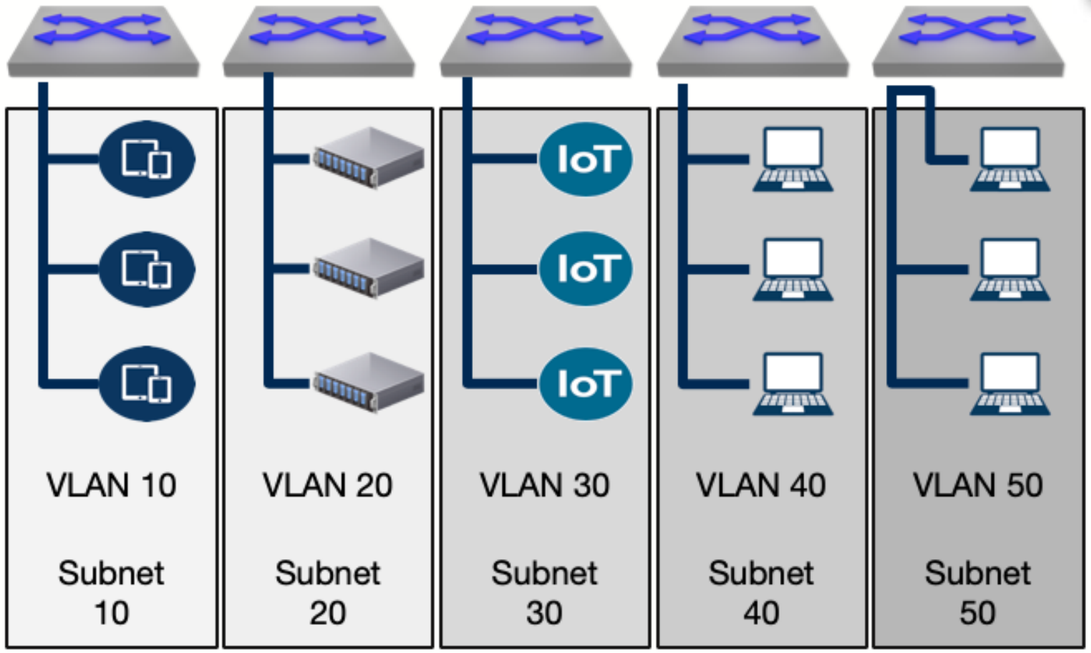
ARISTA

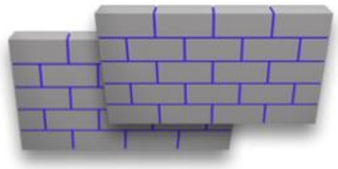
Campus Segmentation Strategies

May 2026

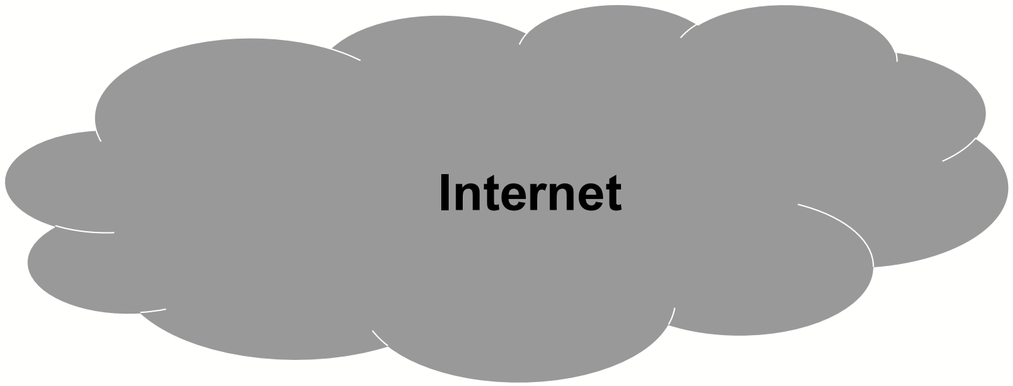
Traditional Security

Trusted Campus (non DC) Networks





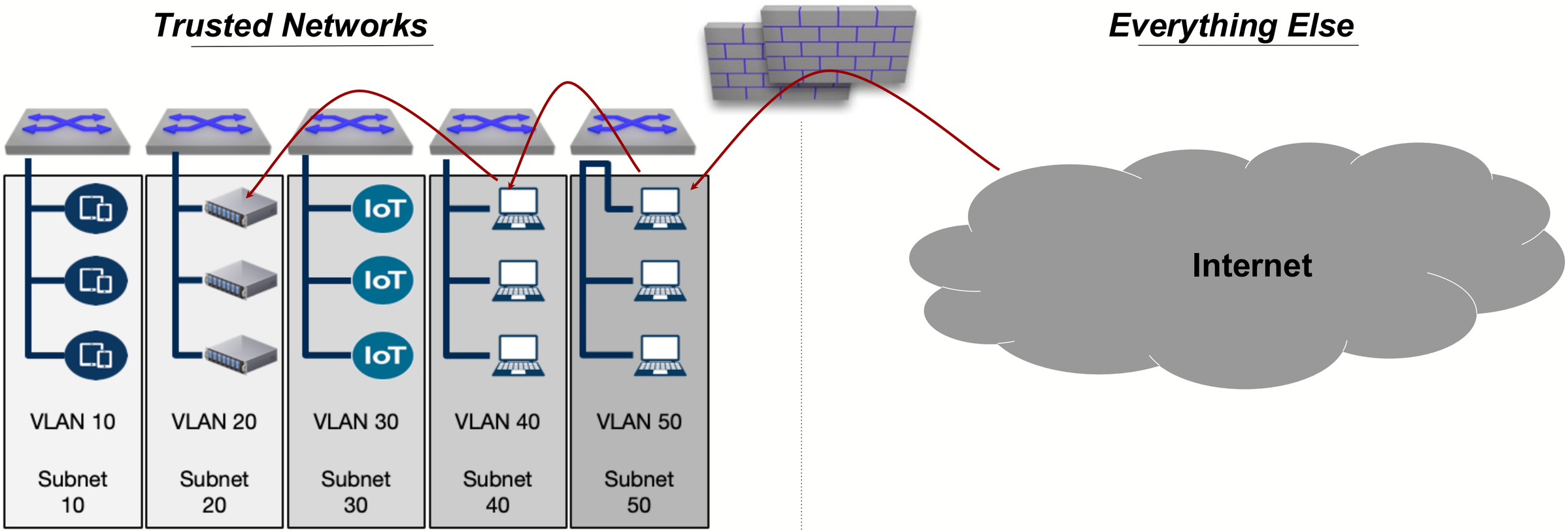
Everything Else



Secure Edge

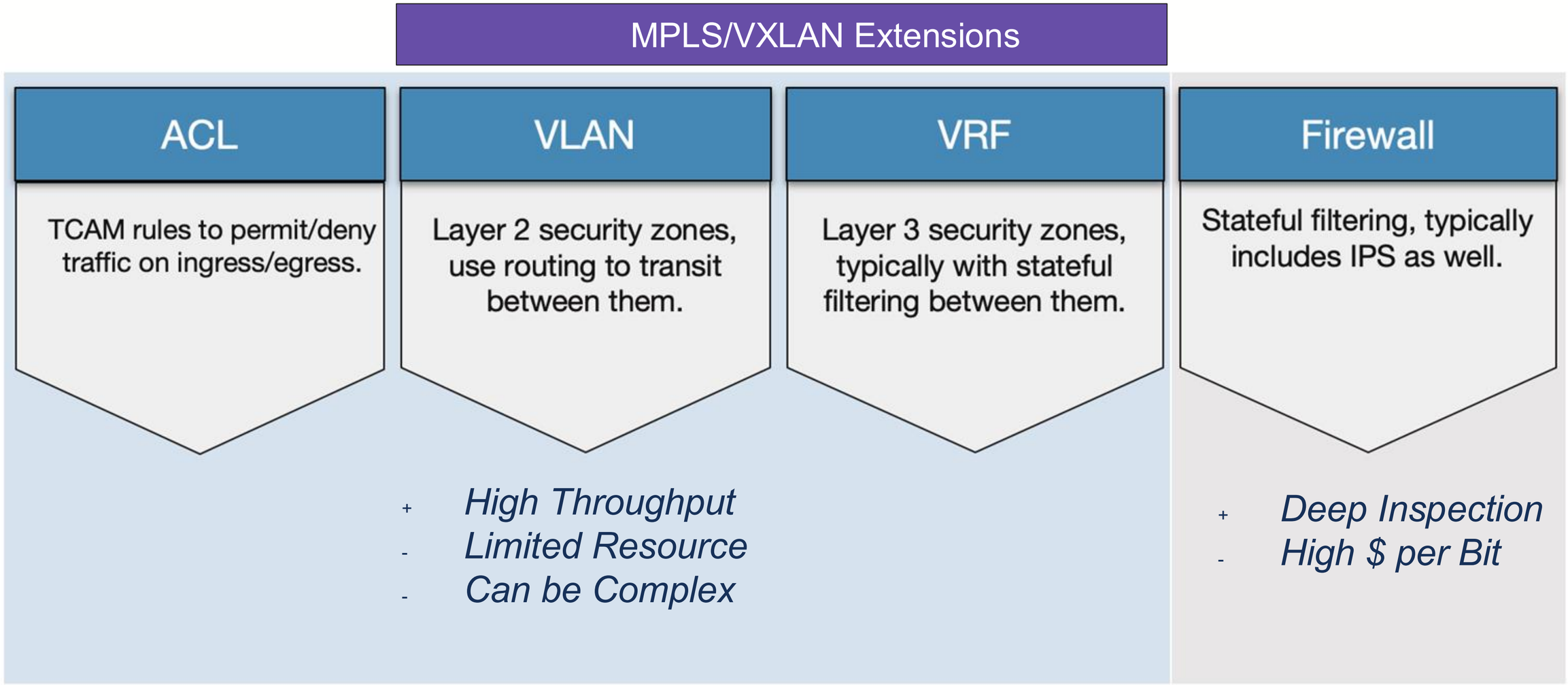
ARISTA

Where it Falls Flat?

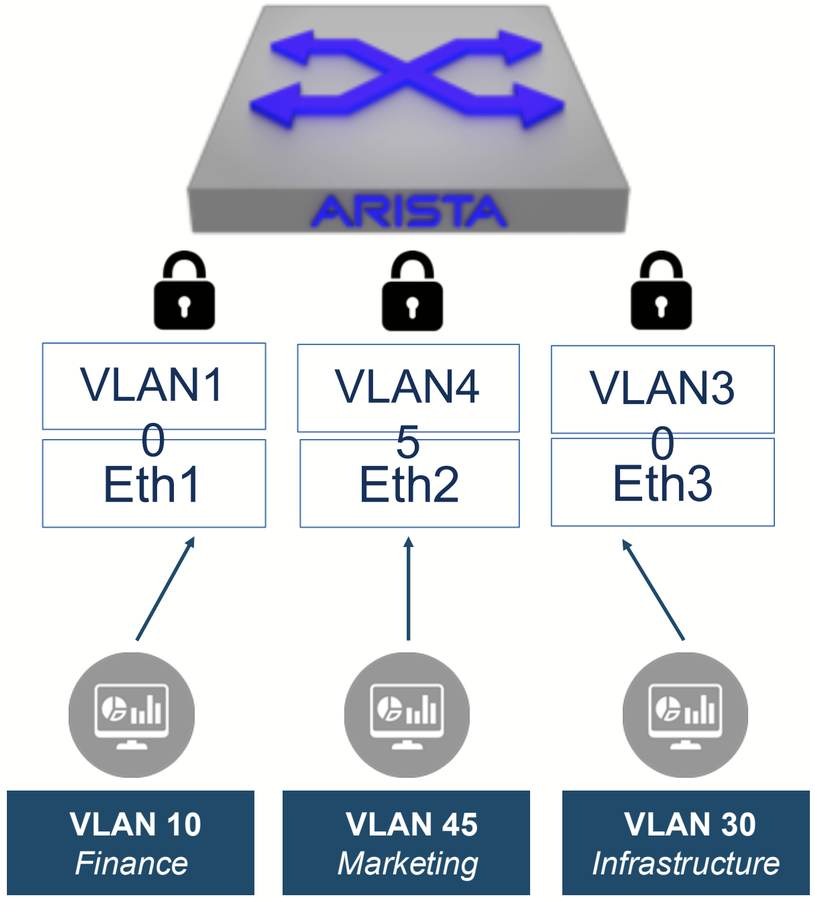


Lateral Movement

Building Blocks



VLAN



VLANs

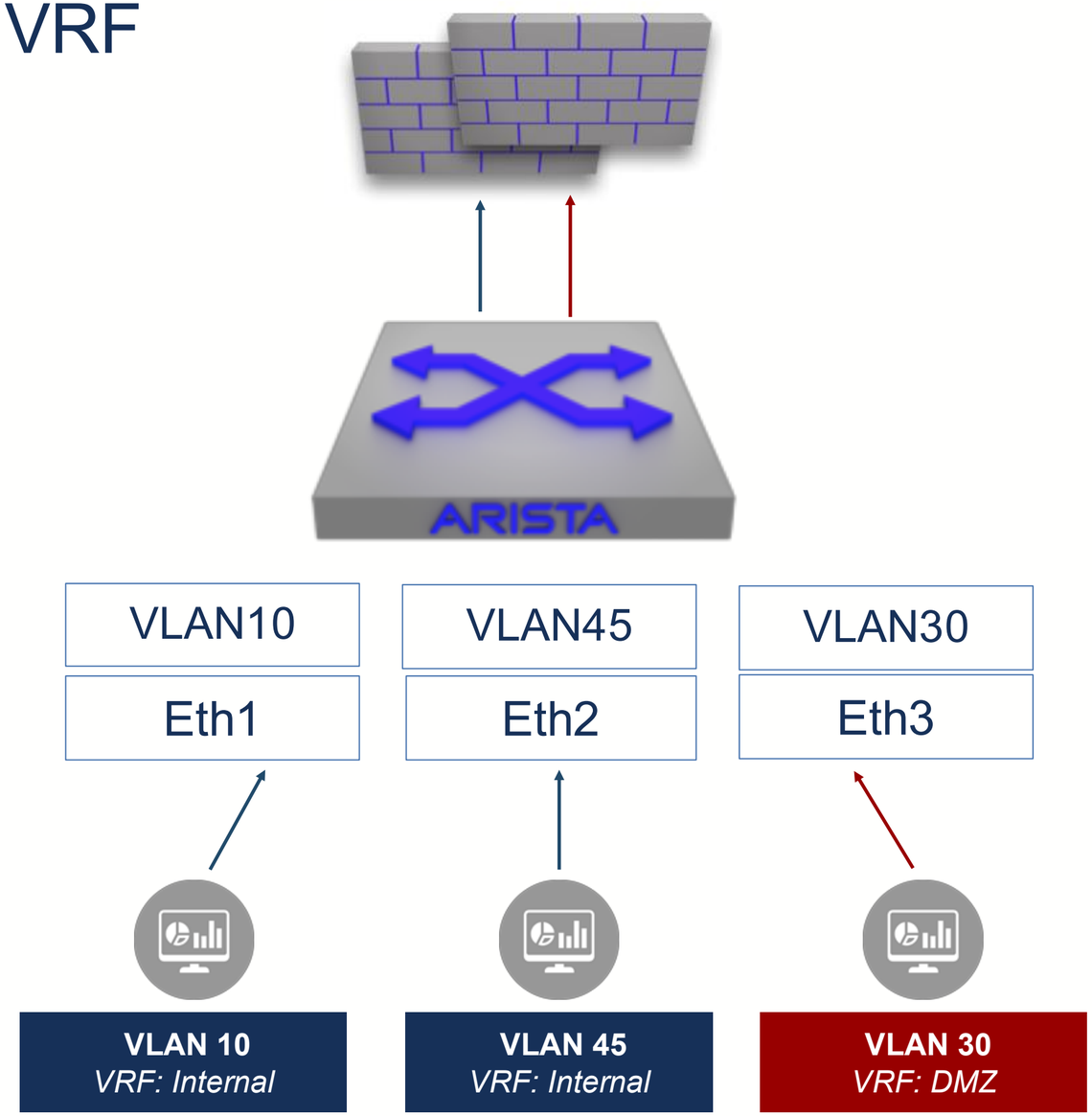
- Can segment a physical switch into multiple logical segments at Layer 2
- VLANs reduce the broadcast domain size
- VLANs can be spanned across the switches using Dot1Q trunk interfaces

```
switch(config)#vlan 45
switch(config-vlan-45)#name Marketing
switch(config-vlan-45)#show vlan 45

VLAN Name StatusPorts
---- -------------------------------- --------- -------
45   Marketing                        active    Et1

switch(config-vlan-45)#
```

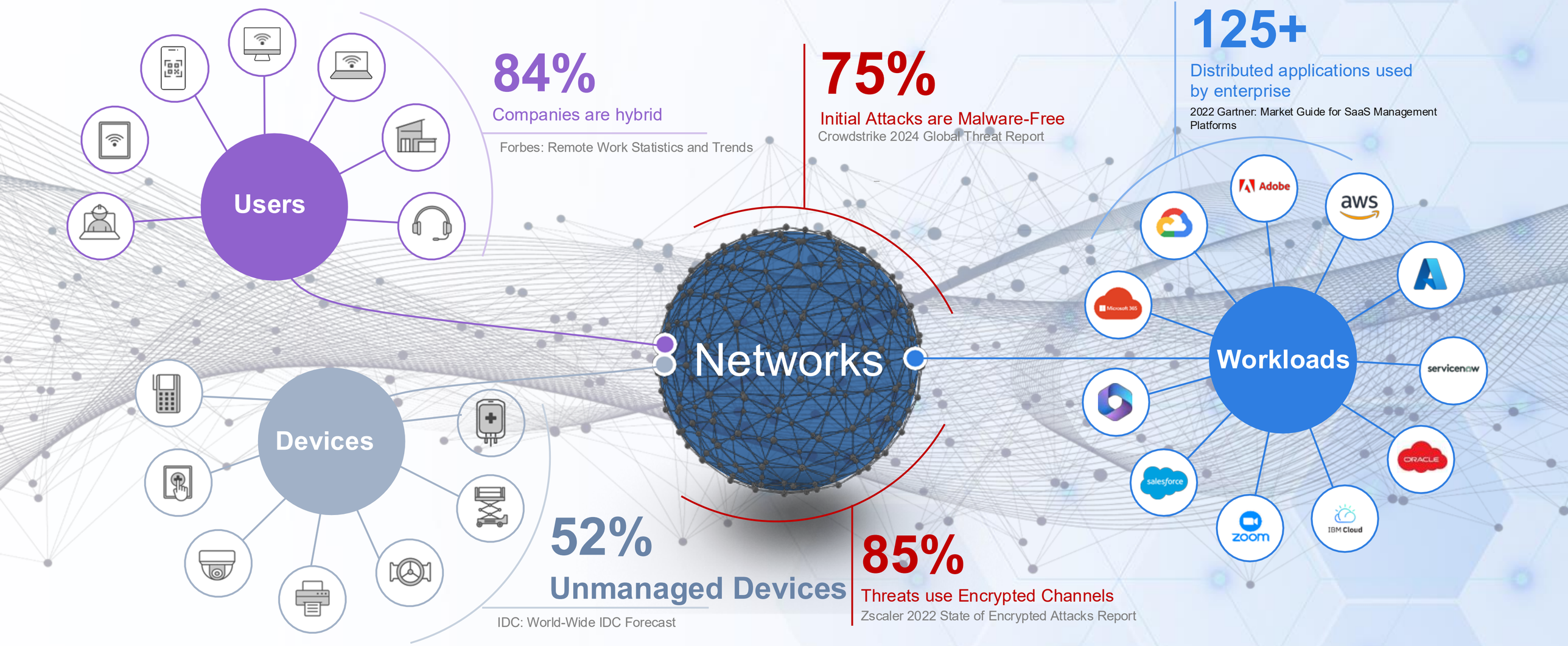
VRF



VRFs

- Can segment a physical switch into multiple logical segments at Layer 3
- VRFs carry a vrf-specific routing table
- VRFs can be extended between switches with Layer 3 links, or with encapsulation protocols (VXLAN/MPLS).

Key Security Challenges – The Vanishing Perimeter



84%
Companies are hybrid
Forbes: Remote Work Statistics and Trends

75%
Initial Attacks are Malware-Free
Crowdstrike 2024 Global Threat Report

125+
Distributed applications used by enterprise
2022 Gartner: Market Guide for SaaS Management Platforms

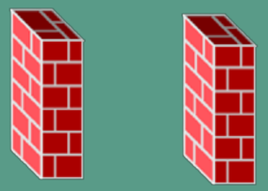
52%
Unmanaged Devices
IDC: World-Wide IDC Forecast

85%
Threats use Encrypted Channels
Zscaler 2022 State of Encrypted Attacks Report

ARISTA

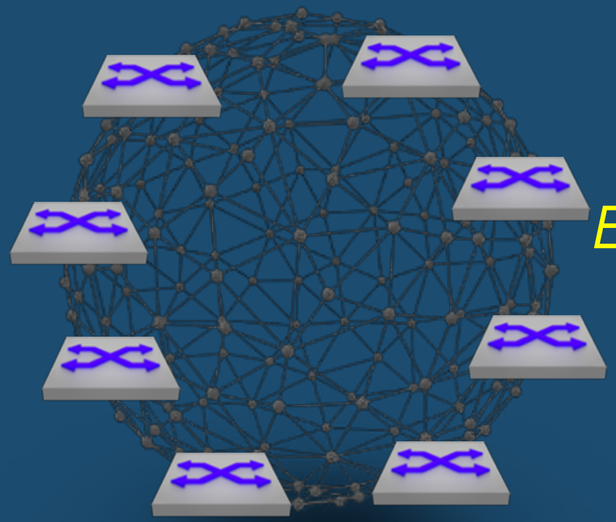
The Role Of The Network In Zero Trust Architectures

Perimeter Firewalls



Do NOT inspect most of the INTERNAL traffic

The Network



EVERY endpoint is connected to it!

Endpoint Security

INCOMPATIBLE with the large % of unmanaged endpoints

The NETWORK is the **only IT asset** that "sees" *all the traffic* and "touches" *all the endpoints*

➞ **The NETWORK** is in a **privileged position** to enable a **Zero Trust** strategy built on *adaptive access control*, *multi-domain segmentation*, and *Threat Detection* services **built into the network infrastructure**

ARISTA

Requirements of Modern Campus Segmentation

- Granular control of lateral movement
- Securing North-South traffic as well as East-West traffic
- Dynamic classification of enterprise device in smaller trust zones (micro-perimeters)

What is a Micro-Perimeter

A micro-perimeter is a network-agnostic construct that defines a logical subset of similar devices.

Devices can be characterized based on:

devices

Device Properties

- Model
- Software version

person

User Properties

- Role
- Group

public

Environment Properties

- Physical
- Logical

Microperimeter Segmentation

The capability to insert a group-based security policy between any two groups with endpoints in the same network or across multiple networks.

Core Capabilities

security

Policy Enforcement

search

Endpoint Discovery

route

Traffic Session Mapping

psychology

Policy Recommendation Engine

hub

Integration with Threat Detection Solutions

Arista Multi-Domain Segmentation (MSS)

Capability	Traditional Switch-Based	Host-Based Firewall	MSS
Wire-speed performance	✅	❌	✅
Any endpoint support	✅	❌	✅
Campus & DC consistency	❌	✅	✅
Any network support	❌	✅	✅
No agent required	✅	❌	✅
No custom protocol dependency	❌	✅	✅

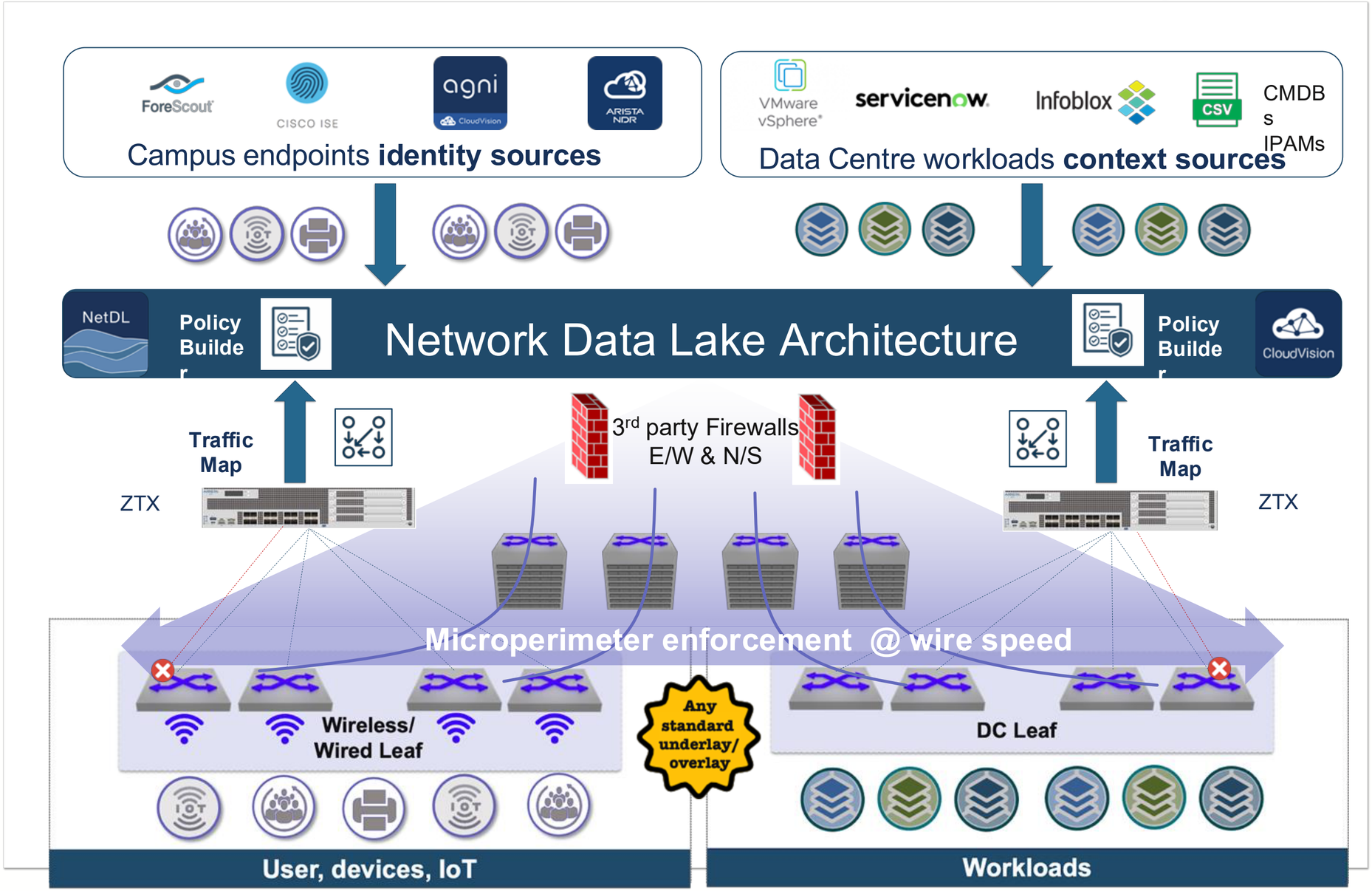
Arista Segmentation Services for Zero Trust Networking

01 **Define Groups / Microperimeters** Directly in CloudVision or via External Identity Databases

02 **Define Policies to allow only trusted traffic**
CV Policy Builder and ZTX Traffic Mapper (Optional)

03 **Distribute enforcement in the network or redirect to Firewall**

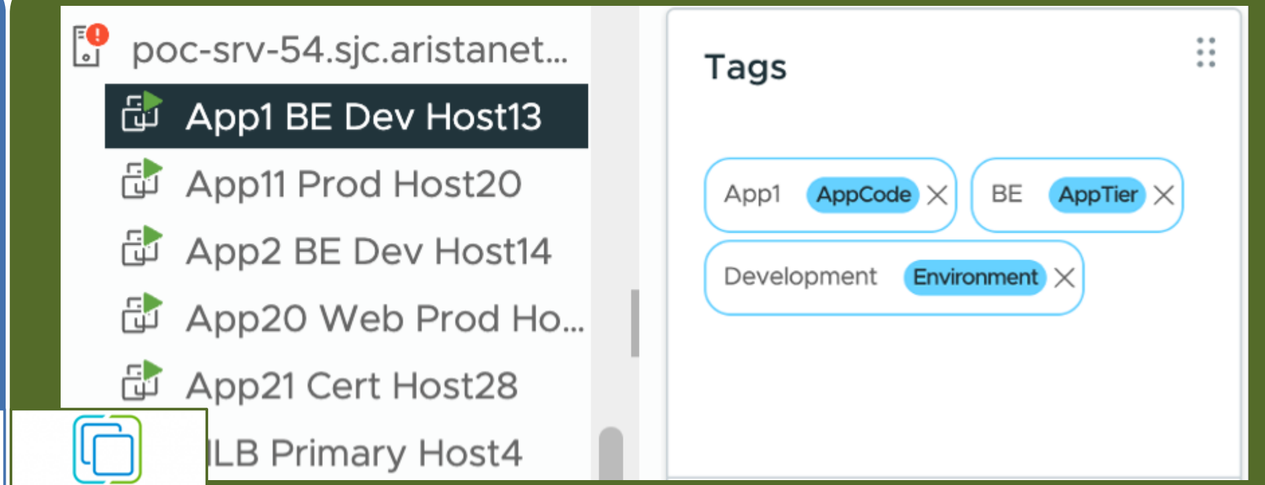
04 **Continuous monitoring and policy update**
ZTX continuous analysis of policy violations



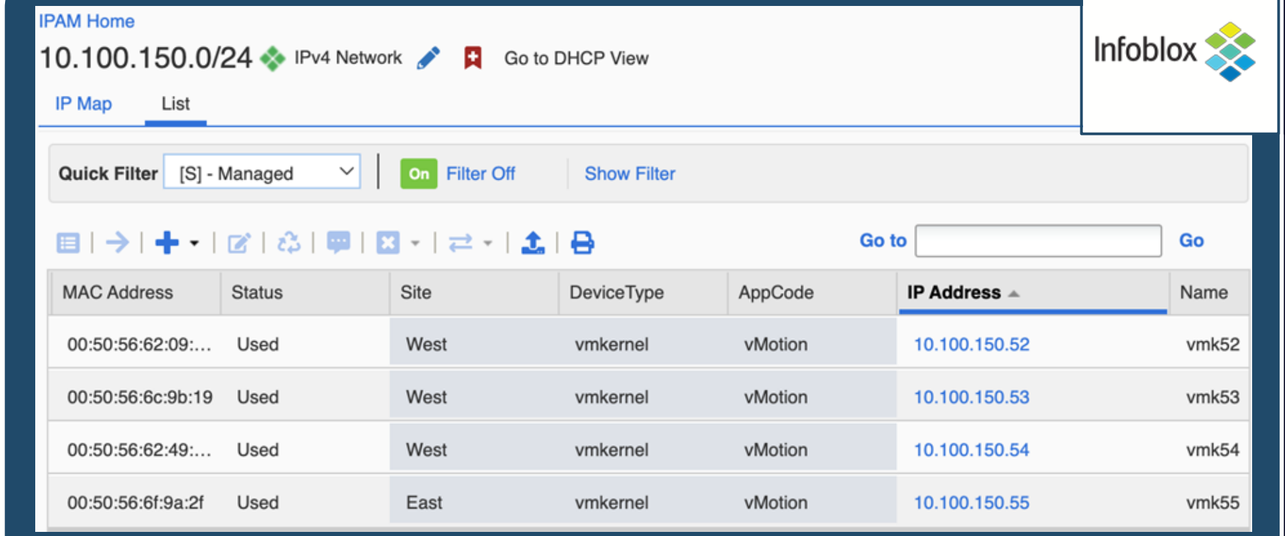
MSS Dynamic Microperimeter Tag Integrations (1/2)

AppCode	AppTier	Env	Hostname	Zone
Search	Search	Search	Search	Search
App2	Web	Prod	app2-web-prod-host2	Production
App3	BE	Prod	app3-be-prod-host7	Production
App1	BE	Prod	app1-be-prod-host5	Production
App2	BE	Prod	app2-be-prod-host6	Production
App3	BE	Prod	app3-be-prod-host10	Production
App2	BE	Prod	app2-be-prod-host9	Production
App3	Web	Prod	app3-web-prod-host3	Production
App1	Web	Prod	app1-web-prod-host1	Production
App1	BE	Prod	app1-be-prod-host8	Production

servicenow



VMware vSphere®



Infoblox

CSV

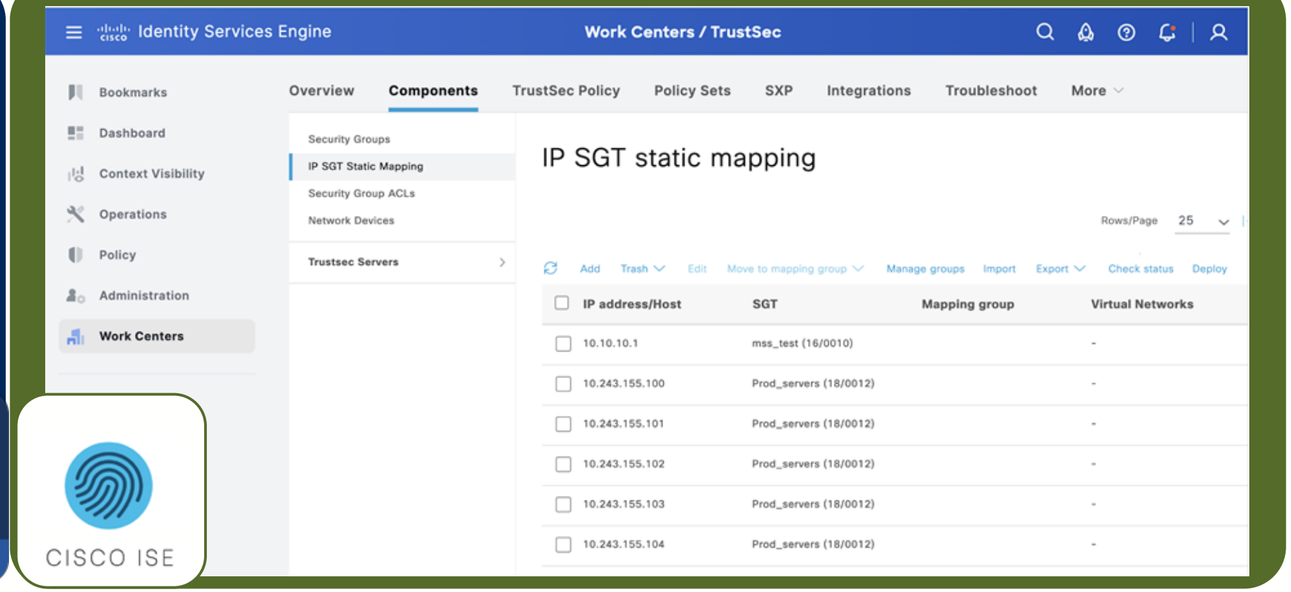
Site	SWCI_ID	IPaddr	Hostname	Management Hostname
Site1	SWIP1	10.100.101.201/32	App1-Web-Prod-host1	poc-mss-host1
PROD App2 Site1	SWIP2	10.100.101.202/32	App2-Web-Prod-host2	poc-mss-host2
PROD App3 Site2	SWIP3	10.100.101.203/32	App3-Web-Prod-host3	poc-mss-host3
PROD App1 Site1	SWIP1	10.100.102.205/32	App1-BE-Prod-host5	poc-mss-host5
PROD App2 Site1	SWIP2	10.100.102.206/32	App2-BE-Prod-host6	poc-mss-host6
PROD App3 Site1	SWIP3	10.100.102.207/32	App3-BE-Prod-host7	poc-mss-host7

ARISTA

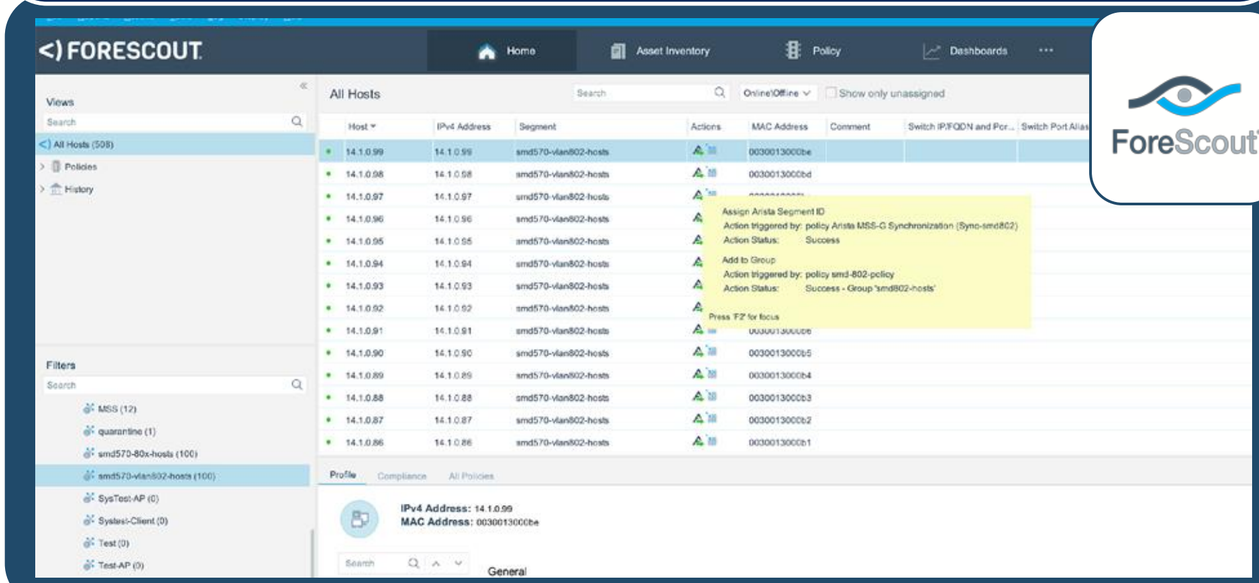
MSS Dynamic Microperimeter Tag

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	iot-group-4	MAC Authentication	00:80:80:00:03:37	10.80.4.55	Success	12/1/2024 23:56:54.143
2	iot-group-2	MAC Authentication	00:80:80:00:02:04	10.80.3.4	Success	12/1/2024 23:56:54.027
3	iot-group-4	MAC Authentication	00:84:84:00:03:a5	10.84.4.165	Success	12/1/2024 23:56:39.932
4	iot-group-2	MAC Authentication	00:82:82:00:01:9f	10.82.2.159	Success	12/1/2024 23:56:12.045
5	IxiaUser2	MAC Authentication	00:90:90:00:00:07	10.90.1.7	Success	12/1/2024 23:54:56.372
6	IxiaUser2	MAC Authentication	00:90:90:00:00:01	10.90.1.1	Success	12/
7	iot-group-4	MAC Authentication	00:80:80:00:03:42	10.80.4.66	Success	12
8	iot-group-1	MAC Authentication	00:80:80:00:01:3d	10.80.2.61	Success	12

agni CloudVision



CISCO ISE



ForeScout

ROADMAP

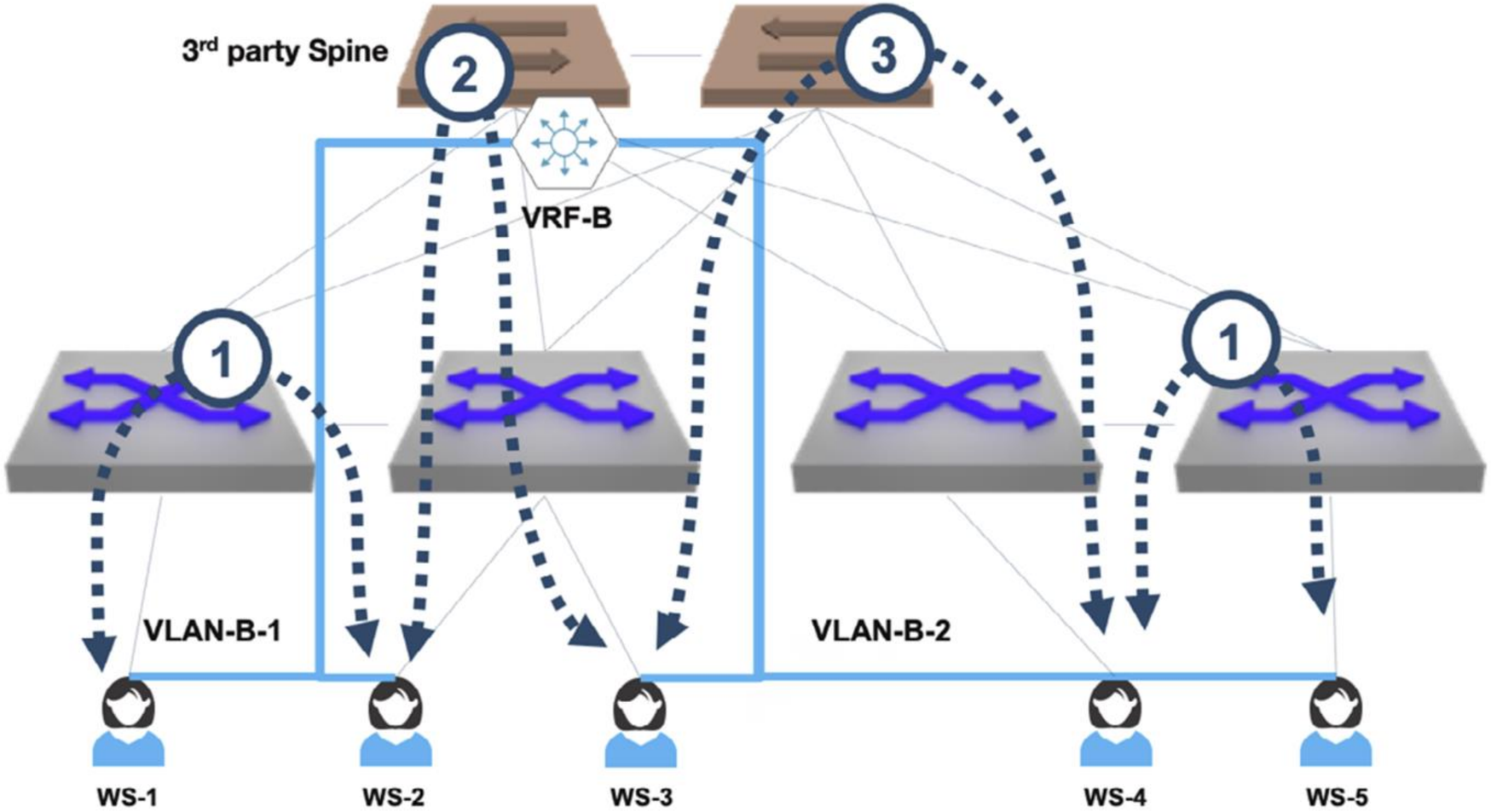
ARISTA

Defining MSS Policy

- Defining a security tag **“WORKSTATIONS”** that includes the list of IP addresses of all five workstations.
- Defining a security tag **“OBSOLETE”** that includes the IP addresses of the two obsolete workstations.
- Define the Policy Enforcement Rule based on these security tags.

Source	Destination	Network Service	Enforcement Action
OBSOLETE	**WORKSTATIONS**	*	DROP MONITOR

Example of lateral conversations



(1) intra-VLAN intra-leaf (2) inter-VLAN inter-leaf (3) intra-VLAN inter-leaf

Example MSS Running Configuration

1. Input Match Lists (Groups)

```
match-list input prefix-ipv4 BLOCK_IP
match prefix-ipv4 212.159.212.231/24
match-list input prefix-ipv4 EXTERNAL_ANY_IP
match prefix-ipv4 0.0.0.0/0
match-list input prefix-ipv4 IPMS_PERMIT_IP
match prefix-ipv4 100.100.100.100/32
```

2. Segment Definition & Defaults

```
router segment-security
no shutdown
segment policy policy-drop-all default
!
vrf default
segment BLOCK_SRC
definition
match prefix-ipv4 BLOCK_IP
```

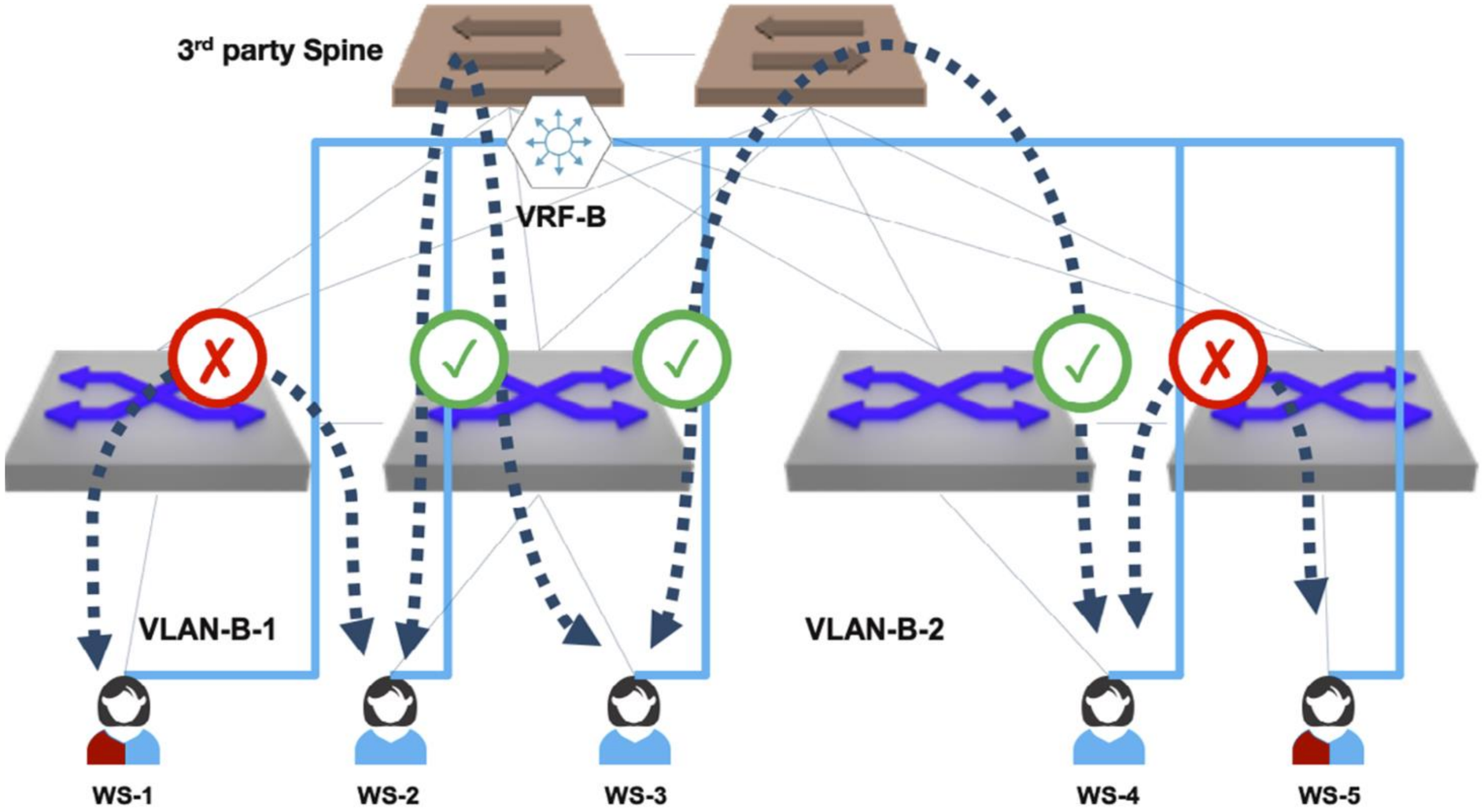
3. Segment Policies (Enforcement Matrix)

```
policies (BLOCK_SRC)
from BLOCK_SRC policy policy-drop-all
from EXTERNAL policy policy-drop-all
from IPMS_PERMIT policy policy-forward-all
from PERMIT_SRC policy policy-forward-all
```

```
policies (EXTERNAL)
from BLOCK_SRC policy policy-drop-all
from EXTERNAL policy policy-forward-all
from IPMS_PERMIT policy policy-forward-all
from PERMIT_SRC policy policy-forward-all
```


ARISTA

MSS enforcement to limit lateral communication of obsolete devices



MSS Wire Speed Enforcement Abstracted From The Network

No tags in the data plane

S-IP	D-IP	Proto	S-Port	D-Port
10.166.42.2	10.175.20.2	TCP	22222	3306

IoT Camera

DVR Server

CloudVision

1 2 3

Standard bridging/routing to destination

S-IP	D-IP	Proto	S-Port	D-Port
10.166.42.2	10.175.20.2	TCP	22222	3306

S-IP	D-IP
10.166.42.2	10.175.20.2

Wirespeed Tag LPM lookups

Endpoint HW "database"

Group Name	Prefix List	Tag (auto)
IoT Group	1 10.166.42.2/32 … 128 10.166.42.4/32	100
IoT Server	1 10.175.20.2/32 … 64 10.175.24.4/32	200

100	200	TCP	3306

Single pass - wirespeed Tag-based TCAM lookup

Tag based TCAM Rules

Source Group	Dest Group	Service		Action
100	200	TCP	3306	*forward*

Rule summarization > scale
Rules independent of changes in the network

ARISTA

ZTN Integration