
TOMORROW starts here.
cisco
Cisco live!

Deploying Security Group Tags

BRKSEC-2690

Kevin Regan
Product Manager, TrustSec,
Secure Access & Mobility Product Group

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.

Introduction to Common Icons

Slide intended for your reference – may be very briefly covered

Identity Services Engine (ISE)

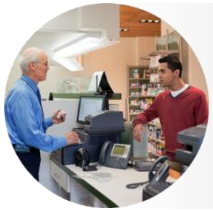
User authenticated by 802.1X, MAC auth-bypass or Web Auth

Agenda

- TrustSec SGT Overview and benefits
- SGT Classification
- SGT Propagation
- Policy Enforcement
- Use Cases
  - User to Data Centre Access Control
  - DC Segmentation
  - Campus and Branch Segmentation
- Case study
- Summary

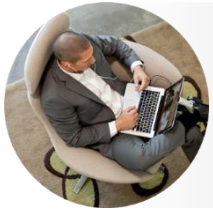
TrustSec SGT Overview

Business Drivers for Improving Security Policy



Meet Compliance Objectives

Authorise access to regulated apps to support compliance mandates



Increase Efficiency

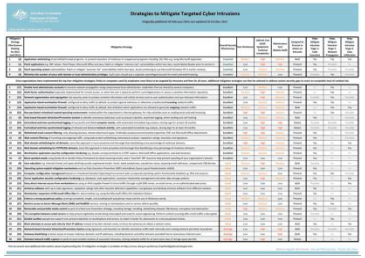
Streamline security processes and reduce OpEx

Improve Productivity

Enable secure access to new applications and services while managing risk

Improving Security..

Strategies
to mitigate APT



Australian Government
Department of Defence
Intelligence and Security

9	(5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator cred
10	(7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services
11	(6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a priv
12	(8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthori
13	(9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted ap
14	(10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's inter

http://www.asd.gov.au/infosec/top-mitigations/top35mitigations-2014-table.htm

TrustSec Security Group Tagging

Desired Policy

- Who can talk to whom
- Who can access protected assets
- How systems can talk to other systems

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

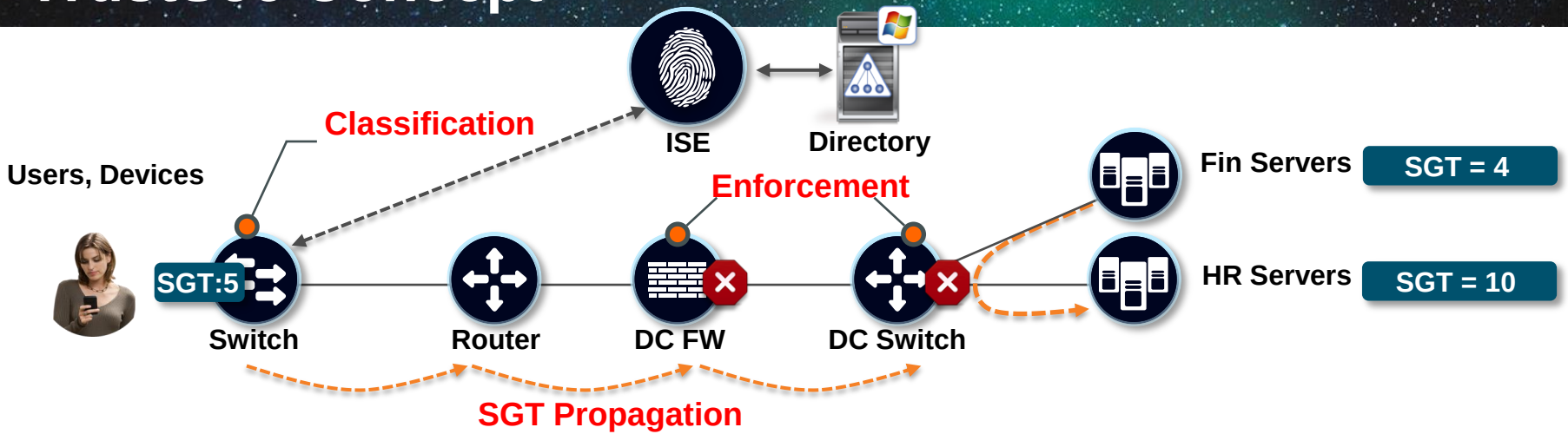
Simplified Access Management

Accelerated Security Operations

Consistent Policy

Flexible and Scalable Policy Enforcement

TrustSec Concept



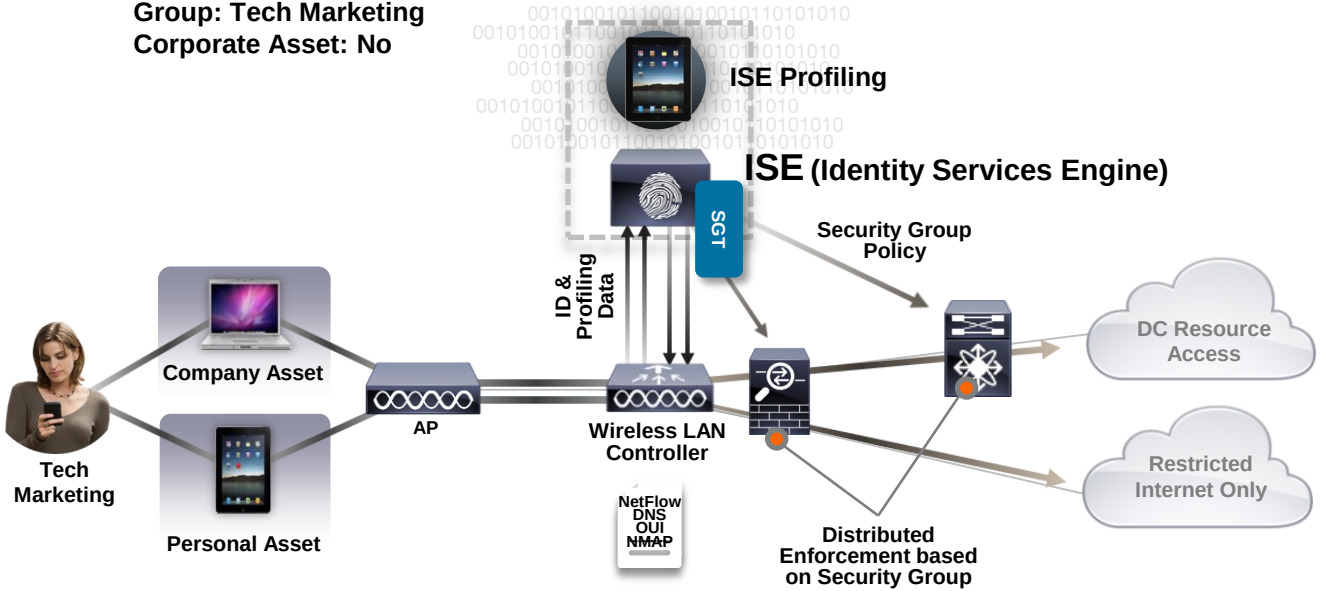
- Classification of systems/users based on **context** (user role, device, location, access method)
- The context-based **classification propagates via a SGT**
- SGT used by firewalls, routers and switches to make intelligent forwarding or blocking decisions

SGT Assignment - BYOD Example

Classification Result:

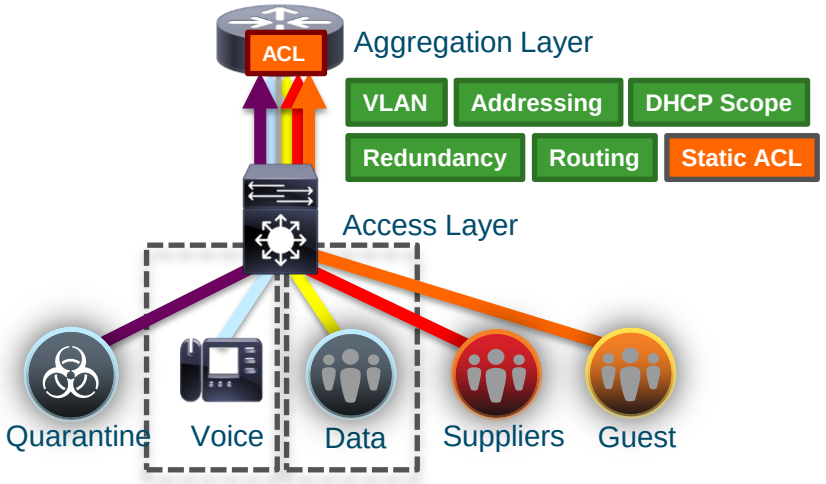
Personal Asset SGT

Device Type: Apple iPAD
User: Fay
Group: Tech Marketing
Corporate Asset: No



Traditional Segmentation

Steps replicated across floors, buildings and sites

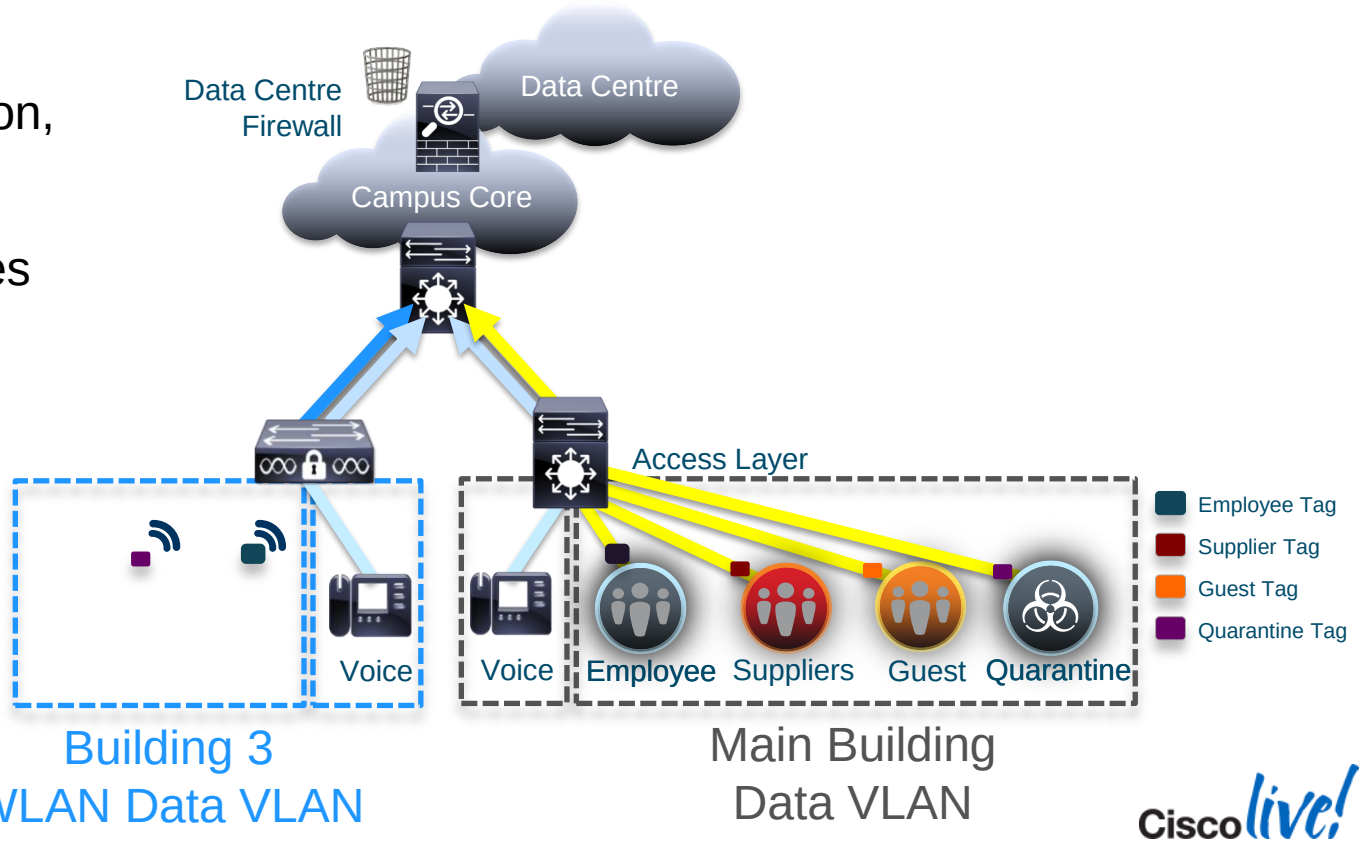


Simple Segmentation with 2 VLANs

More Policies using more VLANs

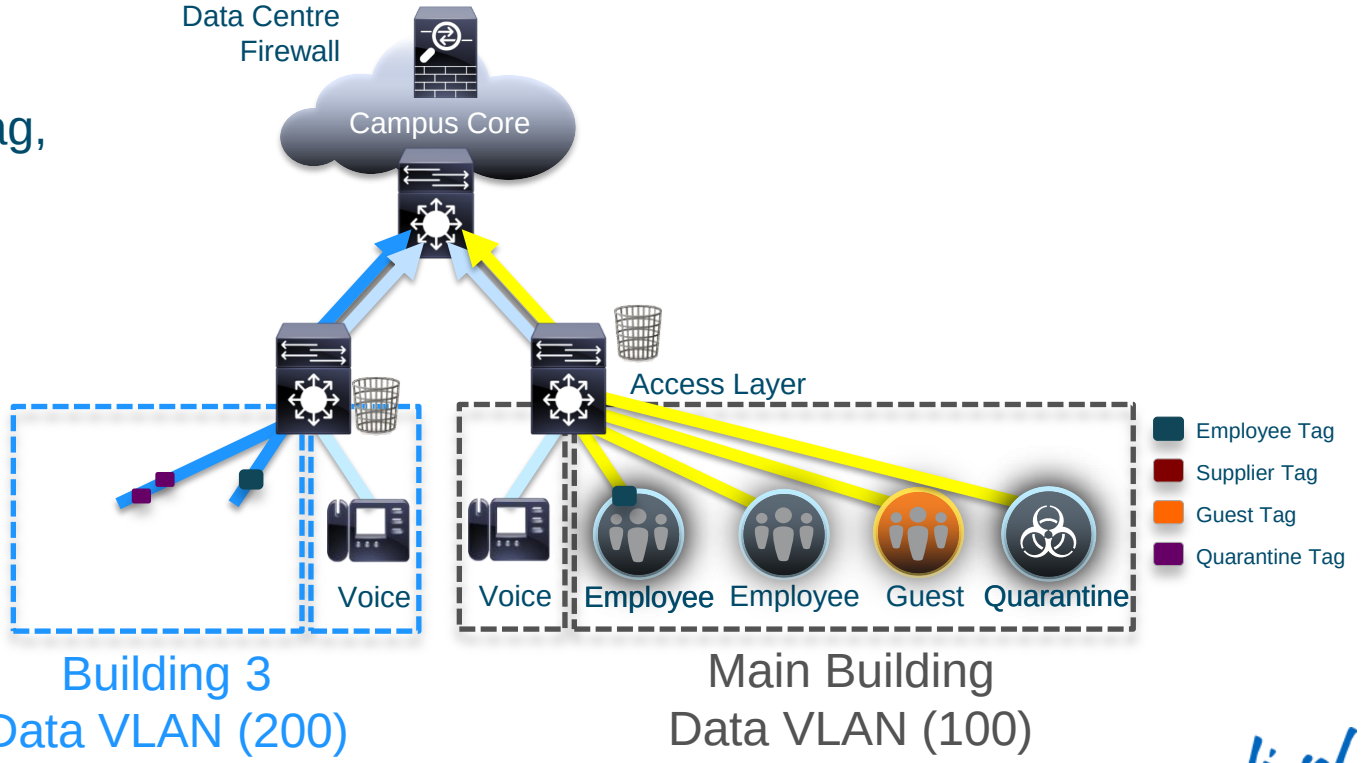
User to Data Centre Access Control with TrustSec SGT

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

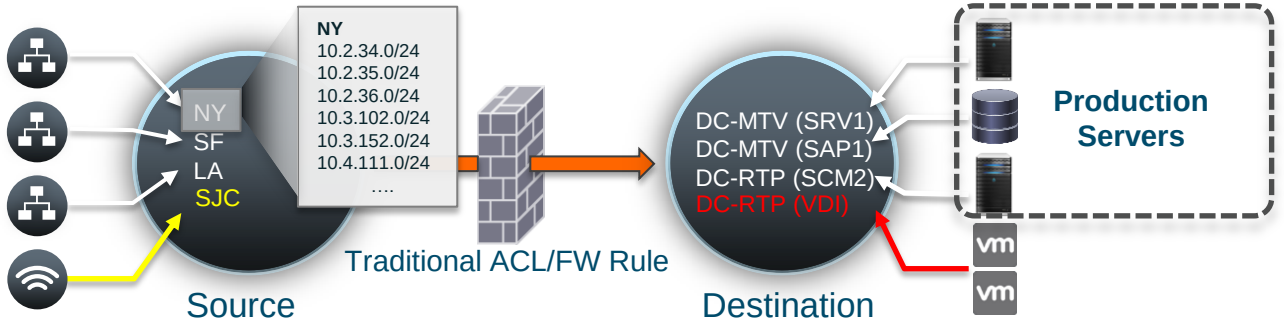


Campus Segmentation with TrustSec SGT

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



Traditional OpEx in Security Policy Maintenance




```
permit NY  to SRV1 for HTTPS
deny   NY  to SAP2 for SQL
deny   NY  to SCM2 for SSH
permit SF  to SRV1 for HTTPS
deny   SF  to SAP1 for SQL
deny   SF  to SCM2 for SSH
permit LA  to SRV1 for HTTPS
deny   LA  to SAP1 for SQL
deny   LA  to SAP  for SSH
```

ACL for 3 source objects & 3 destination objects

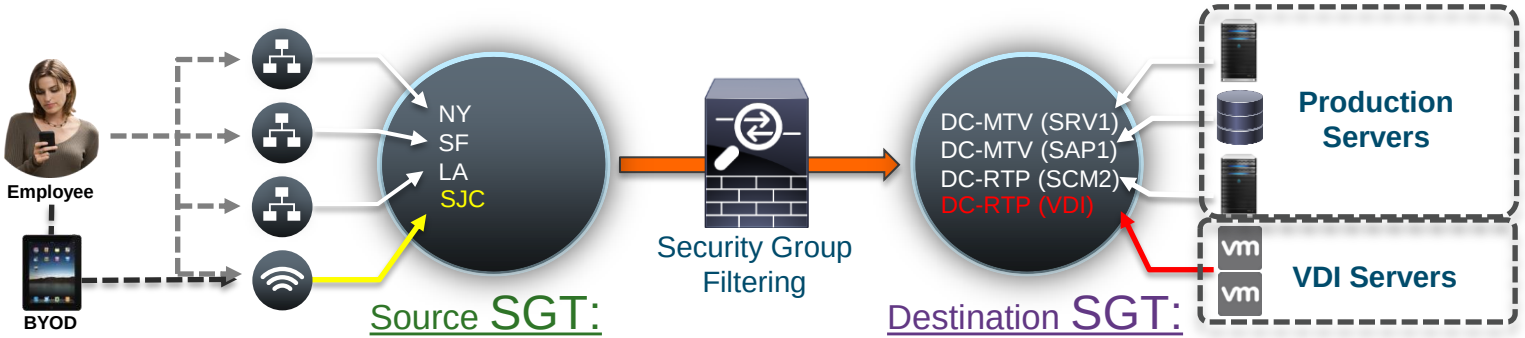
```
Permit SJC to SRV1 for HTTPS
deny   SJC to SAP1 for SQL
deny   SJC to SCM2 for SSH
```

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



Source SGT:

Employee (10)

BYOD (200)

Destination SGT:

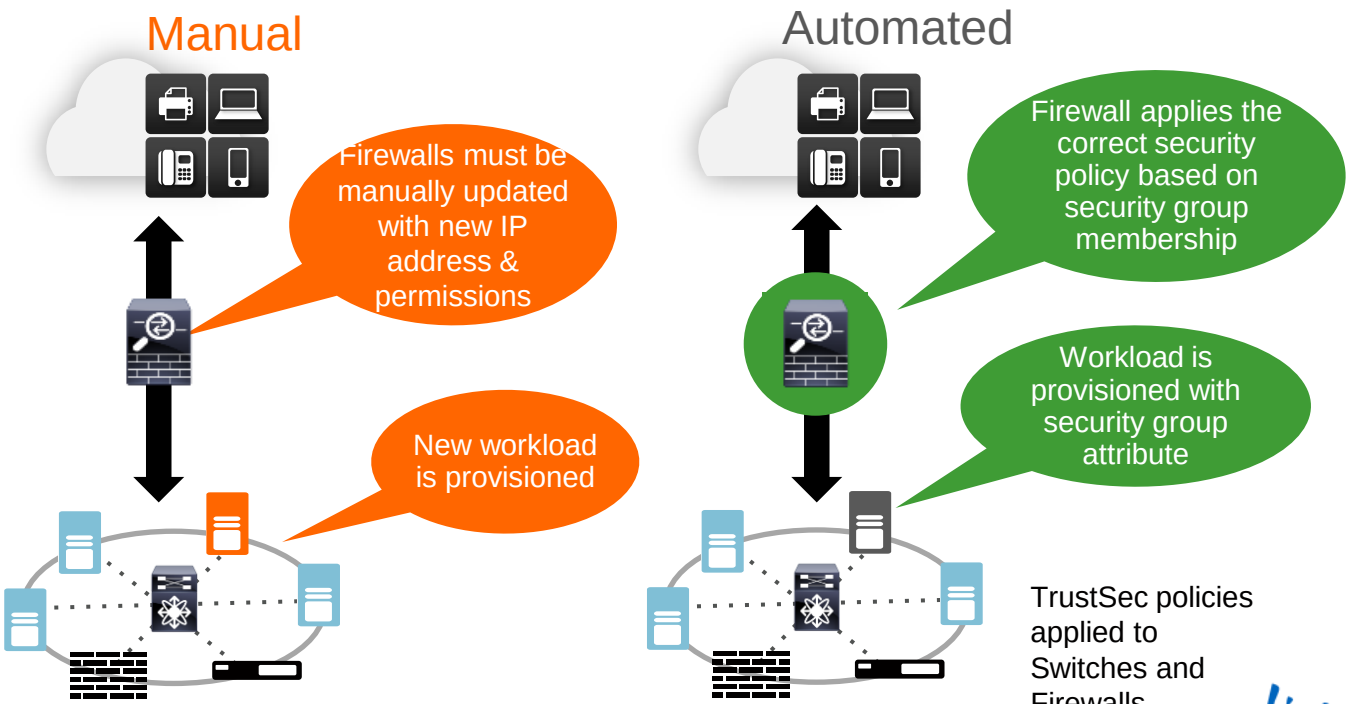
Production_Servers (50)

VDI (201)

```
Permit  Employee     to     Production_Servers  eq  HTTPS
Permit  Employee     to     Production_Servers  eq  SQL
Permit  Employee     to     Production_Servers  eq  SSH
Permit  Employee     to     VDI                 eq  RDP

Deny    BYOD         to     Production_Servers
Deny    BYOD         to     VDI                 eq  RDP
```

Ease of Data Centre Provisioning

Ease of **Provisioning**



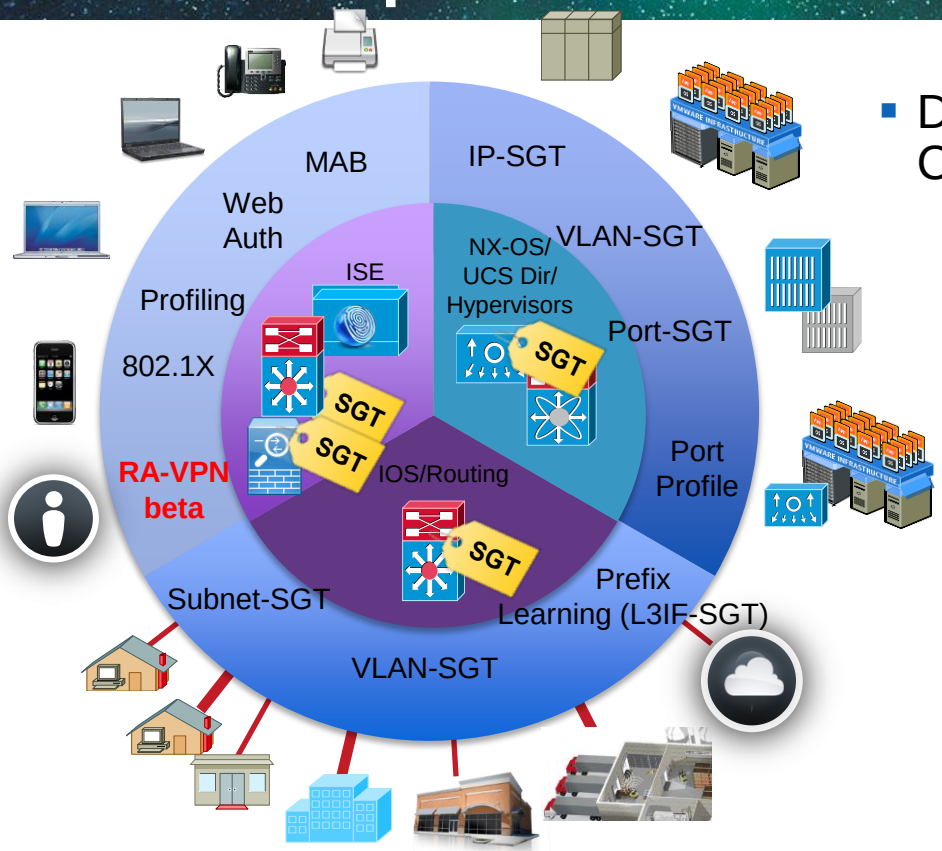
TrustSec policies applied to Switches and Firewalls




SGT Classification

TrustSec Classification Options

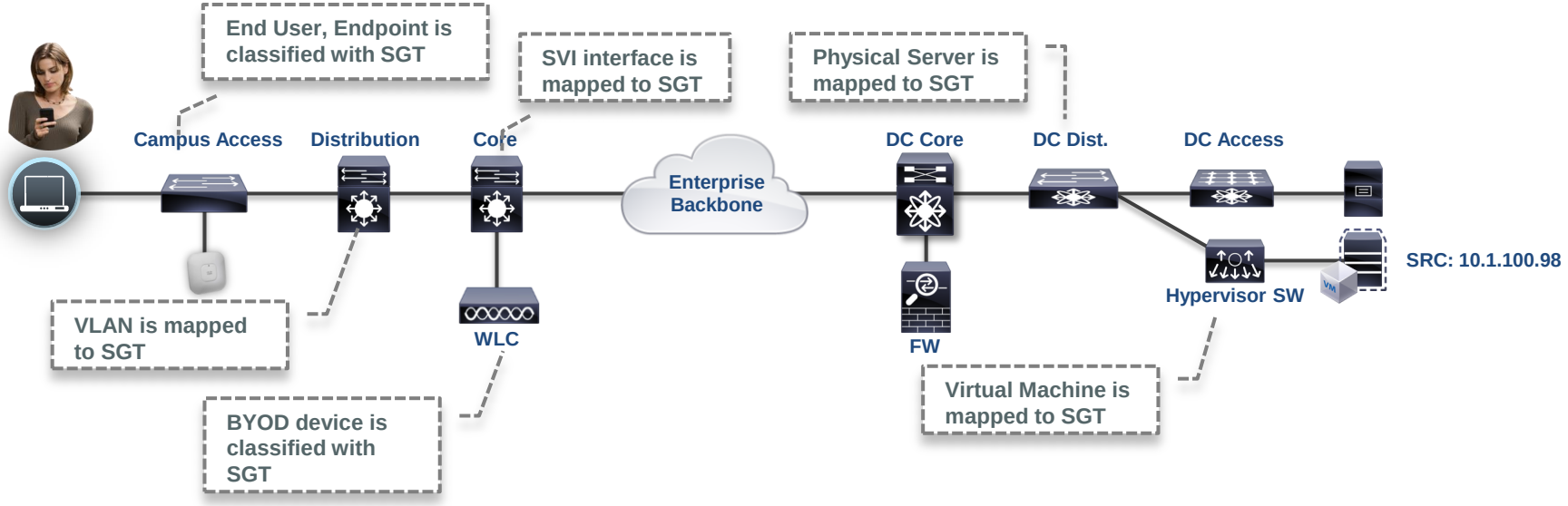
- User/Device SGT assignments
  - Wired
  - Wireless
  - (RA VPN in beta)



- Data Centre Server Classifiers

- Business Partners & 3rd party connections

How a SGT is Assigned



Classification Summary

Dynamic Classification

802.1X Authentication

Web Authentication

MAC Auth Bypass

Static Classification

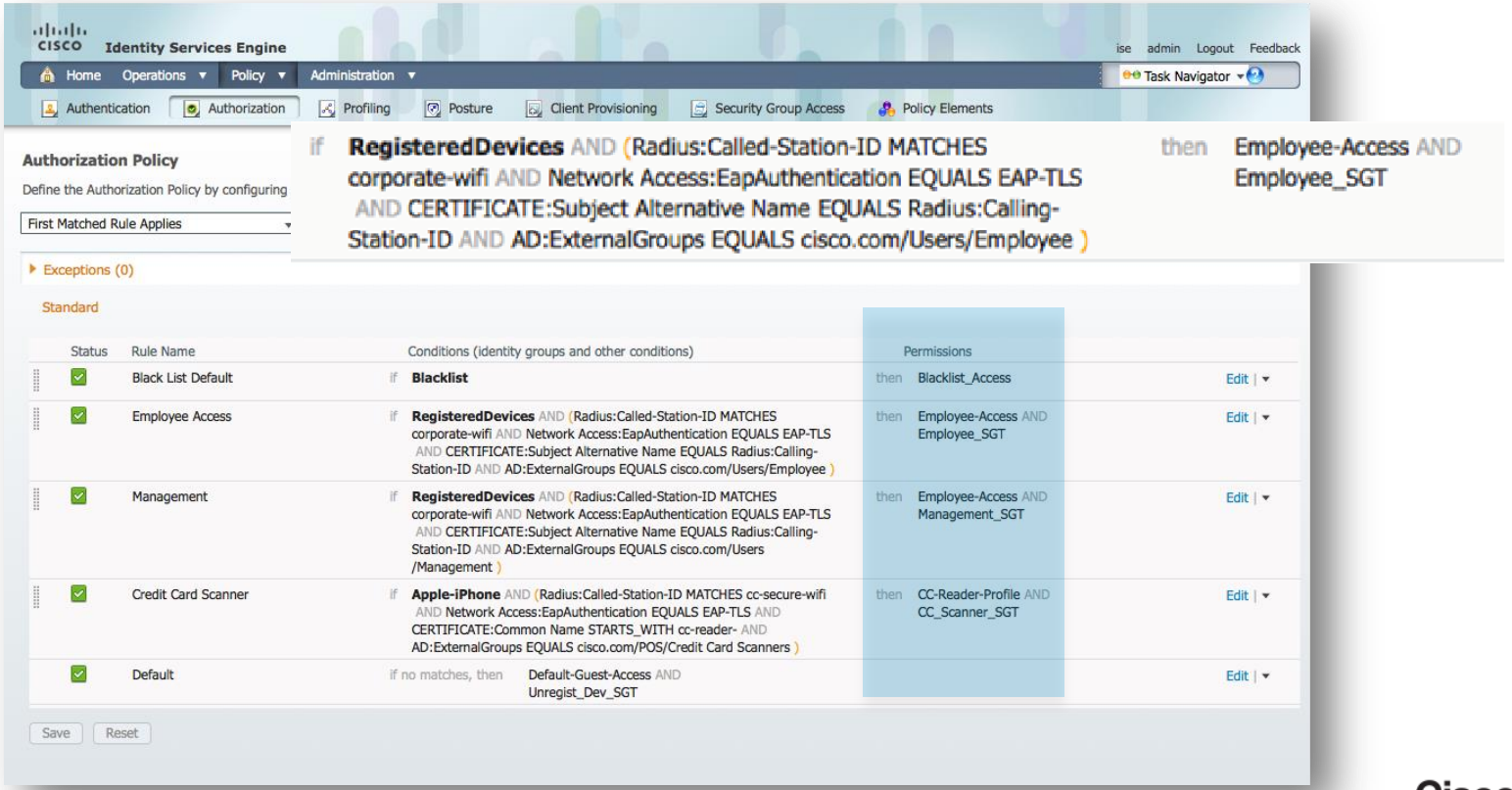
- IP Address
- VLANs
- Subnets
- L2 Interface
- L3 Interface
- Virtual Port Profile
- Layer 2 Port Lookup

SGT

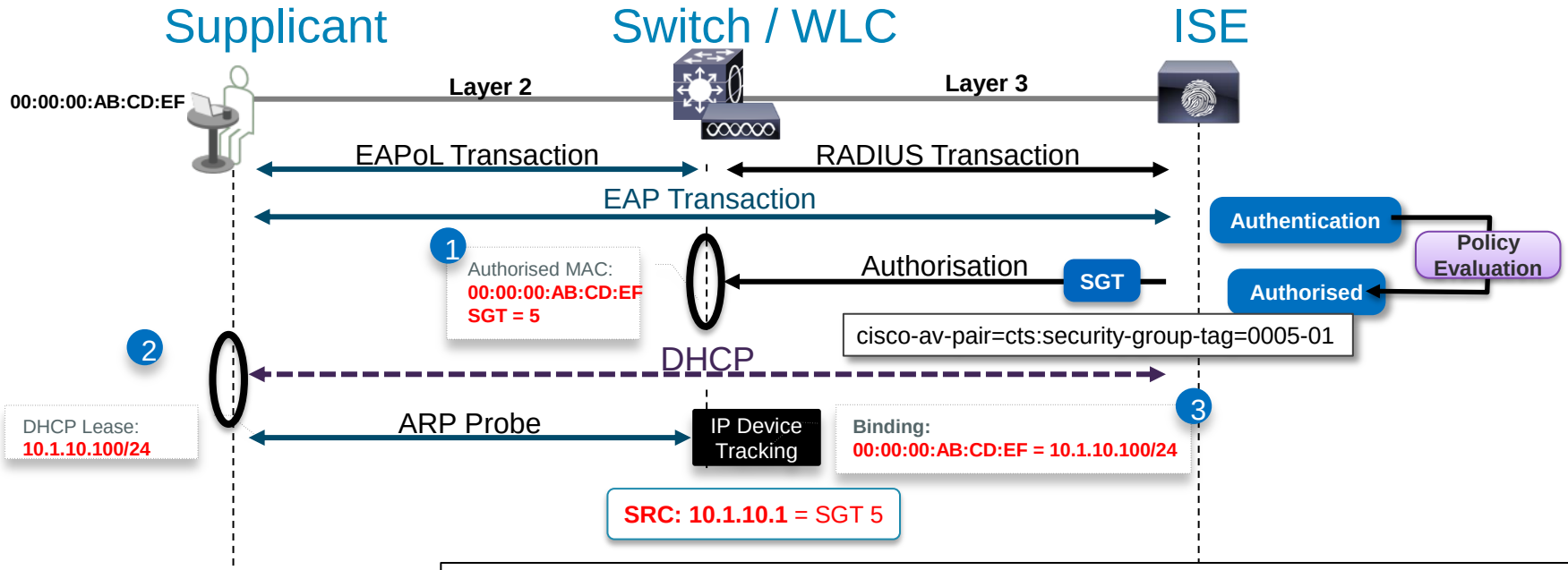
Common Classification for Mobile Devices

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

ISE Dynamic SGT Assignments



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
```

Static Classification

IOS CLI Example

IP to SGT mapping

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

L2IF to SGT mapping*

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

VLAN to SGT mapping*

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

L3IF to SGT mapping**

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

Subnet to SGT mapping

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

Layer 3 Interface to SGT Mapping
(L3IF-SGT) Sup2T introduced in 15.0(1)SY

- 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

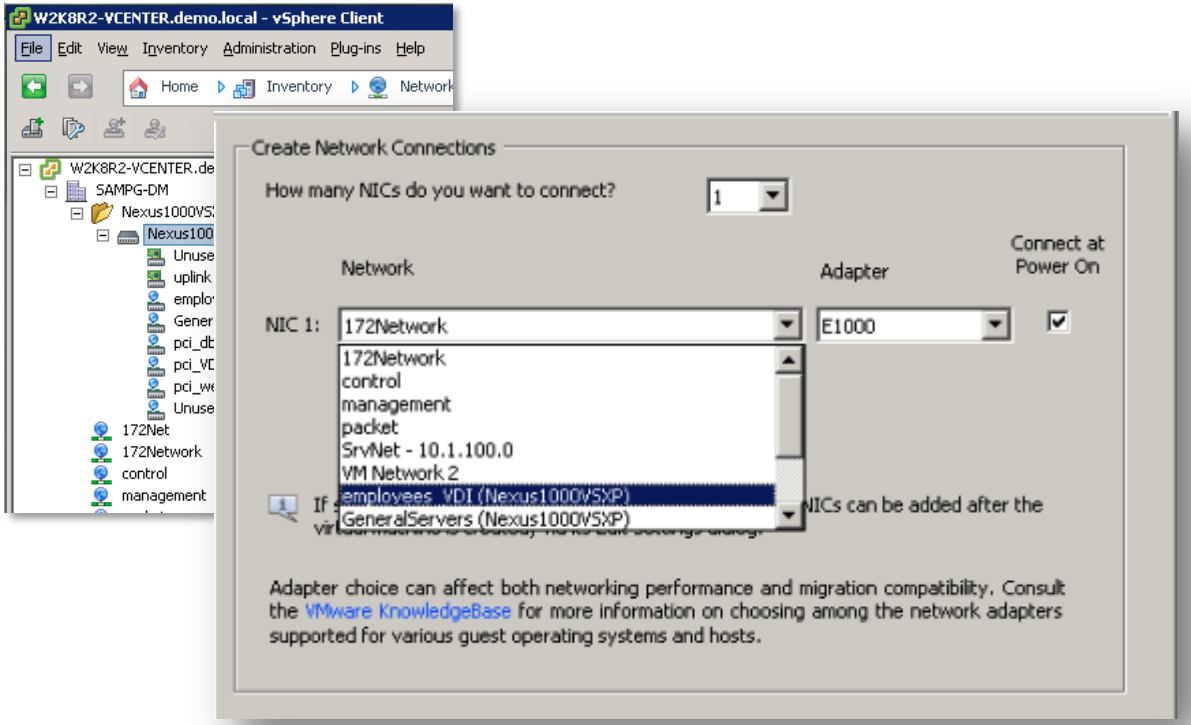
cts role-based sgt-map interface *GigabitEthernet 3/0/1* **sgt** *8*

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
```

Nexus 1000V 2.1 – SGT Assignment

- 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



Nexus 1000V 2.1 – SGT Assignment

- Port Profiles assigned to VMs

```
Nexus1000VSXP# sho cts ipsgt entries
  Interface       SGT            IP ADDRESS       VRF          Learnt
--------------- ------         ---------------- ----------     ---------
Vethernet1       8              10.1.100.121       -          Device Tracking
Vethernet2       7              10.1.100.120       -          Device Tracking
Vethernet3       5              10.1.100.98        -          Device Tracking
Vethernet4       6
Vethernet5       3              10.1.3.108         -          Device Tracking
Vethernet6       6              10.1.3.113         -          Device Tracking
```

SGT Assignment – Access Layer Classification

		Cat2960-S	Cat3750X	Cat3850/5760	Cat4K S7	Cat6x00	ISR	WLC	Notes
Dynamic	802.1X	X	X	X	X	X	X	X	
	MAB	X	X	X	X	X	X	X	
	Web Auth	X	X	X	X	X	X	X	
Static	VLAN/SGT	-	X*	X	X	X*	-	-	
	Subnet/SGT	-	-	X	X	X	-	-	Via Sup2T
	Layer 3 Identity to Port Mapping	-	-		-	X	-	-	Based on routes learned from port via dynamic routing

* - limits on the number of VLANs per platform

Key TrustSec Functions

Classification


Catalyst 2960S/C/Plus/X/XR


Catalyst 3560-E/-C/-X

Catalyst 3750-E/-X


Catalyst 3850 NEW

WLC 5760


Catalyst 4500E (Sup6E/7E)

Catalyst 6500E (Sup720/2T)


Wireless LAN Controller 2500/5500/WiSM2


Nexus 7000

Nexus 5500


Nexus 1000v


ISR G2 , CGR2000


ASA5500 (VPN RAS) Beta

Propagation

SXP — Catalyst 2960-S/-C/-Plus/-X/-XR

SXP — Catalyst 3560-E/-C/, 3750-E

SXP SGT — Catalyst 3560-X, 3750-X

SXP SGT — Catalyst 3850 NEW

SXP — Catalyst 4500E (Sup6E)

SXP SGT — Catalyst 4500E (7E), 4500X

SXP — Catalyst 6500E (Sup720)

SXP SGT — Catalyst 6500E(2T) & 6800 NEW

SXP — WLC 2500, 5500, WiSM2

SXP SGT — WLC 5760 NEW

SXP — Nexus 1000v

SXP SGT — Nexus 5500/22xx FEX

SXP SGT — Nexus 7000/22xx FEX

SXP SGT GETVPN IPsec — ISRG2* CGR2000

SXP SGT GETVPN IPsec — ASR1000

SXP — ASA5500 Firewall, ASASM

Enforcement

SGACL — Catalyst 3560-X

SGACL — Catalyst 3750-X

Catalyst 3850 NEW

WLC 5760 NEW

SGACL — Catalyst 4500E (7E) NEW

Catalyst 6500E (2T)

SGACL — Catalyst 6800 NEW

Nexus 7000

SGACL — Nexus 5500

SGFW — ISR G2, CGR2000

SGFW — ASR 1000 Router
CSR1000v Router

SGFW — ASA 5500 & ASA-SM

ASAv Beta

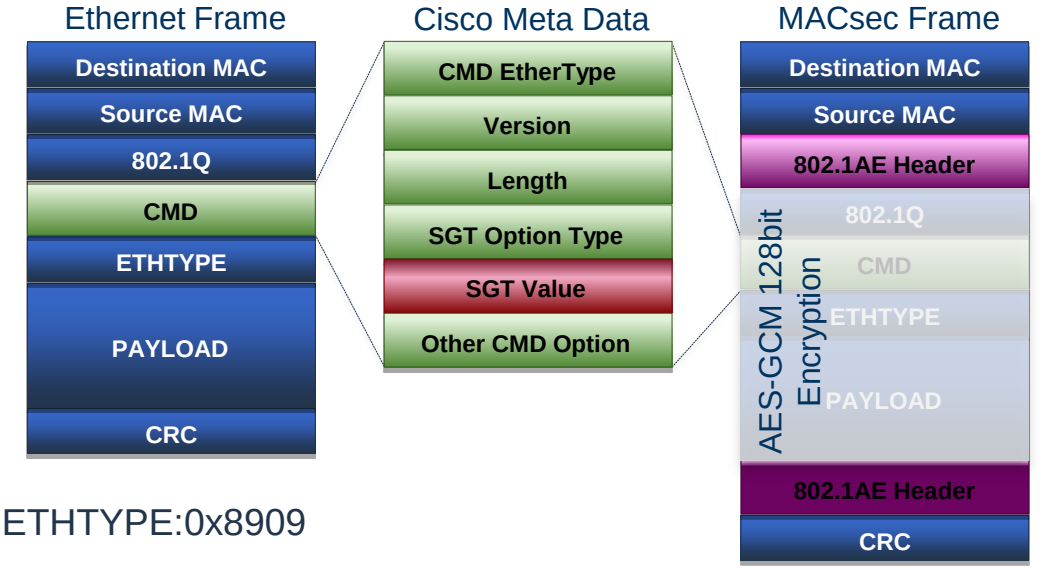
- Inline SGT on all ISRG2 except 800 series:




SGT Propagation

Propagation Option 1: Inline Tagging

- SGT embedded within Cisco Meta Data (CMD) in Layer 2 frame
- Capable switches understands and process SGT at line-rate
- Optional MACsec protection
- No impact to QoS, IP MTU/Fragmentation
- L2 Frame Impact: ~40 bytes
- Recommend L2 MTU~6000 bytes
- N.B. Incapable devices will drop frames with unknown Ethertype



SGT Link Authentication and Authorisation

Mode	MACSEC	MACSEC Pairwise Master Key (PMK)	MACSEC Pairwise Transient Key (PTK)	Encryption Cipher Selection (no-encap, null, GCM, GMAC)	Trust/Propagation Policy for Tags
cts dot1x	Y	Dynamic	Dynamic	Negotiated	Dynamic from ISE/configured
cts manual – with encryption	Y	Static	Dynamic	Static	Static
cts manual – no encryption	N	N/A	N/A	N/A	Static

- CTS Manual is ***strongly*** recommended configuration for SGT propagation
  - "cts dot1x" takes link down with AAA down. Tight coupling of link state and AAA state
  - Some platforms (ISRG2, ASR1K, N5K) only support cts manual/no encryption

Configure Links for SGT Tagging

CTS Manual no encryption

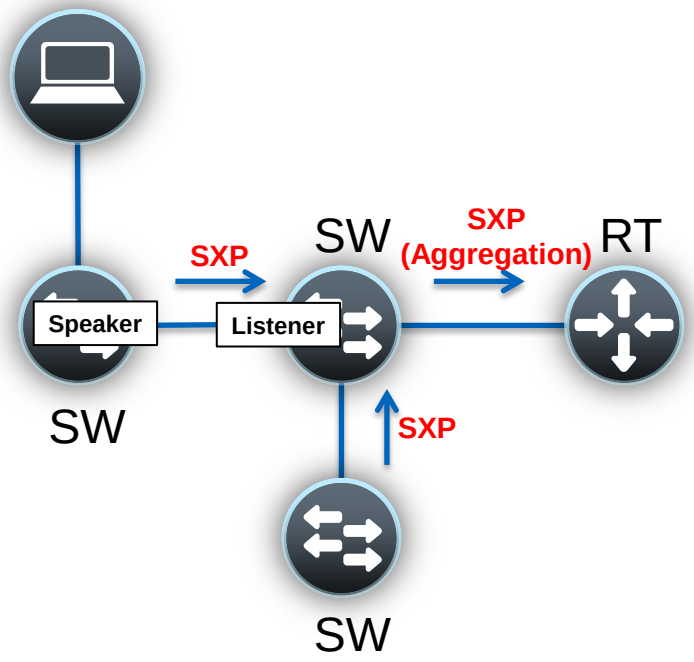
```
interface TenGigabitEthernet1/5
 cts manual
  policy static sgt 2 trusted
```

```
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.
```

Always “shut” and “no shut” and interface for any cts manual or cts dot1x change

Propagation Option 2: SGT eXchange Protocol (SXP)

- Control plane protocol that conveys the IP-SGT map of authenticated hosts to enforcement points
- SXP uses TCP as the transport layer
- Accelerate deployment of SGT
- Support Single Hop SXP & Multi-Hop SXP (aggregation)
- Two roles: Speaker (initiator) and Listener (receiver)

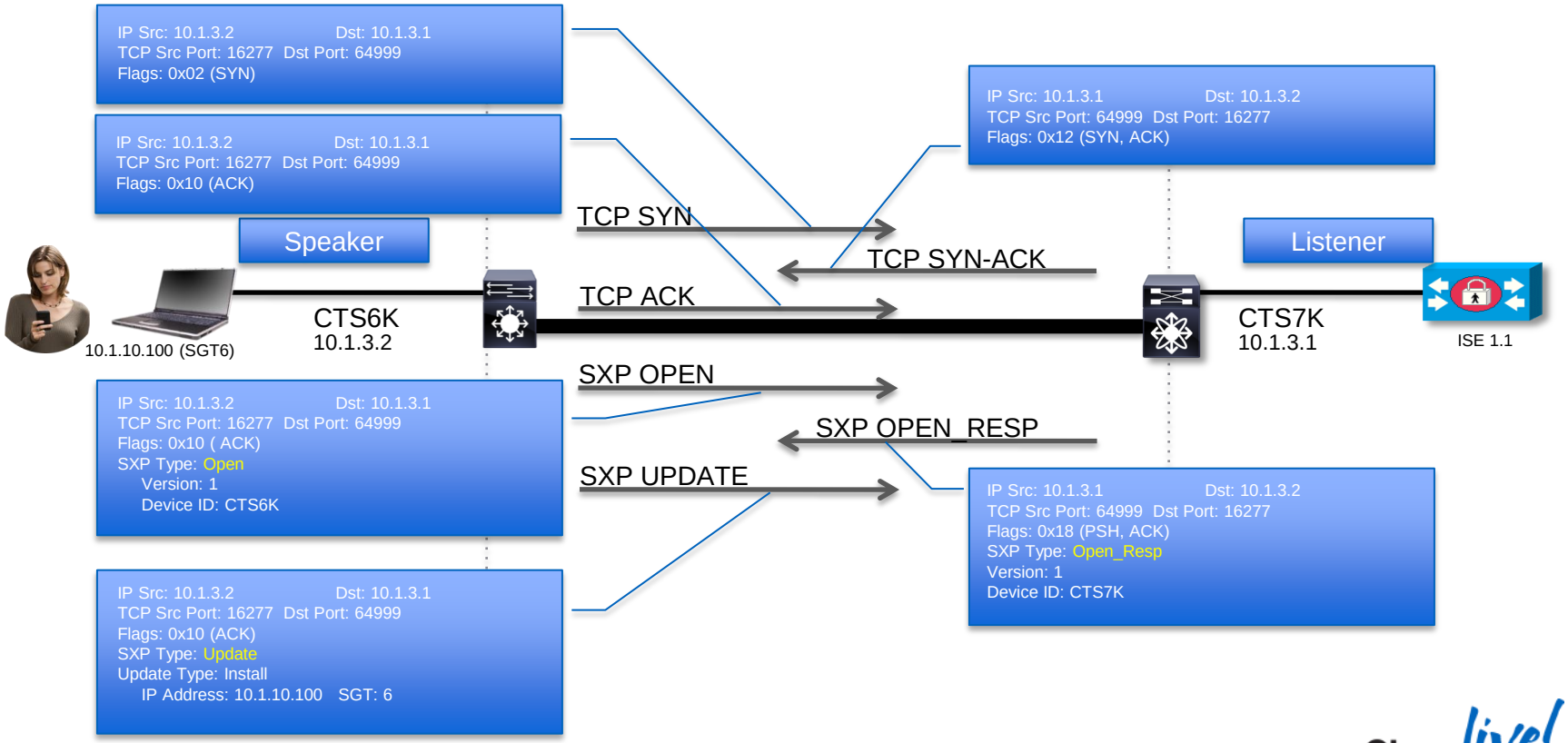


Propagation option 2: SGT eXchange Protocol (SXP)

- SXP accelerates deployment of SGTs
  - Allows classification at the access edge without hardware upgrade
  - Allows communication from access edge to enforcement device
- SXP also used to traverse networks/devices without SGT capabilities
- 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
```

SXP Flow

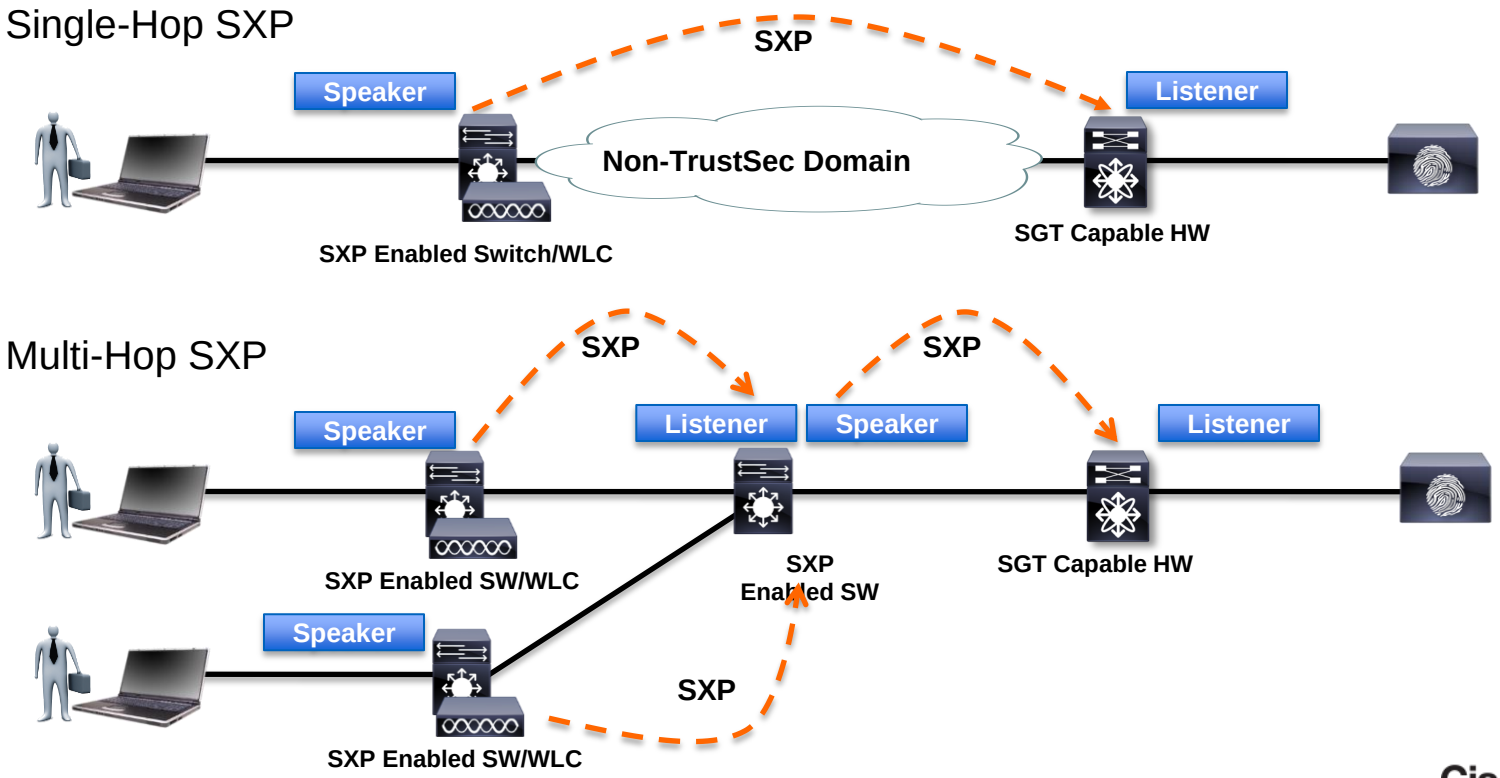


SXP Informational Draft

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

SXP Connection Types

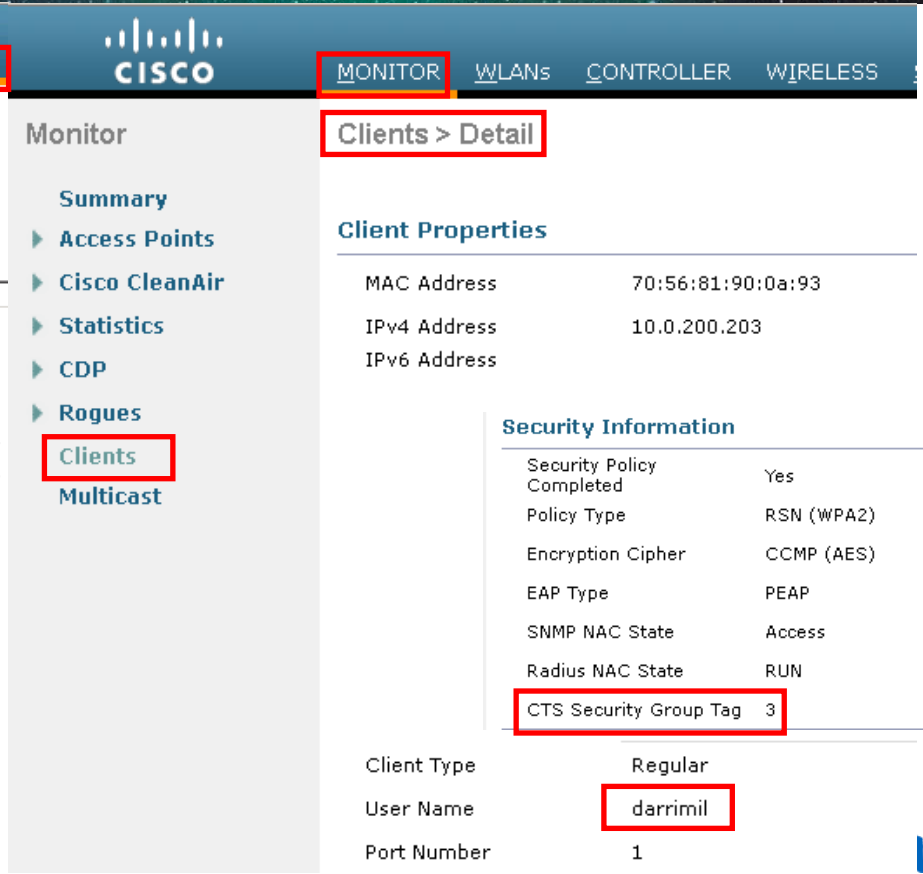


IOS SXP Configuration

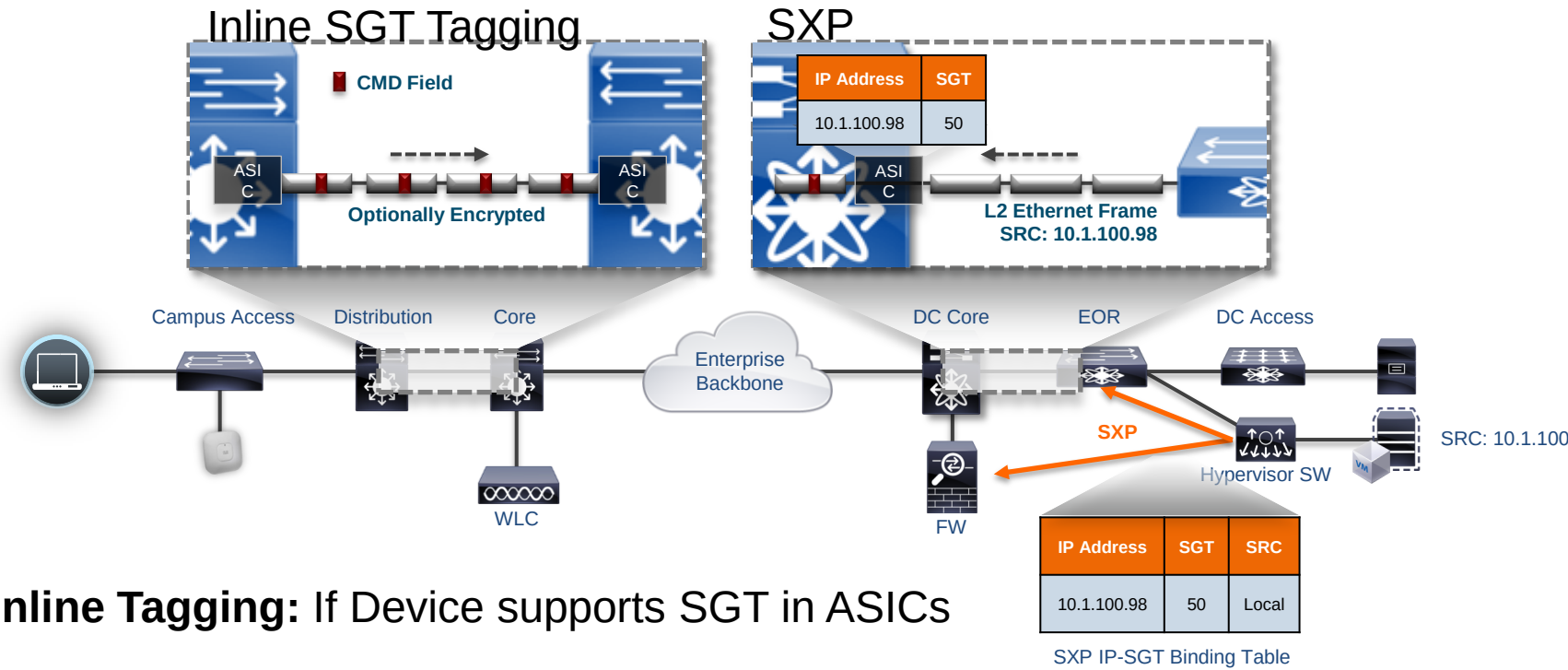
```
3750
cts sxp enable
cts sxp connection peer 10.1.44.1 source
10.1.11.44 password default mode local
! SXP Peering to Cat6K

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



Inline Tagging vs. SXP Tag Propagation



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

Key TrustSec Functions

Classification

Catalyst 2960S/C/Plus/X/XR
Catalyst 3560-E/-C/-X
Catalyst 3750-E/-X
Catalyst 3850 NEW
WLC 5760
Catalyst 4500E (Sup6E/7E)
Catalyst 6500E (Sup720/2T)
Wireless LAN Controller 2500/5500/WiSM2
Nexus 7000
Nexus 5500
Nexus 1000v
ISR G2 , CGR2000
ASA5500 (VPN RAS) Beta

Propagation

SXP				Catalyst 2960-S/-C/-Plus/-X/-XR
SXP				Catalyst 3560-E/-C/, 3750-E
SXP	SGT			Catalyst 3560-X, 3750-X
SXP	SGT			Catalyst 3850 NEW
SXP				Catalyst 4500E (Sup6E)
SXP	SGT			Catalyst 4500E (7E), 4500X
SXP				Catalyst 6500E (Sup720)
SXP	SGT			Catalyst 6500E(2T) & 6800 NEW
SXP				WLC 2500, 5500, WiSM2
SXP	SGT			WLC 5760 NEW
SXP				Nexus 1000v
SXP	SGT			Nexus 5500/22xx FEX
SXP	SGT			Nexus 7000/22xx FEX
SXP	SGT	GETVPN	IPsec	ISRG2* CGR2000
SXP	SGT	GETVPN	IPsec	ASR1000
SXP				ASA5500 Firewall, ASASM

Enforcement

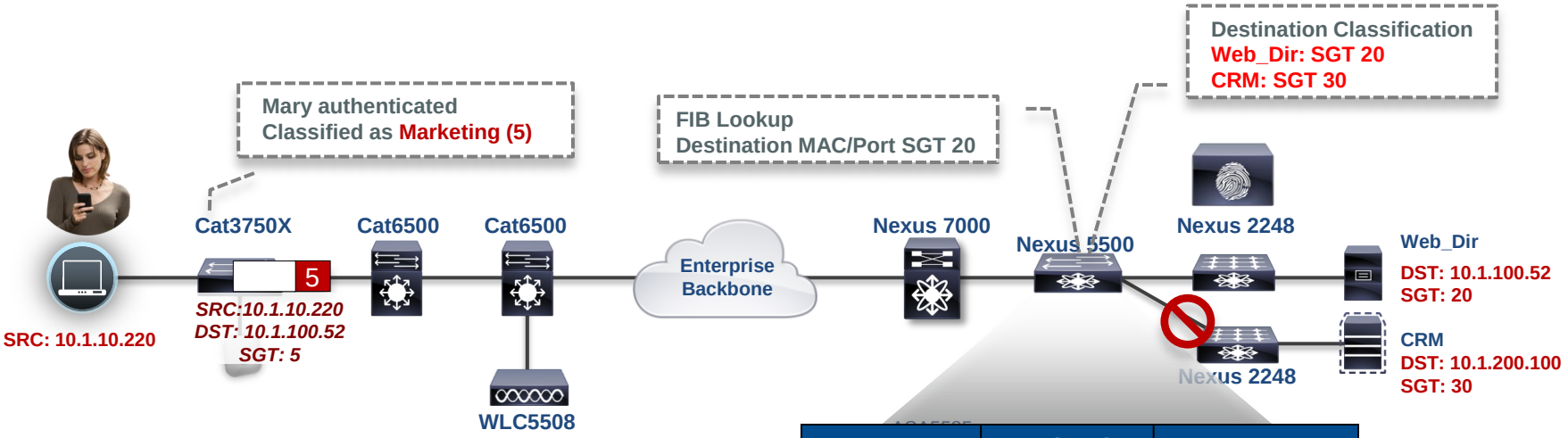
Catalyst 3560-X
Catalyst 3750-X
Catalyst 3850 NEW
WLC 5760 NEW
Catalyst 4500E (7E) NEW
Catalyst 6500E (2T)
Catalyst 6800 NEW
Nexus 7000
Nexus 5500
ISR G2, CGR2000
ASR 1000 Router
CSR1000v Router
ASA 5500 & ASA-SM
ASAv Beta

- Inline SGT on all ISRG2 except 800 series:



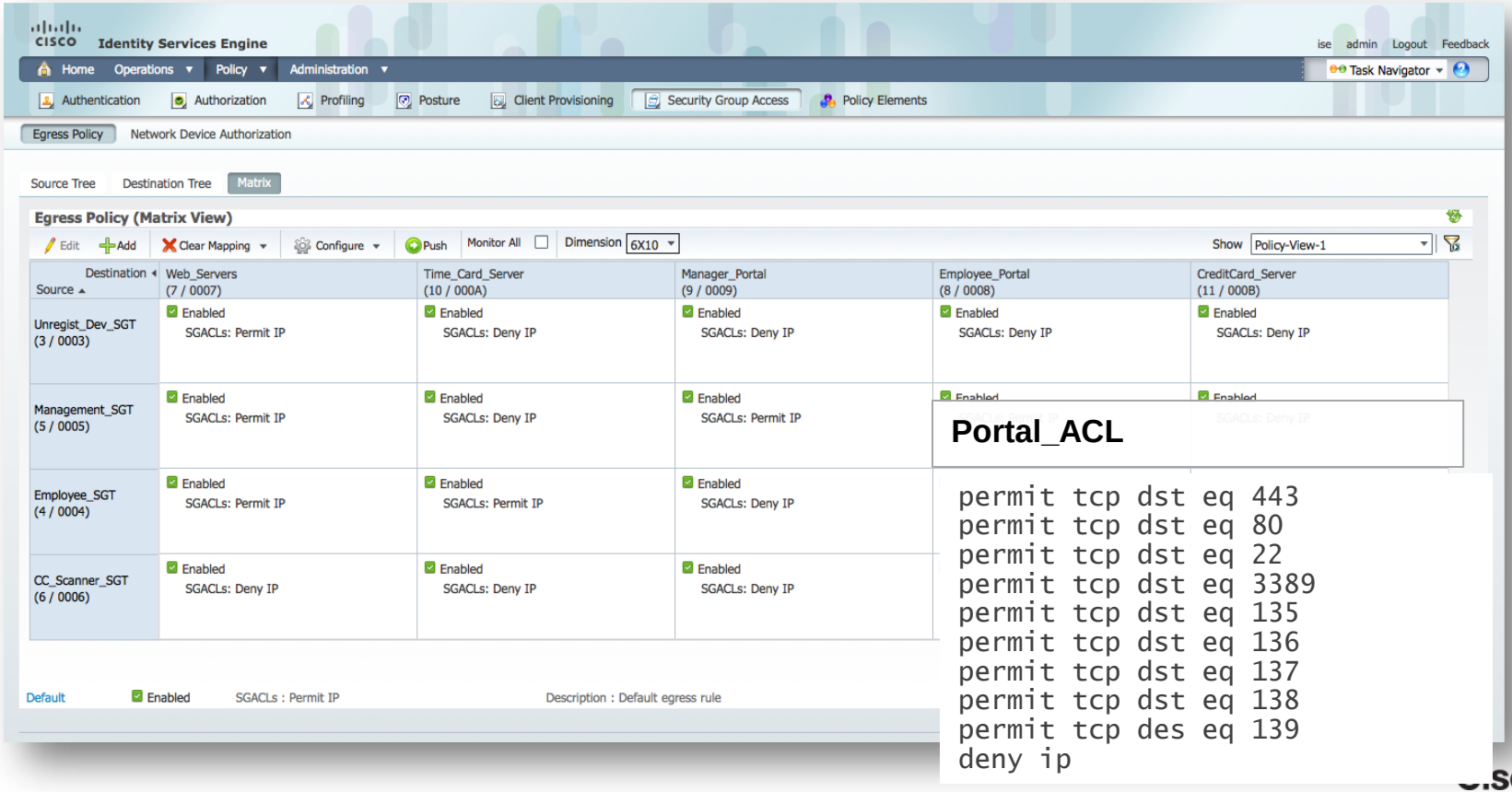

Policy Enforcement

Policy Enforcement - Security Group ACL (SGACL)



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

Centralised SGACL Policy Management in ISE

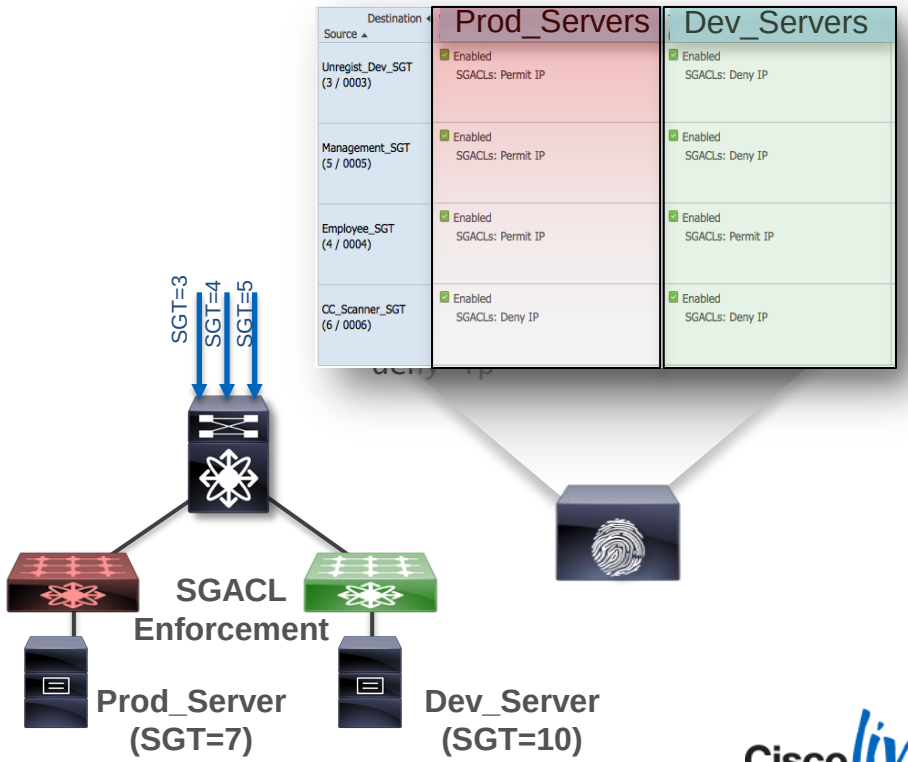


Portal_ACL

```
permit tcp dst eq 443
permit tcp dst eq 80
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 des eq 139
deny ip
```

SGACL Egress Policy Enforcement

- Extended ACL syntax, **without IP addresses**
- Avoids **TCAM** impact, can be IPv6 **agnostic***
- Can be applied anywhere (no IP dependency)
- Switches that classify servers only download SGACLs they need from ISE
- **No device-specific ACL** configs



* Currently only Cat6k Sup 2T supports IPv6 SGACL

Environment Data

```
TS2-6K-DIST#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 -> Device_SGT
    unicast-unknown-98 : 80 -> Unknown
    Any : 80 -> ANY
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 20:56:48 UTC Mon Sep 26 2011
Env-data expires in   0:23:59:59 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:59 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

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

```
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
```

Enabling SGACL Enforcement Globally and for VLAN

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

Distribution 6K – Sup2T - Enabling Ingress Reflector to support SGACL on legacy linecard (if there is any)

```
Switch(config)#platform cts ingress
CTS Ingress reflector will be active only on next system reboot.
Please reboot the system for CTS Ingress reflector to be active.
```

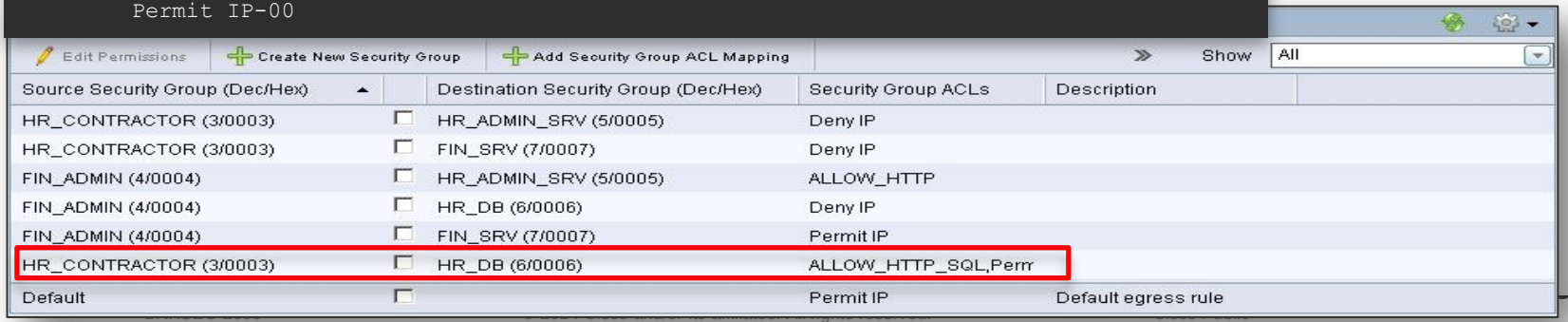
Enabling reflector requires system to reboot.

Downloading SGACL Policy on IOS Switch

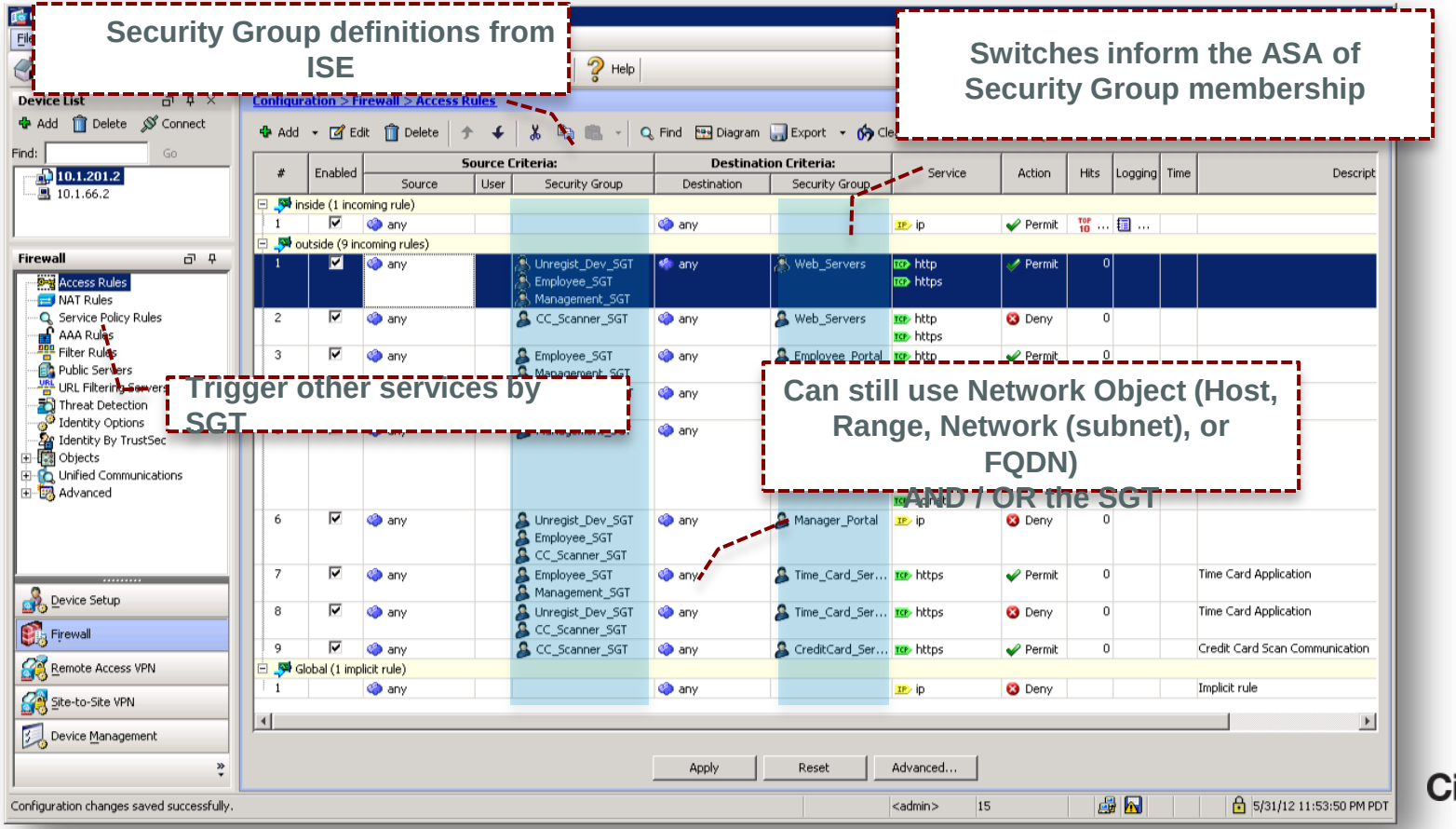
Verify SGACL Content

```
TS2-6K-DIST#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 6:
        ALLOW_HTTP_SQL-10
        Permit 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



Policy Enforcement on Firewalls: ASA SG-FW

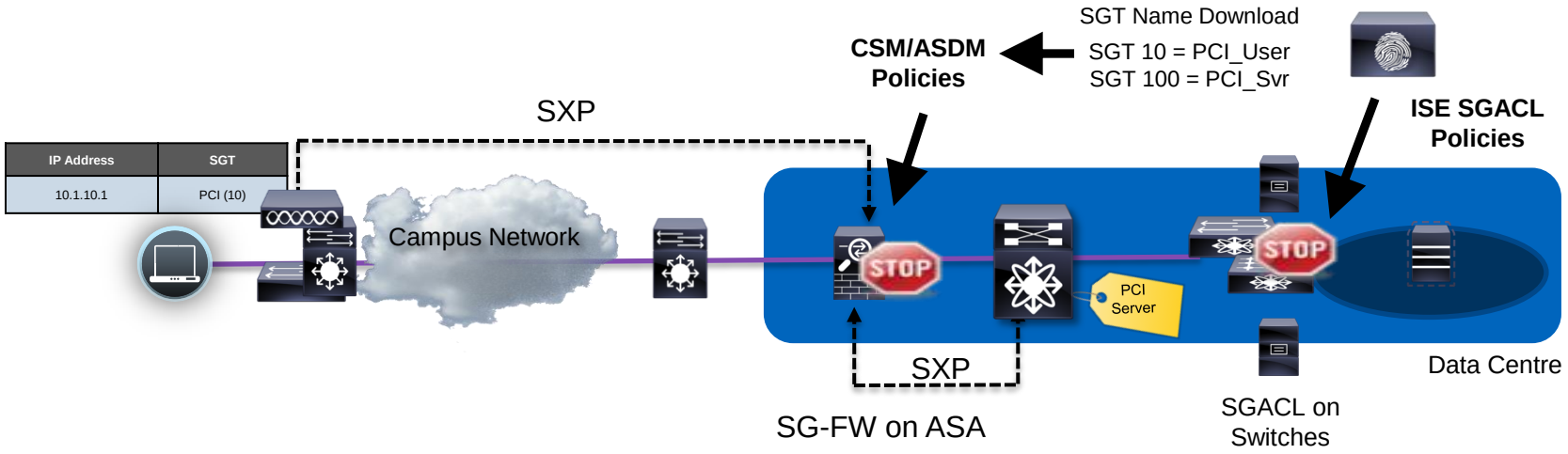


SG-FW Simplifying ASA Rules and Operations

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

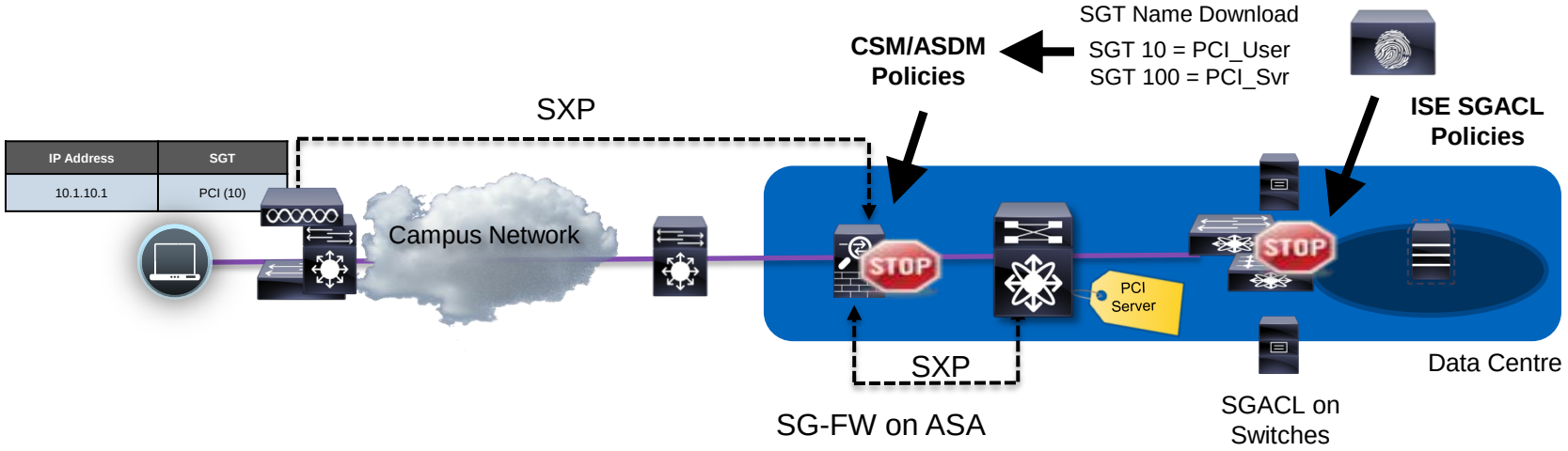
- Policies can use Security Groups for user roles and server roles
- Moves and changes do not require IP-address rule-changes
- New servers/users just require group membership to be established
- Rule-base reduction with Groups instead of IP addresses can be significant
- Common classification method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

Using SG-FW and SGACL Enforcement Together



- Consistent Classification/enforcement between Firewalls and switching.
- SGT Names will be synchronised between ISE and ASDM
- Policy administrators need to ensure SGACL and SG-FW rules are in sync

Logging TrustSec Policy Enforcement



- SG-FW gives richer logging, e.g. URL logging
- Switch logging is best effort via syslog (e.g. N7000) or NetFlow (C6500 Sup2T)
- SGACL counters vary per switch platform
  - Per SGT/DGT on Nexus 7000/Cat6500 Sup2T
  - Per Platform on Nexus 5500

Key TrustSec Functions

Classification

Catalyst 2960S/C/Plus/X/XR

Catalyst 3560-E/-C/-X

Catalyst 3750-E/-X

Catalyst 3850 NEW

WLC 5760


Catalyst 4500E (Sup6E/7E)

Catalyst 6500E (Sup720/2T)

Wireless LAN Controller 2500/5500/WiSM2


Nexus 7000

Nexus 5500


Nexus 1000v

ISR G2 , CGR2000


ASA5500 (VPN RAS) Beta

Propagation

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

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

Catalyst 3560-X, 3750-X

Catalyst 3850 NEW

Catalyst 4500E (Sup6E)

Catalyst 4500E (7E), 4500X

Catalyst 6500E (Sup720)

Catalyst 6500E(2T) & 6800 NEW

WLC 2500, 5500, WiSM2

WLC 5760 NEW

Nexus 1000v

Nexus 5500/22xx FEX

Nexus 7000/22xx FEX

ISRG2* CGR2000

ASR1000

ASA5500 Firewall, ASASM

- Inline SGT on all ISRG2 except 800 series:

Enforcement


Catalyst 3560-X
Catalyst 3750-X


Catalyst 3850 NEW

WLC 5760 NEW


Catalyst 4500E (7E) NEW

Catalyst 6500E (2T)


Catalyst 6800 NEW

Nexus 7000


Nexus 5500


ISR G2, CGR2000


ASR 1000 Router
CSR1000v Router


ASA 5500 & ASA-SM

ASAv Beta

TrustSec Platform Support

Classification


Catalyst 2960S/C/Plus/X/XR


Catalyst 3560-E/-C/-X


Catalyst 3750-E/-X

Catalyst 3850 NEW

WLC 5760


Catalyst 4500E (Sup6E/7E)

Catalyst 6500E (Sup720/2T)


Wireless LAN Controller 2500/5500/WiSM2


Nexus 7000


Nexus 5500


Nexus 1000v


ISR G2 , CGR2000


ASA5500 (VPN RAS) Beta

Propagation

SXP — Catalyst 2960-S/-C/-Plus/-X/-XR

SXP — Catalyst 3560-E/-C/, 3750-E

SXP SGT — Catalyst 3560-X, 3750-X

SXP SGT — Catalyst 3850 NEW

SXP — Catalyst 4500E (Sup6E)

SXP SGT — Catalyst 4500E (7E), 4500X

SXP — Catalyst 6500E (Sup720)

SXP SGT — Catalyst 6500E(2T) & 6800 NEW

SXP — WLC 2500, 5500, WiSM2

SXP SGT — WLC 5760 NEW

SXP — Nexus 1000v

SXP SGT — Nexus 5500/22xx FEX

SXP SGT — Nexus 7000/22xx FEX

SXP SGT GETVPN IPsec — ISRG2* CGR2000

SXP SGT GETVPN IPsec — ASR1000

SXP — ASA5500 Firewall, ASASM

Enforcement


Catalyst 3560-X

Catalyst 3750-X


Catalyst 3850 NEW

WLC 5760 NEW


Catalyst 4500E (7E) NEW

Catalyst 6500E (2T)


Catalyst 6800 NEW

Nexus 7000


Nexus 5500


ISR G2, CGR2000


ASR 1000 Router

CSR1000v Router


ASA 5500 & ASA-SM

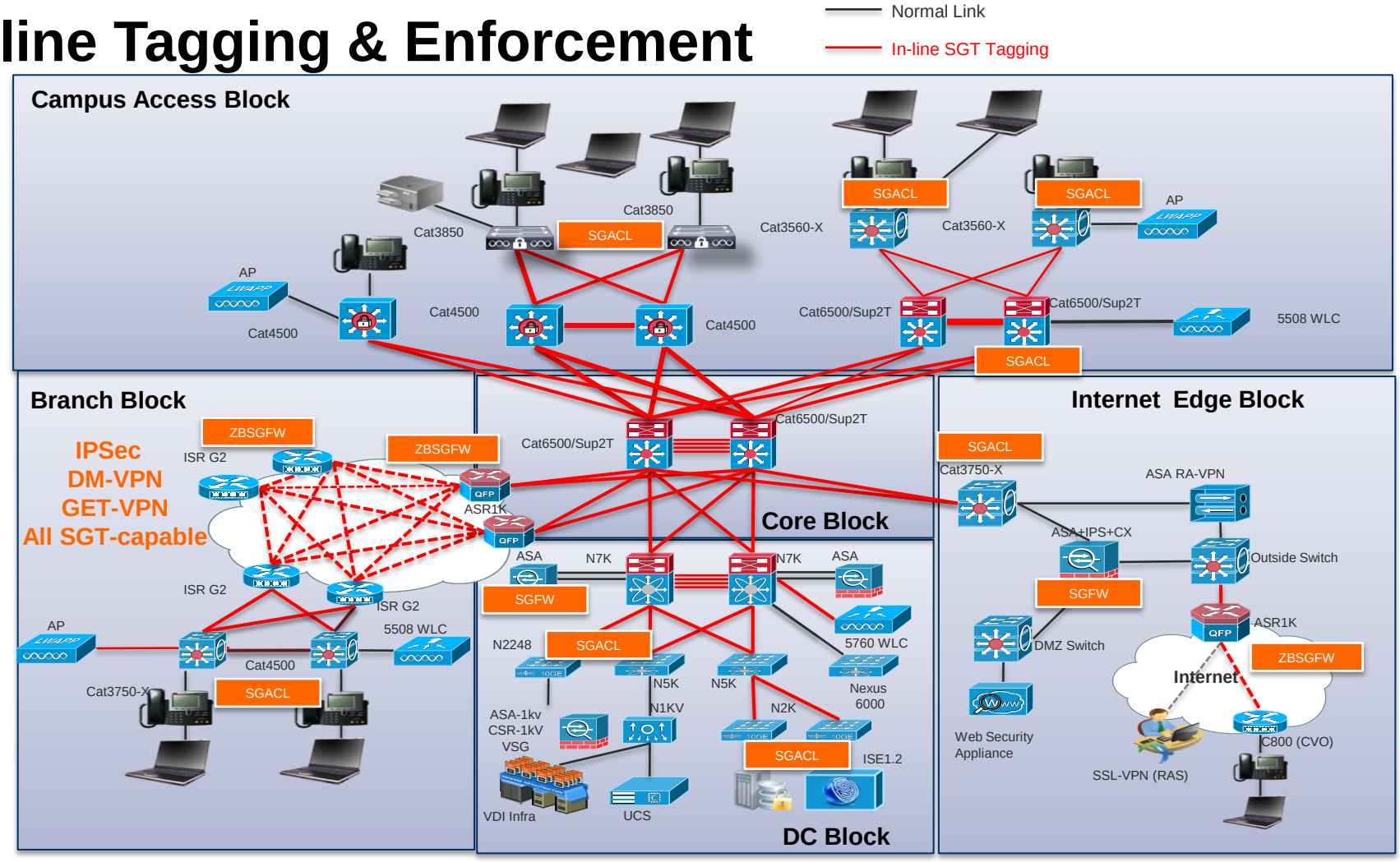
ASAv Beta

- Inline SGT on all ISRG2 except 800 series:

Extract from TrustSec Platform Support Matrix

Platform	Solution Minimum Version	Solution-Level Validated Version	SGT Classification	Control Plane Propagation (SXP)	SGT over Ethernet (Inline SGT)	SGT over MACsec	SGT over xVPN (for WAN)	SGT Enforcement
Cisco Catalyst 2960S/SF Series(LAN Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE2	Dynamic,IP-SGT,VLAN-SGT	SXP (speaker only)	No	No	No	No
Cisco Catalyst 3560-X,3750-X(IP Base required)	IOS 15.0(1)SE2	IOS 15.0(2)SE4	Dynamic,IP-SGT,VLAN-SGT	SXP (S/L)	Yes	Yes (with C3KX - SM-10G)	No	SGACL
Cisco Catalyst 6500 (Sup-2T)(IP Base required)	IOS 15.0(1)SY1	IOS 15.1(1)SY1	Dynamic,IP-SGT,VLAN-SGT,Subnet-SGT,L3IF-SGT	SXP (S/L)	Yes (requires WS-X69xx line card)	Yes (with Sup2T built-in ports and WS-X69xx	No	SGACL
All Cisco Nexus 7000 line cards and chassis	NX -OS 6.1(1) (SGT support in base license from 6.1)	NX -OS 6.2(2)	Static IP-SGT,L2IF-SGT, Port Profile-SGT	SXP (S/L)	Yes	Yes (All line cards except F1 and F2 line cards)	No	SGACL

Inline Tagging & Enforcement



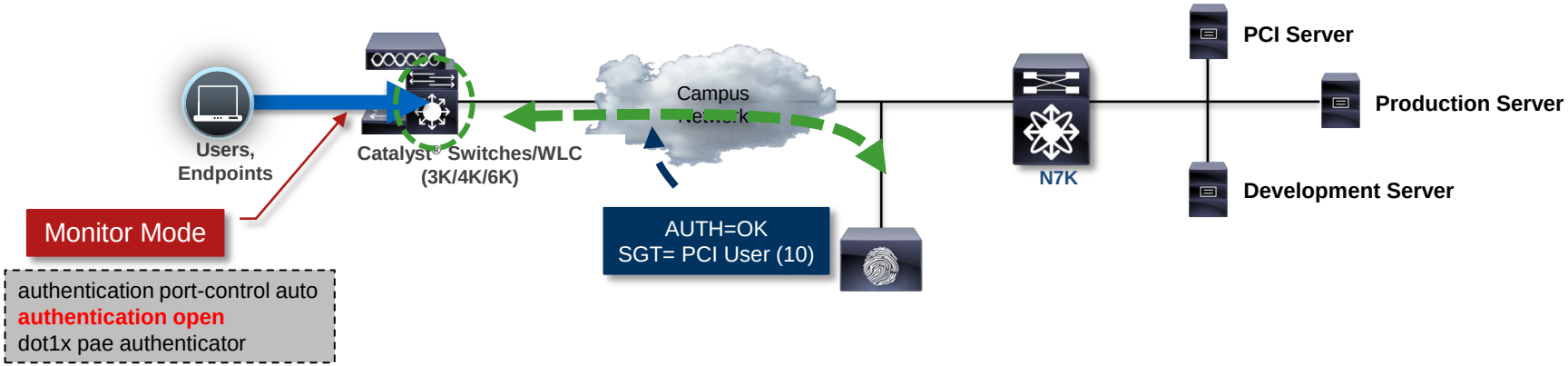
Deployment Questions

- Where do I start?
- How do I define the roles needed for my organisation?
- What about all my network devices that don't support SGT inline tagging?
- How should I assign SGTs?

Frequent discussion topics before deployments:

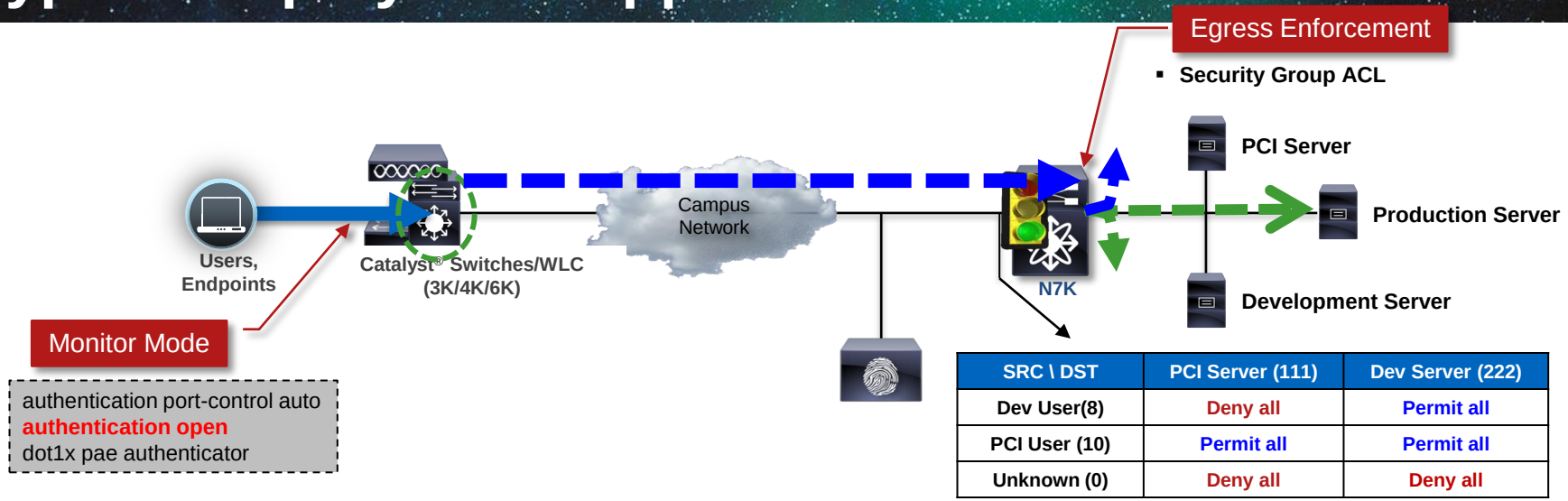
- Identifying use-cases have least HW/upgrade dependency, which are often deployed first
  - E.g. User to DC Access Control
- How we can assign tags in a passive manner – then enforce selectively
- Relative ease of adding more roles later

Typical Deployment Approach



1. User connects to network, Monitor mode allows traffic from before authentication
2. Authentication is performed and results are logged by ISE

Typical Deployment Approach



SRC \ DST	PCI Server (111)	Dev Server (222)
Dev User(8)	Deny all	Permit all
PCI User (10)	Permit all	Permit all
Unknown (0)	Deny all	Deny all

1. User connects to network, Monitor mode allows traffic from before authentication
2. Authentication is performed and results are logged by ISE
3. Traffic traverse to Data Centre and hits SGACL at egress enforcement point
4. SGACLs may be enabled gradually on a destination SGT basis




Use Cases: User to DC Access Control

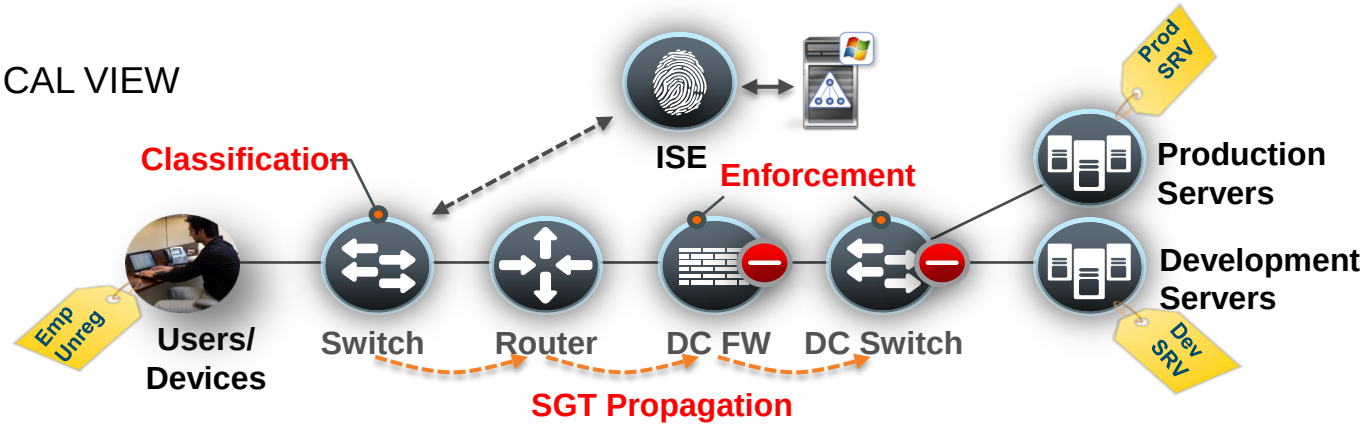
User to Data Centre Access Control

POLICY VIEW

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

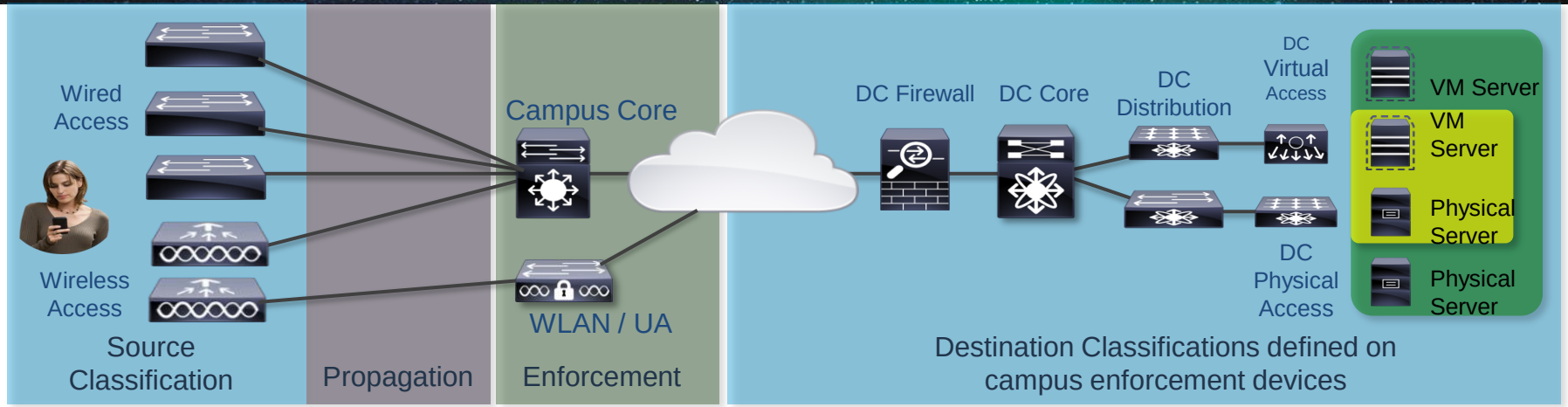
LOGICAL VIEW



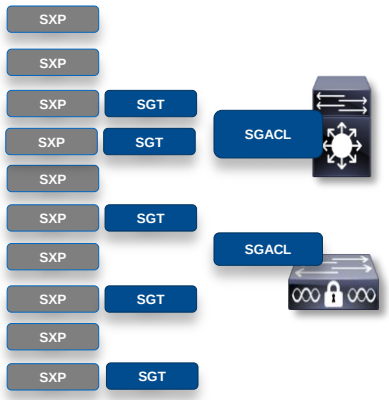
Key SXP Scaling Information to Understand

Platform	Max SXP Connections	Max IP-SGT bindings
Catalyst 6500 Sup2T/ 6800	2000	200,000
Nexus 7000	980	200,000
Catalyst 4500 Sup 7E	1000	256,000
Catalyst 4500-X / 4500 Sup 7LE	1000	64,000
ASA 5585-X SSP60	1000	100,000
ASA 5585-X SSP40	500	50,000
Catalyst 3850/WLC 5760	128	12,000

User to DC Access Control – Campus 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

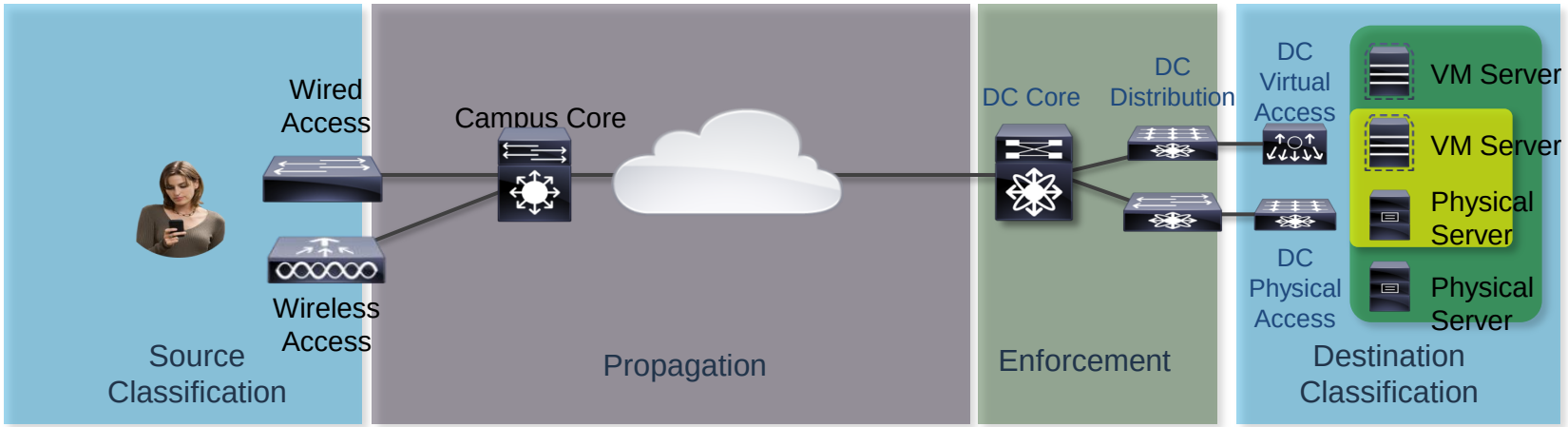


Campus Core Switch:
Catalyst 6500E (2T)
Catalyst 4500 Sup7(L3 cfg)

WLAN/Unified Access:
Catalyst 3850
WLC 5760

Classify destination SGTs in enforcement device using:
- **Subnet-SGT mappings**
- **IP-SGT mappings**

User to DC Access Control – DC Switch 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

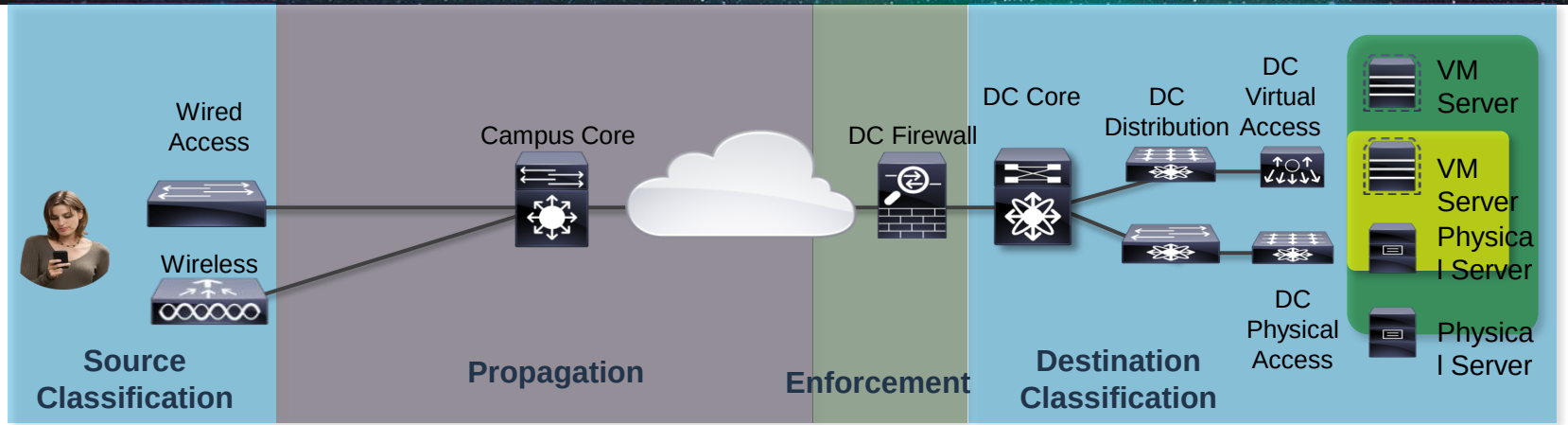
CLASSIFY SERVERS WITH:

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 5500/2200(FEX)
- Port–SGT mappings used for physical servers

User to DC Access Control – SG-Firewall



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

PROPAGATION

SXP to ASA

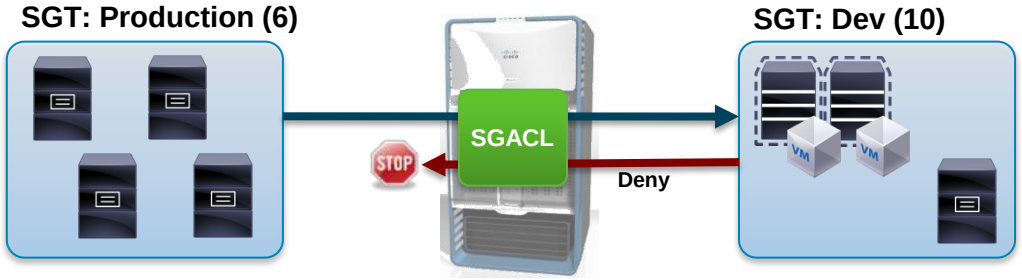
CLASSIFY SERVERS WITH:

IP Firewall rule entries

SXP from Nexus 1000v/5500/7000:
- Nexus 1000v **Port Profile SGT** mappings
- Nexus 7000 **VLAN – SGT** mappings
  IP-SGT mappings (can be from ISE)
- Nexus 5500/2200 IP-SGT mappings (can be from ISE)

Use Cases: Data Centre Segmentation

Data Centre Segmentation



- Segment servers into logical zones
- Control access to logical DC entities based on role
- Apply controls to physical and virtual systems (virtual servers, VDI..

Sample server groups:

- Production, Development, User Acceptance Test
- Export Controlled data
- Engineering vs. Business Servers
- PCI compliance-critical

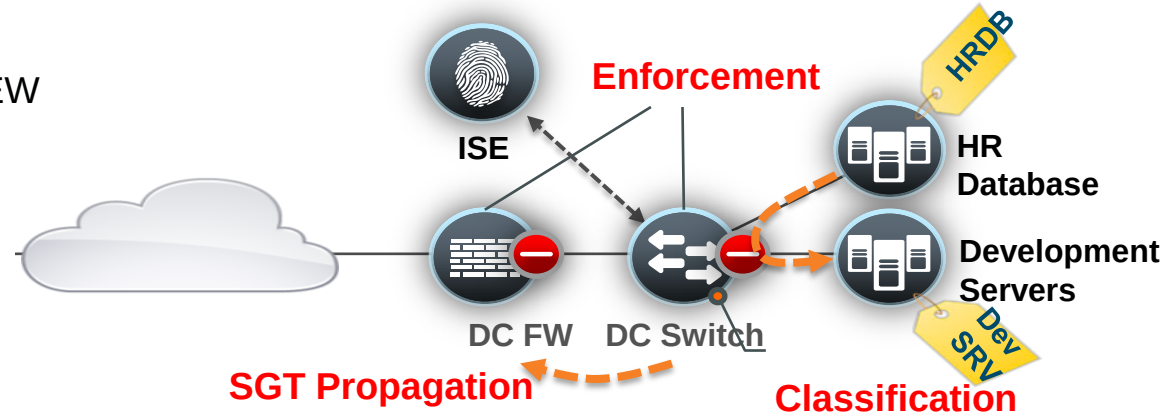
Data Centre Segmentation

POLICY VIEW

Protected Assets

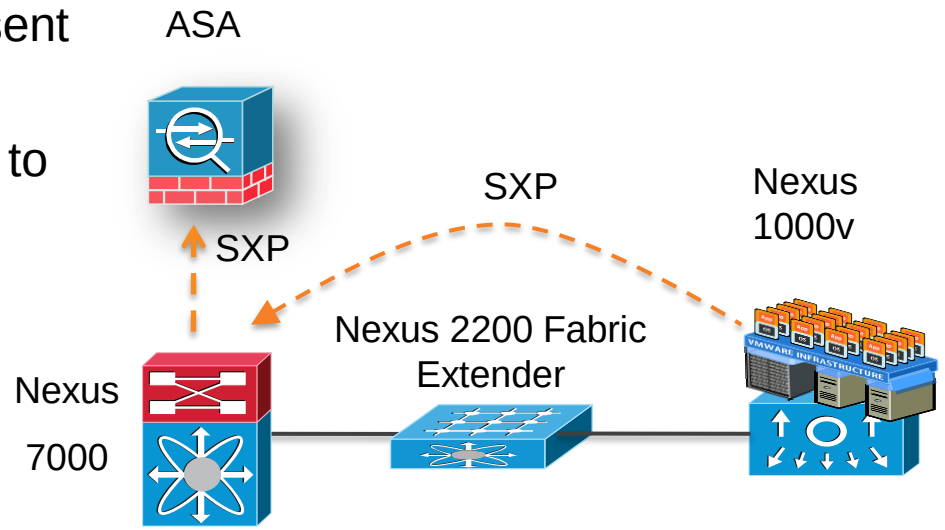
Sources	Production Servers	Development Servers	HR Database	Storage
Production Servers	PERMIT	DENY	DENY	PERMIT
Development Servers	DENY	PERMIT	DENY	PERMIT
HR Database	DENY	DENY	PERMIT	PERMIT
Storage	PERMIT	PERMIT	PERMIT	PERMIT

LOGICAL VIEW



Nexus 7000 / Nexus 1000v Interaction

- Nexus 1000v Port Profile assignment sent to N7000 over SXP (N7k SXP listener)
- N7000 can also send server mappings to ASA over SXP (N7k SXP speaker)



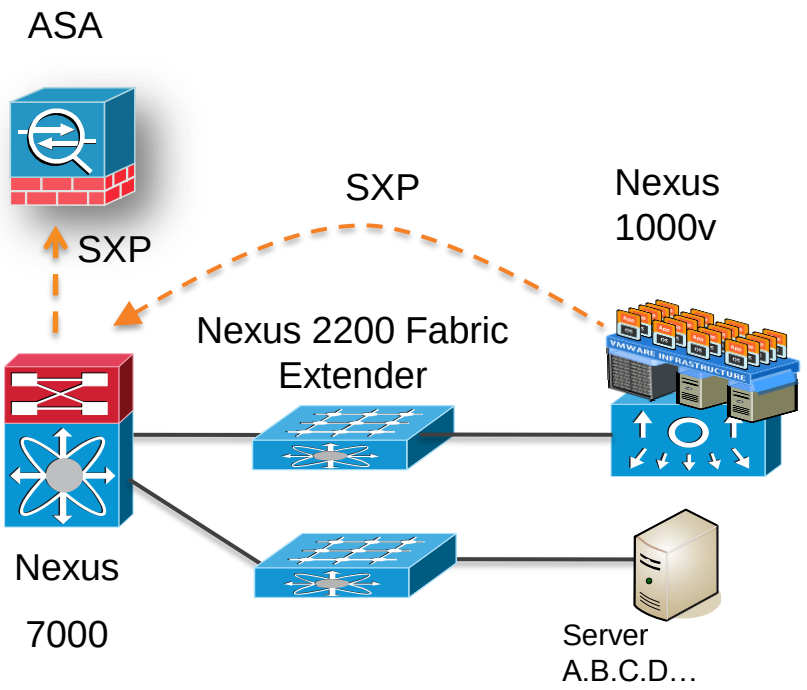

```
Nexus1000VSXP# sho cts ipsgt entries
  Interface      SGT           IP ADDRESS      VRF          Learnt
-------------- ------       --------------- ----------     ---------
Vethernet1      8           10.1.100.121        -          Device Tracking
Vethernet2      7           10.1.100.120        -          Device Tracking
Vethernet3      5           10.1.100.98         -          Device Tracking
Vethernet4      6
Vethernet5      3           10.1.3.108          -          Device Tracking
Vethernet6      6           10.1.3.113          -          Device Tracking
```

Adding Static IP-SGT Mappings

- Nexus 7000 can also classify servers by IP address to SGT mapping
- Mappings can be defined in the switch:-

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

- Mappings can also be pushed from ISE
- N7000 can also send server mappings to ASA over SXP (N7k speaker)

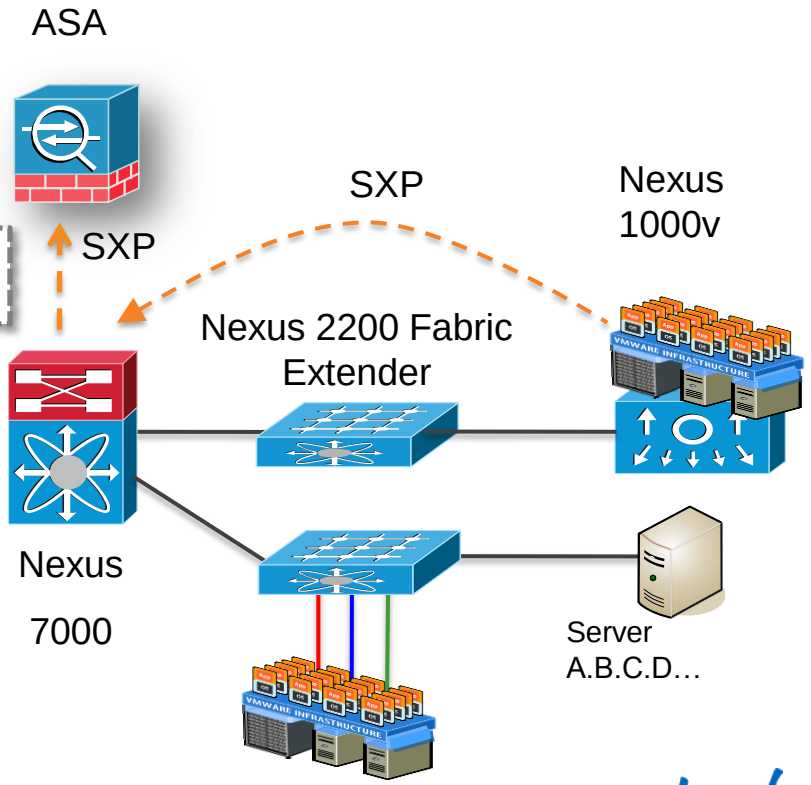


Adding VLAN-SGT Maps

- Classify servers by VLAN they are attached to

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

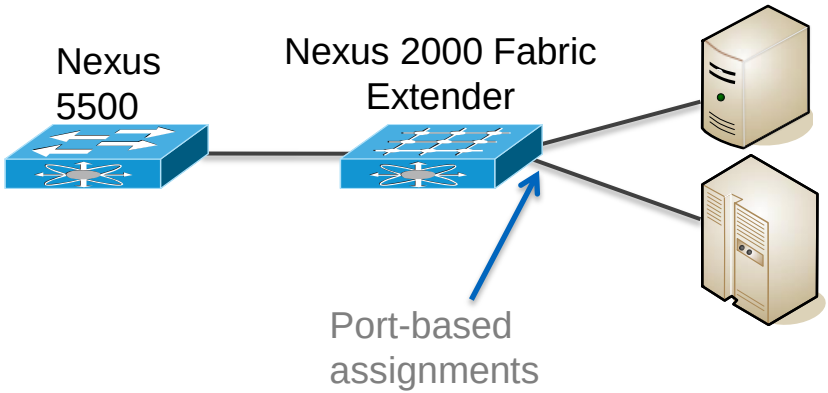
- N7000 will still derive IP-SGT maps from VLANs and send to ASA



Using Nexus 5500 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

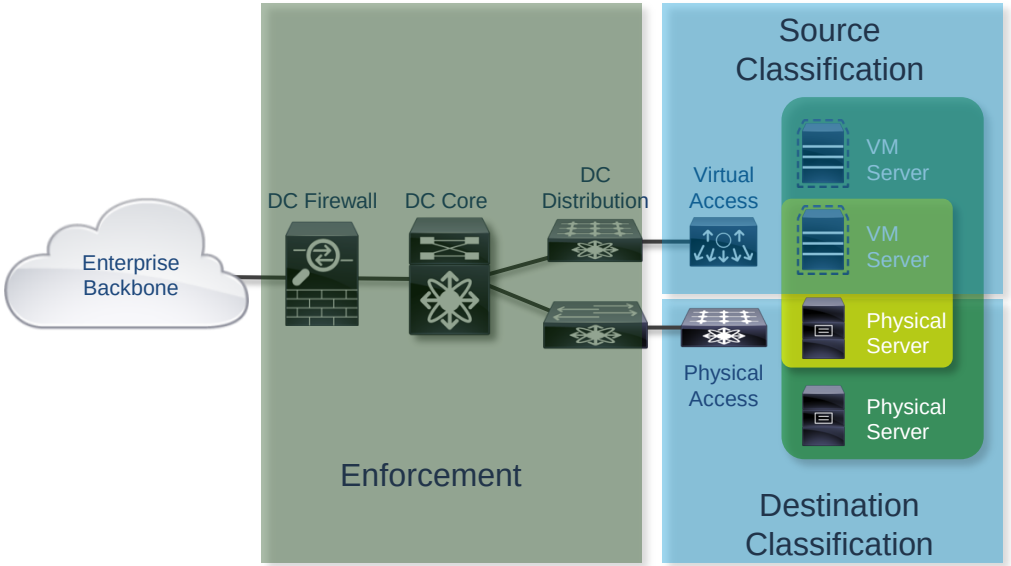
```
interface Ethernet1/20
  cts manual
  policy static sgt <value>
```



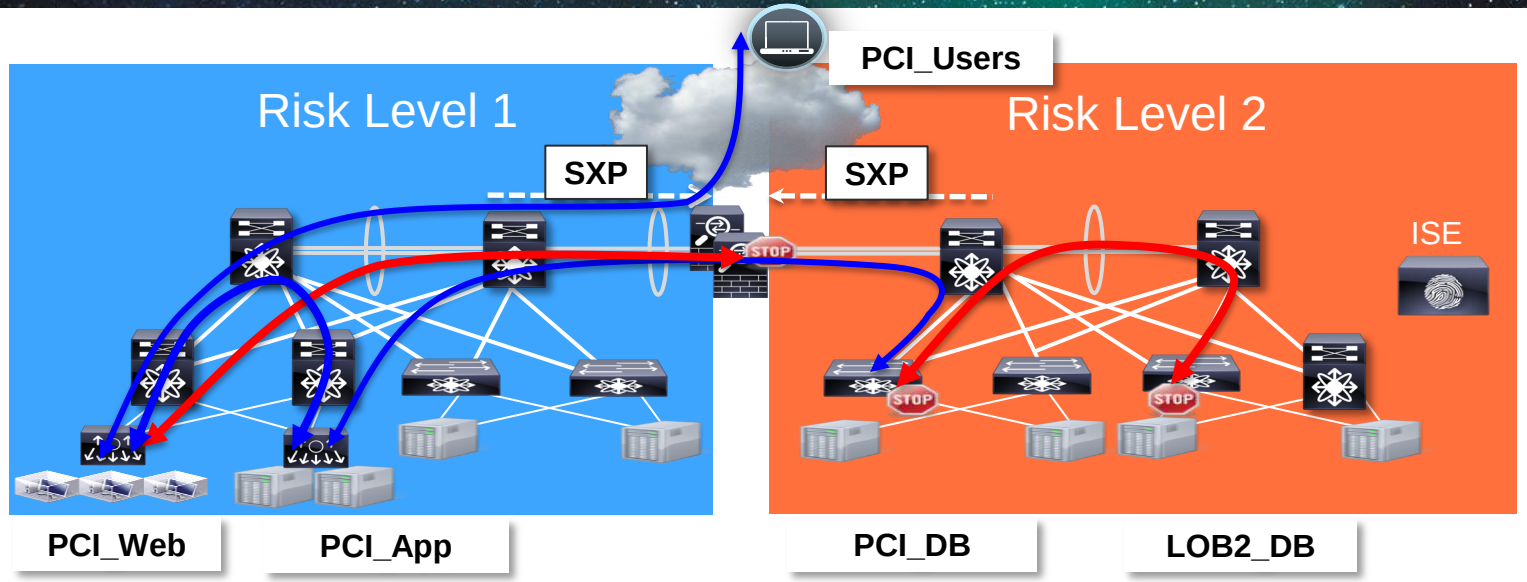
- To send mappings over SXP will also require IP-SGT maps on N5500
- N5500 is not an SXP listener

Server Classifications

- Nexus 1000v Port Profile SGT mappings
- Nexus 7000 VLAN – SGT mappings
- Nexus 7000 IP-SGT mappings
- Nexus 5500 Port-SGT assignments for inline tagging/SGACLs
- Nexus 5500 IP-SGT mappings to send via SXP



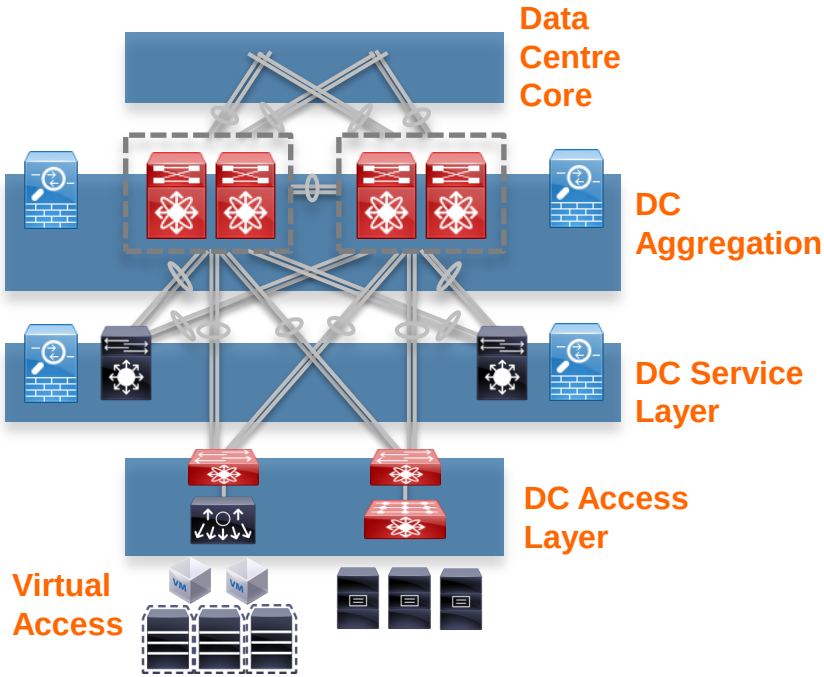
Using SG-FW and SGACL Together in the DC



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

Combining SGACL and SG-FW in the Data Centre

- 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
- **New** SGACL batch programming (needs enabling) & Fragmented SGACL downloads
  - N7000 6.2(6)
  - N5500 6.0(2)N2
- **New** SGT caching + 200k IP-SGT mappings in N7000 6.2(6)



SGACL Guidelines for DC Deployments

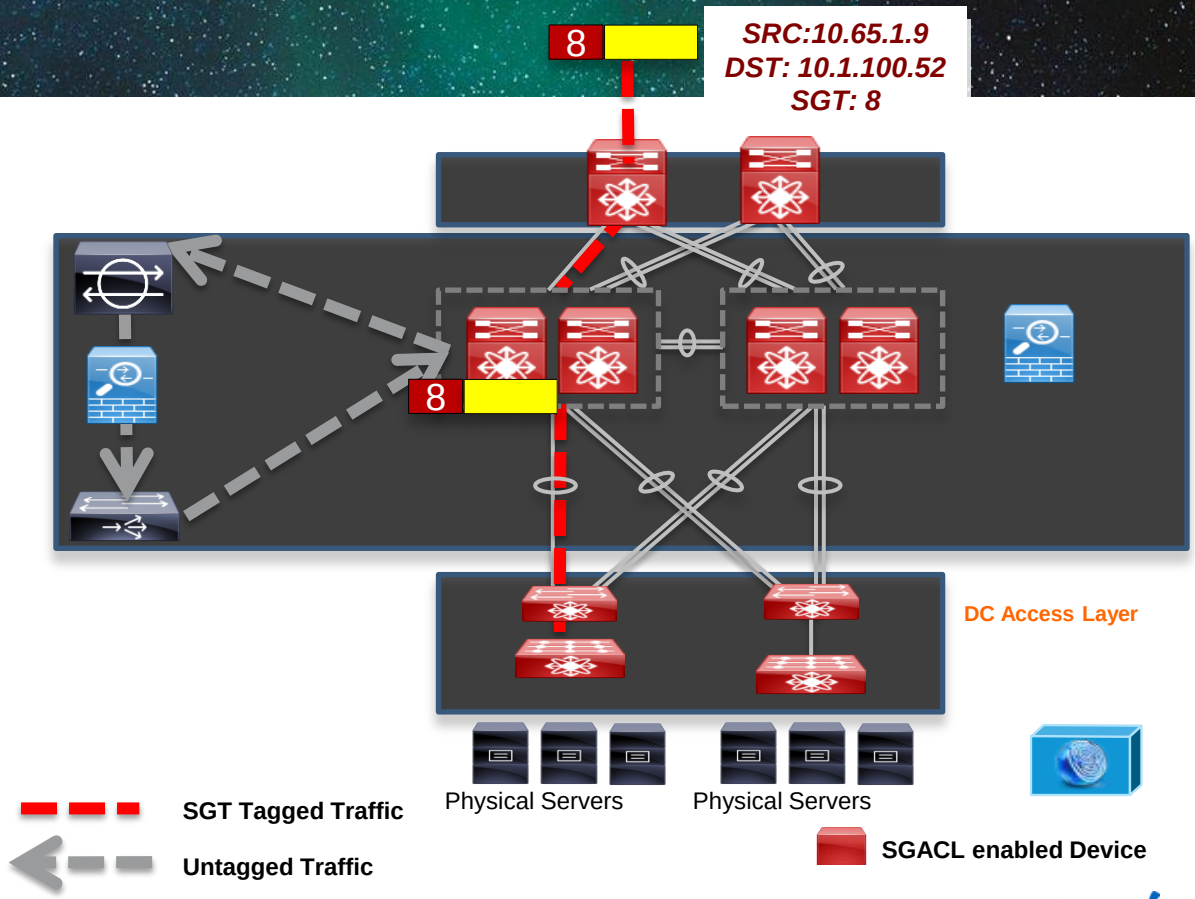
- Nexus 7000 – 16,000 Access Control Entries available
- Nexus 5500 has constraints:
  - 124 SGACL TCAM entries available per bank of 8 ports
  - The sum of the SGACL entries per 8 port bank cannot contain more than 124 permissions in total (diagram shows 3 + 9 as an example)
  - SGACL can be reused extensively - 2000+ SGT,DGT combinations on a N5500 reusing 124 lines of permissions tested

```
WEB-ACL:
permit tcp dst eq 443
permit tcp dst eq 80
deny ip
```

```
HR-DB-ACL:
permit tcp dst eq 443
permit tcp dst eq 80
permit tcp dst eq 22
permit tcp dst eq 135
permit tcp dst eq 136
permit tcp dst eq 137
permit tcp dst eq 138
permit tcp des eq 139
deny ip
```

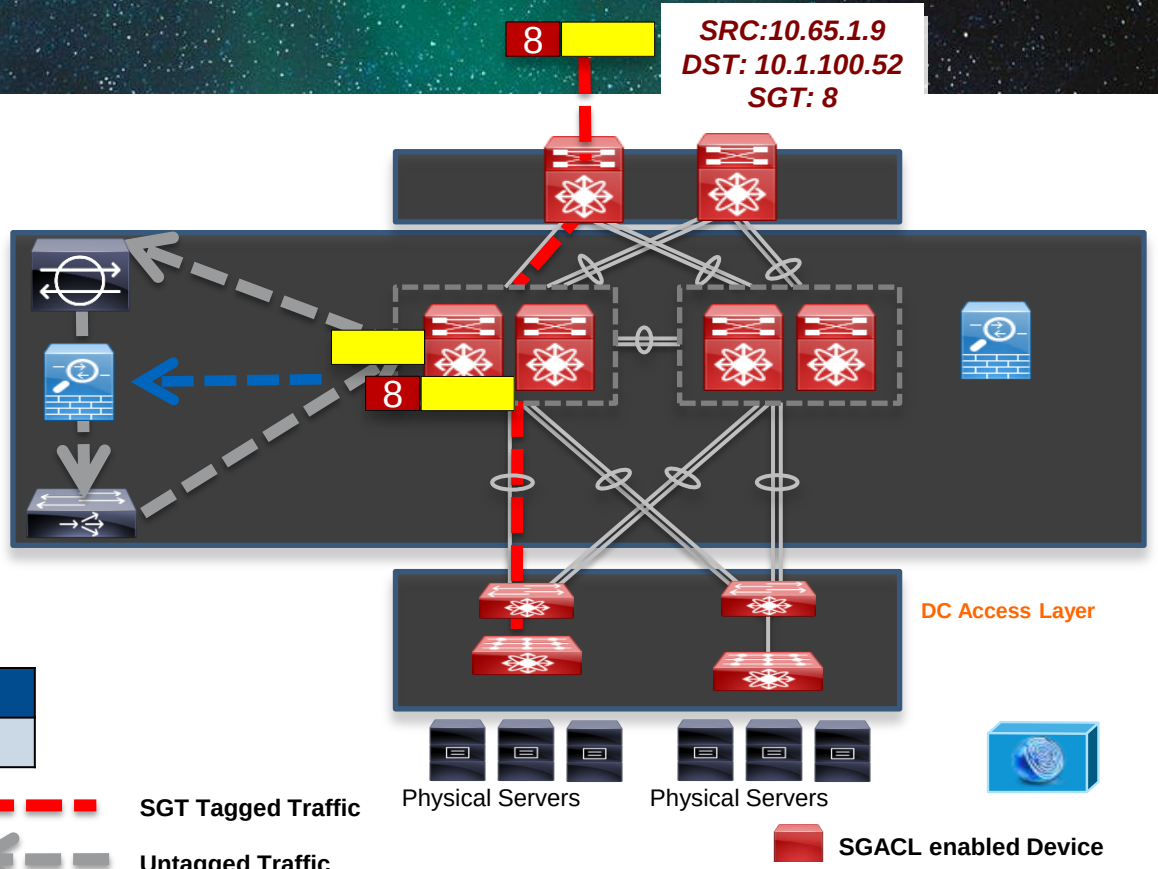
SGT Caching

- Possible 3rd party devices for Server Load Balancing (SLB), Intrusion Prevention Services (IPS), etc
- Caches IP-SGT mappings from data plane
- Passes untagged traffic through services
- Re-tags traffic after service with cached SGT



SGT Caching

- The cached IP-SGT mappings from data plane CAN be used with SXP
- Can send cached IP-SGT mappings to ASA in SXP



IP Address	SGT
10.65.1.9	8 (Employee)

Use Cases: Campus and Branch Segmentation

Campus and Branch Segmentation

POLICY VIEW

Protected Assets

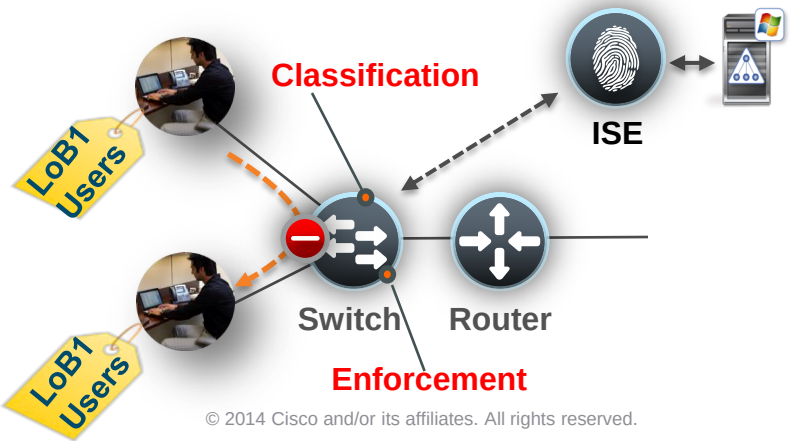
Source	LoB1 Production Users	LoB1 Developers	LoB2 Employees	Guests	Internet Access
LoB1 Production Users	Malware Block	Malware Block	DENY	DENY	PERMIT
LoB1 Developers	Malware Block	Malware Block	DENY		
LoB2 Employees	DENY	DENY	Malware Block		
Guest	DENY	DENY	DENY		

Malware Blocking ACL

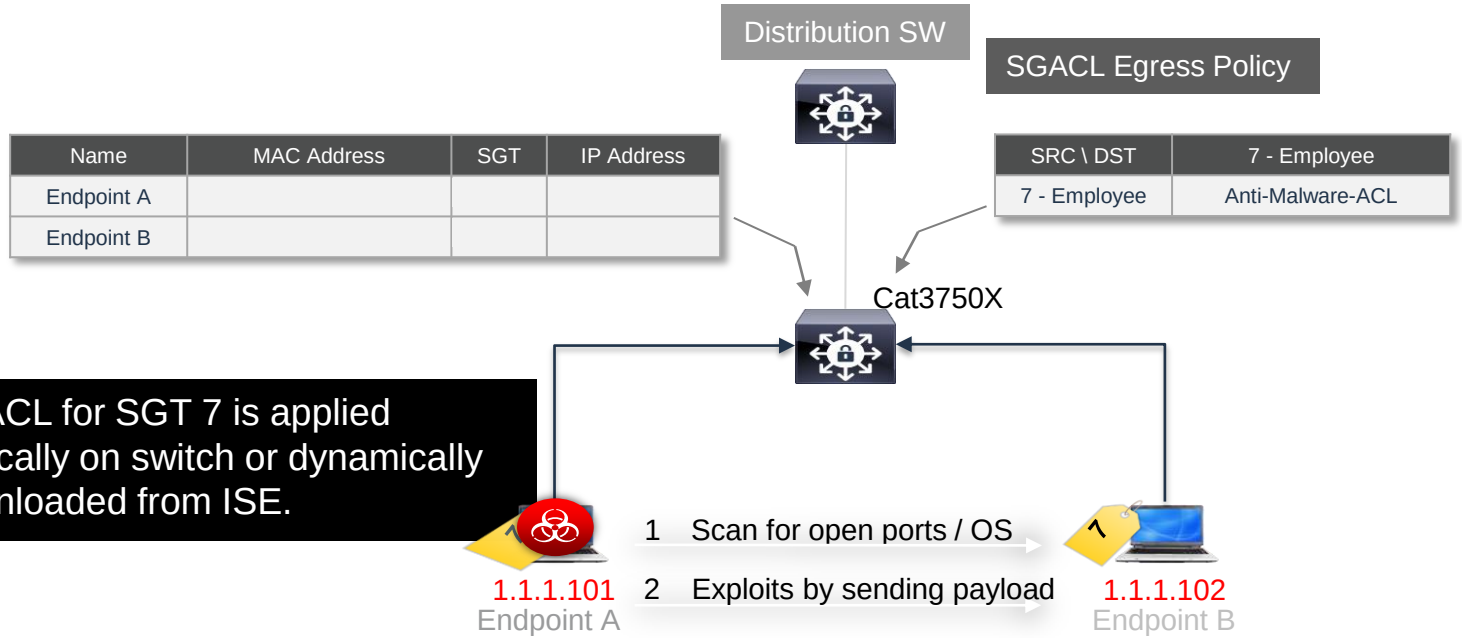
```
Deny tcp dst eq 445 log
Deny tcp dst range 137 139 log
Permit all
```

*LoB = Line of Business

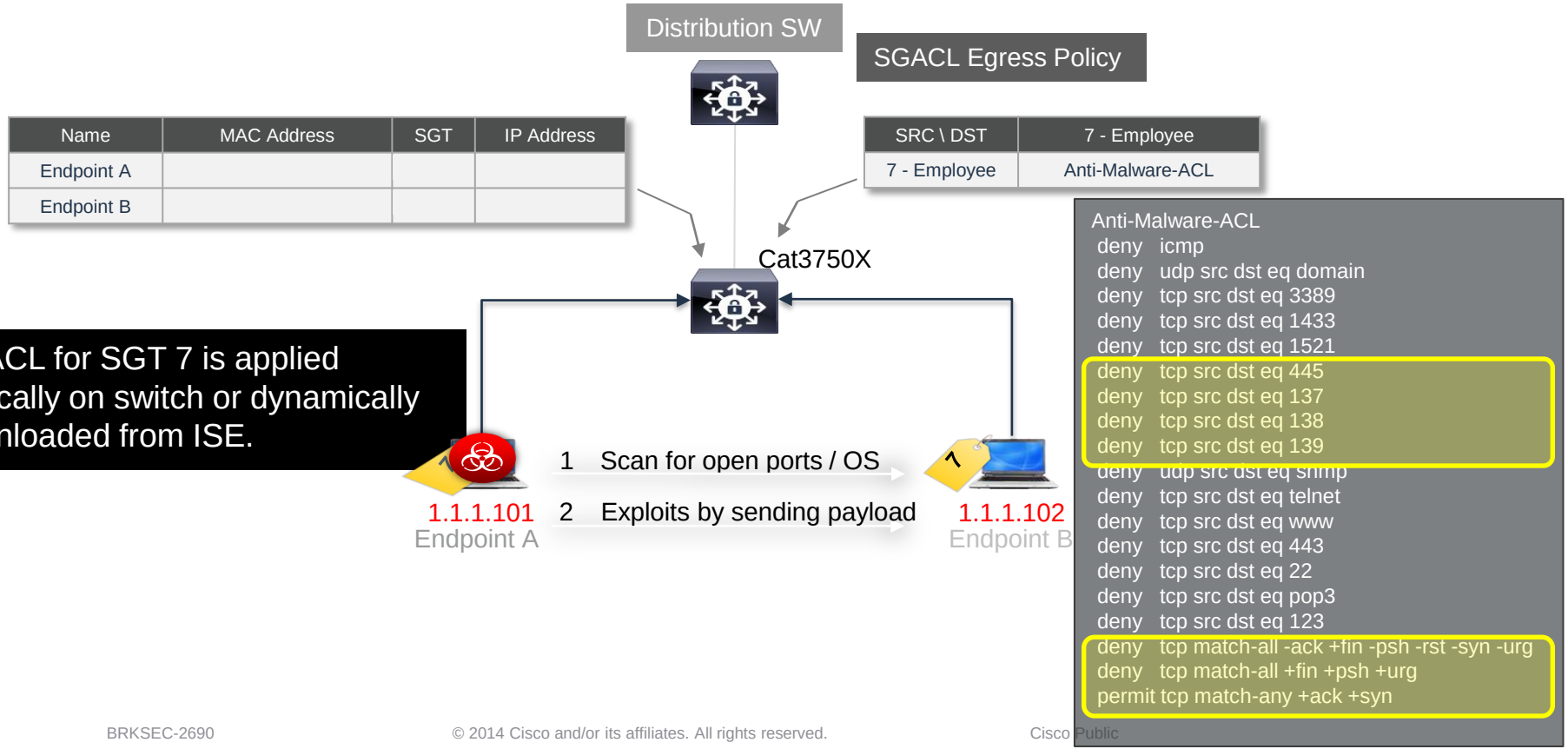
LOGICAL VIEW



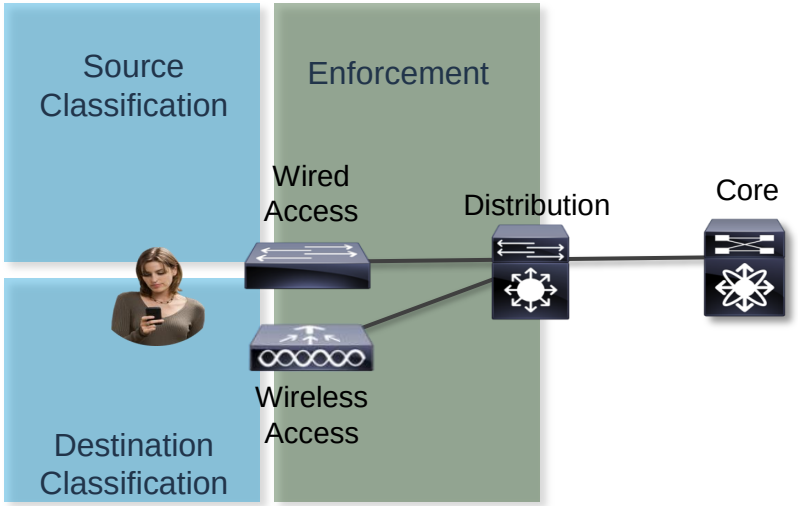
Restricting Malware Recon/Propagation



Restricting Malware Recon/Propagation



Campus Segmentation

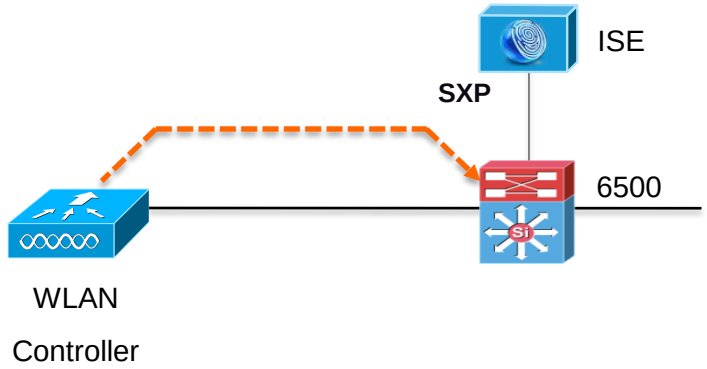


SGACL segmentation available on :-

- Catalyst 3560-X, 3750-X
- Catalyst 3850
- Catalyst 4500E (7E), 4500X
- Catalyst 6500E (2T)
- WLC 5760

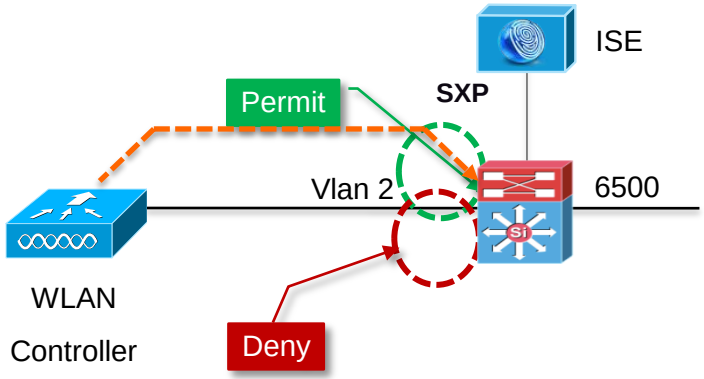
- Other WLC platforms can also be configured to forward all P2P traffic into SGACL-capable switch for policy enforcement
- SXP from WLC to switch propagates role info for the Wireless users

Implementing Wireless User – User Policy Enforcement



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

Implementing Wireless User – User Policy Enforcement

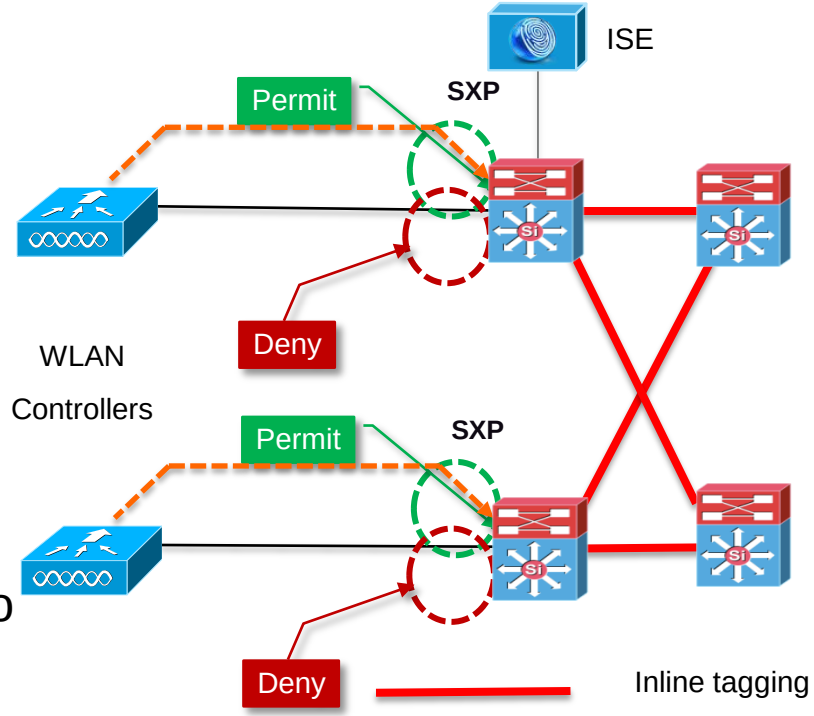


- Apply user-user policies as defined in ISE on traffic from the WLC

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

Implementing Wireless User – User Policy Enforcement

- If inline tagging is enabled between the switches – user to user policies applied to WLAN users across the campus

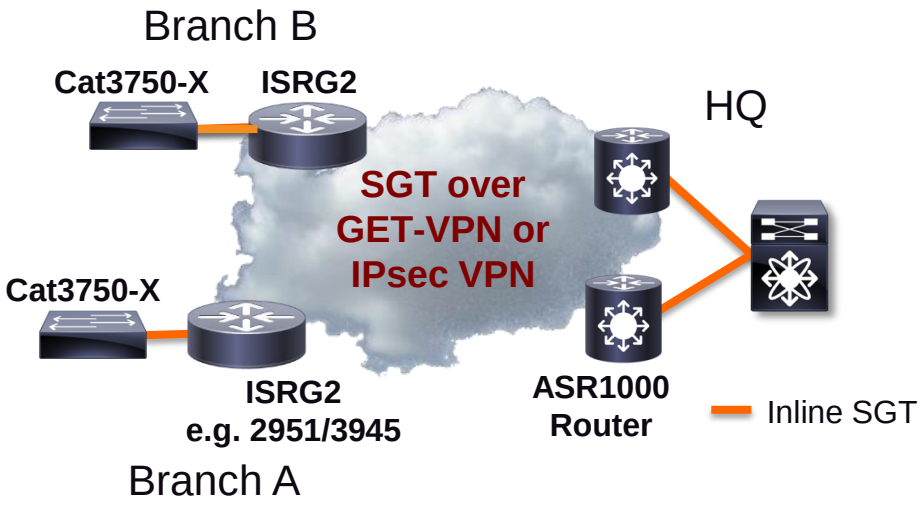


TrustSec Support for WLAN

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	5508, WiSM2 8510, 7510	None - could use VLAN-SGT mapping as workaround	

Extending Inline Tagging Across WAN to Branches

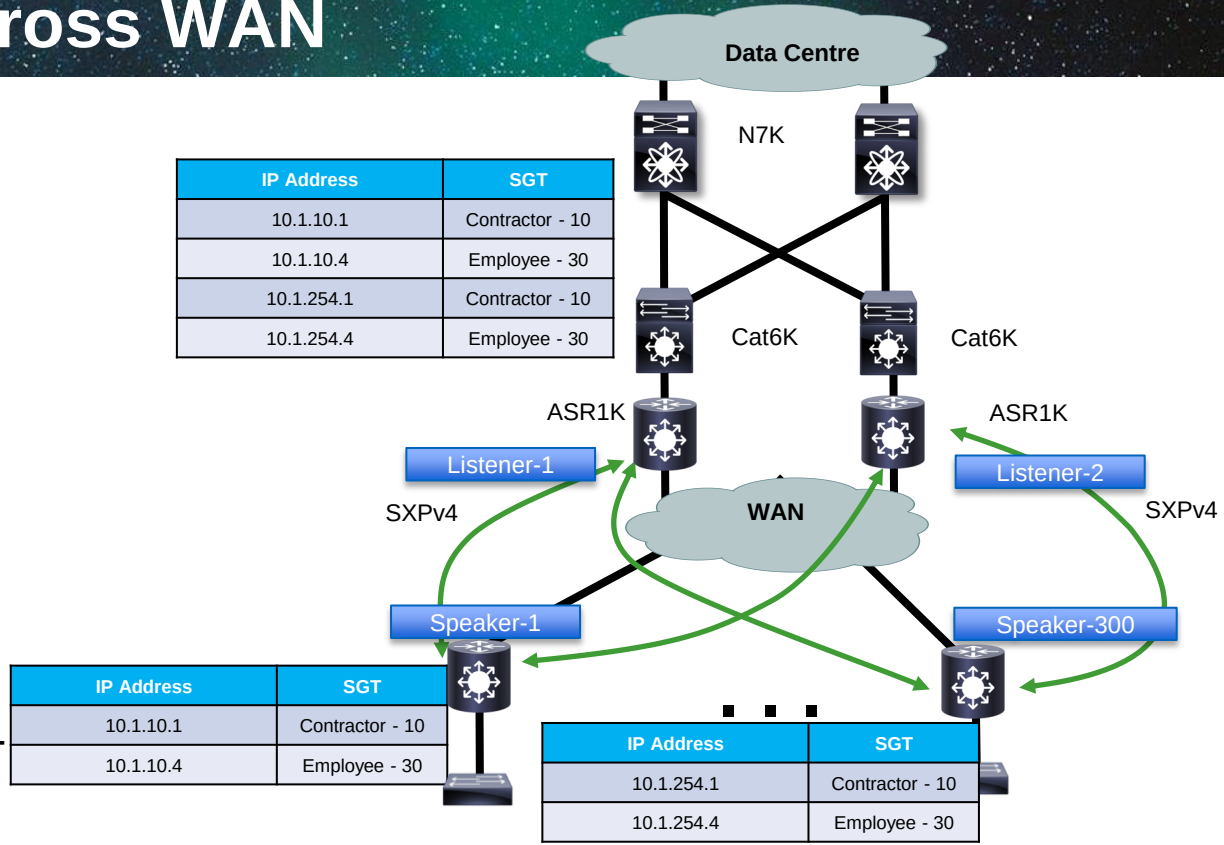
- Inline tagging across WAN :
  - ISR G2 IOS 15.4(1)T &
  - ASR1000 15.4(1)S
- Inline tagging on built-in ISRG2 & ASR 1000 Ethernet interfaces (all except 800 series ISR)
- Carries SGT inline across GET-VPN and IPsec VPN



- Can also use SGT-aware Zone-based Firewall in branch and DC WAN edge for reasons like PCI compliance
- SGT allows more dynamic classification in the branch and DC WAN edge
- SGT is a source criteria only in ISR FW, Source or Dest in ASR 1000

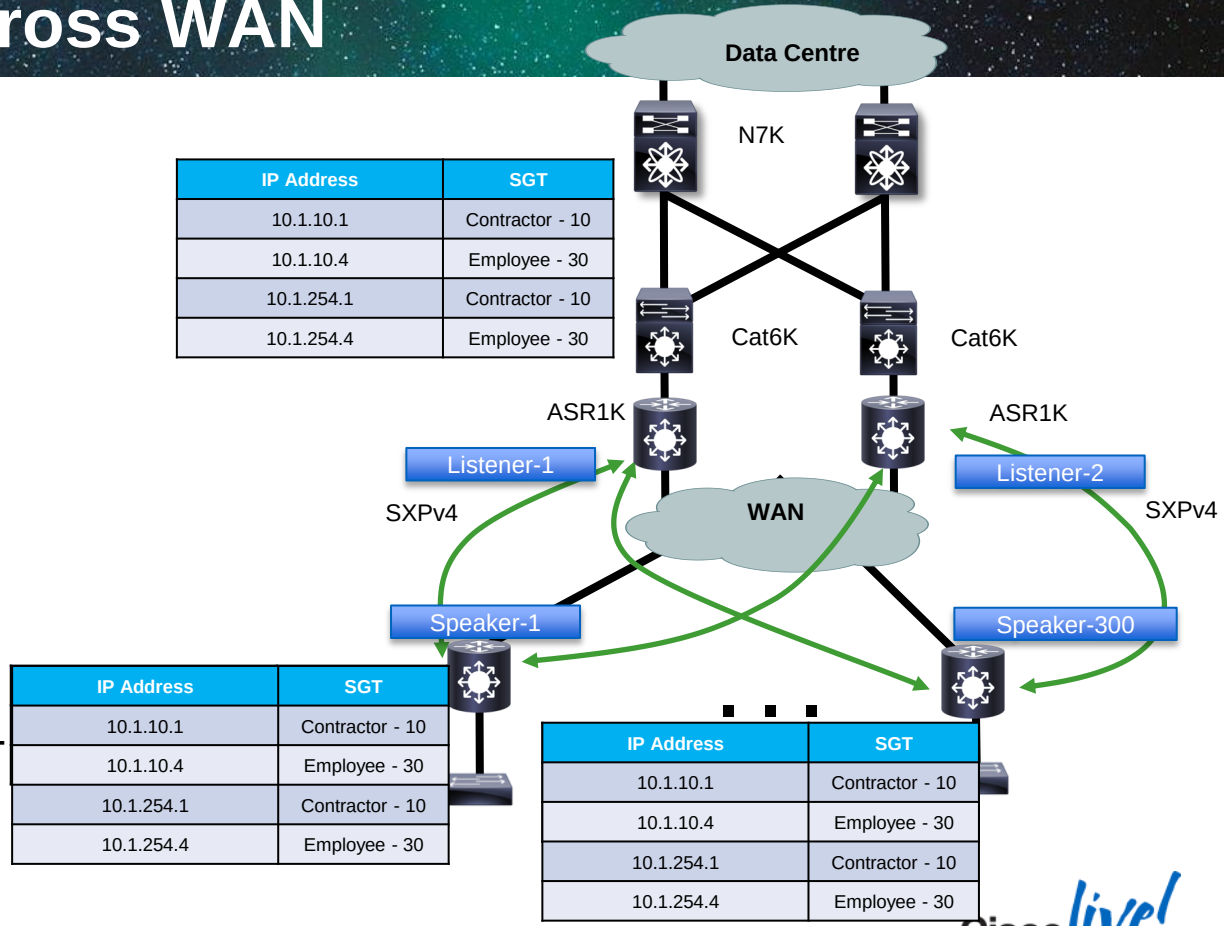
Extending SXP Across WAN

- Bidirectional SXP with Loop Detection available now:
  - ISRG2 – 15.3(2)T
  - ASR1000 IOS XE 3.9
- 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 with this approach



Extending SXP Across WAN

- Bidirectional SXP with Loop Detection available now:
  - ISRG2 – 15.3(2)T
  - ASR1000 IOS XE 3.9
- 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 with this approach



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

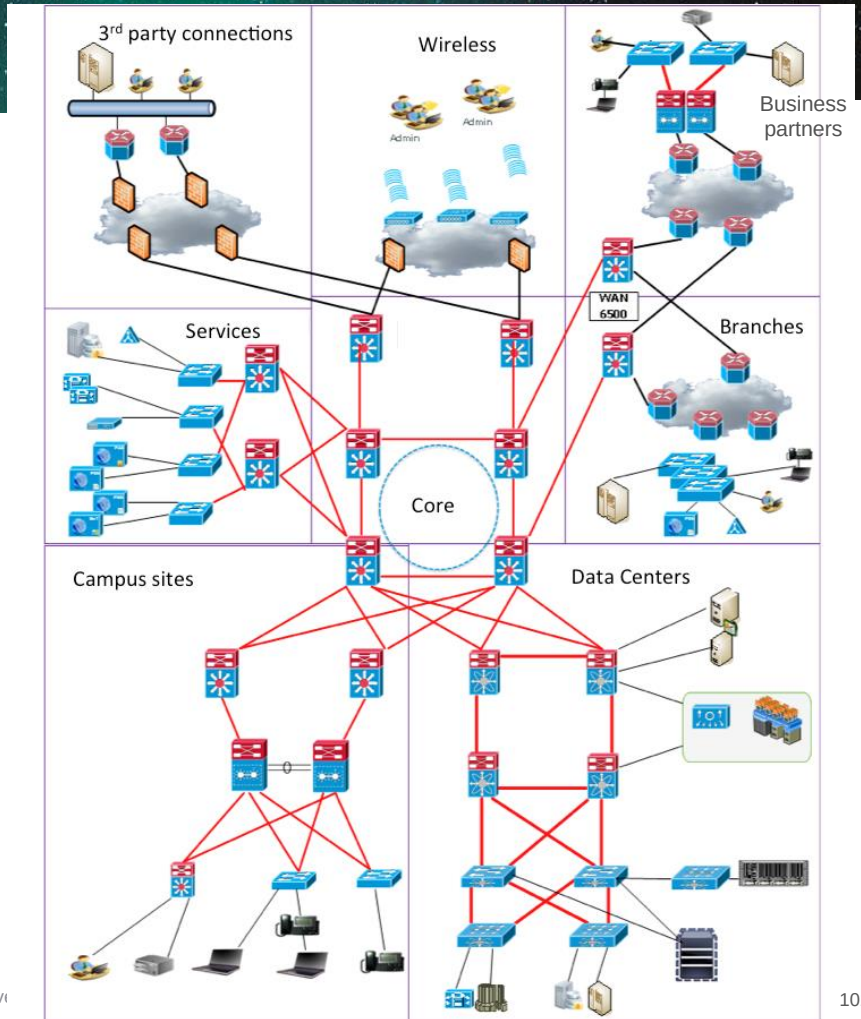
IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30




Case Study

Compliance Use-case

- Meeting compliance requirements with minimal deployment impact
- Use TrustSec to enforce policy on:
  - User to DC access controls
  - DC Segmentation
  - User Segmentation
  - Business partner access
- Security Group Tags applied to
  - Users
  - Servers
  - Business partners
  - 3rd party connections

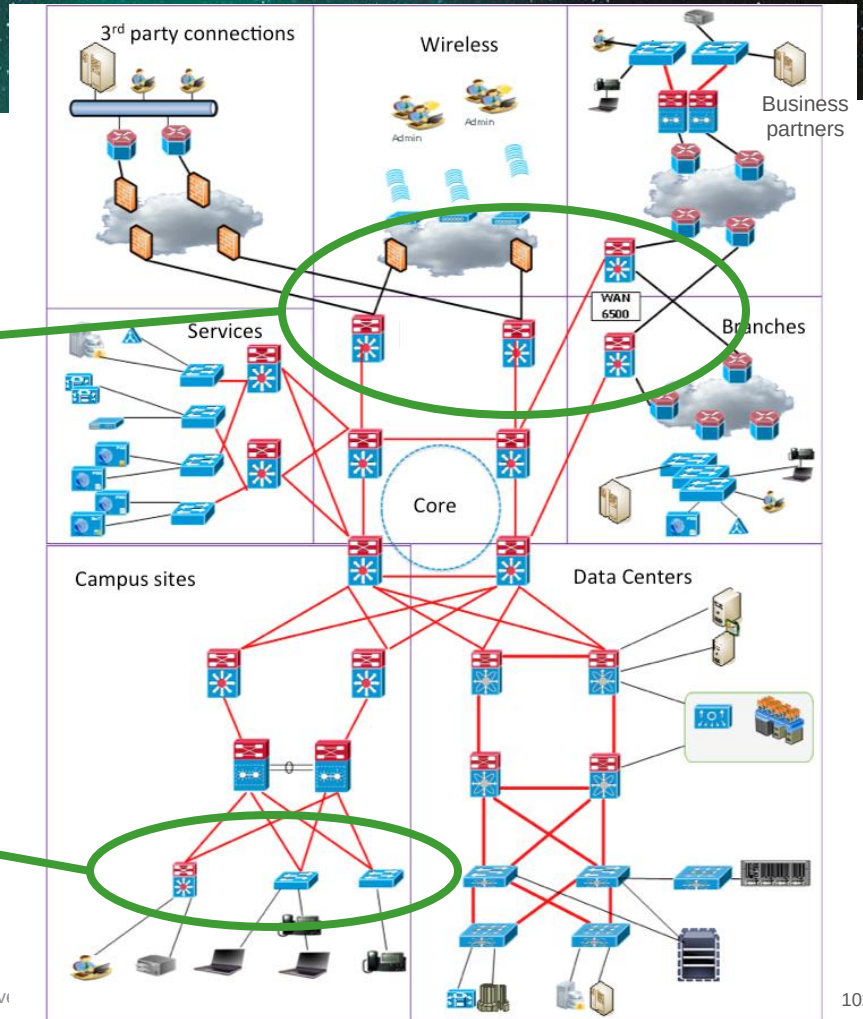


Classifying Access

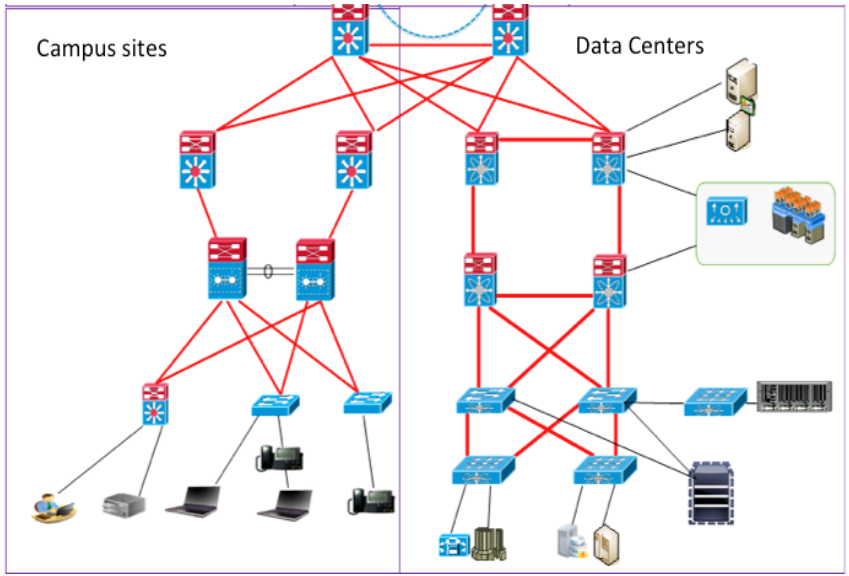
- SGTs assigned to L3 interfaces
  - All traffic on a given interface tagged as from that business partner
- Subnet to SGT mappings
  - SGT assigned to selected subnets of external networks

User/Device classifications

- 802.1X Monitor Mode/Low-impact mode
- Profiling & MAC-Auth-Bypass



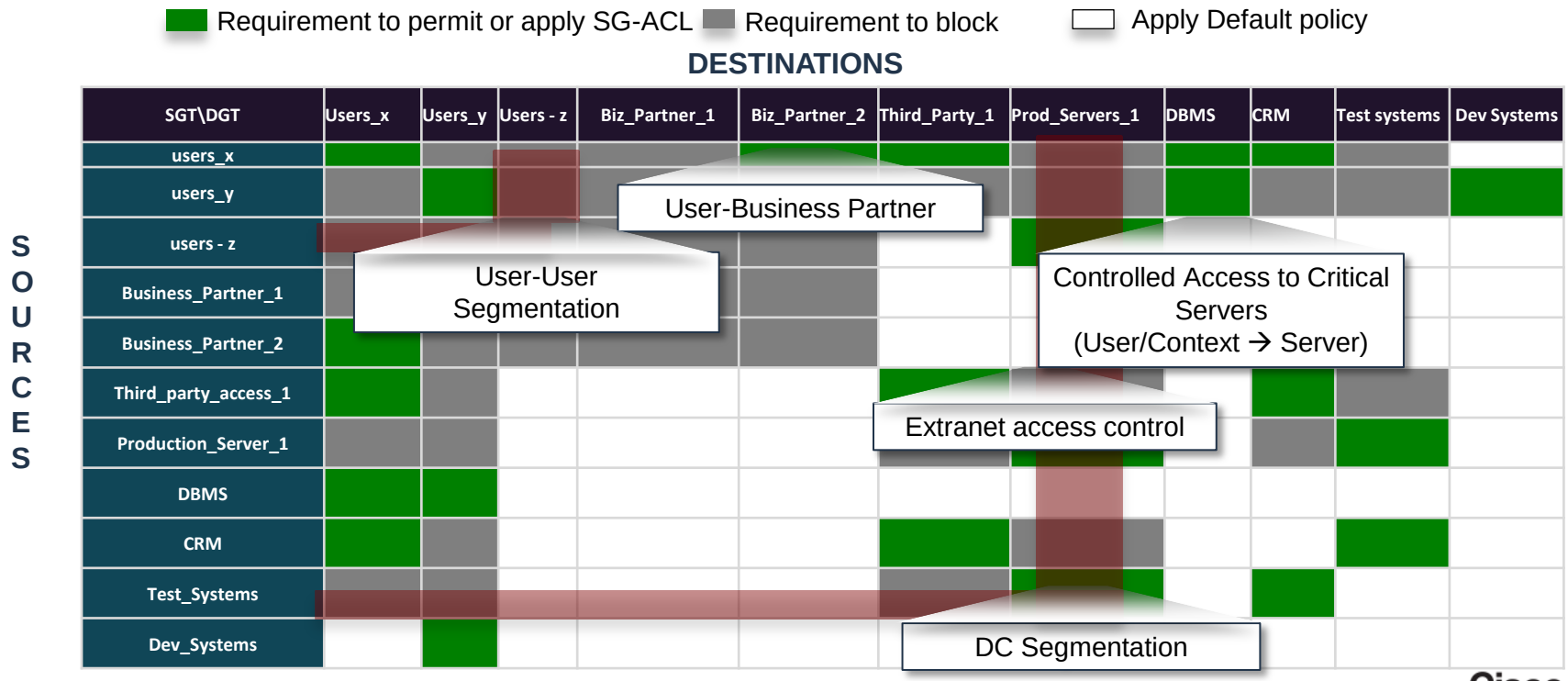
Classifications – in Data Centres



Servers and virtual desktops classified using:-

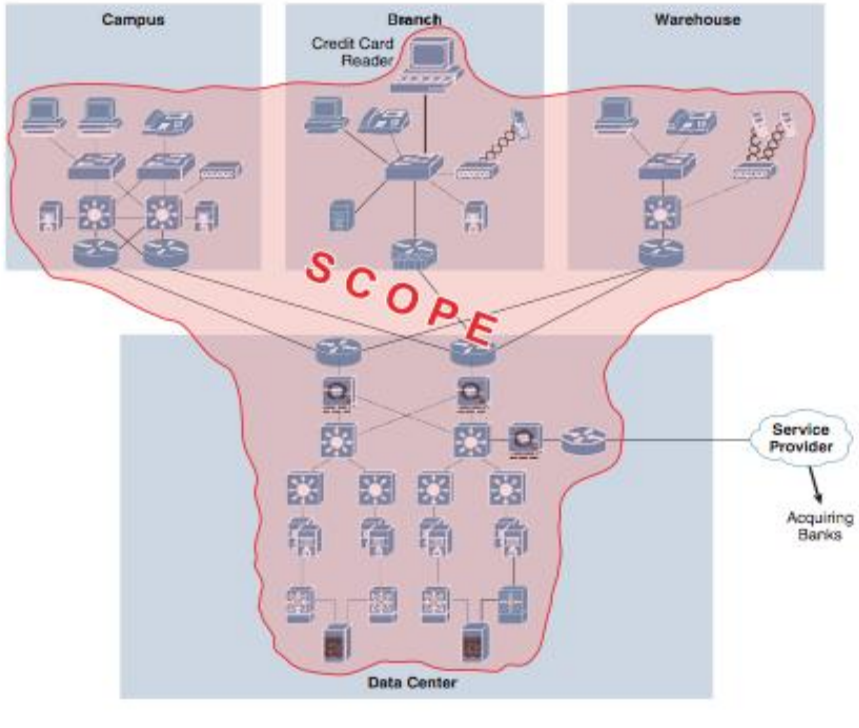
- IP-SGT used for servers:
  - Mappings pushed from ISE to N7000 switches
- Port Profile SGT mappings
  - New VMs are associated with Nexus 1000V Port Profiles
  - N1000v sends SGT assignment to N7000s
- VLAN – SGT mappings
  - (N7000 for some virtual systems)
- Port – SGT mappings used for physical servers
  - (N5500 / N2000 / various FEX)

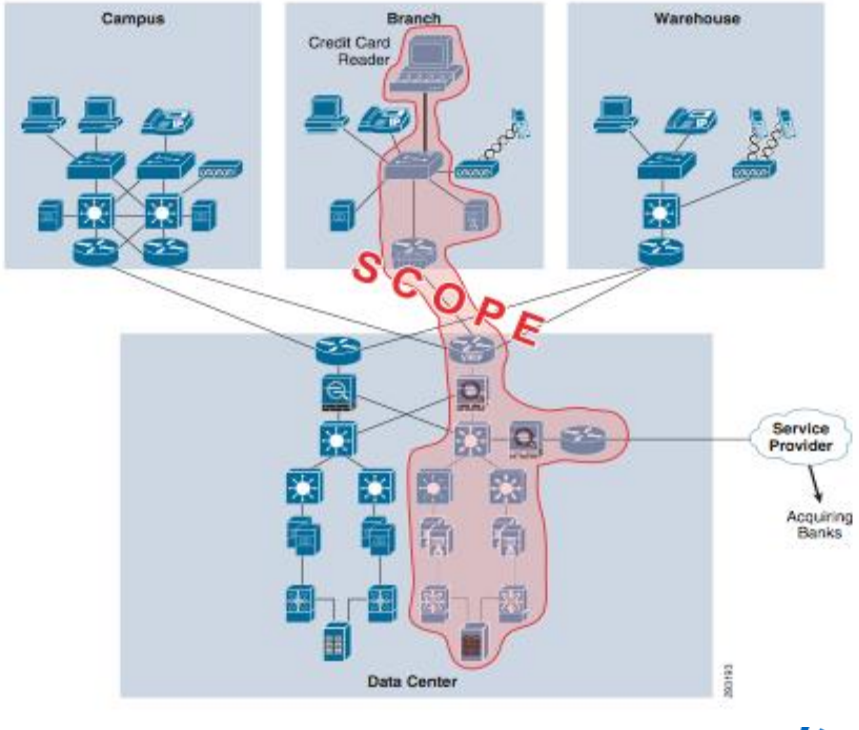
Policy Matrix



PCI Compliance

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

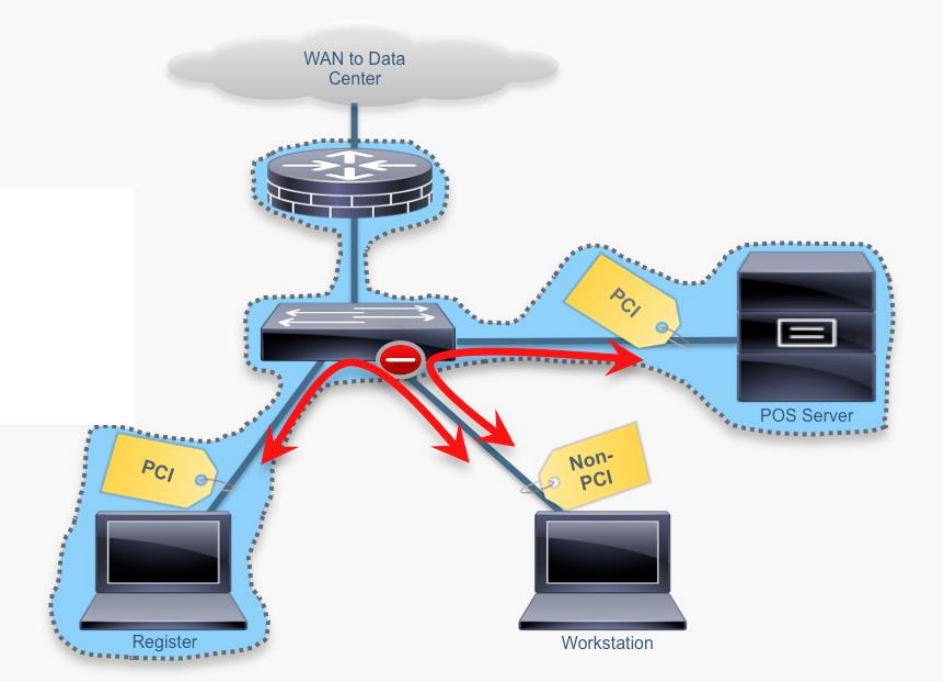
Use Case 1: PCI Scope Reduction with SGT- Wired

Legend:

Segmentation enforcement

PCI scope

All devices in same VLAN



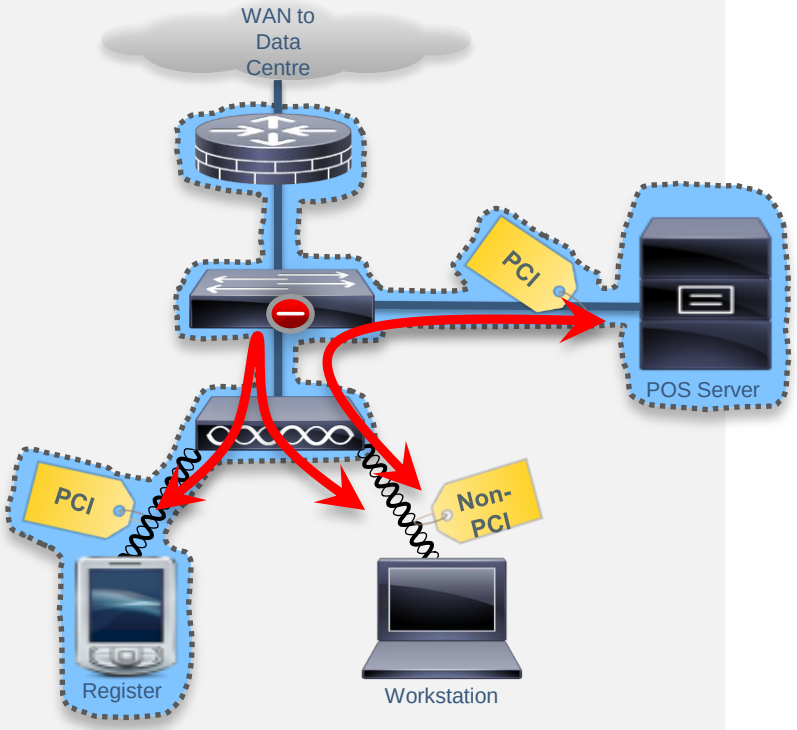
Use Case 2: PCI Scope Reduction with SGT- WLAN

Legend:

Segmentation enforcement

PCI scope

All devices in same VLAN and SSID

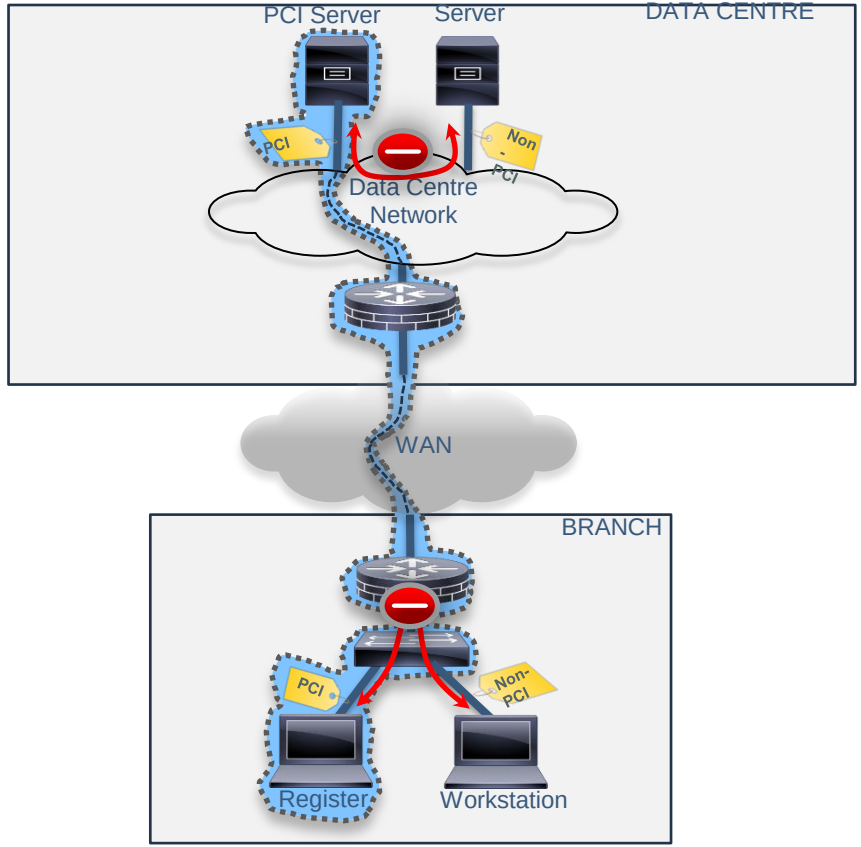


3: PCI Scope Reduction – Branch and Data Centre

Legend:

Segmentation enforcement

PCI scope






Summary

Summary

- TrustSec can be deployed for multiple use-cases
  - 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
- TrustSec SGT can mean
  - Centralised policy for complete network
  - Distributed enforcement and scale
  - No device-specific ACLs or rules to manage - one place to audit
  - Servers can cycle through Dev>UAT> Prod without readdressing
- 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

Links

- For more info:
  - http://www.cisco.com/go/trustsec
- TrustSec platform support matrix
  - http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html
- TrustSec and ISE Deployment Guides:
  - http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.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
- IETF SXP Draft:
  - http://tools.ietf.org/html/draft-smith-kandula-sxp-00




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo 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 www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 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


CISCO
TM