You make **possible**

Advanced Security Group Tags (SGT)

The Detailed Walk Through

Darrin Miller, DTME

BRKSEC-3690

Barcelona | January 27-31, 2020

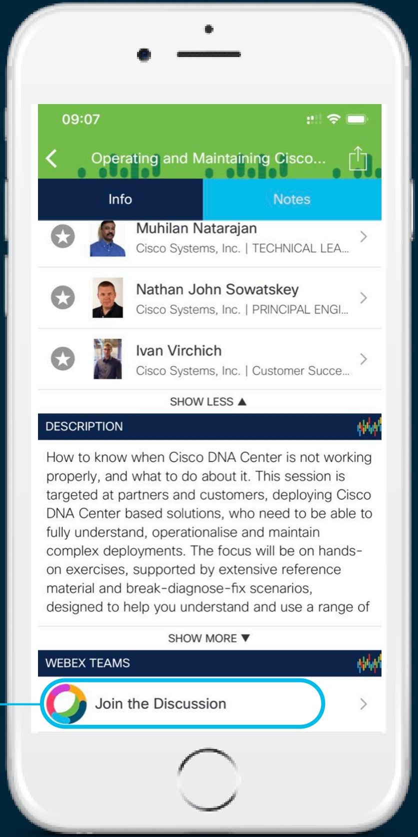
Cisco Webex Teams

Questions?

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

How

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



Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

About Me

Darrin Miller

- Security focused Technical Marketing Engineer
- Focused on 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

Clarification: That is “my” beer. It was placed in front of me. In addition I paid for the dinner where the accuser made this picture. ☺

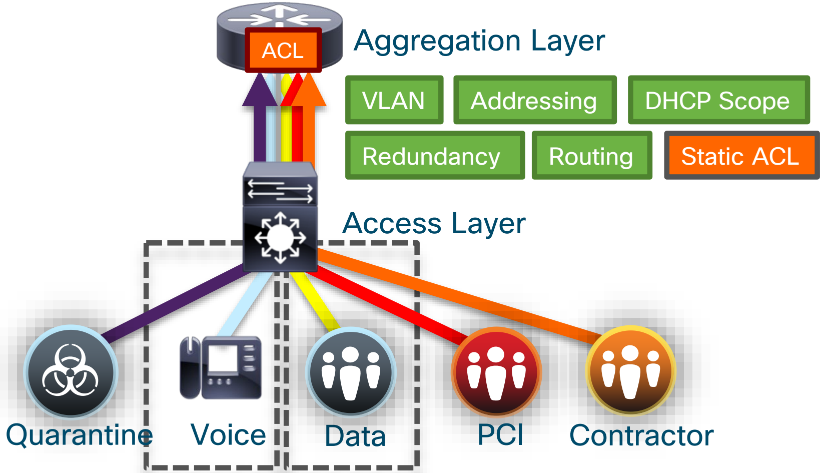
Accuser

Agenda

- Security/Scalable Group Tag (SGT) Review
- Use Case Reviews with Design Considerations
  - Campus
    - WLAN
    - Software Defined Access (SD-Access) – SGT/VXLAN
    - Firewall Integration with SD-Access
    - Meraki/3rd party interop
  - WAN
    - SXP WAN design
    - SGT over WAN
  - Data Center
    - SGT/ACI
    - Cloud
- Summary

Traditional Segmentation

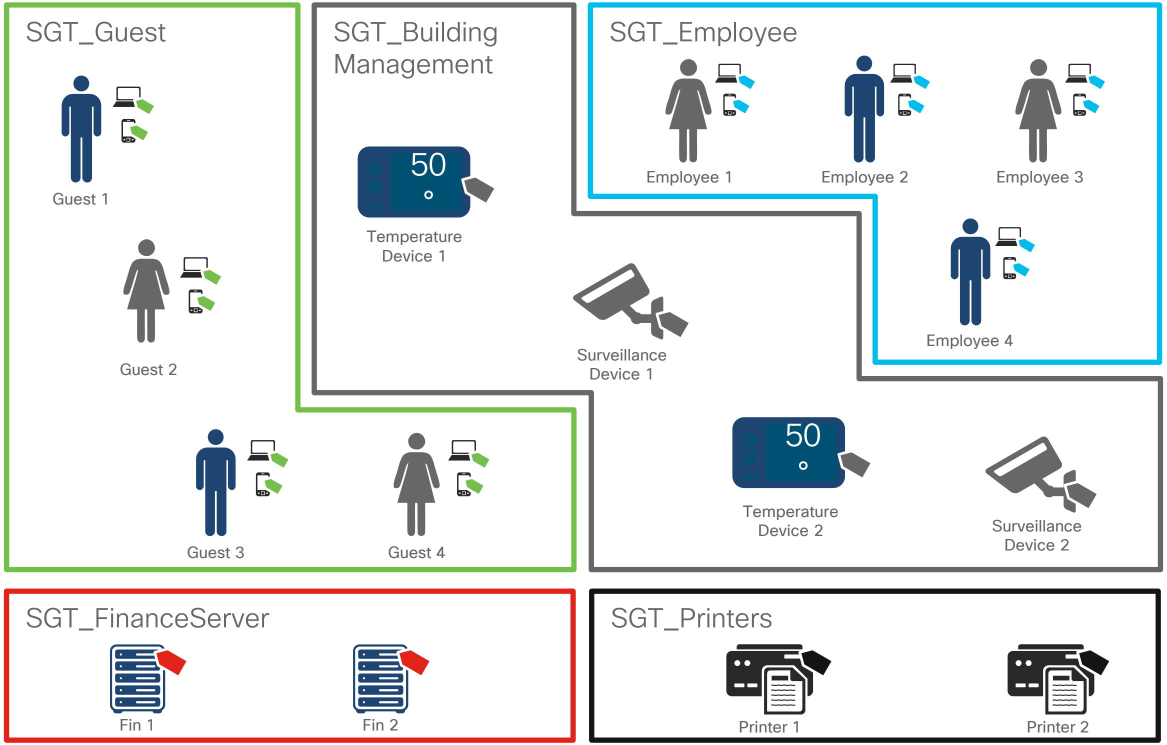
Design needs to be replicated for floors, buildings, offices, and other facilities. Cost could be extremely high



Simple Segmentation with 2 VLANs
More Policies using more VLANs

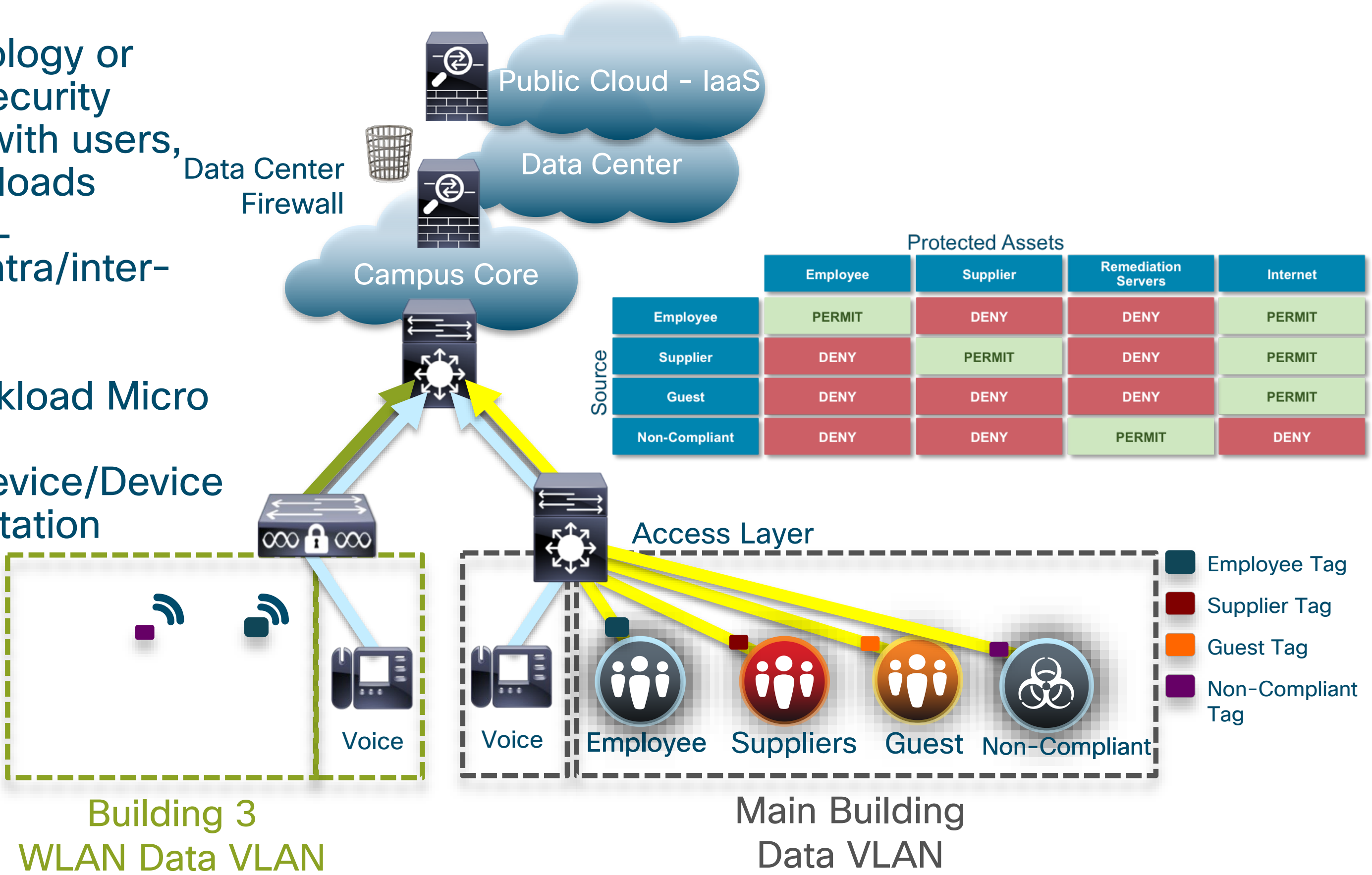
Groups Denote Common Roles and Policy

- Business-based groupings to provide consistent policy and access independent of network topology
- Leverage attributes such as user role, location, and device type to define group assignments



Example: User to Application Access Control

- Regardless of topology or location, policy (Security Group Tag) stays with users, Devices, and workloads
- SGT simplifies ACL management for intra/inter-VLAN traffic
- Other Use Cases
  - Workload/Workload Micro segmentation
  - User/User – Device/Device Micro Segmentation
  - Hybrid Cloud

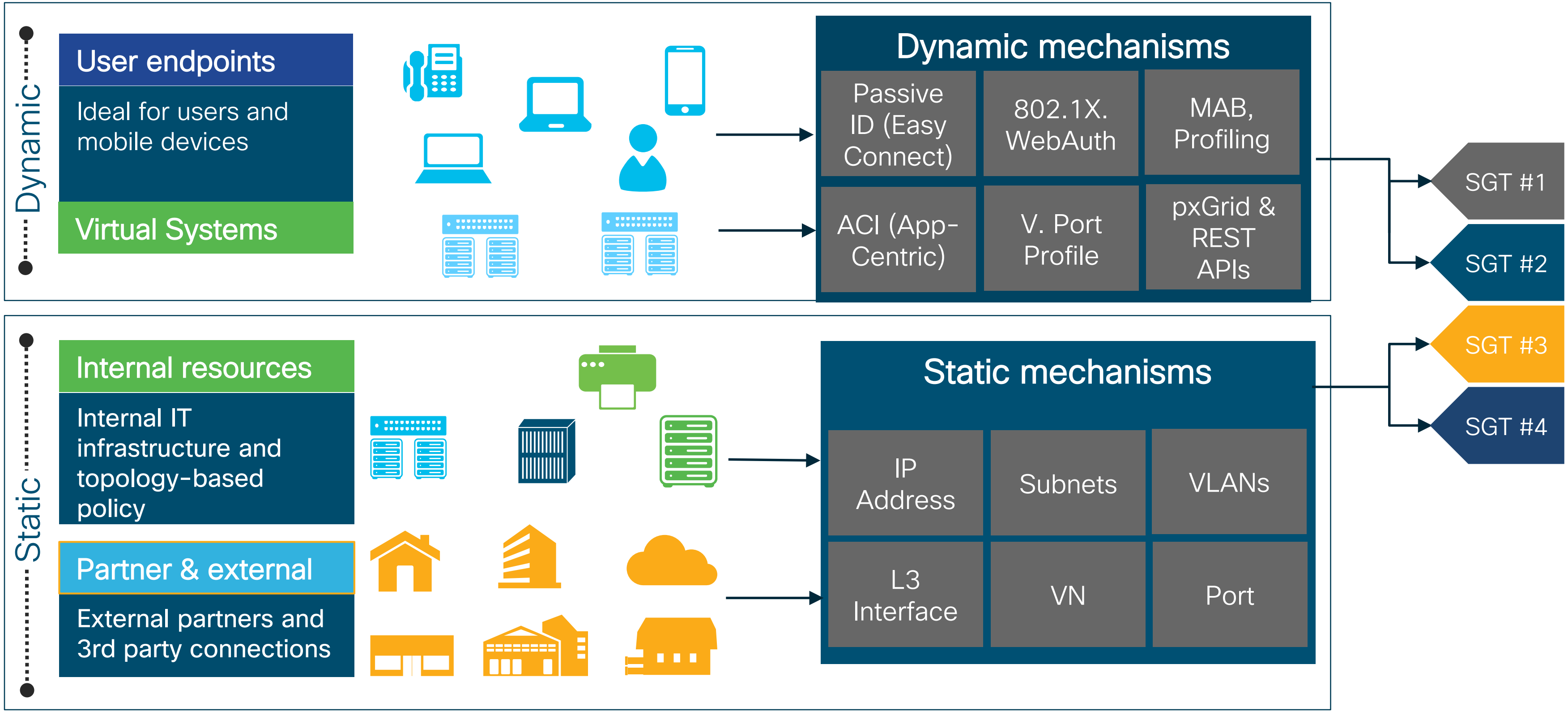


Protected Assets

Source

	Employee	Supplier	Remediation Servers	Internet
Employee	PERMIT	DENY	DENY	PERMIT
Supplier	DENY	PERMIT	DENY	PERMIT
Guest	DENY	DENY	DENY	PERMIT
Non-Compliant	DENY	DENY	PERMIT	DENY

Classification Methods



Dynamic

User endpoints

Ideal for users and mobile devices

Virtual Systems

Dynamic mechanisms

Passive ID (Easy Connect)	802.1X. WebAuth	MAB, Profiling
ACI (App-Centric)	V. Port Profile	pxGrid & REST APIs

Static

Internal resources

Internal IT infrastructure and topology-based policy

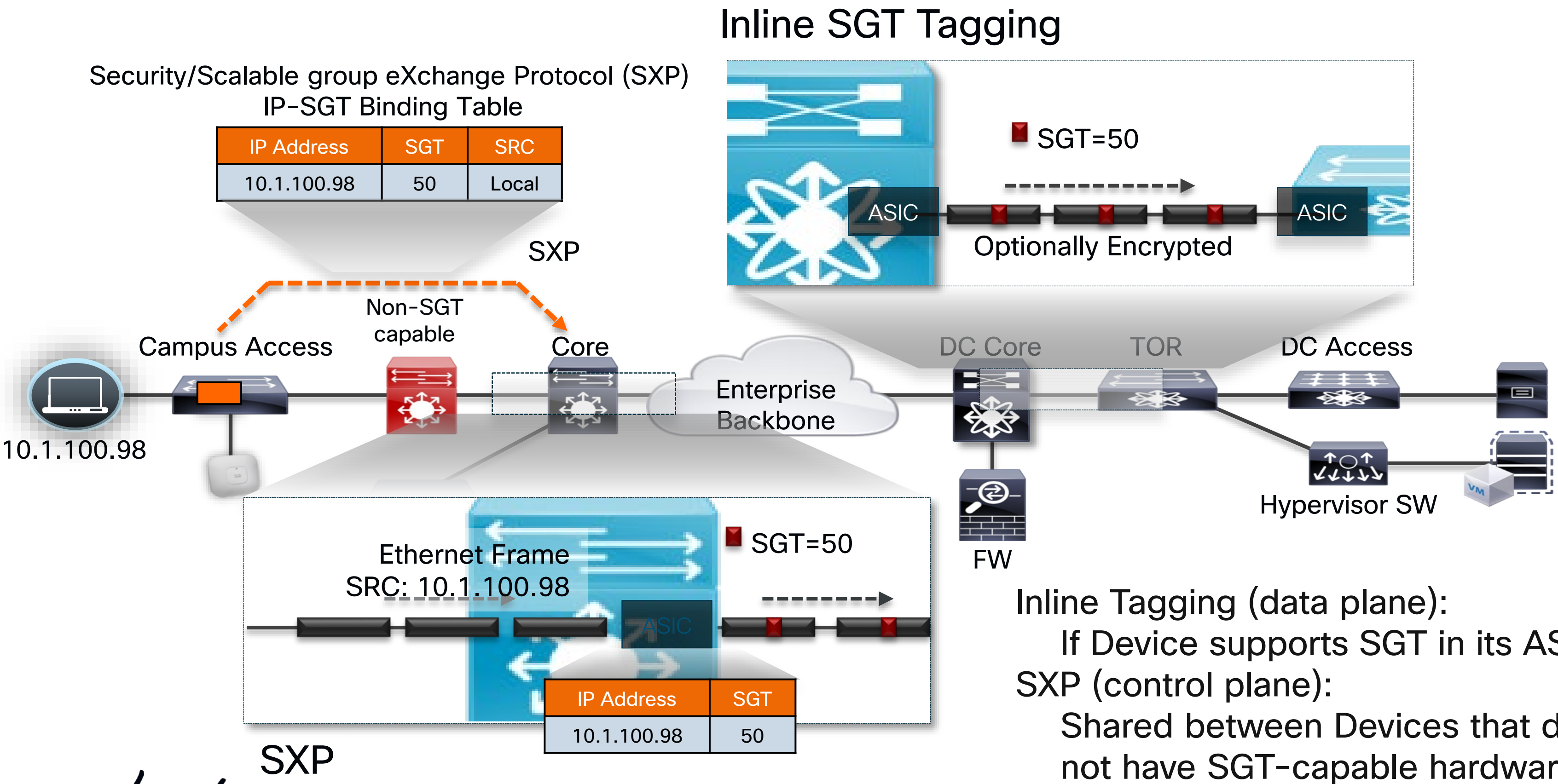
Partner & external

External partners and 3rd party connections

Static mechanisms

IP Address	Subnets	VLANs
L3 Interface	VN	Port

SGT Transport Mechanism



Security/Scalable group eXchange Protocol (SXP)
IP-SGT Binding Table

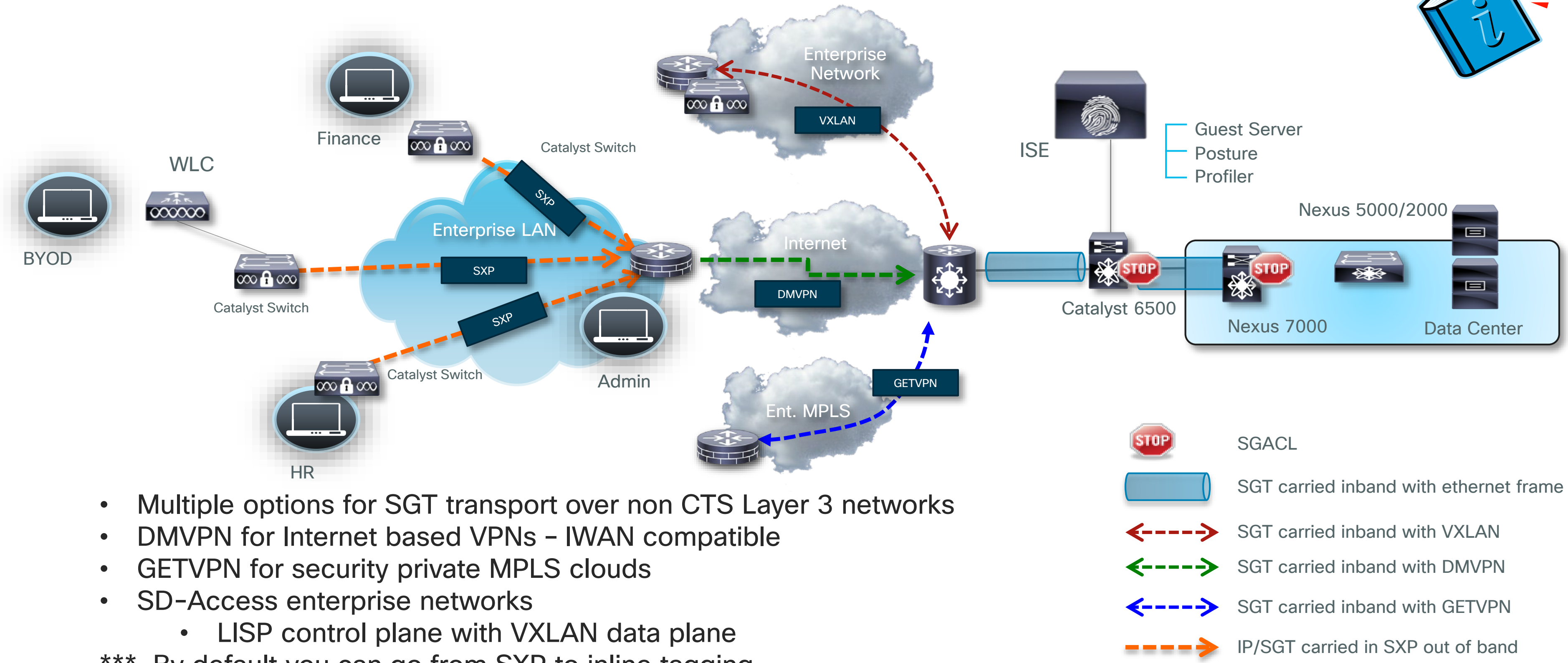
IP Address	SGT	SRC
10.1.100.98	50	Local

IP Address	SGT
10.1.100.98	50

Inline Tagging (data plane):
- If Device supports SGT in its ASIC

SXP (control plane):
- Shared between Devices that do not have SGT-capable hardware

SGT Transport over L3 networks

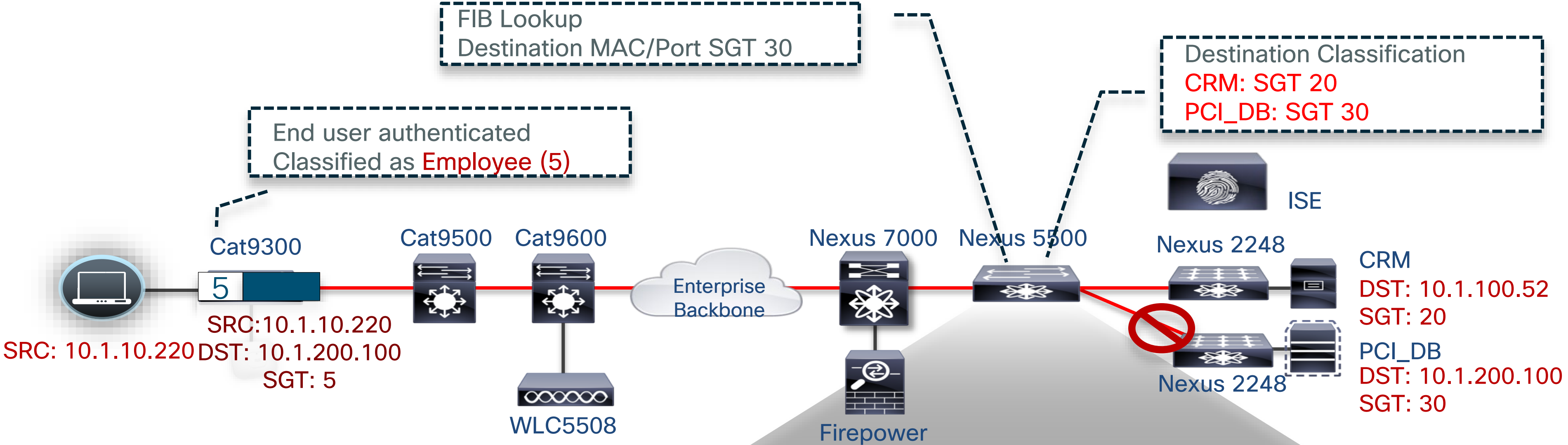


- Multiple options for SGT transport over non CTS Layer 3 networks
- DMVPN for Internet based VPNs – IWAN compatible
- GETVPN for security private MPLS clouds
- SD-Access enterprise networks
  - LISP control plane with VXLAN data plane

*** By default you can go from SXP to inline tagging

*** To go inline tagging to SXP you must use SGT caching

End-to-end SGT Tagging

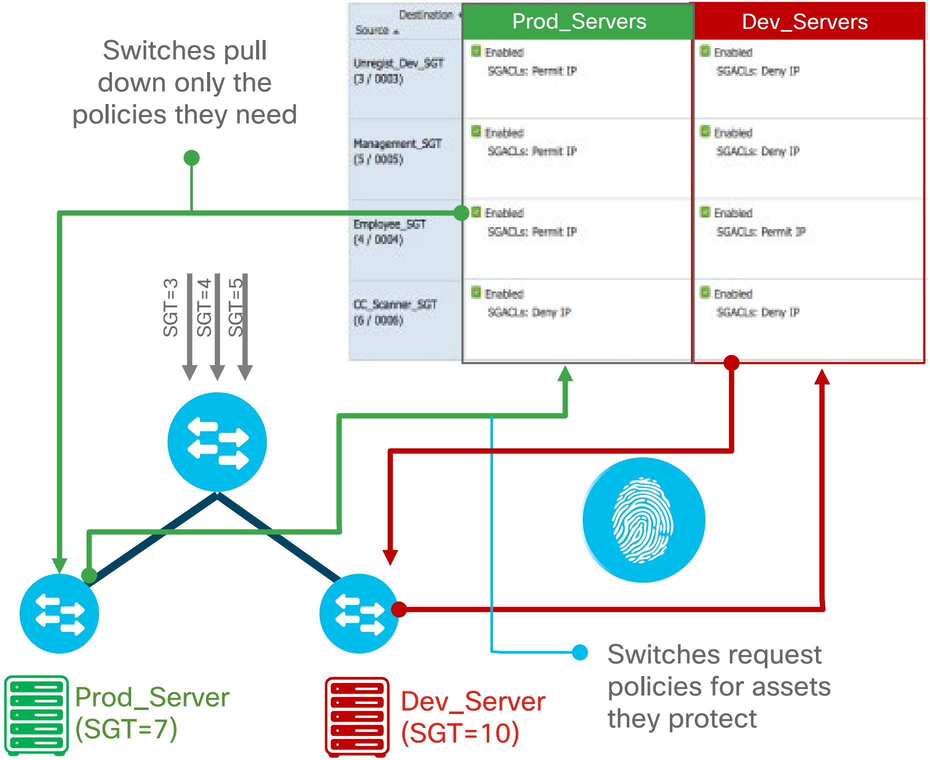


SGT Tagging

SRC\DST	CRM (20)	PCI_DB (30)
Employee (5)	SGACL-A	Deny
BYOD (7)	Deny	Deny

Dynamic Security Group ACL (SGACL) Downloads

- New User/Device/Server provisioned
- Switch requests policies for assets they protect
- Policies downloaded & applied dynamically
- Result: Software-Defined Segmentation
  - All controls centrally managed
  - Security policies de-coupled from network topology
  - No switch-specific security configs needed
  - One place to audit network-wide policies



Destination Source	Prod_Servers	Dev_Servers
Unregist_Dev_SGT (3 / 0003)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Deny IP
Management_SGT (5 / 0005)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Deny IP
Employee_SGT (4 / 0004)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Permit IP
CC_Scanner_SGT (6 / 0006)	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: Deny IP

Switches pull down only the policies they need

Switches request policies for assets they protect

Open Implementations

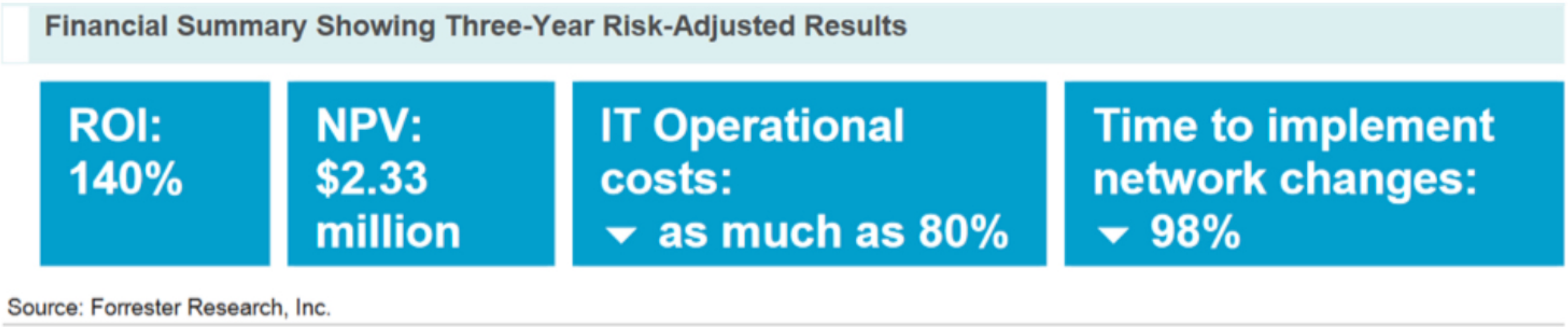
- 3rd parties support SGTs vis pxGrid – IETF proposal for Security Automation and Continuous Monitoring (SACM) – Checkpoint amongst others
- SXP published as an Informational Draft to the IETF, based on customer requests – shipping partner implementations
- Open Source SXP Implementations – Java in OpenDaylight, C on github.com
- Includes the Cisco Meta Data (CMD) format for inclusion of the SGT with Ethernet frames (detailed on the next slides)
  - https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/

Why is this Interesting? – Making “Intent” Real

- There are other management/orchestration offerings that take in IP/object definitions and render them as IP ACLs to the firewall/enforcement point
- The IP ACL does not describe the “intent” of the policy in the device or in the telemetry (logging, etc.) produced by the device
- As we will see in the upcoming sections SGT/SGACLs i.e. actually carry the “intent” and puts that “intent” into the following
  - Policy Definition – ISE
  - Policy on the enforcement point - SGACL on switches, routers, wireless, firewalls
  - Policy in the logging/telemetry analysis – netflow, syslog
- This is done in a dynamic, simple, open, and automated
- All of this results in the following (next slide)

Forrester: The Total Economic Impact of SGTs

Forrester Consulting recently conducted an analysis of customers using TrustSec software-defined segmentation in production networks and deduced the following:



Financial Summary Showing Three-Year Risk-Adjusted Results

ROI: 140%

NPV: $2.33 million

IT Operational costs: ▼ as much as 80%

Time to implement network changes: ▼ 98%

Source: Forrester Research, Inc.

Use Case Reviews with Design Considerations

Use Case - Campus

SGT/SGACL Supported Platforms

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

Classification

Catalyst 2960-S/-SF/-C/-CX/-Plus/-X/-XR
Catalyst 3560-E/-C/-X/-CX/-CG
Catalyst 3750-E/-X
Catalyst 3650, 3850, 3850-XS
Catalyst 4500E (Sup6-E, 6L-E)
Catalyst 4500E (Sup 7-E, 7L-E, 8-E, 8L-E)
Catalyst 4500-X
Catalyst 6500E (Sup720/2T)
Catalyst 6800
WLC 2500/5500/WiSM2/Flex7500
WLC 5760
WLC 8510/8540
Nexus 7000
Nexus 6000/5600
Nexus 5500/2200
Nexus 1000v
ISRG2, ISR4000, ISRv
ASR1000,1000-X; CSR 1000v
IE2000/2000U/3000/4000/5000
CGR 2010, CGS2500
ASA 5500, ASAv, FP4100/9300, ISA 3000
ISE
Catalyst 9K

Propagation

Catalyst 2960-S/-SF/-C/-CX/-Plus/-X/-XR
Catalyst 3560-E/-C/-X/-CX/-CG
Catalyst 3750-E/-X
Catalyst 3650, 3850, 3850-XS
Catalyst 4500E (Sup6-E, 6L-E)
Catalyst 4500E (Sup 7-E, 7L-E, 8-E, 8L-E)
Catalyst 4500-X
Catalyst 6500E (Sup720/2T)
Catalyst 6800
WLC 2500/5500/WiSM2/Flex7500
WLC 5760
WLC 8510/8540
Nexus 7000
Nexus 6000/5600
Nexus 5500/2200
Nexus 1000v
ISRG2, ISR4000, ISRv
ASR1000,1000-X; CSR 1000v
IE2000/2000U/3000/4000/5000
CGR 2010, CGS2500
ASA 5500, ASAv, FP4100/9300, ISA 3000
FP 7000/8000; ISE
Catalyst 9K

Enforcement

Catalyst 3560-X/-CX
Catalyst 3750-E/-X
Catalyst 3650, 3850, 3850-XS

Catalyst 4500E (Sup 7-E, 7L-E, 8-E, 8L-E)
Catalyst 4500-X
Catalyst 6500E (Sup 2T)
Catalyst 6800

WLC 8540/5520

Nexus 7000
Nexus 6000/5600
Nexus 5500/2200
Nexus 1000v
ISRG2, ISR4000, ISRv
ASR1000,1000-X; CSR 1000v
IE4000/5000
CGR 2010
ASA 5500, ASAv, FP4100/9300, ISA 3000
Web Security Appliance
Catalyst 9K

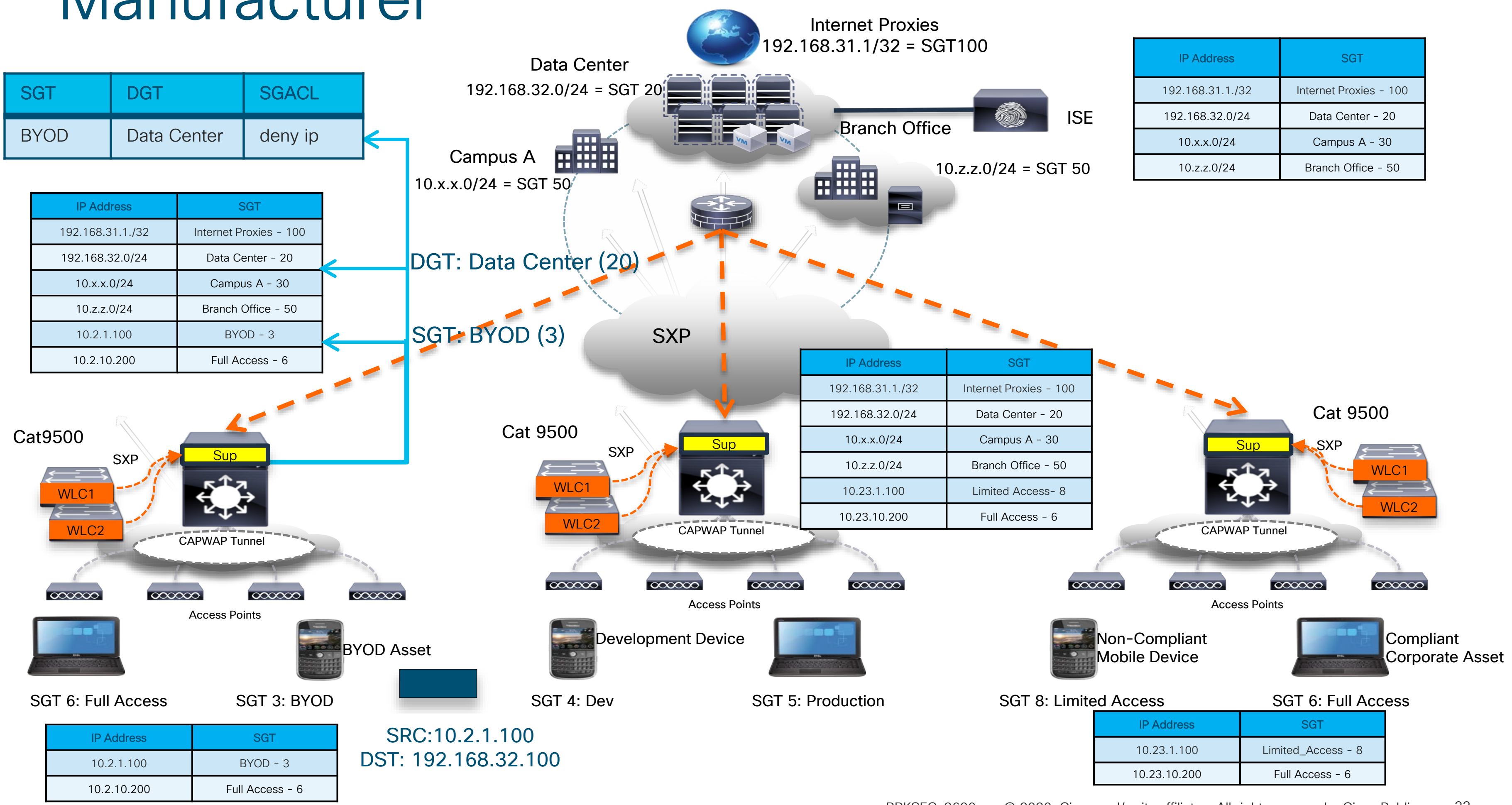
Use Case Review - Campus

Campus Access Control

- Business Problem/Background
  - BYOD assets require restricted access to Corp. network and Internet proxies
  - Production vs. Development Users on Corp. WLAN
  - Compliant vs. Noncompliant Users on Corp. WLAN
  - Centralized compulsory tunneling caused application performance degradation
  - Scaling Decentralized access control – platform, opex, capex
- Solution Overview
  - Use of SXP to communicate IP/SGT of all classes of users above to upstream SGACL switch
  - Use subnet/SGT and IP/SGT definitions published to distributed SGACL switches via SXP, ISE push, or CLI
  - Upstream SGACL switch derives SGT/DGT matches from SXP, ISE 1.3, or CLI.
  - Example - Reduced IOS ACE from approx. 1500 lines to one ACE
    - permit tcp dst eq 443

Manufacturer

Use Case - Campus



SGT	DGT	SGACL
BYOD	Data Center	deny ip

IP Address	SGT
192.168.31.1./32	Internet Proxies - 100
192.168.32.0/24	Data Center - 20
10.x.x.0/24	Campus A - 30
10.z.z.0/24	Branch Office - 50
10.2.1.100	BYOD - 3
10.2.10.200	Full Access - 6

IP Address	SGT
192.168.31.1./32	Internet Proxies - 100
192.168.32.0/24	Data Center - 20
10.x.x.0/24	Campus A - 30
10.z.z.0/24	Branch Office - 50

IP Address	SGT
192.168.31.1./32	Internet Proxies - 100
192.168.32.0/24	Data Center - 20
10.x.x.0/24	Campus A - 30
10.z.z.0/24	Branch Office - 50
10.23.1.100	Limited Access- 8
10.23.10.200	Full Access - 6

IP Address	SGT
10.2.1.100	BYOD - 3
10.2.10.200	Full Access - 6

SRC:10.2.1.100
DST: 192.168.32.100

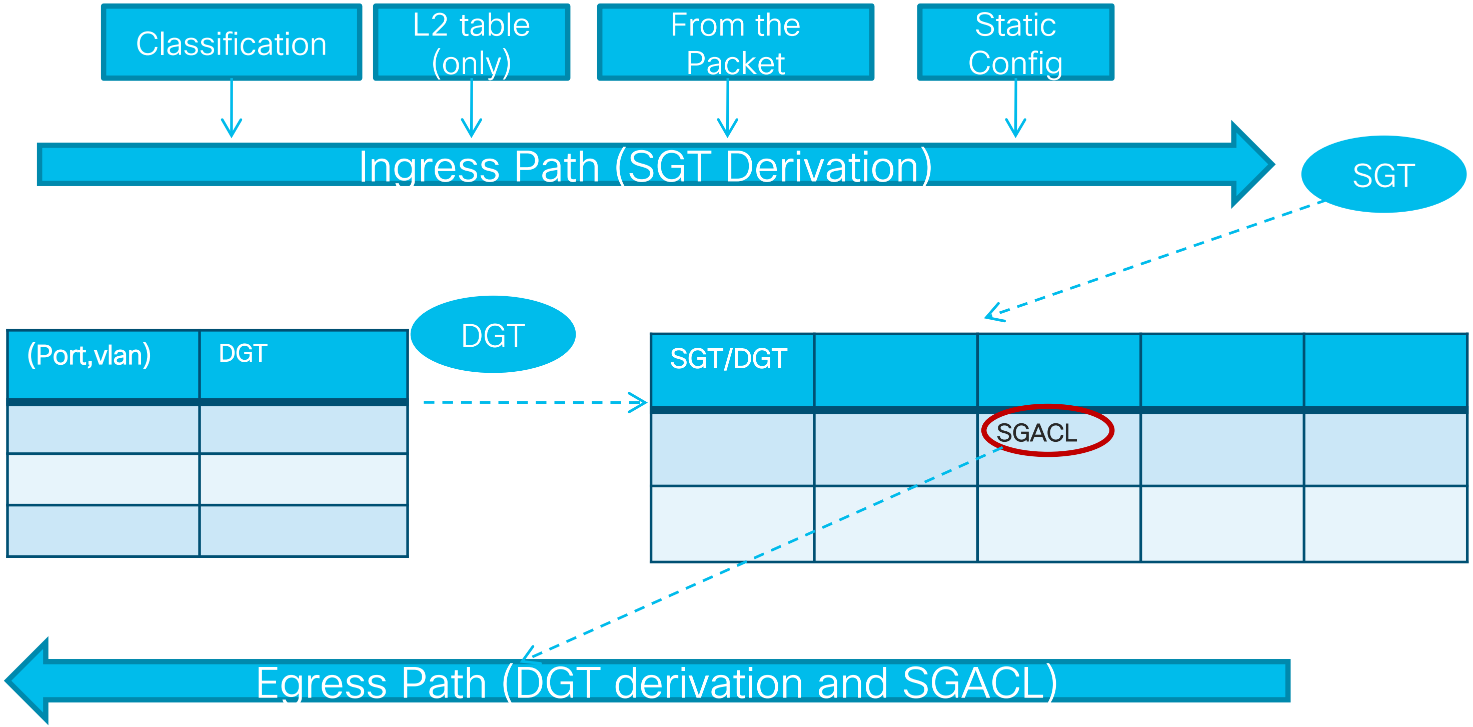
IP Address	SGT
10.23.1.100	Limited_Access - 8
10.23.10.200	Full Access - 6

Hardware Forwarding SGT/SGACL

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

SGT and Destination Group Tag (DGT) Derivation in Cat 3K-X

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

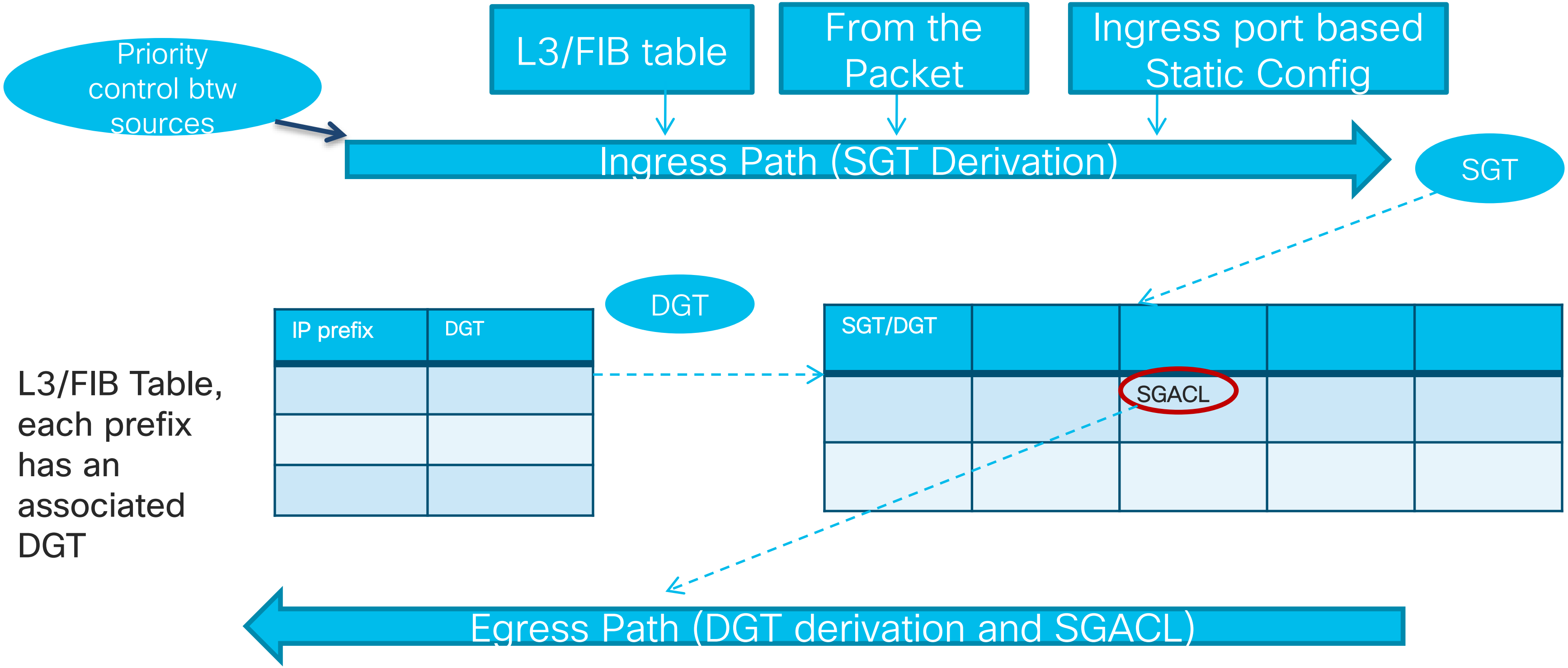

Classification
L2 table (only)
From the Packet
Static Config
Ingress Path (SGT Derivation)
SGT
DGT
Egress Path (DGT derivation and SGACL)

(Port,vlan)	DGT

SGT/DGT				
		SGACL		

Use Case - Campus

SGT and DGT Derivation in Cat9K


Priority control btw sources
L3/FIB table
From the Packet
Ingress port based Static Config
Ingress Path (SGT Derivation)
SGT
DGT
Egress Path (DGT derivation and SGACL)

L3/FIB Table, each prefix has an associated DGT

IP prefix	DGT

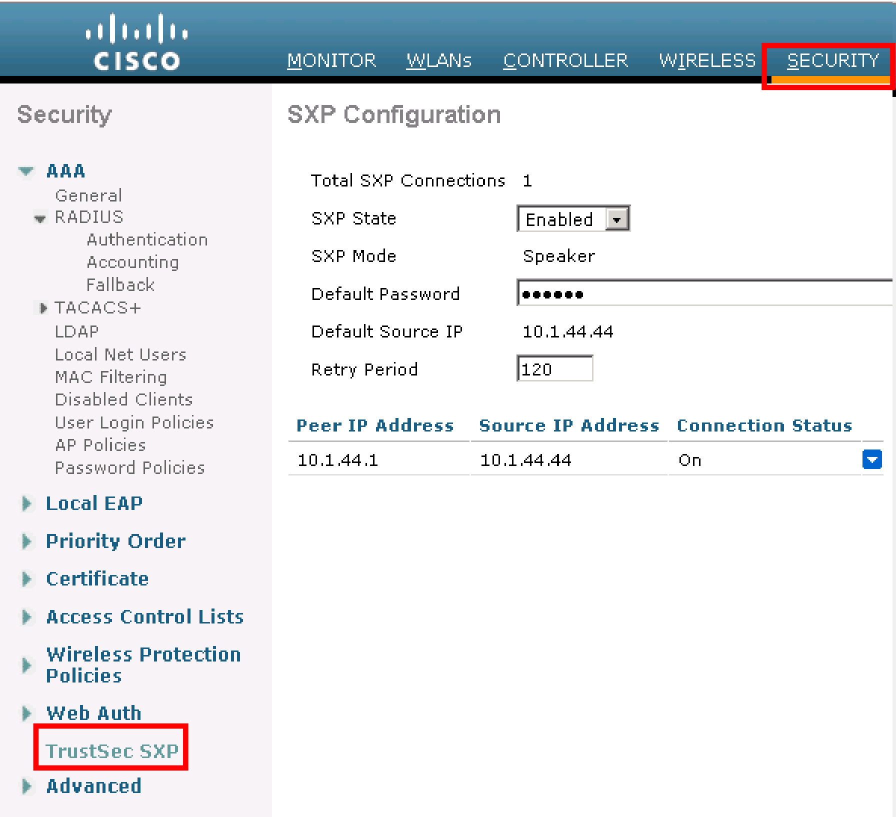
SGT/DGT				
		SGACL		

A number of SGT(DGT) assignment sources, e.g. SXP, VLAN-SGT, Subnet/Host SGT, will be evaluated by SGT software against a priority list, the winning result will be programmed into the L3/FIB table

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

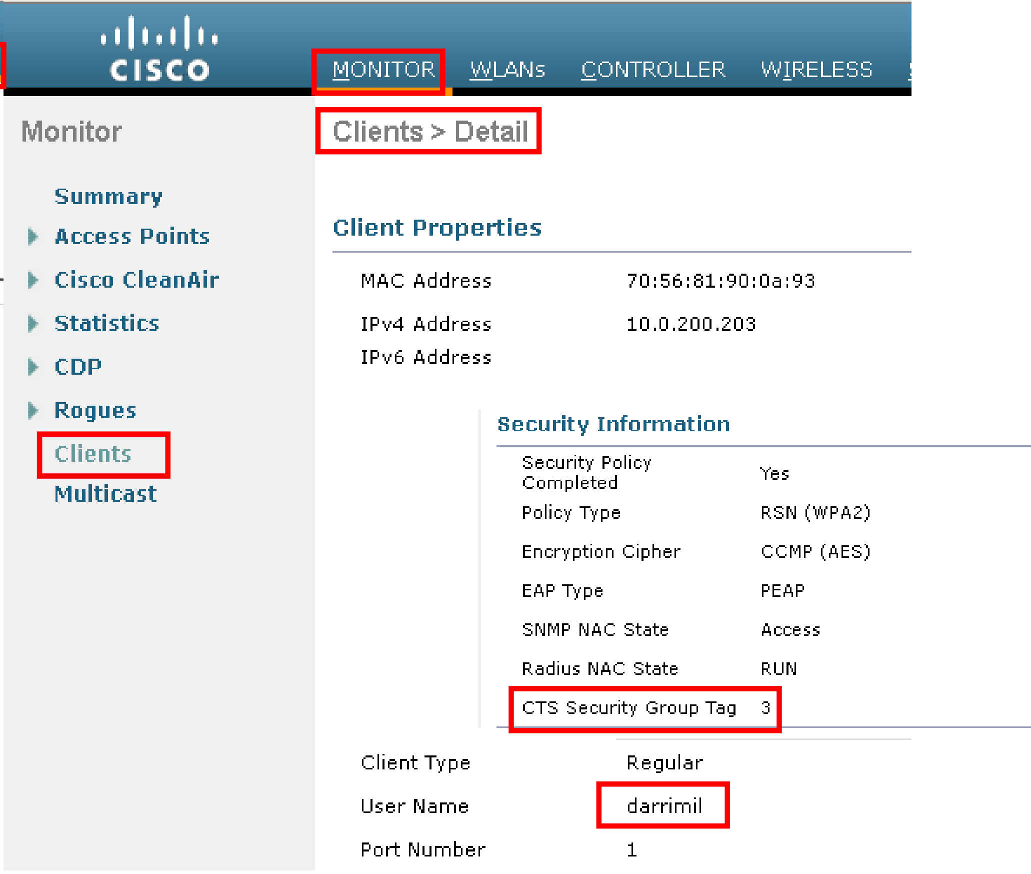
WLC SXP Configuration



SXP Configuration

Total SXP Connections	1
SXP State	Enabled
SXP Mode	Speaker
Default Password	●●●●●●
Default Source IP	10.1.44.44
Retry Period	120

Peer IP Address	Source IP Address	Connection Status
10.1.44.1	10.1.44.44	On



Clients > Detail

Client Properties

MAC Address	70:56:81:90:0a:93
IPv4 Address	10.0.200.203
IPv6 Address	

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	3

Client Type	Regular
User Name	darrimil
Port Number	1

Use Case - Campus

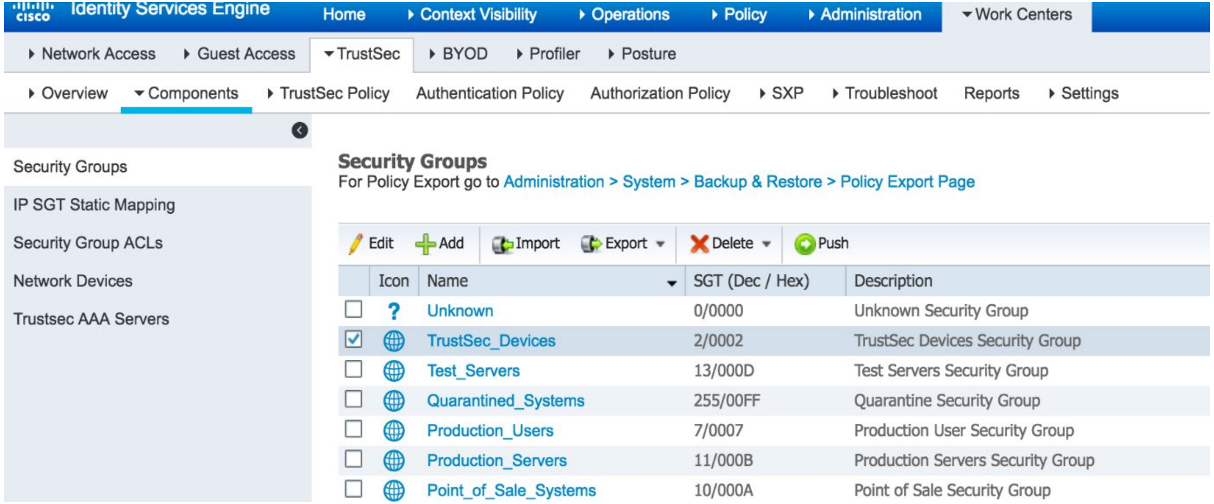
IOS SXP Configuration

```
3850
cts sxp enable
cts sxp connection peer 10.1.44.1 source
10.1.11.44 password default mode local
! SXP Peering to Cat6K

9K
cts sxp enable
cts sxp default password cisco123
!
cts sxp connection peer 10.1.11.44 source
10.1.44.1 password default mode local listener
hold-time 0 0
! ^^ Peering to Cat3K
cts sxp connection peer 10.1.44.44 source
10.1.44.1 password default mode local listener
hold-time 0 0
! ^^ SXP Peering to WLC
```

```
C3850#show cts role-based sgt-map all details
Active IP-SGT Bindings Information

IP Address          Security Group                        Source
======================================================================
10.10.11.1          2:Device_sgt                           INTERNAL
10.10.11.100        6:Full_Access                          LOCAL

C9K-CORE-1#show cts sxp connections brief
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running

-----------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
-----------------------------------------------------------------------------
10.1.11.44       10.1.44.1        On                11:28:14:59 (dd:hr:mm:sec)
10.1.44.44       10.1.44.1        On                22:56:04:33 (dd:hr:mm:sec)

Total num of SXP Connections = 2
C9K-CORE-1#show cts role-based sgt-map all details
Active IP-SGT Bindings Information

IP Address          Security Group                        Source
======================================================================
10.1.40.10          2000:PCI_Servers                       CLI
10.1.44.1           2:Device_sgt                           INTERNAL
--- snip ---
10.0.200.203        3:BYOD                                 SXP
10.10.11.100        6:Full_Access                          SXP
```

Enabling SGT/SGACL on IOS

- Following is a high-level overview of SGT/SGACL configuration on Catalyst switches when used with ISE2.x
- Configure ISE 2.x to the point where you can perform 802.1X authentication (bootstrap, certificate, AD integration, basic authentication & authorization rules)
- Configure Device SGT (**Work Centers > Trustsec > Components > Security Group**)

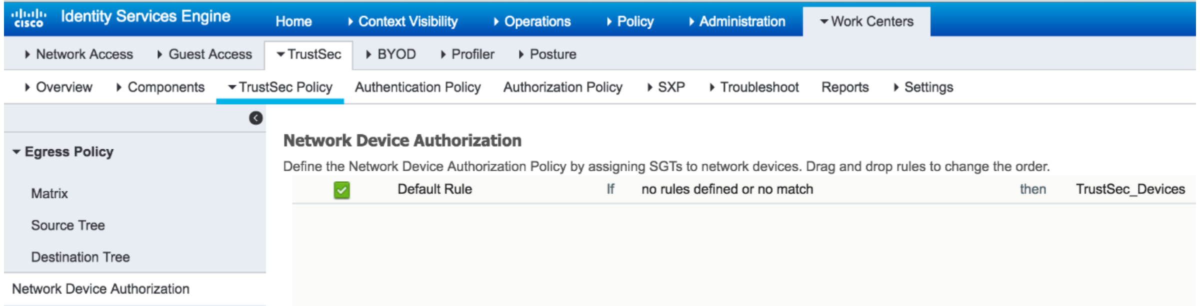


Security Groups
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Icon	Name	SGT (Dec / Hex)	Description
□	?	Unknown	0/0000	Unknown Security Group
☑	🌐	TrustSec_Devices	2/0002	TrustSec Devices Security Group
□	🌐	Test_Servers	13/000D	Test Servers Security Group
□	🌐	Quarantined_Systems	255/00FF	Quarantine Security Group
□	🌐	Production_Users	7/0007	Production User Security Group
□	🌐	Production_Servers	11/000B	Production Servers Security Group
□	🌐	Point_of_Sale_Systems	10/000A	Point of Sale Security Group

SGT Configuration for ISE

- Under **Work Centers > TrustSec > Trustsec Policy > Network Device authorization**, assign Device SGT created in step (2) to default condition

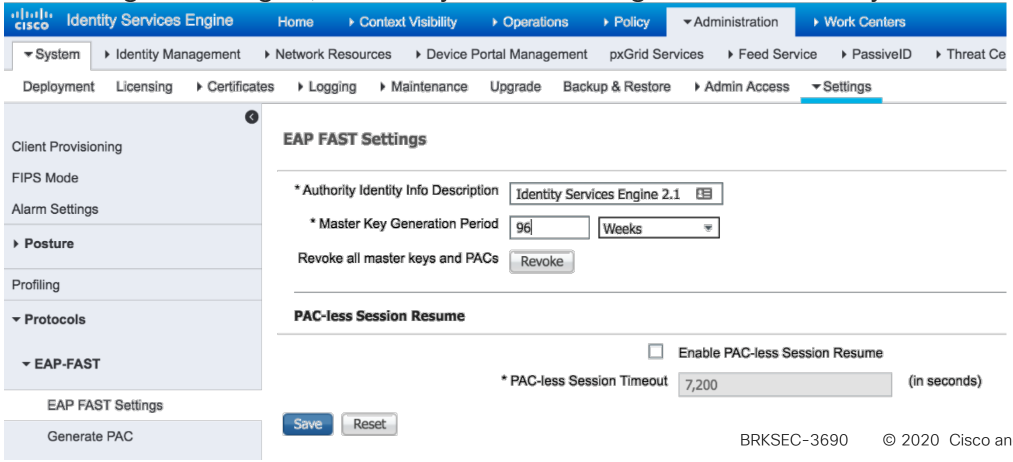


Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

☑	Default Rule	If	no rules defined or no match	then	TrustSec_Devices

- **Optionally** under **Administration > System > Settings > Protocols > EAP-FAST > EAP-FAST Settings**, change A-ID description to something meaningful, so that you can recognise which ISE you are receiving PAC file



EAP FAST Settings

* Authority Identity Info Description: Identity Services Engine 2.1

* Master Key Generation Period: 96 Weeks

Revoke all master keys and PACs: Revoke

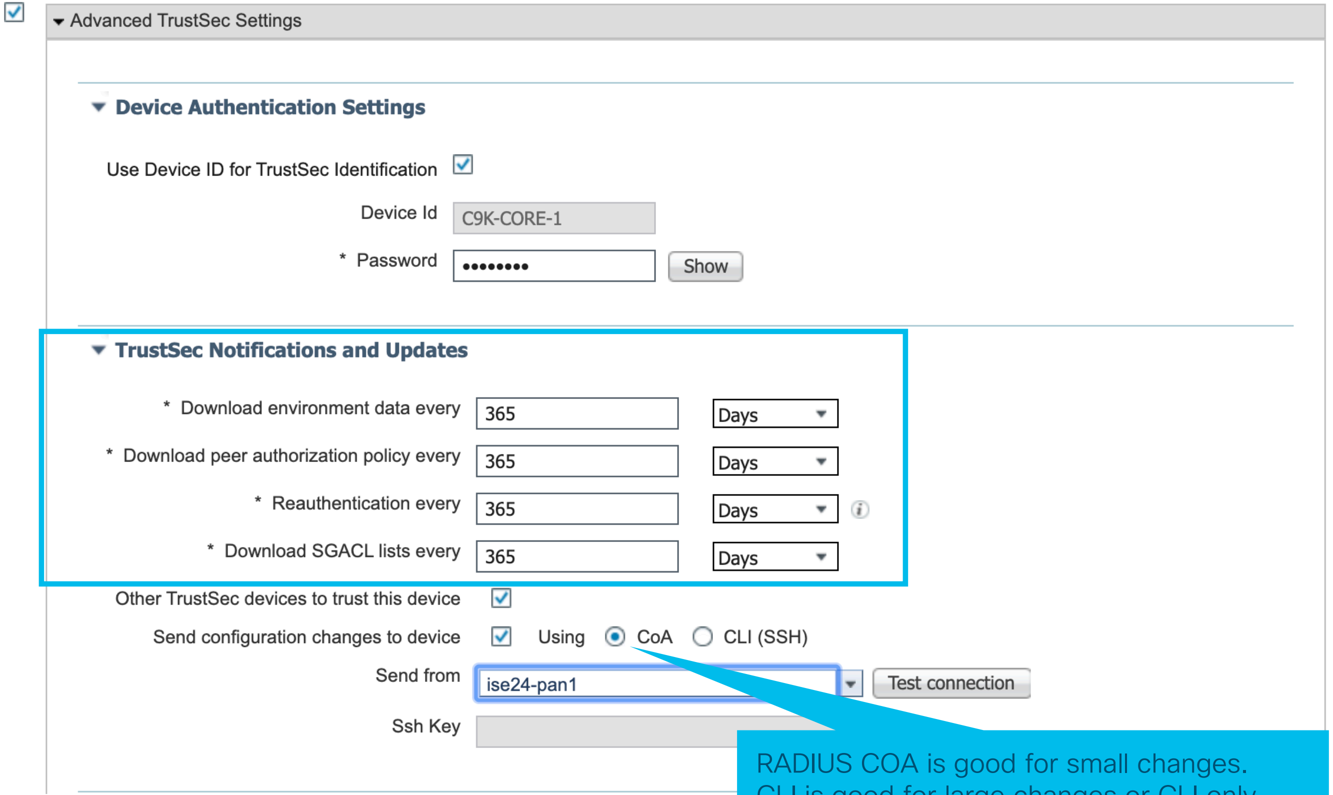
PAC-less Session Resume

□ Enable PAC-less Session Resume

* PAC-less Session Timeout: 7,200 (in seconds)

Configuration an SGT Device

- Configure RADIUS secret. Also Advanced TrustSec Settings, check Use Device ID for TrustSec, then type Device password. This ID and Password needs to be exactly same as you define on network Device CLI
- Best practice for timers is to set for a long duration so policy is only updated on the device via an explicit push/workflow



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification	☑
Device Id	C9K-CORE-1
* Password	••••••••• Show

TrustSec Notifications and Updates

* Download environment data every	365	Days
* Download peer authorization policy every	365	Days
* Reauthentication every	365	Days
* Download SGACL lists every	365	Days

Other TrustSec devices to trust this device	☑
Send configuration changes to device	☑ Using ● CoA ○ CLI (SSH)
Send from	ise24-pan1 Test connection
Ssh Key	

RADIUS COA is good for small changes. CLI is good for large changes or CLI only platforms like N7K

Use Case - Campus

Configuring an Catalyst Switch for SGT

- Following CLI is required to turn on NDAC (to authenticate Device to ISE and receive policies including SGACL from ISE)

- Enabling AAA

```
C9K-CORE-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
C9K-CORE-1(config)#aaa new-model
```

- Defining RADIUS server with PAC keyword

```
C9K-CORE-1(config)#radius-server host <ISE_PSN_IP> pac key <RADIUS_SHARED_SECRET>
```

- Define authorization list name for Trustsec policy download

```
C9K-CORE-1(config)#cts authorization list <AUTHZ_List_Name>
```

- Use default AAA group for 802.1X and “defined authz list” for authorization

```
C9K-CORE-1(config)#aaa authentication dot1x default group radius
C9K-CORE-1(config)#aaa authorization network <AUTHZ_List_Name> group radius
```

Configuring an IOS Switch for SGT(cont.)

- Configure RADIUS server to use VSA in authentication request

```
C9K-CORE-1(config)#radius-server vsa send authentication
```

- Enable 802.1X in system level

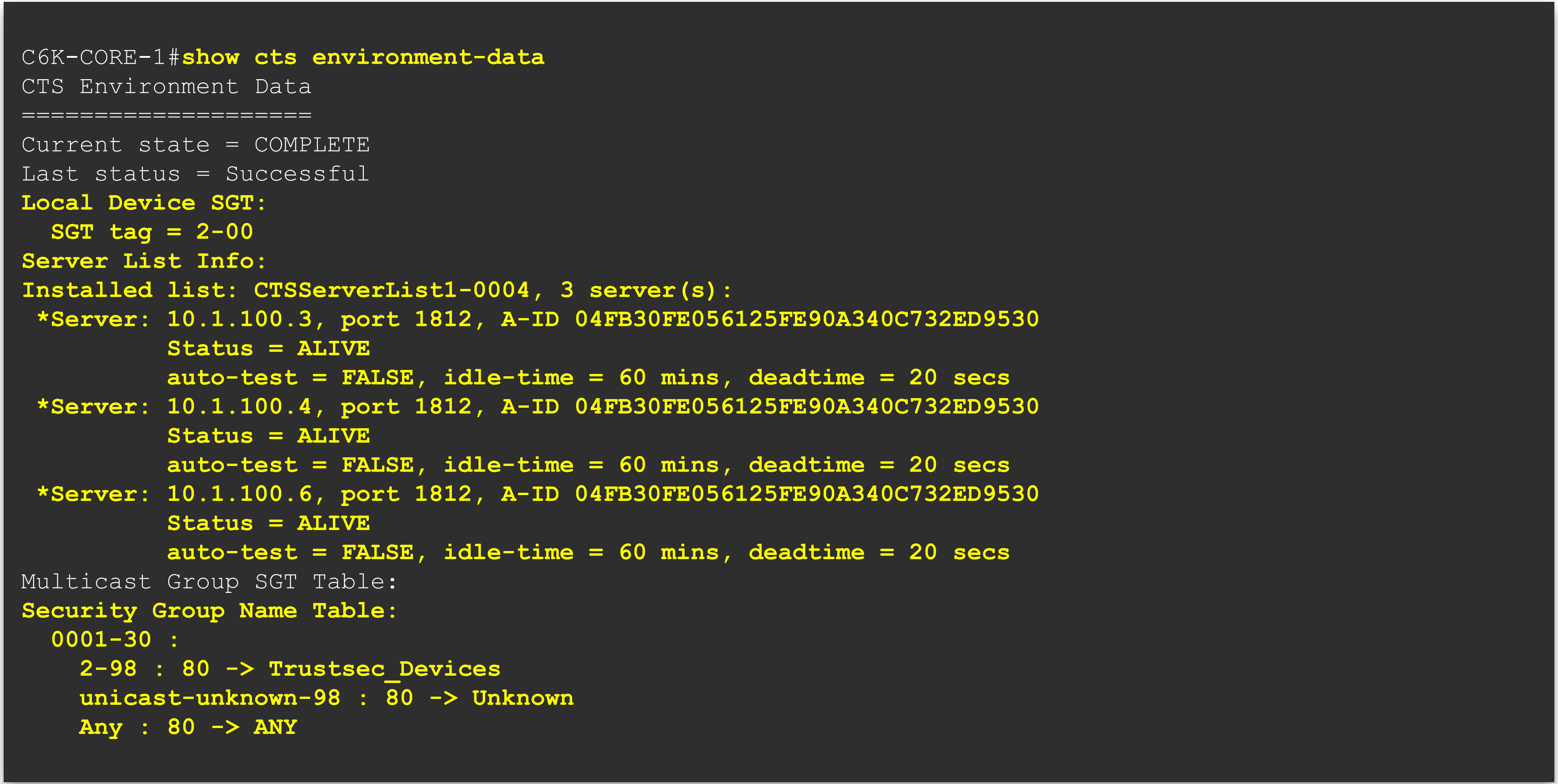
```
C9K-CORE-1(config)#dot1x system-auth-control
```

- Define Device credential (EAP-FAST I-ID), which must match ones in ISE AAA client configuration

```
C9K-CORE-1 #cts credential id <Device_ID> password <Device_PASSWORD>
```

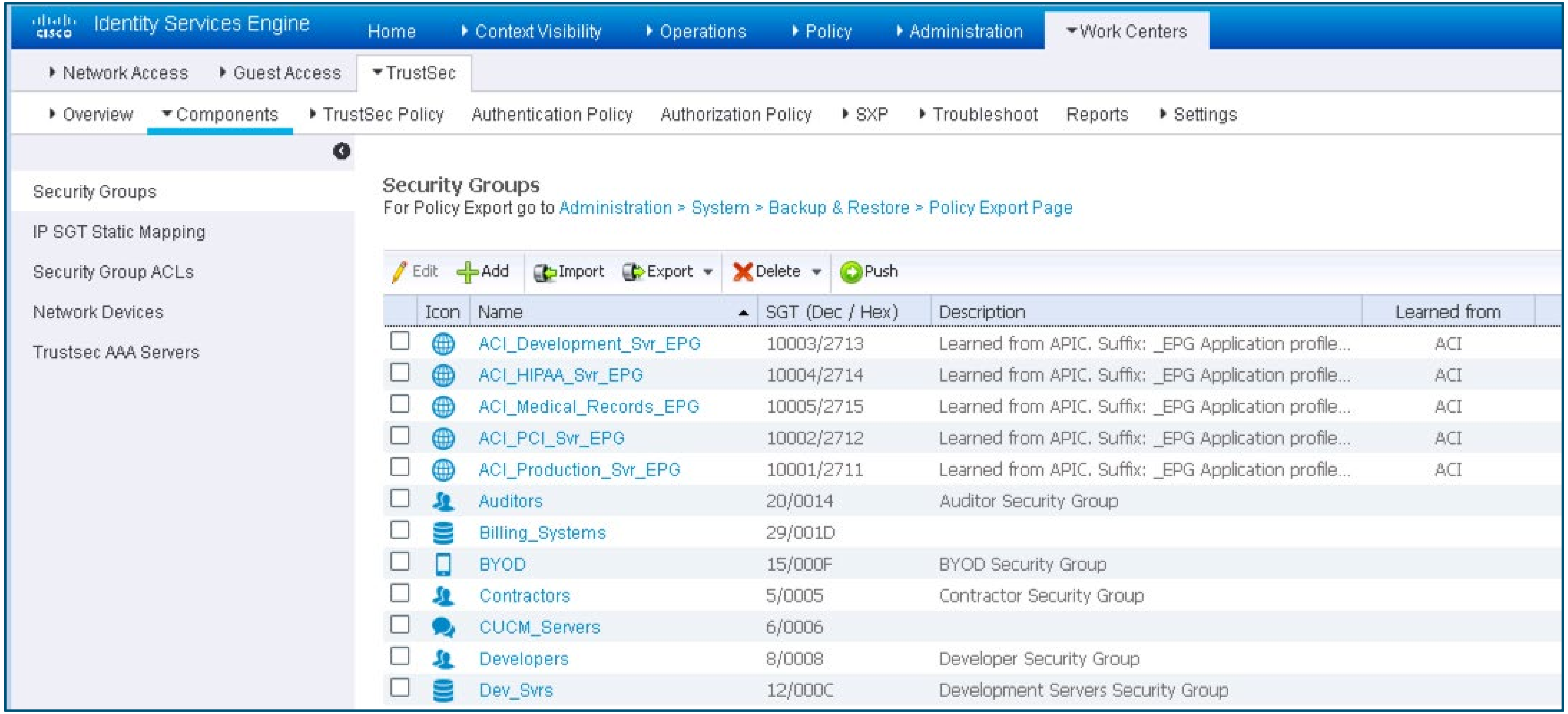
Note: remember that Device credential under IOS is configured in Enable mode, not in config mode. This is different CLI command level between IOS and NX-OS, where you need to configure Device credential in config mode

Verification – Environment Data



```
C6K-CORE-1#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00
Server List Info:
Installed list: CTSServerList1-0004, 3 server(s):
 *Server: 10.1.100.3, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.1.100.4, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.1.100.6, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
  0001-30 :
    2-98 : 80 -> Trustsec_Devices
    unicast-unknown-98 : 80 -> Unknown
    Any : 80 -> ANY
```

Create the SGTs in ISE – UI/REST



Security Groups

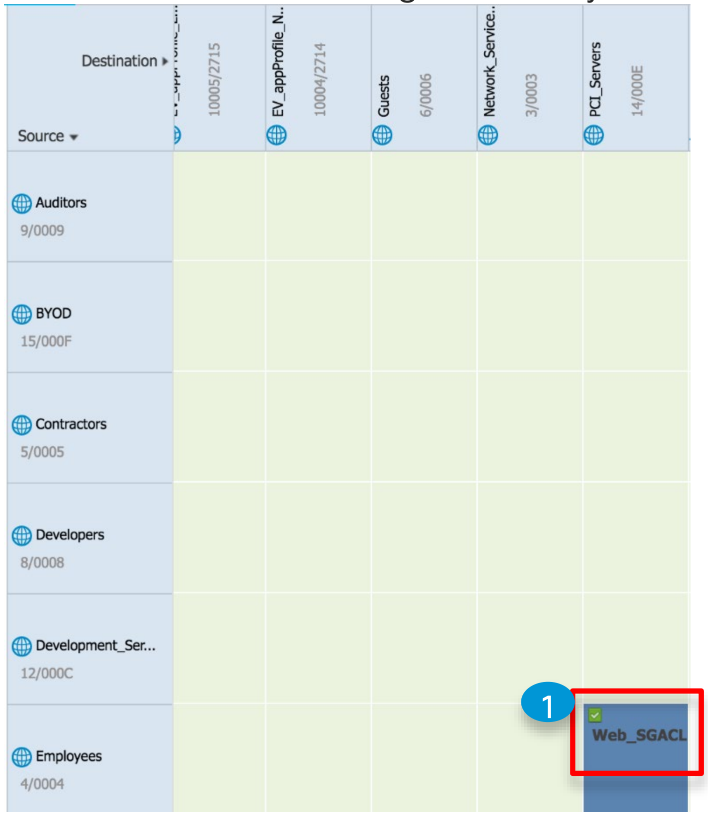
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Icon	Name	SGT (Dec / Hex)	Description	Learned from
□		ACI_Development_Svr_EPG	10003/2713	Learned from APIC. Suffix: _EPG Application profile...	ACI
□		ACI_HIPAA_Svr_EPG	10004/2714	Learned from APIC. Suffix: _EPG Application profile...	ACI
□		ACI_Medical_Records_EPG	10005/2715	Learned from APIC. Suffix: _EPG Application profile...	ACI
□		ACI_PCI_Svr_EPG	10002/2712	Learned from APIC. Suffix: _EPG Application profile...	ACI
□		ACI_Production_Svr_EPG	10001/2711	Learned from APIC. Suffix: _EPG Application profile...	ACI
□		Auditors	20/0014	Auditor Security Group	
□		Billing_Systems	29/001D		
□		BYOD	15/000F	BYOD Security Group	
□		Contractors	5/0005	Contractor Security Group	
□		CUCM_Servers	6/0006		
□		Developers	8/0008	Developer Security Group	
□		Dev_Svrs	12/000C	Development Servers Security Group	

Preparing ISE for SGACL Enforcement

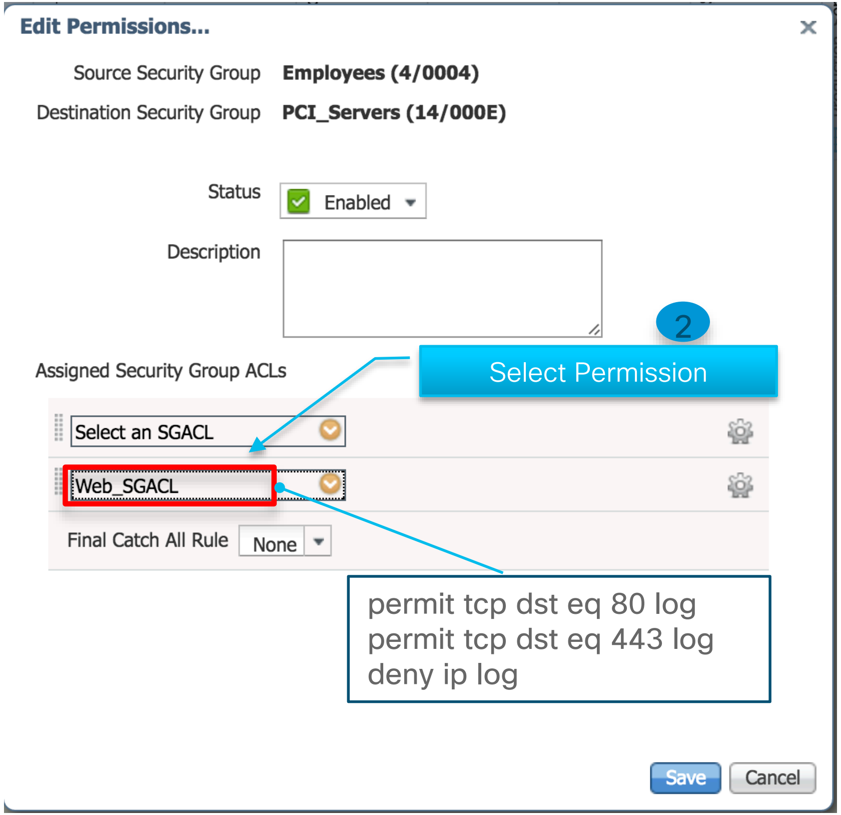
- ISE needs to be configured for SGT/SGACL and associated policies

Under Work Center > TrustSec > Egress Policy



Destination ▸ Source ▾	EV_appProfile_L... 10005/2715	EV_appProfile_N.. 10004/2714	Guests 6/0006	Network_Service.. 3/0003	PCI_Servers 14/000E
Auditors 9/0009					
BYOD 15/000F					
Contractors 5/0005					
Developers 8/0008					
Development_Ser... 12/000C					
Employees 4/0004					✓ Web_SGACL

1



Edit Permissions...

Source Security Group **Employees (4/0004)**

Destination Security Group **PCI_Servers (14/000E)**

Status ✓ Enabled

Description

Assigned Security Group ACLs

Select an SGACL

Web_SGACL

Final Catch All Rule None

2

Select Permission

```
permit tcp dst eq 80 log
permit tcp dst eq 443 log
deny ip log
```

Activating SGACL Enforcement on IOS Switch

- After setting up SGT/SGACL on ISE, you can now enable SGACL Enforcement on IOS switch

Defining IP to SGT mapping for servers – Shown via CLI, but can be pushed from ISE to CLI or via SXP

```
C6K-CORE-1(config)#cts role-based sgt-map 192.168.31.1 sgt 100
C6K-CORE-1(config)#cts role-based sgt-map 192.168.32.0/24 sgt 20
C6K-CORE-1(config)#cts role-based sgt-map 10.x.x.0 sgt 30
```

Enabling SGACL Enforcement Globally and for VLAN

```
C6K-CORE-1(config)#cts role-based enforcement
C6K-CORE-1(config)#cts role-based enforcement vlan-list 40
```

Downloading Policy on IOS Switch

- After enabling SGACL enforcement, policies need to be downloaded to IOS, the egress enforcement point

Refresh Environment Data using cts refresh environment-data

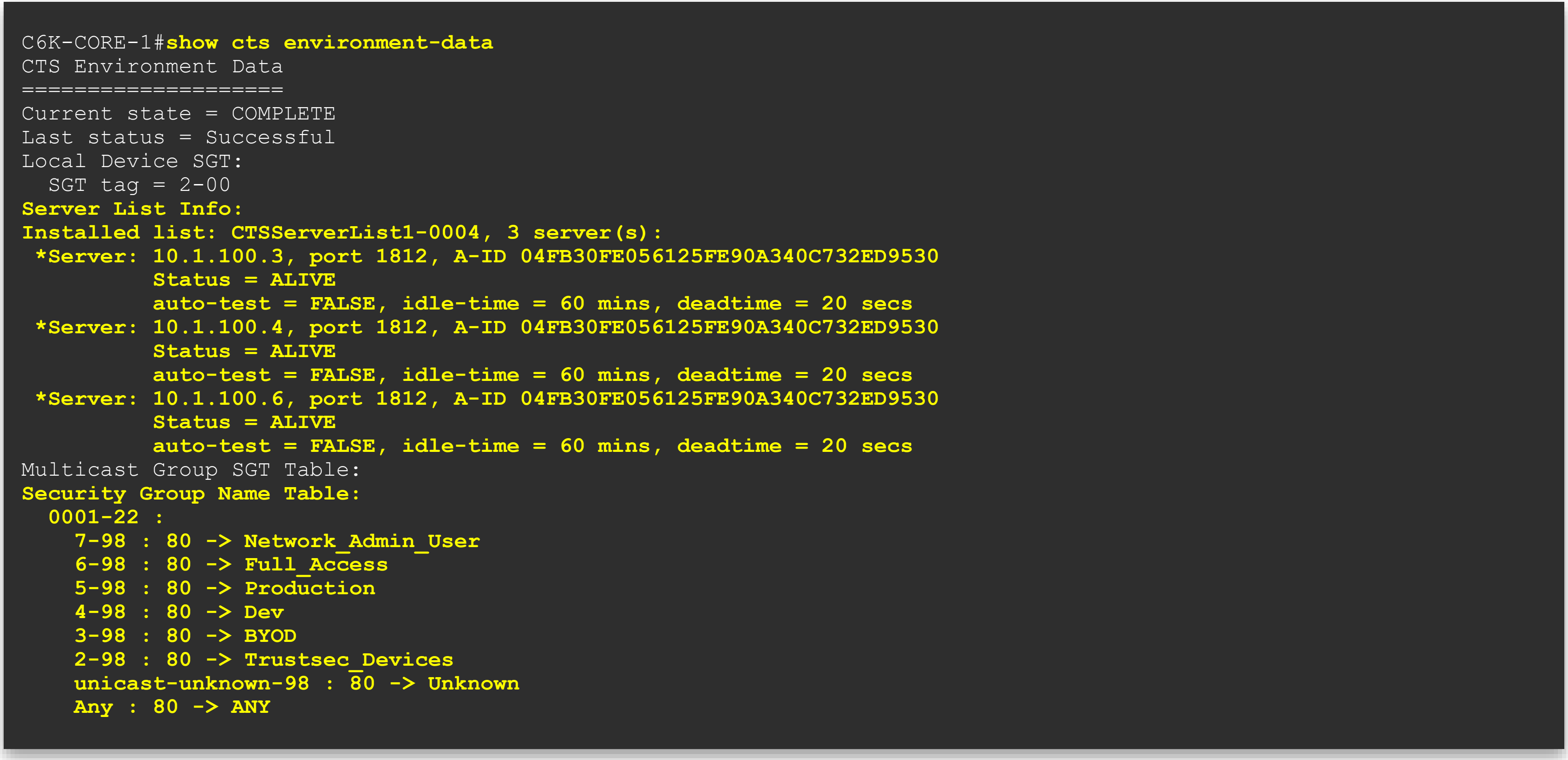
```
C6K-CORE-1# cts refresh environment-data
Environment data download in progress
```

Refresh Policy using cts refresh policy

```
C6K-CORE-1# cts refresh policy
Policy refresh in progress
```

Downloading Policy on IOS Switch

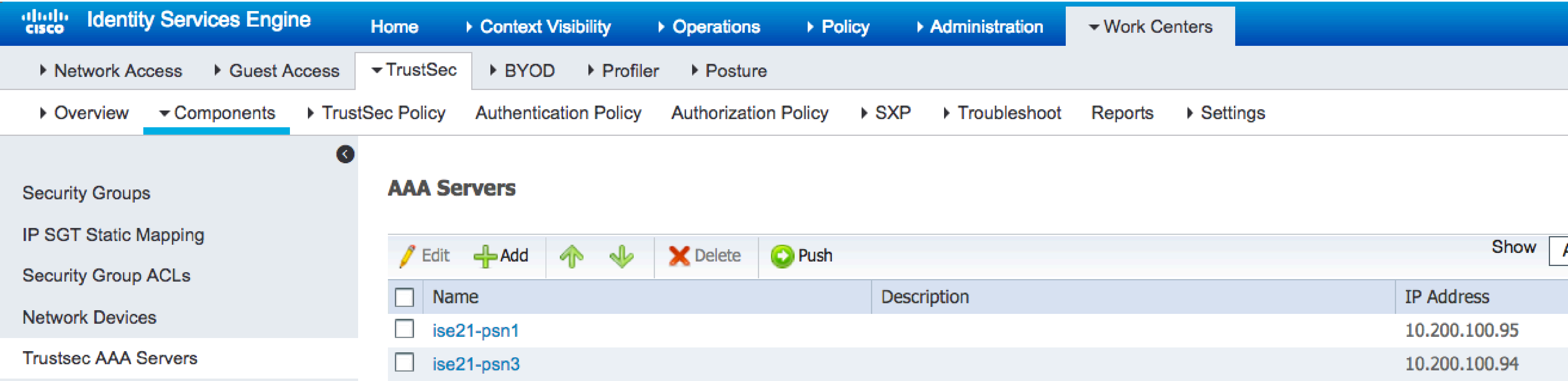
Verify Environment Data



```
C6K-CORE-1#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00
Server List Info:
Installed list: CTSServerList1-0004, 3 server(s):
 *Server: 10.1.100.3, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.1.100.4, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.1.100.6, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
  0001-22 :
    7-98 : 80 -> Network_Admin_User
    6-98 : 80 -> Full_Access
    5-98 : 80 -> Production
    4-98 : 80 -> Dev
    3-98 : 80 -> BYOD
    2-98 : 80 -> Trustsec_Devices
    unicast-unknown-98 : 80 -> Unknown
    Any : 80 -> ANY
```

The Reality of SGACL Download – Server List

- There is one Server List defined in ISE



AAA Servers

□	Name	Description	IP Address
□	ise21-psn1		10.200.100.95
□	ise21-psn3		10.200.100.94

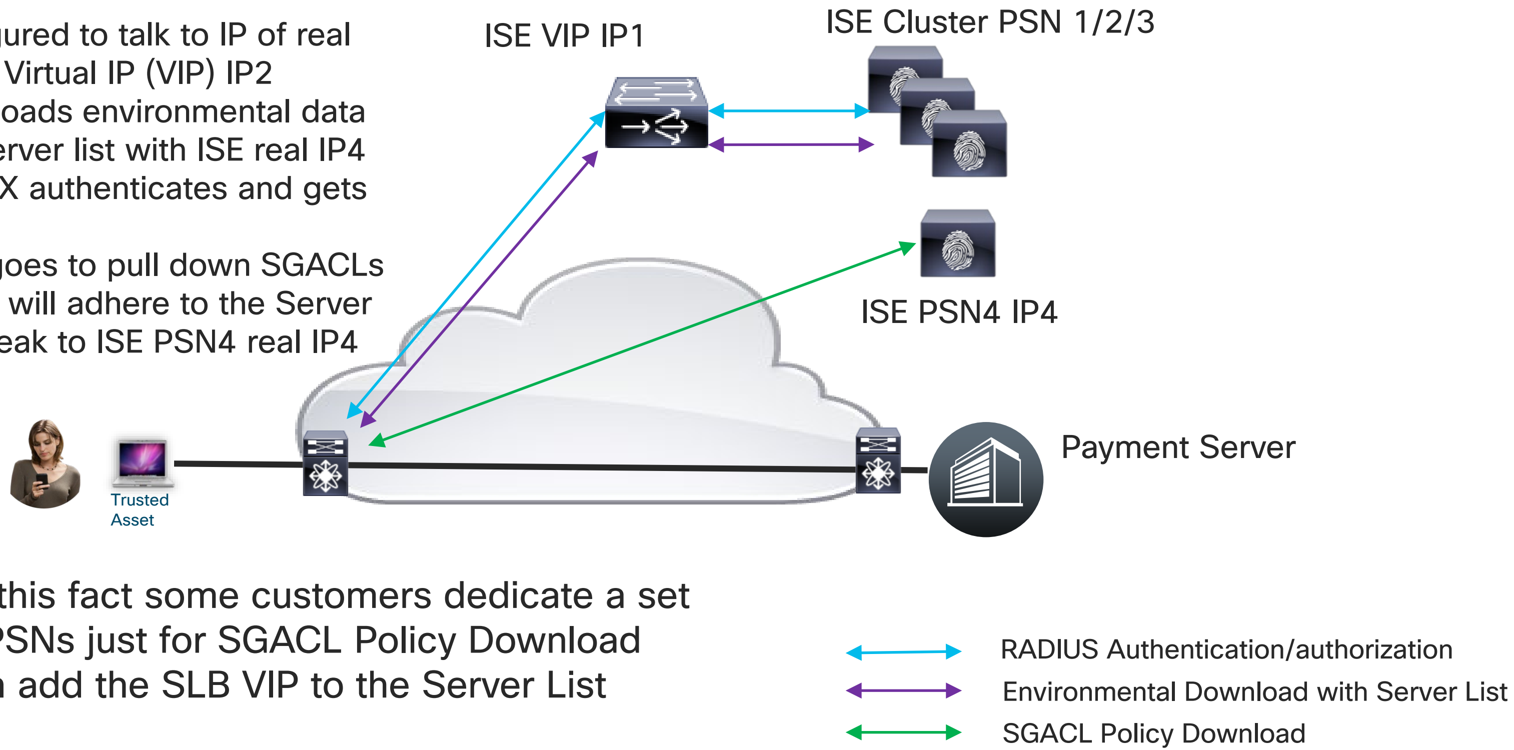
- The NAD can be configured to speak to ISE via real IP of PSN or SLB Virtual IP address for CTS (this is supported)

- Regardless the NAD will download from the IPs in the server list

Use Case - Campus

Server List with Real IP of ISE PSN or Load Balanced Virtual IP (VIP)

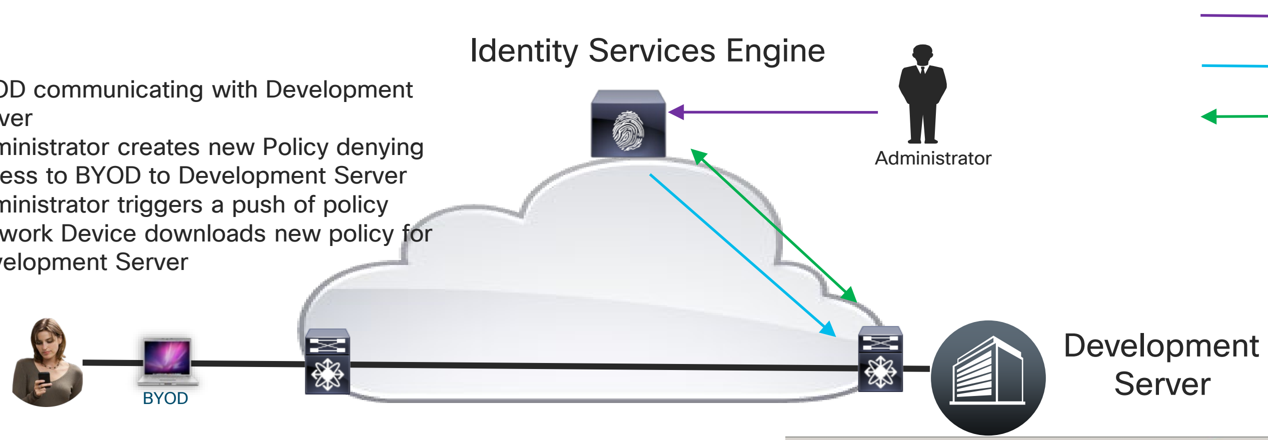
1. NAD configured to talk to IP of real PSN IP1 or Virtual IP (VIP) IP2
2. NAD downloads environmental data and gets server list with ISE real IP4
3. User 802.1X authenticates and gets SGT x
4. When ISE goes to pull down SGACLs for policy it will adhere to the Server List and speak to ISE PSN4 real IP4



- Due to this fact some customers dedicate a set of ISE PSNs just for SGACL Policy Download
- You can add the SLB VIP to the Server List

ISE SGACL Policy Push

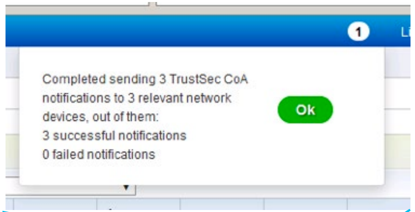
1. BYOD communicating with Development Server
2. Administrator creates new Policy denying access to BYOD to Development Server
3. Administrator triggers a push of policy
4. Network Device downloads new policy for Development Server

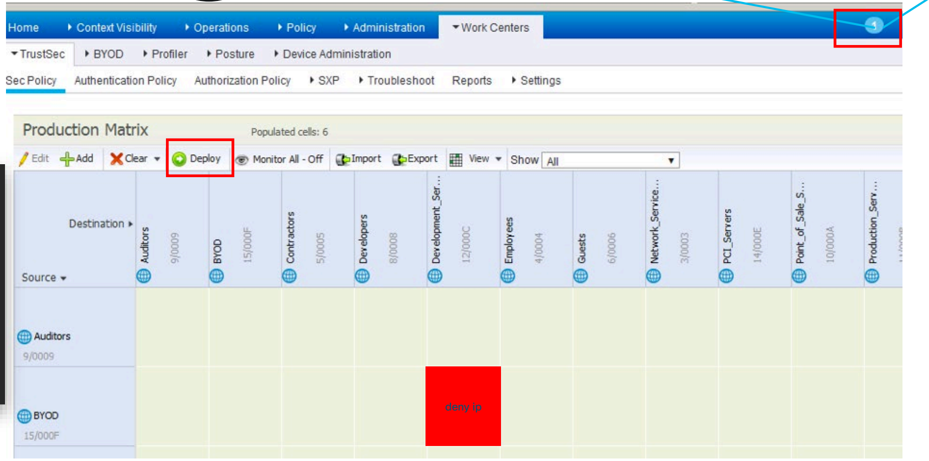


→ UI interaction

→ SGACL COA

↔ SGACL Download


Completed sending 3 TrustSec CoA notifications to 3 relevant network devices, out of them:
3 successful notifications
0 failed notifications



Source ▾ / Destination ▸	Auditors 9/0009	BYOD 15/000F	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004	Guests 6/0006	Network_Service... 3/0003	PCI_Servers 14/000E	Point_of_Sale_S... 10/000A	Production_Serv...
Auditors 9/0009											
BYOD 15/000F					deny ip						

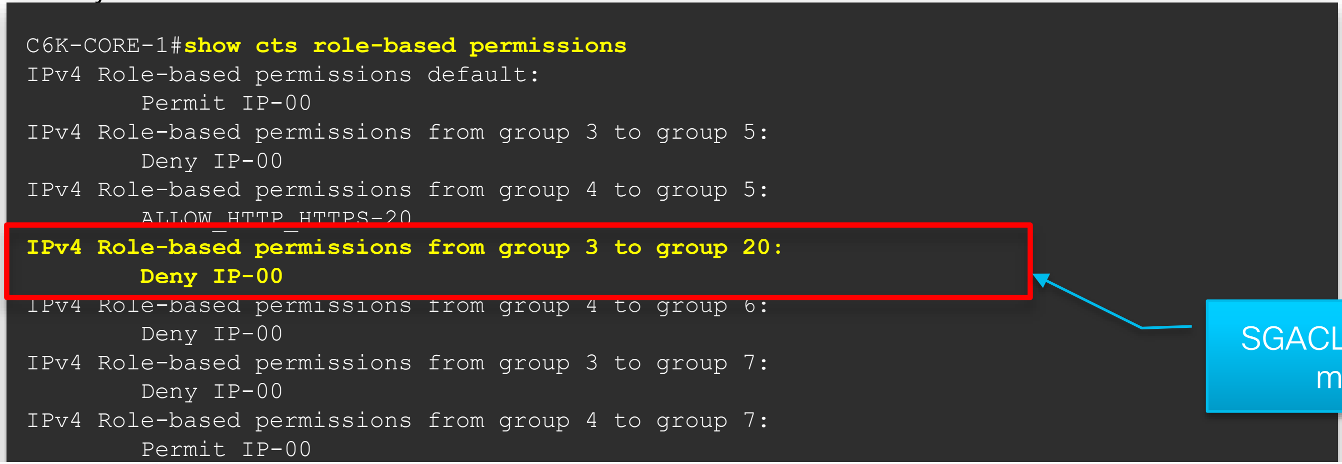
- Applies to SGACL, Environmental Data, and Server-List

```
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

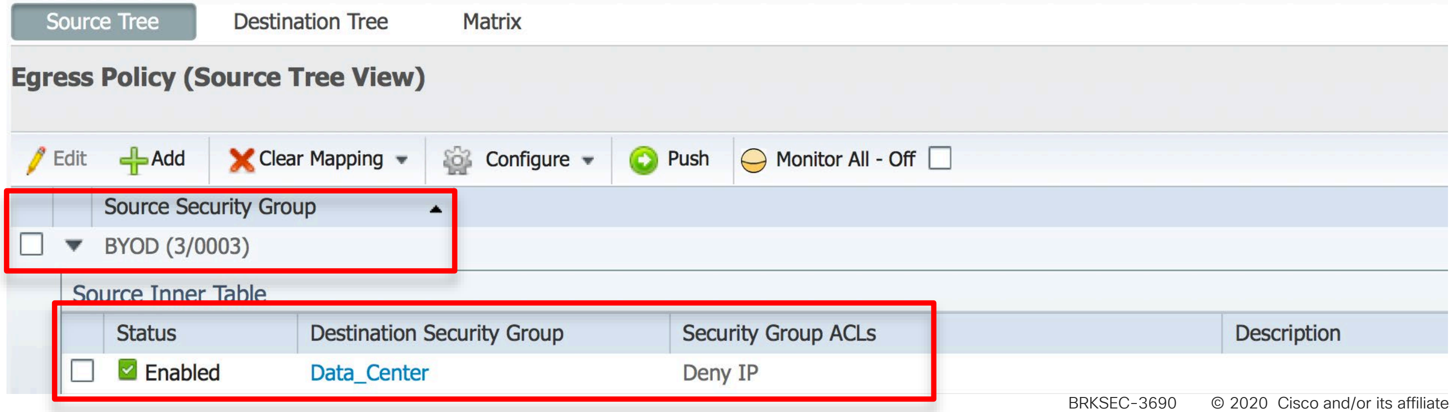
Viewing SGACL Policy on IOS Switch

Verify SGACL Content



```
C6K-CORE-1#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 3 to group 5:
        Deny IP-00
IPv4 Role-based permissions from group 4 to group 5:
        ALLOW_HTTP_HTTPS-20
IPv4 Role-based permissions from group 3 to group 20:
        Deny IP-00
IPv4 Role-based permissions from group 4 to group 6:
        Deny IP-00
IPv4 Role-based permissions from group 3 to group 7:
        Deny IP-00
IPv4 Role-based permissions from group 4 to group 7:
        Permit IP-00
```

SGACL Mapping Policy should match to one on ISE



Egress Policy (Source Tree View)

	Source Security Group
□	BYOD (3/0003)

Source Inner Table

	Status	Destination Security Group	Security Group ACLs	Description
□	☑ Enabled	Data_Center	Deny IP	

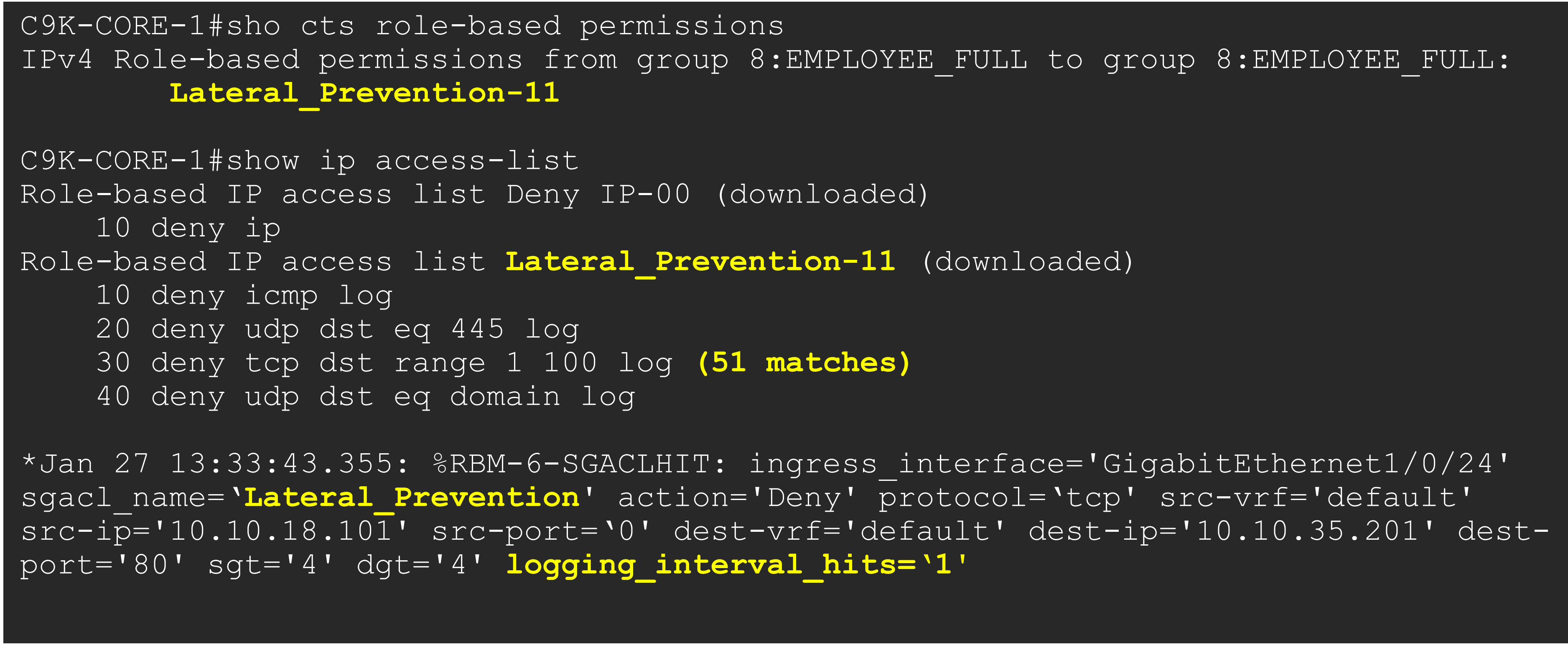
Use Case - Campus

Alternative Policy View on IOS Switch

```
SW1-BRC1#sho cts policy sgt 4
CTS SGT Policy
===============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 4-06:Employees
SGT Policy Flag: 0x41400001
RBACL Source List:
 Source SGT: 4-06:Employees-0, Destination SGT: 4-06:Employees-0
 rbacl_type = 80
 rbacl_index = 1
 name = DenyIP_Log-10
 IP protocol version = IPV4
 refcnt = 2
 flag = 0x41000000
 stale = FALSE
 RBACL ACEs:
  permit tcp dst eq 80
  deny ip log
-- snip --
```

```
-- continued --
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 86400 secs
RBACL Policy Last update time = 21:50:17 UTC
Sun Jan 28 2018
Policy expires in 0:23:59:11 (dd:hr:mm:sec)
Policy refreshes in 0:23:59:11 (dd:hr:mm:sec)
Cache data applied = NONE
```

SGACL Monitoring – Best Effort Syslog

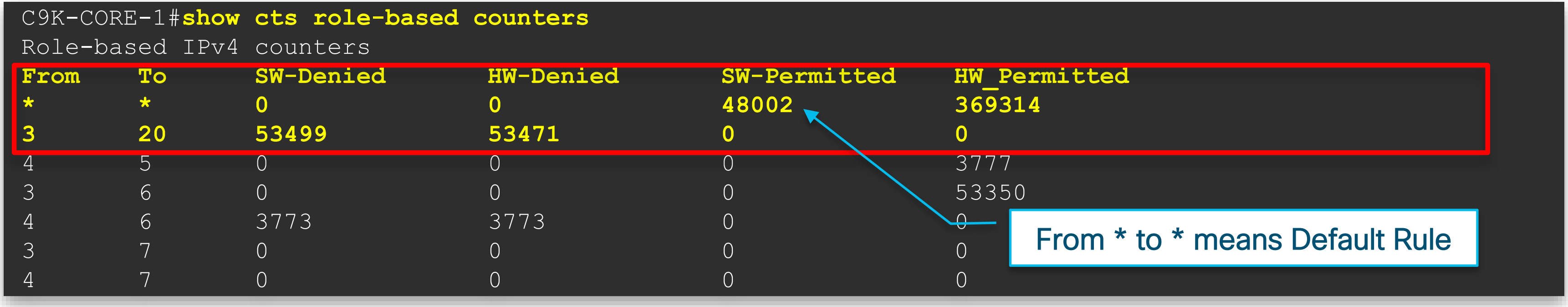


```
C9K-CORE-1#sho cts role-based permissions
IPv4 Role-based permissions from group 8:EMPLOYEE_FULL to group 8:EMPLOYEE_FULL:
        Lateral_Prevention-11

C9K-CORE-1#show ip access-list
Role-based IP access list Deny IP-00 (downloaded)
    10 deny ip
Role-based IP access list Lateral_Prevention-11 (downloaded)
    10 deny icmp log
    20 deny udp dst eq 445 log
    30 deny tcp dst range 1 100 log (51 matches)
    40 deny udp dst eq domain log

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

Use Case - Campus

Verifying SGACL Drops

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

Use Case - Campus

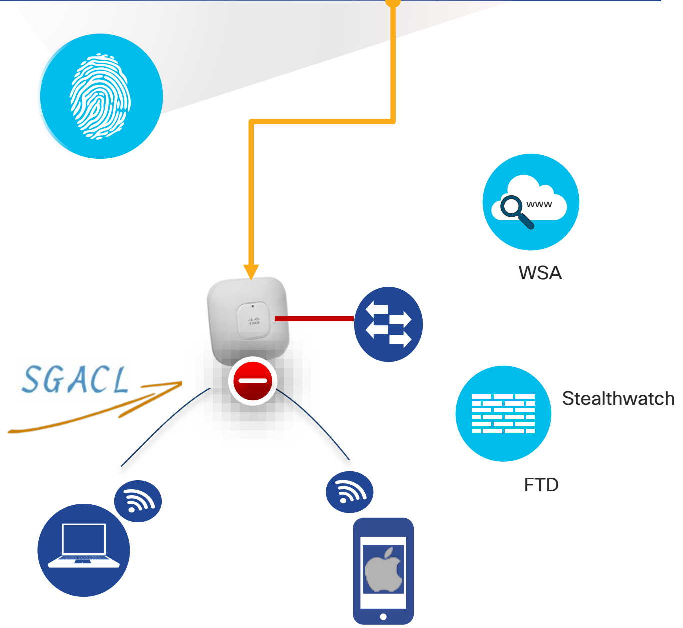
SGT/SGACL for WLC/APs

- Code 8.3 – allows SXP from WLC for FlexConnect
- Code version 8.4
- Models: 2800, 3700, 3800, 1850,1830, 1700, 2700 (AKA wave 1 and wave 2 APs)
- Wireless LAN Controllers: 8540 and 5520 only
- Supported for Centrally switched and FlexConnect SSIDs
- Additional support for inline and SXPv4 propagation to upstream Devices

Benefits

- Restrict Lateral Movement in WLAN natively
- Restrict Lateral Movement to LAN as well
- Use classifications from WLC/AP in ASA, FTD, WSA, StealthWatch policies

Destination Source	BYOD (4)	Employees (5)
Employees (5)	Intra_Jabber_Sig Anti_Malware	Intra_Jabber_Sig Anti_Malware
BYOD (4)	Intra_Jabber_Sig Anti_Malware	Intra_Jabber_Sig Anti_Malware

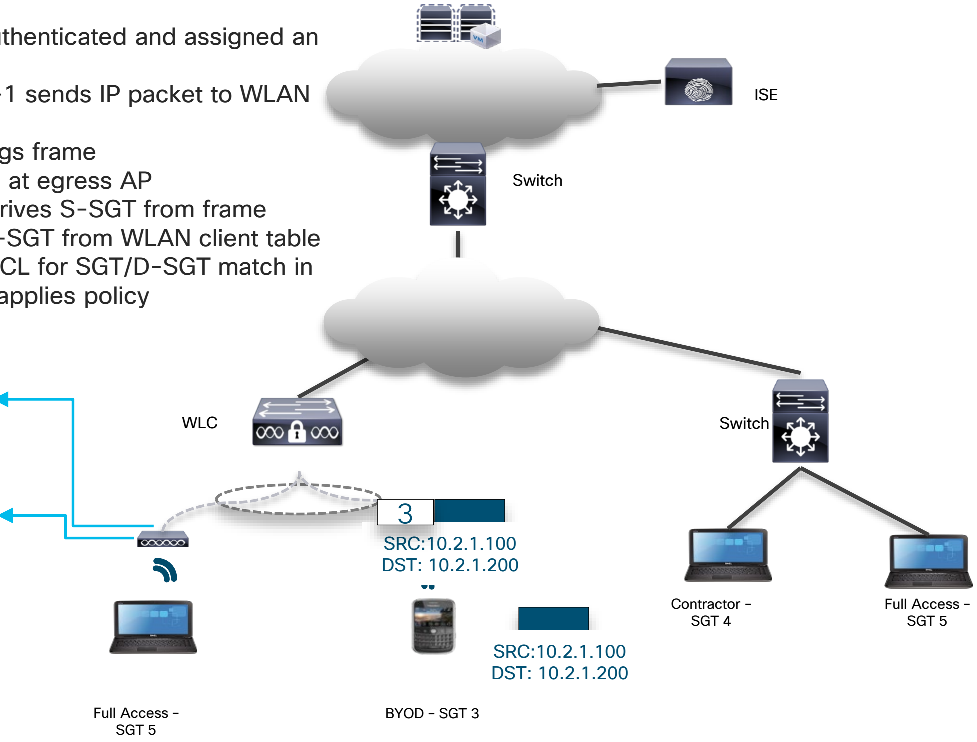


Central Authentication/Switch WLAN User to WLAN User

1. Clients are authenticated and assigned an SGT
2. WLAN Client-1 sends IP packet to WLAN Client-2
3. Ingress AP tags frame
4. Frame arrives at egress AP
5. Egress AP derives S-SGT from frame
6. AP derives D-SGT from WLAN client table
7. AP finds SGACL for SGT/D-SGT match in memory and applies policy

IP Address	SGT
10.2.1.200	Full Access - 5

SGT	D-SGT	SGACL
BYOD	Full Access	permit ip

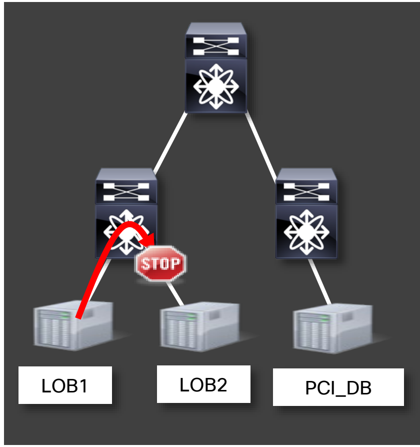


Nexus 7000 SGT Considerations

Use Case - Campus

Nexus 7000 SGT/SGACL Capabilities

- SGT/SGACL supported on M series, F2, F2E cards as of 6.2(6a)
- SGT/SGACL support on F3 as of 6.2(10)*
- VPC and Fabric Path supported in 6.2(10) with IP/SGT only
- NXOS 7.3
  - Subnet/SGT including local only 0.0.0.0/0 for ”Internet use cases”
  - SXPv3 to receive/send subnet/SGT (no IPv6)
  - SGACL Monitor Mode
  - Enhanced SGACL Logging (action in log)
- NXOS 8.0
  - SXPv4 (no IPv6)
  - SGACL per interface enforcement (”no cts role-based enforcement”)
  - SGACL Egress Policy Overwrite(ISE SGACL takes precedence over CLI SGACL)



* F3 can only tag on trunk ports. May require redesign from L3 to trunk/SVI

Nexus F3 Linecard Inline Tagging behavior

- Known behavior that dot1q header be present on links to support CMD header which carries SGT.
  - Not an issue for L2 Trunks where the 802.1q header is present.
  - Point to Point L3 links do not insert a 802.1q header.
- Two configuration options to provide an L3 interface exist that will impose the dot1q header.
  - Interface configuration through the use of sub-interfaces with 802.1q encapsulation enabled.
  - Use of a logical Switched Virtual Interface (SVI) used with interface configured as a L2 Trunk port carrying the VLAN to which the SVI is assigned.
- Can impact L2 control traffic consists of protocols such as CDP, LLDP, LACP, PAgP, STP, BFD, etc working with
- Compatible with other N7K line cards
  - Two fixes for better compatibility in NXOS 8.1(1) - CSCvc42685, CSCvb93553
- SGT Tagging Compatibility of F3 with ISR/ASR/Catalyst switches – Fixed in IOS-XE 16.10 for IOS-XE routers
- Compatibility Table published on CCO.
- https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/security/config/cisco_nexus7000_security_config_guide_8x/configuring_cisco_trustsec.html#concept_06EC3AC2909F4592BCB3862

Nexus 7000 Interface Configuration

Use Case - Campus

```
feature cts
feature dot1x
cts Device-id N7K-DST1 password 7 wnyxlszh123
cts role-based counters enable
cts role-based sgt-map 10.39.1.30 17
……
cts role-based sgt-map 10.87.109.72 3
cts role-based enforcement

vlan 87
  cts role-based enforcement
vlan 118
  cts role-based enforcement
interface Ethernet1/25
  description N5K connection
  cts manual
    policy static sgt 0x0002 trusted  <- Later versions of NXOS allow a decimal for the SGT
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 90,118-120,124
  spanning-tree port type normal
  channel-group 10 mode active
  no shutdown
```

Common Issues

Use Case - Campus

Device Tracking – The Engine that 802.1X/MAB Work for SGT

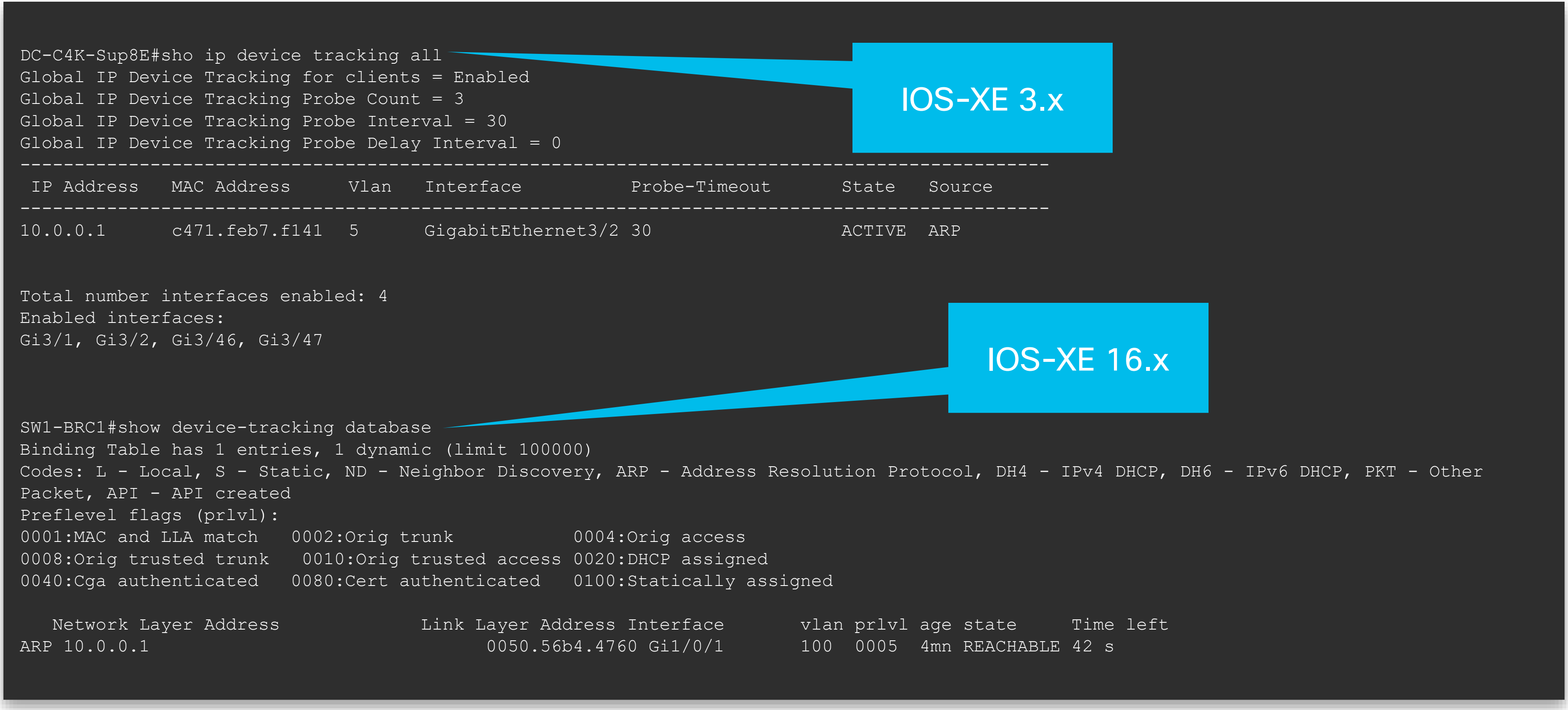
- Device Tracking was enabled by default for 802.1X/MAB in IOS releases prior to 16.x
- In 16.x IP Device Tracking is enabled separately from 802.1X/MAB

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication violation restrict
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 spanning-tree bpduguard enable
 device-tracking attach-policy IPDT_MAX_10

device-tracking policy IPDT_MAX_10
 limit address-count 10
 no protocol udp
 tracking enable
```

IOS-XE 3.x

Mandatory in IOS-XE 16.x

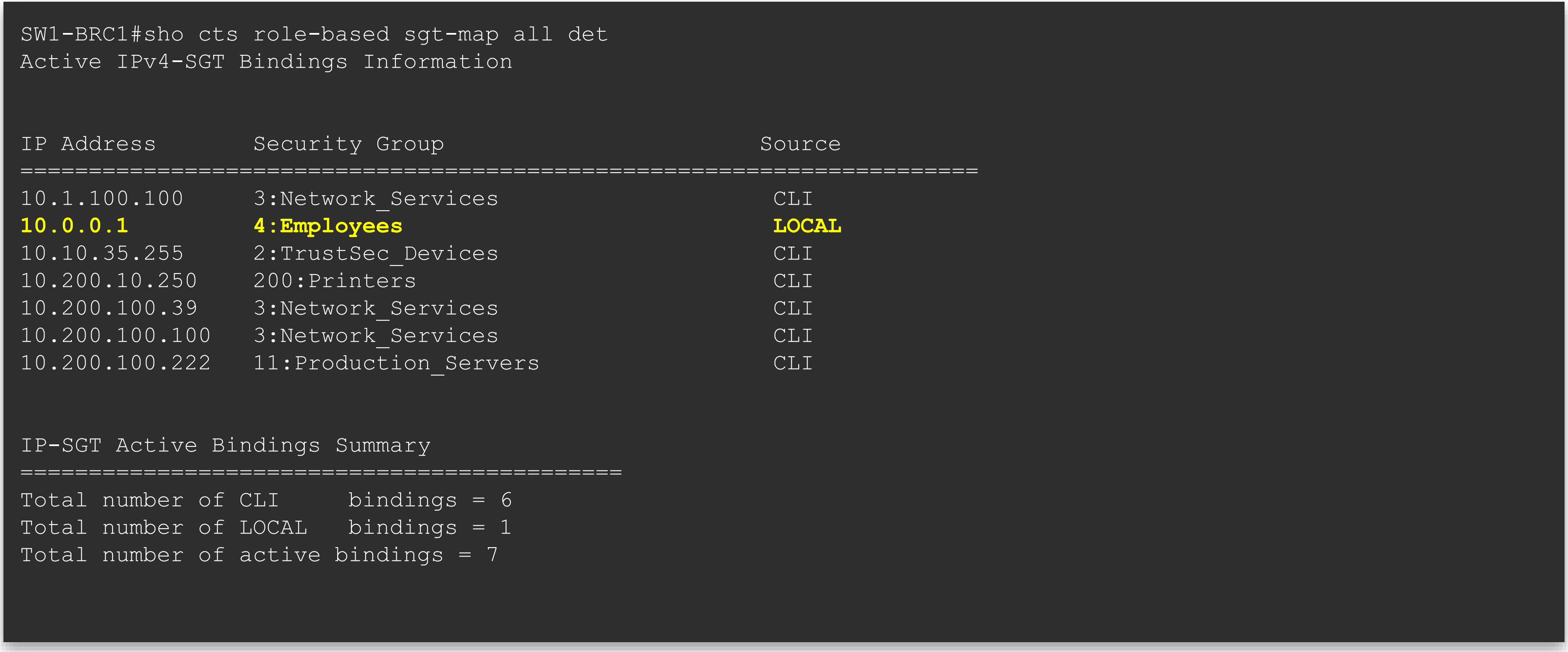
Device Tracking Entry Fundamental to an IP/SGT Entry



```
DC-C4K-Sup8E#sho ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
-----------------------------------------------------------------------------------------------
 IP Address   MAC Address     Vlan   Interface          Probe-Timeout      State   Source
-----------------------------------------------------------------------------------------------
10.0.0.1      c471.feb7.f141  5      GigabitEthernet3/2 30                 ACTIVE  ARP


Total number interfaces enabled: 4
Enabled interfaces:
Gi3/1, Gi3/2, Gi3/46, Gi3/47



SW1-BRC1#show device-tracking database
Binding Table has 1 entries, 1 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match   0002:Orig trunk           0004:Orig access
0008:Orig trusted trunk   0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated   0080:Cert authenticated   0100:Statically assigned

   Network Layer Address             Link Layer Address Interface       vlan prlvl age state     Time left
ARP 10.0.0.1                               0050.56b4.4760 Gi1/0/1       100  0005  4mn REACHABLE 42 s
```

Use Case - Campus

IP/SGT Programming Happens after Device Tracking Learning



```
SW1-BRC1#sho cts role-based sgt-map all det
Active IPv4-SGT Bindings Information


IP Address       Security Group                       Source
======================================================================
10.1.100.100     3:Network_Services                    CLI
10.0.0.1         4:Employees                           LOCAL
10.10.35.255     2:TrustSec_Devices                    CLI
10.200.10.250    200:Printers                          CLI
10.200.100.39    3:Network_Services                    CLI
10.200.100.100   3:Network_Services                    CLI
10.200.100.222   11:Production_Servers                 CLI


IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 6
Total number of LOCAL    bindings = 1
Total number of active bindings = 7
```

Use Case - Campus

CSCvh70725 - SGT Binding Removed After IPv6 Entry Goes to STALE in IPDT Database

```
device-tracking policy IPDT_MAX_10
 no protocol ndp
 no protocol dhcp6
 tracking enable

interface GigabitEthernet1/0/1
 device-tracking attach-policy IPDT_MAX_10
```

```
9410#sh cts role-based sgt-map 10.0.0.1
IP Address      SGT    Source
====================
10.0.0.1         18    LOCAL


9410#sh device-tracking dat int GigabitEthernet2/0/11
   Network Layer Address            Link Layer Address Interface       vlan prlvl age state    Time left
ND FE80::CE99:99FF:FE4E:FCE4        cc00.9100.fce4 Gi2/0/11       417 0005   4mn REACHABLE 18 s try 0
ARP 10.0.0.1                        cc00.9100.fce4 Gi2/0/11       417 0005 69s REACHABLE 239 s try 0
ND FE80::DD99:7D5B:DE67:FE60        cc01.a200.cc38 Gi2/0/11       402 0005   7s REACHABLE 302 s try 0
ARP 10.0.0.2                        cc01.a200.cc38 Gi2/0/11       402 0005 32s REACHABLE 271 s try 0

Once the IPv6 entry goes to STALE, the IPv4 SGT Binding gets removed from the table, causing the phone be considered
Unknown.

9410#sh device-tracking dat int GigabitEthernet2/0/11
   Network Layer Address          Link Layer Address Interface      vlan   prlvl  age    state        Time left
ND FE80::CE99:99FF:FE4E:FCE4        cc00.9100.fce4 Gi2/0/11       417    0005   6mn    STALE        90472 s
ARP 10.0.0.1                        cc00.9100.fce4 Gi2/0/11       417    0005   53s    REACHABLE    249 s try 0
ND FE80::DD99:7D5B:DE67:FE60        cc01.a200.cc38 Gi2/0/11       402    0005   111s   REACHABLE    198 s try 0
ARP 10.0.0.2                        cc01.a200.cc38 Gi2/0/11       402    0005   42s    REACHABLE    266 s try 0


9410#sh cts role-based sgt-map 10.0.0.1
9410#
```

SGACL Download Errors

- Validate AAA is reachable with “show aaa servers”
- Validate the device has a PAC with “show cts pac all”
- Validate the device can communicate with ISE by checking environmental data “show cts environmental-data”
- Check ISE to make sure the SGACL is formatted properly
- No IP/SGT on switch because of an error in device tracking
- TrustSec communities Troubleshooting Guide
  - https://communities.cisco.com/docs/DOC-69479

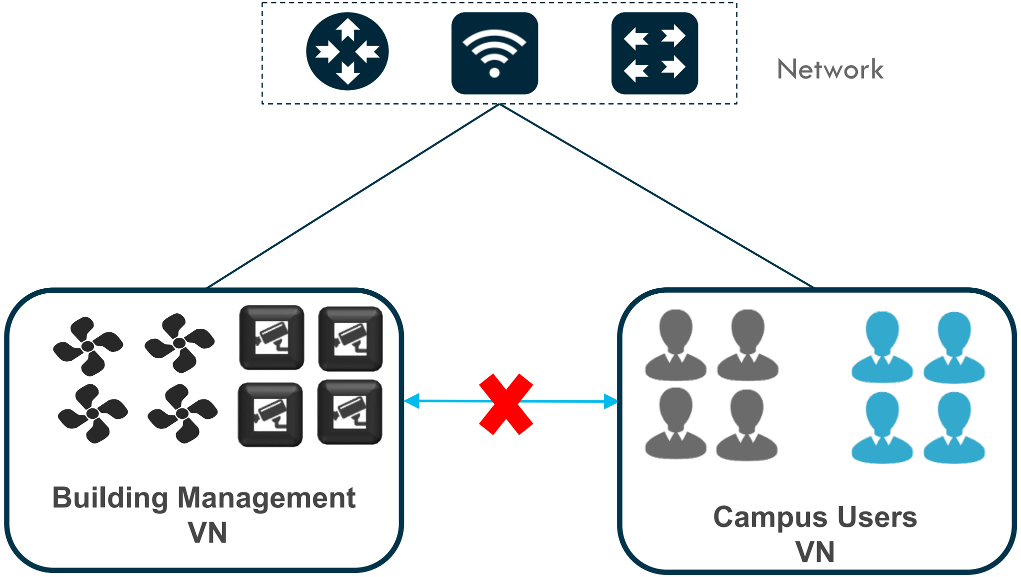
Software Defined Access (SD-Access) – SGT/VXLAN

Use Case – SGT/VXLAN

What is SD-Access?

- Policy/Automation/Assurance for a set of technology innovations solving
  - Subnet availability across access layers w/o stretched VLANs (i.e. spanning tree)
    - Very common in manufacturing, medical, university environments
    - Especially relevant as IoT enters the enterprise campus/WAN (building automation systems that only connect via L2 protocols, connected lighting, etc.)
  - Simplified VRF deployment w/o MPLS
    - 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.
    - More scalable VRF counts than DMVPN, etc.
  - Security using SGT/SGACL – alternative to SXP that allows end to end tagging w/o "all Devices in the middle being Cisco"
    - Easy to handle 3rd party distribution/core layers
    - Easy to handle topologies where the WAN router isn't managed by the enterprise
  - https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html

SD-Access
Two Level Hierarchy – Macro Level

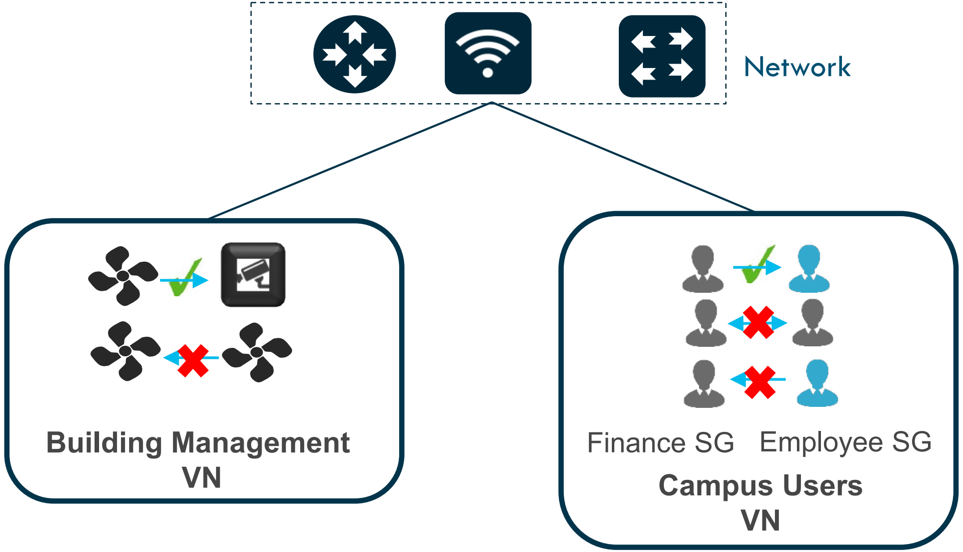


Virtual Network (VN)

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

Use Case – SGT/VXLAN

SD-Access
Two Level Hierarchy – Micro Level

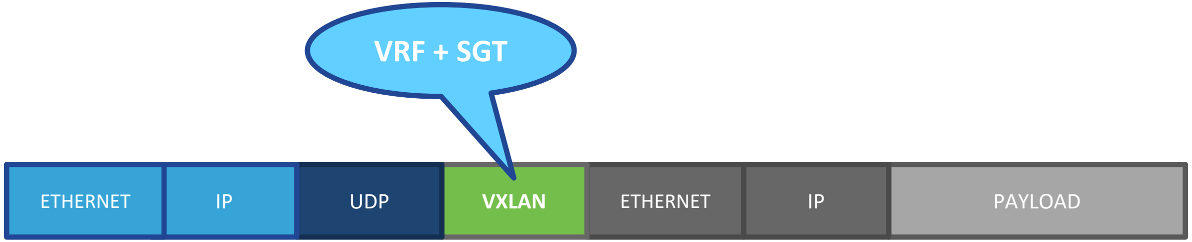


Scalable Group Tag (SGT)

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.

What is Unique About SD-Access?

1. LISP based Control-Plane
2. VXLAN based Data-Plane
3. Integrated SGT/SGACL

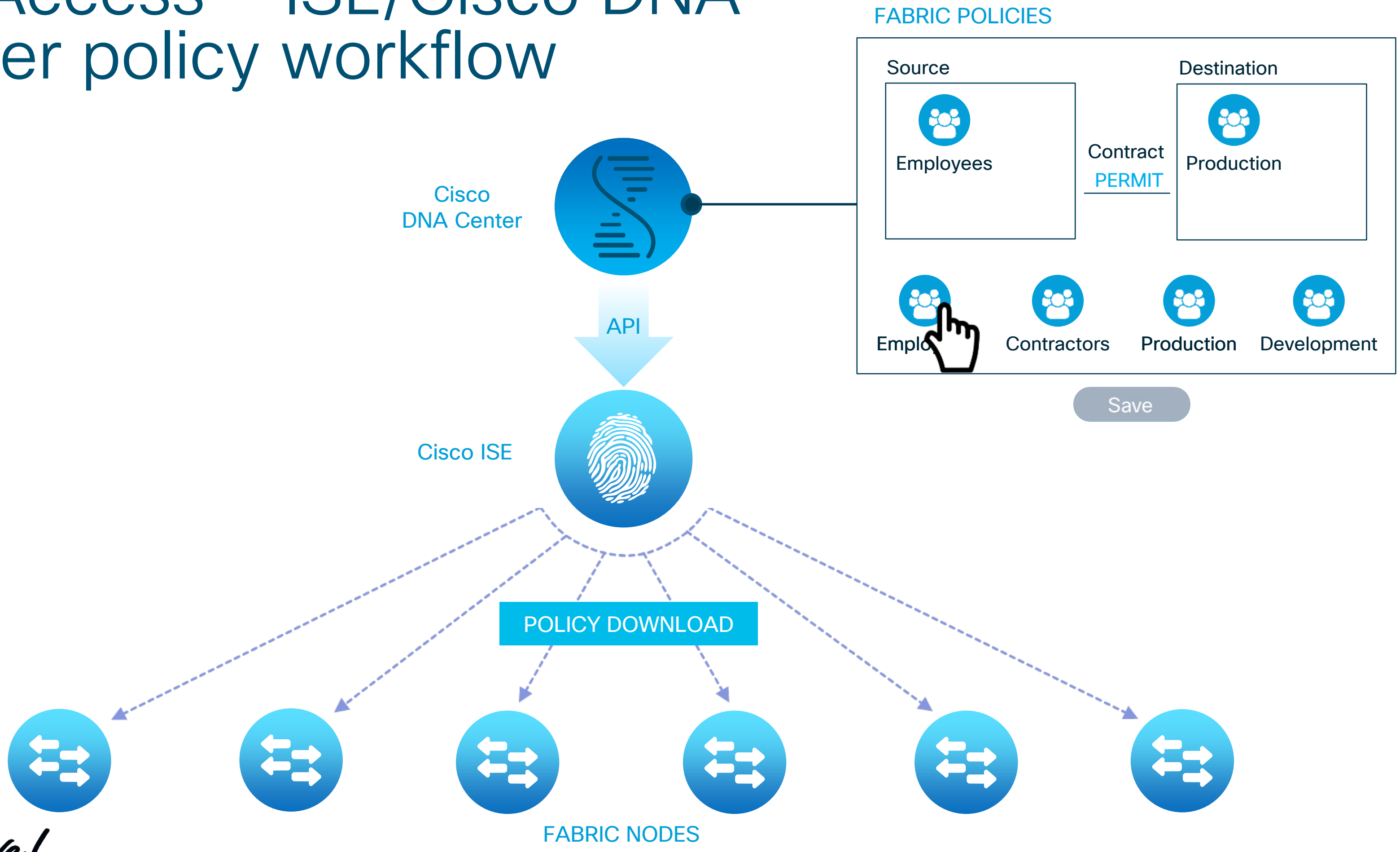


Virtual Routing & Forwarding

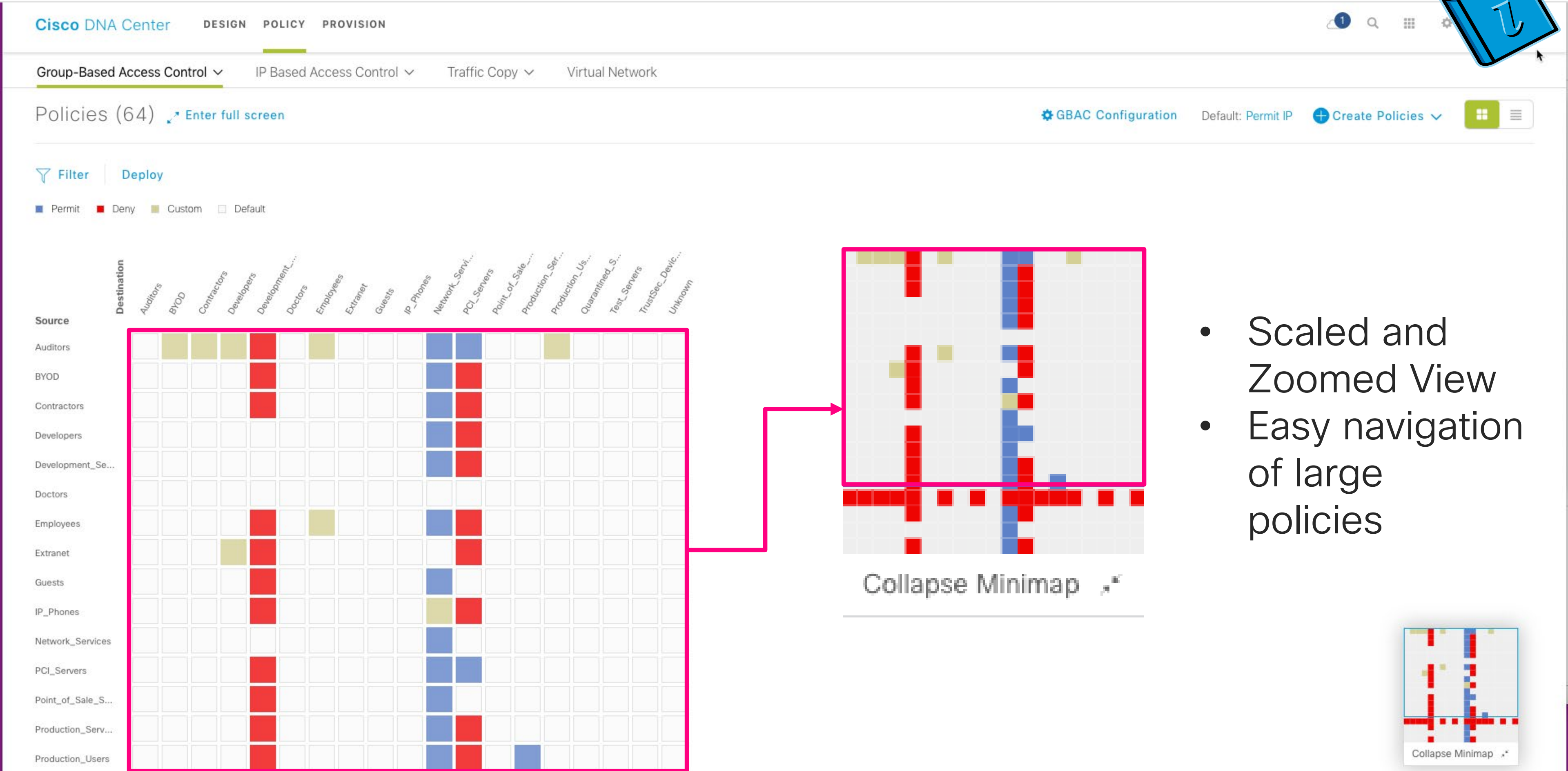
Scalable Group Tagging

Use Case – SGT/VXLAN

SD-Access – ISE/Cisco DNA Center policy workflow



Policy Views in DNAC (Matrix View)



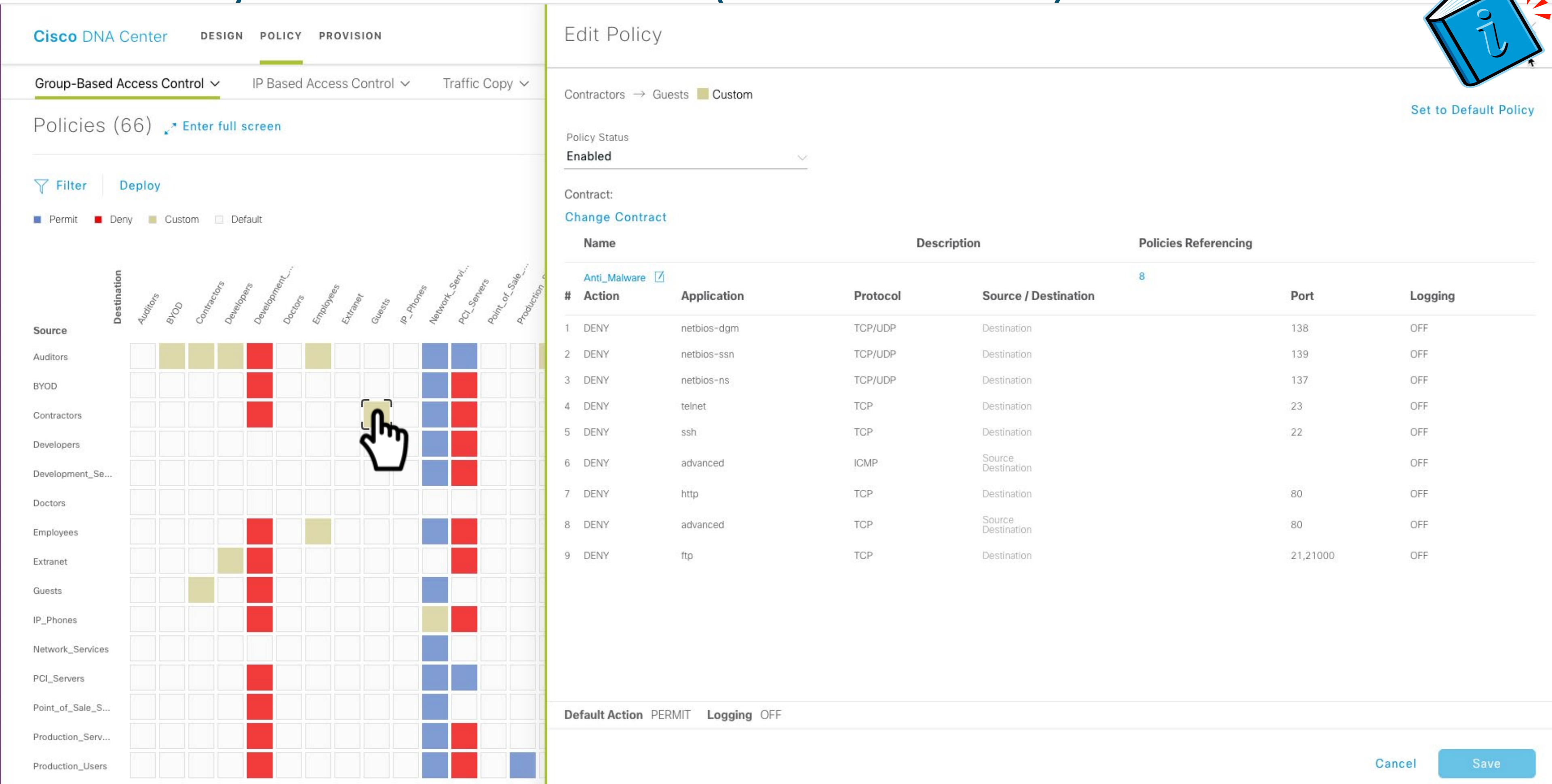
🟦 Permit 🟥 Deny 🟨 Custom □ Default

Source \ Destination	Auditors	BYOD	Contractors	Developers	Development_...	Doctors	Employees	Extranet	Guests	IP_Phones	Network_Servi...	PCI_Servers	Point_of_Sale_...	Production_Ser...	Production_Us...	Quarantined_S...	Test_Servers	TrustSec_Devic...	Unknown
Auditors		🟨	🟨	🟨	🟥		🟨				🟦	🟦			🟨				
BYOD					🟥						🟦	🟥							
Contractors					🟥						🟦	🟥							
Developers											🟦	🟥							
Development_Se...											🟦	🟥							
Doctors																			
Employees					🟥		🟨				🟦	🟥							
Extranet				🟨	🟥							🟥							
Guests					🟥						🟦								
IP_Phones					🟥						🟨	🟥							
Network_Services											🟦								
PCI_Servers					🟥						🟦	🟦							
Point_of_Sale_S...					🟥						🟦								
Production_Serv...					🟥						🟦	🟥							
Production_Users					🟥						🟦	🟥		🟦					

- Scaled and Zoomed View
- Easy navigation of large policies

Use Case – SGT/VXLAN

Policy Views in DNAC (Matrix View)



Policies (66)

🟦 Permit 🟥 Deny 🟨 Custom ⬜ Default

Source \ Destination	Auditors	BYOD	Contractors	Developers	Development_...	Doctors	Employees	Extranet	Guests	IP_Phones	Network_Servi...	PCI_Servers	Point_of_Sale_...	Production
Auditors	⬜	🟨	🟨	🟨	🟥	⬜	🟨	⬜	⬜	⬜	🟦	🟦	⬜	⬜
BYOD	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟦	🟥	⬜	⬜
Contractors	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	🟨	⬜	🟦	🟥	⬜	⬜
Developers	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟦	🟥	⬜	⬜
Development_Se...	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟦	🟥	⬜	⬜
Doctors	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Employees	⬜	⬜	⬜	⬜	🟥	⬜	🟨	⬜	⬜	⬜	🟦	🟥	⬜	⬜
Extranet	⬜	⬜	⬜	🟨	🟥	⬜	⬜	⬜	⬜	⬜	⬜	🟥	⬜	⬜
Guests	⬜	⬜	🟨	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟦	⬜	⬜	⬜
IP_Phones	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟨	🟥	⬜	⬜
Network_Services	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟦	⬜	⬜	⬜
PCI_Servers	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟦	🟦	⬜	⬜
Point_of_Sale_S...	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟦	⬜	⬜	⬜
Production_Serv...	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟦	🟥	⬜	⬜
Production_Users	⬜	⬜	⬜	⬜	🟥	⬜	⬜	⬜	⬜	⬜	🟦	🟥	⬜	🟦

Edit Policy

Contractors → Guests 🟨 Custom

Set to Default Policy

Policy Status: Enabled

Contract:

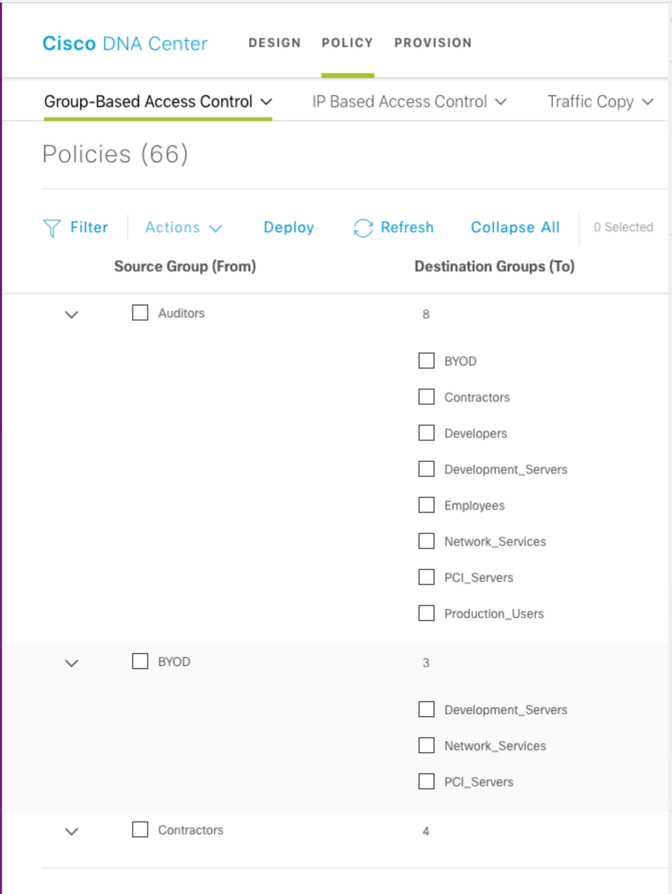
Change Contract

Name	Description	Policies Referencing
Anti_Malware		8

#	Action	Application	Protocol	Source / Destination	Port	Logging
1	DENY	netbios-dgm	TCP/UDP	Destination	138	OFF
2	DENY	netbios-ssn	TCP/UDP	Destination	139	OFF
3	DENY	netbios-ns	TCP/UDP	Destination	137	OFF
4	DENY	telnet	TCP	Destination	23	OFF
5	DENY	ssh	TCP	Destination	22	OFF
6	DENY	advanced	ICMP	Source Destination		OFF
7	DENY	http	TCP	Destination	80	OFF
8	DENY	advanced	TCP	Source Destination	80	OFF
9	DENY	ftp	TCP	Destination	21,21000	OFF

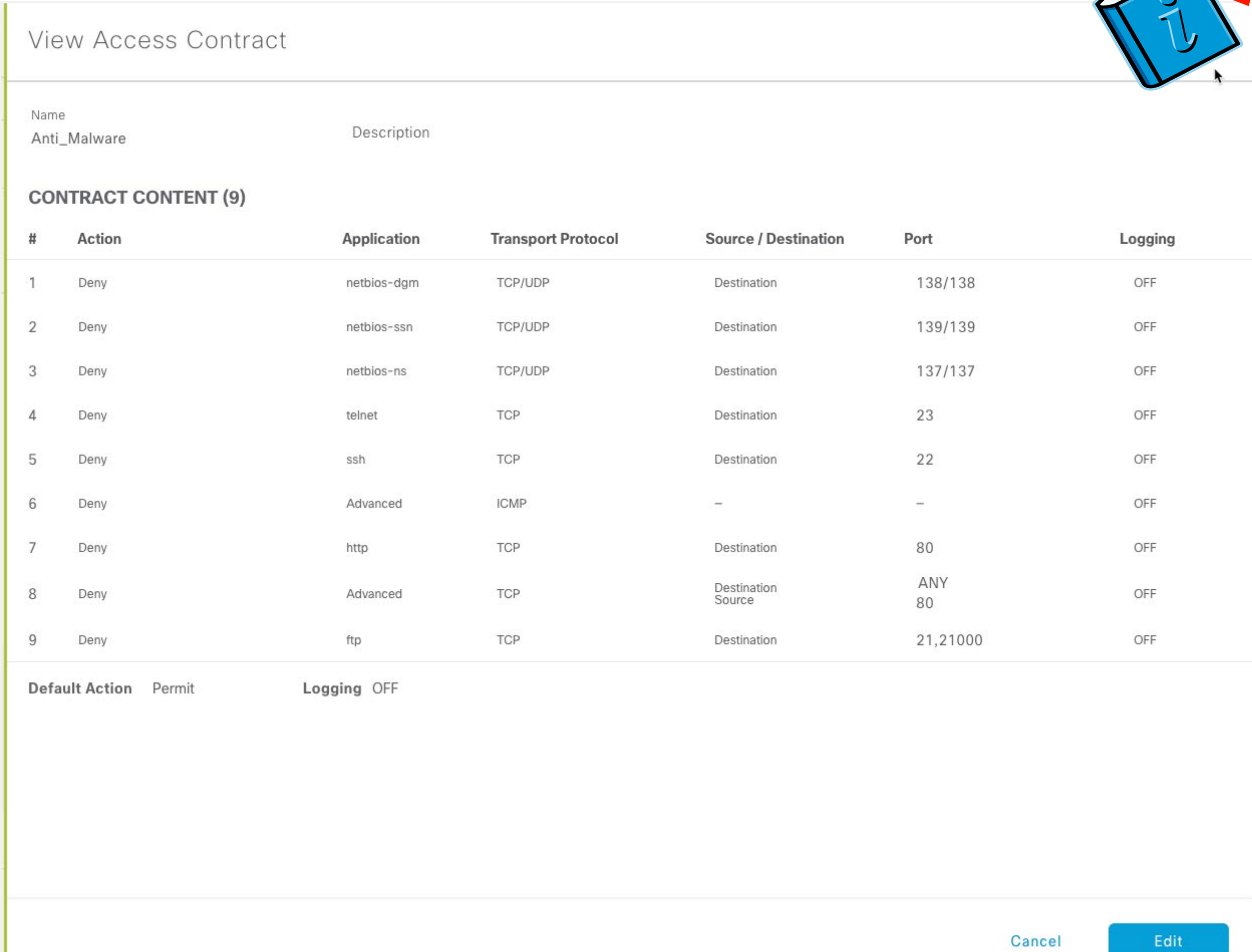
Default Action PERMIT Logging OFF

Policy Views in DNAC (List View)



Policies (66)

Source Group (From)	Destination Groups (To)
□ Auditors	8
	□ BYOD
	□ Contractors
	□ Developers
	□ Development_Servers
	□ Employees
	□ Network_Services
	□ PCI_Servers
	□ Production_Users
□ BYOD	3
	□ Development_Servers
	□ Network_Services
	□ PCI_Servers
□ Contractors	4



Name
Anti_Malware

Description

CONTRACT CONTENT (9)

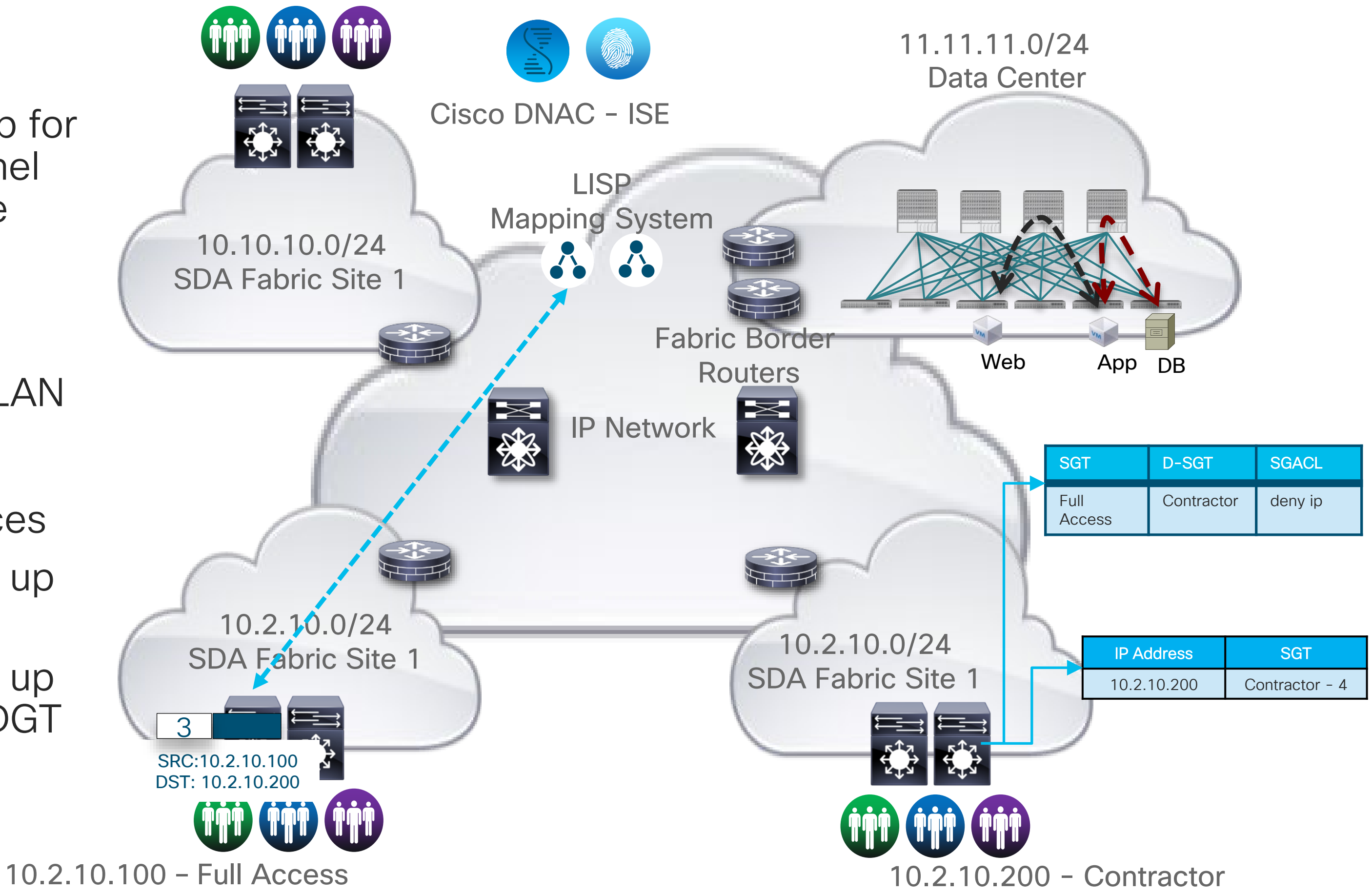
#	Action	Application	Transport Protocol	Source / Destination	Port	Logging
1	Deny	netbios-dgm	TCP/UDP	Destination	138/138	OFF
2	Deny	netbios-ssn	TCP/UDP	Destination	139/139	OFF
3	Deny	netbios-ns	TCP/UDP	Destination	137/137	OFF
4	Deny	telnet	TCP	Destination	23	OFF
5	Deny	ssh	TCP	Destination	22	OFF
6	Deny	Advanced	ICMP	–	–	OFF
7	Deny	http	TCP	Destination	80	OFF
8	Deny	Advanced	TCP	Destination Source	ANY 80	OFF
9	Deny	ftp	TCP	Destination	21,21000	OFF

Default Action Permit **Logging** OFF

Use Case – SGT/VXLAN

SD-Access Example Topology

1. LISP Routing Lookup for destination IP. Tunnel location found – see BRKCRS for all the details
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



SGT	D-SGT	SGACL
Full Access	Contractor	deny ip

IP Address	SGT
10.2.10.200	Contractor – 4

* Needs IOS IP Services license

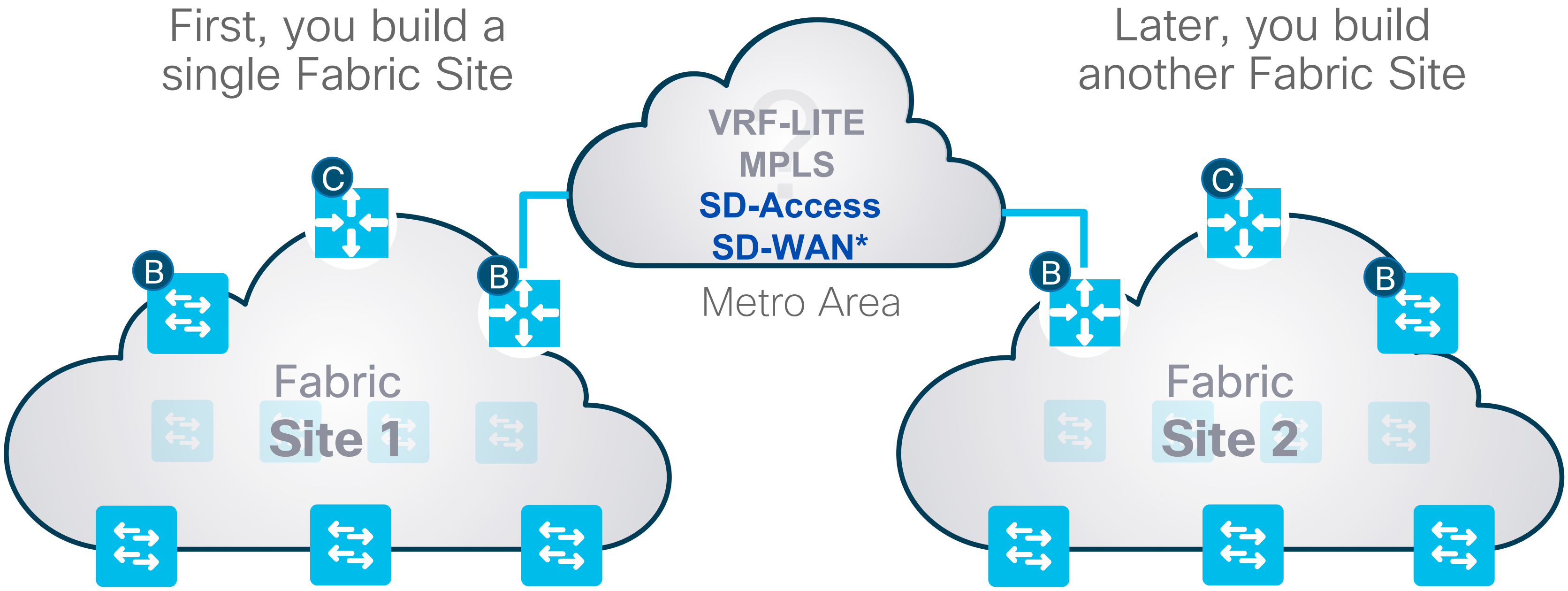
SD-Access – SGT/VXLAN Configuration

- Configuration can be done manually or automated via Cisco DNAC
- Single command for turning on SGT being carried in VXLAN via CLI
- SGT enabled automatically with Cisco DNAC
- 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
```

Fabric Sites & Domains

Connecting Multiple Fabrics


First, you build a single Fabric Site
Later, you build another Fabric Site
VRF-LITE
MPLS
SD-Access
SD-WAN*
Metro Area
C
B
B
Fabric Site 1
C
B
B
Fabric Site 2

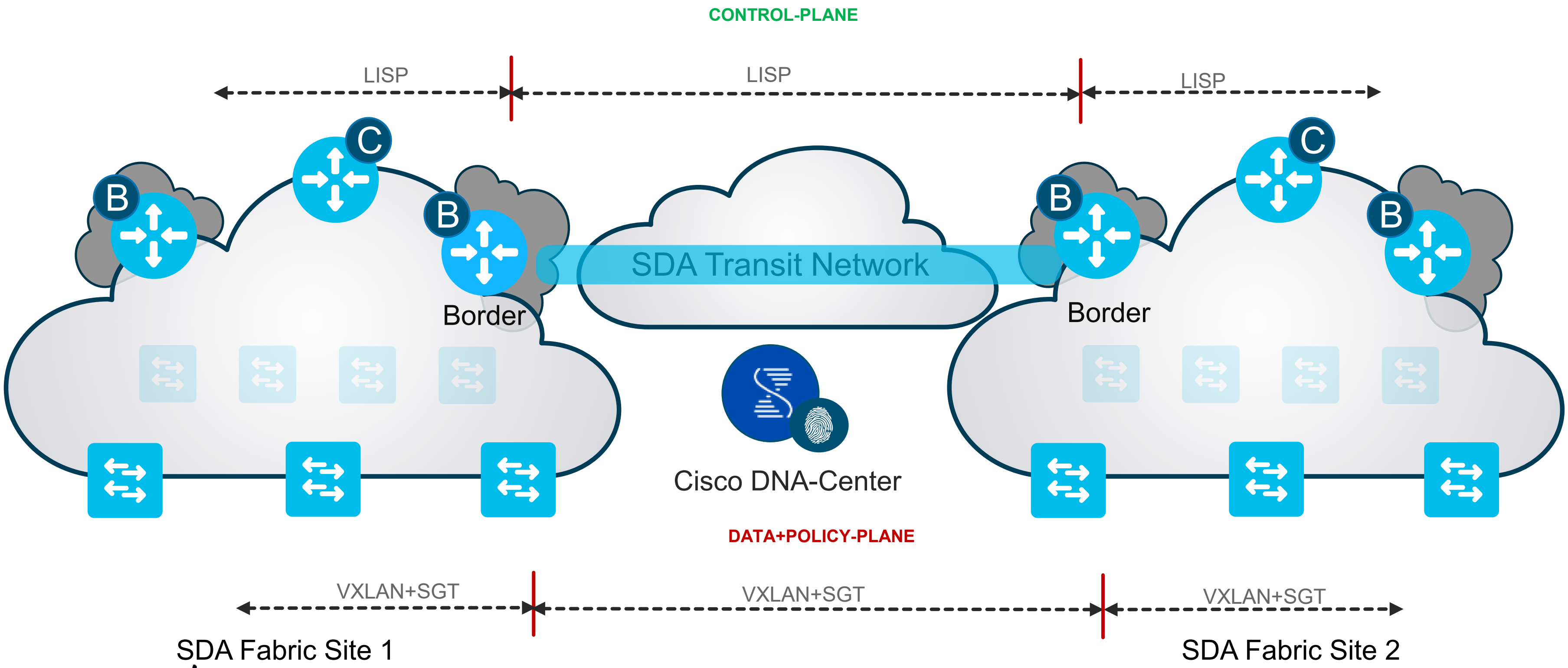
How do you connect them together?

* Q2CY20

SD-Access for Distributed Campus

SD-Access Transit

Use Case – SGT/VXLAN



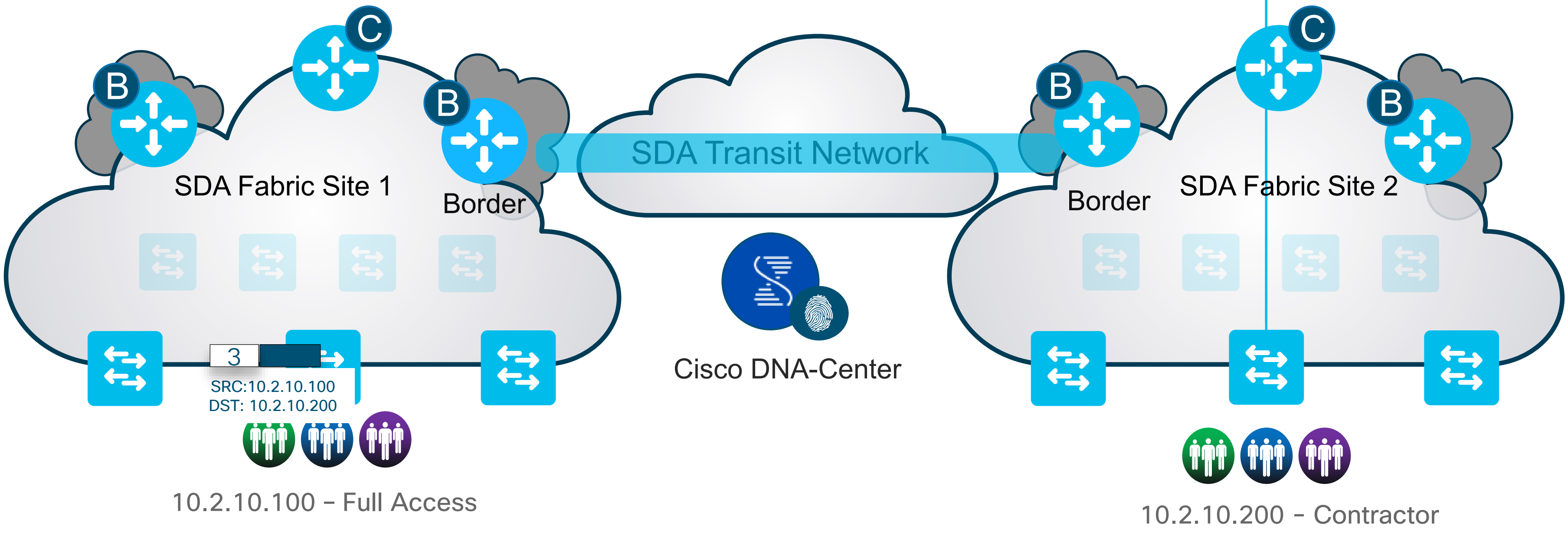
Use Case – SGT/VXLAN

SD-Access for Distributed Campus

SD-Access Transit

SGT	D-SGT	SGACL
Full Access	Contractor	deny ip

IP Address	SGT
10.2.10.200	Contractor – 4



Firewall Integration with SD-Access

Border Deployment Options - Firewalls

Non-SGT aware Firewall:

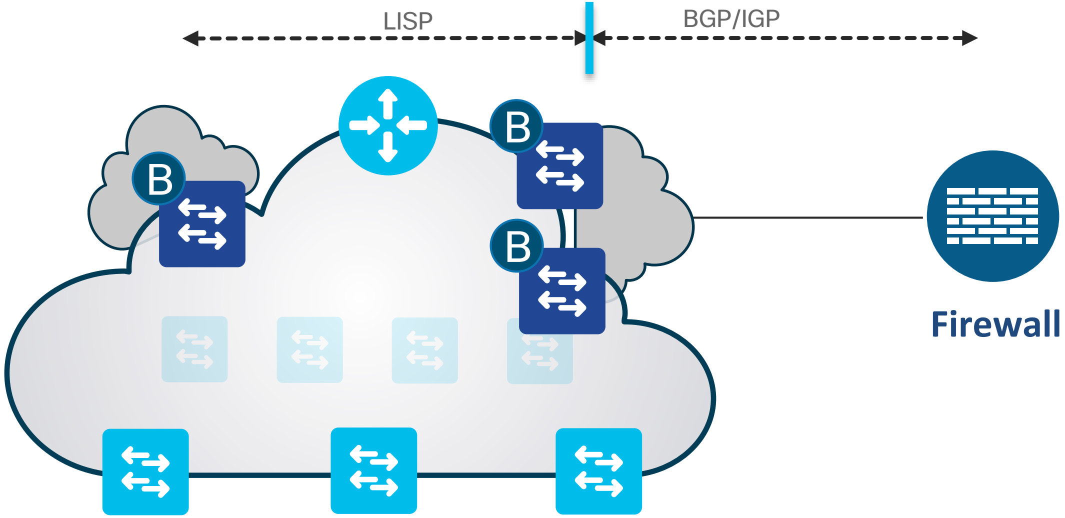
- Firewall is connected externally to the Campus Fabric.
- The prefixes from the local Campus Fabric domain will be advertised to the firewall with a routing protocol of choice.
- Firewall policy is based Interface or Subnet IP/mask and IP ACL's.

SGT aware Firewall :

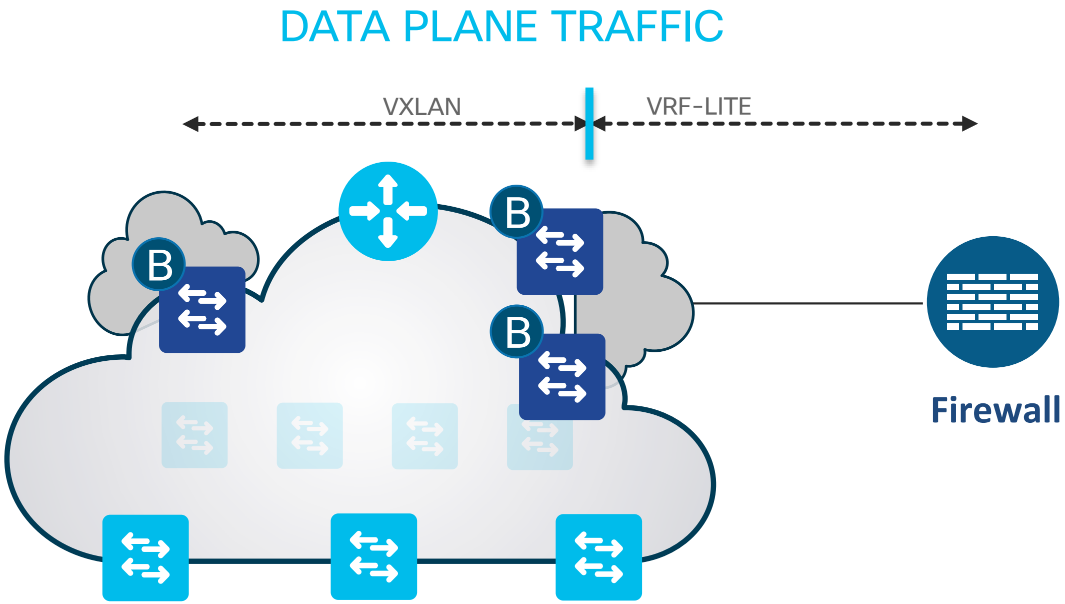
- Firewall is connected externally to the Campus Fabric.
- The prefixes from the local Campus Fabric domain will be advertised to the firewall with a routing protocol of choice.
- SXP connection between ISE and Firewall used for derivation of SGTs on the Firewall.
- Firewall policy is based on SGT's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

Border Deployment Options – Firewalls

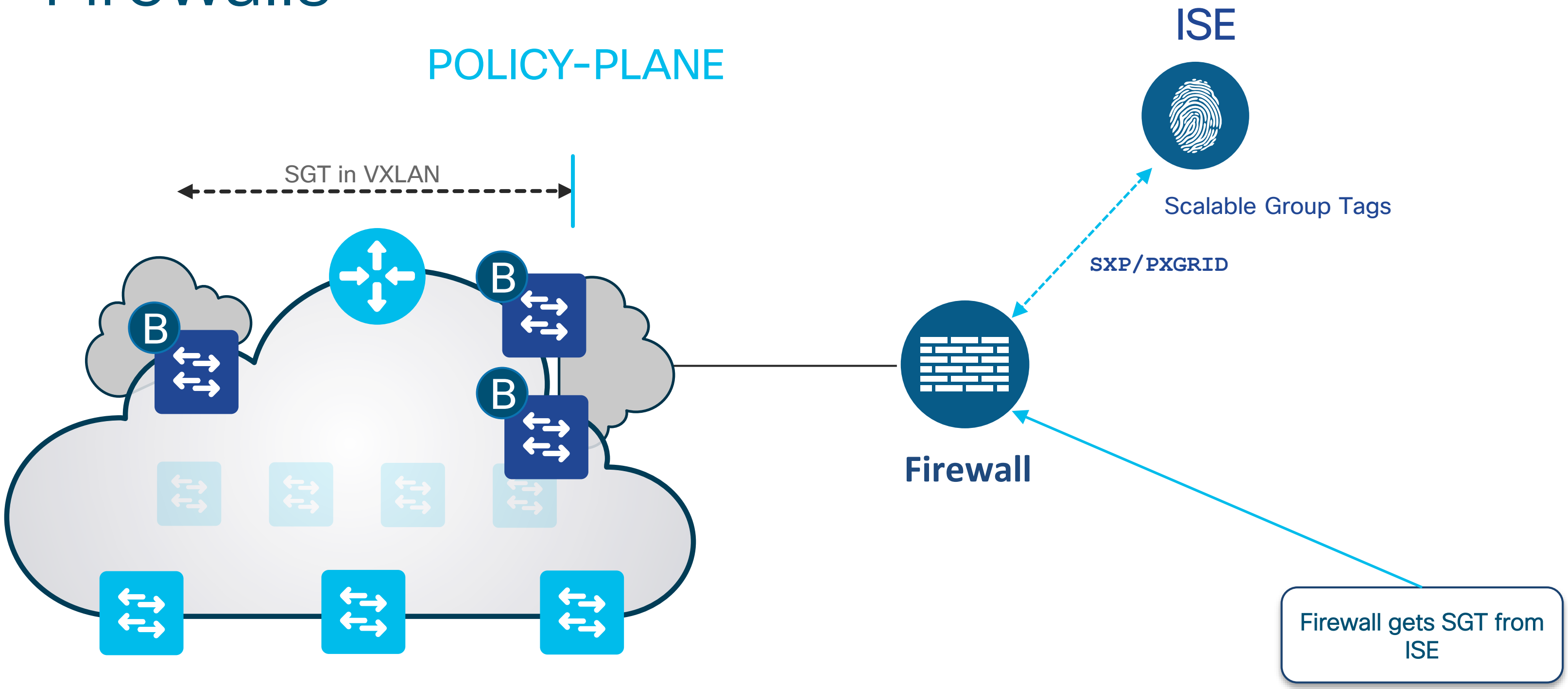
CONTROL PLANE TRAFFIC



Border Deployment Options – Firewalls

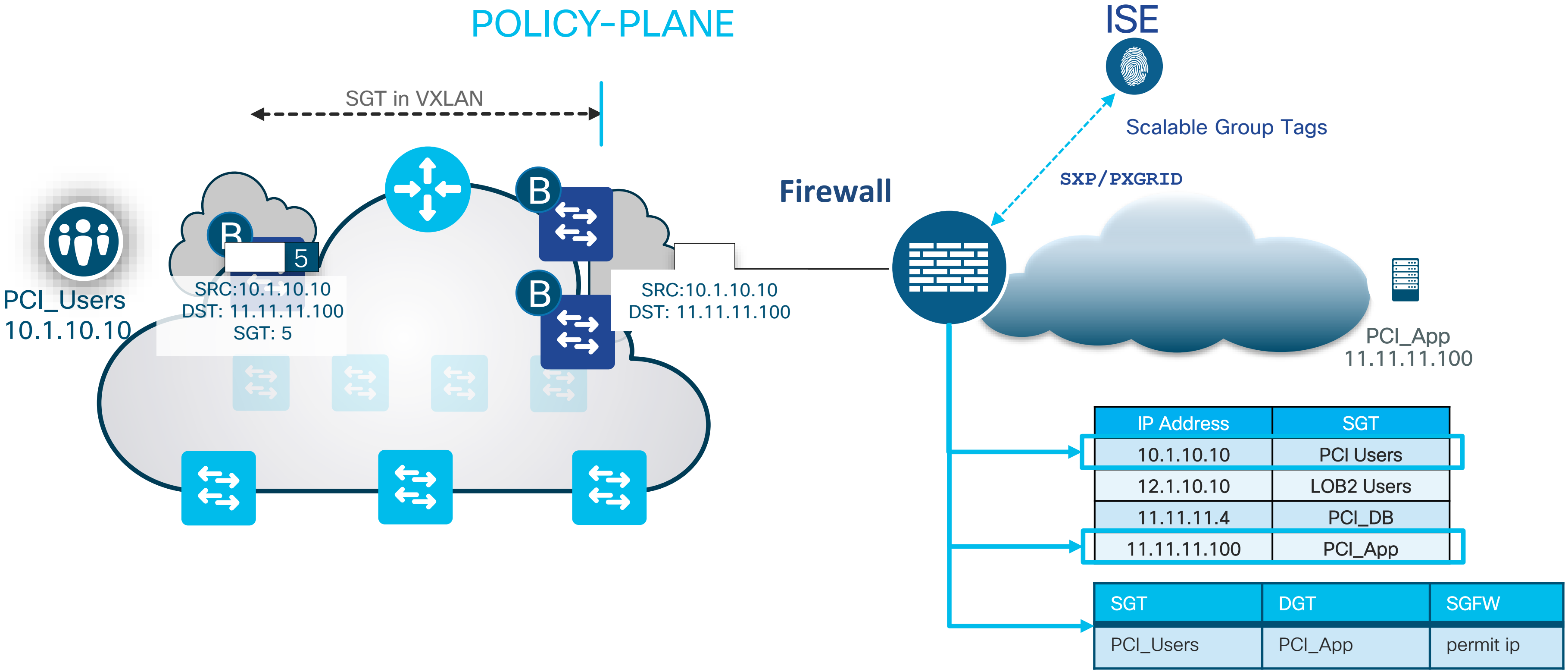


Border Deployment Options – Firewalls



Use Case – SGT/VXLAN

Single VN - Endpoint to Application

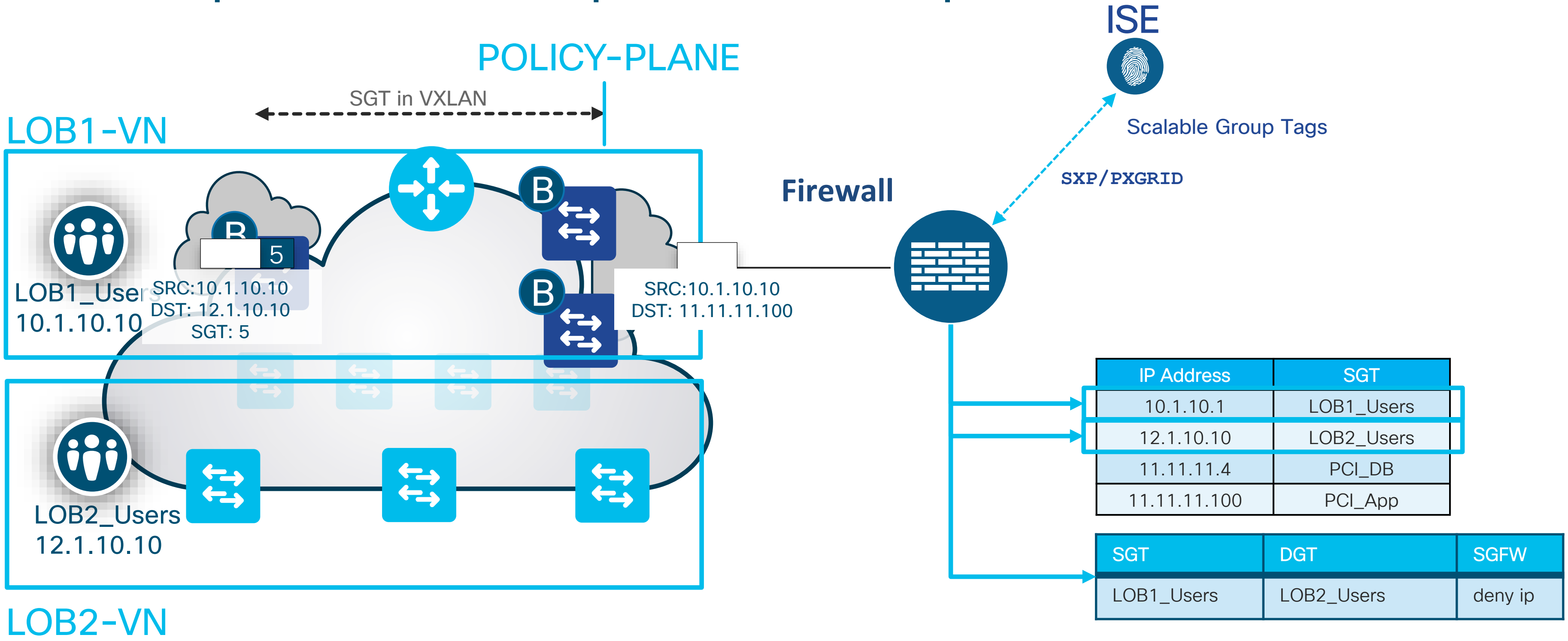


IP Address	SGT
10.1.10.10	PCI Users
12.1.10.10	LOB2 Users
11.11.11.4	PCI_DB
11.11.11.100	PCI_App

SGT	DGT	SGFW
PCI_Users	PCI_App	permit ip

cisco Live!

Multiple 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

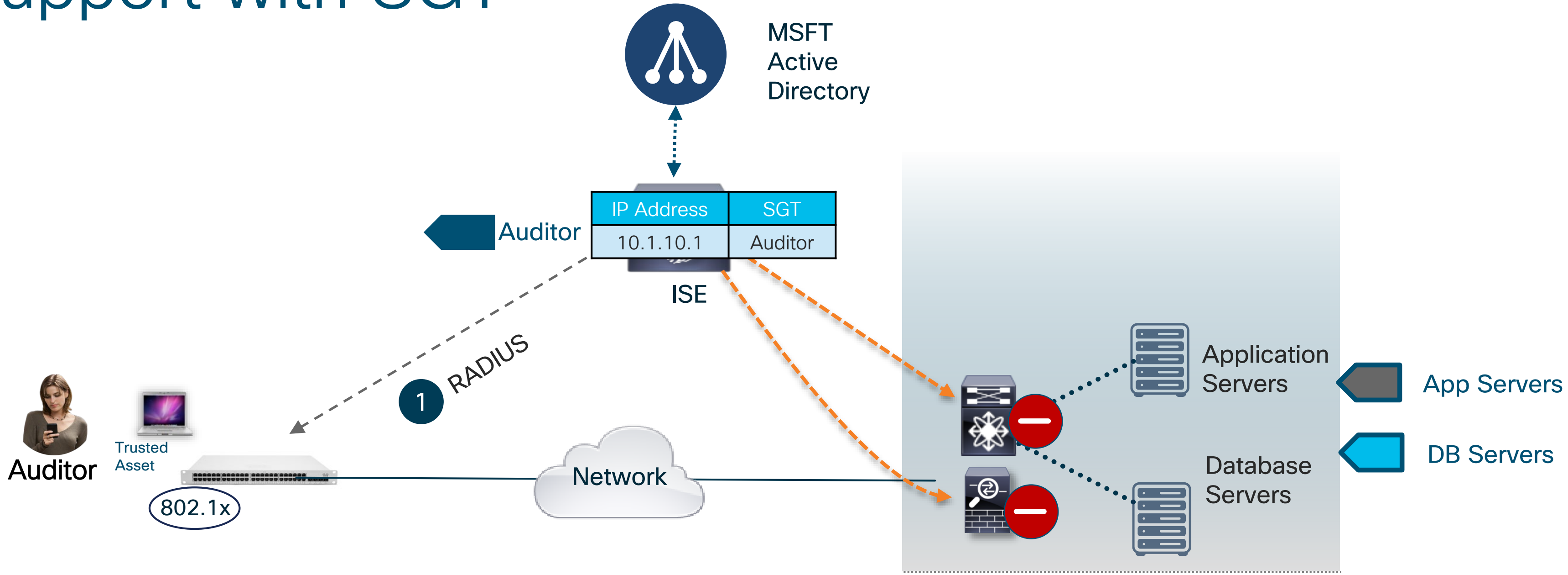
SGT	DGT	SGFW
LOB1_Users	LOB2_Users	deny ip

FTD prior to 6.5 cannot use SGT for Destinations in Policies

FTD as of 6.5 CAN use SGT for Source and Destination in Policy

Meraki and 3rd Party Interop

Meraki* and 3rd Party Switch Support with SGT



IP Address	SGT
10.1.10.1	Auditor

- RADIUS Authentication/authorization/Accounting MUST go to ISE
- RADIUS Accounting MUST be in a format ISE can use to bind the IP and SGT together
- * – MS390 and MR APs will support “Adaptive Policy” i.e. SGT/SGACL

Common Questions about Deployment with Non Cisco RADIUS or NAC Solutions

- ”What if I don’t have ISE for 802.1X/MAB AAA?”
  - Any RADIUS server can return the SGT
  - ISE just for SGACL management
  - ISE proxy and does user authorization/SGACL management
- ”What if I am using a passive monitoring solution for NAC?”
  - Current integration with several vendors
  - Vendors chose one of two options for sharing their classification
  - Some chose to write IP/SGT CLI to access Device
  - Some chose to write to REST API in ISE or IOS API which then sends data to the network

RADIUS Proxy

0 SGACL downloaded from ISE for ‘Protected Services’

1 802.1X / MAC authentication request to Cisco ISE

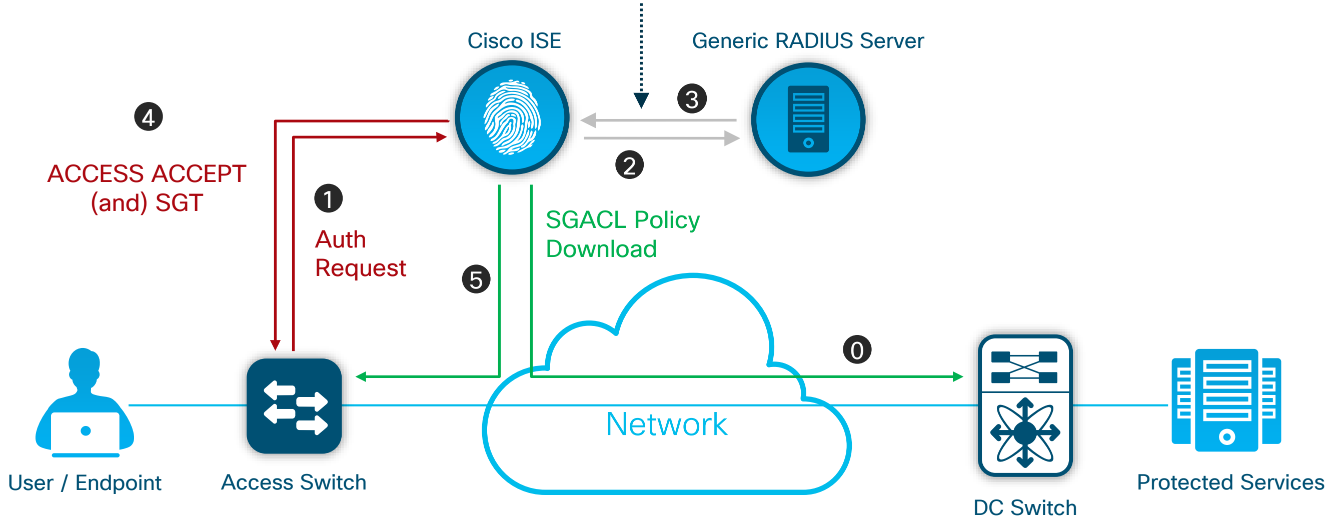
2 ISE proxies the 802.1X / MAB request to RADIUS server

3 RADIUS Server returns access accept with IETF attribute [1] – username

4 ISE inspects username and matches authorization Rule in ISE for SGT assignment

5 SGACL for SGT-100 (Hex 64) “Trusted Asset” is downloaded from ISE

[Cisco RADIUS AVP] cts:security-group-tag-0064-0
Or
Any authorization attributes



- ISE is authoritative for SGT assignment and SGACL definitions.
- Migration to ISE for authorization easy “if” desired

- More complex coexistence for authentications and authorizations

RADIUS → RADIUS Proxy → Policy download

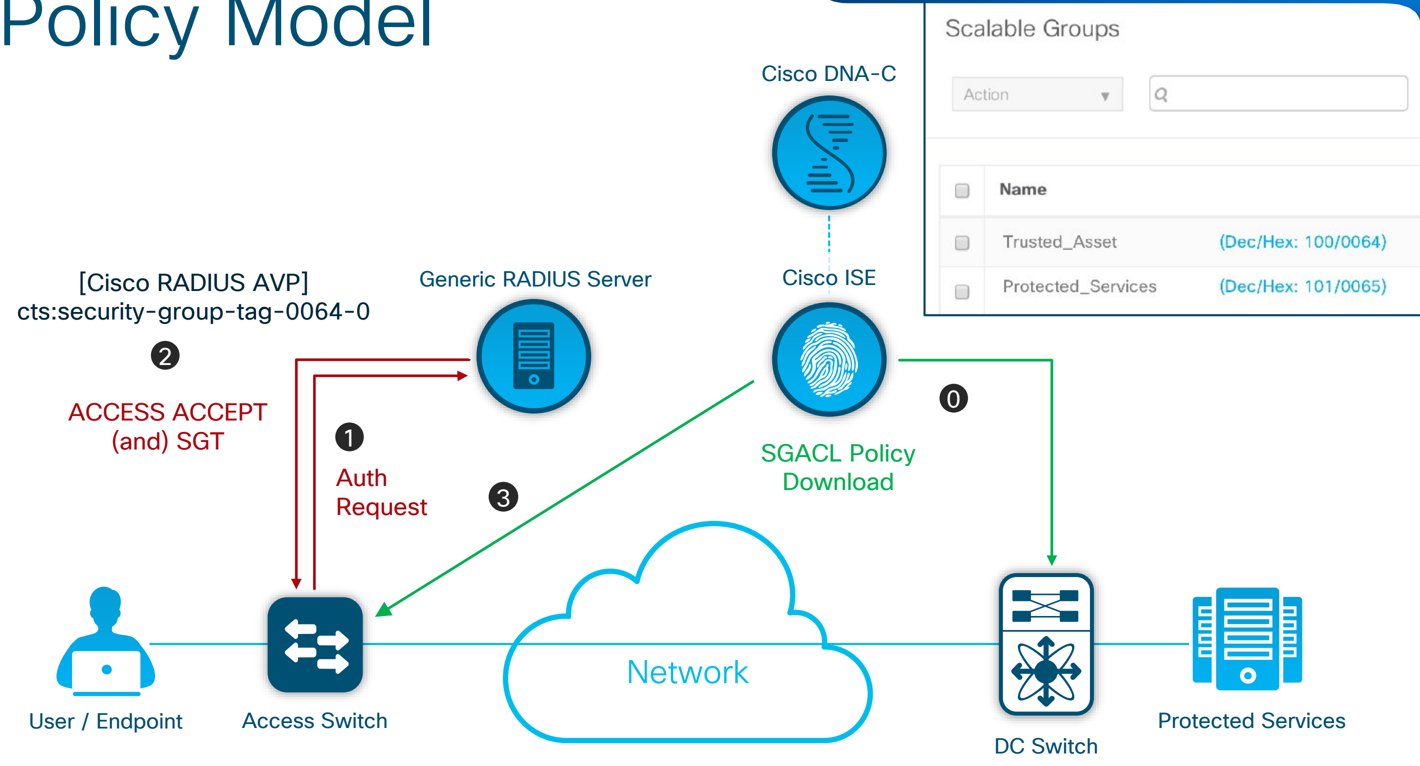
Delineated Policy Model

0. SGACL downloaded from ISE for ‘Protected Services’

1. 802.1X / MAC authentication request to RADIUS server

2. RADIUS server sends ACCESS-ACCEPT and Cisco AVP: cts:security-group-tag-xx

3. SGACL for SGT-100 (Hex 64) is downloaded from ISE



Scalable Groups

Action ▾

□	Name	
□	Trusted_Asset	(Dec/Hex: 100/0064)
□	Protected_Services	(Dec/Hex: 101/0065)

👍
- Any/Existing RADIUS Server can assign an SGT
- Simple coexistence

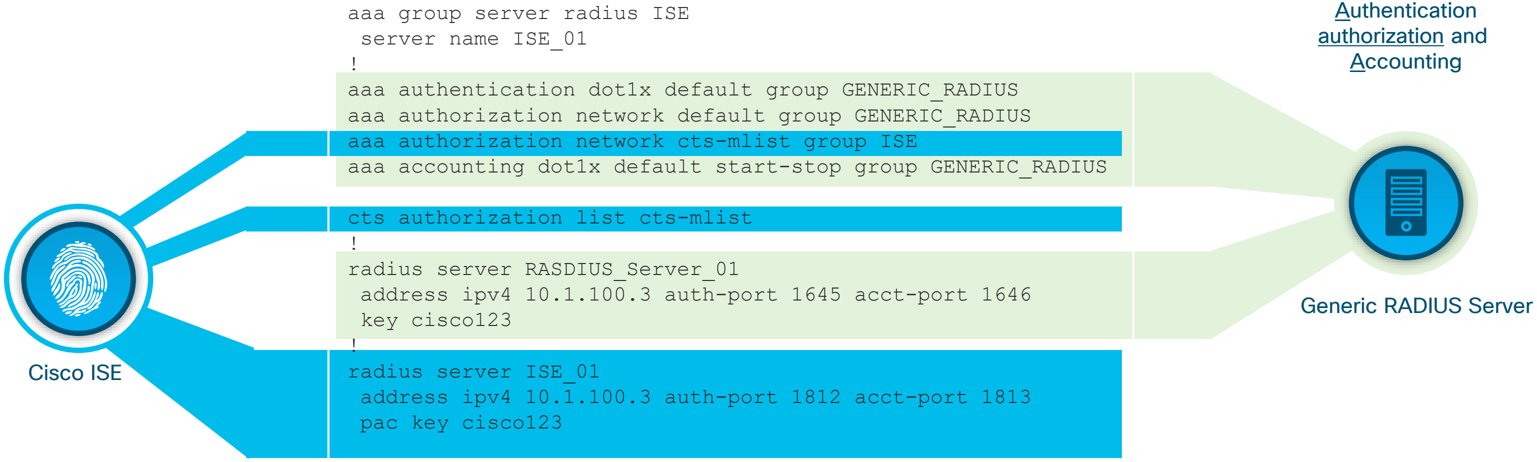
👎
- SGT number value needs to be entered into the RADIUS authorization result by hand

→ RADIUS → Policy download

Delineated Policy Model

Switch configurations

```
3850

!
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
```



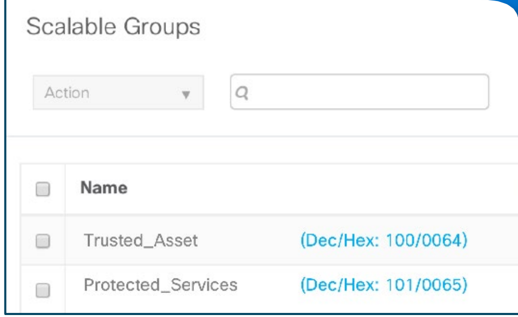
Authentication authorization and Accounting

Generic RADIUS Server

Cisco ISE

Overlay NAC - REST API: IP to SGT

Only officially supported method for SD-Access



Scalable Groups

Action ▾

□	Name	
□	Trusted_Asset	(Dec/Hex: 100/0064)
□	Protected_Services	(Dec/Hex: 101/0065)

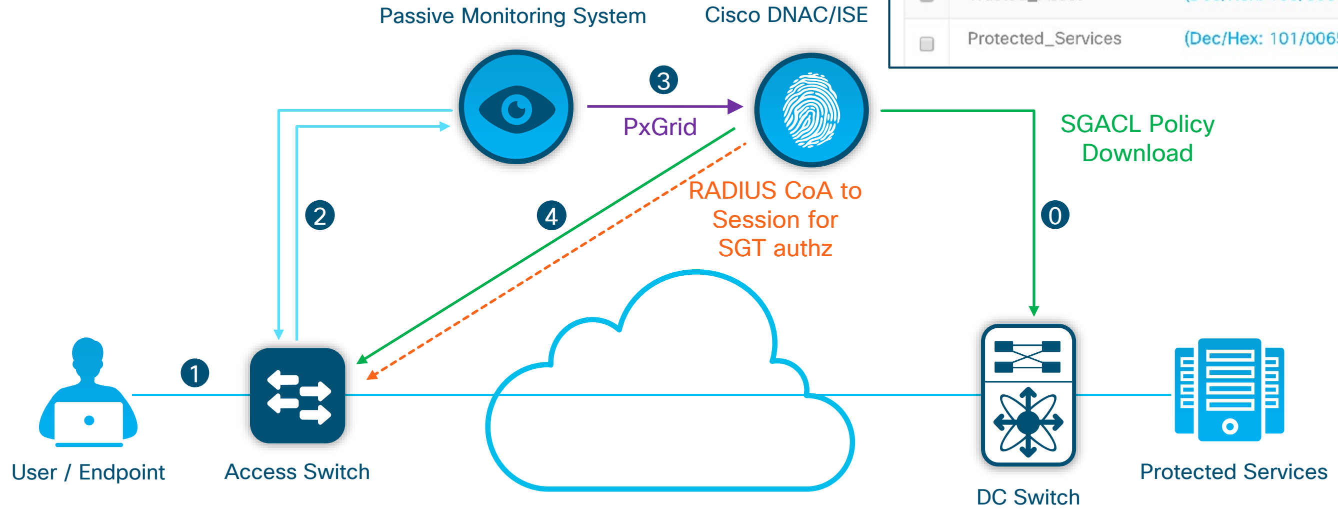
0 SGACL downloaded from ISE for 'Protected Services'

1 Endpoint comes on to the network

2 Passive Monitoring System classifies the endpoint through its mechanisms

3 Passive Monitoring System writes new classification to ISE via PxGrid

4 ISE sends CoA to access switch and this triggers and SGT assignment



👍 Simplified operations through automation

👎 Very chatty, as and when endpoints connect/disconnect to the network, API calls needs to be made to ISE.

→ Discovery/Classification
→ Policy download
⇢ RADIUS/CoA
→ PxGrid

Use Case Review - WAN

Health Care Access Control - Medical Devices (1/2)

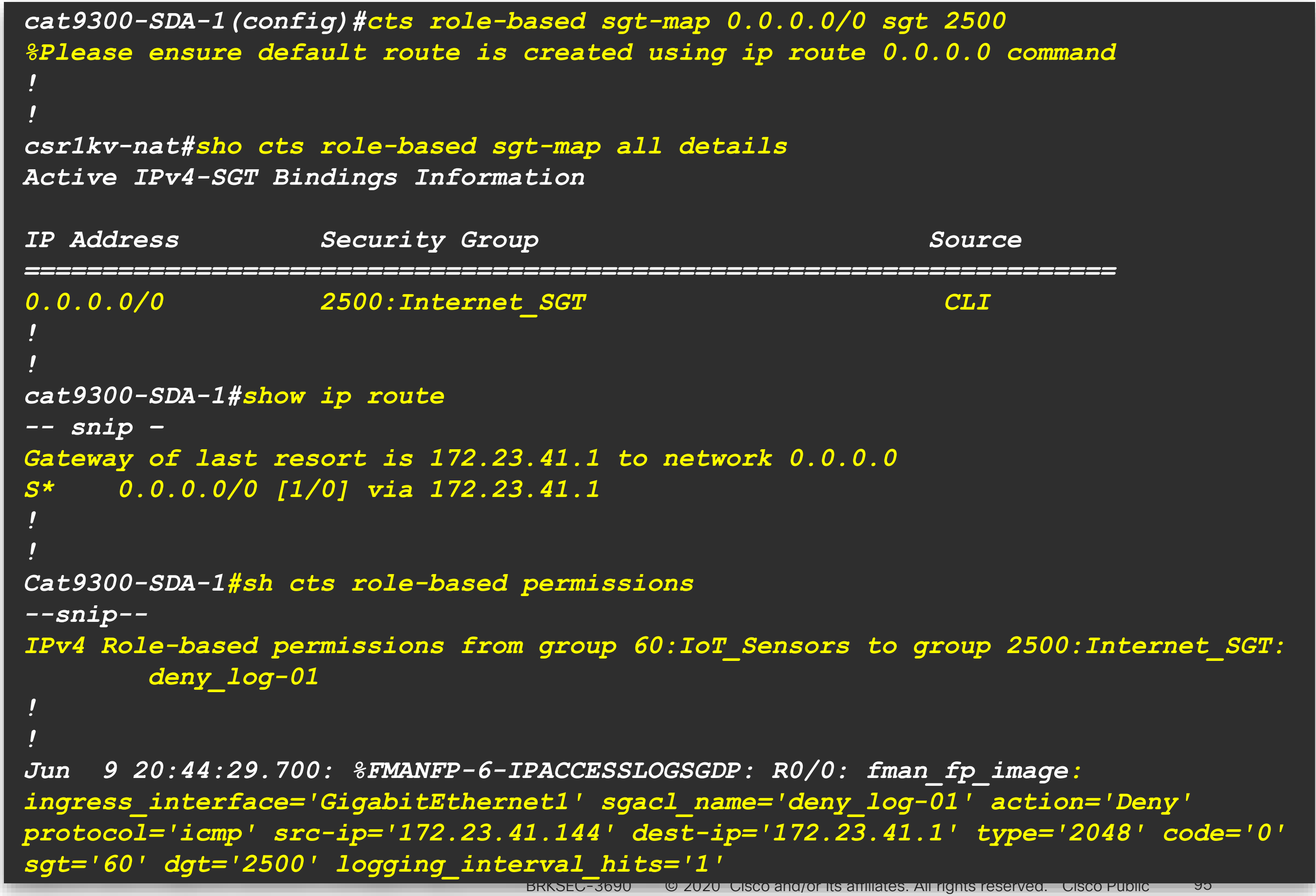
- Business Problem/Background
  - Isolate Medical Devices used for Patient Care
  - Only Authorized users, Devices, and servers access to the medical Devices
- Solution Overview
  - Multi-use workstations use 802.1X to distinguish the user (user experience change)
    - 802.1X is a full machine or user login
    - Windows Fast switching not supported if user identity is needed between desktop swaps.
  - ISE deployed for profiling medical devices
  - Distribution/Core does not support SGT
  - Access Layer capable of bidirectional SXP and filtering on IP/SGT
  - 3650/3850 have limited resource for IP/SGT (12K) and can’t hold all endpoints in network

Health Care Access Control - Medical Devices (2/2)

- Solution Overview
  - Resolved this by only applying SGT to users of medical Device, and servers explicitly allowed access
  - All user or end Devices on network that don't get an SGT assigned do not populate the IP/SGT
  - Advertises a summary IP/SGT (10.0.0.0/8) in SXP.
  - This means only explicitly known users and end Devices get an IP/SGT (/32) while everyone else in the enterprise falls through to the summary IP/SGT (/8)
  - This keeps the SXP total IP/SGT well under 12K for this particular network
- This allows the policy to be Known_SGT <-> Known_SGT = Permit and Summary_SGT<-> Known_SGT = Deny
- Internet Traffic is not tagged. This allows the administrator to use a "reserved" tag called "Unknown" to handle traffic to medical resources.
- Alternative methods for handling "Internet Traffic"
  - Use "default route" classification on N7K, Cat9K to map to a specific 'Internet SGT'
  - Use a range of subnet/SGT on the edge for "public addresses" not owned by the enterprise (i.e. 1.0.0.0/8, 2.0.0.0/7, 4.0.0.0/6, etc…) to map to a specific 'Internet SGT'

Default Route Classification

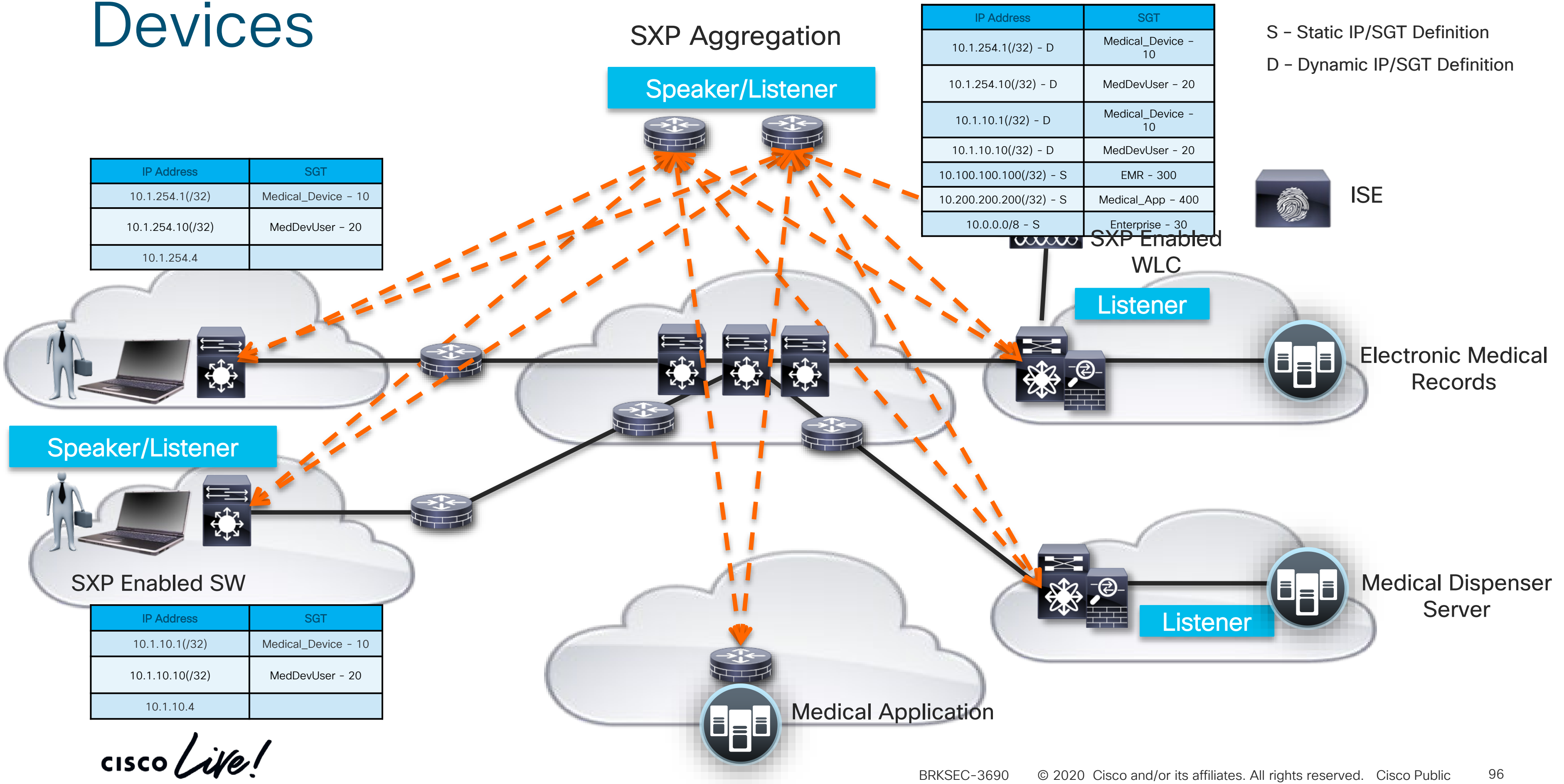
- New in IOS XE 16.11
- Available on N7K in NXOS 7.3(0)D1(1)
- Default route (dynamic or static) must exist for proper classification and enforcement
- 0.0.0.0/0 is not exported via SXP per design specification on IOS XE
- “Except” N7K can allow it via ”cts sxp allow default-route-sgt”



```
cat9300-SDA-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
!
!
csr1kv-nat#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-SDA-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-SDA-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='172.23.41.144' dest-ip='172.23.41.1' type='2048' code='0'
sgt='60' dgt='2500' logging_interval_hits='1'
```

Use Case - WAN

Access Control – Health Care Medical Devices



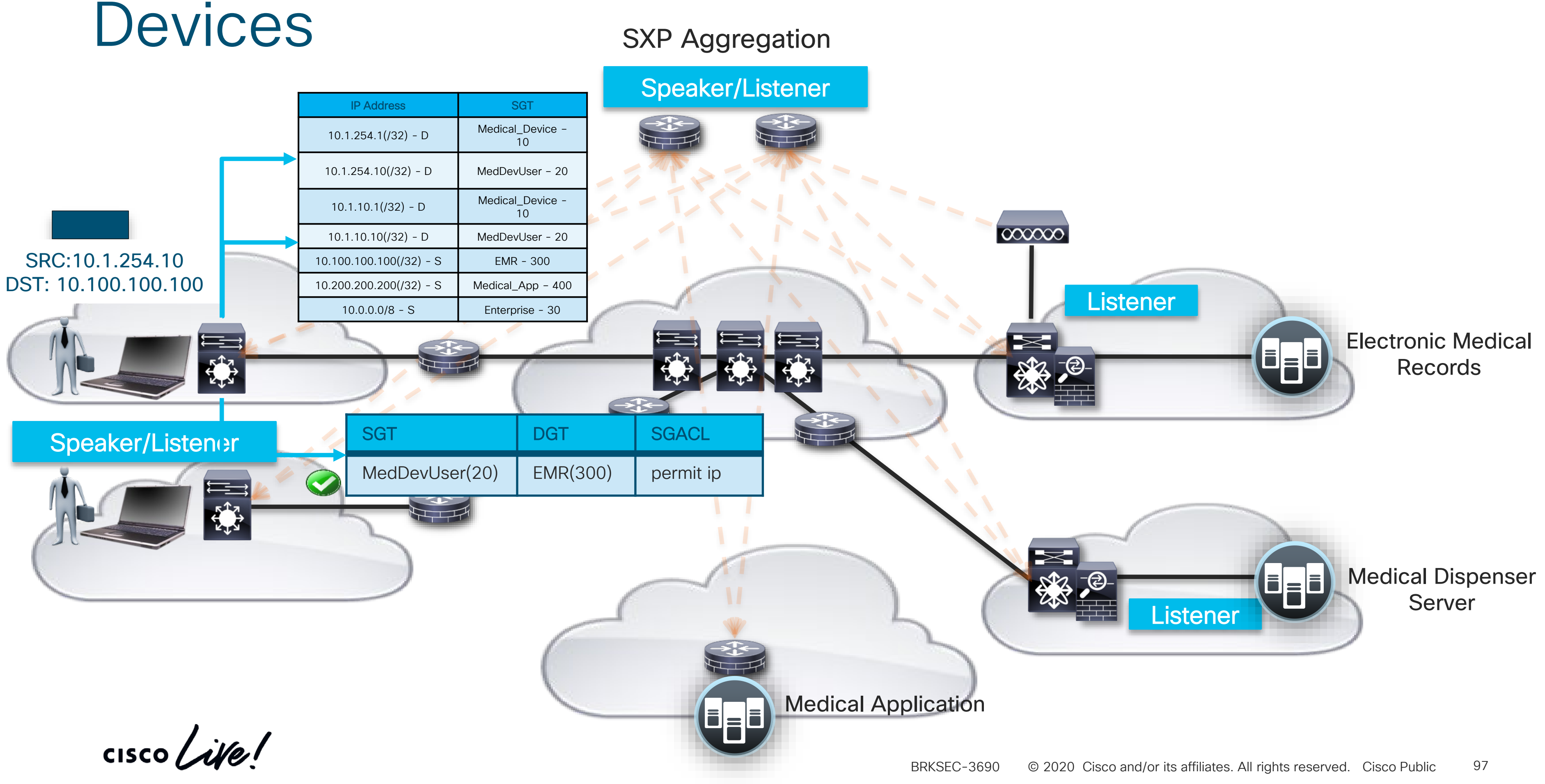
IP Address	SGT
10.1.254.1(/32) – D	Medical_Device – 10
10.1.254.10(/32) – D	MedDevUser – 20
10.1.10.1(/32) – D	Medical_Device – 10
10.1.10.10(/32) – D	MedDevUser – 20
10.100.100.100(/32) – S	EMR – 300
10.200.200.200(/32) – S	Medical_App – 400
10.0.0.0/8 – S	Enterprise – 30

IP Address	SGT
10.1.254.1(/32)	Medical_Device – 10
10.1.254.10(/32)	MedDevUser – 20
10.1.254.4	

IP Address	SGT
10.1.10.1(/32)	Medical_Device – 10
10.1.10.10(/32)	MedDevUser – 20
10.1.10.4	

Use Case - WAN

Access Control – Health Care Medical Devices

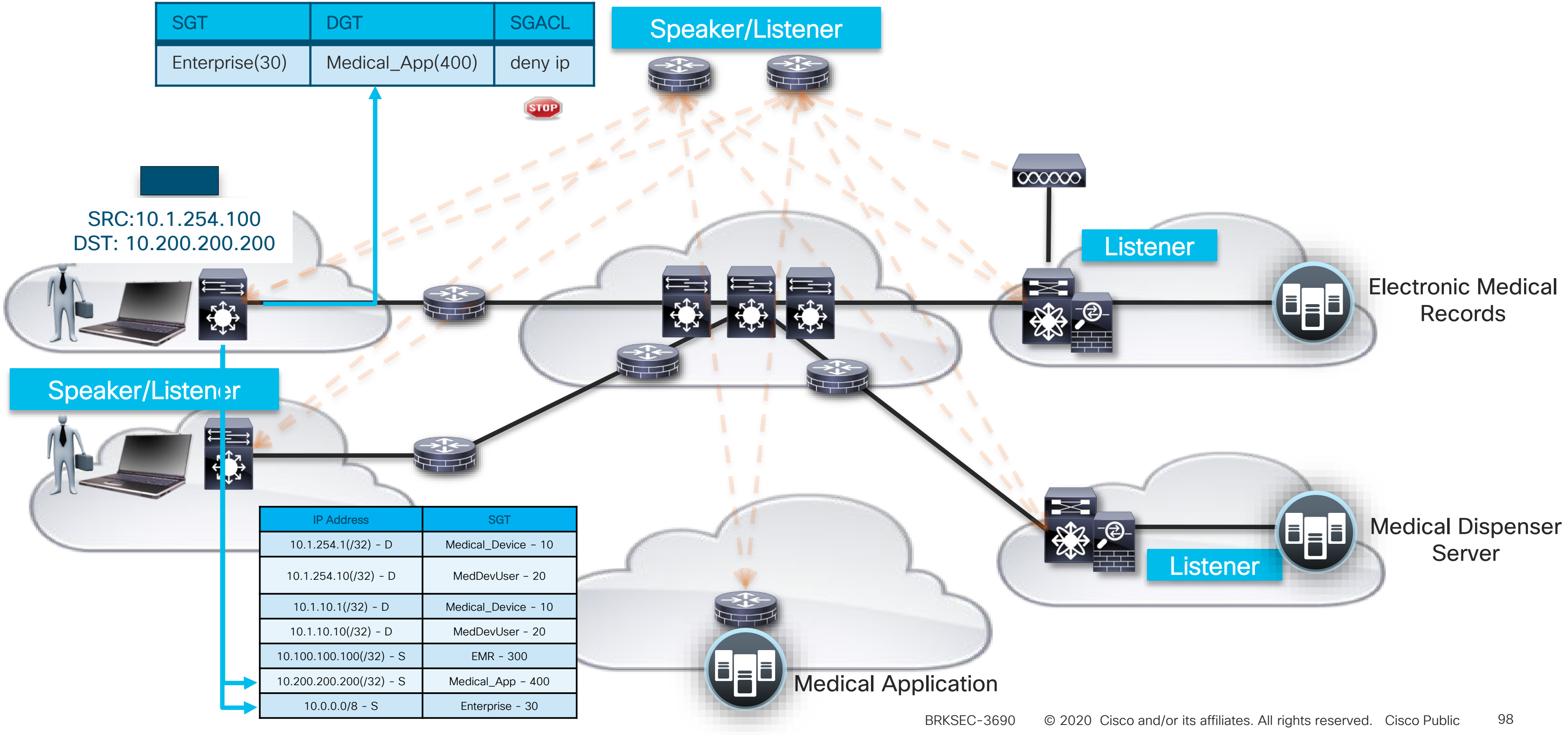


IP Address	SGT
10.1.254.1(/32) - D	Medical_Device - 10
10.1.254.10(/32) - D	MedDevUser - 20
10.1.10.1(/32) - D	Medical_Device - 10
10.1.10.10(/32) - D	MedDevUser - 20
10.100.100.100(/32) - S	EMR - 300
10.200.200.200(/32) - S	Medical_App - 400
10.0.0.0/8 - S	Enterprise - 30

SGT	DGT	SGACL
MedDevUser(20)	EMR(300)	permit ip

Access Control – Health Care Medical Devices

SXP Aggregation



SGT	DGT	SGACL
Enterprise(30)	Medical_App(400)	deny ip

IP Address	SGT
10.1.254.1(/32) – D	Medical_Device – 10
10.1.254.10(/32) – D	MedDevUser – 20
10.1.10.1(/32) – D	Medical_Device – 10
10.1.10.10(/32) – D	MedDevUser – 20
10.100.100.100(/32) – S	EMR – 300
10.200.200.200(/32) – S	Medical_App – 400
10.0.0.0/8 – S	Enterprise – 30

Path Length – Design Consideration

CSCuz01059 –“Path Length Limit” – Integrated 3.6(5)/3.7(4)/16.3(1)/3.17(x)

SXP DB | RBM DB

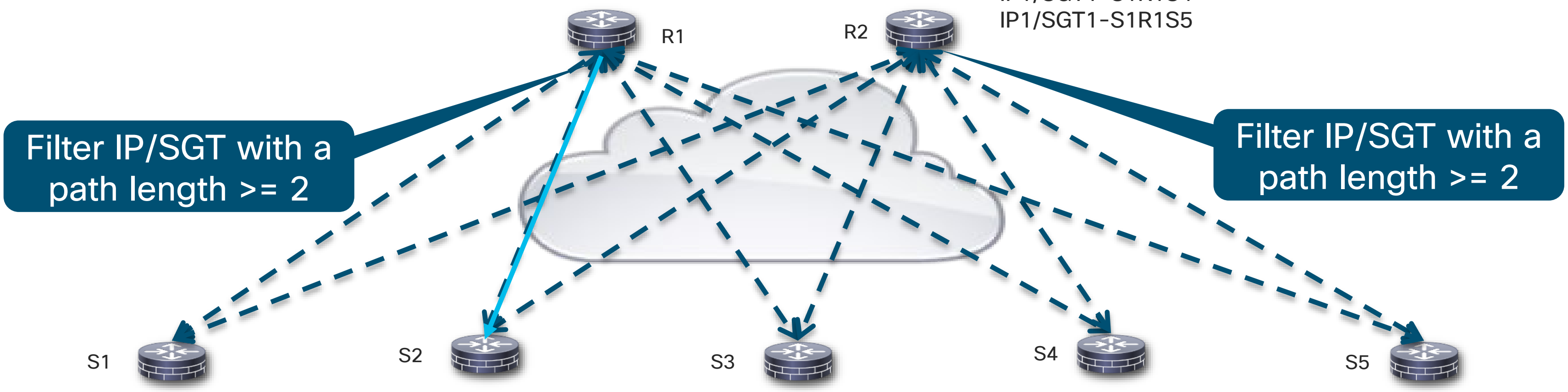
IP1/SGT1-S1
IP1/SGT1-S1R2S2
IP1/SGT1-S1R2S3
IP1/SGT1-S1R2S4
IP1/SGT1-S1R2S5

SXP IP1-SGT1

SXP DB | RBM DB

IP1/SGT1-S1
IP1/SGT1-S1R1S2
IP1/SGT1-S1R1S3
IP1/SGT1-S1R1S4
IP1/SGT1-S1R1S5

SXP IP1/SGT1



Filter IP/SGT with a path length >= 2

Filter IP/SGT with a path length >= 2

SXP DB | RBM DB

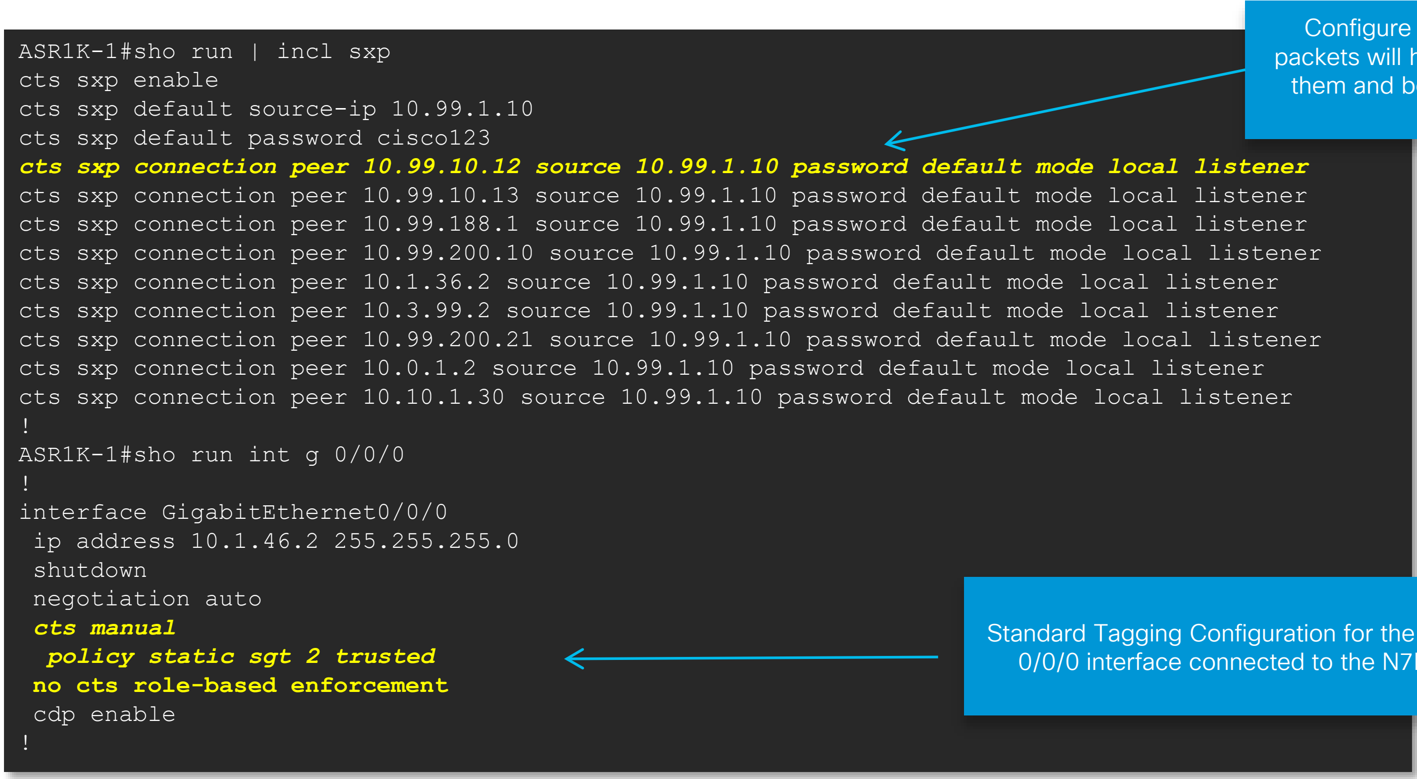
IP1/SGT1-S1R1

IP1/SGT1-S1R2

SXP IP1-SGT1

```
DC-ASR1K-1(config)#cts sxp limit import peer-sequence-nodes 2
DC-ASR1K-1(config)#cts sxp limit export peer-sequence-nodes 2
```

ASR1K Configuration – SXP to Inline SGT

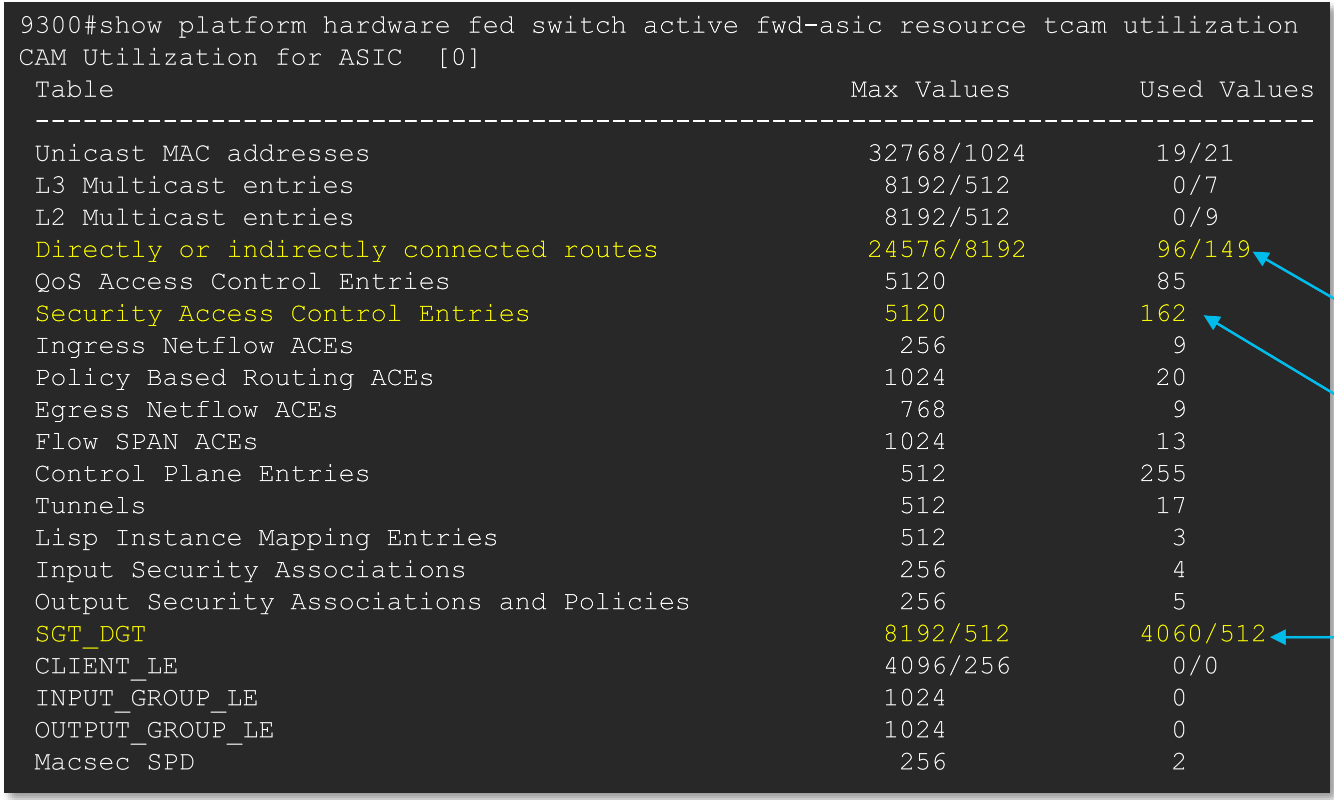


```
ASR1K-1#sho run | incl sxp
cts sxp enable
cts sxp default source-ip 10.99.1.10
cts sxp default password cisco123
cts sxp connection peer 10.99.10.12 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.10.13 source 10.99.1.10 password default mode local listener
cts 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
!
ASR1K-1#sho run int g 0/0/0
!
interface GigabitEthernet0/0/0
 ip address 10.1.46.2 255.255.255.0
 shutdown
 negotiation auto
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
 cdp enable
!
```

Configure SXP as normal. Arriving IP packets will have the SGT associated with them and be tagged on exit via the Gig 0/0/0 int.

Standard Tagging Configuration for the Gig 0/0/0 interface connected to the N7K

Considerations for SGT scaling 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 Counter – 10K limit officially*
- ACE Counter – ACEs are shared with like SGT/DGT
- SGT/DGT Hash table – Cells from the ISE Matrix

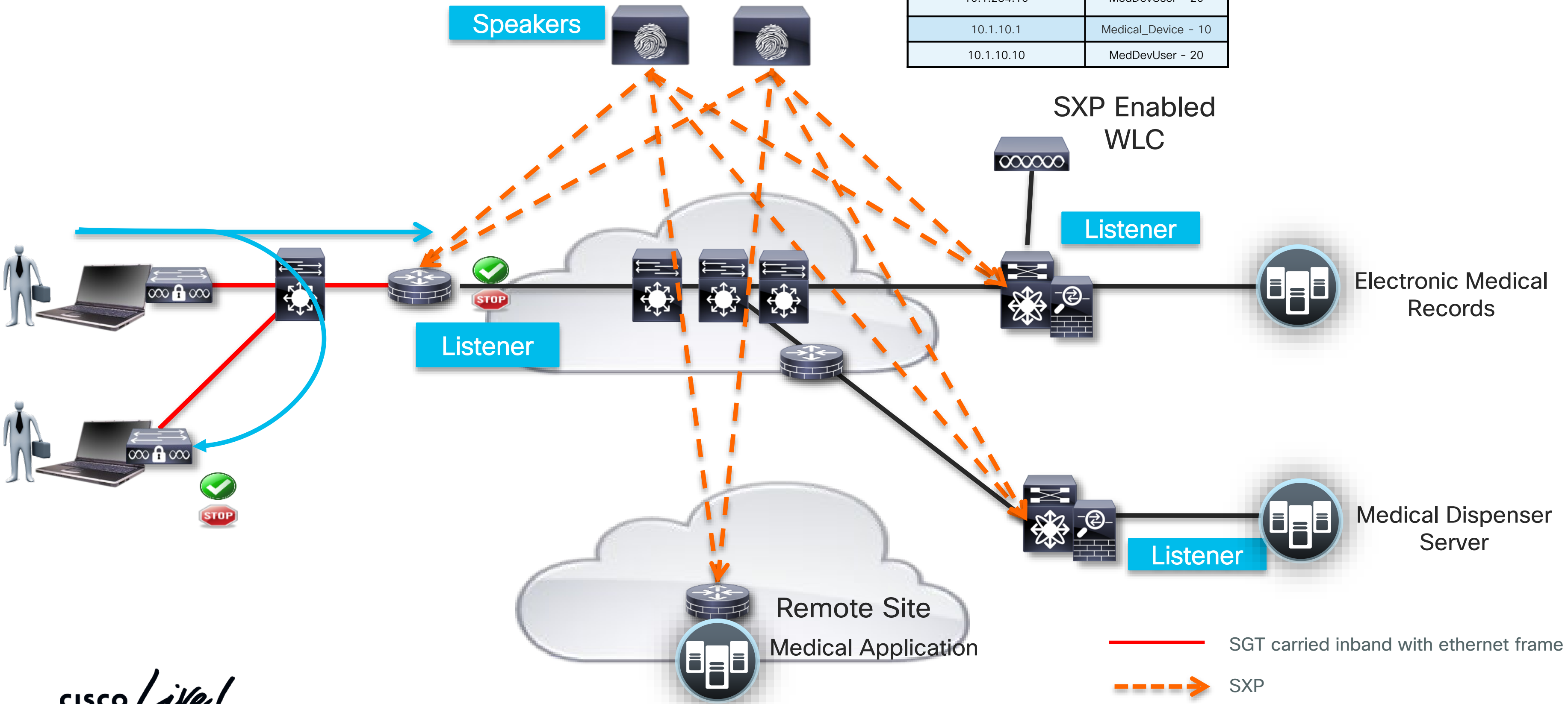
* - IP/SGT scales are per platform. Check limits in TrustSec Systems Bulletin

Use Case - WAN

Health Care Evolution due to scale

Router SGACL and ISE as SXP Speaker

IP Address	SGT
10.1.254.1	Medical_Device - 10
10.1.254.10	MedDevUser - 20
10.1.10.1	Medical_Device - 10
10.1.10.10	MedDevUser - 20



SGT carried inband with ethernet frame

SXP

Use Case - WAN

Configure Links for SGT Tagging

CTS Manual no encryption

```
ISR4K-1
Interface GigabitEthernet1/5
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement

Catalyst 3850
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**

```
ISR4K-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 for any cts manual change

Use Case - WAN

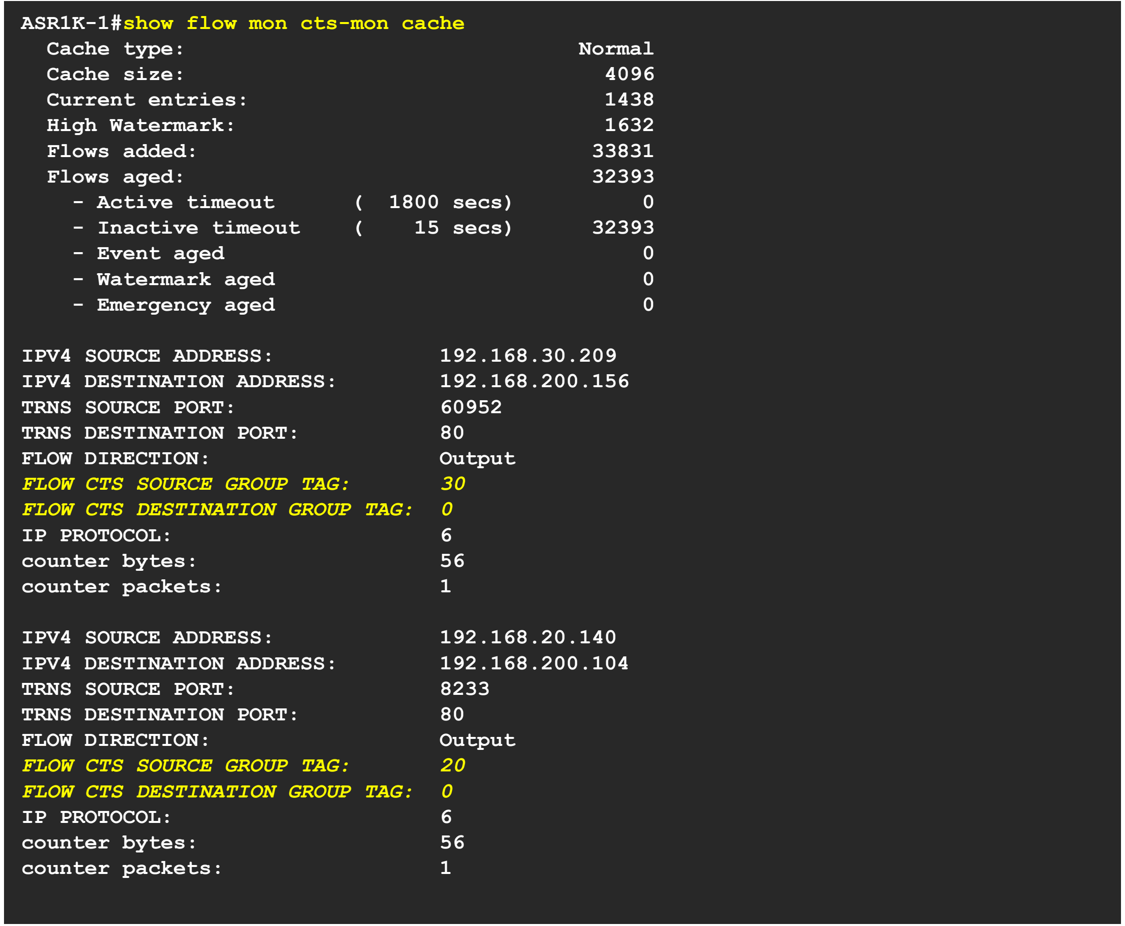
How Do I Know if I am Tagging? SGT and Flexible NetFlow (FNF)

```
flow record cts-v4
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect counter bytes
 collect counter packets

flow exporter EXP1
 destination 10.2.44.15
 source GigabitEthernet3/1

flow monitor cts-mon
 record cts-v4
 exporter EXP1
```

```
Interface vlan 10
ip flow monitor cts-mon input
ip flow monitor cts-mon output

Interface vlan 20
ip flow monitor cts-mon input
ip flow monitor cts-mon output

Interface vlan 30
ip flow monitor cts-mon input
ip flow monitor cts-mon output

Interface vlan 40
ip flow monitor cts-mon input
ip flow monitor cts-mon output
```

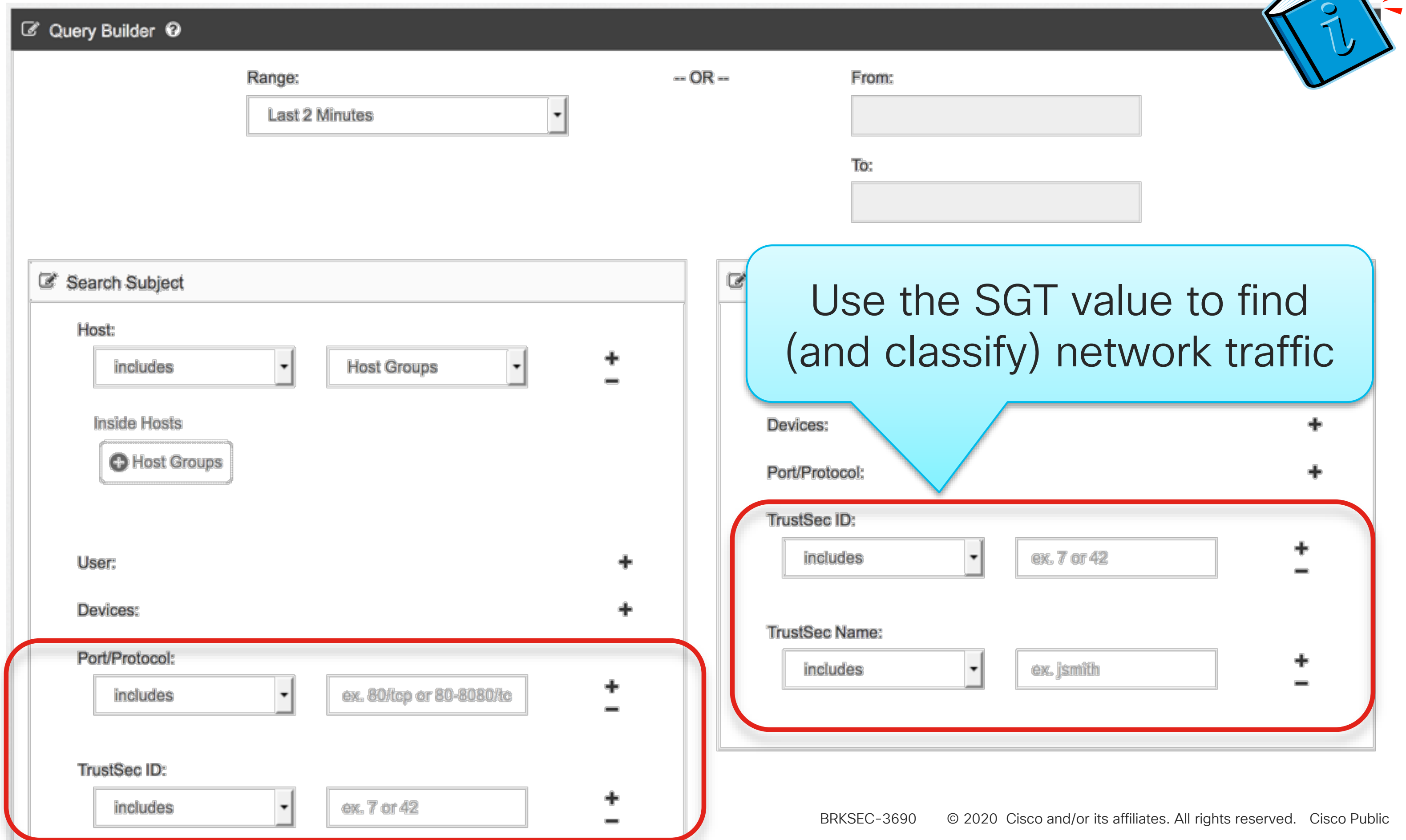
Use Case - WAN

Monitoring SGT/FNF Flow Cache



```
ASR1K-1#show flow mon cts-mon cache
  Cache type:                                        Normal
  Cache size:                                          4096
  Current entries:                                     1438
  High Watermark:                                      1632
  Flows added:                                        33831
  Flows aged:                                         32393
    - Active timeout        (  1800 secs)                 0
    - Inactive timeout      (    15 secs)             32393
    - Event aged                                          0
    - Watermark aged                                      0
    - Emergency aged                                      0

IPV4 SOURCE ADDRESS:                 192.168.30.209
IPV4 DESTINATION ADDRESS:            192.168.200.156
TRNS SOURCE PORT:                    60952
TRNS DESTINATION PORT:               80
FLOW DIRECTION:                      Output
FLOW CTS SOURCE GROUP TAG:           30
FLOW CTS DESTINATION GROUP TAG:      0
IP PROTOCOL:                         6
counter bytes:                       56
counter packets:                     1

IPV4 SOURCE ADDRESS:                 192.168.20.140
IPV4 DESTINATION ADDRESS:            192.168.200.104
TRNS SOURCE PORT:                    8233
TRNS DESTINATION PORT:               80
FLOW DIRECTION:                      Output
FLOW CTS SOURCE GROUP TAG:           20
FLOW CTS DESTINATION GROUP TAG:      0
IP PROTOCOL:                         6
counter bytes:                       56
counter packets:                     1
```

Stealthwatch Flow Query



Query Builder

Range: Last 2 Minutes

-- OR --

From:

To:

Search Subject

Host: includes | Host Groups

Inside Hosts

Host Groups

User:

Devices:

Port/Protocol: includes | ex. 80/tcp or 80-8080/tc

TrustSec ID: includes | ex. 7 or 42

Devices:

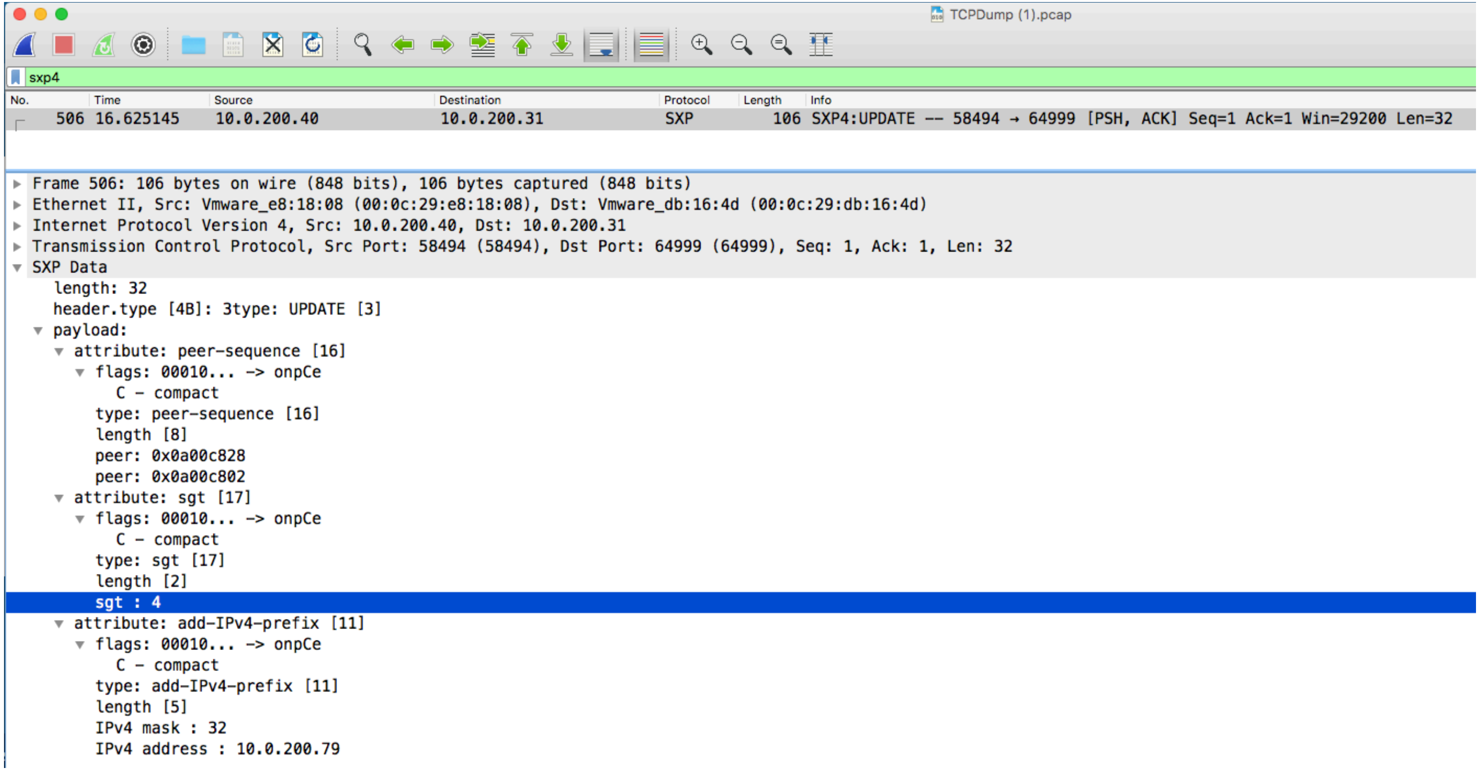
Port/Protocol:

TrustSec ID: includes | ex. 7 or 42

TrustSec Name: includes | ex. jsmith

Use the SGT value to find (and classify) network traffic

SXP and CMD Parsers in Wireshark via LUA

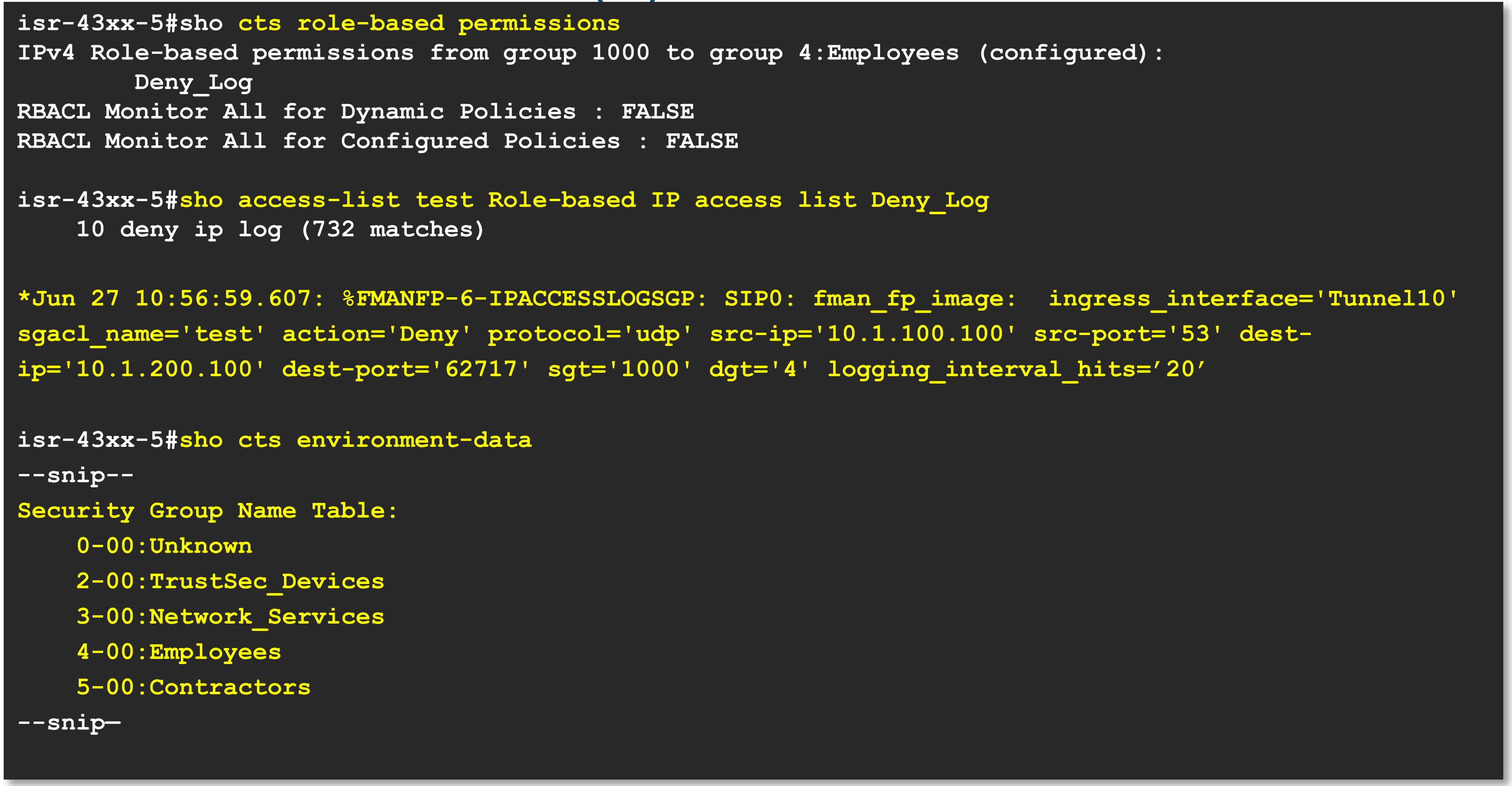


```
No.   Time       Source       Destination  Protocol Length Info
  506 16.625145  10.0.200.40  10.0.200.31  SXP         106 SXP4:UPDATE -- 58494 → 64999 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=32
```

```
▶ Frame 506: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
▶ Ethernet II, Src: Vmware_e8:18:08 (00:0c:29:e8:18:08), Dst: Vmware_db:16:4d (00:0c:29:db:16:4d)
▶ Internet Protocol Version 4, Src: 10.0.200.40, Dst: 10.0.200.31
▶ Transmission Control Protocol, Src Port: 58494 (58494), Dst Port: 64999 (64999), Seq: 1, Ack: 1, Len: 32
▼ SXP Data
    length: 32
    header.type [4B]: 3type: UPDATE [3]
  ▼ payload:
    ▼ attribute: peer-sequence [16]
      ▼ flags: 00010... -> onpCe
          C - compact
        type: peer-sequence [16]
        length [8]
        peer: 0x0a00c828
        peer: 0x0a00c802
    ▼ attribute: sgt [17]
      ▼ flags: 00010... -> onpCe
          C - compact
        type: sgt [17]
        length [2]
        sgt : 4
    ▼ attribute: add-IPv4-prefix [11]
      ▼ flags: 00010... -> onpCe
          C - compact
        type: add-IPv4-prefix [11]
        length [5]
        IPv4 mask : 32
        IPv4 address : 10.0.200.79
```

https://github.com/opendaylight/sxp/tree/master/sxp-dissector

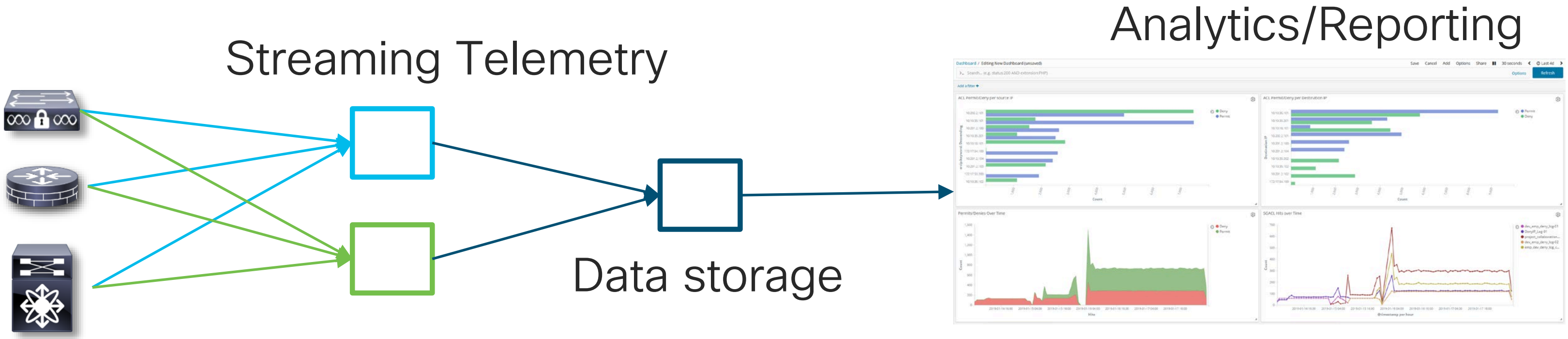
SGFW or SGACL on Router Platforms as of 16.3(3)



```
isr-43xx-5#sho 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

isr-43xx-5#sho 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’

isr-43xx-5#sho 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—
```

Monitoring SGACLs

- SGT/DGT Counters can be exported periodically via streaming telemetry as of IOSXE 16.10 and aggregated across the network
- SGACL Logs are exported via syslog and can be aggregated and parsed for reporting



Analytics/Reporting

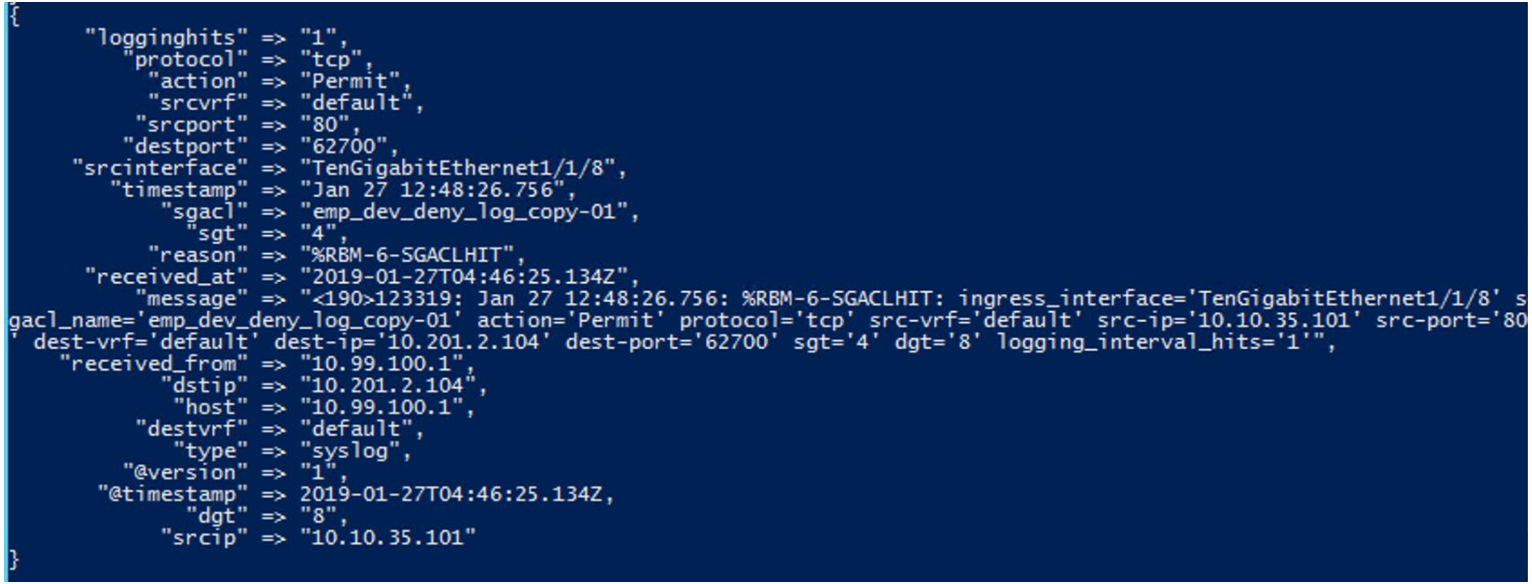
Streaming Telemetry

Data storage

SGACL Syslog Parsing

SGACL Parsing – Logstash example

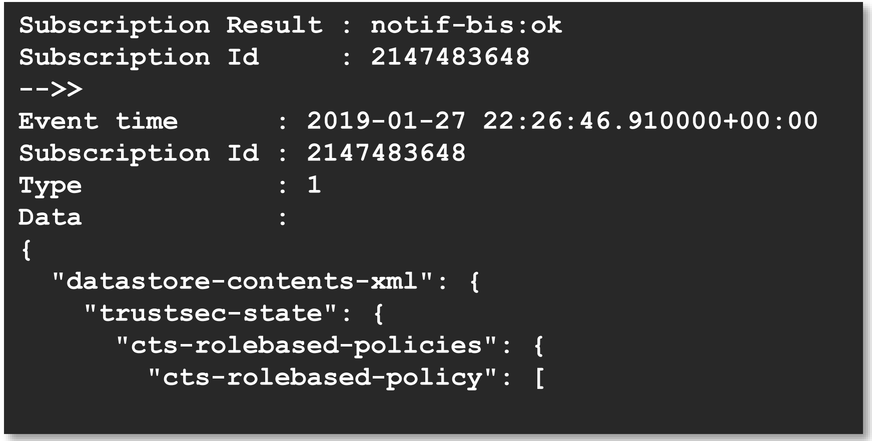
- Grok Parsing of SGACL syslogs to create DB values for SGT/DGT/SGACL, etc.
- *Jan 27 13:33:43.355: %RBM-6-SGACLHIT: ingress_interface='GigabitEthernet1/0/24' sgacl_name='DenyIP_Log-01' action='Deny' protocol='tcp' src-vrf='default' src-ip='10.10.18.101' src-port='64382' dest-vrf='default' dest-ip='10.10.35.201' dest-port='80' sgt='4' dgt='4' logging_interval_hits='1'



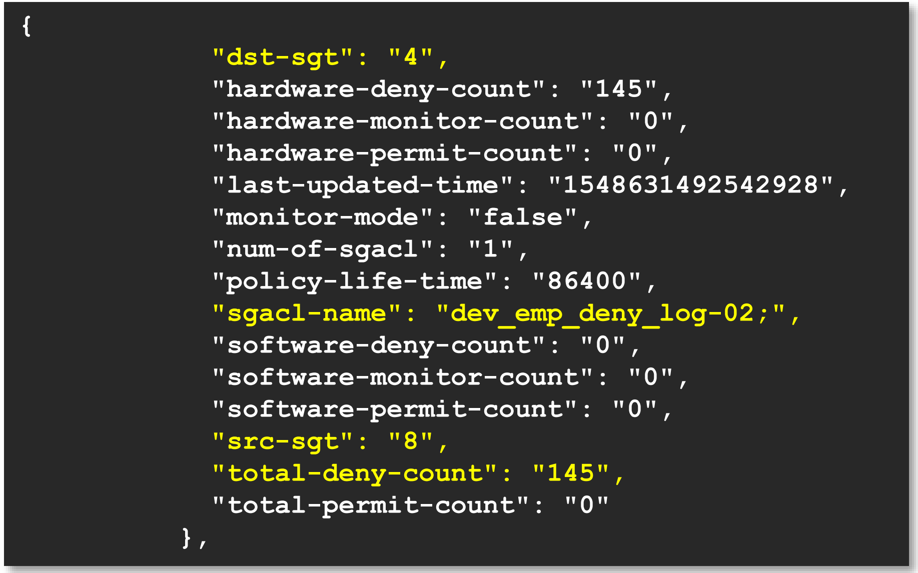
```
{
      "logginghits" => "1",
         "protocol" => "tcp",
           "action" => "Permit",
           "srcvrf" => "default",
          "srcport" => "80",
         "destport" => "62700",
     "srcinterface" => "TenGigabitEthernet1/1/8",
        "timestamp" => "Jan 27 12:48:26.756",
            "sgacl" => "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"
}
```

SGT/DGT Hit Counters via Streaming Telemetry

- 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



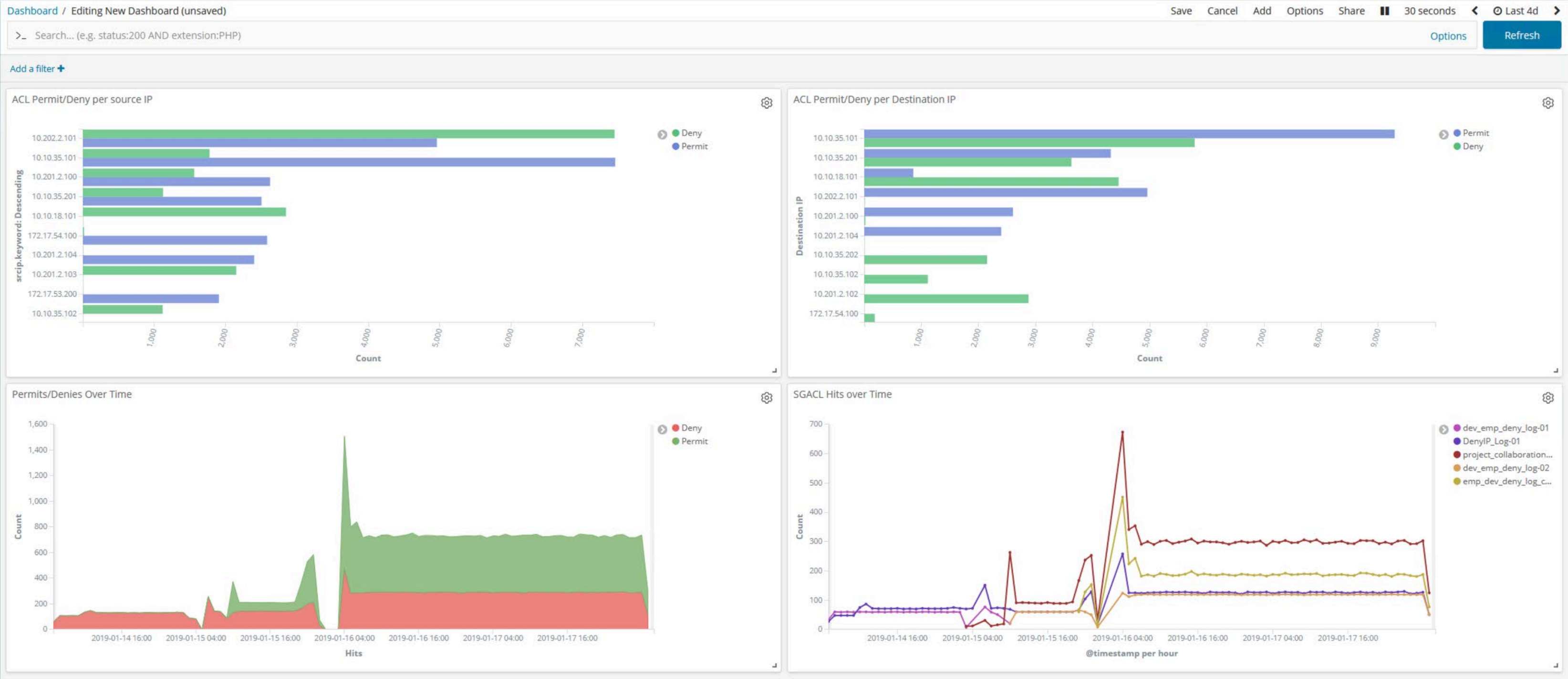
```
Subscription Result : notif-bis:ok
Subscription Id     : 2147483648
-->>
Event time         : 2019-01-27 22:26:46.910000+00:00
Subscription Id : 2147483648
Type               : 1
Data               :
{
  "datastore-contents-xml": {
    "trustsec-state": {
      "cts-rolebased-policies": {
      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

Use Case - WAN

Elasticsearch Example – SGACL Monitoring

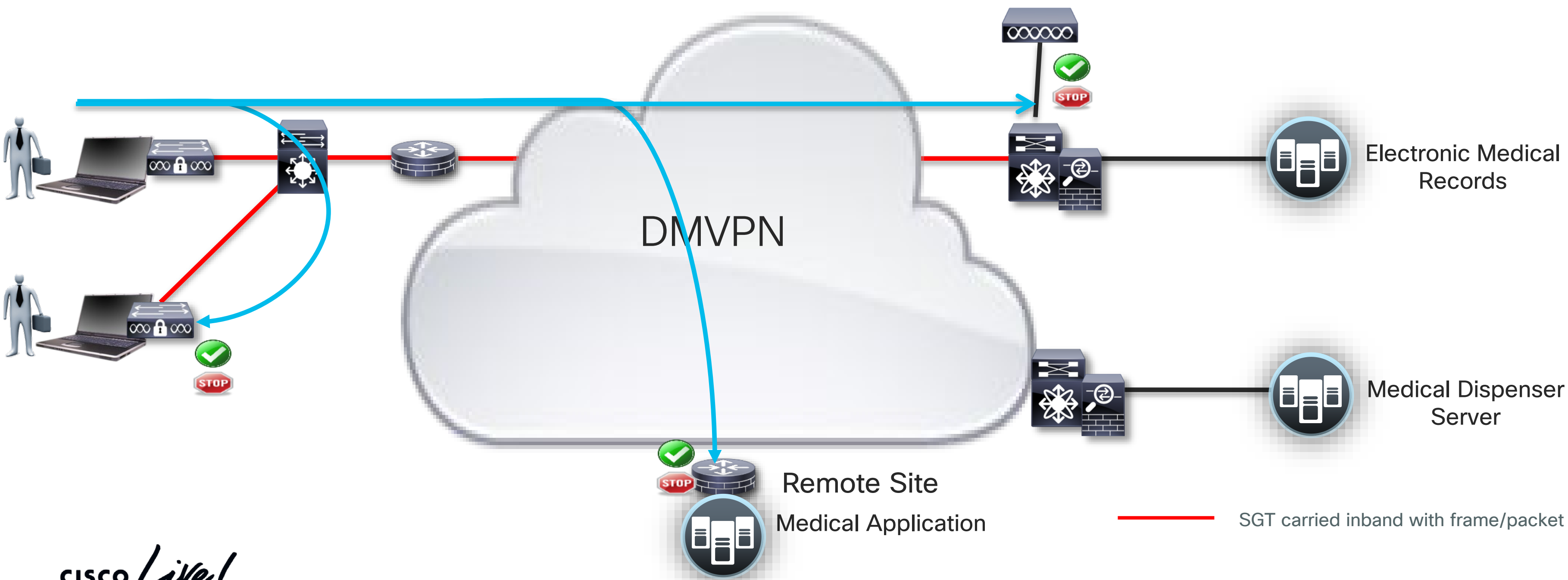


Use Case - WAN

Health Care Evolution due to scale

Move to full tagging DMVPN

IP Address	SGT
10.1.254.1	Medical_Device - 10
10.1.254.10	MedDevUser - 20
10.1.10.1	Medical_Device - 10
10.1.10.10	MedDevUser - 20



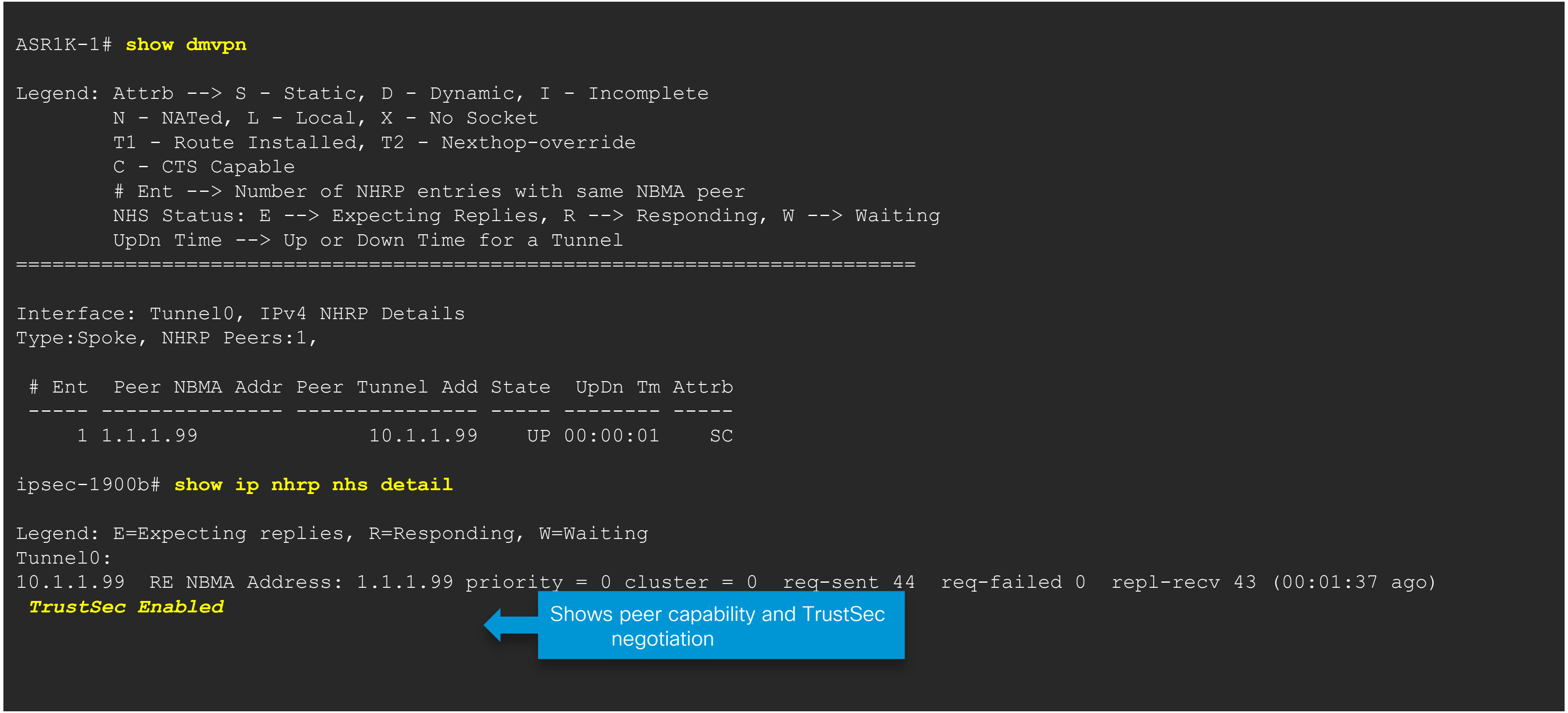
Use Case - WAN

SGT DMVPN Tagging Config

```
interface Tunnel10
 bandwidth 1000000
 ip address 10.210.0.129 255.255.255.128
 no ip redirects
 ip mtu 1360
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip flow monitor FLOW-MONITOR-1 input
 ip flow monitor FLOW-MONITOR-1 output
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 301
 ip nhrp holdtime 600
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1300
 cts sgt inline
 cdp enable
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN-PROFILE
```

Enables SGT propagation on DMVPN. This command is valid for GRE and tunnel interface mode only

SGT DMVPN – Show Commands



```
ASR1K-1# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
=========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- --------- -----
     1 1.1.1.99              10.1.1.99    UP 00:00:01    SC

ipsec-1900b# show ip nhrp nhs detail

Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.99  RE NBMA Address: 1.1.1.99 priority = 0 cluster = 0  req-sent 44  req-failed 0  repl-recv 43 (00:01:37 ago)
 TrustSec Enabled
```

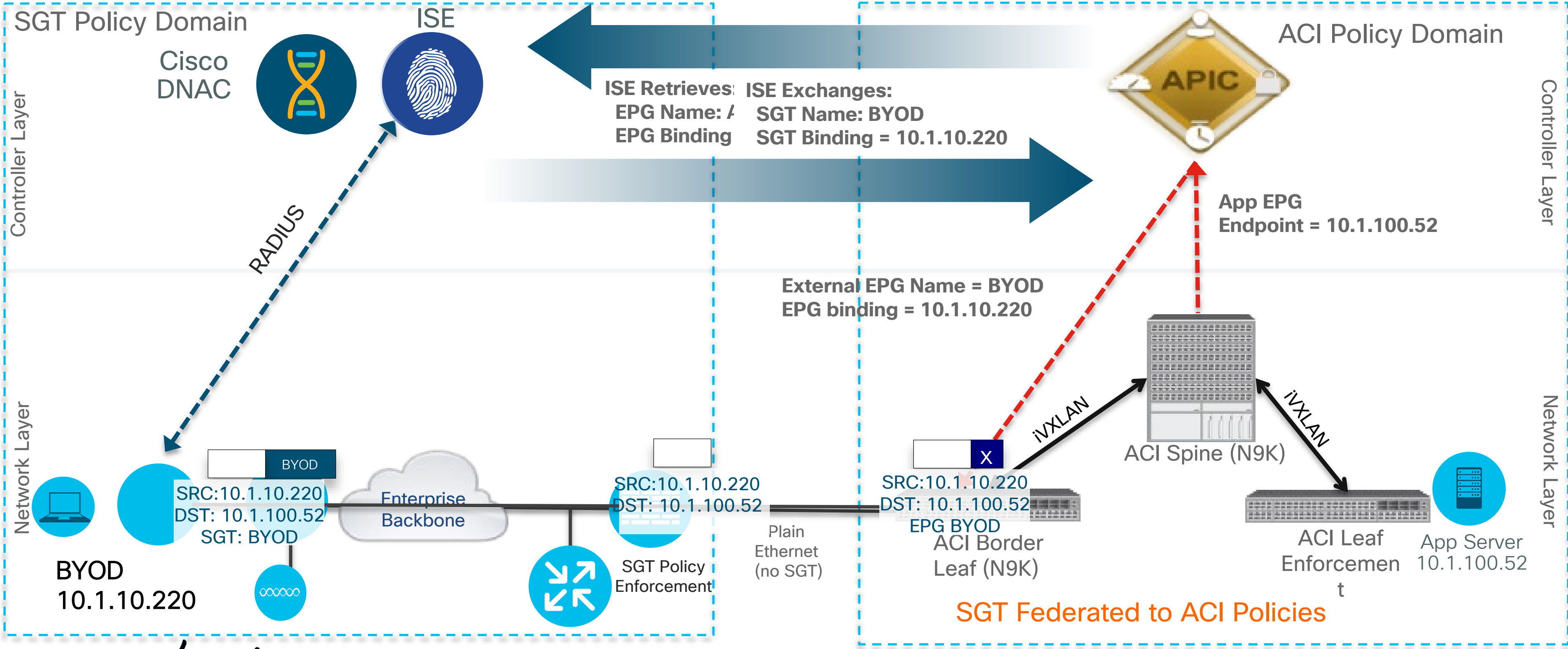
Shows peer capability and TrustSec negotiation

Data Center

SGT/ACI

Policy Federation ISE to APIC Flow:

SGT Policy used to Program ACI EPG Policy



ISE Retrieves:
EPG Name: A
EPG Binding

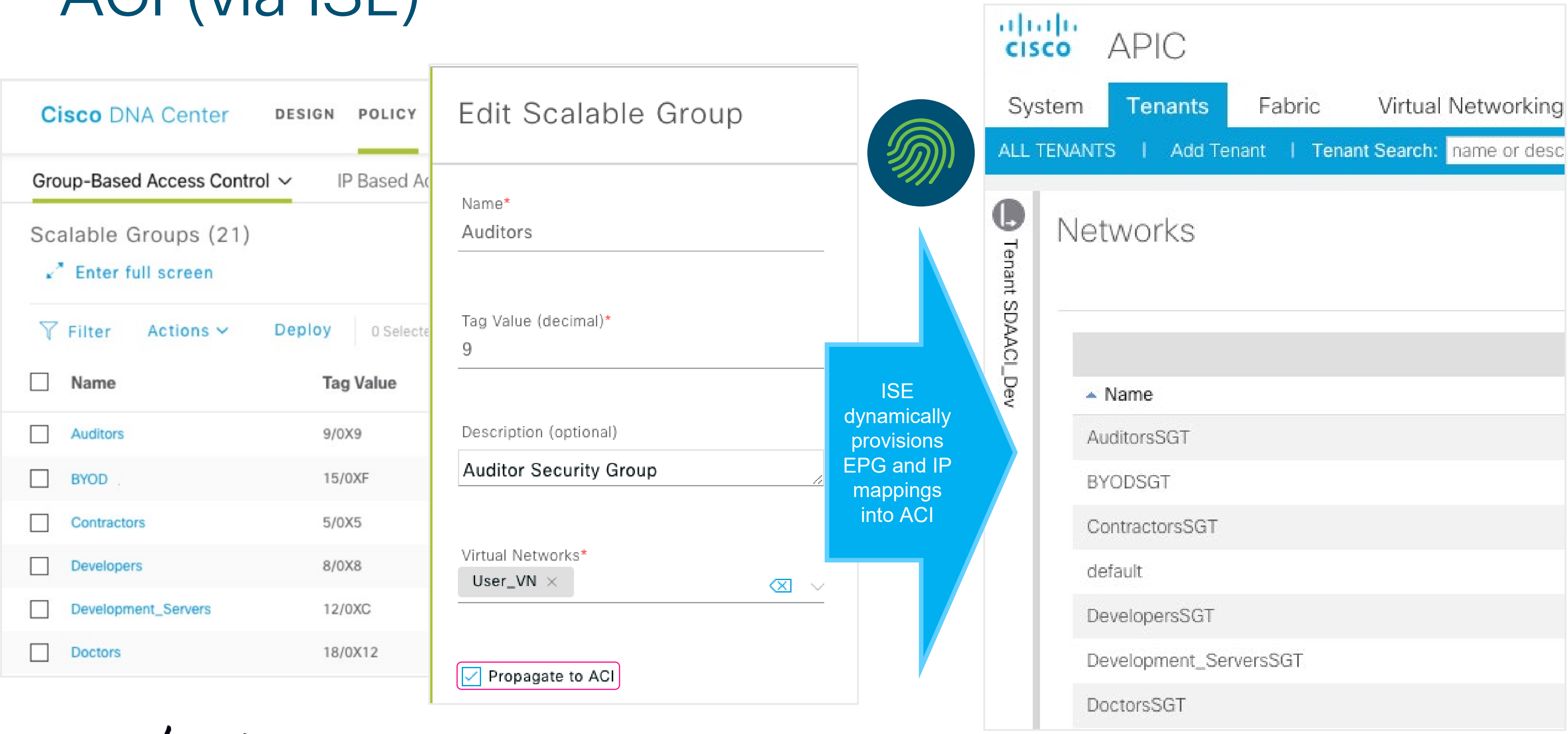
ISE Exchanges:
SGT Name: BYOD
SGT Binding = 10.1.10.220

App EPG
Endpoint = 10.1.100.52

External EPG Name = BYOD
EPG binding = 10.1.10.220

SGT Federated to ACI Policies

Groups Provisioned from SD-Access to ACI (via ISE)



Cisco DNA Center DESIGN POLICY

Group-Based Access Control ⌄ IP Based Ac

Scalable Groups (21)

Enter full screen

Filter Actions ⌄ Deploy 0 Selecte

□	Name	Tag Value
□	Auditors	9/0X9
□	BYOD	15/0XF
□	Contractors	5/0X5
□	Developers	8/0X8
□	Development_Servers	12/0XC
□	Doctors	18/0X12

Edit Scalable Group

Name*
Auditors

Tag Value (decimal)*
9

Description (optional)
Auditor Security Group

Virtual Networks*
User_VN ×

☑ Propagate to ACI

ISE dynamically provisions EPG and IP mappings into ACI

cisco APIC

System Tenants Fabric Virtual Networking

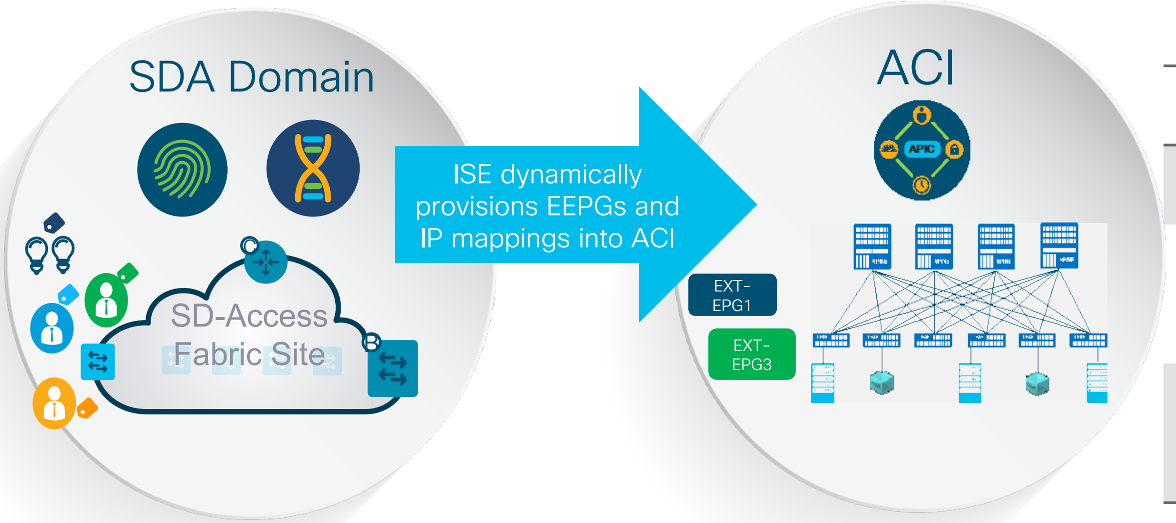
ALL TENANTS | Add Tenant | Tenant Search: name or desc

Tenant SDAACI_Dev

Networks

Name
AuditorsSGT
BYODSGT
ContractorsSGT
default
DevelopersSGT
Development_ServersSGT
DoctorsSGT

Enforcement Scale in ACI



Scalable Groups (SG)

External Endpoint Groups (EPG)

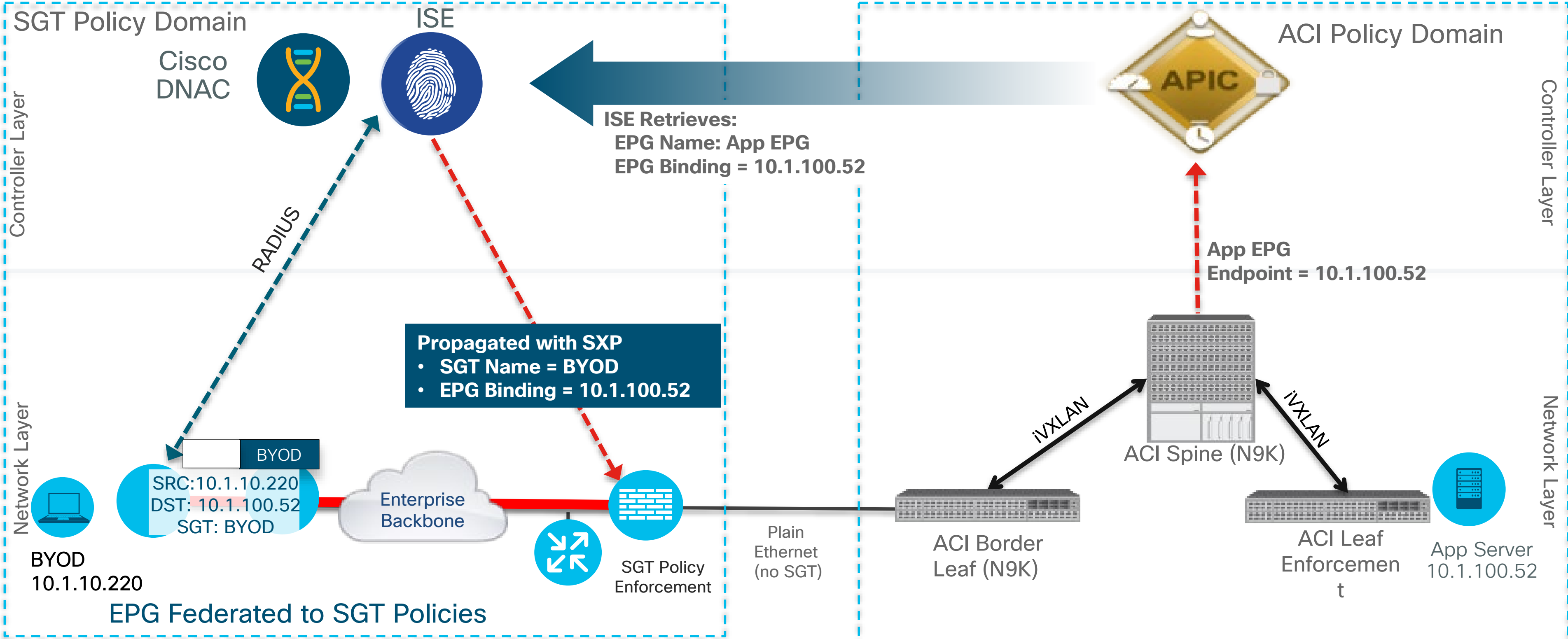
ACI 3.2 Scale
EX, FX and FX2 Hardware

No. of unique EEPGs	250
Total Number of Mappings	64,000
Mappings per EEPG	8000
Transaction rate (target)	100/s

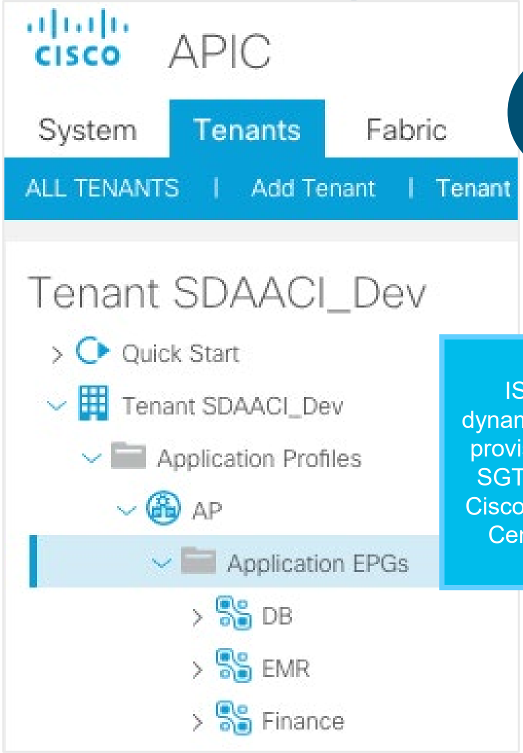
Recommend ISE 2.4 patch 6 or 2.6

Policy Federation APIC to ISE:

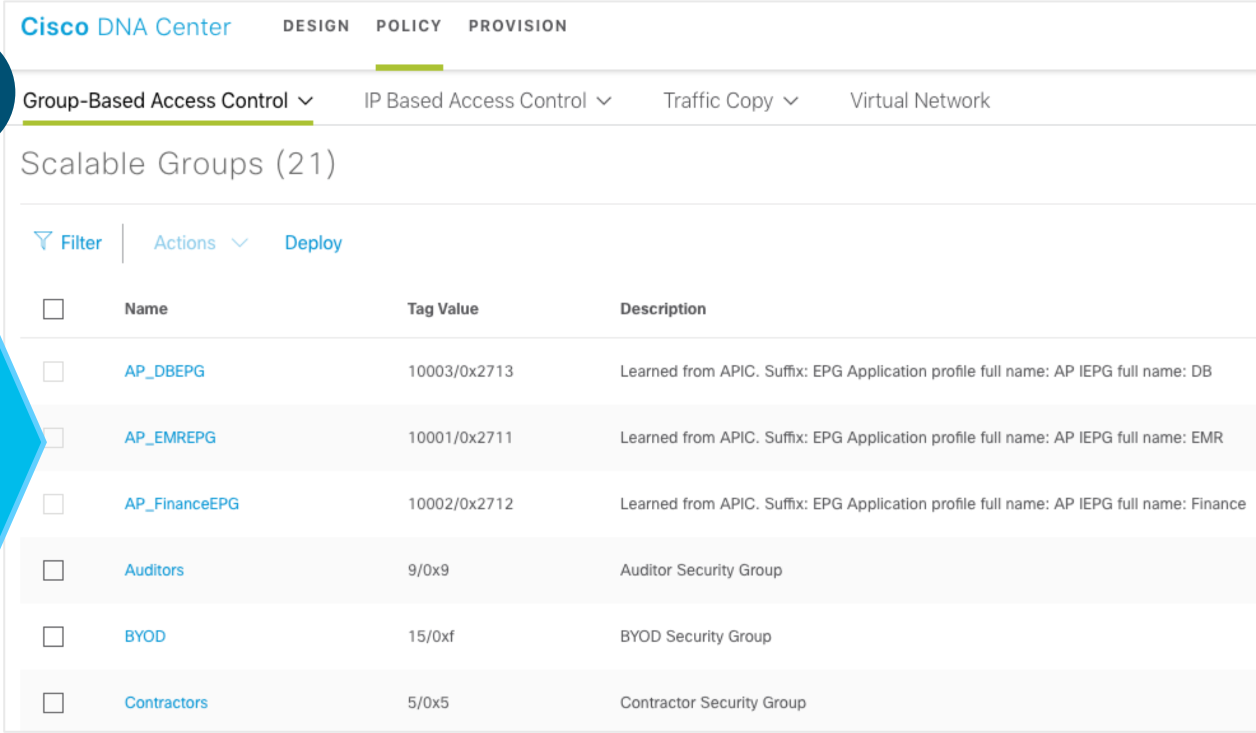
ACI EPG Policy used to Program SGT Policy



Groups Provisioned from ACI to SD-Access (via ISE)



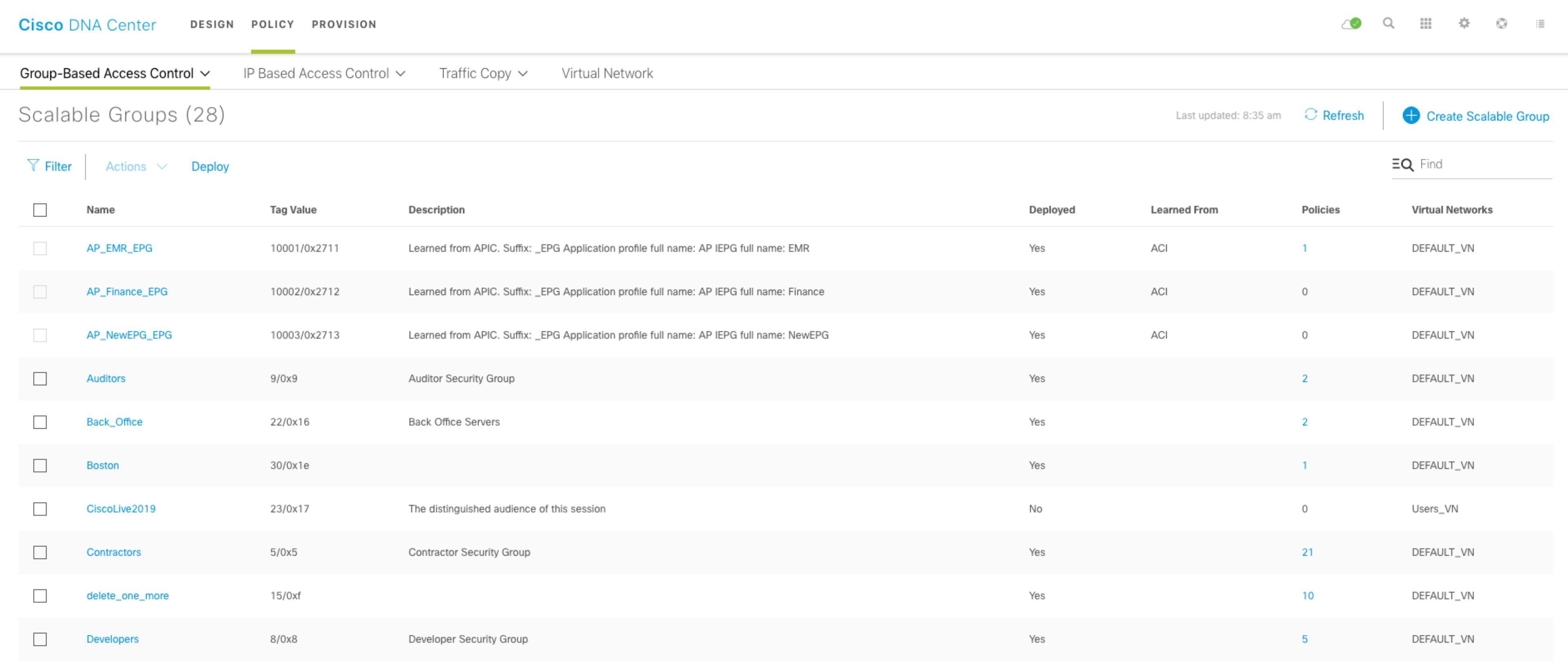
ISE dynamically provisions SGT into Cisco DNA Center



Scalable Groups (21)

	Name	Tag Value	Description
□	AP_DBEPG	10003/0x2713	Learned from APIC. Suffix: EPG Application profile full name: AP IEPG full name: DB
□	AP_EMREPG	10001/0x2711	Learned from APIC. Suffix: EPG Application profile full name: AP IEPG full name: EMR
□	AP_FinanceEPG	10002/0x2712	Learned from APIC. Suffix: EPG Application profile full name: AP IEPG full name: Finance
□	Auditors	9/0x9	Auditor Security Group
□	BYOD	15/0xf	BYOD Security Group
□	Contractors	5/0x5	Contractor Security Group

Scalable Groups in Cisco DNA Center



Scalable Groups (28)

Last updated: 8:35 am

□	Name	Tag Value	Description	Deployed	Learned From	Policies	Virtual Networks
□	AP_EMR_EPG	10001/0x2711	Learned from APIC. Suffix: _EPG Application profile full name: AP IEPG full name: EMR	Yes	ACI	1	DEFAULT_VN
□	AP_Finance_EPG	10002/0x2712	Learned from APIC. Suffix: _EPG Application profile full name: AP IEPG full name: Finance	Yes	ACI	0	DEFAULT_VN
□	AP_NewEPG_EPG	10003/0x2713	Learned from APIC. Suffix: _EPG Application profile full name: AP IEPG full name: NewEPG	Yes	ACI	0	DEFAULT_VN
□	Auditors	9/0x9	Auditor Security Group	Yes		2	DEFAULT_VN
□	Back_Office	22/0x16	Back Office Servers	Yes		2	DEFAULT_VN
□	Boston	30/0x1e		Yes		1	DEFAULT_VN
□	CiscoLive2019	23/0x17	The distinguished audience of this session	No		0	Users_VN
□	Contractors	5/0x5	Contractor Security Group	Yes		21	DEFAULT_VN
□	delete_one_more	15/0xf		Yes		10	DEFAULT_VN
□	Developers	8/0x8	Developer Security Group	Yes		5	DEFAULT_VN

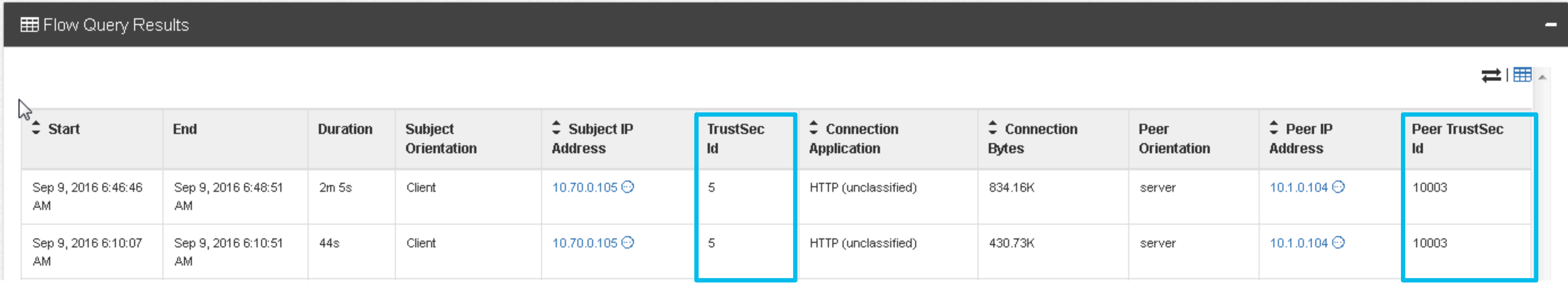
ACI EPG Shared with SGT Infrastructure

```
C9K-CORE-1#$how flow monitor CYBER_MONITOR cache filter ipv4
destination address 10.200.101.105
  --snip--

IPV4 SOURCE ADDRESS:            10.10.18.102
IPV4 DESTINATION ADDRESS:       10.200.101.105
TRNS SOURCE PORT:               0
TRNS DESTINATION PORT:          2048
FLOW CTS SOURCE GROUP TAG:      100
FLOW CTS DESTINATION GROUP TAG: 0
IP PROTOCOL:                    1
tcp flags:                      0x00
interface output:               Te2/1
counter bytes:                  1320
counter packets:                22
timestamp first:                04:04:04.013
timestamp last:                 04:04:24.913

IPV4 SOURCE ADDRESS:            10.10.18.102
IPV4 DESTINATION ADDRESS:       10.200.101.105
TRNS SOURCE PORT:               0
TRNS DESTINATION PORT:          2048
FLOW CTS SOURCE GROUP TAG:      100
FLOW CTS DESTINATION GROUP TAG: 10005
IP PROTOCOL:                    1
tcp flags:                      0x00
interface output:               Te2/1
counter bytes:                  1440
counter packets:                24
timestamp first:                04:04:04.013
timestamp last:                 04:04:26.963
```

```
C9K-CORE-1#sho 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
    6-00:Guests
    7-00:Production_Users
    8-00:Developers
    9-00:Auditors
    10-00:Point_of_Sale_Systems
    11-00:Production_Servers
    12-00:Development_Servers
    13-00:Test_Servers
    14-00:PCI_Servers
    15-00:BYOD
    16-00:pci_users
    255-00:Quarantined_Systems
    10001-00:EV_appProfile_LOB1_Web1EPG
    10002-00:EV_appProfile_LOB1_App1EPG
    10003-00:EV_appProfile_LOB1_DB1EPG
    10004-00:EV_appProfile_NetworkServicesEPG
    10005-00:EV_appProfile_LOB2_App1EPG
--snip--
```

Extended Visibility in Stealthwatch

SGT & ACI Policy Groups in Flow Records



Flow Query Results

Start	End	Duration	Subject Orientation	Subject IP Address	TrustSec Id	Connection Application	Connection Bytes	Peer Orientation	Peer IP Address	Peer TrustSec Id
Sep 9, 2016 6:46:46 AM	Sep 9, 2016 6:48:51 AM	2m 5s	Client	10.70.0.105	5	HTTP (unclassified)	834.16K	server	10.1.0.104	10003
Sep 9, 2016 6:10:07 AM	Sep 9, 2016 6:10:51 AM	44s	Client	10.70.0.105	5	HTTP (unclassified)	430.73K	server	10.1.0.104	10003

Source SGT

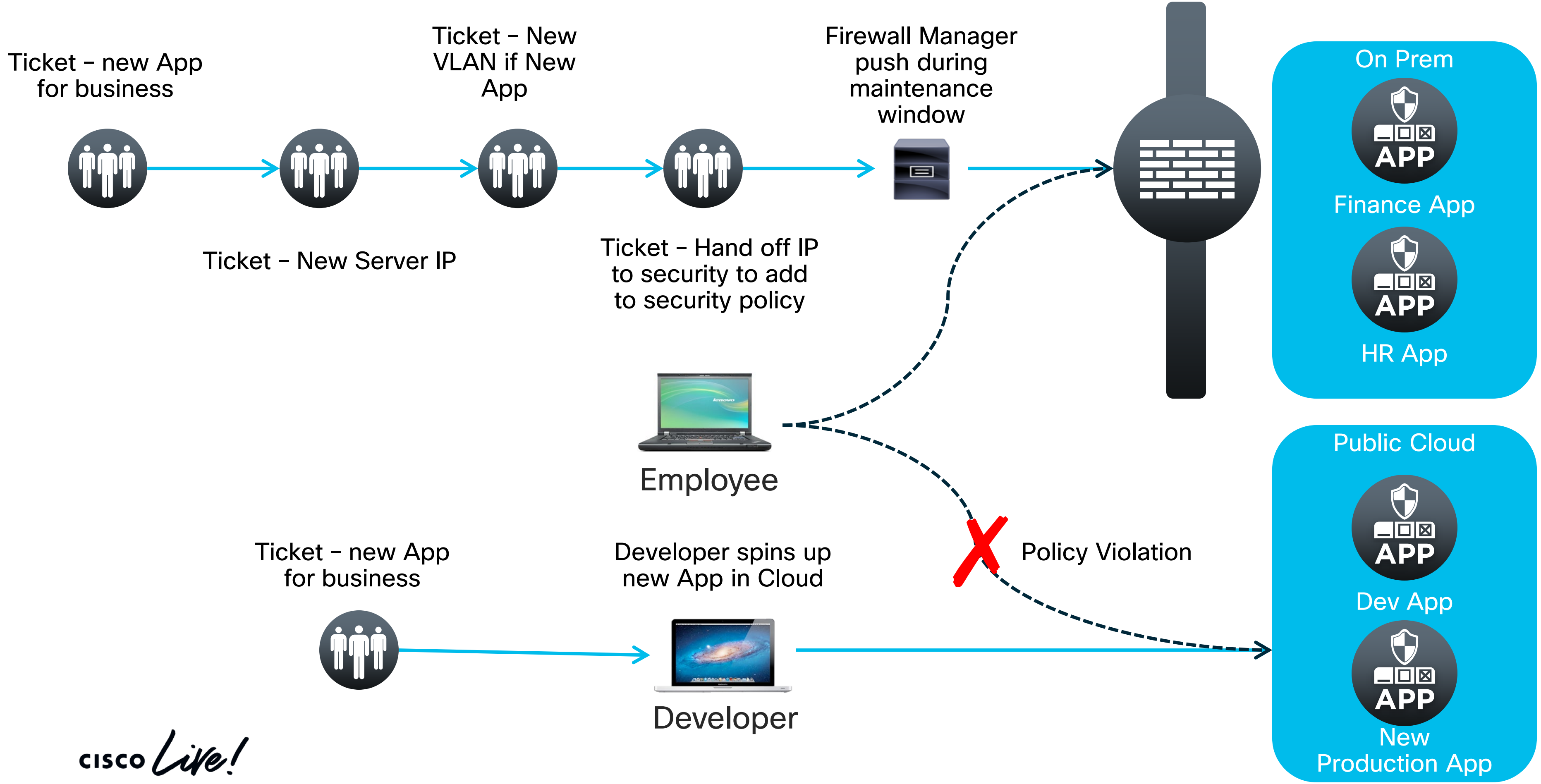
Destination SGT learned from APIC-DC policy group sharing

Cloud

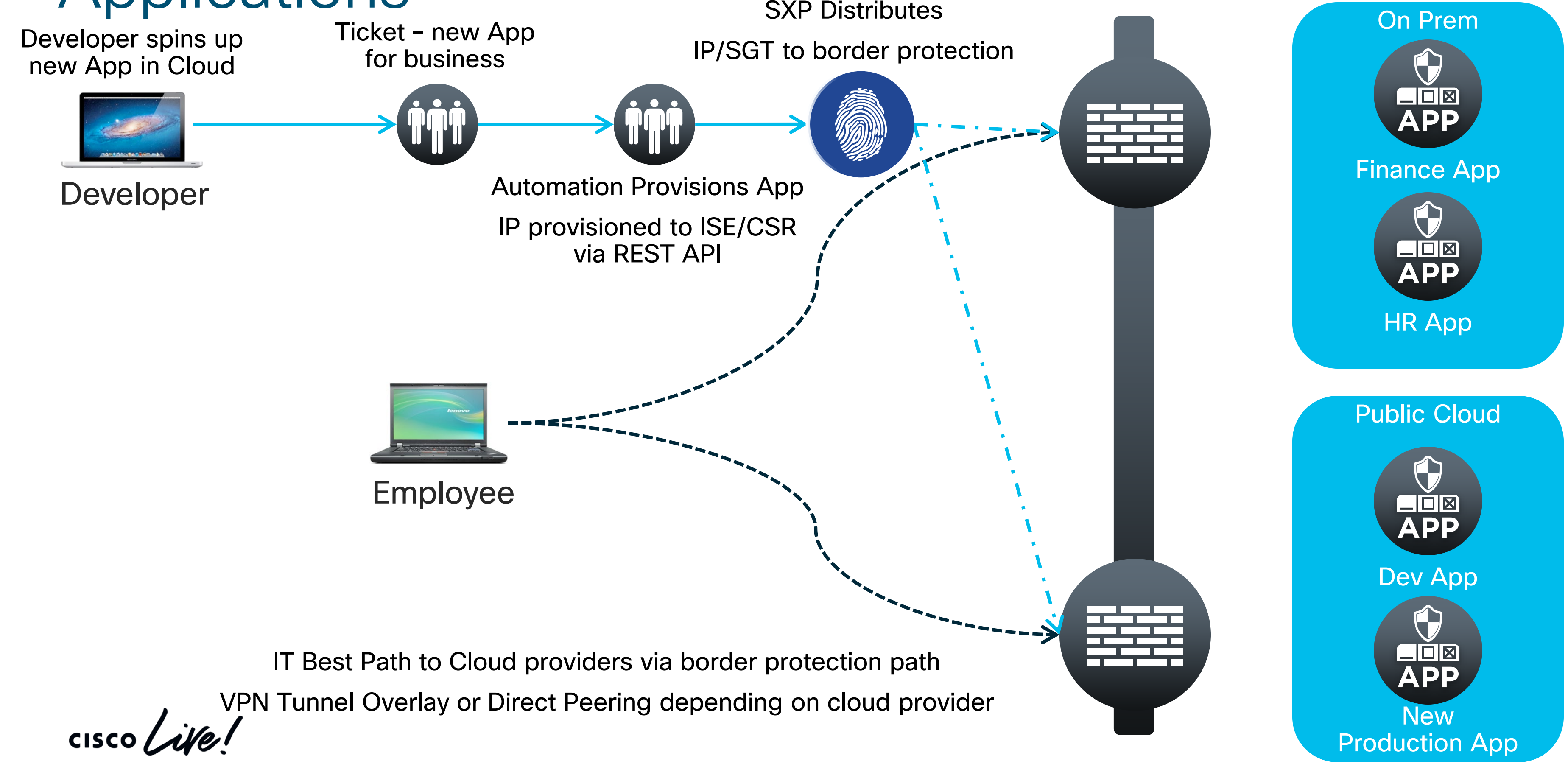
Security Controls for Cloud Applications

- Business Problem/Background
  - Developers were buying VMs in cloud environments since IT was too slow to provision
  - This led to untracked data being exposed in cloud environments
  - This led to issues with production and development cross connections by employees corrupting data sets
  - “De-provisioning” Applications/Servers never happen. Results in stale security rules
    - “What does this rule do? We don’t know we better not remove it”
  - Provisioning of workloads in minutes as opposed to days – “Fast IT”
- Solution Overview
  - Provide automation for on prem and cloud environments with strict access controls
  - Change provisioning to automatically reflect the existence of a new cloud instance
  - Provide best path by tunnelling or peering to the cloud providers
  - Provide access control on best path for development, user acceptance and production workloads

Security Controls for Applications


Ticket – new App for business
Ticket – New Server IP
Ticket – New VLAN if New App
Ticket – Hand off IP to security to add to security policy
Firewall Manager push during maintenance window
On Prem
APP
Finance App
APP
HR App
Employee
Policy Violation
Ticket – new App for business
Developer spins up new App in Cloud
Developer
Public Cloud
APP
Dev App
APP
New Production App

Developer and Production Controls for Applications



Developer spins up new App in Cloud

Ticket – new App for business

SXP Distributes

IP/SGT to border protection

Automation Provisions App

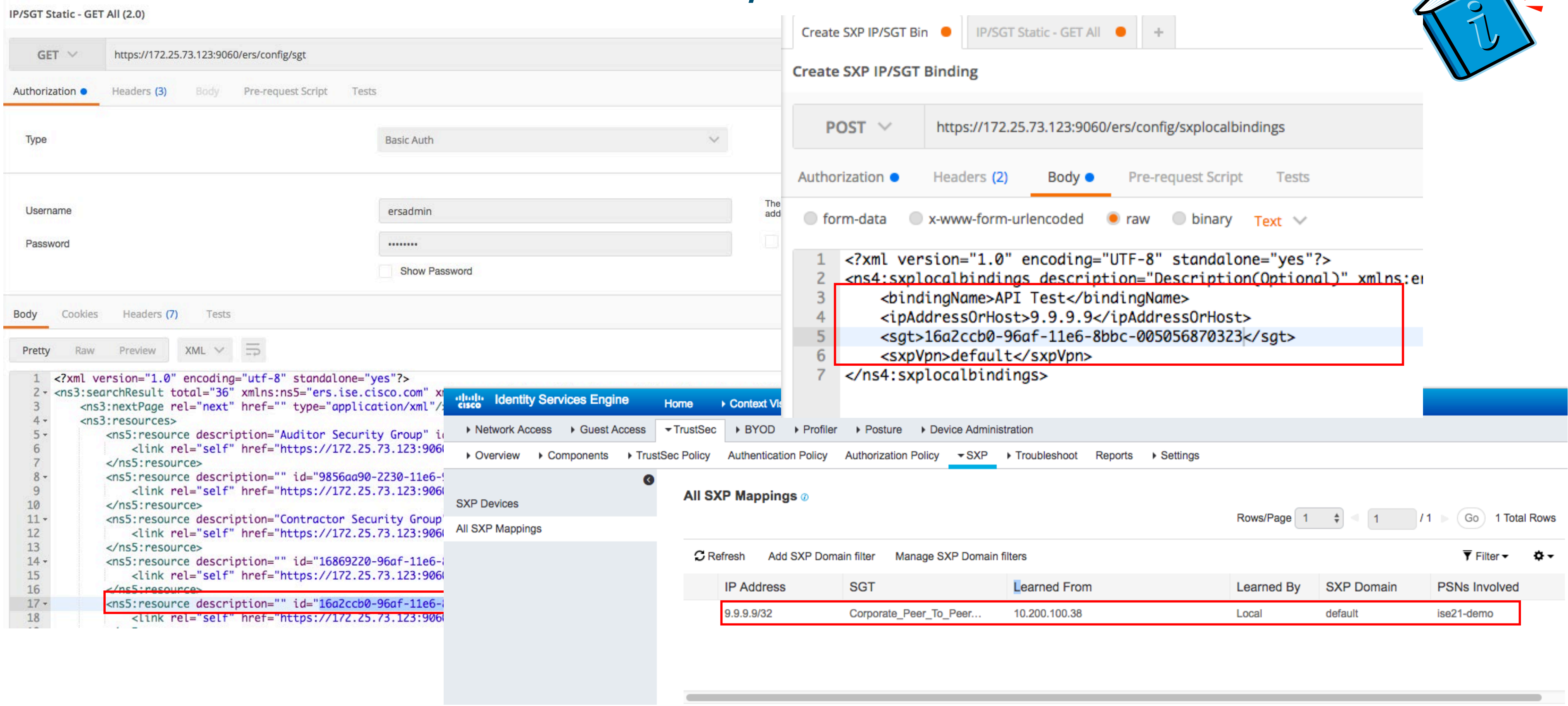
IP provisioned to ISE/CSR via REST API

IT Best Path to Cloud providers via border protection path

VPN Tunnel Overlay or Direct Peering depending on cloud provider

REST API – ISE 2.x – IP/SGT

Use Case – Cloud



IP/SGT Static - GET All (2.0)

GET https://172.25.73.123:9060/ers/config/sgt

Authorization ● | Headers (3) | Body | Pre-request Script | Tests

Type: Basic Auth

Username: ersadmin

Password: ••••••••

□ Show Password

Body | Cookies | Headers (7) | Tests

Pretty | Raw | Preview | XML

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns3:searchResult total="36" xmlns:ns5="ers.ise.cisco.com" x
    <ns3:nextPage rel="next" href="" type="application/xml"/
    <ns3:resources>
        <ns5:resource description="Auditor Security Group" i
            <link rel="self" href="https://172.25.73.123:906
        </ns5:resource>
        <ns5:resource description="" id="9856aa90-2230-11e6-
            <link rel="self" href="https://172.25.73.123:906
        </ns5:resource>
        <ns5:resource description="Contractor Security Group
            <link rel="self" href="https://172.25.73.123:906
        </ns5:resource>
        <ns5:resource description="" id="16869220-96af-11e6-
            <link rel="self" href="https://172.25.73.123:906
        </ns5:resource>
        <ns5:resource description="" id="16a2ccb0-96af-11e6-
            <link rel="self" href="https://172.25.73.123:906
```

Create SXP IP/SGT Bin ● | IP/SGT Static - GET All ● | +

Create SXP IP/SGT Binding

POST https://172.25.73.123:9060/ers/config/sxplocalbindings

Authorization ● | Headers (2) | Body ● | Pre-request Script | Tests

○ form-data ○ x-www-form-urlencoded ● raw ○ binary Text

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns4:sxplocalbindings description="Description(Optional)" xmlns:e
    <bindingName>API Test</bindingName>
    <ipAddressOrHost>9.9.9.9</ipAddressOrHost>
    <sgt>16a2ccb0-96af-11e6-8bbc-005056870323</sgt>
    <sxpVpn>default</sxpVpn>
</ns4:sxplocalbindings>
```

All SXP Mappings

Rows/Page 1 | 1 / 1 | Go | 1 Total Rows

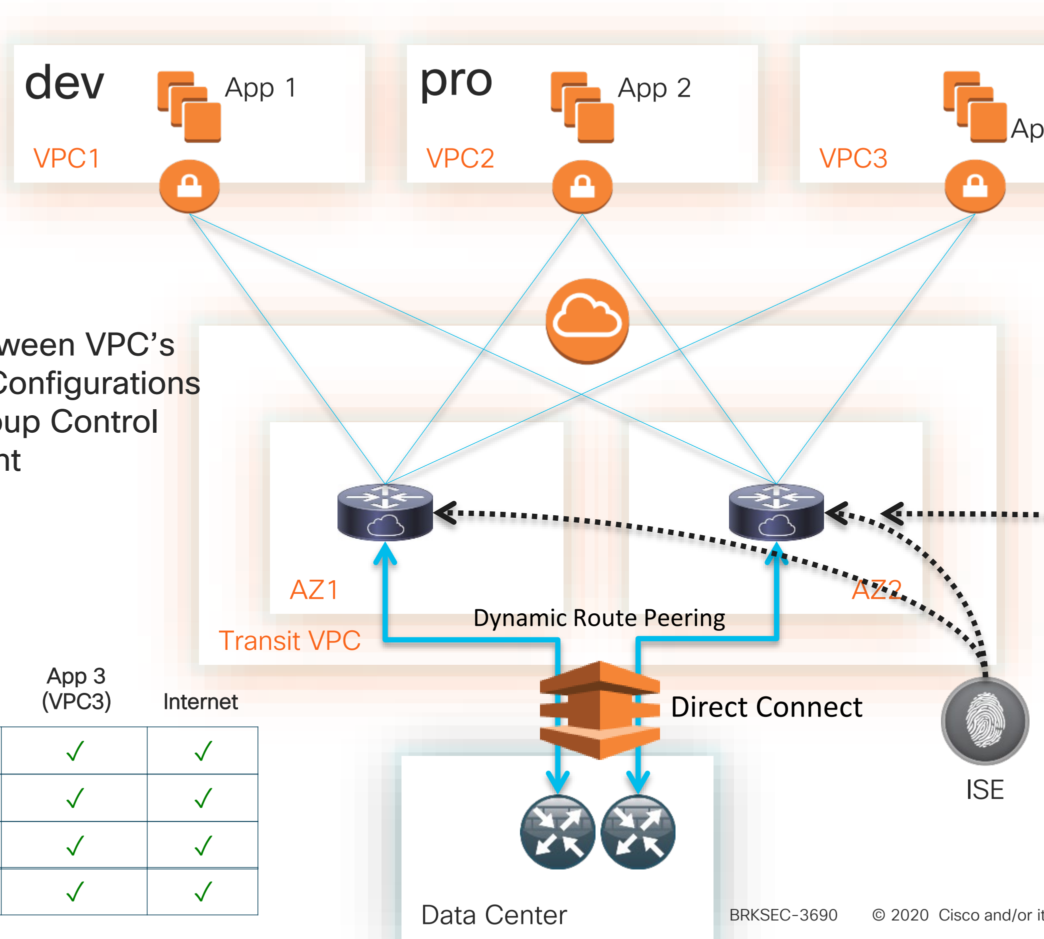
Refresh | Add SXP Domain filter | Manage SXP Domain filters | Filter

IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
9.9.9.9/32	Corporate_Peer_To_Peer...	10.200.100.38	Local	default	ise21-demo

Example script – https://github.com/vkatkade/ISE/blob/master/aws-ise.py

Credit – Vaibhav Katkade

AWS Transit VPC



- Control Traffic between VPC's
- Simplify Security Configurations
- Scale Security Group Control
- Single Control Point

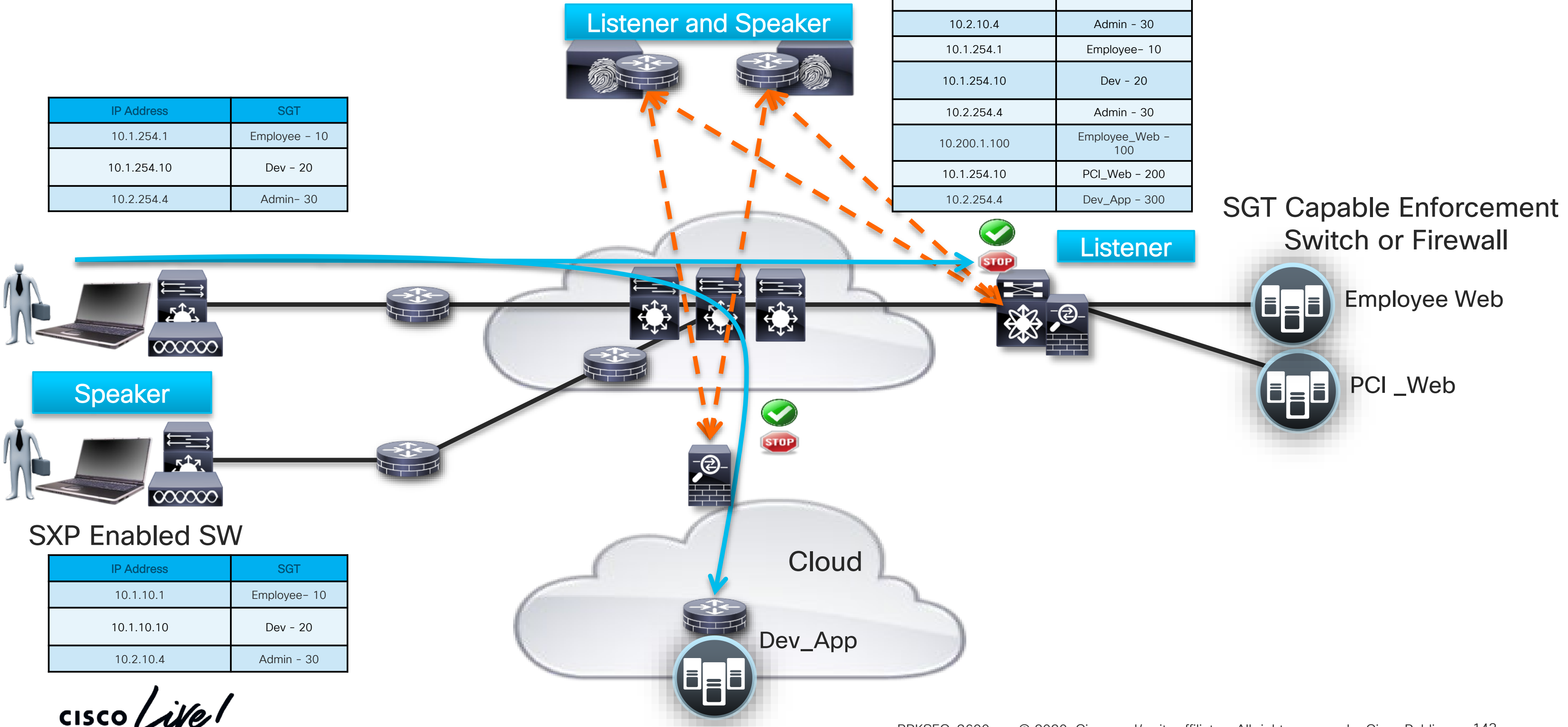
Control Access to spoke VPC's based on SGT Tags and Policy Enforcement within the Transit VPC Hub CSRv's

	App 1 (VPC1)	App 2 (VPC2)	App 3 (VPC3)	Internet
Employee	X	✓	✓	✓
Developer	✓	X	✓	✓
Guest	X	X	✓	✓
Non-Compliant	X	X	✓	✓

- Employee Tag
- Developer Tag
- Guest Tag
- Non-Compliant Tag

Use Case – Cloud

Production and Dev Example



IP/SGT from API or Cloud Policy

Listener and Speaker

IP Address	SGT
10.1.10.1	Employee – 10
10.1.10.10	Dev – 20
10.2.10.4	Admin – 30
10.1.254.1	Employee– 10
10.1.254.10	Dev – 20
10.2.254.4	Admin – 30
10.200.1.100	Employee_Web – 100
10.1.254.10	PCI_Web – 200
10.2.254.4	Dev_App – 300

IP Address	SGT
10.1.254.1	Employee – 10
10.1.254.10	Dev – 20
10.2.254.4	Admin– 30

SGT Capable Enforcement Switch or Firewall

Listener

STOP

Employee Web

PCI _Web

Speaker

STOP

SXP Enabled SW

IP Address	SGT
10.1.10.1	Employee– 10
10.1.10.10	Dev – 20
10.2.10.4	Admin – 30

Cloud

Dev_App

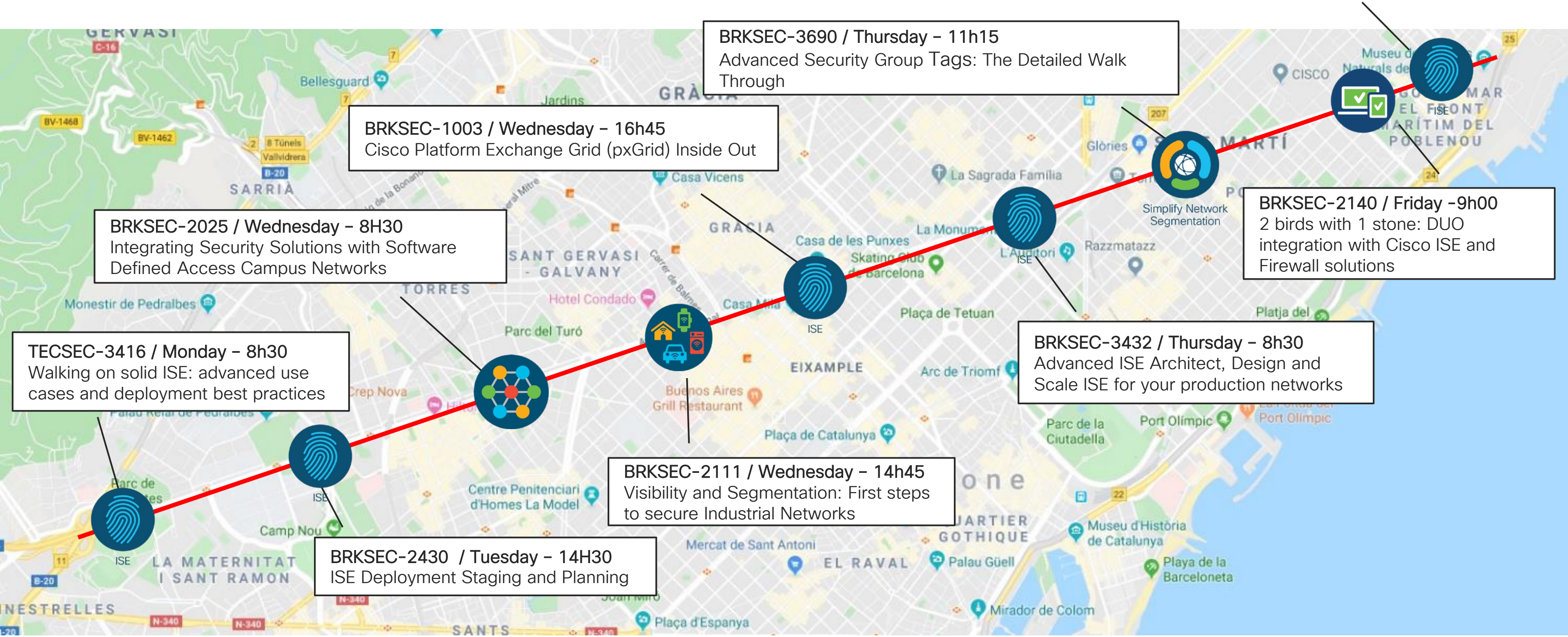
cisco Live!

Summary

Summary

- SGT is the foundation for the newly announce Cisco DNA/SD-Access
- SGT builds upon dynamic classification (802.1X/ACI/etc.), static classification (IP/SGT) and orchestration - REST, Cloud Center 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

ISE Diagonal Learning Map



TECSEC-3416 / Monday – 8h30
Walking on solid ISE: advanced use cases and deployment best practices

BRKSEC-2430 / Tuesday – 14H30
ISE Deployment Staging and Planning

BRKSEC-2025 / Wednesday – 8H30
Integrating Security Solutions with Software Defined Access Campus Networks

BRKSEC-2111 / Wednesday – 14h45
Visibility and Segmentation: First steps to secure Industrial Networks

BRKSEC-1003 / Wednesday – 16h45
Cisco Platform Exchange Grid (pxGrid) Inside Out

BRKSEC-3690 / Thursday – 11h15
Advanced Security Group Tags: The Detailed Walk Through

BRKSEC-3432 / Thursday – 8h30
Advanced ISE Architect, Design and Scale ISE for your production networks

BRKSEC-2140 / Friday -9h00
2 birds with 1 stone: DUO integration with Cisco ISE and Firewall solutions

BRKSEC-3229 / Friday 9h00
ISE under magnifying glass. How to troubleshoot ISE

Links

- Secure Access, TrustSec, and ISE on Cisco.com
  - http://www.cisco.com/go/TrustSec
  - http://www.cisco.com/go/ise
  - http://www.cisco.com/go/isepartner
- TrustSec and ISE Deployment Guides:
  - http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html
- TrustSec Communities
  - https://communities.cisco.com/community/technology/security/pa/trustsec
- YouTube: Fundamentals of TrustSec:
  - http://www.youtube.com/ciscocin#p/c/0/MJJ93N-3Iew

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

cisco

You make **possible**