Strategies in Network Microsegmentation

MONUG - North Kansas City, MO - 1 April 2026

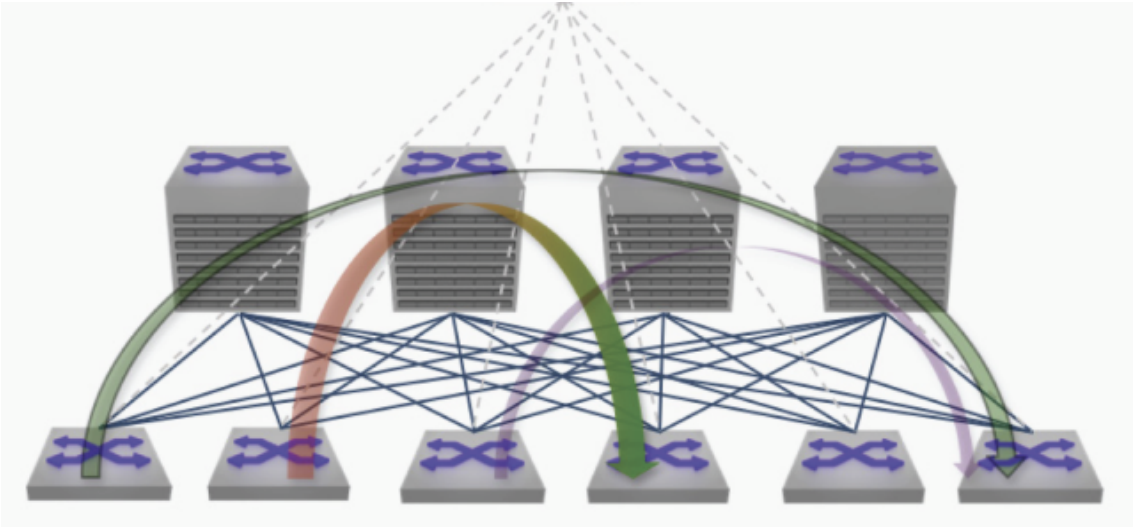
Jayson Tobias, SE - Arista Networks

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

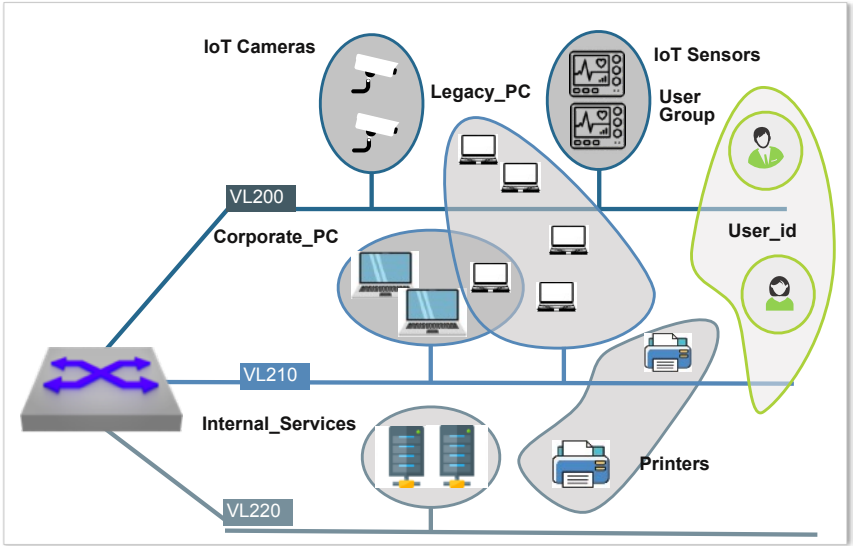
Why Segmentation?

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

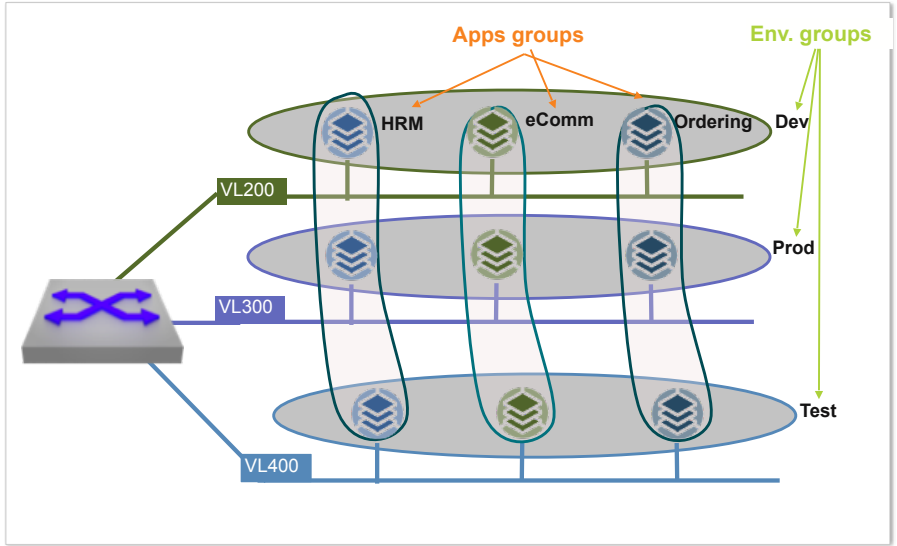


Today's Focus - Microsegmentation

Campus & Branch Endpoint Microperimeters



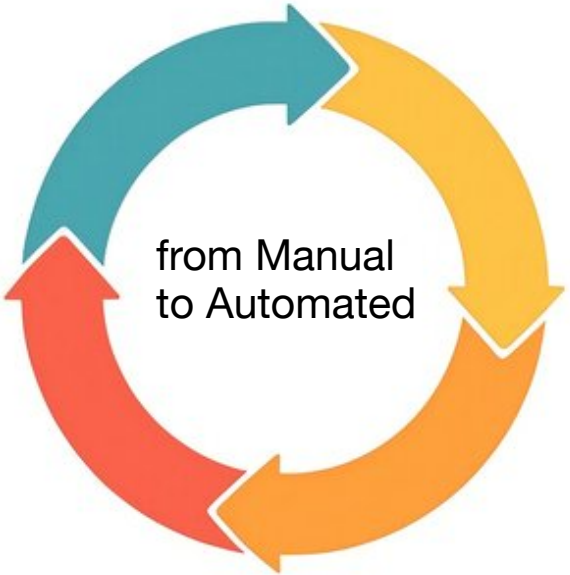
Datacenter Workload Microperimeters



Microsegmentation Lifecycle

(Re-)Assess Assets

Analyze Traffic Patterns

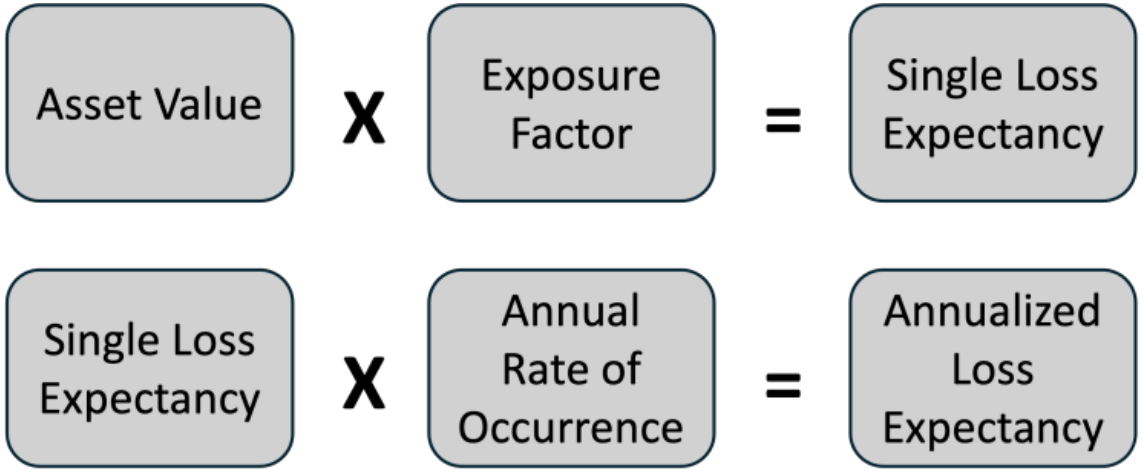


Adjust Network Traffic Policies

Develop, Test, Validate Rulesets

Where to start?

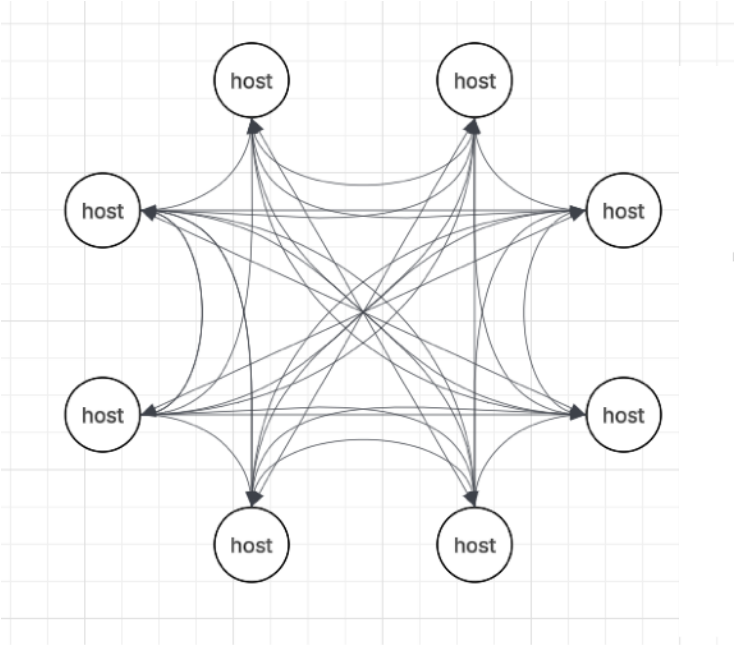
- Calculate Organizational Risk

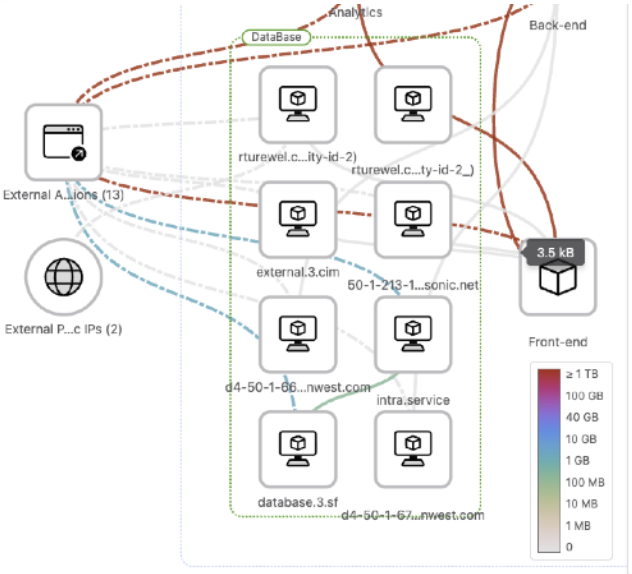


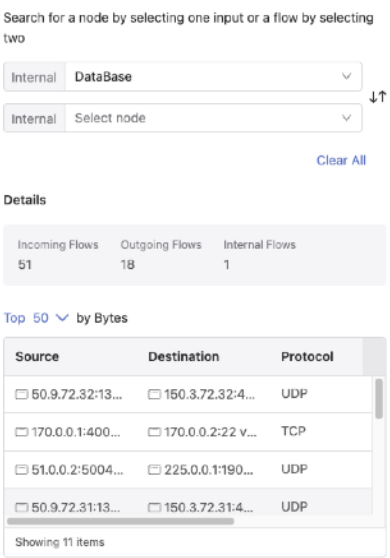
- Look for assets that lack compensating controls (unprotected/unmitigated).
- Remember the internal/back office systems! (Finance, Accounting)

Discovering Host Context - What (and Who)

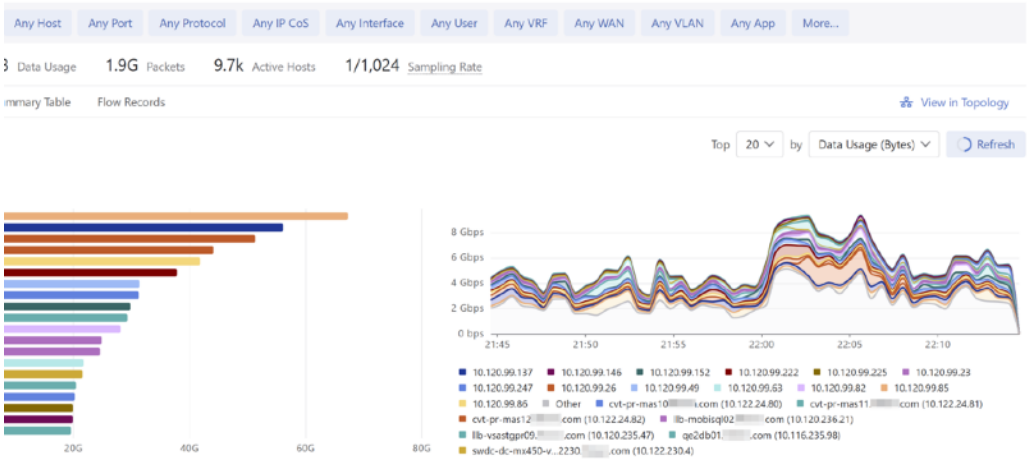
Why Does Context Matter?





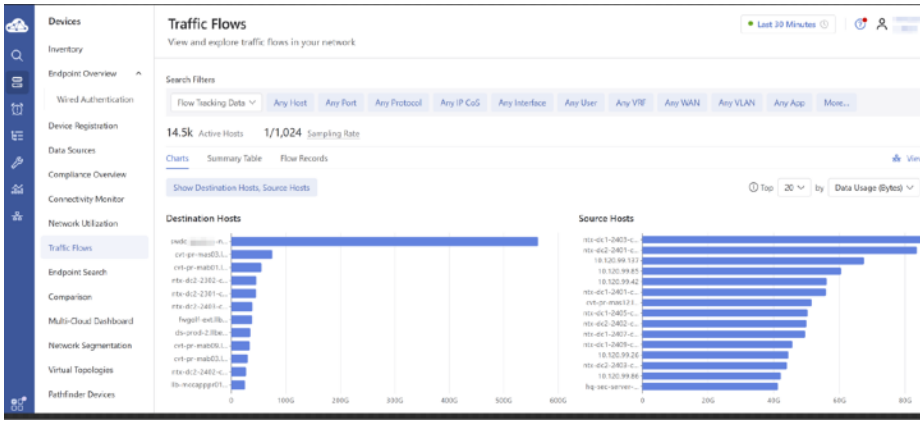


Collecting Traffic - sFlow/Netflow



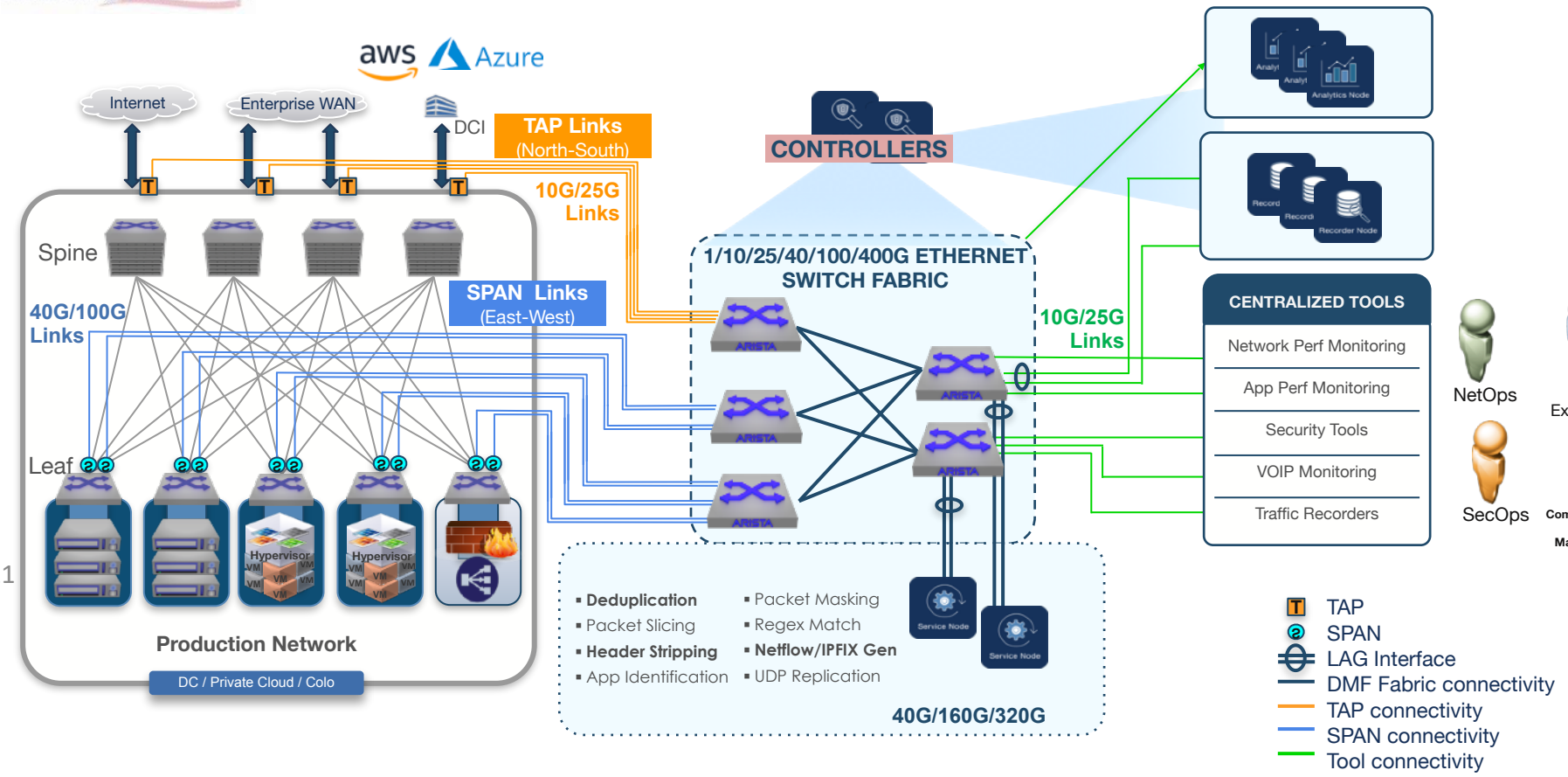
- sFlow, short for "sampled flow", is an industry standard for packet export. This includes Layer 2 (Ethernet), Layer 3 (IP), and Layer 4 (TCP/UDP)
- sFlow is a multi-vendor sampling feature that helps to monitor application mix traffic flow
- Exports counters as well as other details using a push technology 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



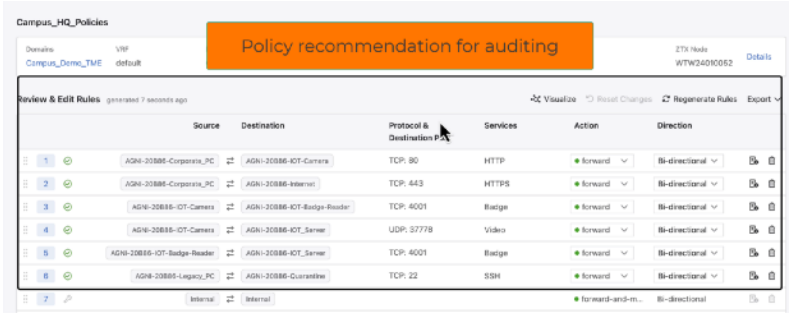
- Internet Protocol Flow Information Export (IPFIX) is an IETF standard (RFC 7011), as well as the name of the IETF working group defining the protocol. It was created based on the need for a common, universal standard of export for Internet Protocol flow information
- Network administrators require 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.
-

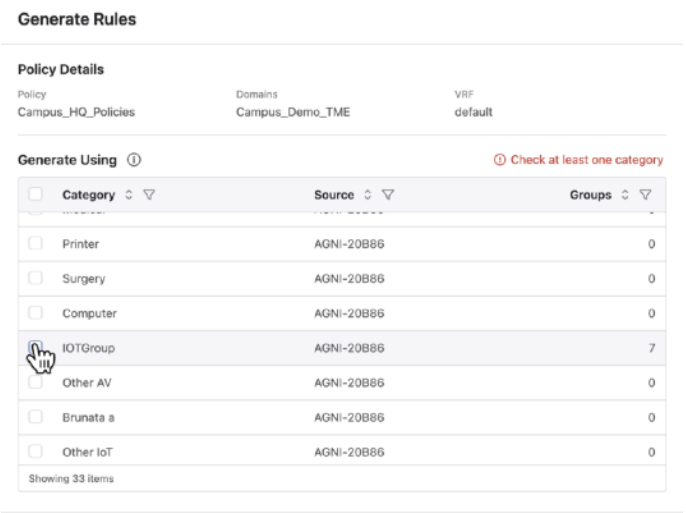
Collecting Traffic - Tunnel In-Band/OOB Fabrics

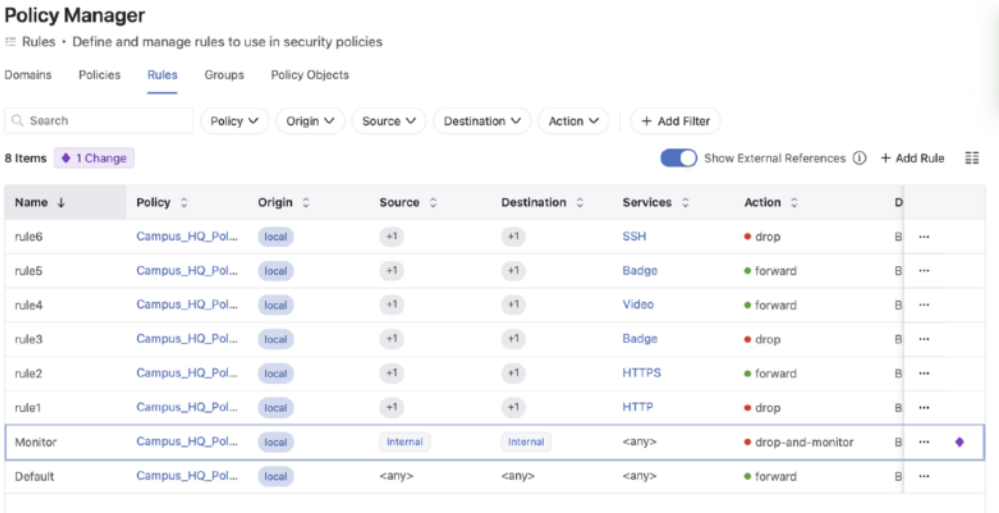


Building Rulesets, Validate, Deploy!

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

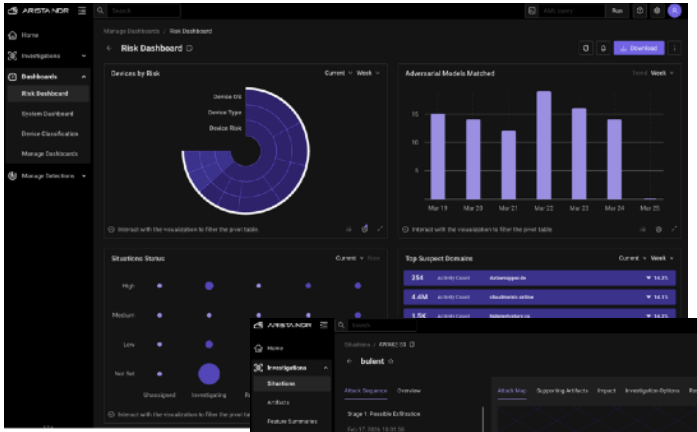


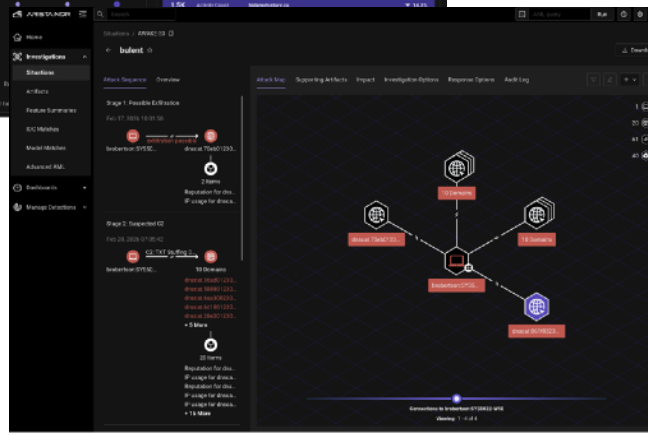


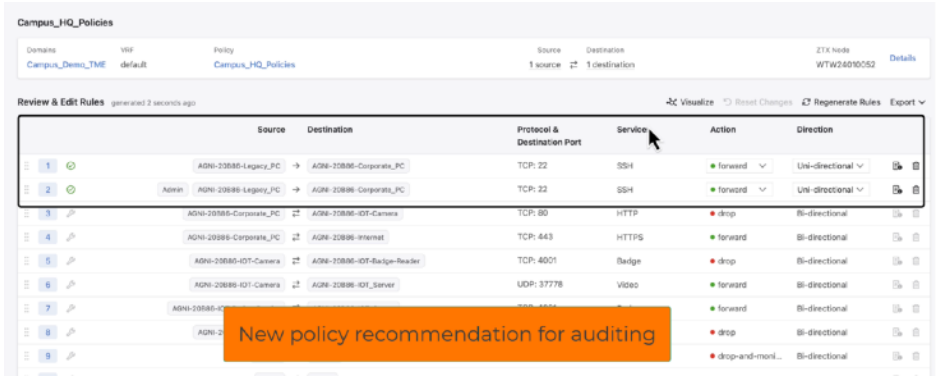


Day 2 - Operationalizing

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







Implementation Frameworks

Data Center-Specific Approaches:

- ESG (SDN)
- EVPN GPO

Campus-Specific Approach:

- Source Group Tags (SGT)

Unified Approach:

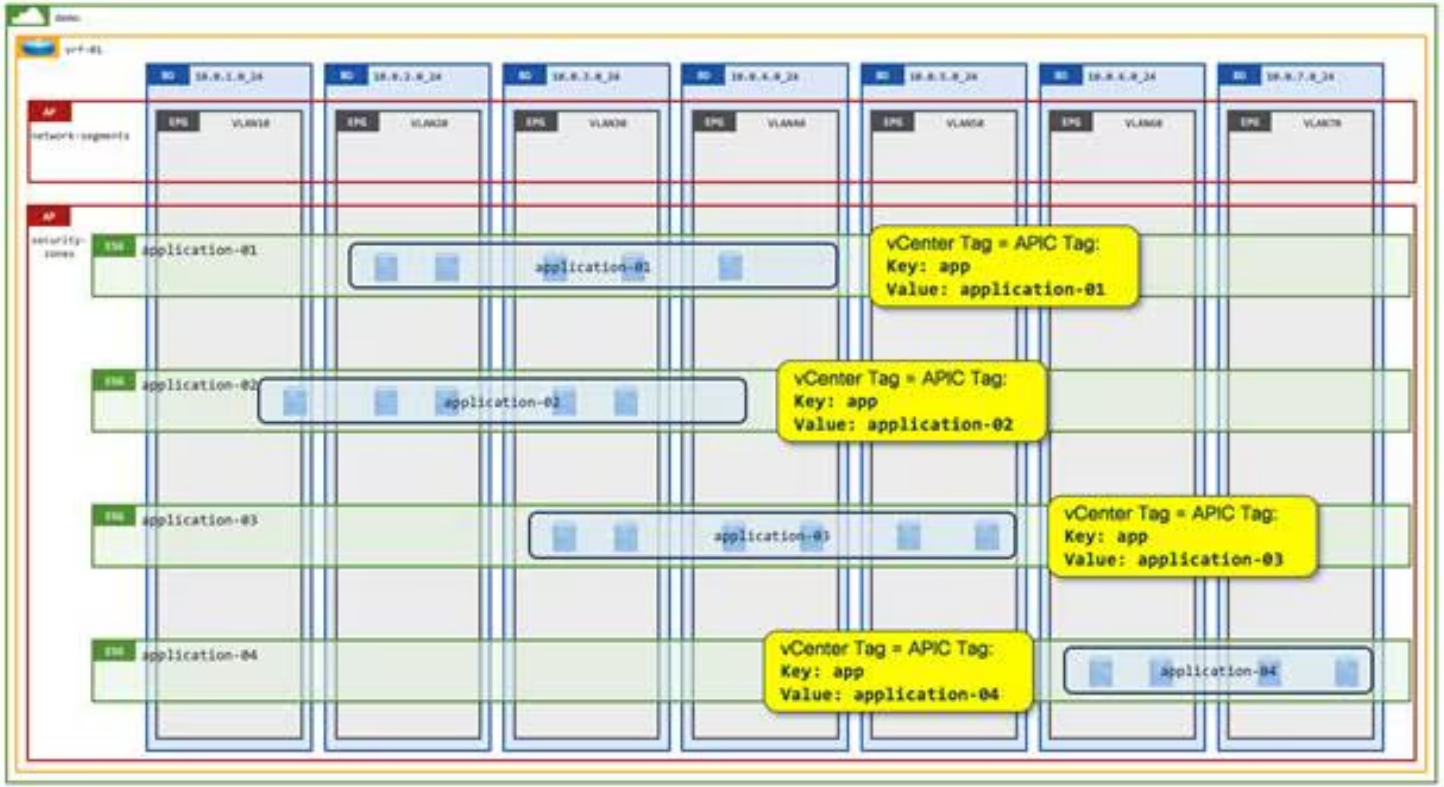
- Locally Significant SGACLs

Implementation Frameworks - Endpoint Security Groups

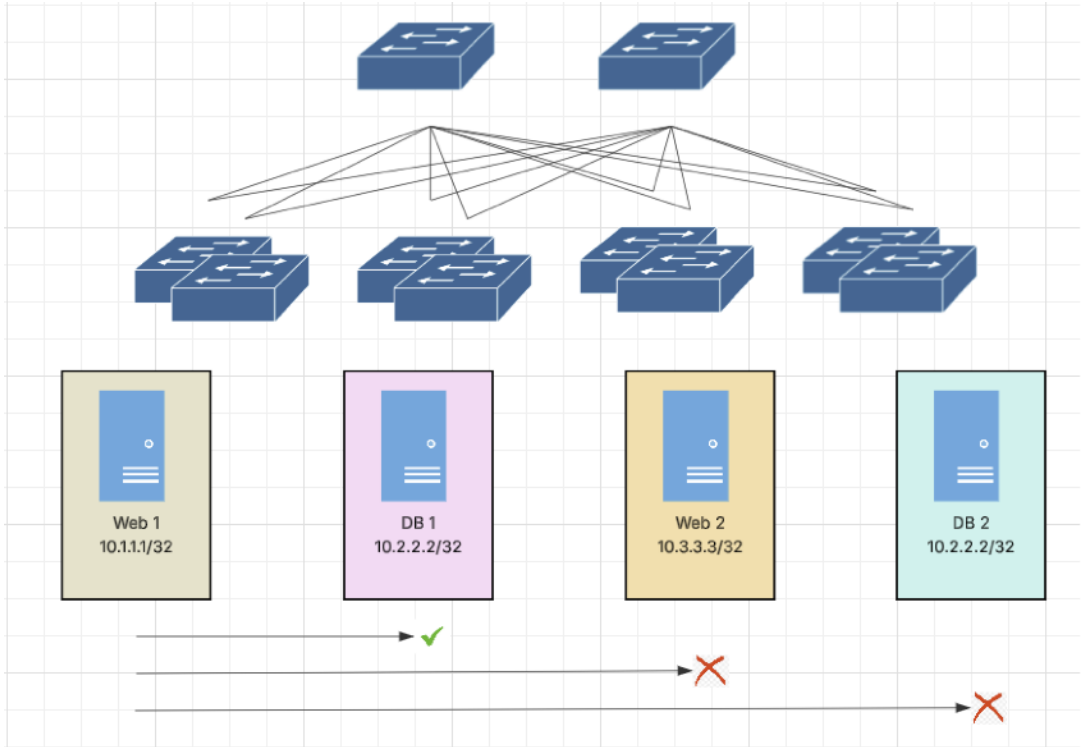
Defines a security group boundary within a VRF instance. Admission to the ESG is defined by one or more of the following methods:

- 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



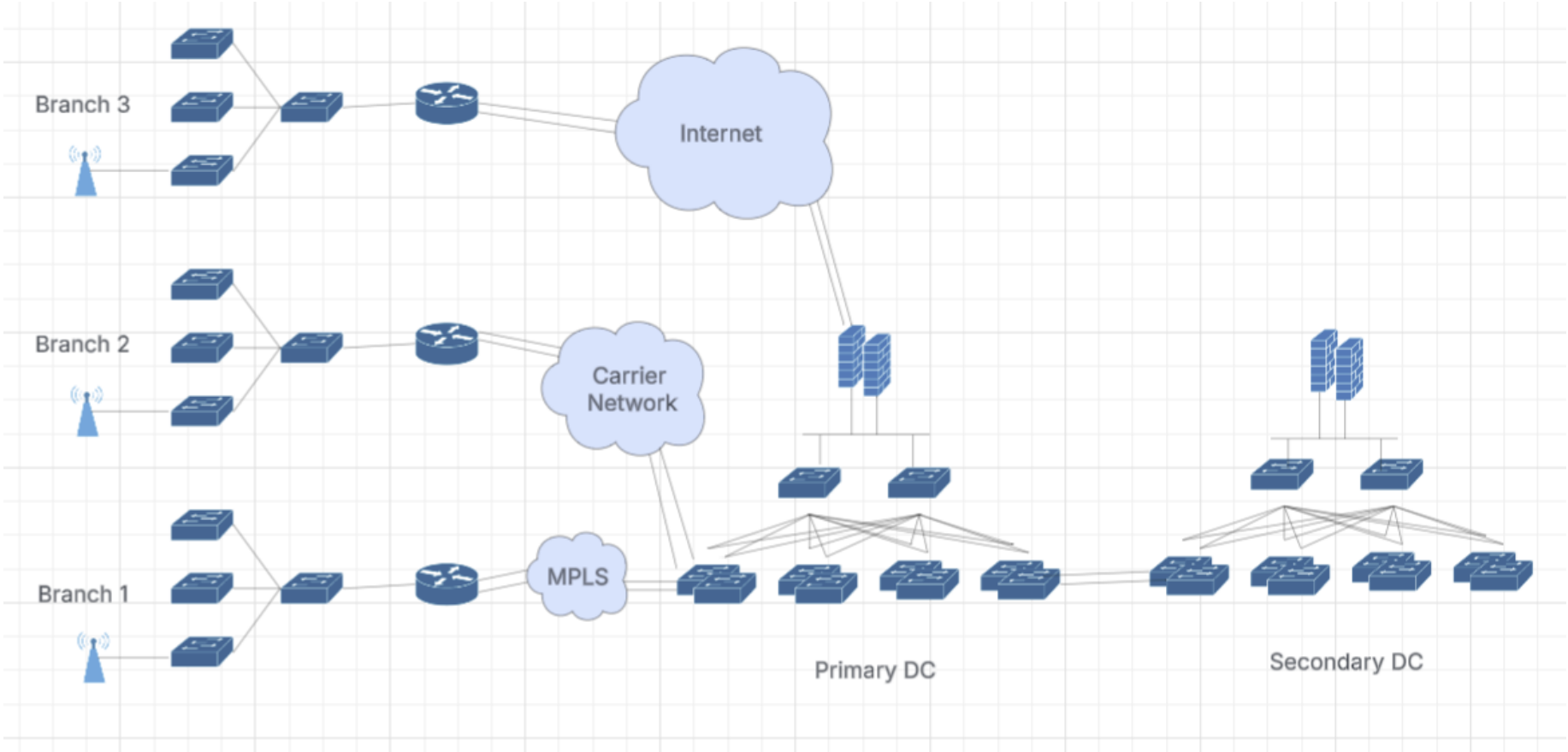
draft-lrss-bess-evpn-group-policy-00

Implementation Framework - Source Group Tags (Campus)

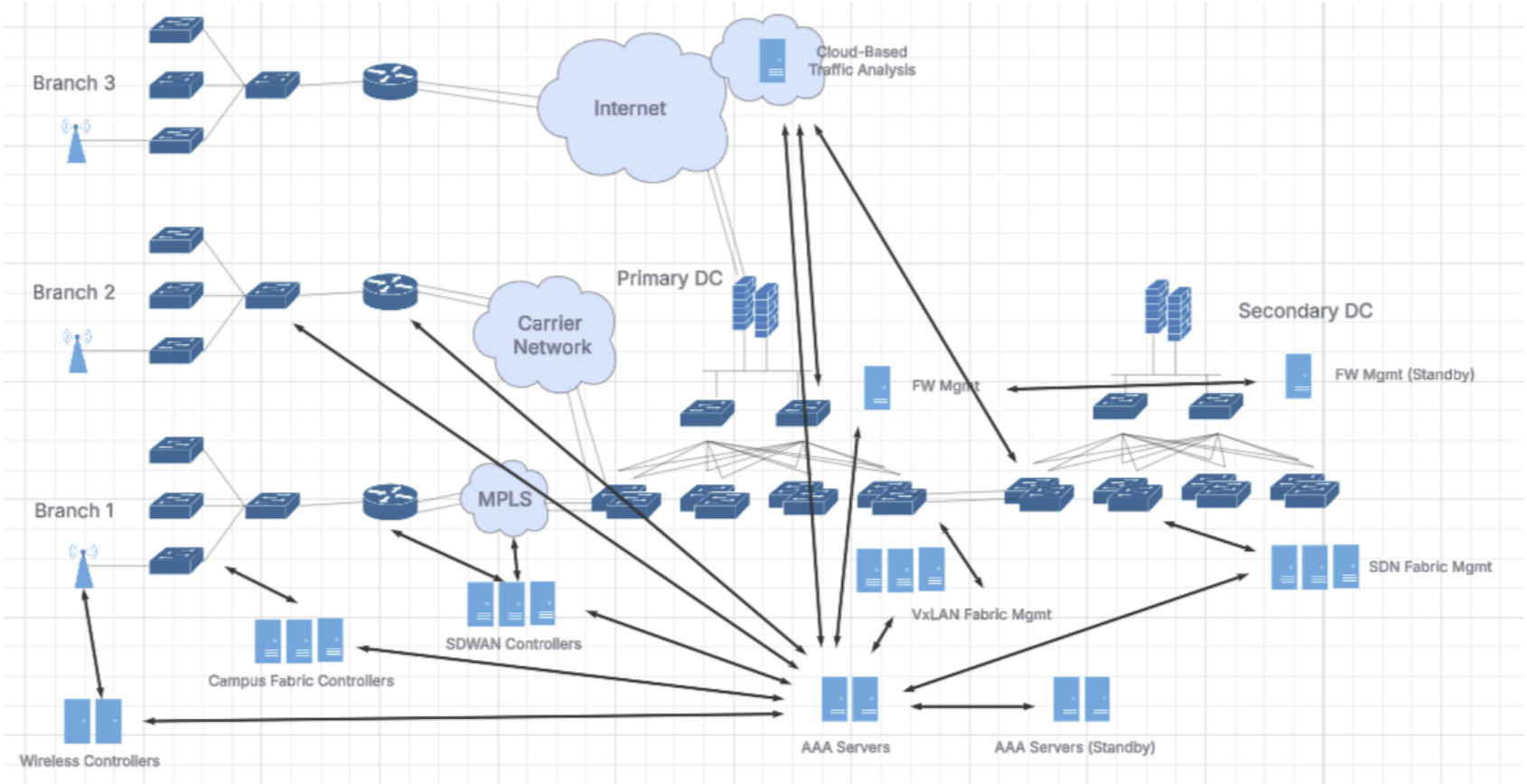
- Each security group is assigned a unique 16-bit tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is propagated between devices allowing any intermediary devices (switches, routers) to enforce policies based on the identity tag.
- Source SGT 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



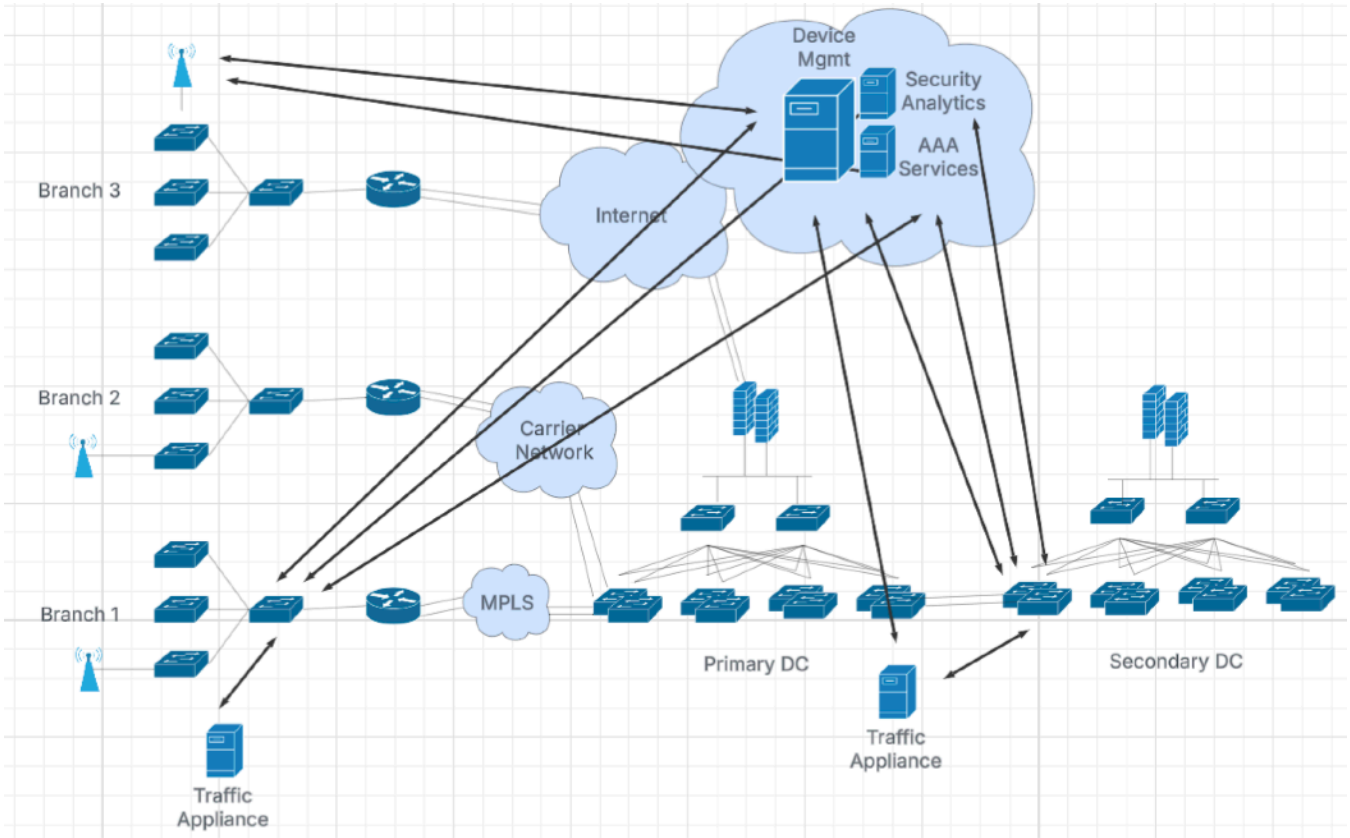
Components of an SGACL Implementation

- 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.

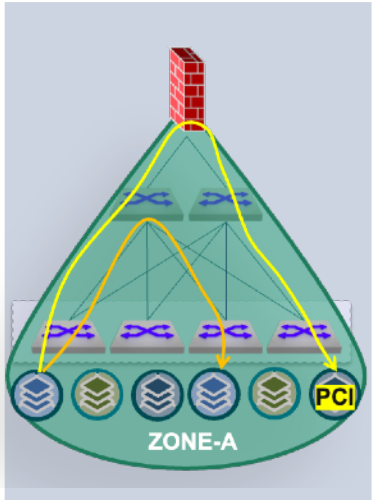
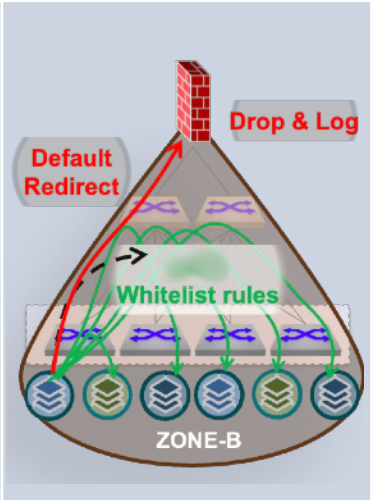
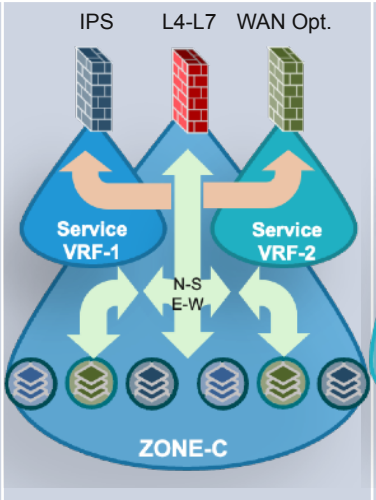
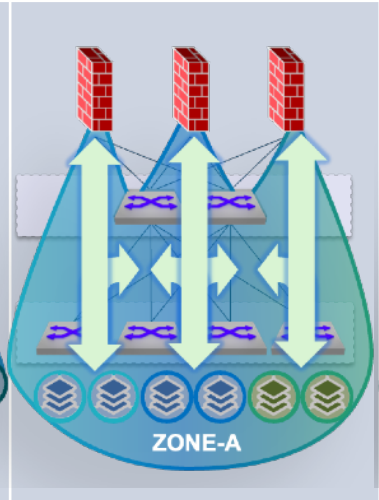
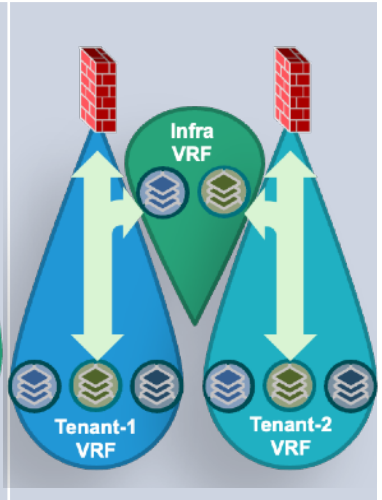
Other Items of Note:

- 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
				
Selective stateful inspection of PCI compliant applications	Hairpin traffic that does not match existing whitelist to dedicated FW interface for drop & log	Selective steering to defined inspection service chains, e.g. regular L4-L7, IPS, WAN optimizer	Intelligent load balancing to multiple independent FWs (scale-out FW)	• Policy-based inter-VRF communication • Per tenant FW redirection

Thank you!

jtobias@arista.com - linkedin.com/in/jaysont