

# Strategies in Network Microsegmentation

## MONUG - North Kansas City, MO - 1 April 2026

Jayson Tobias, SE - Arista Networks

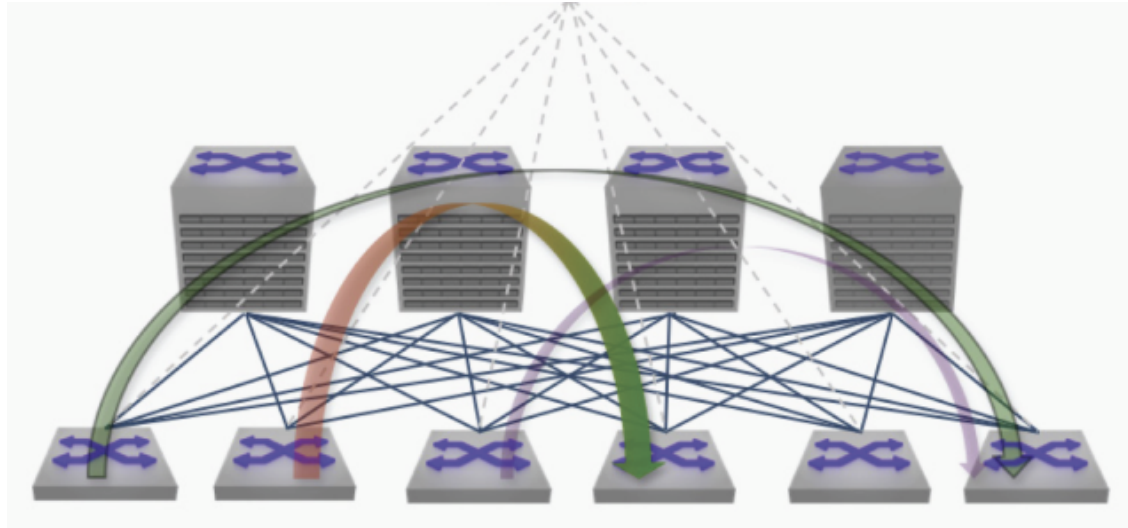
# About Your Speaker

- SE at Arista Networks (KS/MO)
- CCIE #15550 (R&S Lifetime Emeritus)
- ACE L5
- MBA, University of Kansas
- Previously at AOS/ConvergeOne/C1,  
Lumos Consulting



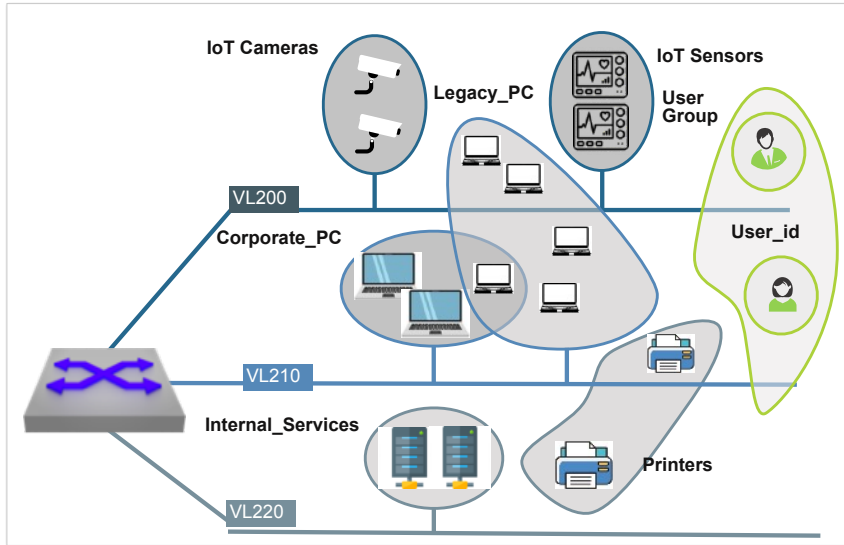
# Why Segmentation?

- Compliance, business unit / customer isolation.
- Prevent malicious actors from leveraging east-west network connectivity for nefarious purposes.

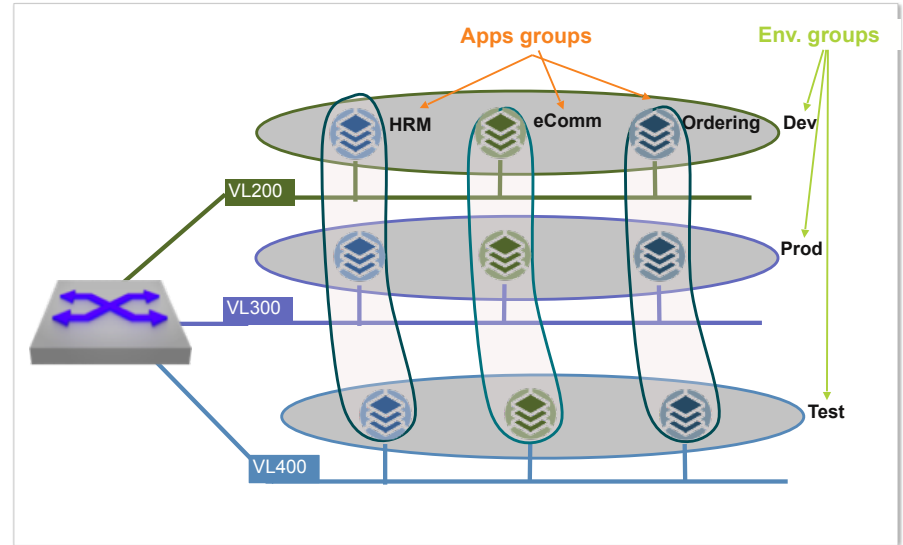


# Today's Focus - Microsegmentation

## Campus & Branch Endpoint Microperimeters



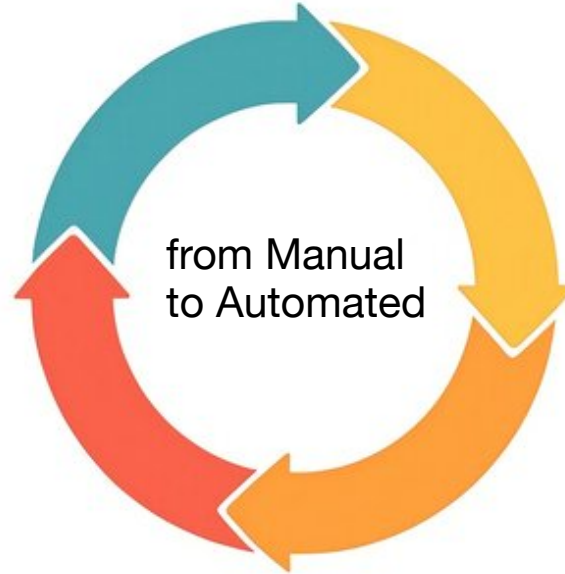
## Datacenter Workload Microperimeters



# Microsegmentation Lifecycle

(Re-)Assess  
Assets

Analyze Traffic  
Patterns

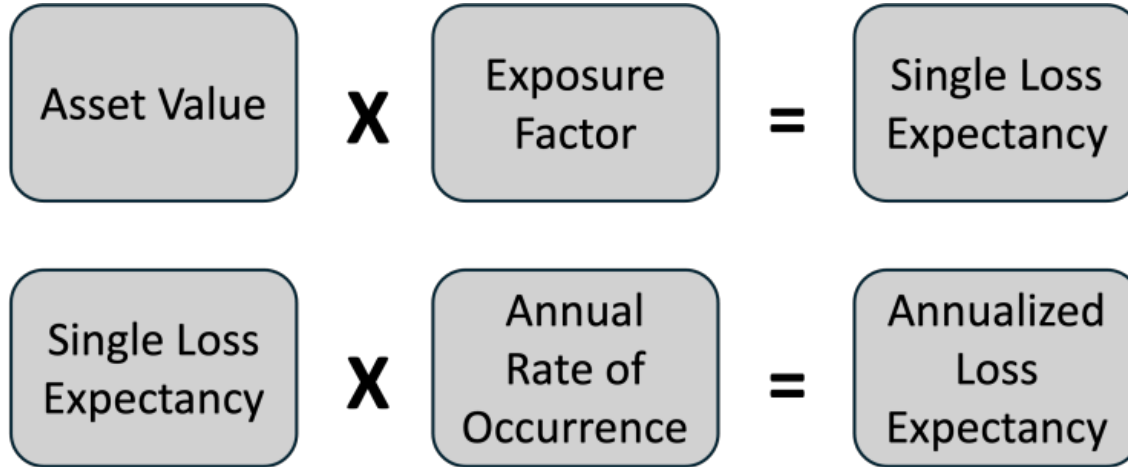


Adjust Network  
Traffic Policies

Develop, Test,  
Validate Rulesets

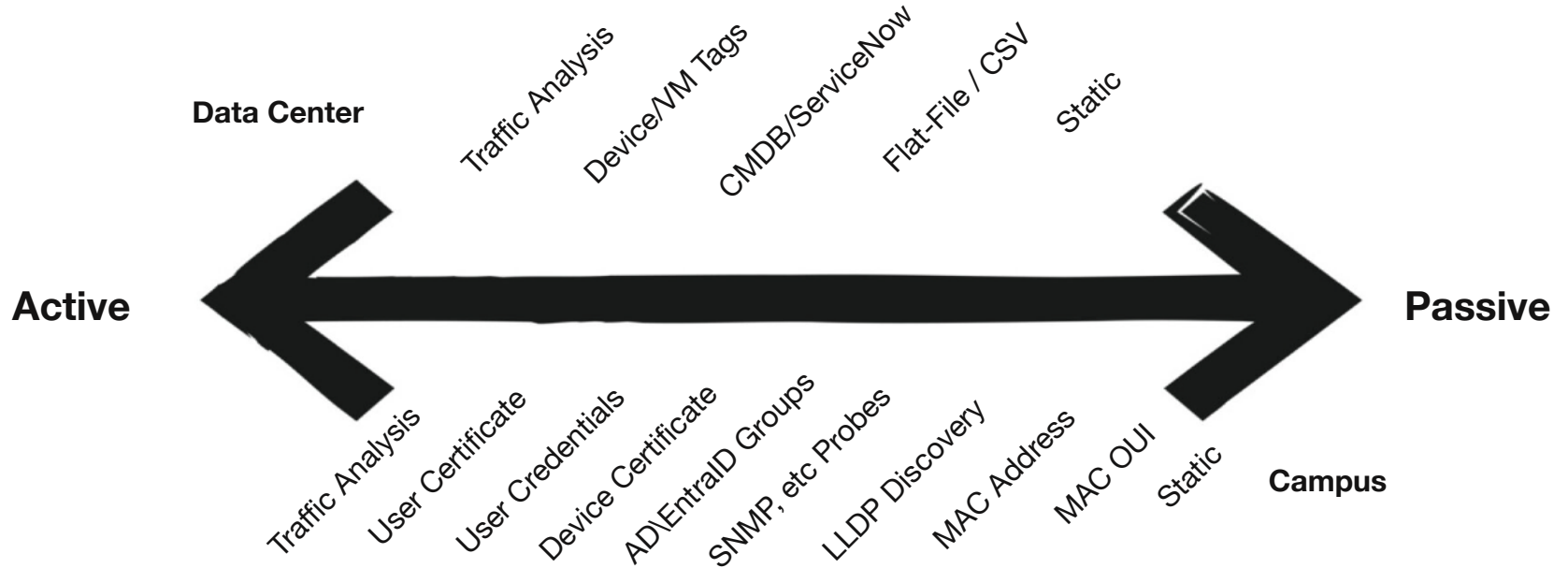
# Where to start?

- Calculate Organizational Risk

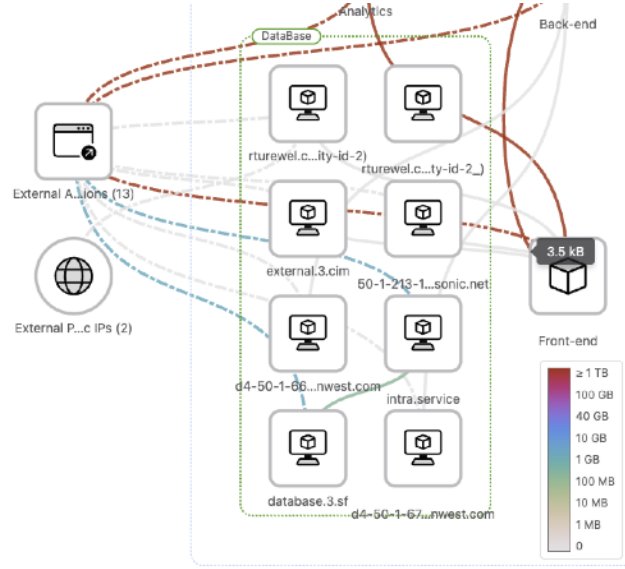
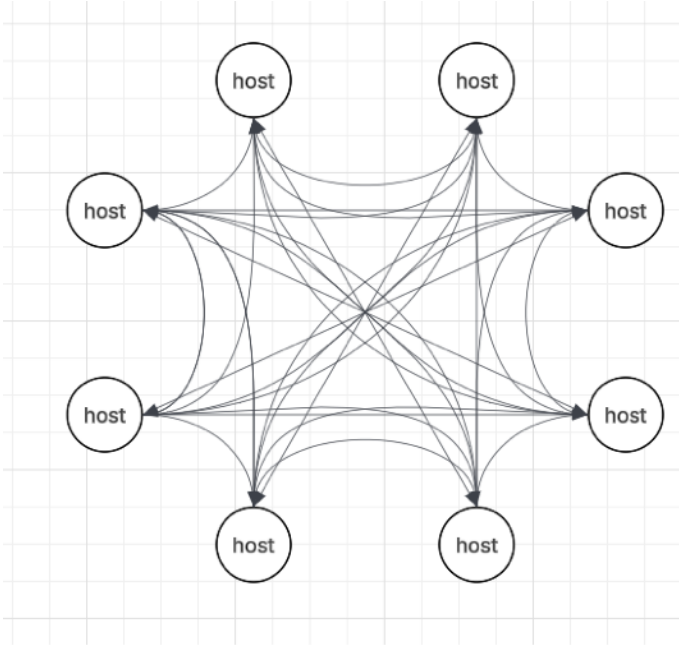


- Look for assets that lack compensating controls (unprotected/unmitigated).
- Remember the internal/back office systems! (Finance, Accounting)

# Discovering Host Context - What (and Who)



# Why Does Context Matter?



Search for a node by selecting one input or a flow by selecting two

Internal  ↓

Internal  ↓ ↑

[Clear All](#)

### Details

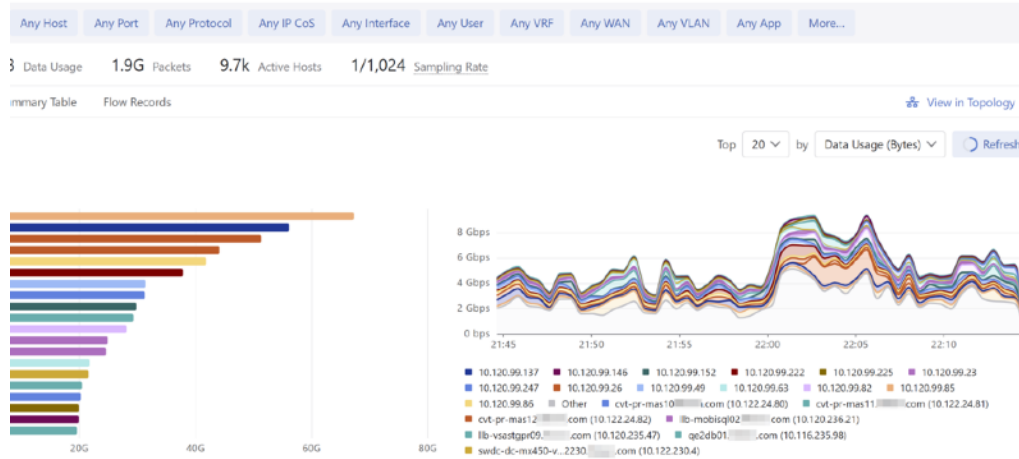
Incoming Flows	Outgoing Flows	Internal Flows
51	18	1

Top 50 ↓ by Bytes

Source	Destination	Protocol
<input type="checkbox"/> 50.9.72.32:13...	<input type="checkbox"/> 150.3.72.32:4...	UDP
<input type="checkbox"/> 170.0.0.1:400...	<input type="checkbox"/> 170.0.0.2:22 v...	TCP
<input type="checkbox"/> 51.0.0.2:5004...	<input type="checkbox"/> 225.0.0.1:190...	UDP
<input type="checkbox"/> 50.9.72.31:13...	<input type="checkbox"/> 150.3.72.31:4...	UDP

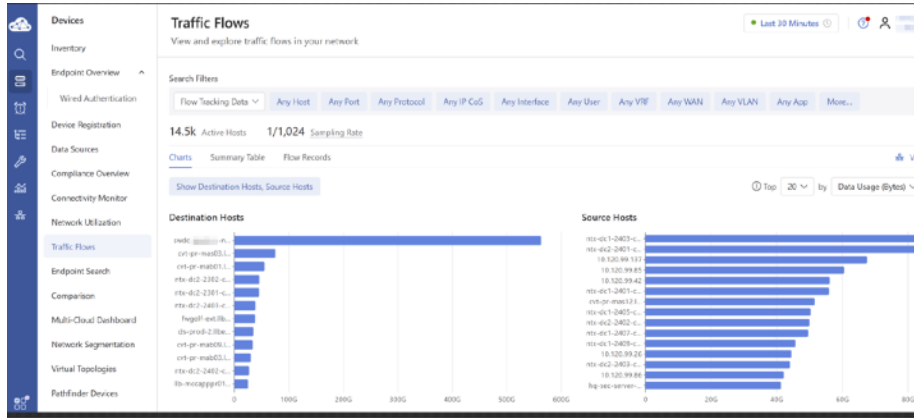
Showing 11 items

# Collecting Traffic - sFlow/Netflow



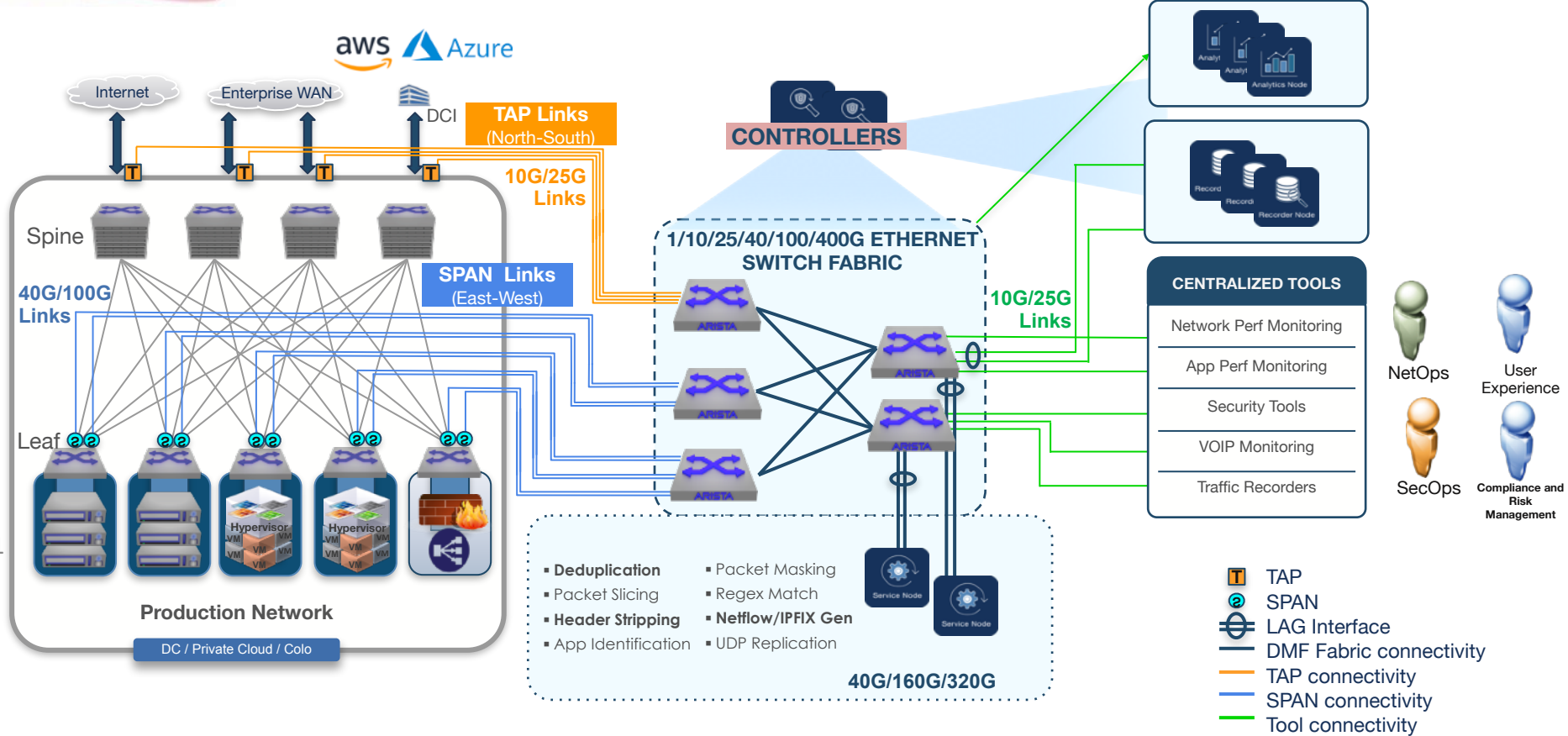
- sFlow, short for "sampled flow", is an industry standard for [packet](#) export. This includes Layer 2 (Ethernet), Layer 3 (IP), and Layer 4 (TCP/UDP)
- sFlow is a multi-vendor sampling feature that helps to monitor application mix traffic flow
- Exports counters as well as other details using a push technology rather than a poll technology like SNMP. Examples include, interface counters and CPU utilization.
- It exports random or predetermined packet samples – not actual flows as its name would imply - think "snatch and grab" of a packet header
- "sflow destination" must be set to 127.0.0.1 as TerminAttr uses an onboard sFlow collector on the device, it does not stream sFlow to CVP

# Collecting Traffic - IPFIX



- Internet Protocol Flow Information Export (IPFIX) is an [IETF standard \(RFC 7011\)](#), as well as the name of the IETF [working group](#) defining the protocol. It was created based on the need for a common, universal standard of export for [Internet Protocol flow information](#)
- Network administrators require access to flow information that passes through various network elements, for the purpose of analyzing and monitoring their networks.
- This feature provides access to IP flow information by sampling traffic flows in ingress and/or egress directions on the interfaces on which it is configured. The samples are then used to create flow records, which are exported to the configured collectors in the IPFIX format.
-

# Collecting Traffic - Tunnel In-Band/OOB Fabrics



# Building Rulesets, Validate, Deploy!

- Don't let perfect be the enemy of good.
- Default Deny fabrics are possible, but deploy with caution!

Campus\_HQ\_Policies

Policy recommendation for auditing

Domains: Campus\_Demo\_TME VRF: default ZTX: WTW340K0682

Review & Edit Rules generated 7 seconds ago

	Source	Destination	Protocol & Destination port	Services	Action	Direction
1	AGNI-20B86-Corporate_PC	AGNI-20B86-IT-Camera	TCP, 80	HTTP	forward	Bi-directional
2	AGNI-20B86-Corporate_PC	AGNI-20B86-Internet	TCP, 443	HTTPS	forward	Bi-directional
3	AGNI-20B86-IT-Camera	AGNI-20B86-IT-Badge-Reader	TCP, 4001	Badge	forward	Bi-directional
4	AGNI-20B86-IT-Camera	AGNI-20B86-IT-Sensor	UDP, 57778	Video	forward	Bi-directional
5	AGNI-20B86-IT-Badge-Reader	AGNI-20B86-IT-Sensor	TCP, 4001	Badge	forward	Bi-directional
6	AGNI-20B86-Legacy_PC	AGNI-20B86-Corporate	TCP, 22	SSH	forward	Bi-directional
7	Internal	Internal			forward-and-m...	Bi-directional

## Generate Rules

### Policy Details

Policy: Campus\_HQ\_Policies  
 Domains: Campus\_Demo\_TME  
 VRF: default

### Generate Using

Check at least one category

Category	Source	Groups
<input type="checkbox"/> Printer	AGNI-20B86	0
<input type="checkbox"/> Surgery	AGNI-20B86	0
<input type="checkbox"/> Computer	AGNI-20B86	0
<input checked="" type="checkbox"/> IOTGroup	AGNI-20B86	7
<input type="checkbox"/> Other AV	AGNI-20B86	0
<input type="checkbox"/> Brunata a	AGNI-20B86	0
<input type="checkbox"/> Other IoT	AGNI-20B86	0

Showing 33 items

## Policy Manager

Rules • Define and manage rules to use in security policies

Domains Policies Rules Groups Policy Objects

Search [ ] Policy Origin Source Destination Action Add Filter

8 Items 1 Change

Show External References Add Rule

Name	Policy	Origin	Source	Destination	Services	Action	D
rule6	Campus_HQ_Pol...	local	+1	+1	SSH	drop	B ...
rule5	Campus_HQ_Pol...	local	+1	+1	Badge	forward	B ...
rule4	Campus_HQ_Pol...	local	+1	+1	Video	forward	B ...
rule3	Campus_HQ_Pol...	local	+1	+1	Badge	drop	B ...
rule2	Campus_HQ_Pol...	local	+1	+1	HTTPS	forward	B ...
rule1	Campus_HQ_Pol...	local	+1	+1	HTTP	drop	B ...
Monitor	Campus_HQ_Pol...	local	Internal	Internal	<any>	drop-and-monitor	B ...
Default	Campus_HQ_Pol...	local	<any>	<any>	<any>	forward	B ...

# Day 2 - Operationalizing

- Continue to Incorporate Needed Rules, Remove Stale Entries
- Look to advanced security/machine learning platforms for adaptive rulesets.

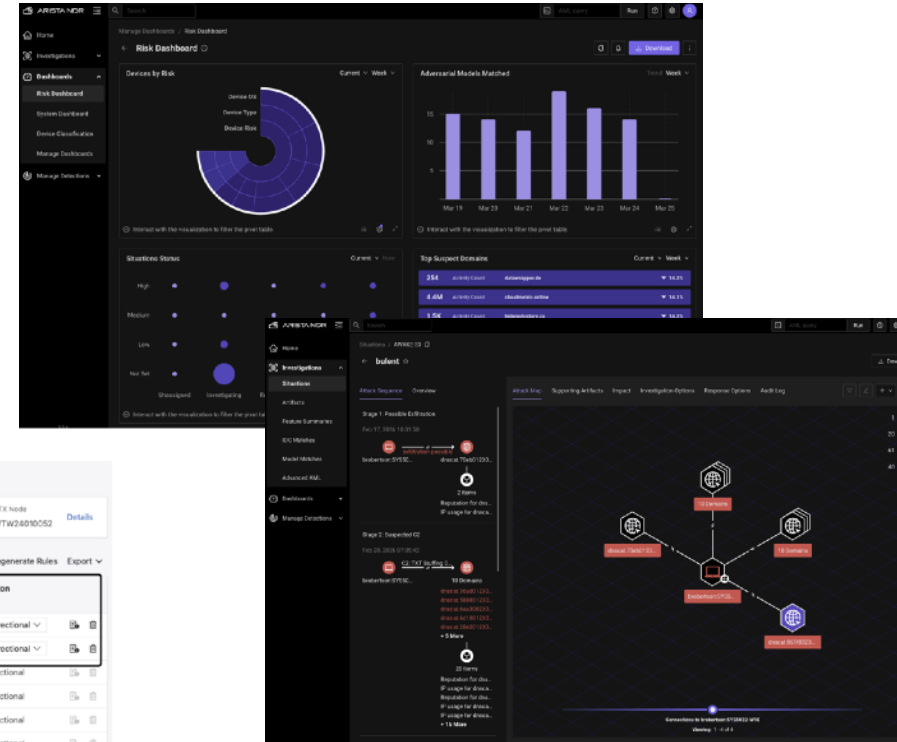
Campus\_HQ\_Policies

Domain	Verif	Policy	Source	Destination	ZTK Node	Details
Campus_Demo_TME	default	Campus_HQ_Policies	1 source	1 destination	WT424010052	

Review & Edit Rules generated 2 seconds ago

	Source	Destination	Protocol & Destination Port	Service	Action	Direction
1	ADN-20885-Legacy_PC	ADN-20886-Corporate_PC	TCP: 22	SSH	forward	Uni-directional
2	Admin	ADN-20886-Legacy_PC	TCP: 22	SSH	forward	Uni-directional
3	ADN-20885-Corporate_PC	ADN-20886-IDT-Camera	TCP: 80	HTTP	drop	Bi-directional
4	ADN-20885-Corporate_PC	ADN-20886-Internet	TCP: 443	HTTPS	forward	Bi-directional
5	ADN-20885-IDT-Camera	ADN-20886-IDT-Barcode-Reader	TCP: 4001	Barcode	drop	Bi-directional
6	ADN-20885-IDT-Camera	ADN-20886-IDT-Server	UDP: 37778	Video	forward	Bi-directional
7	ADN-20885-IDT-Camera	ADN-20886-IDT-Server	TCP: 37778	Video	forward	Bi-directional
8	ADN-2	ADN-2	TCP: 22	SSH	drop	Bi-directional
9	ADN-2	ADN-2	TCP: 22	SSH	drop-and-mon...	Bi-directional

New policy recommendation for auditing



## Data Center-Specific Approaches:

- ESG (SDN)
- EVPN GPO

## Campus-Specific Approach:

- Source Group Tags (SGT)

## Unified Approach:

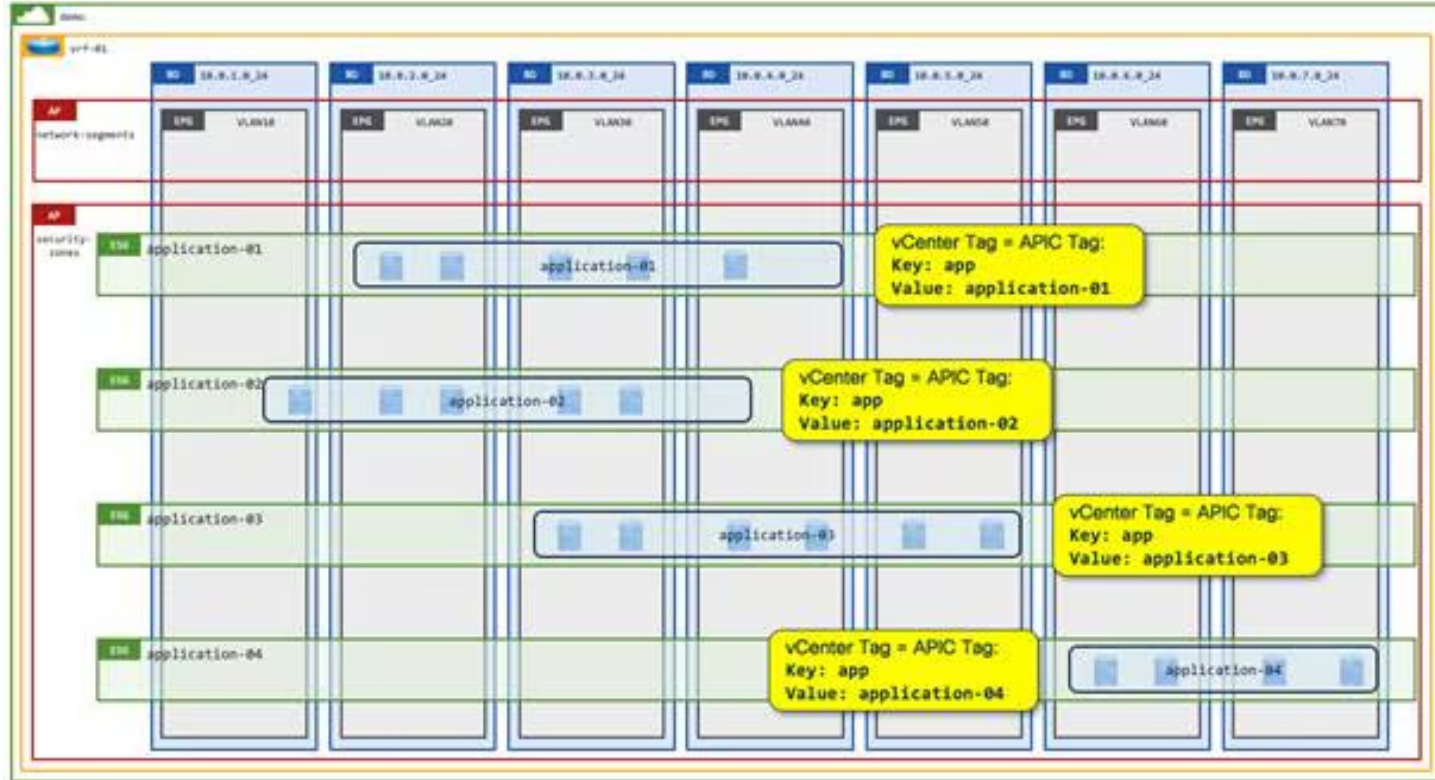
- Locally Significant SGACLs

# Implementation Frameworks - Endpoint Security Groups

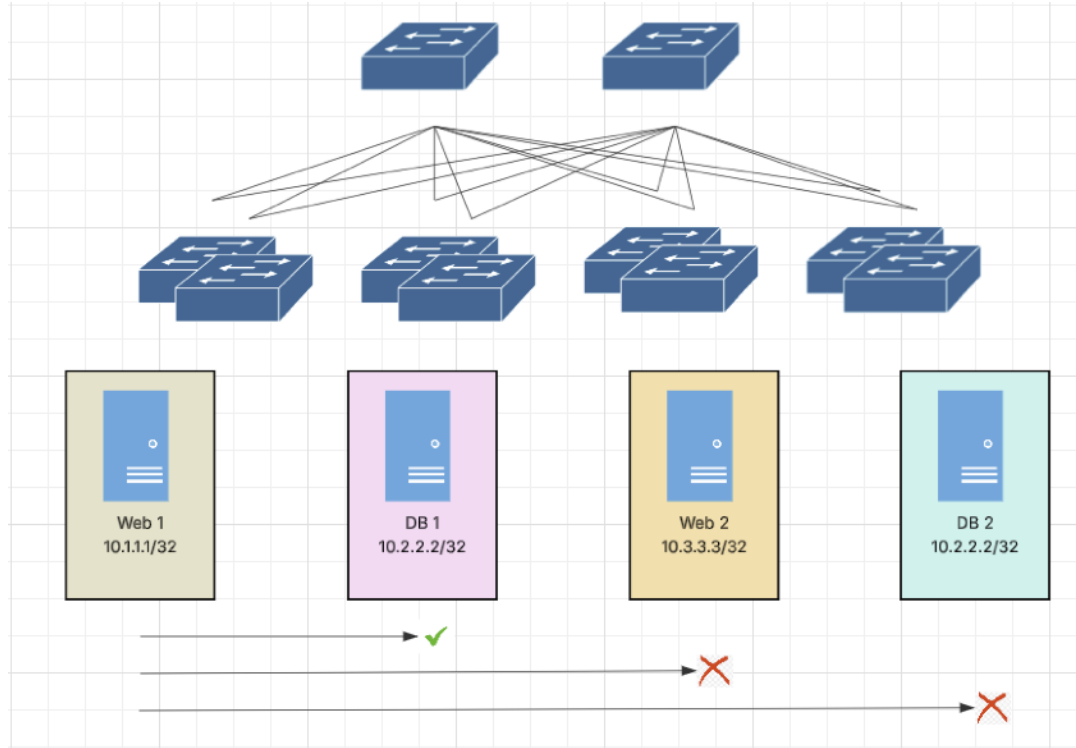
Defines a security group boundary within a VRF instance. Admission to the ESG is defined by one or more of the following methods:

- EPG Selectors – One or more EPGs can be mapped to an ESG
- Tag Selectors – Endpoints can be mapped to an ESG based on:
  - MAC address
  - IP address
  - VM name
  - VM Tag
  - IP Selectors–IP addresses can be mapped to an ESG

# Implementation Framework - Endpoint Security Groups



# Implementation Framework - EVPN Group Policy



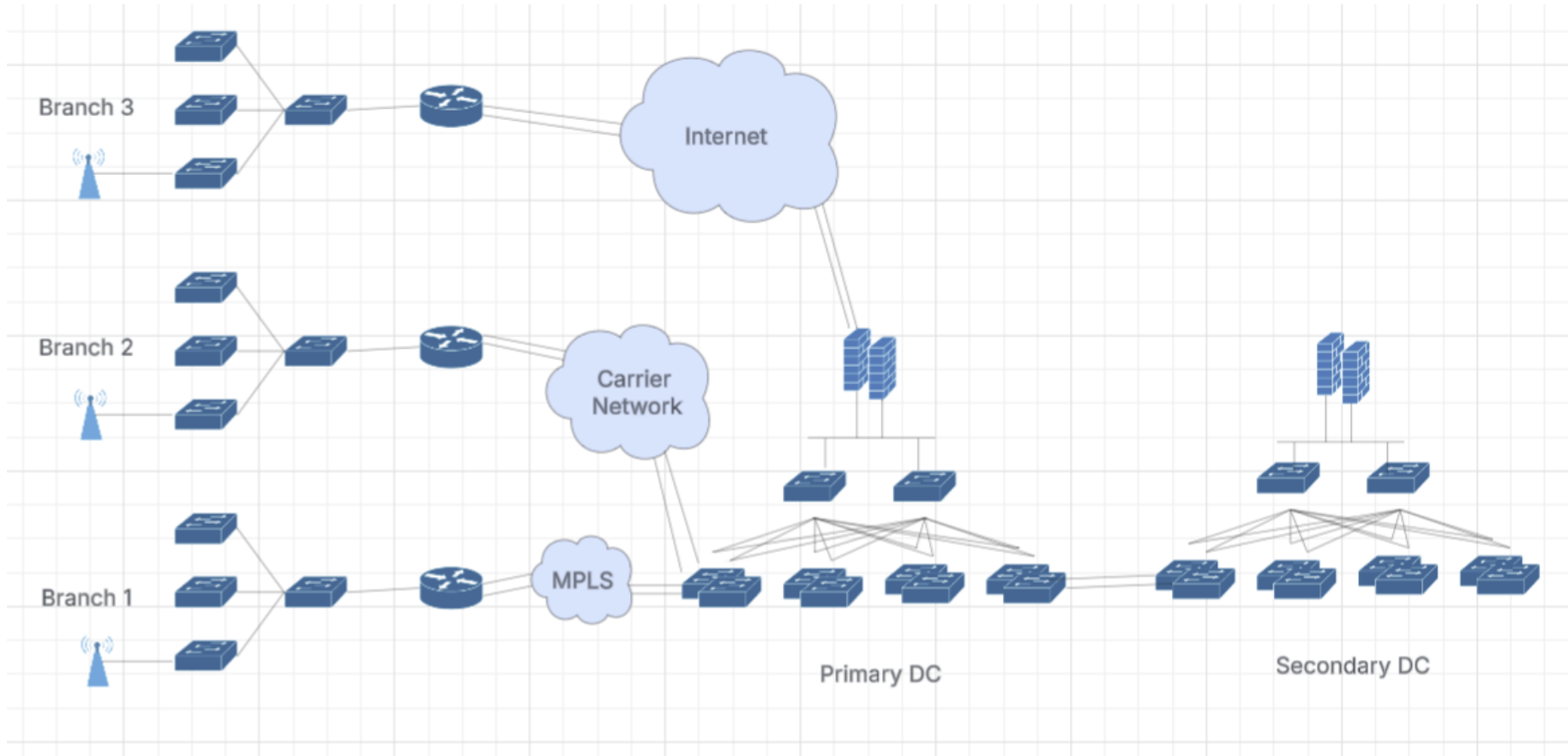
draft-lrсс-bess-evpn-group-policy-00

# Implementation Framework - Source Group Tags (Campus)

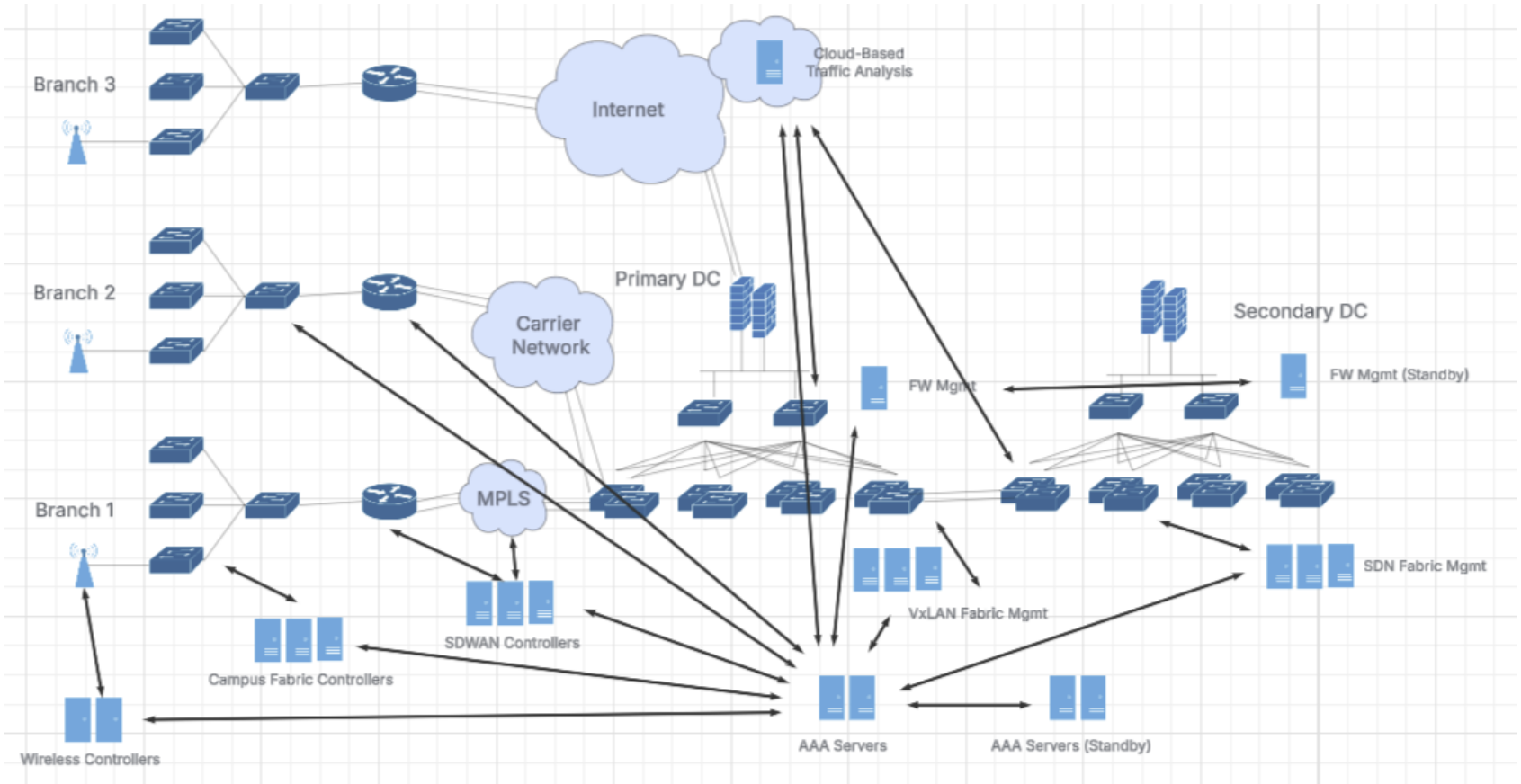
- Each security group is assigned a unique 16-bit tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is propagated between devices allowing any intermediary devices (switches, routers) to enforce policies based on the identity tag.
- Source SGT and destination SGT should be known at the enforcement point, which is at fabric egress.
- Not all manufacturers recognize this tag, some see it as a corrupted ethernet frame and drop. Path MTU may also be a consideration.
- SGTs can be communicated in the data plane (preferred), or control plane via SXP.
- SGTs only support individual IP addresses; no current support for tagging of subnets or summary routes.

Careful planning must be done to ensure that either 1) the underlying infrastructure supports SGT across all potential forwarding paths or 2) workarounds are in place (GRE and/or IPSec).

# Base Topology



# End-to-End SGT Implementation w VxLAN GPO



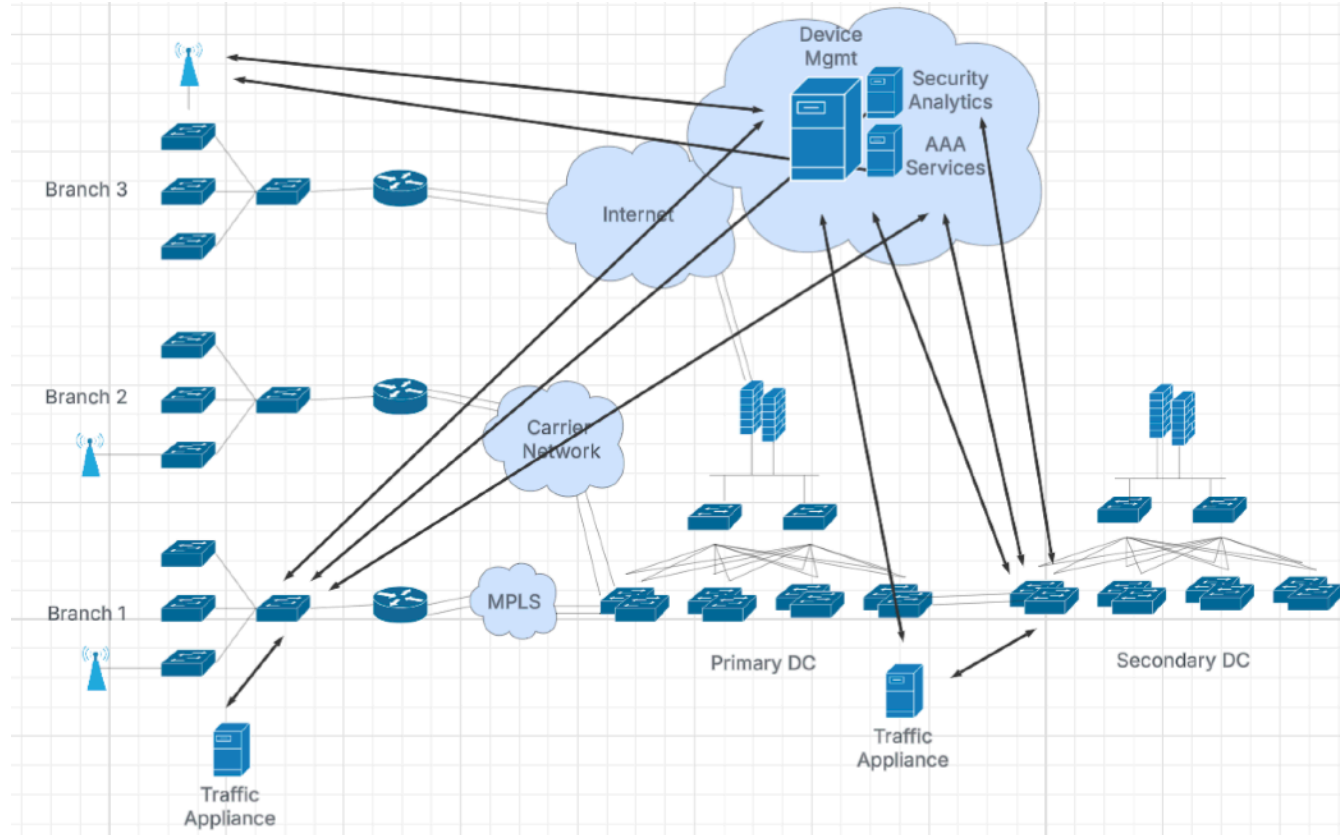
# Components of an SGACL Implementation

- Devices may have a connection to a single monitoring/management platform.
- Devices may use that connection to install locally significant SGACL tags on every switch.
- Traffic is forwarded (or blocked) on the switches in hardware, at up to wire-speed.

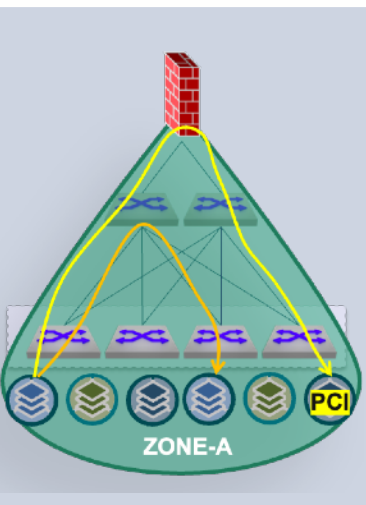
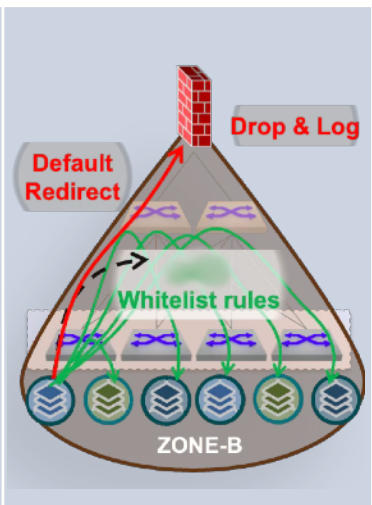
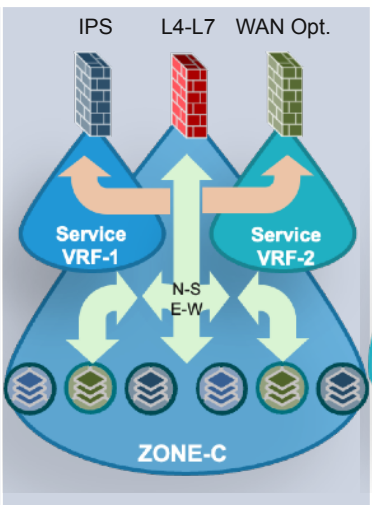
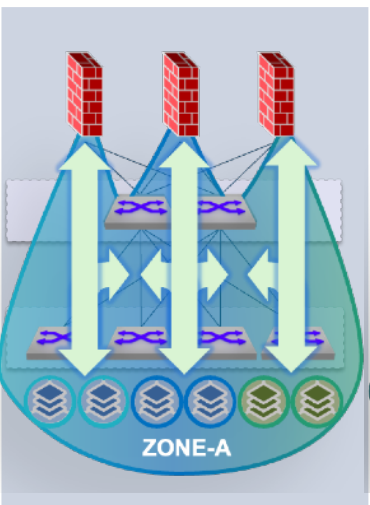
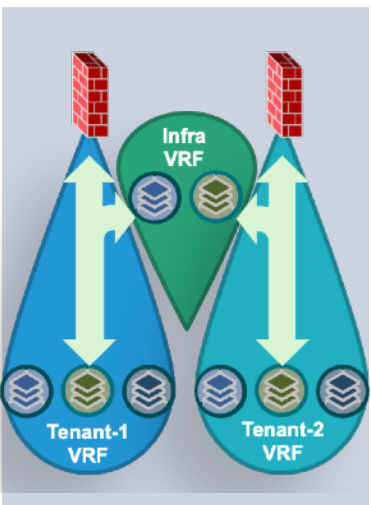
## Other Items of Note:

- All devices (switches and APs) will have a RADIUS/RadSec connection to AAA services.
- Via GRE, switches will tunnel full packets or slices to local appliances for analysis, which then may be aggregated by a centralized platform.
- For deeper analysis, a local service may stream packets to a local or cloud-based security platform for advanced analytics and automated response.

# SGACL DC/Campus Microsegmentation Implementation Example



# Real Environments - Combination of Macro/Microseg

Selective Compliance	Logging Zero Trust Violations	Service Chaining (L4-7 Svc Insertion)	Firewall Load Balancing	Shared Services
				
<p>Selective stateful inspection of PCI compliant applications</p>	<p>Hairpin traffic that does not match existing whitelist to dedicated FW interface for <b>drop &amp; log</b></p>	<p>Selective steering to defined inspection service chains, e.g. regular L4-L7, IPS, WAN optimizer</p>	<p>Intelligent load balancing to multiple independent FWs (scale-out FW)</p>	<ul style="list-style-type: none"> <li>• Policy-based inter-VRF communication</li> <li>• Per tenant FW redirection</li> </ul>

Thank you!

[jtobias@arista.com](mailto:jtobias@arista.com) - [linkedin.com/in/jaysont](https://www.linkedin.com/in/jaysont)