cisco

TOMORROW
starts here.

Cisco Connect

Policy Defined Segmentation with Cisco TrustSec

Session ID 18PT

Rob Bleeker – Consulting System Engineer

CCIE #: 2926

Abstract

- This session will explain how TrustSec Security Group Tagging can be used to simplify access controls and provide software-defined segmentation.
- We will cover how to extend context-aware controls from the access layer to data centers in order to reduce operational effort, support compliance initiatives and facilitate BYOD.
- The session is targeted at network and security architects who want to know more about Secure Access using the TrustSec solution.

Agenda

- TrustSec Overview
- Classification
- Transport
- Enforcement
- MACSec

- TrustSec Overview
- Classification
- Transport
- Enforcement
- MACSec

SANS - 20 Critical Security Controls…

- Control # 1: Inventory of Authorized and Unauthorized devices

  Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access

- Control # 7: Wireless Access Control

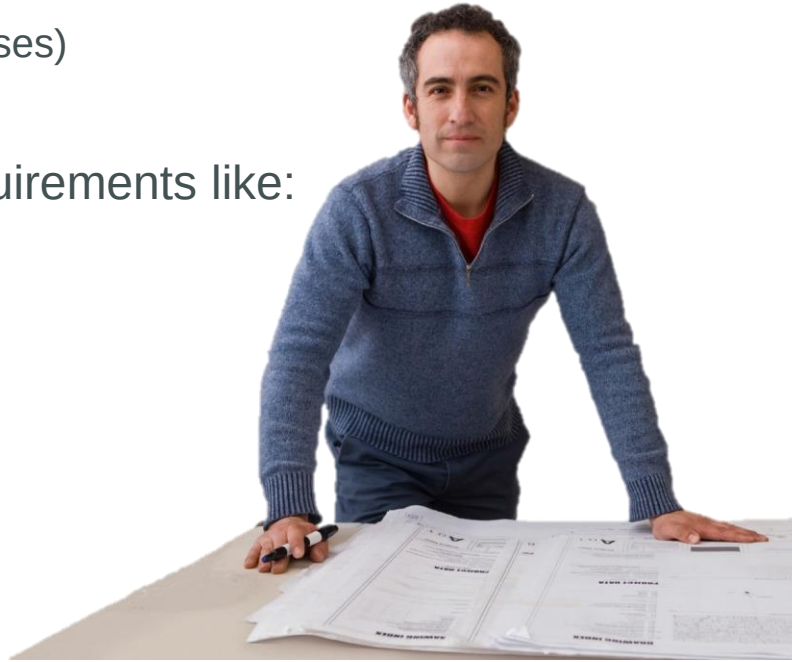
  The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

- Control # 14: Controlled Access Based on the Need to Know

  The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

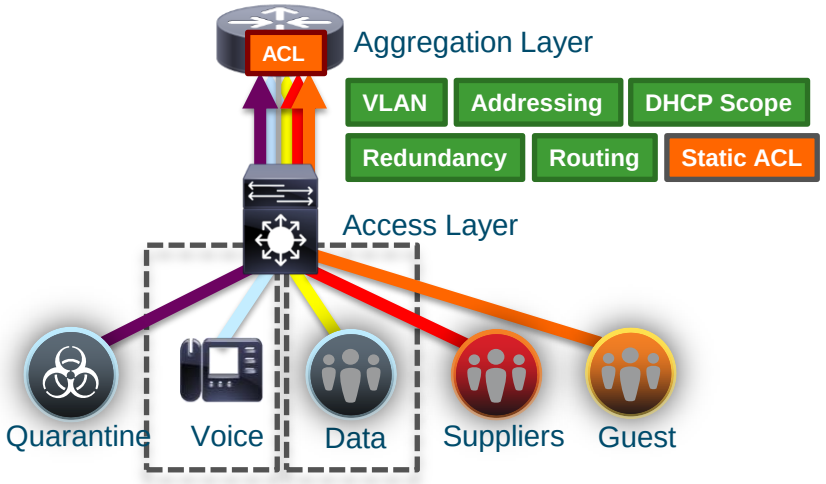
The challenge with current access controls…

- Protected assets are defined by their network connection
  - Policies are statically and manually configured
  - Rules are based on network topology (subnets, addresses)
  - IP Address does not provide user context or meaning
- Method does not facilitate key Business / IT requirements like:
  - Frequent organizational changes
  - Mobile workforces
  - Device choice
  - Virtualization



Traditional Segmentation

Steps replicated across floors, buildings and sites

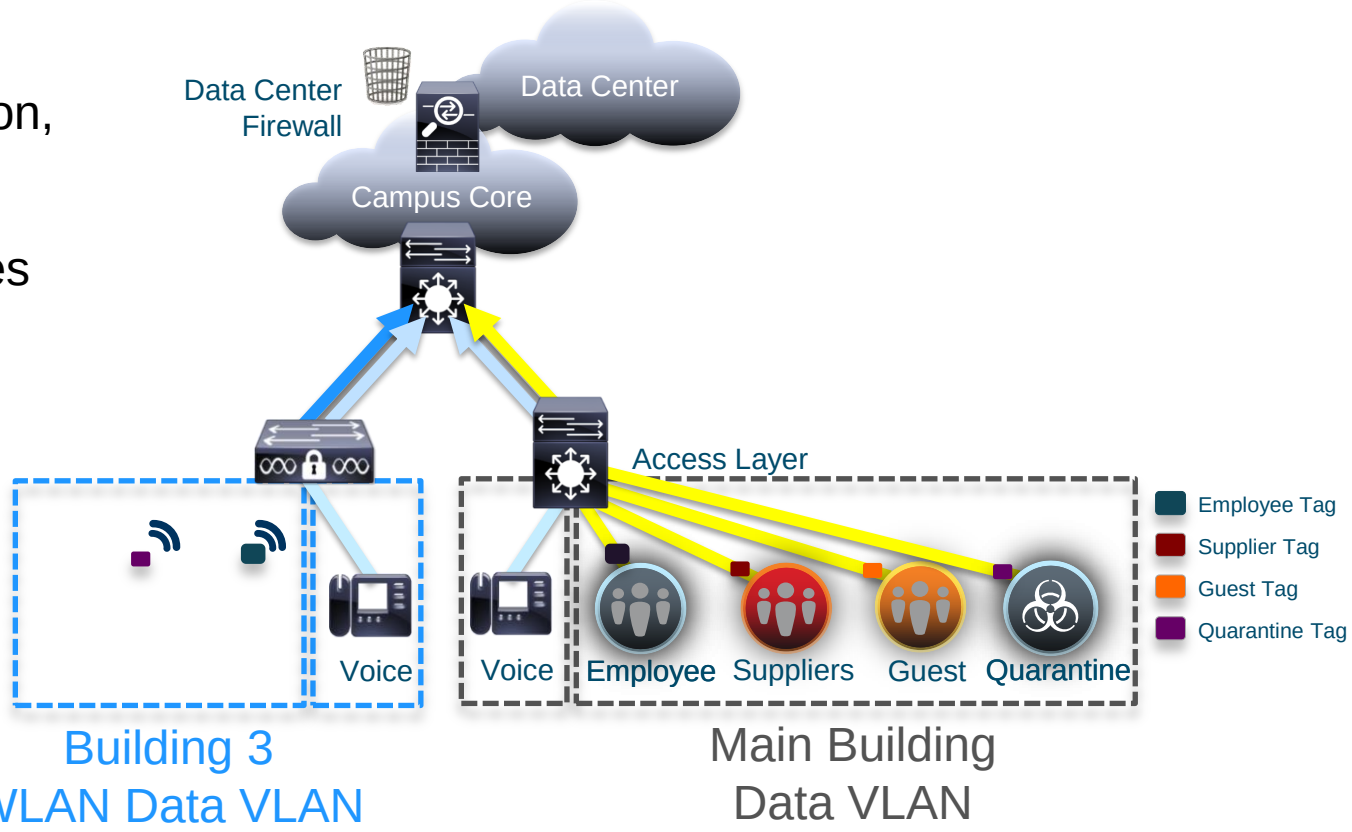


Simple Segmentation with 2 VLANs

More Segmentation with 5 VLANs

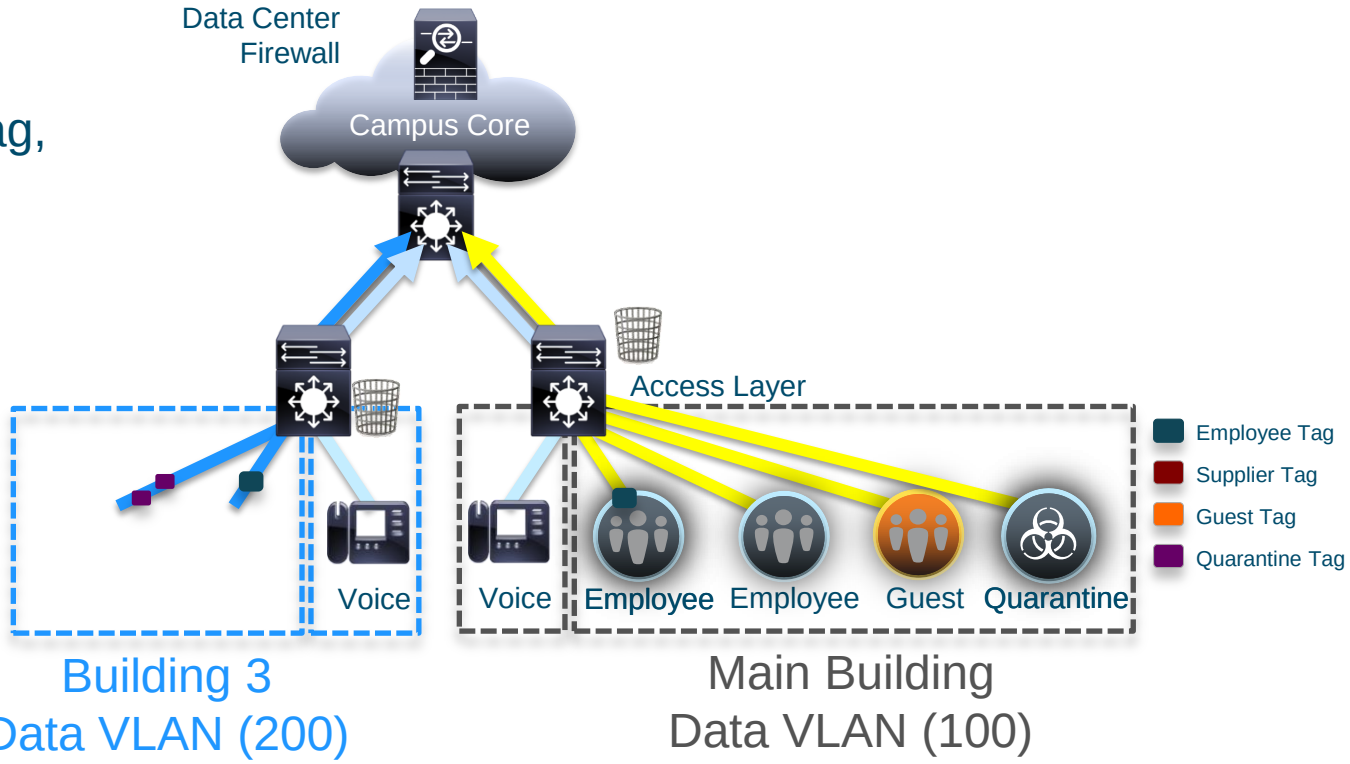
User to Data Center Access Control with TrustSec SGT

- Regardless of topology or location, policy (Security Group Tag) stays with users, devices and servers

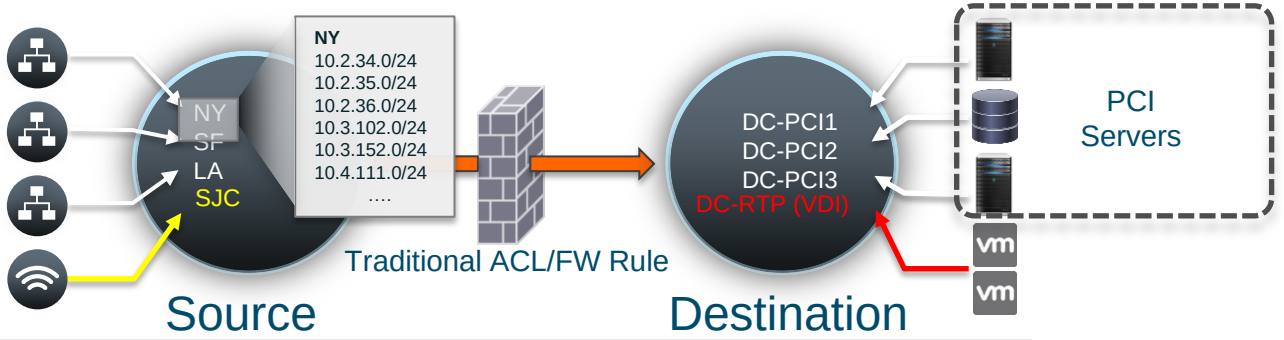


Campus segmentation with TrustSec SGT

- Enforcement is based on the Security Group Tag, can control communication in same VLAN



High OPEX Security Policy Maintenance




```
permit NY  to PCI1 for HTTPS
deny   NY  to PCI2 for SQL
deny   NY  to PCI3 for SSH
permit SF  to PCI1 for HTTPS
deny   SF  to PCI2 for SQL
deny   SF  to PCI3 for SSH
permit LA  to PCI1 for HTTPS
deny   LA  to PCI2 for SQL
deny   LA  to PCI3  for SSH
```

ACL for 3 source objects & 3 destination objects

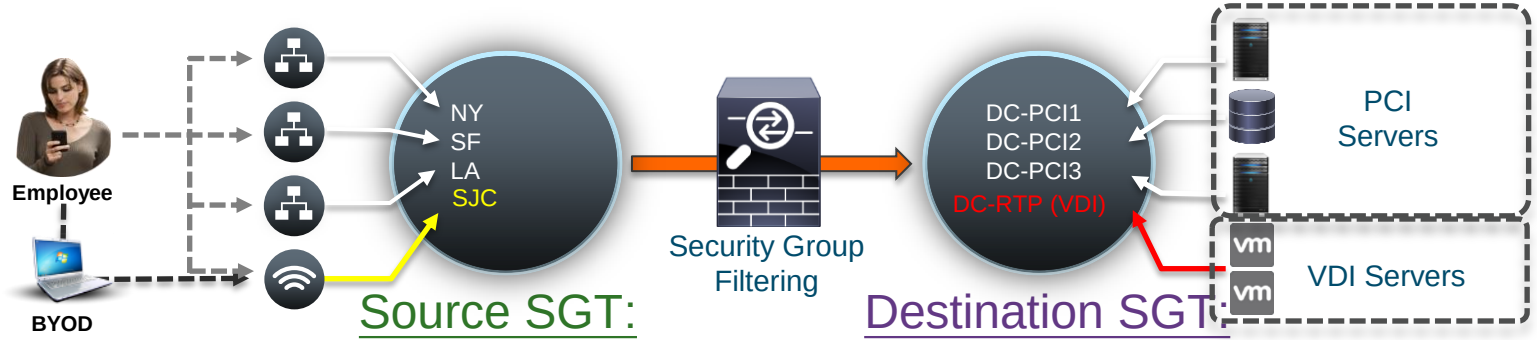
```
Permit SJC to PCI1 for HTTPS
deny   SJC to PCI2 for SQL
deny   SJC to PCI3 for SSH
```

Adding source Object

```
permit NY  to VDI  for RDP
deny   SF  to VDI  for RDP
deny   LA  to VDI  for RDP
deny   SJC to VDI  for RDP
```

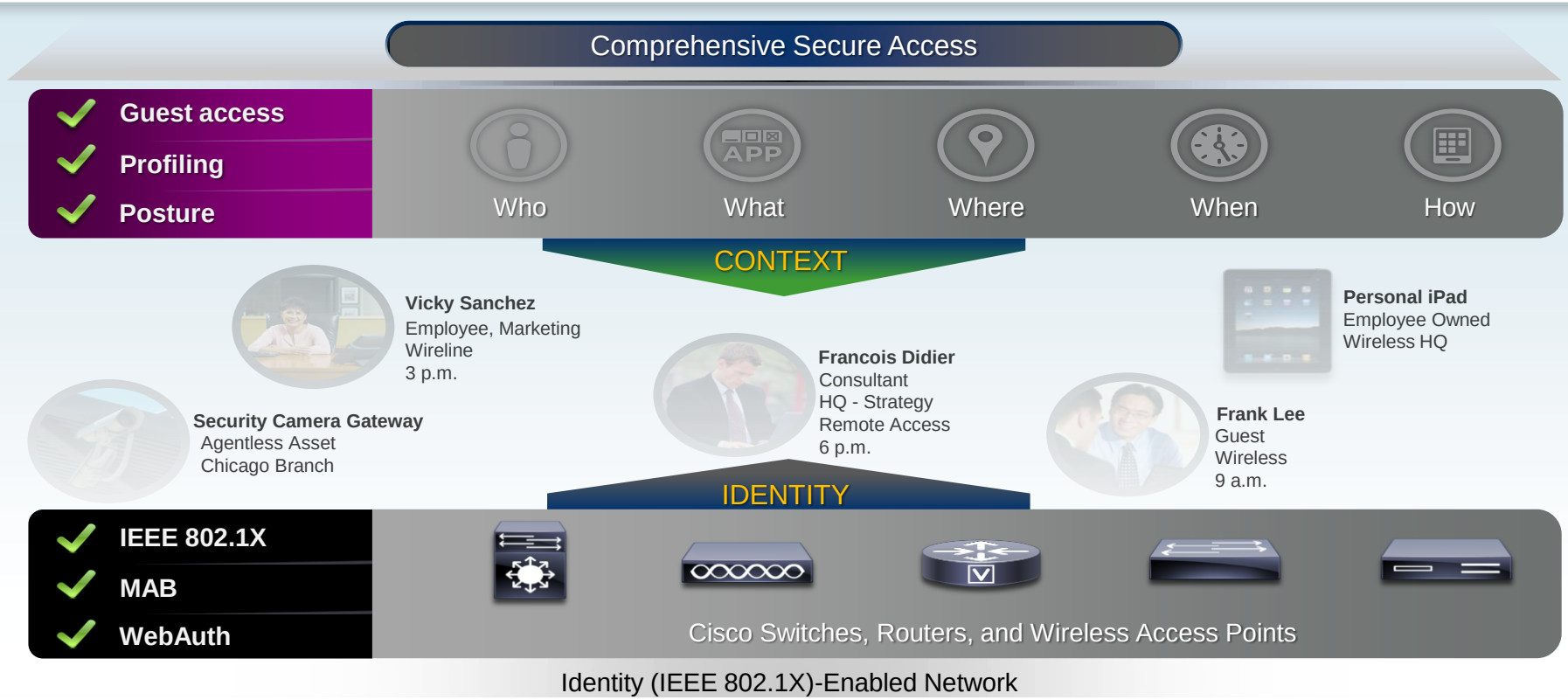
Adding destination Object

Reduced OPEX in Policy Maintenance



Clear ROI in OPEX

Extensive Policy Enforcement
Comprehensive Contextual Identity



Identity (IEEE 802.1X)-Enabled Network

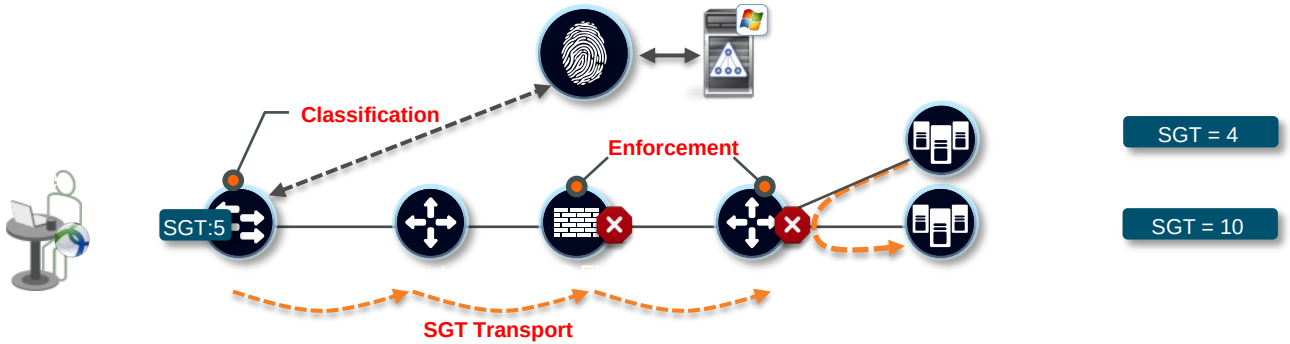
Security Group Access

- Unique 16 bit (65K) tag assigned to unique role
- Represents privilege of the source user, device, or entity
- Tagged at ingress of TrustSec domain
- Filtered (SGACL) at egress of TrustSec domain
- No IP address required in ACE (IP address is bound to SGT)
- Policy (ACL) is distributed from central policy server (ACS) or configured locally on TrustSec device

Customer Benefits

- Provides topology independent policy
- Flexible and scalable policy based on user role
- Centralized Policy Management for Dynamic policy provisioning
- Egress filtering results to reduce TCAM impact

TrustSec In Action



- TrustSec is a context-based firewall or access control solution:
- **Classification** of systems/users based on **context** (user role, device, location, access method)
- The context-based classification **propagates** using SGT
- SGT used by firewalls, routers and switches to make intelligent forwarding or blocking decisions in the DC

- Overview
- Classification
- Transport
- Enforcement
- MACSec

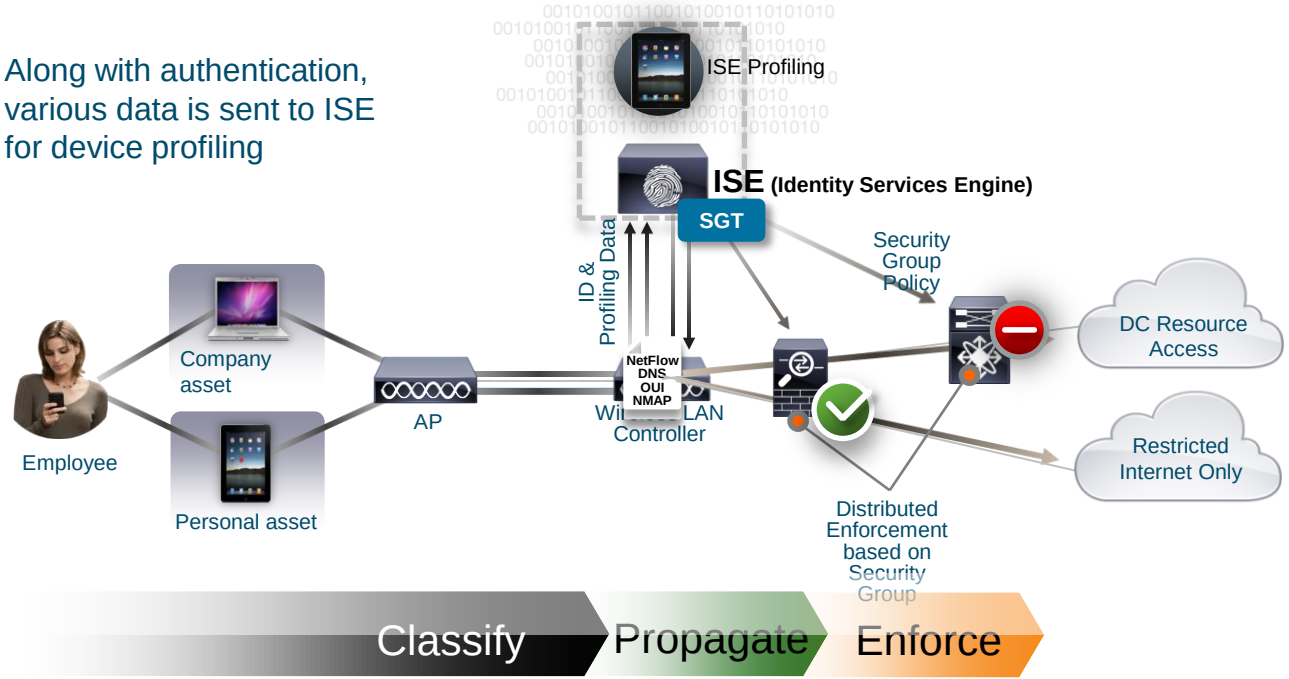
Identification and Classification

Device Type: Apple iPAD
User: Mary
Group: Employee
Corporate Asset: No

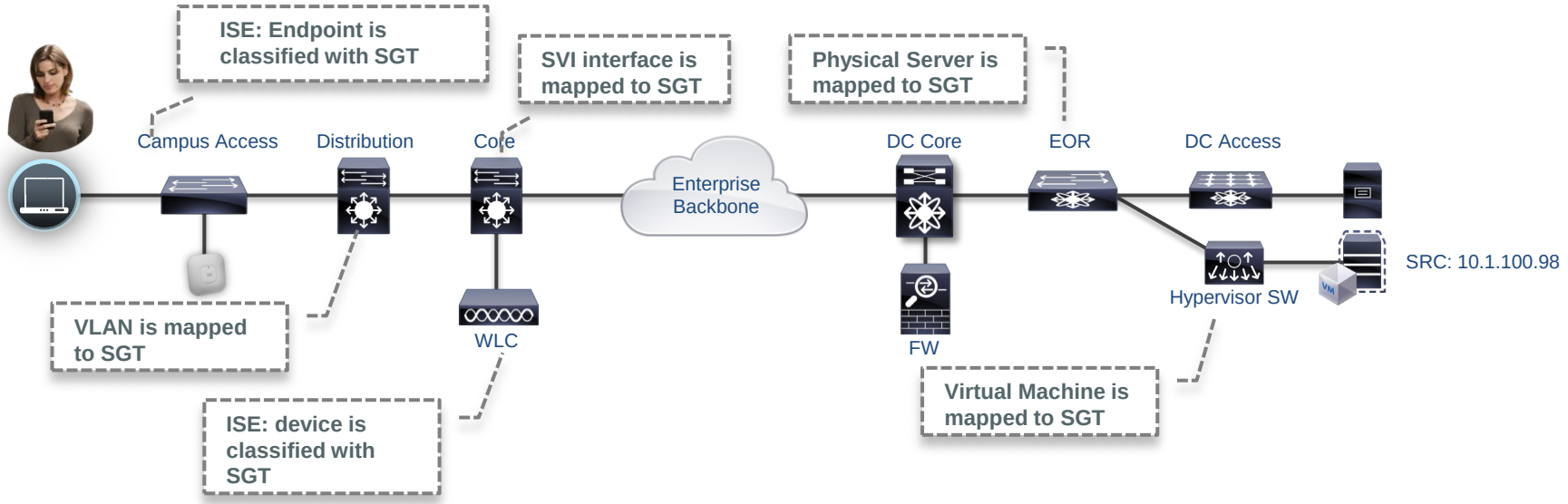
Classification Result:

Personal Asset SGT

Along with authentication, various data is sent to ISE for device profiling



How SGT is Assigned (Tagged)?



Classification summary

Dynamic Classification

802.1X Authentication

Web Authentication

MAC Auth Bypass

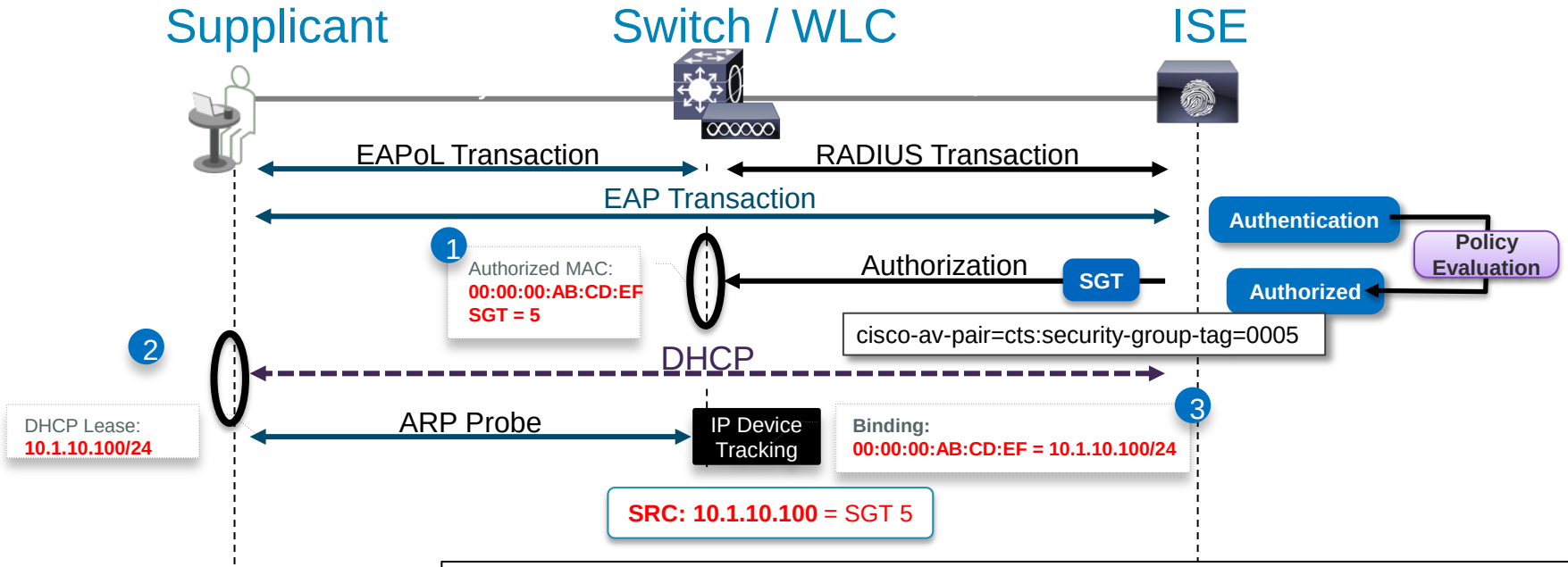
Static Classification

- IP Address
- VLANs
- Subnets
- L2 Interface
- L3 Interface
- Virtual Port Profile
- Layer 2 Port Lookup

Common Classification for End Devices

Common Classification for Servers, Topology-based policy, etc.

Dynamic Classification Process in Detail

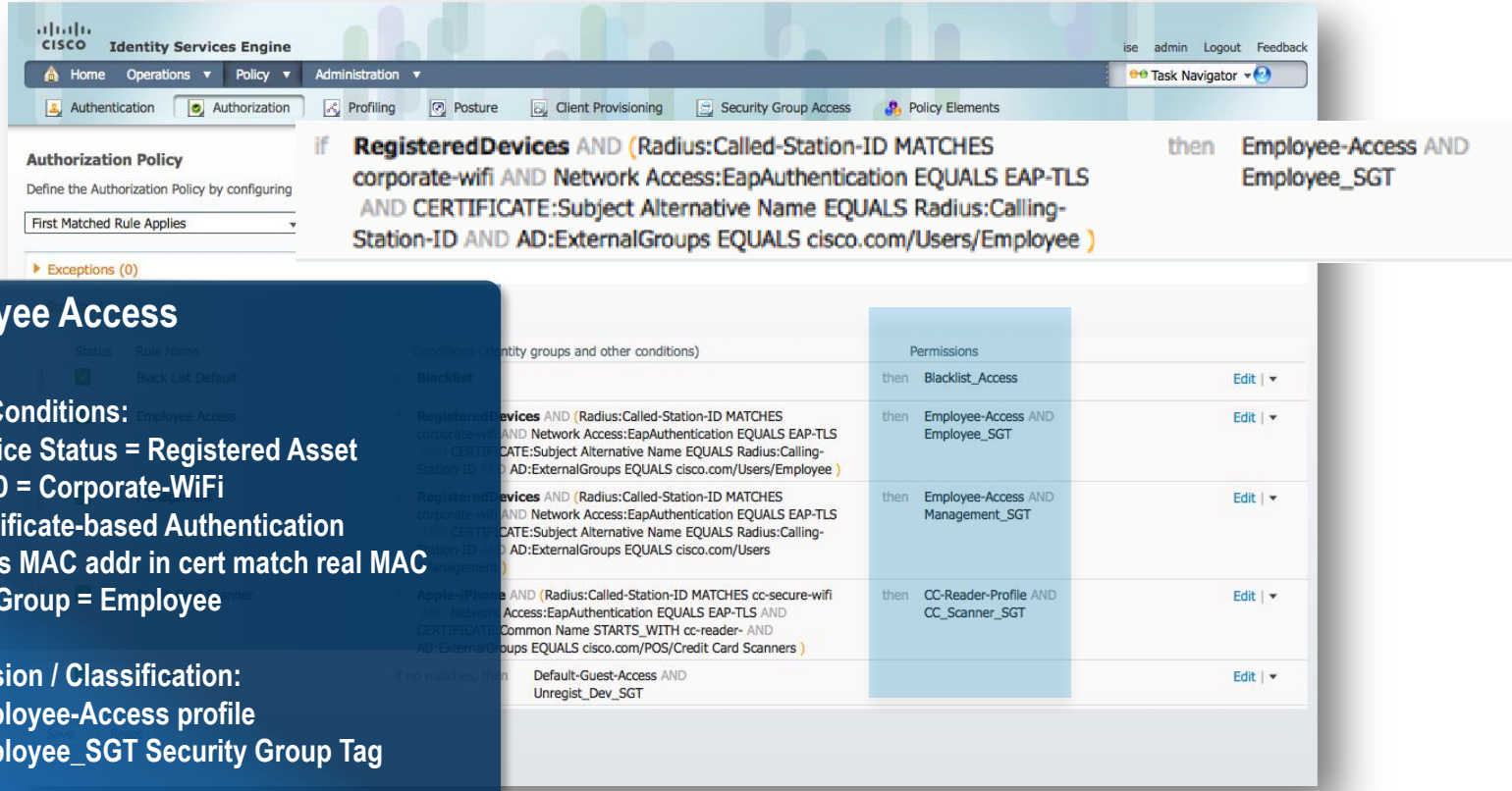


Make sure that IP Device Tracking is TURNED ON

```
3560X#show cts role-based sgt-map all details
Active IP-SGT Bindings Information

IP Address              Security Group          Source
============================================
10.1.10.1               3:SGA_Device            INTERNAL
10.1.10.100             5:Employee              LOCAL
```

ISE as Centralized Policy Manager



Employee Access

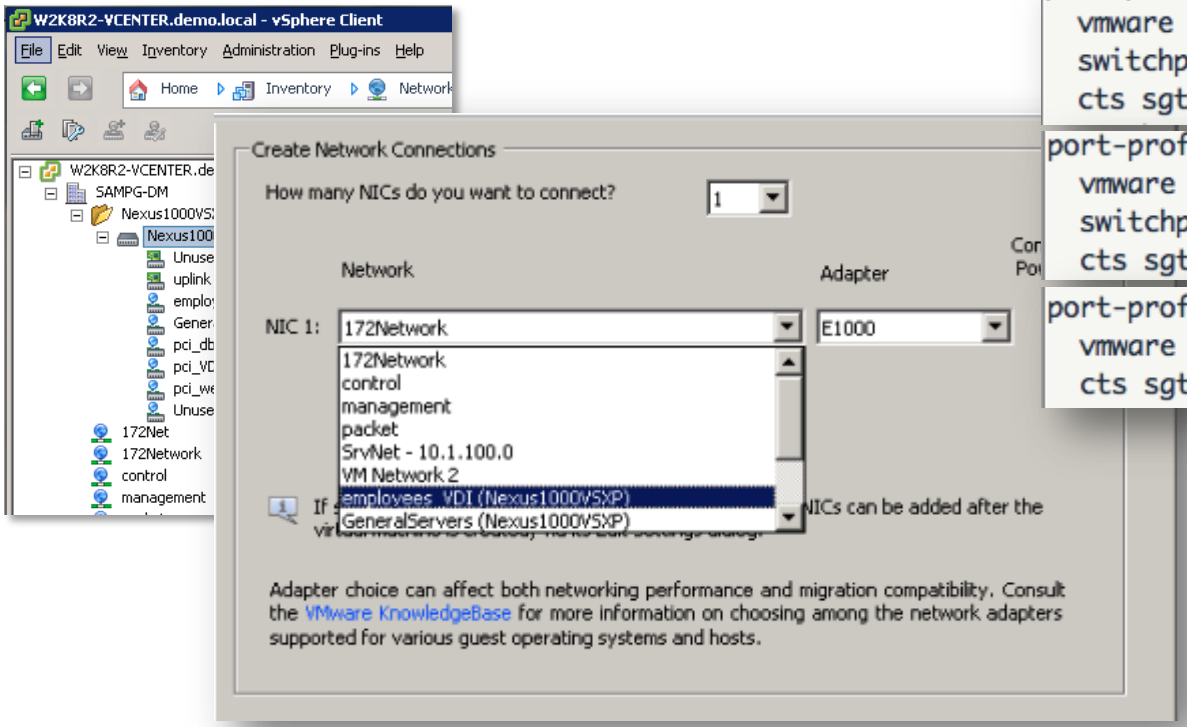
Match Conditions:

- Device Status = Registered Asset
- SSID = Corporate-WiFi
- Certificate-based Authentication
- Does MAC addr in cert match real MAC
- AD Group = Employee

Permission / Classification:

- Employee-Access profile
- Employee_SGT Security Group Tag

SGT to Port Profile




```
port-profile type vethernet GeneralServers
  vmware port-group
  switchport access vlan 100
  cts sgt 5
```

```
port-profile type vethernet pci_web
  vmware port-group
  switchport access vlan 100
  cts sgt 7
```

```
port-profile type vethernet pci_db
  vmware port-group
  cts sgt 8
```

Nexus 1000v version 2

TrustSec Platform Support

Policy Management

Identity Services Engine

Classification

Enforcement

Transport

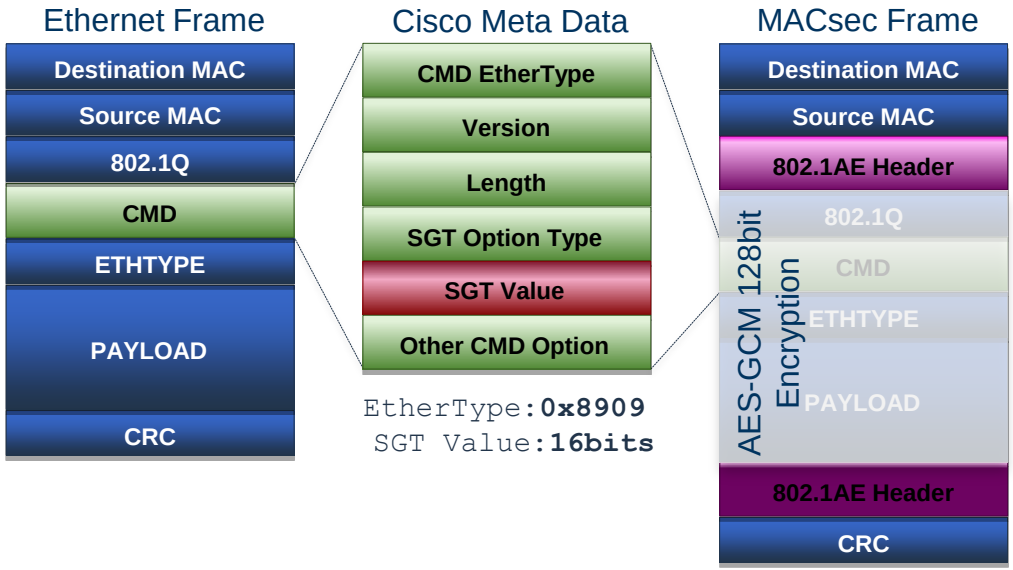
Cat 2K-S (SXP)	N7K (SXP/SGT)	ASR1K (SXP/SGT)
Cat 3K (SXP)	N5K (SGT)	ISR G2 (SXP)
Cat 3K-X (SXP/SGT)	N1Kv (SXP)	ASA (SXP)
Cat 4K (SXP)		
Cat 6K Sup2T (SXP/SGT)		

MACsec Capable with Tagging: Cat3K-X, Cat6K-Sup2T, N7K

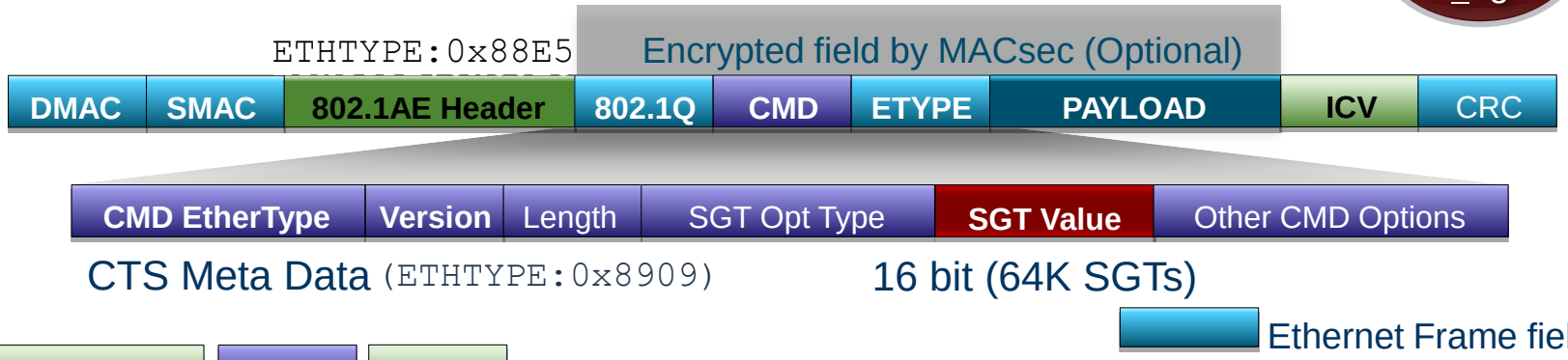
- Overview
- Classification
- Transport
- Enforcement
- MACSec

What is a Security Group Tag?

- Faster, and most scalable way to propagate SGT within LAN or Data Center
- SGT embedded within Cisco Meta Data (CMD) in Layer 2 frame
- Capable switches understands and process SGT in line-rate
- Protected by enabling MACsec (IEEE802.1AE) – optional for capable hardware
- No impact to QoS, IP Fragmentation
- L2 Frame Impact: ~20 bytes
- 16 bits field gives ~ 64,000 tag space
- Non-capable device drops frame with unknown Ethertype

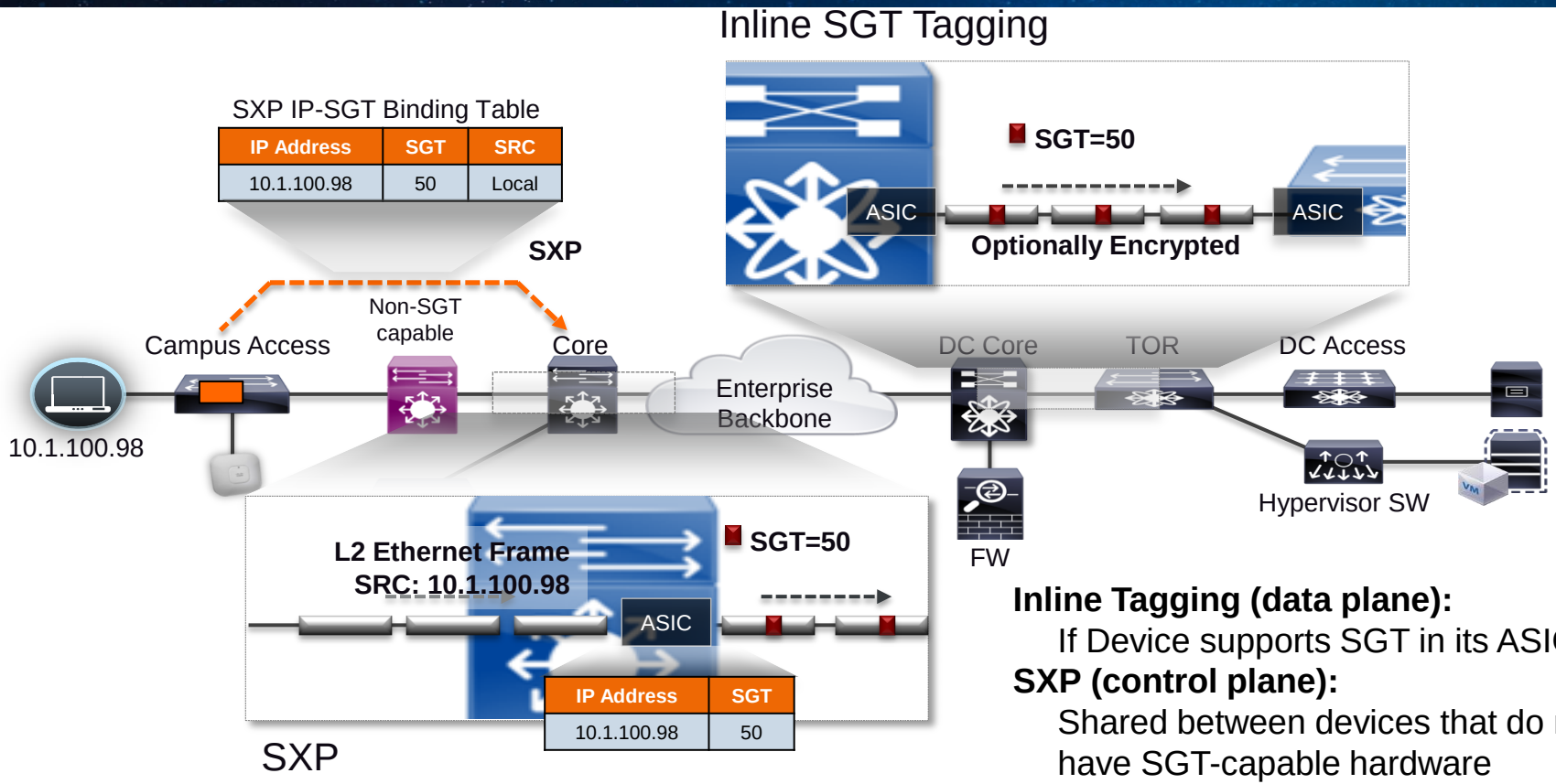


Inline Security Group Tagging



- **802.1AE Header** **CMD** **ICV** are the L2 802.1AE + TrustSec overhead
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 40 bytes
- MACsec is optional for capable hardware

SGT Transport Mechanism



Inline Tagging (data plane):

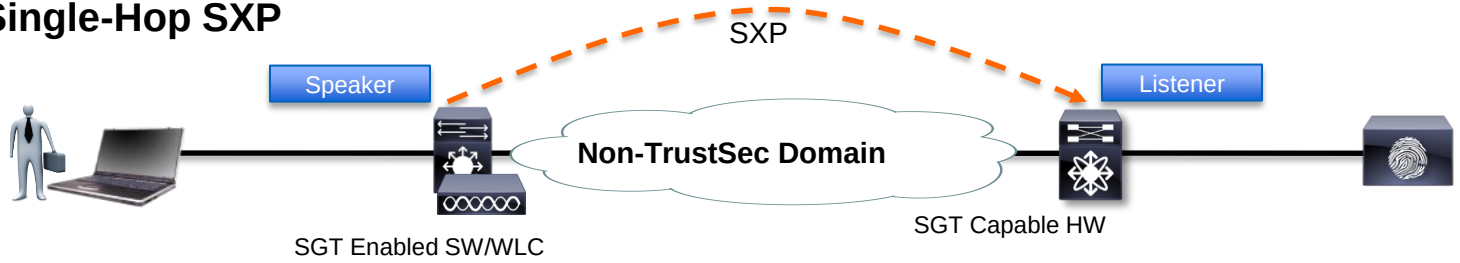
If Device supports SGT in its ASIC

SXP (control plane):

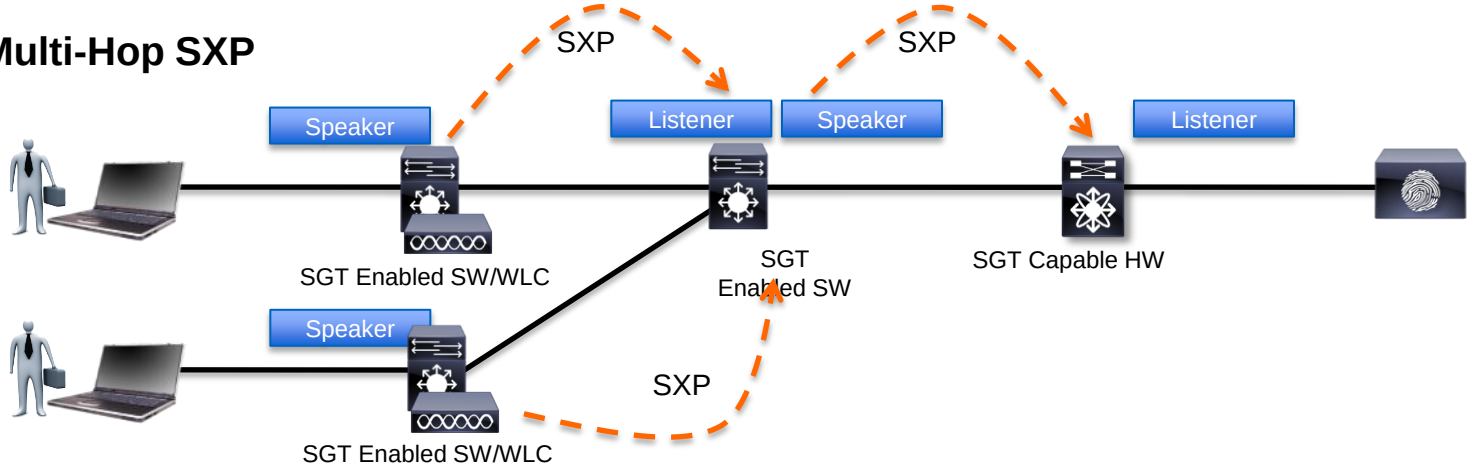
Shared between devices that do not have SGT-capable hardware

SXP Connection Types

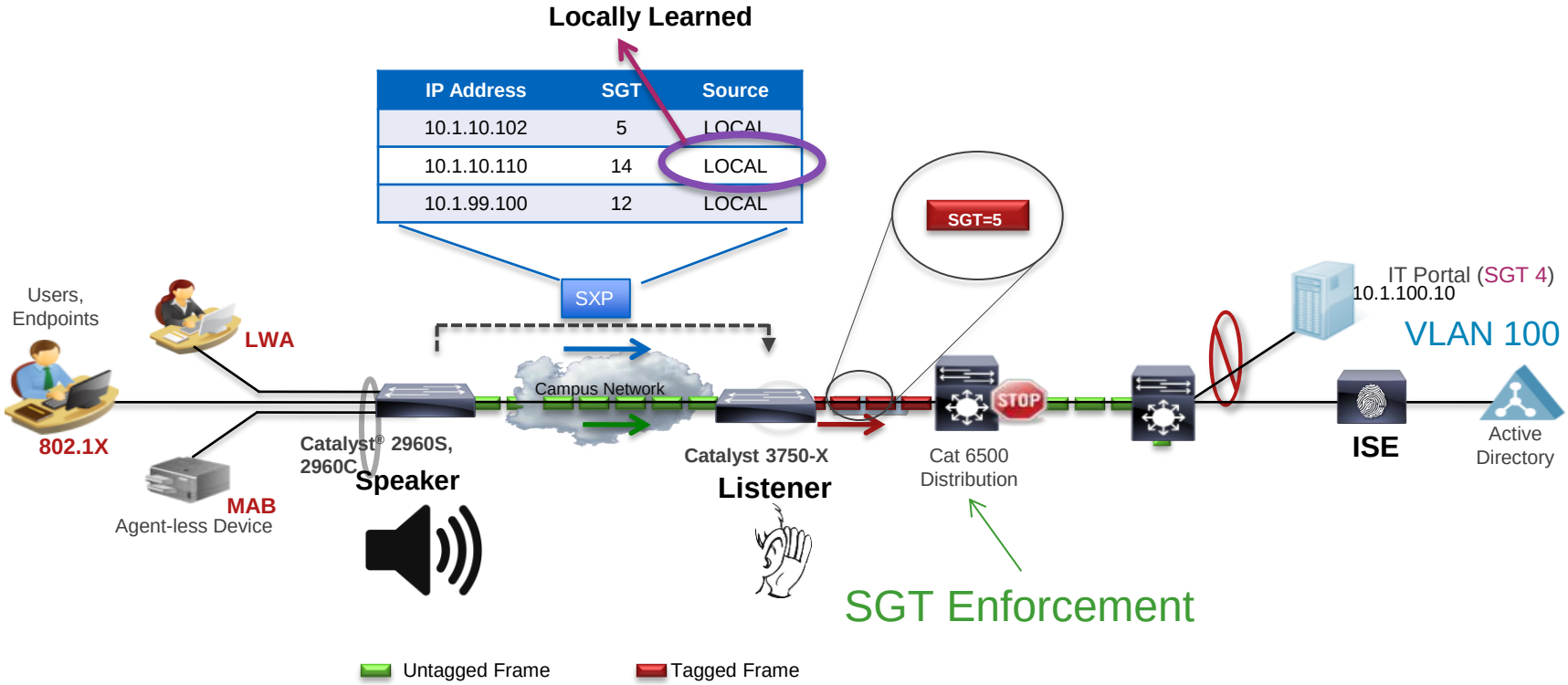
Single-Hop SXP



Multi-Hop SXP



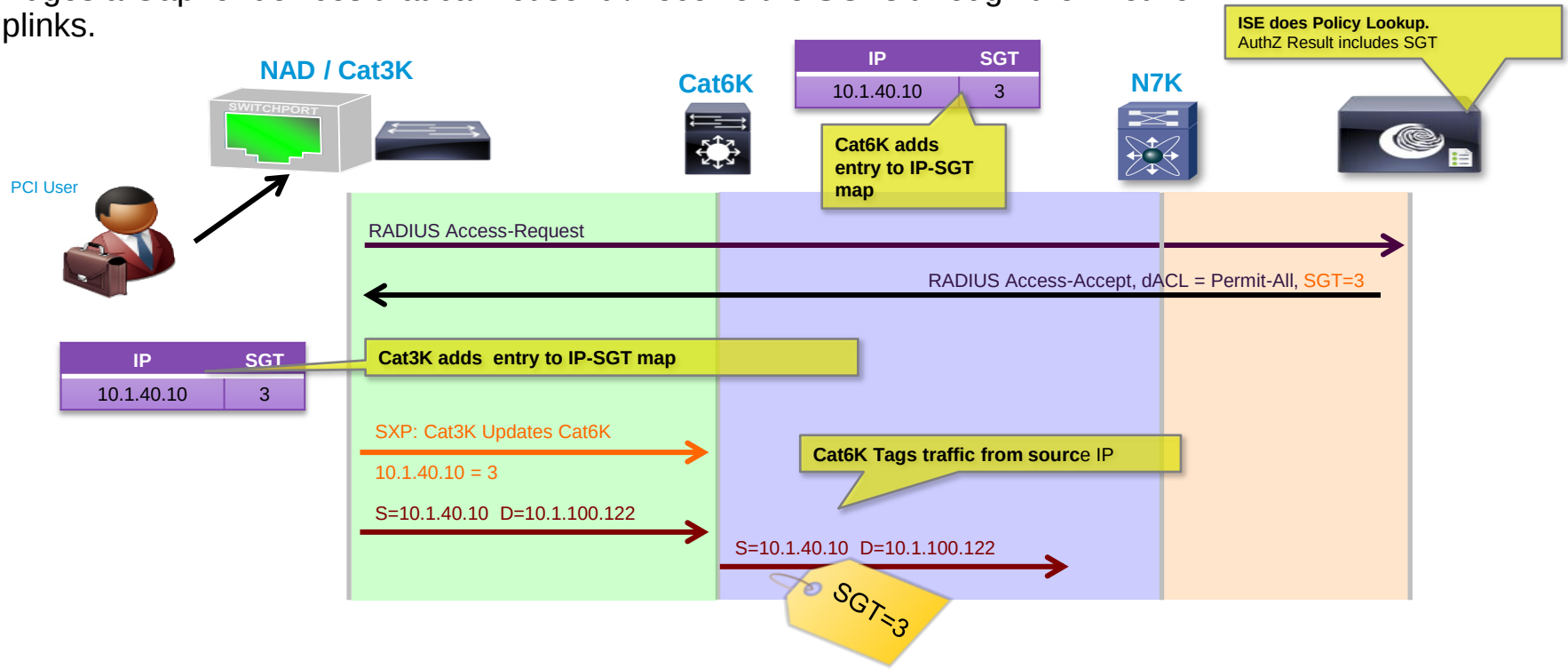
SGTagging based on SXP



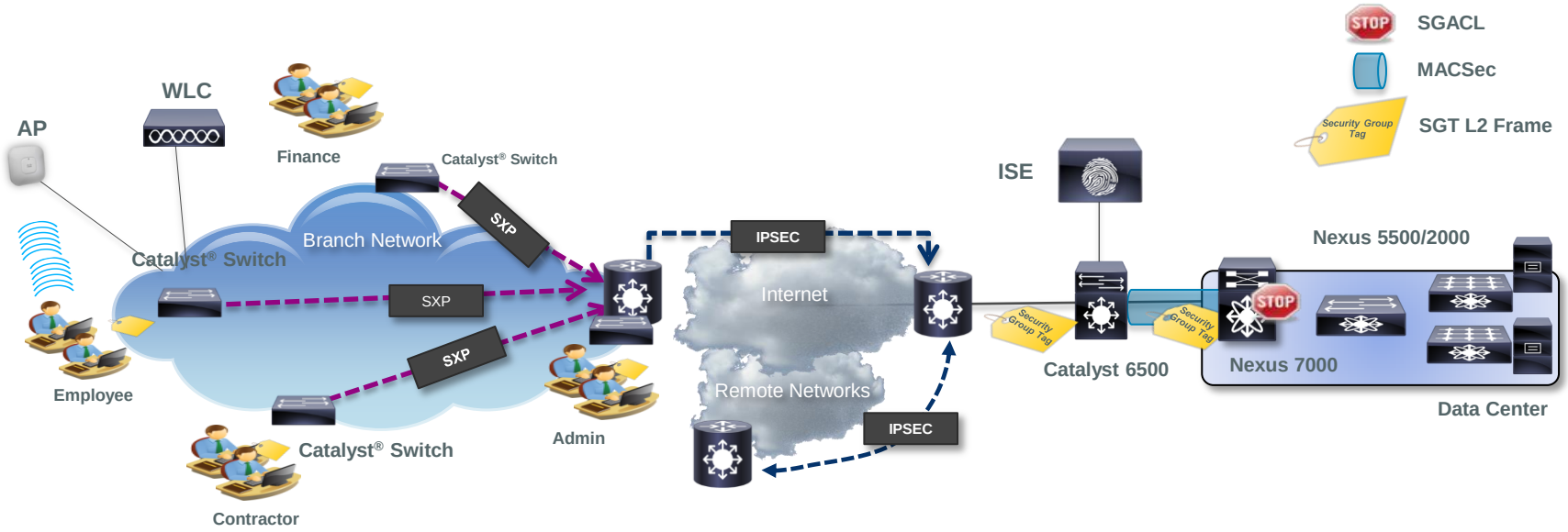
If the switch supports SXP, switch can send IP-to-SGT binding table to SGT capable device (e.g. Catalyst 3750-X)

Security Group eXchange Protocol (SXP)

- Think of SXP similar to a peering protocol like BGP:
- Designed to transmit IP-to-SGT mappings between devices.
- Bridges a Gap for devices that cannot send / receive the SGTs through their network uplinks.



SGT/IPSEC WAN Deployment - ISRG2

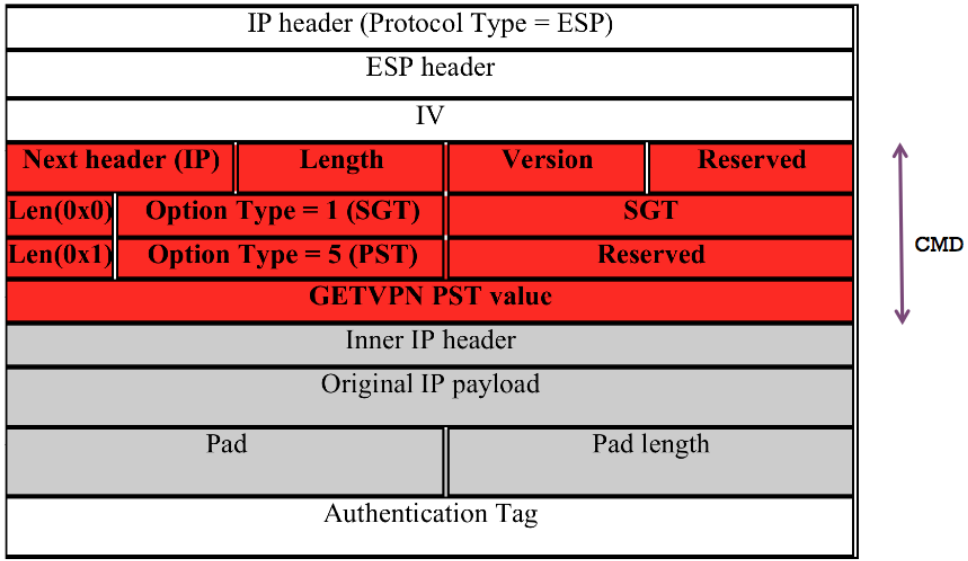


- IPSEC inline Tagging – ESP Header
- SGT Capability exchange during IKEv2 negotiations
- Learn SGT from SXP or Auth-methods

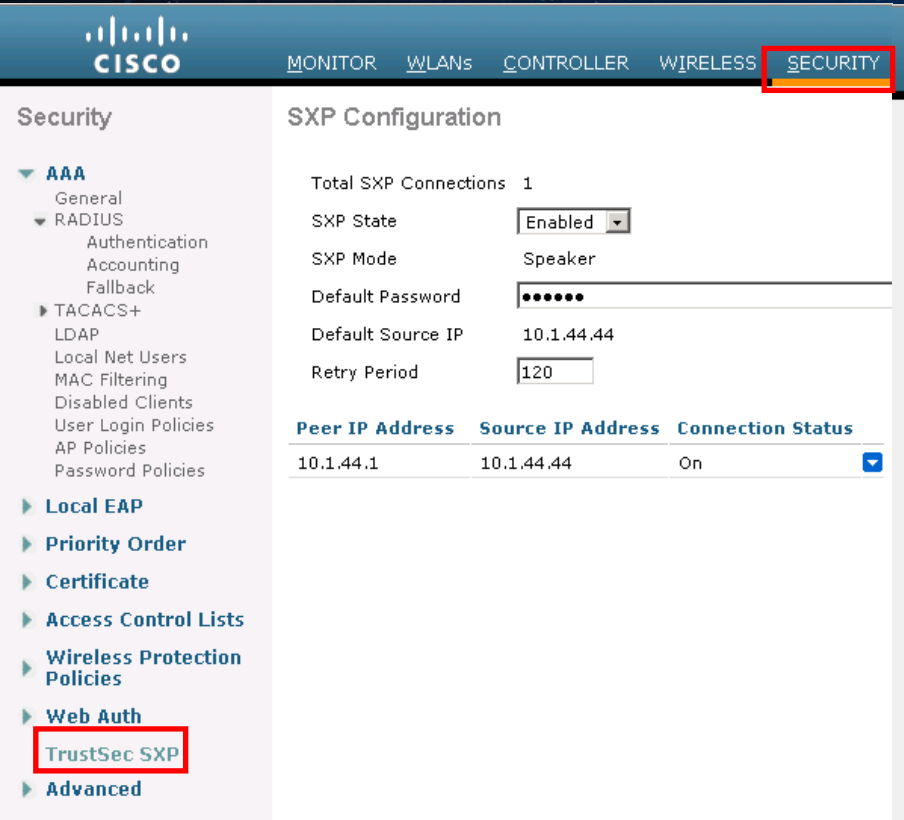
SGT- GETVPN WAN Deployment

- GETVPN inline Tagging – GET Header
- SGT Capability exchange during GET key negotiations
- Learn SGT from SXP, inline tag or Auth-methods

GETVPN Encapsulation of SGT



WLC SXP Configuration



SXP Informational Draft

draft-smith-kandula-**sxp**-00 - **IETF** Tools - **Internet Engineering Task ...**
tools.**ietf**.org/html/draft-smith-kandula-**sxp**-00
3 days ago - Internet-Draft Source-Group Tag eXchange Protocol (**SXP**) January 2014 to this document. Code Components extracted from this document ...

- SXP now published as an Informational Draft to the IETF, based on customer requests
- Draft called ‘Source-Group Tag eXchange Protocol’ because of likely uses beyond security
- Specifies SXP v4 functionality with backwards compatibility to SXP v2
- http://www.ietf.org/id/draft-smith-kandula-sxp-00.txt

TrustSec Platform Support

Classification

Catalyst 2K
Catalyst 3K
Catalyst 4K
Catalyst 6K
WLC (7.2)
Nexus 7000
Nexus 5000
Nexus 1000v

Enforcement

N7K / N5K (SGACL)
Cat6K (SGACL)
Cat3K-X (SGACL)
ASA (SGFW)
ASR1K/ISRG2 (SGFW)

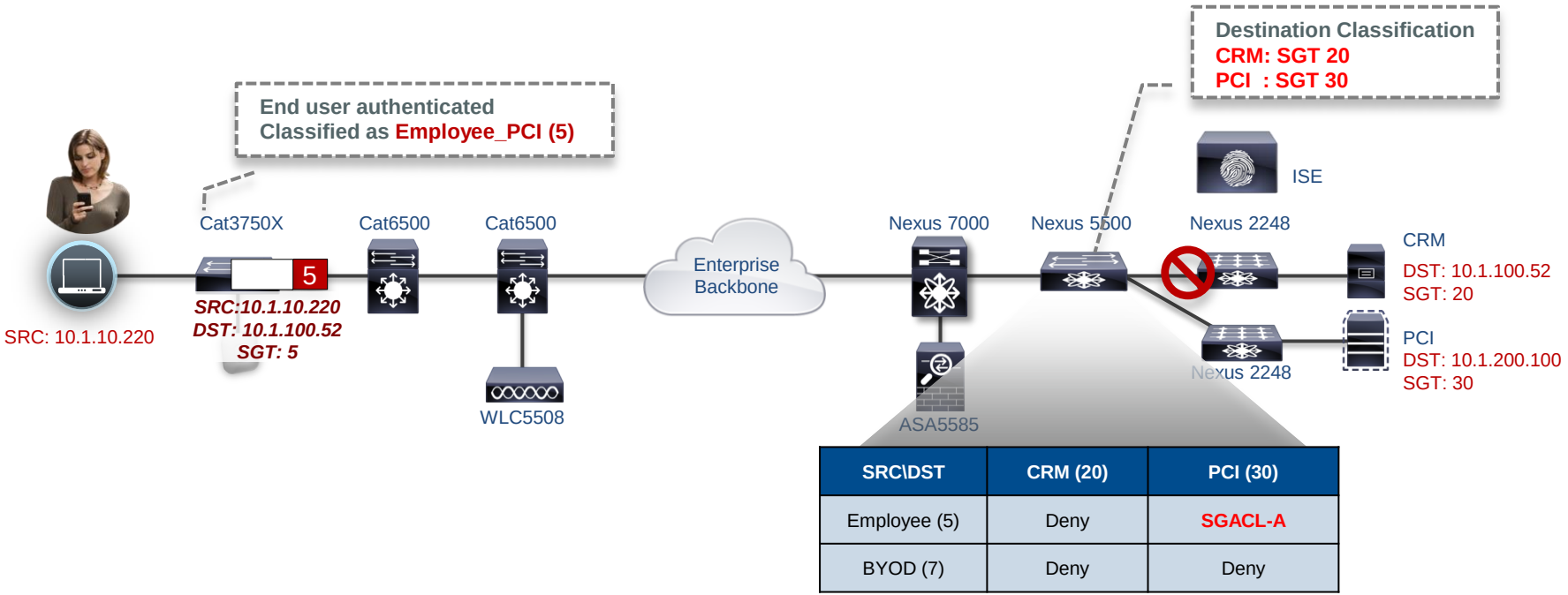
Transport

Cat 2K-S (SXP)	N7K (SXP/Inline)	ASR1K (SXP/Inline)
Cat 3K (SXP)	N5K (SXP Speaker/Inline)	ISR G2 (SXP)
Cat 3K-X (SXP/Inline)	N1Kv (SXP Speaker)	ASA (SXP)
Cat 4K (SXP)		
Cat 6K Sup2T (SXP/Inline)		

MACsec Capable with Tagging: Cat3K-X, Cat6K-Sup2T, N7K

- Overview
- Classification
- Transport
- Enforcement
- MACSec

How is traffic enforced using SGT?



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

SGACL Policy on ISE for Switches

No IP addresses in ACE

Security Group ACLs

* Name: DNS_DHCP

Description: Permit DNS A… …ccess Only

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:
permit udp dst eq 53
permit udp src eq 68 dst eq 67

Edit Permissions...

Source Security Group: **SGT_Employee (2/0002)**

Destination Security Group: **SGT_Server (5/0005)**

Status: Enabled

Description: Employee Access to Server Farm

Assigned Security Group ACLs

Select an SGACL
DNS_DHCP
HTTP_ACCESS
HTTPS_ACCESS

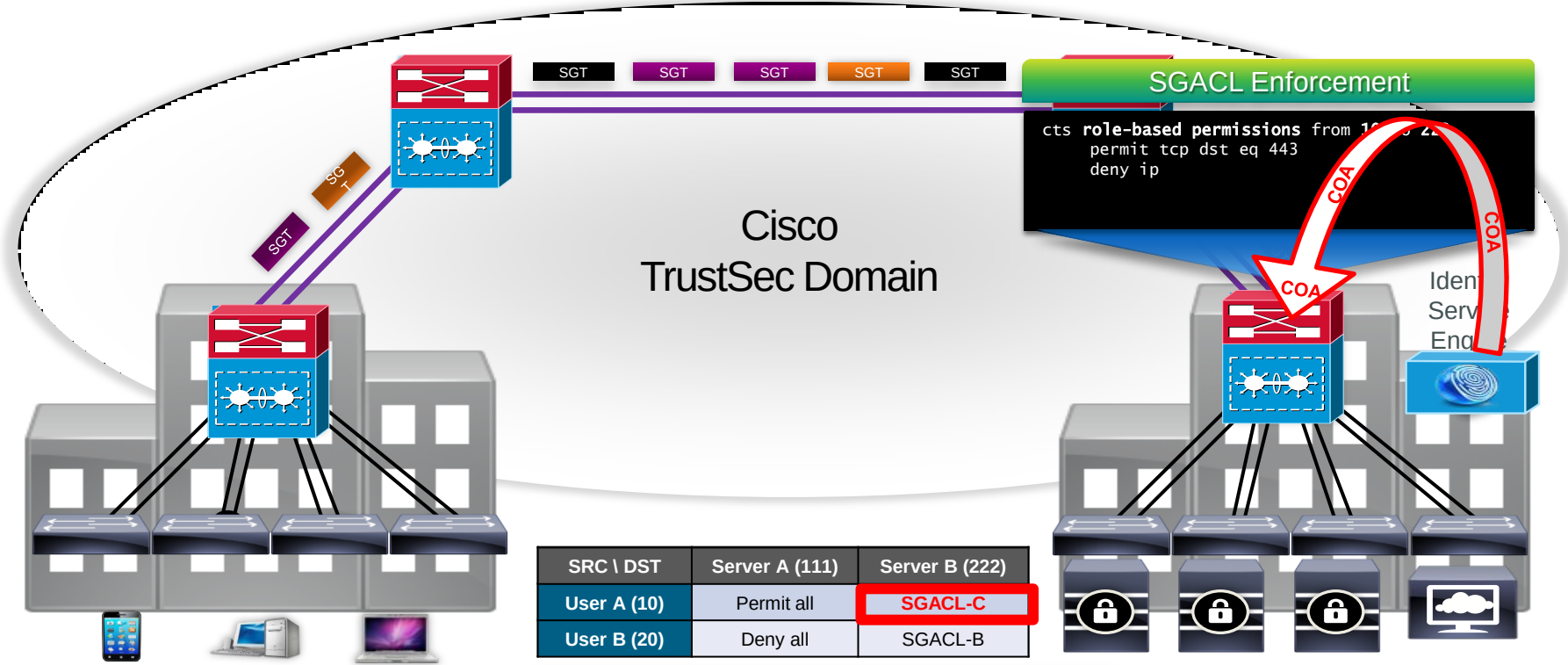
Final Catch All Rule: Deny IP

Egress Policy (Matrix View)

Edit | Add | Clear Mapping | Configure | Push | Monitor All | Dimension 3X5

Source \ Destination	SGT_Contractor (4 / 0004)	SGT_Employee (2 / 0002)	SGT_Guest (3 / 0003)	SGT_Server (5 / 0005)
SGT_Contractor (4 / 0004)	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: DNS_DHCP, HTTP_ACCESS, Deny IP
SGT_Employee (2 / 0002)	Enabled SGACLs: Deny IP	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP	Enabled SGACLs: DNS_DHCP, HTTP_ACCESS, HTTPS_ACCESS, Deny IP
SGT_Guest (3 / 0003)	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: DNS_DHCP, Deny IP

SGT and RADIUS COA

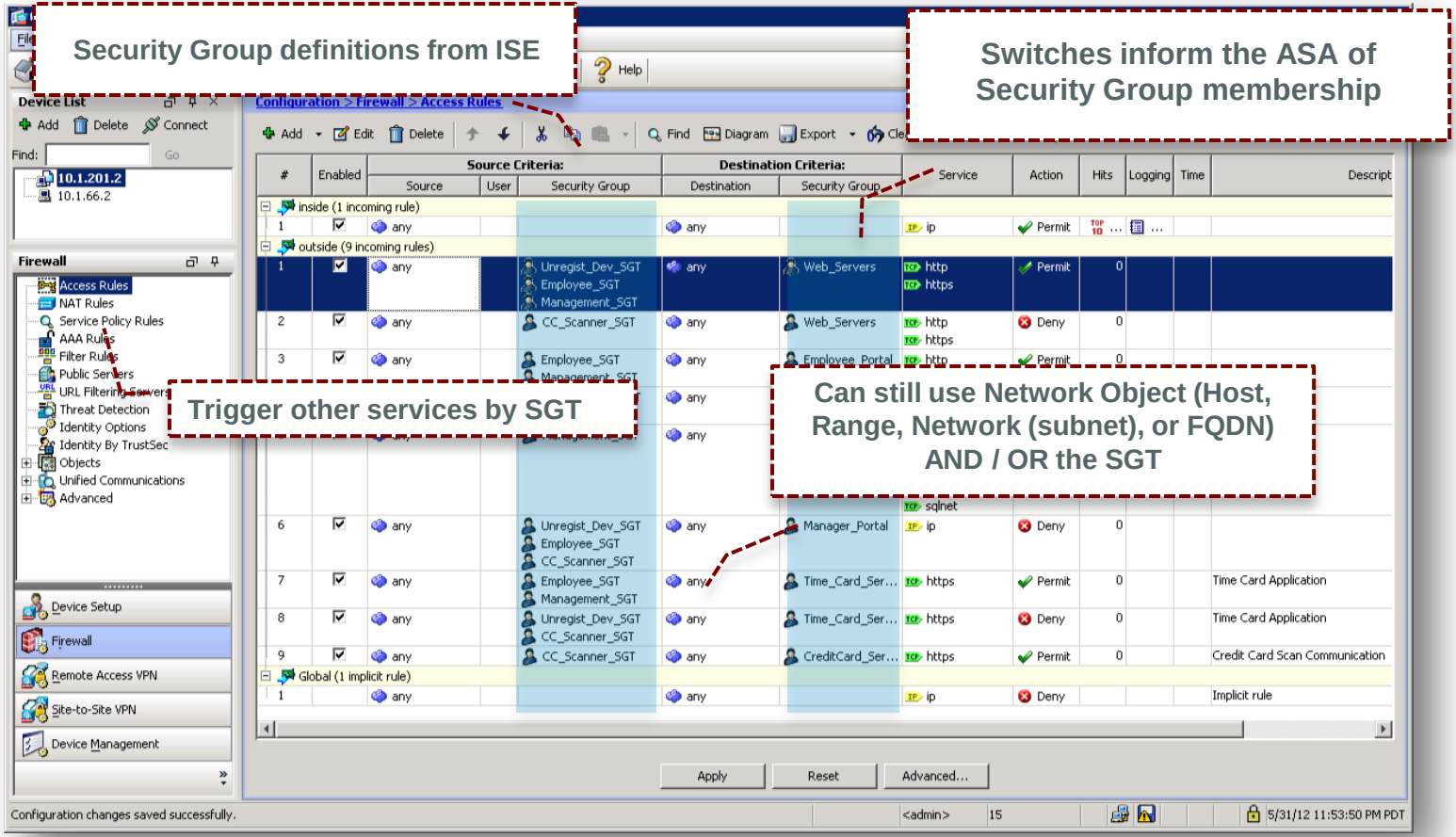


SRC \ DST	Server A (111)	Server B (222)
User A (10)	Permit all	SGACL-C
User B (20)	Deny all	SGACL-B

COA Config on IOS Switch

```
aaa server radius dynamic-author
 client 10.1.100.3 server-key cisco123
```

Policy enforcement **on Firewalls: ASA SG-FW**



SG-FW Simplifying ASA Rules and Operations

Source		Destination			Action
IP	SGT	IP	SGT	Port	Action
Any	Web Server		PCI Servers	SQL	Allow
Any	Audit users		PCI Servers	TCP	Allow
Any	Developers	Any	Dev VDI Systems	Any	Deny

- Policies can use Security Groups for user roles and server roles
- Moves and changes do not require IP-address rule-changes
- New servers/users just require group membership to be established
- Rule-base reduction with Groups instead of IP addresses can be significant
- Common classification method for campus and data center
- Simplified auditing for compliance purposes

TrustSec Platform Support

Policy Management

Identity Services Engine

Classification

Enforcement

Transport

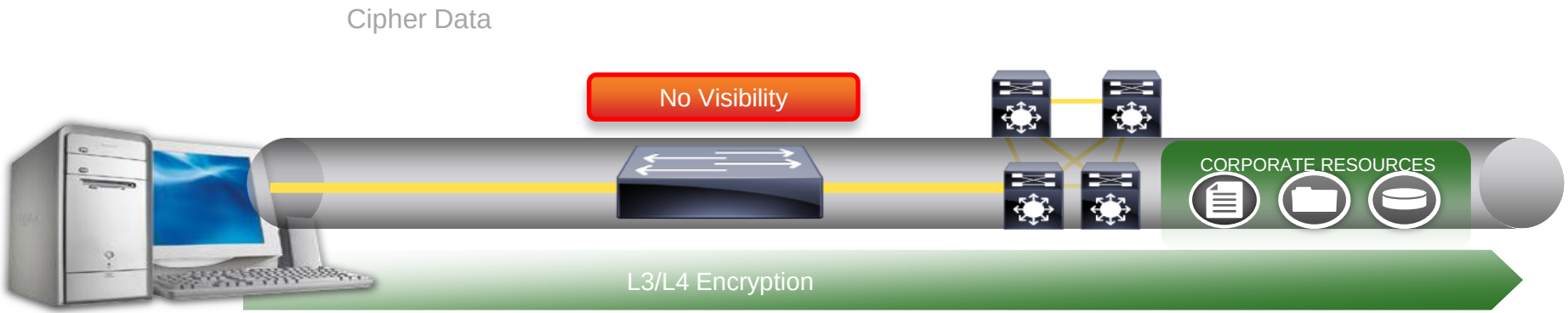
Cat 2K-S (SXP)	N7K (SXP/SGT)	ASR1K (SXP/SGT)
Cat 3K (SXP)	N5K (SGT)	ISR G2 (SXP)
Cat 3K-X (SXP/SGT)	N1Kv (SXP)	ASA (SXP)
Cat 4K (SXP)		
Cat 6K Sup2T (SXP/SGT)		

MACsec Capable with Tagging: Cat3K-X, Cat6K-Sup2T, N7K

- Overview
- Classification
- Transport
- Enforcement
- MACSec

Regulatory Compliance

Data Protection with L3/L4 Encryption



The Challenge

Encryption disables visibility for policy enforcement

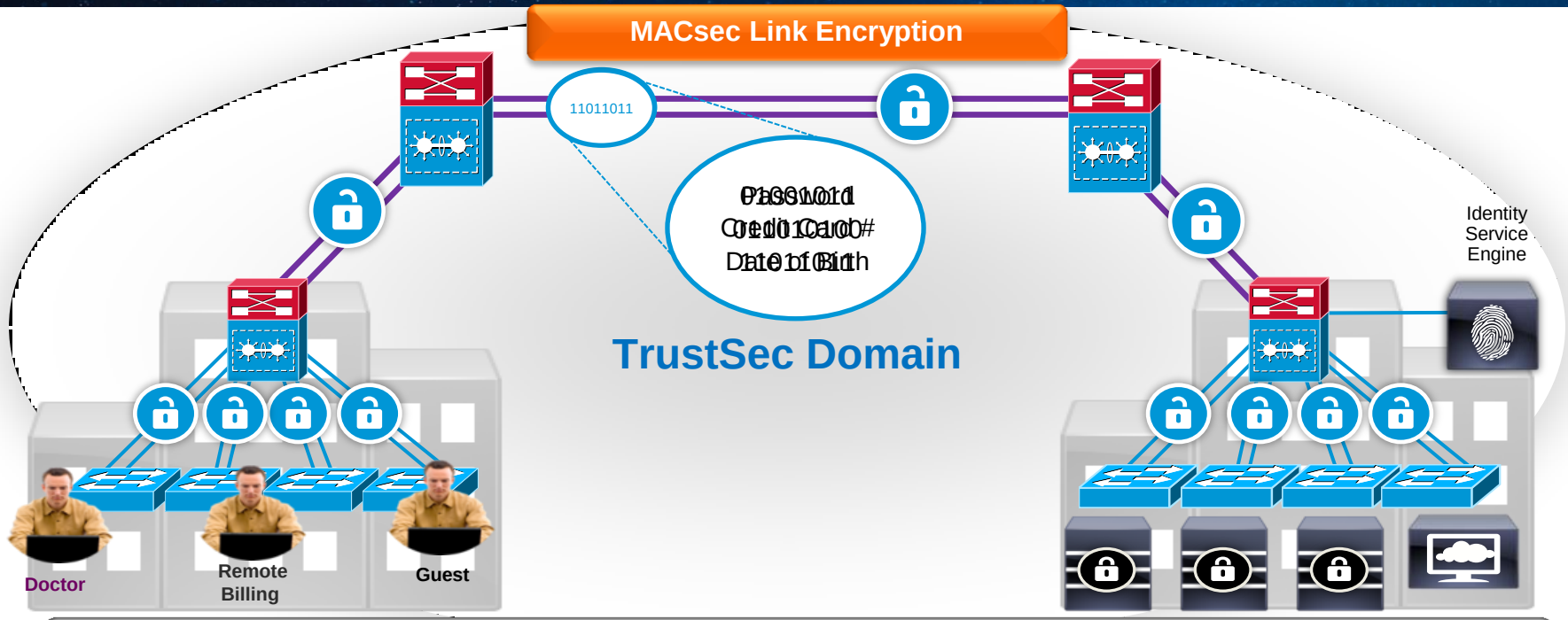
Typical Deployment Scenario

Encryption at IP or application layers

No visibility into the flows for Security and QoS policy enforcement

Securing a Campus BYOD Infrastructure

802.1AE Based Link Encryption



Benefits

- Reduces risk of security breaches by preventing eavesdropping
- Confidentiality of traffic throughout the network

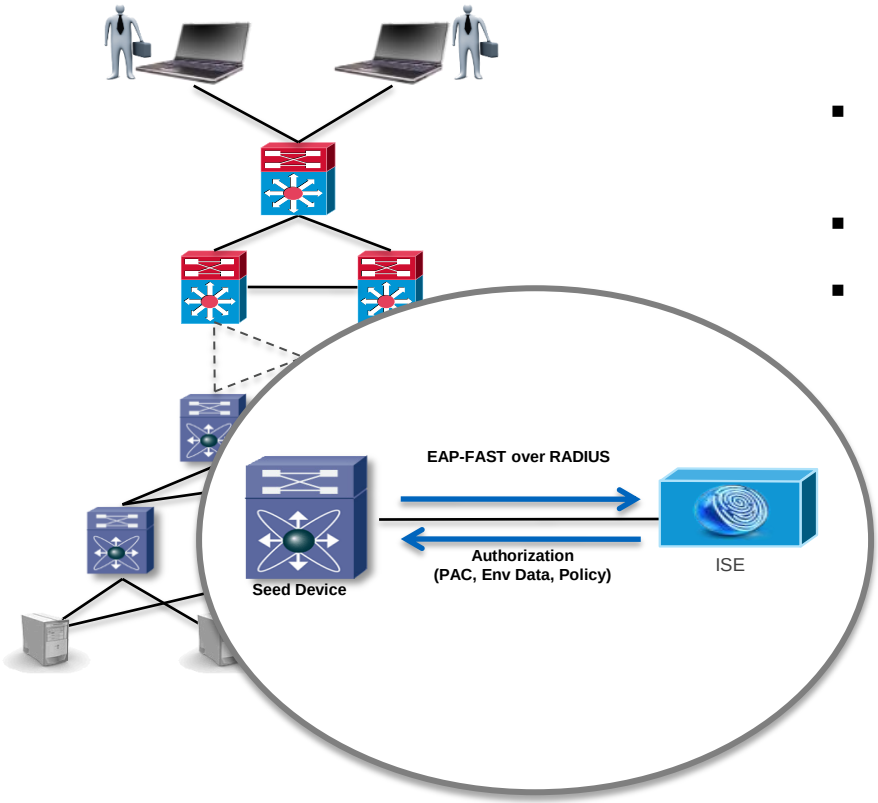
Network Device Admission Control

- Network Device Admission Control (NDAC) provides strong **mutual authentication (EAP-FAST) to form trusted domain**
- Only SGT from **trusted peer is honored**
- Authentication leads to **Security Association Protocol (SAP)** to negotiate keys and cipher suite for encryption automatically (mechanism defined in 802.11i)
- Trusted device acquires trust and policies from ISE server

Benefits

- Mitigate rogue network devices, **establish trusted network fabric** to ensure SGT integrity and its privilege
- Automatic key and cipher suite negotiation for **strong 802.1AE based encryption**

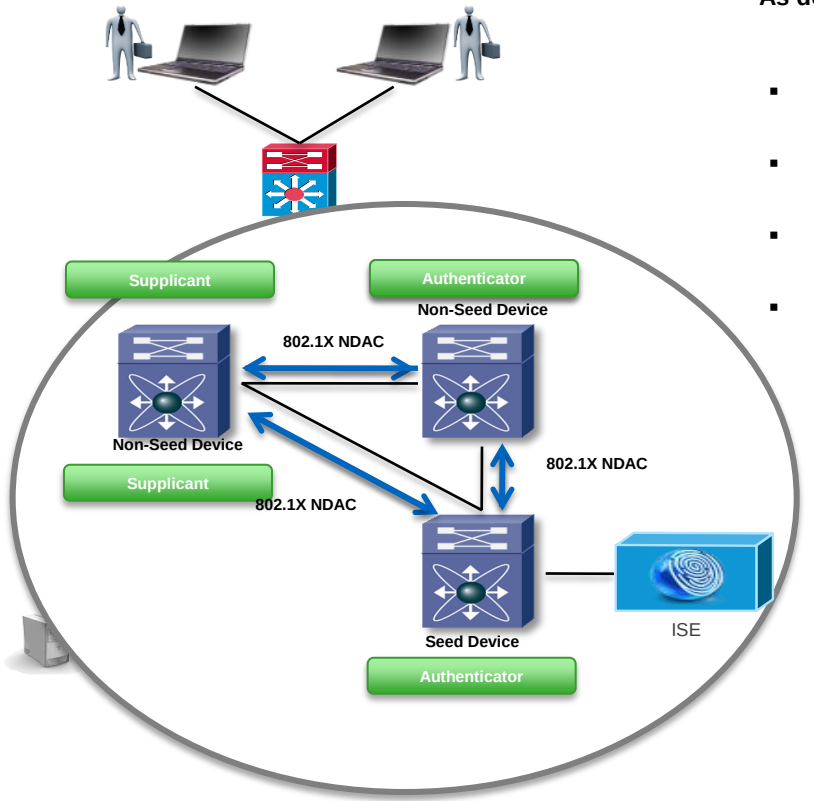
TrustSec Domain Establishment
Device Authentication (1)



NDAC validates peer identity before peer becomes the circle of Trust!

- The first device to communicate with ISE is called TrustSec Seed Device
- NDAC uses EAP-FAST/MSCHAPv2 for authentication
- Credential (including PAC) is stored in hardware key store

TrustSec Domain Establishment Device Authentication (2)

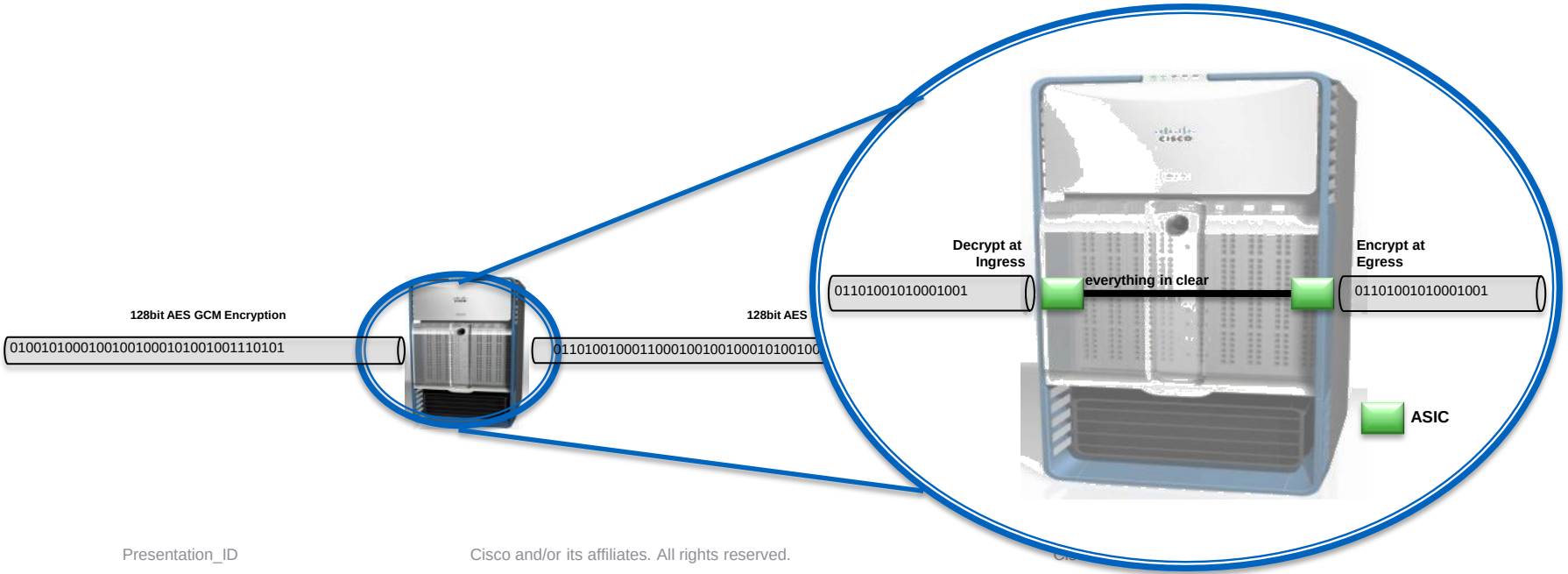


As device connects to its peer, TrustSec domain expands its border of trust

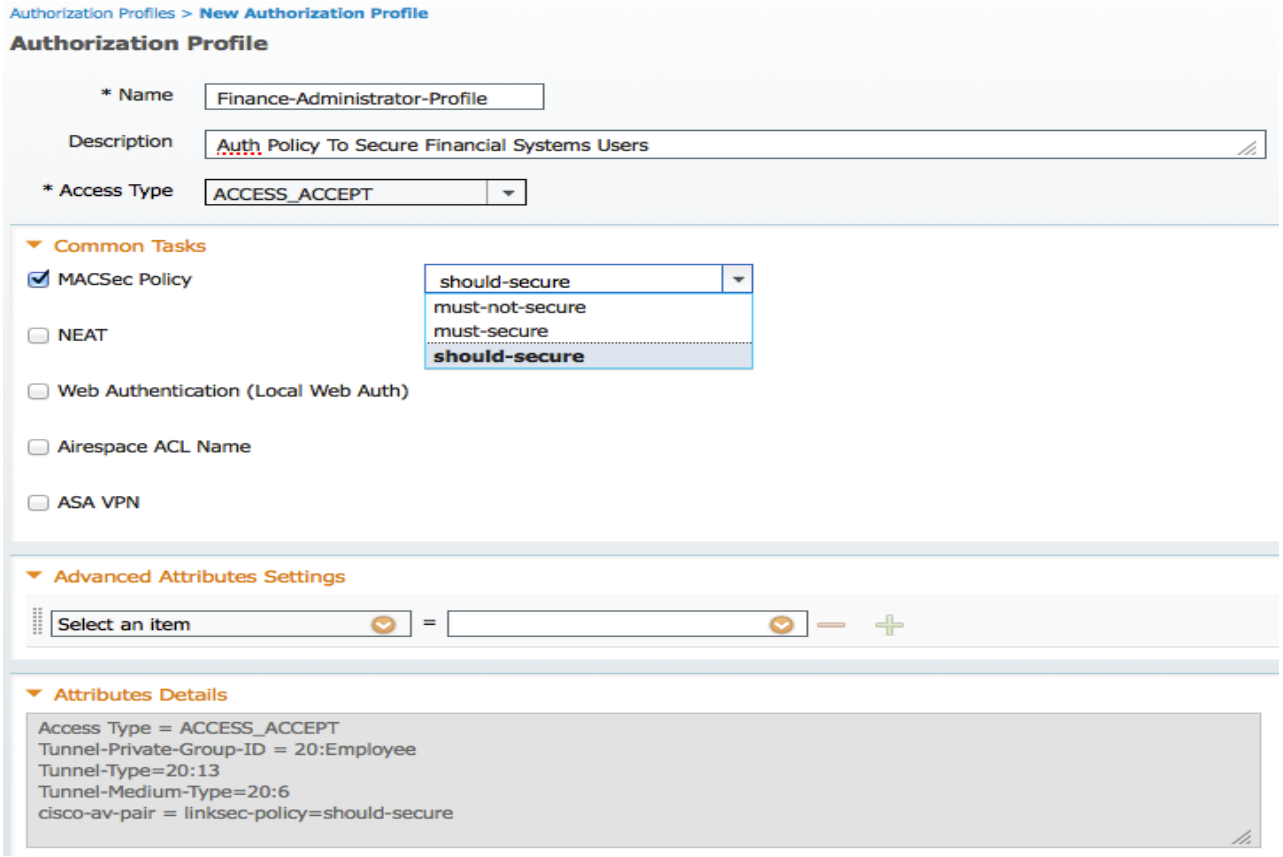
- If the device does not have information to connect to ISE, the device is called non-Seed Device
- When next device connects to device, Role determination process occurs per link basis, and both Authenticator and Supplicant role are determined.
- First peer to gain ISE server connectivity wins authenticator role. Once authenticator role is determined, the device terminates supplicant role by itself.
- In case of tie, lower MAC address wins

Hop-by-Hop Encryption via IEEE802.1AE

- “Bump-in-the-wire” model
  - Packets are encrypted on egress
  - Packets are decrypted on ingress
  - Packets are in the clear in the device
- Allows the network to continue to perform all the packet inspection features currently used



Setting an ISE MACsec Authorization Policy



- Overview
- Classification
- Transport
- Enforcement
- MACSec
- Use Cases

SGA Deployment Use Cases

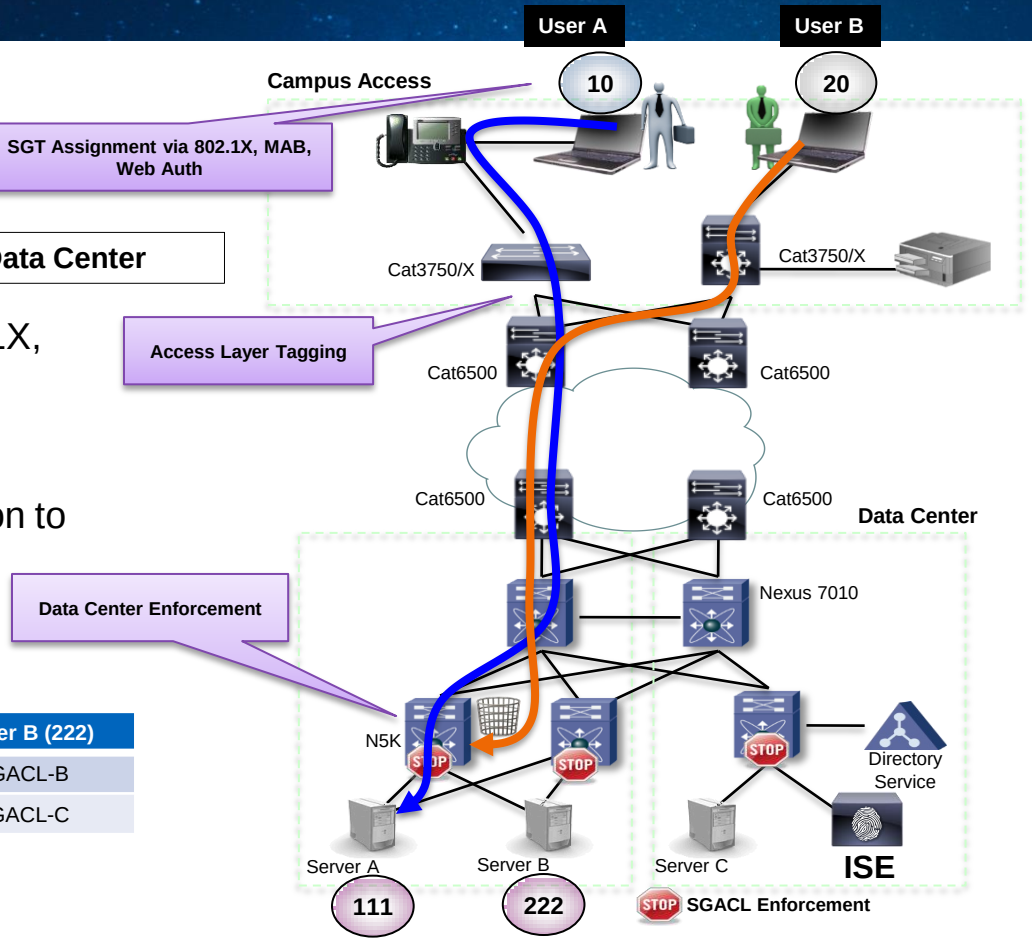
Campus LAN Deployment

Use Case

Campus users accessing resources in Data Center

- User traffic SGTagged at access via 802.1X, MAB, or Web Authentication
- Server SGT assigned via static mapping
- SGTag propagated thru access, distribution to data center
- SGACL enforcement at data center egress switch

SRC \ DST	Server A(111)	Server B (222)
User A (10)	Permit all	SGACL-B
User B (20)	Deny all	SGACL-C



SGA Deployment Use Cases

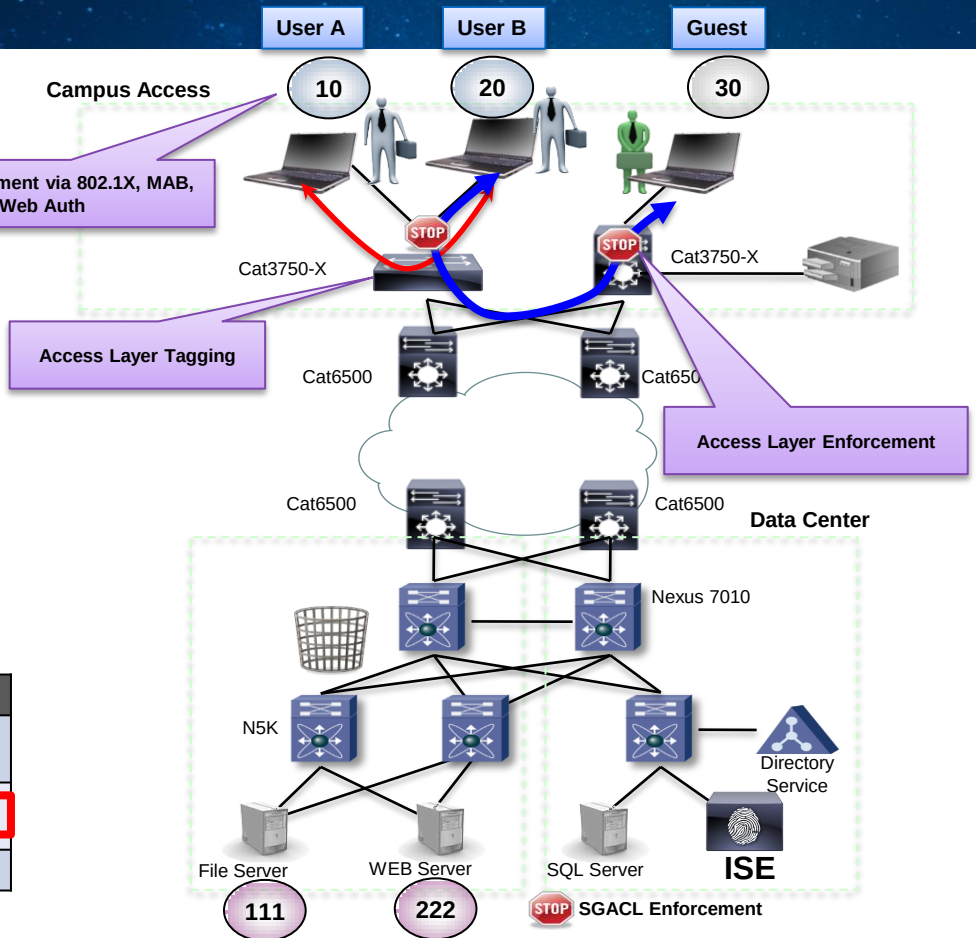
Access Layer Enforcement

Use Case

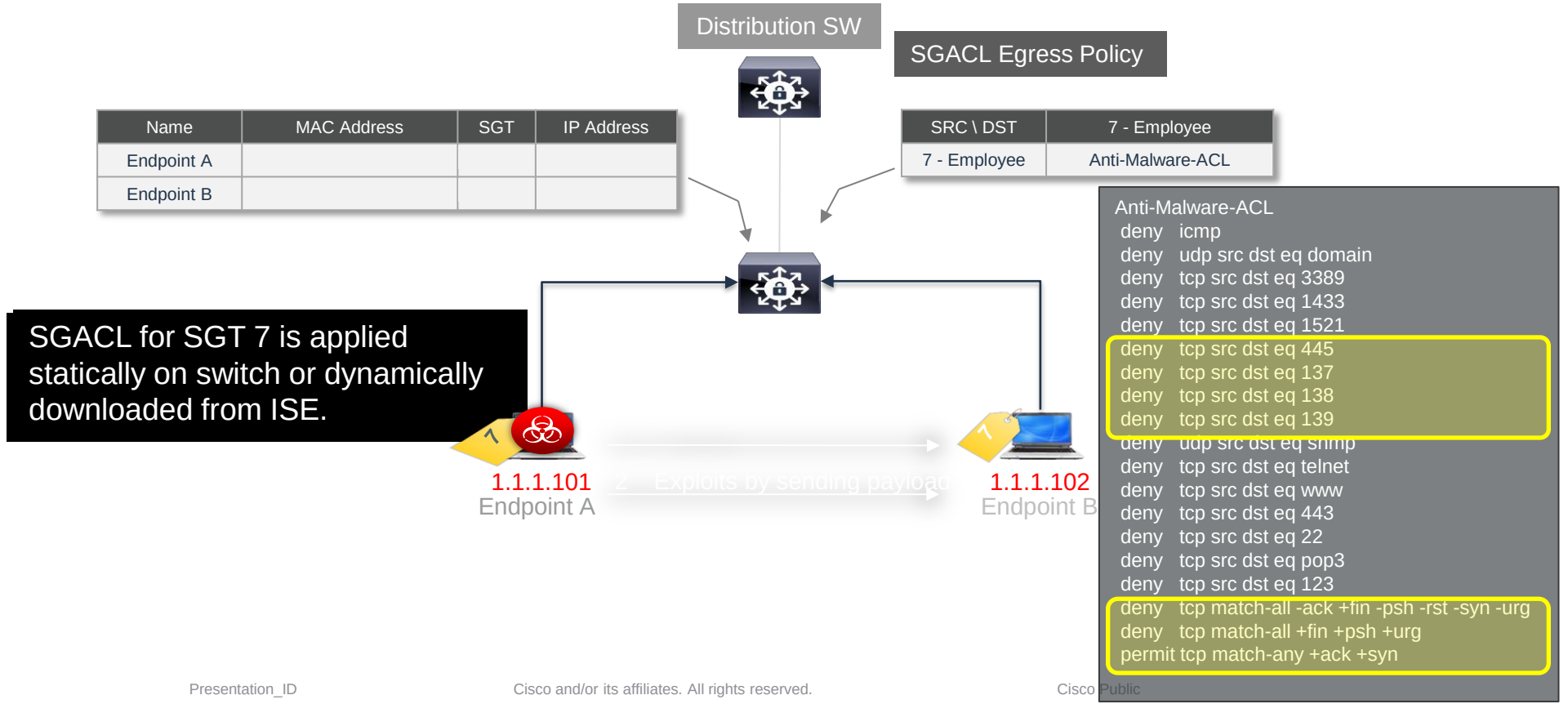
Segmentation between users/resources in campus

- User traffic SGTagged at access via 802.1X, MAB, or Web Authentication
- Resource SGTagged via 802.1X, MAB, or static mapping
- SGACL enforcement at egress access switch

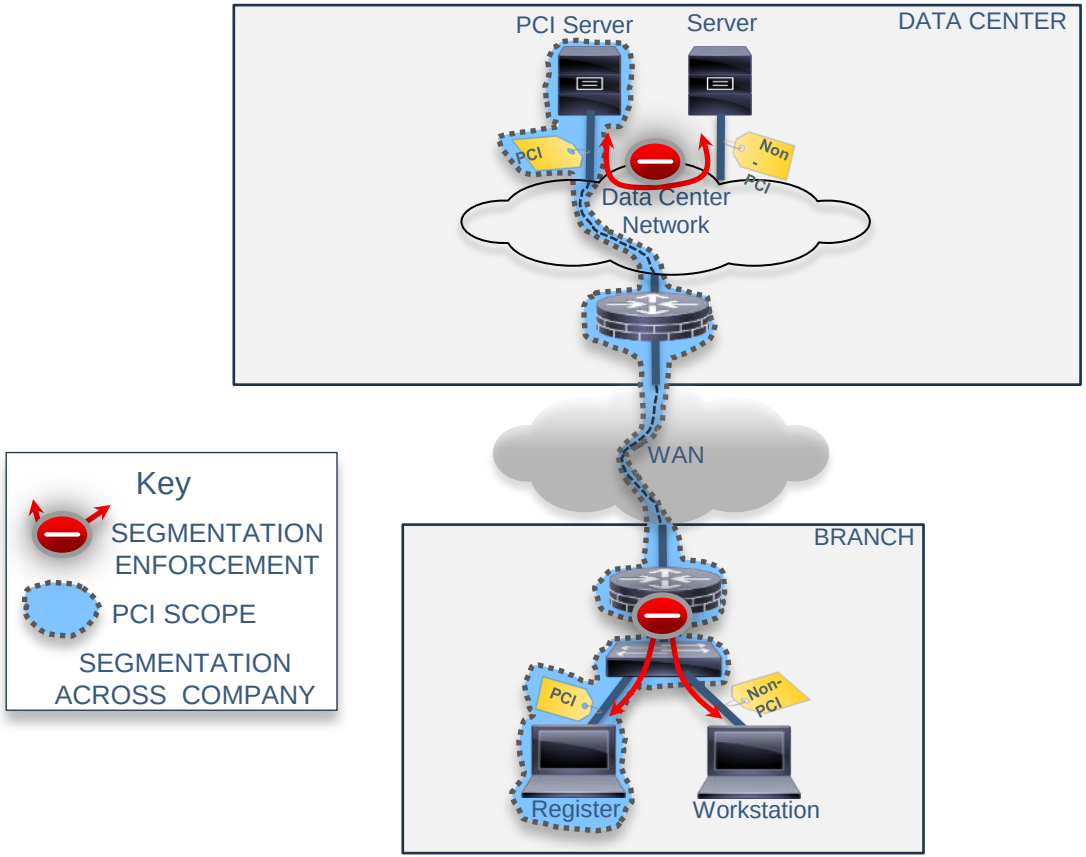
SRC \ DST	User A (10)	User B (20)	Guest (30)
User A (10)	Permit all	Deny all	Deny all
User B (20)	Deny all	Permit all	Deny all
Guest (30)	Deny all	Deny all	Permit all



SGT Malware Recon/Propagation – Security Overlay



PCI Compliance

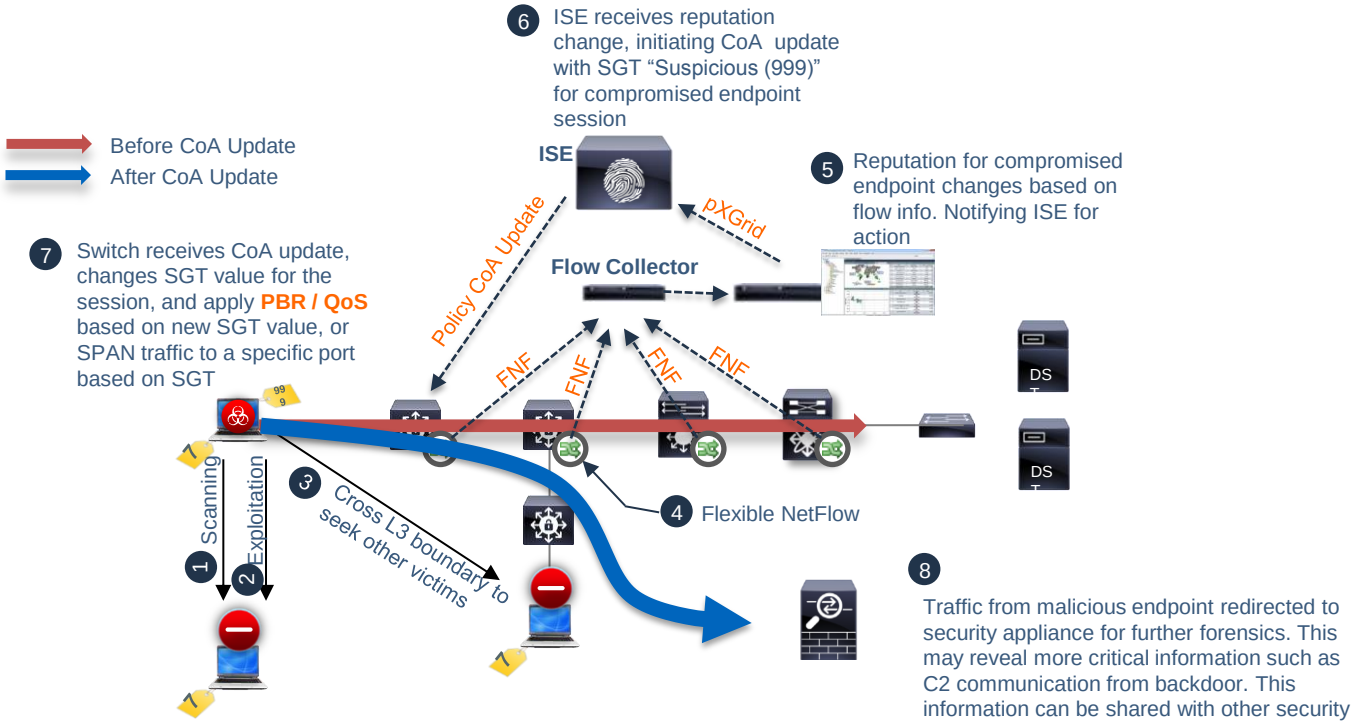


PCI Compliance

Verizon Opinion and Recommendations

Based on the results of the PCI validation and PCI Internal Network Penetration and Segmentation Test, it is Verizon's opinion that Cisco TrustSec can successfully perform network segmentation, for purposes of PCI scope reduction. In order to ensure effective enforcement across the environment in which TrustSec is deployed, it is important to note that proper configuration of the supporting infrastructure and TrustSec policies is essential.

Concept Use Case:
Reputation-based Threat Detection / Mitigation

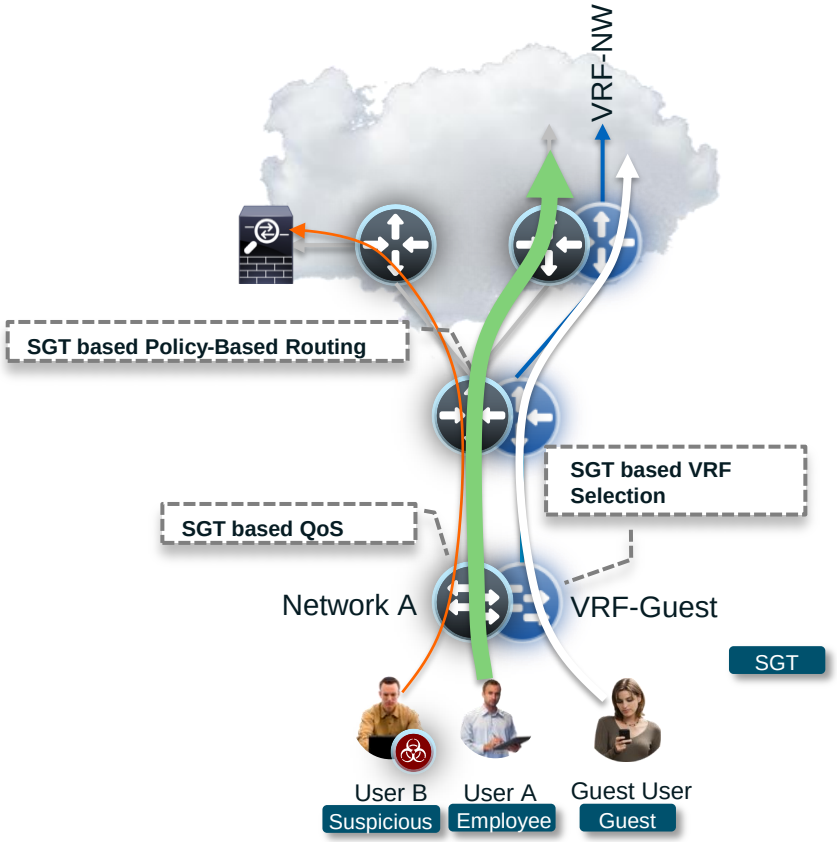


Security Group based Service Insertion

How can I provision QoS rules dynamically based on user type, device type, location, or any other context?

I would like to redirect traffic from malware infected host to other route, so that I can contain threat & analyze packet as well as log

Is there any easy way to segment traffic to different VRFs based on context ?



TrustSec: Taking Complexity out of Network Security

Simplified Access Management

- Manages policies using plain language
- Control access to critical assets by business role
- Maintain policy compliance

Accelerated Security Operations

- Quickly onboard servers
- Speed-up adds, moves and changes, eliminate many
- Automate FW & ACL administration

Consistent Policy Anywhere

- Segments networks using central policy management
- Enforces policy on wired, wireless & VPN
- Scales to remote, branch, campus & data center

```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255
gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt
3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt
1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt
2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq
1479
```

Traditional Security Policy

Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

Summary

- SGTs builds upon Secure Access and TrustSec services
- SGTs provides a scalable Identity and TrustSec access control model
- SGTs has new, advanced features to handle many use cases
- SGTs has migration strategies allow organizations to deploy with existing hardware
- TrustSec and SGTs are deployable **today**

“When building out your security strategy consider solutions with a strong architectural component.”

Some Final Thoughts…

“Build security strategies with the “big picture” in mind. Layers that build and integrate with each other provides an overall stronger defense.”

Support Matrix for IOS Switches

Platforms	Model	Version	802.1X/Identity Features	TrustSec (Security Group Access)				Device Sensors	MACSec	
				SGT Classification	SGT Transport		SGT Enforcement		Switch to Switch	Client to Switch
					Control Plane	Data Plane				
Catalyst 2000	Cat2960	15.0(2)SE	✓	-	-	-	-	-	-	-
	Cat2960-X, Cat2960-S, Cat2960-SF, Cat2960-C	15.0(2)SE	✓	✓	SXPv2(S)	-	-	-	-	-
Catalyst 3000	Cat3560, Cat3560-E, Cat3750, Cat3750-E	15.0(2)SE	✓	✓	SXPv2(S)	-	-	✓	-	-
	Cat3560-X, Cat3750-X	15.0(2)SE	✓	✓	SXPv2(S,L)	SGT	SGACL	✓	✓	✓
	Cat3560-C	15.0(2)SE	✓	✓	SXPv2(S,L)	-	-	✓	✓	✓
	Cat3650, Cat3850	XE 3.3.0SE	✓	✓	SXPv2(S,L)	SGT	SGACL	CY14	CY14	CY14
Cat4000	Sup6E, Sup6E-L	15.0(2)SG	✓	✓	SXPv2(S)	-	-	✓	-	-
	Sup7E, Sup7E-L	IOS XE 3.3.0SG	✓	✓	SXPv2(S)	SGT	SGACL	✓	✓	✓
	Sup8E	IOS XE 3.3.0SG	✓	✓	SXPv2(S)	SGT	SGACL	✓	✓	✓
Cat6000	Sup32/Sup720	15.1(1)SY	✓	✓	SXPv4(S,L)	-	-	-	-	-
	Sup2T	15.1(1)SY	✓	✓	SXPv4(S,L)	SGT	SGACL	-	✓	-

Support Matrix for NXOS, ASA, and WLC

Platforms	Model	Version	802.1X/Identity Features	TrustSec (Security Group Access)				Device Sensors	MACSec	
				SGT Classification	SGT Transport		SGT Enforcement		Switch to Switch	Client to Switch
					Control Plane	Data Plane				
Nexus 7000	Sup1&2	6.1(1)	-	✓	SXPv1 (S,L)	SGT	SGACL	-	✓	-
Nexus 5000	N5548P, N5548P and N5596UP. No support for N5010 or N5020	5.1(3)N1(1)	-	✓ ✓	SXPv1 (S)	SGT	SGACL	-	-	-
Nexus 1000v		4.2(1)SV2(1.1)	-		SXPv1 (S)	-	-	-	-	-
ASA/ASASM	5505,5510,5520,5540,5550,5580,5585-X, ASA-SM, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X	9.0.1, ASDM7.0.1	✓	✓	SXPv2 (S,L)	-	SGFW	✓	-	-
WLC/WiSM2	WLC2500, WLC5500, WiSM2, SRE	7.4			SXPv2 (S)	-	-		-	-


CISCO
TM