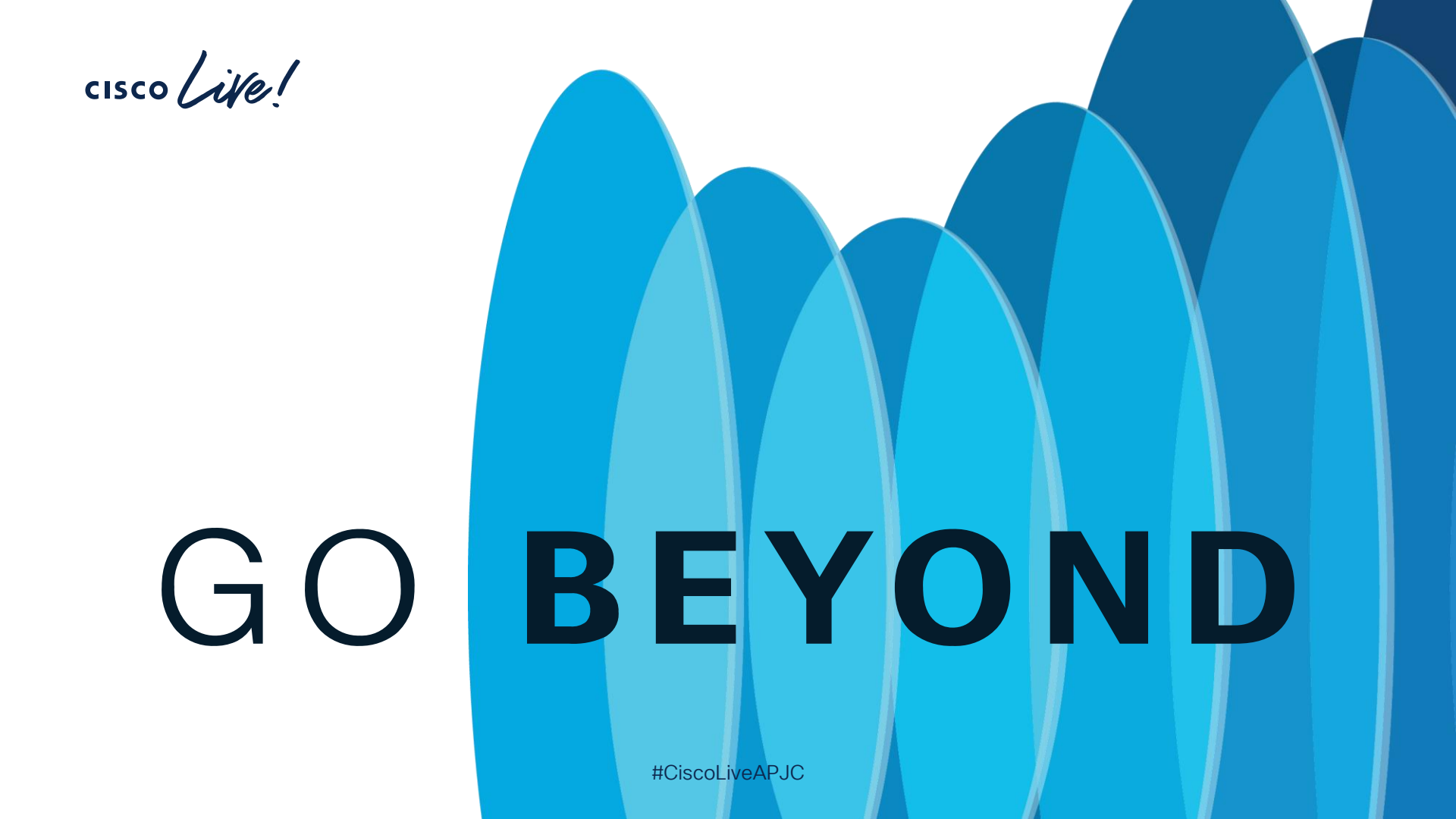

cisco Live!
GO BEYOND
#CiscoLiveAPJC

"Reconciliation"- Dustin Koa Art

TrustSec SGT

Security Innovations for Group-Based Segmentation

Jonothan Eaves, Technical Marketing Engineer

BRKENS-1852

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-1852

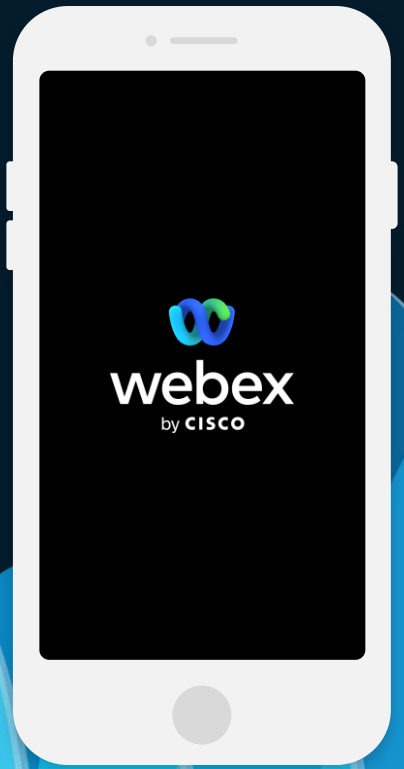
Questions?

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 November 15, 2024.

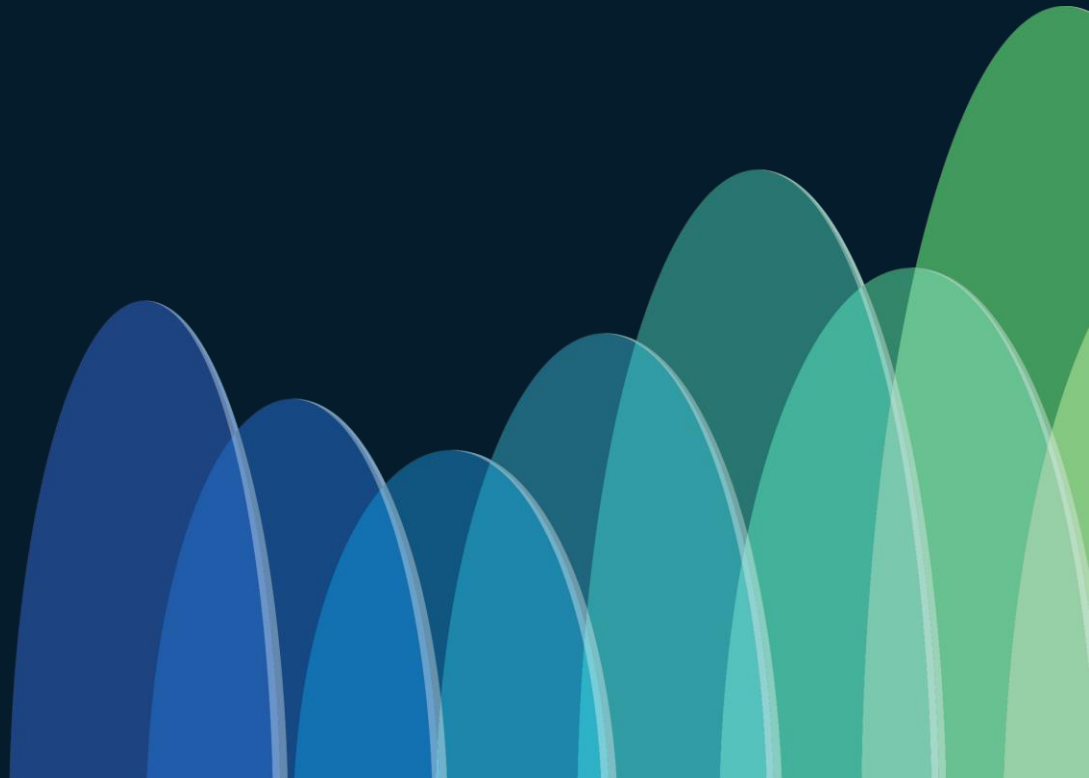


cisco Live!

Agenda

- Introduction
- Classification
- Propagation
- Enforcement
- Common Policy

Introduction



Identifying Uses for Group-Based Policies

Simple ways to add access control & protect new things

Reduce IP ACL complexity.
Reduce and simplify FW rules.
Meet compliance goals easier.
Simple segregation protection.

Reduce Risk & Represent threat state or vulnerable devices

- Use groups to protect device types that you cannot patch
- Restrict lateral movement
- Protect vulnerable systems
- Use Groups to represent suspicious devices & handle appropriately

Reduce SecOps effort in adds, moves & changes

Why it Matters

Southern Water customers hit by cyber attack

SPYWARE/MALWARE

Data from charities stolen in ransomware attack

RANSOMWARE

Spider-Man 2 maker angered by massive hack

North London school closed due to cyber attack

School IT network held to ransom in cyber attack

SUPPLY CHAIN ATTACKS

Weeks of disruption after council 'cyber incident'

DATA/IP THEFT

Cyber attack affecting museum's system one year on

MALVERTISING

Poland investigates cyber-attack on rail network

British Library's hacked customer data on dark web

UNPATCHED SOFTWARE

MAN IN THE MIDDLE

ROGUE SOFTWARE

Health board fears hackers have stolen patient data

DRIVE BY DOWNLOADS

Council facing 10,000 cyber attacks a day

Cyber-attack on electoral registers revealed

'Worrying precedent' as hackers target water firm

BOTNETS

DDOS

Scottish university targeted by cyber attackers

WIPER ATTACKS

Cyber attack continues to hit NHS trust's services

CREDENTIAL COMPROMISE

NHS IT supplier held to ransom by hackers

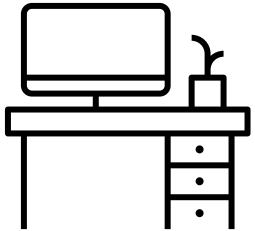
ADVANCED PERSISTENT THREATS

Australia phones cyber-attack exposes personal data

PHISHING

Nato investigates hacker sale of missile firm data

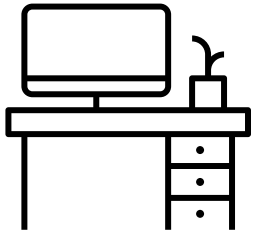
Policy Challenge

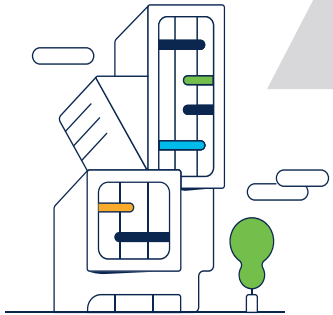


VLAN 100
Subnet A.B.C.D
⬇
IPACL 1
IPACL 2 ....

VLAN 103
Subnet M.N.O.P
⬇
IPACL 31
IPACL 32 ....

Security Policy Tied to Infra





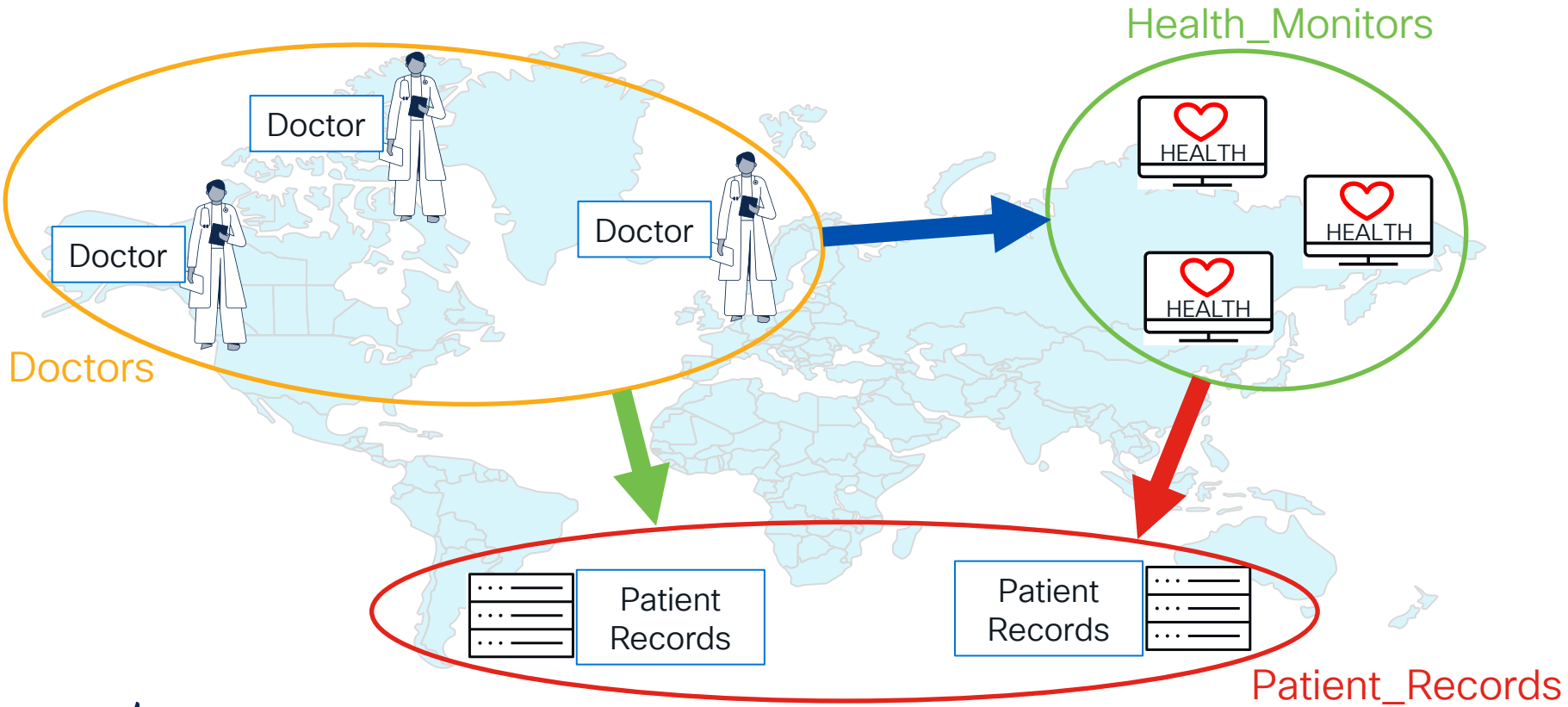
VLAN 101
Subnet E.F.G.H
⬇
IPACL 11
IPACL 12 ....

VLAN 102
Subnet I.J.K.L
⬇
IPACL 21
IPACL 22 ....

Can you see the Business Intent Here?

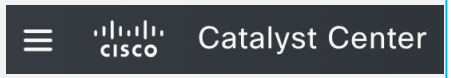
```
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 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
access-list 102 deny ip 124.236.172.134 255.255.255.255 gt 859 56.81.14.184 255.55.255.255 gt 2754
```

Simplifying Security Policy



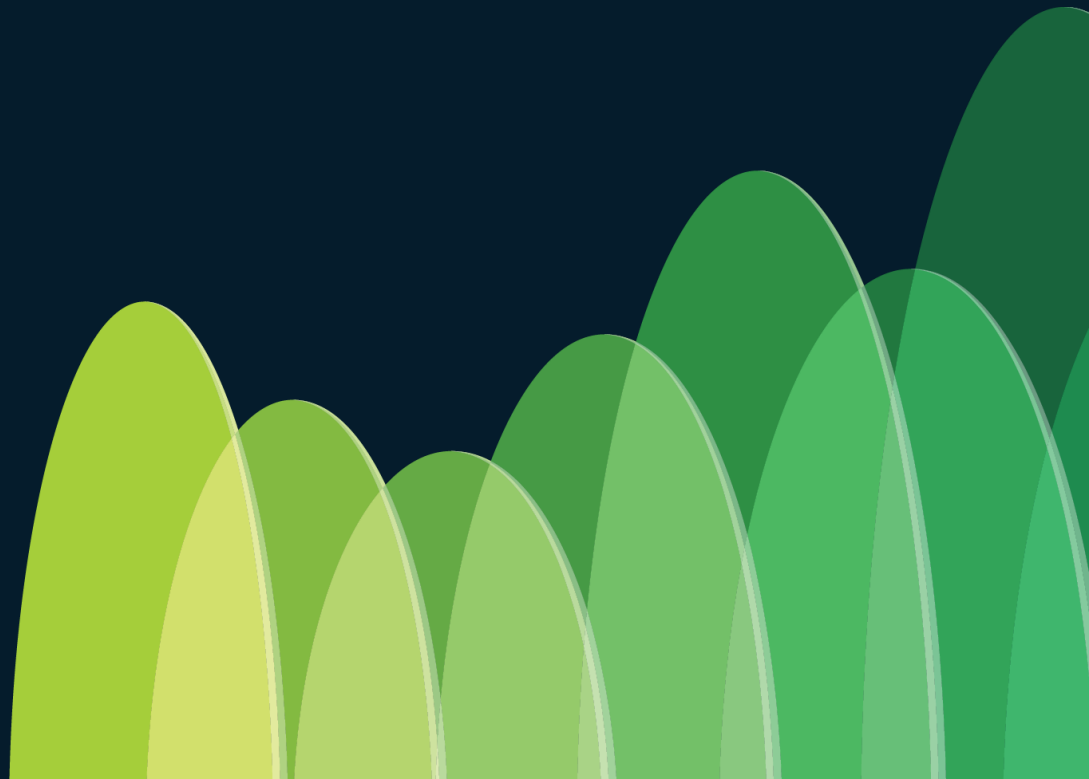
Business Intent is Clear

With meaningful group-based policies aligned to business needs



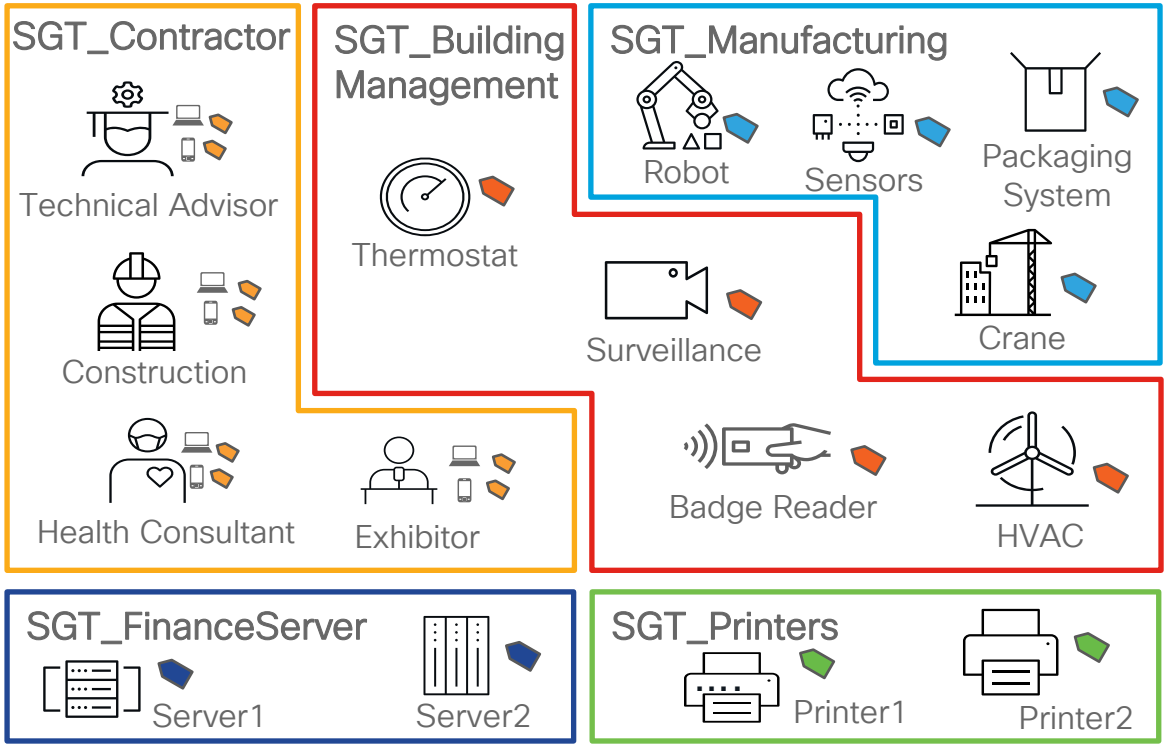

```
Edge-Cat9300#show cts role-based permissions
IPv4 Role-based permissions default:
        Deny IP-00
IPv4 Role-based permissions from group 36:Scanners to group 27:Storage:
        Permit_IP_Log
IPv4 Role-based permissions from group 4:Employees to group 12:Directory_Systems:
        Permit_LDAP_HTTP
```

Classification



Classification into Intent-Based Groups

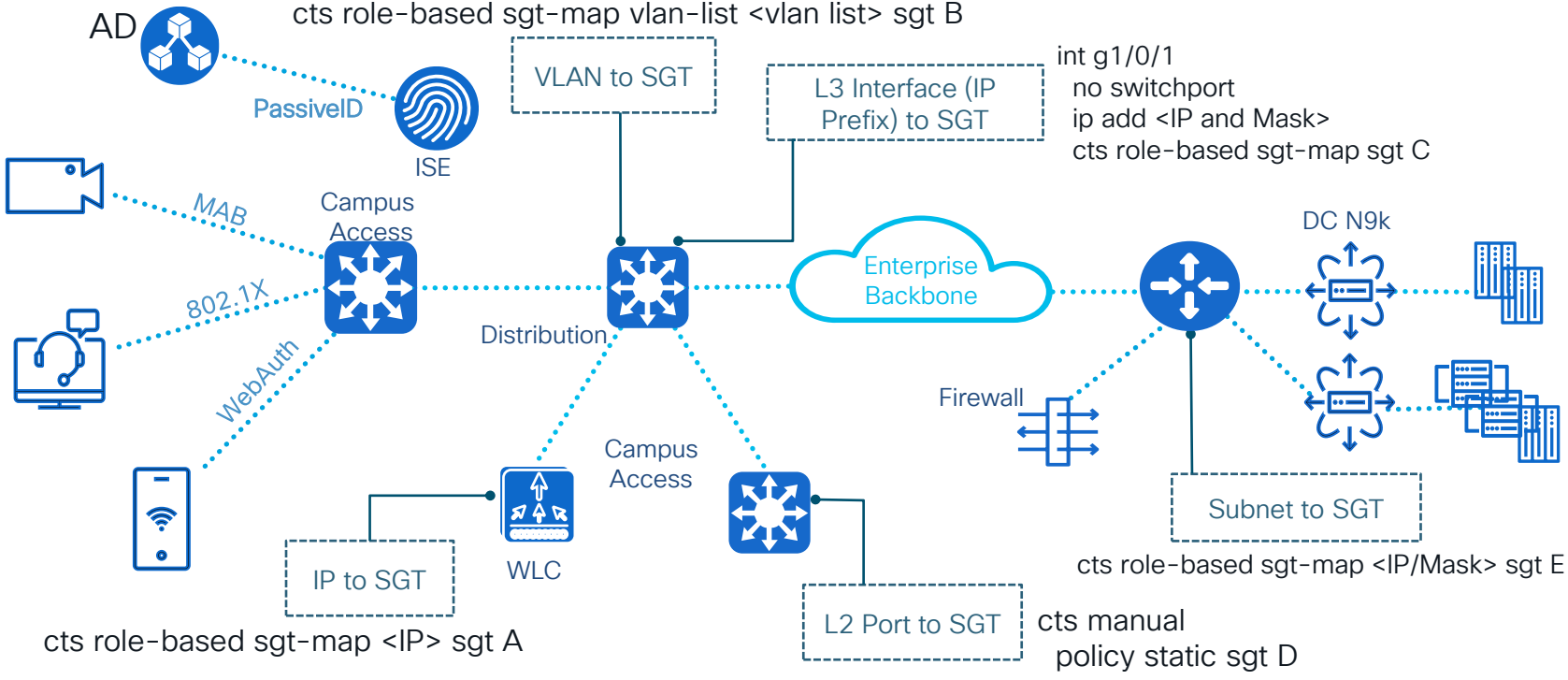
- Business-based groupings to provide consistent policy and access independent of network topology
- Leverage items such as location, device type, RADIUS attributes, AD membership etc. to allocate group assignments



Classification Mechanisms

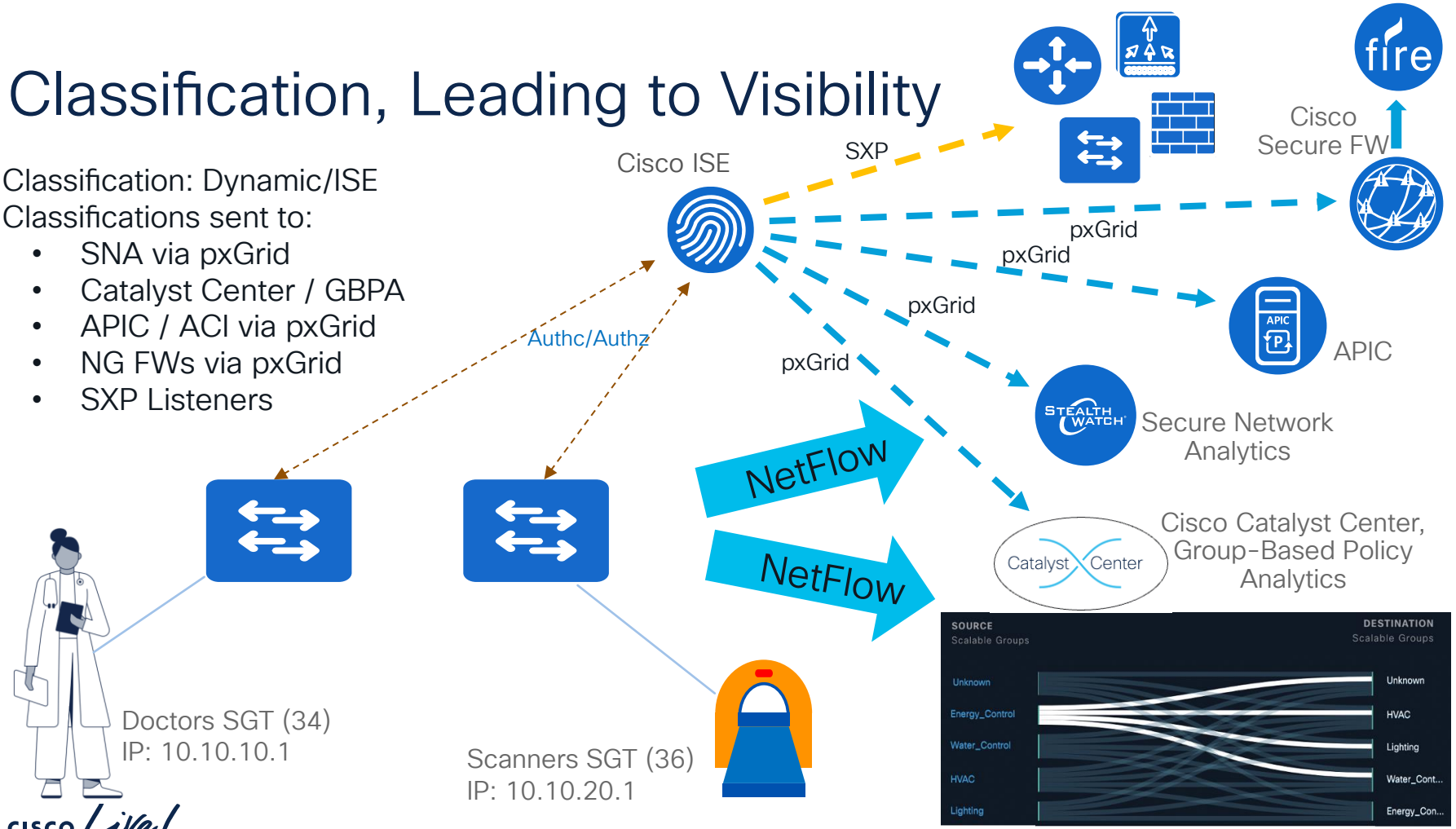
Dynamic Classification

Static Classification

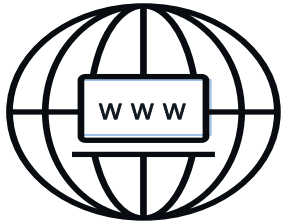


Classification, Leading to Visibility

- Classification: Dynamic/ISE
- Classifications sent to:
  - SNA via pxGrid
  - Catalyst Center / GBPA
  - APIC / ACI via pxGrid
  - NG FWs via pxGrid
  - SXP Listeners



Default Route SGT



There must be a default route (dynamic or static)

Cat9000

Classification Inbound

Enforcement Outbound

```
device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
IP Address          SGT         Source
==============================
0.0.0.0/0           123         CLI

Active IPv6-SGT Bindings Information
IP Address          SGT         Source
==============================
::/0                123         CLI
```

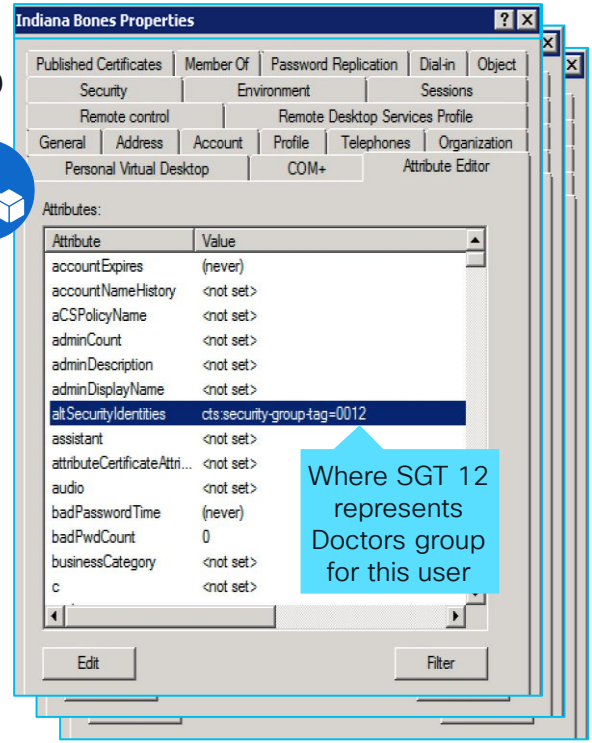
```
cts role-based sgt-map vrf x 0.0.0.0/0 sgt 123
```

```
cts role-based sgt-map vrf x  0:0::/0 sgt 123
```

SGT Assigned from AD

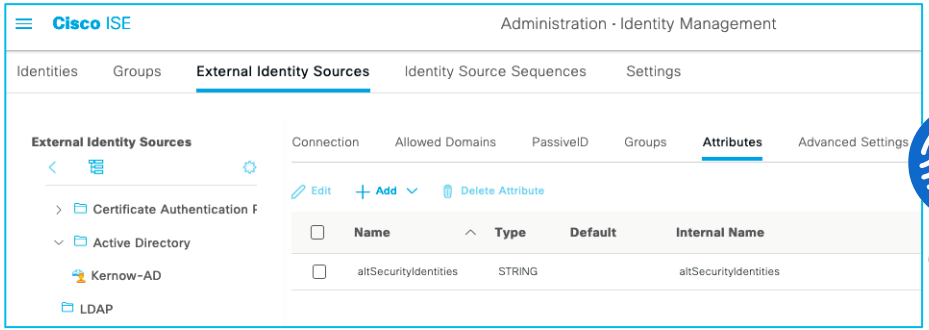
Reduces Authz Rules Required

Add or reuse attribute in AD for SGT



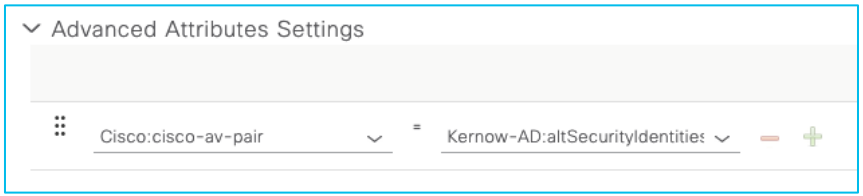
Where SGT 12 represents Doctors group for this user

Retrieve into ISE to use in the authorisation process:



Authc

Configure ISE Authz Profile:



Authz:

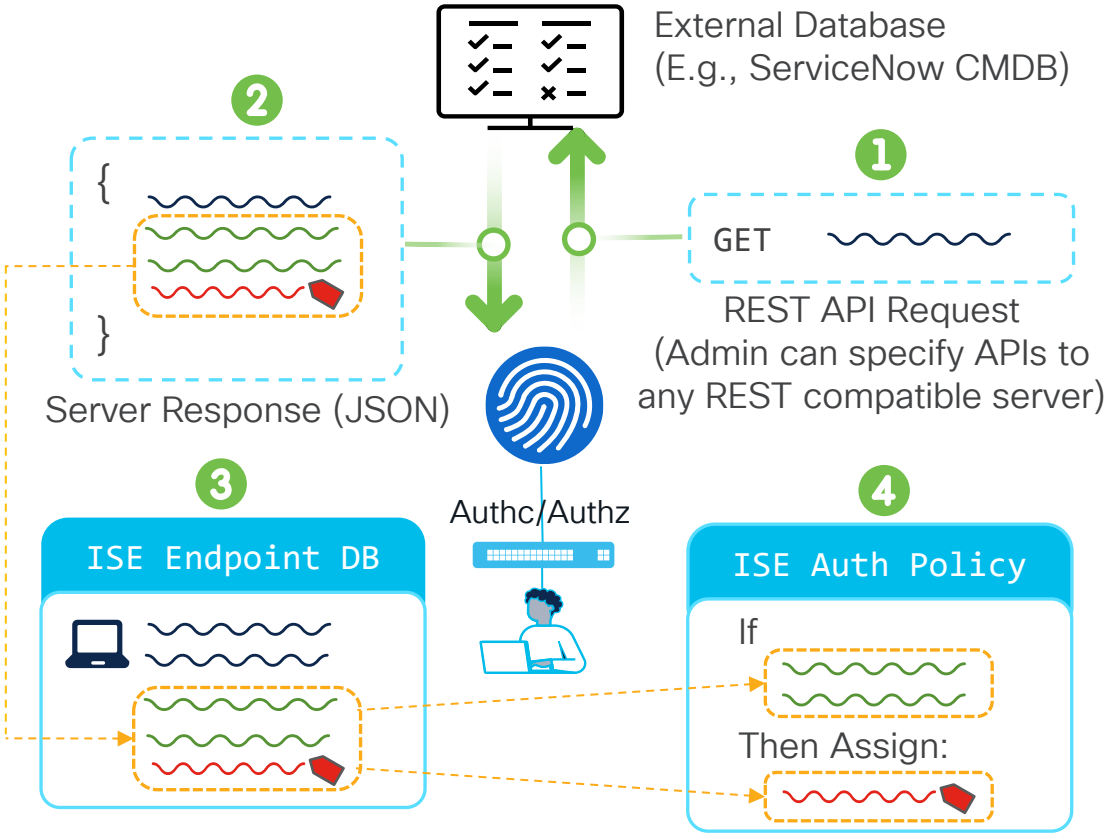
cisco-av-pair=“cts:security-group-tag=0012”

Dr. Indiana Bones

Classified into Doctors / SGT 12 Group

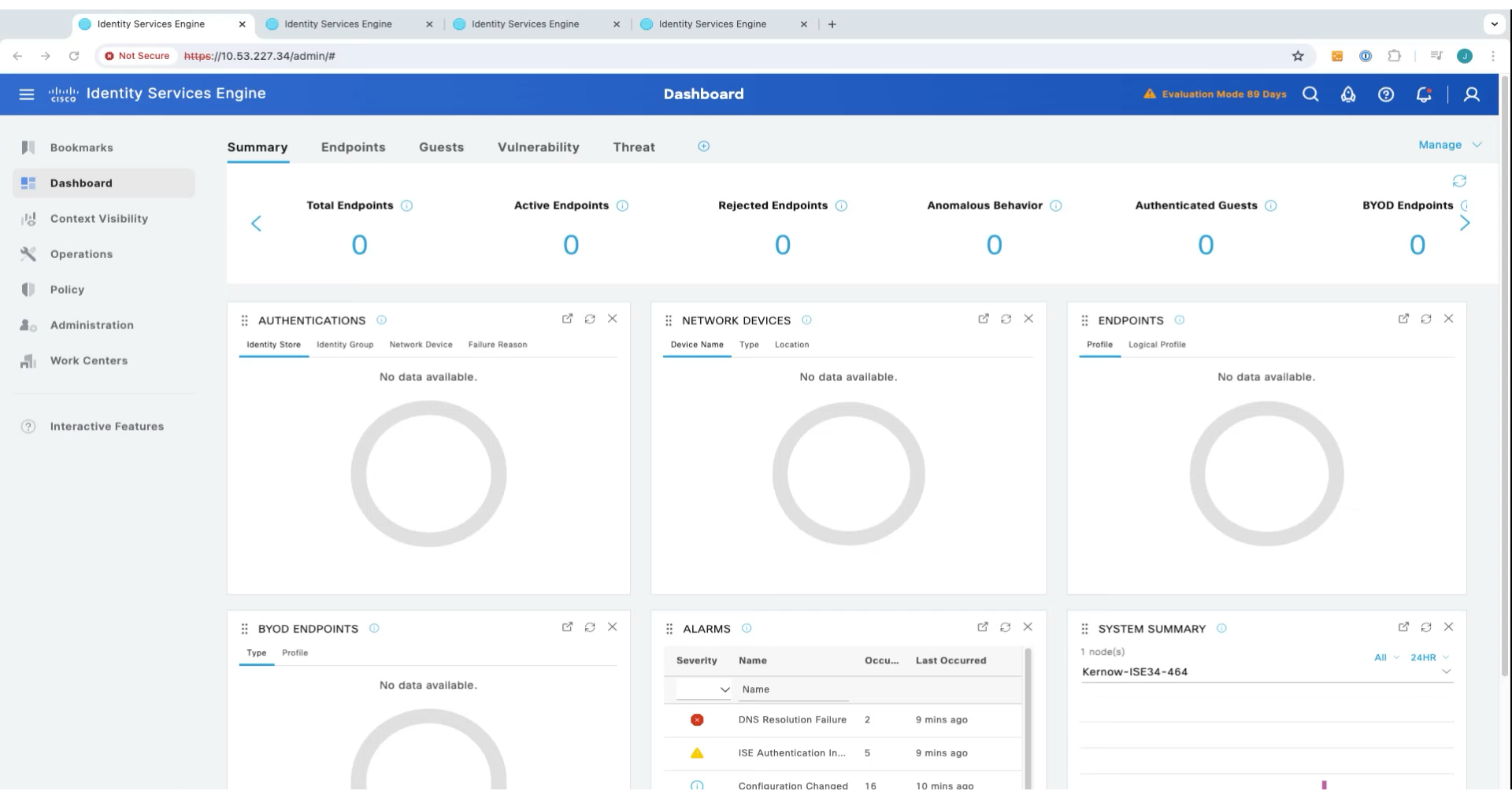
SGT Classification from pxGrid Direct Attributes

{"result":[{
"owned_by":"jeaves",
"operational_status":"Operational",
"sys_updated_on":"2022-04-22 16:44:52",
"sys_created_by":"jeaves",
"warranty_expiration":"",
"cpu_speed":"",
"checked_out":"",
"maintenance_schedule":"",
"group_tag":"cts:security-group-tag=12-00",
"managed_by":"jeaves",
"sys_class_name":"Computer",
"assigned_to":"jeaves@example.org",
"install_date":"",
"asset_tag":"",
"subcategory":"Computer",
"sys_id":"0009ef70dbcf01101f3961997",
"mac_address":"00:50:56:A0:F7:3A",
"company":"Cisco",
"department":"Marketing",
"ip_address":"10.6.5.129",
...

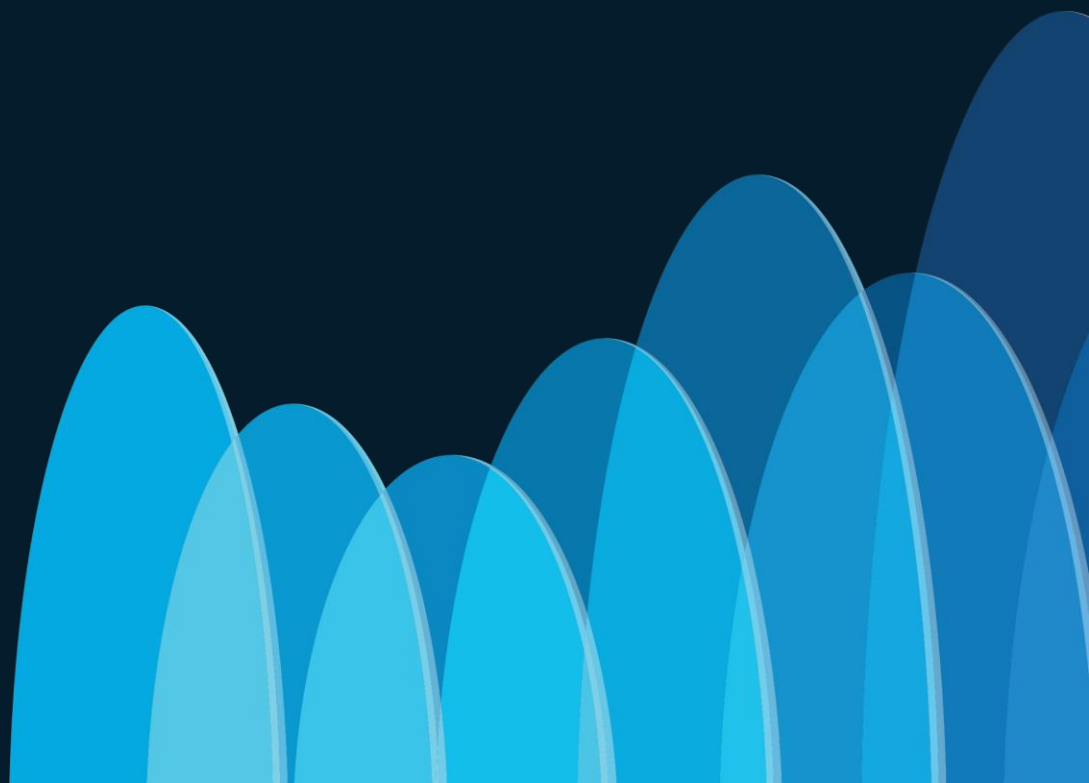


Demo:

pxGrid Direct



Propagation

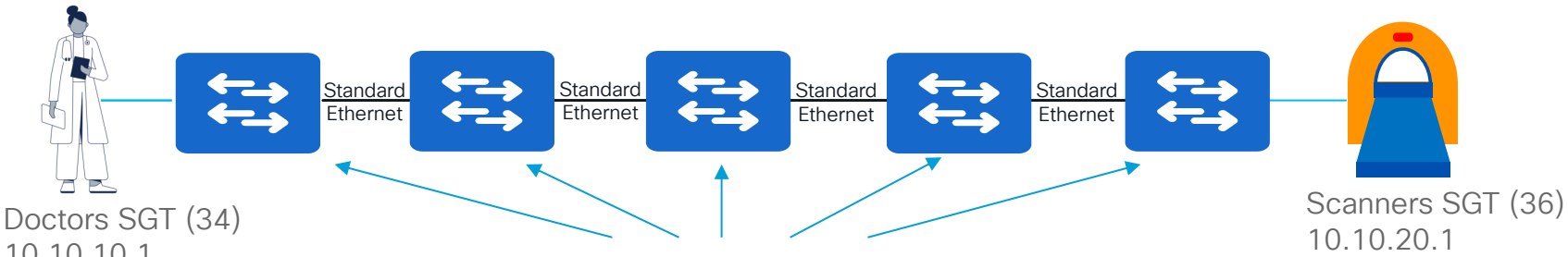


Where does enforcement occur?

Enforcement occurs at the first platform in the traffic path which has all the following:

- Source IP:SGT binding
- Destination IP:SGT binding
- Platform and VLAN has enforcement enabled
- A policy is downloaded from ISE (either default or specific)

NO ENFORCEMENT

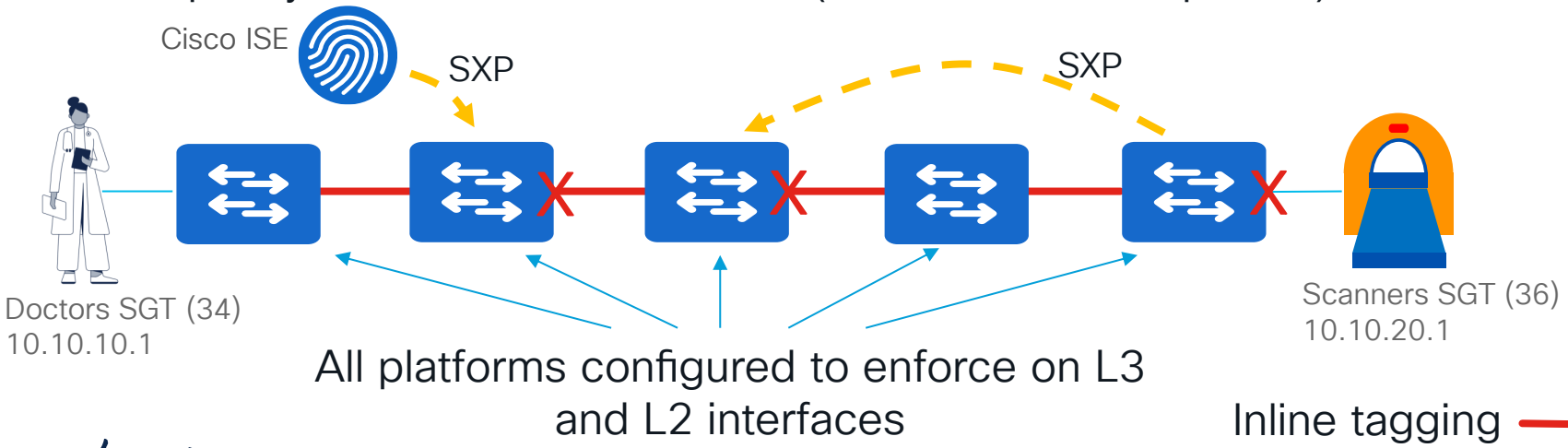


All platforms configured to enforce on L3 and L2 interfaces

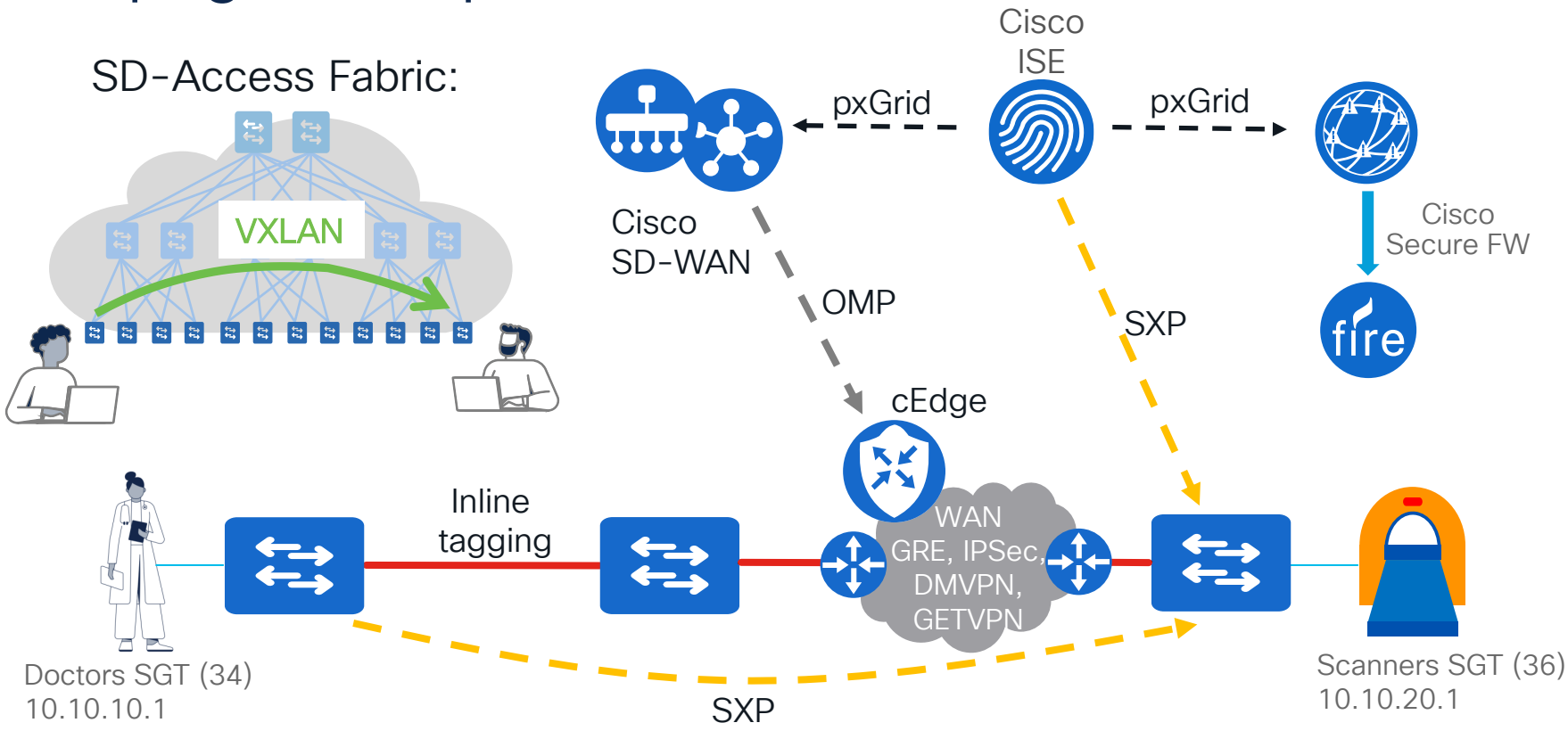
This is where Propagation comes in

Enforcement occurs at the first platform in the traffic path which has all the following:

- Source binding
- Destination binding
- Platform and VLAN has enforcement enabled
- A policy is downloaded from ISE (either default or specific)

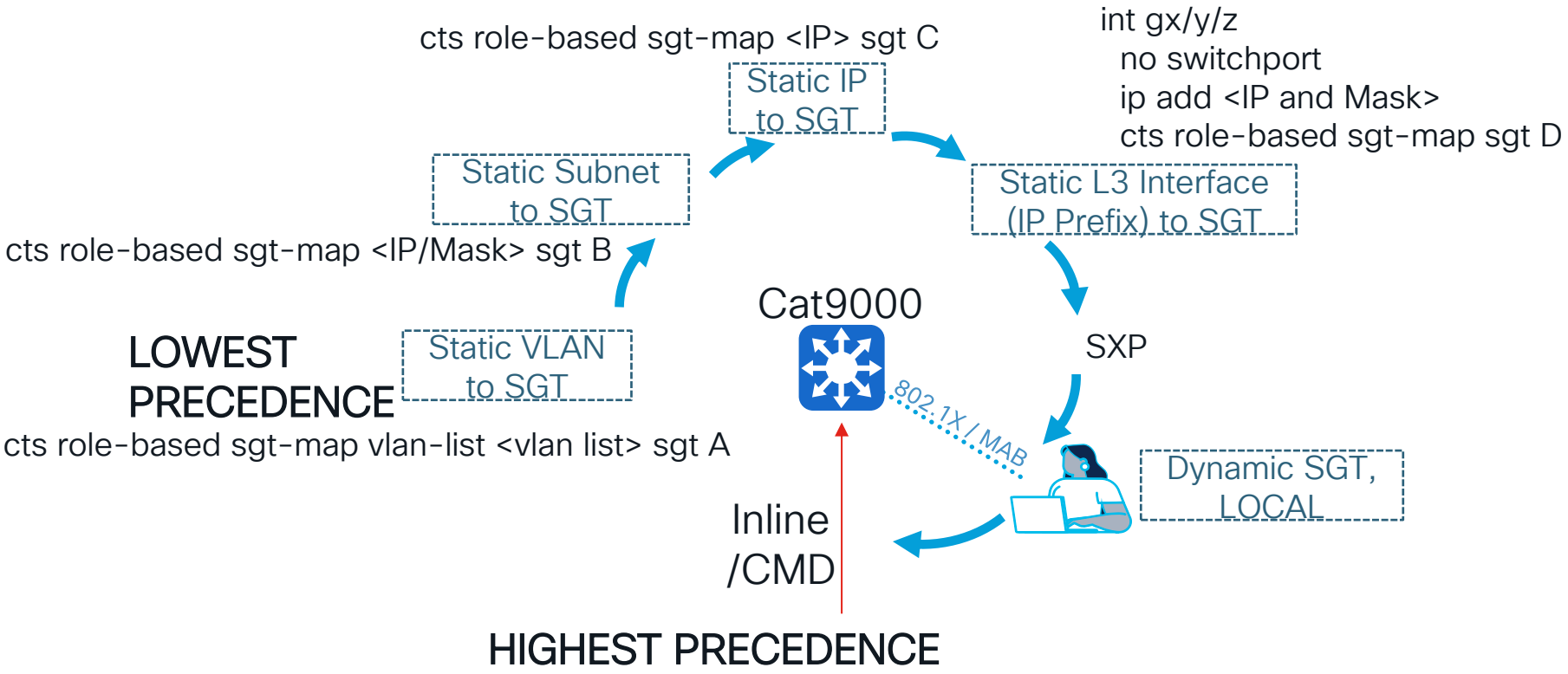


Propagation Options



Order of Precedence

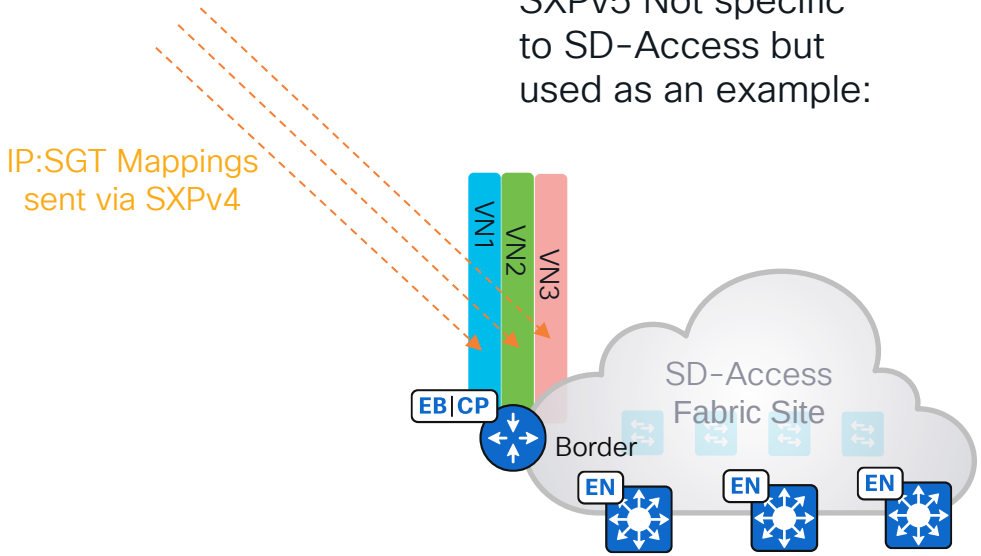
For Reference



SXPv5 Introduction and Issue Being Resolved

SXP Version 1	Initial SXP version supporting IPv4 binding propagation.
SXP Version 2	Includes support for IPv6 binding propagation and version negotiation.
SXP Version 3	Adds support for Subnet-SGT binding propagation. If speaking to a lower version, then the subnet will be expanded to individual IP-SGT entries.
SXP Version 4	Loop detection and prevention, capability exchange and built-in keep-alive mechanism.

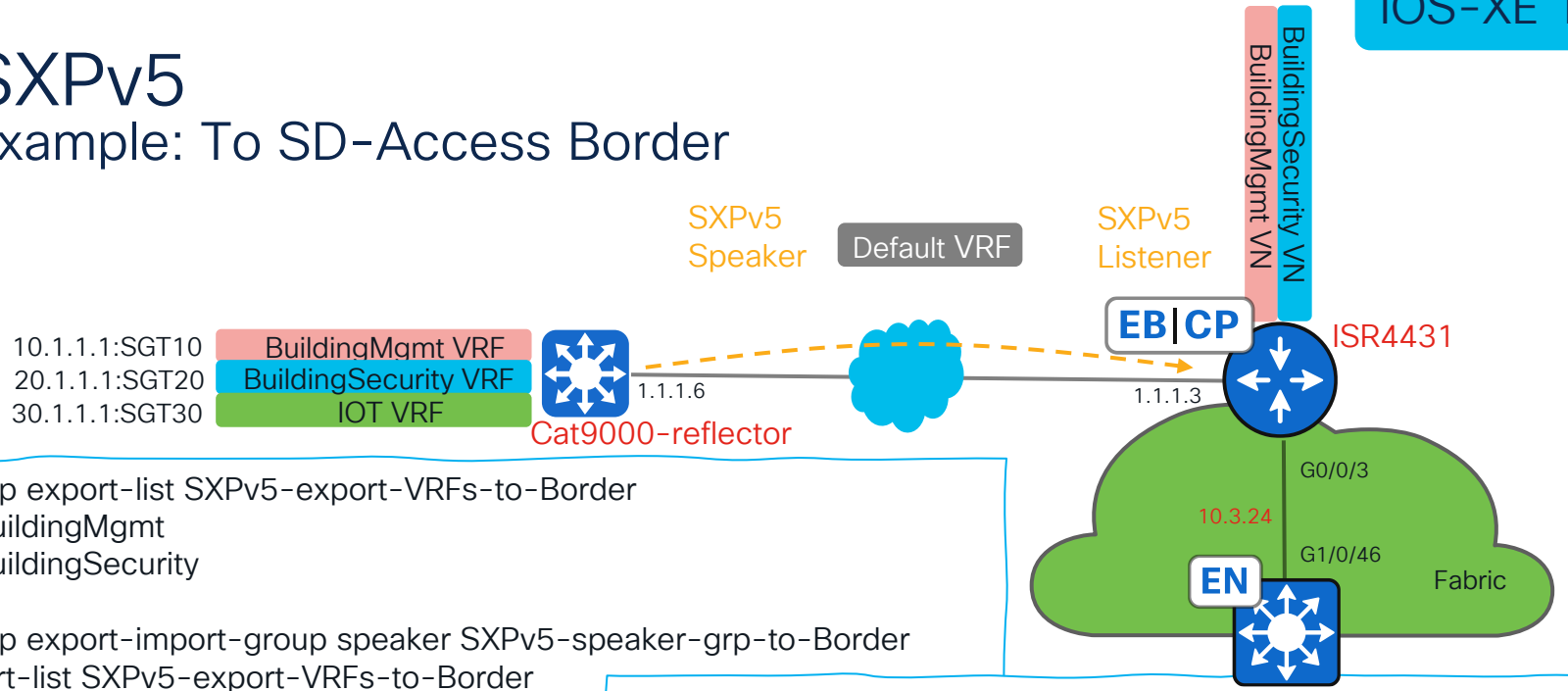
SXPv5 Not specific to SD-Access but used as an example:



Latest SXP version before 17.9.1 is SXPv4 (not VRF aware)

SXPv5
Example: To SD-Access Border

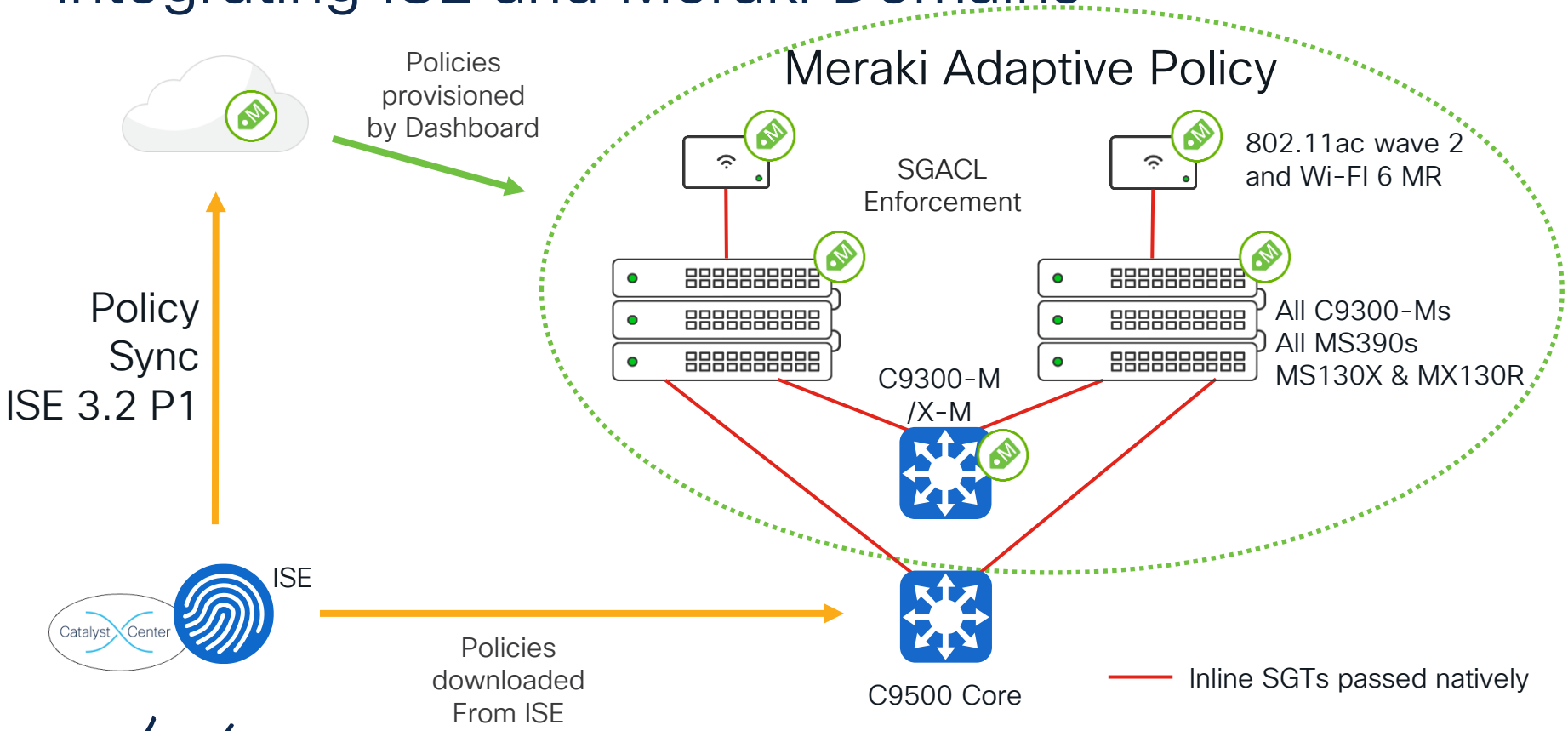
IOS-XE 17.9.1



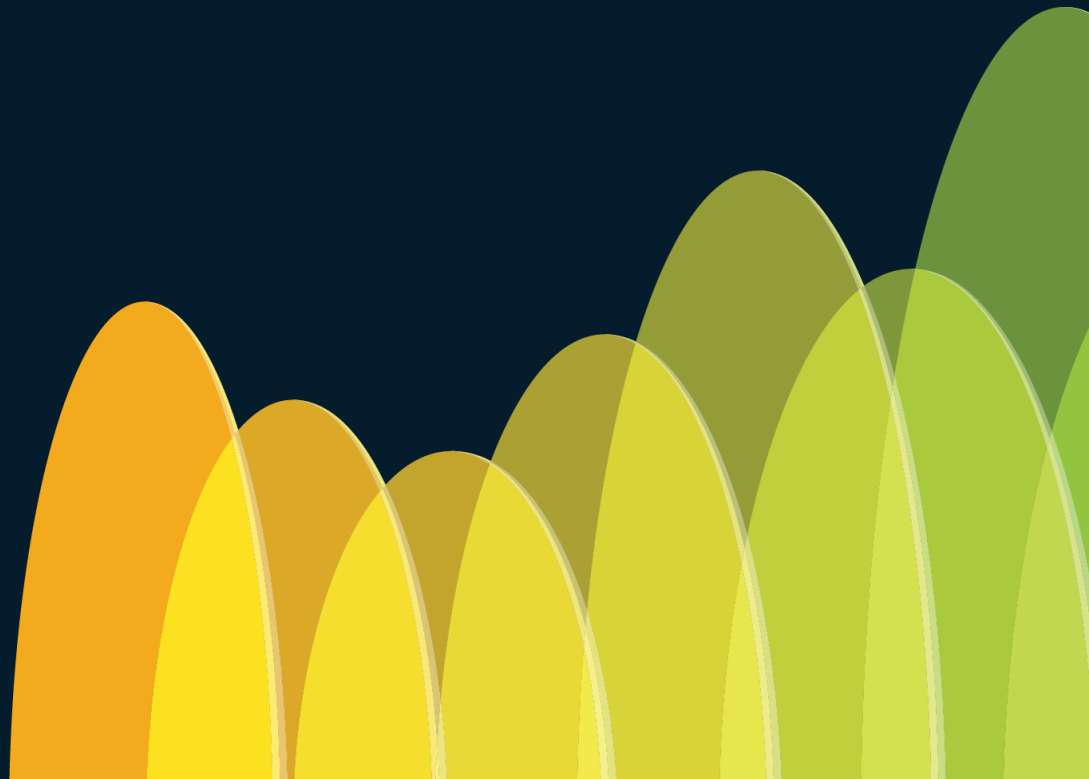

```
cts sxp export-list SXPv5-export-VRFs-to-Border
 vrf BuildingMgmt
 vrf BuildingSecurity
!
cts sxp export-import-group speaker SXPv5-speaker-grp-to-Border
 export-list SXPv5-export-VRFs-to-Border
 peer 1.1.1.3
```

```
cts sxp import-list SXPv5-import-from-Reflector
 vrf
!
cts sxp export-import-group listener SXPv5-import-grp-from-Reflector
 import-list SXPv5-import-from-Reflector
 peer 1.1.1.6
```

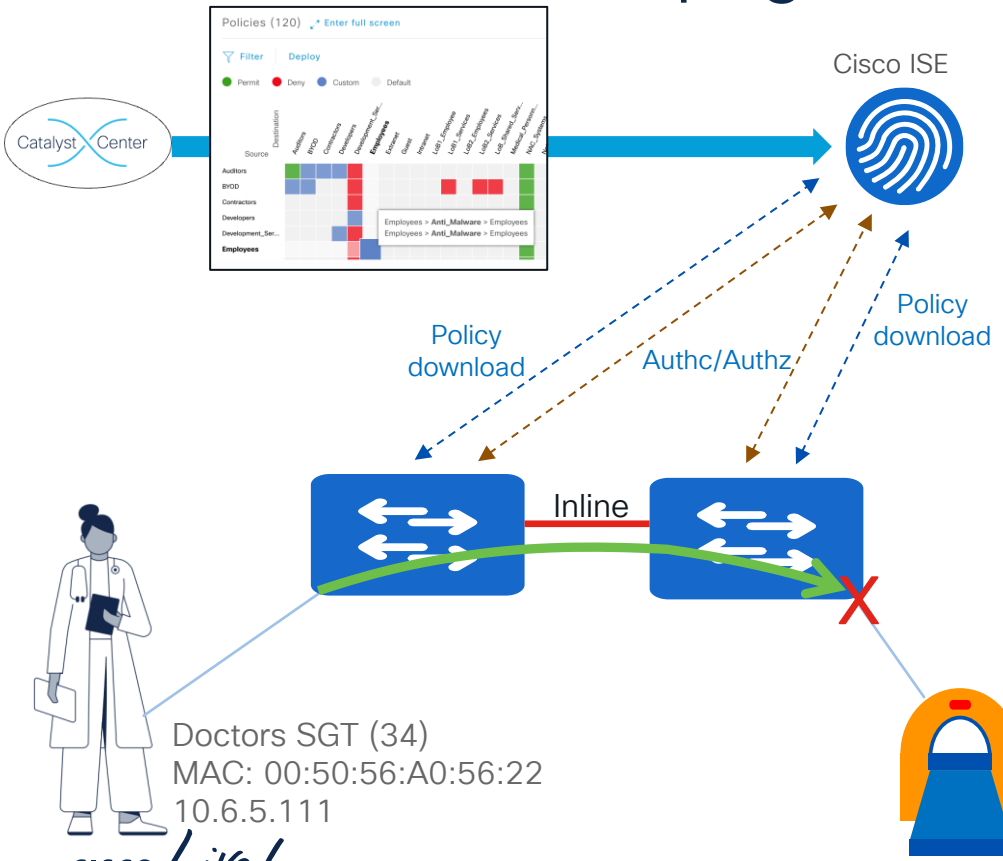
Integrating ISE and Meraki Domains



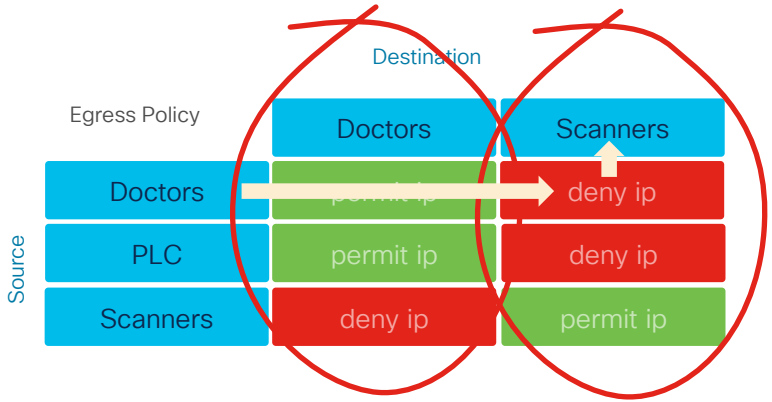
Enforcement



Classification, Propagation and Enforcement

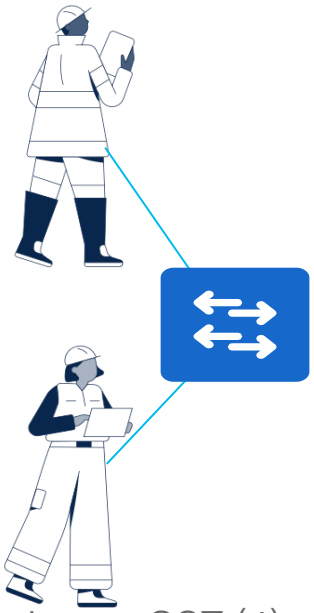


- Classification: Dynamic/ISE
- Propagation (Source SGT)
- Enforcement: At Egress

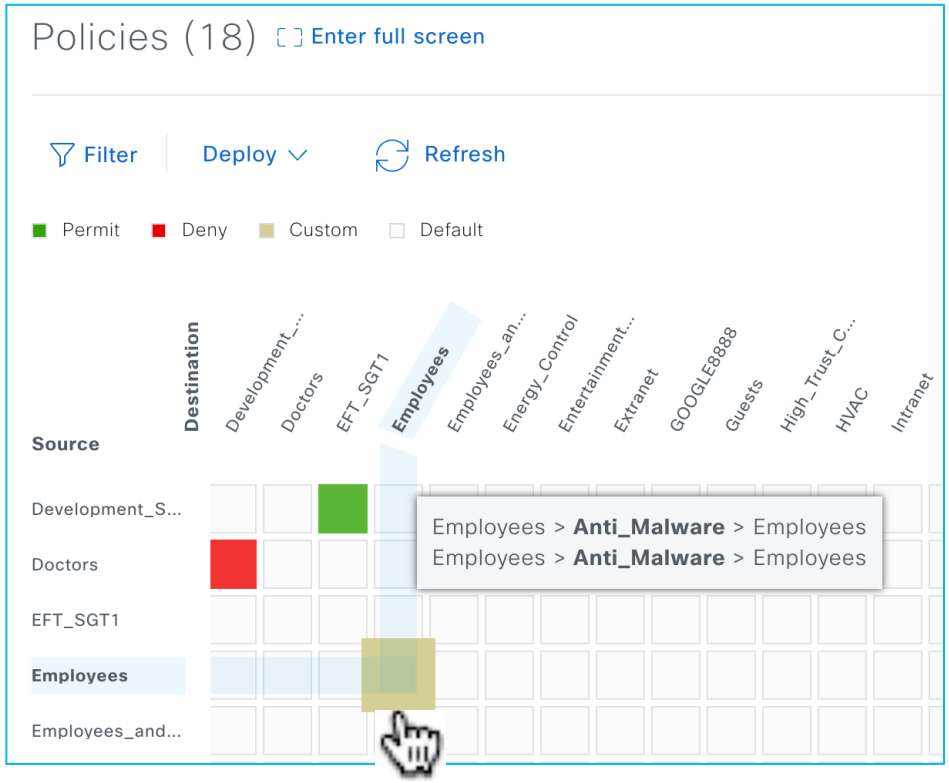


Limit Lateral Movement; Reduce Malware Propagation

Employees SGT (4)
10.20.30.5



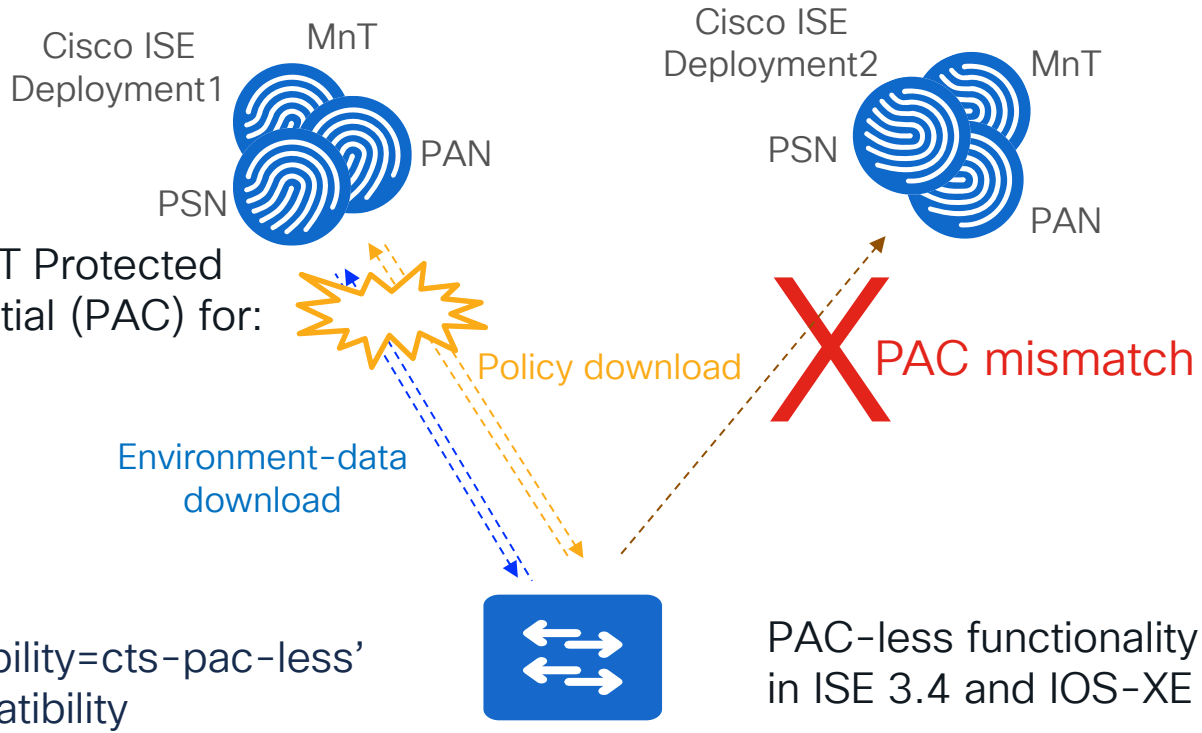
Employees SGT (4)
10.20.30.9



Anti_Malware SGACL:

deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
deny tcp src dst eq 443
deny tcp src dst eq 22
deny tcp src dst eq pop3
deny tcp src dst eq 123
etc

PAC-less Communication



Uses 'cts-pac-capability=cts-pac-less' for backwards compatibility

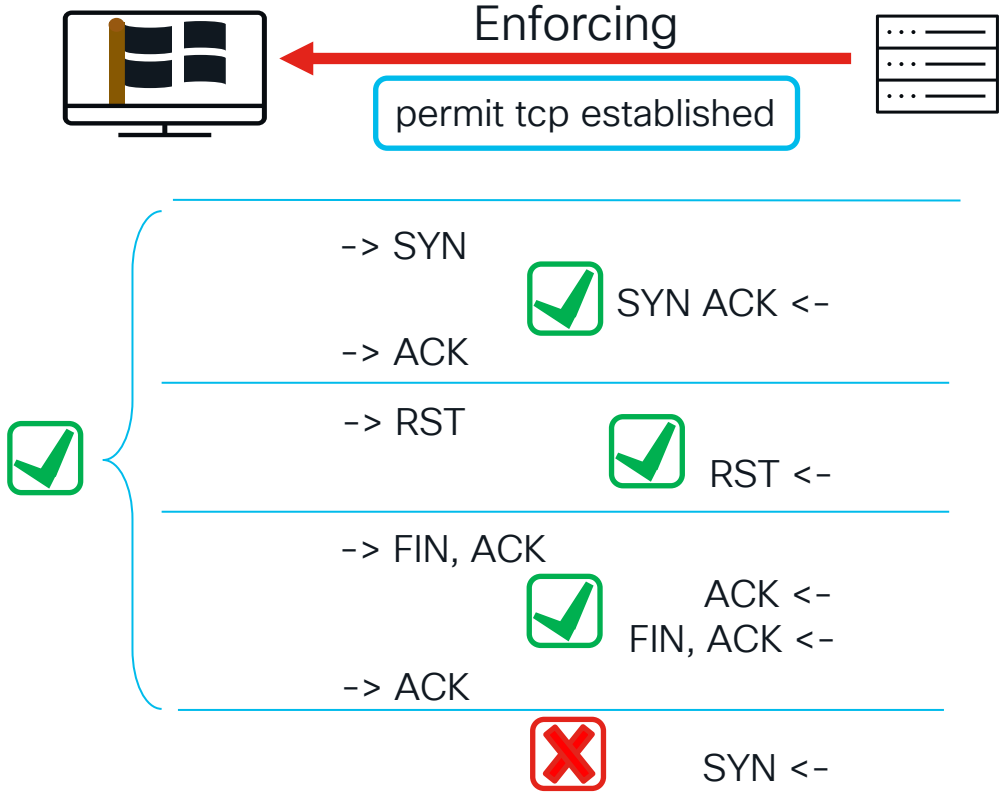
PAC-less functionality added in ISE 3.4 and IOS-XE 17.15.1

SGACL is Stateless, isn't it?

Yes, it is, but you can use the **Established** keyword:

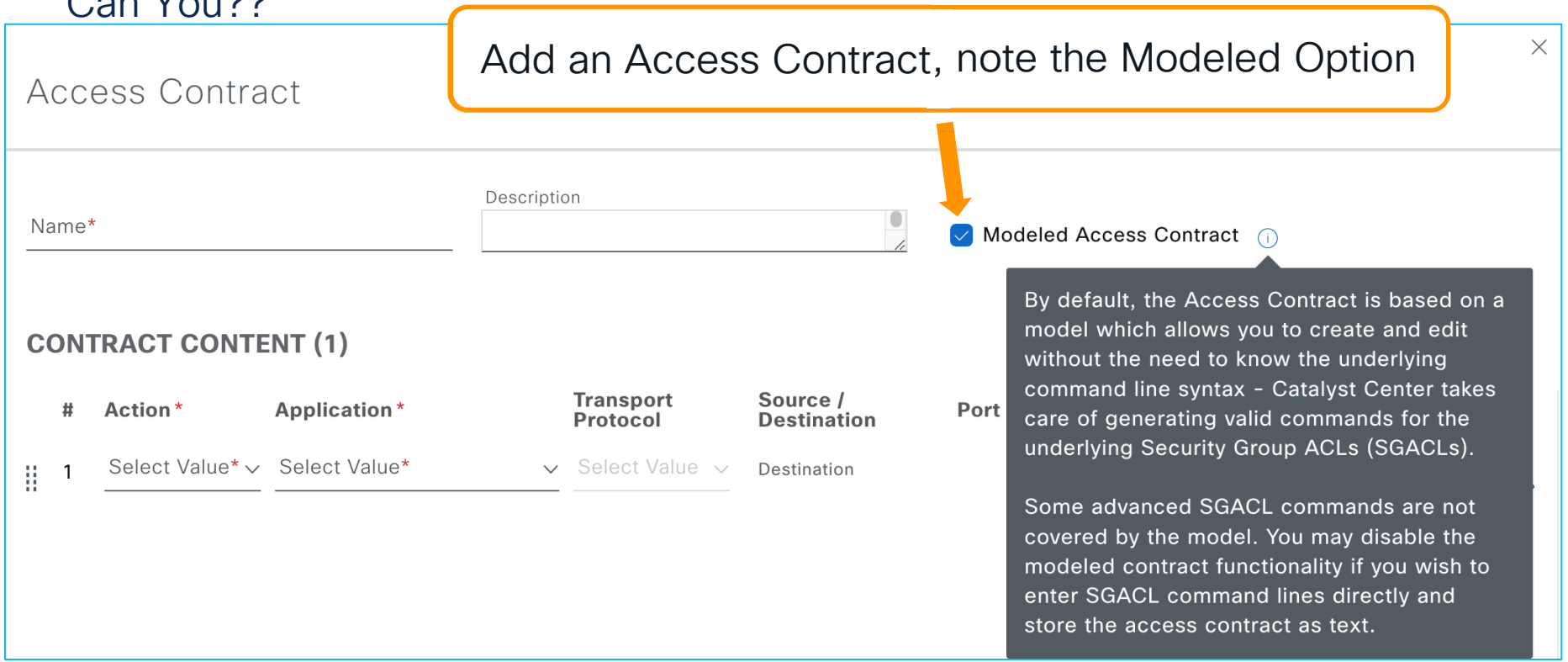
permit tcp established

This monitors TCP flags. Act on packets with ACK or RST (communication that has been established)

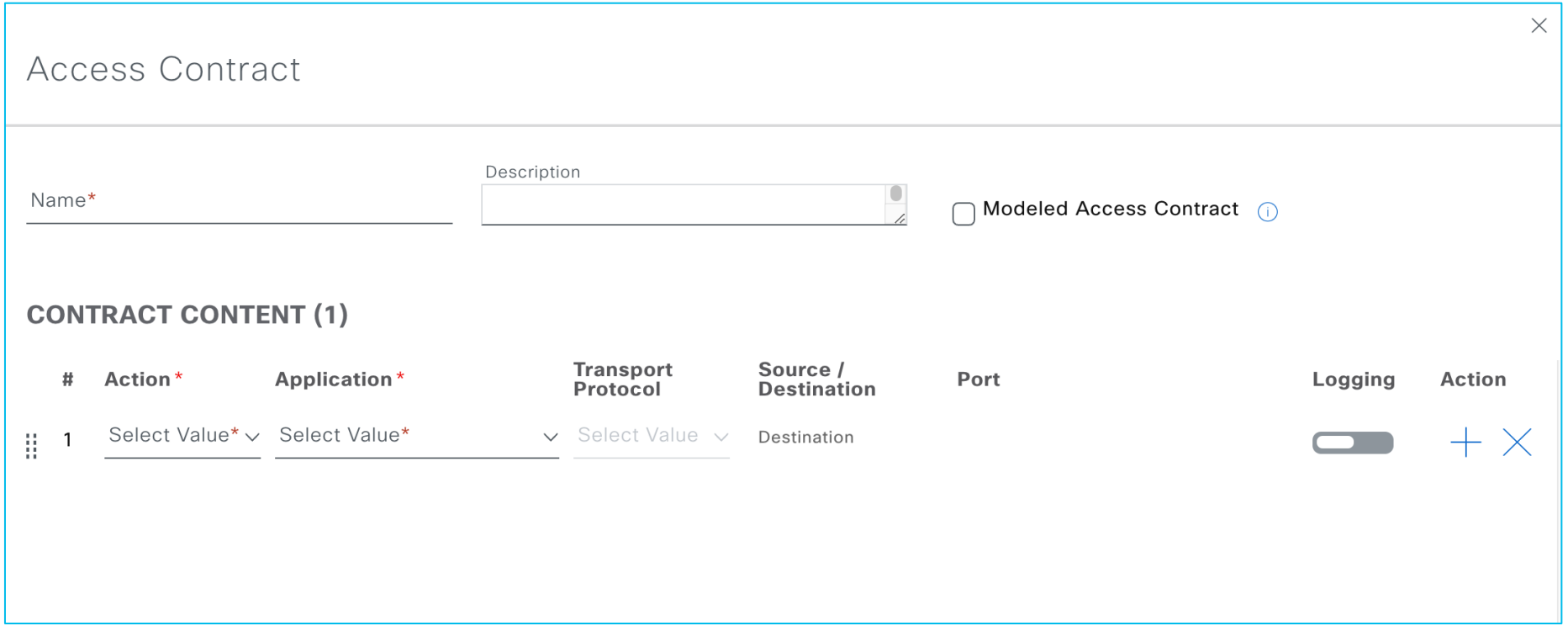


If using TCP Flags, cannot use Catalyst Center

Can You??

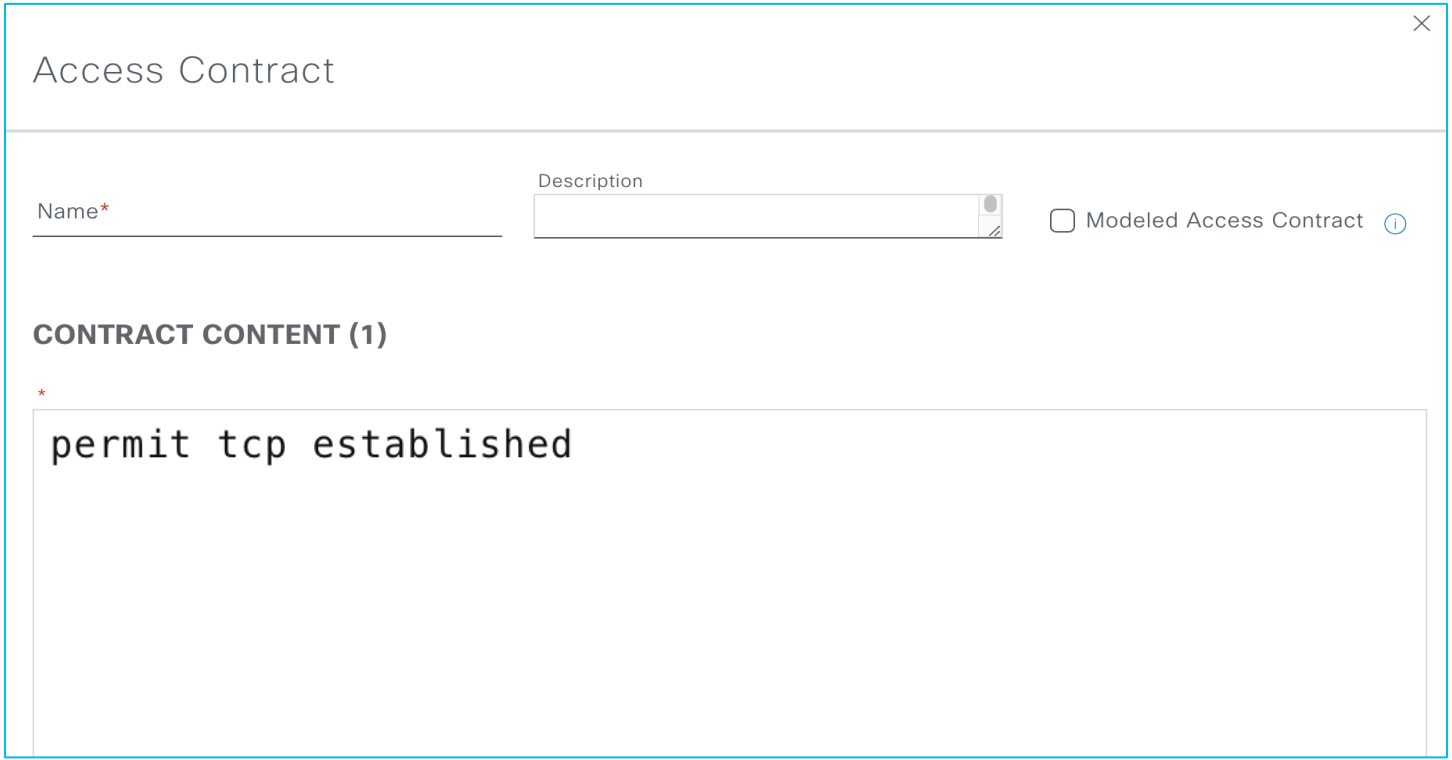


If using TCP Flags, cannot use Catalyst Center
Can You??



Non-Modeled Contract

Enter Text as you would in ISE

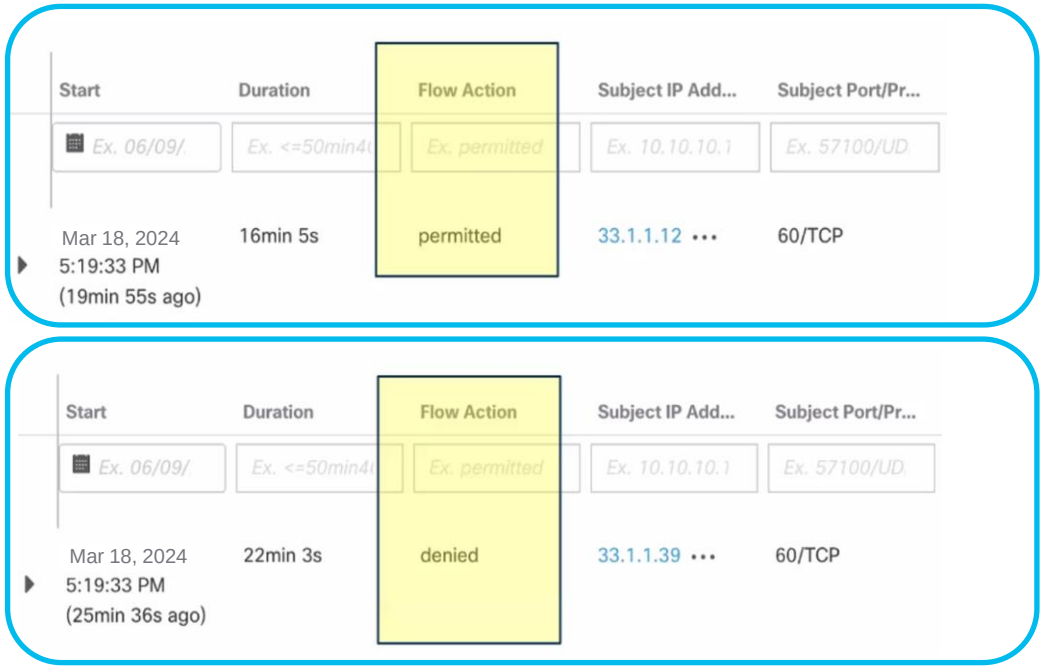


SGACL Enforcement Monitoring via NetFlow

IOS-XE 17.13 release supports export of firewallEvent (233) on Doppler ASIC platforms (92/93/94/95/9600).
SNA v7.4.2 has support for this field.

```
Flow record <record_name>
  match ipv4 version
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect policy firewall event
!
Interface G1/0/1
  ipv6 flow monitor <monitor_name> output
```

firewallEvent (233) received by SNA:



show flow monitor <monitor name> cache:
fw event: 1 (PERMIT) / 3 (DENY)

Common Policy

Need for Common Policy

Separate Policy Domains

Meraki

Security

SASE/SSE

Cisco Secure Access

Microsoft 365

aws

Google Cloud

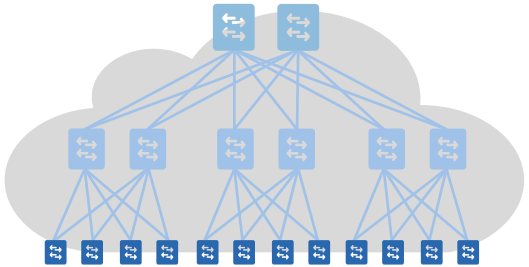
Azure

vmware by Broadcom

Cloud

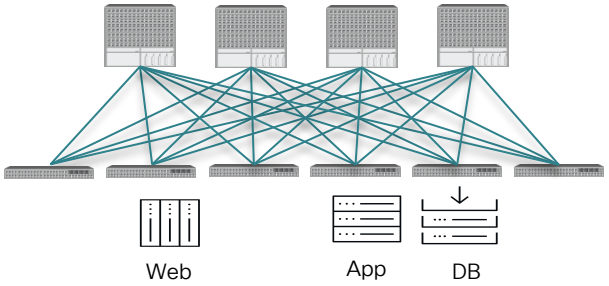
Catalyst Center

SD-Access



Non-Fabric

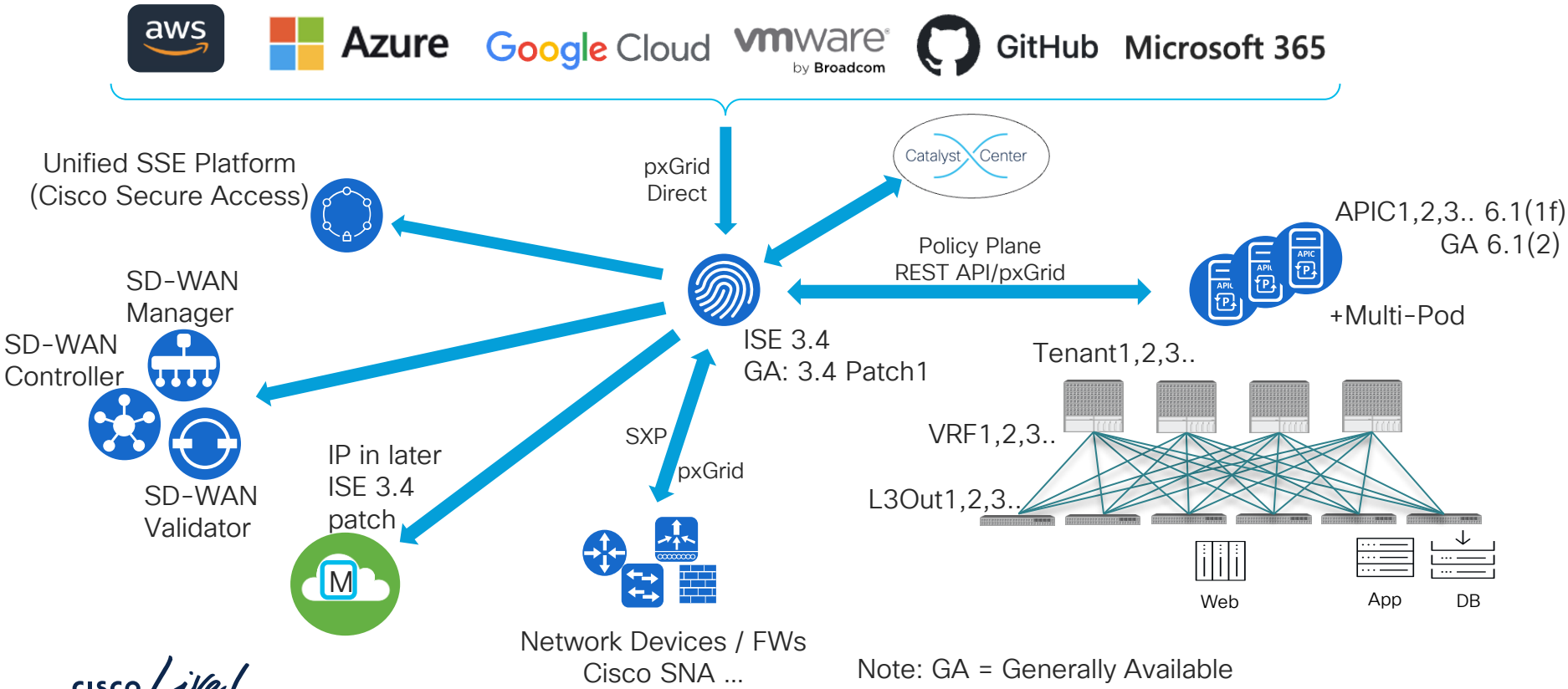
SD-WAN



Data Center / ACI

Common Policy Context Sharing

Classification
Normalisation



Note: GA = Generally Available

From ISE, Create Connection to ACI

ISE

1) Name Connection, Add creds; REST API

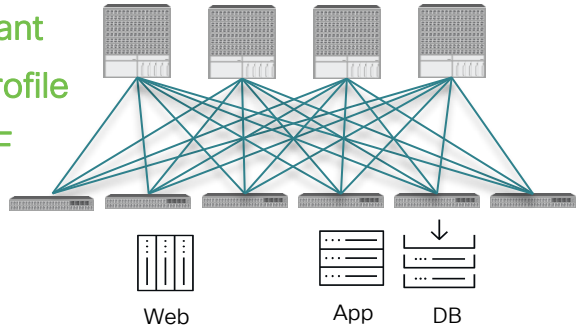
pxGrid

APIC

Tenant

Application Profile

VRF



Endpoint Group Type: EPG, ESG

2) Group Name Normalisation

[Can use these names/values and can customise]

<DC_Group_Name>_<Tenant>_<VRF>

Or add any prefix or suffix:

ACI_<DC_Group_Name>
<DC_Group_Name>_ACI

3) Choose which EPG/ESGs to sync:

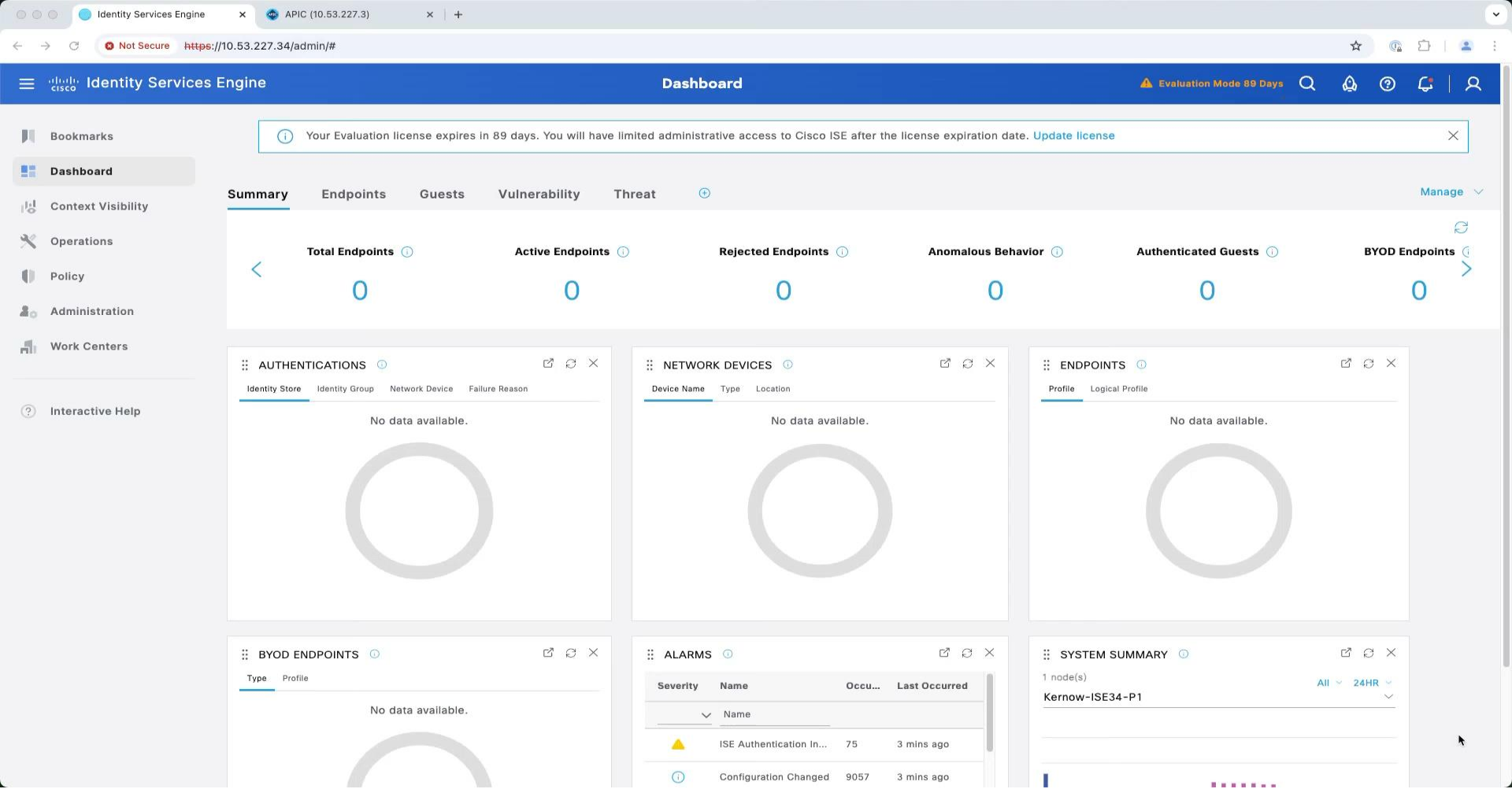
EPG/ESG name	Generated SGT Name	Tenant	VRF	Application Profile	Endpoint Group Type
Demo-ClientEPG	ACI_Demo_ClientEPG	Demo	vrf-1	Demo-AP	
Demo-WebEPG	ACI_Demo_WebEPG	Demo	vrf-1	Demo-AP	
Finance_Srvrs	Finance_Srvrs_APIC_from_ISE_P1	test-delete-at-will	default	AP-test-delete-at-will	

4) Choose the SGT Number Range:

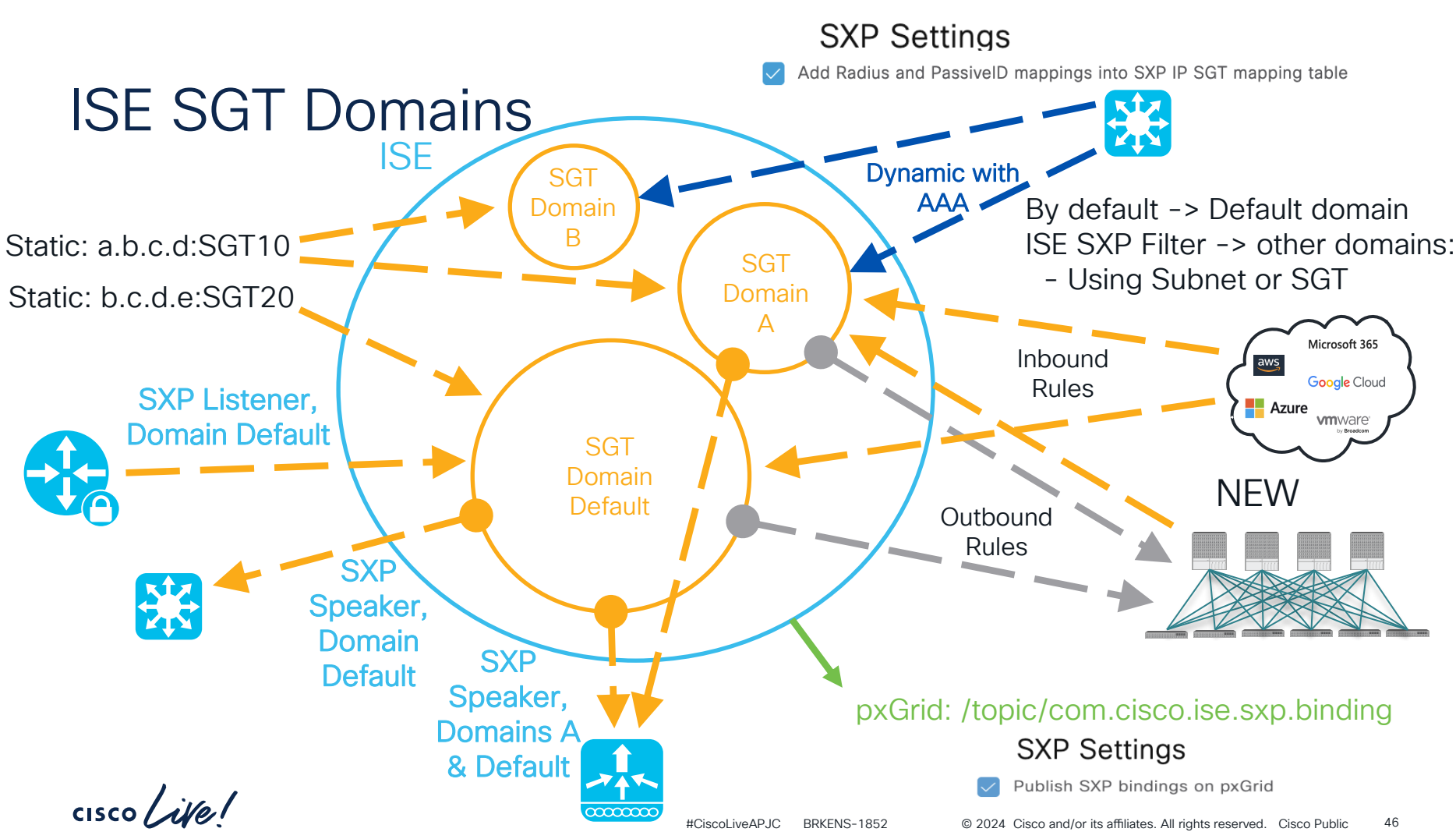
From 2 to 65535

Demo:

Create connection from ISE (Campus) to APIC (DC)



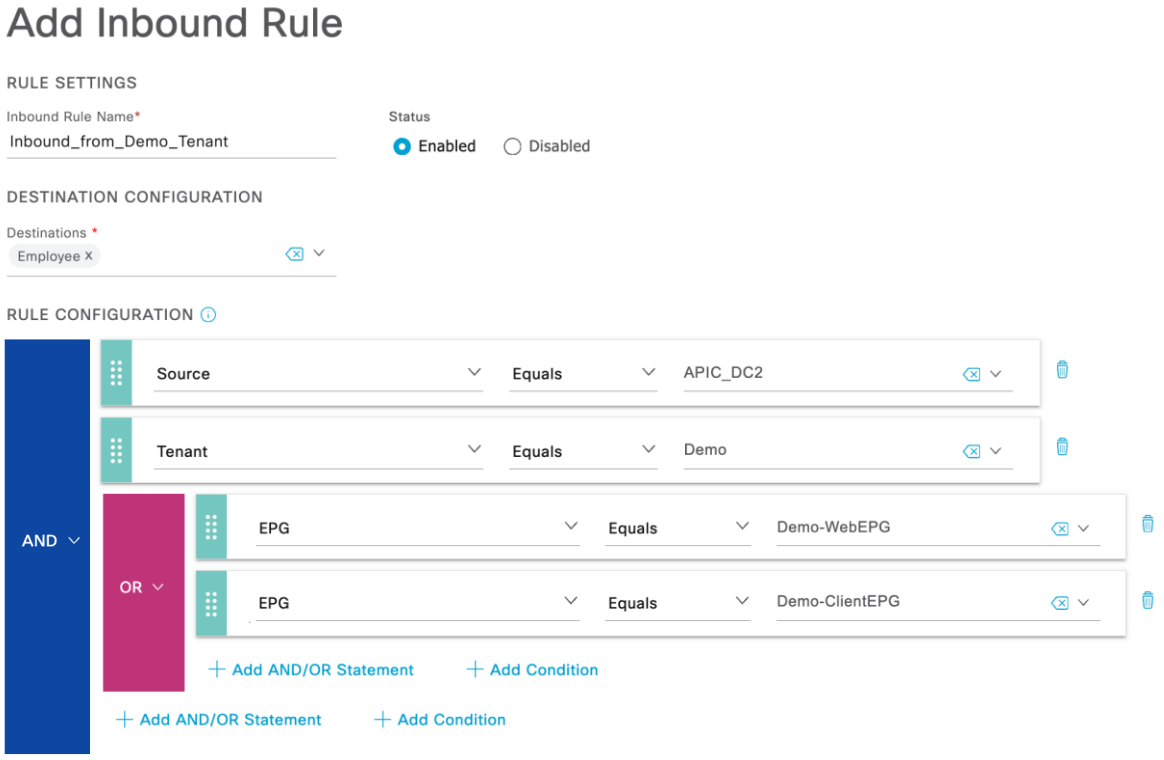
ISE SGT Domains



ISE Inbound SGT Domain Rule

Inbound destination to SGT Domain(s)

The context to receive into ISE

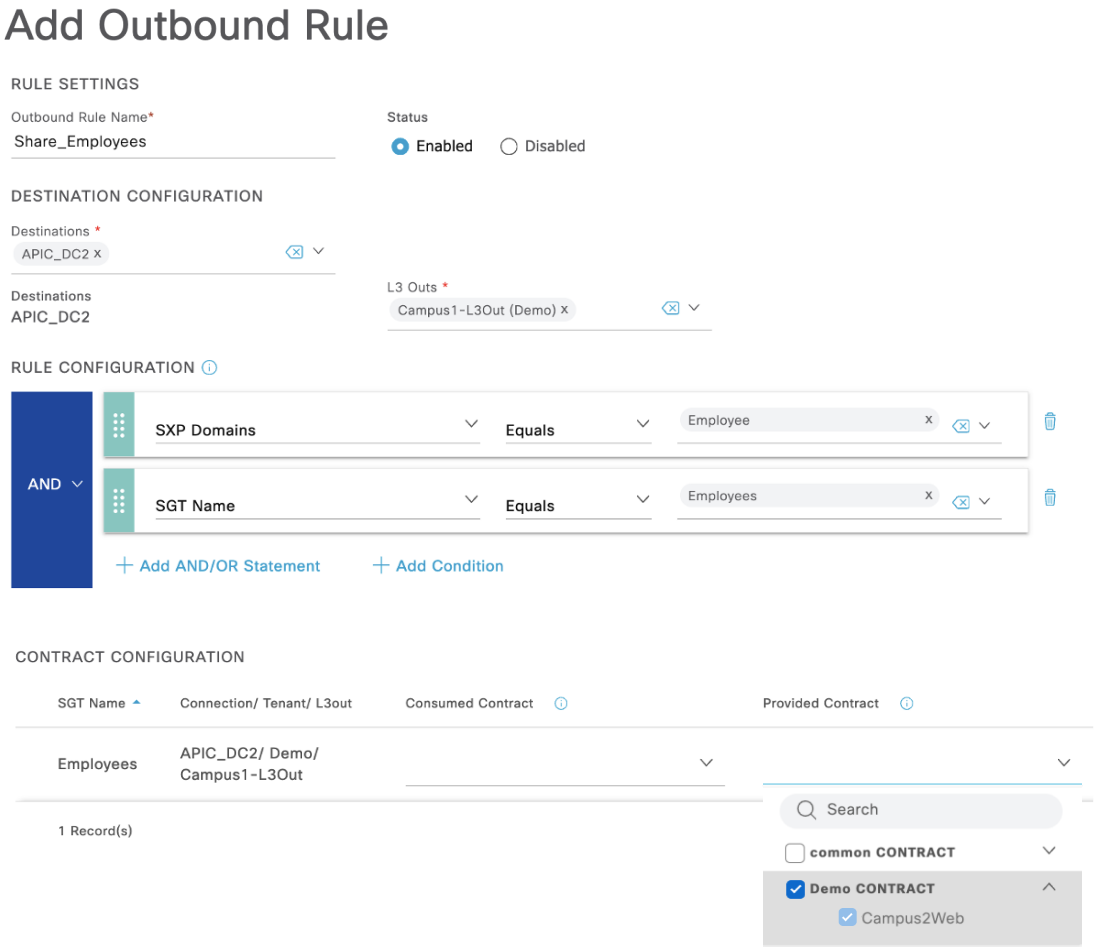


ISE Outbound SGT Domain Rule

Selects ACI destination criteria

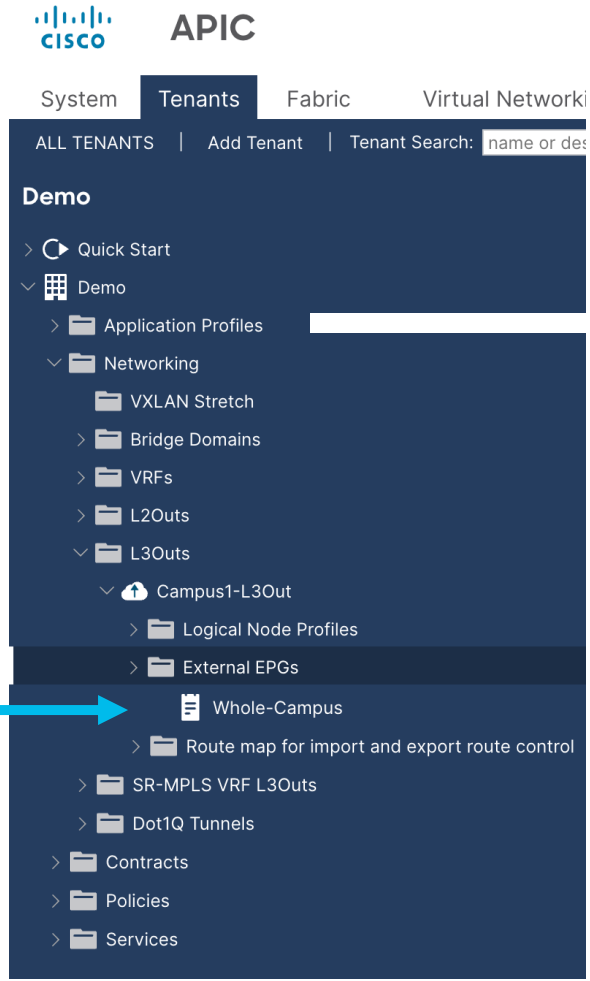
The context to send

Optionally attach to any existing contract already provisioned in ACI

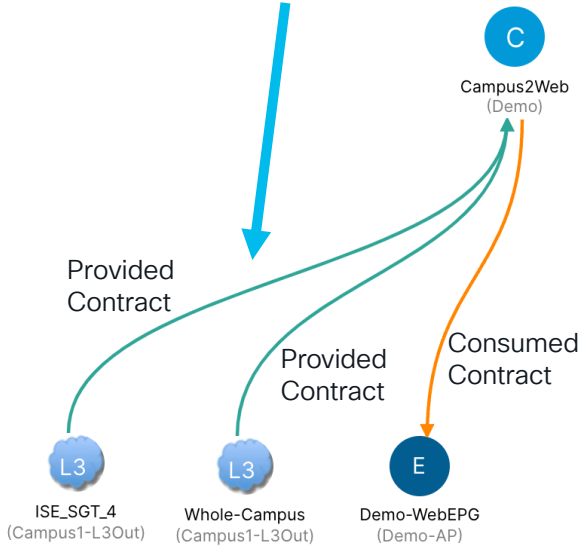


ISE Outbound Rule Effect in APIC

SGT added as External EPG

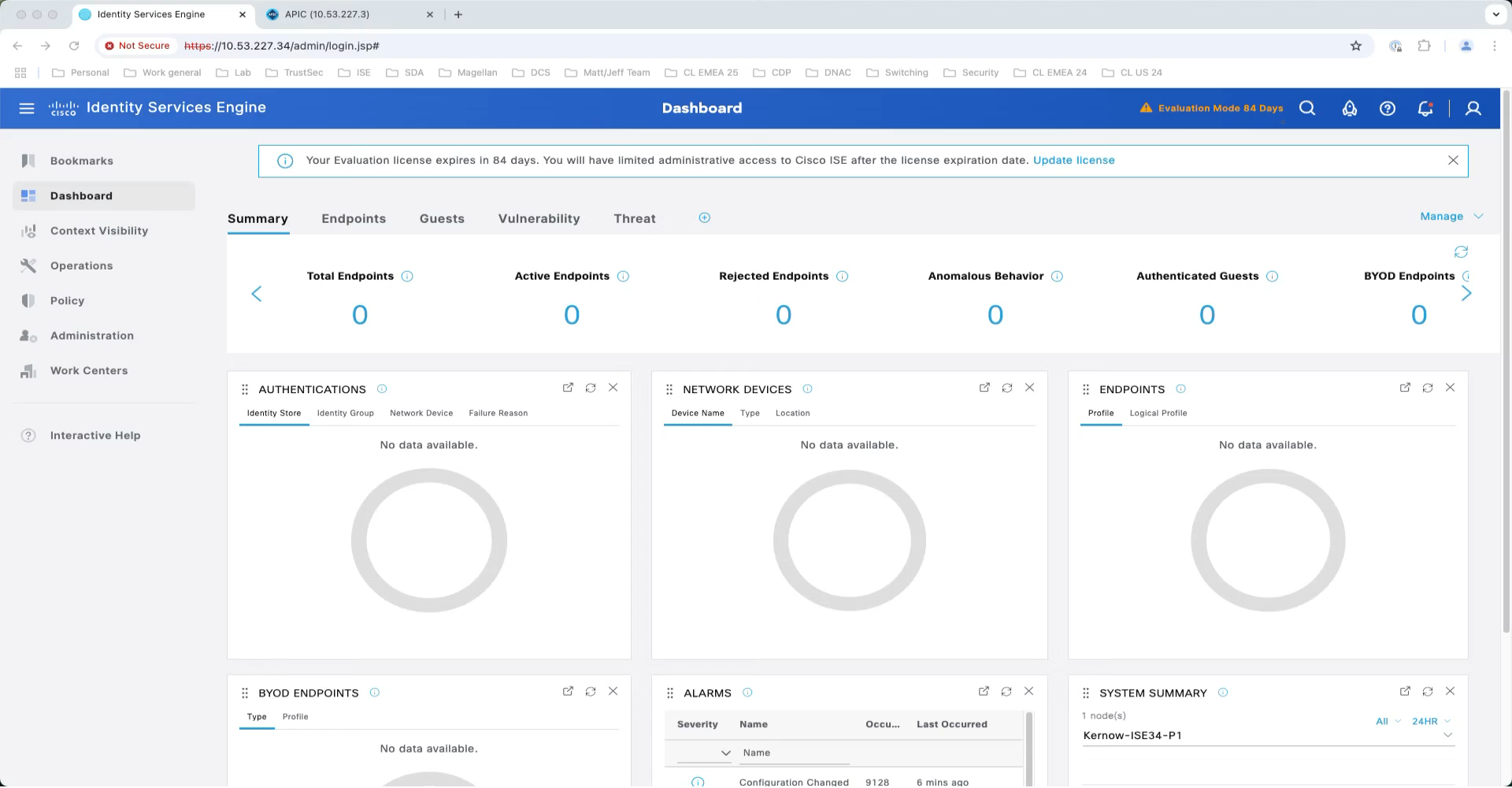


Newly added Group attached to existing Contract in APIC:

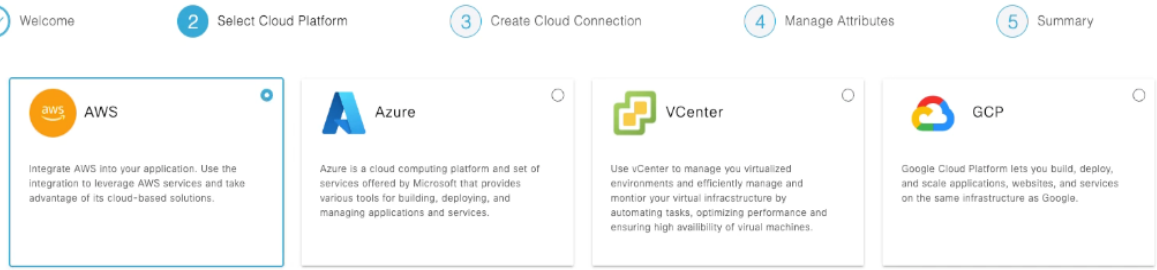


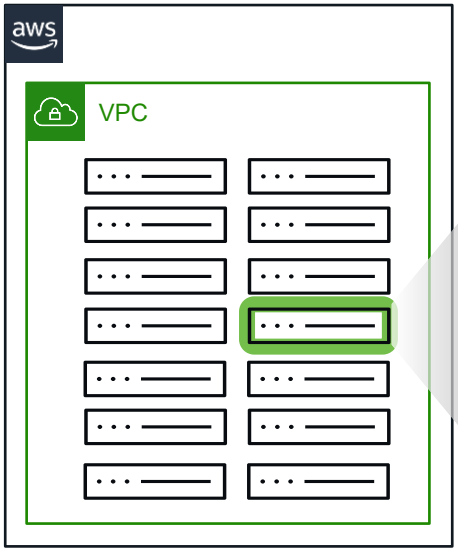
Demo:

Sharing groups with ACI, creating Outbound SGT Domain Rules



Classifying Cloud Workloads





Workload Attributes
VPC
Created
State
Name
Application
Version
Owner
OS
IP
Location
...

ISE Dictionary
- Name
- Application
- IP
- Location

ISE

Classification Policy

Primary SGT (pxGrid & SXP)
Secondary SGT (pxGrid)

ISE Workload Classification Rules

Add Classification Rule

Assign Primary & optional Secondary SGTs

Classification Conditions

Primary SGT → pxGrid Session Topic as ‘Security Group’

Primary SGT → SXP

Secondary SGT → pxGrid Session Topic as ordered array named ‘Secondary Security Groups’

RULE SETTINGS

Rule Name* Classify-PCI

Status: Enabled / Disabled

AUTHORIZATION CONFIGURATION

Primary SGT * PCI_Servers

Secondary SGTs (Optional) Production_Servers x

RULE CONFIGURATION

OR

AND
- Source In AWS1 x
- AWS - Owner Contains Label Joff (Enter text to search)

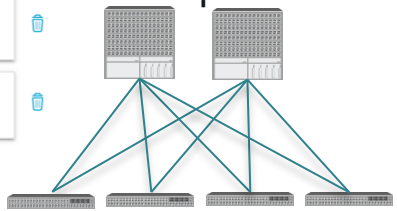
+ Add AND/OR Statement + Add Condition

AND
- Source Equals APIC_from_ISE_P1
- EPG Equals Demo-ClientEPG

+ Add AND/OR Statement + Add Condition

+ Add AND/OR Statement + Add Condition

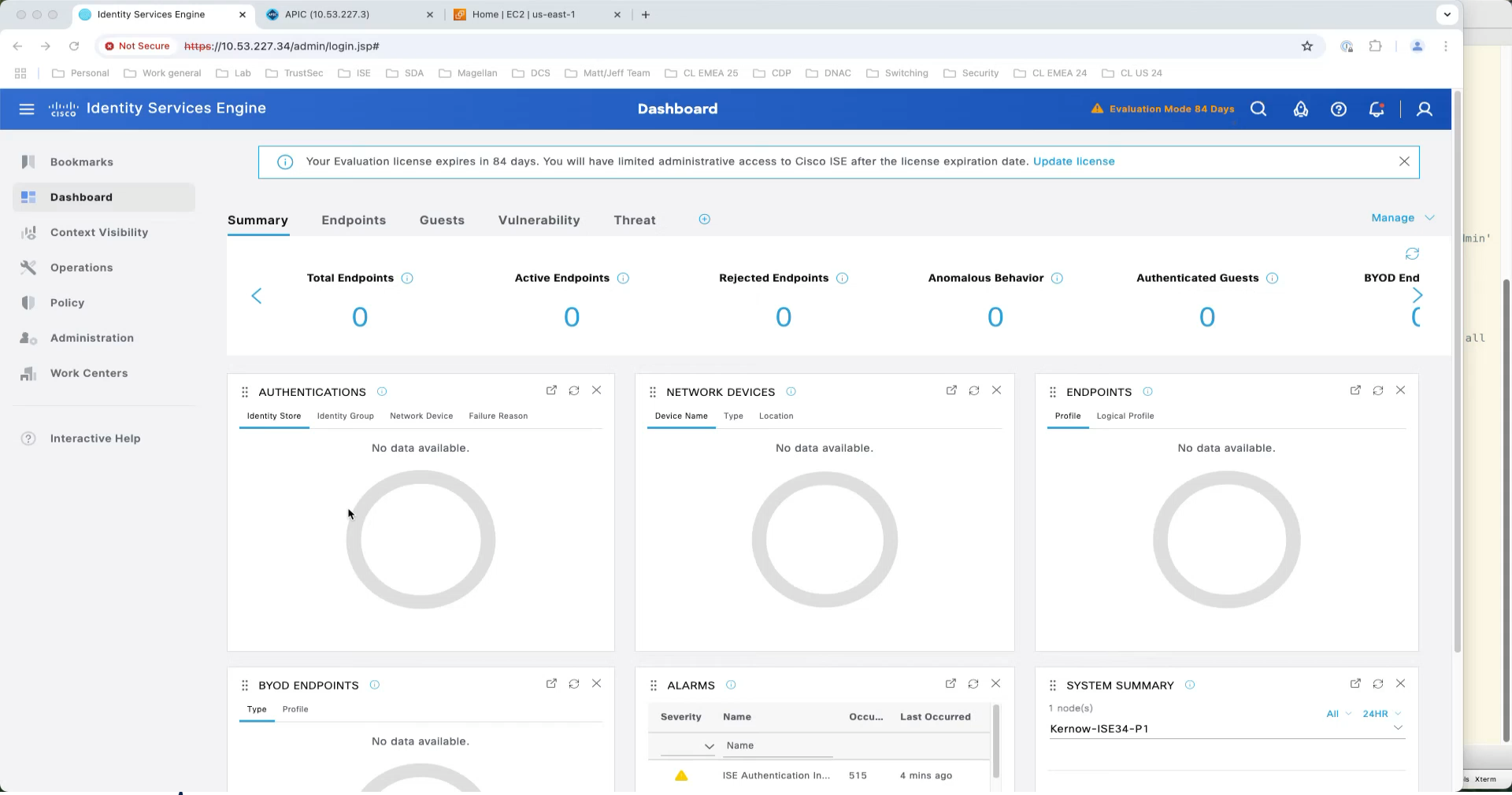
ACI Optional



Primary SGT derived from EPG/ESG

Demo:

Classify Cloud Workloads



Recap

- Introduction
- Classification
- Propagation
- Enforcement
- Common Policy

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

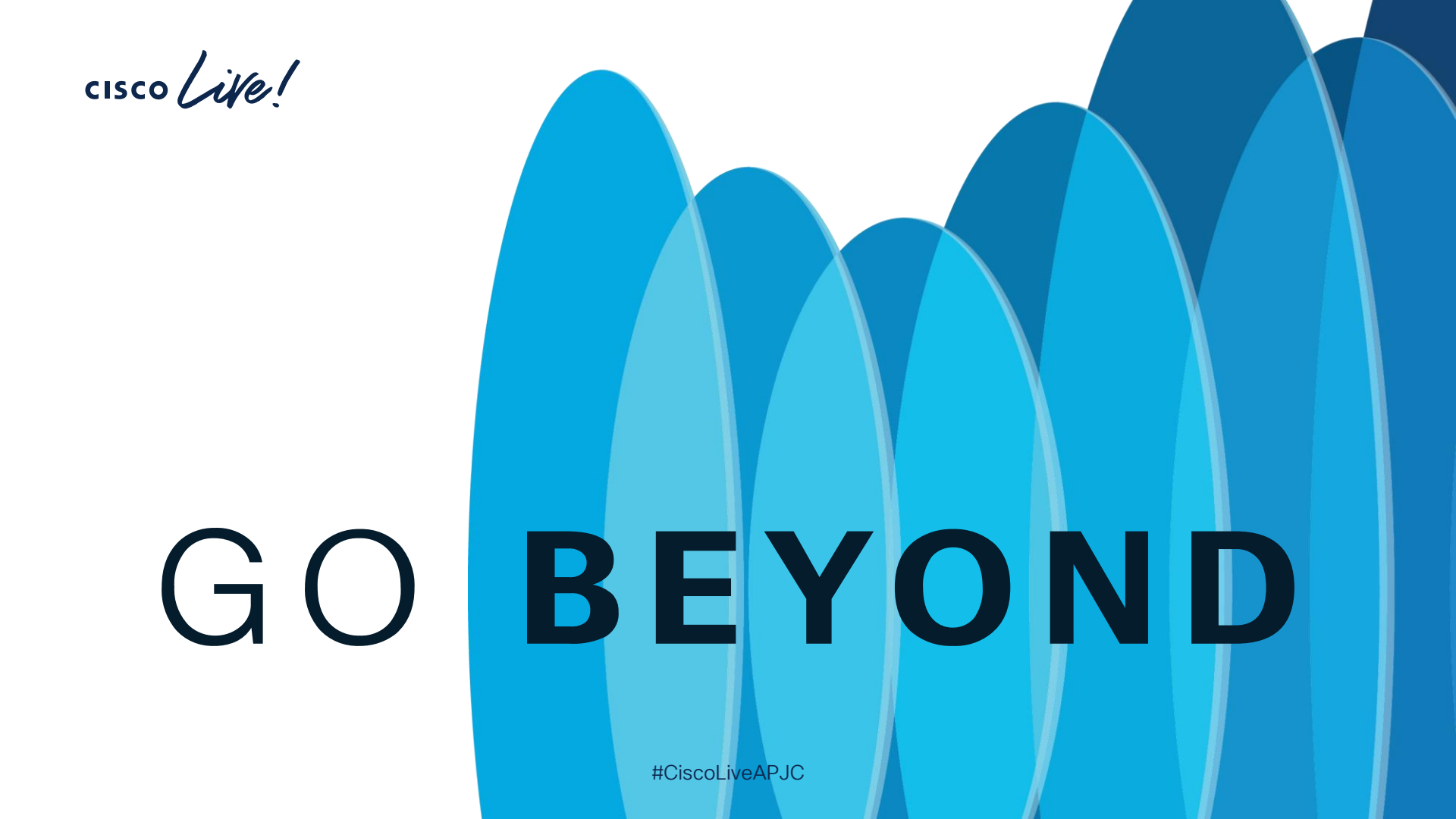
Complete your surveys in the **Cisco Live mobile app**.

Continue your education

- Visit the Cisco Stand for related demos: “Universal security translator - Common policy” [DEMNET-13]
- Book your one-on-one Meet the Expert meeting – I’m at The Hub Wed for 2 hours from 11:30
- 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

Contact me at: trustsec@cisco.com


cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC