



*TOMORROW  
starts here.*

Cisco *live!*



# Deploying Security Group Tags

BRKSEC-2690

Kevin Regan

Product Manager, TrustSec Solution Team

#clmel

Cisco *live!*

# 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 centres 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 the TrustSec solution.





# Presentation Decode



Slide intended for your reference – may be very briefly covered



Identity Services Engine (ISE, pronounced 'ice')



User authenticated by 802.1X, MAC auth-bypass or Web Auth (Flexible Auth)



Circle Line, London Underground Railway (aka The Tube)

SGT

Security Group Tag (Cisco), Source Group Tag (IETF) or Stiff Gin & Tonic (later)

# Agenda

- Introduction
- Deployment Drivers & Goals
- Essential TrustSec Functions to Understand
- Deploying our Three Main Use-Cases
- Examples
- Where to get more information
- Questions



# Introduction

- Functions of the Tower of London
- Protects the Crown Jewels
  - Secure facility
  - Paying visitors get limited access to view some of them

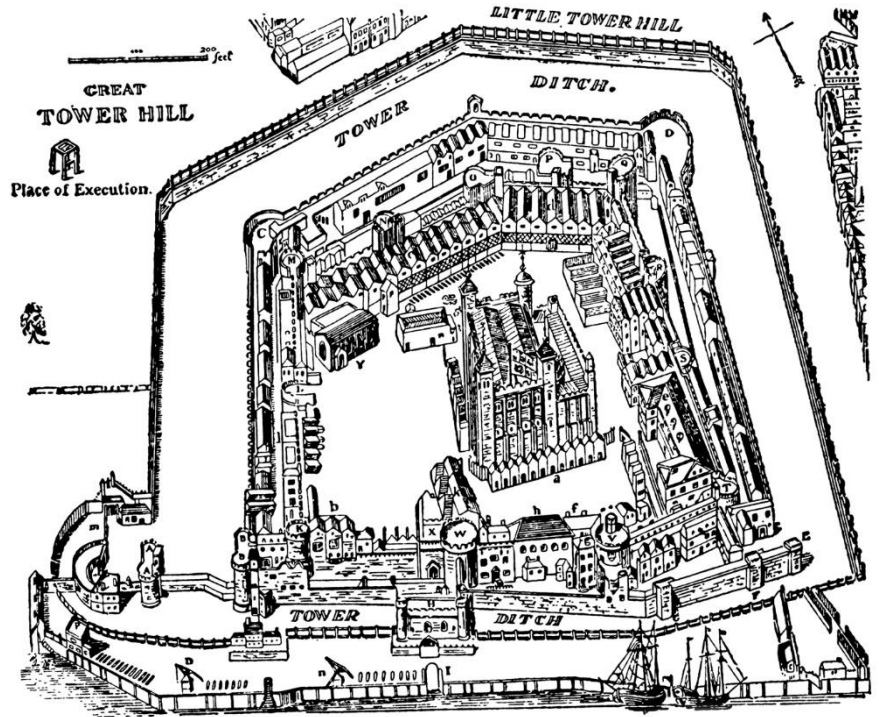


Tower of London



# Introduction

- Functions of the Tower of London
  - Protects the Crown Jewels
    - Secure facility
    - Paying visitors get limited access to view some of them
- Prison (until 1950s)
  - Multiple concentric walls segregating zones
  - Users (prisoners) segregated from each other in cells and blocks



Tower of London



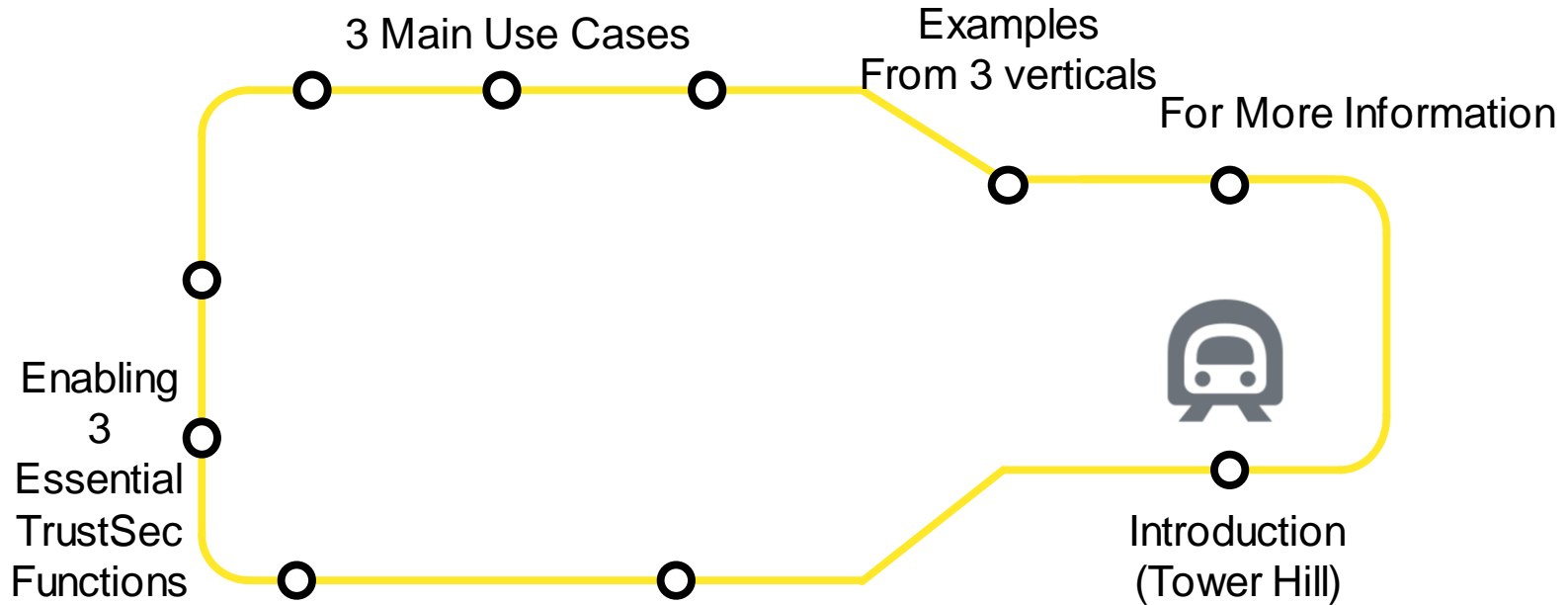
# Introduction - TrustSec

- Two main mechanisms we use TrustSec for:-
- Access Control
  - Controlling access to the Crown Jewels (ticket 'attribute' needed)
  - Crown Jewels could be:
    - Credit card data
    - Intellectual property
- Segmentation
  - Restricted communication between zones
  - Users could be dynamically segmented by their role



Tower of London

# Agenda



# Agenda

3 Main Use Cases

Examples

For More Information

Policy Enforcement

Propagating SGTs



Classification  
(Assigning SGTs)

Deployment Drivers and Goals

Introduction  
(Tower Hill)



# Typical Goals for TrustSec Deployments



**Mitigate Risk**

**Reducing attack surface  
with segmentation**



**Increase SecOps  
efficiency**

**Manage security using  
logical groups not IP  
addresses/VLANs**

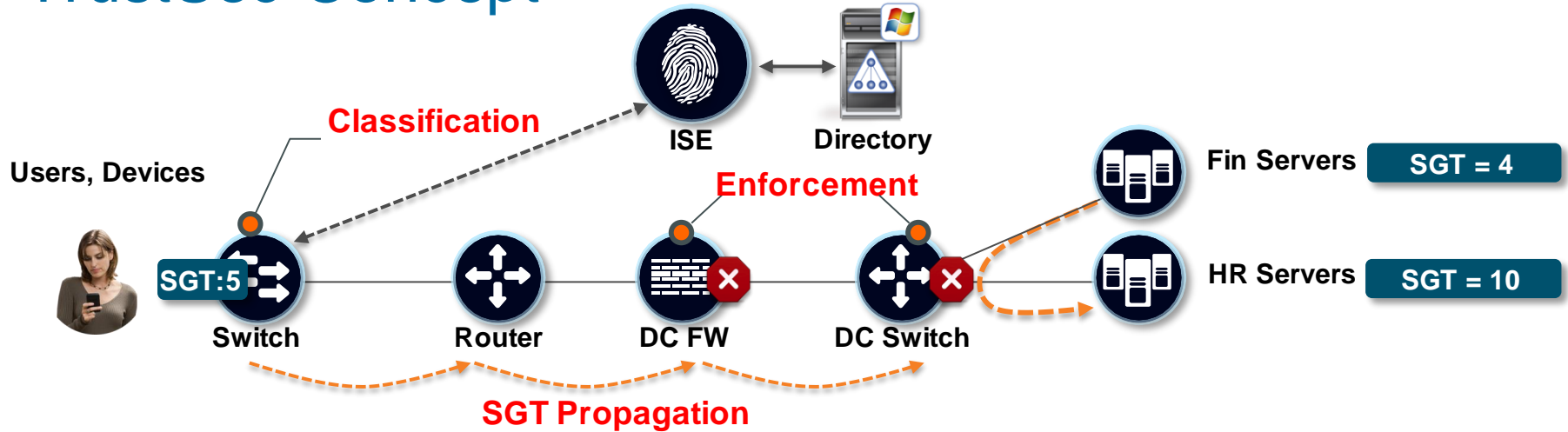


**Meet Compliance  
Objectives**

**Authorise access to  
compliance-critical  
apps**



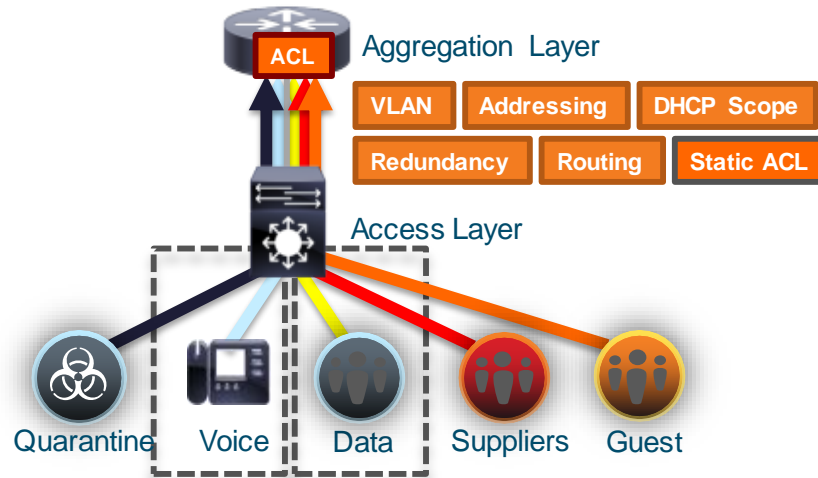
# TrustSec Concept



- Classification of systems/users based on **context** (user role, device, location, access method)
- Context (role) expressed as Security Group Tag (SGT)
- Firewalls, routers and switches use SGT to make filtering decisions
- Classify once – reuse result multiple times

# Traditional Segmentation

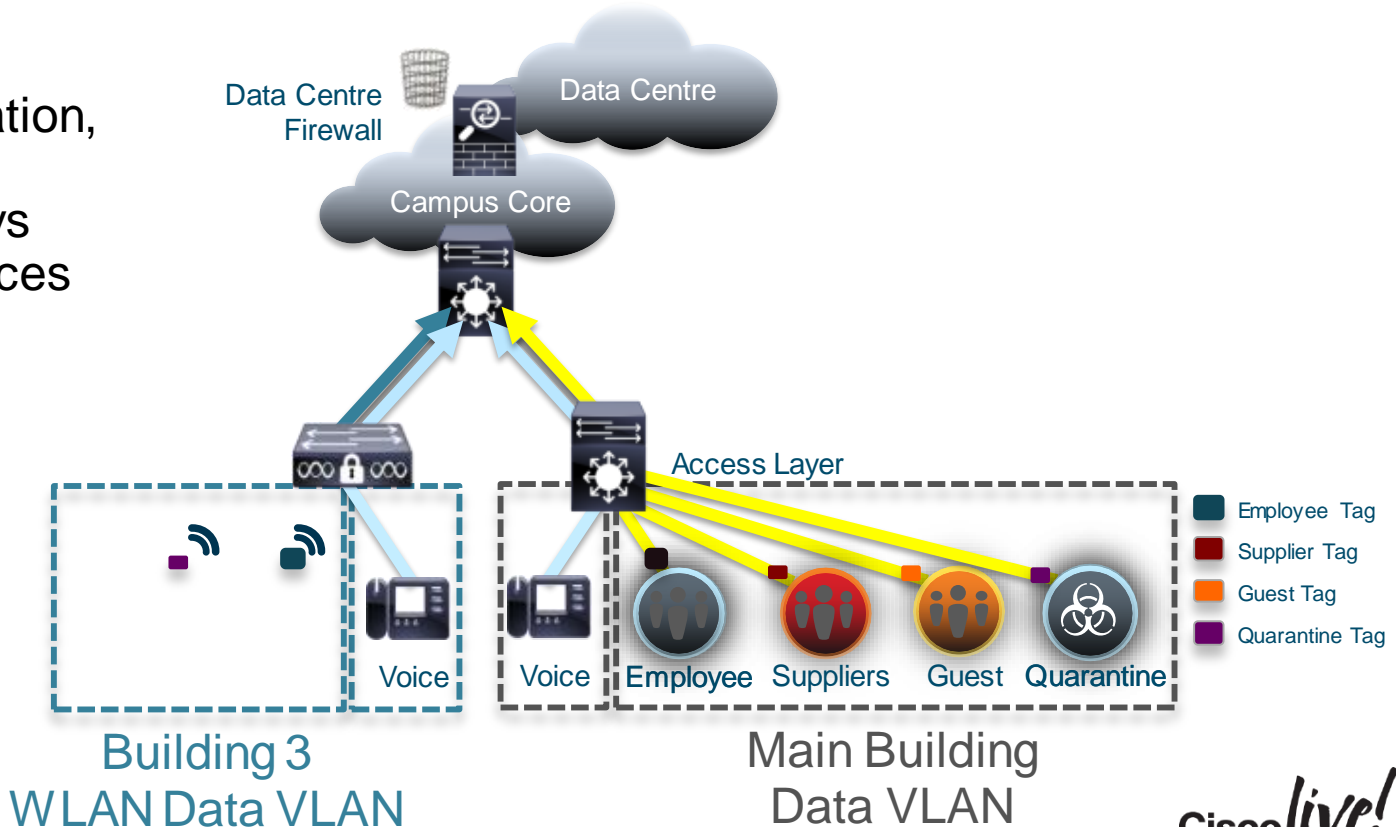
Steps replicated across floors, buildings and sites



Simple Segmentation with 2 VLANs

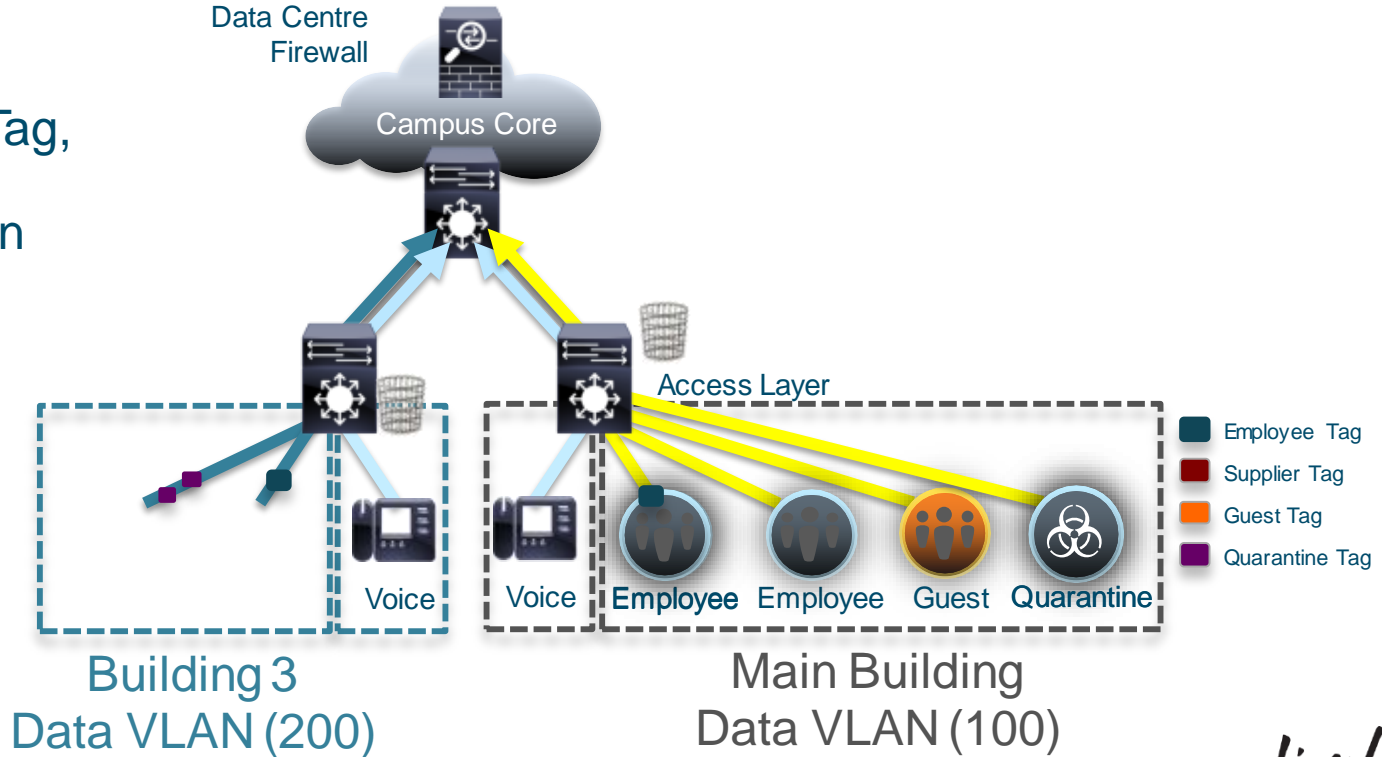
# User to Data Centre Access Control with TrustSec

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



# Campus Segmentation with TrustSec

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

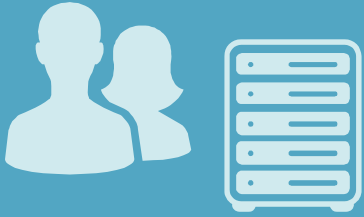




# Simplicity of Group-Based Policies

- Managing security rules by groups instead of individual identifiers can mean:
  - Fewer rules/access control entries
  - Easier to understand and audit policies
  - New assets can join a group without changing the policy
- Automating assignment of group membership – avoids rule provisioning effort/lag
  - Less SecOps effort
  - Avoids time required for manual provisions of new apps/services
- If group membership can be independent of the network topology
  - Can apply group-based policies anywhere on the network
  - Avoids/reduces need for device-specific ACL configurations

# TrustSec Common Deployment Scenarios



## User to Data Centre Access Control

- Context-based access
- Compliance requirements PCI, HIPAA, export controlled information
- Merger & acquisition integration, divestments



## Data Centre Segmentation

- Zoning & Micro-segmentation
- Production vs Development Server segmentation
- Compliance requirements, PCI, HIPAA
- Firewall rule automation



## Campus and Branch Segmentation

- Line of business segregation
- PCI, HIPAA and other compliance regulations
- Malware propagation control/quarantine

# Agenda

## 3 Main Use Cases

Policy Enforcement

SGT Propagation



Classification  
(Assigning  
SGTs)

Deployment  
Drivers and  
Goals

Examples

For More Information

Introduction

# Classification = Assignment of Security Groups

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, a secondary navigation bar contains 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'TrustSec', and 'Policy Elements'. The 'Policy Elements' section is active, with sub-tabs for 'Dictionaries', 'Conditions', and 'Results'. The 'Results' tab is selected, displaying a search bar and a tree view on the left. The tree view shows a hierarchy of folders: Authentication, Authorization, Profiling, Posture, Client Provisioning, and TrustSec. Under TrustSec, there are folders for Security Group ACLs, Security Groups (which is highlighted), and Security Group Mappings. The main content area is titled 'Security Groups' and includes a breadcrumb trail: 'Administration > System > Backup & Restore > Policy Export Page'. Below the breadcrumb, there are action buttons: Edit, Add, Import, Export, Delete, and Push. A table lists the security groups with columns for Name, SGT (Dec / Hex), and Description.

	Name	SGT (Dec / Hex)	Description
<input type="checkbox"/>	Developers	4/0004	
<input type="checkbox"/>	Development_Servers	101/0065	
<input type="checkbox"/>	Engineering	3/0003	
<input type="checkbox"/>	Production_Servers	103/0067	
<input type="checkbox"/>	Production_Users	5/0005	
<input type="checkbox"/>	TrustSec_Devices	2/0002	Assigned to all TrustSec network devices
<input type="checkbox"/>	Unknown	0/0000	Unknown Security Group



# Assigning Security Groups

## Dynamic Classification



802.1X Authentication



Web Authentication



MAC Auth Bypass

Common Classification for  
Mobile Devices

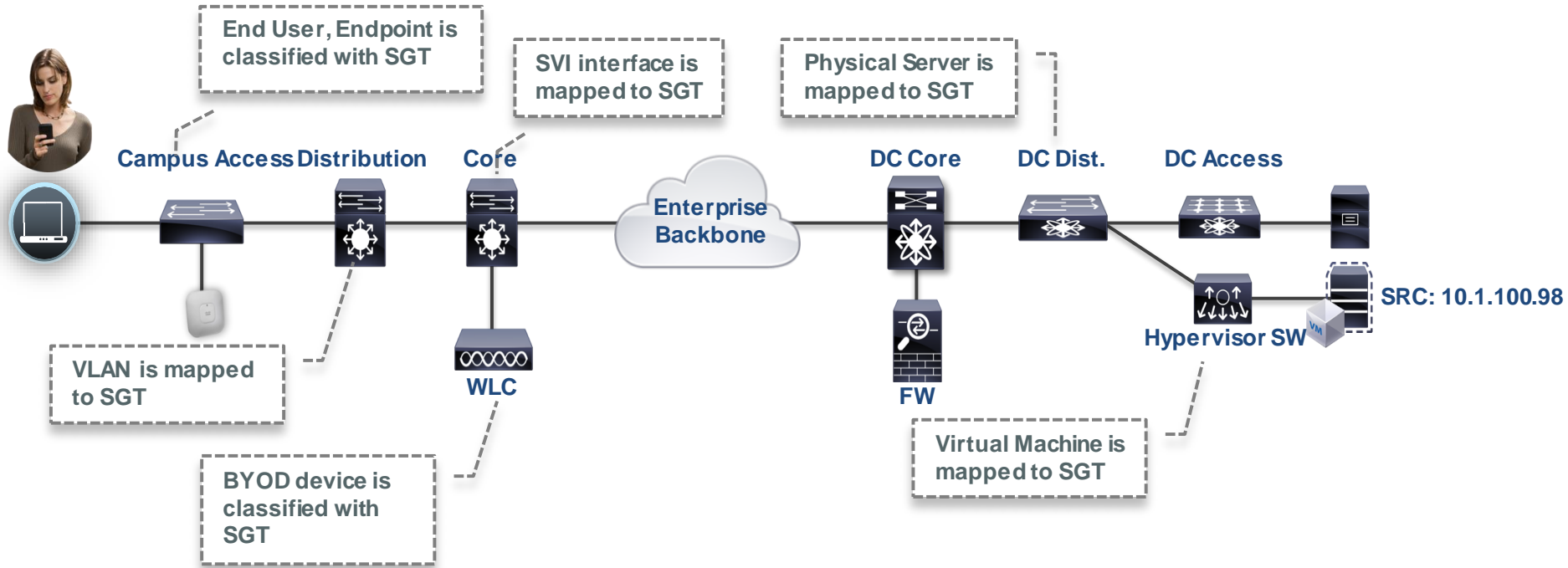
## Static Classification

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



Classification for Servers,  
Topology-based assignments.

# How Security Group Tags are Assigned



# Dynamic SGT Assignments in Authorisation Rules

**Authorization Policy**  
Define the Authorization Policy by configuring rules based on...  
For Policy Export go to [Administration > System > Backup & Restore](#)

First Matched Rule Applies

**Exceptions (0)**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Developers	if Any and AD:ExternalGroups EQUALS cts.io...	then Engineer...
✓	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then t
✓	Default	if no matches, then	DenyAccess

**Security Group**

- Developers
- Development\_Servers
- Engineering
- Production\_Servers
- Production\_Users
- TrustSec\_Devices
- Unknown

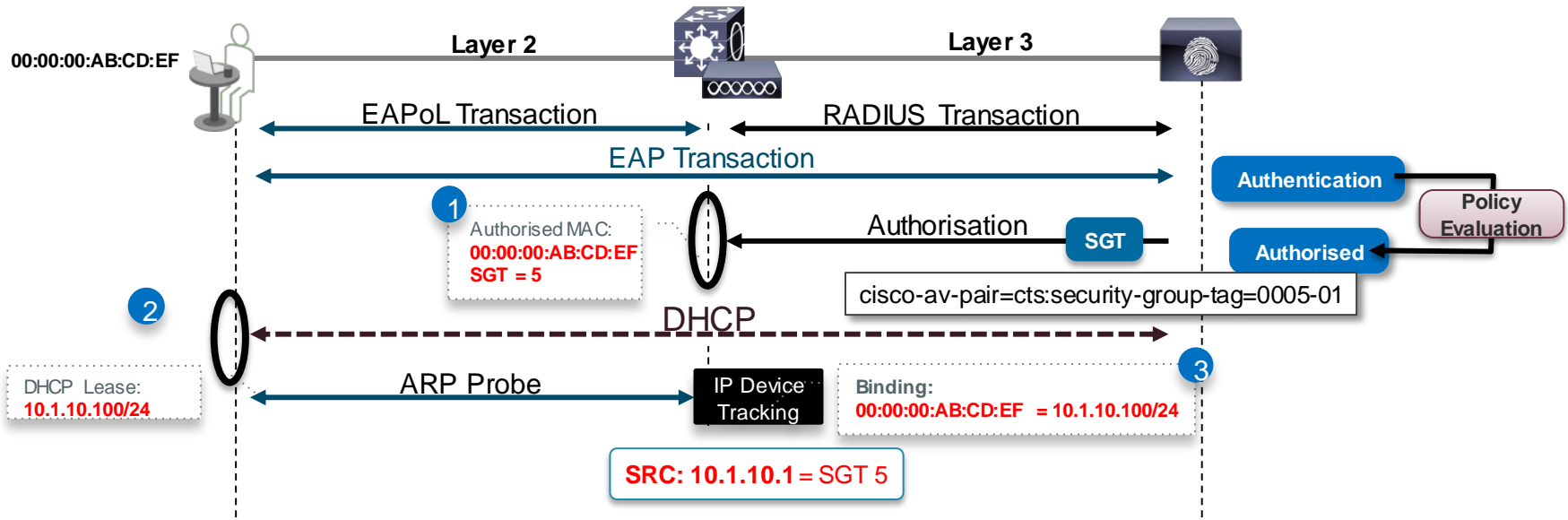
**Permissions**

Developers and PermitAccess

**Navigation Path:**

- Policy > Authorisation > Permissions > Security Groups
- Requires basic authorisation profile (Access Accept, Access Reject)

# Dynamic SGT Assignment 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

# Static SGT Assignments



## IOS CLI Example

### IP to SGT mapping

```
cts role-based sgt-map A.B.C.D sgt SGT_Value
```

### VLAN to SGT mapping\*

```
cts role-based sgt-map vlan-list VLAN sgt SGT_Value
```

### Subnet to SGT mapping

```
cts role-based sgt-map A.B.C.D/nn sgt SGT_Value
```

### L2IF to SGT mapping\*

```
(config-if-cts-manual)#policy static sgt SGT_Value
```

### L3IF to SGT mapping\*\*

```
cts role-based sgt-map interface name sgt SGT_Value
```

### L3 ID to Port Mapping\*\*

```
(config-if-cts-manual)#policy dynamic identity name
```

\* relies on IP Device Tracking

\*\* relies on route prefix snooping



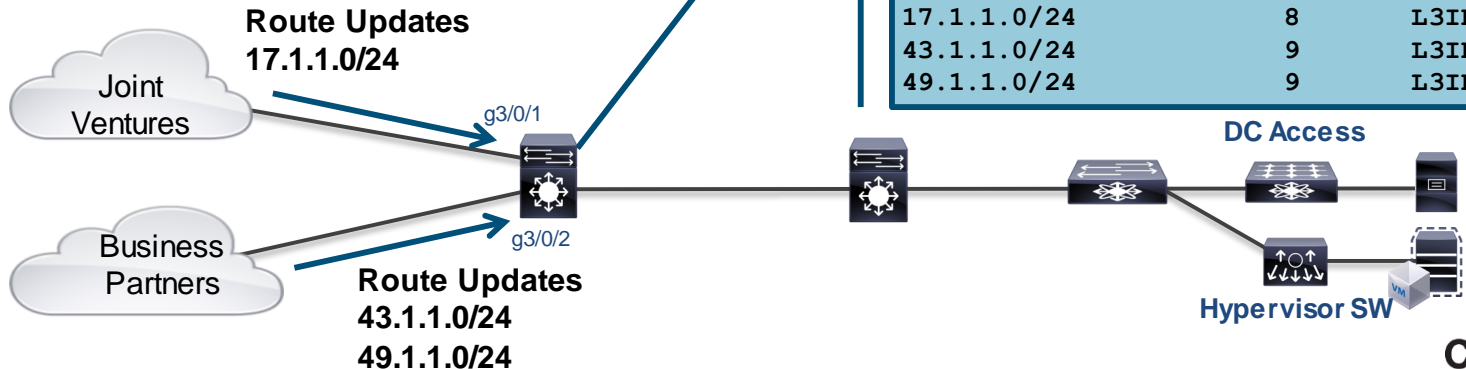


# L3 Interface to SGT Mappings

- Route Prefix Monitoring on a specific Layer 3 Port mapping to a SGT
- Can apply to Layer 3 interfaces regardless of the underlying physical interface:
  - Routed port, SVI (VLAN interface) , Tunnel interface

cts role-based sgt-map interface *GigabitEthernet 3/0/1* sgt 8

cts role-based sgt-map interface *GigabitEthernet 3/0/2* sgt 9



```
VSS-1#show cts role-based sgt-map all
Active IP-SGT Bindings Information
IP Address          SGT      Source
=====
11.1.1.2            2        INTERNAL
12.1.1.2            2        INTERNAL
13.1.1.2            2        INTERNAL
17.1.1.0/24        8        L3IF
43.1.1.0/24        9        L3IF
49.1.1.0/24        9        L3IF
```

# Access Layer Classification Summary



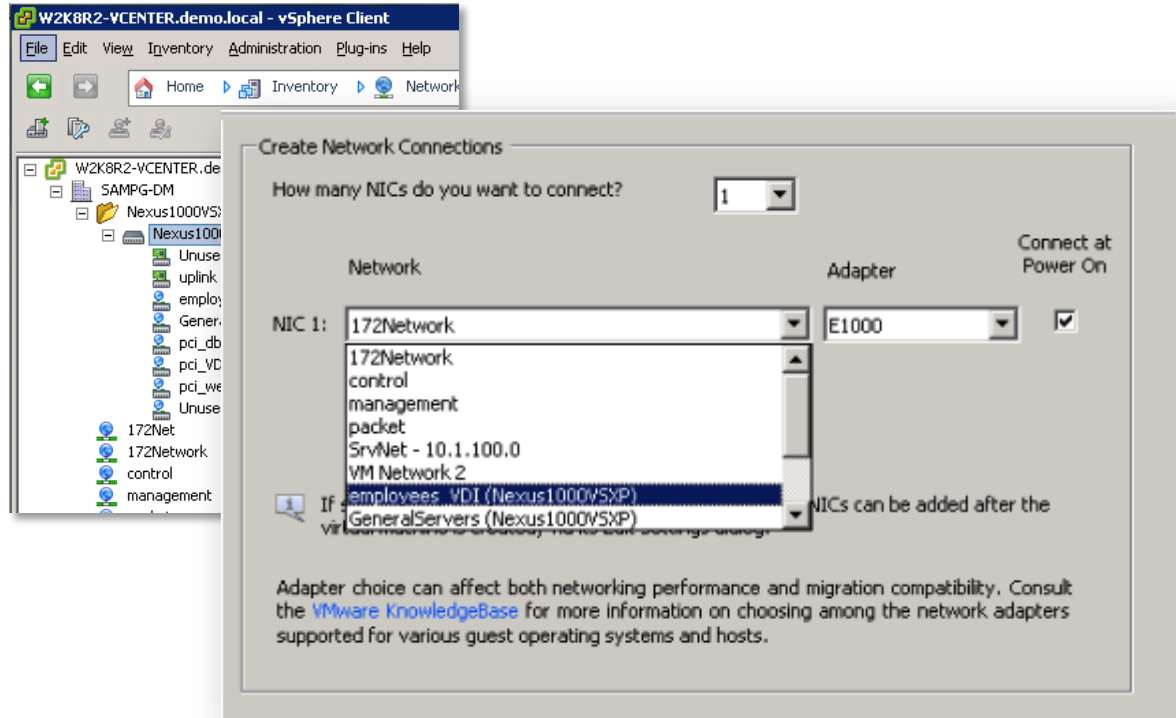
		C2960-S	C3750X	**C3850/W LC 5760	C4500	C6x00	ISR/ASR100 0	WLC
<b>Dynamic</b>	<b>802.1X</b>	X	X	X	X	X	X	X
	<b>MAB</b>	X	X	X	X	X	X	X
	<b>Web Auth</b>	X	X	X	X	X	X	X
<b>Static</b>	<b>VLAN/SGT</b>	-	X*	X	X	X*	-	-
	<b>Subnet/SGT</b>	-	-	X	X	X	X	-
	<b>Layer 3 Interface Mapping</b>	-	-	-	-	X	X	-

\*\* limits on number of SGTs (255) \* - limits on the number of VLANs

Cisco *live!*

# Nexus 1000V: SGT Assignment in Port Profile

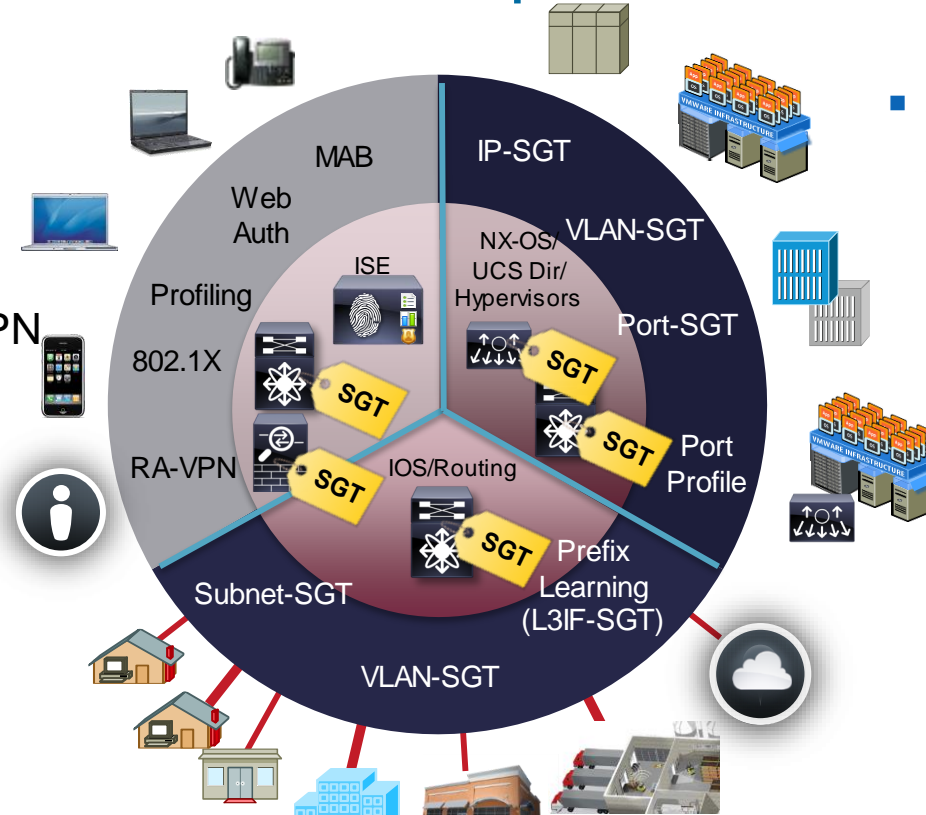
- Port Profile
  - Container of network properties
  - Applied to different interfaces
- Server Admin may assign Port Profiles to new VMs
- VMs inherit network properties of the port-profile including SGT
- SGT stays with the VM even if moved



# Summary of Classification Options

- User/Device SGT assignments

- Wired
- Wireless
- Remote Access VPN



- Data Centre Server Assignments

- Business Partners & 3<sup>rd</sup> party connections

# Agenda

## 3 Main Use Cases

Policy Enforcement

SGT Propagation



Classification  
(Assigning  
SGTs)

Deployment  
Drivers and  
Goals

Examples

For More Information

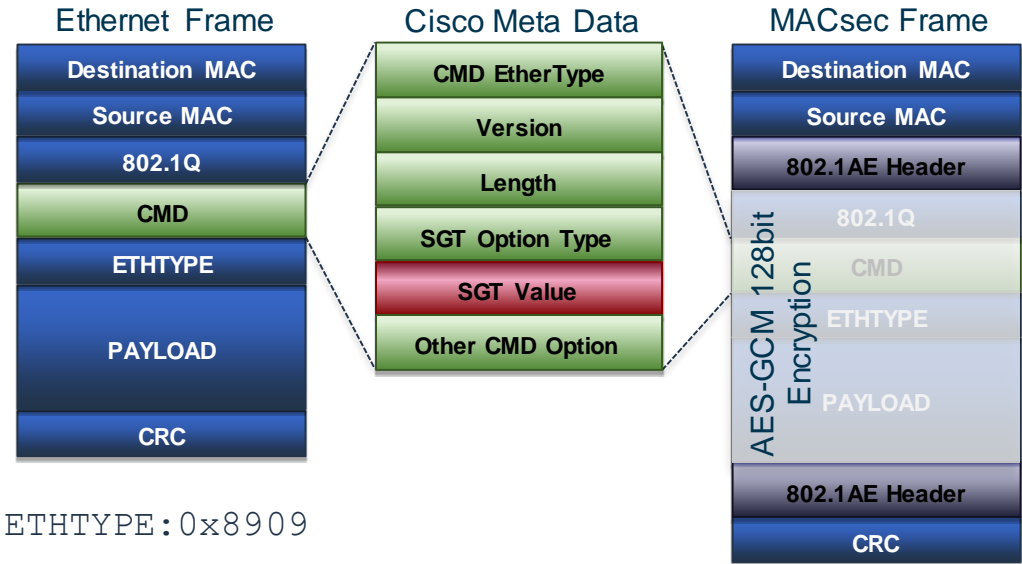
Introduction



# Inline Tagging (SGT in data plane)



- SGT embedded within Cisco Meta Data (CMD) in Layer 2 frame
- Capable switches process SGT at line-rate
- Optional MACsec protection
- No impact to QoS, IP MTU/Fragmentation
- L2 Frame Impact: ~40 bytes
- Recommend L2 MTU~1600 bytes
- N.B. Assume incapable devices will drop frames with unknown Ethertype



ETHTYPE: 0x8909

ETHTYPE: 0x88E5

# Configuring Inline Tagging



'cts manual' config for inline tagging generally used

'cts dot1x' alternative depends on AAA reachability - unless new 'critical auth' feature used & timers set carefully

```
interface TenGigabitEthernet1/5
  cts manual
  policy static sgt 2 trusted
```

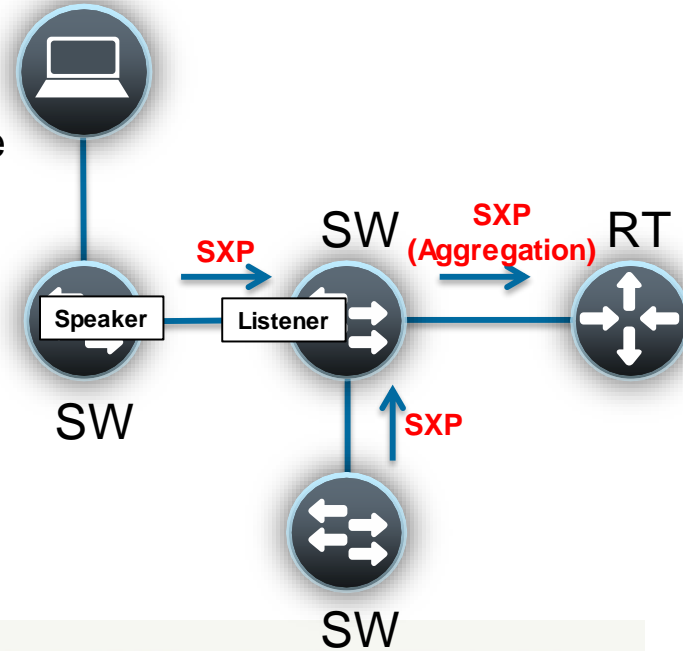
Always "shut" and "no shut" interfaces after any cts manual or cts dot1x change

```
C6K2T-CORE-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.
```

# SGT eXchange Protocol (SGT in Control Plane)

- SXP very simple to enable
  - SGT propagation without hardware dependencies
  - Propagation poss from access edge to enforcement device
- Uses TCP for transport protocol
- TCP port 64999 for connection initiation
- Use MD5 for authentication and integrity check
- Two roles: Speaker (initiator) and Listener (receiver)



```
Nexus1000VSXP# sh cts sxp conn
PEER_IP_ADDR      VRF          PEER_SXP_MODE  SELF_SXP_MODE  CONNECTION STATE
10.1.2.1          management   listener        speaker        connected
```



# IOS SXP Configuration

3750

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

6K

```
cts sxp enable
cts sxp default password cisco123
!
cts sxp connection peer 10.10.11.1 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
```

```
C3750#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	8:EMPLOYEE_FULL	LOCAL

```
C6K2T-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
```

```
C6K2T-CORE-1#show cts role-based sgt-map all details
Active IP-SGT Bindings Information
```

IP Address	Security Group	Source
10.1.40.10	5:PCI_Servers	CLI
10.1.44.1	2:Device_sgt	INTERNAL
---	snip ---	
10.0.200.203	3:GUEST	SXP
10.10.11.100	8:EMPLOYEE_FULL	SXP

# WLC SXP Configuration



**CISCO**    [MONITOR](#)    [WLANs](#)    [CONTROLLER](#)    [WIRELESS](#)    **SECURITY**

### Security

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec SXP**
- Advanced

### SXP Configuration

Total SXP Connections: 1

SXP State:

SXP Mode: Speaker

Default Password:

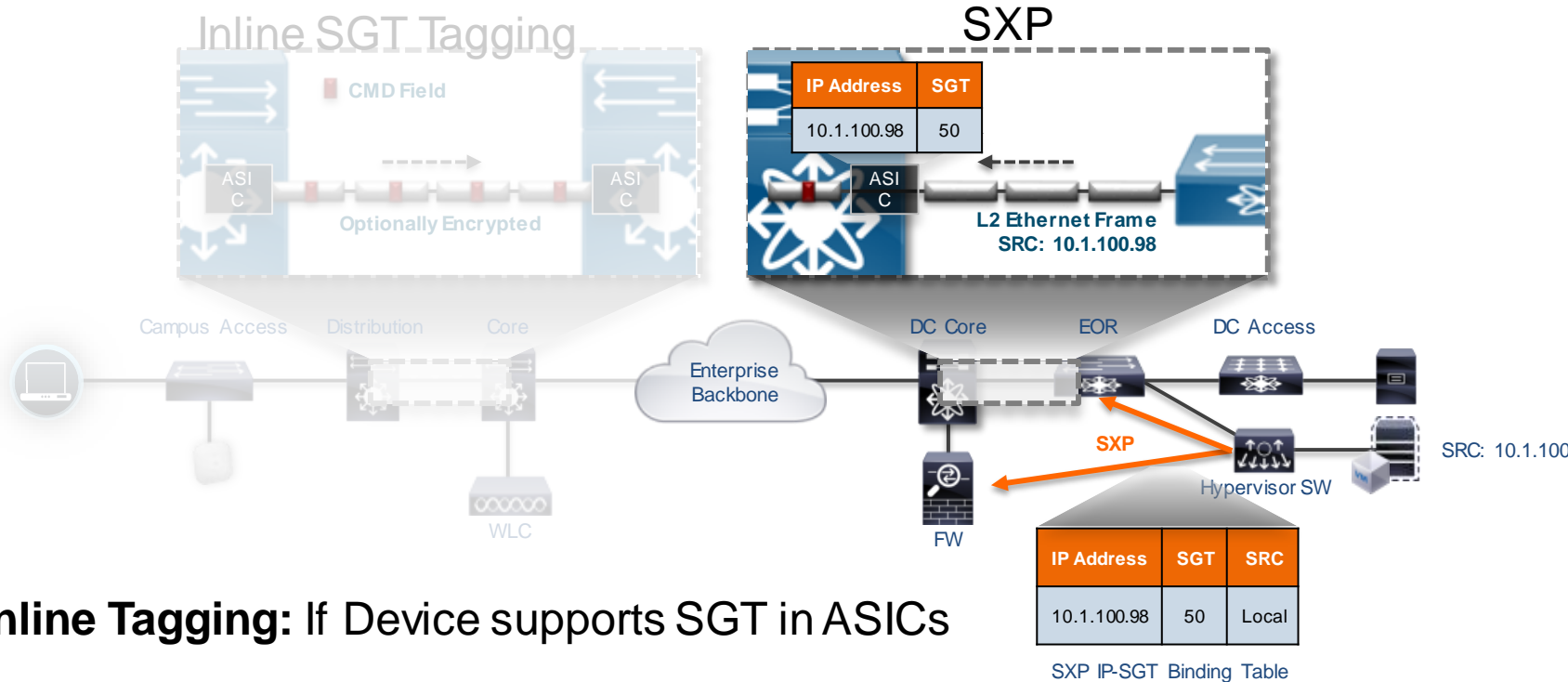
Default Source IP: 10.1.44.44

Retry Period:

Peer IP Address	Source IP Address	Connection Status
10.1.44.1	10.1.44.44	On <input type="checkbox"/>



# Inline Tagging vs. SXP Tag Propagation



- **Inline Tagging:** If Device supports SGT in ASICs
- **SXP:** Where devices are not SGT-capable



# For More Info on SGT Propagation

- 'Source-Group Tag eXchange Protocol' IETF Informational Draft  
<https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/>

Source-Group Tag eXchange Protocol (SXP)  
draft-smith-kandula-sxp-01

## Abstract

This document discusses source-group tag exchange protocol (SXP), a control protocol to propagate IP address to Source Group Tag (SGT) binding information across network devices.

## Appendix A. SGT Ethernet Frame Format

The Source Group Tag can be carried in the control plane (using SXP described in the main body of this I-D), or in the data plane. Appendix A describes Cisco Metadata (CMD) Version 1, the format for carrying SGT in the data plane at L2. The SGT is processed hop-by-hop.

- Further alignment with other metadata carrying formats like the Network Services Header (NSH)
  - Allows SGT(s) to be mapped to Source Class and Destination Class (if available)
  - <https://tools.ietf.org/html/draft-guichard-sfc-nsh-dc-allocation-01>

# TrustSec Functions and Platform Support

## Classification

	Catalyst 2960-S/-C/-Plus/-X/-XR
	Catalyst 3560-E/-C/-X
	Catalyst 3750-E/-X
	Catalyst 3850/3650 WLC 5760
	Catalyst 4500E (Sup6E/7E)
	Catalyst 4500E (Sup8)
	Catalyst 6500E (Sup720/2T)
	Wireless LAN Controller 2500/5500/WiSM2
	Nexus 7000
	<b>Nexus 6000</b> <span>NEW</span>
	<b>Nexus 5600</b> <span>NEW</span>
	Nexus 5500
	Nexus 1000v (Port Profile)
	ISR G2 Router, CGR2000
	<b>IE2000/3000, CGS2000</b> <span>NEW</span>
	<b>ASA5500 (VPN RAS)</b> <span>NEW</span>

## Propagation

	Catalyst 2960-S/-C/-Plus/-X/-XR		
	Catalyst 3560-E/-C/-, 3750-E		
		Catalyst 3560-X, 3750-X	
		Catalyst 3850/3650	
	Catalyst 4500E (Sup6E)		
		Catalyst 4500E (7E, 8), 4500X	
	Catalyst 6500E (Sup720)		
		Catalyst 6500E (2T), 6800	
	WLC 2500, 5500, WiSM2		
		WLC 5760	
		<b>Nexus 1000v</b> <span>NEW inline tagging</span>	
		<b>Nexus 6000/5600</b> <span>NEW</span>	
		Nexus 5500/22xx FEX	
		Nexus 7000/22xx FEX	
			ISR G2, CGS2000
			ASR1000
		ASA5500 Firewall, ASASM	

• Inline SGT on all ISR G2 except 800 series:

## Enforcement

	Catalyst 3560-X
	Catalyst 3750-X
	Catalyst 3850/3650
	WLC 5760
	Catalyst 4500E (7E)
	Catalyst 4500E (8E)
	Catalyst 6500E (2T)
	Catalyst 6800
	Nexus 7000
	<b>Nexus 6000</b> <span>NEW</span>
	<b>Nexus 5600</b> <span>NEW</span>
	Nexus 5500
	<b>Nexus 1000v</b> <span>NEW</span>
	ISR G2 Router, CGR2000
	ASR 1000 Router
	CSR-1000v Router
	ASA 5500 Firewall
	ASAv Firewall <span>NEW</span>

[www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec\\_matrix.html](http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html)

# Agenda

## 3 Main Use Cases

Policy Enforcement



SGT Propagation

Classification  
(Assigning SGTs)

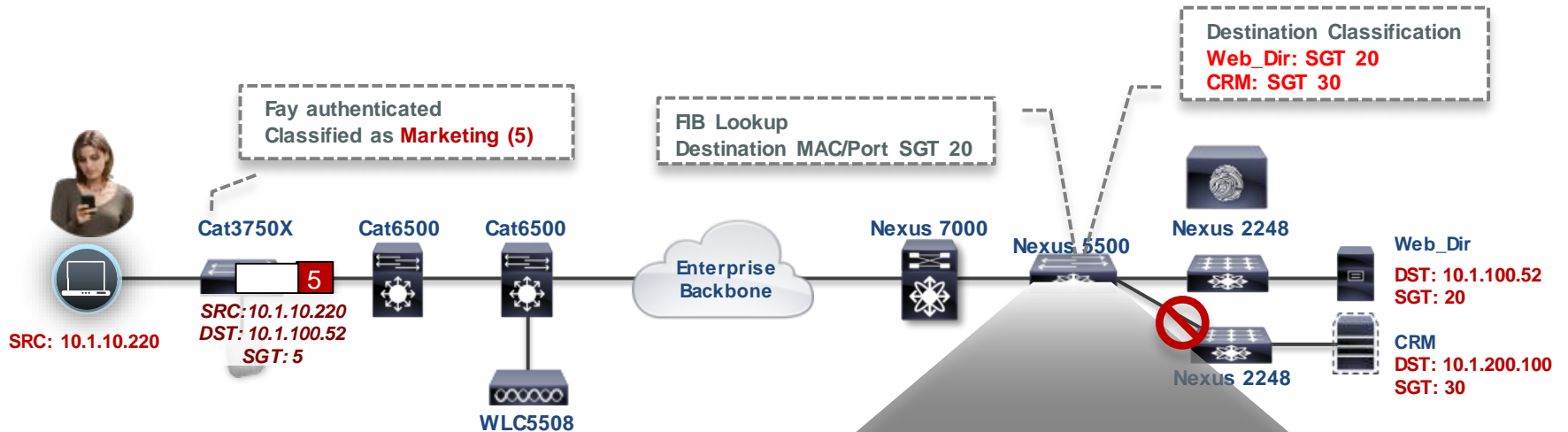
Deployment Drivers and Goals

Examples

For More Information

Introduction

# Policy Enforcement - Security Group ACL (SGACL)



SRC\DST	Web_Dir (20)	CRM (30)
Marketing (5)	<b>SGACL-A</b>	SGACL-B
BYOD (7)	Deny	Deny



# Centralised SGACL Management in ISE

Security Groups ACLs List > [Common\\_Services](#)

## Security Group ACLs

\* Name

Description

IP Version  IPv4  IPv6  Agnostic

\* Security Group ACL content

```
permit tcp dst eq 80
permit tcp dst eq 443
permit tcp dst eq 22
permit tcp dst eq 3389
permit tcp dst eq 135
permit tcp dst eq 136
permit tcp dst eq 137
permit tcp dst eq 138
permit tcp dst eq 139
deny ip
```

Security Groups ACLs List > [Web\\_SGACL](#)

## Security Group ACLs

\* Name

Description

IP Version  IPv4  IPv6  Agnostic

\* Security Group ACL content







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

# Applying SGACL Policies in ISE (Tree View)

Egress Policy Network Device Authorization

Source Tree Destination Tree Matrix

## Egress Policy (Source Tree View)

 Edit  Add  Clear Mapping  Configure  Push  Monitor All - Off

Source Security Group ▲

- ▶ Developers (4/0004)
- ▶ Development\_Servers (101/0065)
- ▶ Production\_Servers (103/0067)
- ▼ Production\_Users (5/0005)

Source Inner Table				
	Status	Destination Security Group	Security Group ACLs	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	Development_Servers	Deny IP	
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	Production_Servers	Web_SGACL	

# Applying SGACL Policies (Matrix View)

Source Tree    Destination Tree    **Matrix**

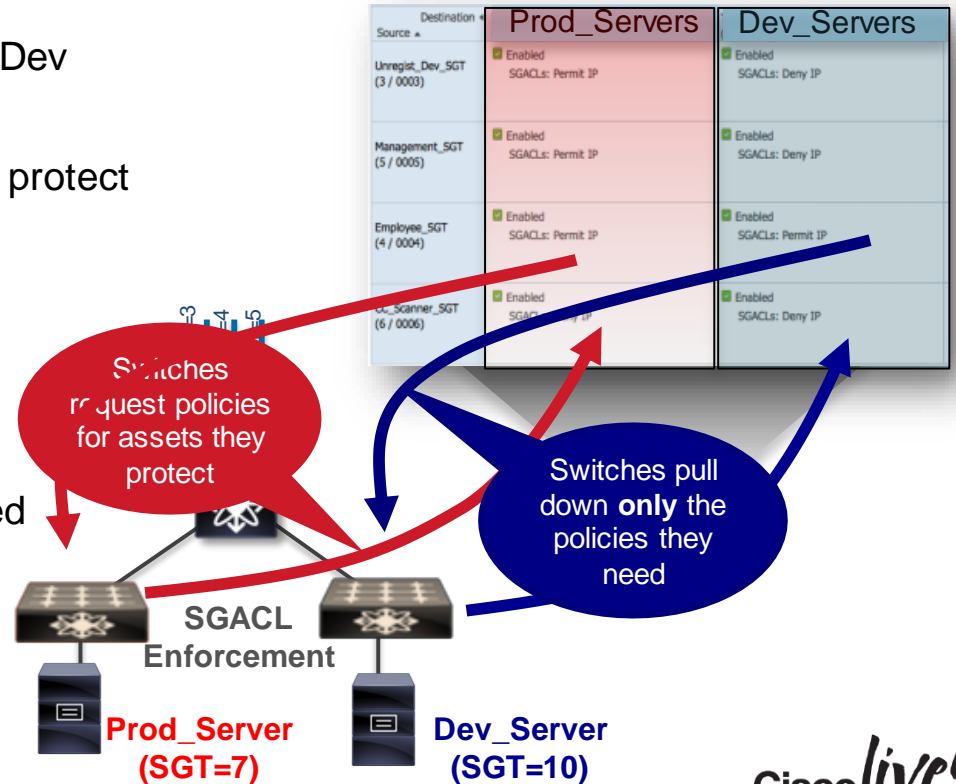
**Egress Policy (Matrix View)**

Edit   
 Add   
 Clear Mapping   
 Configure   
 Push   
 Monitor All - Off    
 View   
 Dimension **6X10**   
 Import   
 Export

Destination ▶ Source ▼	Developers (4/0004)	Development_Servers (101/0065)	Engineering (3/0003)	Production_Servers (103/0067)
Developers (4/0004)		<input checked="" type="checkbox"/> Permit IP		<input checked="" type="checkbox"/> Deny IP
Development_Servers (101/0065)		<input checked="" type="checkbox"/> Common_Services		<input checked="" type="checkbox"/> Deny IP
Engineering (3/0003)				
Production_Servers (103/0067)		<input checked="" type="checkbox"/> Deny IP		<input checked="" type="checkbox"/> Permit IP
Production_Users (5/0005)		<input checked="" type="checkbox"/> Deny IP		<input checked="" type="checkbox"/> Web_SGACL

# SGACL Downloads

- New Servers provisioned, e.g. Prod Server & Dev Server Roles
- DC switches request policies for assets they protect
- Policies downloaded & applied dynamically
- What this means:
  - All controls centrally managed
  - Security policies de-coupled from network
  - **No switch-specific security** configs needed
  - Wire-rate policy enforcement
  - One place to audit network-wide policies



# Enabling Policy Enforcement in Switches

- After setting up SGT/SGACL in ISE, you can now enable SGACL Enforcement on network devices
- Devices need to be defined in ISE and provisioned to talk to ISE (omitted from these slides for brevity)

Enabling SGACL Enforcement Globally and for VLAN

```
Switch(config)#cts role-based enforcement
Switch(config)#cts role-based enforcement vlan-list 40
```

- If switches have SGT assignments they will download policy for the assets they are protecting

As example - defining IP to SGT mapping for servers on a switch

```
Switch(config)#cts role-based sgt-map 10.1.40.10 sgt 5
Switch(config)#cts role-based sgt-map 10.1.40.20 sgt 6
Switch(config)#cts role-based sgt-map 10.1.40.30 sgt 7
```

# Policy Enforcement on Firewalls: ASA SG-FW

The screenshot displays the Cisco ASDM 6.7 for ASA - 10.1.201.2 interface. The main window shows a table of firewall rules. The left sidebar contains a tree view of configuration objects, and the bottom status bar shows 'Configuration changes saved successfully.'

**Security Group definitions from ISE**

**Switches inform the ASA of Security Group membership**

#	Enabled	Source Criteria			Destination Criteria		Service	Action	Hits	Logging	Time	Descript
		Source	User	Security Group	Destination	Security Group						
inside (1 incoming rule)												
1	<input checked="" type="checkbox"/>	any			any		ip	Permit	TOP 10 ...			
outside (9 incoming rules)												
1	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit	0			
2	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny	0			
3	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Employee_Portal	http	Permit	0			
6	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT CC_Scanner_SGT	any	Manager_Portal	ip	Deny	0			
7	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Time_Card_Ser...	https	Permit	0			Time Card Application
8	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Time_Card_Ser...	https	Deny	0			Time Card Application
9	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	CreditCard_Ser...	https	Permit	0			Credit Card Scan Communication
Global (1 implicit rule)												
1	<input checked="" type="checkbox"/>	any			any		ip	Deny				Implicit rule

**Trigger FirePower services by SGT policies**

**Can still use Network Object (Host, Range, Network (subnet), or FQDN) AND / OR the SGT**

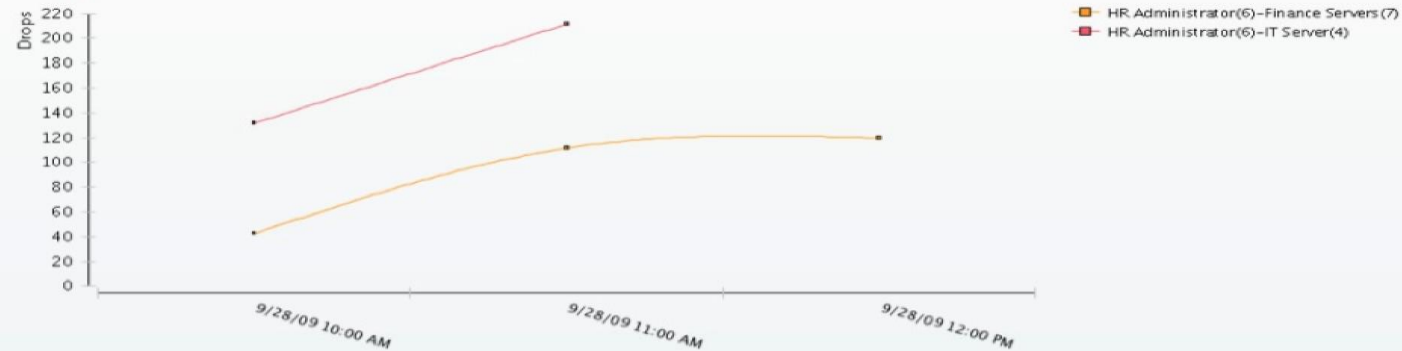
BRK: Configuration changes saved successfully. <admin> 15 5/31/12 11:53:50 PM PDT

# Monitoring

- SGACL syslogs, NetFlow events and ASA logging all useful

## TrustSec > RBACL Drop Summary

Reload



Time	Drops	User	Src Address	Src Port	Destination	Dest Address	Dest Port	Protocol	SGACL	SGT	DGT
September 28 10:00:00 AM	<u>43</u>	CTS\hradmin	10.1.10.100	20134	10.1.200.300	80	tcp (6)	Deny IP, Permit IP		HR Administrator(6)	Finance Servers(7)
	<u>132</u>	CTS\hradmin	10.1.10.100	20134	10.1.200.200	80	tcp (6)	Permit IP		HR Administrator(6)	IT Server(4)
September 28 11:00:00 AM	<u>112</u>	CTS\hradmin	10.1.10.100	20134	10.1.200.300	80	tcp (6)	Deny IP, Permit IP		HR Administrator(6)	Finance Servers(7)
	<u>212</u>	CTS\hradmin	10.1.10.100	20134	10.1.200.200	80	tcp (6)	Permit IP		HR Administrator(6)	IT Server(4)
September 28 12:00:00 PM	<u>120</u>	CTS\hradmin	10.1.10.100	20134	10.1.200.300	80	tcp (6)	Deny IP, Permit IP		HR Administrator(6)	Finance Servers(7)



# Using NetFlow for Policy Validation – with Lancope

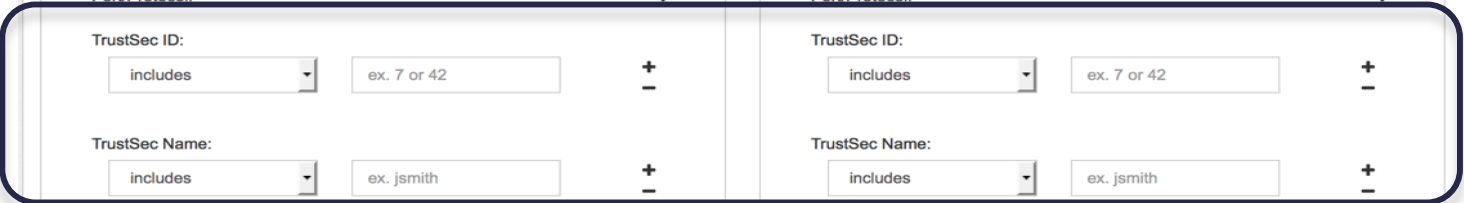
**Custom Event**

Rule/Event Name:

Description:

Object		Peer	
Host:	+	Host:	+
User:	+	User:	+
Devices:	+	Devices:	+
Port/Protocol:	+	Port/Protocol:	+
TrustSec ID:		TrustSec ID:	
<input type="text" value="includes"/>	<input type="text" value="ex. 7 or 42"/>	<input type="text" value="includes"/>	<input type="text" value="ex. 7 or 42"/>
	+		+
TrustSec Name:		TrustSec Name:	
<input type="text" value="includes"/>	<input type="text" value="ex. jsmith"/>	<input type="text" value="includes"/>	<input type="text" value="ex. jsmith"/>
	+		+
Application:	+	Application:	+
Orientation:			
<input type="text" value="either"/>			

Generate a security event when a flow condition based on the SGT value is seen



# Using NetFlow for Policy Validation – with Lancope

The screenshot displays the 'Query Builder' interface with the following elements:

- Range:** A dropdown menu set to 'Last 2 Minutes'.
- Search Subject:** A section containing several search criteria:
  - Host:** Includes a dropdown set to 'includes' and a text box containing 'Host Groups'.
  - Inside Hosts:** A button labeled '+ Host Groups'.
  - User:** A dropdown set to 'includes'.
  - Devices:** A dropdown set to 'includes'.
  - Port/Protocol:** A dropdown set to 'includes' and a text box containing 'ex. 80/tcp or 80-8080/tc'.
  - TrustSec ID:** A dropdown set to 'includes' and a text box containing 'ex. 7 or 42'.

A blue callout box with a downward-pointing arrow contains the text: "Use the SGT value to find (and classify) network traffic". This callout points to the 'TrustSec ID' field in the right-hand section of the interface.

The right-hand section of the interface includes:

- From:** A text input field.
- To:** A text input field.
- Host:** A dropdown set to 'includes'.
- User:** A dropdown set to 'includes'.
- Devices:** A dropdown set to 'includes'.
- Port/Protocol:** A dropdown set to 'includes'.
- TrustSec ID:** A dropdown set to 'includes' and a text box containing 'ex. 7 or 42'.
- TrustSec Name:** A dropdown set to 'includes' and a text box containing 'ex. jsmith'.

# NetFlow Monitoring






Who

What

How

Who

Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 01/19 - 01:43:22 PM End: 01/19 - 02:15:59 PM Duration: 32m 37s	 10.10.18.103  RFC 1918 <a href="#">View Details</a>	ICMP	45.23KB   772 packets	ICMP	

When

Where

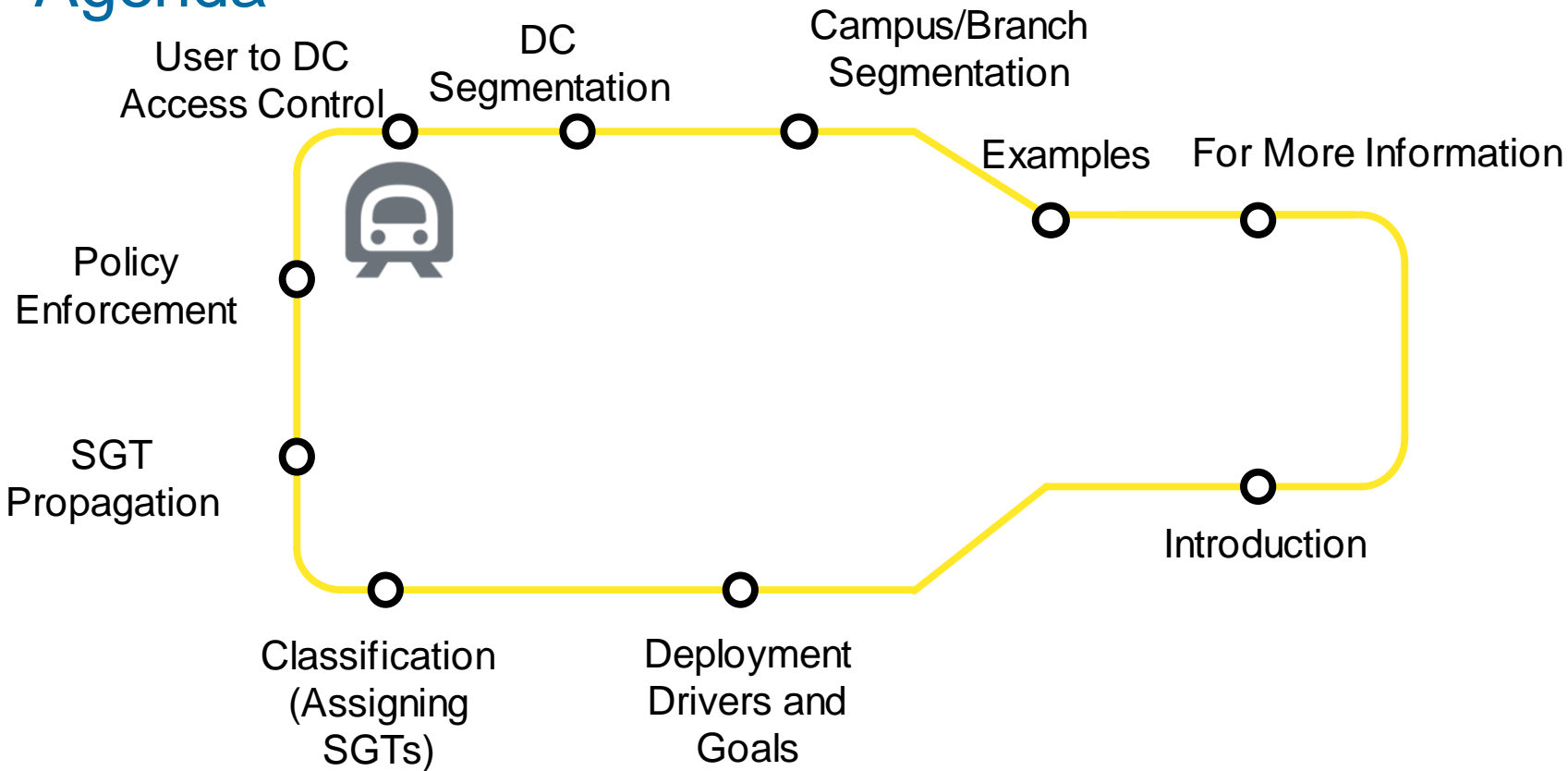
Security Group

Flow Detailed Summary: 10.10.18.103

Search Subject Details	Totals	Peer Details
Packets: 772 Packet Rate: 0.39pps Bytes: 45.23KB Byte Rate: 23.67bps Percent Transfer: 100% Host Groups: Catch All TrustSec ID: 8 TrustSec Name: EMPLOYEE_FULL	Packets: 772 Packet Rate: 0.39pps Bytes: 45.23KB Byte Rate: 23.67bps Search Subject/Peer Ratio: all search subject RTT: 0s SRT: 0s	Packets: 0 Packet Rate: 0pps Bytes: 0B Byte Rate: 0bps Percent Transfer: 0% Host Groups: Catch All

[Close](#)

# Agenda

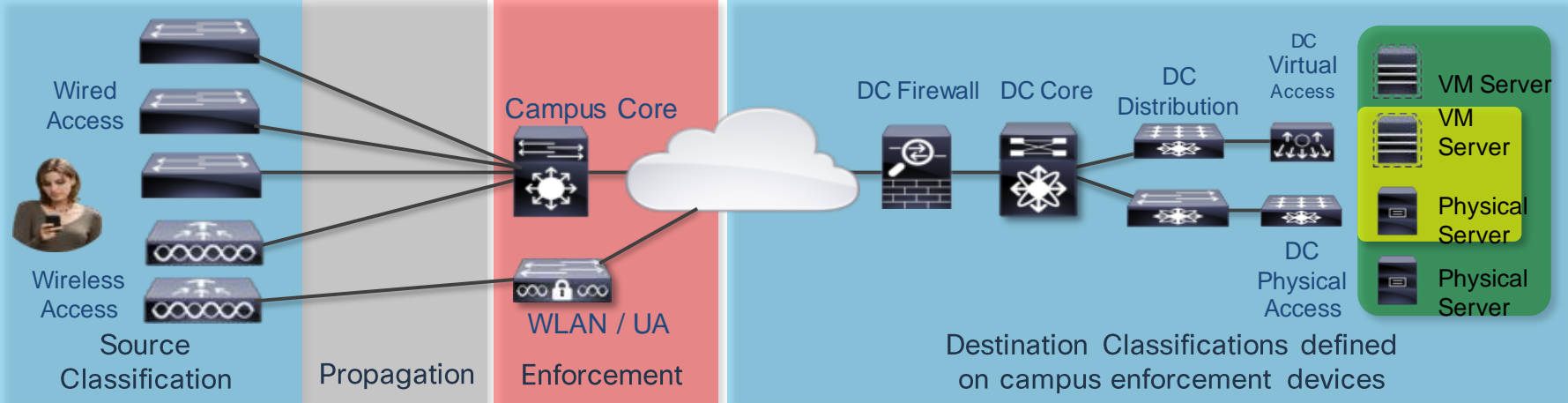


# Controlling User Access to DC Resources

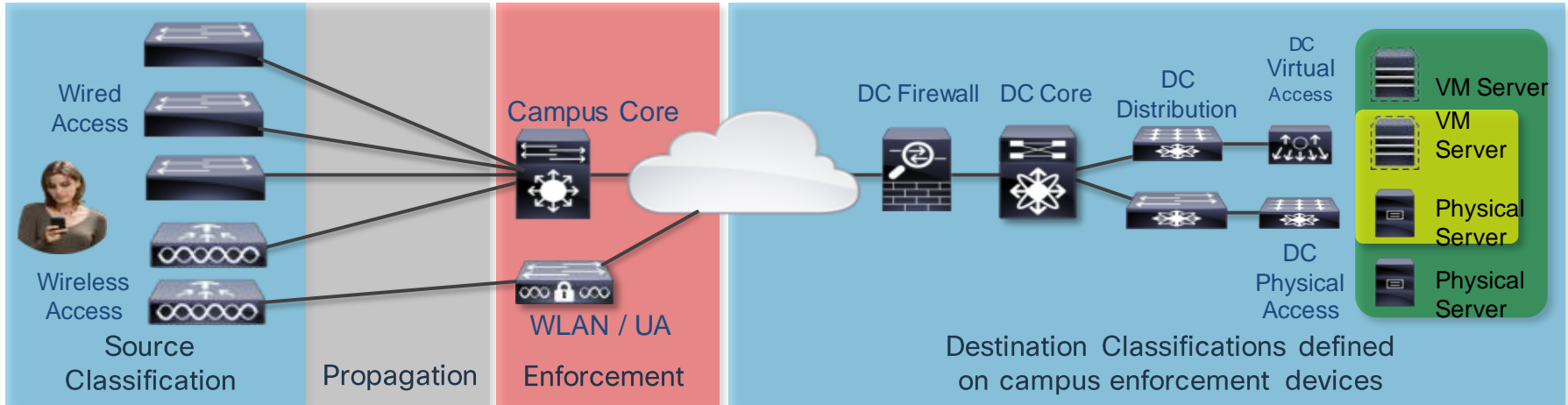
## User/Device Classifications



# User to DC Access Control: Campus Enforcement



# User to DC Access Control: Campus Enforcement



Catalyst 2960-S/-C/-Plus/-X/-XR

SXP

Catalyst 3560-E/-C/, 3750-E

SXP

Catalyst 3560-X, 3750-X

SXP

SGT

Catalyst 3850

SXP

SGT

Catalyst 4500E (Sup6E)

SXP

Catalyst 4500E (S7,8), 4500X

SXP

SGT

Catalyst 6500E (Sup720)

SXP

Catalyst 6500E (2T)

SXP

SGT

WLC 2500, 5500, WiSM2

SXP

WLC 5760

SXP

SGT



Campus Dist/Core Switch:

Catalyst 6500E(2T)/6800  
(200k IP-SGT)

Catalyst 4500 Sup7/8(L3 cfg)  
(64k or 256k IP-SGT)

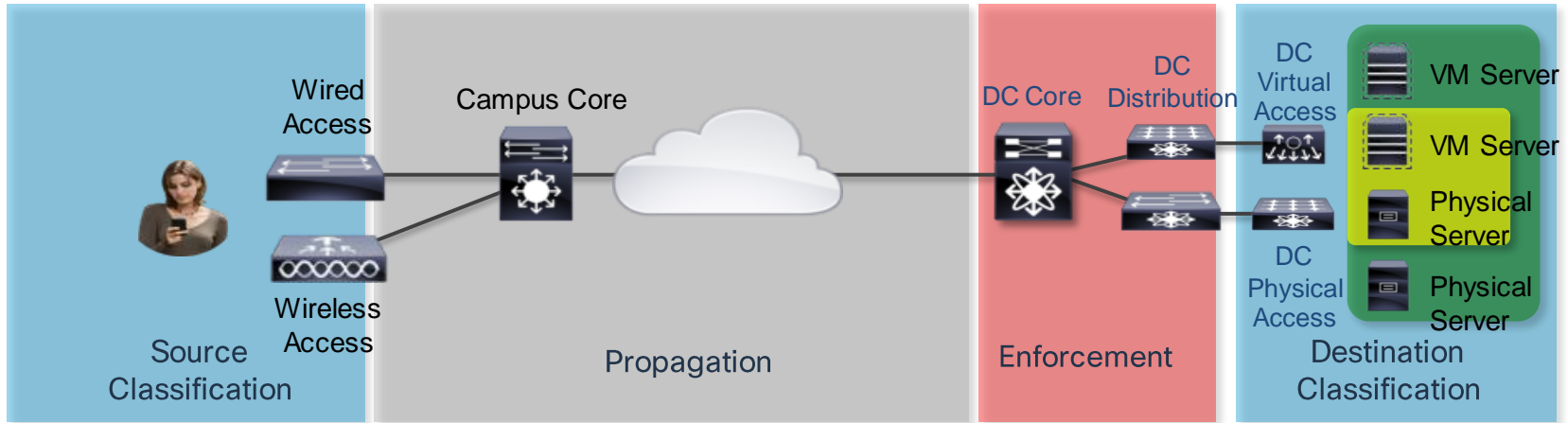
Classify destination SGTs in enforcement device using:

**Subnet-SGT mappings**

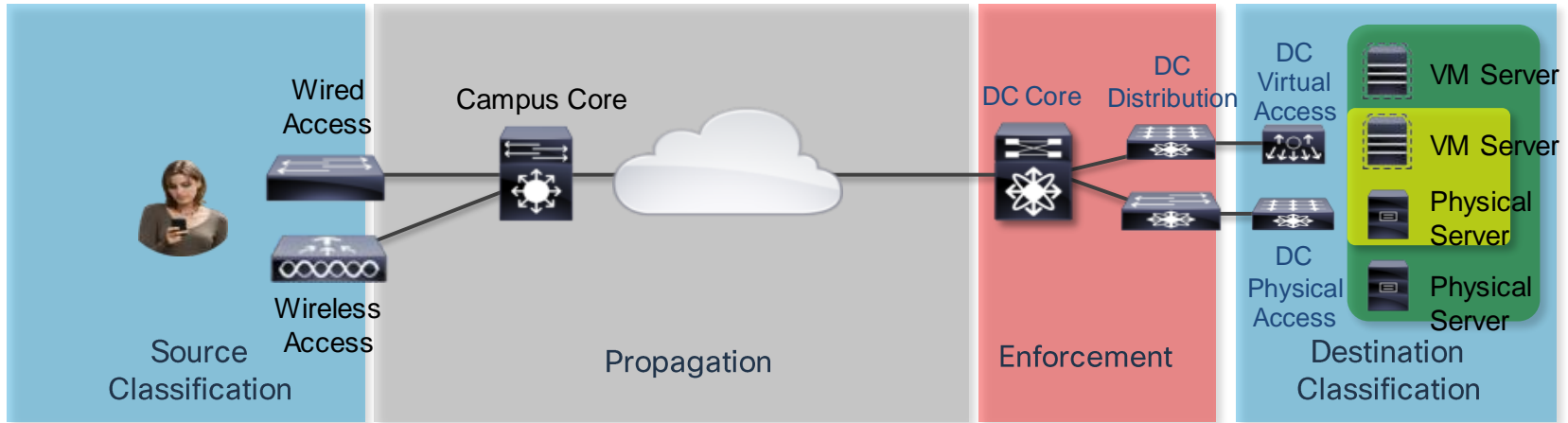
**IP-SGT mappings**



# User to DC Access Control: DC Enforcement



# User to DC Access Control: DC Enforcement



Catalyst 2960-S/-C/-Plus/-X/-XR  
 Catalyst 3560-E/-C/, 3750-E  
 Catalyst 3560-X, 3750-X  
 Catalyst 3850  
 Catalyst 4500E (Sup6E)  
 Catalyst 4500E (7E), 4500X  
 Catalyst 6500E (Sup720)  
 Catalyst 6500E (2T)  
 WLC 2500, 5500, WiSM2  
 WLC 5760



## CLASSIFY SERVERS WITH:

### Nexus 1000v Port Profile SGT mappings

- VMs are associated with Nexus 1000V Port Profiles
- N1000v sends SGT assignment to N7000s

### Nexus 7000

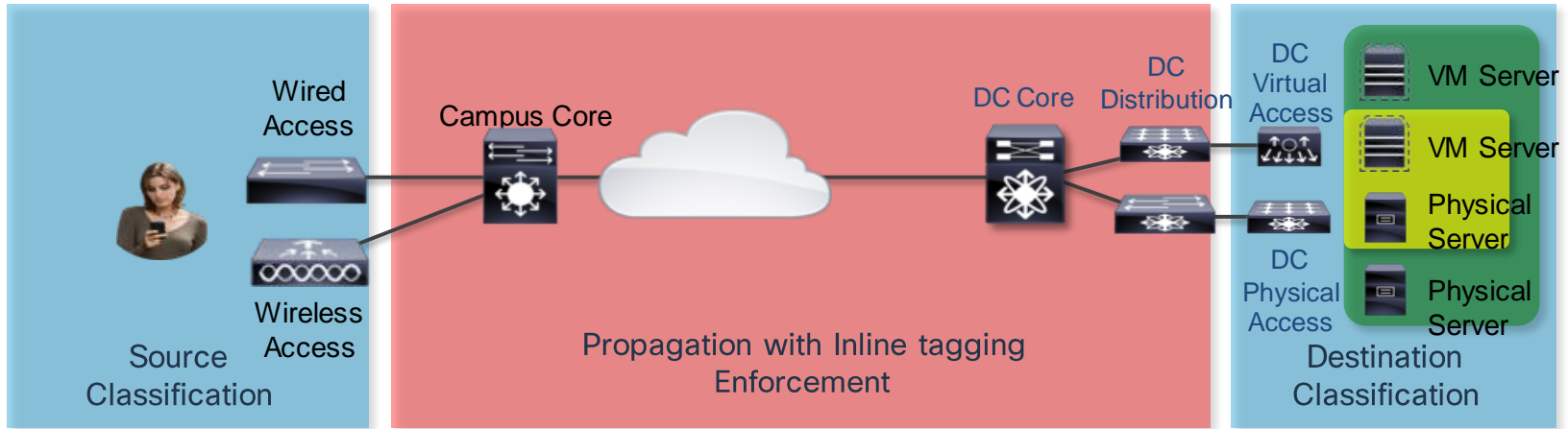
- VLAN – SGT mappings
- IP-SGT used for physical servers:
- IP Mappings pushed from ISE to N7000 switches

### Nexus 5500/5600//2200(FEX)

- Port-SGT mappings used for physical servers

*CiscoLive!*

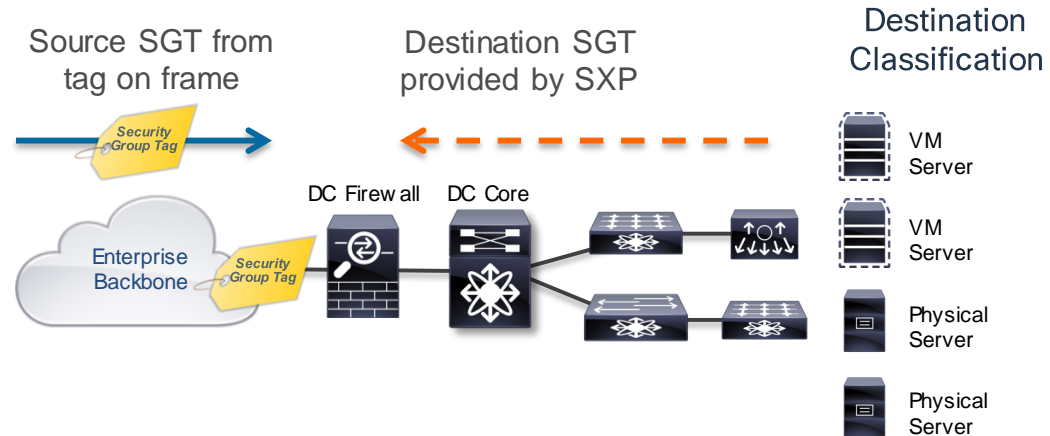
# User to DC Access Control – Extending Enforcement



- Extend tagging from campus distribution or core to DC ingress
- Apply cts manual functions on inter-switch links to carry SGT  
(Note: this disrupts link operation, as after config a shut + no shut required)
- Enable role-based enforcement on campus and DC switches

# ASA Inline Tagging and SXP DC Design

- ASA derives Source SGT for campus traffic from tagged frames
- For enforcement, ASA must know the Destination SGT for each server
- SXP still used to provide Destination SGT for each server to ASA



# User to DC: SXP Scaling



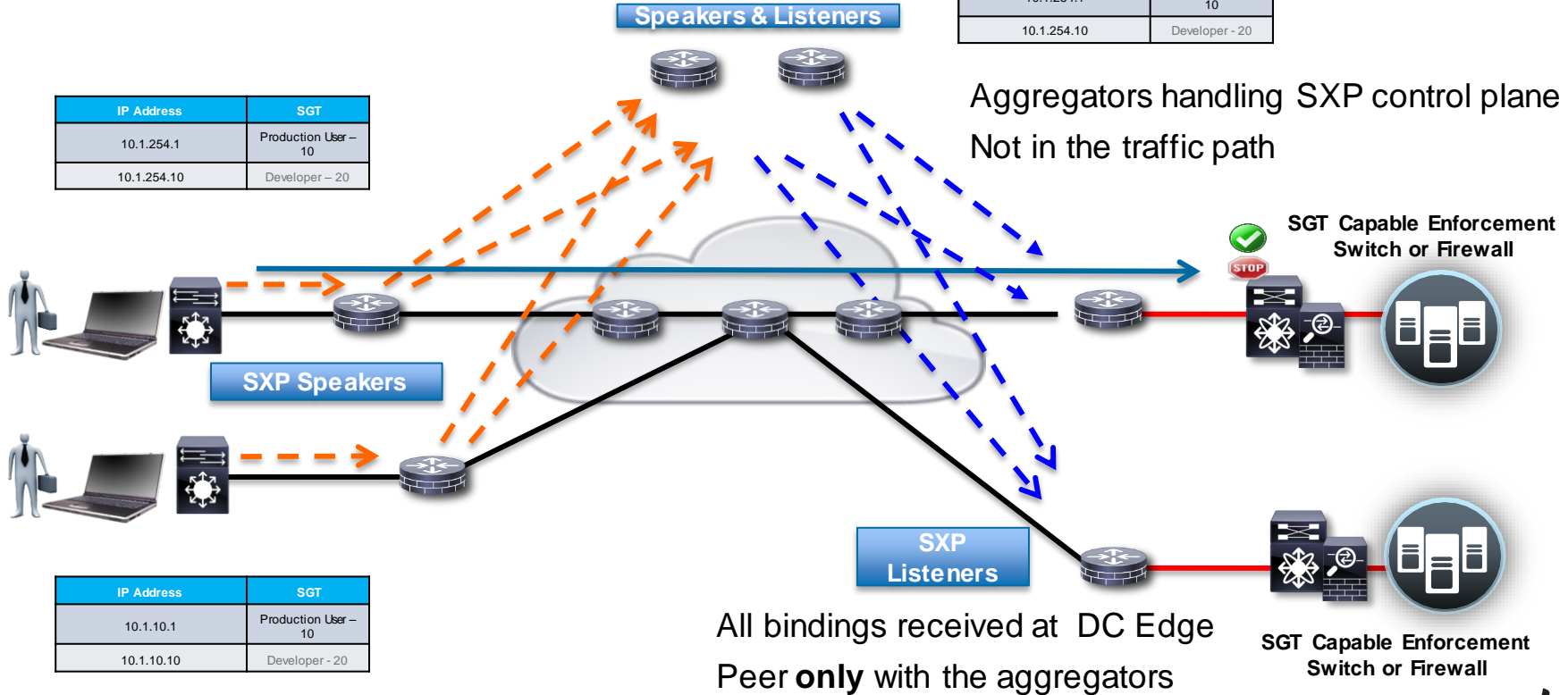
Platform	Max SXP Connections	Max IP-SGT bindings
<b>Catalyst 6500 Sup2T/ 6800</b>	2000	200,000
<b>Nexus 7000</b>	980	M series 50,000 F3 64,000 (recommend 50k) F2e 32,000 (recommend 25k)
<b>Catalyst 4500 Sup 7E</b>	1000	256,000
<b>Catalyst 4500-X / 4500 Sup 7LE</b>	1000	64,000
<b>ASA 5585-X SSP60</b>	1000	100,000
<b>ASA 5585-X SSP40</b>	500	50,000
<b>Catalyst 3850/WLC 5760</b>	128	12,000

# SXP WAN Aggregation Option

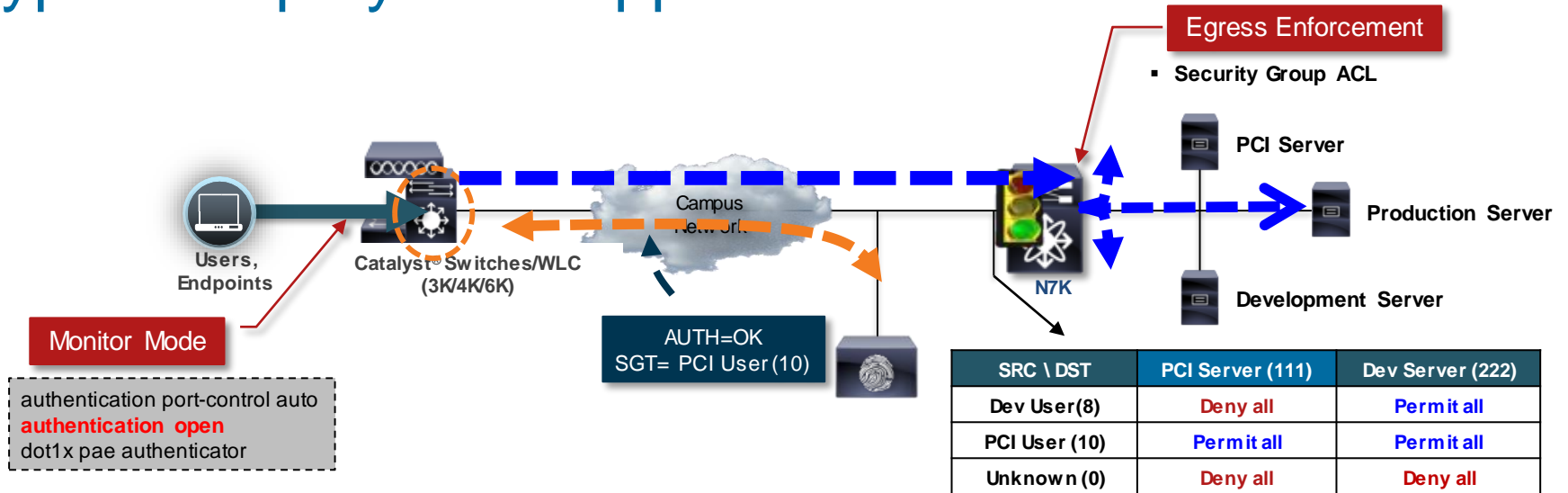
IP Address	SGT
10.1.10.1	Production User - 10
10.1.10.10	Developer - 20
10.1.254.1	Production User - 10
10.1.254.10	Developer - 20

IP Address	SGT
10.1.254.1	Production User - 10
10.1.254.10	Developer - 20

IP Address	SGT
10.1.10.1	Production User - 10
10.1.10.10	Developer - 20



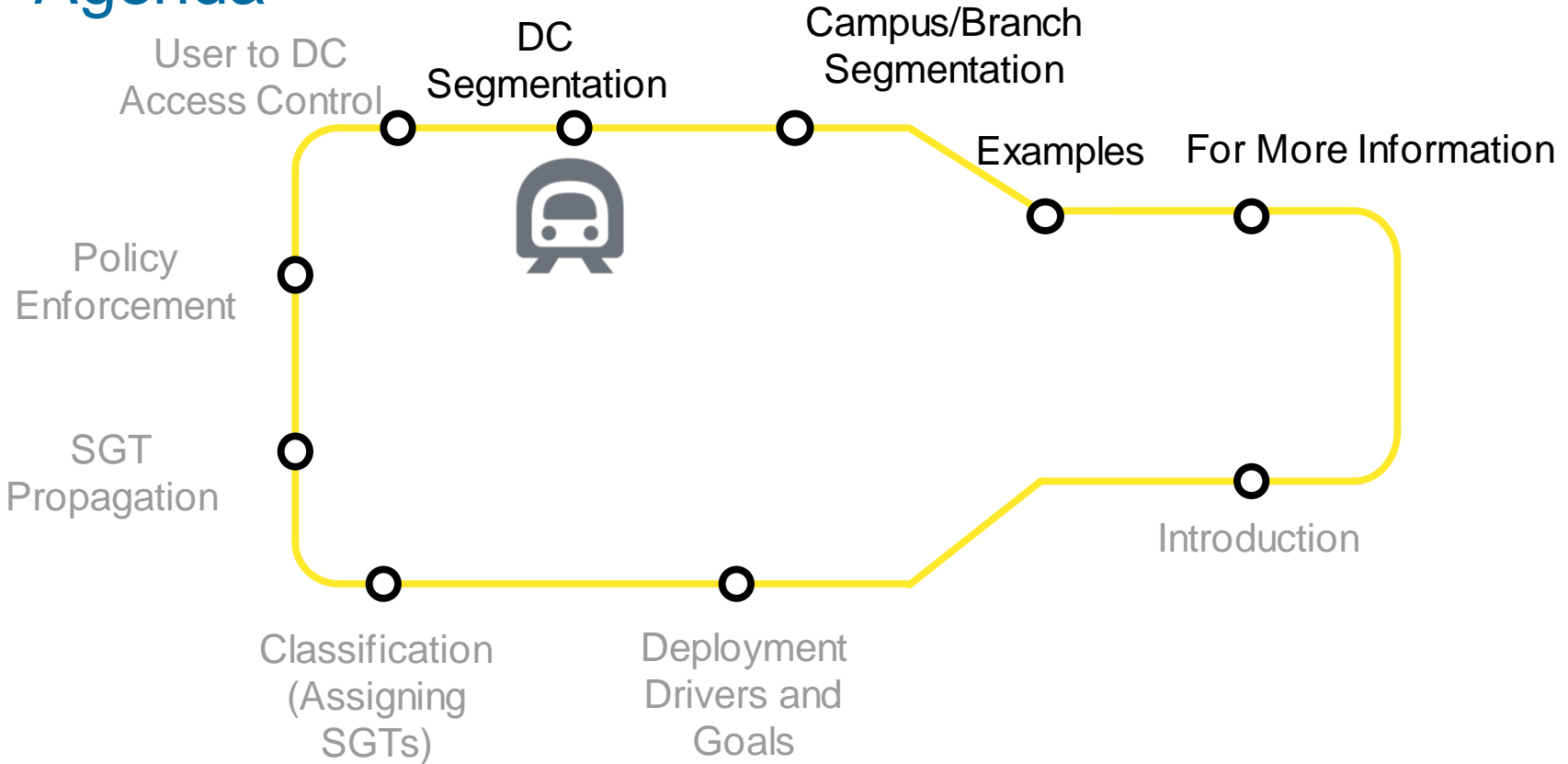
# Typical Deployment Approach



1. Users connect to network, Monitor mode allows traffic regardless of authentication
2. Authentication can be performed passively resulting in SGT assignments
3. Traffic traverses network to Data Centre enforcement points
4. Enforcement may be enabled gradually per destination Security Group



# Agenda

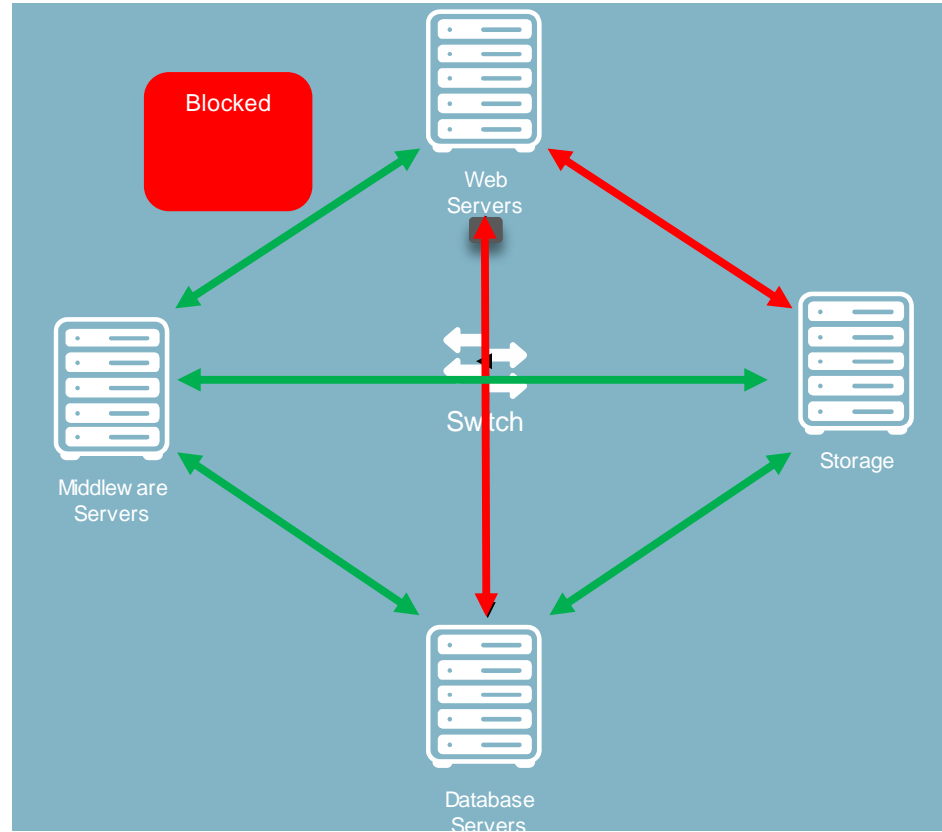


# Data Centre Segmentation

How to define this policy:

	Web Servers	Middle are Servers	Database Servers	Storage
Web Servers	✓	✓	✗	✗
Middle are Servers	✓	✓	✓	✓
Database Servers	✗	✓	✓	✓
Storage	✗	✓	✓	✓

- Segment servers into logical zones
- Control access to logical DC entities based on role
- Apply controls to physical and virtual servers



# Defining Server Classifications in ISE (IP-SGT)

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, a secondary navigation bar features 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'TrustSec', and 'Policy Elements'. The 'Results' tab is active, showing a search bar and a tree view on the left. The tree view is expanded to 'TrustSec' > 'Security Group Mappings' > 'Hosts'. The main content area, titled 'Hosts', contains a table with columns for 'IP Address/Mask', 'Hostname', 'SGT', 'Group', and 'Deployed To'. The table lists four entries, each with a checkbox in the first column. A mouse cursor is pointing at the 'Hosts' folder in the left sidebar.

	IP Address/Mask	Hostname	SGT	Group	Deployed To
<input type="checkbox"/>	10.1.1.1/32		Development_Servers ...		Device Group: DC1_Distribution_N7000s
<input type="checkbox"/>	10.1.1.2/32		Production_Servers (1...		Device Group: DC1_Distribution_N7000s
<input type="checkbox"/>	172.16.1.1/32		Development_Servers ...		Device Group: DC2_Distribution_N7000s
<input type="checkbox"/>	172.16.1.2/32		Production_Servers (1...		Device Group: DC2_Distribution_N7000s

# Grouping Server Classifications in ISE



**CISCO Identity Services Engine**

Home | Operations | Policy | Guest Access | Administration

Authentication | Authorization | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

Dictionary | Conditions | Results

Authentication | Authorization | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

Dictionary | Conditions | Results

### Results

Search:

- Authentication
- Authorization
- Profiling
- Posture
- Client Provisioning
- TrustSec
  - Security Group ACLs
    - Common\_Services
    - Web\_SGACL
  - Security Groups
  - Security Group Mappings
    - Groups
    - Hosts

### Groups

Edit | Add | Deploy | Check Status | Delete

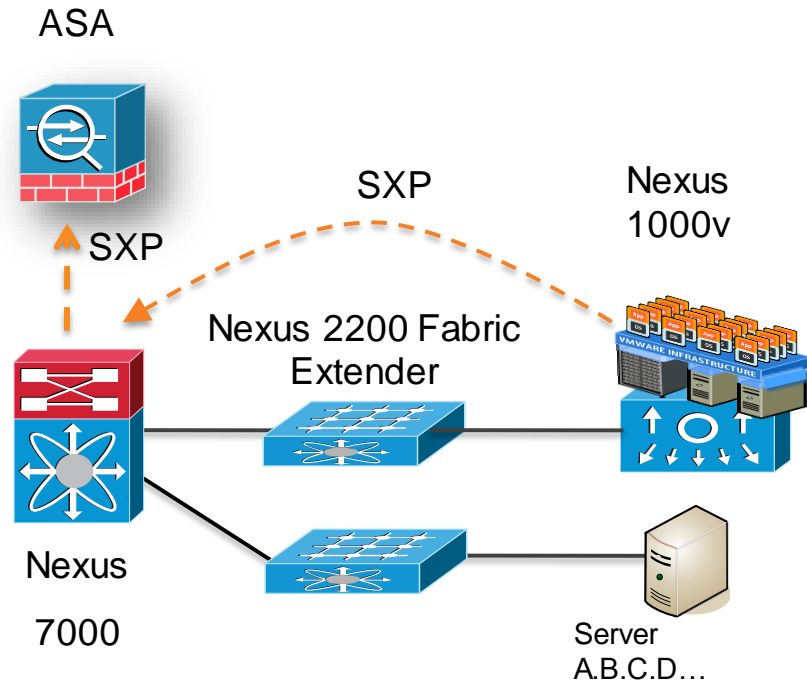
Name	Description	SGT	Deployed To
<input type="checkbox"/> DC1_Production_Servers		Production_Servers (103/0067)	Device Group: DC1_Distribution_N7000s
<input type="checkbox"/> DC2_Production_Servers		Production_Servers (103/0067)	Device Group: DC2_Distribution_N7000s
<input type="checkbox"/> DC1_Development_Servers		Development_Servers (101/0065)	Device Group: DC1_Distribution_N7000s
<input type="checkbox"/> DC2_Development_Servers		Development_Servers (101/0065)	Device Group: DC2_Distribution_N7000s

# Using Static IP-SGT Mappings in Nexus 7000

- Mappings pushed from ISE or defined in the switch:-

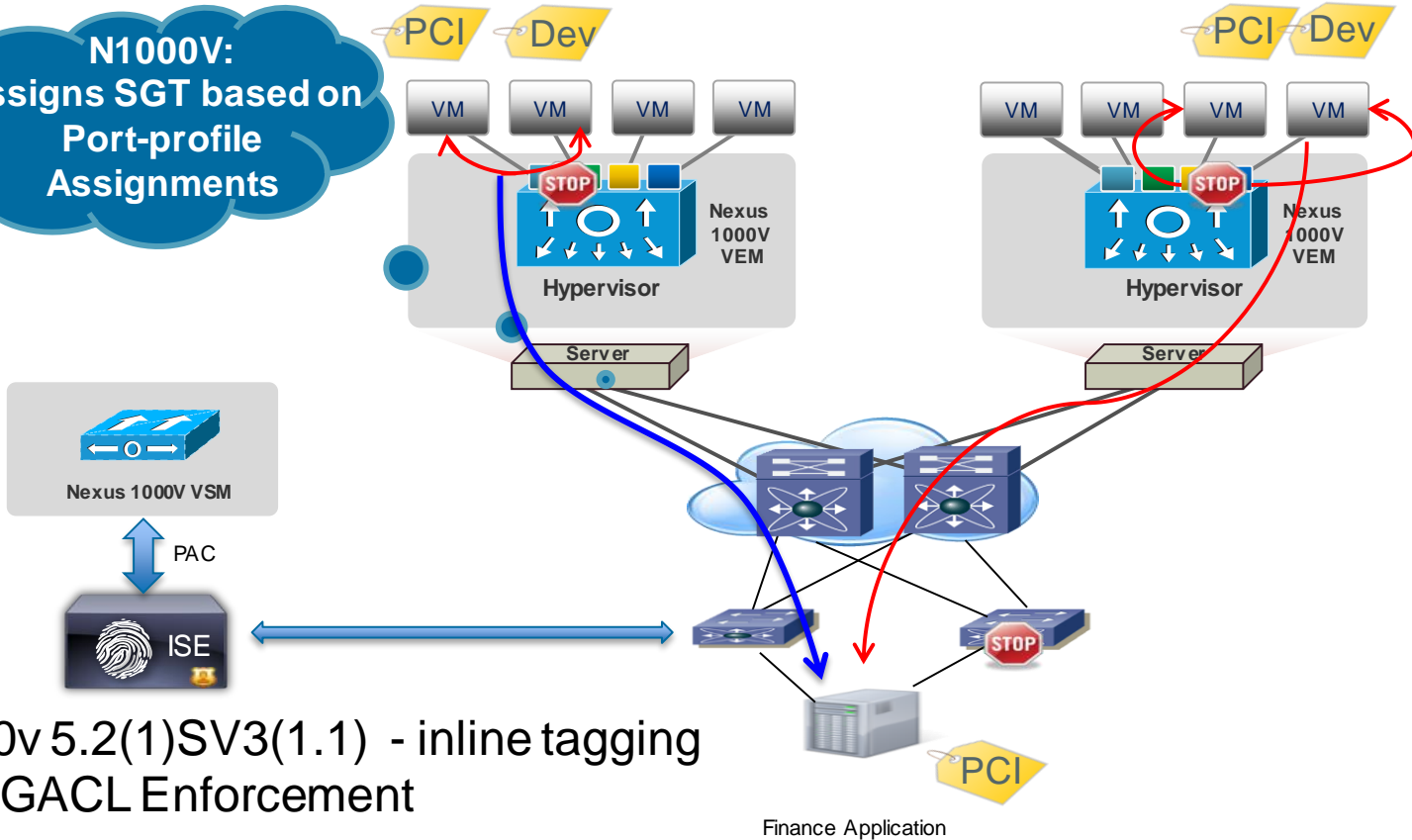
```
cts role-based sgt-map A.B.C.D sgt SGT_Value
```

- Nexus 7000 may also receive bindings from other SXP speakers e.g. Nexus 1000v
- N7000 can also send server mappings to ASA over SXP (ASA as SXP listener)
- All bindings (static + dynamic) would be sent over SXP



# SGACLs on Nexus 1000v Virtual Switch

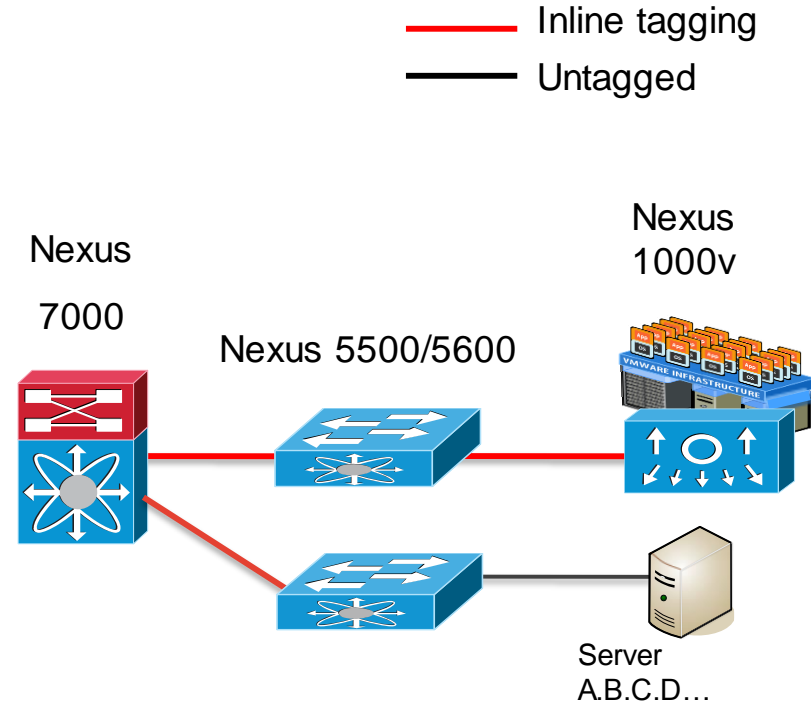
**N1000V:**  
Assigns SGT based on  
Port-profile  
Assignments



N1000v 5.2(1)SV3(1.1) - inline tagging  
and SGACL Enforcement

# Nexus 7x00 / Nexus 1000v Interaction

- N1000v 5.2(1)SV3(1.1) for inline tagging and SGACL
- N1000v5.2(1)SV3(1.2) introduced SGACL logging
- For TrustSec + FabricPath and vPC/vPC+ recommend
  - Nexus 7000 6.2.10
  - Nexus 5600/6000 7.1(0)N1(1)
  - Nexus 5500 6.0(2)N2(6)



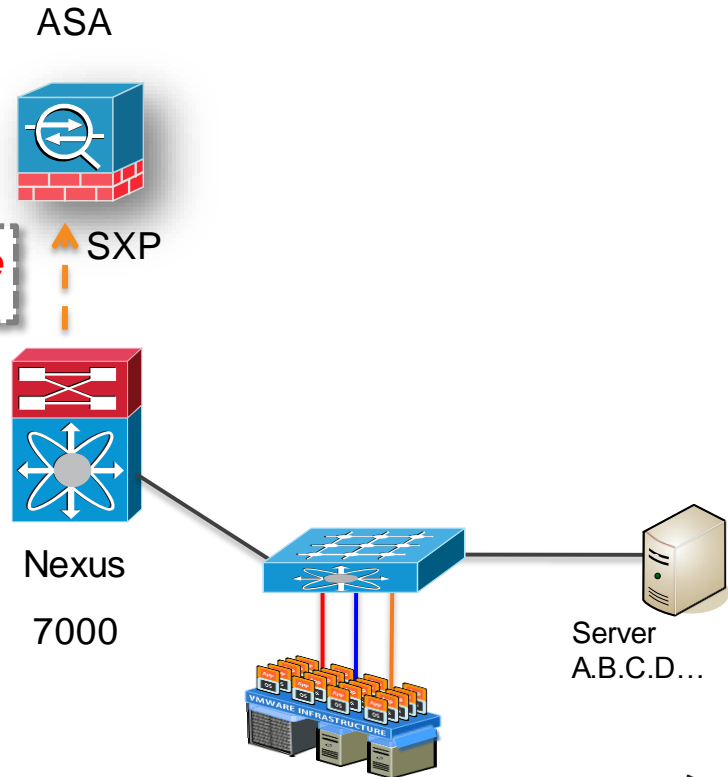


# Nexus 7x00 VLAN-SGT Maps

- Classify servers by VLAN they are attached to

cts role-based sgt-map vlan-list *VLAN* sgt *SGT\_Value*

- N7000 will still derive IP-SGT maps from VLANs and send to ASA
- N7k VLAN-SGT and Port-SGT with vPC/vPC+ requires enhancement in 7.x
- IP-SGT supported with vPC/vPC+ in 6.2.10

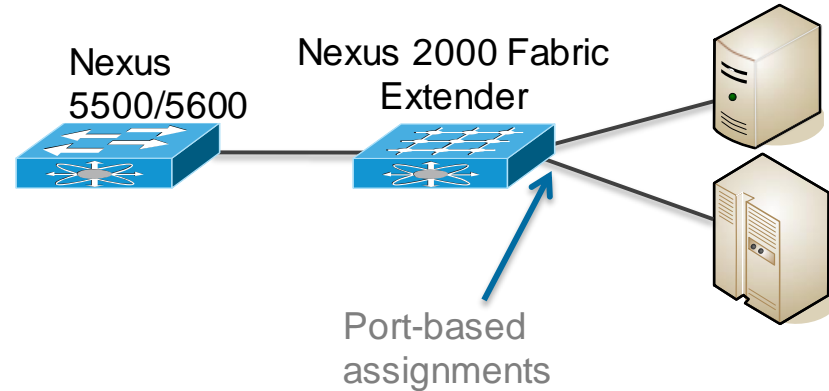


# Using Nexus 5500/5600 for Physical Servers

- Nexus 5500 with N2200 FEX
- All SGT processing on N5500
- SGT assignments applied in N5k SGACLs are port-based
- Policy static – SGT assigned on interface

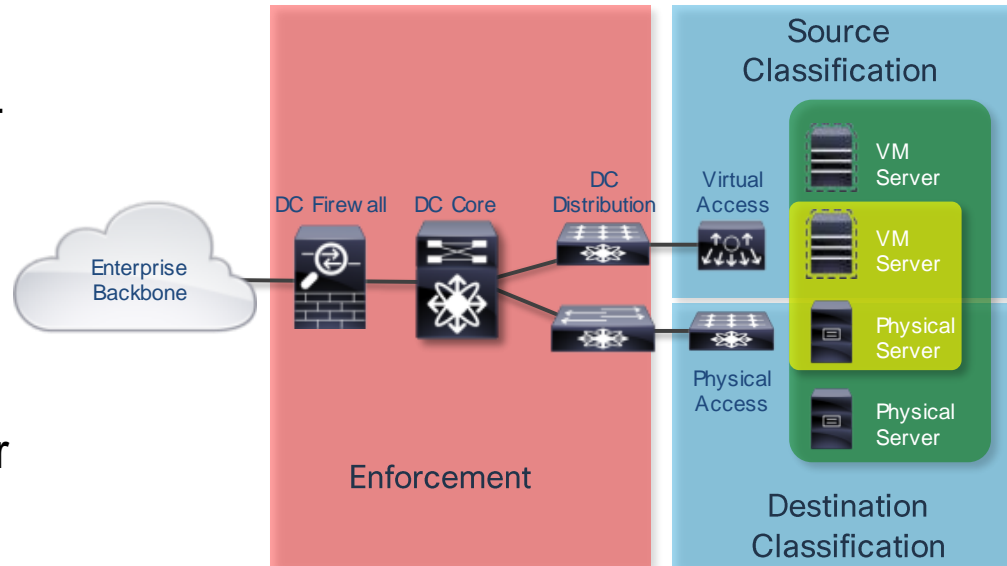
```
interface Ethernet1/20
  cts manual
  policy static sgt <value>
```

- No SXP listening capabilities

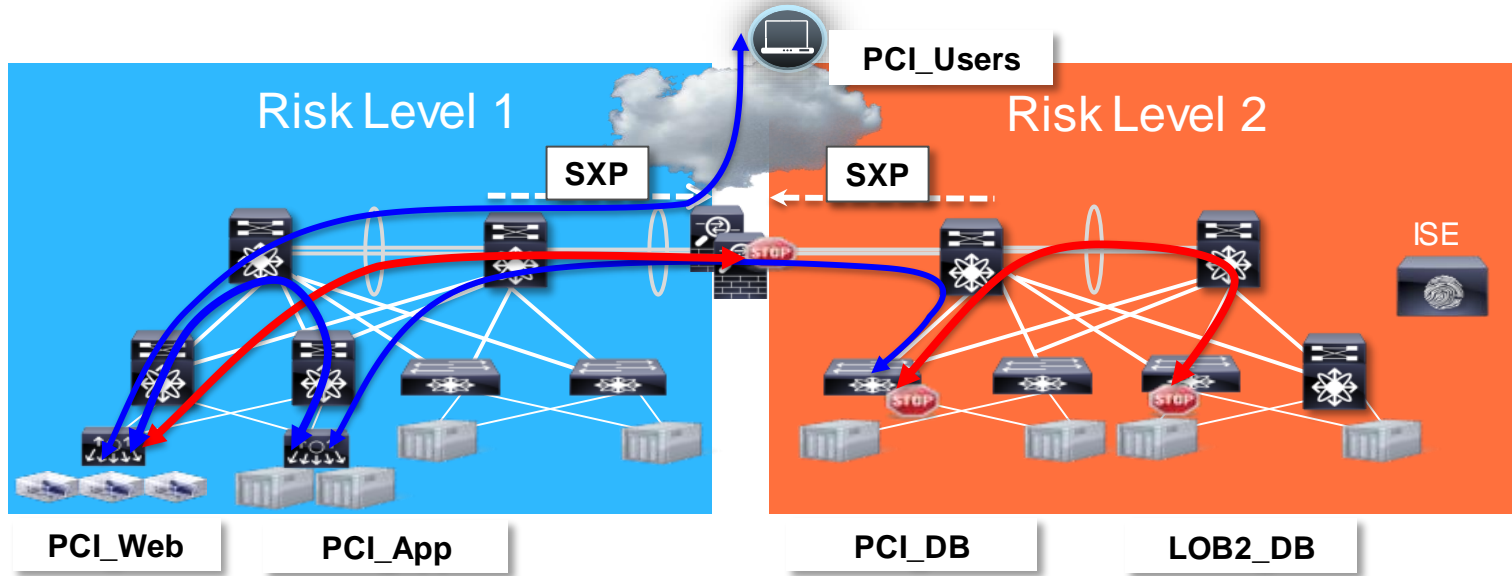


# Server Classifications

- Nexus 1000v Port Profile SGT mappings
- Nexus 7000 VLAN – SGT mappings
- Nexus 7000 IP-SGT mappings
- Nexus 6000/5600/5500 Port-SGT assignments for inline tagging



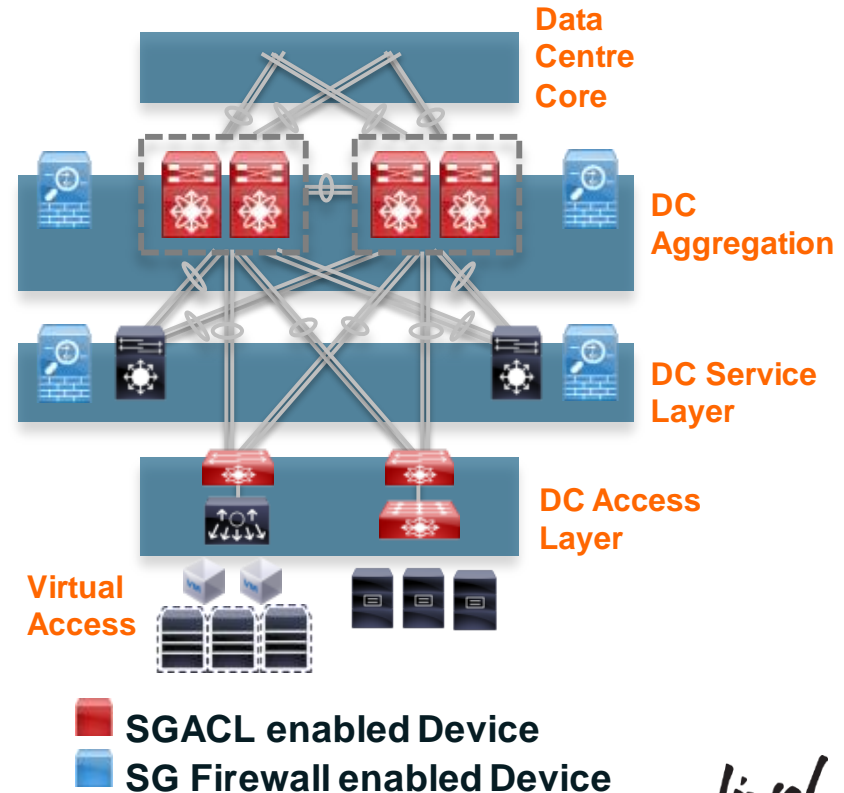
# Using SGACL and SG-FW Functions Together



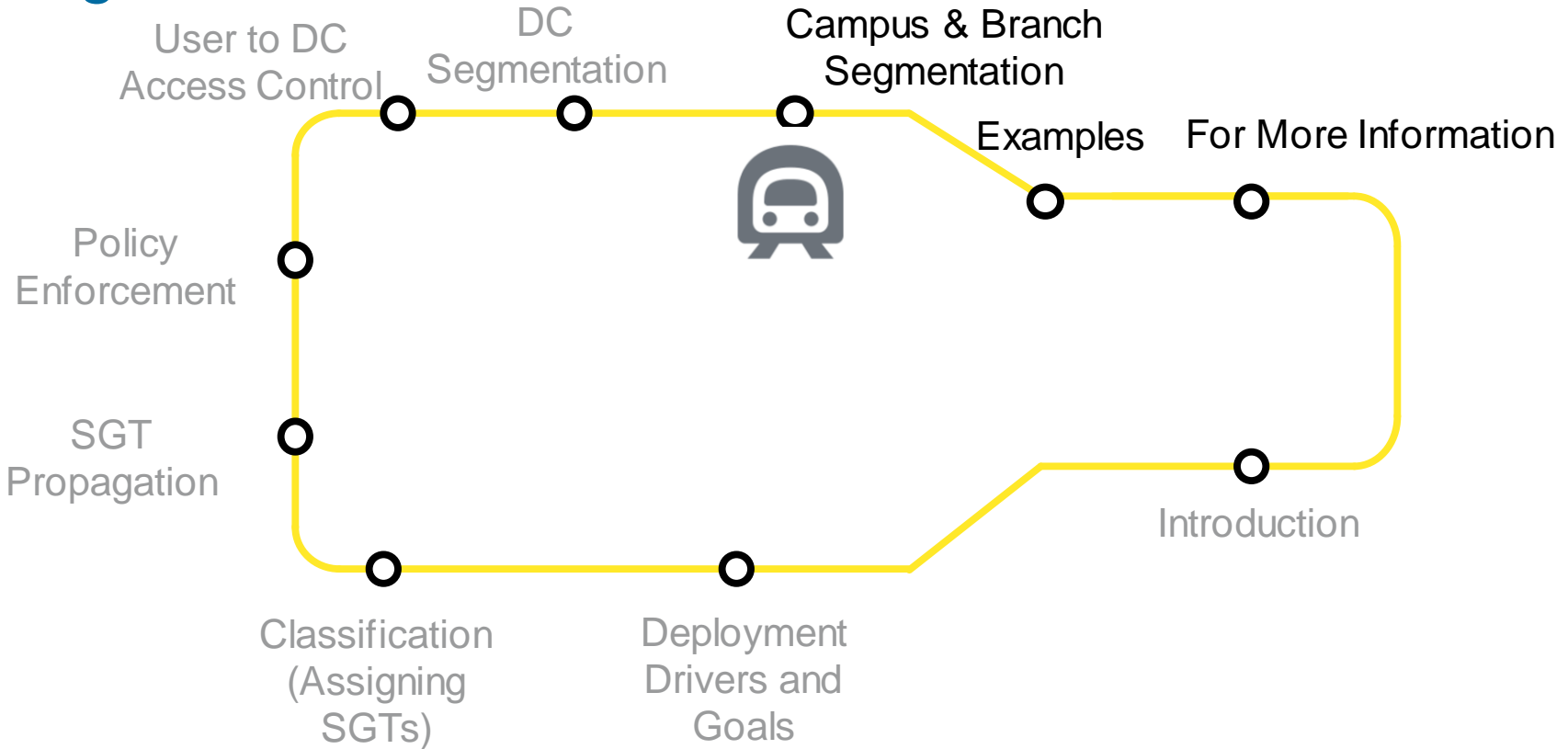
- SGACL on switches enforcing policy within each Risk Level
- ASA enforcing policy between Risk Levels (with IP/SGT mappings supplied from switch infrastructure)

# Data Centre Segmentation

- SGT provides common policy objects used throughout FW and ACL rules
- Centralised SGACL definition & automation
- SGT can be propagated to other DCs to further simplify policy
- SGT caching in N7000 allows tags to be removed for 3<sup>rd</sup> party inspection devices and reapplied afterwards
- Good practice on Nexus to use SGACL batch programming features for complex policies (needs enabling)



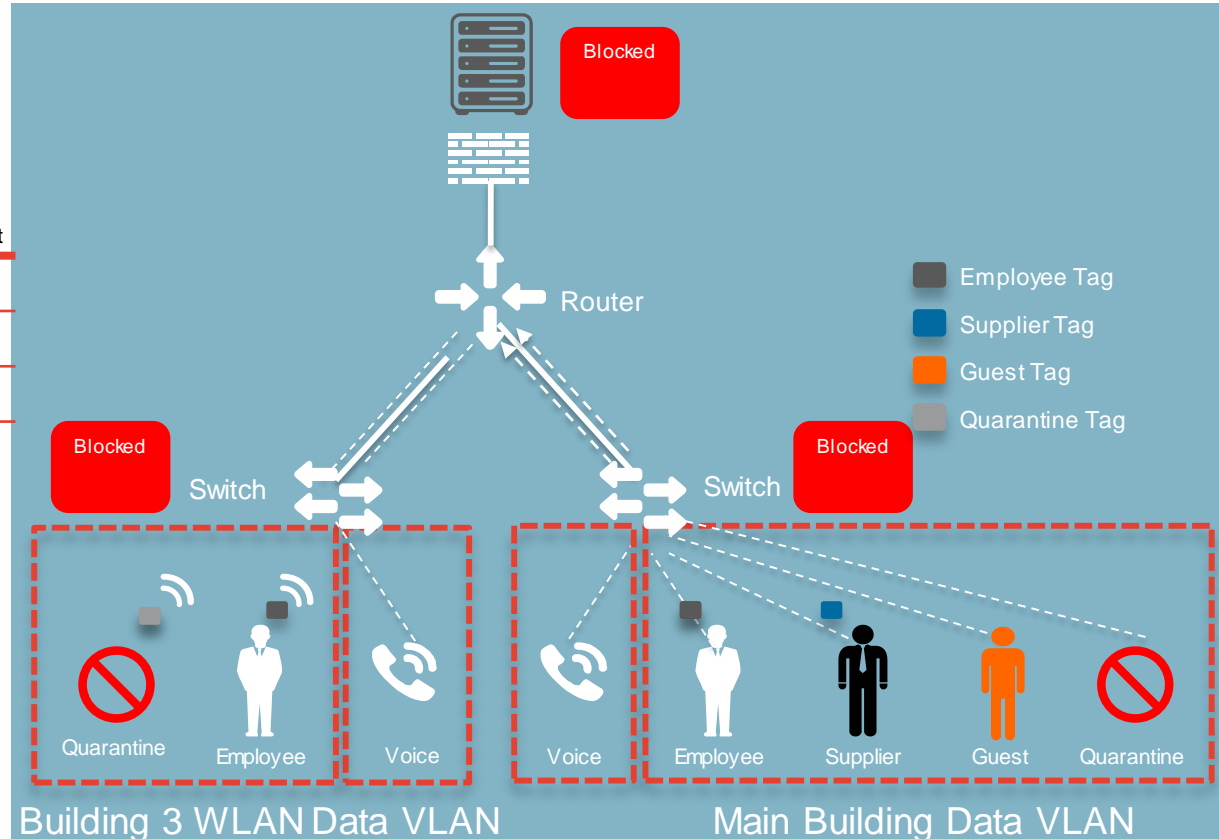
# Agenda



# Campus Segmentation

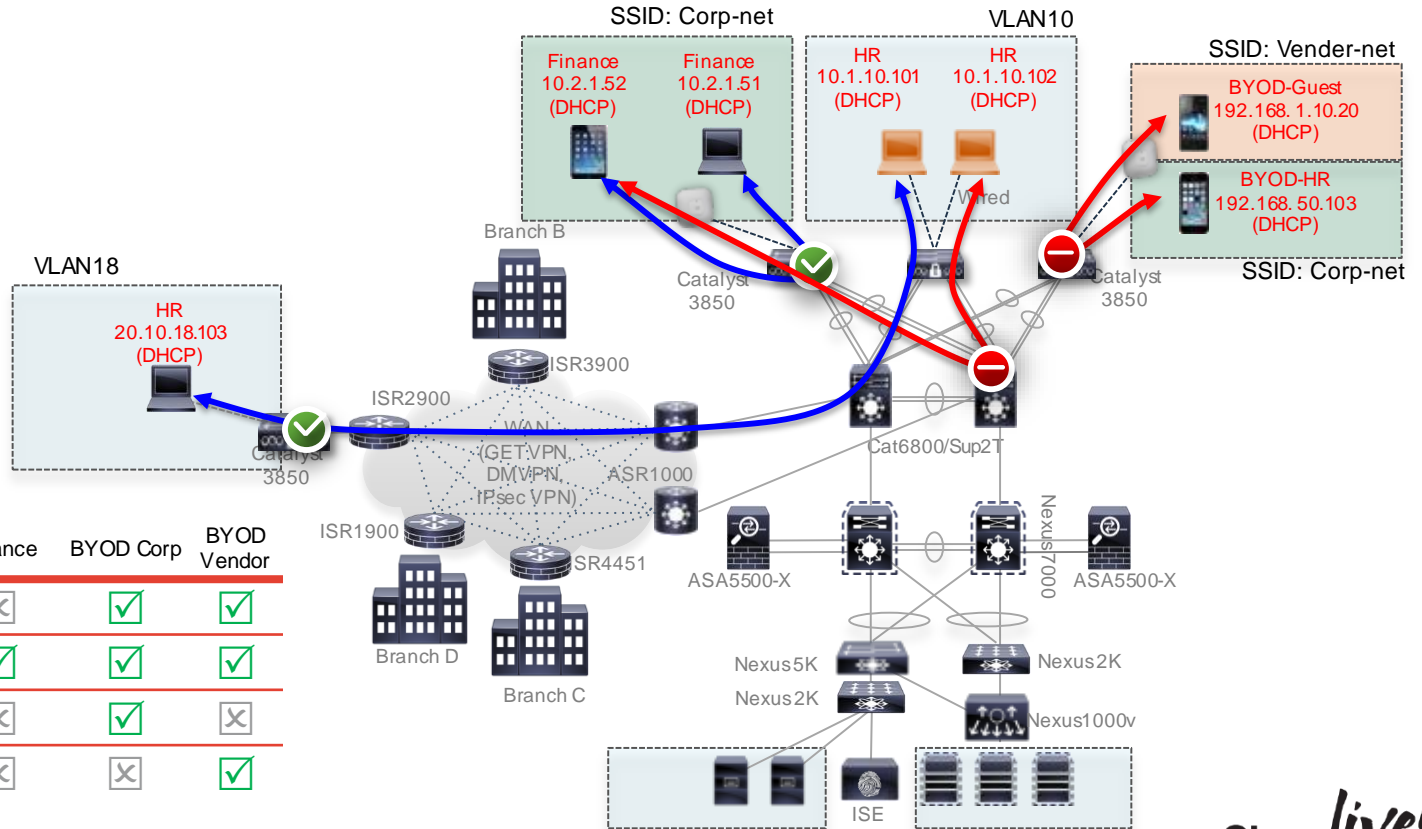
Policy:

	Employee	Supplier	Data centres	Internet
Employee	✓	✓	✓	✓
Supplier	✓	✗	✗	✓
Guest	✗	✗	✗	✓
Quarantine	✗	✗	✗	✗



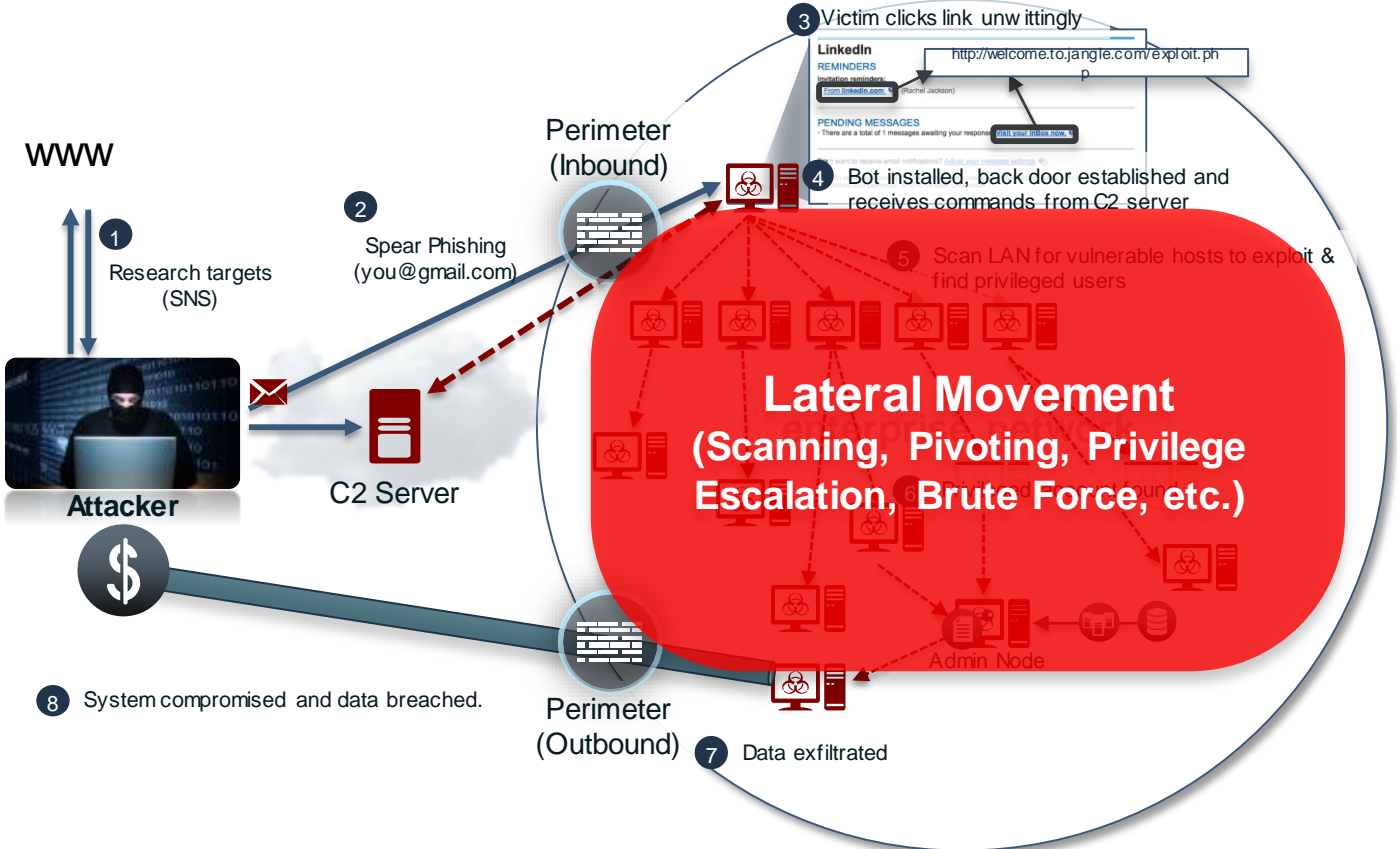


# Campus and Branch Segmentation

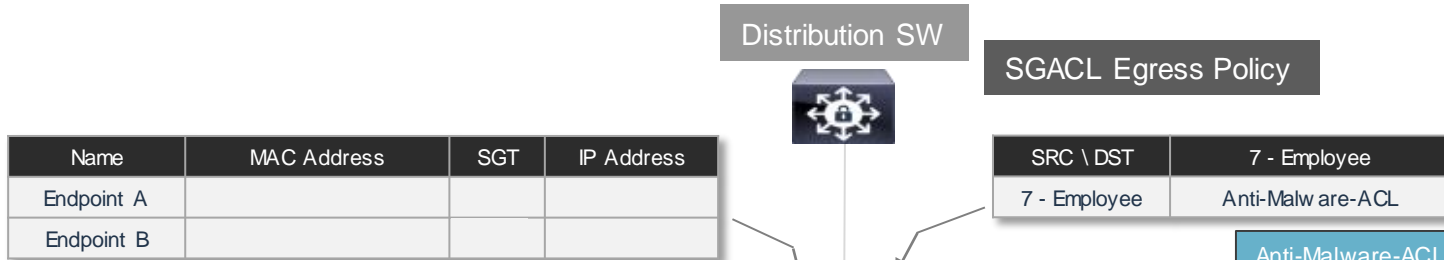


	HE	Finance	BYOD Corp	BYOD Vendor
HR	✓	✗	✓	✓
Finance	✗	✓	✓	✓
BYOD-Corp	✗	✗	✓	✗
BYOD-Vendor	✗	✗	✗	✓

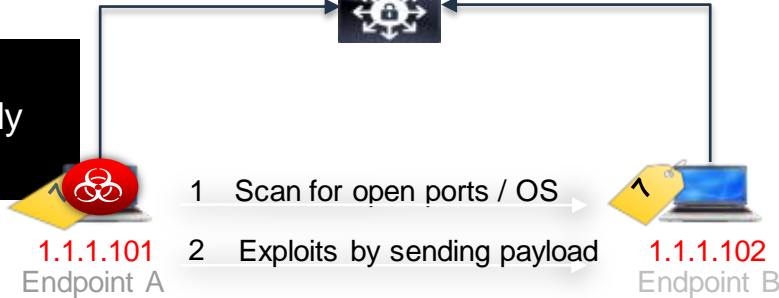
# Lateral Movement



# Restricting Lateral Movement



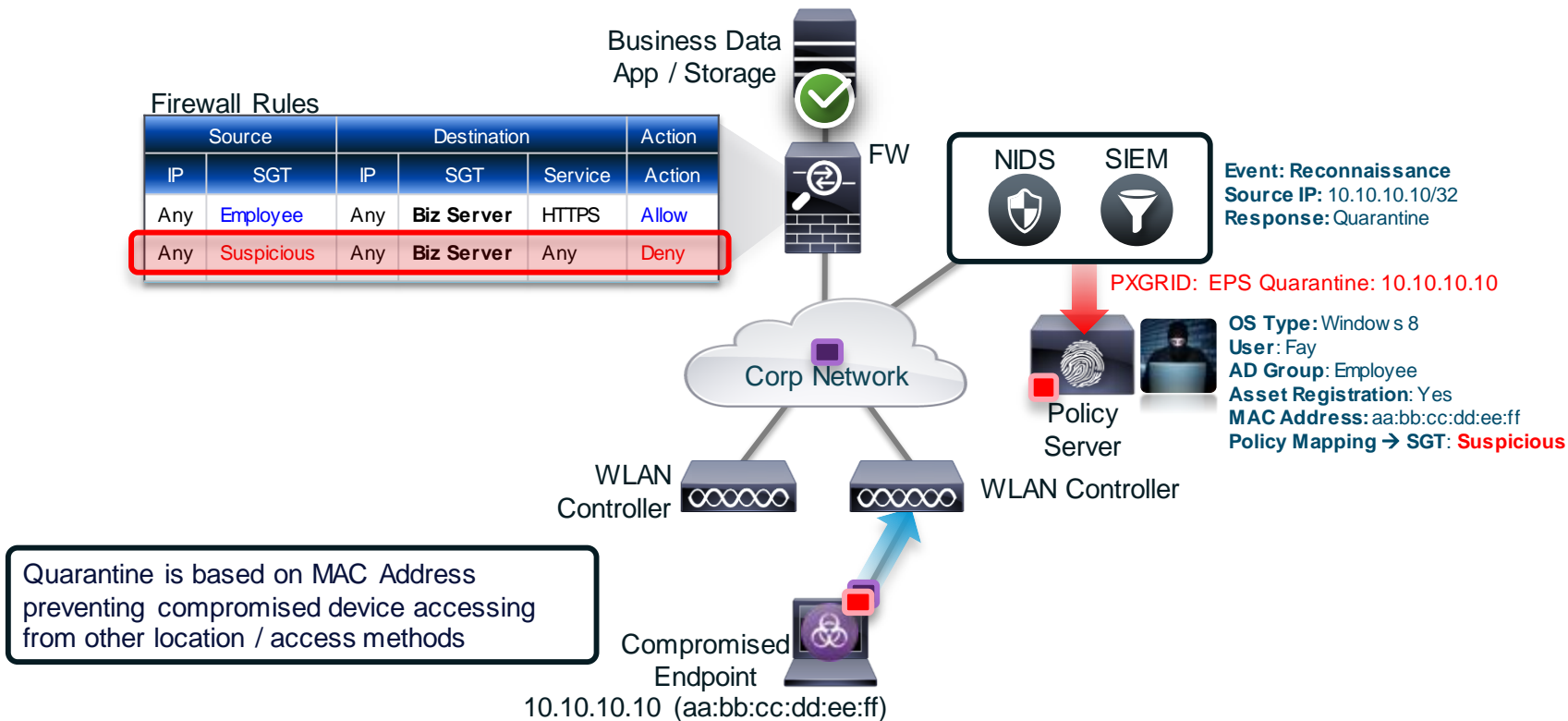
SGACL for SGT 7 is applied statically on switch or dynamically downloaded from ISE.



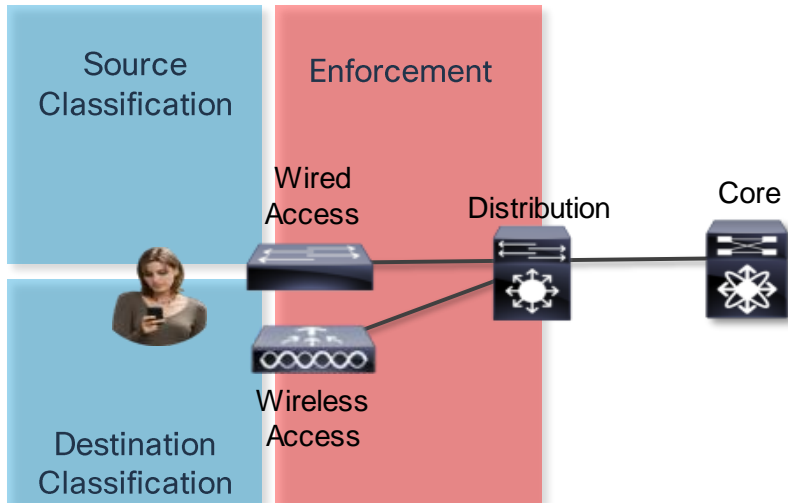
```

Anti-Malware-ACL
deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
deny tcp src dst eq 443
deny tcp src dst eq 22
deny tcp src dst eq pop3
deny tcp src dst eq 123
deny tcp match-all -ack +fin -psh -rst -syn -urg
deny tcp match-all +fin +psh +urg
permit tcp match-any +ack +syn
    
```

# Acting on Potentially Compromised Hosts



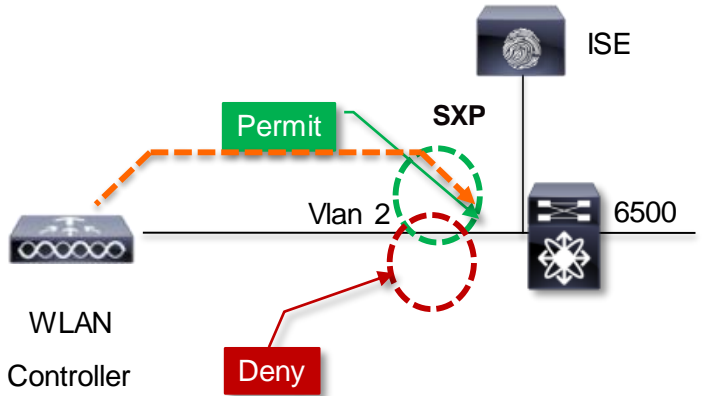
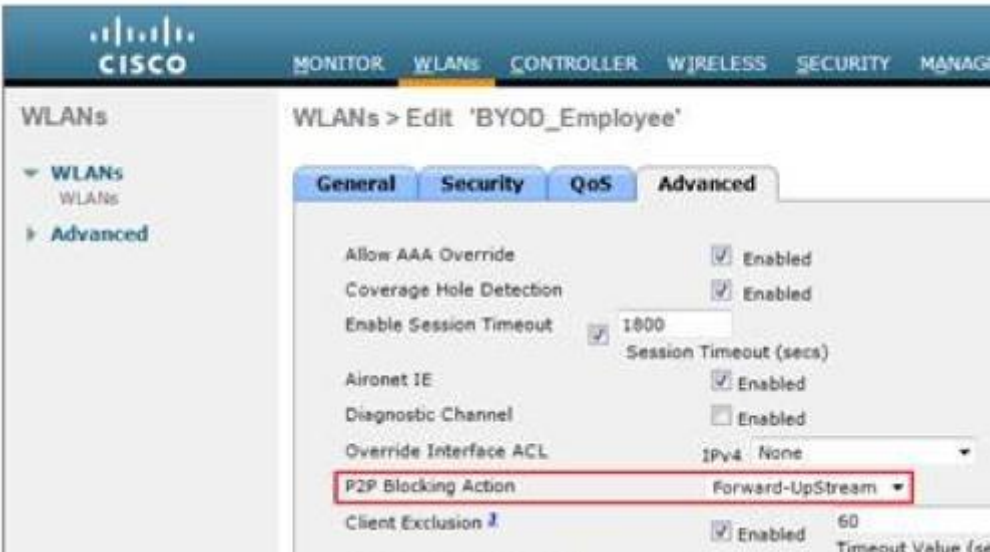
# Campus Segmentation



SGACL segmentation available on :-

- Catalyst 3560-X, 3750-X
- Catalyst 3650, 3850
- Catalyst 4500E S7E, S8, 4500X
- Catalyst 6500(2T)/6800
- WLC 5760

# Implementing Wireless User – User Policy Enforcement



- Apply user-user policies as defined in ISE on traffic from the WLC

```
interface Vlan2
ip local-proxy-arp
ip route-cache same-interface
!
cts role-based enforcement
cts role-based enforcement vlan-list 2
```

# WLAN Support Summary

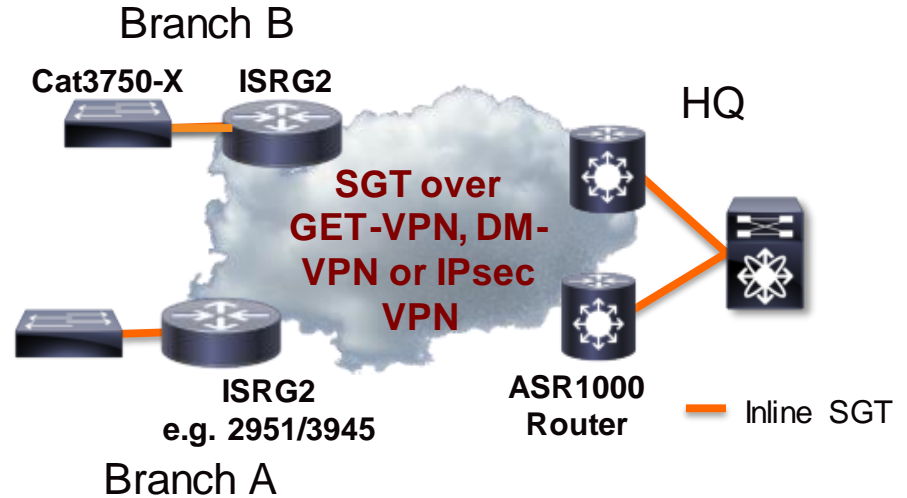


Deployment Mode	Controller Platforms	TrustSec Support	Release
Centralised AireOS	2504, 5508 WiSM2	SXP	7.4 onwards
Centralised IOS	5760	SGT, SGACL SXP	IOS XE 3.3.0 SE
Converged Access IOS	3850, 3650	SGT, SGACL SXP	IOS XE 3.3.0 SE
FlexConnect – locally switched SSIDs	5508, WiSM2 8510, 7510	None - use VLAN assignments + VLAN- SGT mappings	
FlexConnect – Centrally switched SSIDs	5508, WiSM2	SXP	8.0



# Branch Segmentation/Inline Tagging Across WAN

- Inline tagging across WAN -
  - IPsec, DM-VPN, GET-VPN
- Inline tagging on built-in ISRG2 & ASR 1000 Ethernet interfaces (all except 800 series ISR)



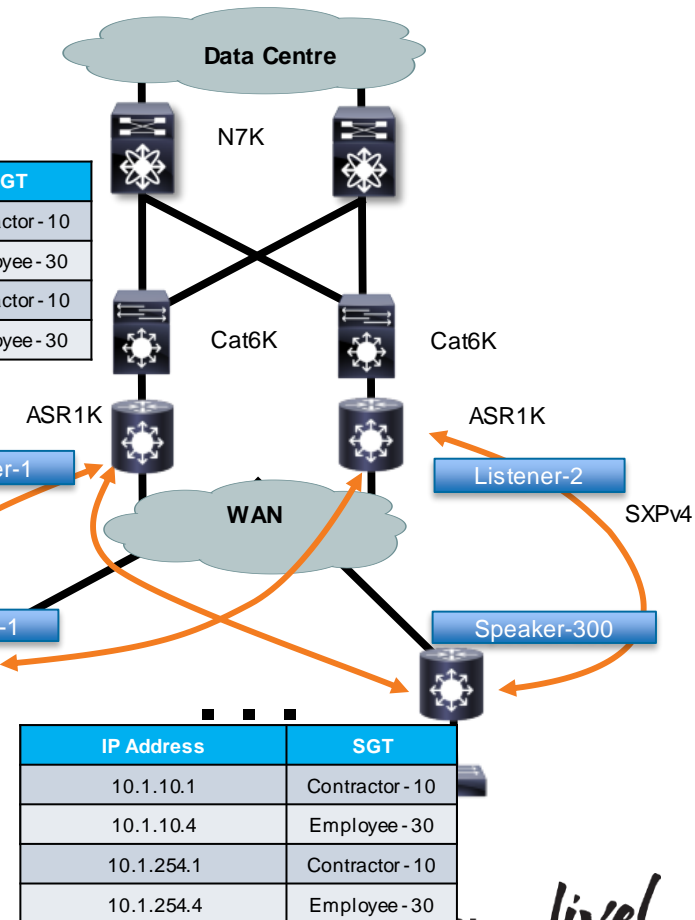
- Can also use SGT-aware Zone-based Firewall in branch and DC WAN edge for reasons like PCI compliance
- SGT is used only as a source criteria only in ISR G2 Zone-Based Firewall

# Branch Segmentation/SXP WAN

- Bidirectional SXP with Loop Detection available now:
  - ISRG2 15.4(1)S
  - ASR1000/ISR4k/CSR XE 3.11
- Allows ASR1000 to be an IP/SGT relay from remote to remote
- SXP is a full replication model – each remote router will learn all IP/SGT bindings

IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30

IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30



# Bidirectional SXP WAN Scaling

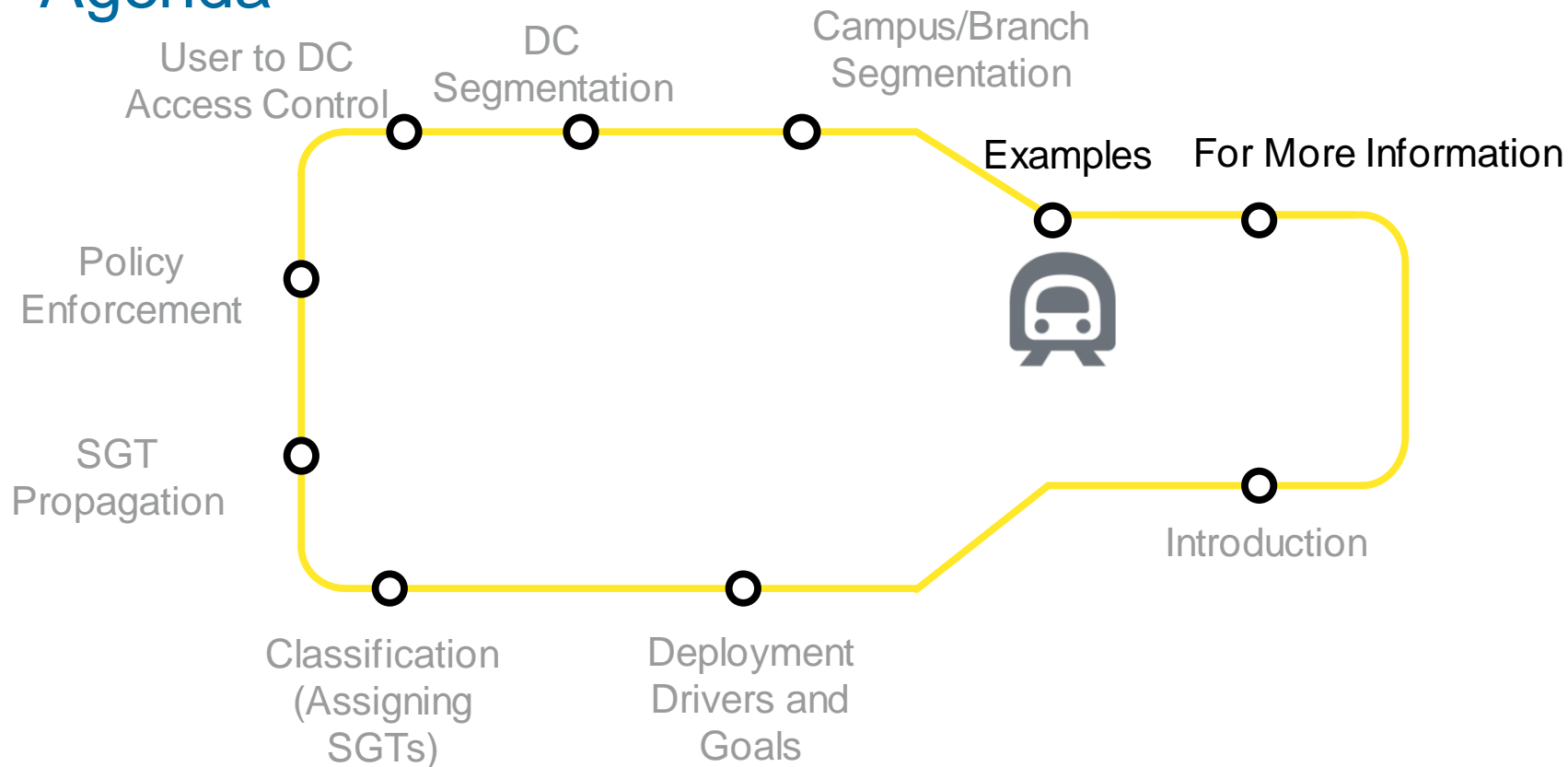


- From previous slide - SXP is a full replication model – each remote router will learn all IP/SGT bindings with this approach
- [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_cts/configuration/xs-3s/asr1000/sec-usr-cts-xe-3s-asr-1000-book/cts-bi-sxp.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xs-3s/asr1000/sec-usr-cts-xe-3s-asr-1000-book/cts-bi-sxp.html)

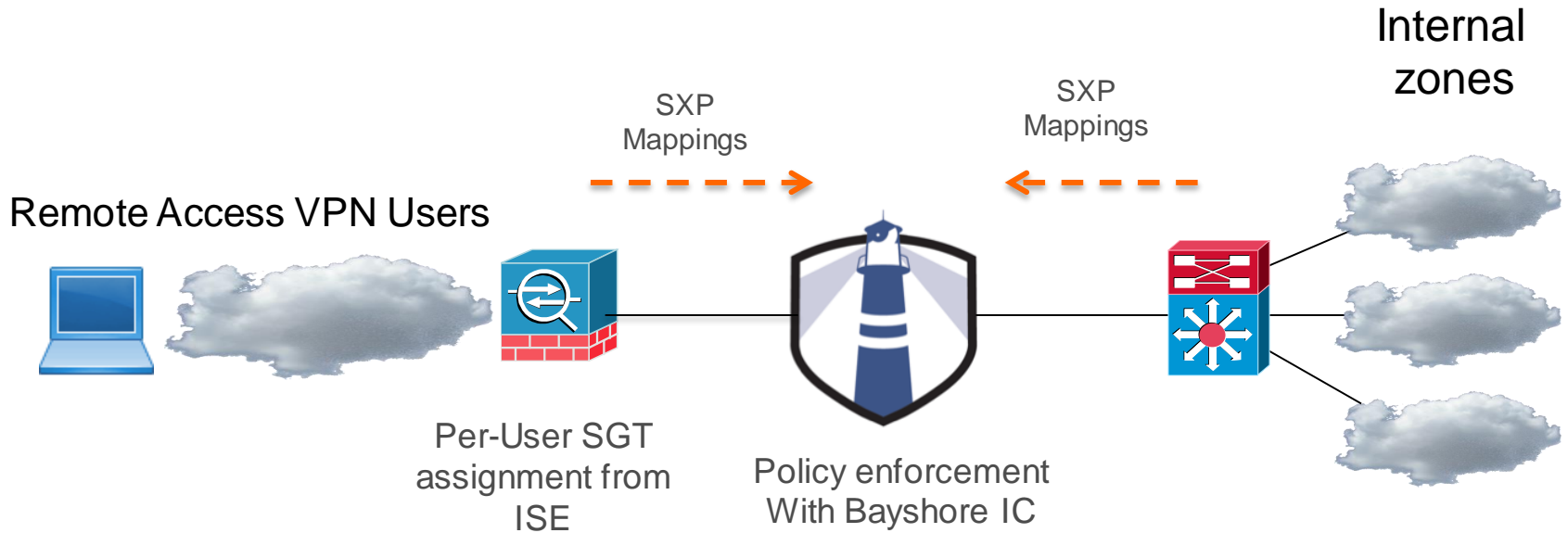
**Table 1 Scalability Numbers for SXP Connections and IP SGT Bindings**

Platform	Unidirectional SXP Connections (Speaker only/Listener only)	Bidirectional SXP Connections	IP SGT Bindings
CSR 1000v	900	450	135K
ISR 4400	1800	900	135K
ASR 1000	1800	900	180K
ISR 2900, ISR 3900	250	125	<ul style="list-style-type: none"><li>○ 180K for unidirectional SXP connections</li><li>○ 125K for bidirectional SXP connections</li></ul>

# Agenda



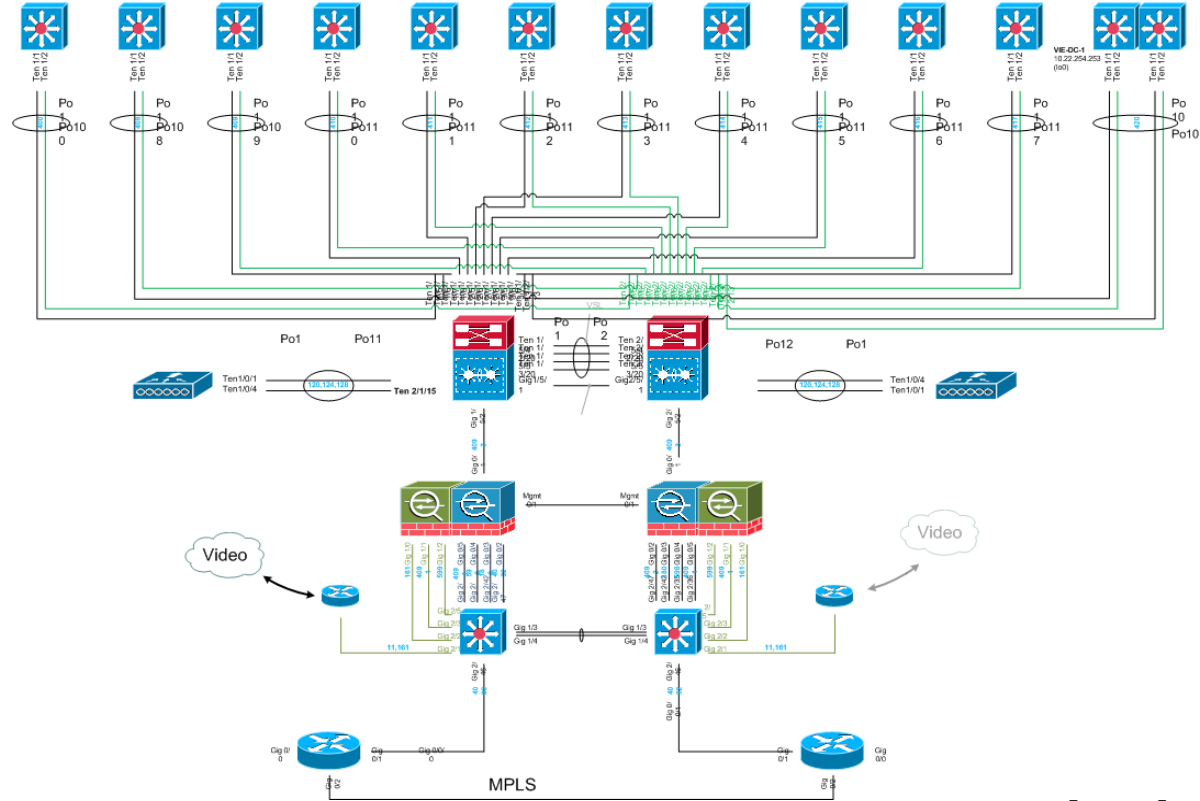
# Partner/Extranet Access - Manufacturing



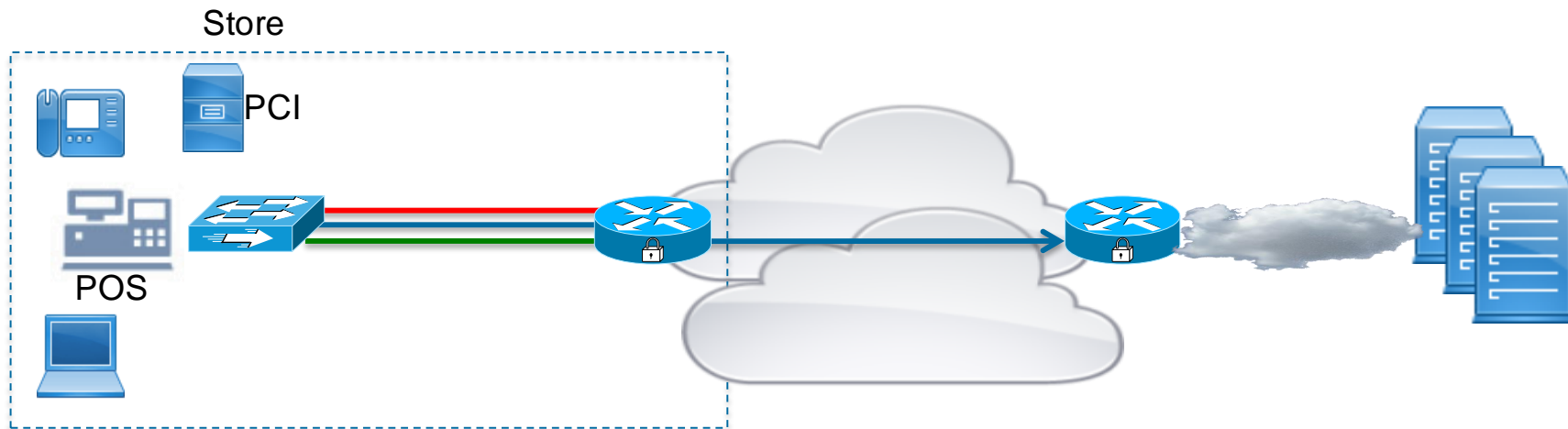
- Bayshore IC allows different industrial protocols to each internal zone

# Manufacturing Customer

- HQ location
- User segmentation across campus
  - Cat 4500 Sup7
  - WLC 5760
- User to DC Access Control
  - Nexus 1000v
  - ASA 5585-X



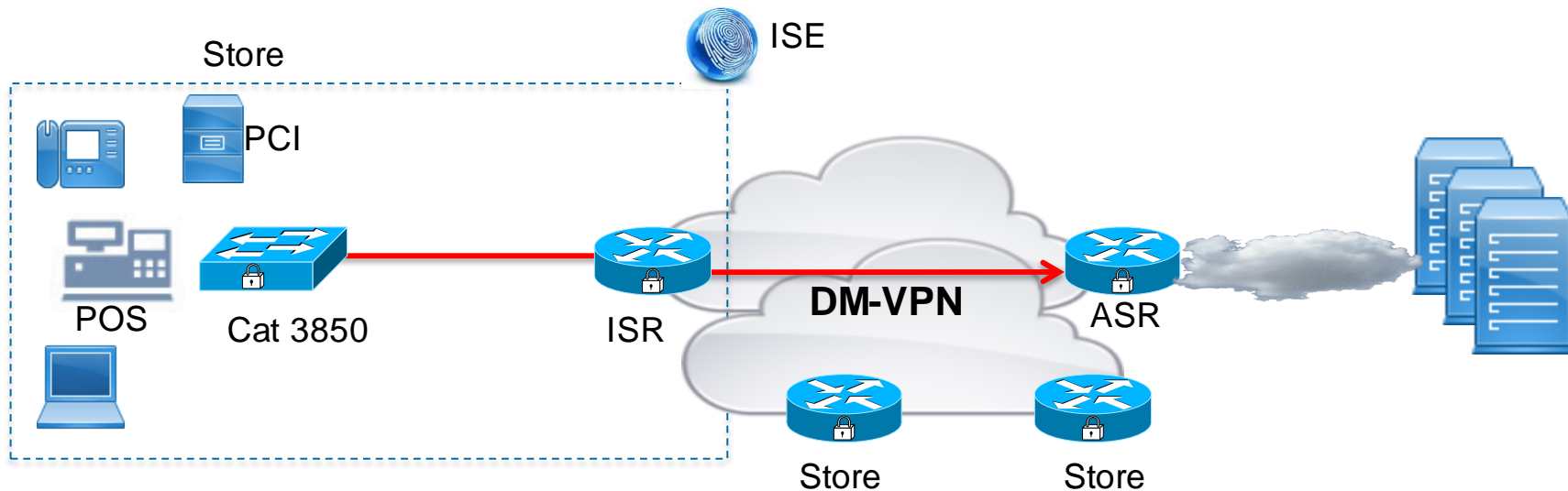
# Retail Customer



- Existing segmentation scheme used up to 25 subnets/VLANs in stores
- Segmentation for reasons including PCI
- Additional segments would break route summarisation

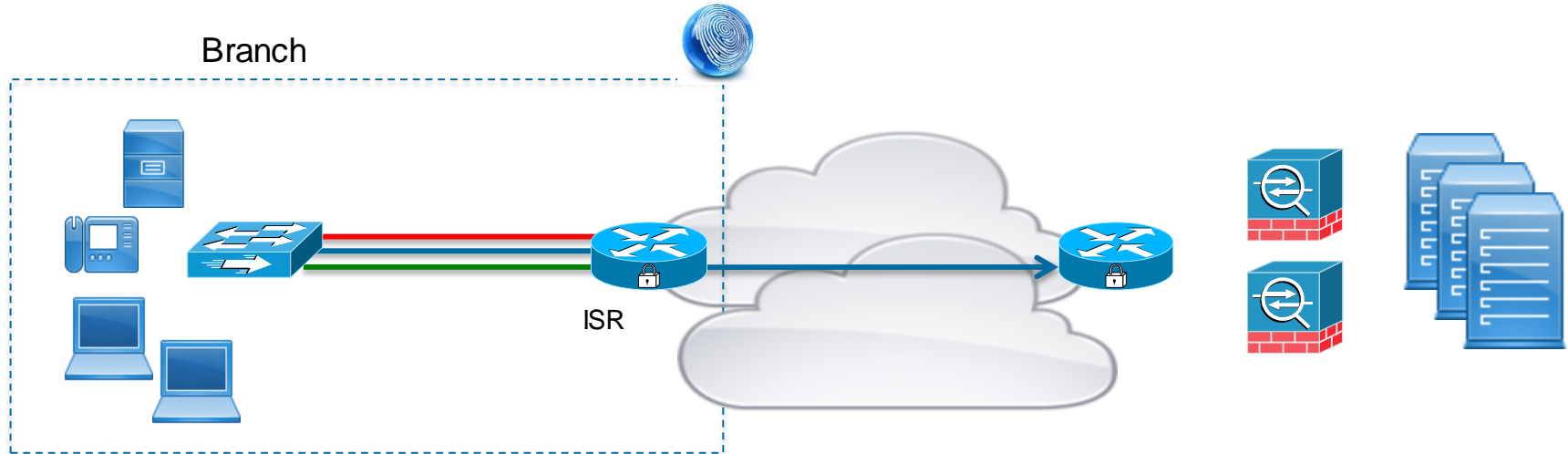


# Retail Customer



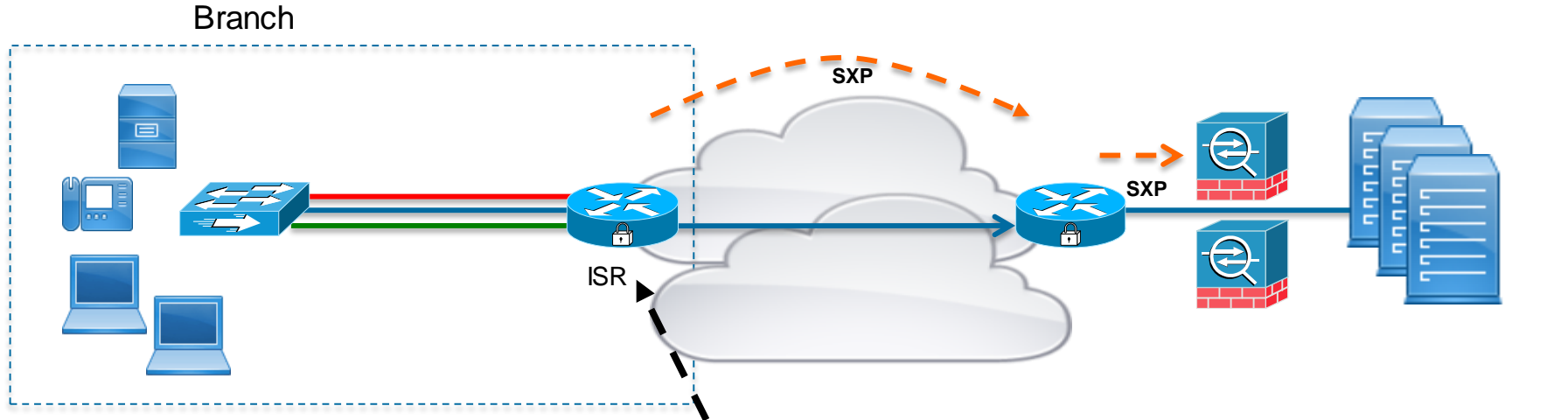
- Catalyst 3850 allowed SGACL segmentation in stores
- No new VLANs/segments required
- DM-VPN used to carry SGT inline between stores

# Financial Branch - Before



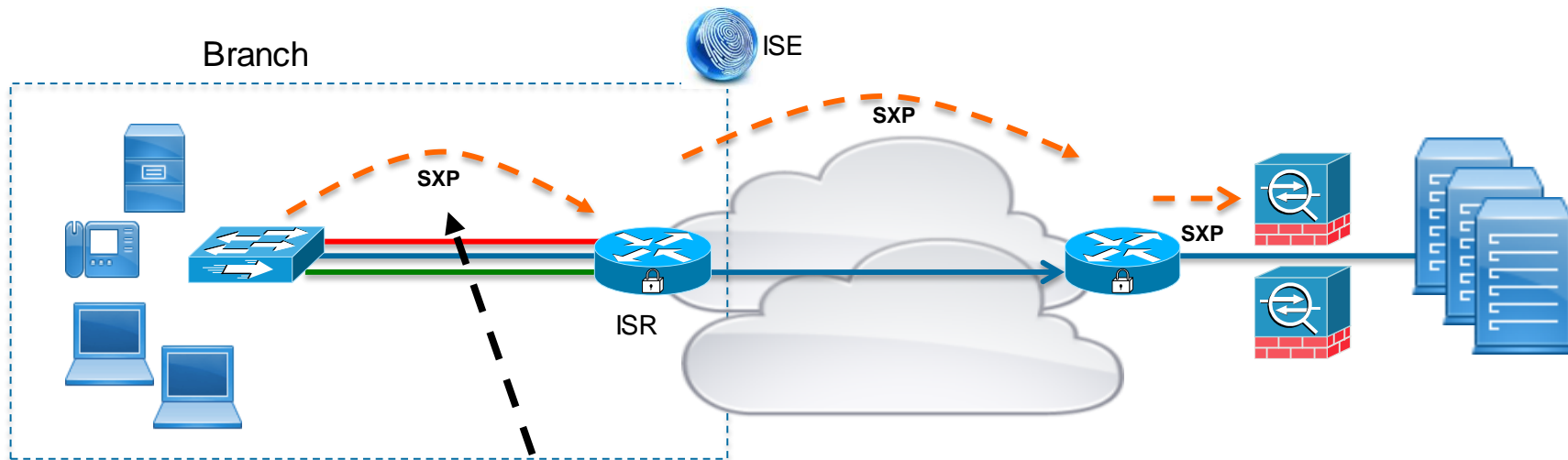
- Existing network had 4 subnets/VLANs per branch
- No use of 802.1X
- Extensive IP-based rules in DC Firewalls

# Financial Branch



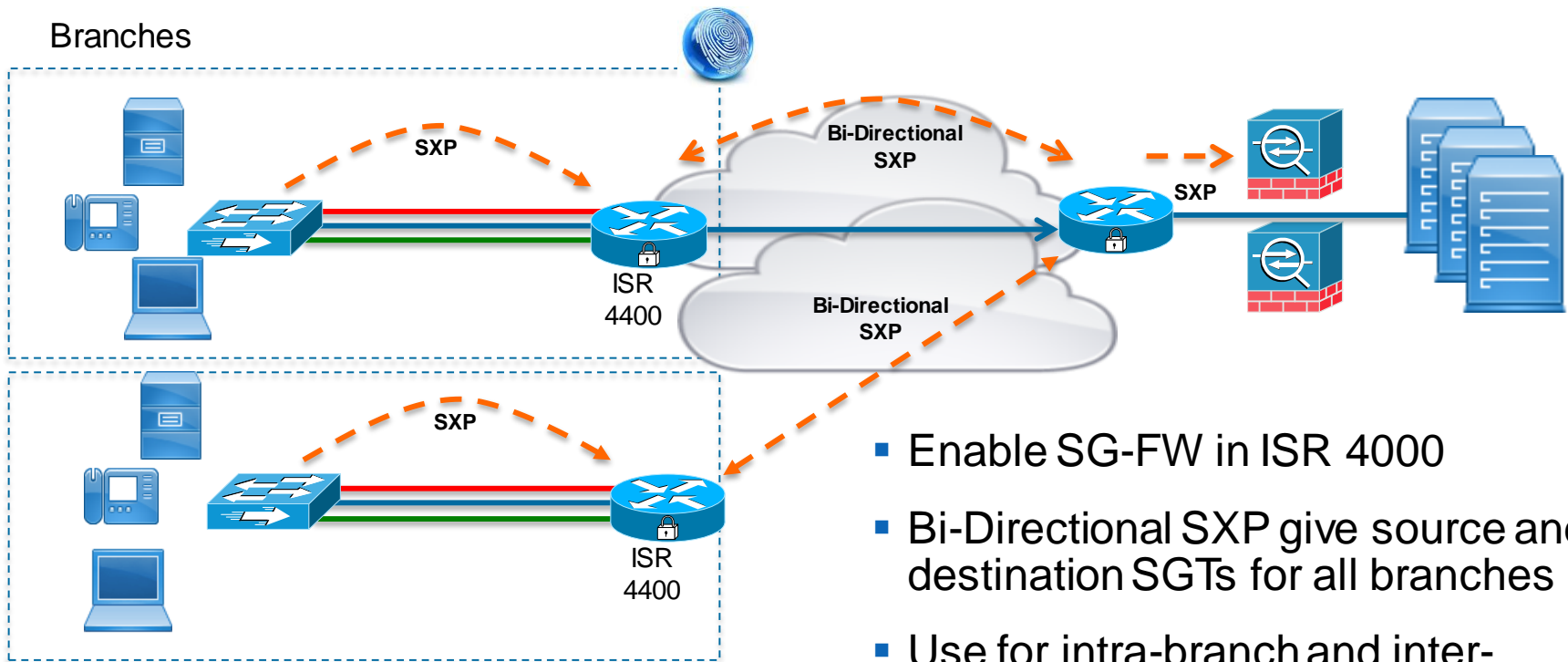
- L3 Interface-SGT maps
  - Each subnet/VLAN gets an SGT, IP-SGT bindings created
  - Same SGTs in every branch
- Rules in DC Firewalls based on simple categories

# Financial Branch



- Enable 802.1X passively
- Enable SXP in access switch (Switches only capable of SXP)
- L3 Interface-SGT maps still in place
- Bindings from SXP take priority over static SGTs
- Coarse-grained roles from VLAN mappings
- AND Fine-grained roles from authentication

# Financial Branch – Possible Future



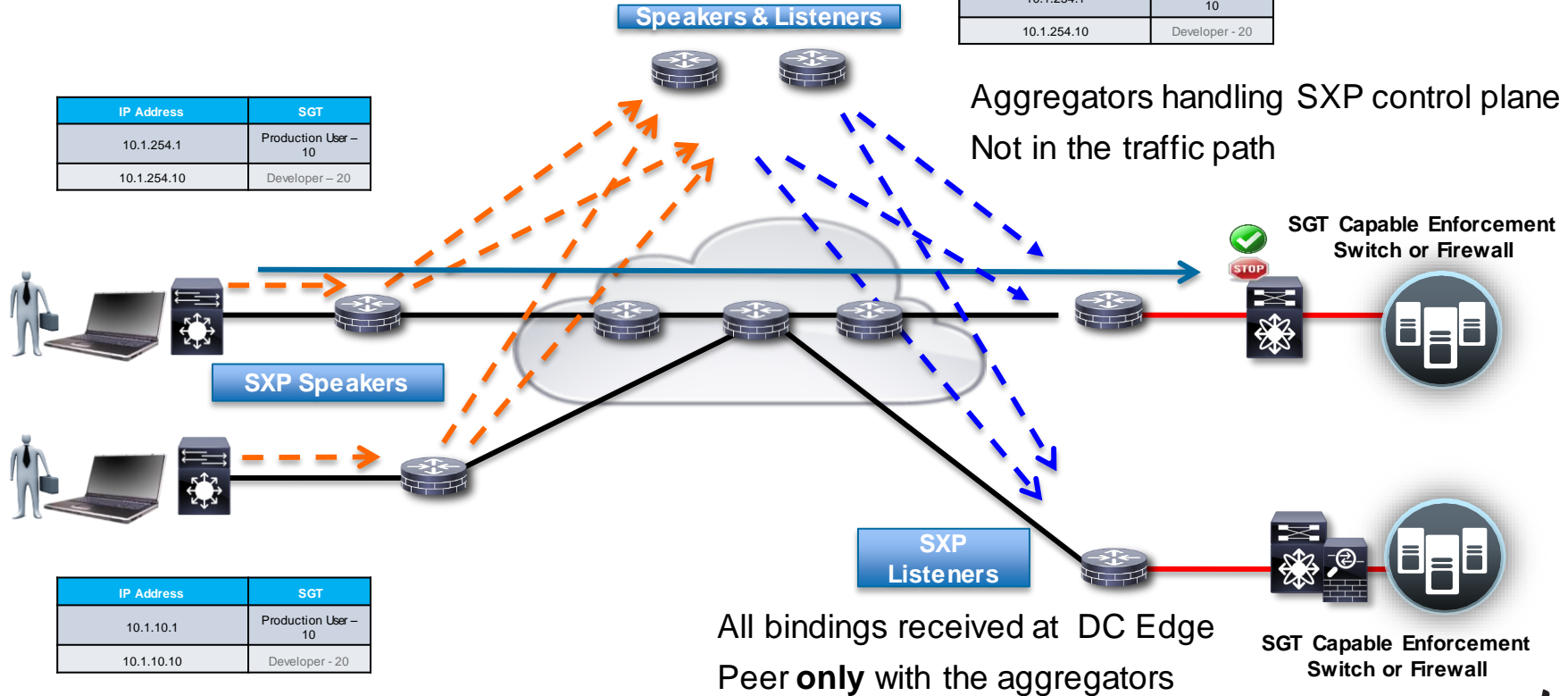
- Enable SG-FW in ISR 4000
- Bi-Directional SXP give source and destination SGTs for all branches
- Use for intra-branch and inter-branch policy enforcement - all based on same roles

# Financial Customer

IP Address	SGT
10.1.10.1	Production User - 10
10.1.10.10	Developer - 20
10.1.254.1	Production User - 10
10.1.254.10	Developer - 20

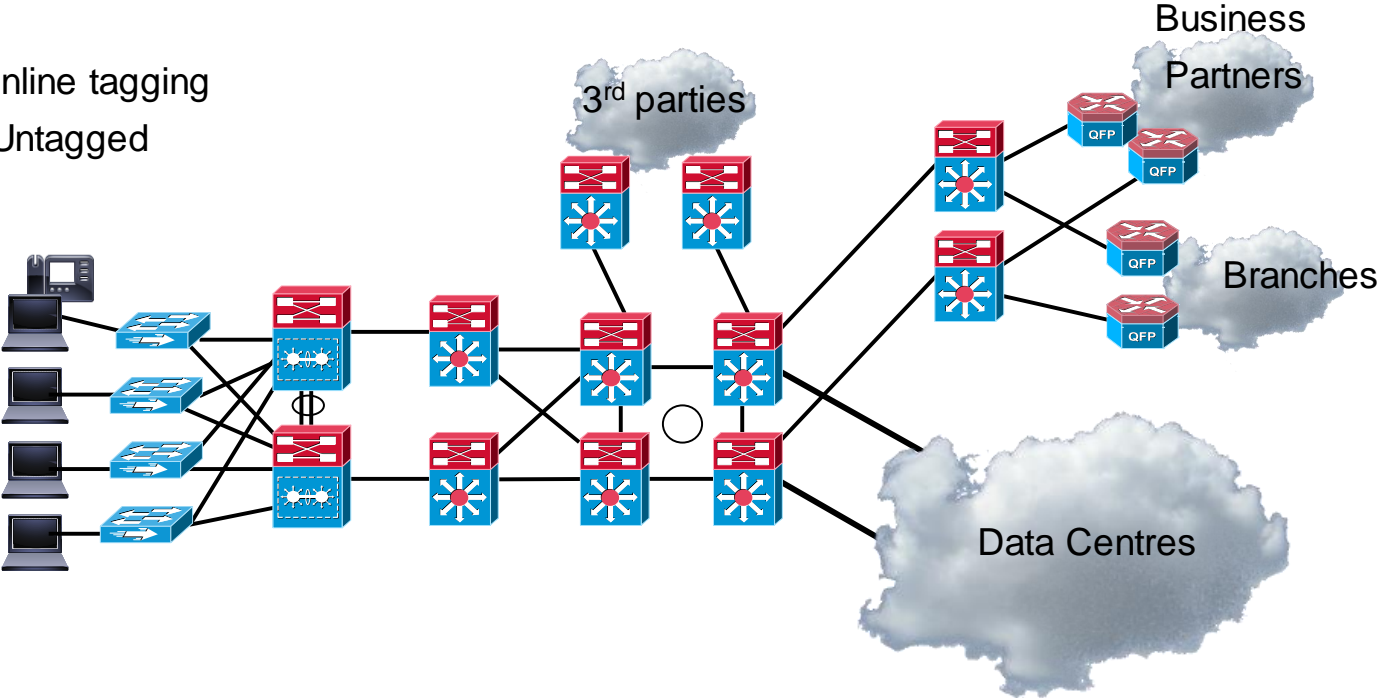
IP Address	SGT
10.1.254.1	Production User - 10
10.1.254.10	Developer - 20

IP Address	SGT
10.1.10.1	Production User - 10
10.1.10.10	Developer - 20



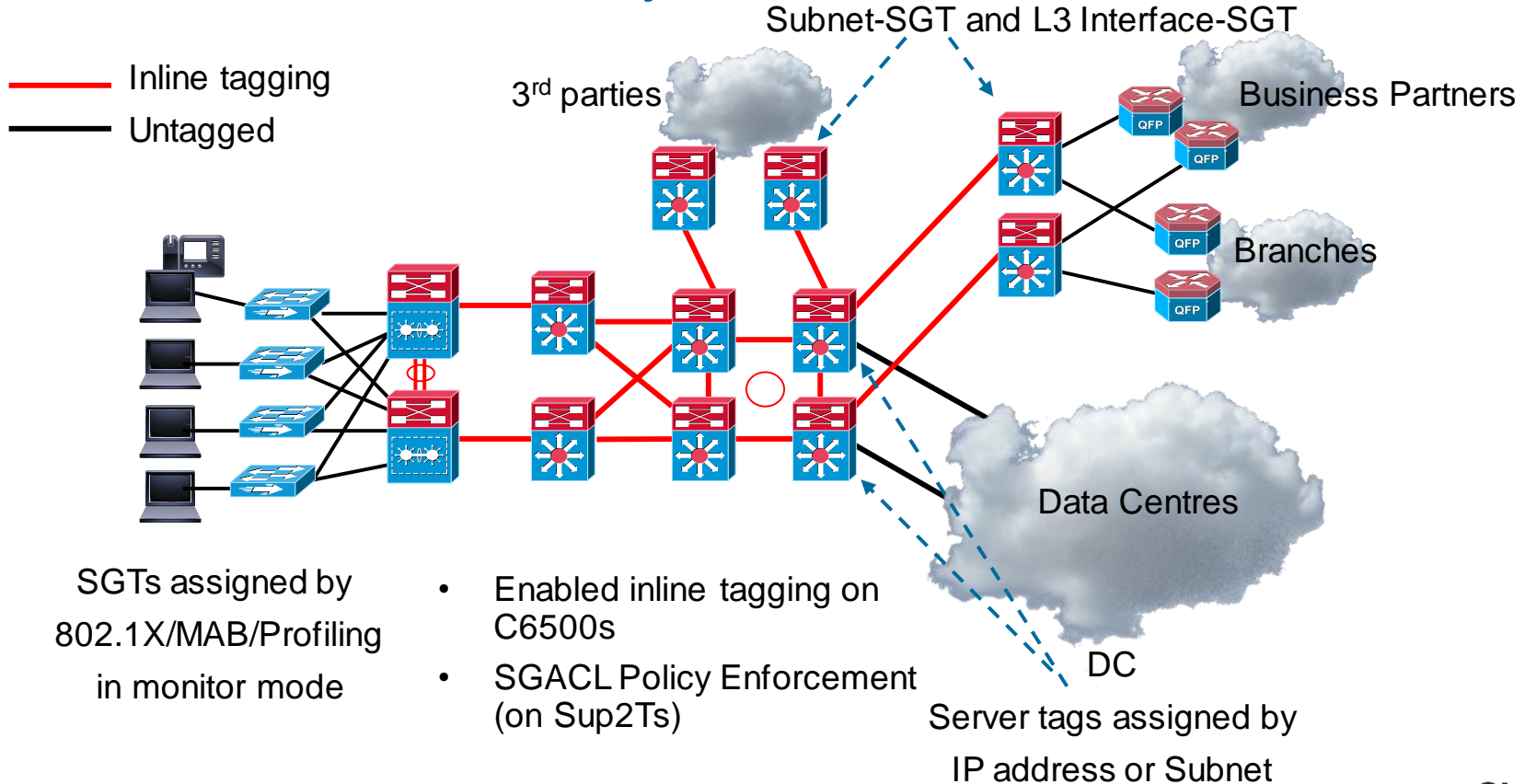
# Financial Case Study

— Inline tagging  
— Untagged

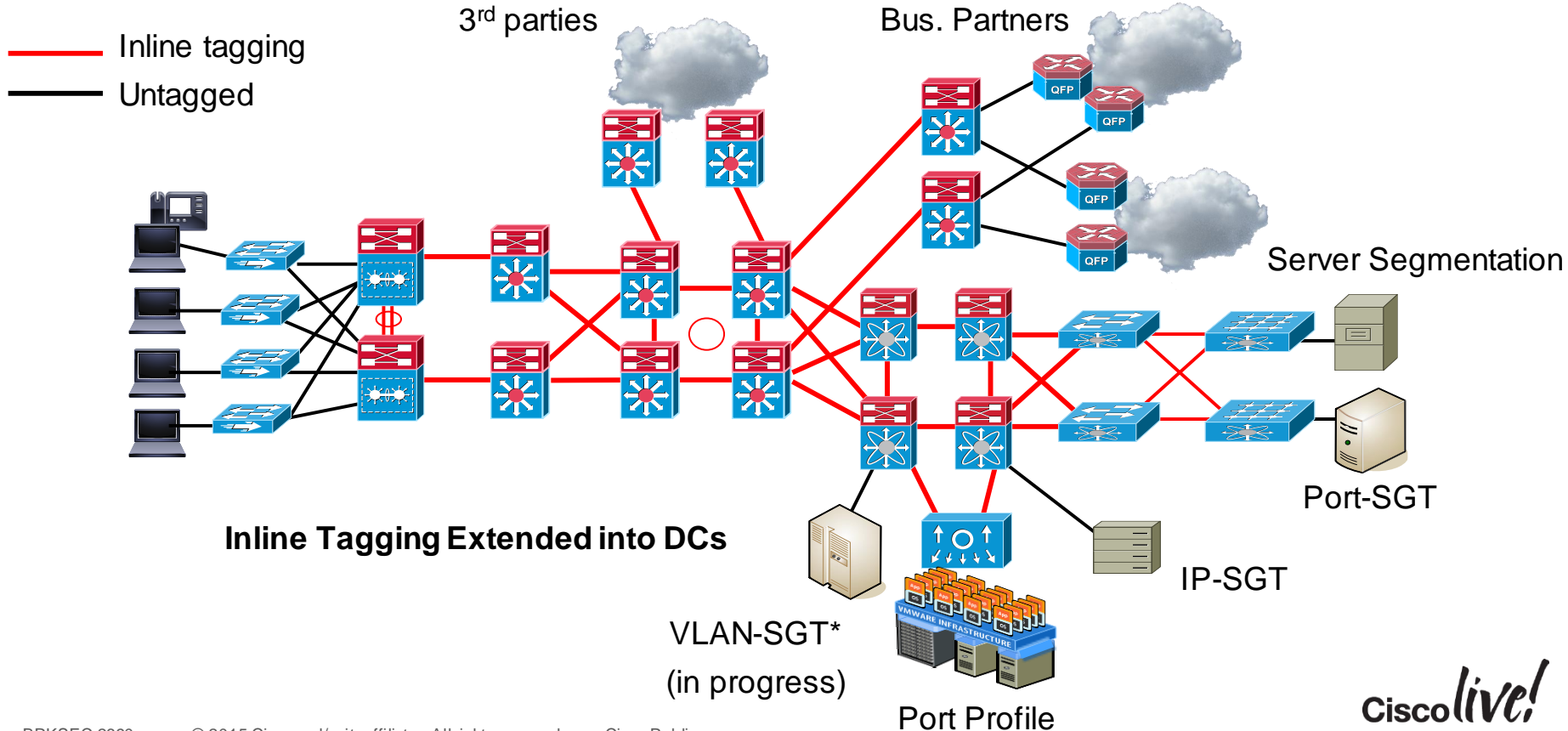




# Financial Case Study: Phase 1 User to DC Access

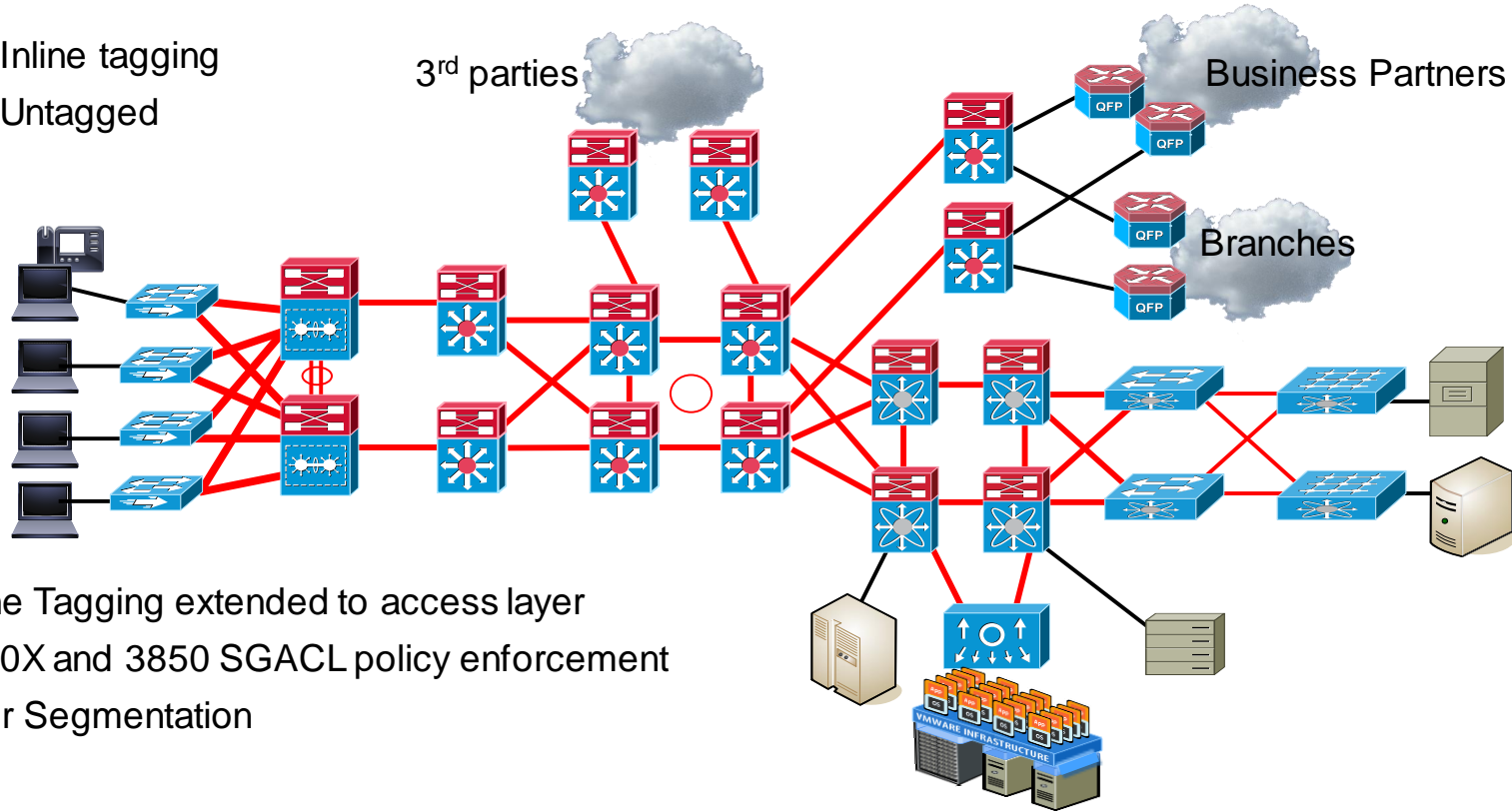


# Financial Case Study: Phase 2 DC Segmentation



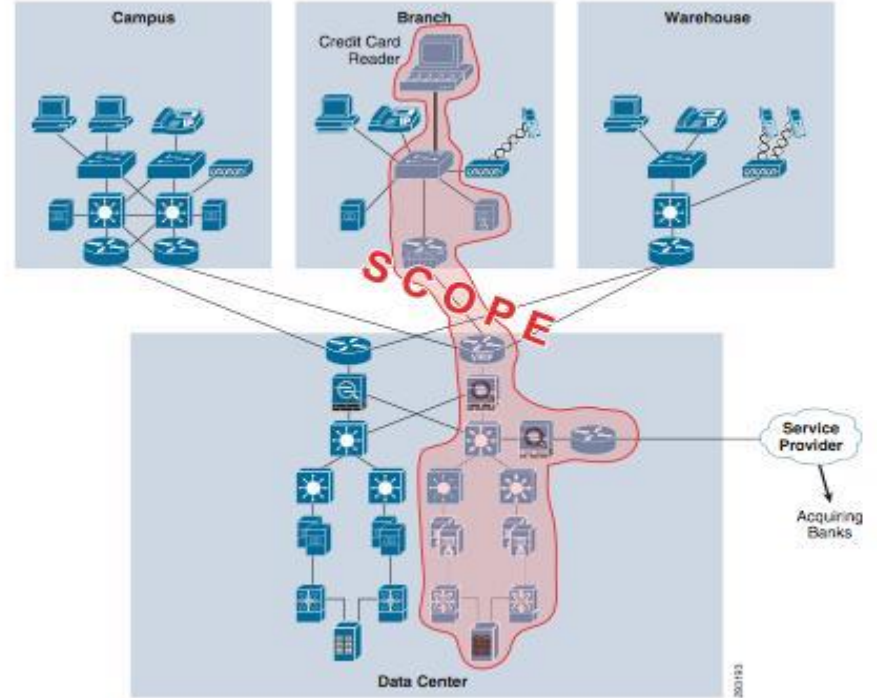
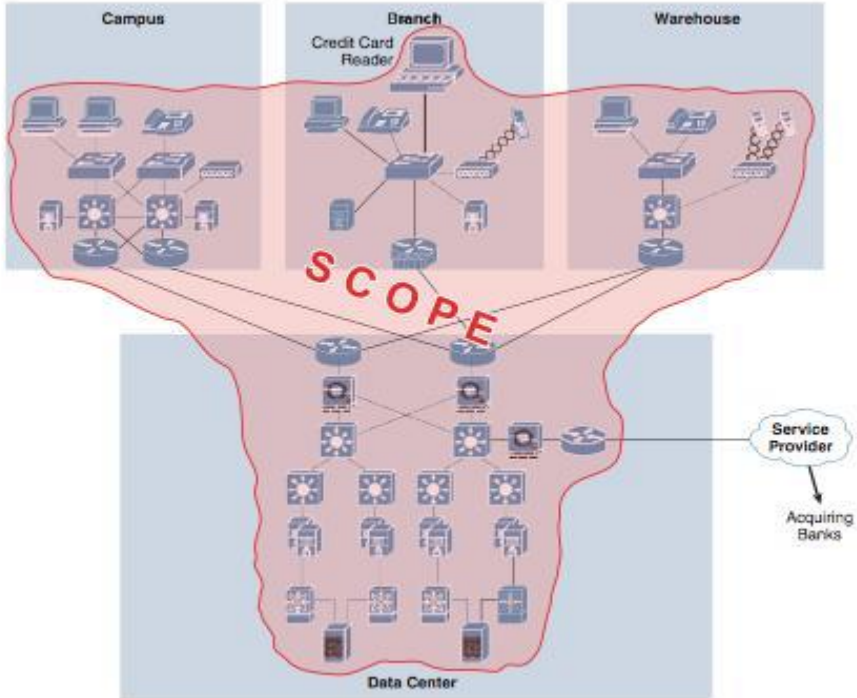
# Financial Case Study: Phase 3 Campus Segmentation

— Inline tagging  
— Untagged



Inline Tagging extended to access layer  
3750X and 3850 SGACL policy enforcement  
User Segmentation

# PCI Compliance – Scope Reduction



# 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.

[http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/trustsec\\_pci\\_validation.pdf](http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/trustsec_pci_validation.pdf)

# PCI Compliance Branch and Data Centre

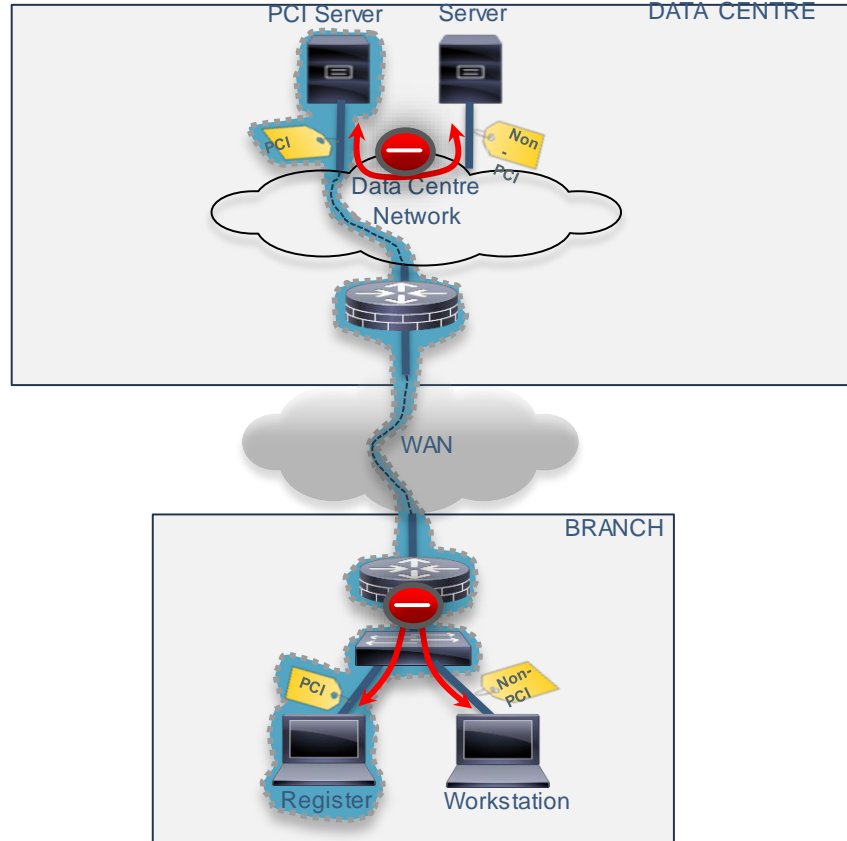


Legend:

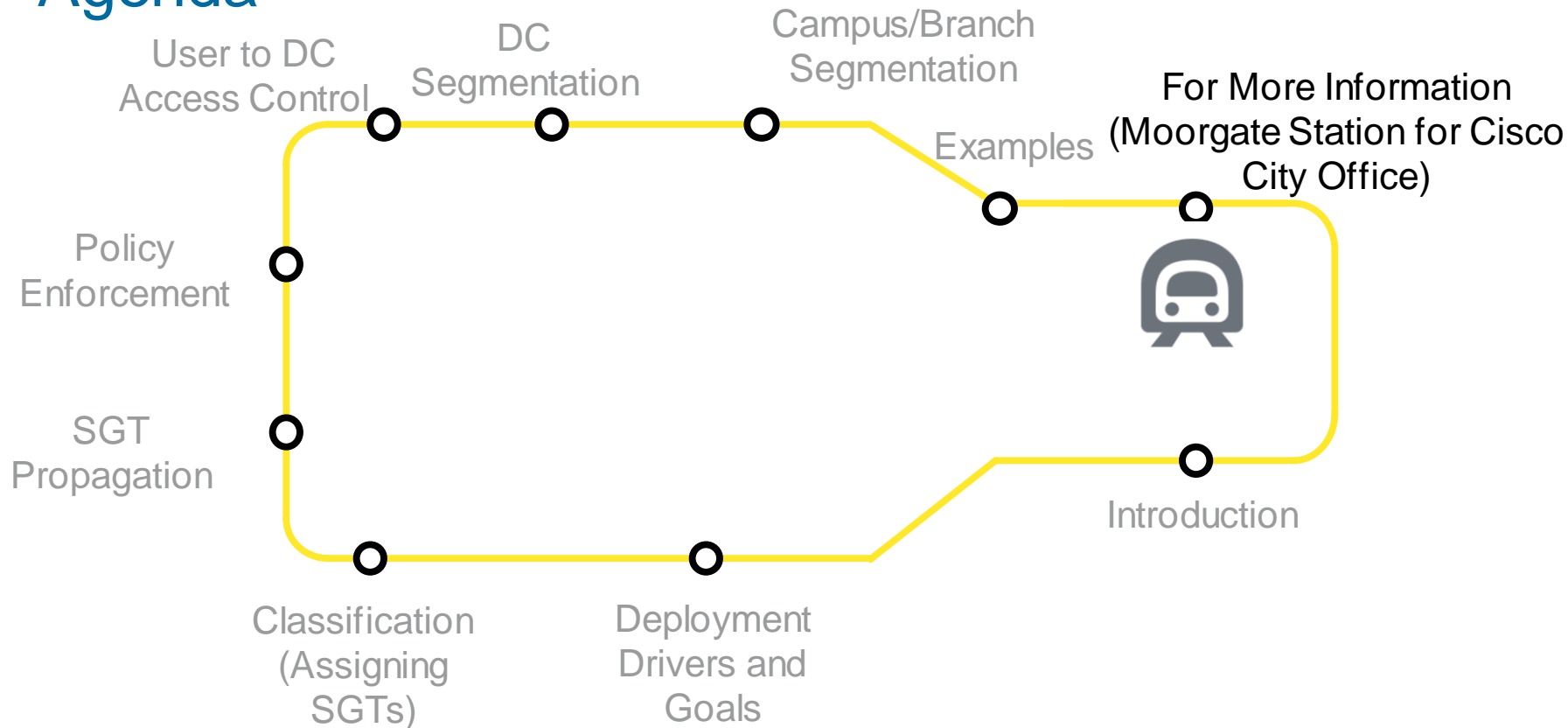
Segmentation enforcement



PCI scope



# Agenda





# For More Information

- For everything TrustSec-related:-
  - <http://www.cisco.com/go/trustsec>
- TrustSec platform support matrix
  - [http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec\\_matrix.html](http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html)
- Case studies
  - <http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/customer-case-study-listing.html>
- Securing BYOD with TrustSec Security Group Firewalling
  - <http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/white-paper-c11-732290.html>
- PCI Scope Reduction with Cisco TrustSec – QSA (Verizon) Validation:
  - [http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/trustsec\\_pci\\_validation.pdf](http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/trustsec_pci_validation.pdf)



# Gartner on TrustSec

“logical source and destination security groups are more flexible, are easier to maintain and reduce runtime overhead in the network’s switching fabric.”

“There is much to like about Cisco’s ambitious and innovative initiative....”

“Cisco has made great strides in integrating support for the TrustSec framework across its product lines”

“Flexibility to Segregate Resources Without Physical Segmentation or Managing VLANs”

“Reduction in ACL Maintenance, Complexity and Overhead”

<http://blogs.cisco.com/security/gartners-perspective-on-cisco-trustsec>



## Cisco TrustSec Deployed Across Enterprise Campus, Branch and Data Center Networks

Software-defined segmentation with Cisco TrustSec



### Issue 1

- 2 Introduction
- 3 Research from Gartner: Maturing Support for Cisco's TrustSec Framework
- 14 TrustSec Summary
- 15 Recent Developments
- 15 Customer Case Study
- 15 Cisco Validated Designs

# Summary

- TrustSec is easy to enable and manage
  - Can start with specific use-cases with minimal platform dependencies
  - Non-disruptive deployments; SGACL enforcement can be enabled incrementally and gradually via the policy matrix
- Operational benefits
  - SGACLs avoid VLAN/dACL efforts and admin
  - Security policy managers/auditors do not need to understand the topology or the underlying technology to use the policy matrix
  - Firewall rule simplification and OpEx reduction
  - Faster and easier deployment of new services



# Related Breakouts

- BRKSEC-3690 - Advanced Security Group Tags: The Detailed Walk Through
- BRKSEC-3697 - Advanced ISE Services, Tips and Tricks
- BRKSEC-2044 - Building an Enterprise Access Control Architecture Using ISE and TrustSec





Q & A

Cisco *live!*

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site  
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm



### Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. [www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)

**Cisco** *live!*





Thank you.

Cisco *live!*



**CISCO**