The bridge to possible

TrustSec Refresh

Reinforced with latest segmentation innovations

Jonothan Eaves
Technical Marketing Engineer
BRKENS-1852

cisco Live!

#CiscoLive

Cisco Webex App

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

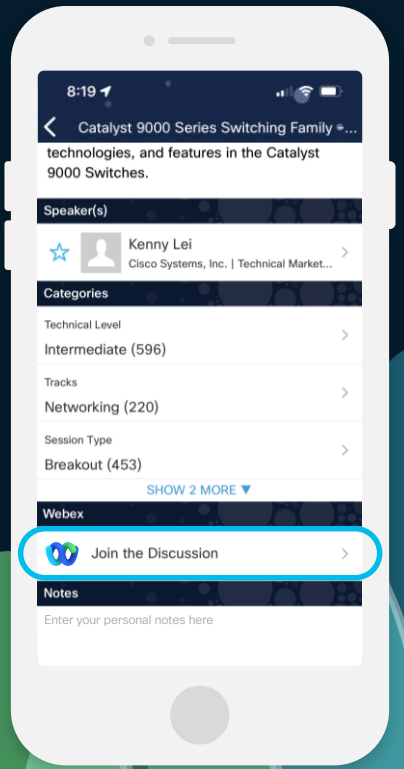
Questions?

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 June 7, 2024.

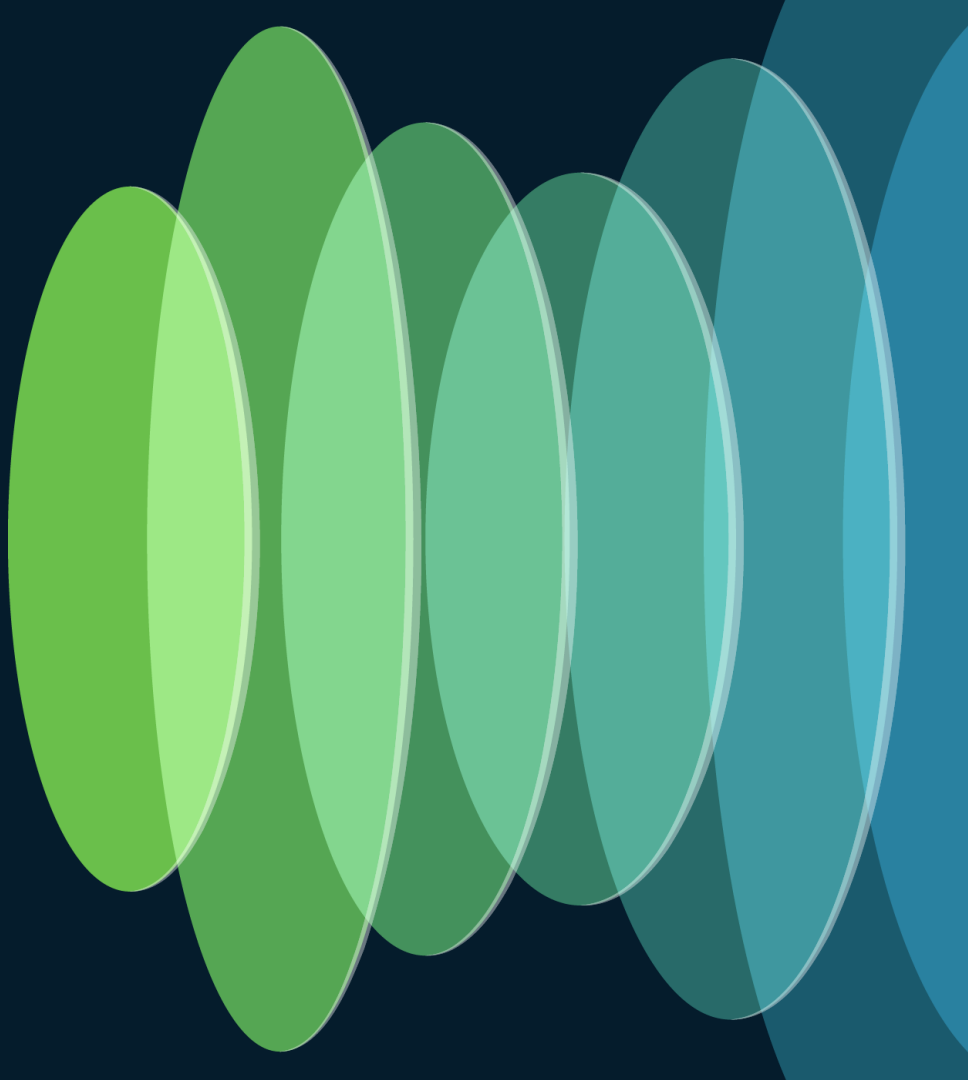


cisco Live!

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

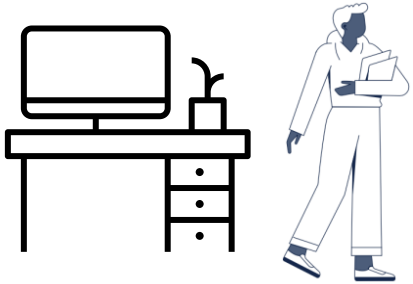
ADVANCED PERSISTENT THREATS

Australia phones cyber-attack exposes personal data

PHISHING

Nato investigates hacker sale of missile firm data

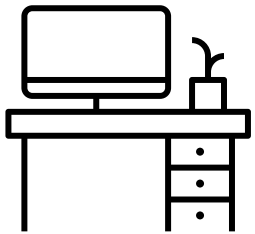
Policy Challenge

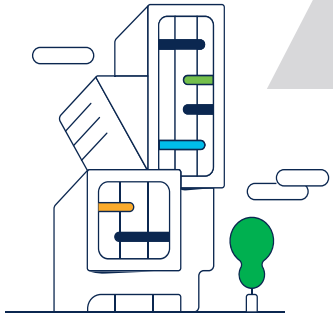


VLAN 100
Subnet A.B.C.D
↓
IPACL 1
IPACL 2 ....

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

Security Policy Tied to Infra





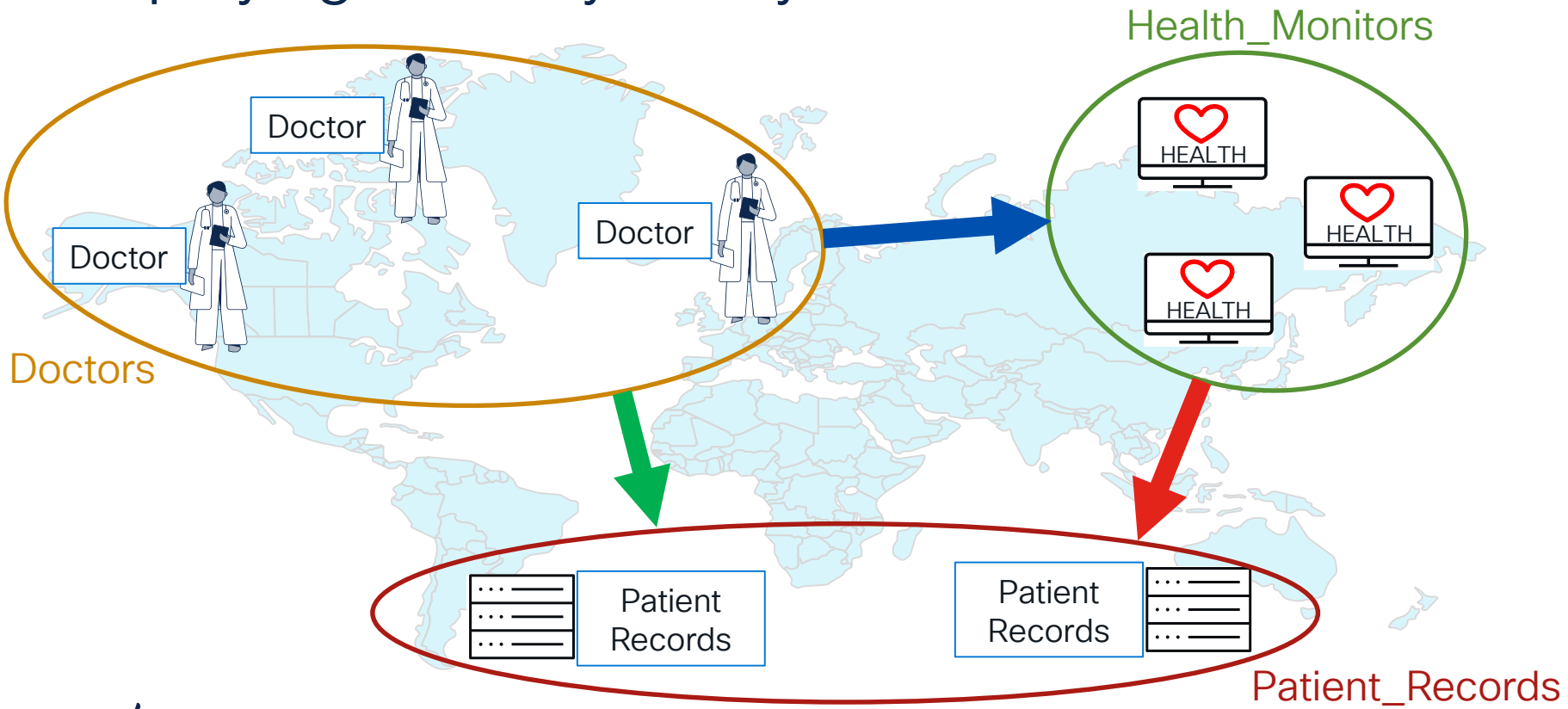
VLAN 101
Subnet E.F.G.H
↓
IPACL 11
IPACL 12 ....

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

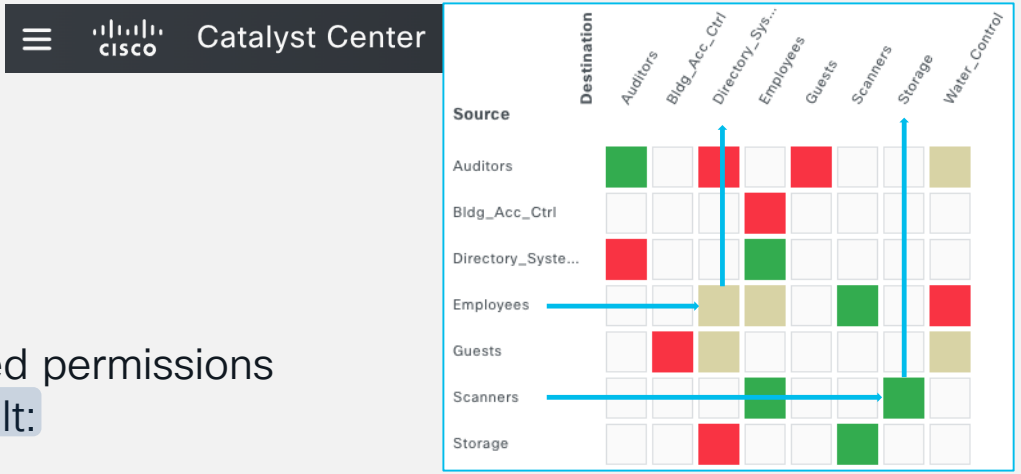
Can you see the Business Intent Here?

```
access-list 102 deny icmp 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

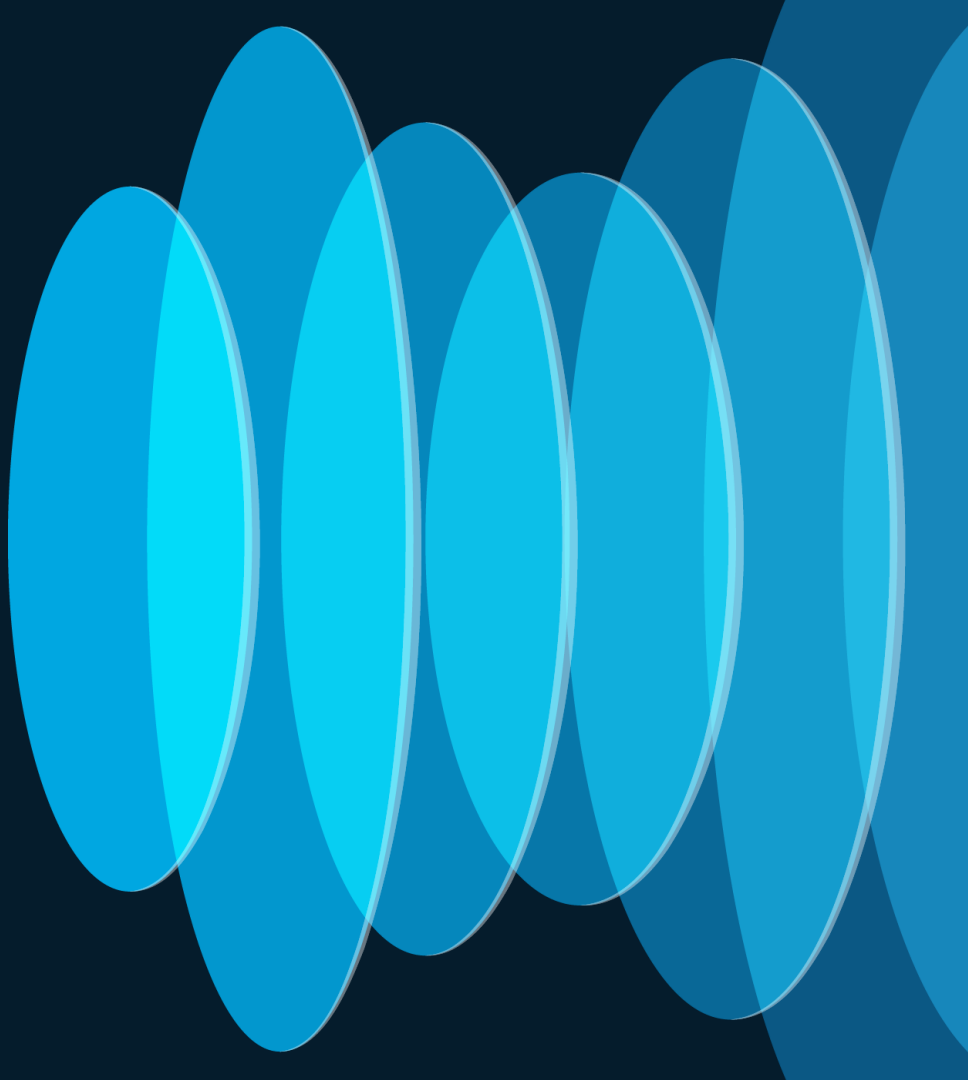


Business Intent is Clear
With meaningful group-based policies aligned to business needs



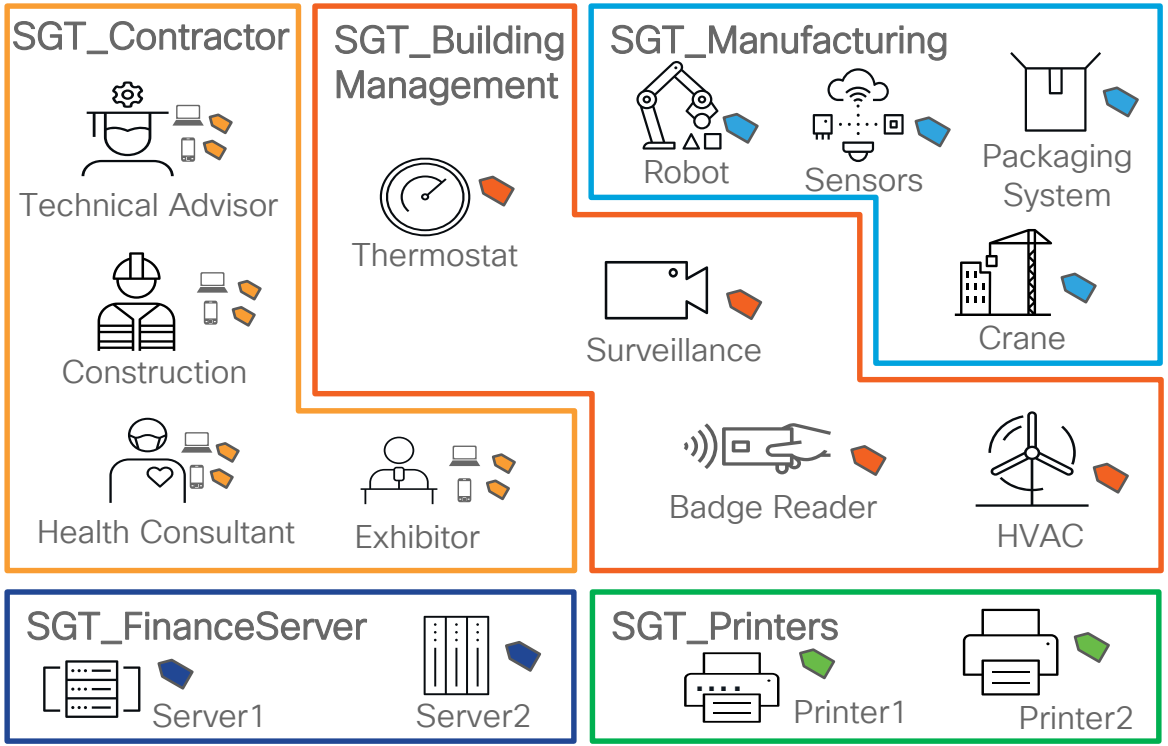
Edge-Cat9300#show cts role-based permissions
IPv4 Role-based permissions default:
    Deny IP-00
IPv4 Role-based permissions from group 36:Scanners to group 27:Storage:
    Permit_IP_Log
IPv4 Role-based permissions from group 4:Employees to group 12:Directory_Systems:
    Permit_LDAP_HTTP

Classification



Classification into Intent-Based Groups

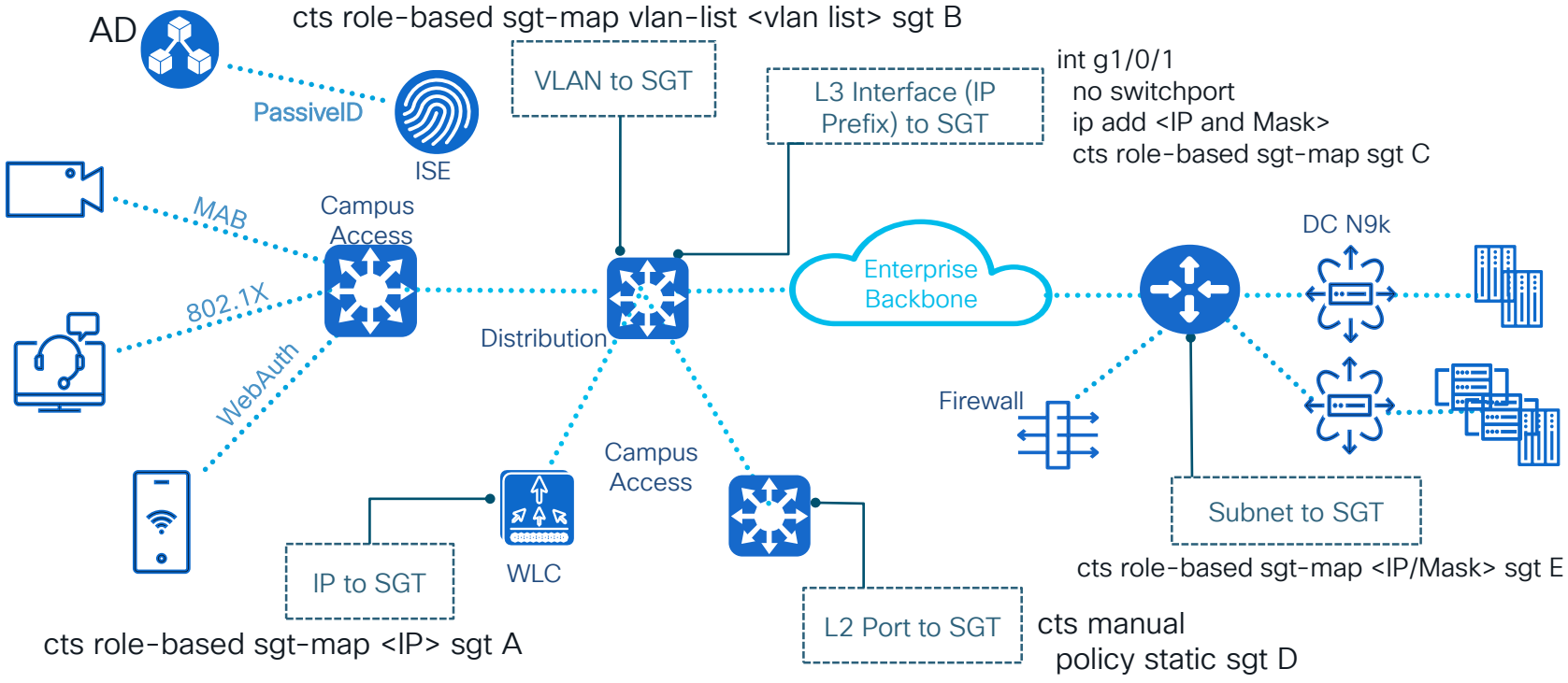
- Business-based groupings to provide consistent policy and access independent of network topology
- Leverage items such as location, device type, RADIUS attributes, AD membership etc. to allocate group assignments



Classification Mechanisms

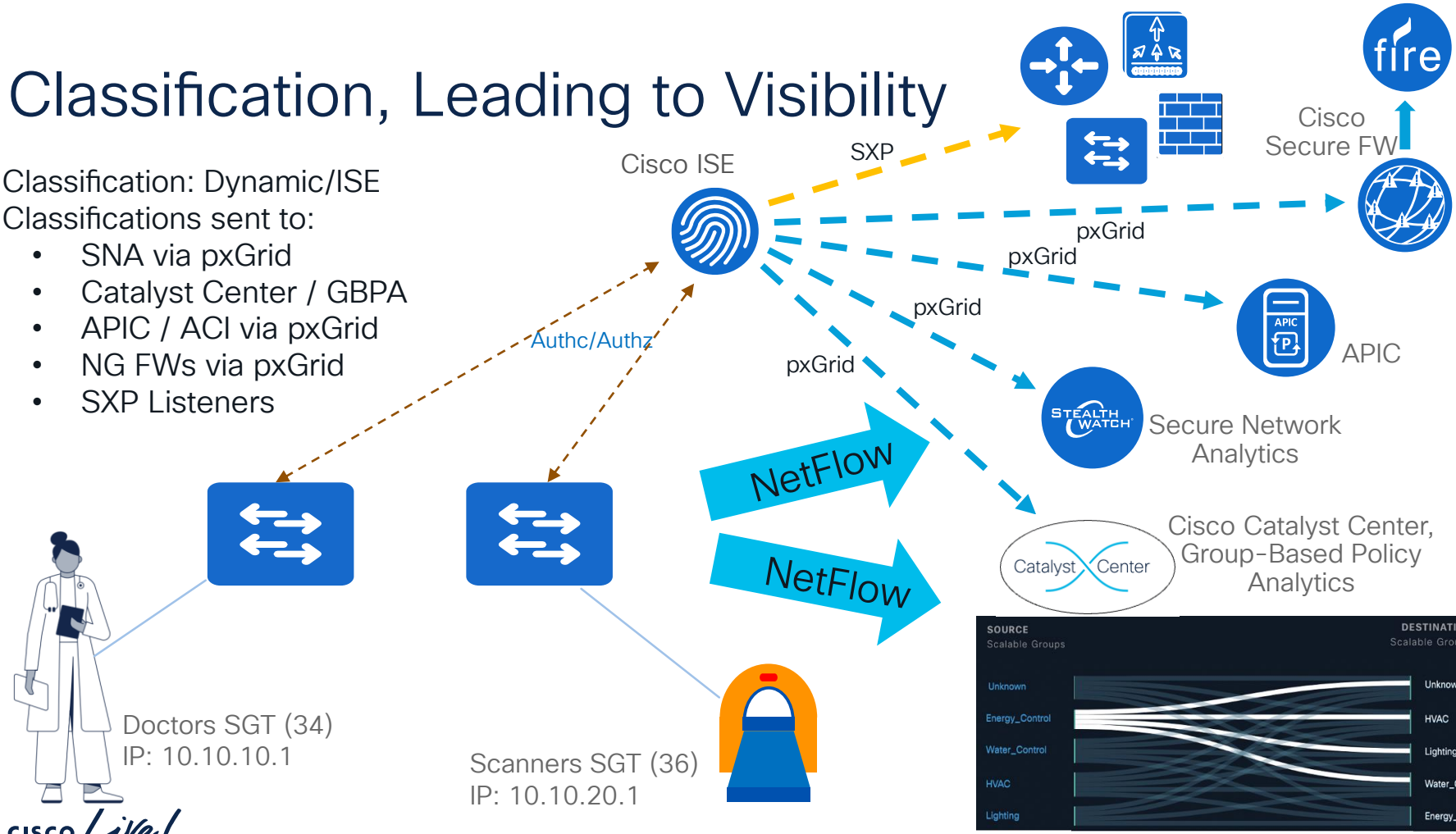
Dynamic Classification

Static Classification

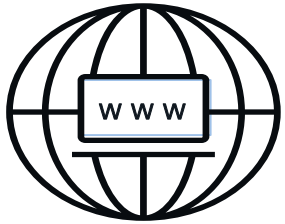


Classification, Leading to Visibility

- 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

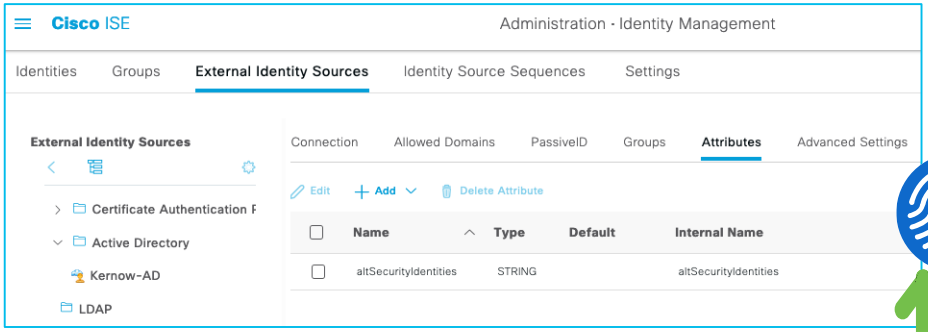
```
device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
IP Address          SGT         Source
==============================
0.0.0.0/0           123         CLI

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

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

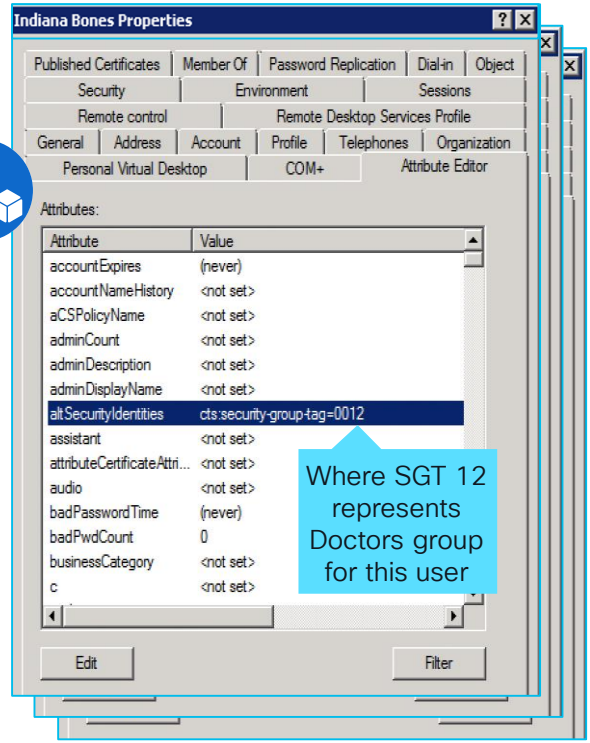
```
cts role-based sgt-map 0:0::/0 sgt 123
```

SGT Assigned from AD
Reduces Authz Rules Required



Add or reuse attribute in AD for SGT

Retrieve into ISE to use in the authorization process:



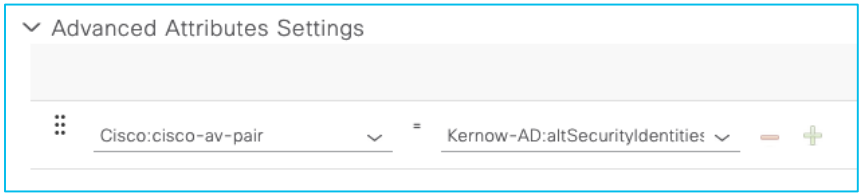
Where SGT 12 represents Doctors group for this user

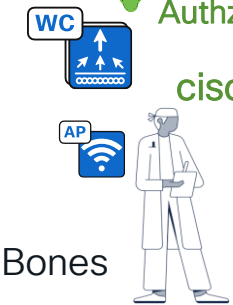
Authc

Authz:

cisco-av-pair="cts:security-group-tag=0012"

Configure ISE Authz Profile:



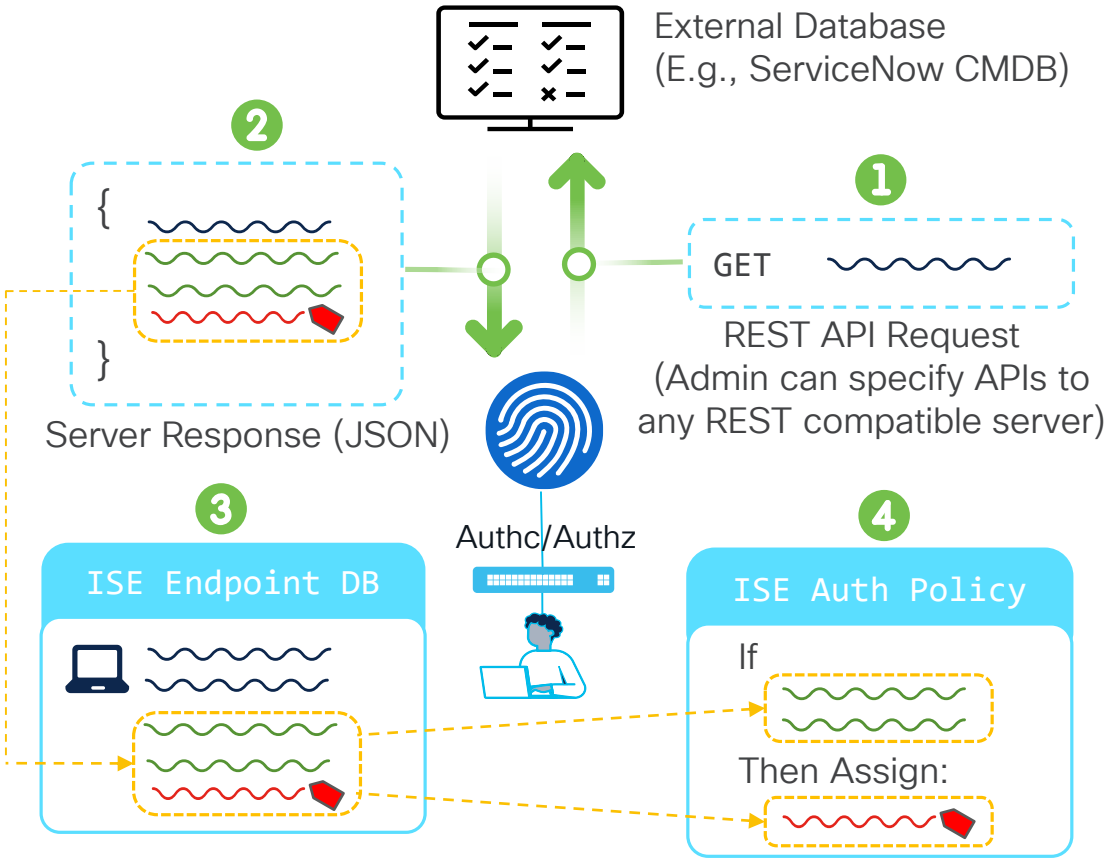


Dr. Indiana Bones

Classified into Doctors / SGT 12 Group

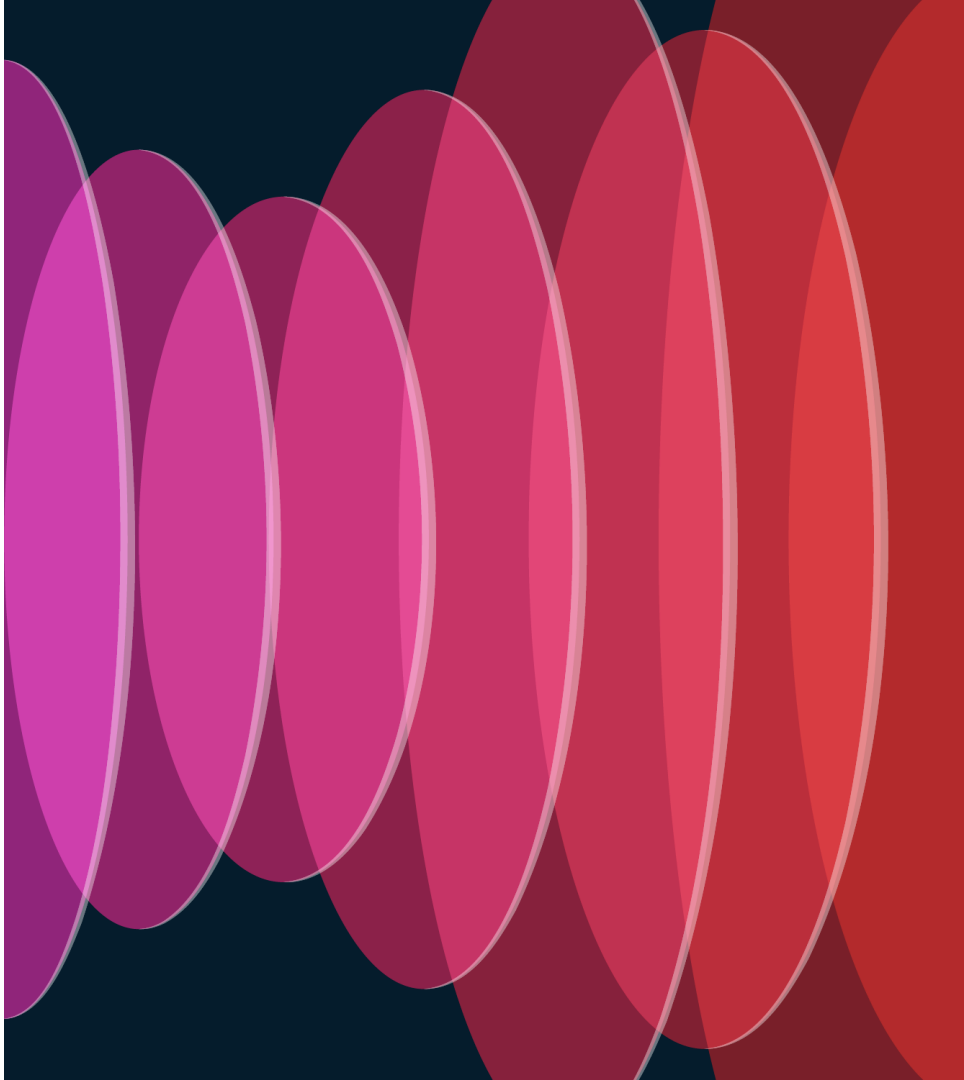
SGT Classification from pxGrid Direct Attributes

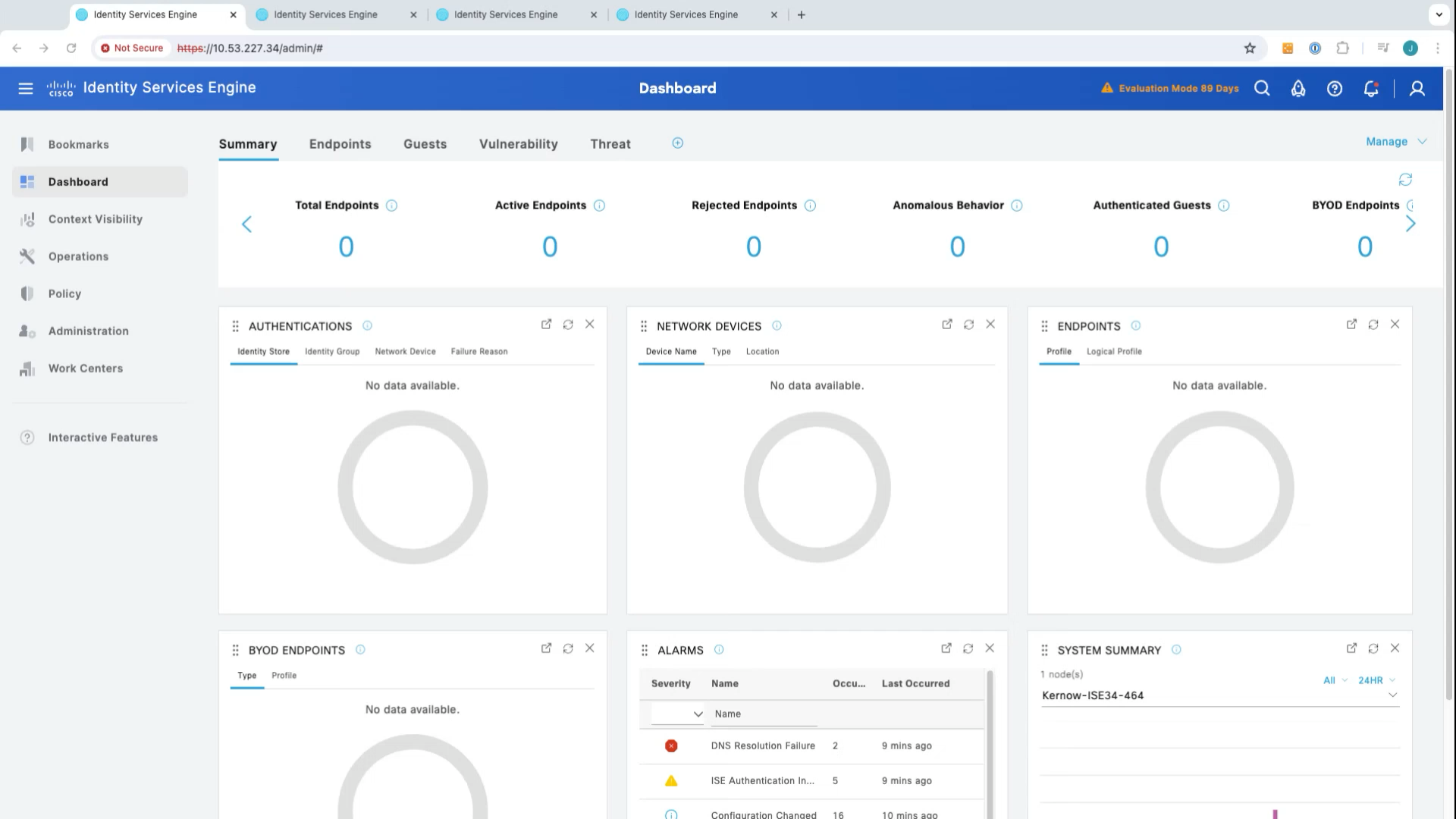

```
{"result":[{
"owned_by":"jeaves",
"operational_status":"Operational",
"sys_updated_on":"2022-04-22 16:44:52",
"sys_created_by":"jeaves",
"warranty_expiration":"",
"cpu_speed":"",
"checked_out":"",
"maintenance_schedule":"",
"group_tag":"cts:security-group-tag=12-00",
"managed_by":"jeaves",
"sys_class_name":"Computer",
"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",
...
```

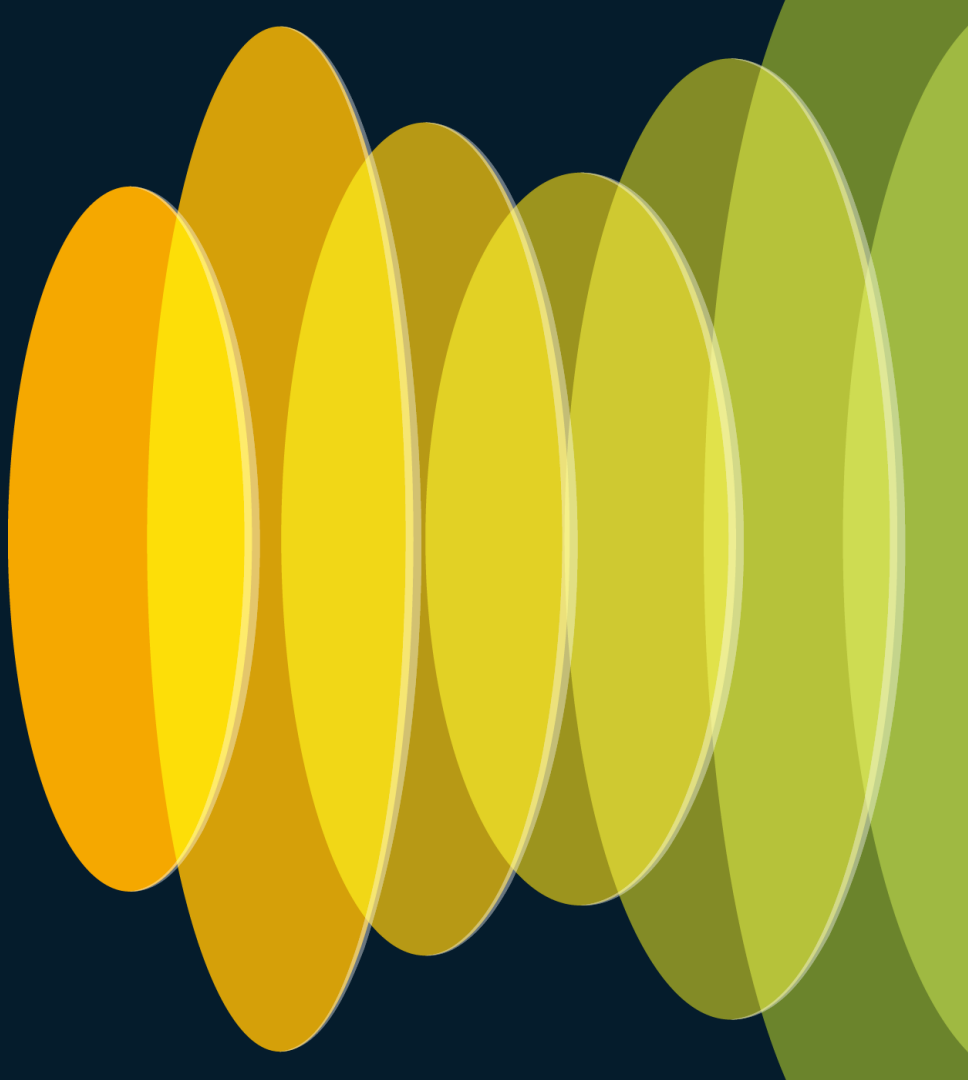
Demo:

pxGrid Direct




Identity Services Engine
Identity Services Engine
Identity Services Engine
Identity Services Engine
Not Secure
https://10.53.227.34/admin/#
Identity Services Engine
Dashboard
Evaluation Mode 89 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
0
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
BYOD Endpoints
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
No data available.
NETWORK DEVICES
Device Name
Type
Location
No data available.
ENDPOINTS
Profile
Logical Profile
No data available.
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
Severity
Name
Occu...
Last Occurred
Name
DNS Resolution Failure
2
9 mins ago
ISE Authentication In...
5
9 mins ago
Configuration Changed
16
10 mins ago
SYSTEM SUMMARY
1 node(s)
All
24HR
Kernow-ISE34-464

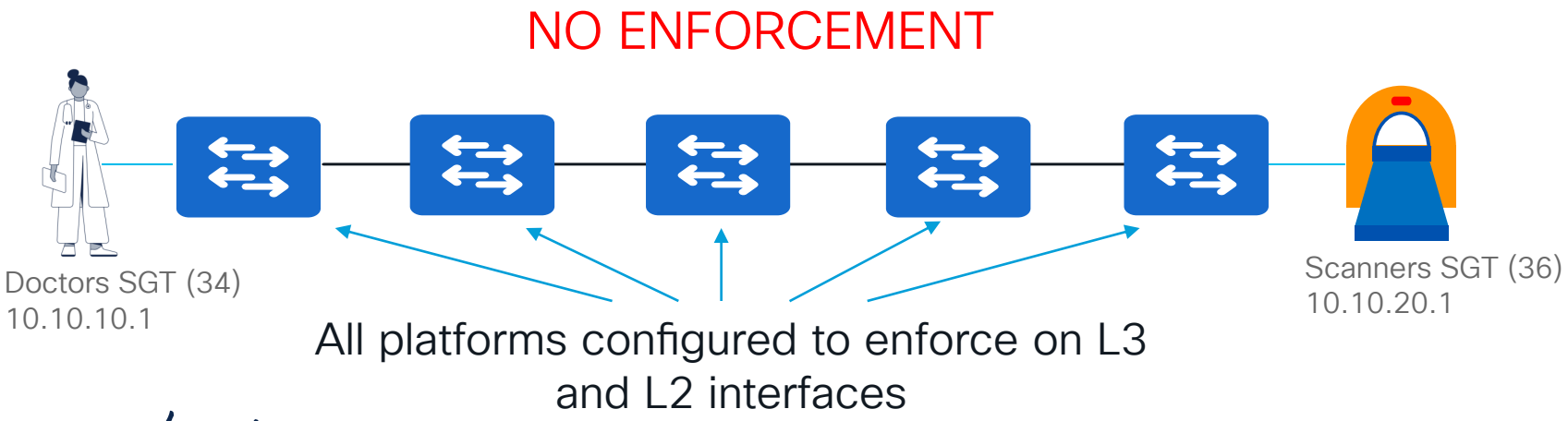
Propagation



Where does enforcement occur?

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

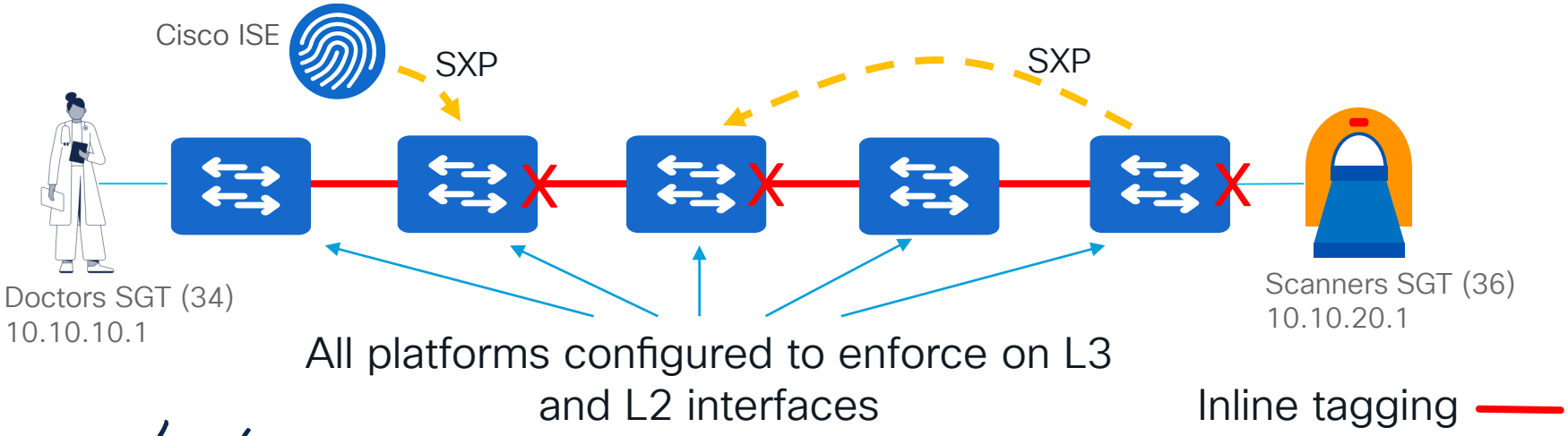
- Source IP:SGT binding
- Destination IP:SGT binding
- Platform and VLAN has enforcement enabled
- A policy is downloaded from ISE (either default or specific)



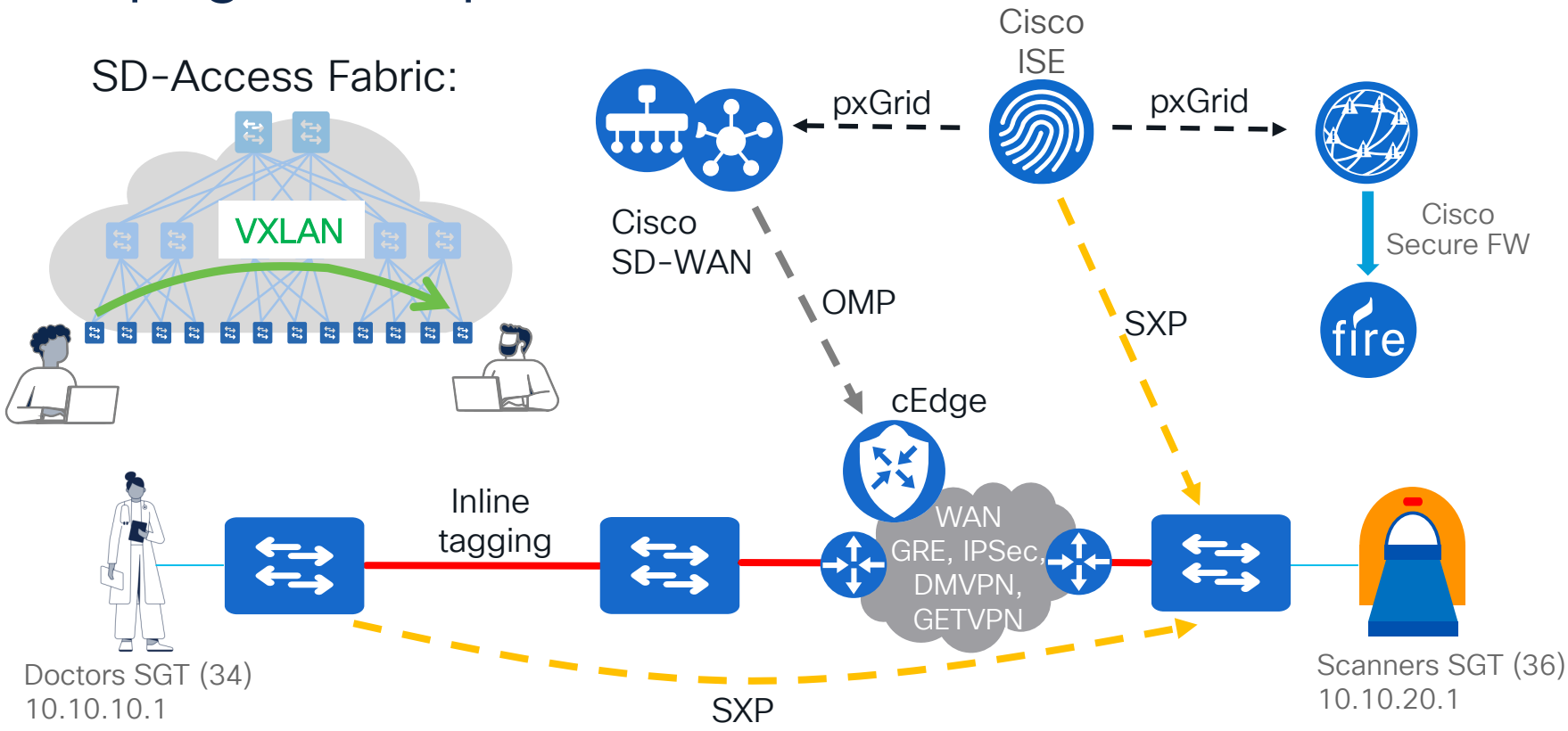
This is where Propagation comes in

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)

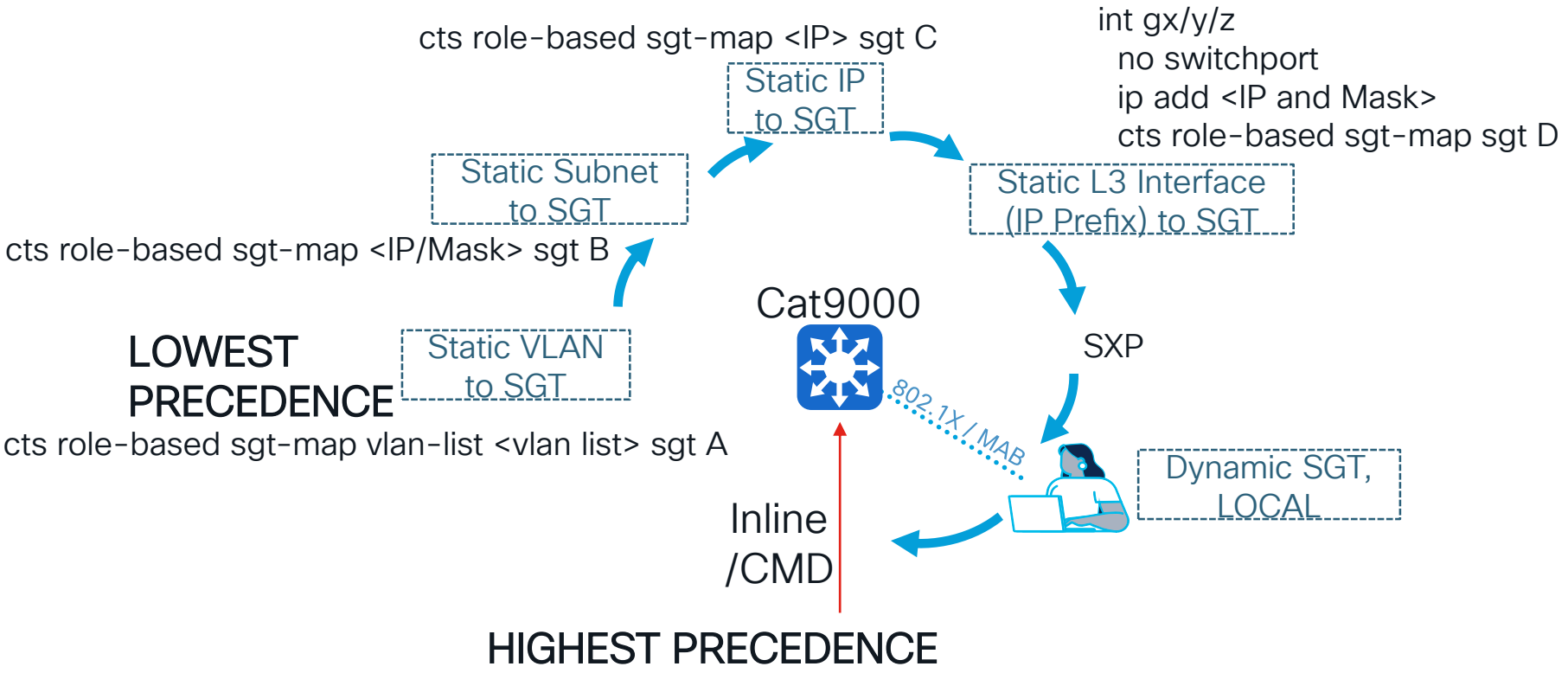


Propagation Options



Order of Precedence

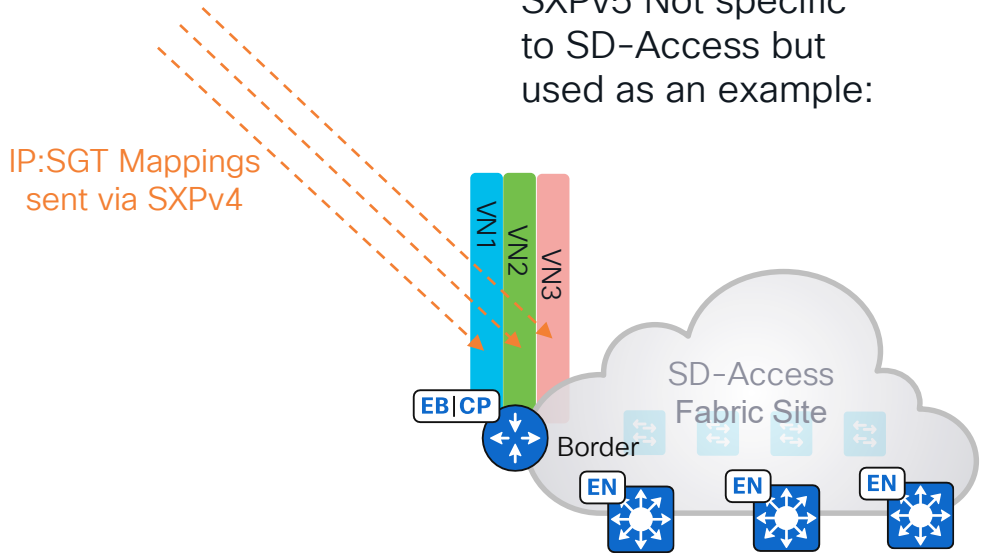
For Reference



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.

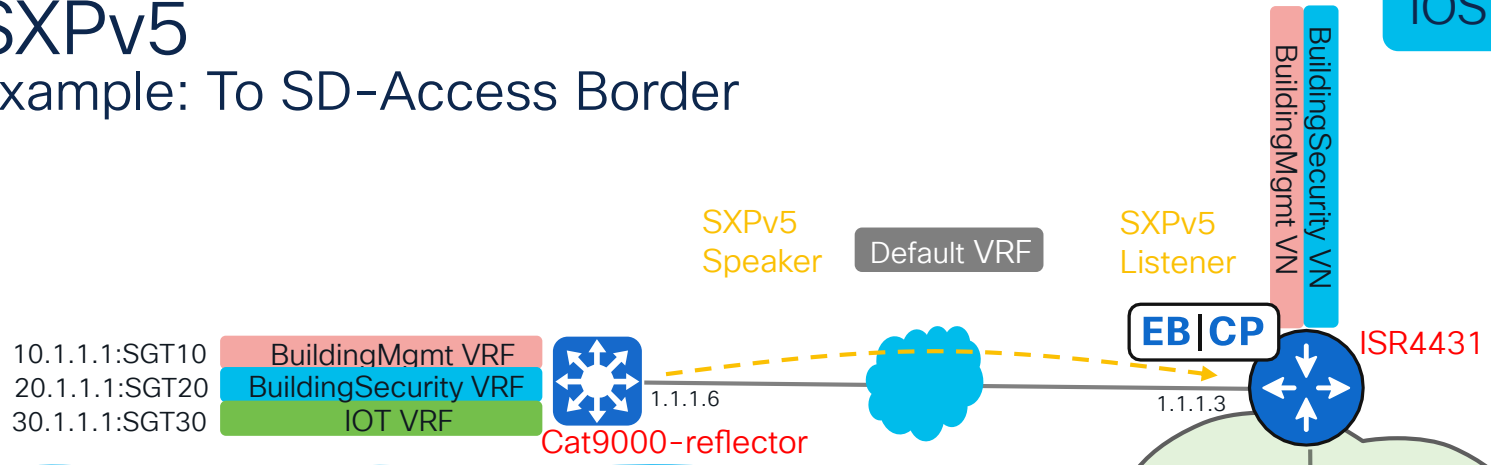
SXPv5 Not specific to SD-Access but used as an example:



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

SXPv5
Example: To SD-Access Border

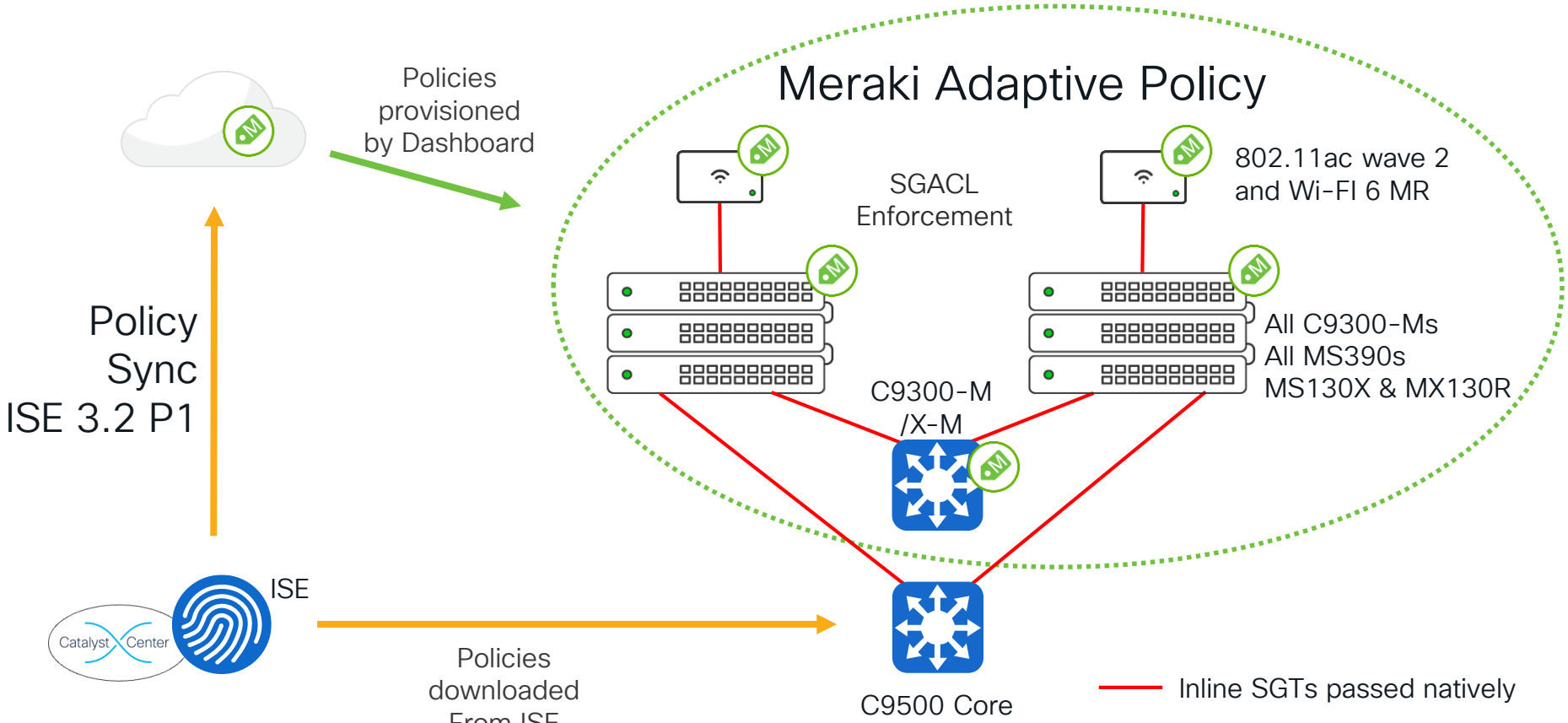
IOS-XE 17.9.1



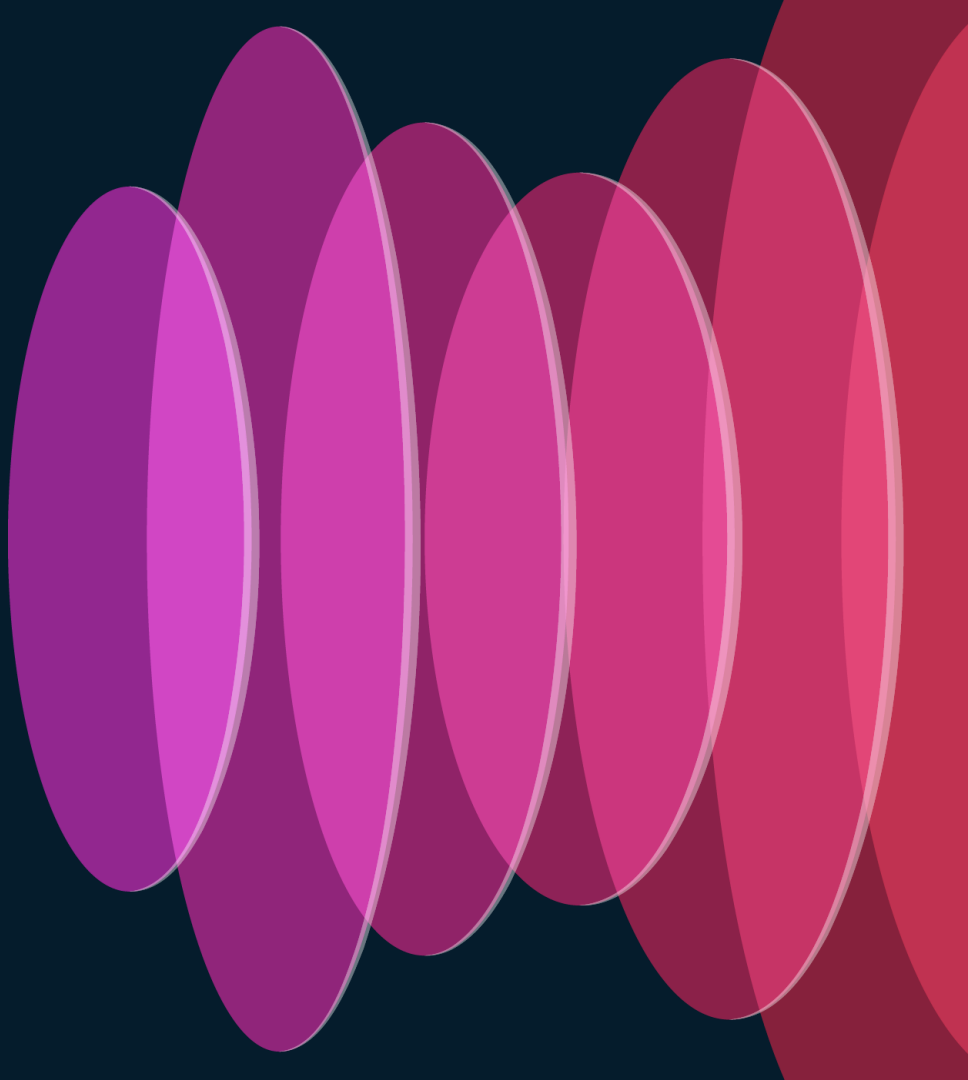

```
cts sxp export-list SXPv5-export-VRFs-to-Border
 vrf BuildingMgmt
 vrf BuildingSecurity
!
cts sxp export-import-group speaker SXPv5-speaker-grp-to-Border
 export-list SXPv5-export-VRFs-to-Border
 peer 1.1.1.3
```

```
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
```

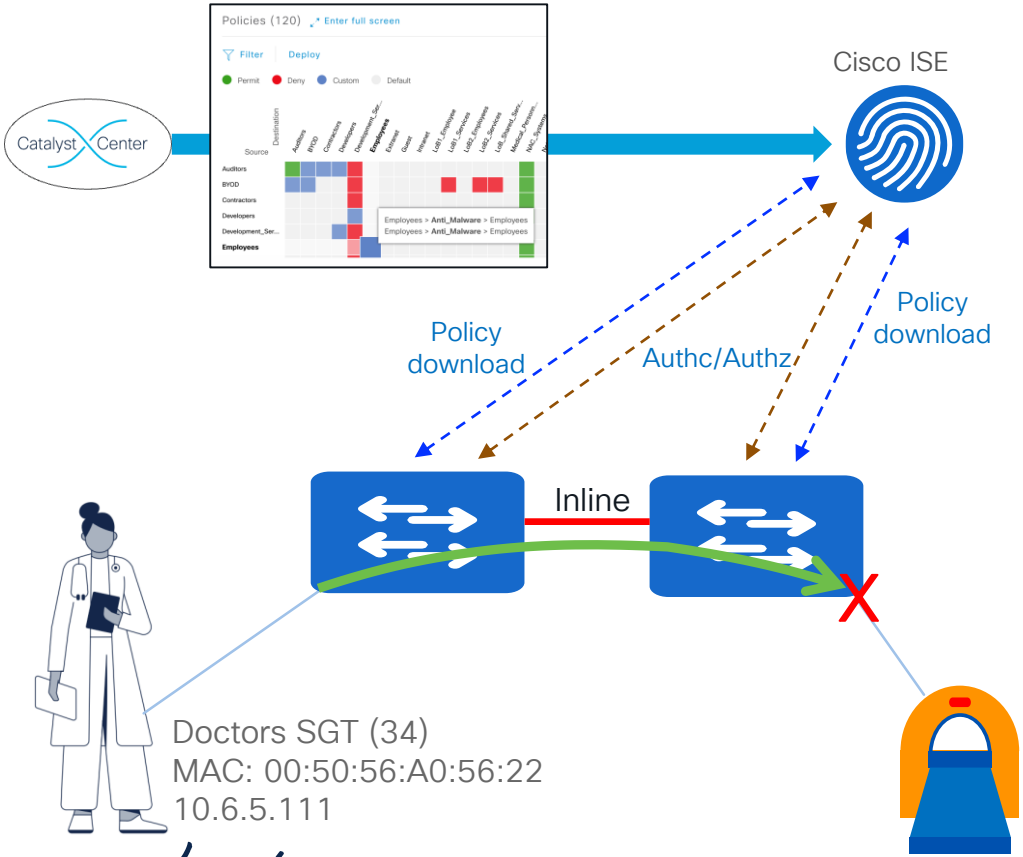
Integrating ISE and Meraki Domains



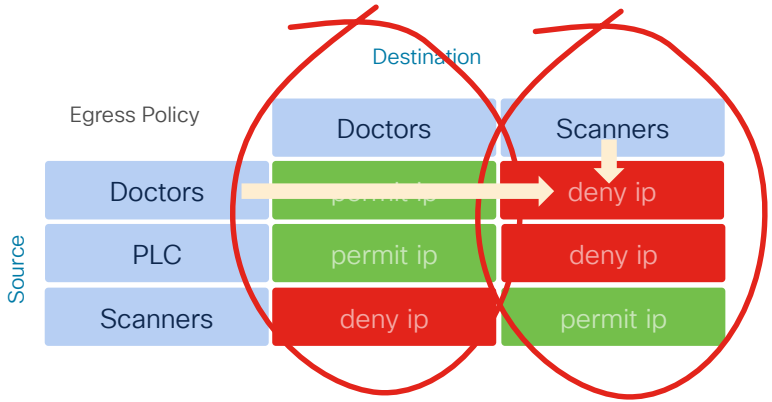
Enforcement



Classification, Propagation and Enforcement

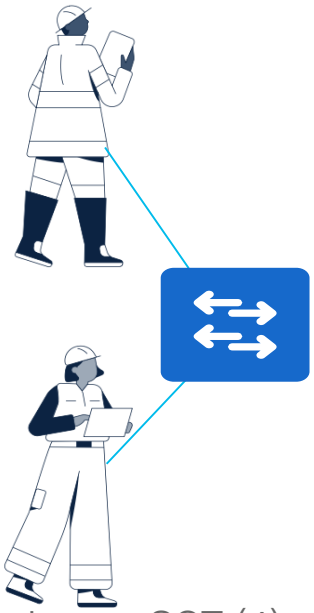


- Classification: Dynamic/ISE
- Propagation (Source SGT)
- Enforcement: At Egress



Limit Lateral Movement; Reduce Malware Propagation

Employees SGT (4)
10.20.30.5

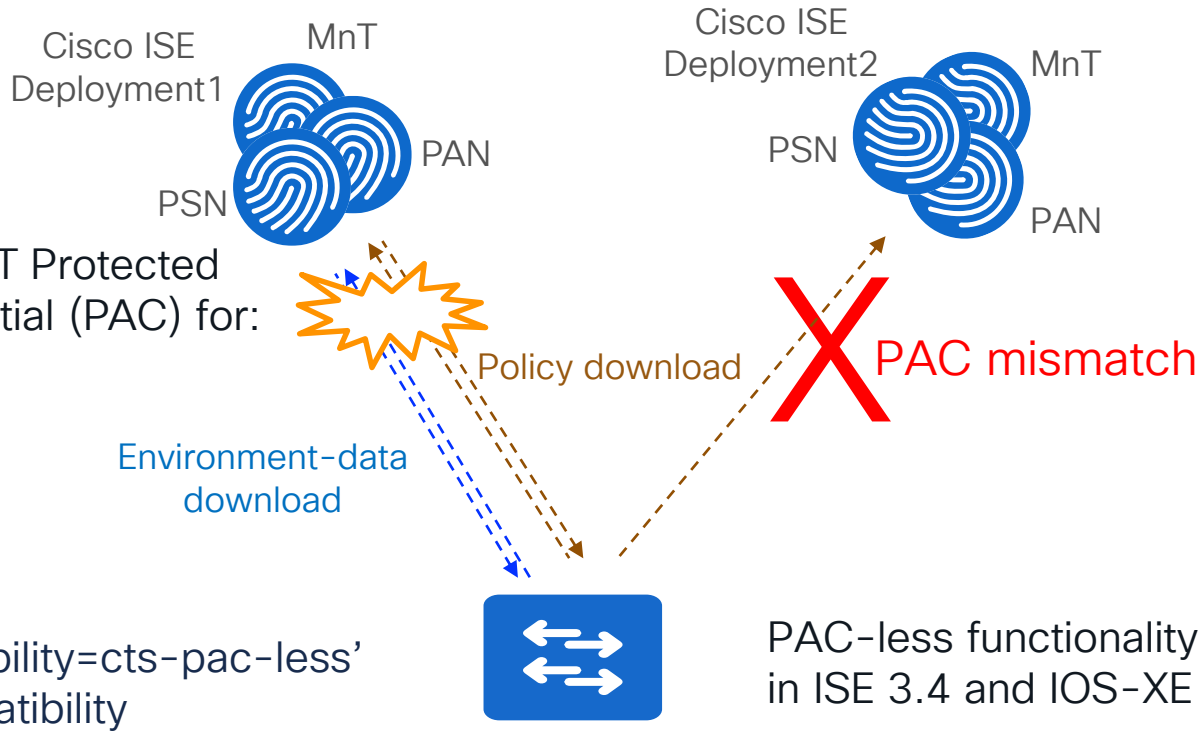


Employees SGT (4)
10.20.30.9

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

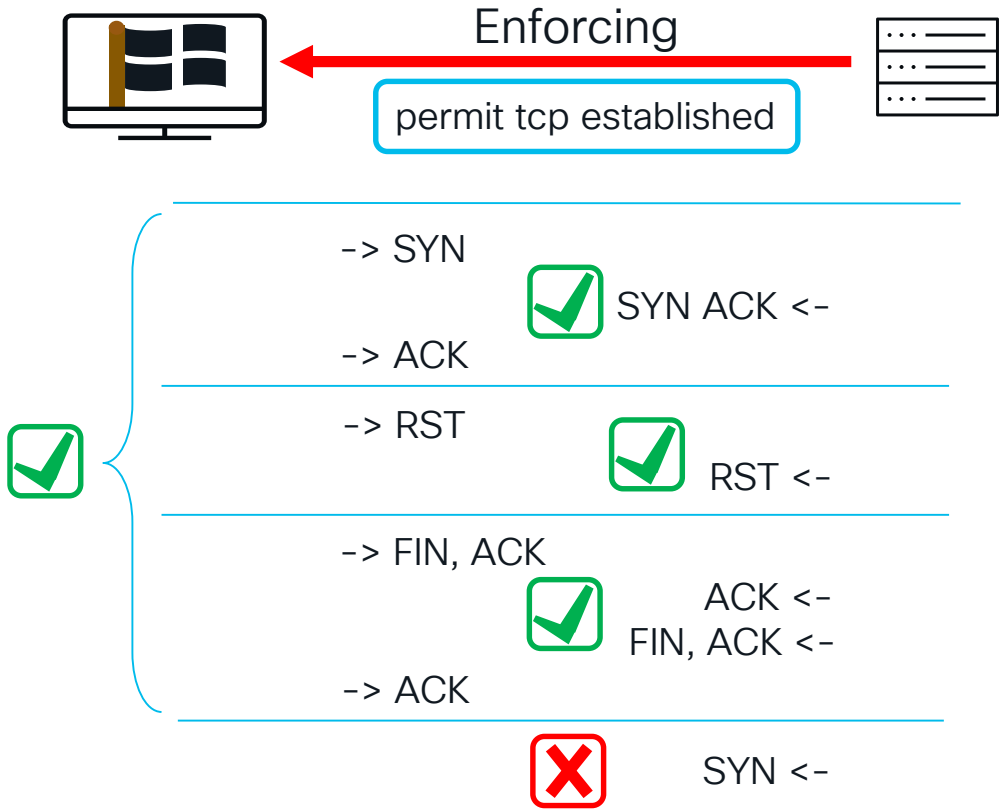
PAC-less functionality added in ISE 3.4 and IOS-XE 17.15.1

SGACL is Stateless, isn't it?

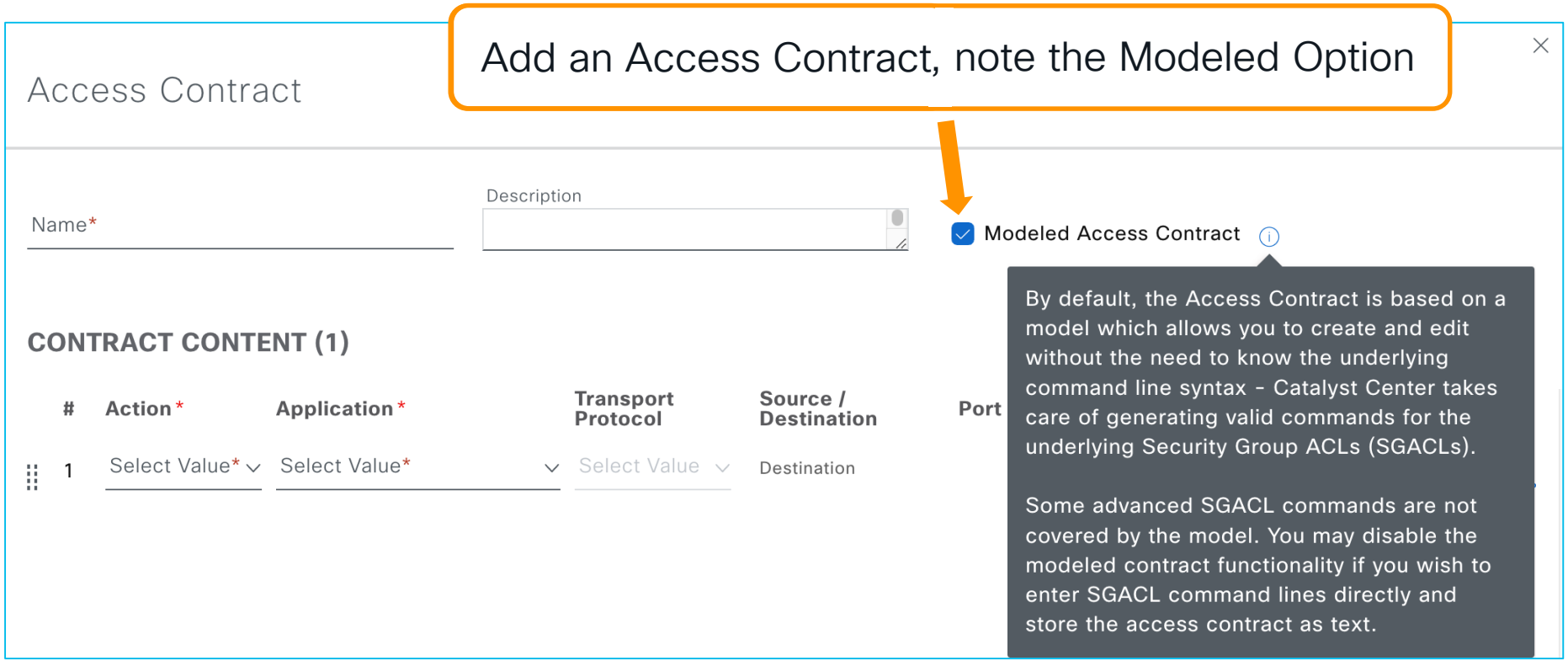
Yes, it is, but you can use the **Established** keyword:

permit tcp established

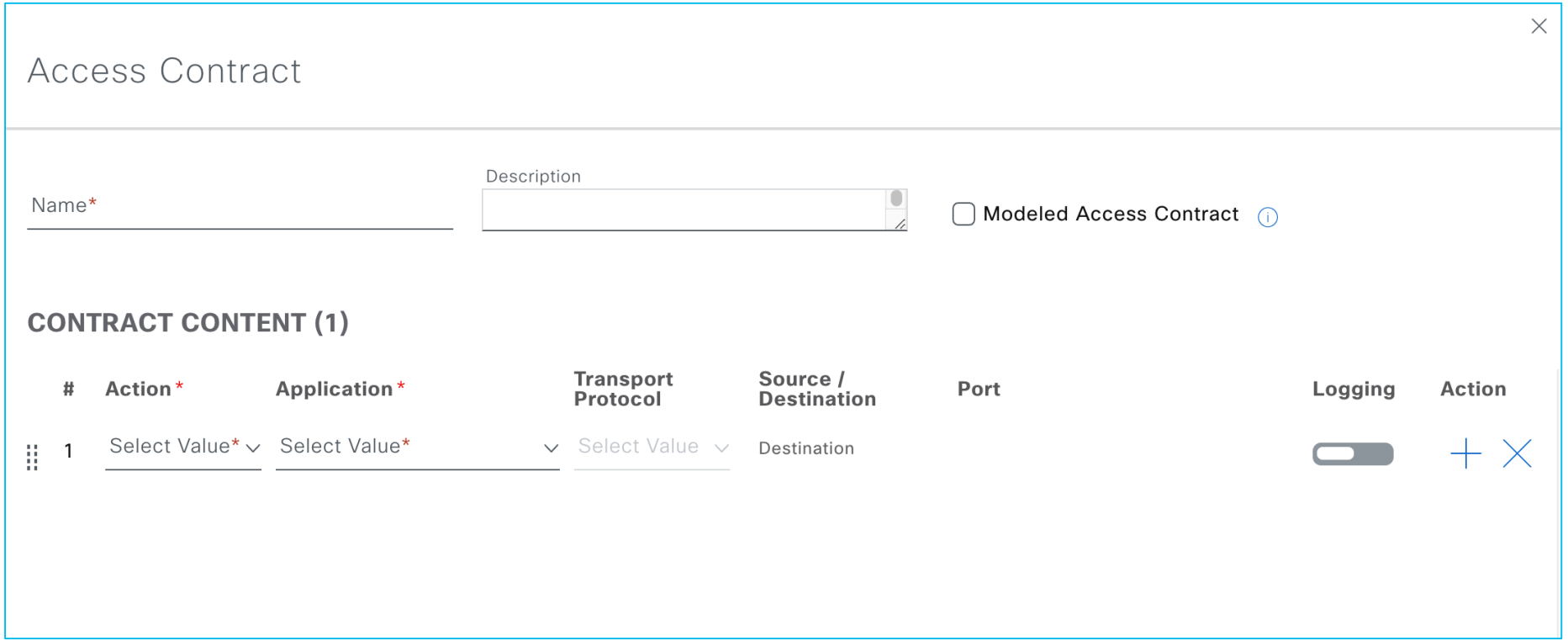
This monitors TCP flags. Act on packets with ACK or RST (communication that has been established)



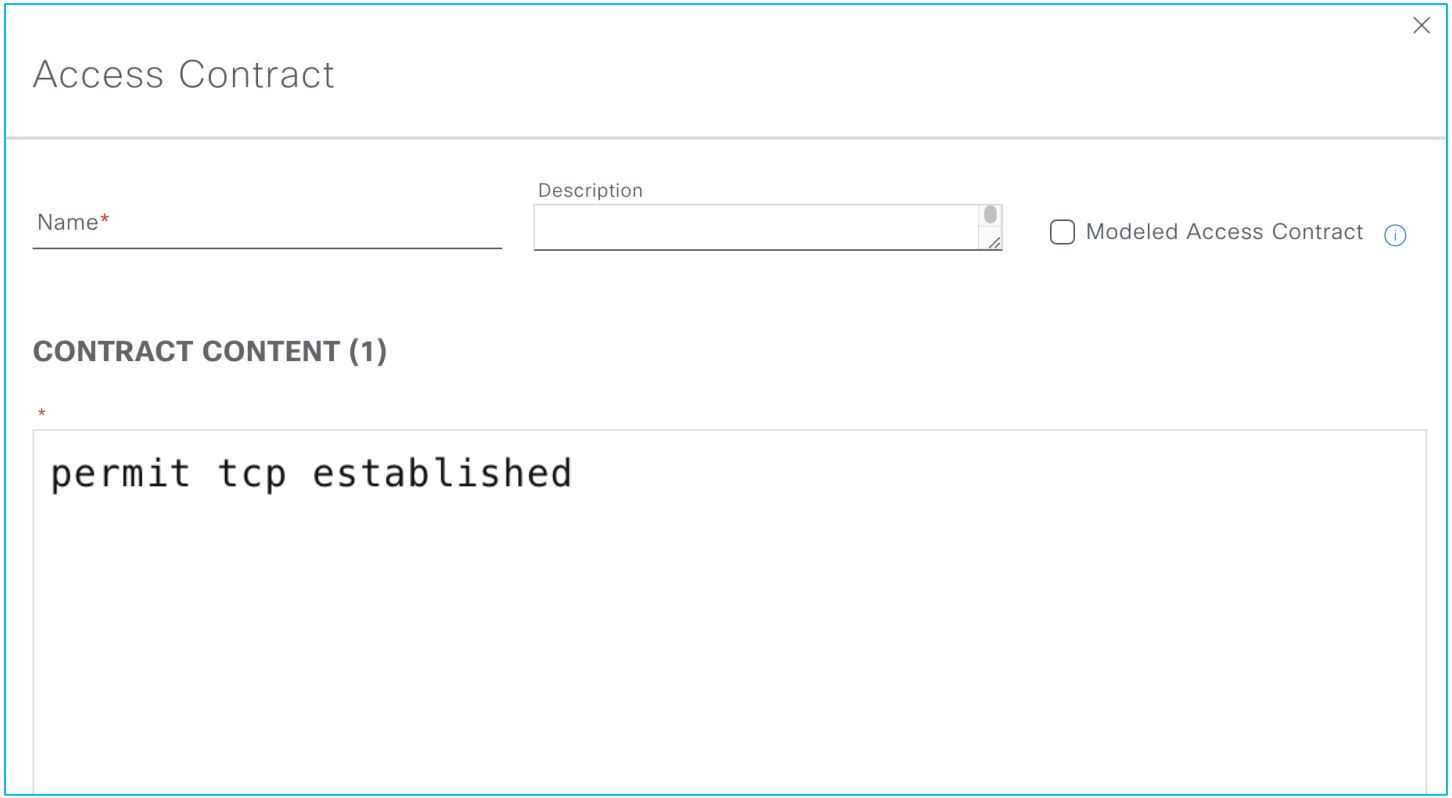
If using TCP Flags, cannot use Catalyst Center
Can You??



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

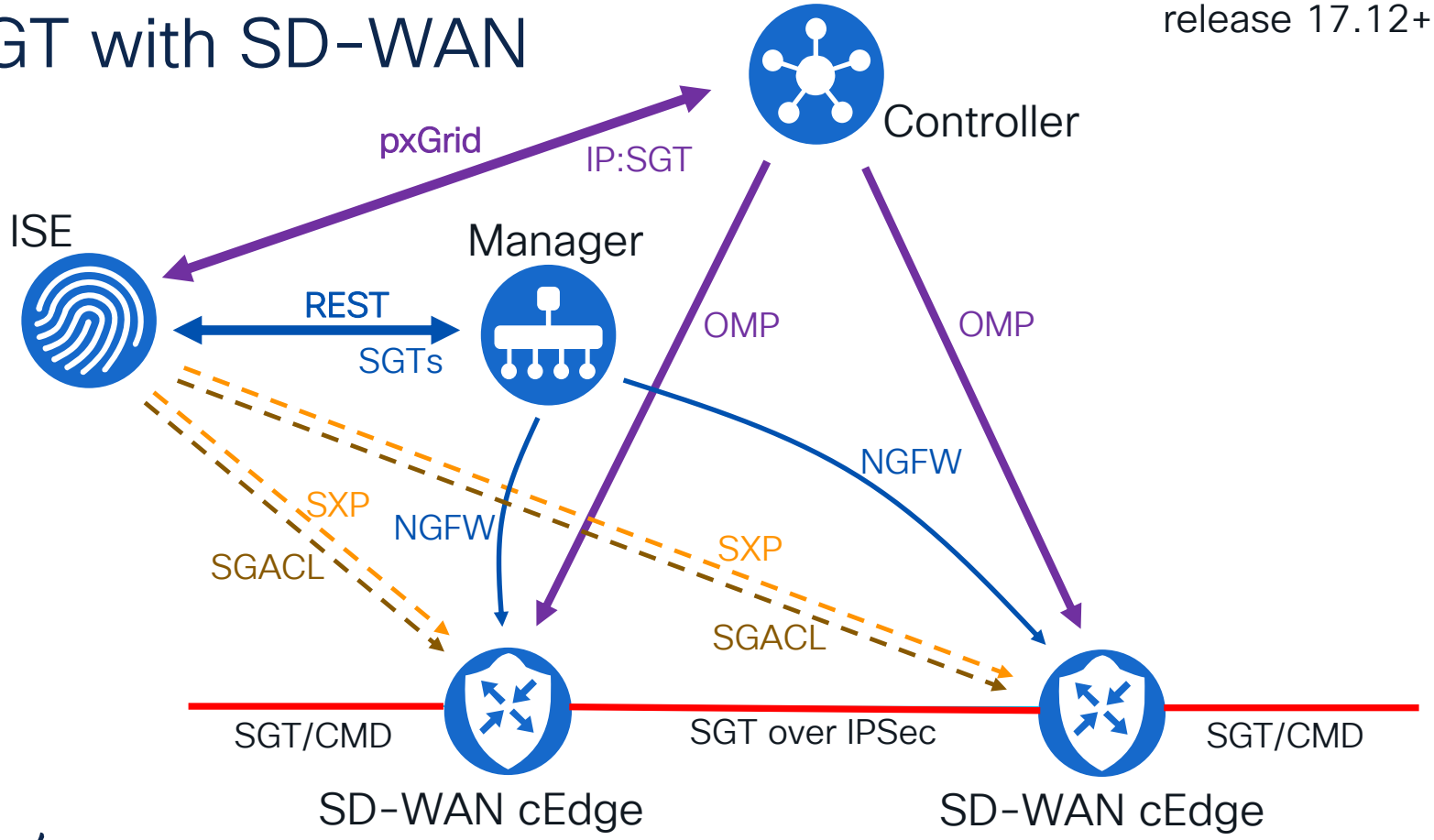


Non-Modeled Contract
Enter Text as you would in ISE



SGT with SD-WAN

Preferred software release 17.12+

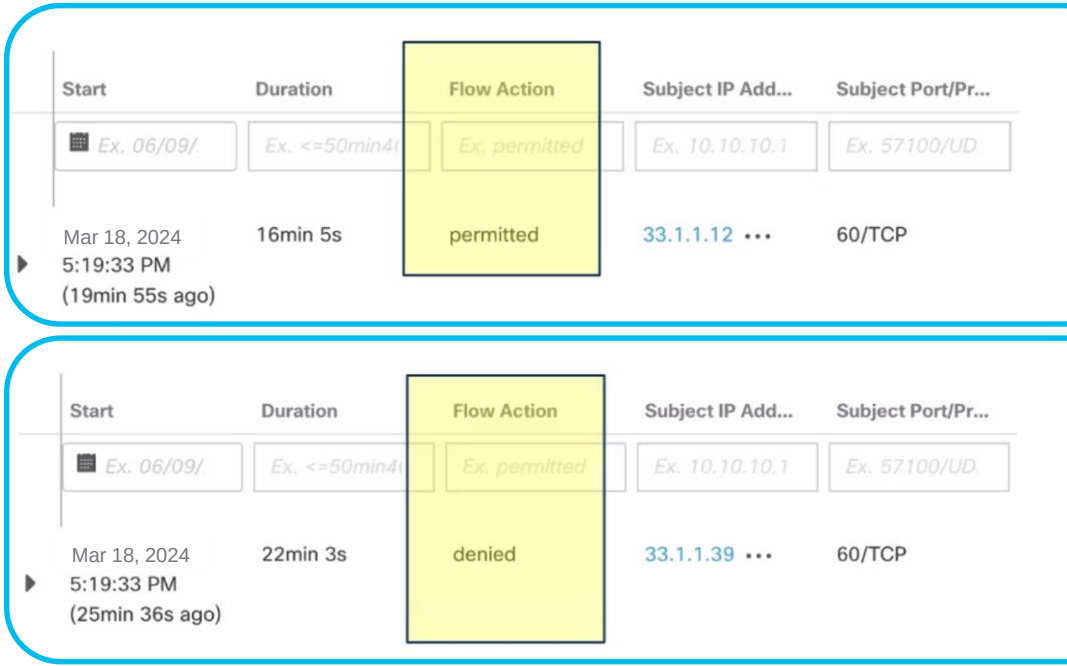


SGACL Enforcement Monitoring via NetFlow

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.

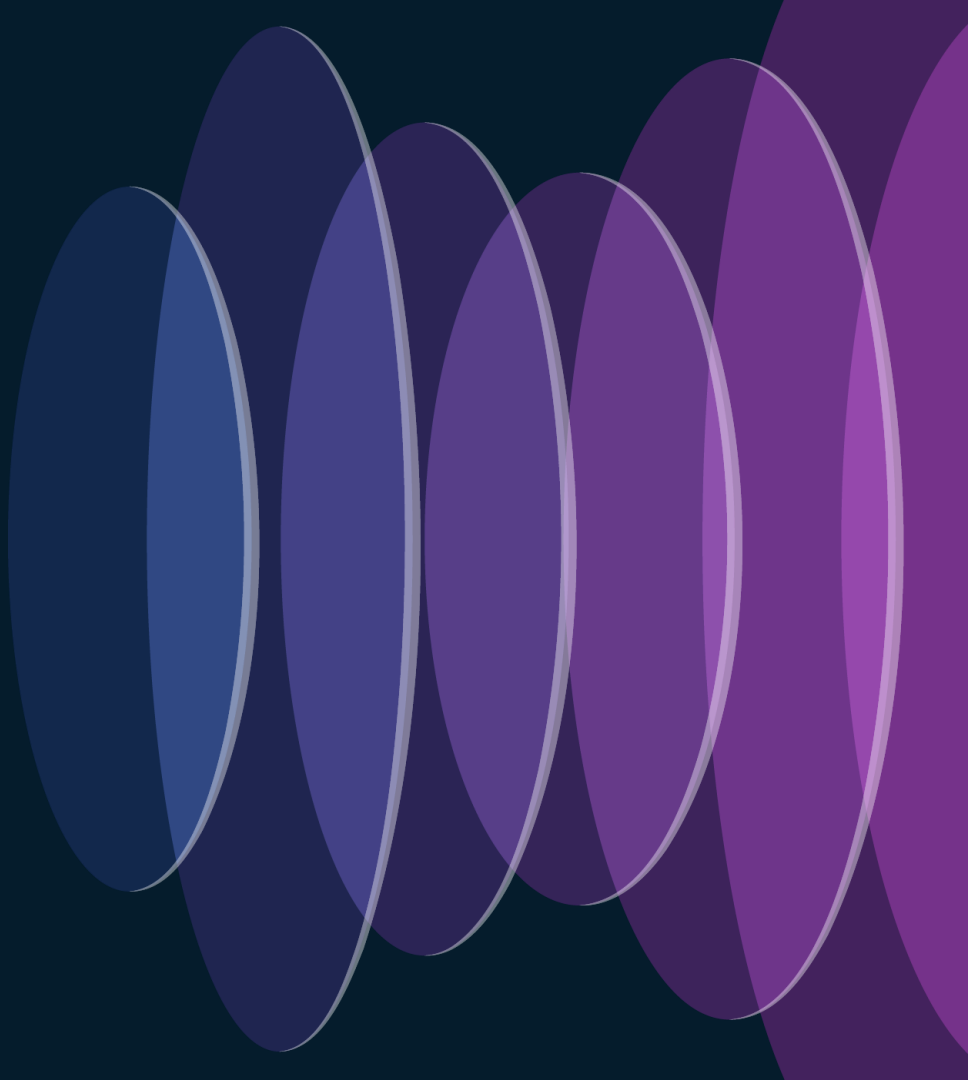
```
Flow record <record_name>
  match ipv4 version
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect policy firewall event
!
Interface G1/0/1
  ipv6 flow monitor <monitor_name> output
```

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

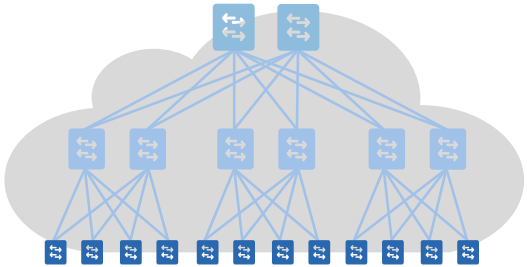
Security

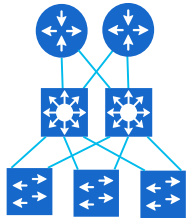
SASE/SSE

Cisco Secure Access

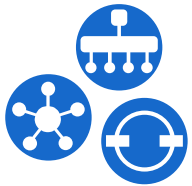
Cloud

SD-Access

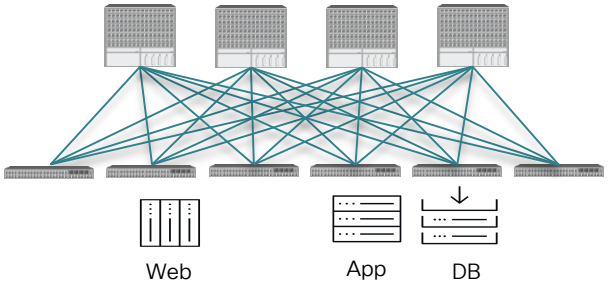




Non-Fabric



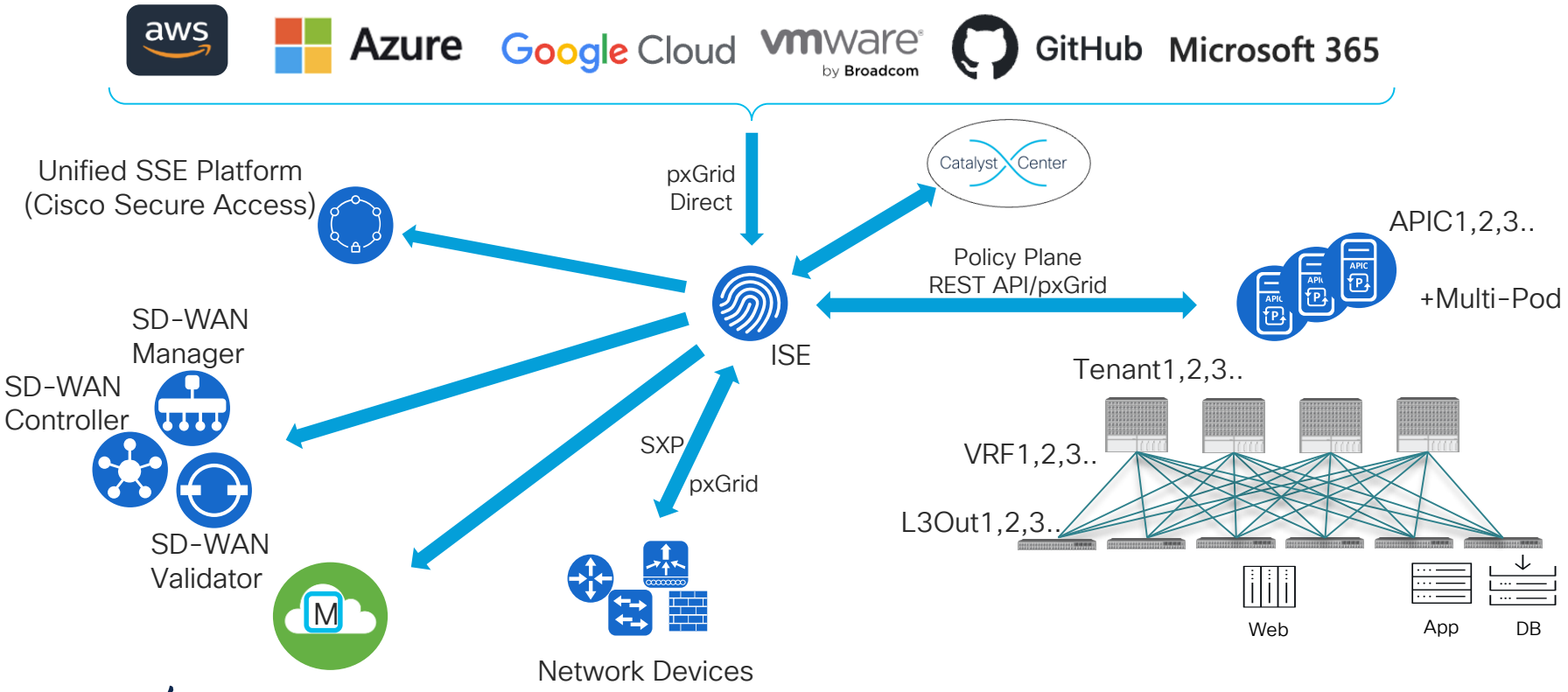
SD-WAN



Data Center / ACI

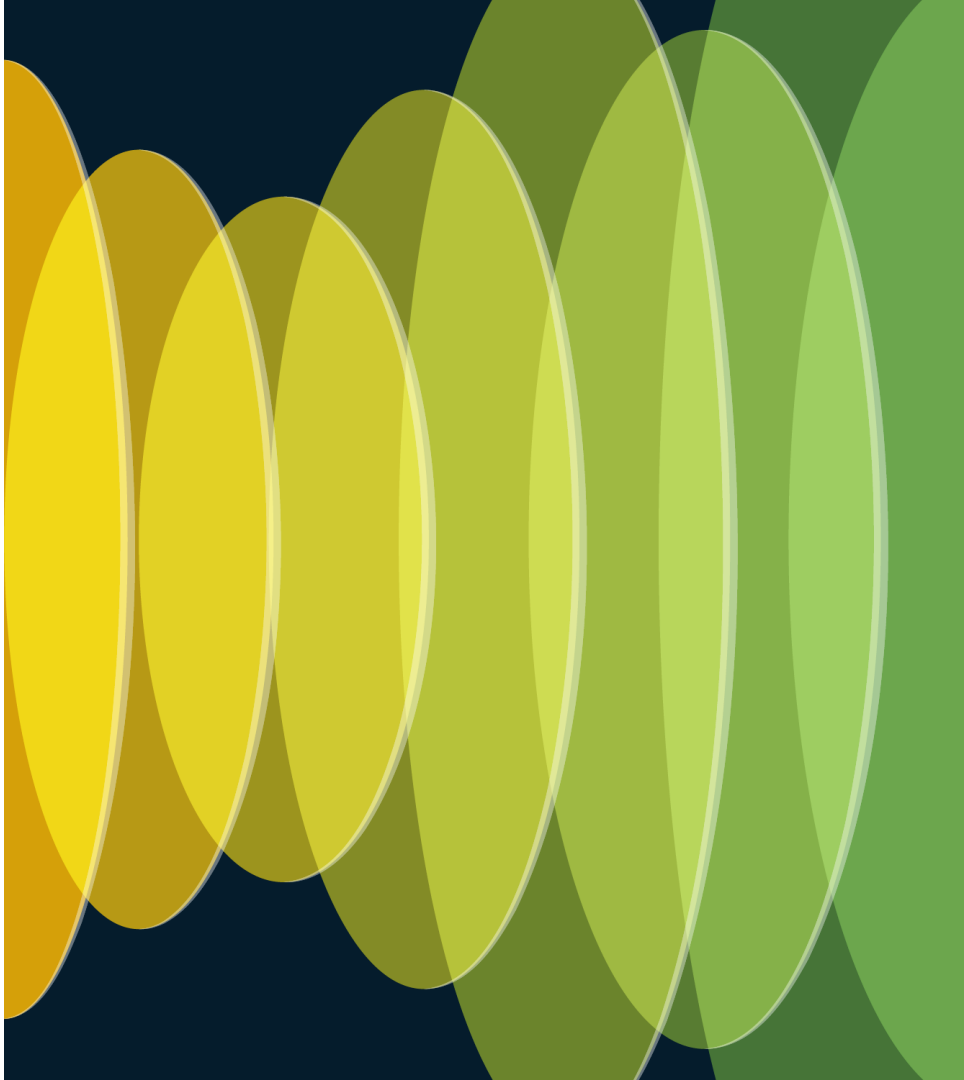
Common Policy Context Sharing

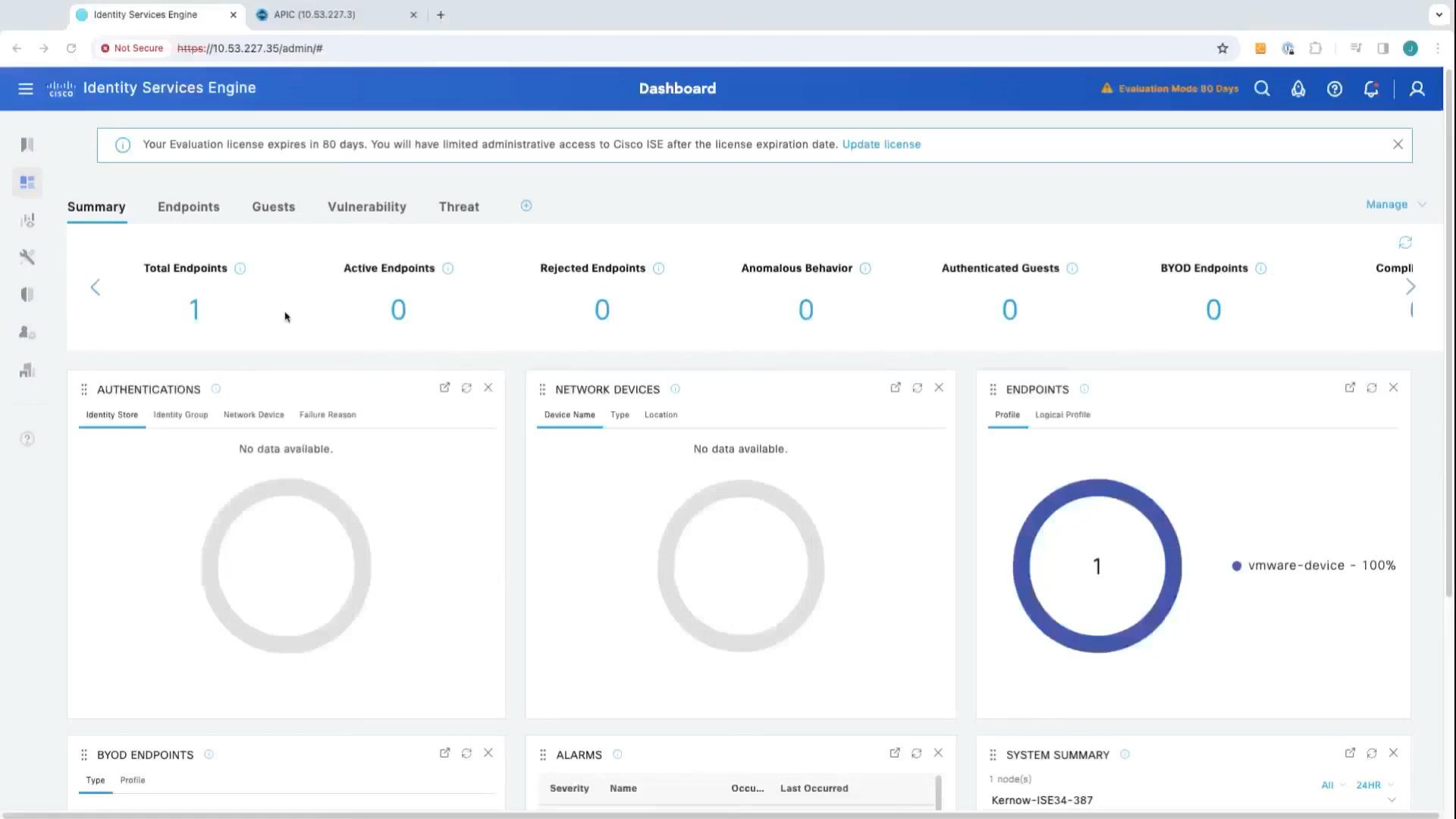
Classification
Normalization



Demo:

ISE – ACI Integration with enforcement on Campus for flows to the DC




Identity Services Engine
APIC (10.53.227.3)
Not Secure
https://10.53.227.35/admin/#
Identity Services Engine
Dashboard
Evaluation Mode 80 Days
Your Evaluation license expires in 80 days. You will have limited administrative access to Cisco ISE after the license expiration date. Update license
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
1
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
BYOD Endpoints
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
No data available.
NETWORK DEVICES
Device Name
Type
Location
No data available.
ENDPOINTS
Profile
Logical Profile
1
vmware-device - 100%
BYOD ENDPOINTS
Type
Profile
ALARMS
Severity
Name
Occu...
Last Occurred
SYSTEM SUMMARY
1 node(s)
All
24HR
Kernow-ISE34-387

Recap

- Introduction
- Classification
- Propagation
- Enforcement
- Common Policy

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

Contact me at: trustsec@cisco.com

Global Partner Solution Advisors

NEW - Fully Virtualized, SD-Access Secure Campus Lab

Virtualized SD-Access Lab

- Fully Customizable Topology with virtualized 9kv's and 8kv's
- Access on dCloud or build on your existing Data Center
- Fraction of the cost
- GPSA mentored lab buildout support available!

CTF Mission

- Experience the SD-Access Virtual Lab at Capture the Flag in The World of Solutions
- Use Cases – Fabric Sites and Virtual Network Provisioning, Fusion Automation, Extranet, Micro Segmentation, and more!

Contact

- GPSA is your source for no-cost, partner enablement and practice building!
- Visit the Global Partner Experience booth (4227) across from Capture the Flag, for more information.

Virtual SD-Access Lab on dCloud

GPSA Sales Connect Page

CTF at Cisco Live
Check out Secure Campus Section

cisco Live!

New Feature
Enhanced

Catalyst Leadership in Enterprise Networks

A Platform based Approach

Catalyst Center and Meraki Dashboard

28M Network Devices Managed

50% Y/Y

19M APs | 6M Switches | 2.5M Routers | 830M Clients

13M
Devices on Catalyst Center

15.3M
Devices on Meraki Dashboard

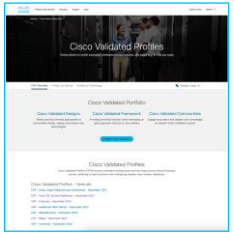
Catalyst 9000 Family

100,000+ Customers, Millions of Switches

"Catalyst 9K continues to be the fastest ramping product in the company's history"

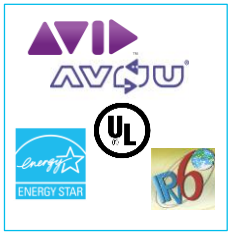
- Chuck Robbins, CEO Cisco Systems

Secure Networking	Digital Experience	Operational Simplicity
Common Policy	Campus Automation	Cloud Managed Catalyst
Secure Equipment Access	AI Endpoint Analytics	Infrastructure as a Code
SD-Access (LISP & EVPN)	Digital Experience ThousandEyes	S3 & CloudWatch Integration
High-speed Encryption	AI Ops & Assurance	Visibility, Control & Rollback

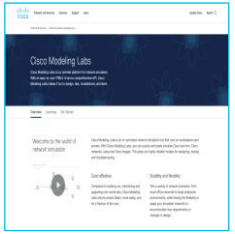


Cisco Validated Profiles (CVP)

Industry Validated Reports



Industry Certifications



Cisco Modeling Labs

cisco Live!

Cisco Live US SD-Access/ISE Learning Map

Sunday–2nd

- TECENS-2820 9AM
  Cisco Software-Defined Access LISP: Architecture Overview

Monday–3rd

- BRKENS-2810 8:30AM
  Cisco Software-Defined Access LISP Solution Fundamentals
- BRKENS-2800 9:30AM
  Cisco SD-Access Zero-Touch Provisioning Using LAN Automation
- BRKENS-2811 1PM
  Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation
- LTRENS-2419 1PM
  SD-Access LISP Pub/Sub Wired Lab
- BRKENS-2816 3PM
  Cisco SD-Access Transit: Advanced Design Principles
- BRKSEC-2100 10:30AM
  ISE Your Meraki Network with Group Based Adaptive Policy
- BRKENS-1802 2:30PM
  SD-Access Success Stories: Concept to Reality by Petrobras and Ford Motor
- BRKSEC-2091 3PM
  Cisco ISE Performance, Scalability and Best Practices
- BRKENS-1852 4PM
  TrustSec Refresh Reinforced with Latest Segmentation Innovations

Tuesday–4th

- BRKENS-2502 10:30AM
  Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment
- BRKENS-1801 4PM
  SD-Access Success Stories: Concept to Reality by Stanford Health and Yale University

Wednesday–5th

- BRKENS-2833 10:30AM
  LISP: Optimized Control Plane for Software-Defined Access
- BRKENS-2819 2:30PM
  Cisco SD-Access and Multi-Domain Segmentation
- CIUG-1003 2:30PM
  Zero Trust with Software-Defined Access Roadmap Update
- BRKENS-2821 4:00PM
  Cisco SD-Access LISP VXLAN Fabric for Manufacturing Verticals

Thursday–6th

- BRKENS-2827 11:00AM
  Cisco SD-Access Migration Tools and Strategies

Catalyst Center

Cisco SD-Access LISP

ISE

Cisco ISE

BU-led sessions

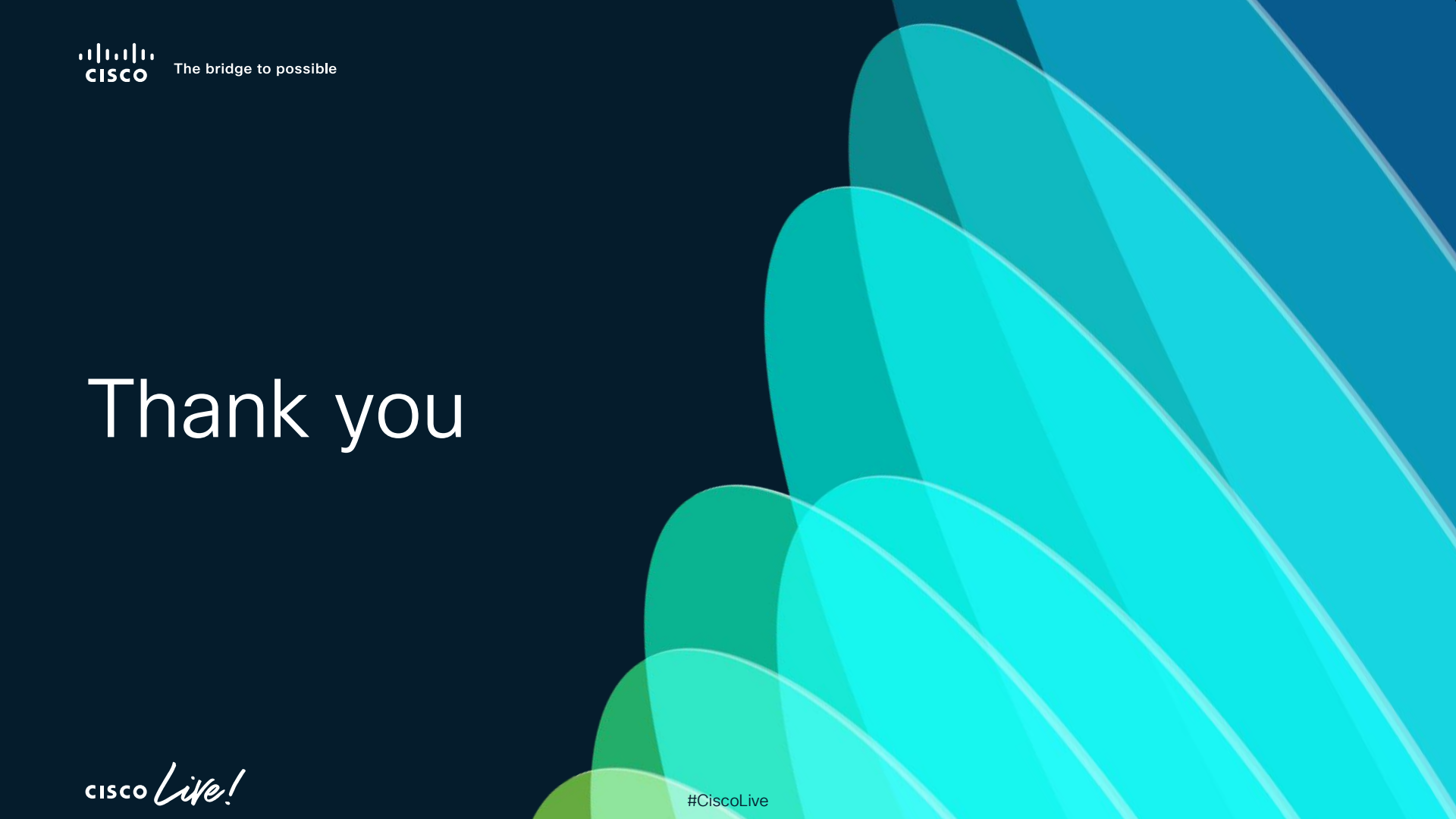
Complete Your Session Evaluations

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 2025.

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.**


The bridge to possible
Thank you
cisco Live!
#CiscoLive