Advanced Security Group Tags

Multi Domain Context

Darrin Miller
Distinguished TME
@vancspr

Agenda

01 Cisco Live Housekeeping

02 Security Group Tag (SGT) Review

03 Use Case Review and SGT Detail

- Campus/Branch
- Hybrid Work
- IaaS/Data Center

04 Summary

Cisco Webex App

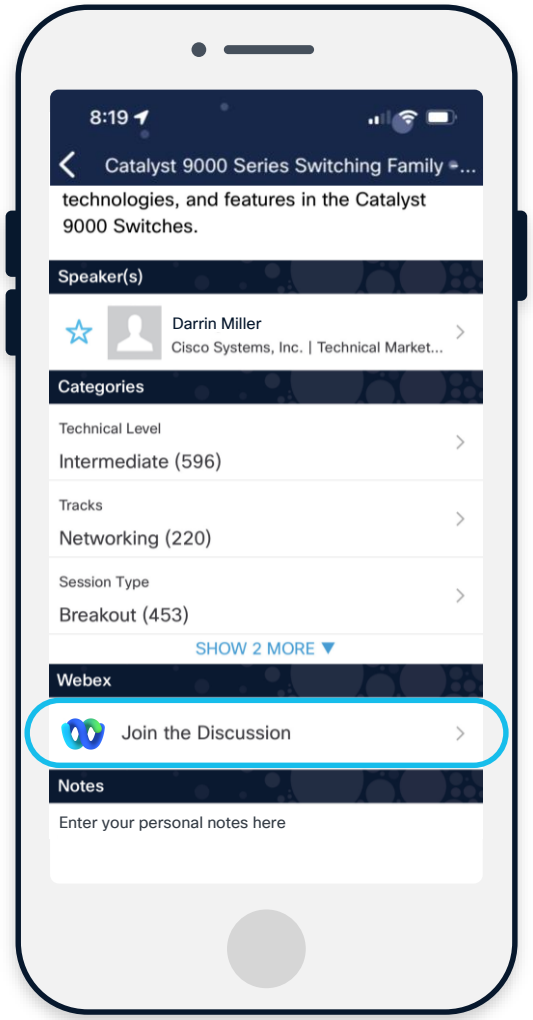
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



Abstract

- This session examines the use cases for Security Group Tags (SGTs) and how SGTs have evolved into the defacto language for security policy within Cisco and the industry.
- SGT uses software defined networking abstractions to enable scaling of network security within enterprises for a Universal Zero Trust Network Access (UZTNA) solution.
- This session will review lower level design, configuration, monitoring and troubleshooting of SGTs and SGACLs applied to use cases like user/device segmentation, IaaS and SaaS policy controls as well malware mitigate Security Group technology will be discussed as applied to LAN, WLAN, WAN and Data Center networks.
- This session is aimed at Network/Network Security Specialists and Architects involved in designing and building advanced security solutions scenarios using Cisco network and security appliance deployment models.
- Attendees should be familiar with SGTs, Cisco routing, switching, wireless and security appliances at a conceptual level and a detail knowledge of one of those disciplines.
- Suggested prior sessions include sessions on the Identity Services Engine (ISE), SDA, Segmentation and network authentication (802.1X on wired and WLAN).

Objectives: Understand Security Group Tag Advanced Concepts

About Me

Darrin Miller

- Security focused Technical Marketing Engineer
- Focused on Security Architecture, Policy, and Threat
- Author of Books, CVDs, Whitepapers, Patents, etc.
- Cisco Live Distinguished Speaker Hall of Fame Elite
- 20+ years at Cisco: Research, Development, TME

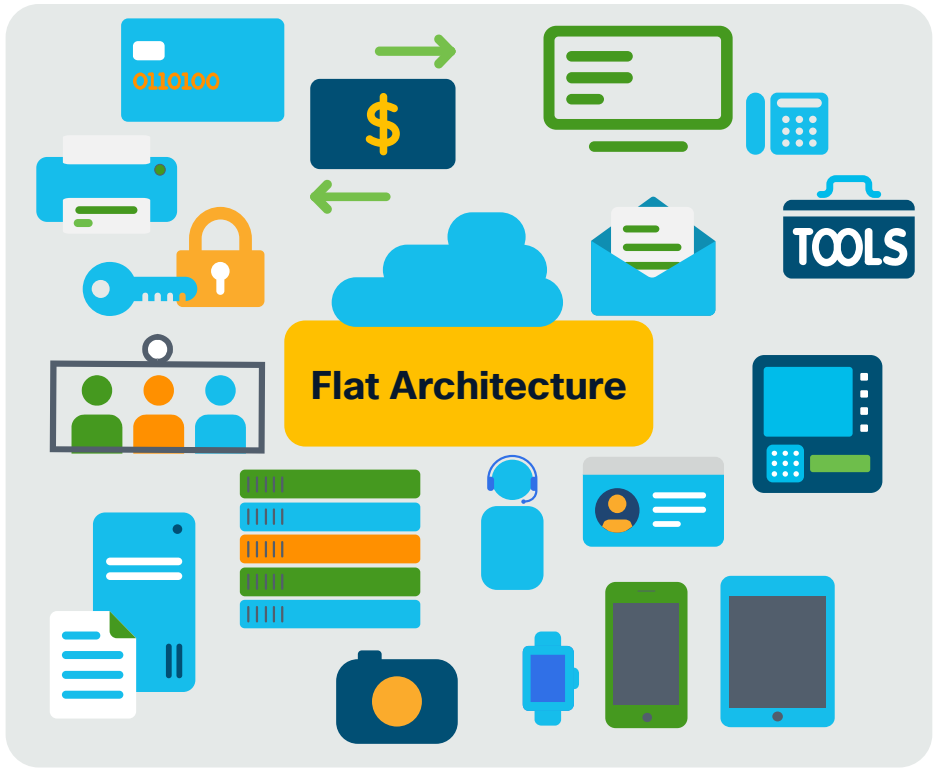
For your reference

- There are slides in your PDF that will not be presented, or quickly presented
- They are valuable, but included only “For your reference”

Security Group Tag (SGT) Review

Customer Goal – Transition from Flat Network to Zero Trust Segmentation

Current State



Zero Trust Segmentation State

As Published by Cisco Press Book: "Zero Trust Architecture"

Zero Trust Principles

Cisco’s Zero Trust capabilities

Establish Trust

- User / device / service identity
- Posture + context
- Risk-based authentication

Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Behavior monitoring – threat and non-threat activity
- Vulnerability management

Respond to Change in Trust

- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

Never Assume Trust → Always Verify → Enforce Least Privilege

Can You See the Business Intent here?

```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
```

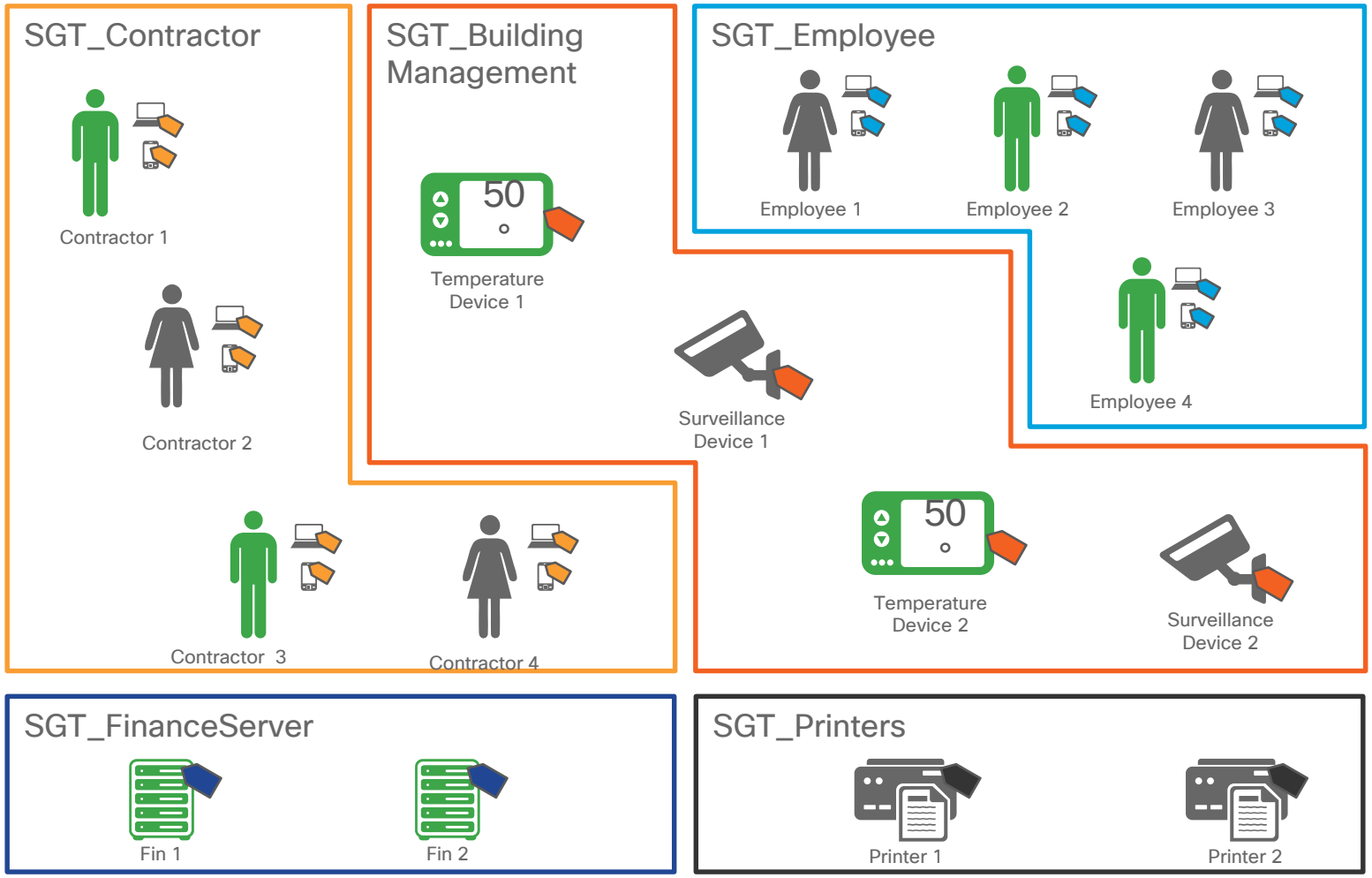
Business Intent is Clear

With meaningful group-based policies aligned to business needs


```
Edge-Cat9300#show cts role-based permissions
IPv4 Role-based permissions default:
        Deny IP-00
IPv4 Role-based permissions from group 19:nvr to group 24:ipcamera
        Permit IP-01
IPv4 Role-based permissions from group 9:Employees to group 23:ipcamera
        Deny IP-00
```

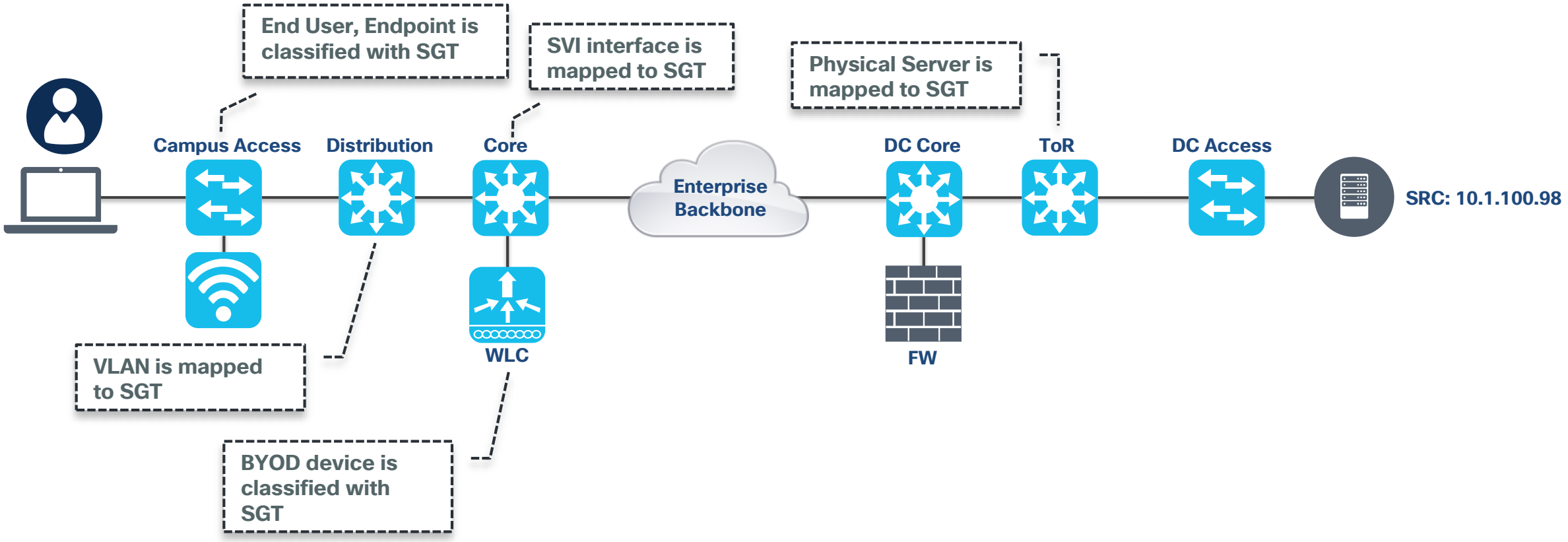
Classification into Functional Groups

- Business-based groupings to provide consistent policy and access independent of network topology
- Leverage items such as location, device type, RADIUS attributes, AD membership etc. to allocate group assignments



Classify where appropriate for the use case

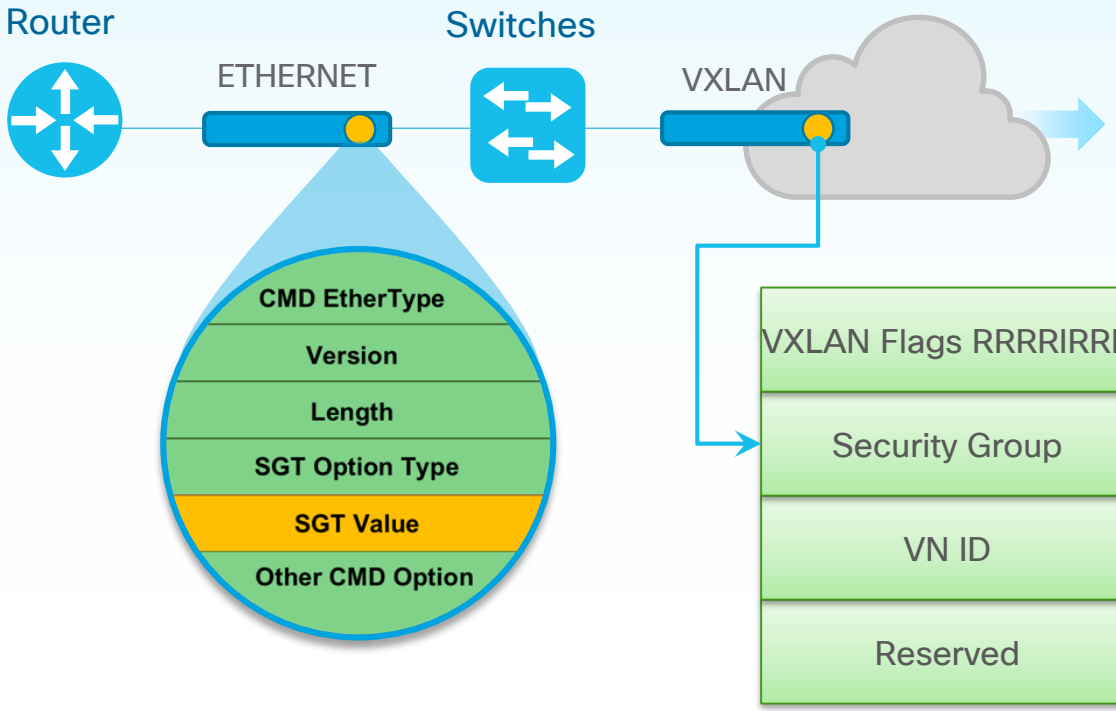
- Based on the assets to protect – identify where we need to classify



Propagation Methods (Inline)

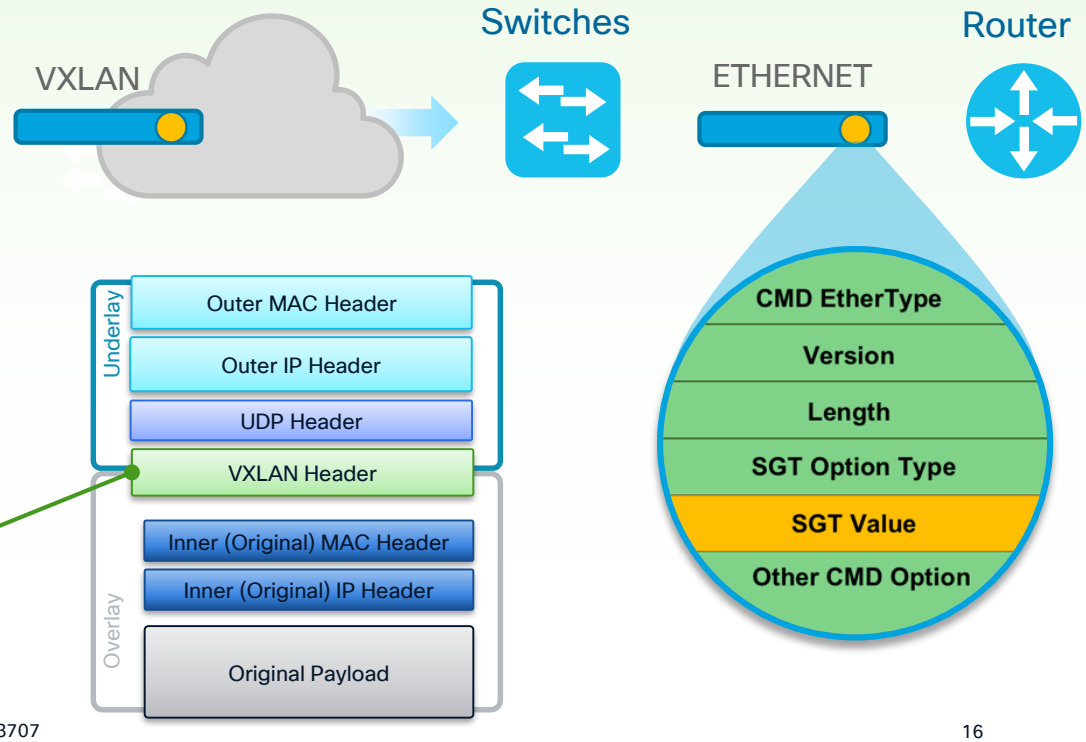
Inline Methods (Micro)

- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT encapsulated within Cisco Meta Data (CMD) payload
- **IPsec / L3 Crypto:** SGTs are carried inside IPsec header
- **VXLAN:** SGT (16 bit) inserted into Segment ID of VXLAN Header



Inline Methods (Macro)

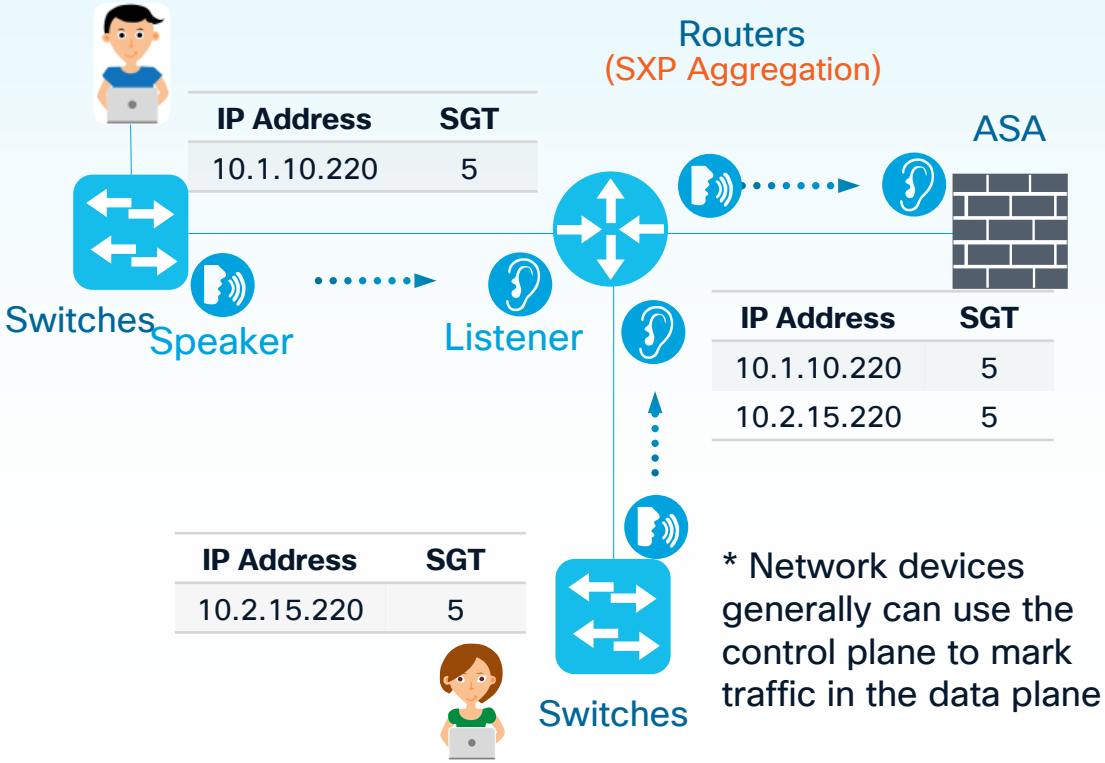
- **802.1Q:** VRF is mapped to VLAN via VRF-Lite
- **IPsec:** VRF/VPN
- **VXLAN:** VXLAN Network Identifier (VNI)



Propagation Methods (Control-/Management Plane)

SGT eXchange Protocol (SXP)*

- IP-to-SGT binding exchange over 64999/TCP
- Cisco ISE can be an SXP Speaker / Listener
- SXP5 is VRF-aware. An ISE SGT Domain represents a VN/VPN/VRF



* Network devices generally can use the control plane to mark traffic in the data plane

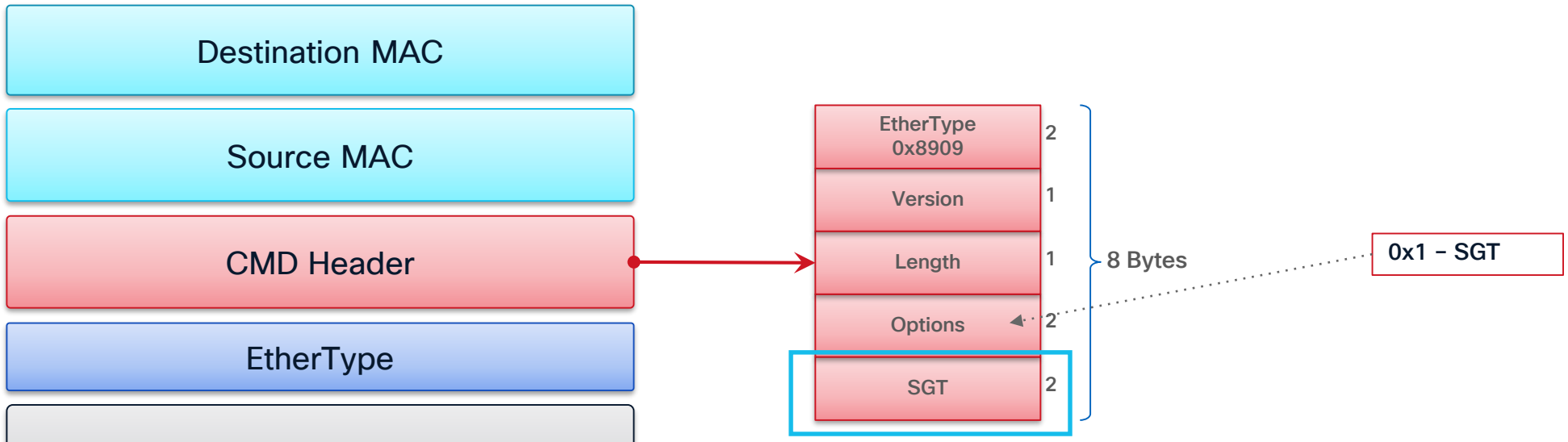
Platform eXchange Grid (pxGrid)

- **Cisco and 3rd party Ecosystem:** Context-out, Context-in, Adaptive Network Control (Threat Mitigation)
- Subscribers can consume SGT Domains (VN/VPN/VRF) as part of the pxGrid SXP Topic

CMD Header

L2 Ethernet Frame

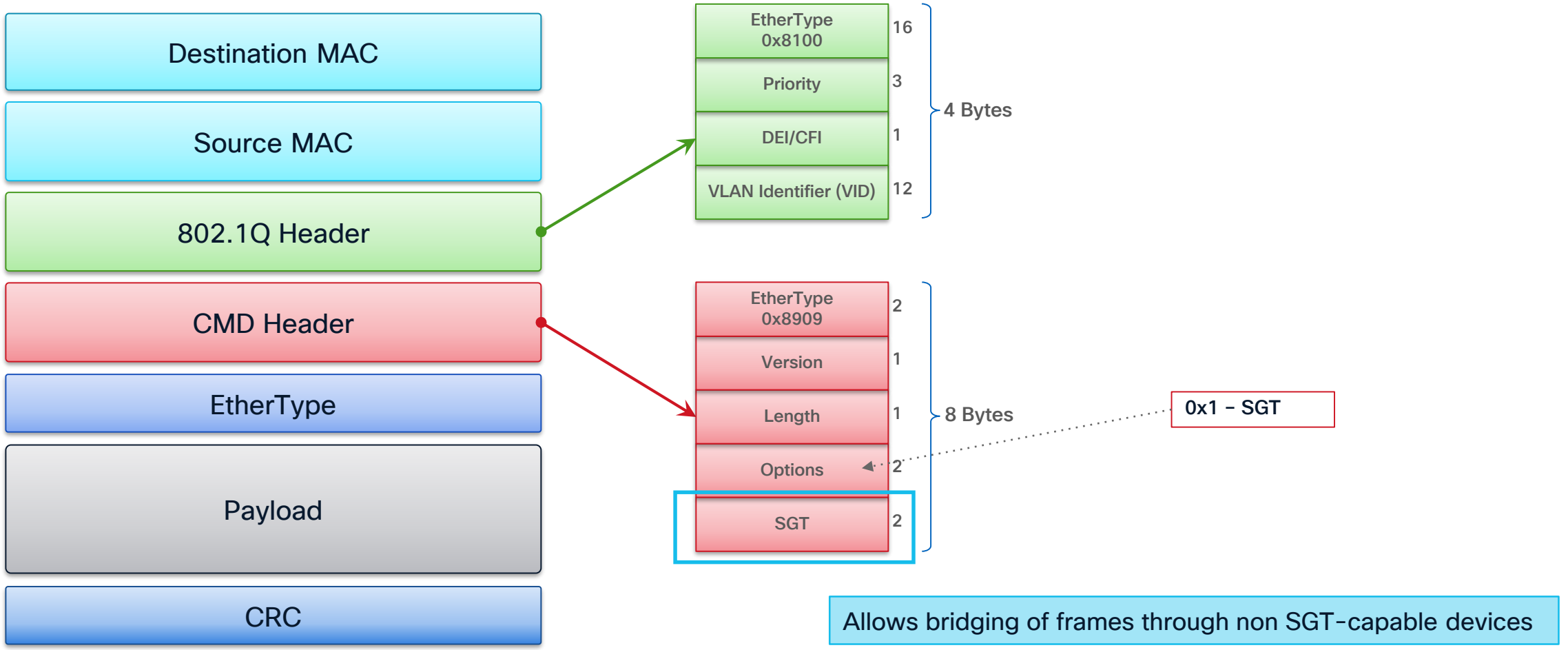
For your reference



Layer 2 only process will look at destination MAC and forward the packet
Layer 3 processing by a non SGT device to drop the frame due to unknown EtherType

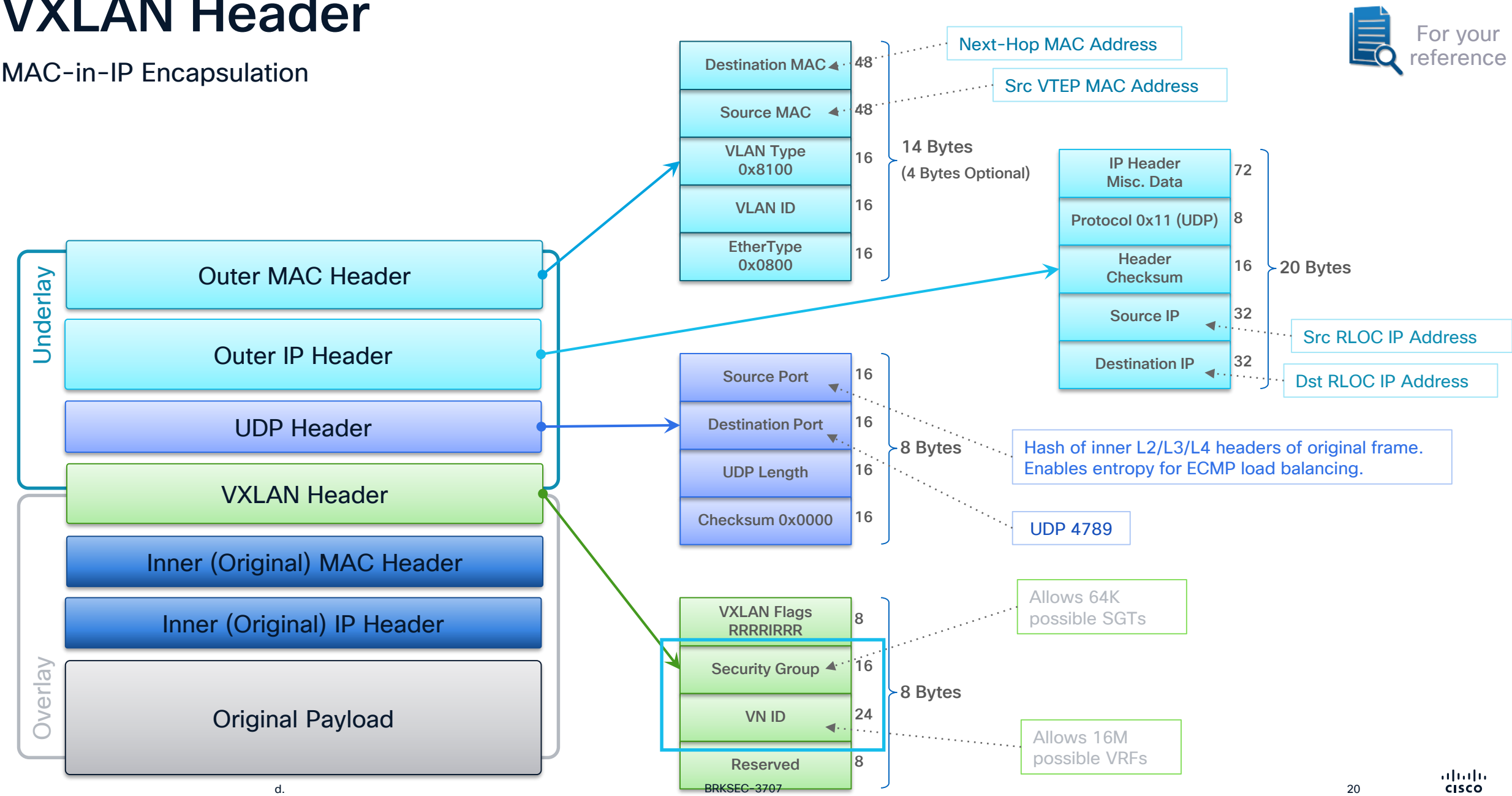
802.1Q Header

For your reference

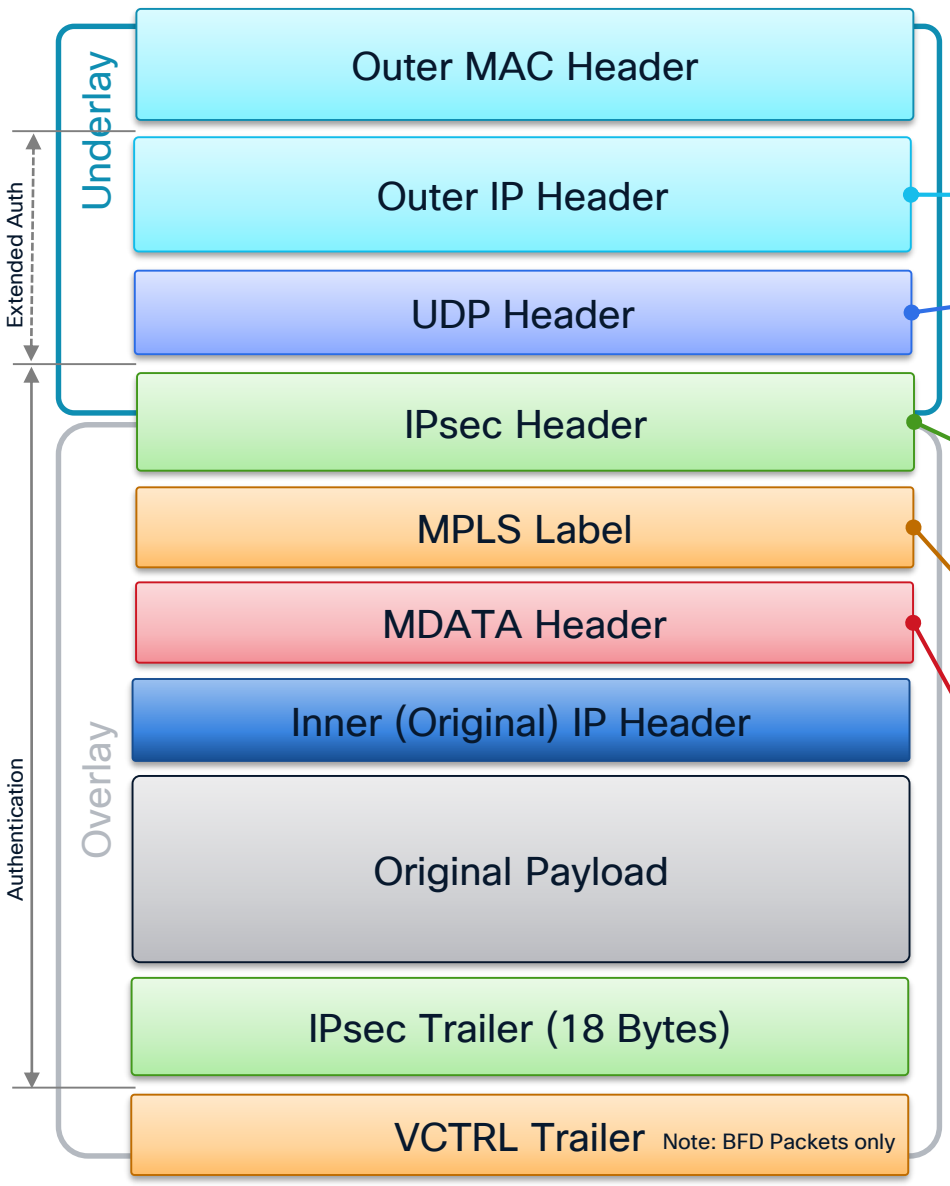


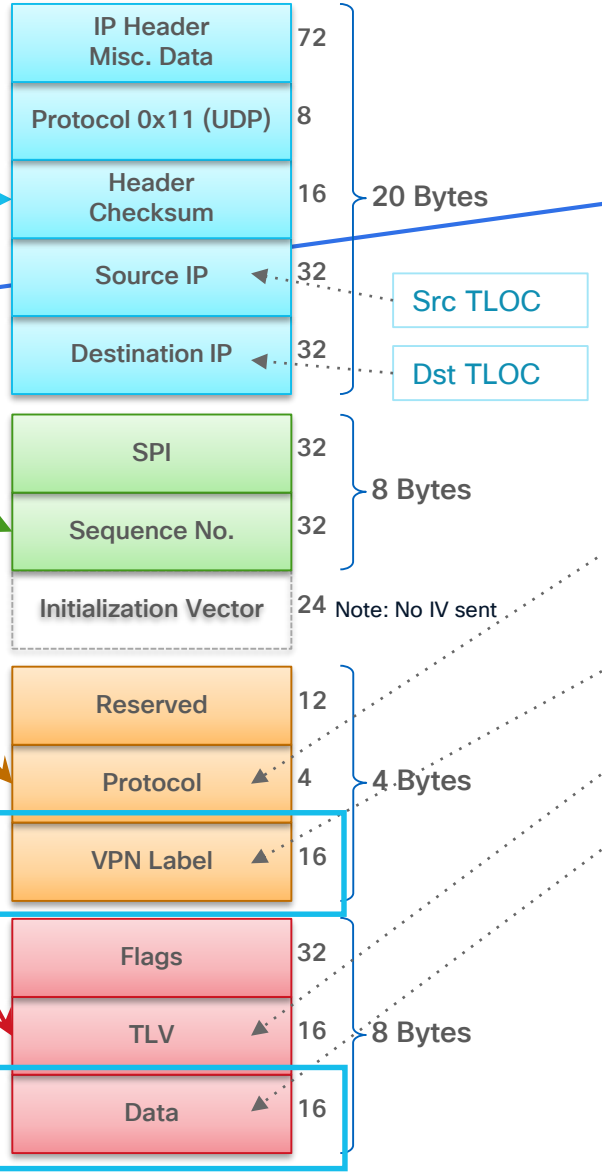
VXLAN Header

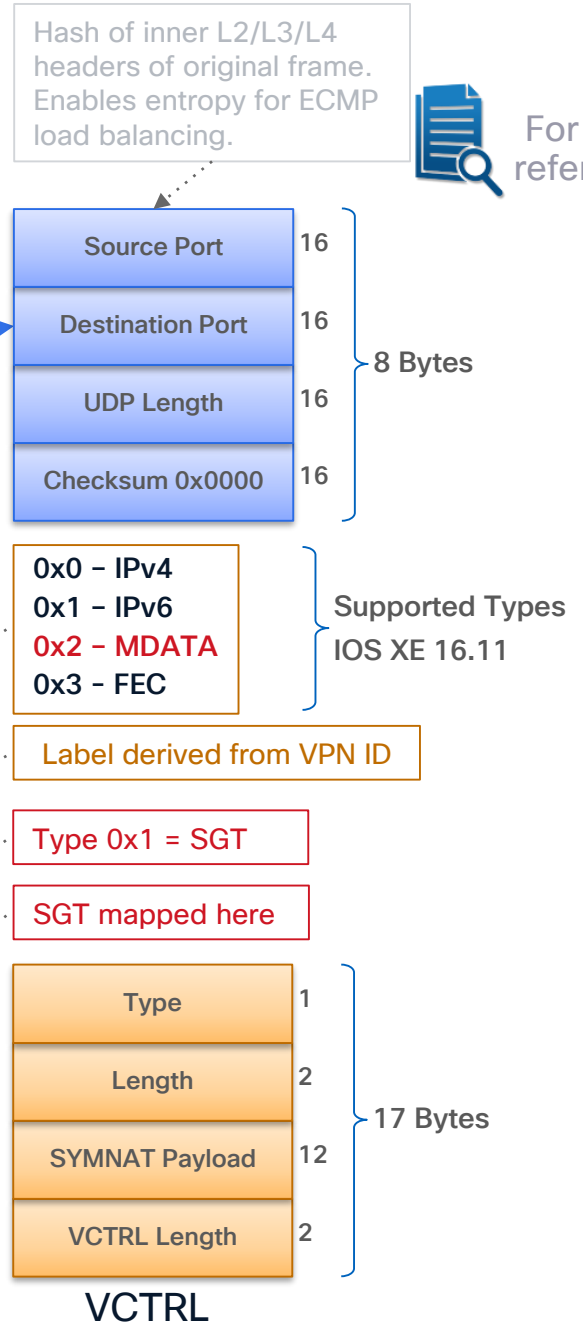
MAC-in-IP Encapsulation



SD-WAN Header

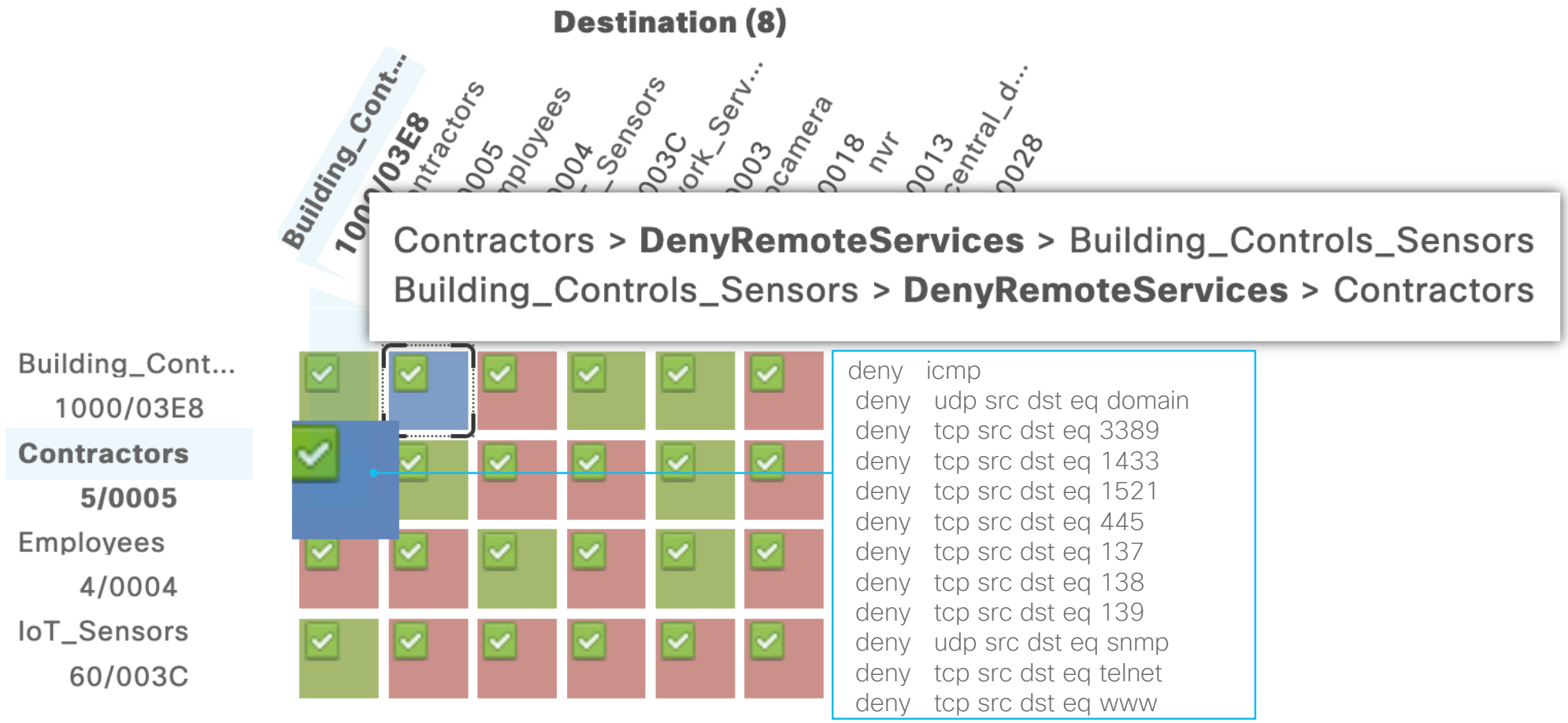






Enforcement (SGACL) - Egress Policy Matrix

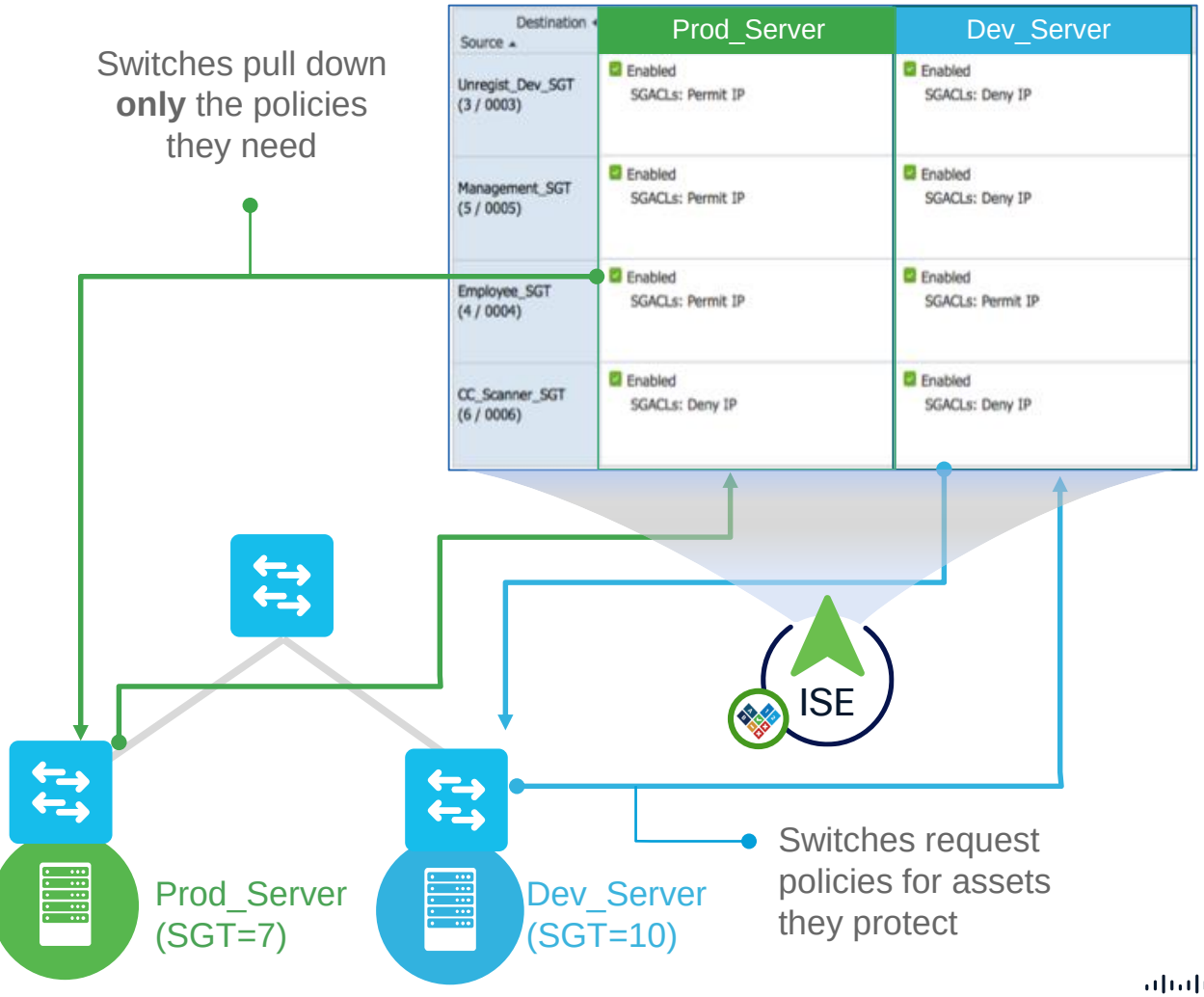
CLASSIFICATION PROPAGATION ENFORCEMENT



Dynamic Policies

- New User/Device/Server provisioned
- Switch requests policies for assets they protect
- Policies downloaded & applied dynamically

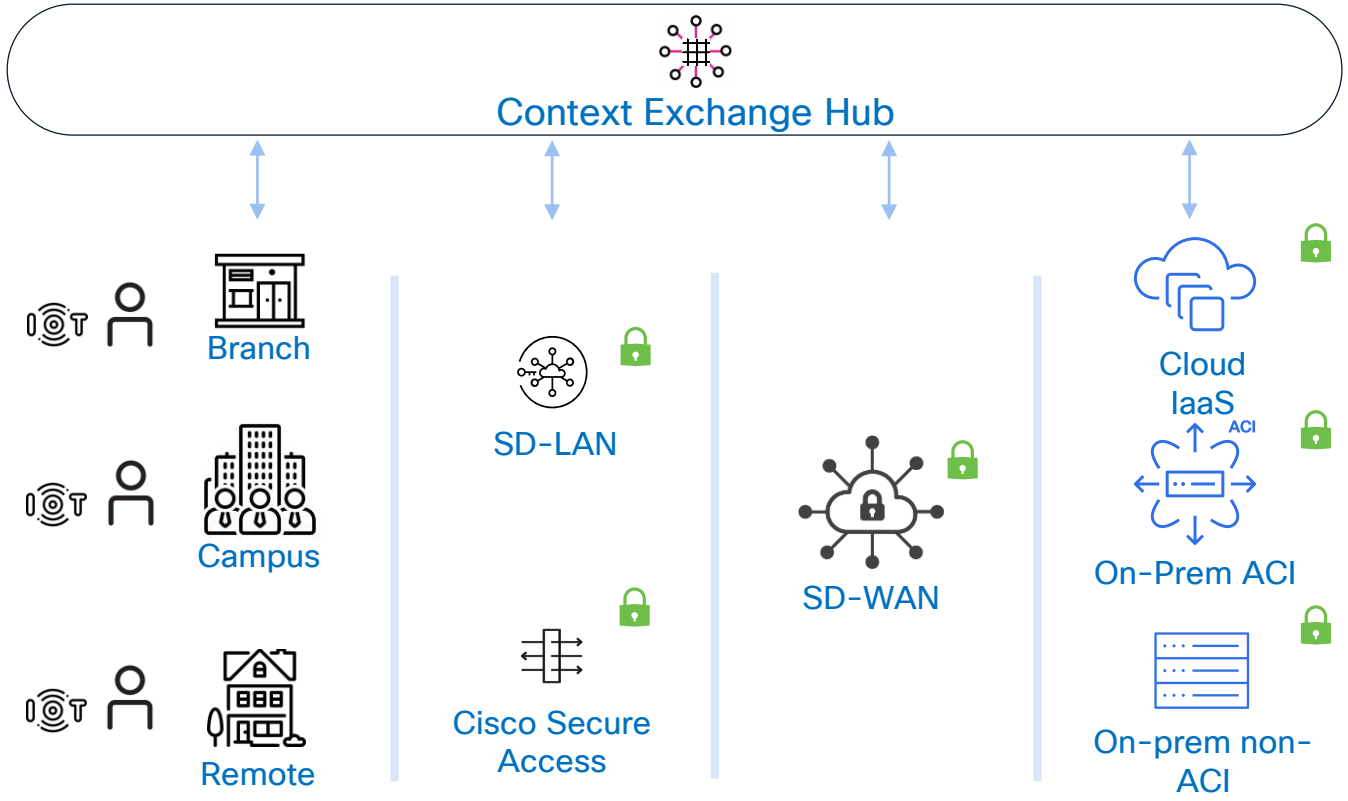
- Result: All controls centrally managed
  - Security policies de-coupled from network topology
  - No switch-specific security configs needed
  - One place to audit network-wide policies



Open Implementations

- 3rd parties support SGTs via pxGrid – branded/unbranded partnership
- SXP published as an Informational Draft to the IETF, based on customer requests
  - shipping partner implementations
  - Open Source SXP Implementations – Java in OpenDaylight, C on github.com
- Cisco Meta Data (CMD) and GRE encapsulations of SGT published into SXP IETF draft
- VXLAN GPO published via IETF Draft
- All Major NGFW Vendors are interoperable via pxGrid
- SASE/SIG Vendors are interoperable via pxGrid
- SD-WAN competitors are interoperable via inline tagging and pxGrid
- Switching and Wireless Competitors have implemented SGT
- 3rd Party ASIC Vendors have public documentation of CMD and VXLAN GPO support

Open Implementations enables Common Policy



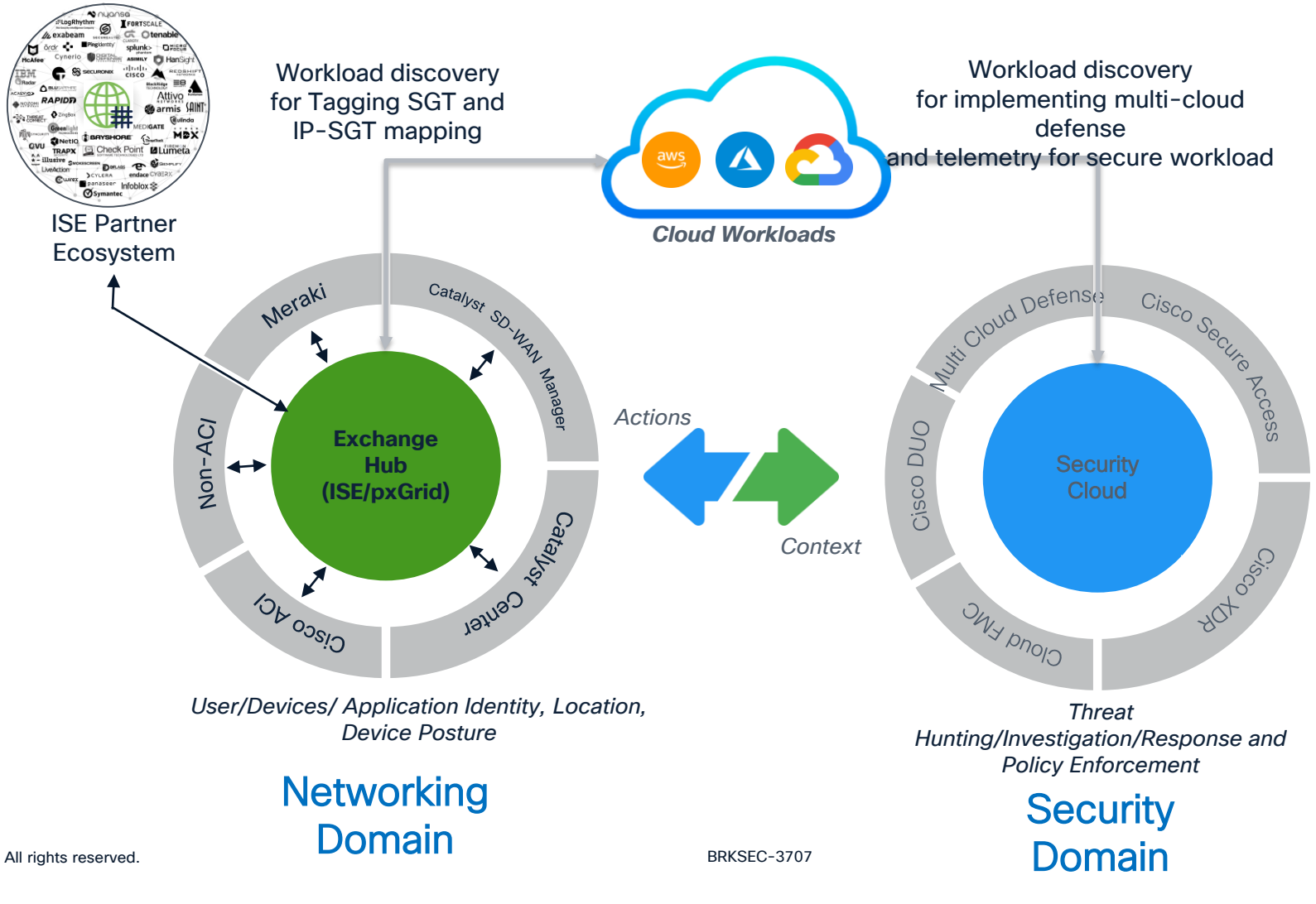
Policy Enforcement Points: Consistent Policies

- Build context in its local domain and store it as standard scalable group tags (SGT)
- Share context everywhere, across networking and security domains
- Enforce consistent SGT based policies, enable simple and unified policy experience

Context-aware policies for on-prem app and cloud workloads for multiple enforcement points

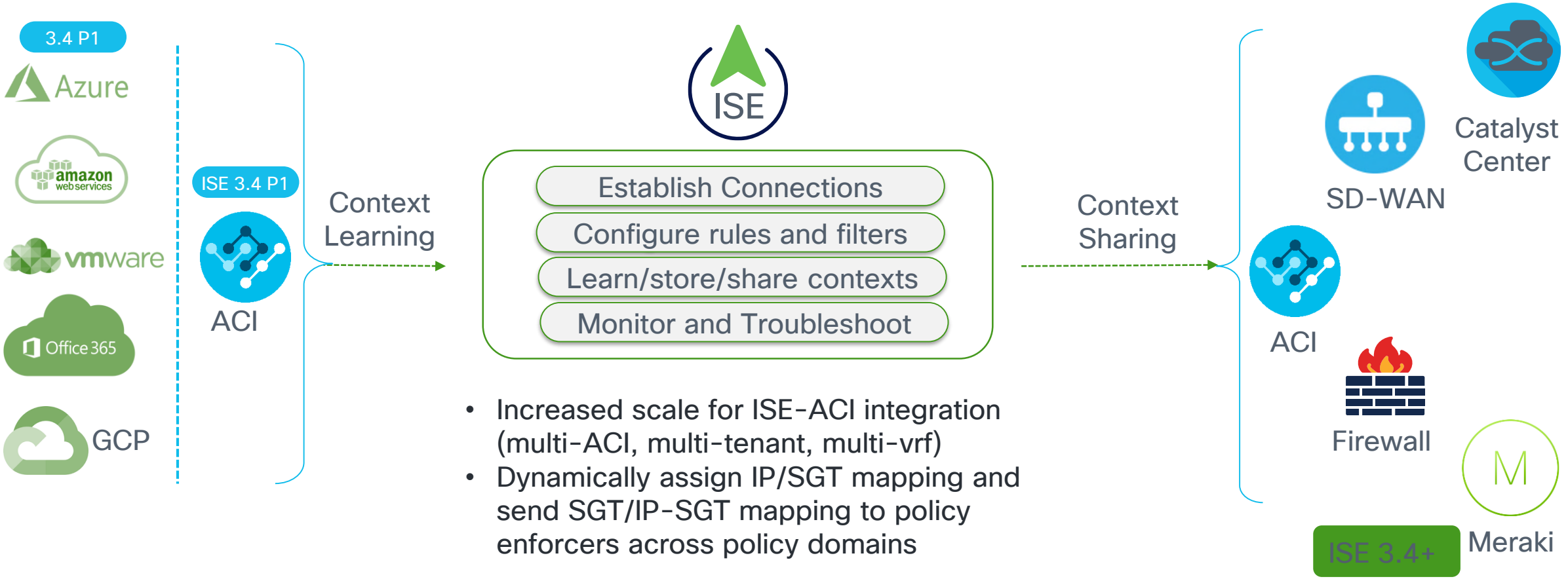
Common Policy – Common Language for Security

Normalizing and sharing context across domains



Common Policy Capabilities

Enabling consistent Zero Trust policies in a multidomain environment



- Increased scale for ISE-ACI integration (multi-ACI, multi-tenant, multi-vrf)
- Dynamically assign IP/SGT mapping and send SGT/IP-SGT mapping to policy enforcers across policy domains

Use Case Review

Current SGT/SGACL Supported Platforms

For your reference

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/policy-platform-capability-matrix.pdf

Classification

- Catalyst 9200, 9300, 9300-M, 9400, 9500, 9600
- IE 9300
- IE 4000
- IE 3100, 3200, 3300, 3400
- IE 2000
- IR 8340
- WLC 9800
- WLC 8510, 8540
- WLC 5760
- WLC 5508, 5520
- vWLC
- AP x700, x800, 9100
- Catalyst 8000V, 8200, 8300, 8500
- ISR 1000, 4000
- ASR 1000
- CSR
- CGR 2010, CGS 2500
- ASAv, FTDv
- CSF 1200, 3100, 4200
- FP 1010, 1100, 2100, 4100, 9300
- ISA 3000
- MS390, MS130X/R
- MR30H/33/42/42E/52/53/53E/74/84, MR36/36H/44/45/46/46E/55/56/57/76/86
- CW916x
- MX64/65, MX67/68, MX84/100, MX75/85/95/105, MX250/450
- Z3/4/C
- ISE

Propagation

- Catalyst 9200, 9300, 9300-M, 9400, 9500, 9600
- IE 9300
- IE 4000*
- IE 3100*, 3200*, 3300*, 3400
- IE 2000*
- IR 8340
- WLC 9800
- WLC 8510*, 8540*
- WLC 5760
- WLC 5508*, 5520*
- vWLC*
- AP x700, x800, 9100
- Catalyst 8000V, 8200, 8300, 8500
- ISR 1000, 4000
- ASR 1000
- CSR
- CGR 2010, CGS 2500
- ASAv, FTDv
- CSF 1200, 3100, 4200
- FP 1010, 1100, 2100, 4100, 9300
- ISA 3000
- MS390, MS130X/R
- MR30H/33/42/42E/52/53/53E/74/84, MR36/36H/44/45/46/46E/55/56/57/76/86
- CW916x
- MX64/65, MX67/68, MX84/100, MX75/85/95/105, MX250/450
- Z3/4/C
- ISE

Enforcement

- Catalyst 9200, 9300, 9300-M, 9400, 9500, 9600
- IE 9300
- IE 3400, 4000
- IR 8340
- WLC 9800
- WLC 8540
- WLC 5760
- WLC 5520
- vWLC**
- AP x700, x800, 9100
- Catalyst 8000V, 8200, 8300, 8500
- ISR 1000, 4000
- ASR 1000
- CSR
- CGR 2010
- ASAv, FTDv
- CSF 1200, 3100, 4200
- FP 1010, 1100, 2100, 4100, 9300
- ISA 3000
- MS390, MS130X/R
- MR30H/33/42/42E/52/53/53E/74/84, MR36/36H/44/45/46/46E/55/56/57/76/86
- CW916x
- MX64/65, MX67/68, MX84/100, MX75/85/95/105, MX250/450
- Z3/4/C
- Secure Web Appliance

* Speaker only
** APs in FlexConnect mode only

Cisco Meraki Access Control Capabilities with ISE

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redir	CoA	Profiling
Wireless								
MR20, MR70, MR28, MR78	✓	✓	✓	✓	–	✓	✓	–
MR30H/33/42/42E/52/53/53E/74/84 MR36/36H/44/45/46/46E/55/56/57/76/86 CW916x	✓	✓	✓	✓	✓ 802.11ac Wave2 or higher. Min 27.6	✓	✓	–
Teleworker								
Z3/4/C	✓	✓	–	–	✓ Transport MX18.1+	–	–	–
Switching								
MS120, MS125, MS130	✓	✓	✓	–	–	–	✓	CDP+LLDP
MS130X/R	✓	✓	✓		✓ MS17 (initial release)		✓	CDP+LLDP
MS210, MS225, MS250 MS350, MS355	✓	✓	✓	✓	–	✓	✓	CDP+LLDP
MS390, C9300-M	✓	✓	✓	✓	✓ 14.2+	✓	✓	Device Sensor CDP/LLDP/DHCP/HTTP
MS410, MS425, MS450 (aggregation)	✓	✓	✓	✓	–	✓	✓	CDP+LLDP
Security & SD-WAN								
MX64/65, MX67/68, MX84/100, MX75/85/95/105,MX250/450	✓ 802.1X *or* MAB	✓ 802.1X *or* MAB	–	–	✓ Transport MX18.1+	–	–	–
vMX	–	–	–	–	–	–	–	–

Minimum Advanced Licensing

Use Case Review – Campus/Branch

Manufacturer with Campus and Branch

- Business Problem/Background
  - Allow Authorized Users on Trusted Devices onto the site LAN/WLAN
  - Isolate IOT devices (Building Automation, Physical Security, etc.) from Managed Users/Devices
  - 12 month time limit to deploy solution due to Governance Risk and Compliance directive from company board
- Solution Overview
  - ISE deployed for Authenticating Users via Certificates on WLAN already. Deploy ISE for LAN ports
  - Implement ZTNA for user application access – removes use cases from network security
  - Trusted Device status determined via MDM
  - ISE used to profile OT Devices
  - Some sites had multivendor offers which dictated ingress switch enforcement initially
  - Some sites had 3rd party WLAN that dictated upstream switch enforcement
  - The solution design was directly impacted solution due to site size and enforcement scaling

Methodology for an effective Segmentation

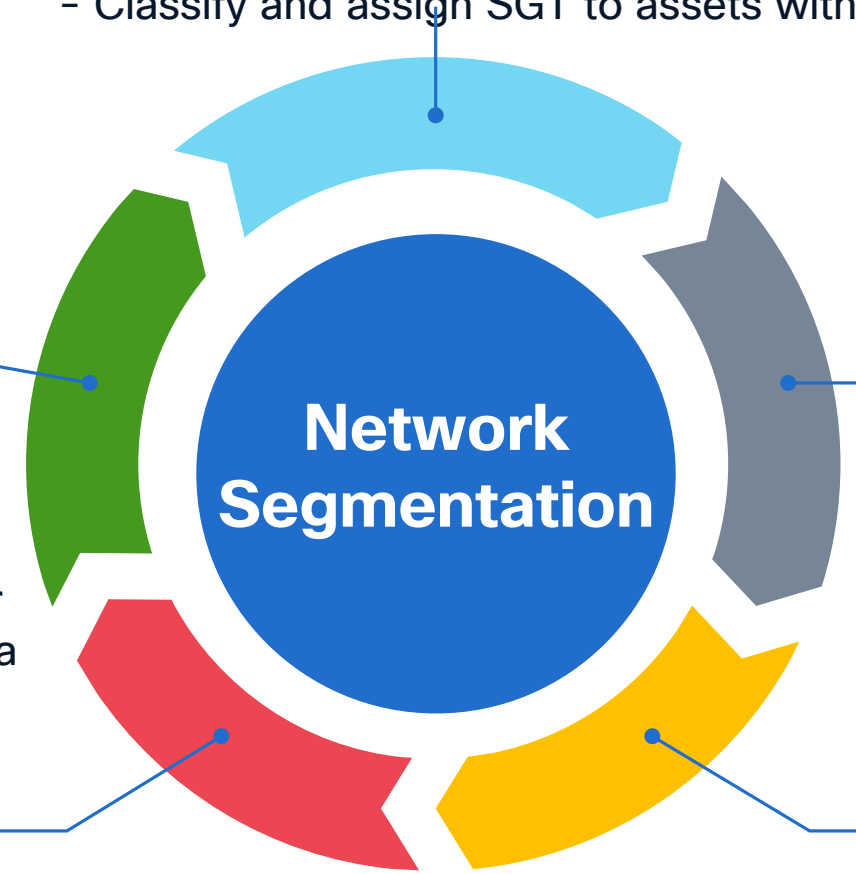
Step 1. Discover and Classify Assets
- Identify assets to protect
- Classify and assign SGT to assets with ISE

Step 2. Understand Behavior
- Use NetFlow to understood the communication between groups

Step 3. Design and Model Policy
- Observe communication between SGTs
- Create policies (SGACLs) for SGT/DGT pairs

Step 4. Enforce Policy
- Optionally, enable TrustSec Monitor Mode for “Shadow-Policing“ in Data Plane and observe results
- Enforce policy at the appropriate enforcement points for a given use case

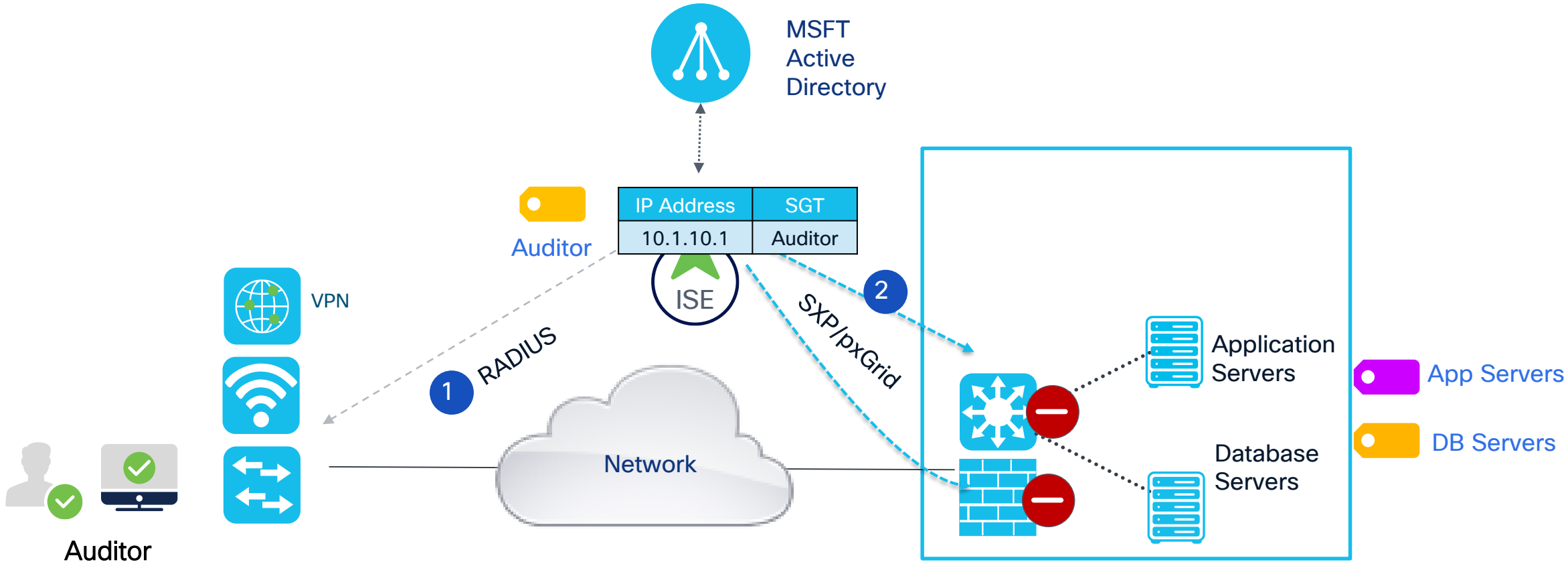
Step 5. Active Monitoring
- Monitor SGT policy violations and events with SNA, SIEM tools, etc.
- Optionally, identify threats and contain misbehaving endpoints/assets



Segmentation Methodology Lifecycle

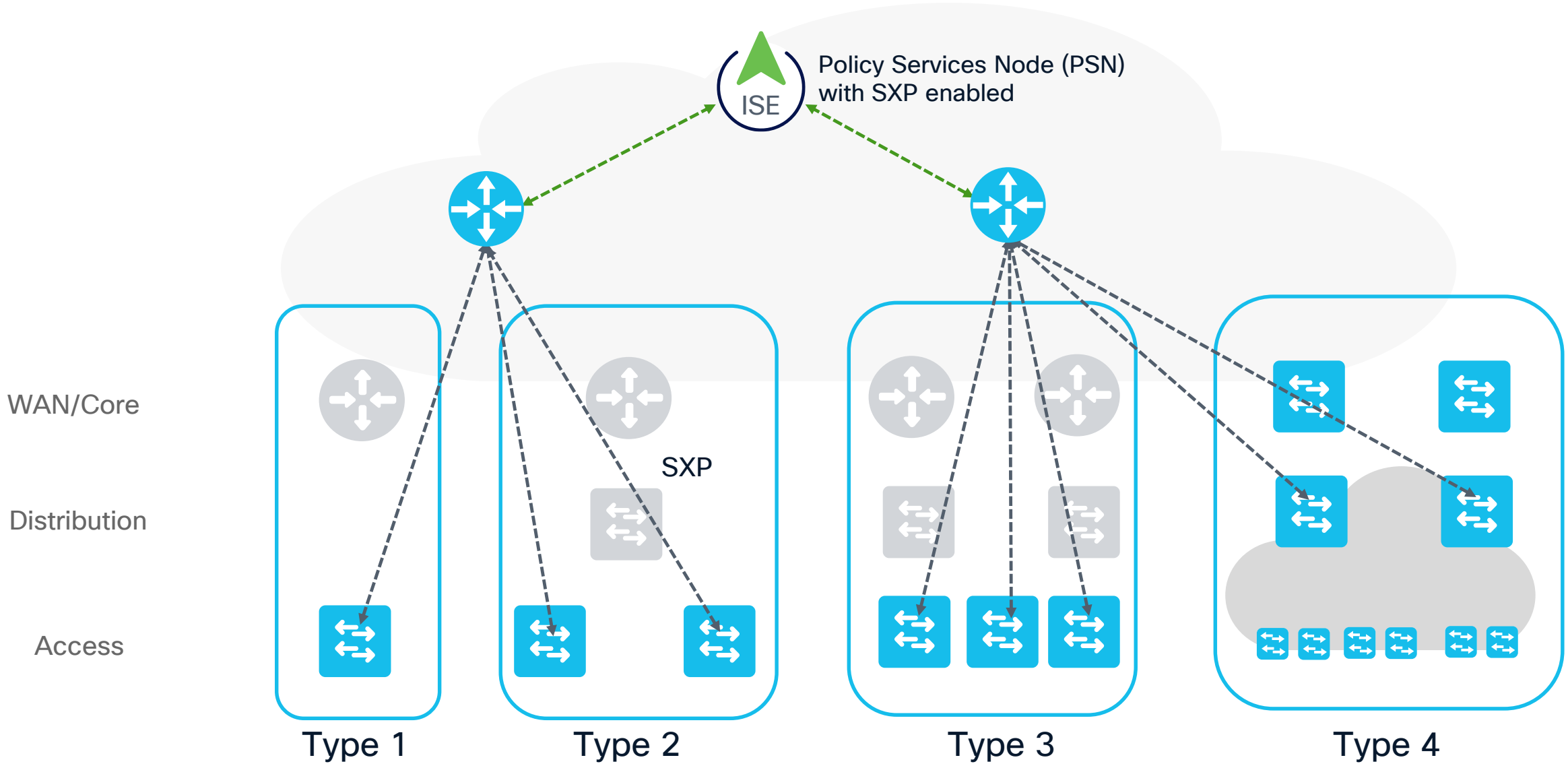
For your reference

ISE creation of IP/SGT from AAA



- RADIUS Authentication/Authorization/Accounting go to ISE
- RADIUS Accounting MUST be in a format ISE can use to bind the IP and SGT together
- Any access device can be used “if” RADIUS accounting is formatted according to specification

Starting Design – Ingress Filtering via Site IP/SGT



Design Details

- Single ISE Cluster For Global Network
- Chose to use IOS SXP Peering routers below ISE for scaling and filtering capability
- SGT Domains will be utilized to create site level IP/SGT groupings
- SXP would deliver all site level IP/SGT for in scope SGTs to Ingress
- In Scope Policy/Endpoints only get SGTs assigned
  - Not all devices need an SGT – Only assign SGTs to the OT/IOT devices in scope. This reduces the count if IP/SGT at the edge.
  - Out of scope devices (Users with ZTNA agent) would inherit a “Enterprise SGT” – i.e. 10.0.0.0/8 = Enterprise_SGT
- ”Internet” or Software as a Service (Including ZTNA termination) handled with an “Internet_SGT” – Classified with a default route or a list of prefixes

Example Policy – Partial View for Example

SRC/DST	ipcamera (24)	nvr (19)	nvr_central_data (40)	Employees (4)	Network_Services (3)	Internet_SGT (2500)
ipcamera (24)	deny	permit	deny	deny	permit	deny
nvr (19)	permit	deny	permit	deny	permit	deny
nvr_central_data (40)	deny	permit	deny	deny	deny	deny
Employees (4)	deny	deny	deny	deny	permit	permit
Network_Services (3)	permit	permit	deny	permit	permit	deny
Internet_SGT (2500)	deny	deny	deny	permit	deny	deny
Default - Deny						

ISE SGT Domains (formerly SXP Domains)

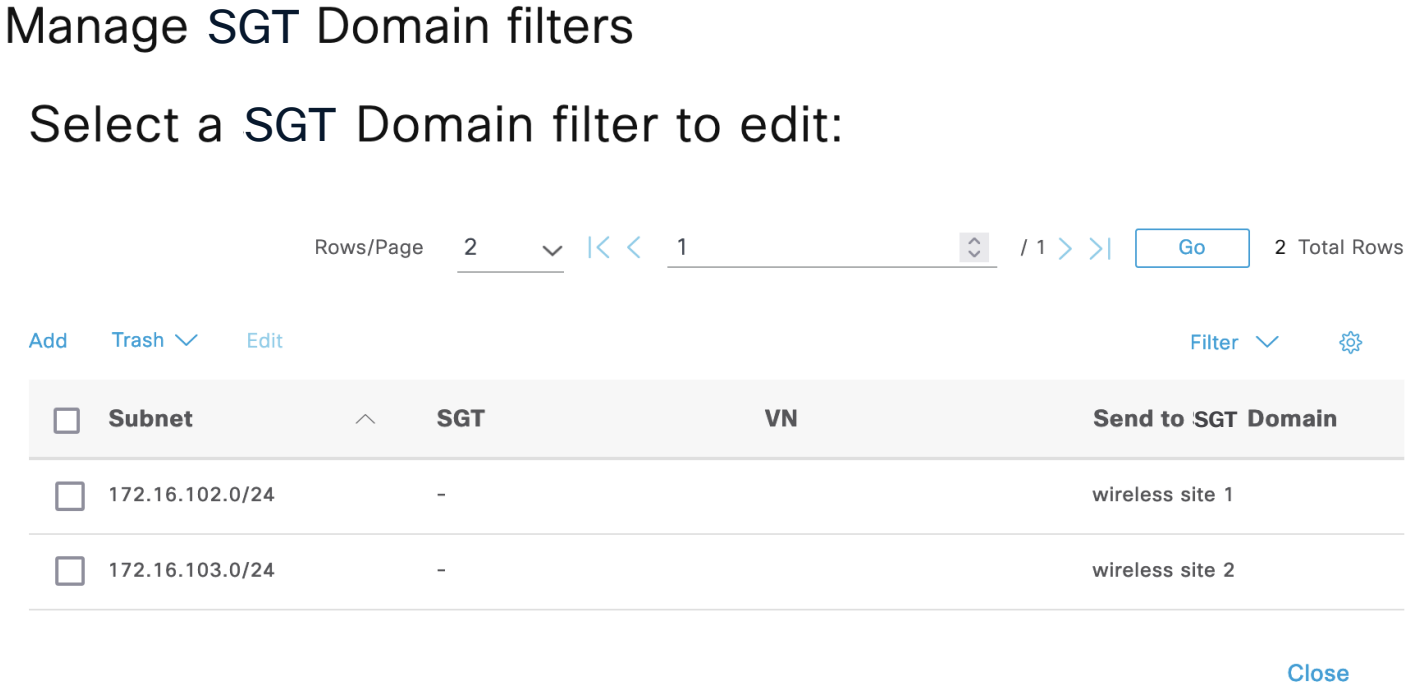
- SGT Domains separate the global SGT binding table into separate tables for a specific purpose
- Granular control over mapping distribution
- By default, IP-SGT mappings to SXP peers shared within SGT Domain Default
- Dynamic Session mappings go to SGT Domain Default
- SGT carried in data plane removes need to exchange IP-SGT mappings between SGT Domains

IP/SGT mappings and SGT Domains

SGT Domain Filters

For your reference

- Use SGT Domain filters to send dynamic session mappings selectively to one or multiple SGT Domains
- In this scenario we only share the bindings of the Wireless LAN to the upstreams switch for a particular site

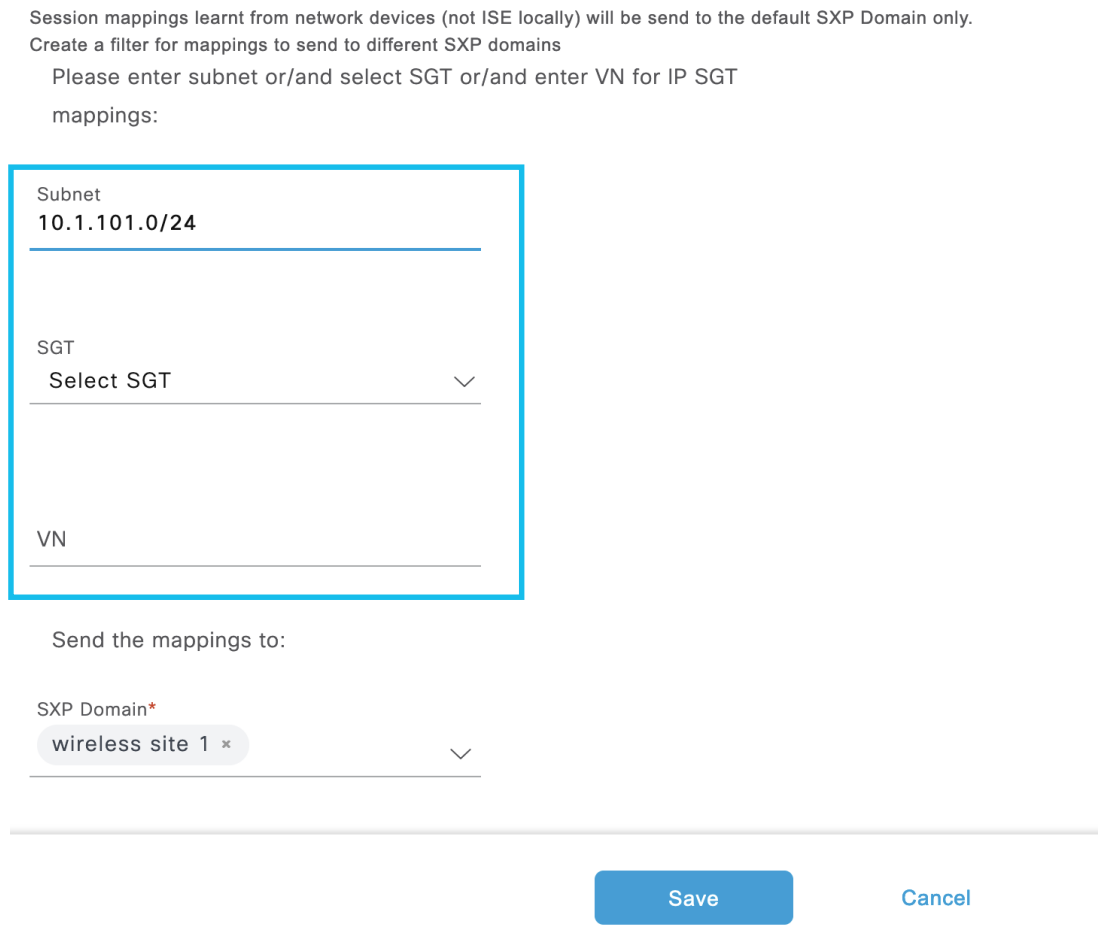


Dynamic mappings for SGT Domains

SGT Domain Filters

For your reference

- Chose one or a combination of the following:
  - Subnet
  - SGT
  - VN



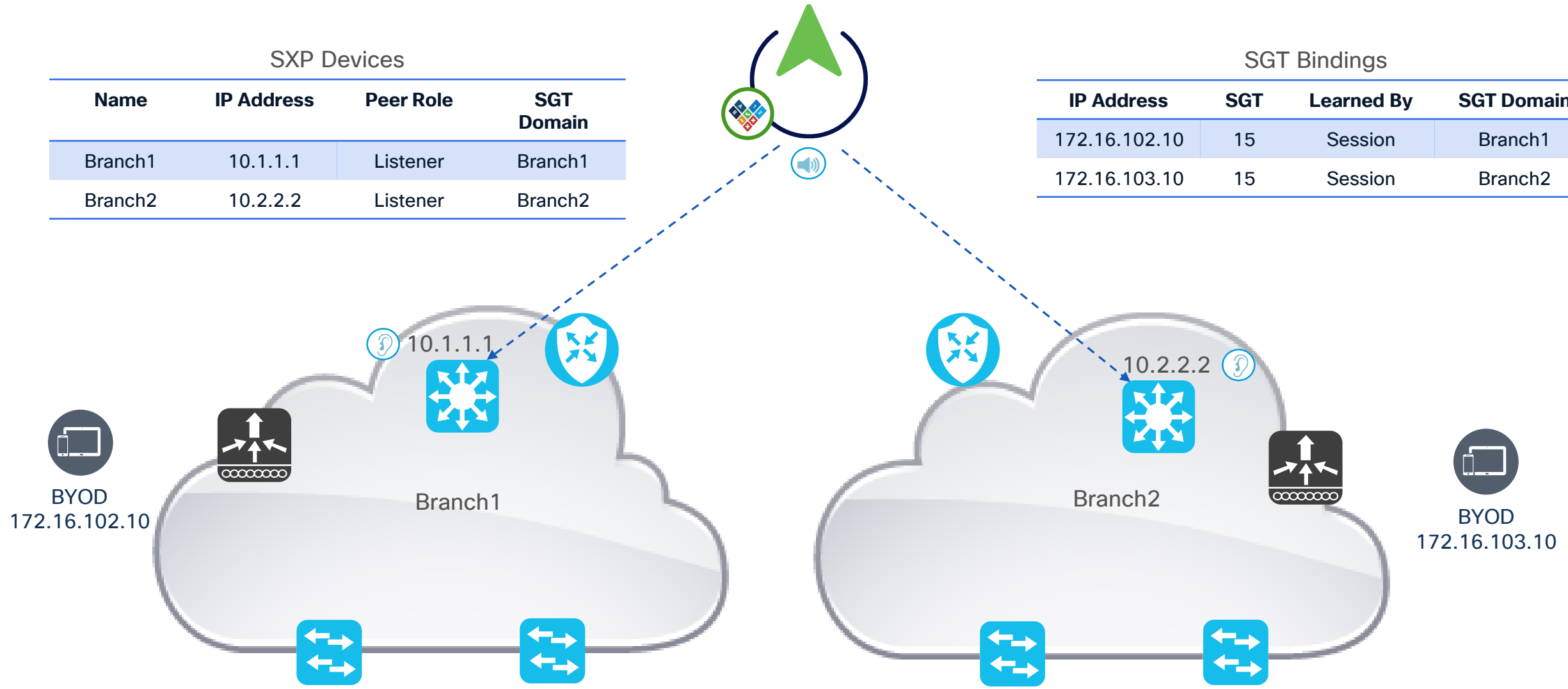
Segmentation with ISE SGT Domains

SXP Devices

Name	IP Address	Peer Role	SGT Domain
Branch1	10.1.1.1	Listener	Branch1
Branch2	10.2.2.2	Listener	Branch2

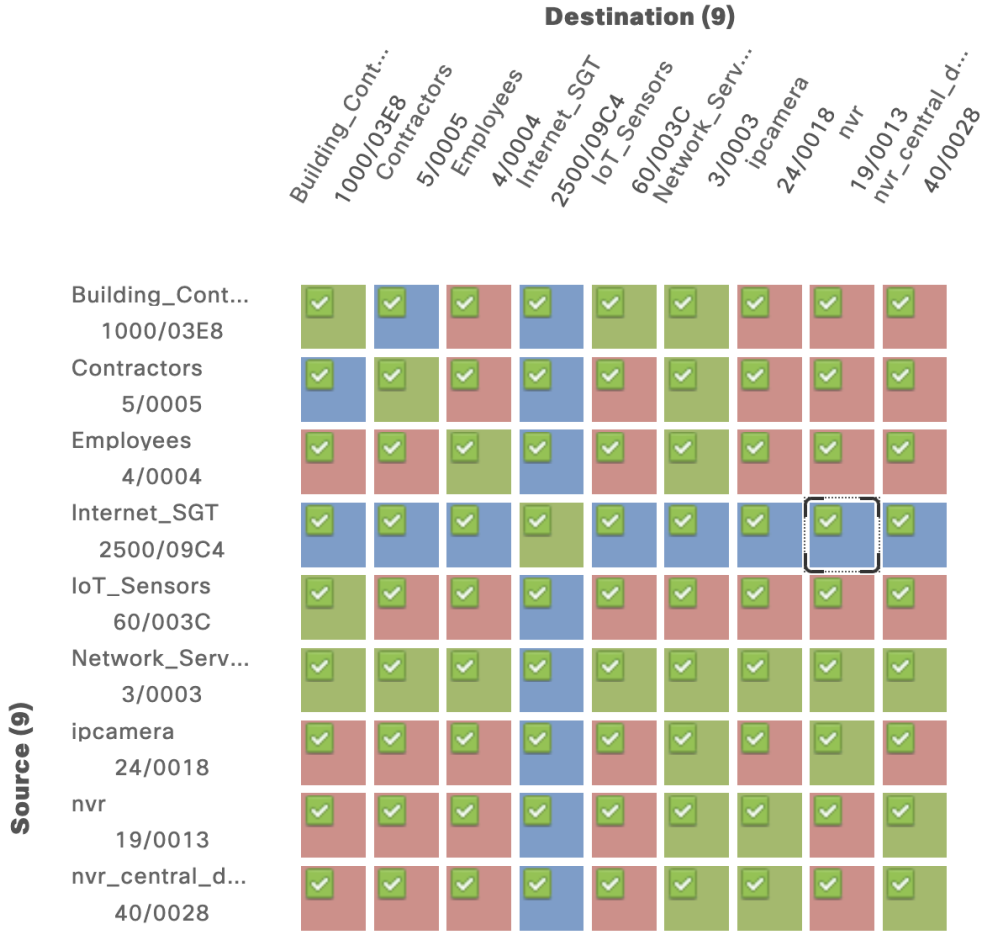
SGT Bindings

IP Address	SGT	Learned By	SGT Domain
172.16.102.10	15	Session	Branch1
172.16.103.10	15	Session	Branch2

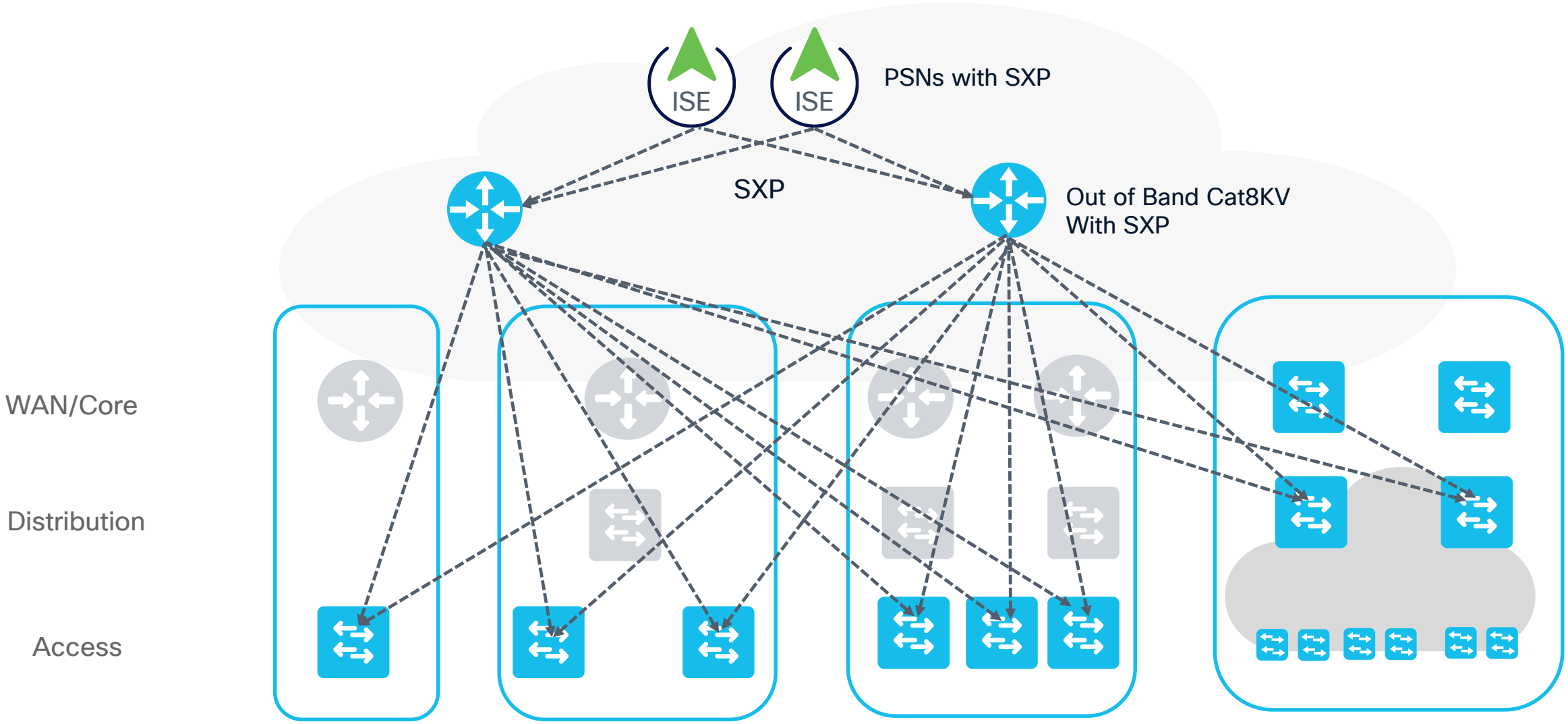


Policy Example – Full View Reference

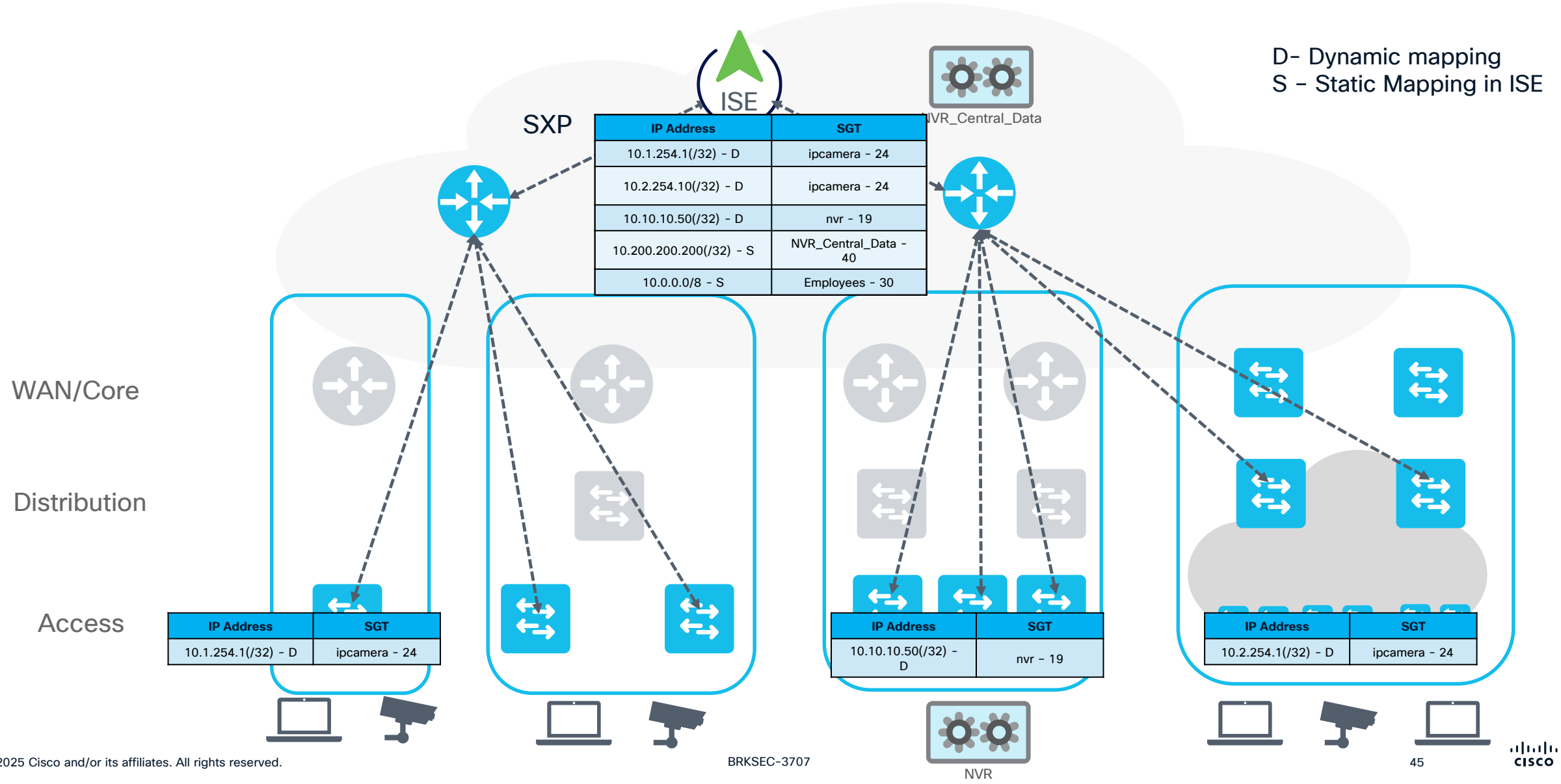
For your reference



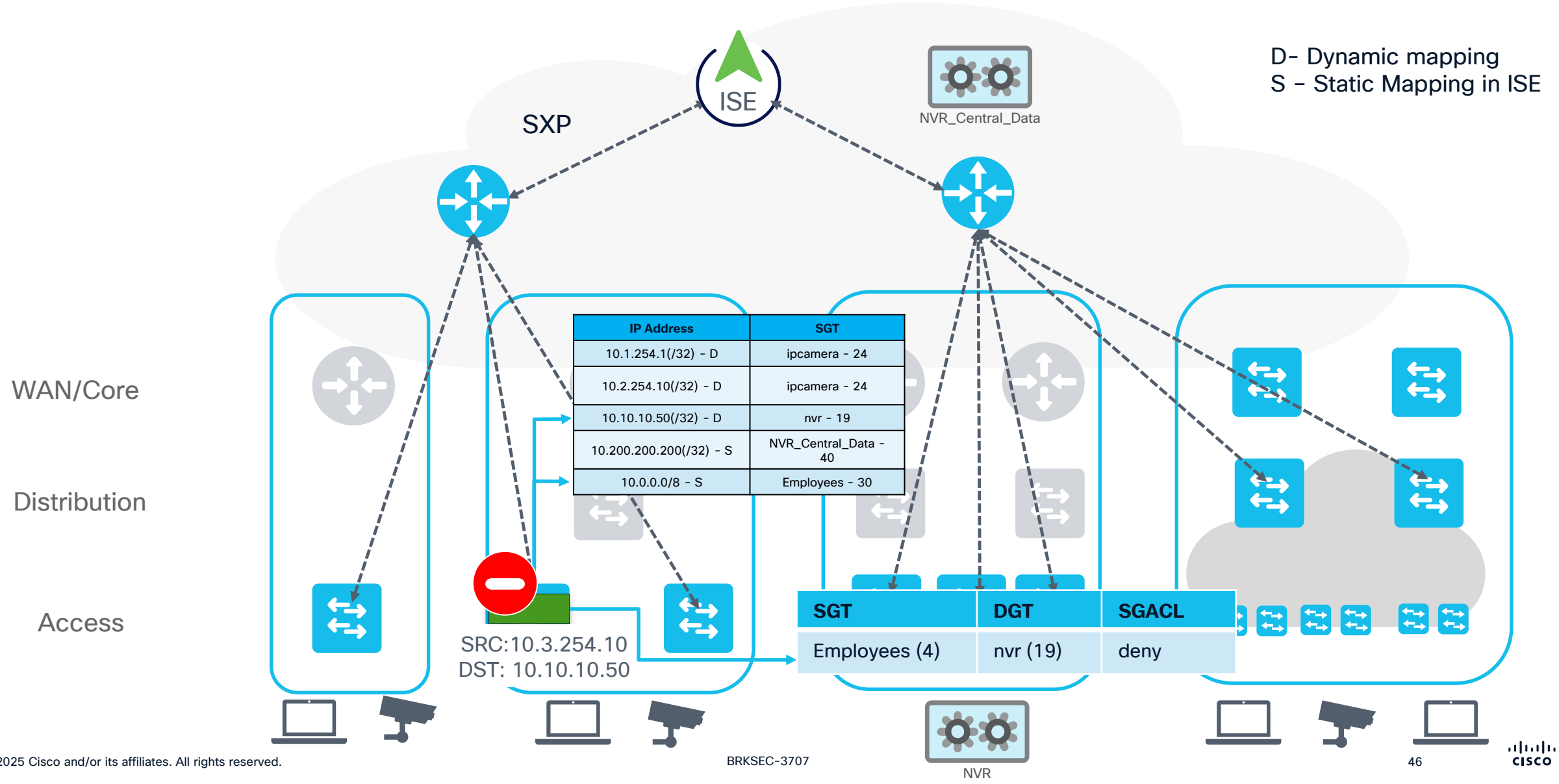
Starting Design – SXP redundancy



Starting Design – Ingress Filtering via Site IP/SGT



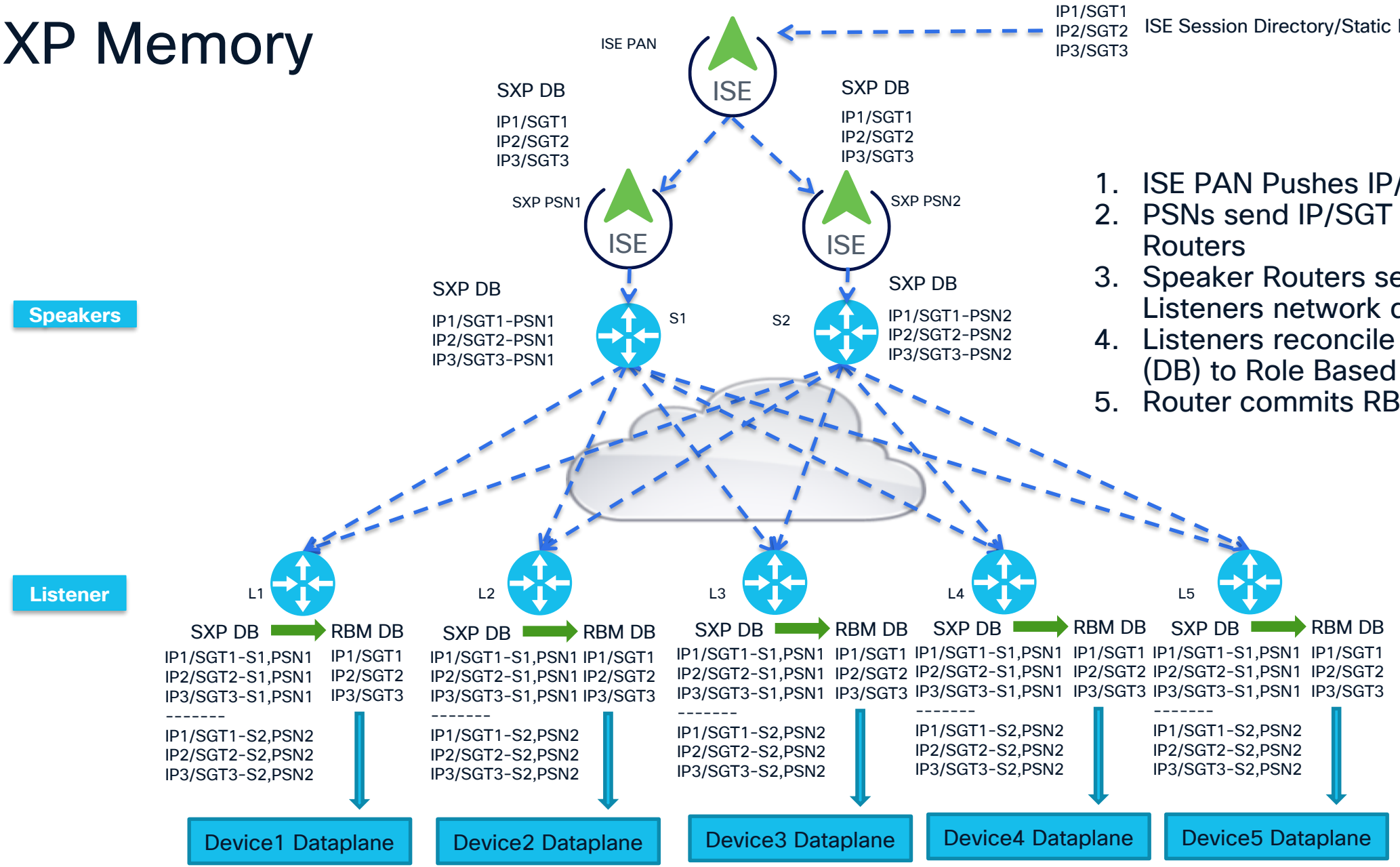
Starting Design – Ingress Filtering via Site IP/SGT



Memory Usage of IP/SGT in Network Device

- Three places the IP/SGT uses memory in a platform
- SXP DataBase
  - Stored in RAM
  - IP/SGT kept for every peer
  - IP/SGT has an attached path length
  - Multiple Paths can exist for each IP/SGT
  - IP/SGT has origin SXP Node-ID
- Role-Based Master (RBM) DataBase
  - Stored in RAM
  - Normalized IP/SGT binding for use by dataplane
    - Hardware platforms have limits as noted in the dataplane
    - It is possible to have more IP/SGT in the Master DB than the dataplane can handle. This is acceptable if you are only using the Device for SXP relay/aggregation
  - Normalized with the Tag Priority defined for each major platform IOS vs NXOS
  - Published Numbers on CCO and in this presentation are for the Master DB with a minimum of two IP/SGT in the SXP DB.
- Dataplane Memory <---- This is the published number for scaling of the platform
  - Stored in TCAM for ASICs
  - High speed Memory for NPUs
  - DRAM/SRAM for CPU forwarding platforms

SXP Memory

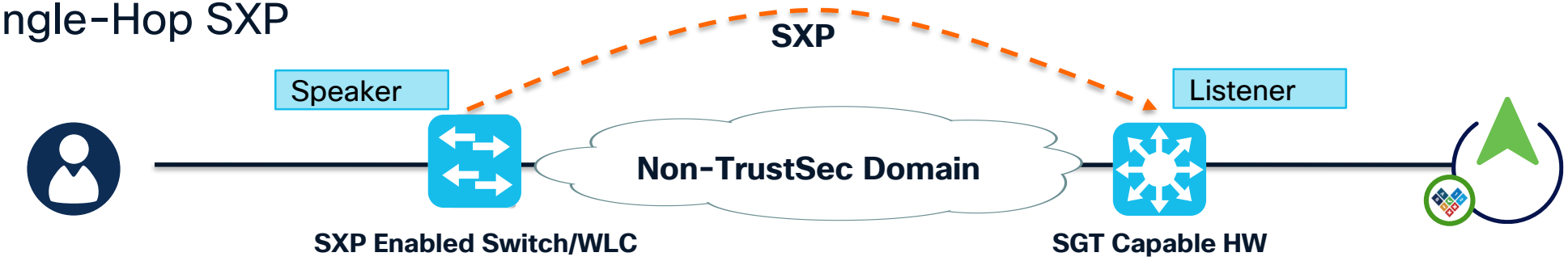


1. ISE PAN Pushes IP/SGT to SXP PSN
2. PSNs send IP/SGT to Speaker Routers
3. Speaker Routers send IP/SGT to Listeners network devices
4. Listeners reconcile SXP Data Base (DB) to Role Based Master DB (RBM)
5. Router commits RBM to DataPlane

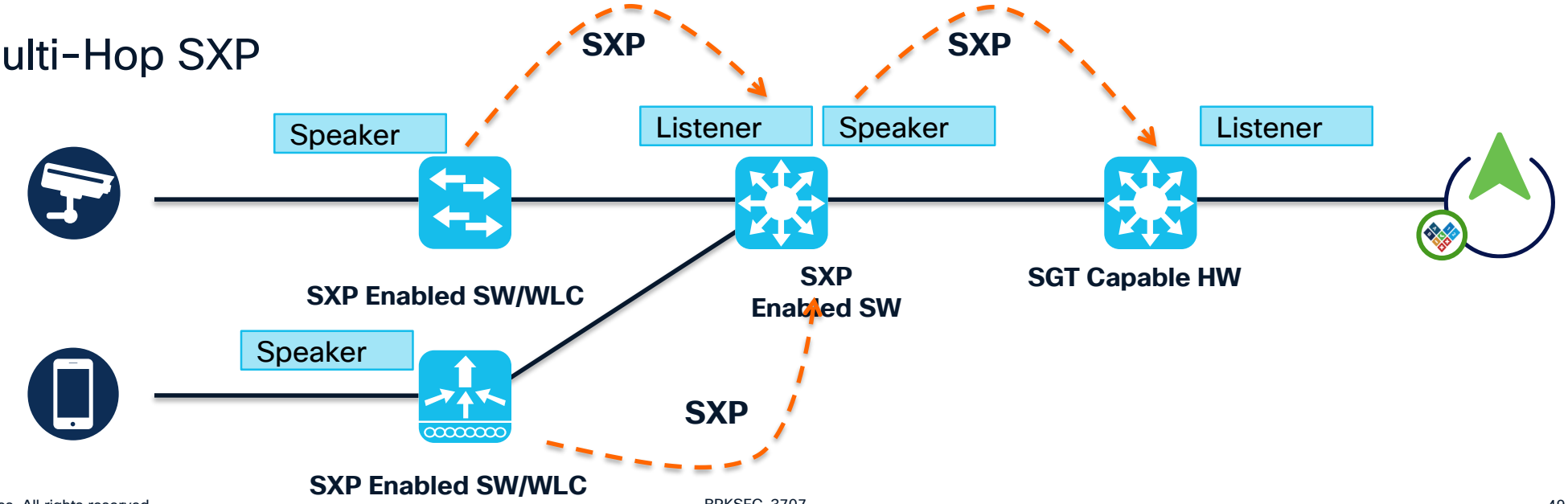
SXP Connection Types

For your reference

Single-Hop SXP

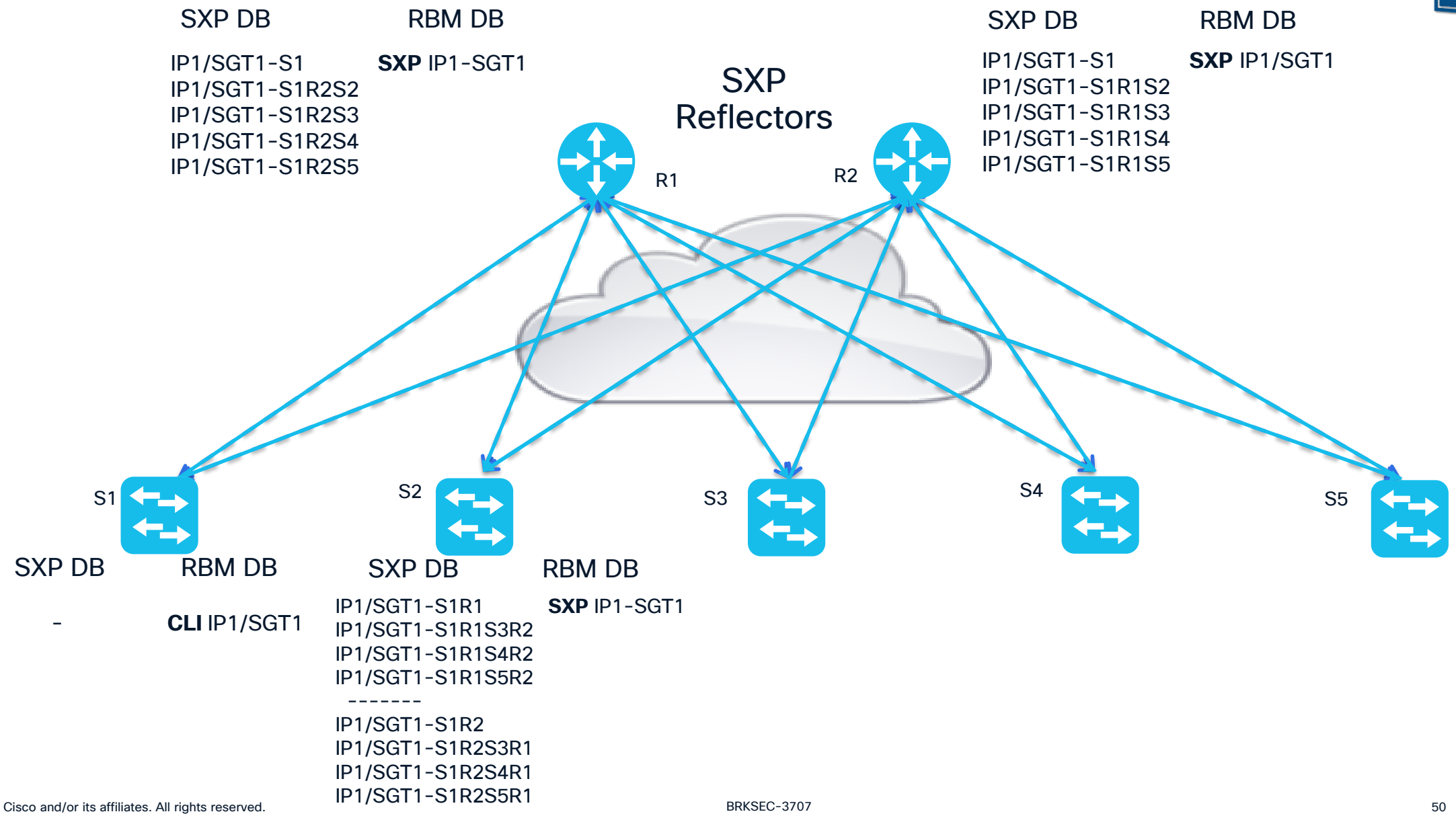


Multi-Hop SXP

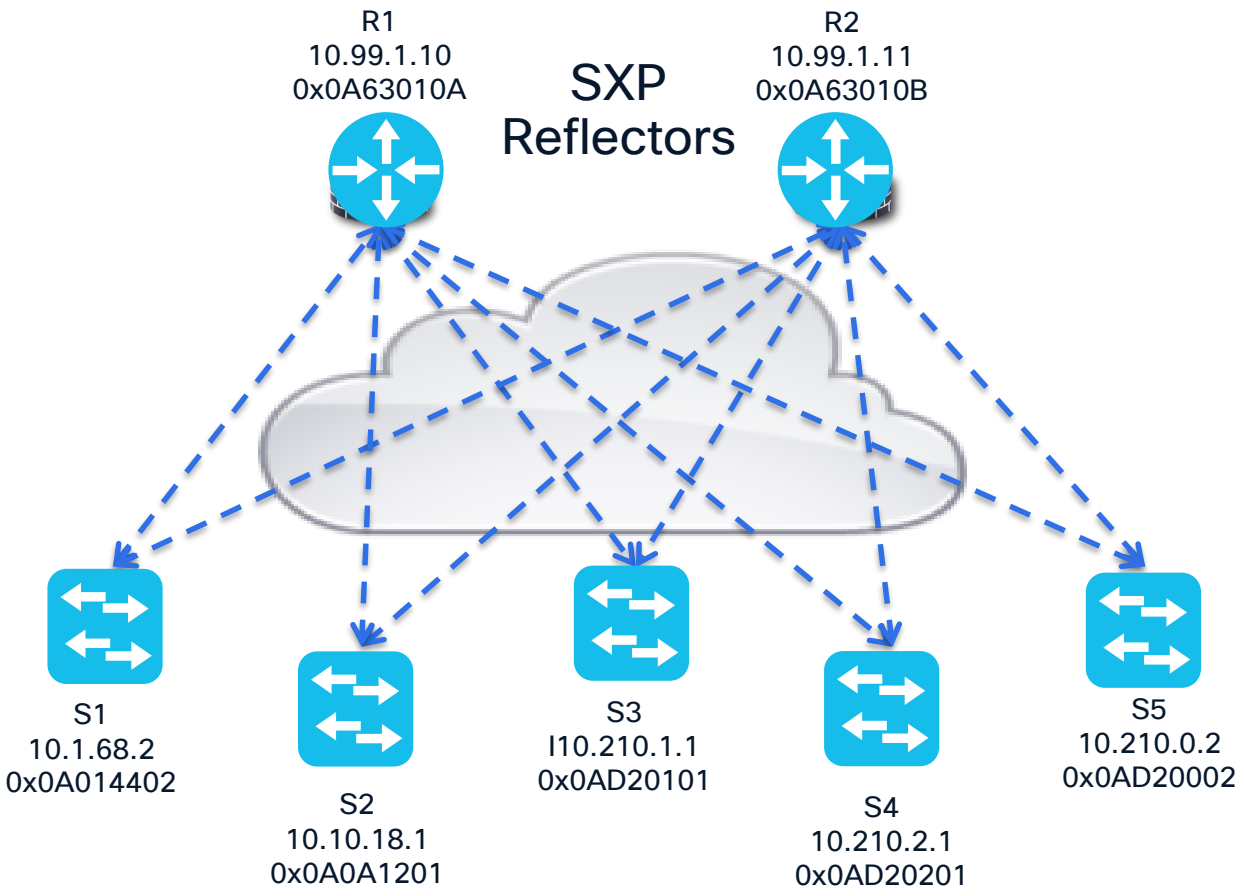


SXP Database creation

For your reference



SXP Database creation




```
R1#show cts sxp sgt-map
SXP Node ID(generated):0x0A63010A(10.99.1.10)
IP-SGT Mappings as follows:
IPv4,SGT: <10.7.7.7 , 1000>
source  : SXP;
Peer IP : 10.1.68.2;
Ins Num : 1;
Status  : Active;
Seq Num : 3412617
Peer Seq: 0A014402 (S1)
IPv4,SGT: <10.7.7.7 , 1000>
source  : SXP;
Peer IP : 10.10.18.1;
Ins Num : 1;
Seq Num : 3412775
Peer Seq: 0A0A1201(S2),0A63010B (R2),0A014402(S1)
IPv4,SGT: <10.7.7.7 , 1000>
source  : SXP;
Peer IP : 10.210.1.1;
Ins Num : 1;
Seq Num : 3412809
Peer Seq: 0AD20101(S3),0A63010B (R2),0A014402(S1)
IPv4,SGT: <10.7.7.7 , 1000>
source  : SXP;
Peer IP : 10.210.2.1;
Ins Num : 1;
Seq Num : 91
Peer Seq: 0AD20201 (S4),0A63010B (R2),0A014402(S1)
IPv4,SGT: <10.7.7.7 , 1000>
source  : SXP;
Peer IP : 10.210.0.2;
Ins Num : 1;
Seq Num : 3412807
Peer Seq: 0AD20002(S5),0A63010B (R2),0A014402(S1)
```

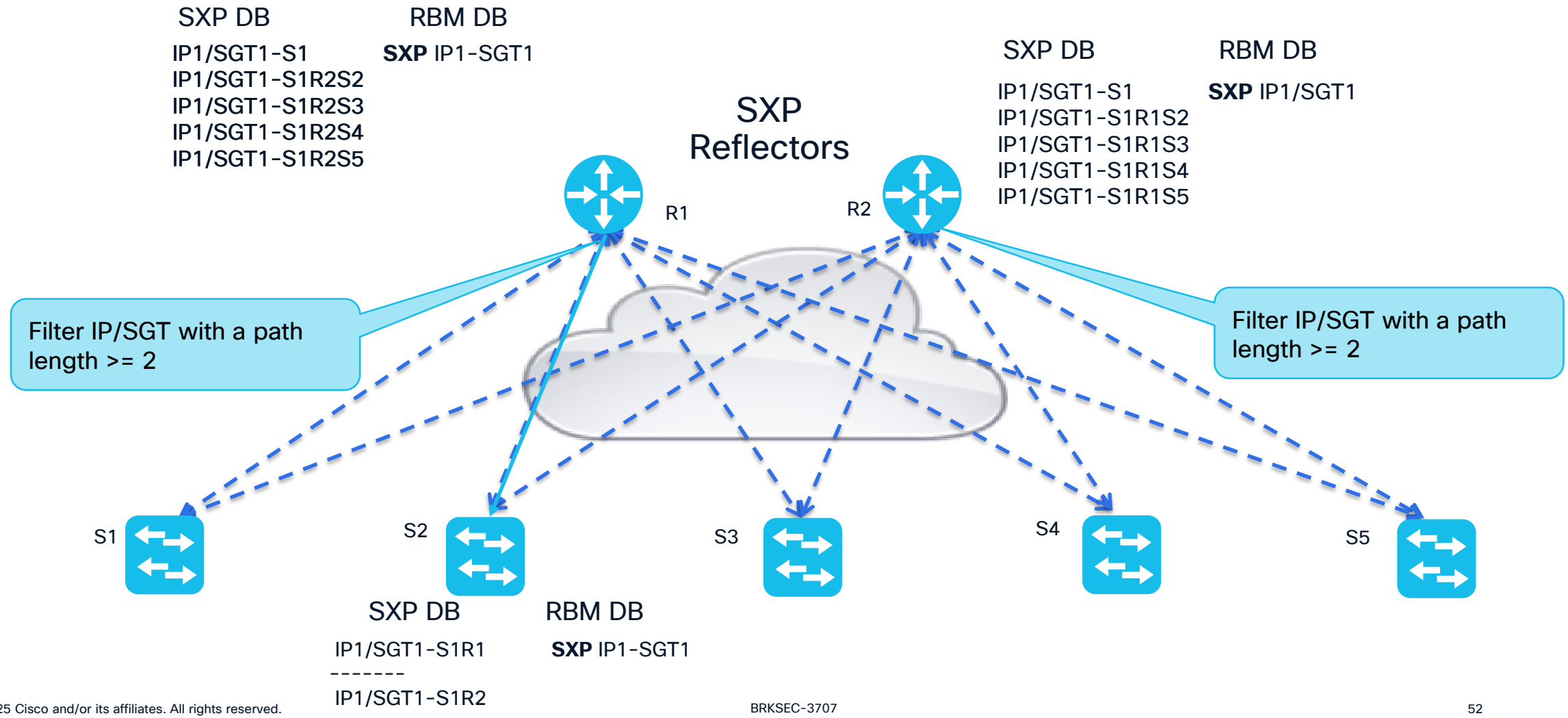
For your reference

Peer Speaker

Originator

Path Length – Design Consideration

For your reference



Enable SXP Path Length Filtering

- Implement SXP path length override option to limit the SXP database size, before activating SXP
  - Limits the path length for re-advertisement
- Primarily important when bi-directional SXP is in use

```
cts sxp limit export peer-sequence-nodes 2
cts sxp limit import peer-sequence-nodes 2
no cts sxp enable
cts sxp enable
```

Filter IP-SGT with a path length >= 2

May need to ‘cycle’ SXP so that filtering is applied at the creation of the SXP DB

SXP Filters – Option 2

IOS 16.6+

- A “filter-list” based on permit/deny action with matches on IP prefix and/or SGT
- “filter-lists” can be applied globally or to a “filter-group” which can have one or more peers
- The ”filter-list” applied to the updates as they happen in the protocol
  - SXP Listener – As the IP/SGT is received
  - SXP Speaker – As the IP/SGT is sent
- If the ”filter-list” is applied after the SXP/Master DBs are built, then it will only be applied to “new” IP/SGTs sent/received
- A max. of 256 filters are allowed with each filter having a maximum of 128 rules
- 8 SGTs can be specified for each line
- IPv6 supported

```
cts sxp filter-enable
!
cts sxp filter-list ingress-filter
 permit ipv4 10.1.101.0/24
 deny ipv4 0.0.0.0/0
!
cts sxp filter-list egress-filter
 deny sgt 6 10 100
 permit sgt all
 deny ipv4 11.0.0.0/8
 permit ipv4 0.0.0.0/0
!
cts sxp filter-group speaker egress-group
 filter egress-filter
 peer ipv4 10.200.100.39
!
cts sxp filter-group listener ingress-
group
 filter ingress-filter
 peer ipv4 10.200.100.39
!
Site_1_WAN#show cts sxp filter-list
Filter-name: ingress-filter (0)
    10 permit ipv4 10.1.101.0/24 (0)
    20 deny ipv4 0.0.0.0/0 (0)
```

Default Route Classification

- New in IOS XE 16.11
- **Default route (dynamic or static) must exist for proper classification and enforcement**
- 0.0.0.0/0 is not exported via SXP per design specification on IOS XE
- Available on N7K in NXOS 7.3(0)D1(1) – N7K can allow it via ”cts sxp allow default-route-sgt”

```
cat9300-1(config)#cts role-based sgt-map 0.0.0.0/0 sgt 2500
%Please ensure default route is created using ip route 0.0.0.0 command
!
!
Cat9300-1#sho cts role-based sgt-map all details
Active IPv4-SGT Bindings Information

IP Address              Security Group                          Source
========================================================================
0.0.0.0/0               2500:Internet_SGT                        CLI
!
!
cat9300-1#show ip route
-- snip –
Gateway of last resort is 172.23.41.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.23.41.1
!
!
Cat9300-1#sh cts role-based permissions
--snip--
IPv4 Role-based permissions from group 60:IoT_Sensors to group 2500:Internet_SGT:
        deny_log-01
!
!
Jun  9 20:44:29.700: %FMANFP-6-IPACCESSLOGSGDP: R0/0: fman_fp_image:
ingress_interface='GigabitEthernet1' sgacl_name='deny_log-01' action='Deny'
protocol='icmp' src-ip='10.2.254.10' dest-ip='172.23.41.1' type='2048' code='0'
sgt='19' dgt='2500' logging_interval_hits='1'
```

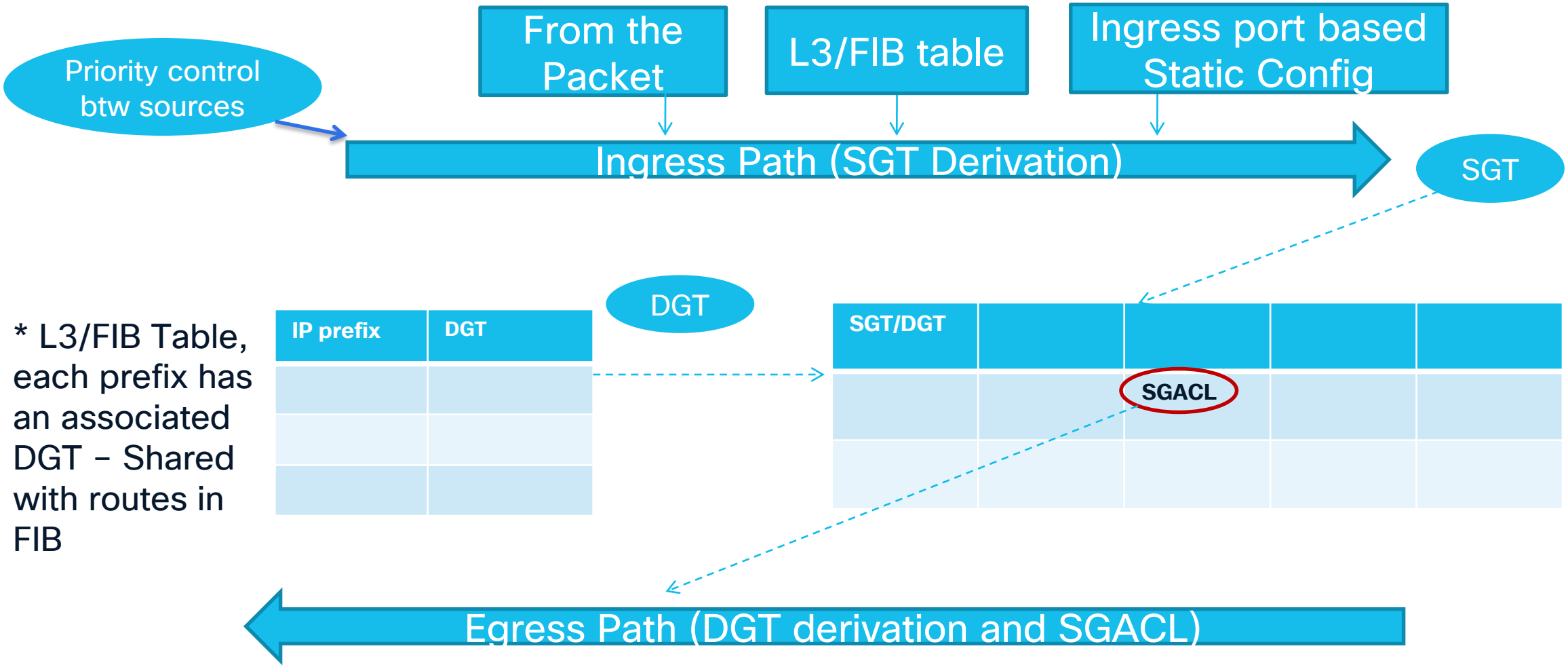
Manual classification of the “Internet”

- Internet could be classified using the allowed IP CIDRs, either via ISE or directly on perimeter devices
- 1.0.0.0/8, 2.0.0.0/7, 4.0.0.0/6, 8.0.0.0/7, 11.0.0.0/8, 12.0.0.0/6, 16.0.0.0/4, 32.0.0.0/3, 64.0.0.0/3, 96.0.0.0/6, 100.0.0.0/10, 100.128.0.0/9, 101.0.0.0/8, 102.0.0.0/7, 104.0.0.0/5, 112.0.0.0/5, 120.0.0.0/6, 124.0.0.0/7, 126.0.0.0/8, 128.0.0.0/3, 160.0.0.0/5, 168.0.0.0/8, 169.0.0.0/9, 169.128.0.0/10, 169.192.0.0/11, 169.224.0.0/12, 169.240.0.0/13, 169.248.0.0/14, 169.252.0.0/15, 169.255.0.0/16, 170.0.0.0/7, 172.0.0.0/12, 172.32.0.0/11, 172.64.0.0/10, 172.128.0.0/9, 173.0.0.0/8, 174.0.0.0/7, 176.0.0.0/4, 192.0.1.0/24, 192.0.3.0/24, 192.0.4.0/22, 192.0.8.0/21, 192.0.16.0/20, 192.0.32.0/19, 192.0.64.0/18, 192.0.128.0/17, 192.1.0.0/16, 192.2.0.0/15, 192.4.0.0/14, 192.8.0.0/13, 192.16.0.0/12, 192.32.0.0/11, 192.64.0.0/10, 192.128.0.0/11, 192.160.0.0/13, 192.169.0.0/16, 192.170.0.0/15, 192.172.0.0/14, 192.176.0.0/12, 192.192.0.0/10, 193.0.0.0/8, 194.0.0.0/7, 196.0.0.0/6, 200.0.0.0/5, 208.0.0.0/4, 224.0.1.0/24, 224.0.2.0/23, 224.0.4.0/22, 224.0.8.0/21, 224.0.16.0/20, 224.0.32.0/19, 224.0.64.0/18, 224.0.128.0/17, 224.1.0.0/16, 224.2.0.0/15, 224.4.0.0/14, 224.8.0.0/13, 224.16.0.0/12, 224.32.0.0/11, 224.64.0.0/10, 224.128.0.0/9, 225.0.0.0/8, 226.0.0.0/7, 228.0.0.0/6, 232.0.0.0/6, 236.0.0.0/7, 238.0.0.0/8, 64:ff9b::/96, 2000::/3, ff0e::/16

Hardware Forwarding SGT/SGACL

- Two Groupings of Hardware Forwarding
- Port/VLAN based
  - Cat 3K-X , IE4K, etc.
  - N5500
- IP/SGT Based
  - Cat9K/Cat9K-X/Cat 6K-Sup2T
  - N7K – M series and F series
  - Cat 4K/Sup7E/Sup8E
  - Cat 3850/5760
  - Cat 8K/ISR1100/ ASR1K
- Each type of hardware has different scaling limits
  - There are limits on the number of SGT/DGT policies as well as Access Control Entries (ACE) in TCAM
  - All hardware shares ACE entries when possible, amongst SGT/DGT

SGT and DGT Derivation in Cat9K

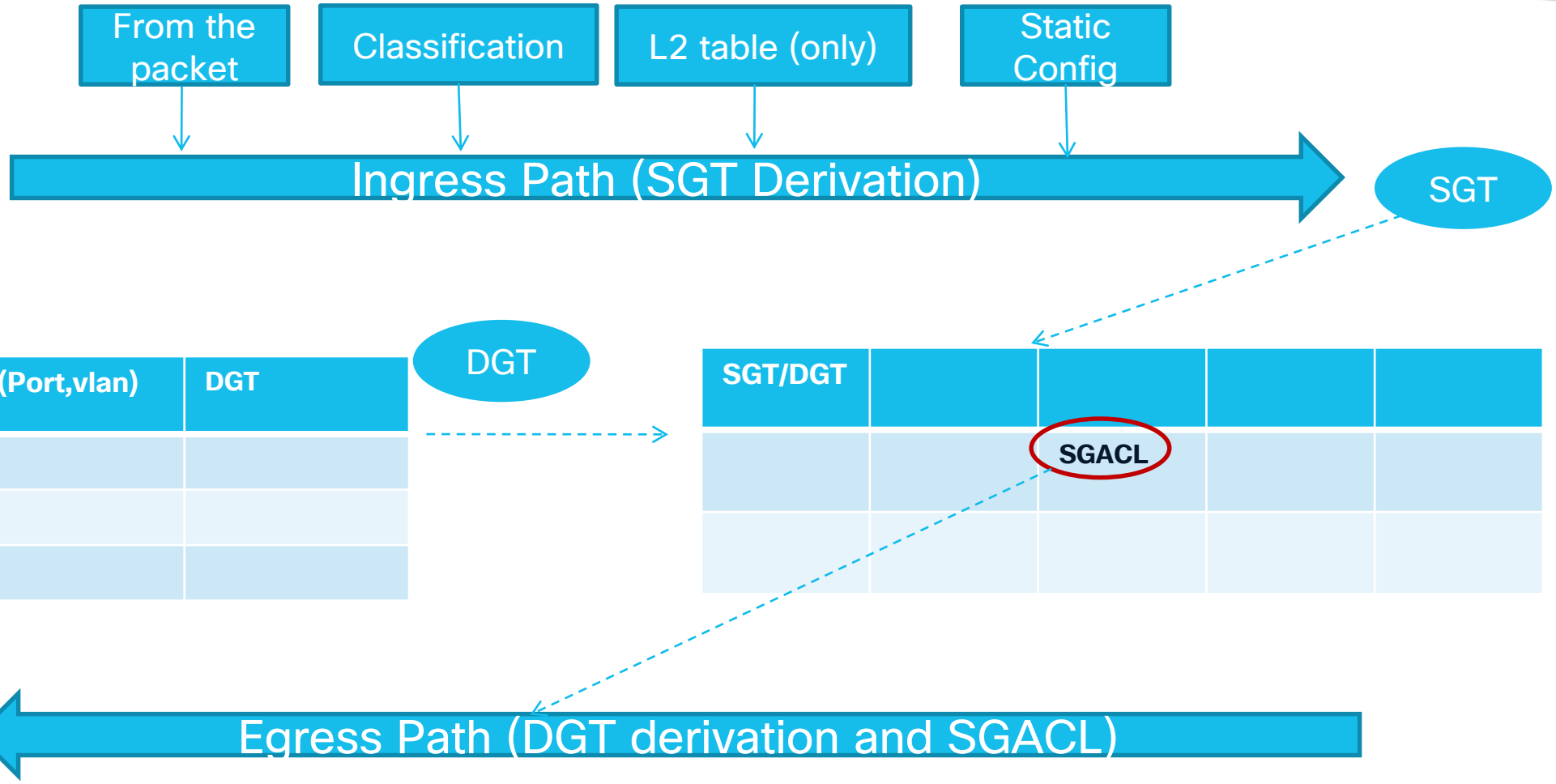


* L3/FIB Table, each prefix has an associated DGT – Shared with routes in FIB

* A number of SGT(DGT) assignments, e.g. SXP, VLAN-SGT, Subnet/Host SGT can exist at the same time. Each will be against a priority list and the winning result will be programmed into the L3/FIB table

SGT and DGT Derivation in some IE switches and 3K-X product line

For your reference



Each (Port,vlan) can have one DGT associated with it.

Implications of Hardware Forwarding Capabilities

- Port/VLAN Based Hardware
- Limited SXP applicability due to the SGT derivation on mac/port
- Fine to be speakers/relays but not SGT/DGT derivation for enforcement from SXP
- Limited number of SGTs per port (one or one per vlan/port)
- Not appropriate for this WLAN access control use case
- IP/SGT Based Hardware Implications
  - Behaves like routing/forwarding – longest match determines SGT
  - Tagging/Enforcement for incoming packet due to FIB lookup for IP/SGT
  - Allows for bidirectional SXP
  - Allows for multi-hop SXP coming into the switch due to FIB lookup for IP/SGT
  - Scale varies per platform since IP/SGT shares FIB TCAM with routing

For your reference

SGT Classification – Binding Source Priority

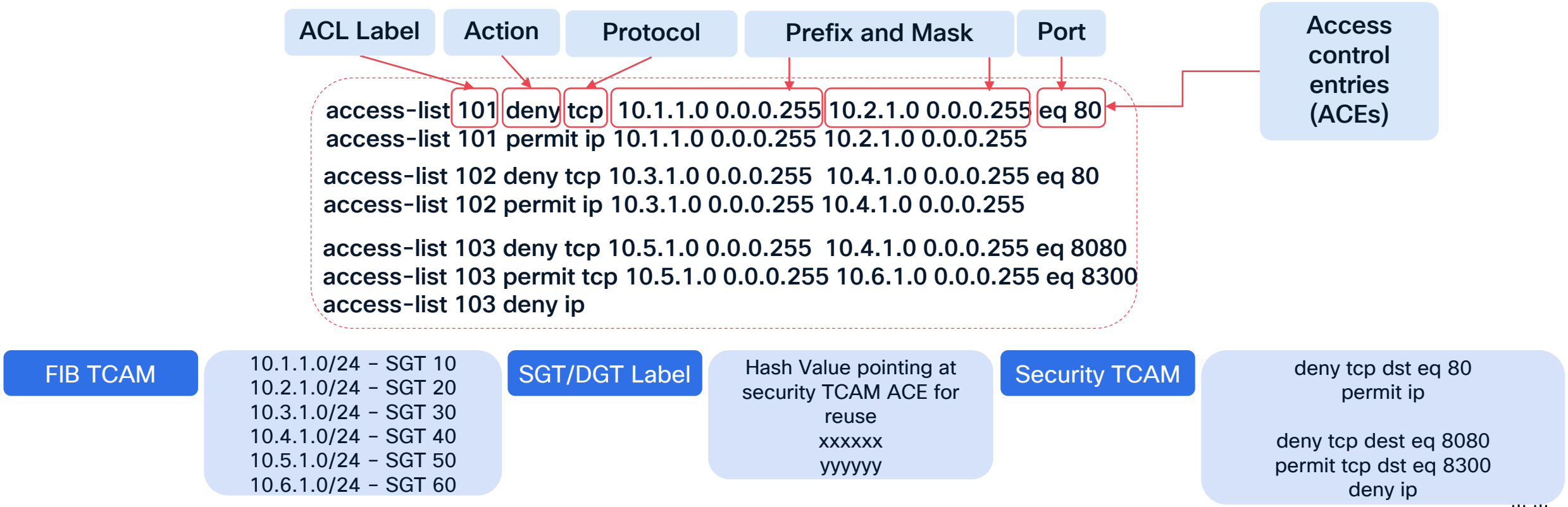
IOS XE

The current priority enforcement order, from lowest (1) to highest (11), is as follows:

1. VLAN – Bindings learned from snooped ARP packets on a VLAN that has VLAN-SGT mapping configured.
2. CLI – Address bindings configured using the IP-SGT form of the cts role-based sgt-map global configuration command.
3. L3IF (Layer 3 Interface) – Bindings added due to FIB forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or Identity Port Mapping on routed ports.
4. LISP-REMOTE-HOST – Bindings for SDA Fabric remote hosts (does not trigger an SGACL download).
5. LISP-LOCAL-HOST – Bindings for SDA Fabric local hosts (does trigger an SGACL download).
6. OMP – Bindings learned from Catalyst SD-WAN Controller (vSmart).
7. SXP – Bindings learned from SXP peers.
8. IP_ARP – Bindings learned when tagged ARP packets are received on a CTS capable link.
9. LOCAL – Bindings of authenticated hosts which are learned via EPM and device tracking. This type of binding also include individual hosts that are learned via ARP snooping on L2 [I]PM configured ports.
10. CACHING – Bindings learned through the SGT Caching feature by gleaning the inline SGT in the packet.
11. INTERNAL – Bindings between locally configured IP addresses and the device own SGT.

Ingress Filtering at Access

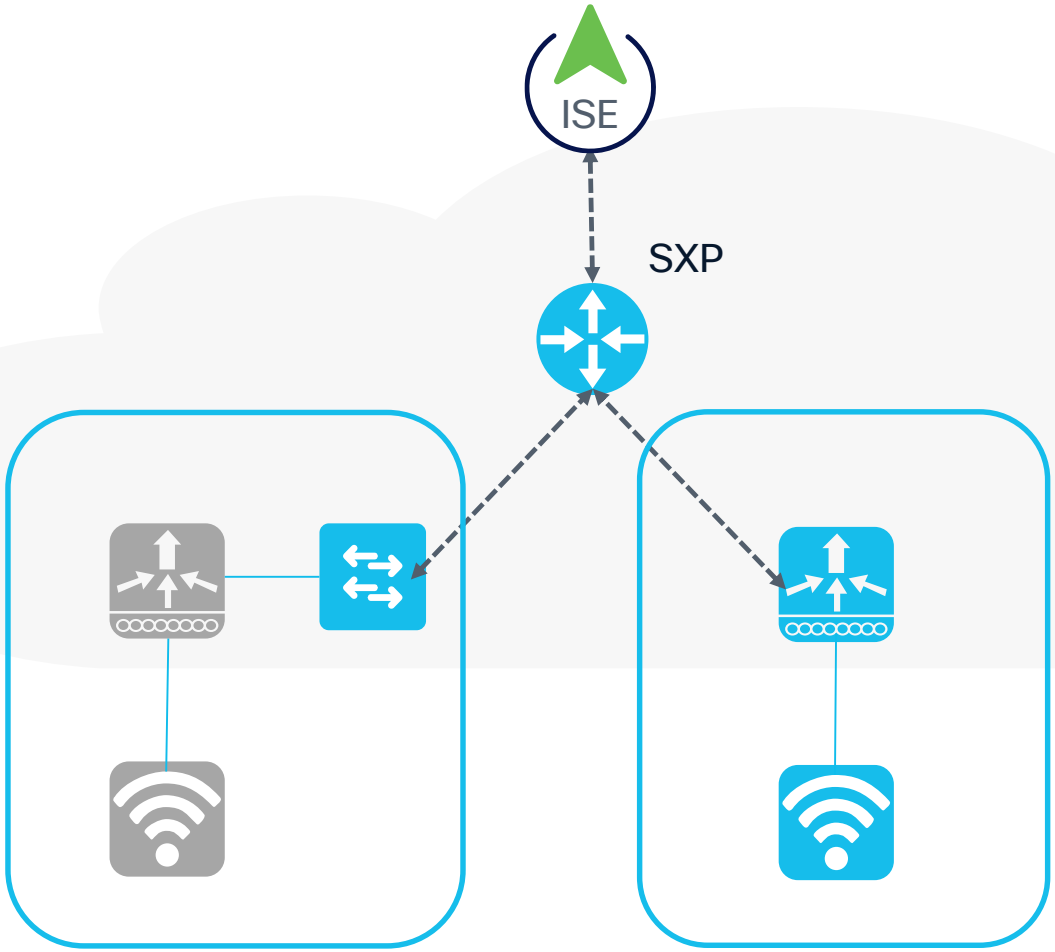
- Put the source IP and/or destination IP into the FIB TCAM
- Create a label for the SGT/DGT pointing at SGACL that allow reuse of security TCAM ACEs
- Security TCAM is only programmed with action/port/protocol match



Wireless Considerations in Design

3rd party WLAN

- VLAN assignment with P2P blocking to force traffic to upstream SGT capable switch
- Alternatively, to SXP the switch can do VLAN/SGT or Subnet/SGT for WLAN VLANs



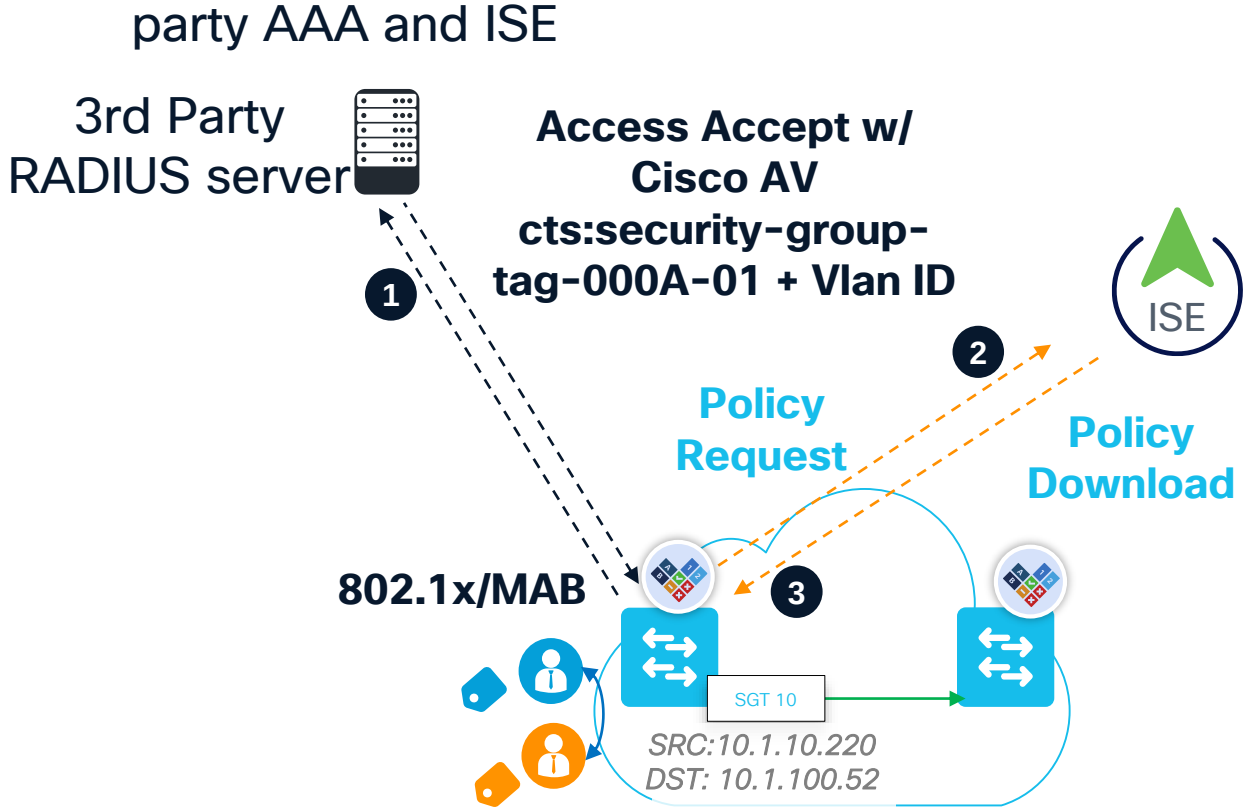
Catalyst 9800

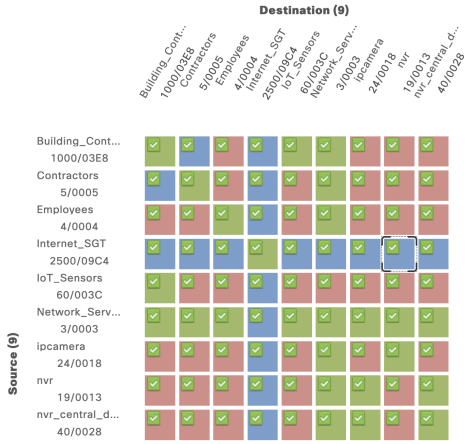
- SXP to C9800 allows North/South enforcement
- East/West traffic even on the same AP is forced to C9800 for enforcement

Document – Cisco Catalyst Wireless Group Based Policy – Link in Notes

3rd Party AAA Integration (ClearPass / FreeRADIUS)

- Authentication and Authorization requests directed to 3rd party
- Policy/SGACL from ISE
- SGT and VN assignments must be coordinated between 3rd party AAA and ISE





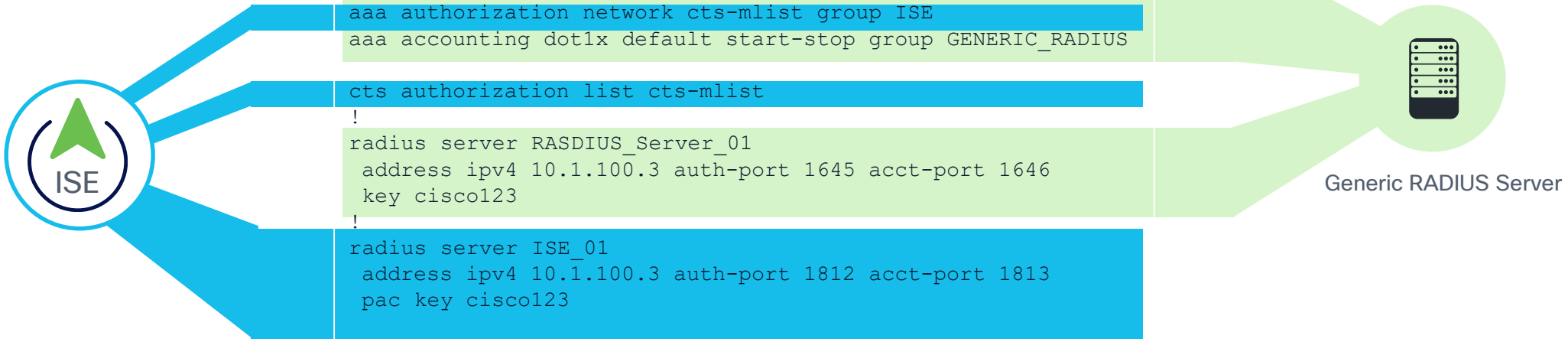
Sample configuration:
https://community.cisco.com/t5/networking-documents/how-to-use-group-based-policies-with-3rd-party-radius-using/ta-p/3930041

3rd party AAA integration

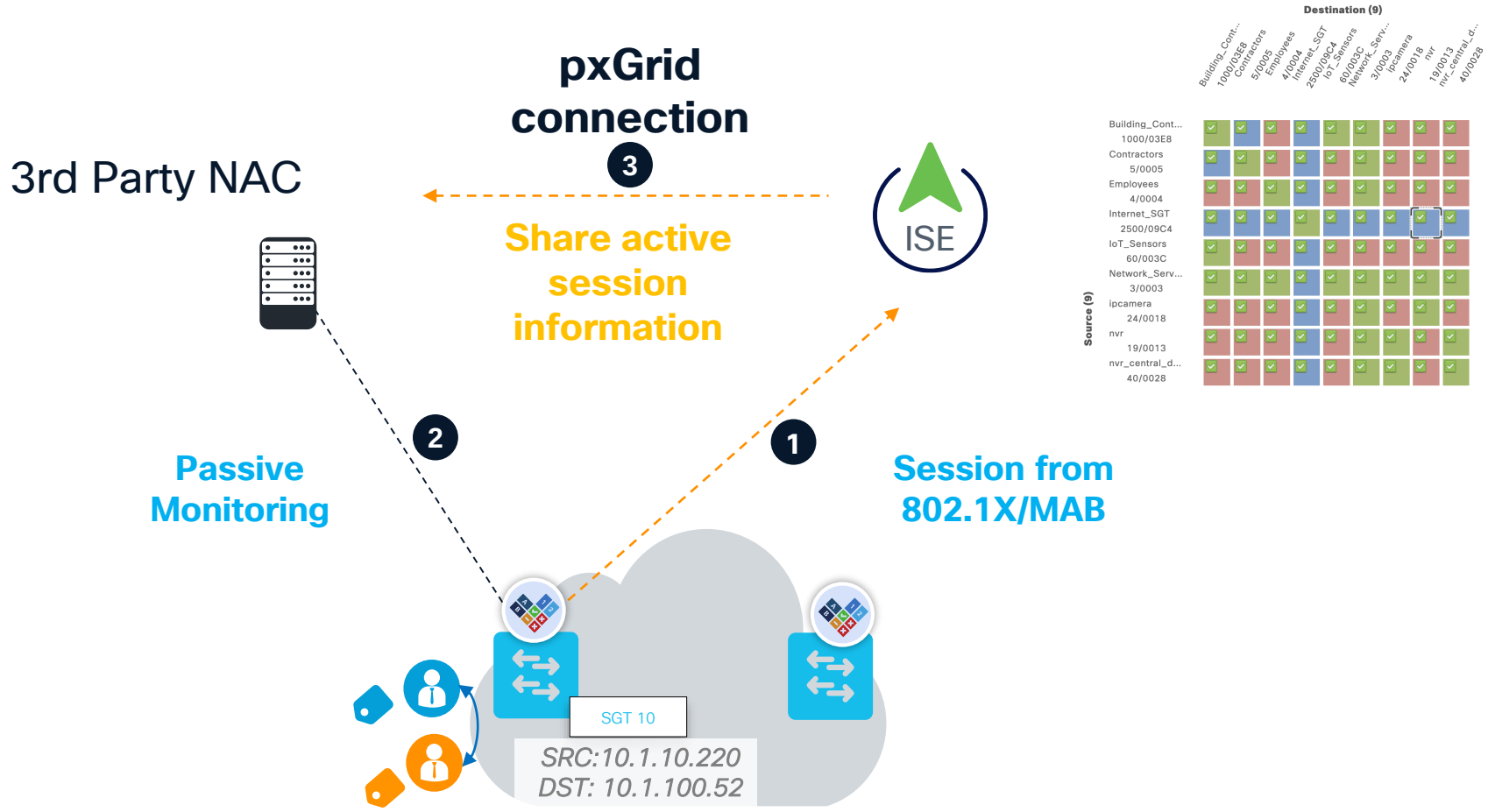
Switch configurations

For your reference

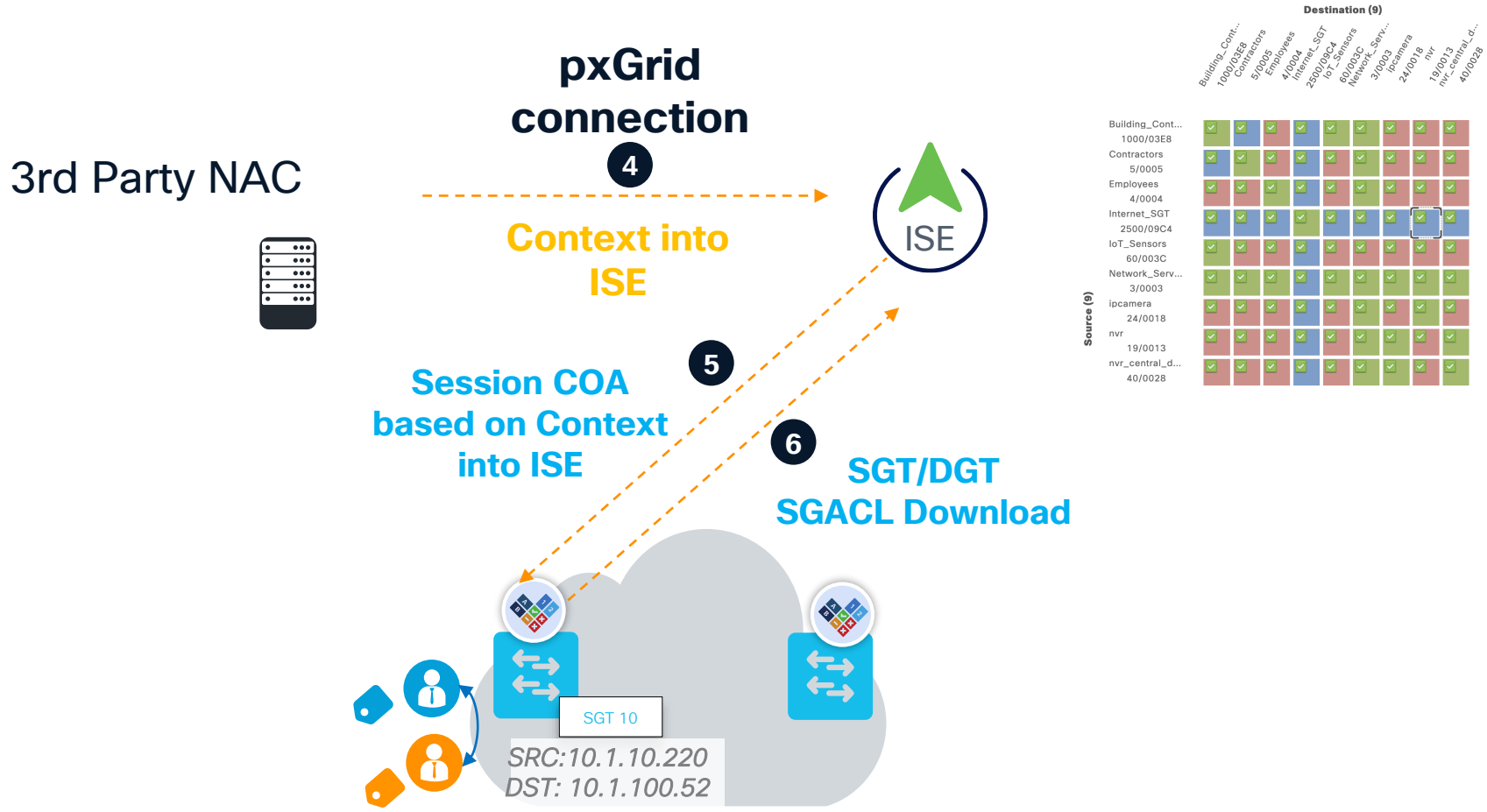
```
9300

!
aaa new-model
!
!
aaa group server radius GENERIC_RADIUS
 server name RADIUS_Server_01
!
aaa group server radius ISE
 server name ISE_01
!
aaa authentication dot1x default group GENERIC_RADIUS
aaa authorization network default group GENERIC_RADIUS
aaa authorization network cts-mlist group ISE
aaa accounting dot1x default start-stop group GENERIC_RADIUS

cts authorization list cts-mlist
!
radius server RASDIUS_Server_01
 address ipv4 10.1.100.3 auth-port 1645 acct-port 1646
 key cisco123
!
radius server ISE_01
 address ipv4 10.1.100.3 auth-port 1812 acct-port 1813
 pac key cisco123
```



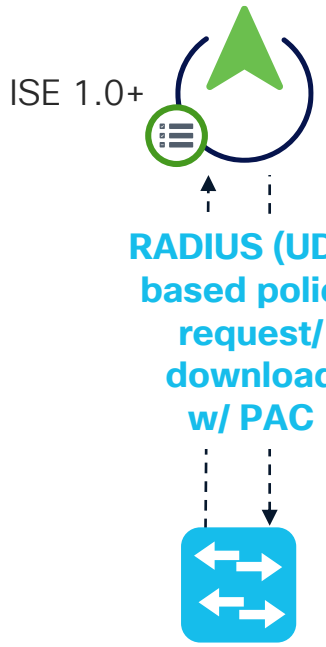
3rd Party NAC Integration 1/2



3rd Party NAC Integration 2/2



Getting SGT Info to Network Devices



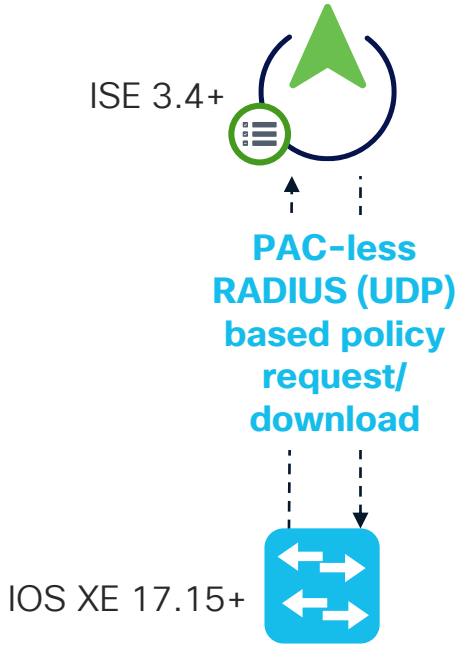
- Large numbers of responses from devices
- Bulk changes fragmented over multiple packets
- Prirt to ISE 3.0P5 switch and ISE PAC process with TLS 1.0
- After ISE 3.0p5 and 17.1(1) for switches and 17.6 for routers PAC process can use TLS 1.2

Reliable transport

No PAC requirement

Future versions to provide additional assurance capabilities

Lossy WAN



Simple RADIUS configuration w/o PAC

No requirement to enable TLS 1.0

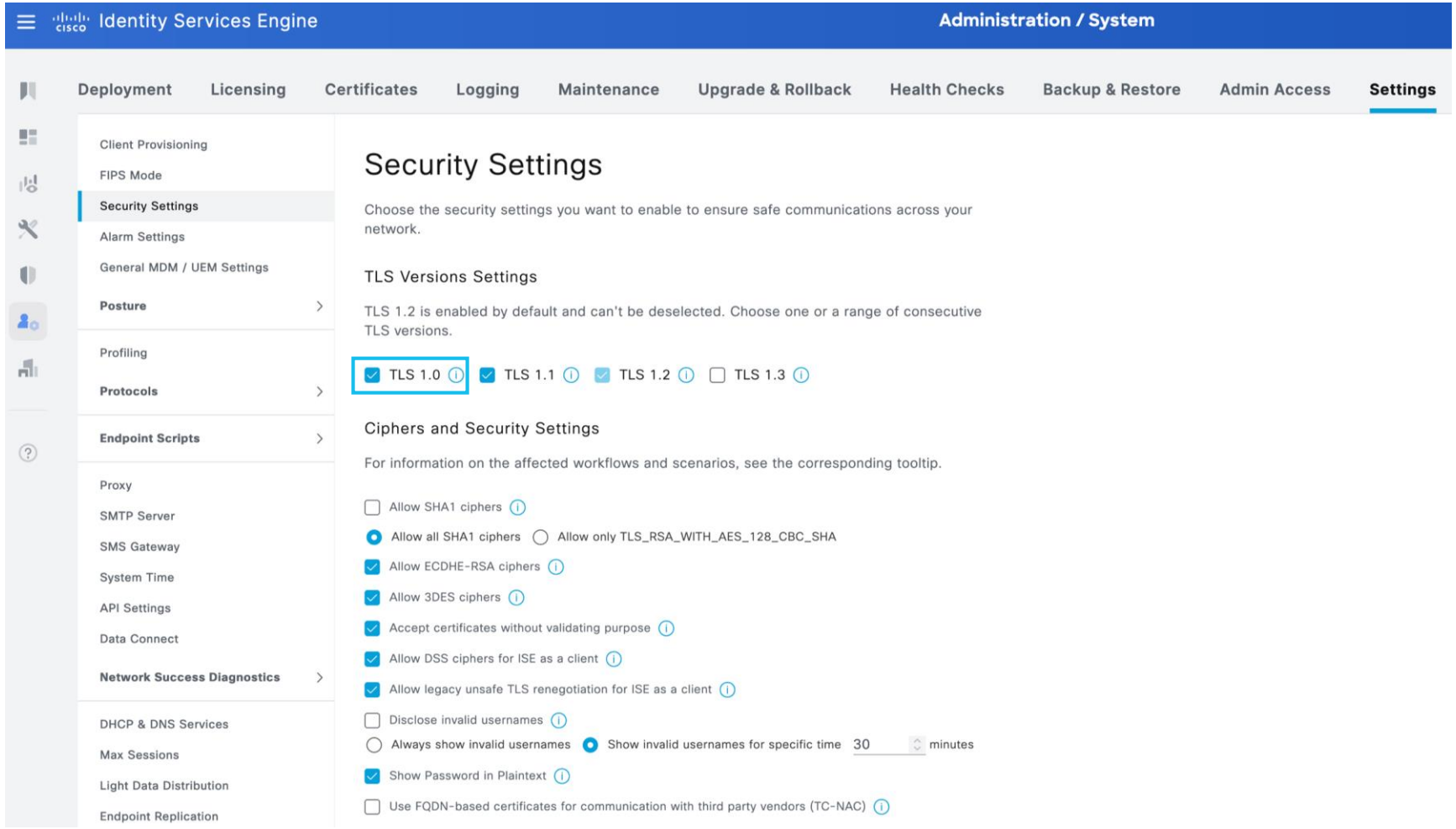
Backwards compatibility

NOTE - ISE FIPS mode disables SGT/SGACL/SXP due to certification testing. FIPS compliance via audit is possible without ISE FIPS mode

Note PACs and TLS

For your reference

- Prior to IOS XE 17.1, TLS 1.0 was required for TrustSec operations
- TLS 1.0 disabled by default in ISE 3.3+
  - Upgrades will retain previous settings
- Since IOS XE 17.1.1 for switches and IOS XE 17.6 for routers, NADs can process PACs using TLS 1.2 (CSCvz48491)



PAC-less RADIUS for CTS

- ISE < 3.4
  - ISE uses a protected access credential (PAC) to authenticate Cisco TrustSec (CTS) NADs
  - PAC can be automatically negotiated (EAP-FAST) between ISE and NADs
- ISE 3.4+
  - Option to communicate with CTS NADs using a shared secret instead of a PAC
  - PAC-less communication is only supported on NADs with IOS-XE 17.5.1+
  - Existing PAC functionality is retained for backward compatibility purposes, although the new shared secret method is preferred

PAC-less RADIUS for CTS

Enable

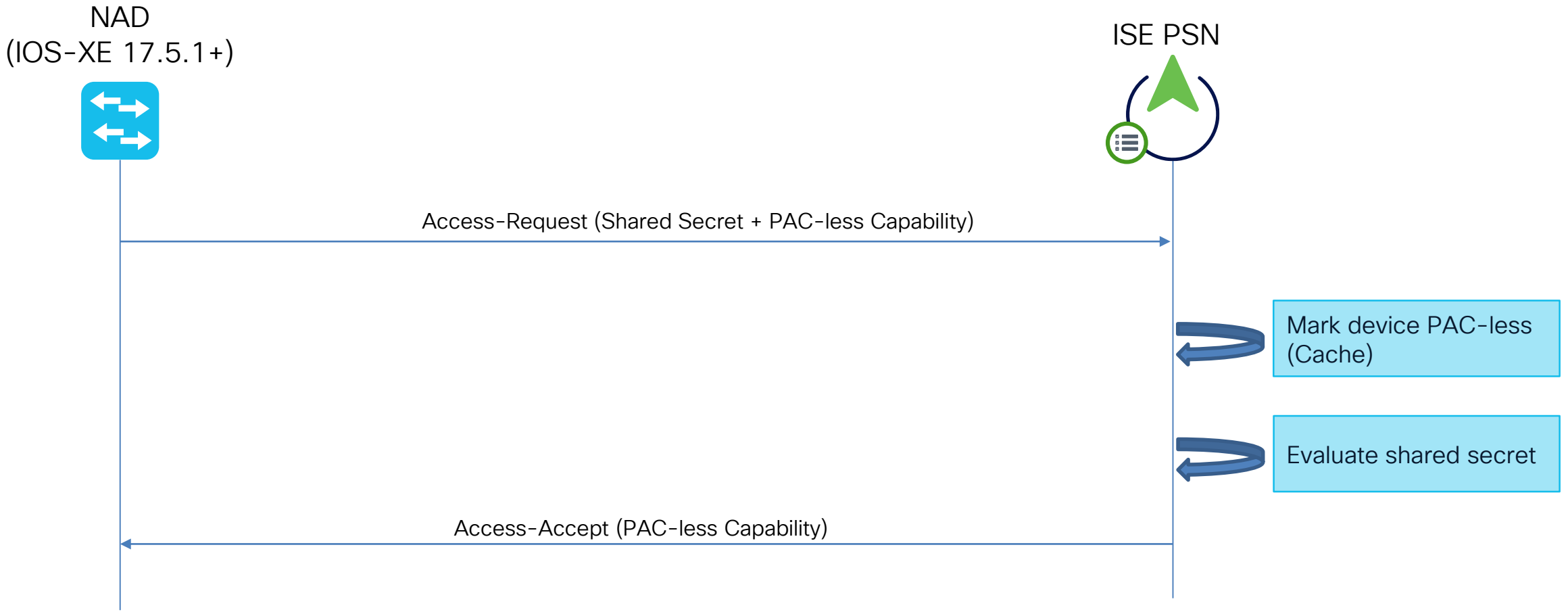
- Does not require configuration changes in ISE
- NADs may require a change in configuration
  - Remove PAC key

```
radius server ISE
  no pac key "encryption-key"
```

PAC-less RADIUS for CTS

Flow

For your reference



PAC-less RADIUS for CTS

Negotiation

	ISE < 3.4		ISE 3.4+	
	Attribute sent by NAD	Result	Attribute sent by NAD	Result
IOS IOS-XE < 17.15.1 Any other CTS NAD	cts-pac-opaque	ISE accepts PAC	cts-pac-opaque	ISE accepts PAC
IOS-XE 17.15.1+ (PAC-less enabled)	cts-pac-capability= cts-pac-less	ISE skips cts-pac-less attribute and sends Access-Reject	cts-pac-capability= cts-pac-less	ISE sends “cts-pac-capability= cts-pac-less“ back with Access-Accept

TrustSec configuration behavior

Local NAD configuration vs. ISE

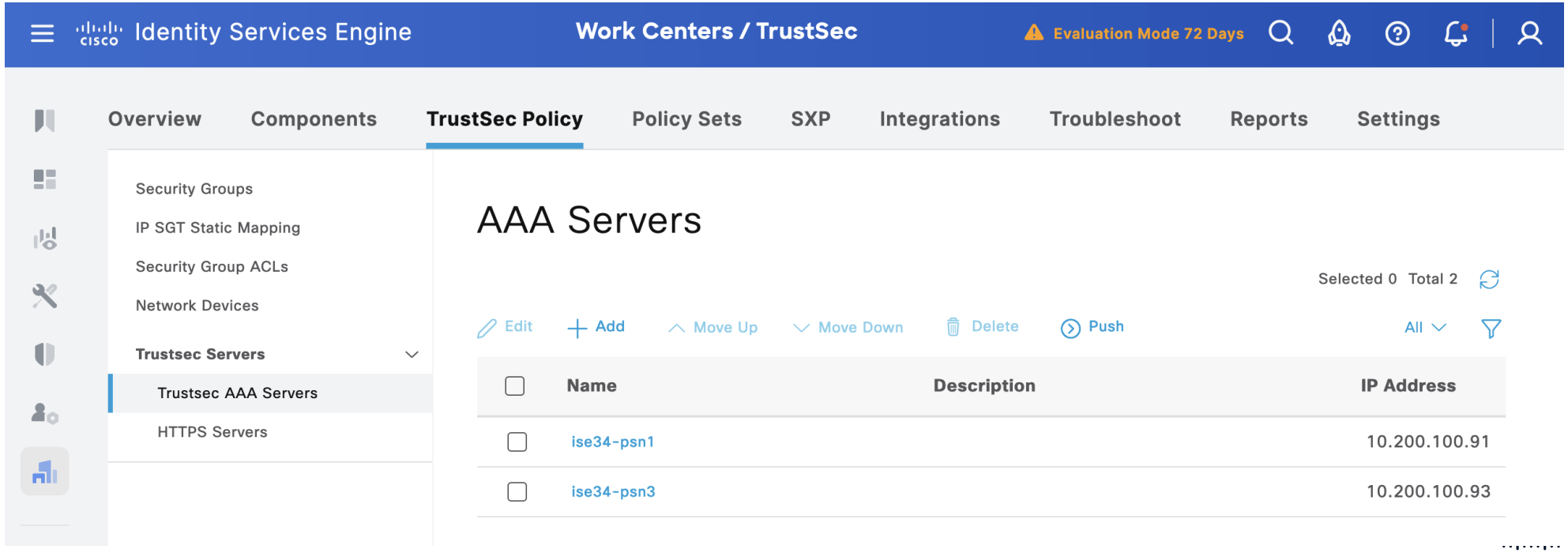
- The ISE policy takes precedence over any local TrustSec policy configuration
  - SGT/DGT Policy
  - SGACL definitions
  - CTS server list
  - Some IP-SGT binding configurations
- Local TrustSec configuration can act as a fallback mechanism

CTS Server List for SGACL Download

For your reference

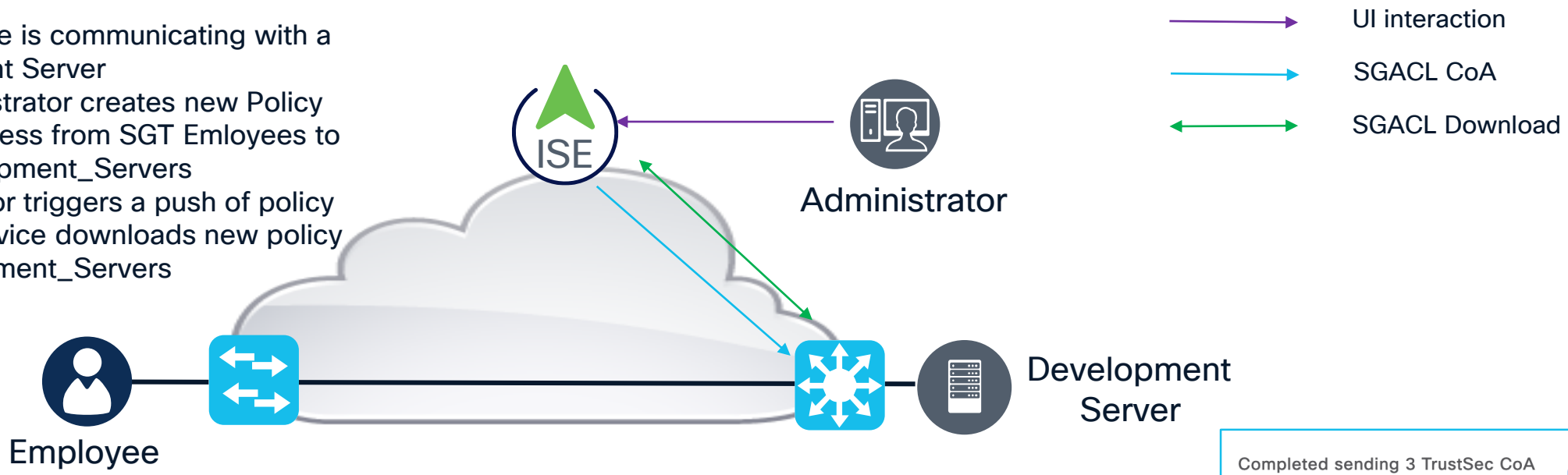
- Server List needs to be defined in ISE in case of multiple PSNs
- Switch requests the policy from the first server (PSN) for the SGT it protects
- Fallbacks to the next server when the first one goes down
- Default server list will only have Primary PAN name and address

Use dedicated CTSPSNs or SLB VIPs in large environments



ISE SGACL Policy Push

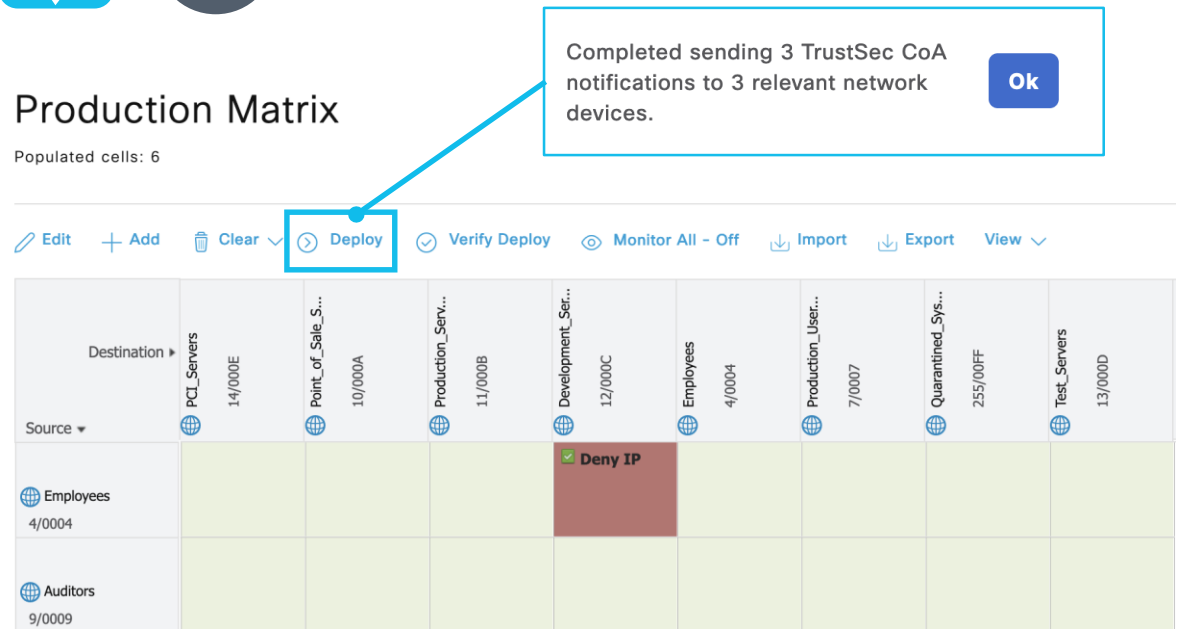
1. An Employee is communicating with a Development Server
2. The Administrator creates new Policy denying access from SGT Emloyees to SGT Development_Servers
3. Administrator triggers a push of policy
4. Network Device downloads new policy for Development_Servers



Applies to SGACL, Environment Data, and Server-List

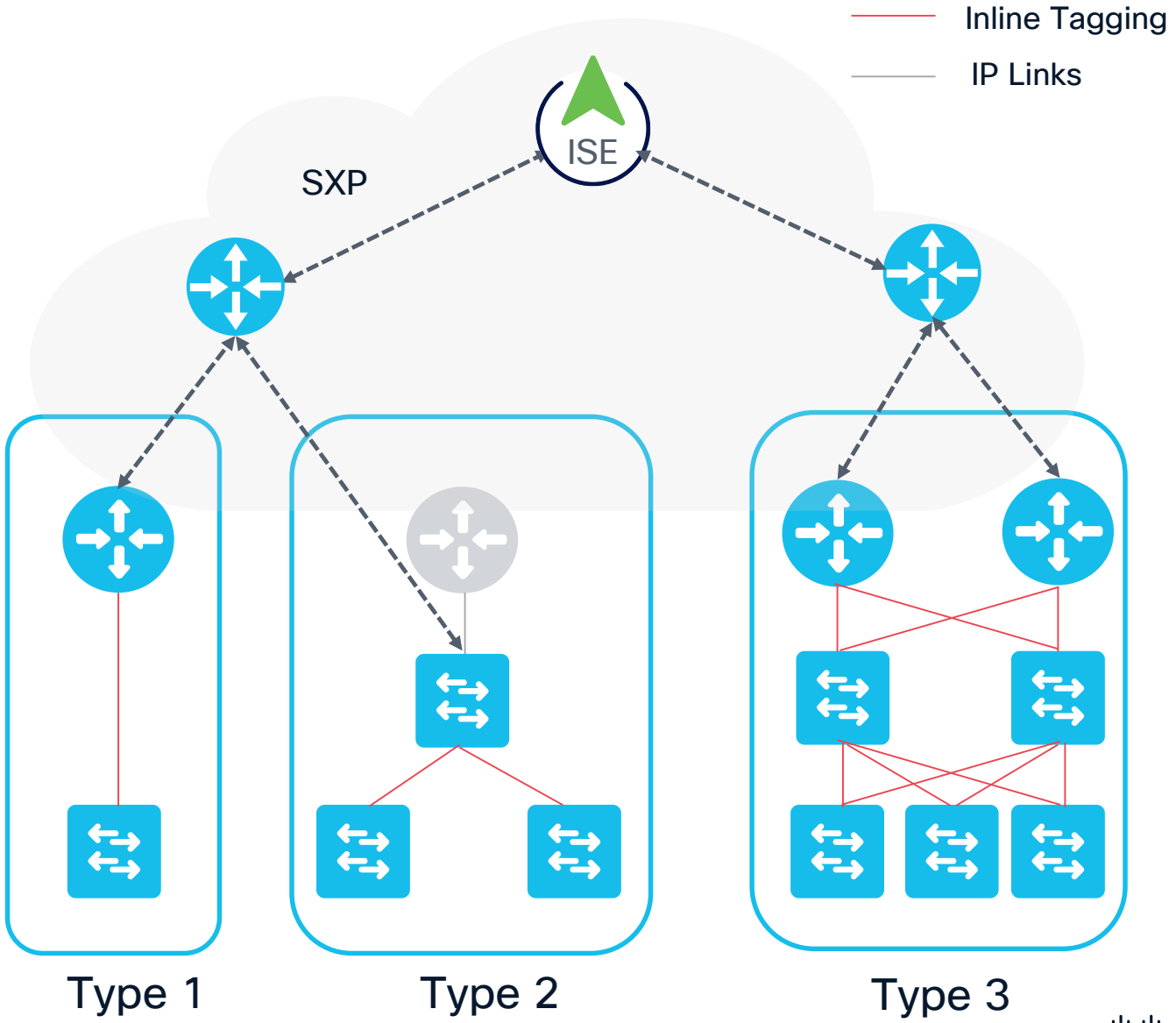
```
aaa server radius dynamic-author
 client 10.200.100.39 server-key 7 01100F175804575D72
! PAN IP Address for SGT related CoA/PSN opt. in 2.4+
 client 10.200.100.40 server-key 7 060506324F41584B5
! PSN IP Address for 802.1X/MAB related CoA
```

* - Reminder to choose RADIUS CoA or CLI depending on needs



Design Evolution – Scaling beyond Ingress

- Challenge: Some sites encountered scale issues with ingress switch and policy directionality
- Solution – Move enforcement closer to egress
  - The source SGT is derived from the packet
  - This allows the egress point to only store the IP/SGT of the destination. And hence only the policy of the destination.
  - The return traffic benefits from the same architecture
  - Hence, the access layer only stores the policies for the endpoints attached to it at any given moment.
  - Use Directional Policy in SGACL



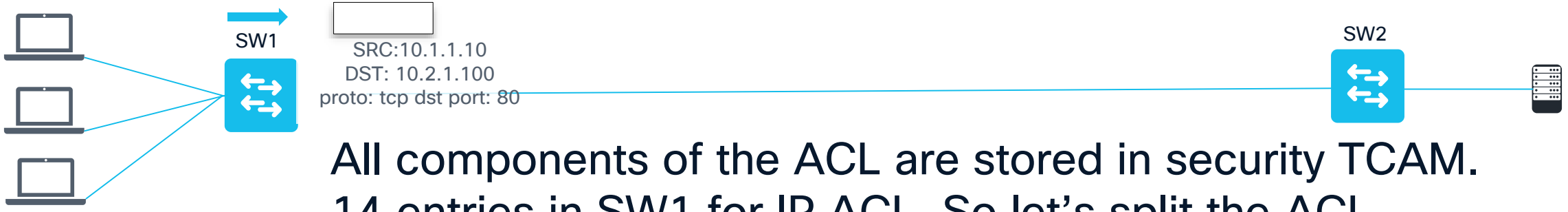
Ingress Enforcement – src/dst ACL on switch

SW1 - Ingress ACL

```
access-list 101 deny tcp 10.1.1.10 255.255.255.255 10.2.1.0 0.0.0.255 eq 80
access-list 101 permit ip 10.1.1.10 255.255.255.255 10.2.1.0 0.0.0.255
access-list 102 deny tcp 10.3.1.10 255.255.255.255  10.4.1.0 0.0.0.255 eq 80
access-list 102 permit ip 10.3.1.10 255.255.255.255 10.4.1.0 0.0.0.255
access-list 103 deny tcp 10.5.1.10 255.255.255.255  10.4.1.0 0.0.0.255 eq 8080
access-list 103 permit tcp 10.5.1.10 255.255.255.255 10.6.1.0 0.0.0.255 eq 8300
access-list 103 deny ip
```

SW1 - Egress ACL

```
access-list 101 deny tcp 10.2.1.0 0.0.0.255 10.1.1.10 255.255.255.255 eq 80
access-list 101 permit ip 10.2.1.0 0.0.0.255  10.2.1.10 255.255.255.255
access-list 102 deny tcp 10.4.1.0 0.0.0.255 10.4.1.10 255.255.255.255 eq 80
access-list 102 permit ip 10.4.1.0 0.0.0.255 10.4.1.10 255.255.255.255
access-list 103 deny tcp 10.6.1.0 0.0.0.255  10.5.1.10 255.255.255.255 eq 8080
access-list 103 permit tcp 10.6.1.0 0.0.0.255 10.5.1.10 255.255.255.255 eq 8300
access-list 103 deny ip
```



All components of the ACL are stored in security TCAM.
14 entries in SW1 for IP ACL. So let's split the ACL

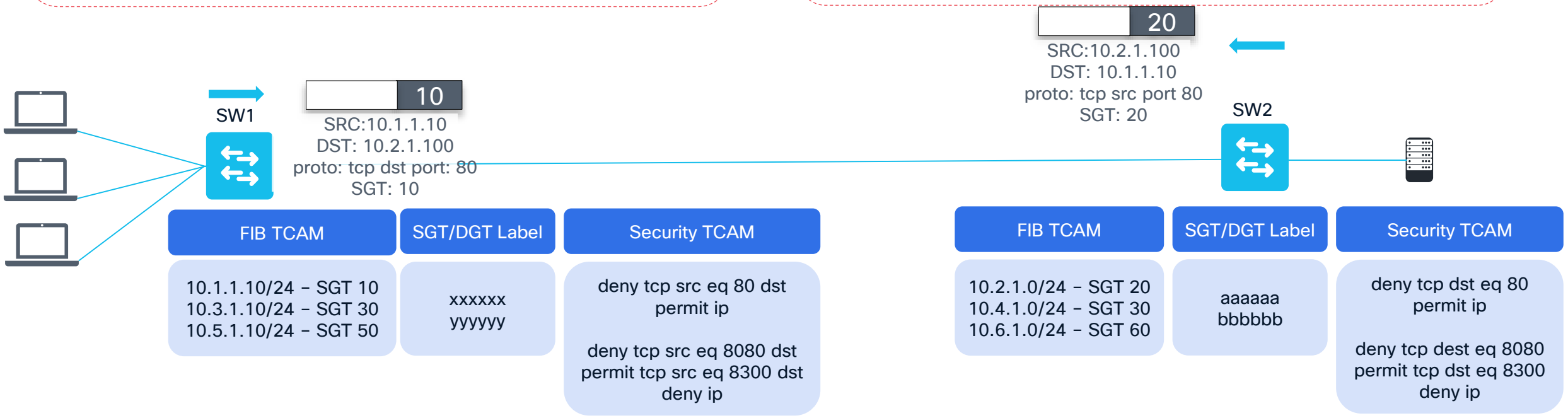
Egress Enforcement – Split src/dst for scaling

SW1 –Without SGT Ingress ACL

```
access-list 101 deny tcp 10.1.1.10 255.255.255.255 10.2.1.0 0.0.0.255 eq 80
access-list 101 permit ip 10.1.1.10 255.255.255.255 10.2.1.0 0.0.0.255
access-list 102 deny tcp 10.3.1.10 255.255.255.255  10.4.1.0 0.0.0.255 eq 80
access-list 102 permit ip 10.3.1.10 255.255.255.255 10.4.1.0 0.0.0.255
access-list 103 deny tcp 10.5.1.10 255.255.255.255  10.4.1.0 0.0.0.255 eq 8080
access-list 103 permit tcp 10.5.1.10 255.255.255.255 10.6.1.0 0.0.0.255 eq 8300
access-list 103 deny ip
```

SW2 – Without SGT Ingress ACL

```
access-list 101 deny tcp 10.2.1.0 0.0.0.255 10.1.1.10 255.255.255.255 eq 80
access-list 101 permit ip 10.2.1.0 0.0.0.255  10.2.1.10 255.255.255.255
access-list 102 deny tcp 10.4.1.0 0.0.0.255 10.4.1.10 255.255.255.255 eq 80
access-list 102 permit ip 10.4.1.0 0.0.0.255 10.4.1.10 255.255.255.255
access-list 103 deny tcp 10.6.1.0 0.0.0.255  10.5.1.10 255.255.255.255 eq 8080
access-list 103 permit tcp 10.6.1.0 0.0.0.255 10.5.1.10 255.255.255.255 eq 8300
access-list 103 deny ip
```



Simple comparison is 14 entries in Security TCAM vs 5 in SW1/2

Configure Links for SGT Tagging

CTS Manual no encryption

```
C9K-1
Interface GigabitEthernet1/5
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement

C9K-2
interface GigabitEthernet1/0/14
 no switchport
 ip address 10.10.20.2 255.255.255.0
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
```

- **port-channel support - cts is configured on the physical interface then added to the port channel**

```
C9K-1#sho cts interface brief
Global Dot1x feature is Enabled
Interface GigabitEthernet1/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:            2:Device_sgt
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration             : N/A
        Cache applied to link  : NONE


    L3 IPM:    disabled.
```

Best Practice - “shut” and “no shut” and interface if device does not after configuration

SXP to Inline SGT*

```
RTR-1#sho run | inc sxp
cts sxp enable
cts sxp default source-ip 10.99.1.10
cts sxp default password cisco123
cts sxp connection peer 10.99.10.12 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.10.13 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.188.1 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.200.10 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.1.36.2 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.3.99.2 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.200.21 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.0.1.2 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.10.1.30 source 10.99.1.10 password default mode local listener
!
RTR-1#sho run int gi 0/0/0
!
interface GigabitEthernet0/0/0
 ip address 10.1.46.2 255.255.255.0
 negotiation auto
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
 cdp enable
!
```

Using standard SXP configuration, arriving IP packets with an existing IP-SGT binding, will be tagged on egress interface (e.g. Gig 0/0/0), when inline tagging is configured

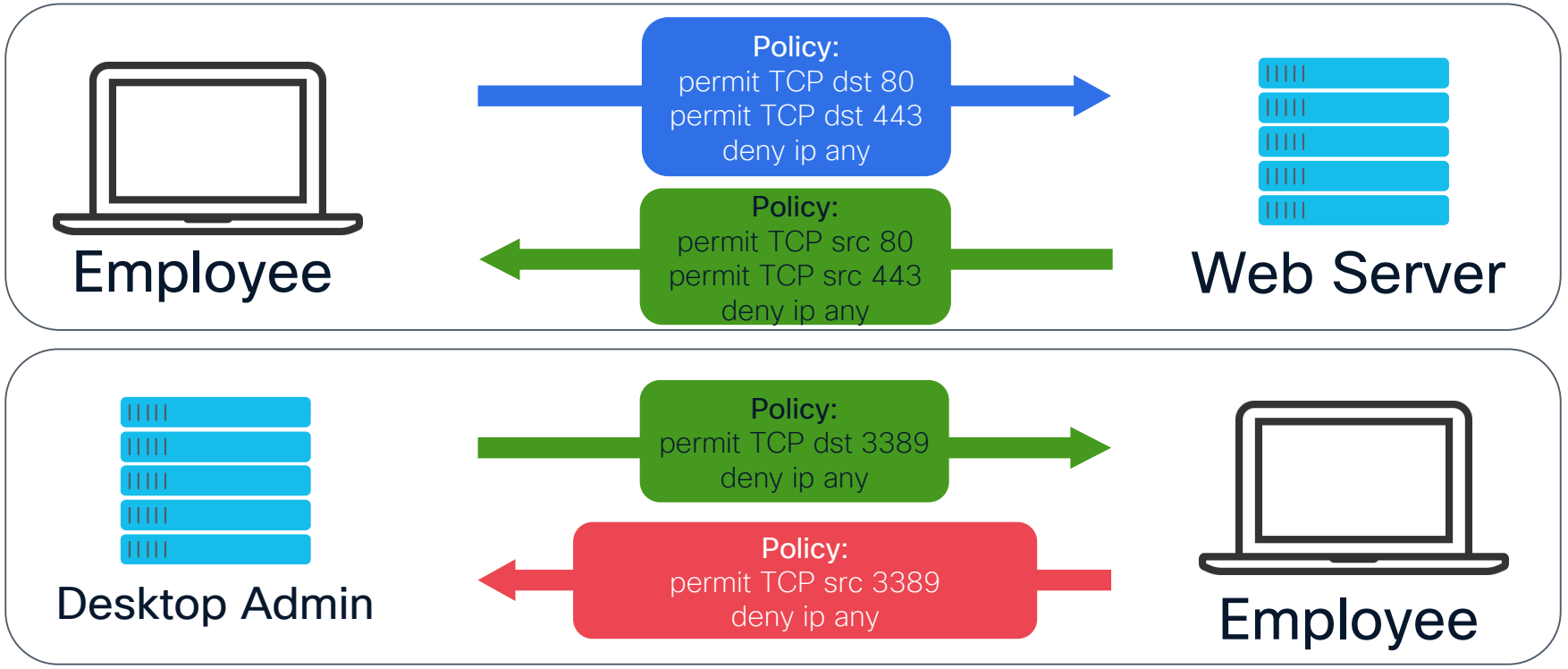
Inline Tagging enabled

Recommended to turn off enforcement when tagging between network devices

* - Control plane to data plane happens by default. Data plane to control plane (SGT caching) is routers only

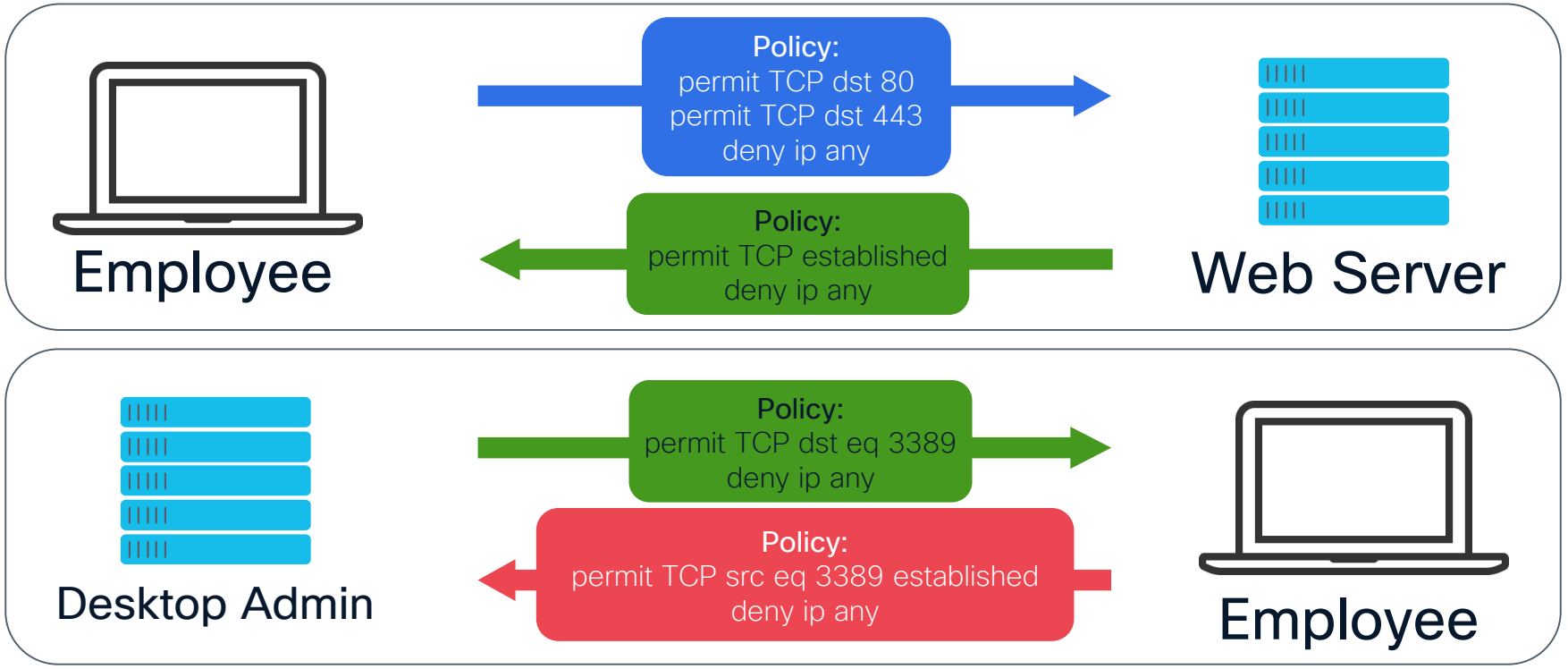
Policy Admin Scaling

SGACL – Bi-Directional Policy – Manual Definition



Policy Admin Scaling

Directional SGACL – TCP Established Usage

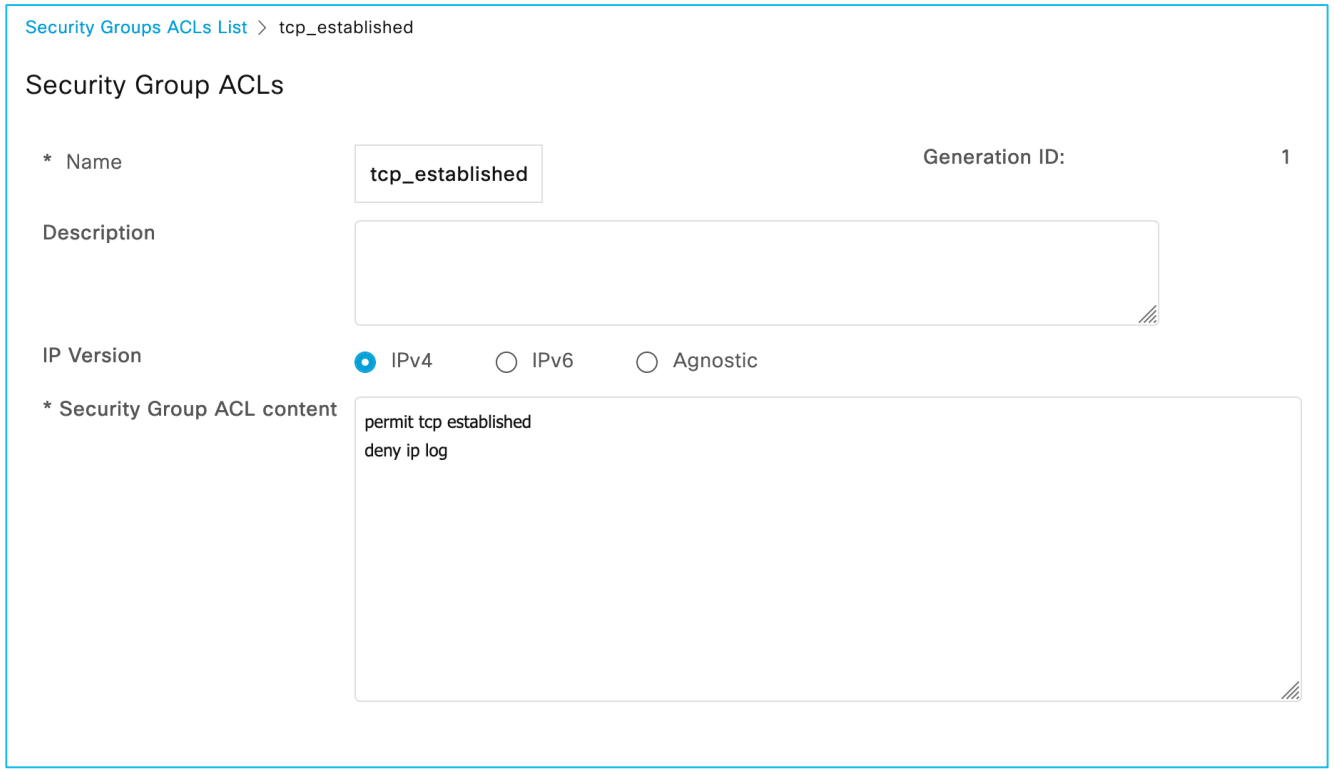


- Reduces manual port matching on TCP based protocols for simpler policy administration
- Supported since IOSXE 17.1

Enforce Based on Directional Traffic

For your reference

- ISE allows for TCP established keyword
- Supported since IOS XE 17.1



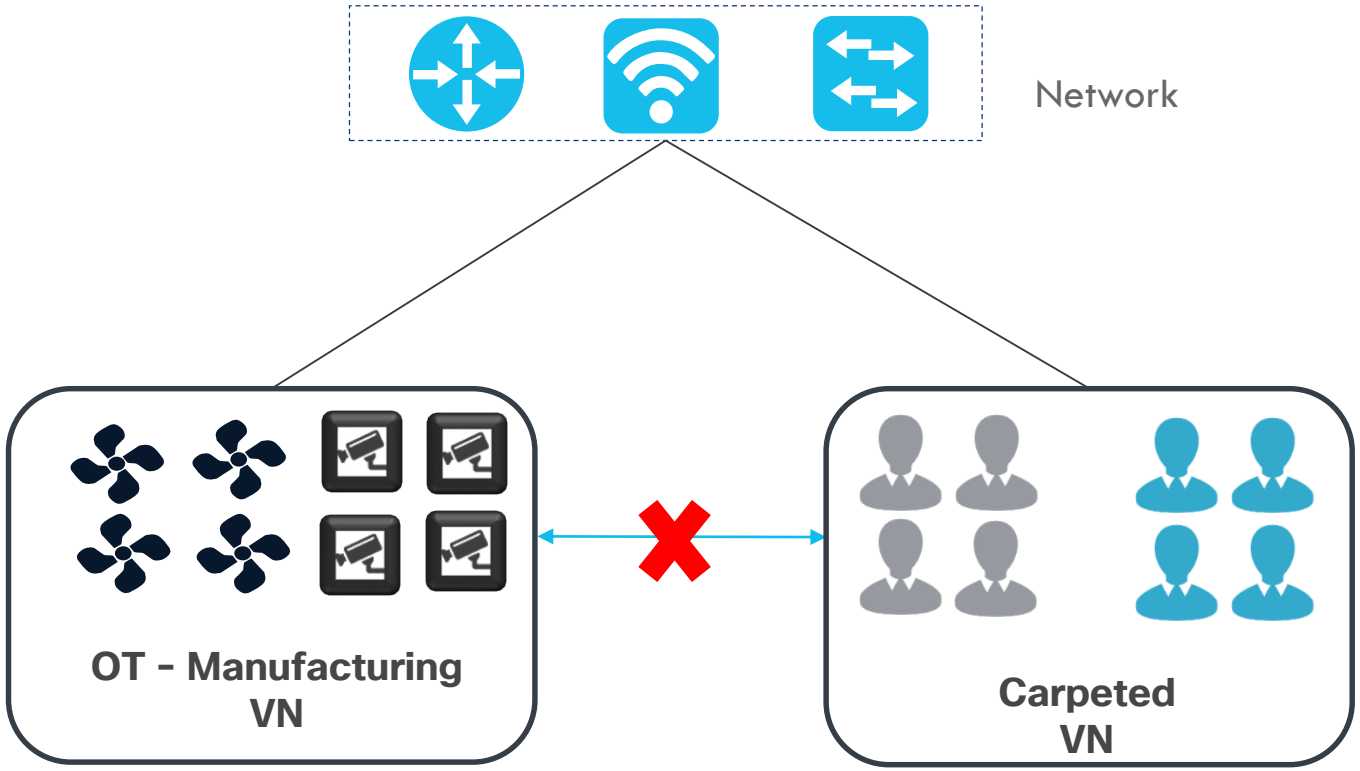
Type 4 Sites – Manufacturing Design Considerations

- Separation of Carpeted and Manufacturing Space
- Traffic to/from Manufacturing Space must transverse a firewall
- Physical Dimensions of Site requires virtualized overlays
- Manufacturer has selected a VXLAN Fabric for creating the virtualized overlays for Manufacturing and Carpeted Space

What is SD-Access?

- Policy/Automation/Assurance for a set of technology innovations
- Subnet availability across access layers w/o stretched VLANs (i.e. spanning tree)
  - Very common in manufacturing, medical, university environments, etc.
  - Especially relevant as IOT enters the enterprise campus/WAN
- Simplified VRF deployment w/o MPLS or VRF lite
  - Distribution/Core can be plain IP while the edges can be the VRF point of presences
  - Simpler connection of VRFs via on demand tunnels as opposed to GRE, etc.
  - EVPN or LISP control planes with VXLAN encapsultion
- Security using SGT/SGACL – Allows end to end tagging via an overlay i.e. “all devices in the middle don’t have to be Cisco”
  - Easy to handle 3rd party distribution/core layers
  - Easy to handle topologies where the WAN router isn’t managed by the enterprise

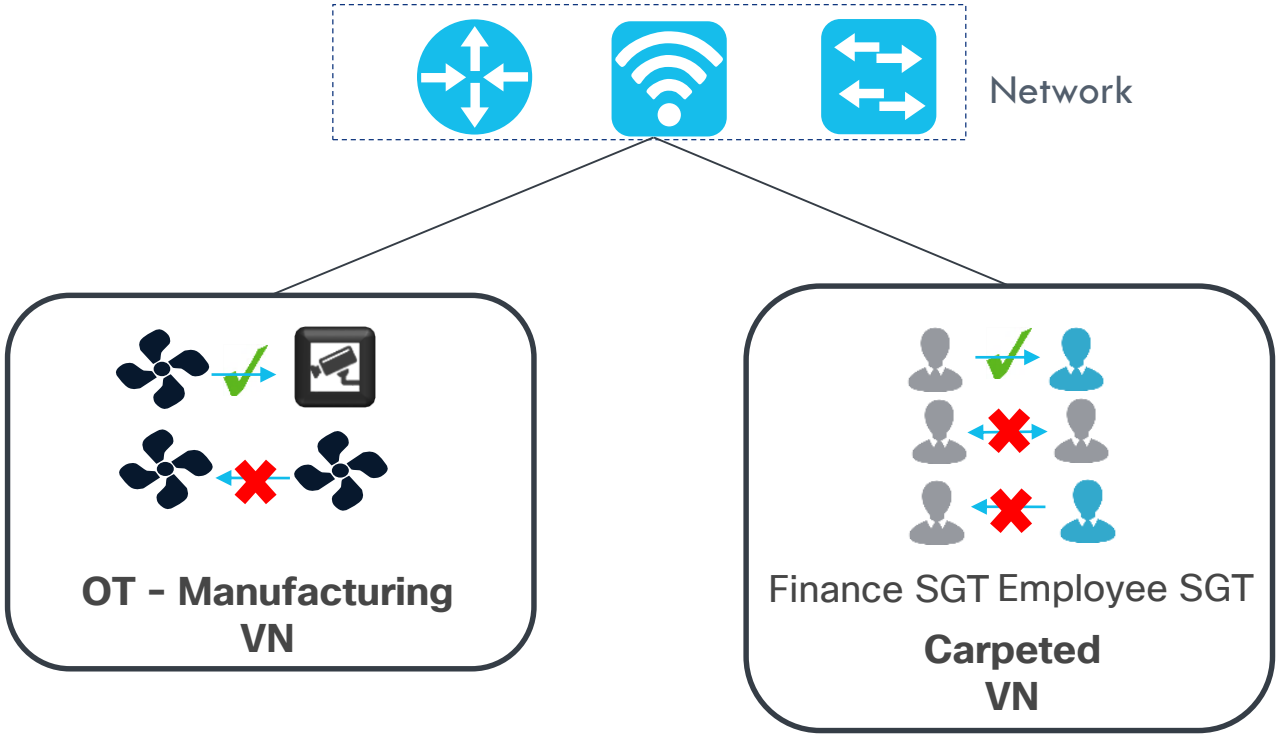
SD-Access
Two Level Hierarchy – Macro Level



Virtual Network (VN)

First level Segmentation that ensures **zero** communication between specific groups. Ability to consolidate multiple networks into one management plane.

SD-Access
Two Level Hierarchy – Micro Level



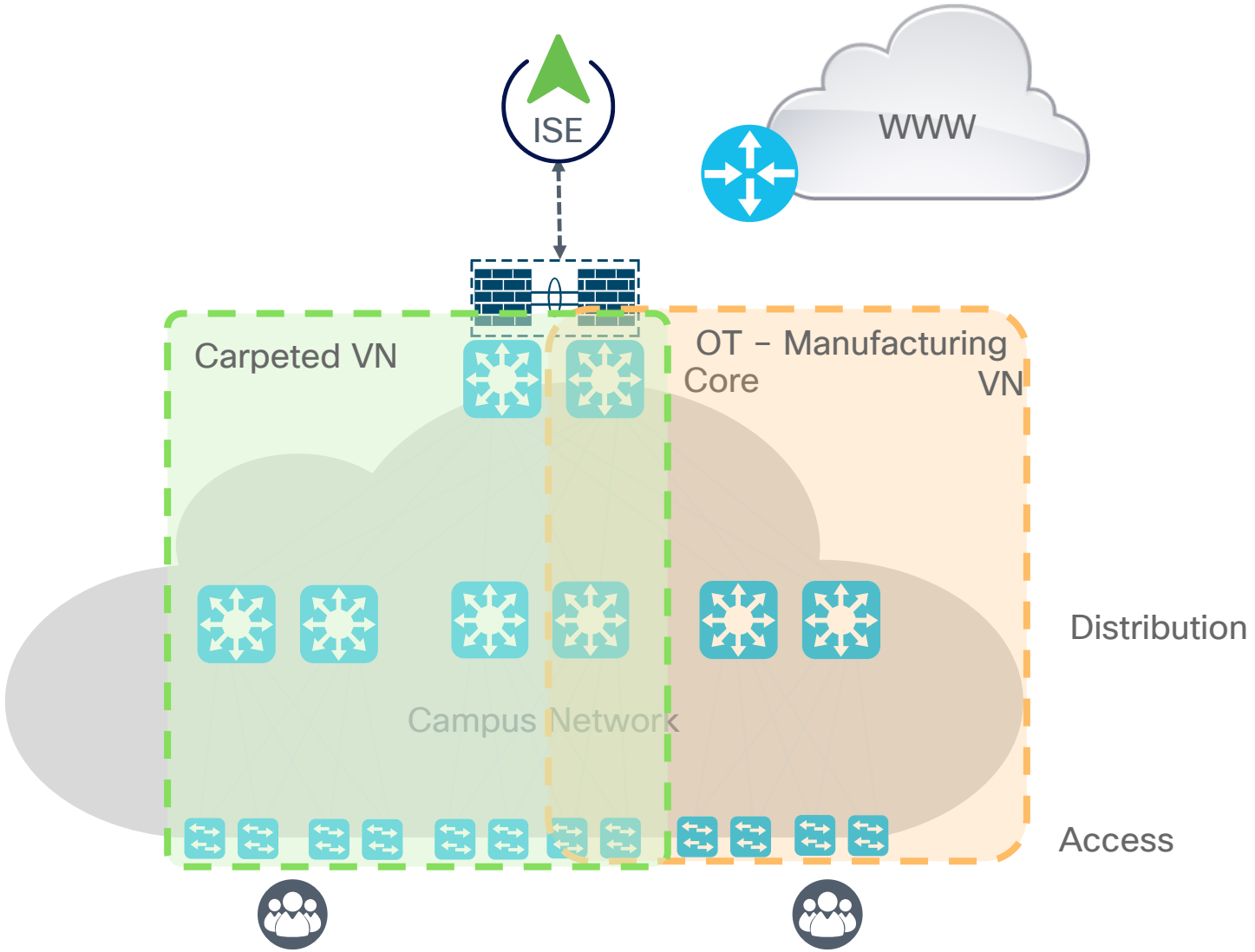
Security Group Tag (SGT)

Second level Segmentation **ensures role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

Groups & Virtual Networks

Type 4 Site – Carpeted and OT VNs

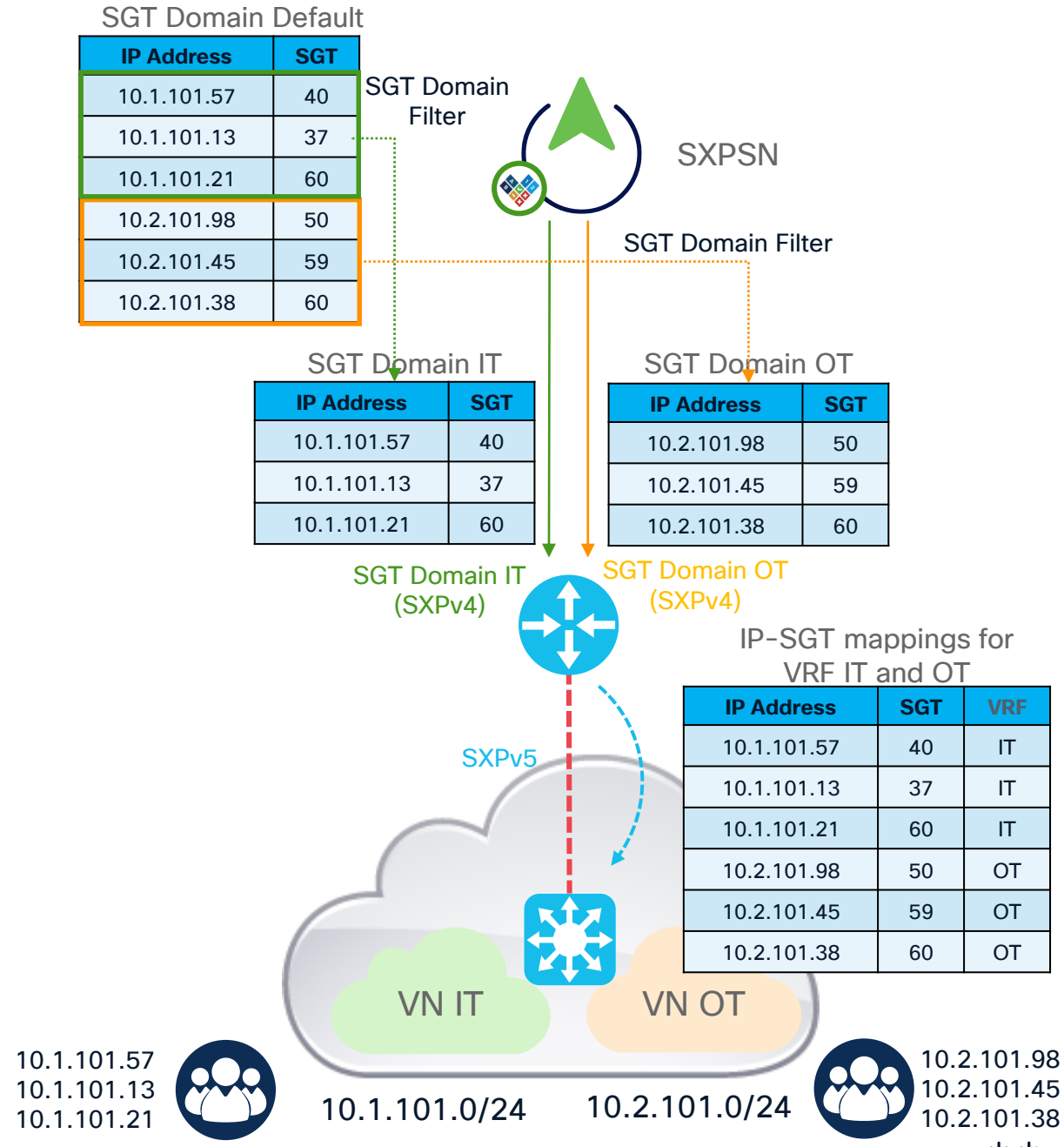
- With SDA – SGTs Groups can be mapped to specific Virtual Networks (VRFs)
- SGTs normally are used across VNs



ISE SGT Domains

SGT propagation using SXP to VN sites

- Since SXPv4 is not VRF-aware, ISE must peer with every VRF on a particular router if SXP bindings are required
- In our scenario, there are two SXPv4 connections from ISE to two different VRFs at the same router at the branch site
- A single SXPv5 connection from the branch router to the branch switch carrying mappings from both VRFs
- SXPv5 delivered in IOS XE 17.9.1



ISE SXPv4 Peering to Router SXPv5

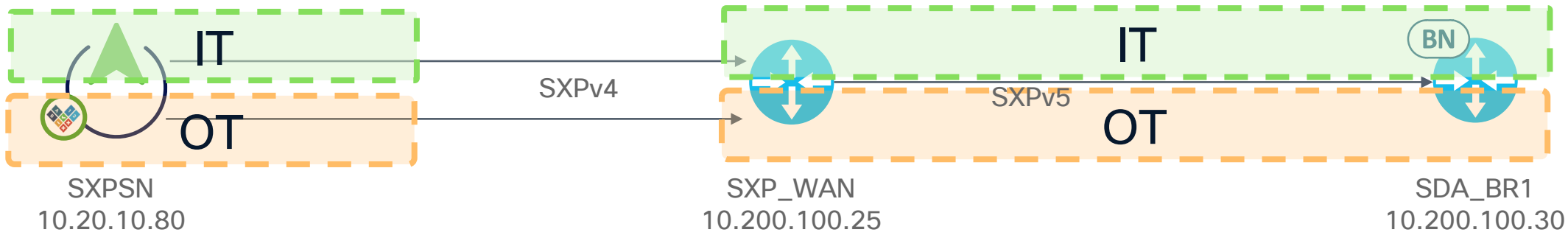
For your reference

```
Site_1_WAN#show run | section sxp
cts sxp enable
cts sxp export-list SXPv5-export-to-BR
 vrf Default-vrf
 vrf IT
 vrf OT
cts sxp export-import-group speaker SXPv5-speaker-to-BR
 export-list SXPv5-export-to-BR
 peer 10.200.100.30
cts sxp default source-ip 10.200.100.25
cts sxp default password cisco123
cts sxp connection peer 10.20.10.80 source 1.1.1.9 password default mode local listener hold-time 0 0 vrf IT
cts sxp connection peer 10.20.10.80 source 1.1.1.30 password default mode local listener hold-time 0 0 vrf OT
cts sxp connection peer 10.20.100.30 source 10.200.100.25 password default mode local speaker hold-time 0
```

SXPv4 from ISE

SXPv5 between Router and Switch

```
Site_1_WAN#show cts role-based sgt-map vrf IT all details
Active IPv4-SGT Bindings Information

IP Address              Security Group                          Source
=========================================================================
=
1.1.1.9                 2:TrustSec_Devices                       INTERNAL
2.2.2.3                 5:Contractors                            SXP
```



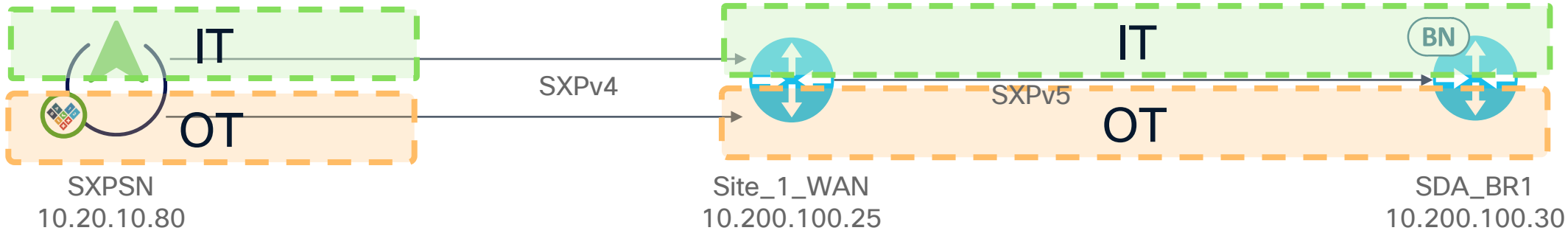
Router SXPv5 Peering to Switch SXPv5

For your reference

```
SDA-BR1#show run | section sxp
cts sxp enable
cts sxp import-list all-vrfs
 vrf
cts sxp export-import-group listener from-site-wan-router
 import-list all-vrfs
 peer 10.200.100.25
cts sxp default source-ip 10.200.100.30
cts sxp default password cisco123
cts sxp connection peer 10.200.100.25 source 10.200.100.30 password default mode local listener hold-time 0
0
```

```
Site_1_WAN#show cts role-based sgt-map vrf IT all details
Active IPv4-SGT Bindings Information

IP Address              Security Group                  Source
============================================================
1.1.1.9                 2:TrustSec_Devices               INTERNAL
2.2.2.3                 5:Contractors                    SXP
```

```
SDA-BR1#show cts role-based sgt-map vrf IT all details
Active IPv4-SGT Bindings Information

IP Address              Security Group                  Source
============================================================
=
1.1.1.9                 2:TrustSec_Devices               SXP
2.2.2.3                 5:Contractors                    SXP
20.20.20.1              2:TrustSec_Devices               INTERNAL
```



SXPv4 compared to SXPv5

For your reference

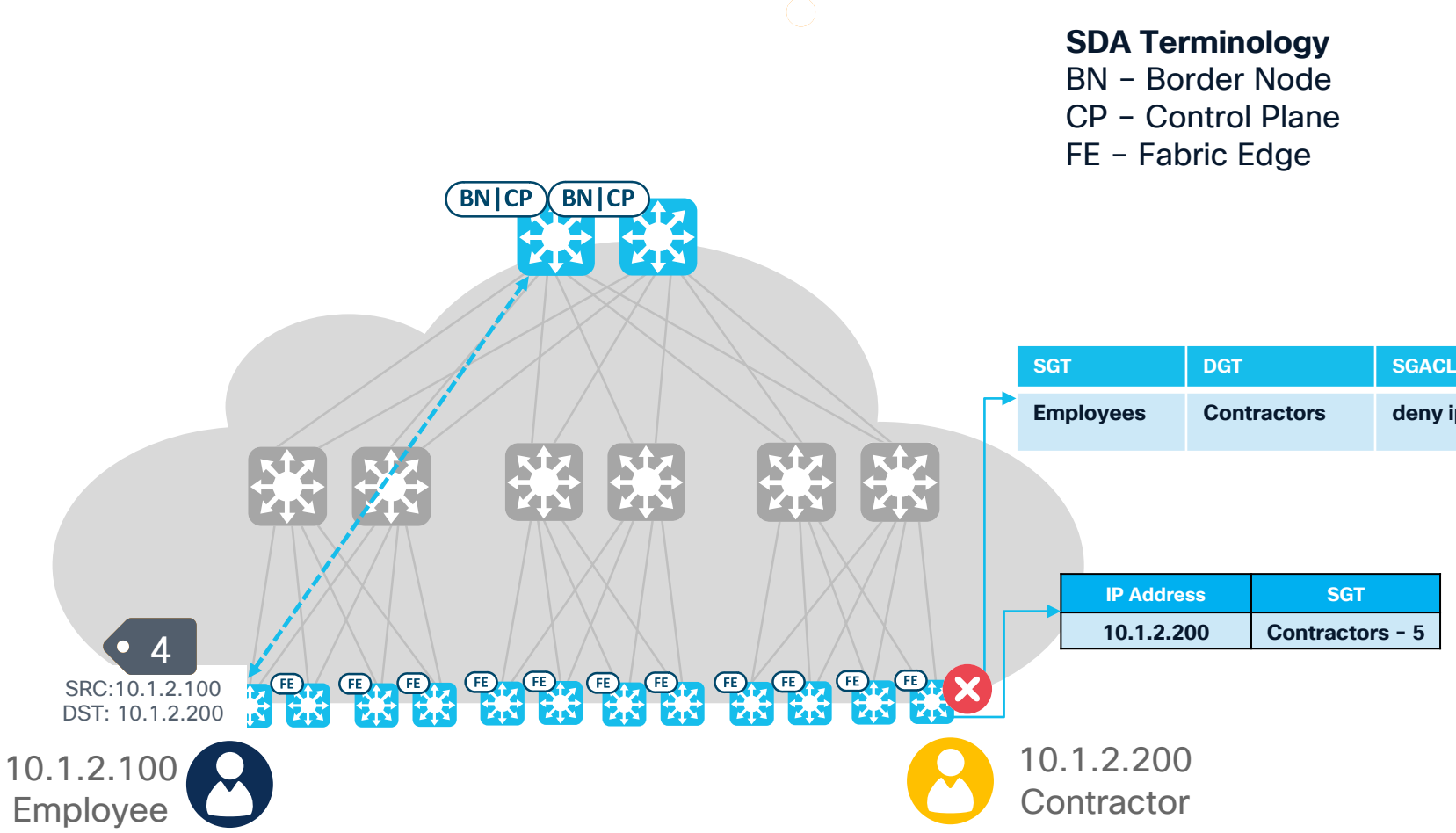
```
Site_1_WAN#show cts sxp connections vrf IT
 SXP                : Enabled
 Highest Version Supported: 5
 Default Password : Set
 Default Key-Chain: Not Set
 Default Key-Chain Name: Not Applicable
 Default Source IP: 10.200.100.25
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
---------------------------------------------
Peer IP           : 10.200.100.80
Source IP         : 1.1.1.9
Conn status       : On
Conn version      : 4
Conn capability   : IPv4-IPv6-Subnet
Conn hold time    : 120 seconds
Local mode        : SXP Listener
Connection inst#  : 1
TCP conn fd       : 1
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 0:02:23:07
(dd:hr:mm:sec)

Total num of SXP Connections = 1
```

```
SDA-BR1#show cts sxp connection
 SXP                : Enabled
 Highest Version Supported: 5
 Default Password : Set
 Default Key-Chain: Not Set
 Default Key-Chain Name: Not Applicable
 Default Source IP: 10.200.100.30
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
---------------------------------------------
Peer IP           : 10.200.100.25
Source IP         : 10.200.100.30
Conn status       : On
Conn version      : 5
Conn capability   : IPv4-IPv6-Subnet
Conn hold time    : 120 seconds
Local mode        : SXP Listener
Connection inst#  : 1
TCP conn fd       : 1
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 0:02:06:15
(dd:hr:mm:sec)

Total num of SXP Connections = 1
```

Type 4 Site – Intra VN Policy

SDA-based micro-segmentation example

1. Routing Lookup for destination IP – Tunnel location found
2. SGT Tagged traffic encapsulated in VXLAN and sent to tunnel location over “non-SGT” capable Devices
3. Egress switch looks up the DGT for IP
4. Egress switch looks up the policy for SGT/DGT
5. Action according to policy



SD-Access – SGT/VXLAN Configuration

- Configuration can be done manually or automated via Catalyst Center
- Single command for turning on SGT being carried in VXLAN via CLI for EVPN or LISP
- SGT enabled automatically with Catalyst Center
- IPv4 any version of code, IPv6 16.9

```
router lisp
 encapsulation vxlan
 locator-table default
 locator-set rloc_5ac867cf-dcaf-4537-a043-da8b4c91c21f
  IPv4-interface Loopback0 priority 10 weight 10
  exit
 !
 eid-table default instance-id 0
  exit
 !
 eid-table vrf enterprise instance-id 10
  dynamic-eid enterprise_10_240_1_0
   database-mapping 10.240.1.0/24 locator-set
rloc_5ac867cf-dcaf-4537-a043-da8b4c91c21f
   exit
  !
  exit
 !
 eid-table vrf Guest instance-id 11
  dynamic-eid Guest_10_241_1_0
   database-mapping 10.241.1.0/24 locator-set
rloc_5ac867cf-dcaf-4537-a043-da8b4c91c21f
   exit
  !
  exit
 !
 disable-ttl-propagate
 ipv4 sgt
 ipv4 use-petr 10.99.200.39
 ipv4 itr map-resolver 10.99.200.39
 ipv4 itr
 ipv4 etr map-server 10.99.200.39 key uci
 ipv4 etr
 exit
```

Type 4 Site – Policy via Firewalls

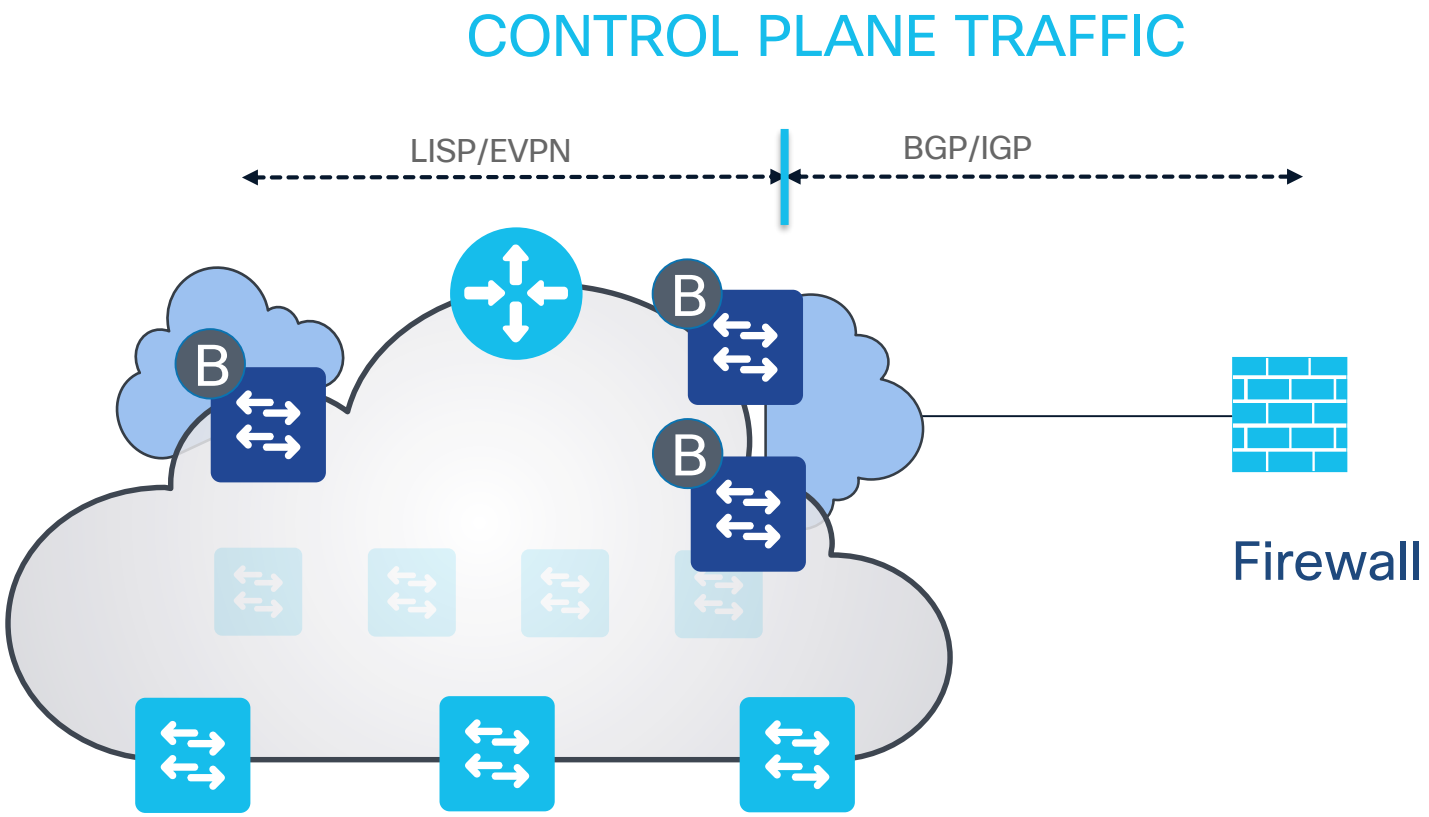
Non-SGT aware Firewall:

- Firewall is connected externally to the Campus Fabric.
- The prefixes from the local Campus Fabric domain will be advertised to the firewall with a routing protocol of choice.
- Firewall policy is based Interface or Subnet IP/mask and IP ACL's.

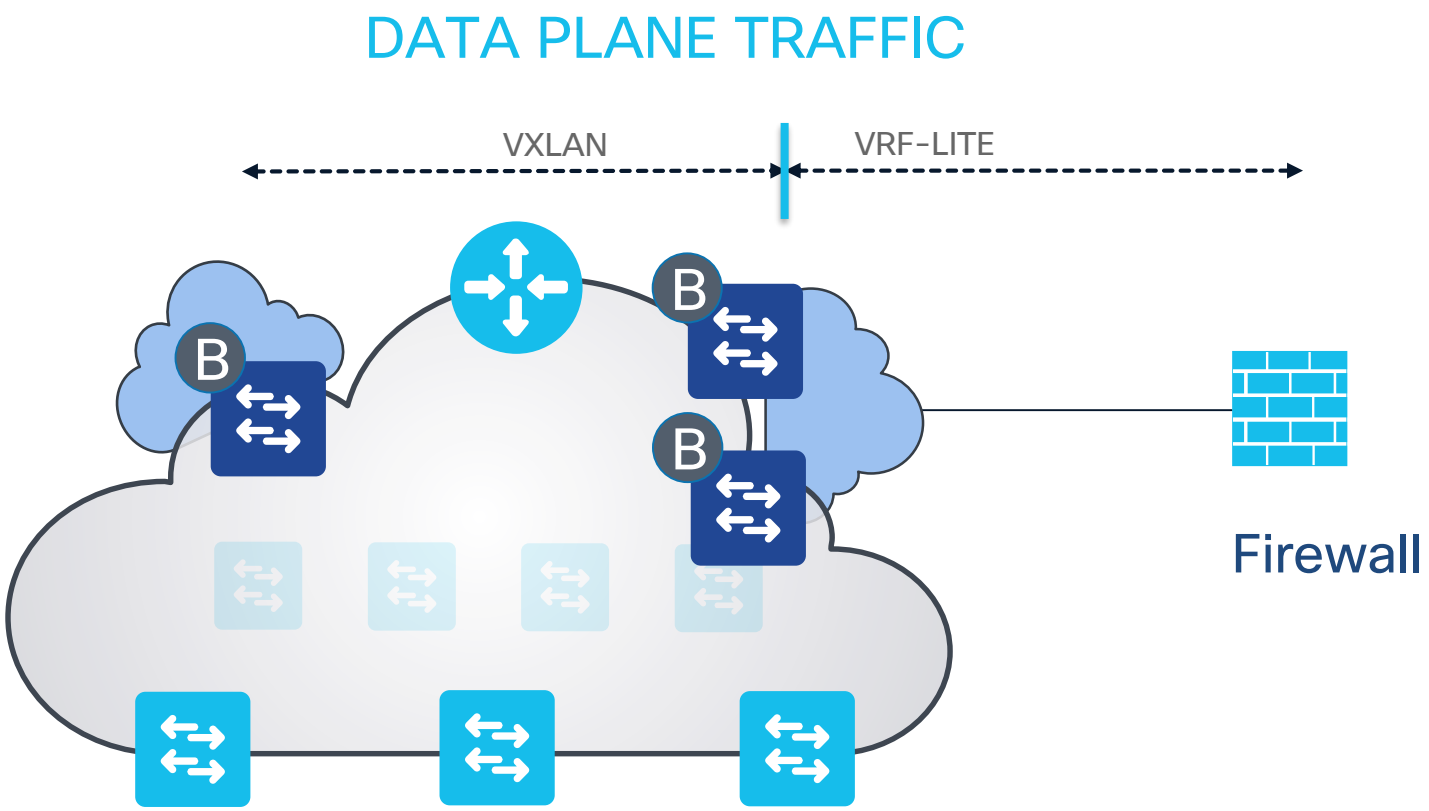
SGT aware Firewall :

- Firewall is connected externally to the Campus Fabric.
- The prefixes from the local Campus Fabric domain will be advertised to the firewall with a routing protocol of choice.
- SXP connection between ISE and Firewall used for derivation of SGTs on the Firewall.
- Firewall policy is based on SGT's and SGACL's (Group Based Policy).
- Firewall also has Interface or Subnet IP based policy, for brownfield integration

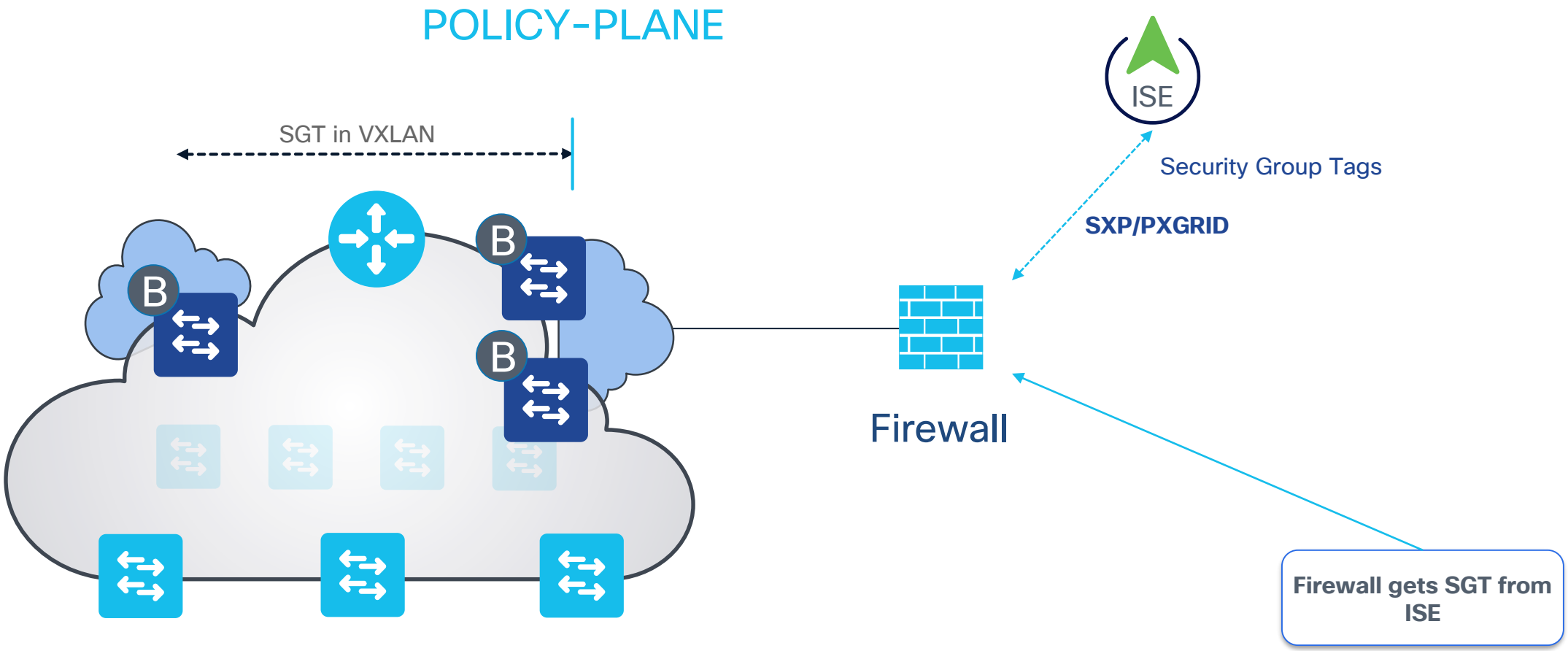
Border Policy via Firewalls



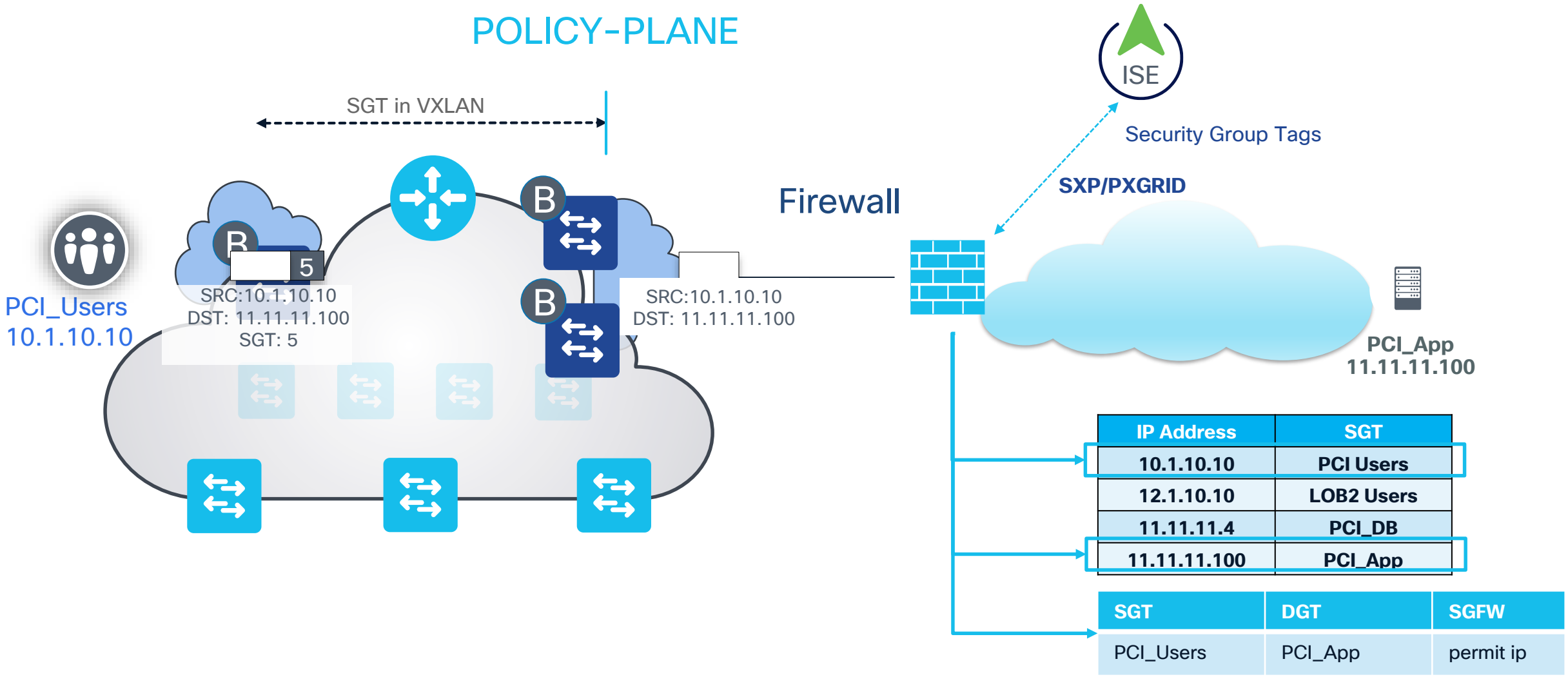
Border Policy via Firewalls



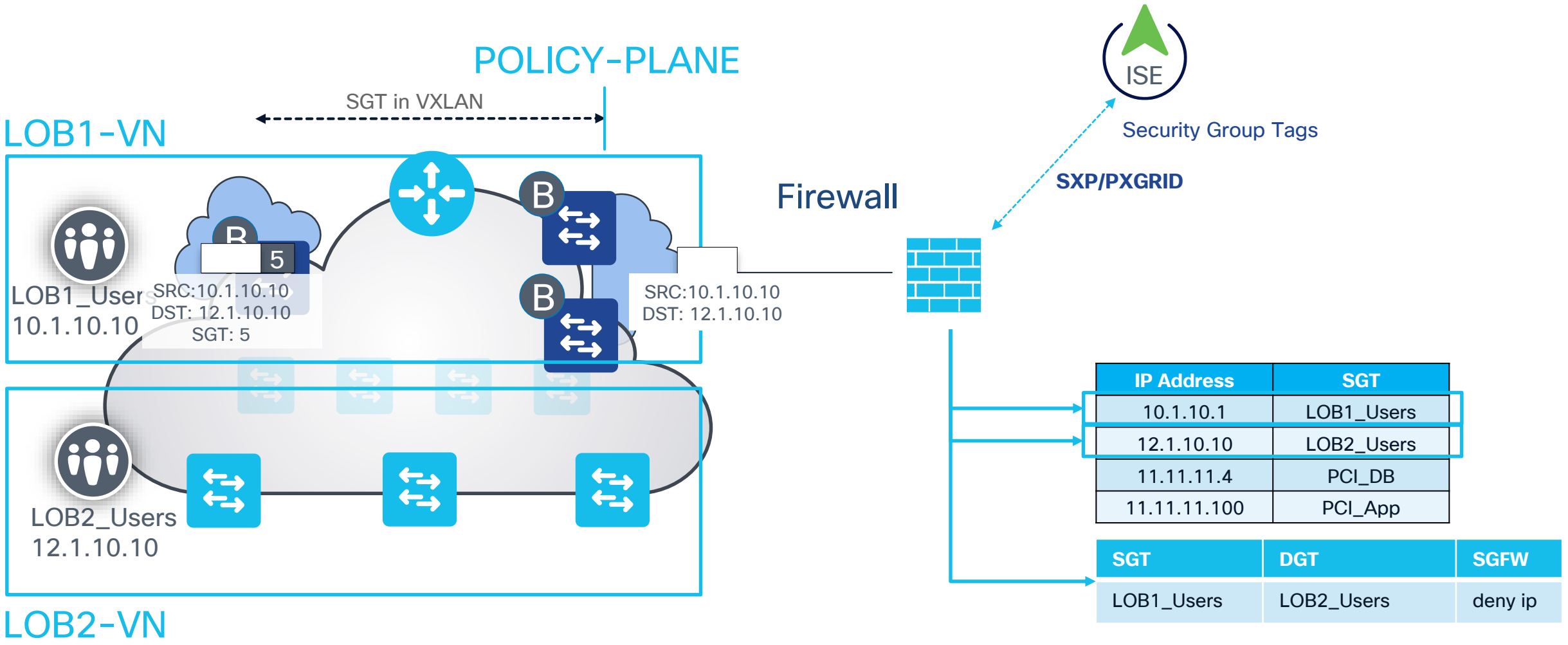
Border Policy via Firewalls



Single VN – Endpoint to Application



Inter VN – Endpoint to Endpoint

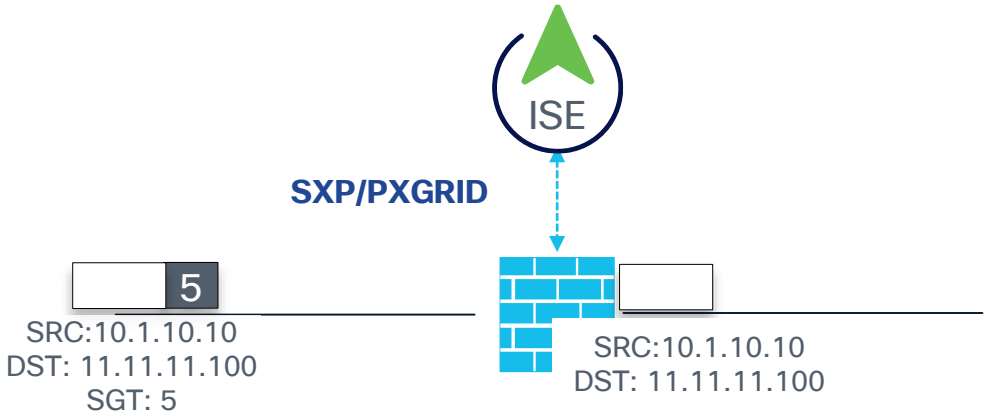


IP Address	SGT
10.1.10.1	LOB1_Users
12.1.10.10	LOB2_Users
11.11.11.4	PCI_DB
11.11.11.100	PCI_App

SGT	DGT	SGFW
LOB1_Users	LOB2_Users	deny ip

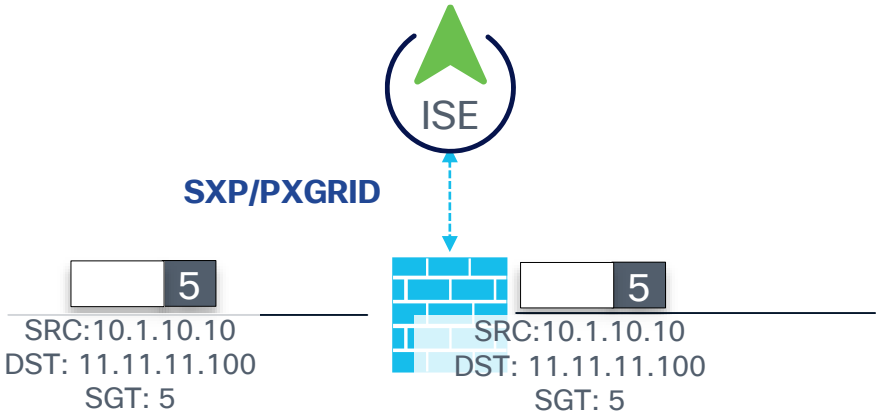
FTD 7.4 – PBR any/any/any enable SGT tagging

- Prior to FTD 7.4 firewalls could not use IP/SGT from pxGrid/SXP to tag outgoing traffic.
- Starting in FTD 7.4 PBR policy that matches src IP any/dst IP any/SGT any triggers internal table loading that enales control plane to tag outgoing data plane traffic



FTD <= 7.4

w/o PBR

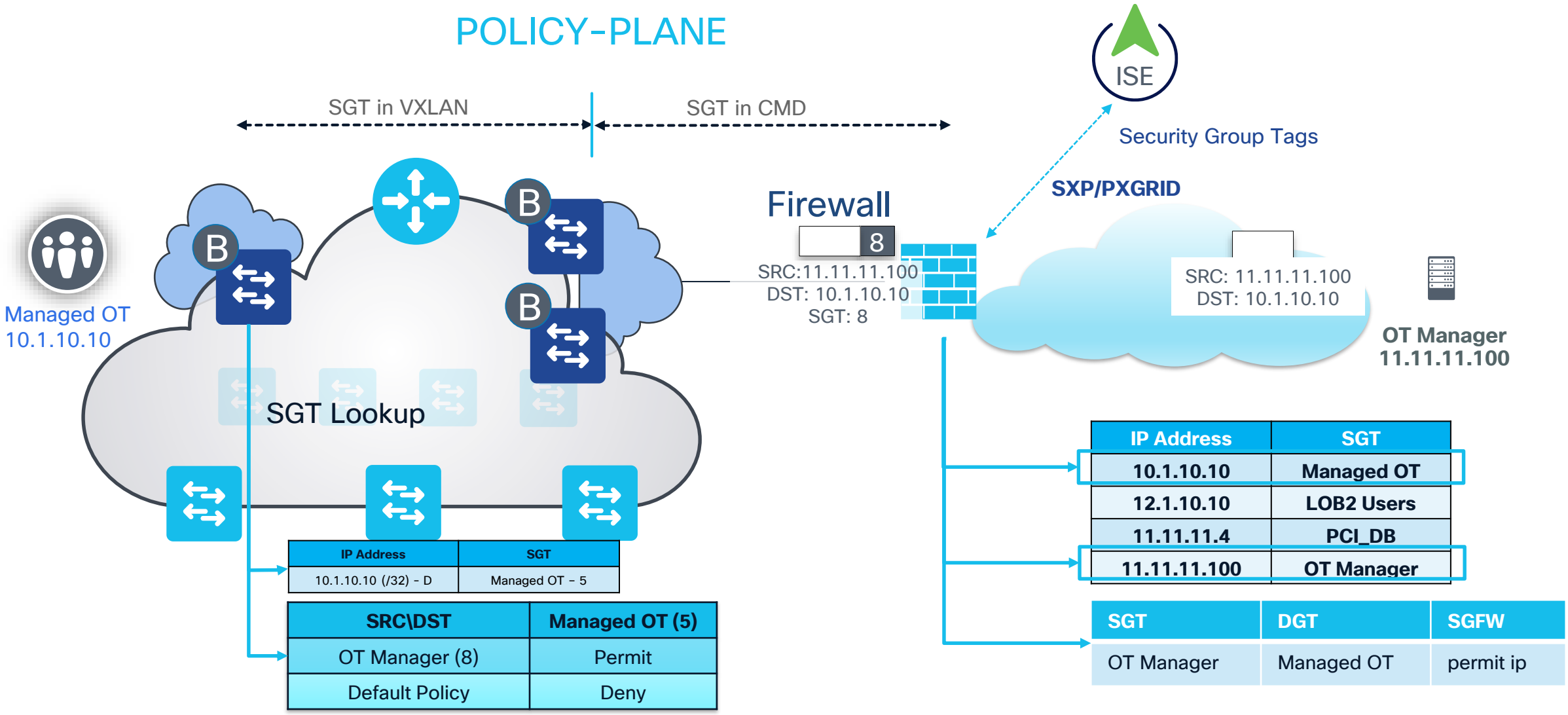


FTD >= 7.4 with

PBR with src IP any/dst IP any/SGT any

PBR policy can be applied to any interface not just SGT propagation interfaces

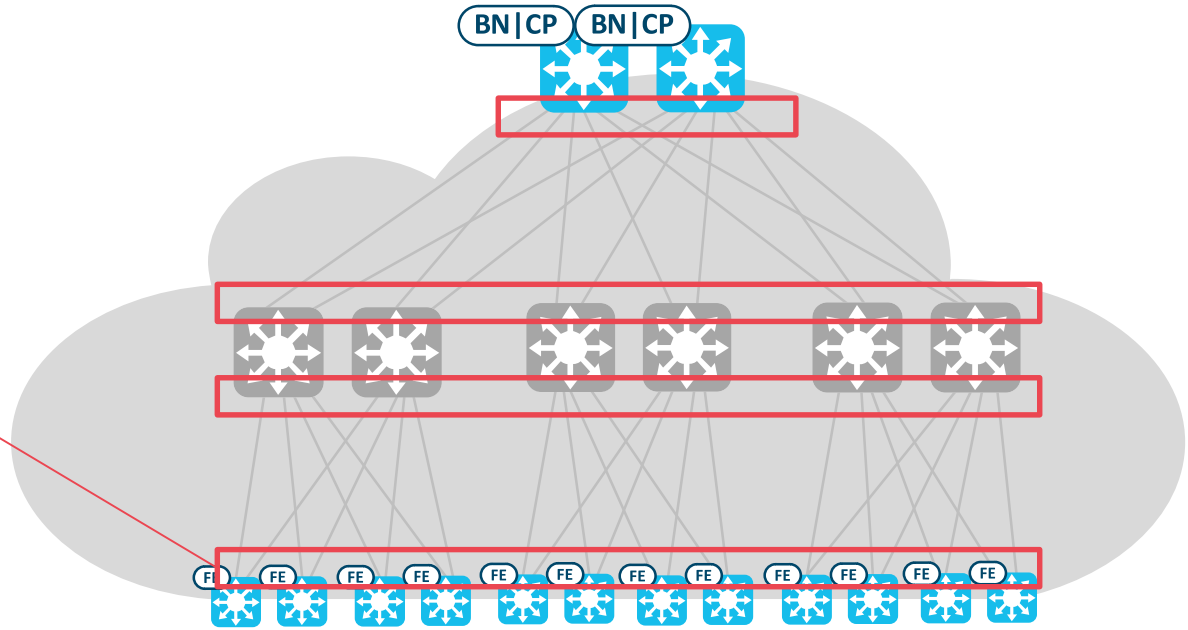
Single VN – Endpoint to Application



Type 4 Site – Default Deny Fabrics

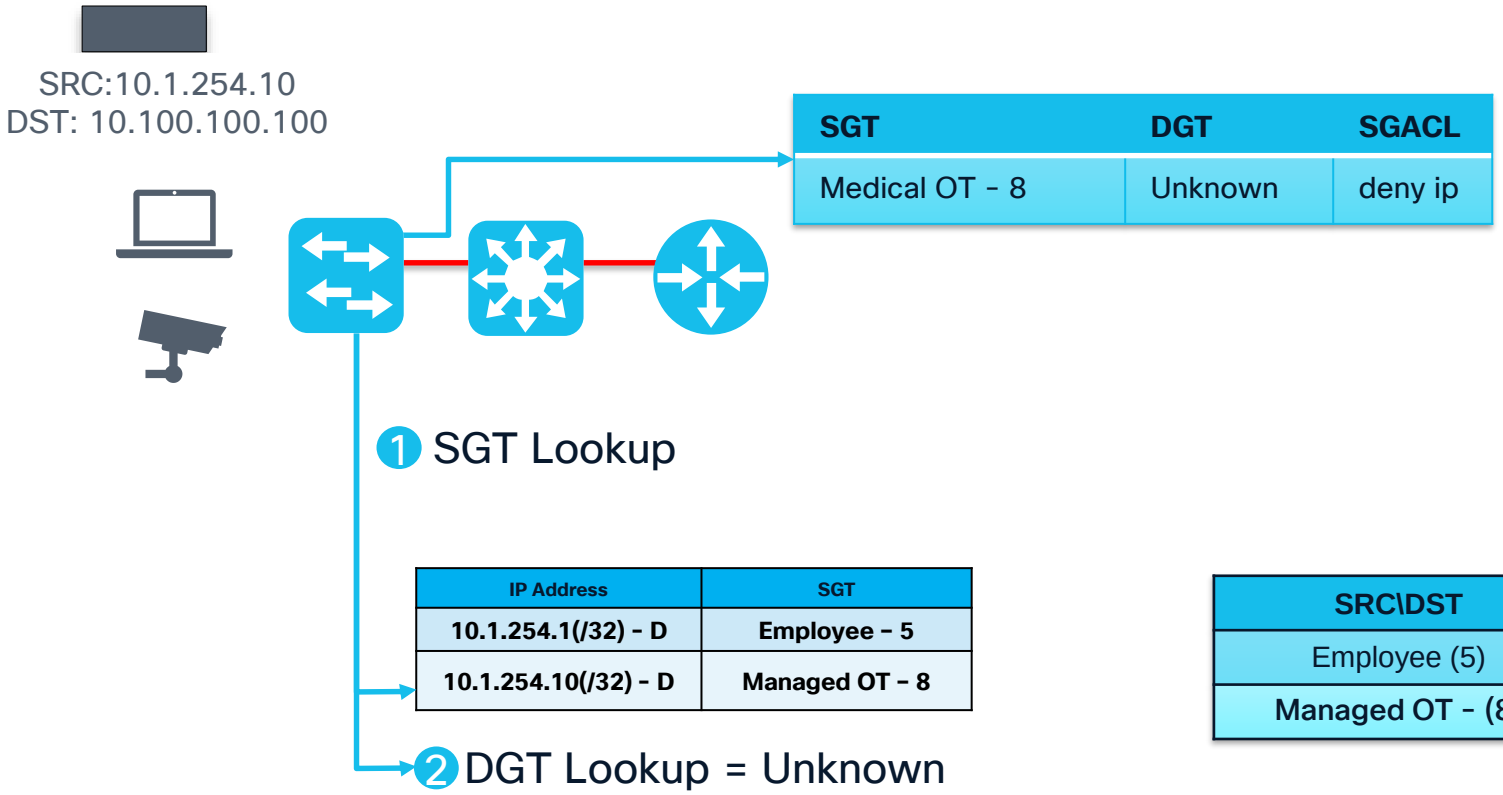
- The principle of least privilege can mean drop any traffic that's not explicitly identified in a Fabric
- End Goal for many customer Zero Trust deployment
- Without Planning Default Deny Fabrics can be difficult to deploy
- Best practices make Default Deny Fabrics easier to deploy
- Please review "BRKENS – 3810 – How to Adopt Zero Trust with SD-Access (and Default-Deny without Tears)" for a full methodology

```
C9K-2
interface GigabitEthernet1/0/14
 no switchport
 ip address 10.10.20.2 255.255.255.0
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
```



Why no enforcement on CMD links? (1/2)

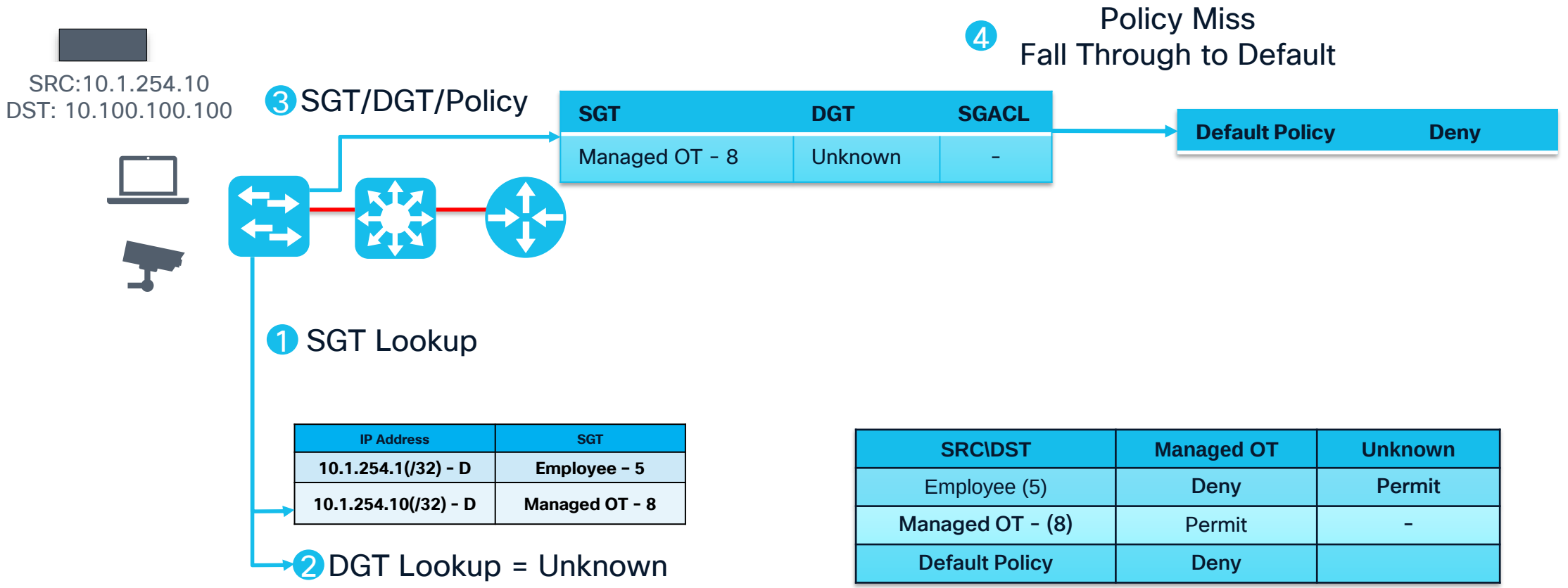
On links between network devices we recommend turning off enforcement to avoid issues with SGT/Unknown SGT = Deny



SRC\DST	Managed OT	Unknown
Employee (5)	Deny	Permit
Managed OT - (8)	Permit	Deny

Why no enforcement on CMD links? (2/2)

On links between network devices we recommend turning off enforcement to avoid issues with Default Policy = Deny



SRC\DST	Managed OT	Unknown
Employee (5)	Deny	Permit
Managed OT - (8)	Permit	-
Default Policy	Deny	

Monitoring the Solution

Validating the SGT scale on Cat 9K

```
9300#show platform hardware fed switch active fwd-asic resource tcam utilization
CAM Utilization for ASIC   [0]
 Table                                              Max Values          Used Values
 ------------------------------------------------------------------------------
 Unicast MAC addresses                               32768/1024          19/21
 L3 Multicast entries                                 8192/512            0/7
 L2 Multicast entries                                 8192/512            0/9
 Directly or indirectly connected routes             24576/8192          96/149
 QoS Access Control Entries                           5120                85
 Security Access Control Entries                      5120                162
 Ingress Netflow ACEs                                  256                 9
 Policy Based Routing ACEs                            1024                20
 Egress Netflow ACEs                                   768                 9
 Flow SPAN ACEs                                       1024                13
 Control Plane Entries                                 512                255
 Tunnels                                               512                17
 Lisp Instance Mapping Entries                         512                 3
 Input Security Associations                           256                 4
 Output Security Associations and Policies             256                 5
 SGT_DGT                                             8192/512            4060/512
 CLIENT_LE                                           4096/256            0/0
 INPUT_GROUP_LE                                      1024                0
 OUTPUT_GROUP_LE                                     1024                0
 Macsec SPD                                            256                2
```

Total SGT it can enforce policy upon:
- 255 prior to 17.1(1)
- 4K as of 17.1(1)

IP-SGT bindings Counter – 10K limit officially* (9300)

SG ACE Counter – ACEs are shared with like SGT/DGT

SGT/DGT Hash table (Policies) – Cells from the ISE Matrix

* IP-SGT scales are per platform. Check limits in Group Based Policy Solution Guide

NETCONF Monitoring of SXP

For your reference

Memory (RBM):

```
curl --silent -k -H 'Accept:
application/yang-data+json' -u sda-
admin:Cisco123
https://172.31.186.221/restconf/data/memory-
usage-processes/memory-usage-
process=535,RBM%20CORE
{
  "Cisco-IOS-XE-process-memory-oper:memory-
usage-process": [
    {
      "pid": 535,
      "name": "RBM CORE",
      "tty": 0,
      "allocated-memory": "511496",
      "freed-memory": "40936",
      "holding-memory": "515048",
      "get-buffers": 0,
      "ret-buffers": 0
    }
  ]
}
```

Memory (SXP):

```
curl --silent -k -H 'Accept: application/yang-
data+json' -u sda-admin:Cisco123
https://172.31.186.221/restconf/data/memory-
usage-processes/memory-usage-
process=80,SXP%20CORE
{
  "Cisco-IOS-XE-process-memory-oper:memory-
usage-process": [
    {
      "pid": 80,
      "name": "SXP CORE",
      "tty": 0,
      "allocated-memory": "2608",
      "freed-memory": "223240",
      "holding-memory": "56008",
      "get-buffers": 0,
      "ret-buffers": 0
    }
  ]
}
```

SXP bindings:

```
curl --silent -H "Accept: application/yang-
data+json" -k -u sda-admin:Cisco123
https://172.31.186.221/restconf/data/trustse
c-state/cts-rolebased-sgtmaps
{
  "Cisco-IOS-XE-trustsec-oper:cts-rolebased-sgtmaps": {
    "cts-rolebased-sgtmap": [
      {
        "ip": "192.168.6.2/32",
        "vrf-name": "Default",
        "sgt": 2,
        "source": "from-cli-hi"
      },
      {
        "ip": "192.168.60.3/32",
        "vrf-name": "Default",
        "sgt": 2,
        "source": "from-cli-hi"
      },
      {
        "ip": "172.31.186.221/32",
        "vrf-name": "Mgmt-vrf",
        "sgt": 2,
        "source": "from-cli-hi"
      },
      {
        "ip": "10.90.1.100/32",
        "vrf-name": "Engineering",
        "sgt": 15,
        "source": "from-local"
      },
      {
        "ip": "10.90.1.101/32",
        "vrf-name": "Engineering",
        "sgt": 8,
        "source": "from-vlan"
      },
      {
        "ip": "10.90.2.254/32",
        "vrf-name": "Engineering",
        "sgt": 2,
        "source": "from-cli-hi"
      }
    ]
  }
}
```

- Available on IOS XE in Non-Fabric and Fabric Mode
- Enable RESTCONF for Switches (Catalyst Center or CLI)
- Binding Source “Internal” shown as “cli-hi” (e.g. SVI IPs, etc.)

Netconf TrustSec Operational Model


```
curl --silent -H "Accept: application/yang-data+json" -k -u user:password https://1.1.1.1/restconf/data/trustsec-state/
```

```
{
  "Cisco-IOS-XE-trustsec-oper:trustsec-state":
{
    "cts-rolebased-sgtmaps": {
      "cts-rolebased-sgtmap": [
        {
          "ip": "192.168.6.2/32",
          "vrf-name": "Default",
          "sgt": 2,
          "source": "from-cli-hi"
        },
—snip—
```

```
    "cts-rolebased-policies": {
      "cts-rolebased-policy": [
        {
          "src-sgt": 65535,
          "dst-sgt": 65535,
--snip--
    "cts-pac": {
      "pac": [
        {
          "pac-type": "pac-type-cisco-trustsec",

—snip—
```

```
  "cts-env-data": {
    "status": "env-download-success",
    "device-sgt": 2,
    "total-num-servers": 1,
```

- Available on IOS XE
- Enable RESTCONF for Switches
  - PAC
  - Environmental Data
  - SXP
  - SGT/SGACL
  - IP/SGT Bindings

Netconf TCAM Operation Model


```
~ curl --silent -H "Accept: application/yang-data+json" -k -u user:pwd https://1.1.1.1/restconf/data/tcam-details
    {
      "Cisco-IOS-XE-tcam-oper:tcam-details": {
        "tcam-detail": [
    --snip--
      {
            "asic-no": 0,
            "name": "CTS Cell Matrix",
            "hash-entries-max": 32768,
            "tcam-entries-max": 768,
            "hash-entries-used": 0,
            "tcam-entries-used": 0
          },
```

```
-- snip --
        {
          "asic-no": 0,
          "name": "Security ACL Ipv4",
          "hash-entries-max": 0,
          "tcam-entries-max": 7168,
          "hash-entries-used": 0,
          "tcam-entries-used": 0
        },
```

- Available on IOS XE
- Enable RESTCONF for Switches
- L3 routes Shared with IP/ST, etc.

Verifying SGACL Drops

For your reference

Use show cts role-based counter to show traffic drop by SGACL

```
C9K-CORE-1#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
*       *       0               0               48002           369314
3       20      53499           53471           0               0
4       5       0               0               0               3777
3       6       0               0               0               53350
4       6       3773            3773            0               0
3       7       0               0               0               0
4       7       0               0               0               0
```

From * to * means Default Rule

show command displays the content statistics of RBACL enforcement. Separate counters are displayed for HW and SW switched packets. The user can specify the source SGT using the “from” clause and the destination SGT using the “to” clause.

Mostly SGACL is done in HW. Only if the packet needs to be punted to SW (e.g. TCAM is full, marked to be logged) , SW counter increments

Policy Counters Catalyst Center

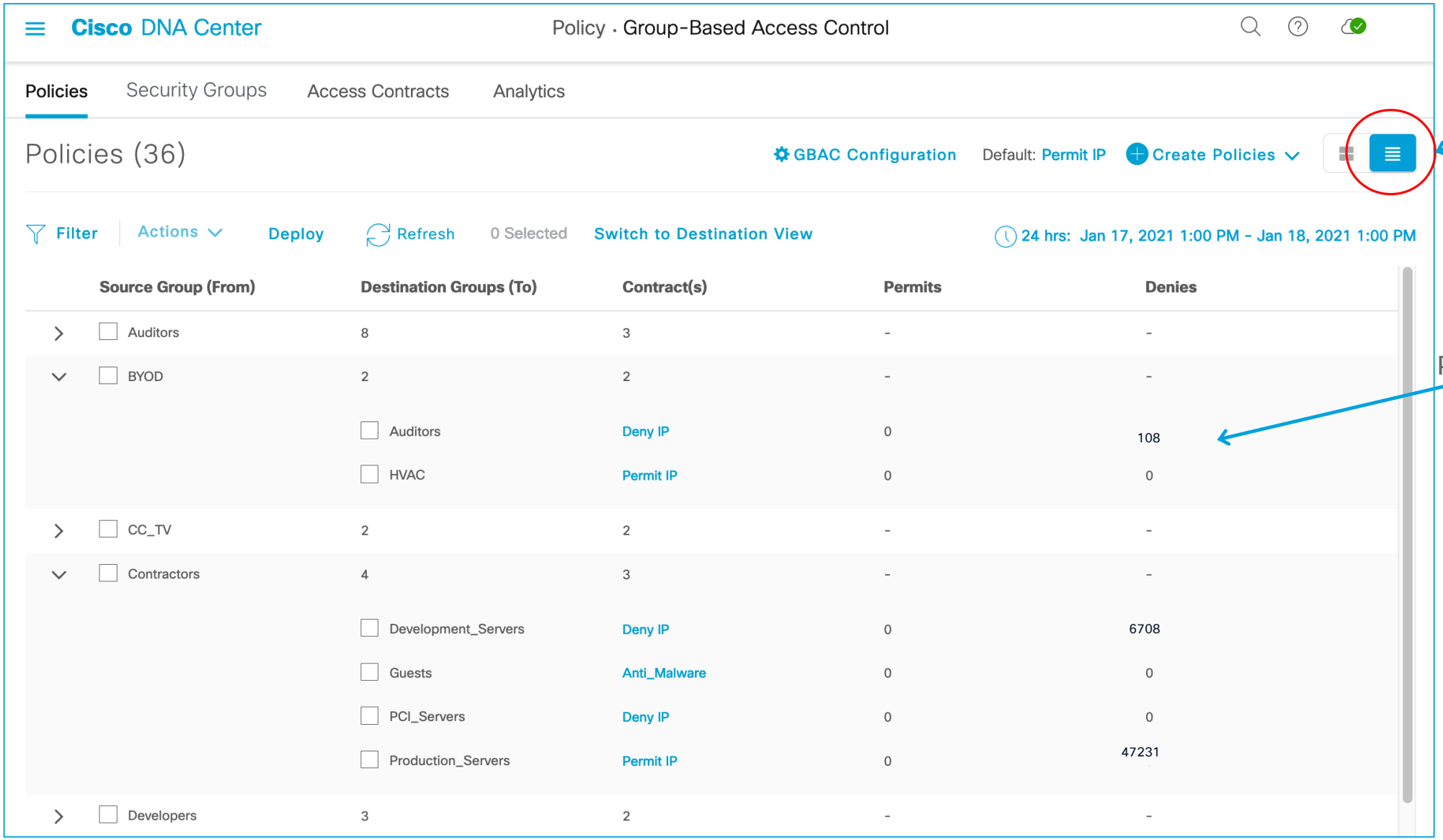


Table View

Permits and Denies per policy

SGT/DGT Hit Counters via Netconf

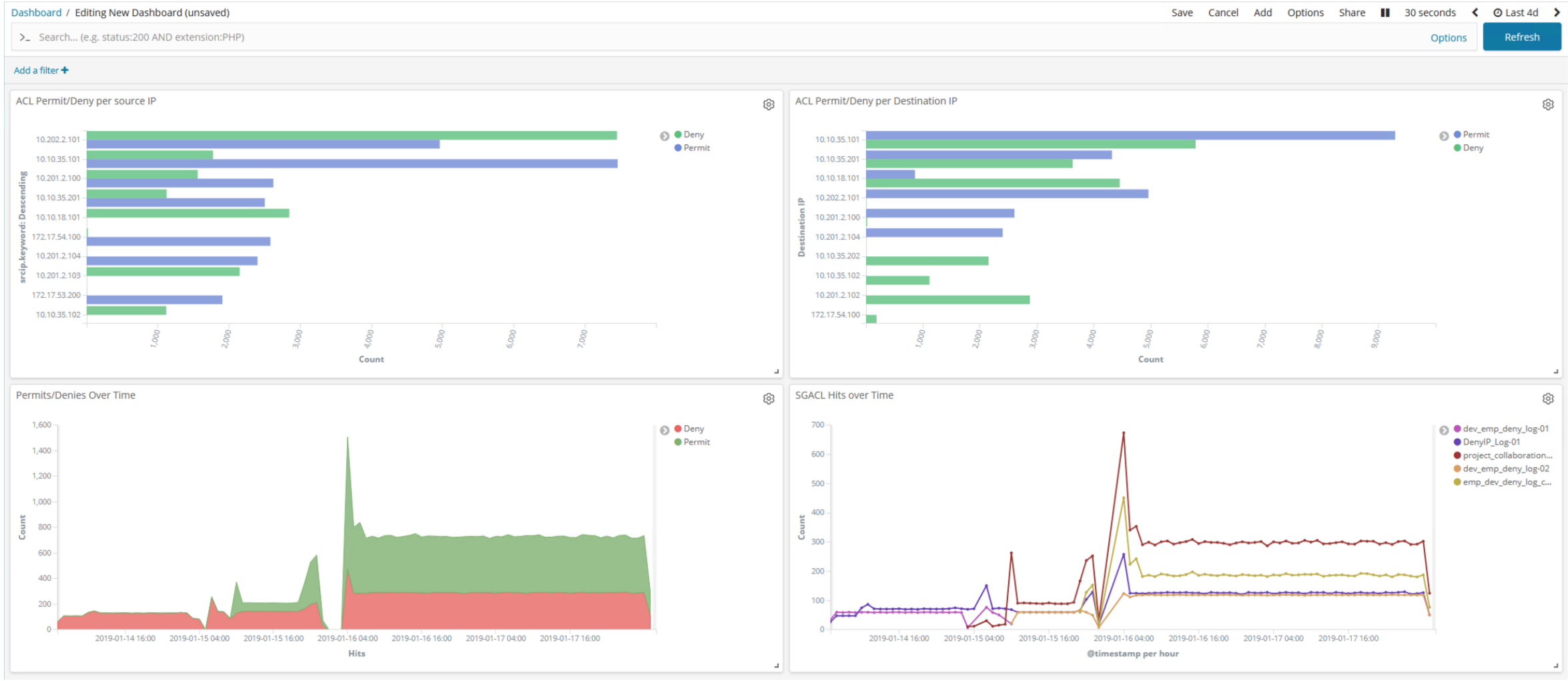
- NCC –
  - https://github.com/CiscoDevNet/ncc
  - ./ncc-establish-subscription.py --host=172.23.41.129 -u cisco -p nbv_1234 -x /trustsec-state --period 50--callback sample > trustsec-state.txt

```
Subscription Result : notif-bis:ok
Subscription Id     : 2147483648
-->>
Event time      : 2019-01-27 22:26:46.910000+00:00
Subscription Id : 2147483648
Type            : 1
Data            :
{
  "datastore-contents-xml": {
    "trustsec-state": {
      "cts-rolebased-policies": {
        "cts-rolebased-policy": [
```

```
{
            "dst-sgt": "4",
            "hardware-deny-count": "145",
            "hardware-monitor-count": "0",
            "hardware-permit-count": "0",
            "last-updated-time": "1548631492542928",
            "monitor-mode": "false",
            "num-of-sgacl": "1",
            "policy-life-time": "86400",
            "sgacl-name": "dev_emp_deny_log-02;",
            "software-deny-count": "0",
            "software-monitor-count": "0",
            "software-permit-count": "0",
            "src-sgt": "8",
            "total-deny-count": "145",
            "total-permit-count": "0"
          },
```

Open Telemetry Example – SGACL Monitoring

For your reference

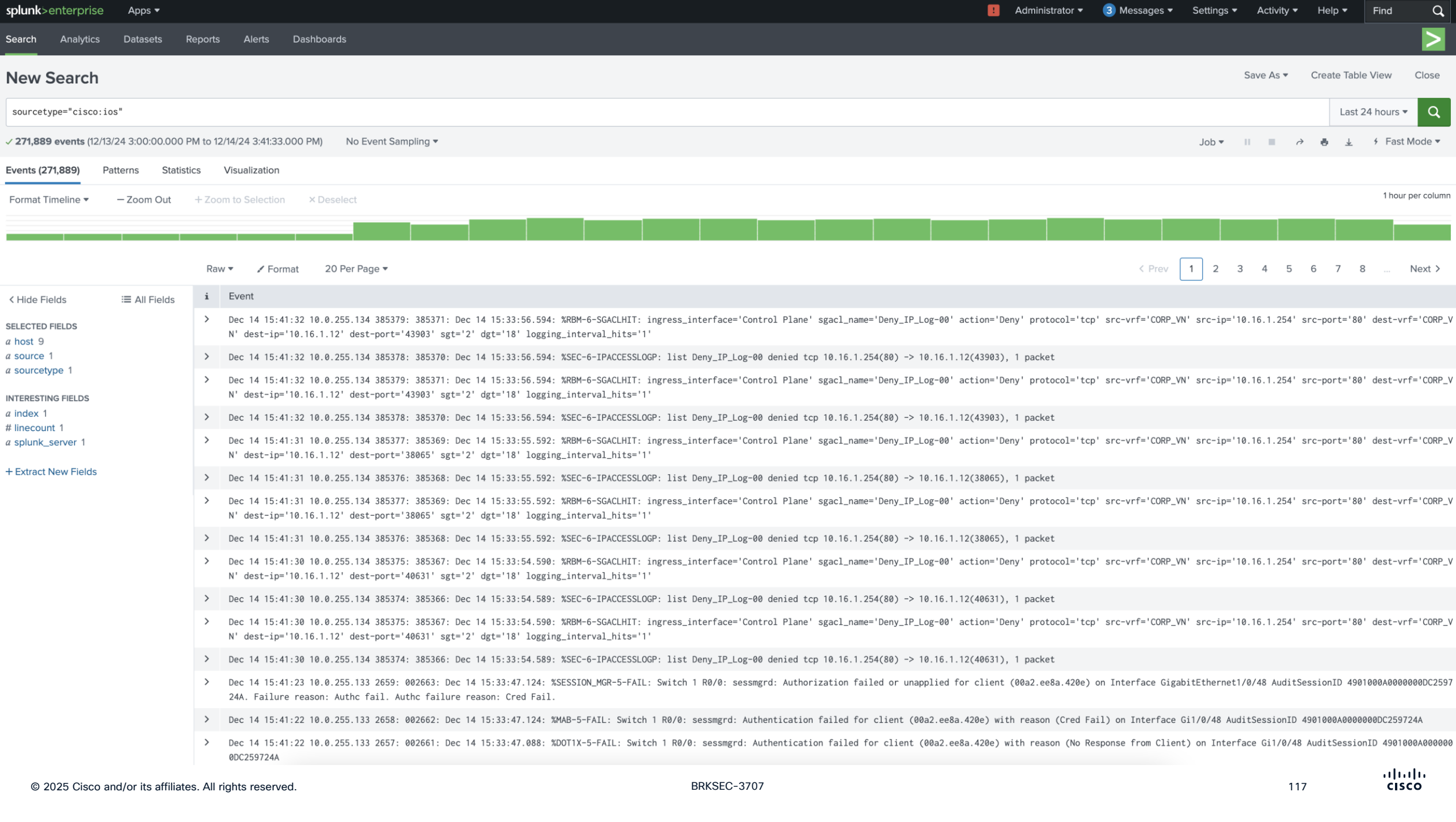


SGACL Logging – Open Telemetry

- 16.3 Initial support in C9k
- 17.3 Performance optimization for CPU protection

*Jan 27 13:33:43.355: %RBM-6-SGACLHIT: ingress_interface='GigabitEthernet1/0/24' sgacl_name='DenyIP_Log-01' action='Deny' protocol='tcp' src-vrf='default' src-ip='10.10.18.101' src-port='64382' dest-vrf='default' dest-ip='10.10.35.201' dest-port='80' sgt='4' dgt='4' logging_interval_hits='1'


```
{
      "logginghits" => "1",
         "protocol" => "tcp",
           "action" => "Permit",
           "srcvrf" => "default",
          "srcport" => "80",
         "destport" => "62700",
      "srcinterface" => "TenGigabitEthernet1/1/8",
        "timestamp" => "Jan 27 12:48:26.756",
            "sgacl" => "emp_dev_deny_log_copy-01",
              "sgt" => "4",
           "reason" => "%RBM-6-SGACLHIT",
      "received_at" => "2019-01-27T04:46:25.134Z",
          "message" => "<190>123319: Jan 27 12:48:26.756: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/1/8' s
gacl_name='emp_dev_deny_log_copy-01' action='Permit' protocol='tcp' src-vrf='default' src-ip='10.10.35.101' src-port='80
' dest-vrf='default' dest-ip='10.201.2.104' dest-port='62700' sgt='4' dgt='8' logging_interval_hits='1'",
    "received_from" => "10.99.100.1",
            "dstip" => "10.201.2.104",
             "host" => "10.99.100.1",
          "destvrf" => "default",
             "type" => "syslog",
         "@version" => "1",
       "@timestamp" => 2019-01-27T04:46:25.134Z,
              "dgt" => "8",
            "srcip" => "10.10.35.101"
}
```



Flexible NetFlow Record for SGACL Permit and Deny

For your reference

17.13.1 NetFlow Record for SGACL Deny

```
    Field (10/11): firewallEvent
        Type: firewallEvent (233)
        Length: 1
    Field (11/11): PROTOCOL
FlowSet 2 [id=261] (1 flows)
  FlowSet Id: (Data) (261)
  FlowSet Length: 56
  [Template Frame: 178]
  Flow 1
    SrcAddr: 131.131.131.10
    DstAddr: 201.201.201.2
    SrcPort: 0
    DstPort: 0
    OutputInt: 10
    Octets: 10000
    Packets: 100
    [Duration: 198.000000000 seconds (milliseconds)]
    Firewall Event: Flow denied (3)
    Protocol: ICMP (1)
  Padding: 0000
```

```
Cisco NetFlow/IPFIX
  Version: 9
  Count: 2
  SysUptime: 16281.000000000 seconds
  Timestamp: Mar 21, 2023 11:18:18.000000000 EDT
    CurrentSecs: 1679411898
  FlowSequence: 688
  SourceId: 16777217
  FlowSet 1 [id=0] (Data Template): 261
    FlowSet Id: Data Template (V9) (0)
    FlowSet Length: 52
    Template (Id = 261, Count = 11)
      Template Id: 261
      Field Count: 11
      Field (1/11): IP_SRC_ADDR
      Field (2/11): IP_DST_ADDR
      Field (3/11): L4_SRC_PORT
      Field (4/11): L4_DST_PORT
      Field (5/11): OUTPUT_SNMP
      Field (6/11): BYTES
      Field (7/11): PKTS
      Field (8/11): flowStartMilliseconds
      Field (9/11): flowEndMilliseconds
      Field (10/11): firewallEvent
        Type: firewallEvent (233)
        Length: 1
      Field (11/11): PROTOCOL
  FlowSet 2 [id=261] (1 flows)
    FlowSet Id: (Data) (261)
    FlowSet Length: 56
    [Template Frame: 178]
    Flow 1
      SrcAddr: 131.131.131.10
      DstAddr: 201.201.201.2
      SrcPort: 0
      DstPort: 0
      OutputInt: 10
      Octets: 10000
      Packets: 100
      [Duration: 198.000000000 seconds (milliseconds)]
      Firewall Event: Flow denied (3)
      Protocol: ICMP (1)
    Padding: 0000
```

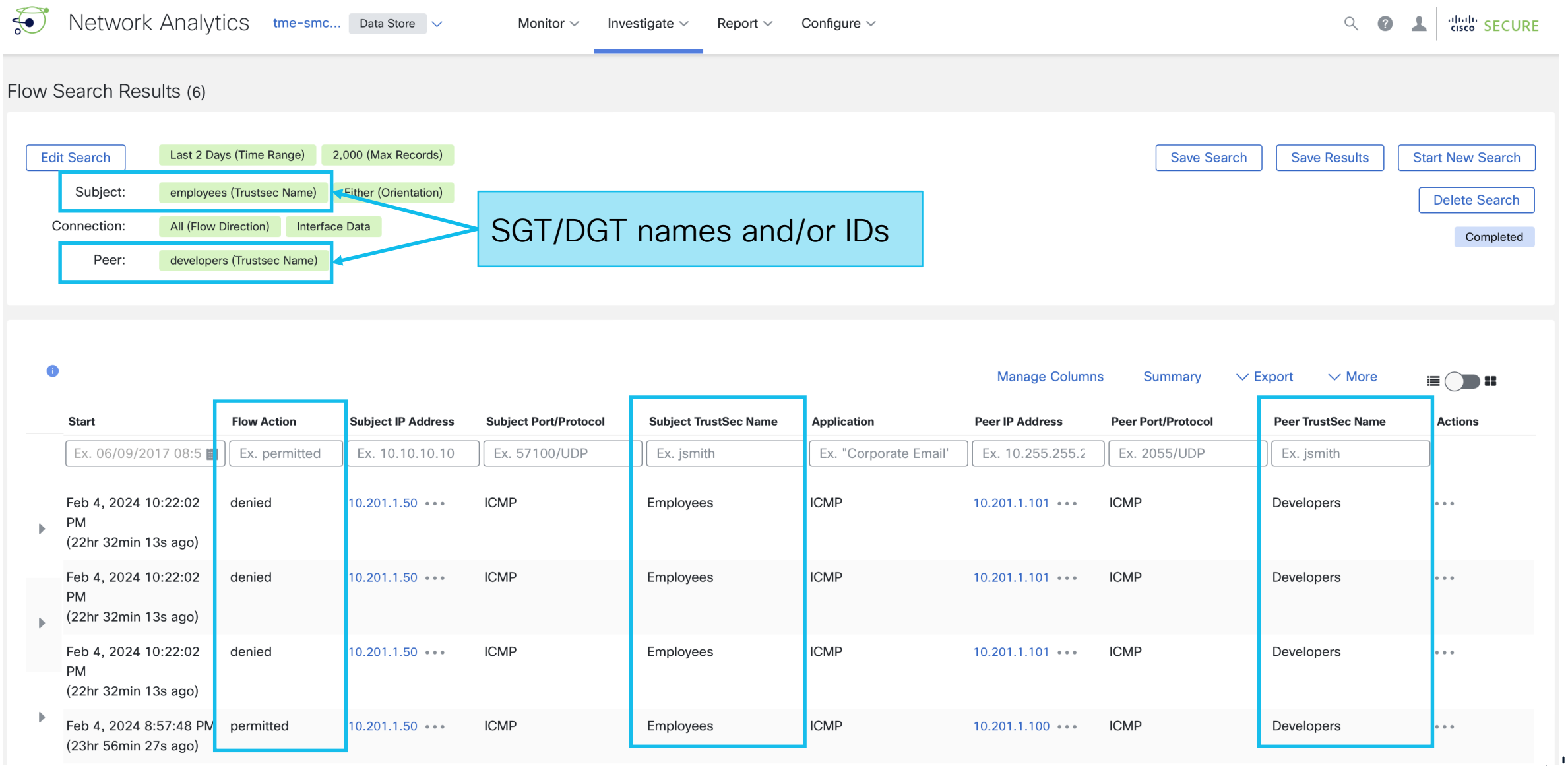
Flexible NetFlow SGACL Drop Record Format


```
DC-C9300-MDA-Access-1#sho run | section flow
flow record sgaclrecord
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 match flow cts source group-tag
 match flow cts destination group-tag
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 collect policy firewall event
```

```
interface GigabitEthernet1/0/1
 switchport access vlan 510
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 ip flow monitor sgaclmon output
 load-interval 30
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 macro description CISCO_LAST_RESORT_EVENT
 no macro auto processing
 source template DefaultWiredDot1xOpenAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

- Output flow record
- Incompatible with SD-AVC Flow monitors on interface

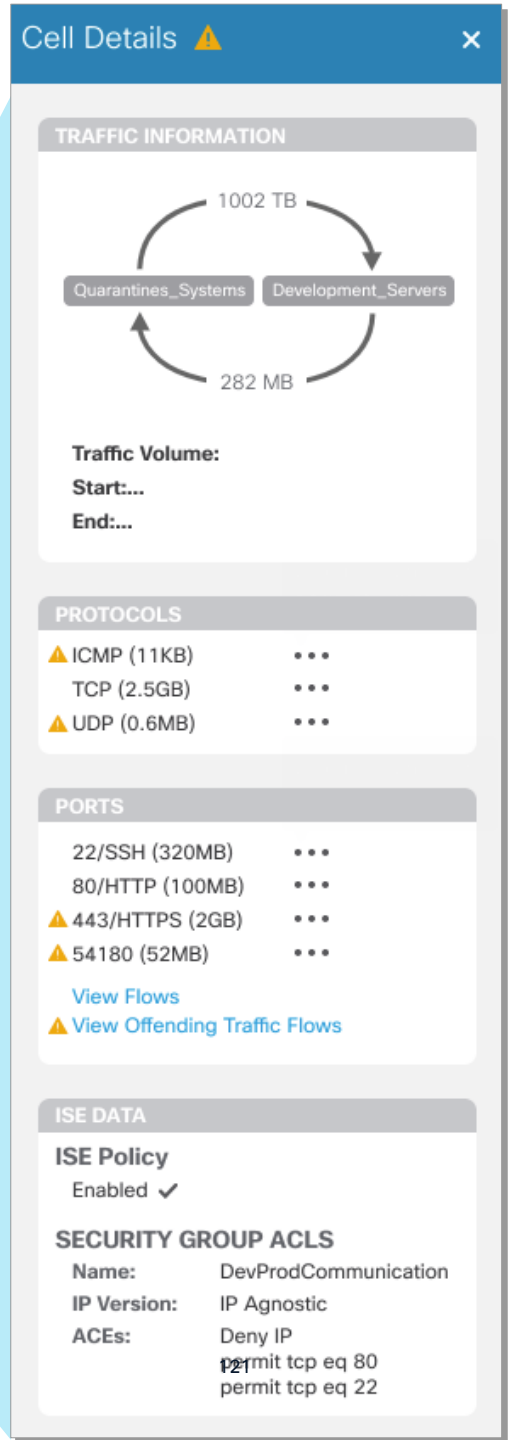
SNA: Flow Search based on SGTs (NetSecOps)



SNA: Validate ISE policy is being observed

Near real time network telemetry (NetSecOps)

	No Traffic
	Allowed Traffic
	Denied Traffic
	Traffic with Custom Policy
	Policy Analysis Pending
	Policy Disabled
	Policy Enabled
	Policy Monitor Mode
	Possible Policy Violation
	Unknown



Manufacturer Design Update

- Customer wants to extend IT/OT VNs across the SD-WAN
- Optionally use SD-WAN firewall for enforcement
- An acquisition also brough Meraki MR/MS/MX solutions into the design patter for Site Types 1 and 2

Extending Inline Tagging to WAN Topologies

Inline Tagging from Multi-VN Site to Multi-N Site

1. SGT encapsulated in VXLAN across SDA Fabric in VN OT
2. Border node strips the VXLAN header and transports the SGT in CMD via a Trunk port
3. SD-WAN router encapsulates the SGT into IPsec an VPN-ID 20

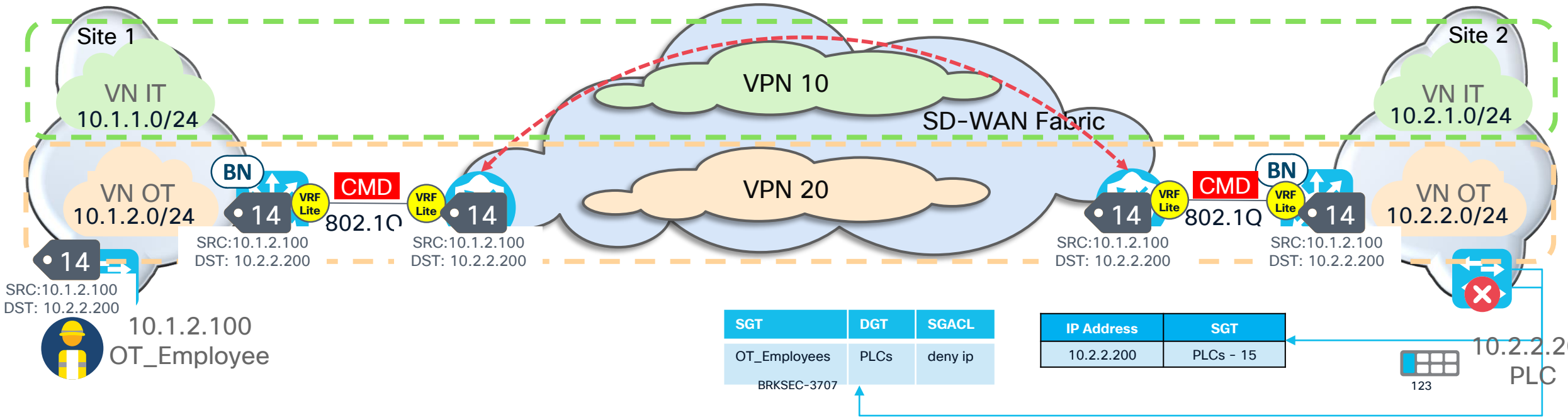
Catalyst Center

ISE

SD-WAN
17.5/20.5

4. SD-WAN router strips the IPsec header and transports the SGT in CMD via a Trunk port
5. Border node encapsulates the SGT in the VXLAN header in VN OT
6. Egress switch looks up the DGT for IP
7. Egress switch looks up the policy for SGT/DGT
8. Action according to policy

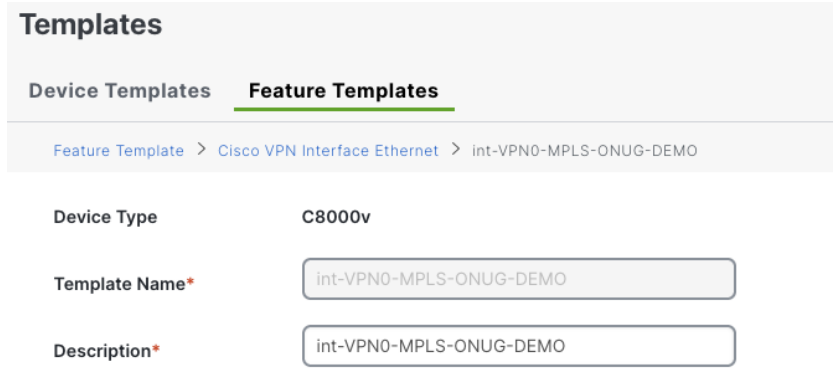
VRF-aware SGT Inline Tagging via IPsec



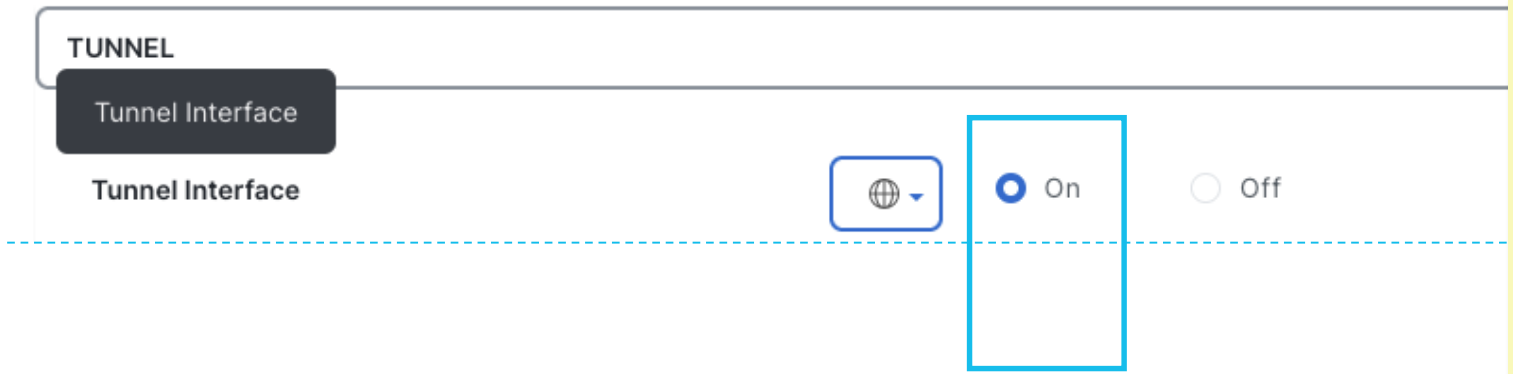
SD-WAN SGT Transport

VPN 0 Template – Tunnel Interface

For your reference



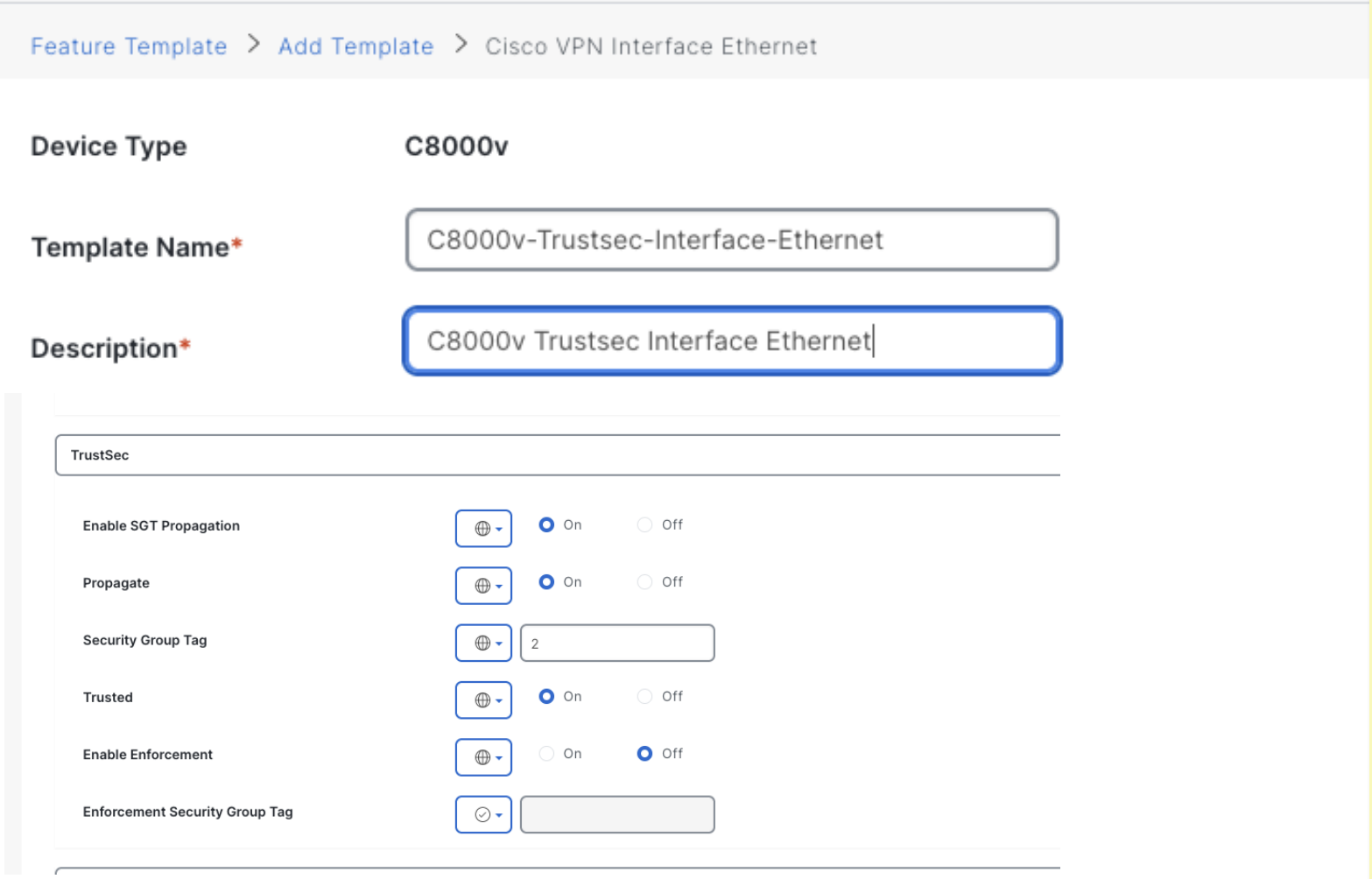
CTS SGT F




```
interface Tunnel1
 ip unnumbered GigabitEthernet0/0/1
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/1
 no ipv6 redirects
 cts manual
 tunnel source GigabitEthernet0/0/1
 tunnel mode sdwan
```

SD-WAN – TrustSec configuration

Ethernet Interface



For your reference

```
interface GigabitEthernet1
 no ip address
 no ip redirects
 ip mtu 1500
 load-interval 30
 negotiation auto
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
 arp timeout 1200
!
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 vrf forwarding 10
 ip address 10.200.10.20 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
 arp timeout 1200
!
interface GigabitEthernet1.20
 encapsulation dot1Q 20
 vrf forwarding 20
 ip address 10.1.20.20 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
arp timeout 1200
```

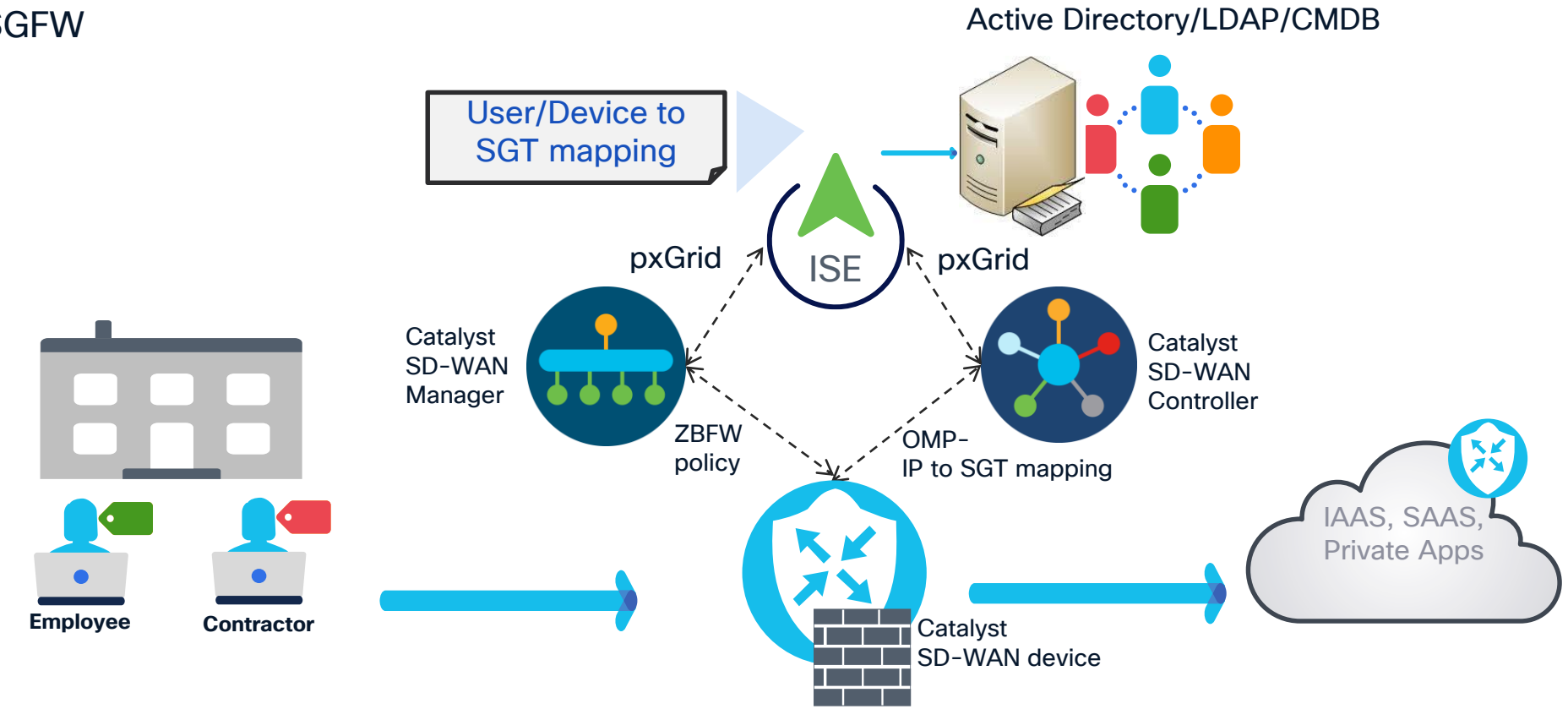
Router SVIs – Switch SVI/Trunks for CTS


```
DC-ASR1K-1#
interface TenGigabitEthernet0/0/0
 description Connection to DC-C9600-1
 mtu 9208
 no ip address
 ip mtu 9208
 ip tcp adjust-mss 1452
 cdp enable
 cts manual
  policy static sgt 2 trusted
!
interface TenGigabitEthernet0/0/0.2
 encapsulation dot1Q 2 native
 ip address 10.20.3.254 255.255.255.252
 ip mtu 9208
 ip nbar protocol-discovery
 cdp enable
 cts manual
  policy static sgt 2 trusted
!
interface TenGigabitEthernet0/0/0.3004
 description vrf interface to External router
 encapsulation dot1Q 3004
 vrf forwarding DEFAULT_VN
 ip address 10.20.3.225 255.255.255.252
 ip mtu 9208
 cts manual
  policy static sgt 2 trusted
```

```
DC-C9606-1#
system mtu 9100
!
interface HundredGigE1/0/3/2
 switchport trunk native vlan 2
 switchport mode trunk
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
end

DC-C9606-1#sho run int vlan 2
Building configuration...

Current configuration : 63 bytes
!
interface Vlan2
 ip address 10.20.3.253 255.255.255.252
end

DC-C9606-1#sho run int vlan 3004
Building configuration...

Current configuration : 66 bytes
!
interface Vlan3004
 ip address 10.20.3.226 255.255.255.252
end
```

ISE/Cisco SD-WAN Integration

17.10.1 SGFW



Destination

Source	ZBFW Policy	Employees	Contractors
	Employees	Deny All	Deny All
	PLCs	Permit All	Deny All
	Contractors	Deny All	Permit All

- Granular Security Control using SGTs
- Unified Security policy and intent

SGACL on Router Platforms as of 16.3(3)

TrustSec on Routers similar to Switches


```
Cat8k#show cts role-based permissions
IPv4 Role-based permissions from group 1000 to group 4:Employees (configured):
        Deny_Log
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Cat8k#show access-list test Role-based IP access list Deny_Log
    10 deny ip log (732 matches)

*Jun 27 10:56:59.607: %FMANFP-6-IPACCESSLOGSGP: SIP0: fman_fp_image:  ingress_interface='Tunnel10'
sgacl_name='test' action='Deny' protocol='udp' src-ip='10.1.100.100' src-port='53' dest-
ip='10.1.200.100' dest-port='62717' sgt='1000' dgt='4' logging_interval_hits='20'

Cat8k#show cts environment-data
--snip--
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Devices
    3-00:Network_Services
    4-00:Employees
    5-00:Contractors
--snip—
```

SD-WAN TrustSec Monitoring

Inline Tagging

For your reference

```
ASR1KX-1#show platform hardware qfp active feature cts datapath stats
 Tagged Packets rcv: 883329 xmt: 625925     Def tag: 0
         Unknown SGT: 4986    Unknown DGT: 0
 Invalid tags (drop): 0 Bad format (drop): 0
 No xmt buffer: 0
 IPSec SGT tagged packets received: 0
 IPSec Invalid SGT tagged packets received: 0
 GRE SGT tagged packets received: 0
 GRE Invalid SGT tagged packets received: 0
 GRE invalid next protocol 0
 LISP SGT tagged packets received: 0
 LISP Invalid SGT tagged packets received: 0
 VXLAN SGT tagged packets received: 0
 VXLAN Invalid SGT tagged packets received: 0
```

```
ASR1KX-1#show platform hardware qfp active feature cts client interface
Interface internal0/0/rp:0(2):
        Enable=1, Policy=1, Trust=0, Propagate=0, Internal=1
        SGT=0, SGT_caching_in=0 SGT_caching_eg=0
        IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0

Interface GigabitEthernet0/0/0(5):
        Enable=1, Policy=0, Trust=1, Propagate=1, Internal=0
        SGT=2, SGT_caching_in=0 SGT_caching_eg=0
        IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0

Interface GigabitEthernet0/0/0.10(12):
        Enable=1, Policy=0, Trust=1, Propagate=1, Internal=0
        SGT=2, SGT_caching_in=0 SGT_caching_eg=0
        IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0

Interface GigabitEthernet0/0/0.20(13):
        Enable=1, Policy=0, Trust=1, Propagate=1, Internal=0
        SGT=2, SGT_caching_in=0 SGT_caching_eg=0
        IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0

Interface Tunnel1(16):
        Enable=1, Policy=0, Trust=0, Propagate=0, Internal=0
        SGT=0, SGT_caching_in=0 SGT_caching_eg=0
        IN_dbg/ IN_err=0/0, OUT_dbg/ OUT_err=0/0
```

SGT on the link trusted and propagate SGT enabled

'policy static sgt 2' configured and caching is not enabled

SD-WAN SGFW Logging

SD-WAN App for Splunk

splunk>enterprise Apps

Apps Manage

Search apps by name...

Search & Reporting

Cisco SD-WAN App for Splunk Pin

For your reference

Dropped ZBFW Flows

Source IP: * Destination IP: * Ingress VRF ID: *
Egress VRF ID: * FW Rule Name: *

Source IP	Destination IP	Ingress VRF ID	Egress VRF ID	FW Rule Name	Count
34.120.208.123	10.0.31.12	4	4	N/A	12
34.120.208.123	10.0.31.12	4	4	N/A	11
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10
34.120.208.123	10.0.31.12	4	4	N/A	10

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Inspected ZBFW Flows

Source IP: * Destination IP: * Ingress VRF ID: *
Egress VRF ID: * FW Rule Name: *

Source IP	Destination IP	Ingress VRF ID	Egress VRF ID	FW Rule Name	
10.0.130.100	8.8.8.8	1	0	SJC24_DMZ_C8KV_B1_USP-seq-1-cm_	15721
10.0.2.10	8.8.8.8	2	0	US-WEST-SEC-POLICY_17_1886420553-seq-GST_INTE-210881171-cm_	10053
10.0.130.200	8.8.8.8	1	0	SJC24_DMZ_C8KV_B1_USP-seq-21-cm_	8800
10.0.31.11	8.8.8.8	4	0	C8200_DMZ_USP-seq-1-cm_	6227
10.0.31.2	192.168.2.206	4	0	C8200_DMZ_USP-seq-11-cm_	4645
10.0.31.11	142.250.189.206	4	0	C8200_DMZ_USP-seq-1-cm_	3883
10.0.1.10	8.8.8.8	1	0	US-WEST-SEC-POLICY_17_1886420552-seq-EMP_INTE-1071953325-cm_	2742
10.0.31.11	142.251.32.46	4	0	C8200_DMZ_USP-seq-1-cm_	1981
10.0.31.11	172.217.164.110	4	0	C8200_DMZ_USP-seq-1-cm_	1878
10.0.31.11	142.250.72.206	4	0	C8200_DMZ_USP-seq-1-cm_	1709

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

in 22m

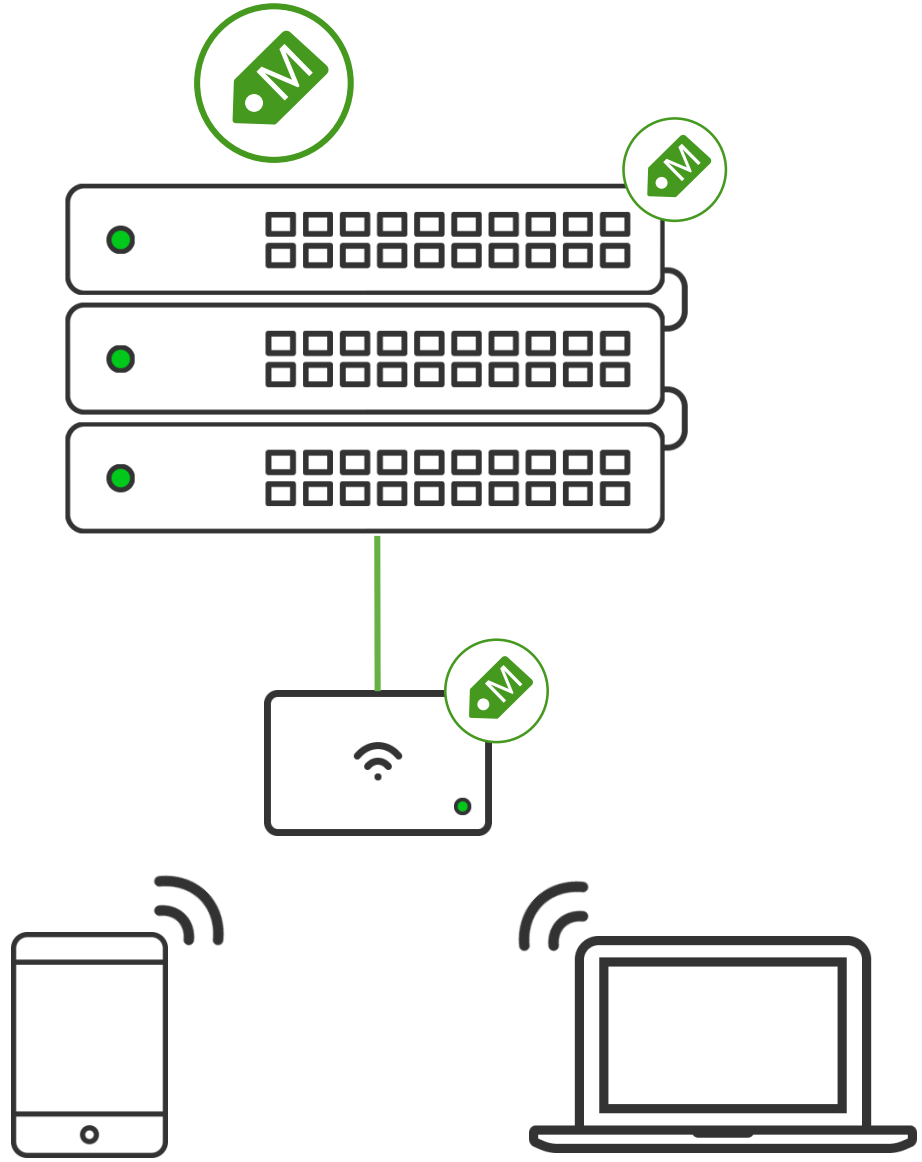
Inspected Flow Details Between "10.0.130.200" and "8.8.8.8"

Time	Source IP	Destination IP	Source Port	Destination Port	Application	FlowClass ID	Source Group Tag	NAT Source IP	NAT Destination IP	NAPT Source Transport Port	NAPT Destination Transport Port
2024-05-28 11:53:55	10.0.130.200	8.8.8.8	0 8	0 54806	ping	12363425	17	192.168.2.194	8.8.8.8	0 54806	0
2024-05-28 11:53:55	10.0.130.200	8.8.8.8	0 8	0 54805	ping	12363425	17	192.168.2.194	8.8.8.8	0 54805	0

Meraki Adaptive Policy

TrustSec

- Security policy based on identifying tags, not IP
- Uses inline SGTs as tag mechanism
- Consistent organization wide policy
- Provides micro-segmentation within VLANs
- Flexible tag assignment
- Supported platforms:
  - All Meraki 802.11ac wave 2 and Wi-Fi 6 MR
    - Requires MR27 Firmware
  - All Meraki MS390 switching platforms
  - Requires MR Advanced License



• TrustSec

Static Data/Voice VLAN assignment

Previously Port/SGT was limited to just Data VLAN SGT assingment

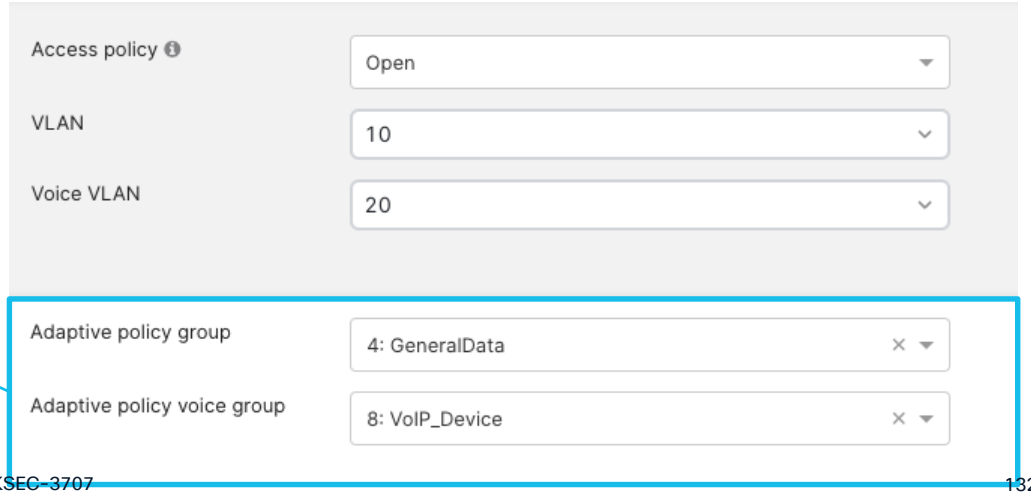
```
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 20
 device-tracking attach-policy access_track
 cts manual
  policy static sgt 4
  no propagate sgt
end
```

New IOS-XE Feature

```
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 20
 device-tracking attach-policy access_track
 cts role-based sgt-map vlanid 10 sgt 4
 cts role-based sgt-map vlanid 20 sgt 8
end
```

IOS-XE 17.15(2)/17.16(1)

Meraki Dashboard



MX/Z Supported Models and Firmware

For your reference

Models:
MX64/65/100*
MX67/68/75/85/95/105/250/450
Z3/Z4
Not supported on:
MX84

MX18.1+	NAT mode AutoVPN Support
MX18.2+	VPNc WAN propagation VLAN/Port SGT Inter-VLAN Preservation
**MX19+	Enforcement and further classification support

Licensing:
MX Advanced Licensing / SD-WAN

*only supported for AutoVPN transport in NAT mode
** subject to change based on release timelines for MX/Z

MX/Z Documentation and Support

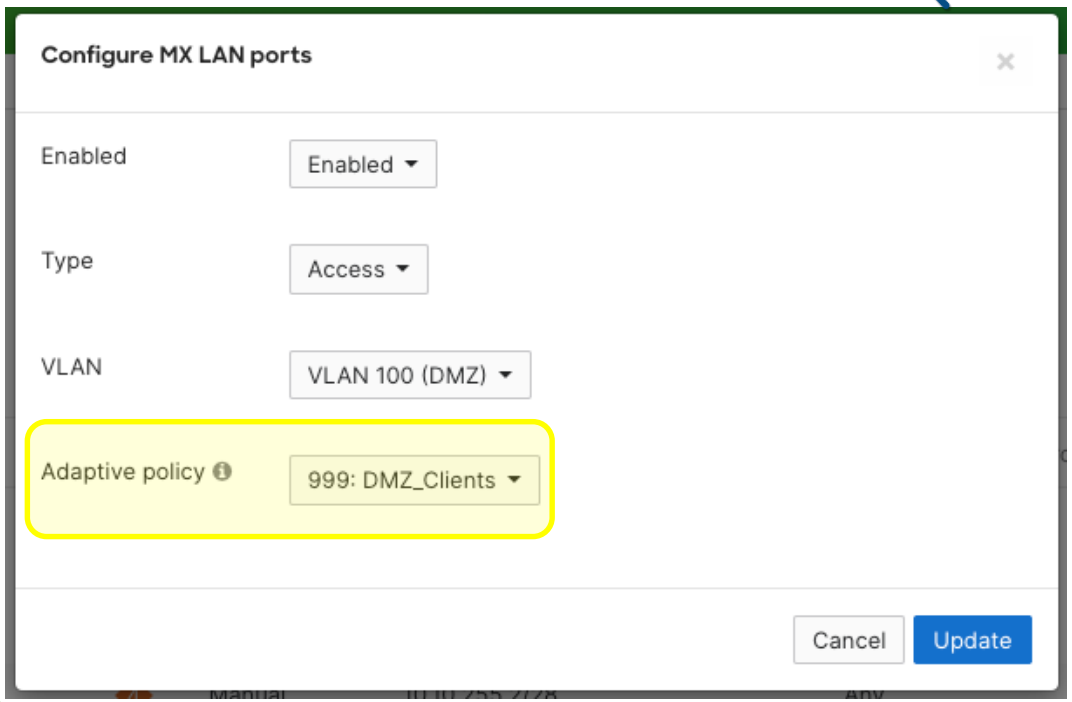
MX/Z Port to SGT classification

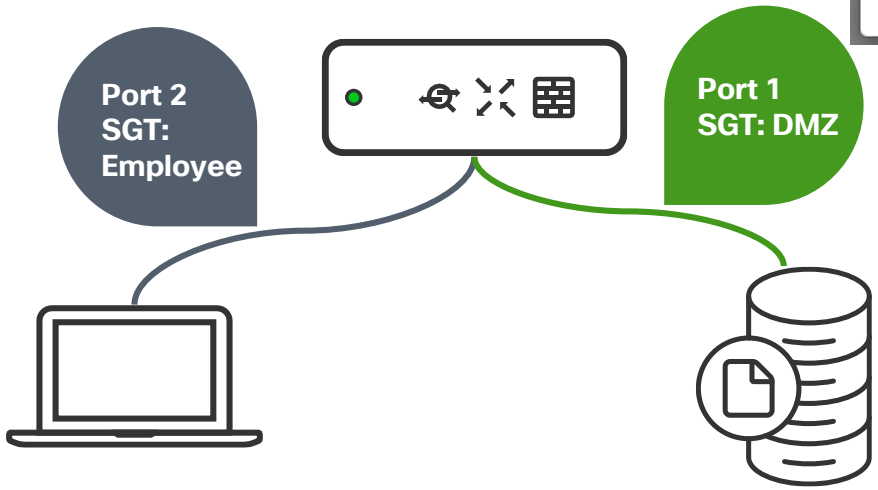
For your reference

Static SGT classification based on physical port

- Supported on Access and Trunk ports
- Classifies all devices and traffic behind the port with the configured SGT

Support starting in MX18.2+





MX/Z VLAN to SGT classification

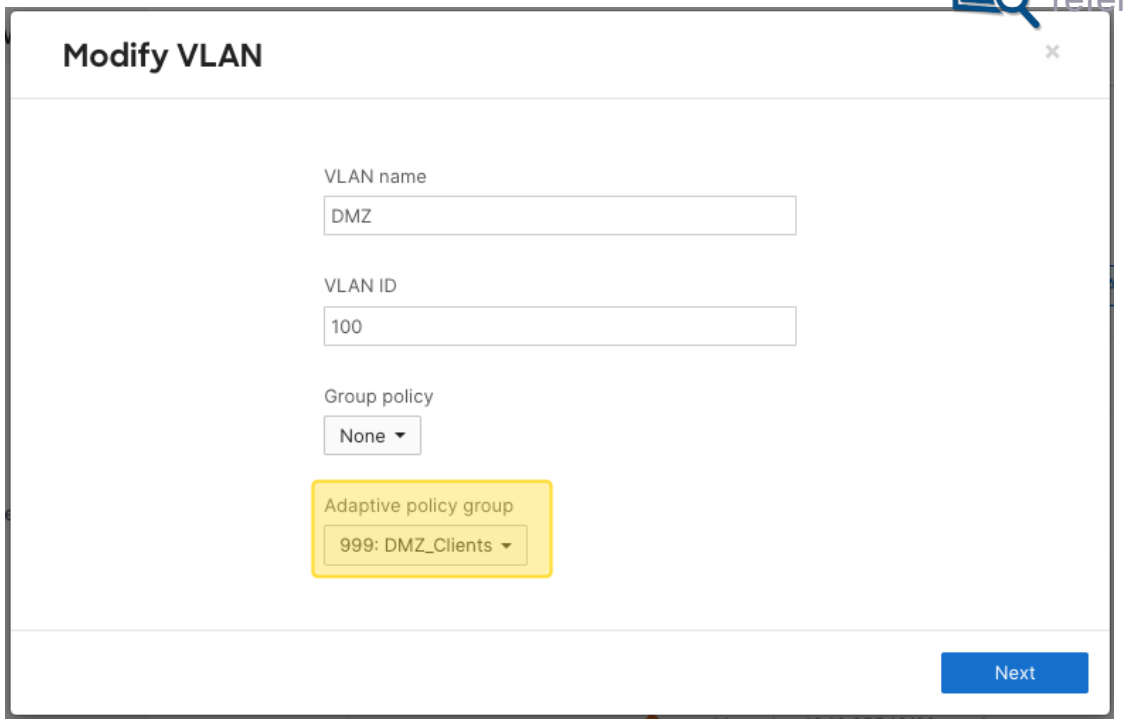
For your reference

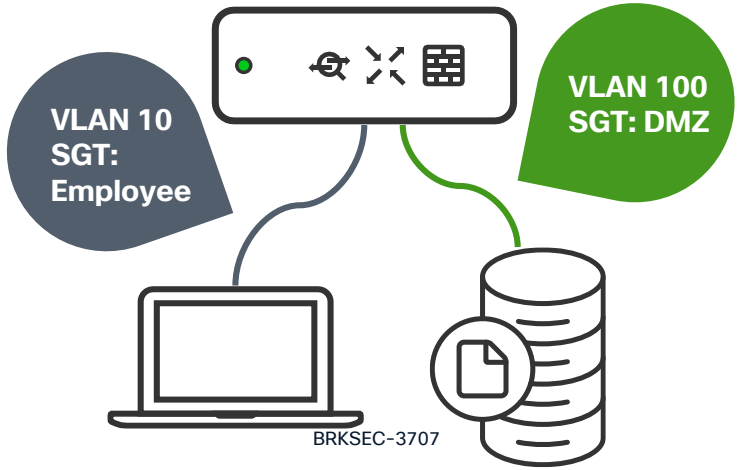
Static SGT classification based on physical port

Utilized for traffic ingress on a port where:

- There is no SGT configuration defined on the port

Supported in MX18.2+

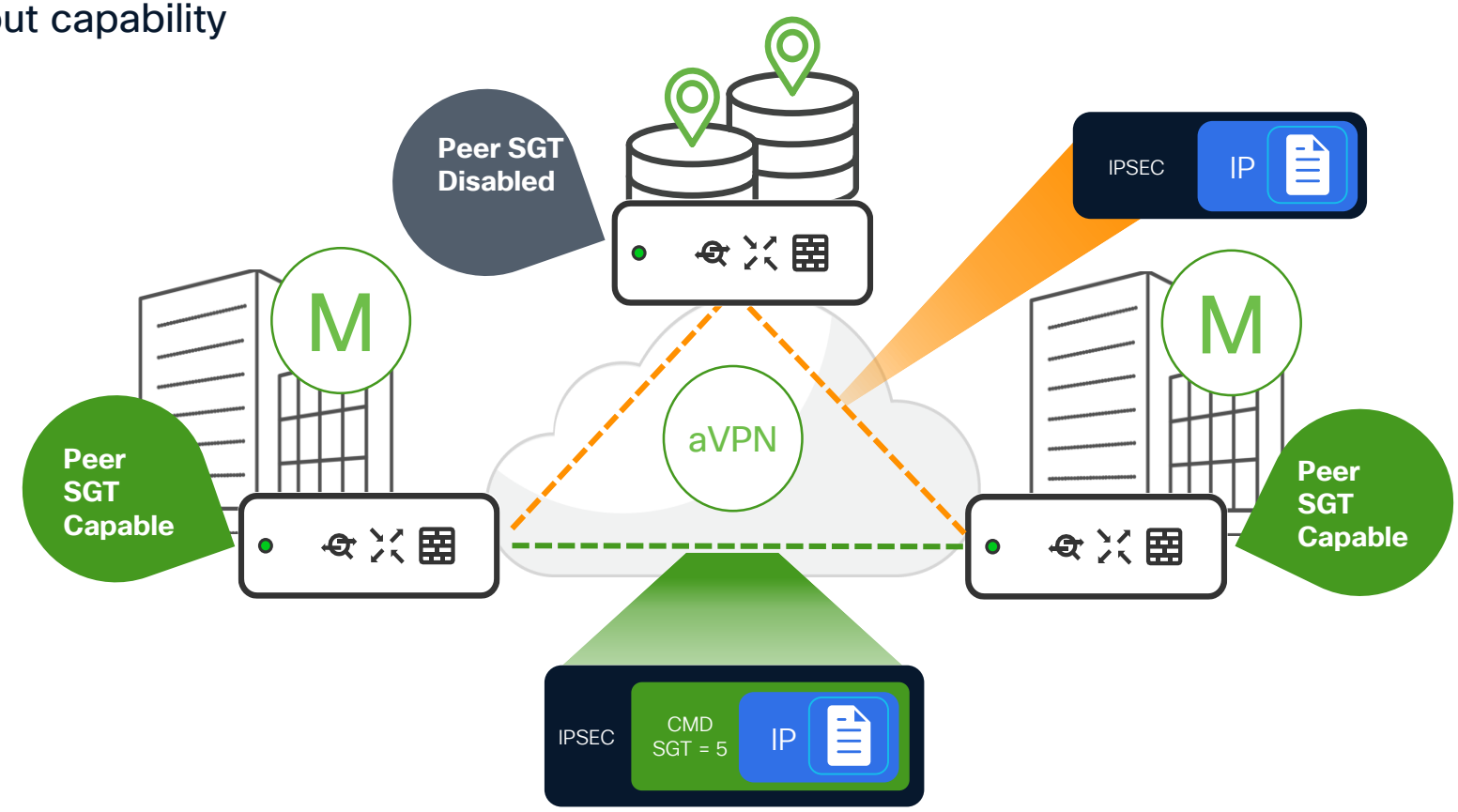




Expanding the policy scope beyond a site

A simple phased rollout capability

For your reference



- Sites with Adaptive Policy enabled will propagate SGTs to like peers
- Sites without Adaptive Policy enabled will still be able to communicate with the AutoVPN topology
  - Sites enabled will strip the header to non capable peers

AutoVPN Propagation + Preservation

For your reference

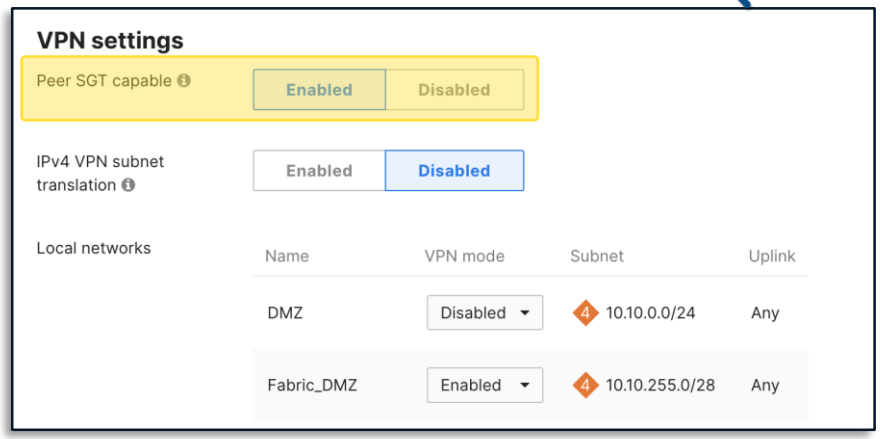
Enabling SGT Propagation and Preservation over AutoVPN takes 3 steps

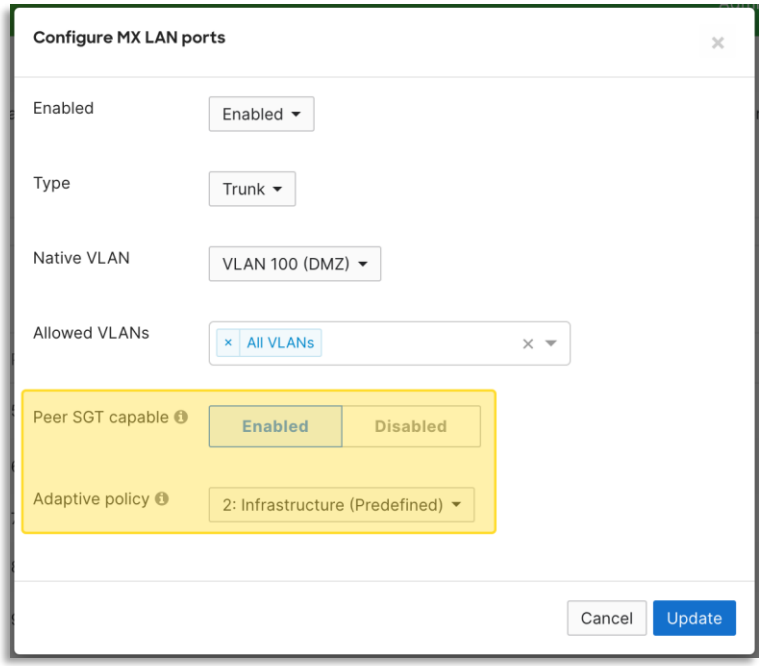
Step 1: Configure VLAN support on MX

Step 2: Set Site-to-Site VPN to Peer SGT capable

Step 3: Convert downlink to Trunk and enable Peer SGT Capable + Infrastructure SGT (when connected to a supported switch or access point)

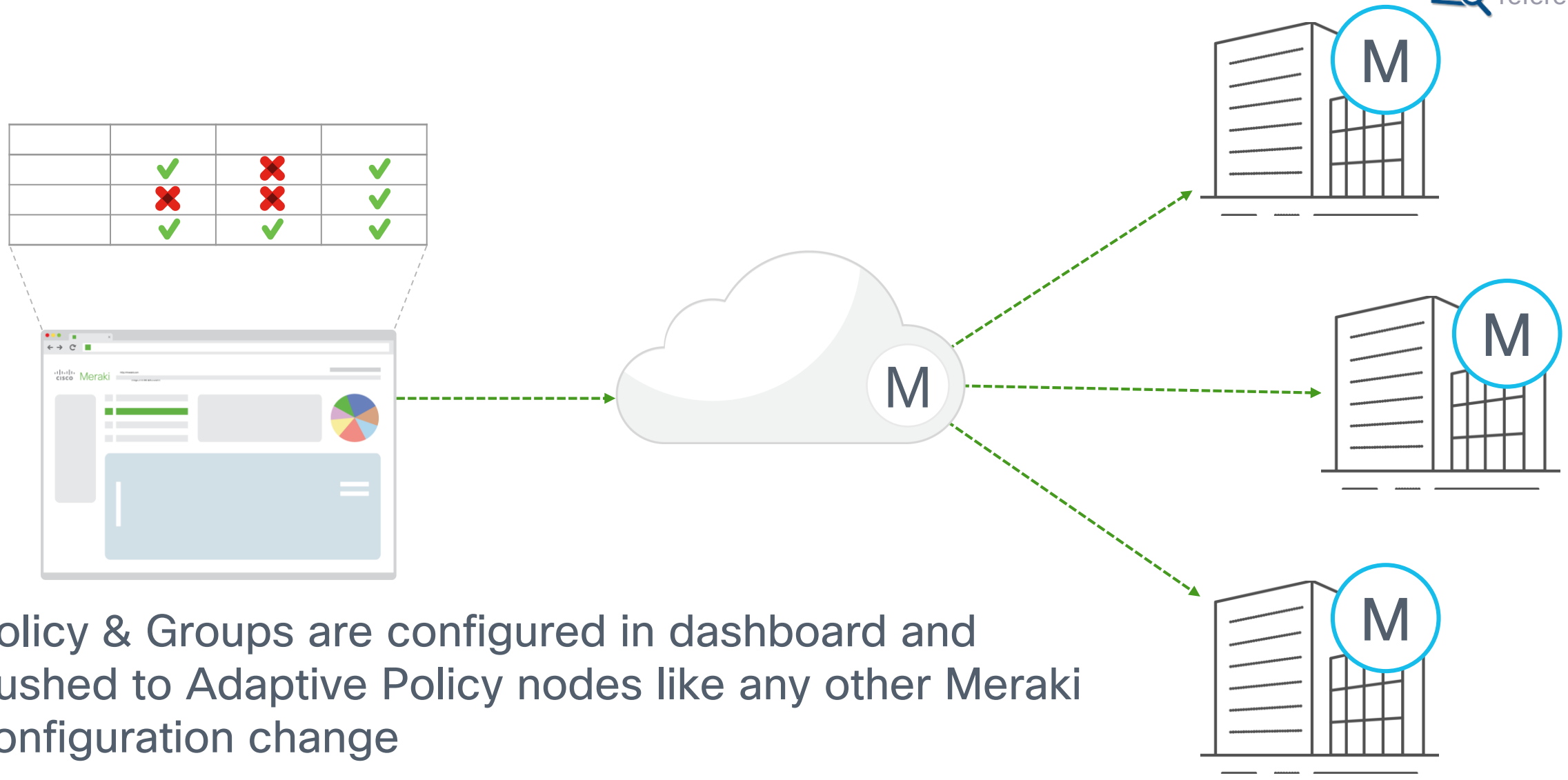
Step 2	Tells all VPN peers it can receive SGT encapsulated traffic
Step 3	Propagates SGTs from VPN to Port Trusts incoming tagged traffic





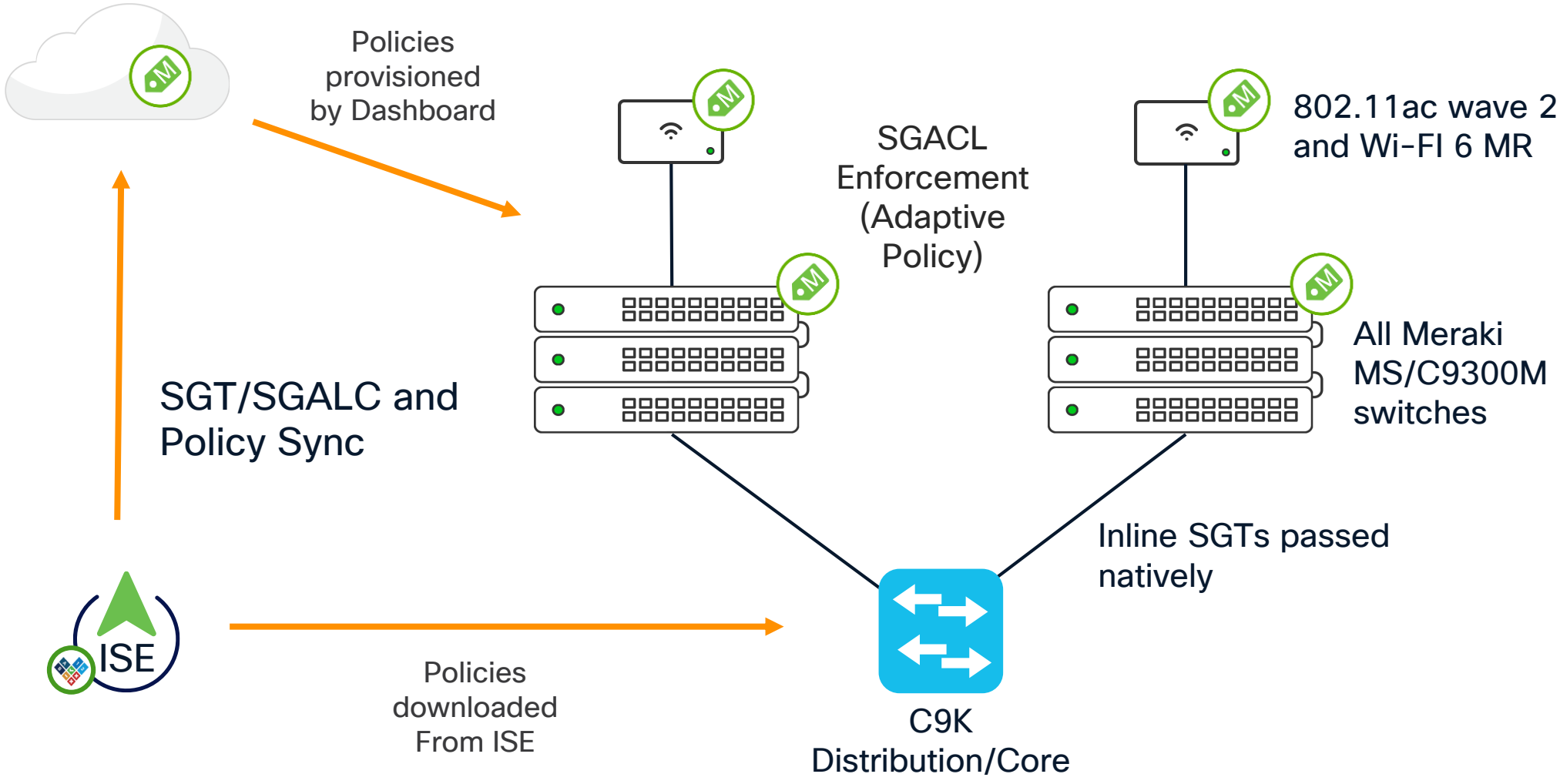
Consistent Policy Across Organization(s)

For your reference

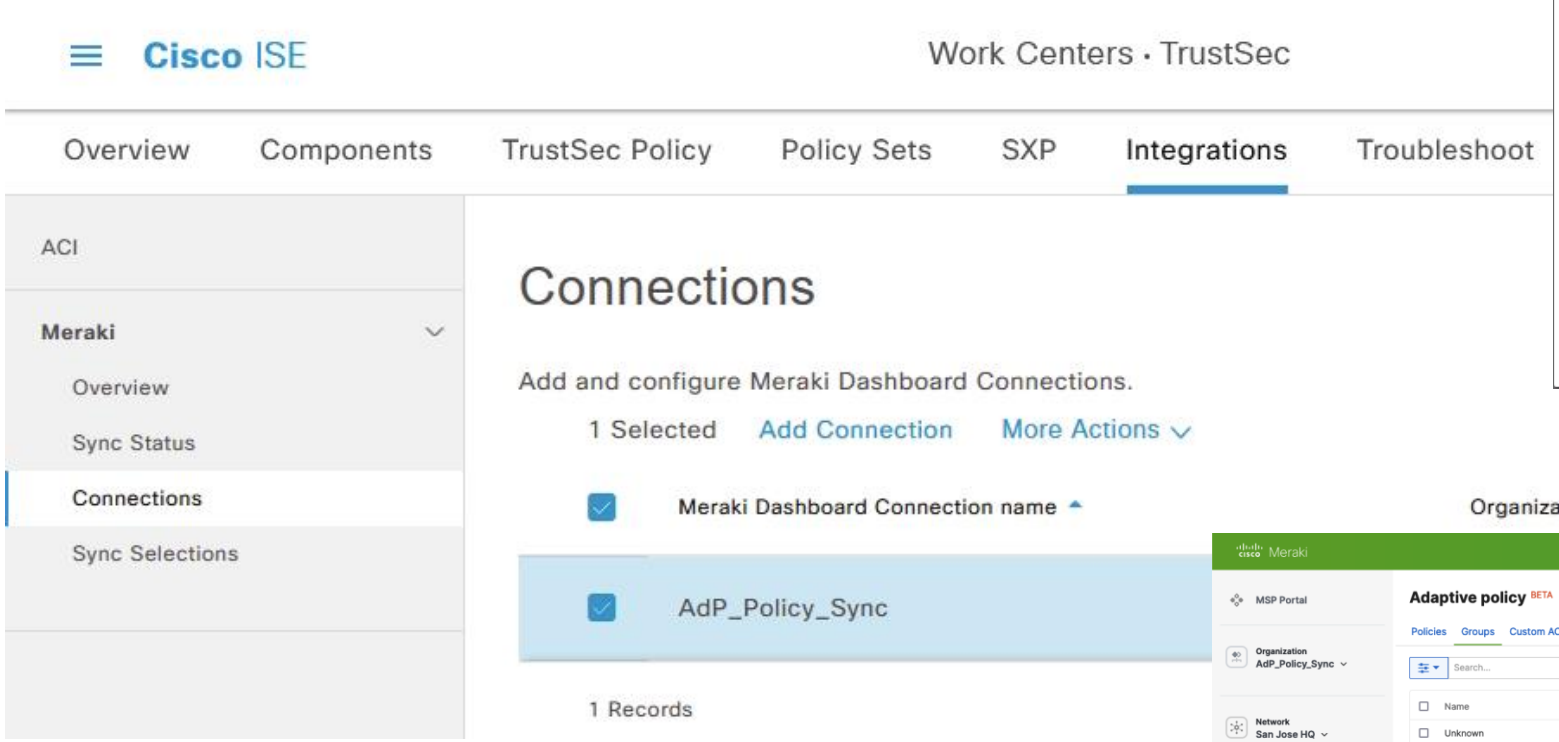


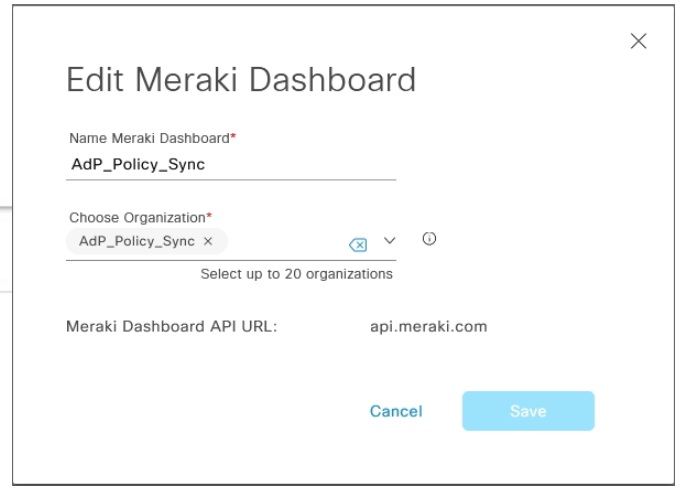
Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

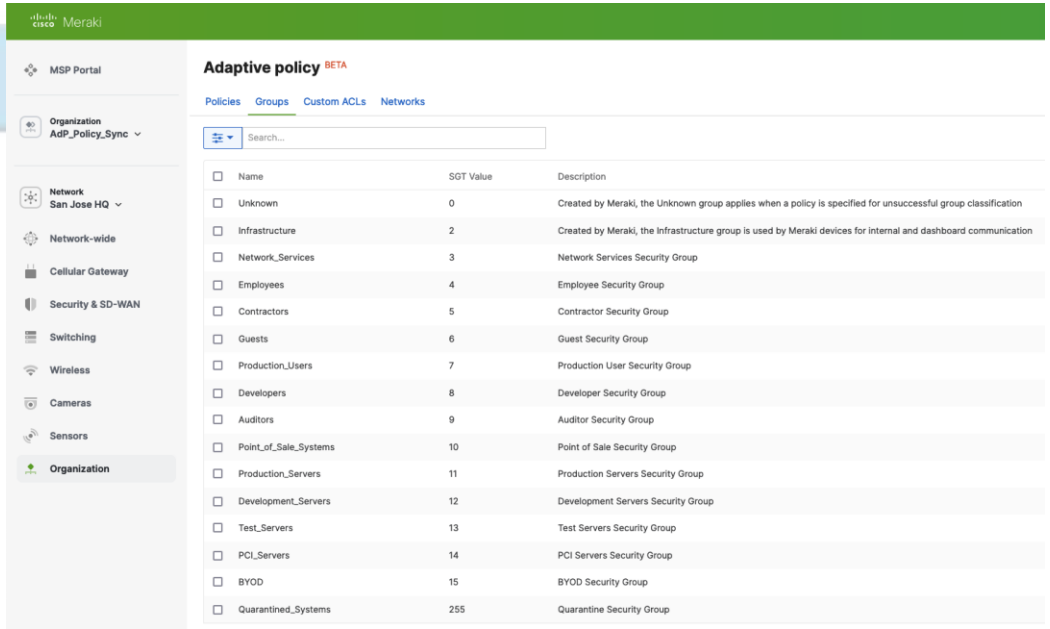
Meraki / Catalyst SGT Site



ISE – Meraki Policy Sync





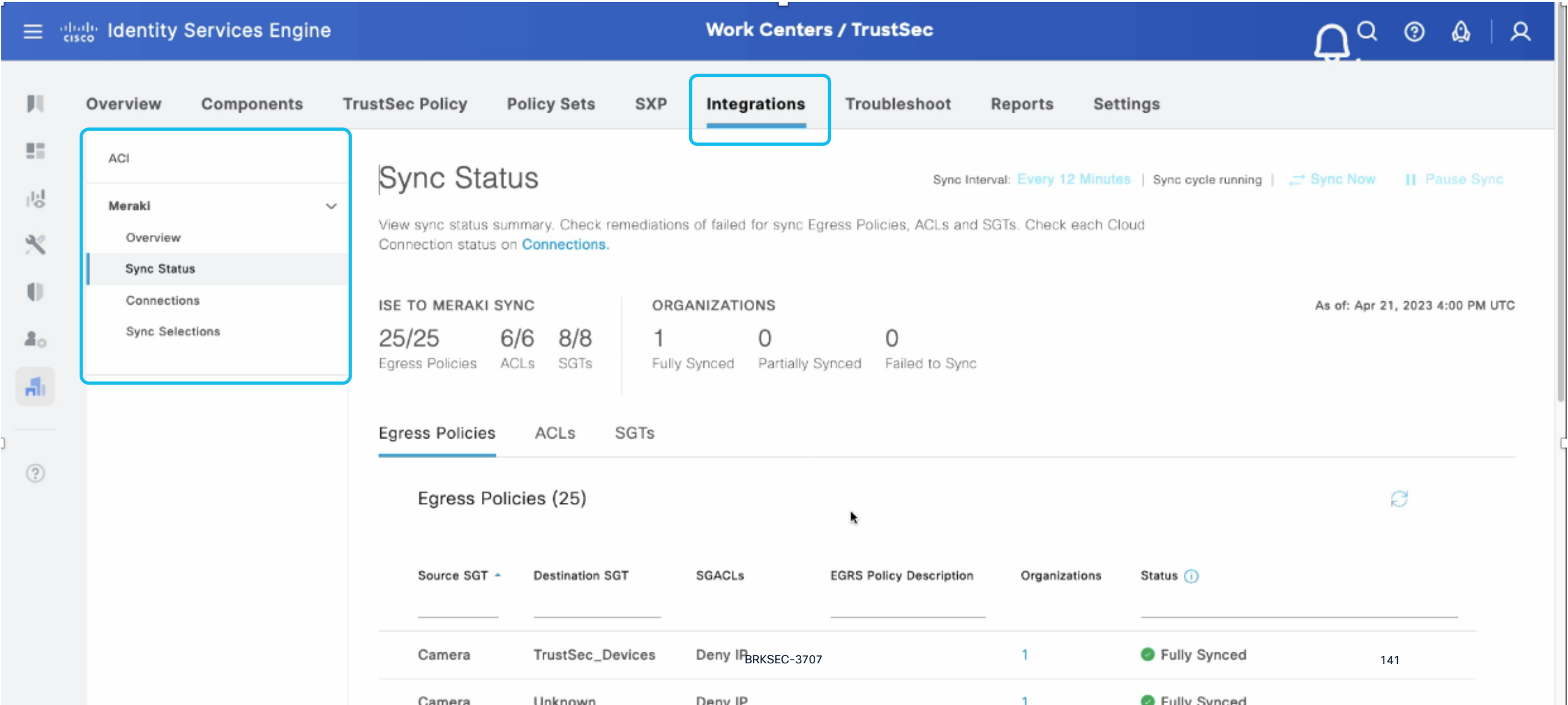


For your reference

ISE Meraki Connector

ISE 3.2p1

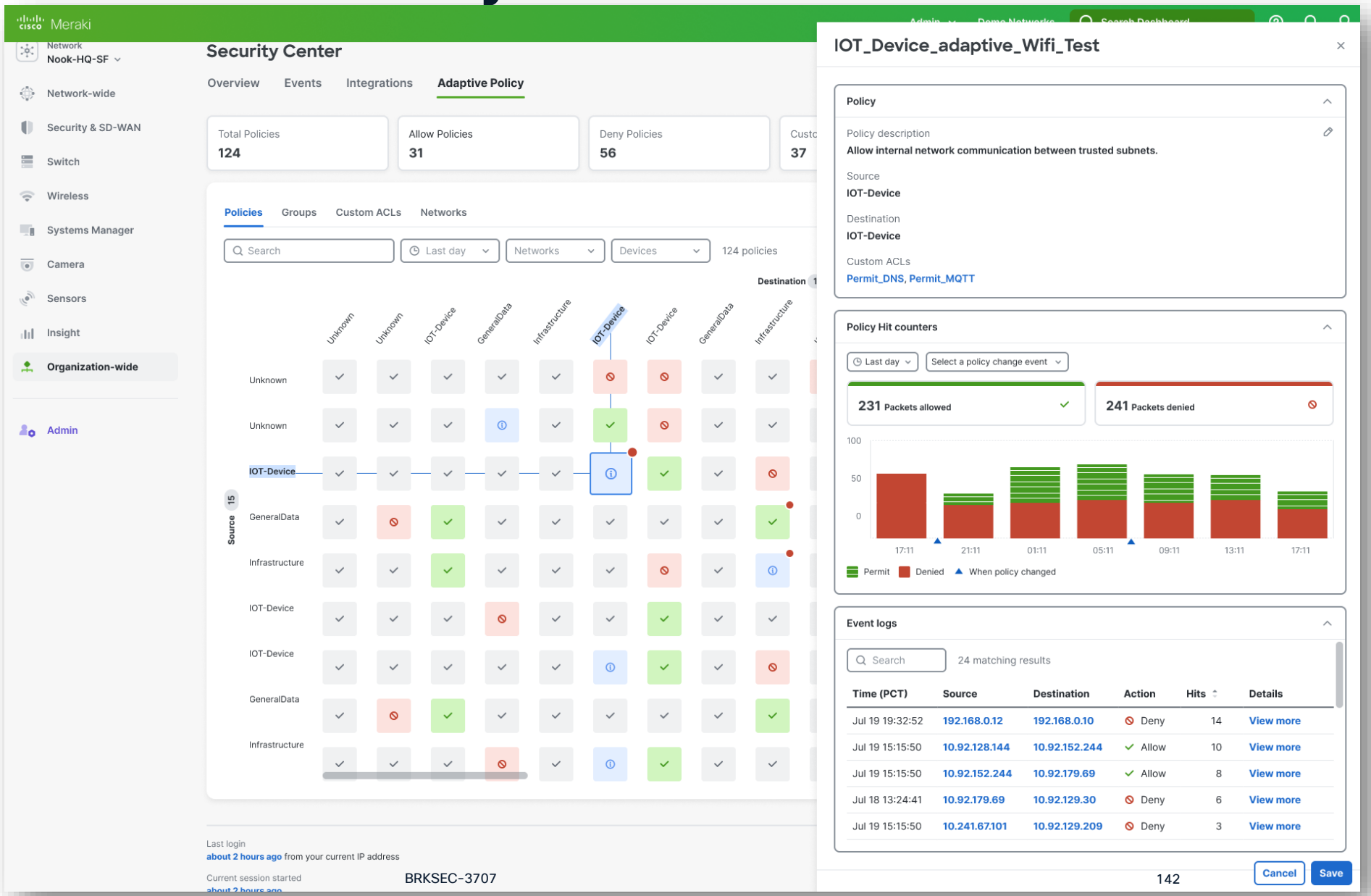
For your reference



Enhanced Matrix and Policy Visualization

Improvements in dashboard near term

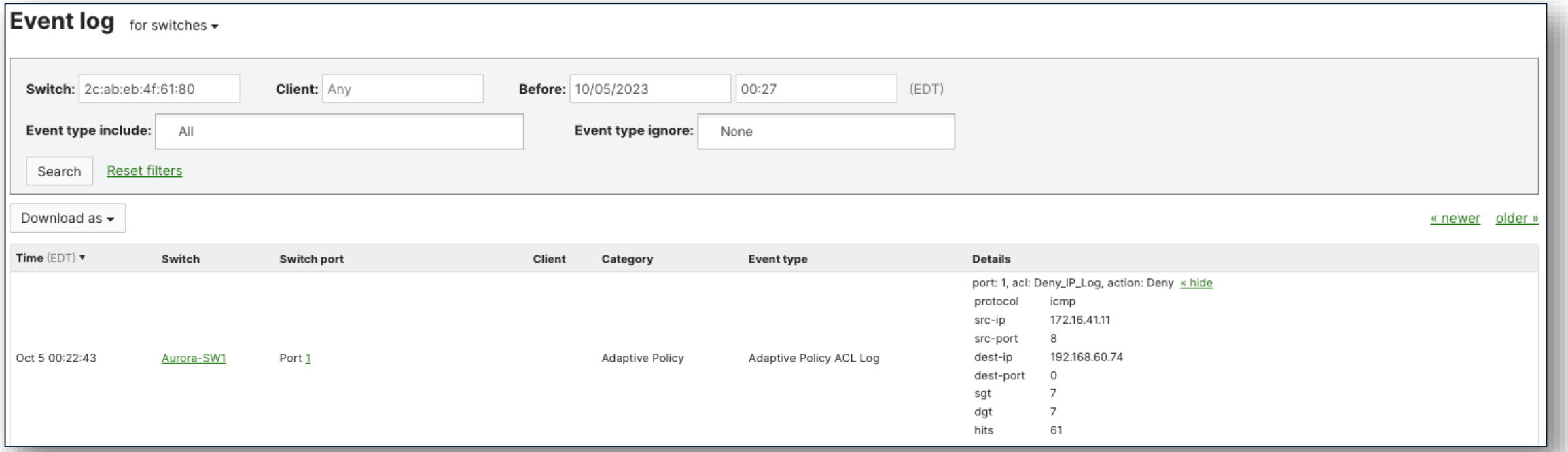
- Policy Management
- Activity Indicators
- Policy Visualization
- Historical Hit Counters
- Historical ACL Logging
- Policy change filtering for validation pre<>post change



Troubleshooting Tools – ACL Logging

Meraki logging per device

For your reference



Interval Log Reporting on ACE Processing

Switch Collects hits over interval and reports via Syslog + Dashboard Event Log

Logs are only collected on ACEs with logging enabled

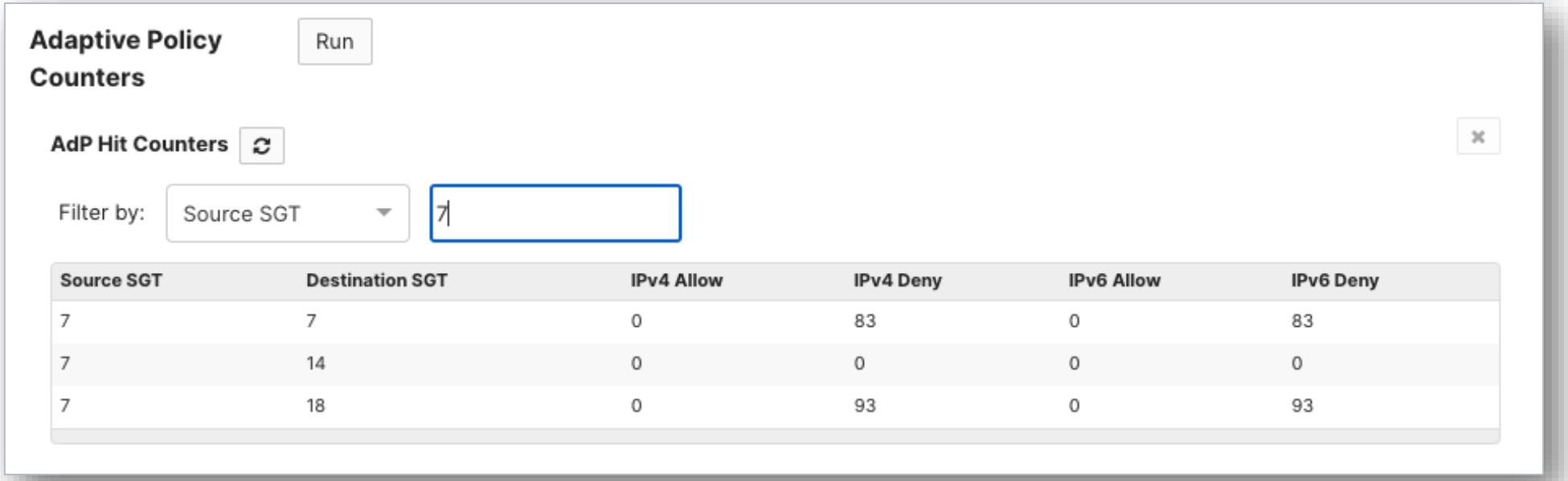
MS/CS Support for CS16 GA

MR/CW Support for MR31 GA

Troubleshooting Tools – Hit Counters

Meraki Dashboard

For your reference



Source SGT	Destination SGT	IPv4 Allow	IPv4 Deny	IPv6 Allow	IPv6 Deny
7	7	0	83	0	83
7	14	0	0	0	0
7	18	0	93	0	93

Live tool capture of hits between SGTs
Switch local data updated every 30 seconds
Hits are captured between groups when policy is explicitly defined (Allow/Deny/CustomACL)

MS/CS Support for CS16 GA

MR/CW Support for MR31 GA

Use Case Review – Hybrid Work

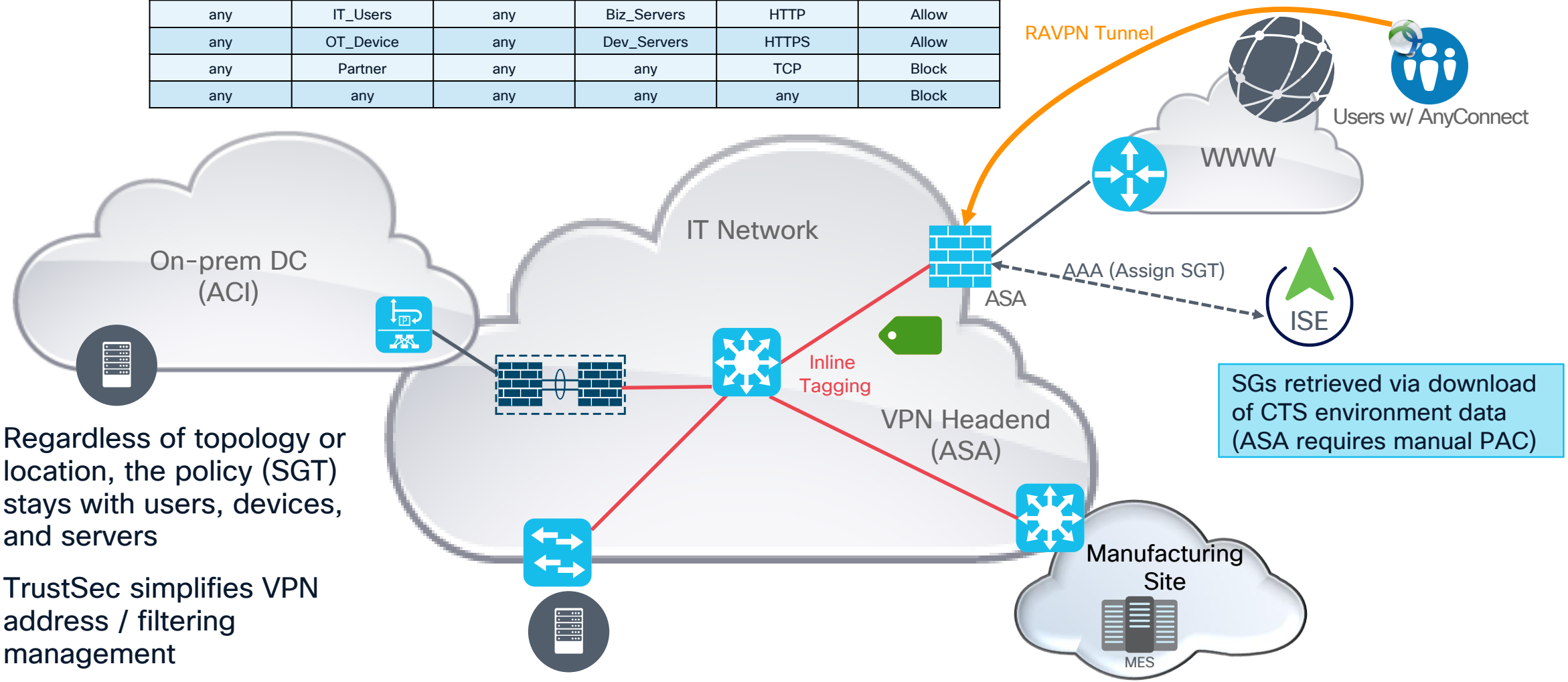
Manufacturer Design Update

- Acquisition of another company has led to an RFP for evaluation of hybrid work options
- Mergers and acquisitions have led to a reevaluation of Zero Trust Network Access Solutions

Add Segmentation to current RAVPN solution

ASA

Source Criteria		Destination Criteria		Service	Action
IP	SGT	IP	SGT		
any	IT_Users	any	Biz_Servers	HTTP	Allow
any	OT_Device	any	Dev_Servers	HTTPS	Allow
any	Partner	any	any	TCP	Block
any	any	any	any	any	Block



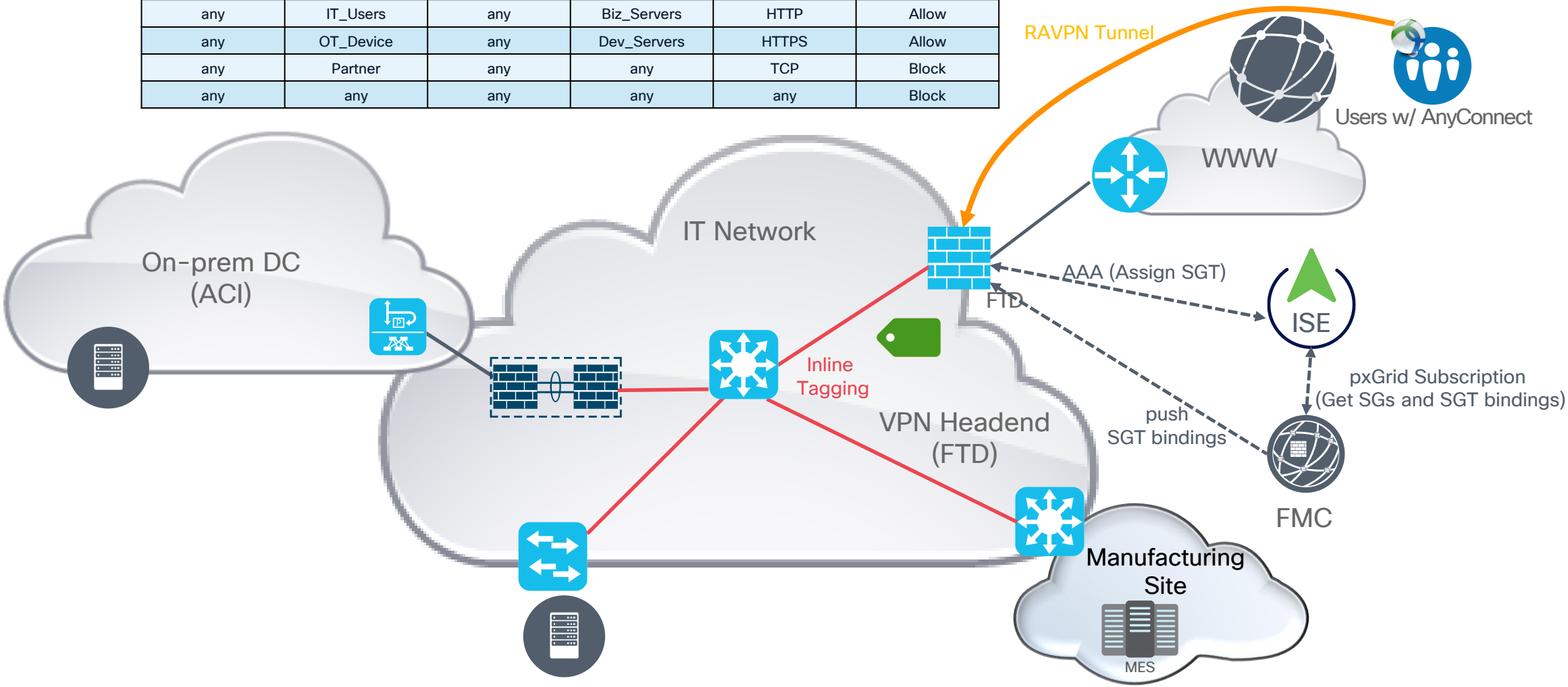
- Regardless of topology or location, the policy (SGT) stays with users, devices, and servers
- TrustSec simplifies VPN address / filtering management

SGs retrieved via download of CTS environment data (ASA requires manual PAC)

Add Segmentation to current RAVPN solution

FTD

Source Criteria		Destination Criteria		Service	Action
IP	SGT	IP	SGT		
any	IT_Users	any	Biz_Servers	HTTP	Allow
any	OT_Device	any	Dev_Servers	HTTPS	Allow
any	Partner	any	any	TCP	Block
any	any	any	any	any	Block

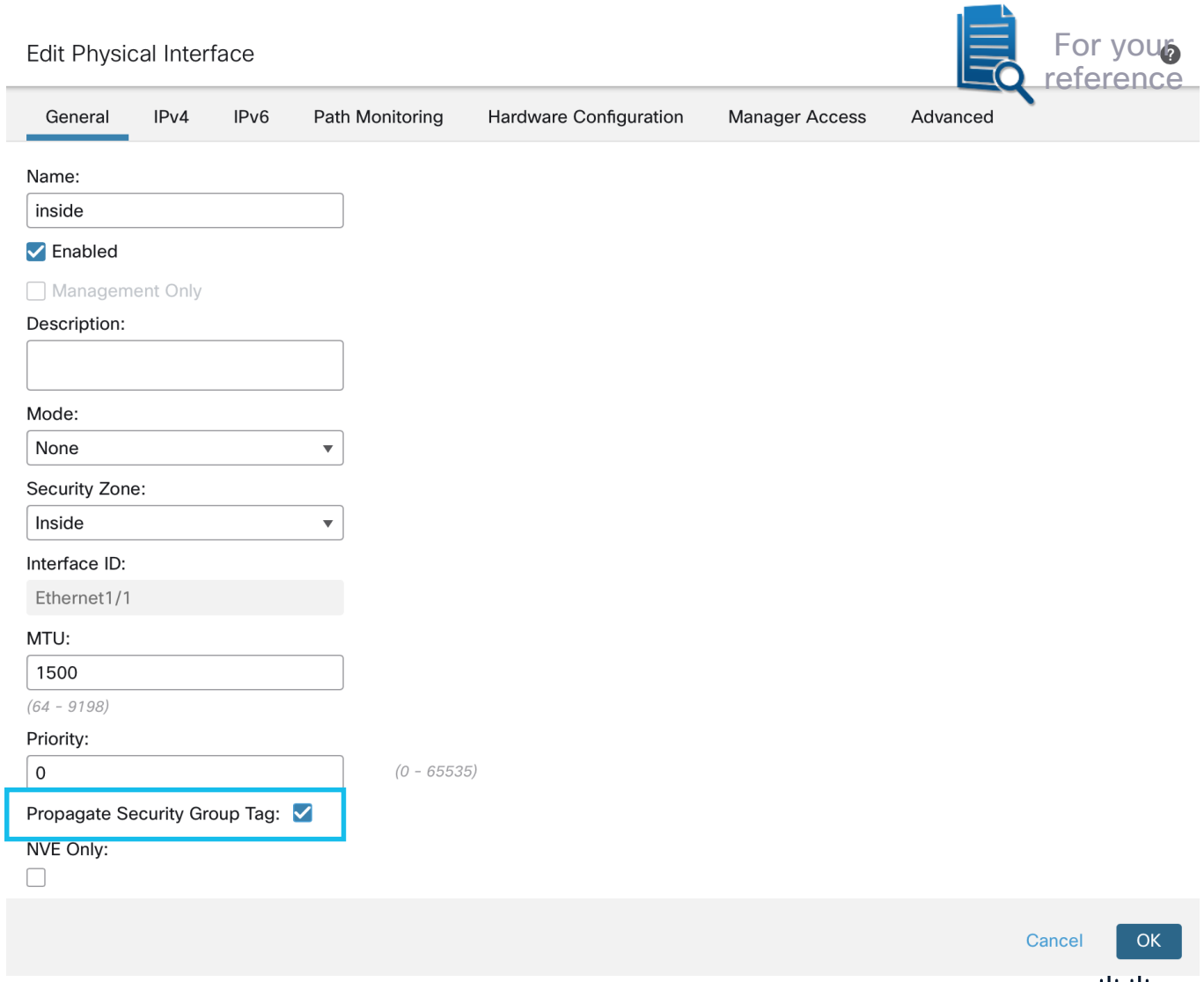


Enable FTD SGT inline tagging for RAVPN users

Enable/Disable CTS on interface

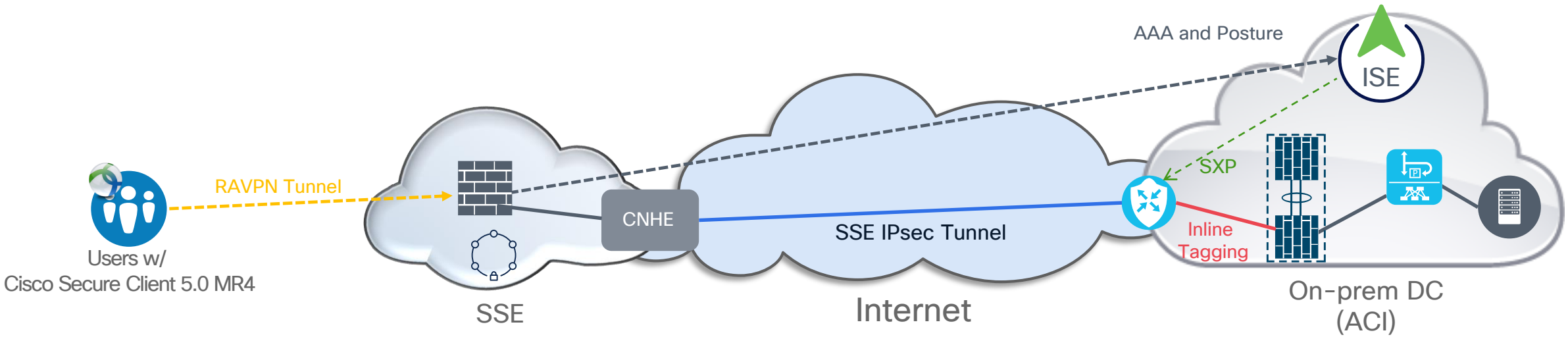
- CTS is disabled by default on all FTD interfaces
- You need to enable CTS depending on your ISE and Switch configuration

```
interface Ethernet1/1
 cts manual
  propagate sgt preserve-untag
```



RAVPN consumed as VPNaaS

Cisco Secure Access

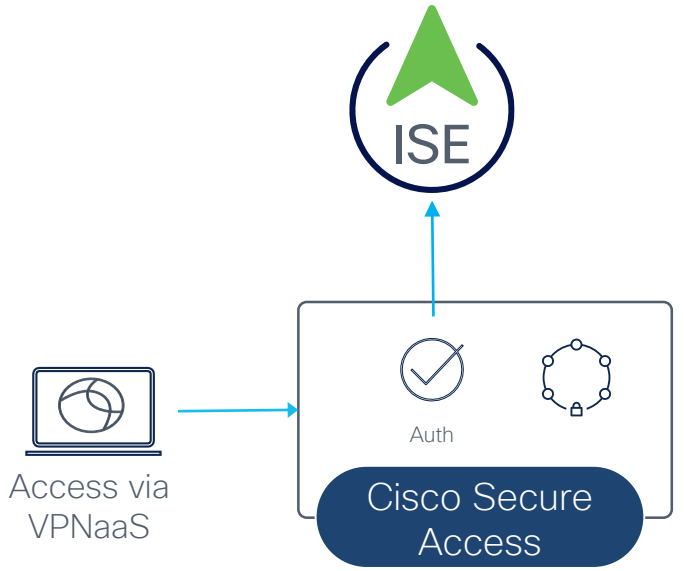


VPNaaS ISE integration

Cisco Secure Access

For your reference

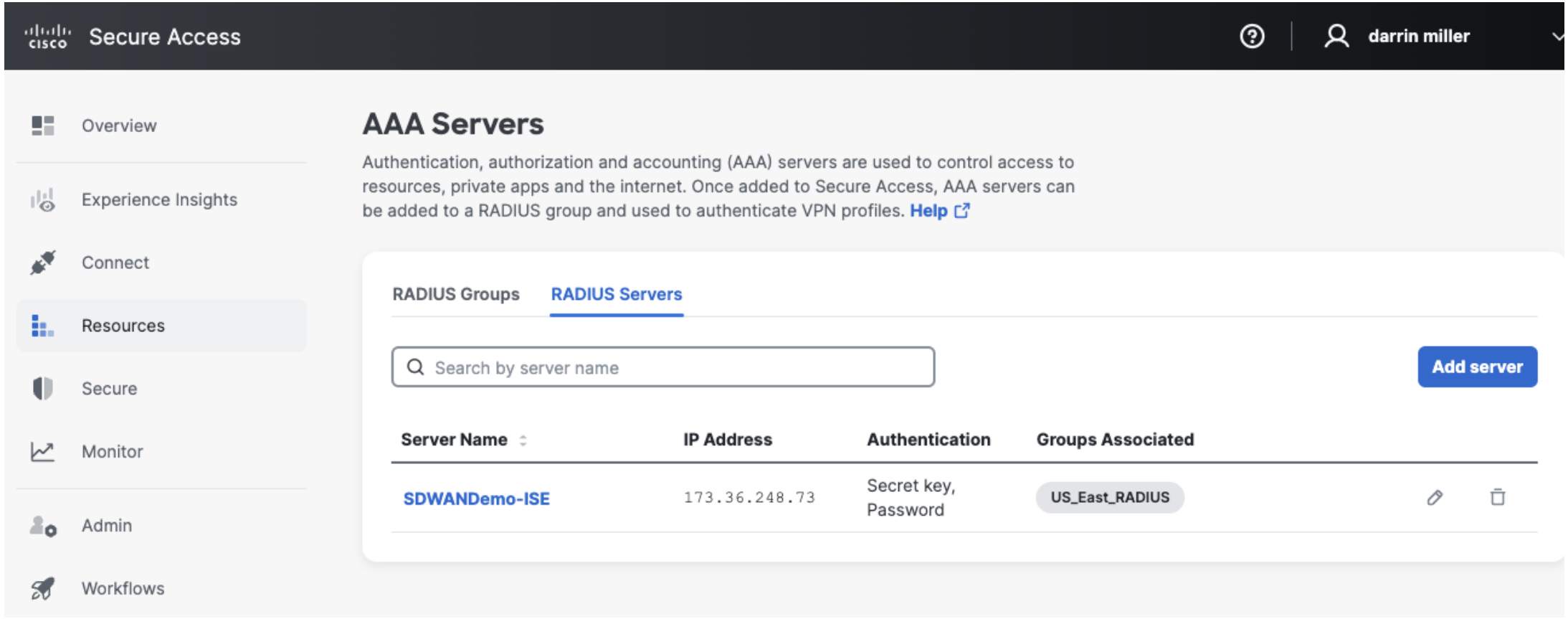
- RADIUS authentication, in addition to SAML authentication
- Simplifies IT operations as RADIUS is already widely used for identity-based access - includes CoA support
- Foster consistency with RADIUS to manage identity for remotely connected users (VPNaaS) and on-premises users.
- Leverage ISE identity and posture context to deepen Cisco Secure Access's visibility into what users are doing, when, and how
- Secure Access ingests the identity and posture context from ISE to inform security policy creation and enforcement
- In the future: AI analytics will be able to detect anomalies in device posture and automatically apply the correct policy



ISE for Remote Access VPNaaS

Cisco Secure Access

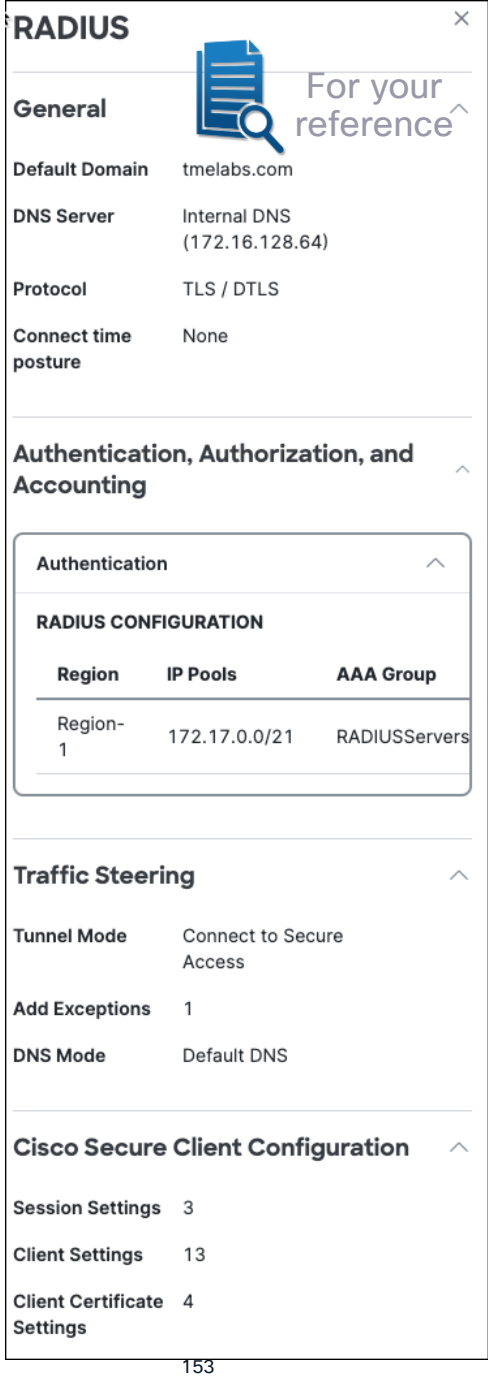
For your reference



VPNaaS Authentication Methods: RADIUS

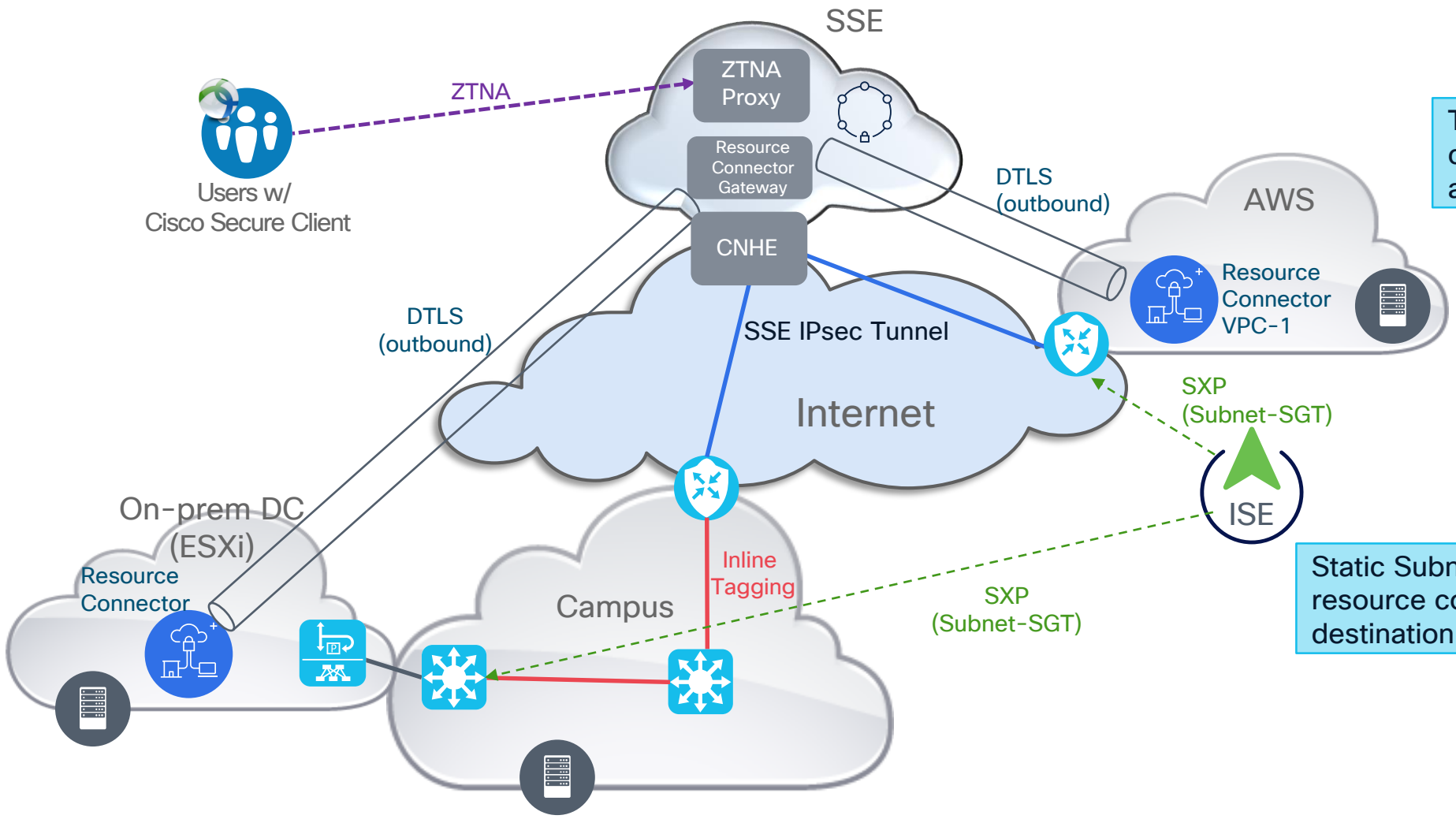
Cisco Secure Access

- Cisco Identity Services Engine (ISE) or 3rd Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- Dynamic ACLs supported
- CoA support with Cisco ISE
- ISE posture supported (optional)



ZTNA

Cisco Secure Access



The resource connectors are currently supported on AWS and VMware ESXi

Static Subnet-SGT bindings for resource connector regional destination FQDNs or IP addresses

Access rules for resource connectors to work

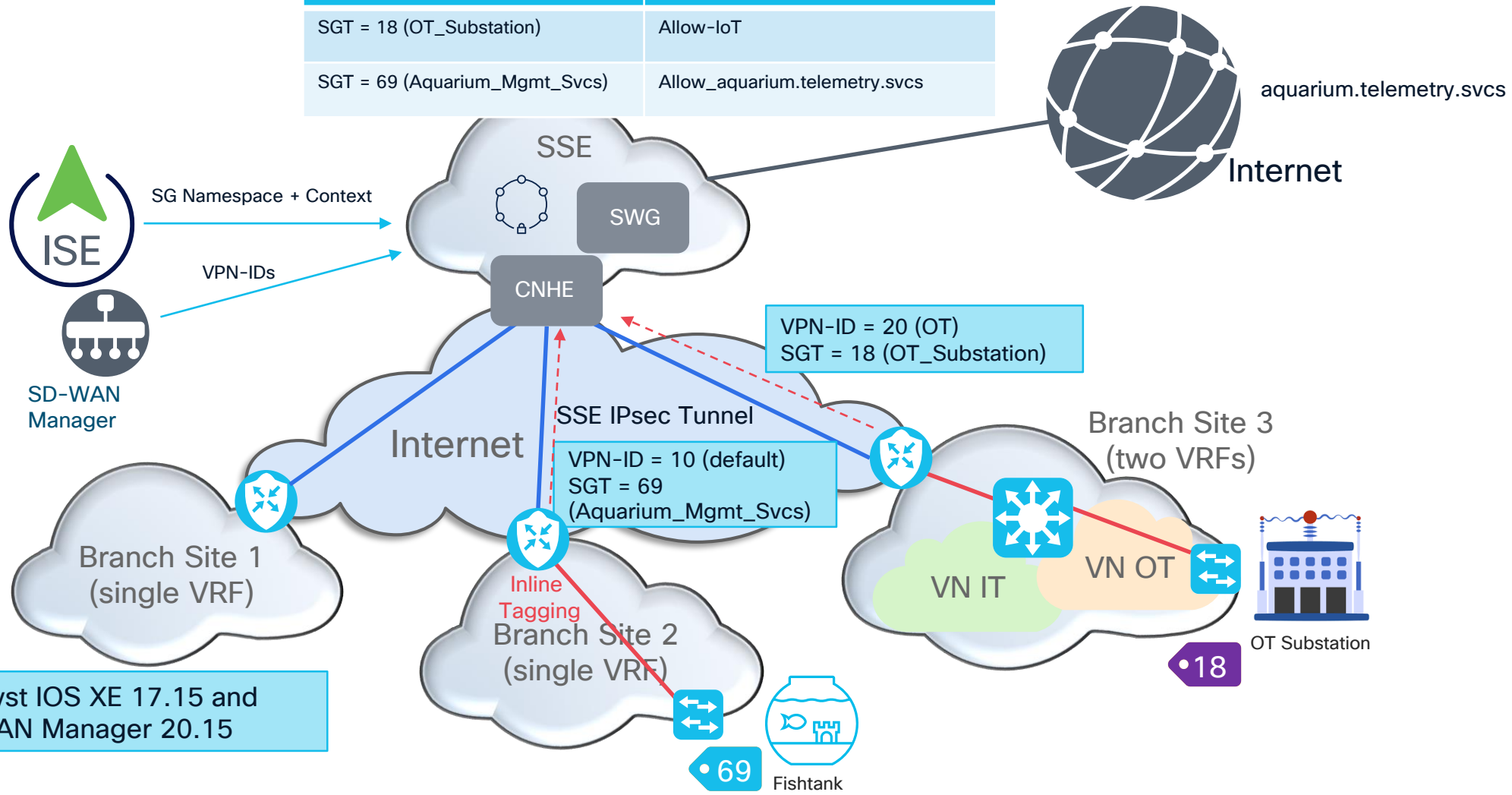
Customer edge firewall rules for Cisco Secure Private Access

Secure Access Services	FQDN or IP addresses for Whitelisting	Port/Protocol
Gateway	Regional, see https://docs.sse.cisco.com/sse-user-guide/docs/allow-resource-connector-traffic-to-secure-access	TCP/UDP 443
Controller	us.controller.acgw.sse.cisco.com eu.controller.acgw.sse.cisco.com ap.controller.acgw.sse.cisco.com Will resolve to AWS Static IPs	TCP 443
Repo (Auto upgrades)	us.repro.acgw.sse.cisco.com eu.repo.acgw.sse.cisco.com ap.repo.acgw.sse.cisco.com	TCP 443
ACME	prod.acme.sse.cisco.com	TCP 443
API Gateway	api.sse.cisco.com	TCP 443
PKI	ssepki.cryptosvcs.cisco.com	TCP 80

ISE / SD-WAN – SSE Context Sharing

Cisco Secure Access

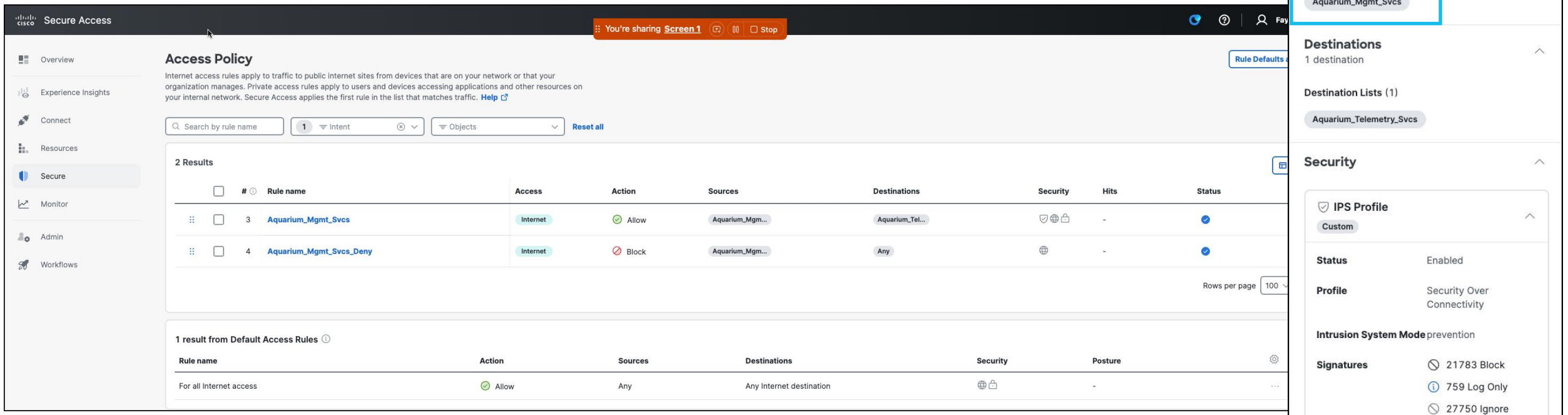
SGT OR VPN-ID	Action
SGT = 18 (OT_Substation)	Allow-IoT
SGT = 69 (Aquarium_Mgmt_Svcs)	Allow_aquarium.telemetry.svcs

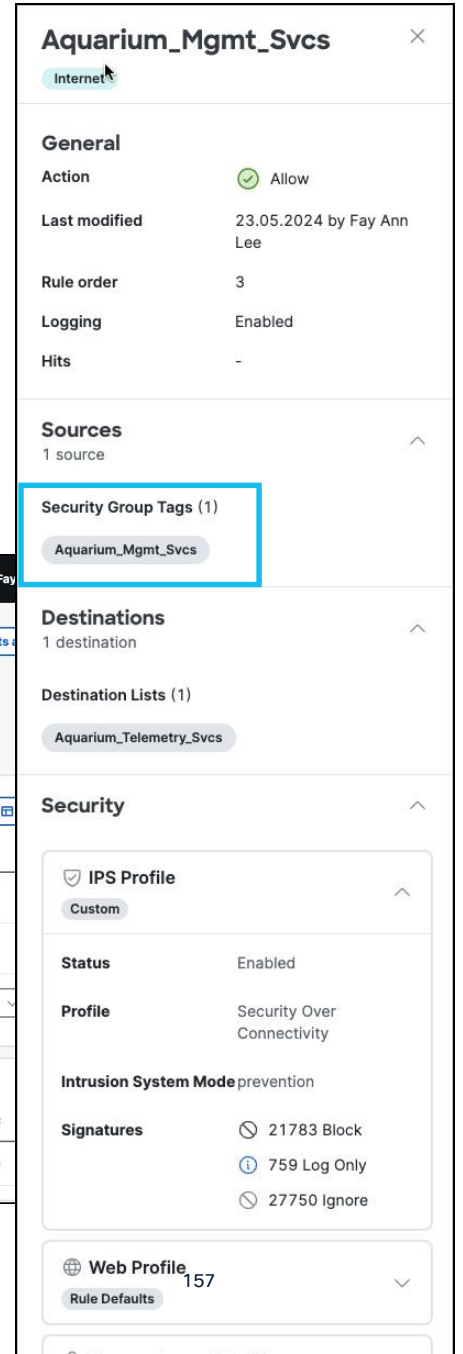


Requires Catalyst IOS XE 17.15 and Catalyst SD-WAN Manager 20.15

SGT-based Internet Policy

Cisco Secure Access





IaaS and Data Center

Manufacturer Design Update

- Acquisitions have led to a re-evaluation of IaaS and Data Center Network Security architecture and solutions
- Lateral movement within a single DC is within scope
- Lateral movement between DCs and IaaS is within scope

Inbound and Outbound SGT Domain Rules

ISE 3.4 New Concept

For your reference

RADIUS | ACI | Workload Connectors

Inbound SGT Domain Rule

Name	Logic	Result
SDA OT Inbound Logic	SGT PLC & VN OT	SGT Domain - OT
ACI Tenant OT Inbound Logic	ACI1 Tenant OT	SGT Domain - OT
Global Table	Any	SGT Domain - Default

SGT Domain OT

IP1/SGT OT
IP2/SGT ACI_OT (From ACI Tenant OT)
...

SGT Domain Default

IP3/SGT Employee
IP4/SGT ACI_App1 (From other ACI Tenant)
IP5/SGT Developer
...

Outbound SGT Domain Rule

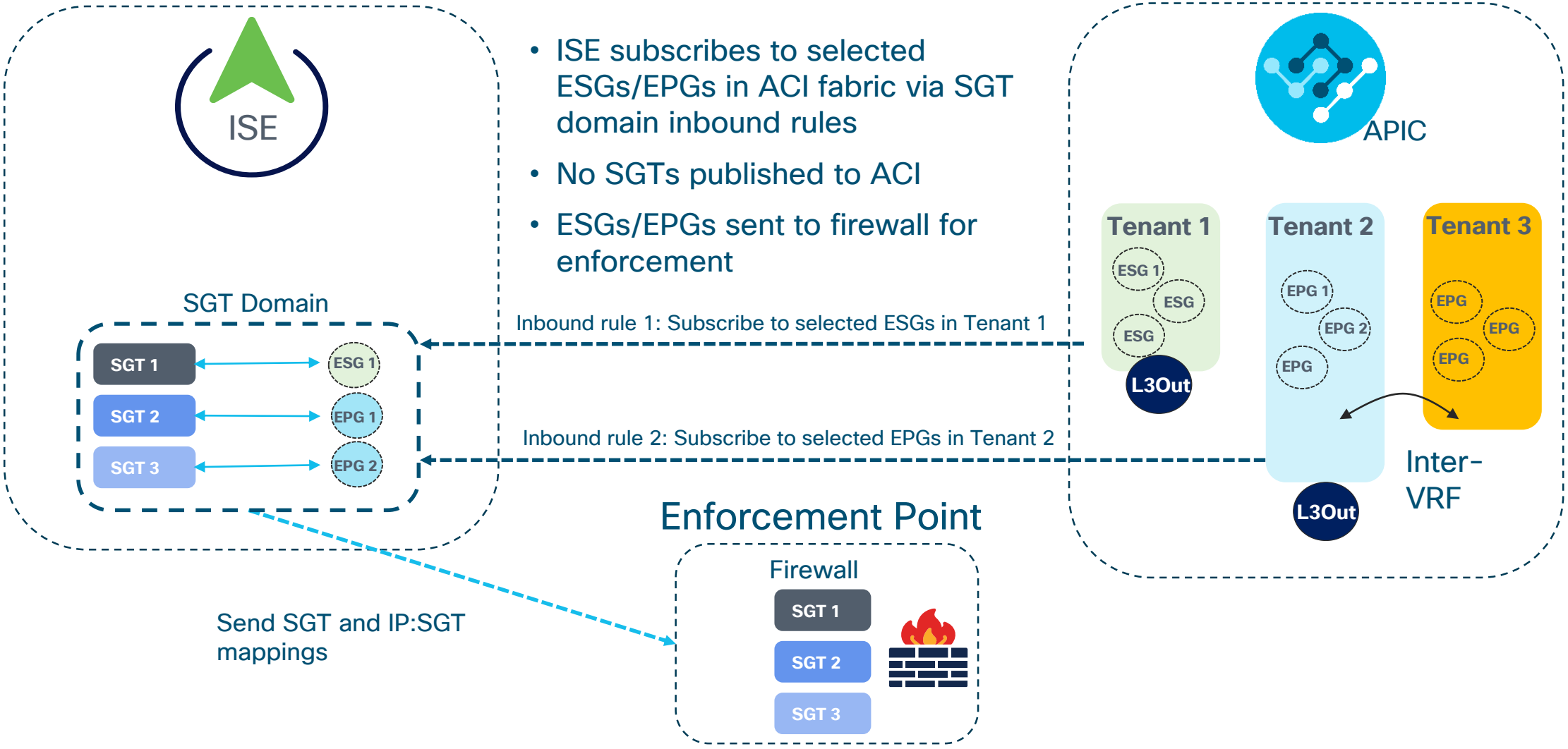
Name	Logic	Result
SDA OT Outbound Logic to AC1	SGT Domain OT	ACI1 Tenant OT
SDA OT to SXP VRF OT	SGT Domain OT	SXP Peer 1 – VRF OT
Global Table	Any	Any pxGrid or SXP Listener

pxGrid with Server-side filters | pxGrid with Client-side filters | SXPv5 with VRF (SGT Domain)*

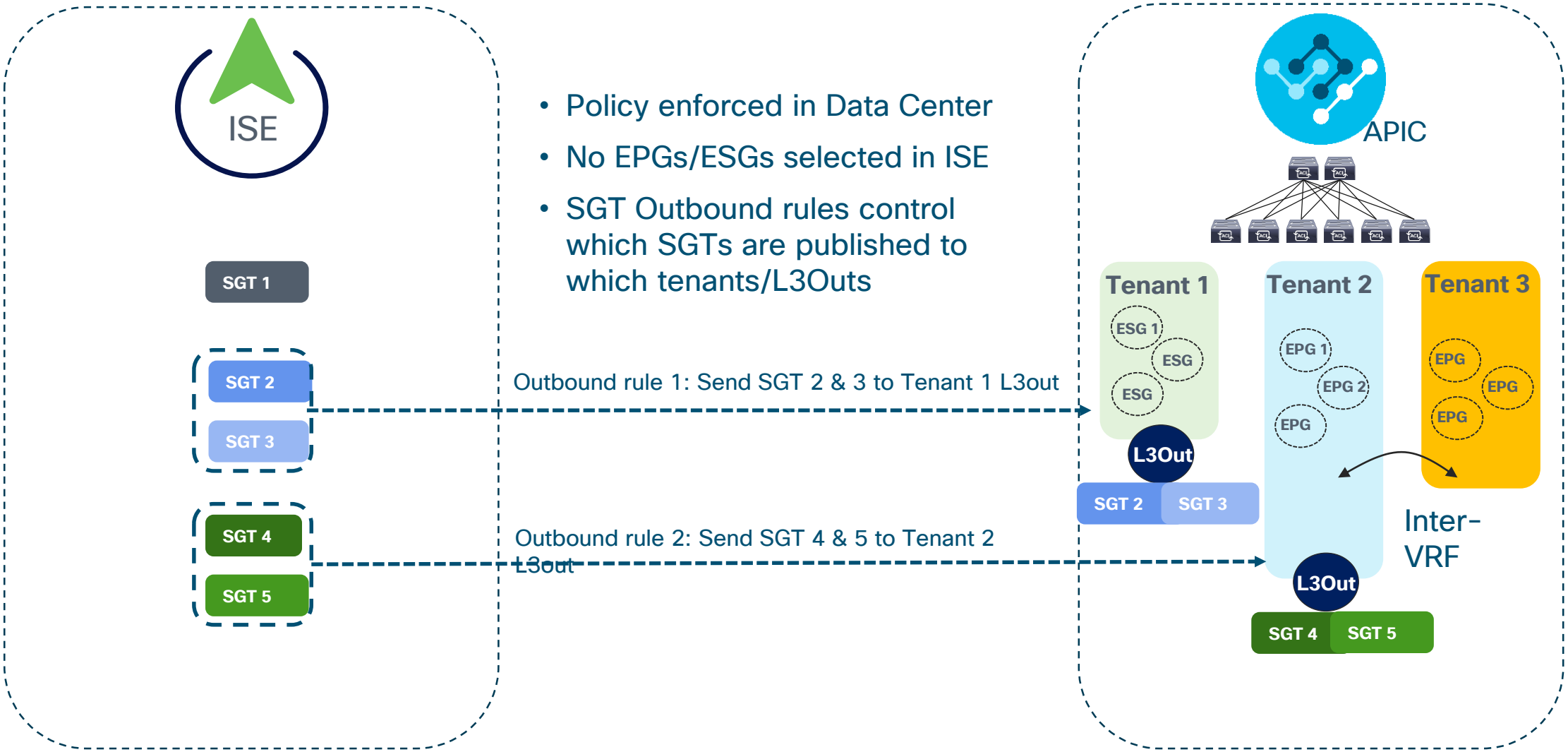
* SXPv5 future ISE 3.4 patch

cisco

Use Case: Policy Enforcement in Firewall

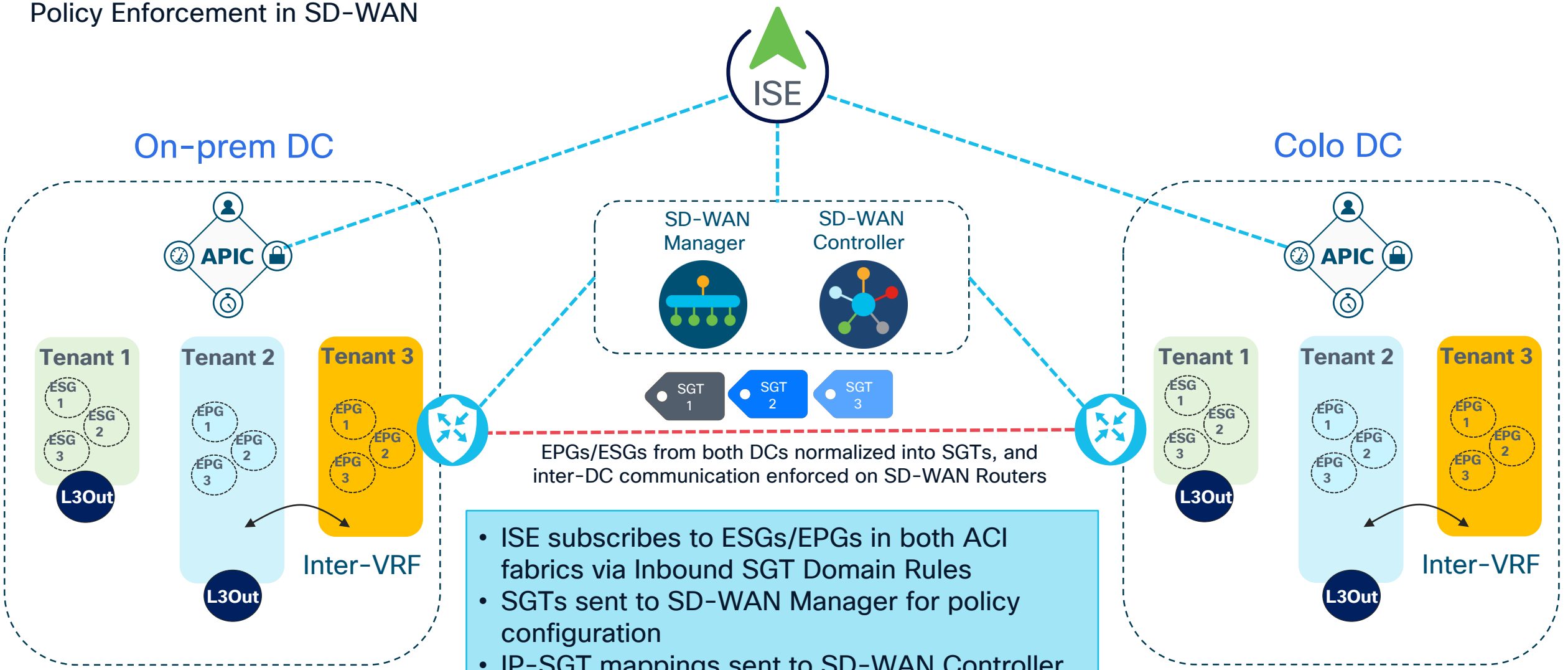


Use Case: Policy Enforcement in Data Center



On-prem DC to Colo DC access

Policy Enforcement in SD-WAN

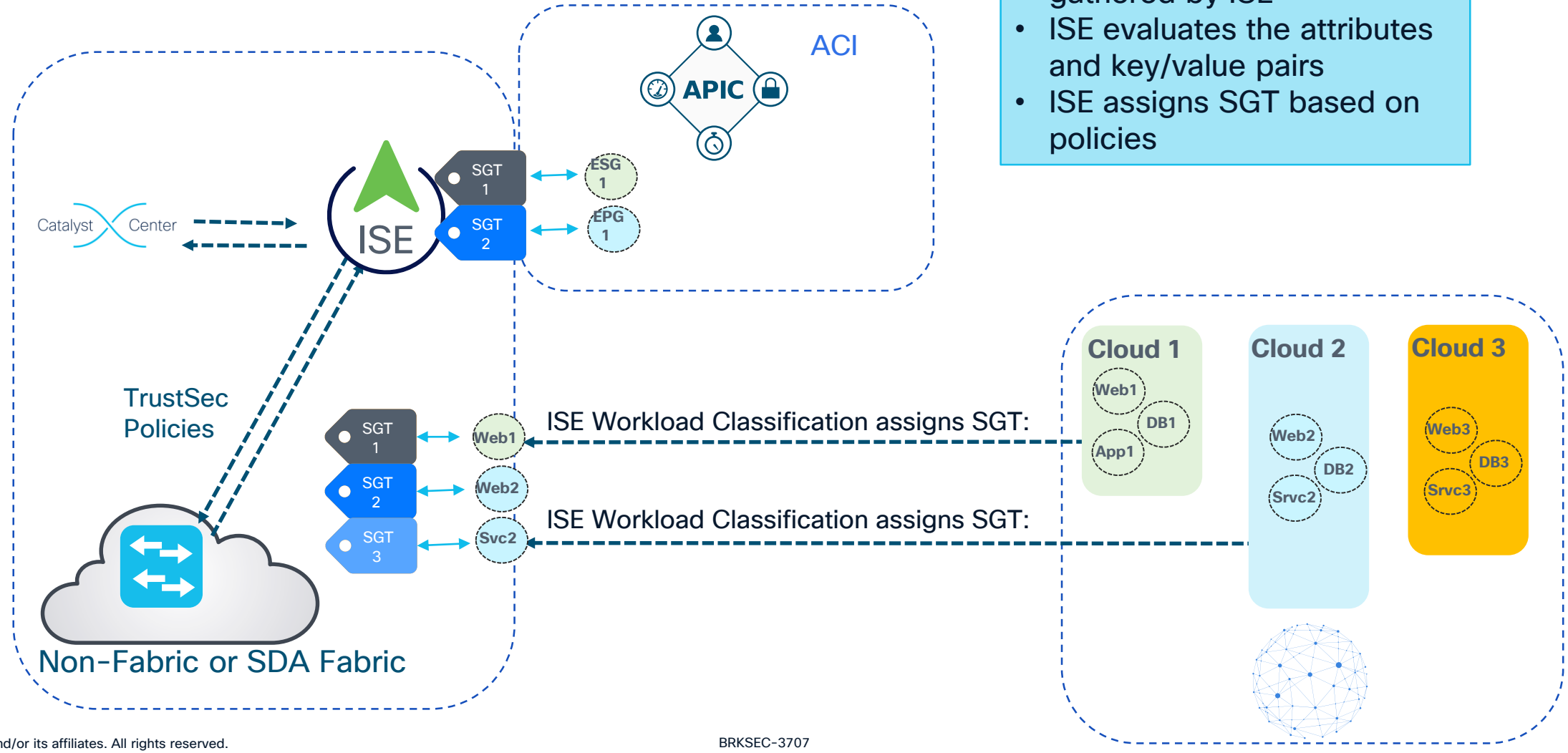


- ISE subscribes to ESGs/EPGs in both ACI fabrics via Inbound SGT Domain Rules
- SGTs sent to SD-WAN Manager for policy configuration
- IP-SGT mappings sent to SD-WAN Controller
- Supports ACI Multi-Site, Multi-Tenant, and Multi-VRF

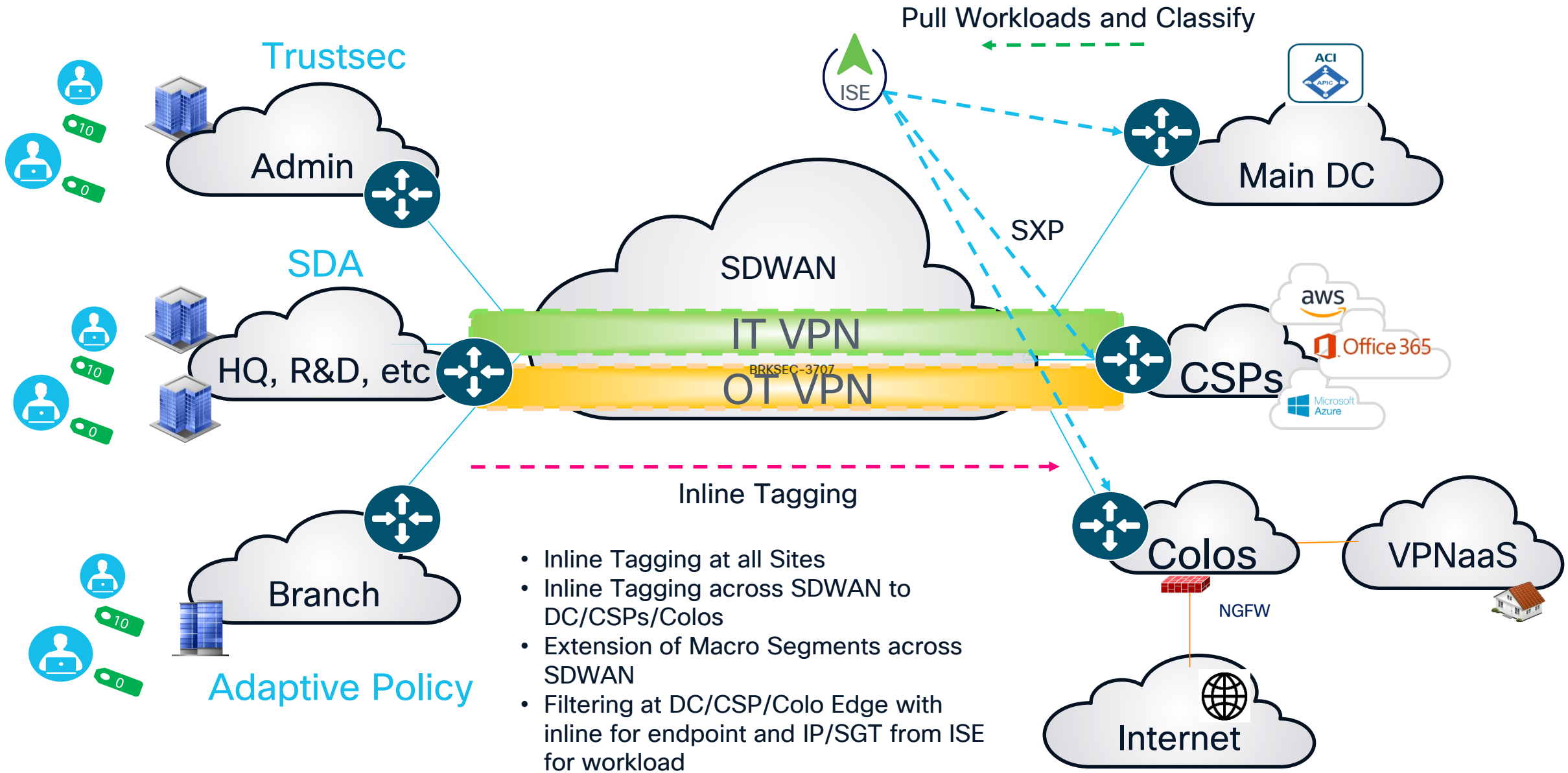
Cloud Connectors

Classification of Hybrid Cloud Workloads

- Cloud Information is gathered by ISE
- ISE evaluates the attributes and key/value pairs
- ISE assigns SGT based on policies



End to End Segmentation



- Inline Tagging at all Sites
- Inline Tagging across SDWAN to DC/CSPs/Colos
- Extension of Macro Segments across SDWAN
- Filtering at DC/CSP/Colo Edge with inline for endpoint and IP/SGT from ISE for workload

Summary

Summary

- SGT is the foundation for the newly announce Cisco Common Policy Framework
- SGT builds upon dynamic classification (802.1X/ACI/etc.), static classification (IP/SGT) and orchestration – REST, Cloud Connectors to classify users and endpoints on enterprise networks
- SGT provides a scalable enterprise network access control model that is deployed in customer networks today
- SGT provides operational savings by decoupling security policy from the network topology
- SGT has broad Cisco and 3rd party software and hardware support
- SGT has easily adopted migration strategies for deployment
- SGT is deployable today in your network

Complete your session evaluations

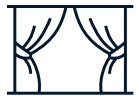
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank You

cisco Live !


CISCO