TOMORROW starts here.

Advanced Security Group Tags: The Detailed Walk Through

BRKSEC-3690

Darrin Miller
Distinguished TME

Agenda

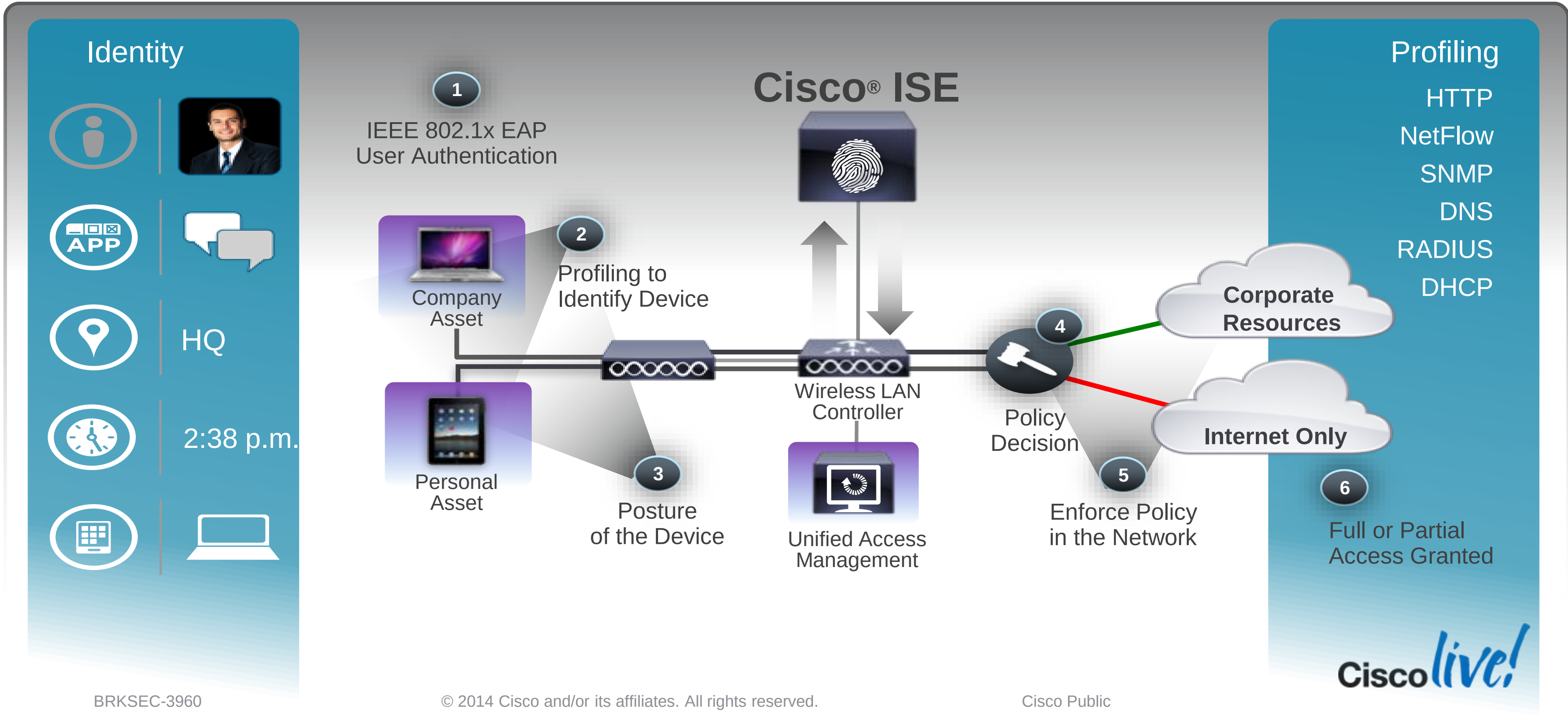
- Security Group Tag (SGT) Review
  - SGT Drivers
  - SGT Technology Review
- Use Case Review
  - Use Case Review
  - Customer Case Overviews
- Design Consideration and Implementation Details
  - Campus
  - Branch
  - Data Centre
- Summary

Security Group Tag (SGT) Review

Policy: Who, What, Where, When, and How?

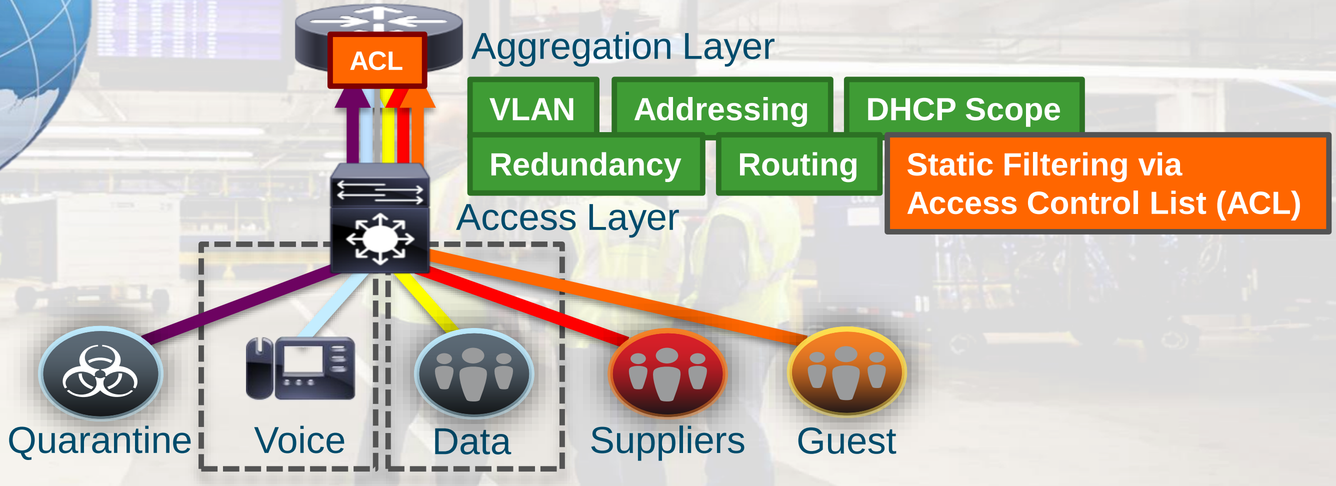
Network Access Workflow

Policy-governed Unified Access



Policy and Segmentation

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

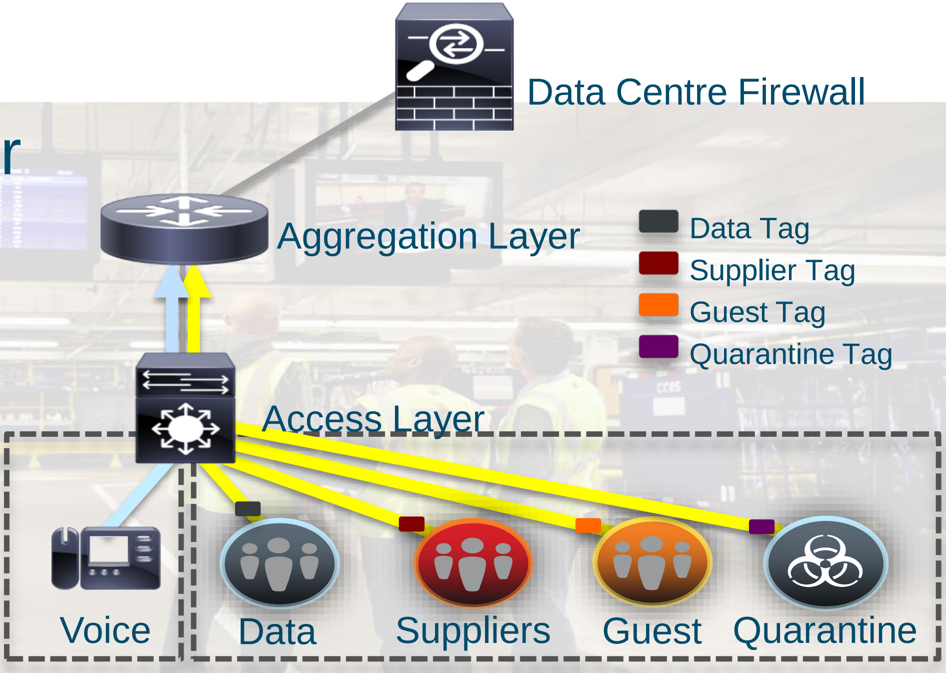


Simple Segmentation with 2 VLANs

More Policies using more VLANs

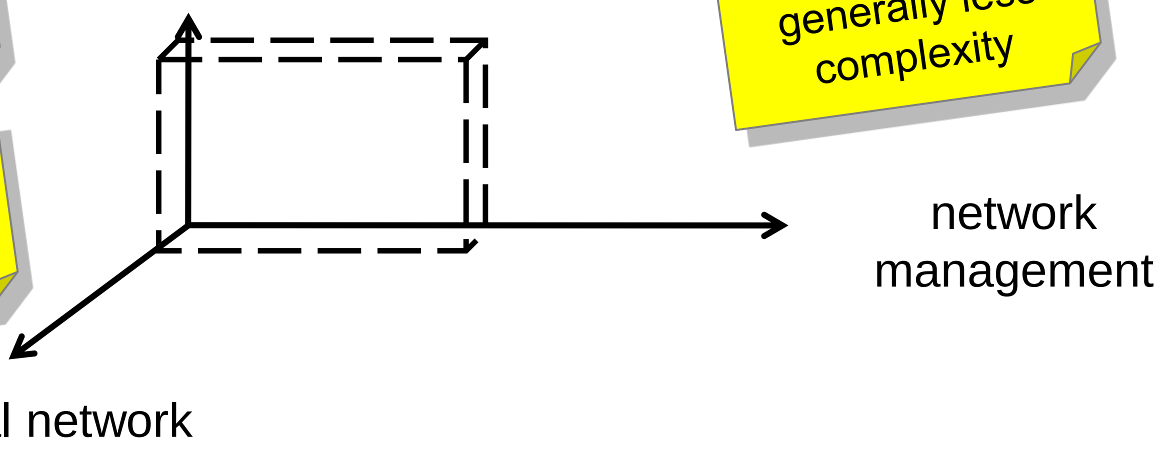
Segmentation with Security Group

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



Retaining initial VLAN/Subnet Design

"State" – Traditional Role Based Access



The operator constitutes state

You can shift complexity

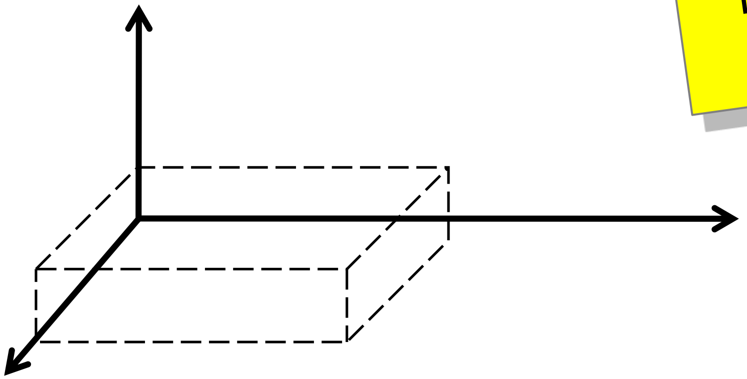
Less human intervention: generally less complexity

The "Complexity Cube"

“State” – Desired End State

The operator constitutes state

You can shift complexity

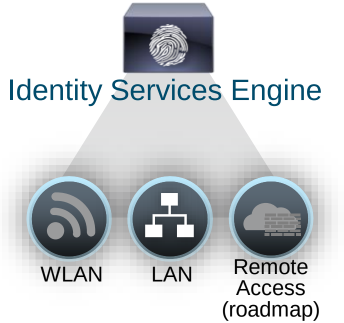


Shifting state may reduce complexity

The “Complexity Cube”

SGT Architecture Components

Policy Management



Identity Services Engine

WLAN

LAN

Remote Access (roadmap)

Classification

Catalyst 2K
Catalyst 3K

Catalyst 4K
Catalyst 6K

WLC (7.2)

Nexus 7000
Nexus 5000

Nexus 1000v

Transport

Cat 2K-S (SXP)
Cat 3K (SXP)
Cat 3K-X (SXP/Inline)
Cat 4K Sup7 (SXP/Inline)
Cat 6K Sup720 (SXP)
Cat 6K Sup2T (SXP/Inline)

N7K (SXP/Inline)
N5K (SXP Speaker/Inline)
N1Kv (SXP Speaker)

ASR1K (SXP/Inline)
ISR G2 (SXP/Inline)
ASA (SXP)

Enforcement

N7K / N5K
(SGACL)

Cat6K/4K
(SGACL)

Cat3K-X/3850
(SGACL)

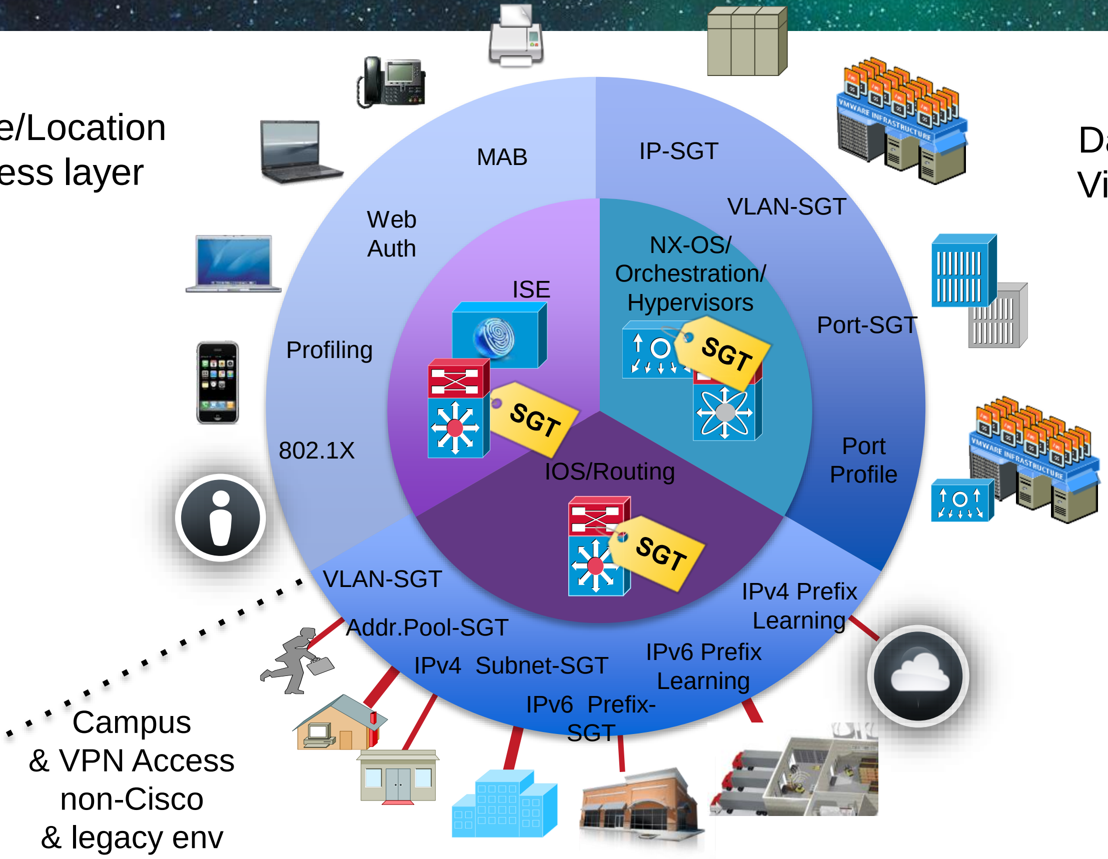
ASA (SGFW)

ASR1K/ISRG2
(SGFW)

TrustSec Classification Functions

User/Device/Location
Cisco access layer

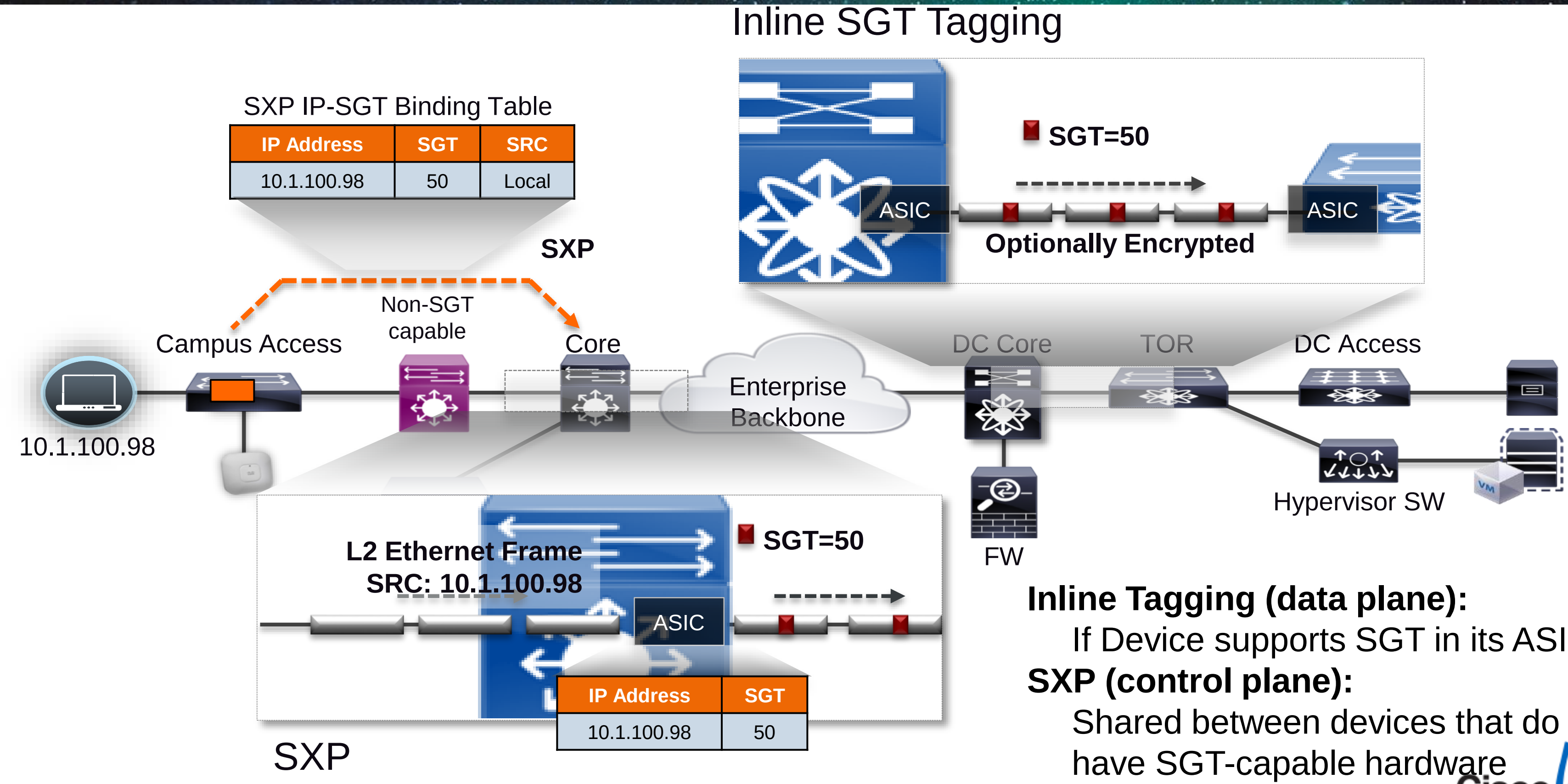
Data Centre/
Virtualisation



Campus
& VPN Access
non-Cisco
& legacy env

Business Partners & Supplier access controls

SGT Transport Mechanism



SXP IP-SGT Binding Table

IP Address	SGT	SRC
10.1.100.98	50	Local

IP Address	SGT
10.1.100.98	50

Inline Tagging (data plane):

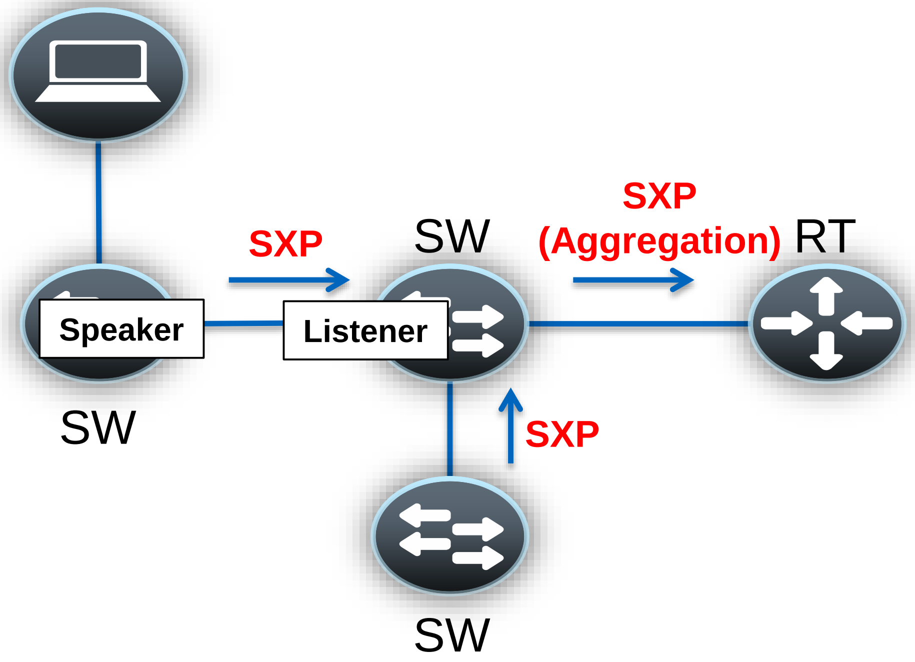
If Device supports SGT in its ASIC

SXP (control plane):

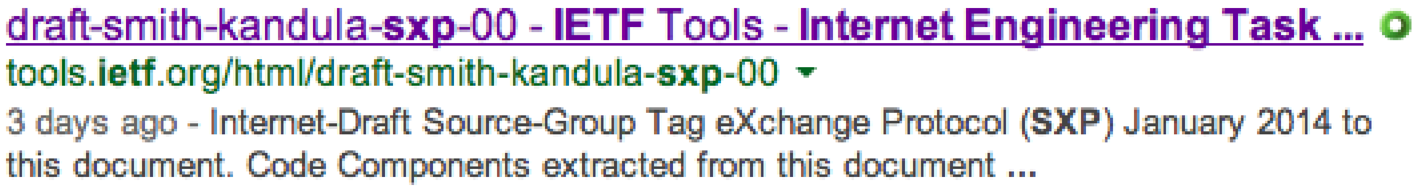
Shared between devices that do not have SGT-capable hardware

SGT Exchange Protocol

- Control plane protocol that conveys the IP-SGT map of endpoints to enforcement point
- Uses TCP as the transport layer
- Accelerate deployment of SGTs
- Support Single Hop SXP & Multi-Hop SXP (aggregation)
- Two roles: Speaker (initiator) and Listener (receiver)
- Loop protection with version 4



SXP Informational Draft



draft-smith-kandula-**sxp**-00 - **IETF** Tools - Internet Engineering Task ...

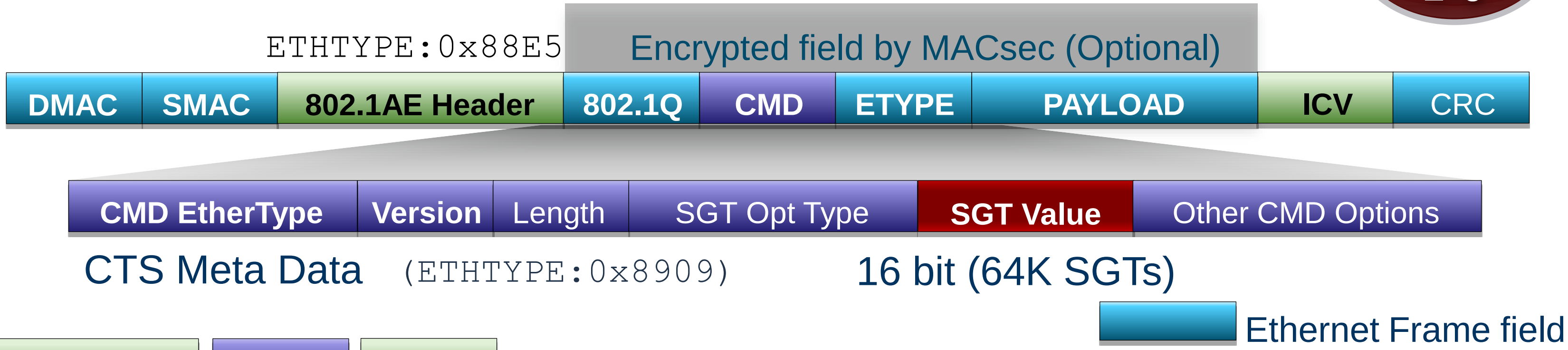
tools.**ietf**.org/html/draft-smith-kandula-**sxp**-00

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

Inline Security Group Tagging

Security
Group
Tag



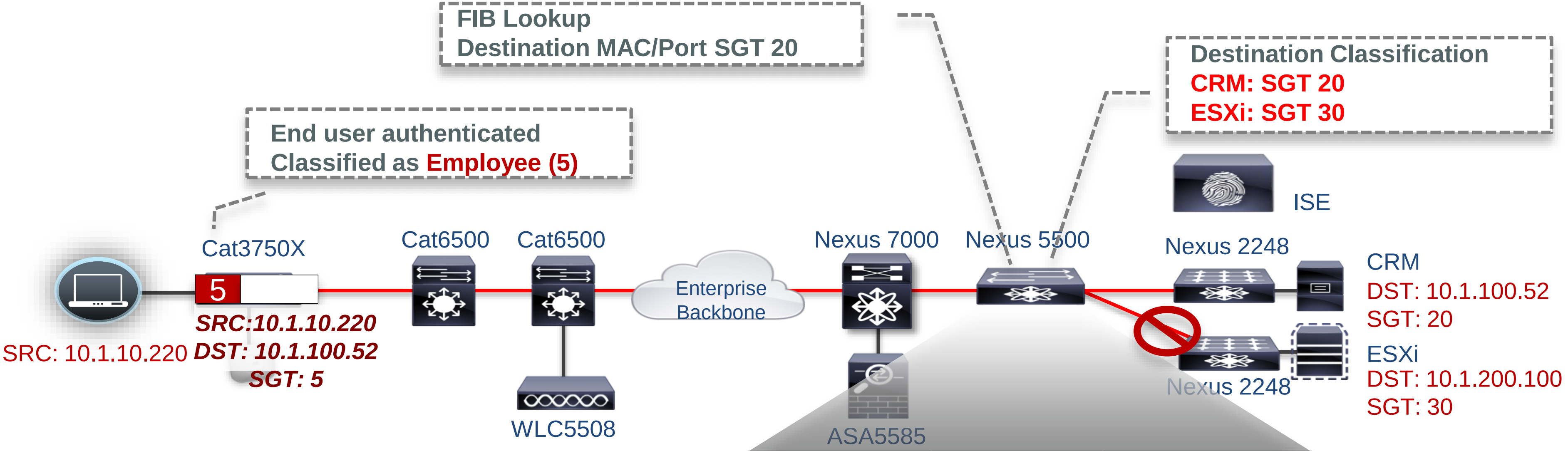
- **802.1AE Header** **CMD** **ICV** are the L2 802.1AE + TrustSec overhead
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 40 bytes (~1600 bytes with 1552 bytes MTU)
- MACsec is optional for capable hardware

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

End to End SGT Tagging



FIB Lookup
Destination MAC/Port SGT 20

Destination Classification
CRM: SGT 20
ESXi: SGT 30

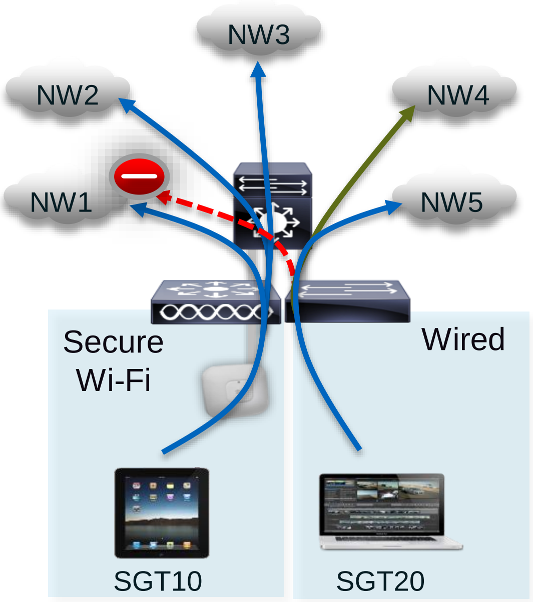
End user authenticated
Classified as **Employee (5)**

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

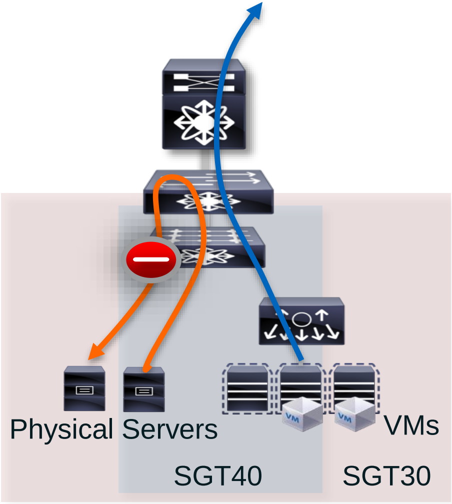
L2 SGT Tagging

Use Case Review

Common SGT Use Cases



Resource Access Control



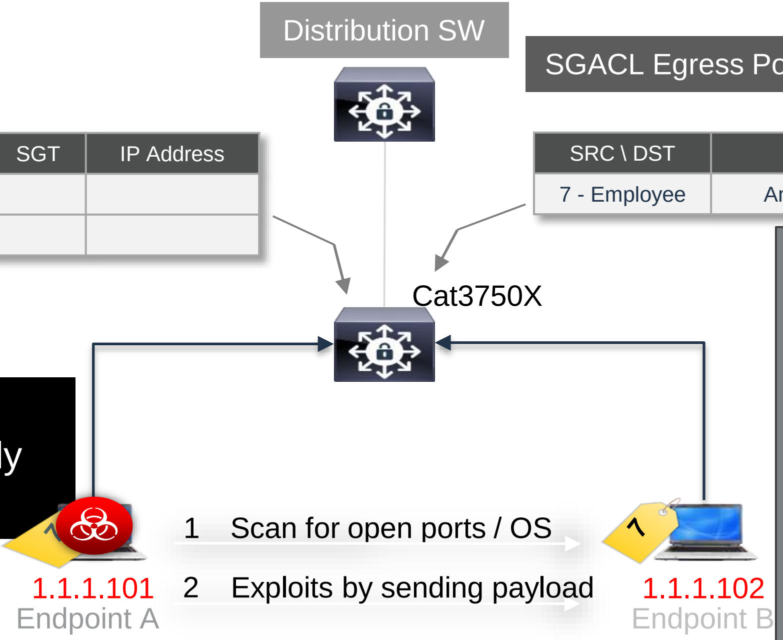
Data Centre Server Segmentation

SGT Malware Recon/Propagation – Security Overlay

Name	MAC Address	SGT	IP Address
Endpoint A			
Endpoint B			

SGACL Egress Policy

SRC \ DST	7 - Employee
7 - Employee	Anti-Malware-ACL



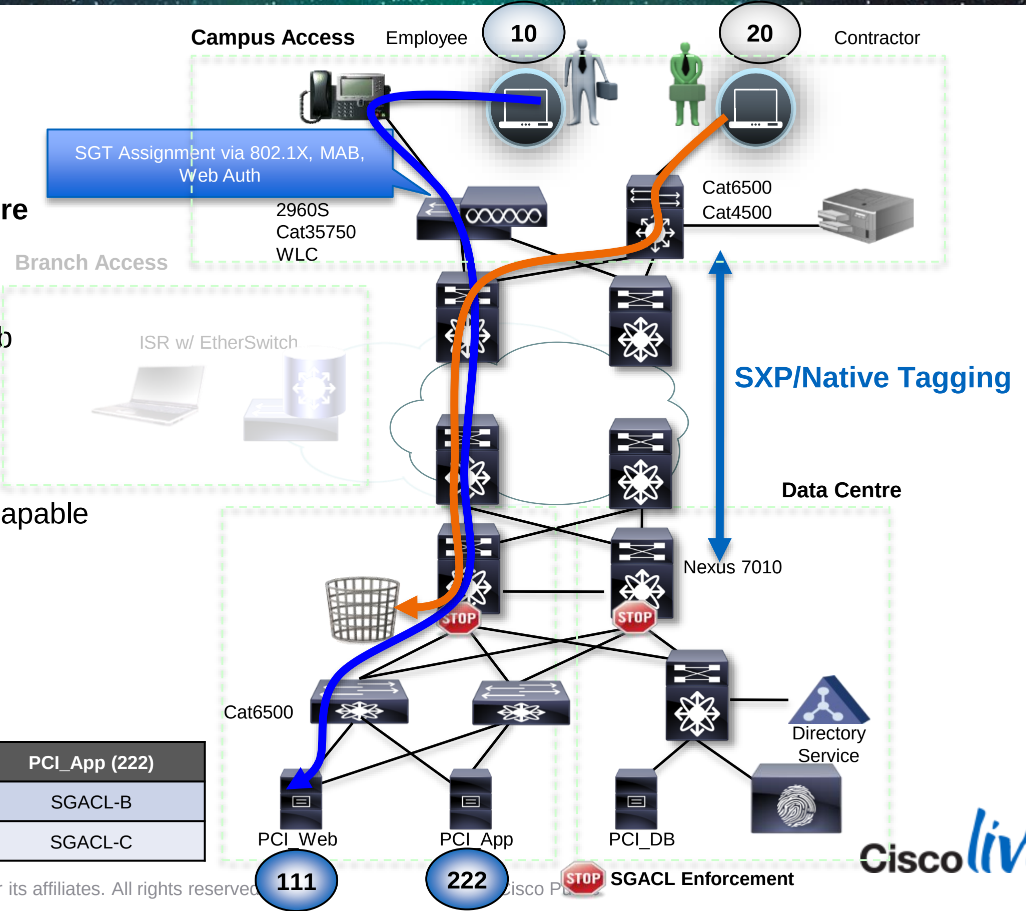
SGACL for SGT 7 is applied statically on switch or dynamically downloaded from ISE.

```
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
```

Campus/Branch LAN Deployment

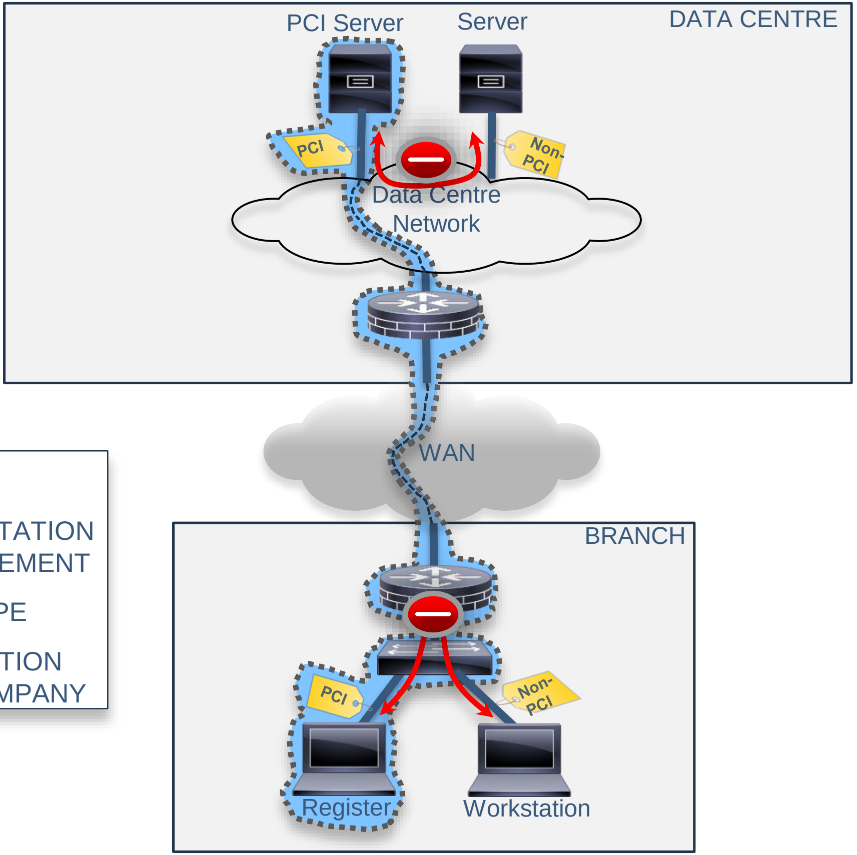
SGT to cover campus network as well as Data Centre network

- Support for Campus / Branch access
- Source SGT assigned via 802.1X, MAB, or Web Authentication
- Server SGT assigned via IPM or statically
- IP-to-SGT binding table is exchanged between Campus access switch and Data Centre SGT capable device



SRC \ DST	PCI_Web (111)	PCI_App (222)
Employee (10)	Permit all	SGACL-B
Contractor (20)	Deny all	SGACL-C

PCI Compliance

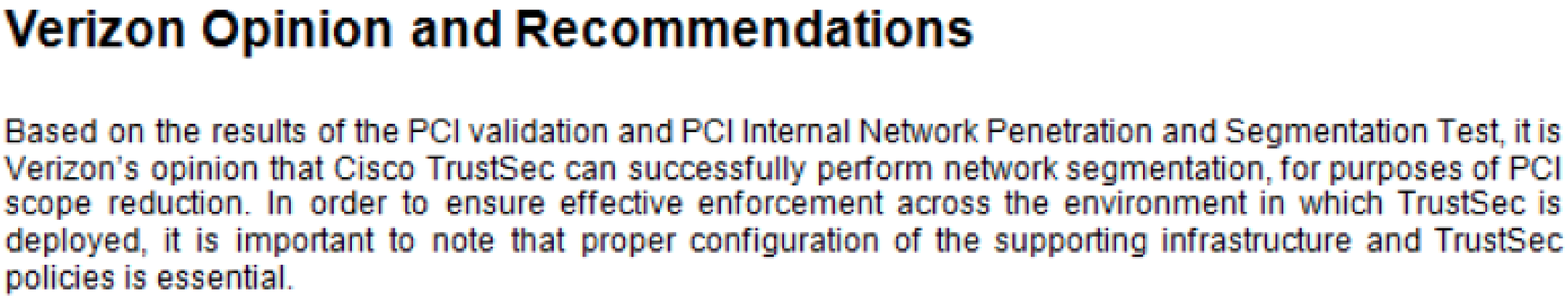


Key

- SEGMENTATION ENFORCEMENT
- PCI SCOPE

SEGMENTATION ACROSS COMPANY

PCI Compliance

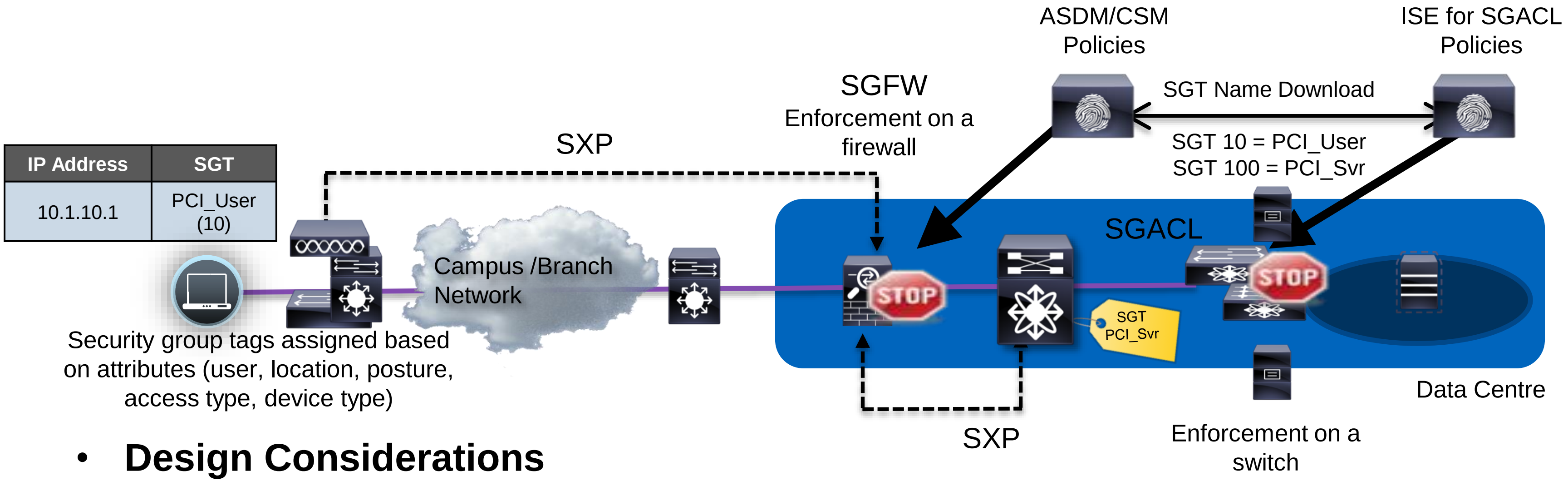


Verizon Opinion and Recommendations

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

Security Group Firewall (SGFW) – ASA Data Centre



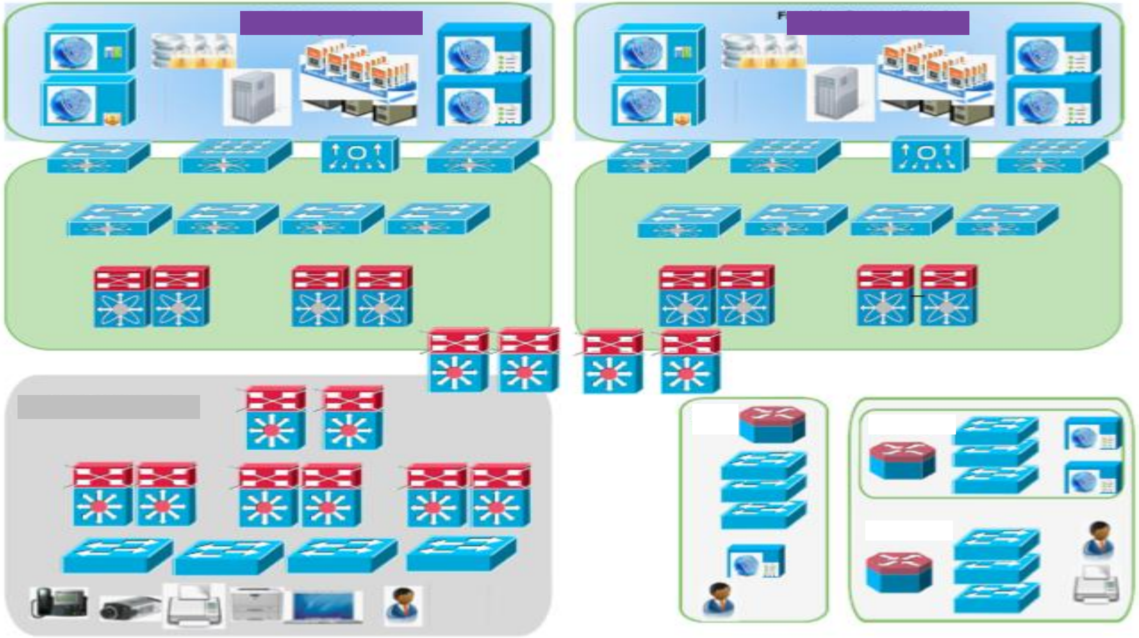
IP Address	SGT
10.1.10.1	PCI_User (10)

Security group tags assigned based on attributes (user, location, posture, access type, device type)

- **Design Considerations**
  - **Consistent Classification/enforcement between FW and switching.**
  - **SGT Names sych’d ISE and CSM/ASDM**
  - **Rich Logging requirements will be fulfilled on SGFW – URL logging, etc.**
  - **Switch logging is best effort via syslog (N7K/N5K) or netflow (Cat6K Sup2T)**
  - **Automation of Firewall Rules for Users “and” Servers**

Financial

- Multiple phases and use-cases
- Currently enforcement on Catalyst switches
- User devices classified by 802.1X or MAB
- Servers defined by IP address or Nexus 1kV Port Profile
- Use-cases
  - Controlled access to DC applications – for compliance
  - User – User control
  - Planning DC segmentation now



Manufacturer

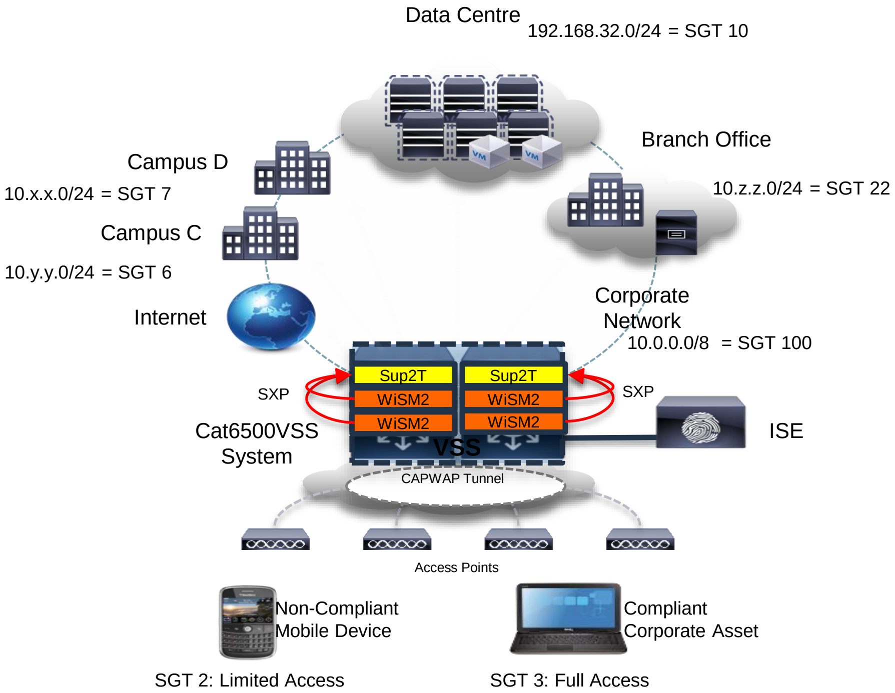
- Large Manufacturing Company deploying Secure Wi-Fi
- ACL needs to scale more than 64 lines of ACL (>1,500) on WLC
- SGT solution within C6K chassis

  WiSM2 aggregates AP traffic

  Policy enforcement Sup2T based on SGT

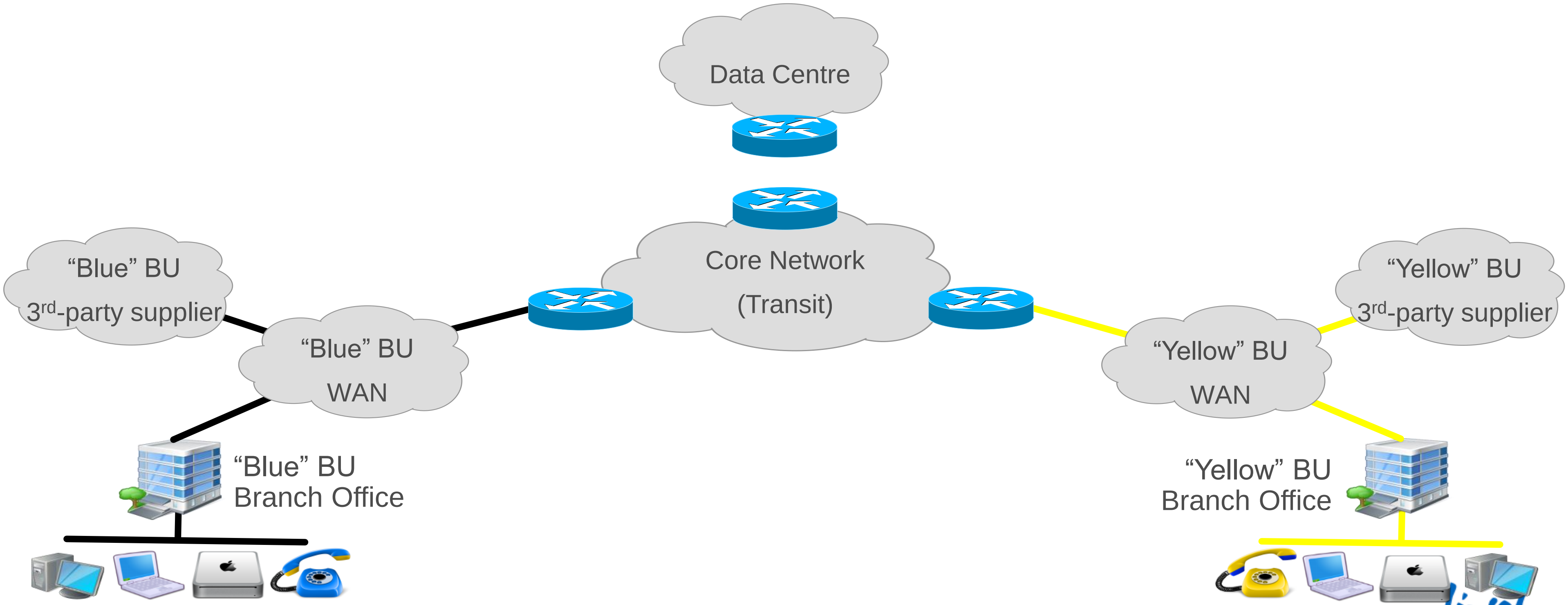
  Destination SGT values defined by IP & Subnet
- Reduced IOS static ACL → managing policy using Egress Matrix
  - e.g. about 500 lines of ACL allowing HTTPS is now supported by single line of SGACL
  - permit tcp dst eq 443

Large Campus Wireless Deployment



Controlling Inter-BU Traffic with SGT

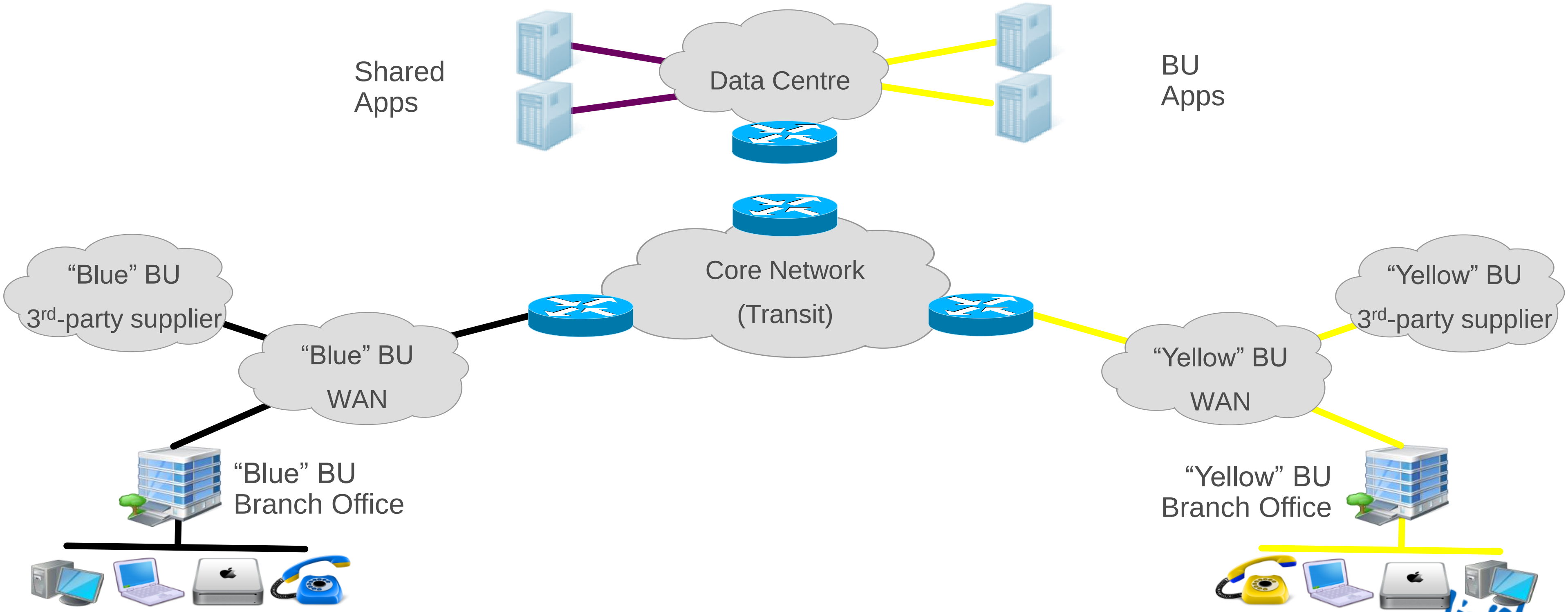
BU-level classifications



Controlling Inter-BU Traffic with SGT

BU-level classifications

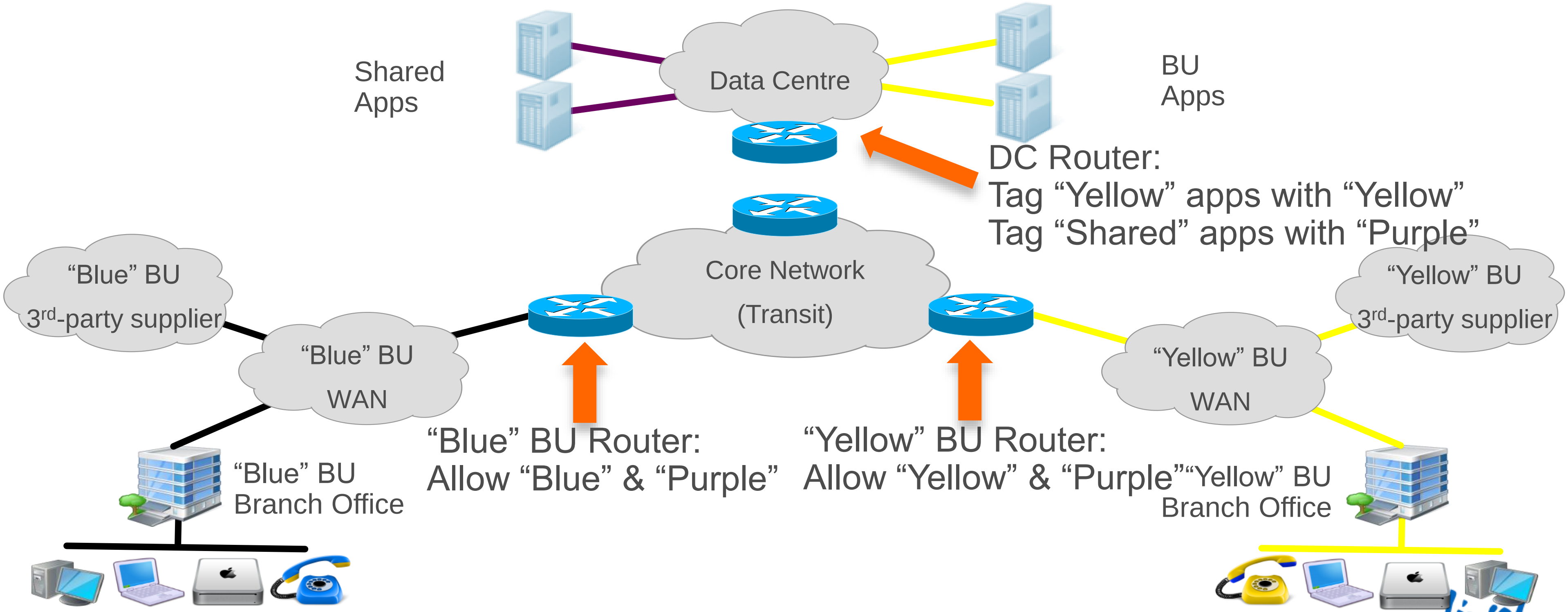
- DC has both shared apps and BU-specific apps



Controlling Inter-BU Traffic with SGT

BU-level classifications

- BU routers accept their own SGT and the shared application SGT values



DC Router:
Tag "Yellow" apps with "Yellow"
Tag "Shared" apps with "Purple"

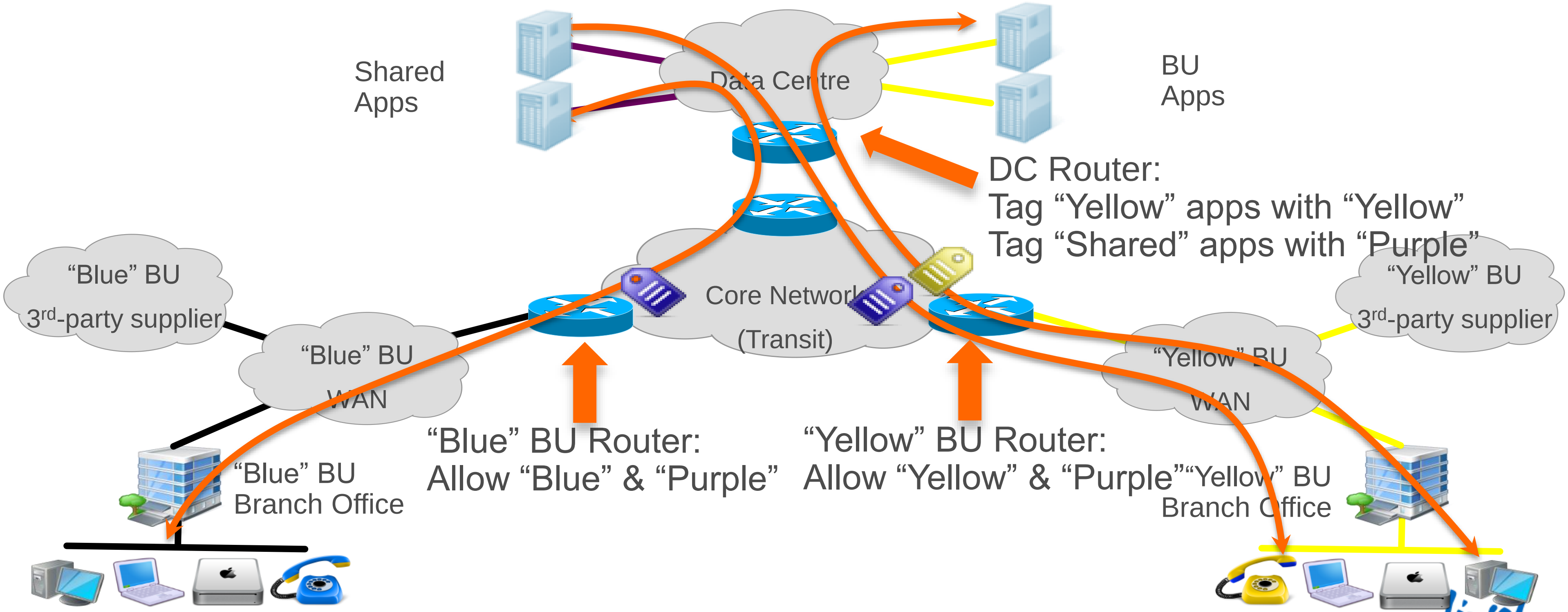
"Blue" BU Router:
Allow "Blue" & "Purple"

"Yellow" BU Router:
Allow "Yellow" & "Purple"

Controlling Inter-BU Traffic with SGT

BU-level classifications

- Shared and BU-specific apps flow properly. Standard SGACLs simplifies base policy



DC Router:
Tag “Yellow” apps with “Yellow”
Tag “Shared” apps with “Purple”

“Blue” BU Router:
Allow “Blue” & “Purple”

“Yellow” BU Router:
Allow “Yellow” & “Purple”

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
- IE2000/3000, CGS2000
- 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)
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, CSR
SXP				ASA5500 Firewall, ASASM, ASAv

- Inline SGT on all ISRG2 except 800 series:

Enforcement

- SGACL Catalyst 3560-X
- SGACL Catalyst 3750-X
- Catalyst 3850 NEW
- WLC 5760 NEW
- SGACL Catalyst 4500E (7E) NEW
- Catalyst 6500E (2T)
- SGACL Nexus 7000
- SGACL Nexus 5500
- SGFW ISR G2, CGR2000
- SGFW ASR 1000 Router, CSR
- SGFW ASA 5500 Firewall, ASAv, ASASM

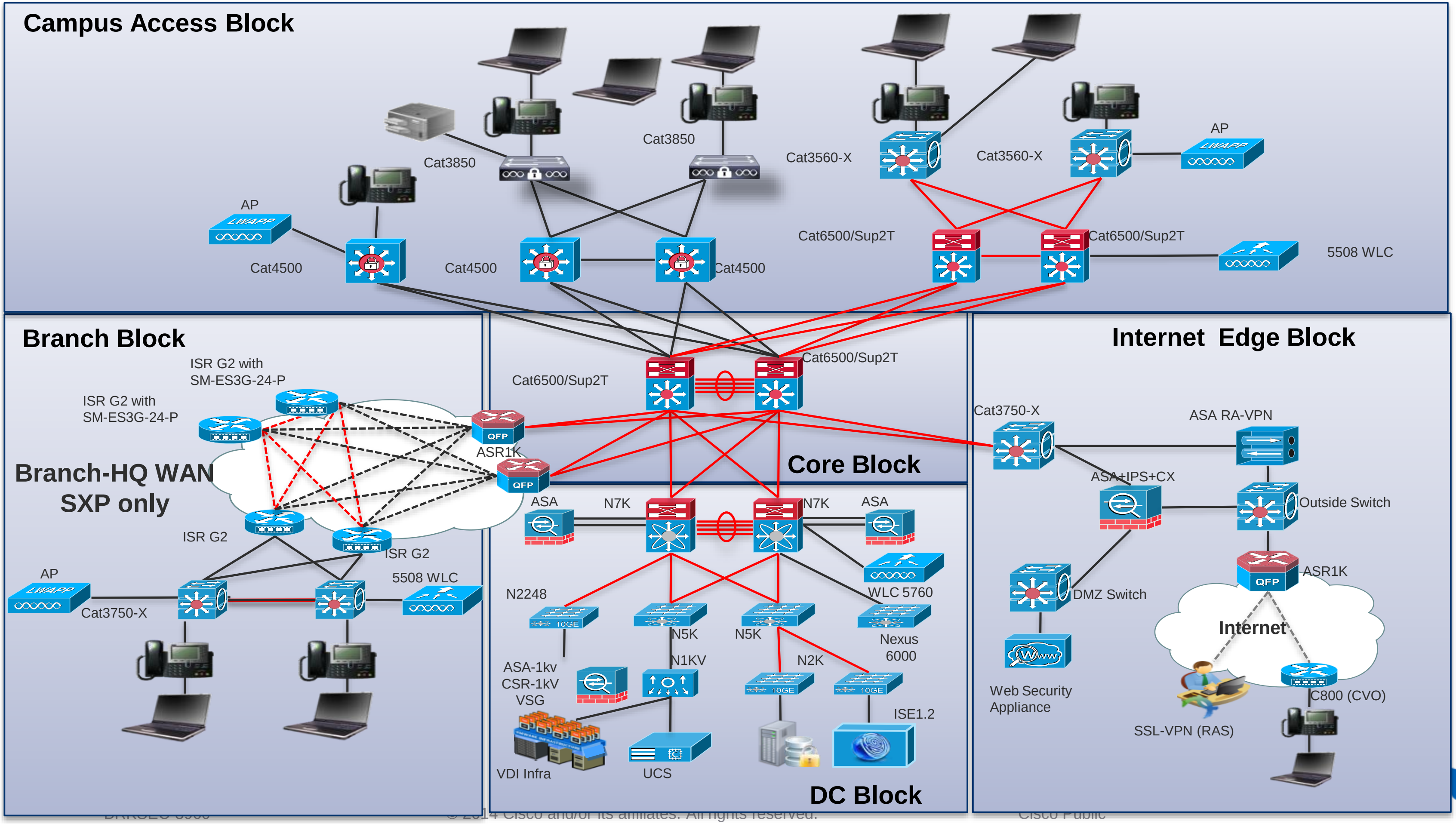
Design Considerations and Implementation Details

SGT Transport – CY12

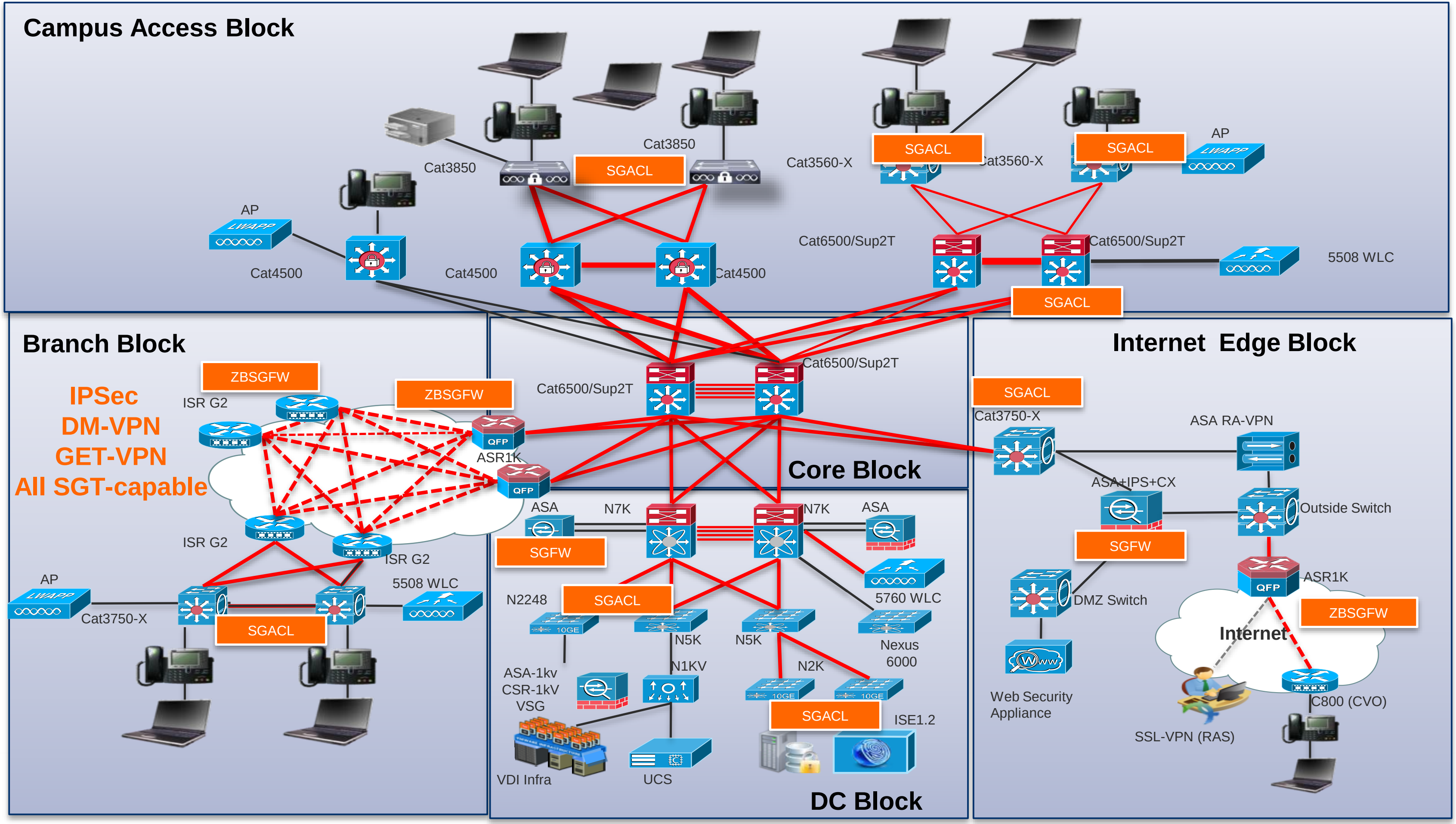
Normal Link

In-line SGT Tagging

Design Consideration

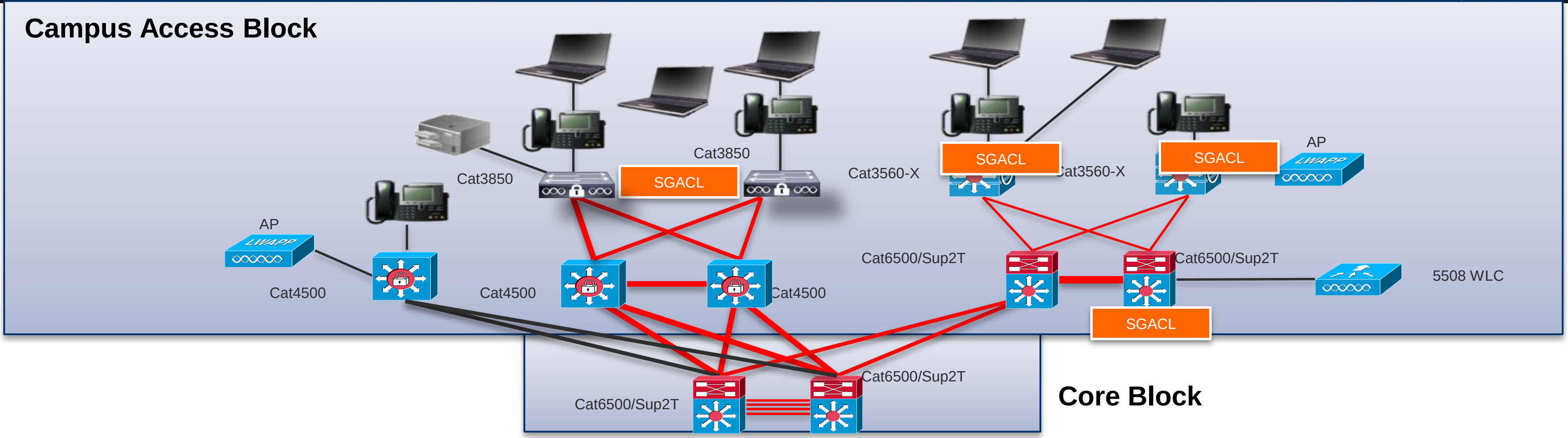


SGT Enforcement Jan. 2014



Campus Design Considerations

Campus Block



- Campus to/from Data Centre (North-South Traffic)
  - Easily accomplished with SXP to Distribution layer or directly to DC (ASR/N7K/ASA)
  - SXP converting to inline tagging allows scaling and removal of SXP state from enforcement device
- Campus to/from Campus/Branch (East-West)
  - SXP only at access layer can still accomplish east-west traffic blocking with 4500/6500. Access layer exposed and have to use VLAN segmentation
  - SGACL at access layer requires distribution layer to convey tag to other network block

Campus Design Consideration

- Platform Hardware capabilities - Two types of SGT/SGACL switch hardware
  - Port/VLAN - SGT/SGACL tagging/enforcement
  - IP/SGT – tagging/enforcement

- Hardware capabilities impact
  – SXP Design
  – SGT/SGACL enforcement scaling

- Use Cases drive whether the hardware is impactful to the design

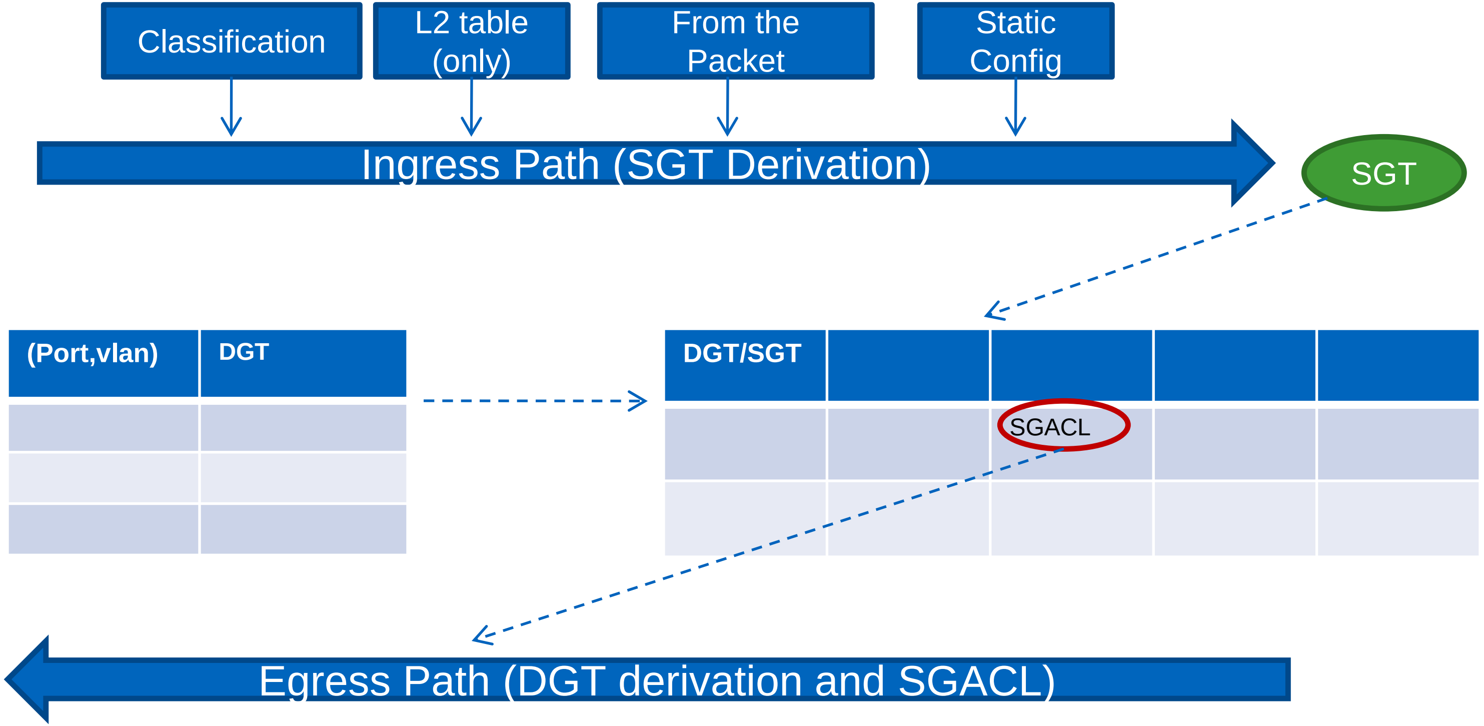
- General rule of thumb “Tag when you can , SXP when you have to”

Hardware Forwarding SGT/SGACL Today

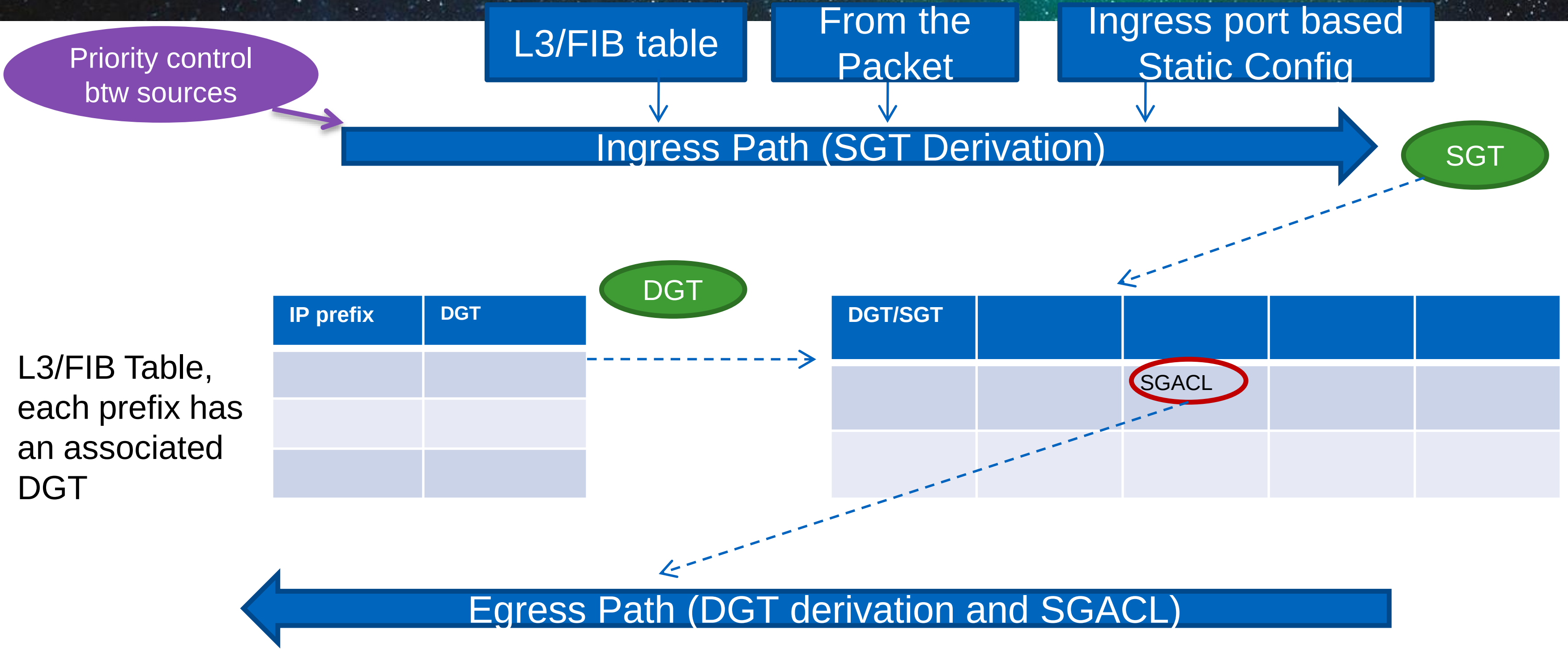
- Two Groupings of Hardware Forwarding
- Port/VLAN based
  - Cat 3K-X
  - N5K
- IP/SGT Based
  - Cat 6K/Sup2T
  - N7K – M series and F series
  - Cat 4K/Sup7E/Sup8E
  - Cat 3850/5760
  - ASR1K
- Each type of hardware has different scaling limits
  - There are limits on the number of SGT/DGT as well as Access Control Entries (ACE) in TCAM
  - All hardware shares ACE entries when possible amongst SGT/DGT

SGT and DGT Derivation in Cat 3K-X

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



SGT and DGT Derivation in Cat6K/Sup2T


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

L3/FIB Table, each prefix has an associated DGT

IP prefix	DGT

DGT/SGT				
		SGACL		

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

Implications of Hardware Forwarding Capabilities

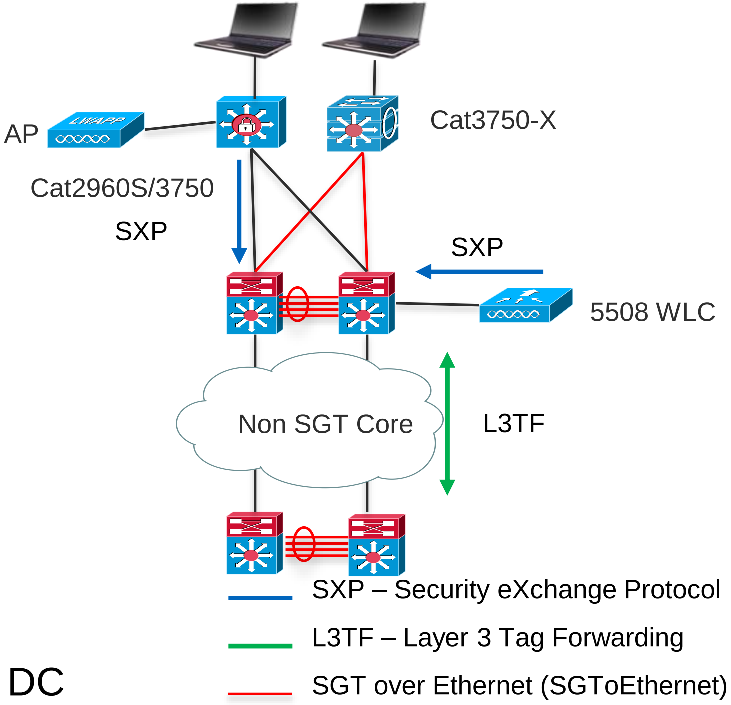
- Port/VLAN Based Hardware
    - Limited SXP applicability due to the SGT derivation on mac/port
    - Limited number of SGTs per port (one or per vlan/port)
- IP/SGT Based Hardware Implications
    - – Allows for bidirectional SXP
    - – Allows for multi-hop SXP coming into the switch due to FIB lookup for IP/SGT
    - – Tagging/Enforcement for incoming packet due to FIB lookup for IP/SGT
    - – Scale varies per platform. Think hundreds of groups with simple reused permissions (ACEs)

Implications of Hardware Forwarding Capabilities

- Cat 3K-X can take IP/SGT from SXP for L2 adjacent traffic.
  - L2 adjacency can allow mac/port/vlan pairing to be able to tag or filter at egress
  - Cat 3K-X can have Layer 2 adjacent hosts (small WLCs) trunked to Cat3K-X
    - Since Cat 3K-X can only have 1 SGT/VLAN on a port. This means all users in a VLAN must have the same SGT. Assign VLAN policy in ISE or use "VLAN/SGT" on the switch.
    - Cat 3K-X can only have a maximum of 8 SGT/VLANs on a trunk
  - Cat 3K-X are listeners for SXP relay functionality
  - Cat 3K-X CANNOT take IP/SGT (SXP) from across L3 hop (SXP multi-hop)
    - Cat 3K-X can't find the proper mac/port/vlan pairing due to L2 lookup for SGT.
    - If across L3 the mac/port/vlan will be the L3 hop peer SGT not the IP/SGT in SXP
- N5K limited since it can't find SGT via SXP.
  - No N5K SXP listener - even for L2 adjacent hosts
  - N5K can't be a listener for an N1KV

Simple Topology Enablement

- East-West traffic enforced via SGACL
  - From Cat 2960S/3750 -> 3750X enforced on 3750X
    - DGT at 3750X
    - No IP/SGT on Cat6K
  - From 3750X-> 2960S/3750 enforced on Cat6K
    - IP/SGT in Cat6K for DGT lookup
  - From WLC-> 3750X enforced on 3750X
    - DGT at 3750X
    - No IP/SGT on Cat6K
  - From WLC-> 2960S/3750 enforced on Cat6K
    - IP/SGT in Cat 6K for DGT lookup
- North-South traffic
  - From access layer (3K, 3KX, WLC) to DC enforced in DC
  - From DC to access layer (3K, 3KX, WLC)
    - DC -> 3K and WLC enforced on Cat6K
    - DC -> 3KX enforced on 3KX


AP
LWAPP
Cat3750-X
Cat2960S/3750
SXP
SXP
5508 WLC
Non SGT Core
L3TF
SXP – Security eXchange Protocol
L3TF – Layer 3 Tag Forwarding
SGT over Ethernet (SGToEthernet)

IPv6 and Security Group Tags – Status

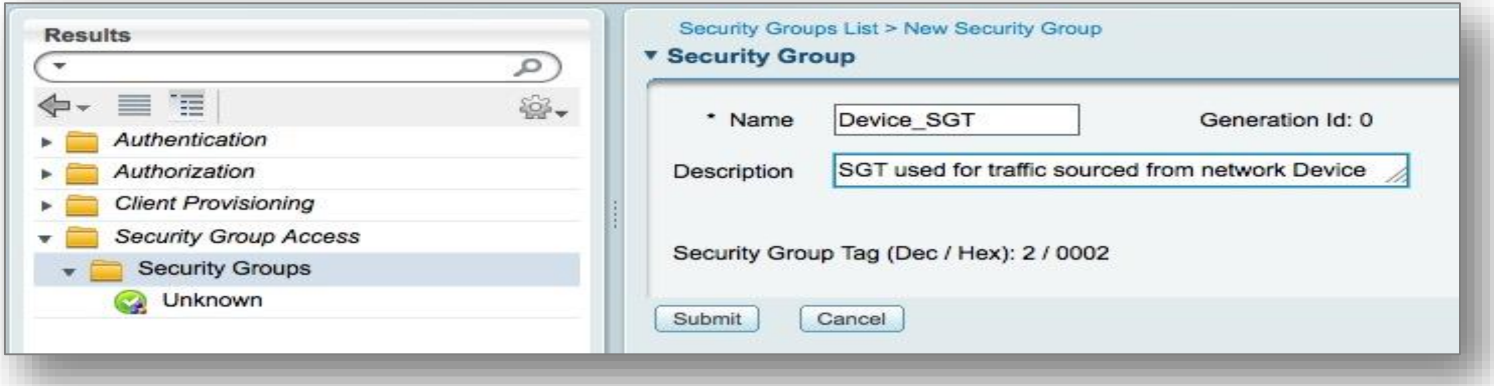
- ISE can manage IP agnostic SGACL policy today for switches
  - IPv4 only SGACL
  - IPv6 only SGACL
  - IPv4 and IPv6 SGACL
- CSM can manage IPv6 FW rules on ASA
- IPv6 Device Discovery
  - WLC – WLC 8.0 CY14 via IPv6/SGT
  - Amur (3750, 3650, 3850, 5760, 4500) 1HCY14
    - IPv6 device discovery supported by IPv6 First Hop Security (SISF)
    - Will export in IPv6/SGT in SXPv4, but will not tag on ethernet
    - This will allow an upstream enforcement device to filtering on IPv6/SGT
- SGT enforcement capable devices
  - ASA for SGFW
  - Sup2T for SGACL

Enabling SGT/SGACL on IOS

- Following is a high-level overview of SGT/SGACL configuration on Cat6K Sup2T when used with ISE1.x

① Configure ISE 1.x to the point where you can perform 802.1X authentication (bootstrap, certificate, AD integration, basic authentication & authorisation rules)

② Configure Device SGT (**Policy > Policy Elements > Results > Security Group Access > Security Group**)



* Name: Device_SGT

Generation Id: 0

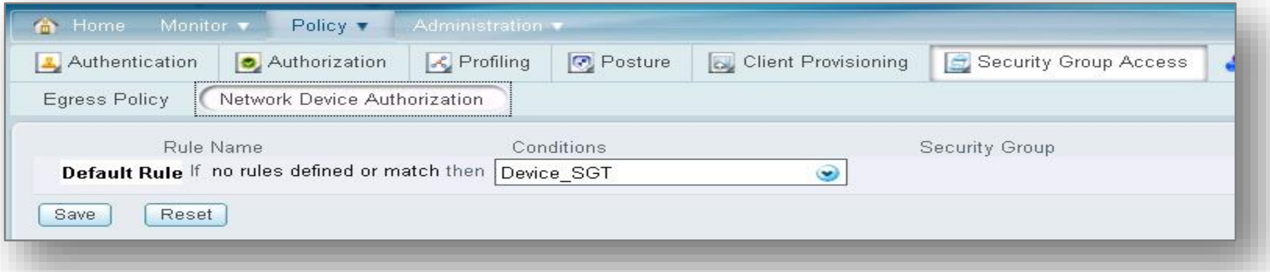
Description: SGT used for traffic sourced from network Device

Security Group Tag (Dec / Hex): 2 / 0002

All SGTs should have access to Device_SGT by policy (ARP needs to work ☺)

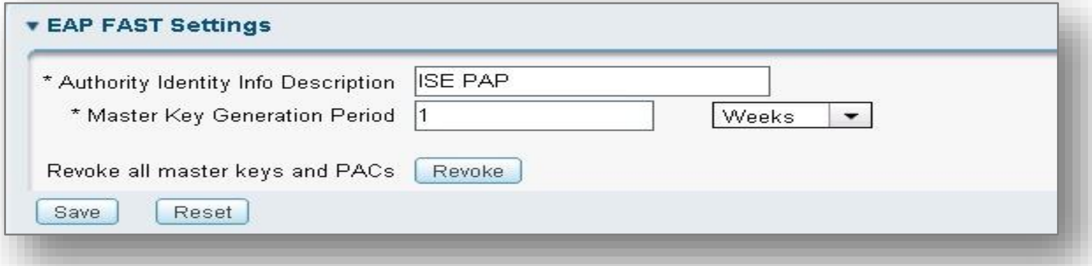
SGT Configuration for ISE

③ Under **Policy > Security Group Access > Network Device Authorization**, assign Device SGT created in step (2) to default condition



Rule Name	Conditions	Security Group
Default Rule	If no rules defined or match then	Device_SGT

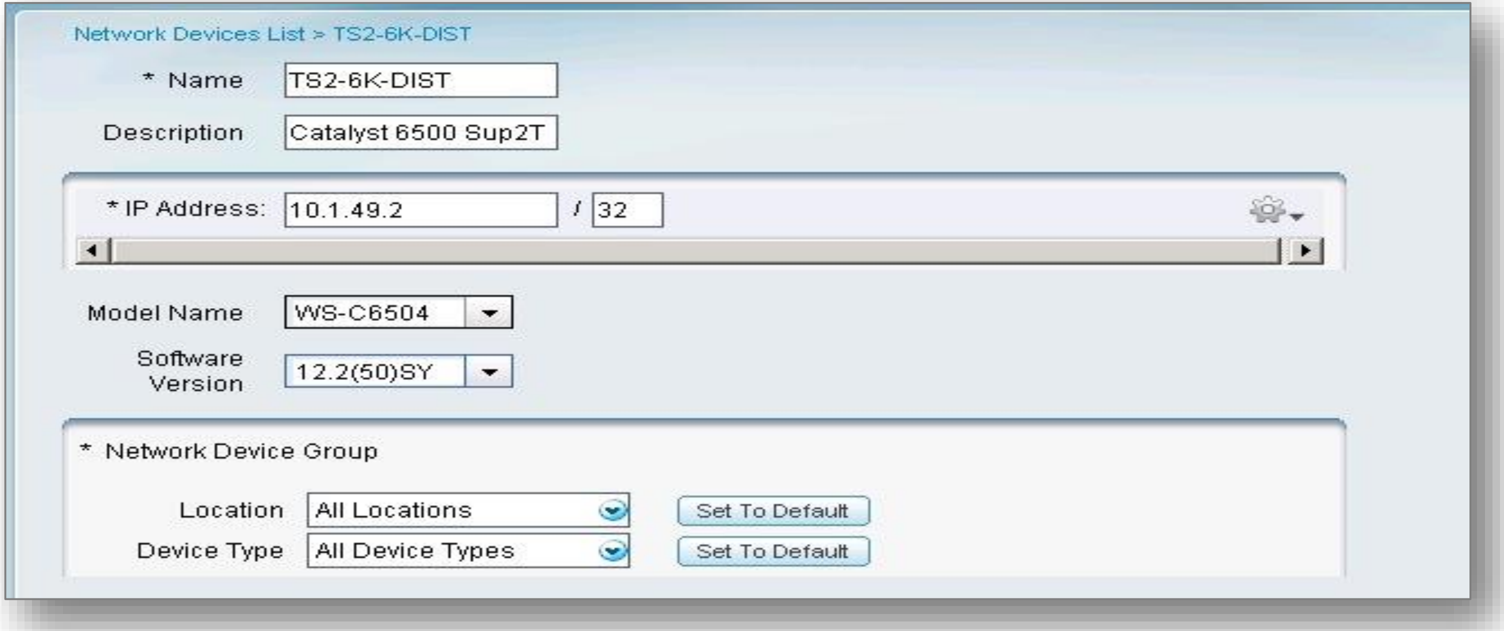
④ **Optionally** under **Admin > System > Settings > Protocols > EAP-FAST > EAP-FAST Settings**, change A-ID description to something meaningful, so that you can recognise which ISE you are receiving PAC file on the switch CLI.



* Authority Identity Info Description: ISE PAP
* Master Key Generation Period: 1 Weeks
Revoke all master keys and PACs

Configuration Cat6K Sup2T as Seed Device

⑤ Under **Admin > Network Resources > Network Devices**, create AAA client entry for Cat6500 Sup2T



Network Devices List > TS2-6K-DIST

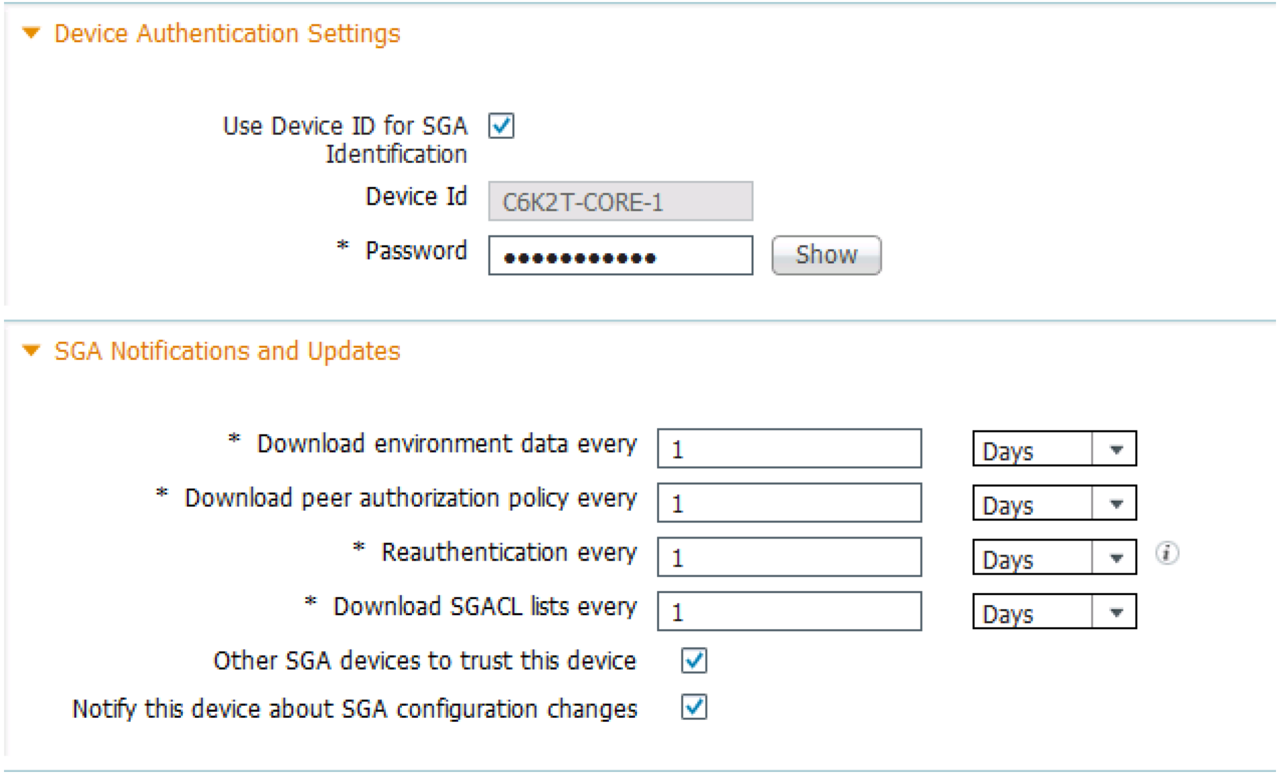
* Name	TS2-6K-DIST
Description	Catalyst 6500 Sup2T
* IP Address:	10.1.49.2 / 32
Model Name	WS-C6504
Software Version	12.2(50)SY

* Network Device Group

Location	All Locations	Set To Default
Device Type	All Device Types	Set To Default

Configuration an SGT Device

⑥ Configure RADIUS secret. Also Enable Security Group Access (SGA), check Use Device ID for SGA, then type device password. This ID and Password needs to be exactly same as you define on network device CLI



▼ Device Authentication Settings

Use Device ID for SGA Identification ☑

Device Id: C6K2T-CORE-1

* Password: ●●●●●●●●●●●● Show

▼ SGA Notifications and Updates

* Download environment data every	1	Days
* Download peer authorization policy every	1	Days
* Reauthentication every	1	Days
* Download SGACL lists every	1	Days

Other SGA devices to trust this device ☑

Notify this device about SGA configuration changes ☑

Configuring an IOS Switch for SGT

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

① Enabling AAA

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

② Defining RADIUS server with PAC keyword

```
Switch(config)#radius-server host <ISE_PDP_IP> pac key <RADIUS_SHARED_SECRET>
```

③ Define authorization list name for SGA policy download

```
Switch(config)#cts authorization list <AUTHZ_List_Name>
```

④ Use default AAA group for 802.1X and “defined authz list” for authorization

```
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#aaa authorization network <AUTHZ_List_Name> group radius
```

Configuring an IOS Switch for SGT(cont.)

⑤ Configure RADIUS server to use VSA in authentication request

```
Switch(config)#radius-server vsa send authentication
```

⑥ Enable 802.1X in system level

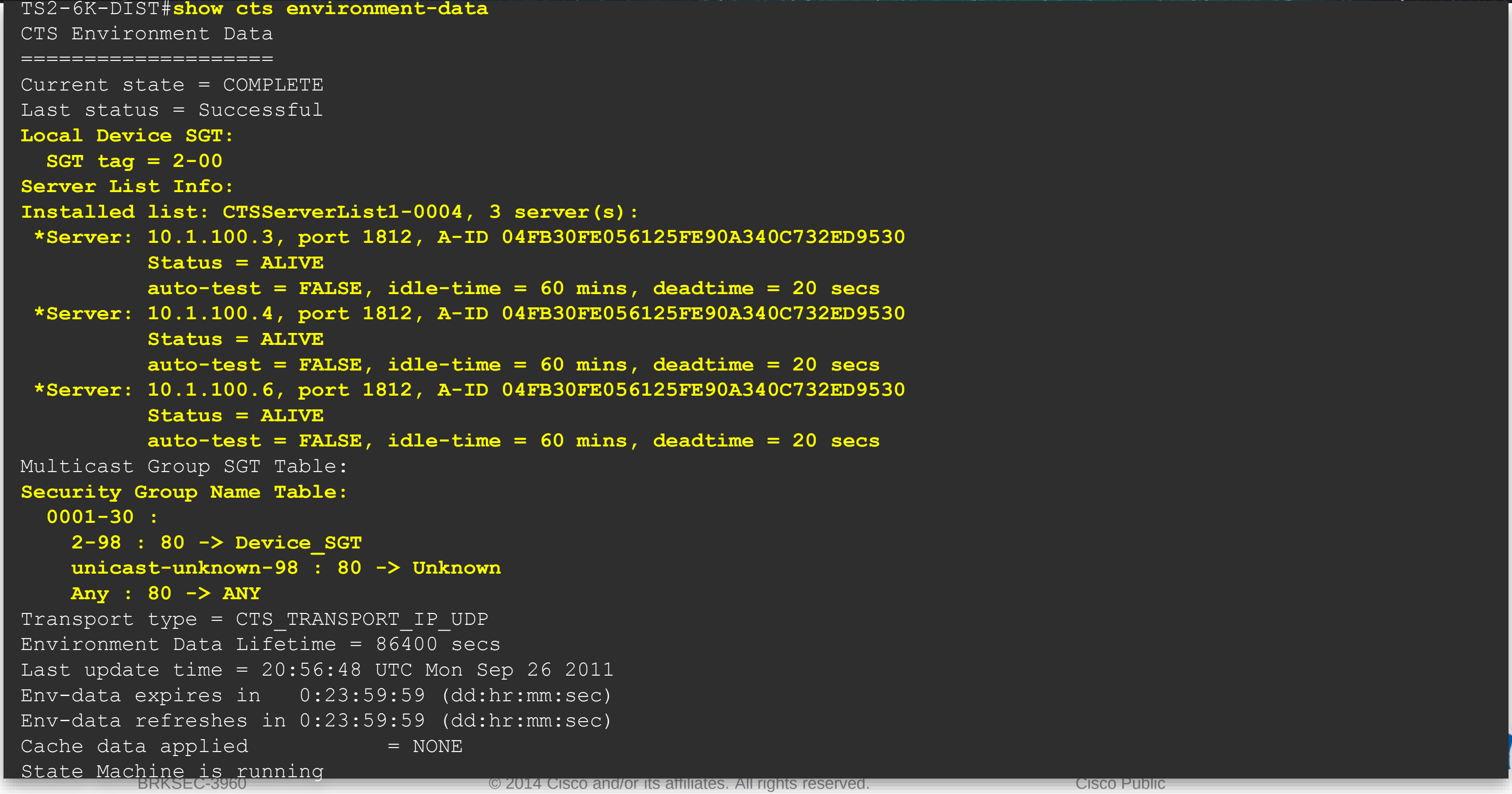
```
Switch(config)#dot1x system-auth-control
```

⑦ Define device credential (EAP-FAST I-ID), which must match ones in ISE AAA client configuration

```
Switch#cts credential id <DEVICE_ID> password <DEVICE_PASSWORD>
```

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

Verification – Environment Data



```
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
```

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

Sample Topology 3750-X (SGT Tagging)

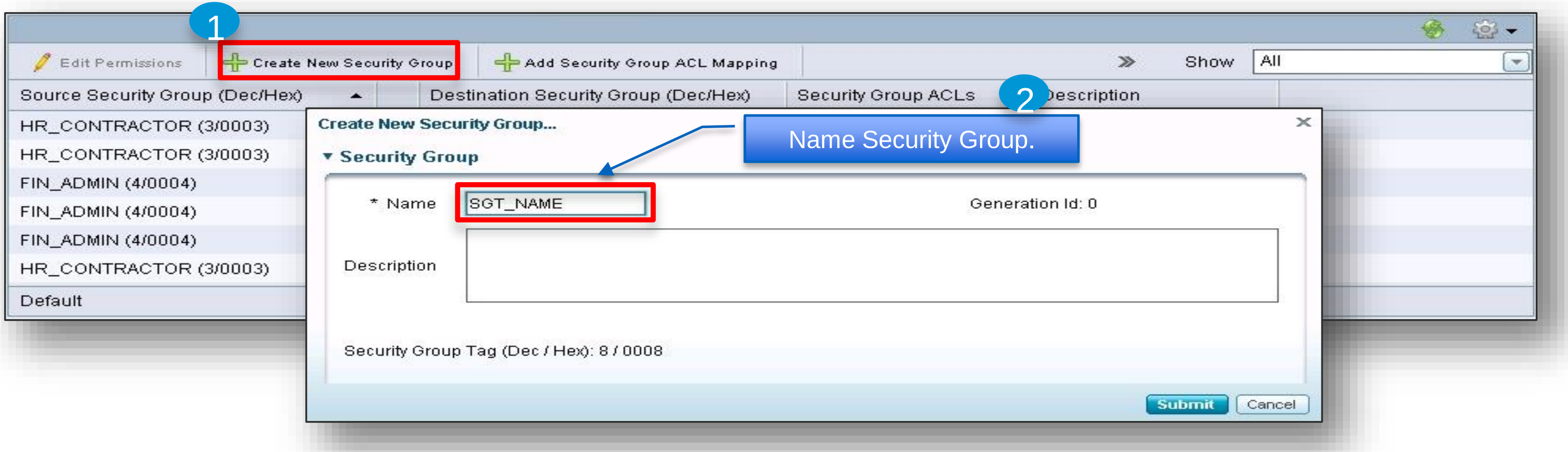
```
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network cts-mlist group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 10.1.100.3 server-key cisco123
!
aaa session-id common
ip device tracking
!
cts authorization list cts-mlist
cts role-based enforcement
cts role-based enforcement vlan-list 20
!
dot1x system-auth-control
interface GigabitEthernet1/0/1
 switchport access vlan 20
 switchport mode access
 ip access-group DefaultIn in
 authentication event fail action next-method
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
```

```
interface GigabitEthernet1/0/14
 no switchport
 ip address 10.10.20.2 255.255.255.0
 cts manual
  policy static sgt 2 trusted
 no cts role-based enforcement
!
radius-server host 10.1.100.3 pac key cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
C3750X#sho auth session int g 1/0/1
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0014.5e42.9c69
           IP Address:  10.10.15.100
            User-Name:  CTS\Administrator
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
                  SGT:  0008-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0B01000002682408110A
      Acct Session ID:  0x0000043F
               Handle:  0x80000269

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run
```

Preparing ISE for SGACL Enforcement

- In order to provision SGACL policy automatically to Sup2T, ISE needs to be configured for SGT/SGACL and associated policies

Under Policy > Security Group Access > Egress Policy, create Security Group Tag for roles



Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	Security Group ACLs	Description
HR_CONTRACTOR (3/0003)			
HR_CONTRACTOR (3/0003)			
FIN_ADMIN (4/0004)			
FIN_ADMIN (4/0004)			
FIN_ADMIN (4/0004)			
HR_CONTRACTOR (3/0003)			
Default			

Create New Security Group...

Security Group

* Name SGT_NAME

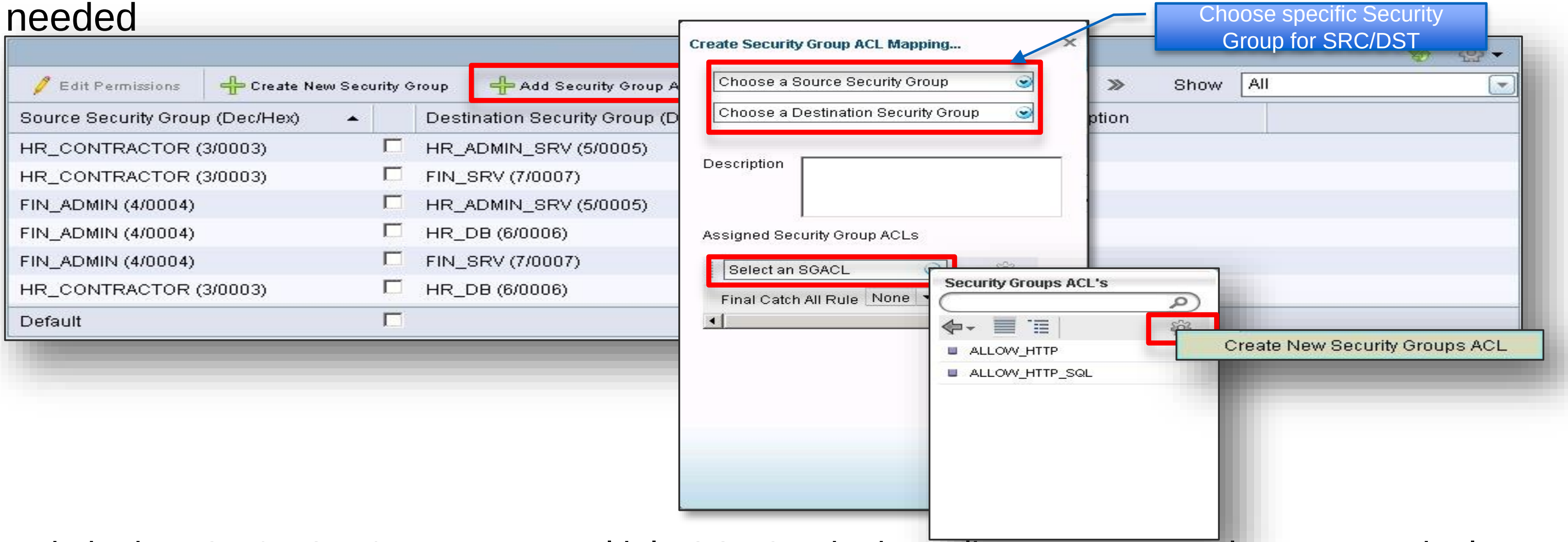
Generation Id: 0

Description

Security Group Tag (Dec / Hex): 8 / 0008

Preparing ISE for SGACL Enforcement

In same screen, add Security Group ACL Mapping. Create additional Security Group ACL if needed



Choose specific Security Group for SRC/DST

Source Security Group (Dec/Hex)		Destination Security Group (D
HR_CONTRACTOR (3/0003)	□	HR_ADMIN_SRV (5/0005)
HR_CONTRACTOR (3/0003)	□	FIN_SRV (7/0007)
FIN_ADMIN (4/0004)	□	HR_ADMIN_SRV (5/0005)
FIN_ADMIN (4/0004)	□	HR_DB (6/0006)
FIN_ADMIN (4/0004)	□	FIN_SRV (7/0007)
HR_CONTRACTOR (3/0003)	□	HR_DB (6/0006)
Default	□	

Create Security Group ACL Mapping...

Choose a Source Security Group

Choose a Destination Security Group

Description

Assigned Security Group ACLs

Select an SGACL

Final Catch All Rule: None

Security Groups ACL's

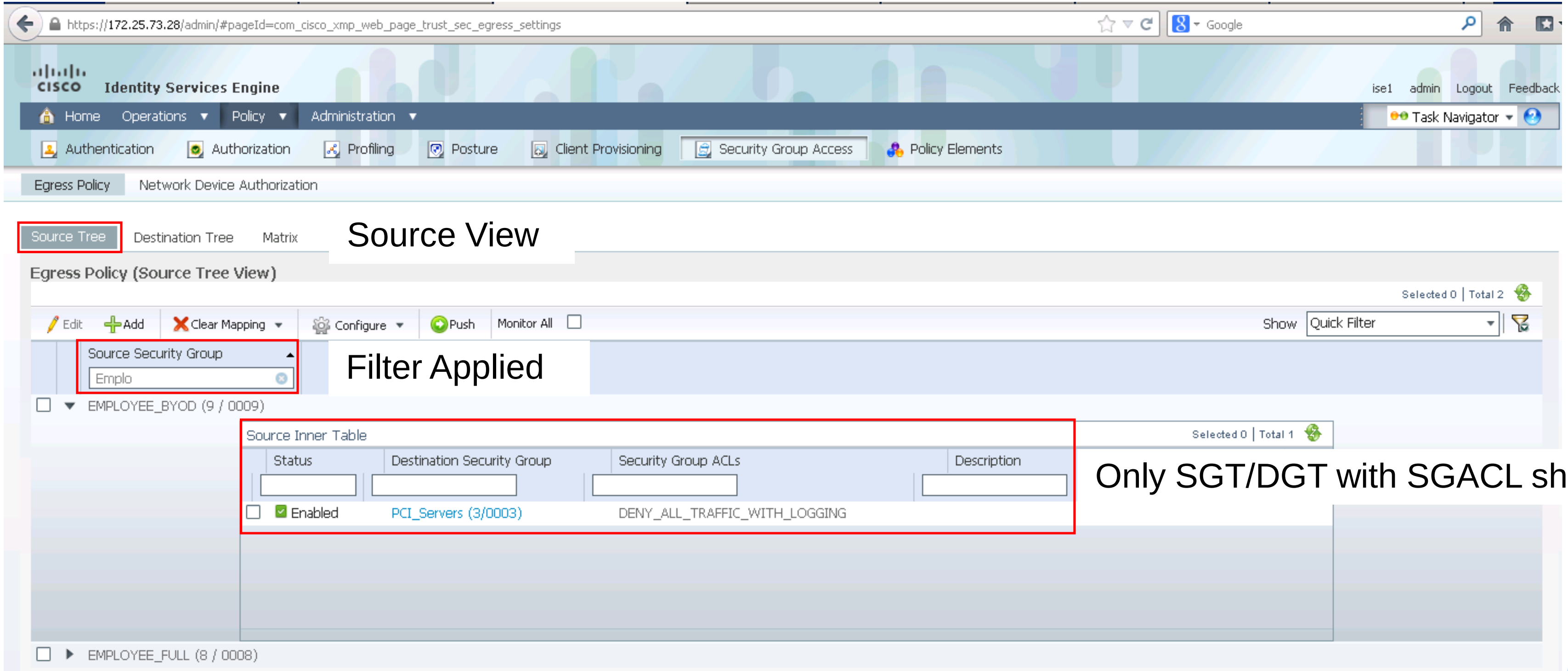
- ALLOW_HTTP
- ALLOW_HTTP_SQL

Create New Security Groups ACL

Known Limitation: Cat6K Sup2T supports multiple SGACLs in the policy. Nexus 7K only supports single SGACL therefore ***best practice is to select one SGACL*** and add explicit deny or permit in the SGACL itself, not in Final Catch Rule

ISE Policy View

- 3 Views – Source Tree, Destination Tree, Matrix



https://172.25.73.28/admin/#pageId=com_cisco_xmp_web_page_trust_sec_egress_settings
Google
cisco Identity Services Engine
ise1 admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Egress Policy Network Device Authorization
Source Tree Destination Tree Matrix
Edit Add Clear Mapping ▼ Configure ▼ Push Monitor All □
Show Quick Filter
Selected 0 | Total 2
Selected 0 | Total 1

Source View

Egress Policy (Source Tree View)

Source Security Group: Emplo

Filter Applied

□ ▼ EMPLOYEE_BYOD (9 / 0009)

Source Inner Table

	Status	Destination Security Group	Security Group ACLs	Description
□	☑ Enabled	PCI_Servers (3/0003)	DENY_ALL_TRAFFIC_WITH_LOGGING	

Only SGT/DGT with SGACL shown

□ ▶ EMPLOYEE_FULL (8 / 0008)

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

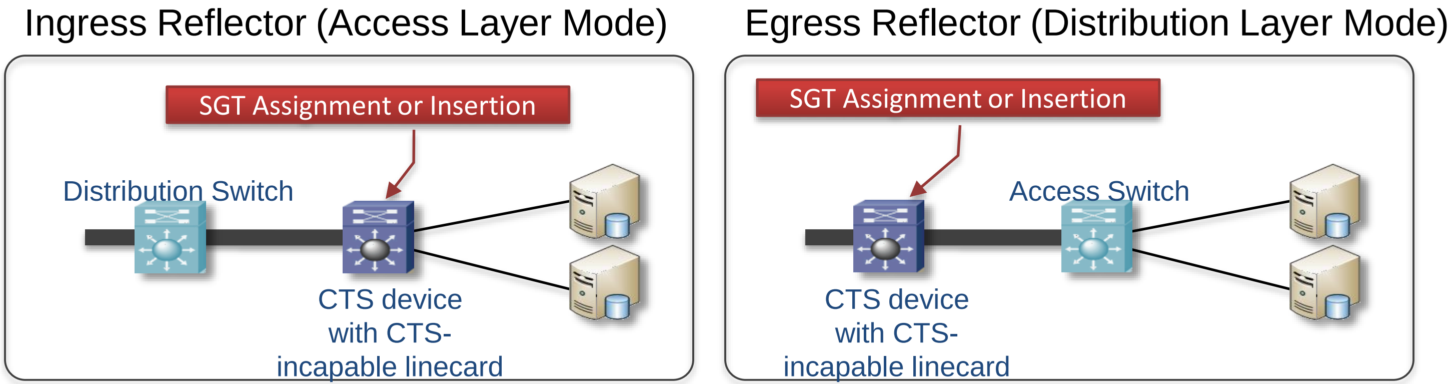
```
Switch(config)#cts role-based enforcement
Switch(config)#cts role-based enforcement vlan-list 40
```

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. More information about reflector is on next slide

Ingress / Egress Reflector


Ingress Reflector (Access Layer Mode)
SGT Assignment or Insertion
Distribution Switch
CTS device with CTS-incapable linecard
Egress Reflector (Distribution Layer Mode)
SGT Assignment or Insertion
Access Switch
CTS device with CTS-incapable linecard

- Cisco TrustSec reflector uses SPAN to reflect traffic from a non-SGACL-capable switching module to the supervisor engine for SGT assignment and insertion.
- Two manually exclusive modes, ingress and egress, are supported for Cisco TrustSec reflector
- By default no reflector is enabled (assumes Sup2T/69xx linecards)

Downloading Policy on IOS Switch

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

Refresh Environment Data using cts refresh environment-data

```
Switch#cts refresh environment-data
Environment data download in progress
```

Refresh Policy using cts refresh policy

```
Switch#cts refresh policy
Policy refresh in progress
```

Downloading Policy on IOS Switch

Verify Environment Data

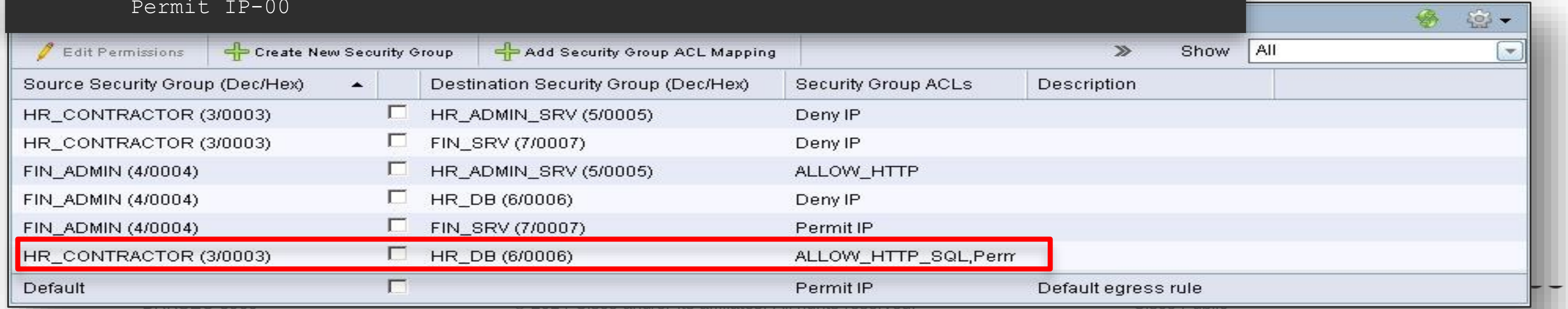
```
TS2-6K-DIST#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00
Server List Info:
Installed list: CTSServerList1-0004, 3 server(s):
 *Server: 10.1.100.3, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          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:
  0001-22 :
    7-98 : 80 -> FIN_SRV
    6-98 : 80 -> HR_DB
    5-98 : 80 -> HR_ADMIN_SRV
    4-98 : 80 -> FIN_ADMIN
    3-98 : 80 -> HR_CONTRACTOR
    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 = 22:50:57 UTC Mon Sep 26 2011
Env-data expires in   0:23:59:49 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:49 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

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
```

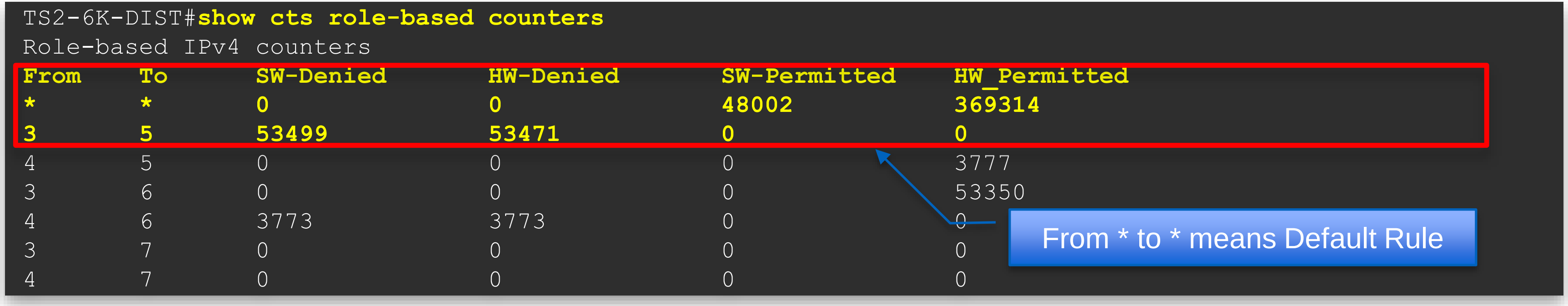
SGACL Mapping Policy should match to one on ISE



Source Security Group (Dec/Hex)		Destination Security Group (Dec/Hex)	Security Group ACLs	Description
HR_CONTRACTOR (3/0003)	□	HR_ADMIN_SRV (5/0005)	Deny IP	
HR_CONTRACTOR (3/0003)	□	FIN_SRV (7/0007)	Deny IP	
FIN_ADMIN (4/0004)	□	HR_ADMIN_SRV (5/0005)	ALLOW_HTTP	
FIN_ADMIN (4/0004)	□	HR_DB (6/0006)	Deny IP	
FIN_ADMIN (4/0004)	□	FIN_SRV (7/0007)	Permit IP	
HR_CONTRACTOR (3/0003)	□	HR_DB (6/0006)	ALLOW_HTTP_SQL,Perm	
Default	□		Permit IP	Default egress rule

Verifying SGACL Drops

Use show cts role-based counter to show traffic drop by SGACL



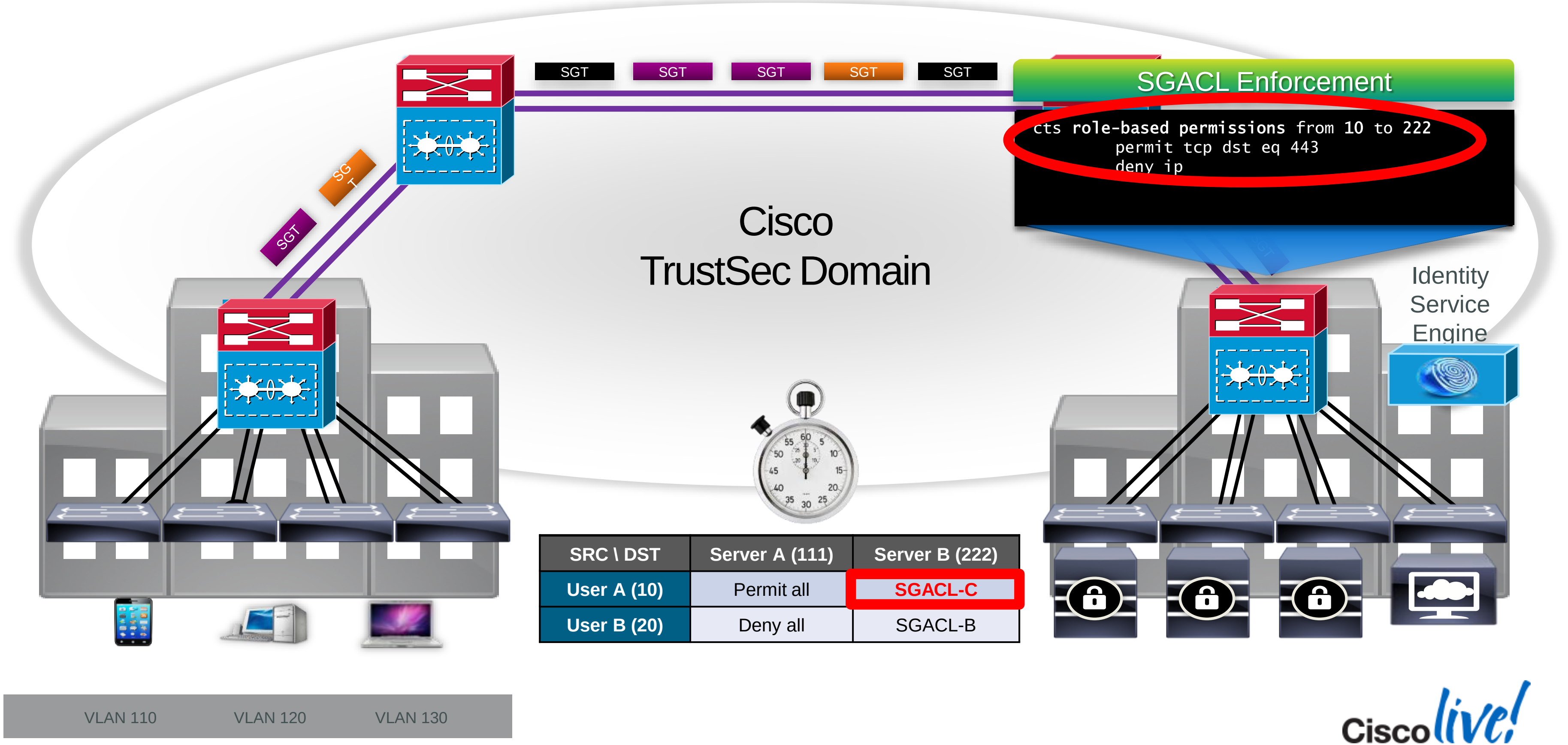
```
TS2-6K-DIST#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
*       *       0               0               48002           369314
3       5       53499           53471           0               0
4       5       0               0               0               3777
3       6       0               0               0               53350
4       6       3773            3773            0               0
3       7       0               0               0               0
4       7       0               0               0               0
```

From * to * means Default Rule

show command displays the content statistics of RBACL enforcement. Separate counters are displayed for HW and SW switched packets. The user can specify the source SGT using the "**from**" clause and the destination SGT using the "**to**" clause.

Mostly SGACL is done in HW. Only if the packet needs to be punted to SW (e.g. TCAM is full, marked to be logged) , SW counter increments

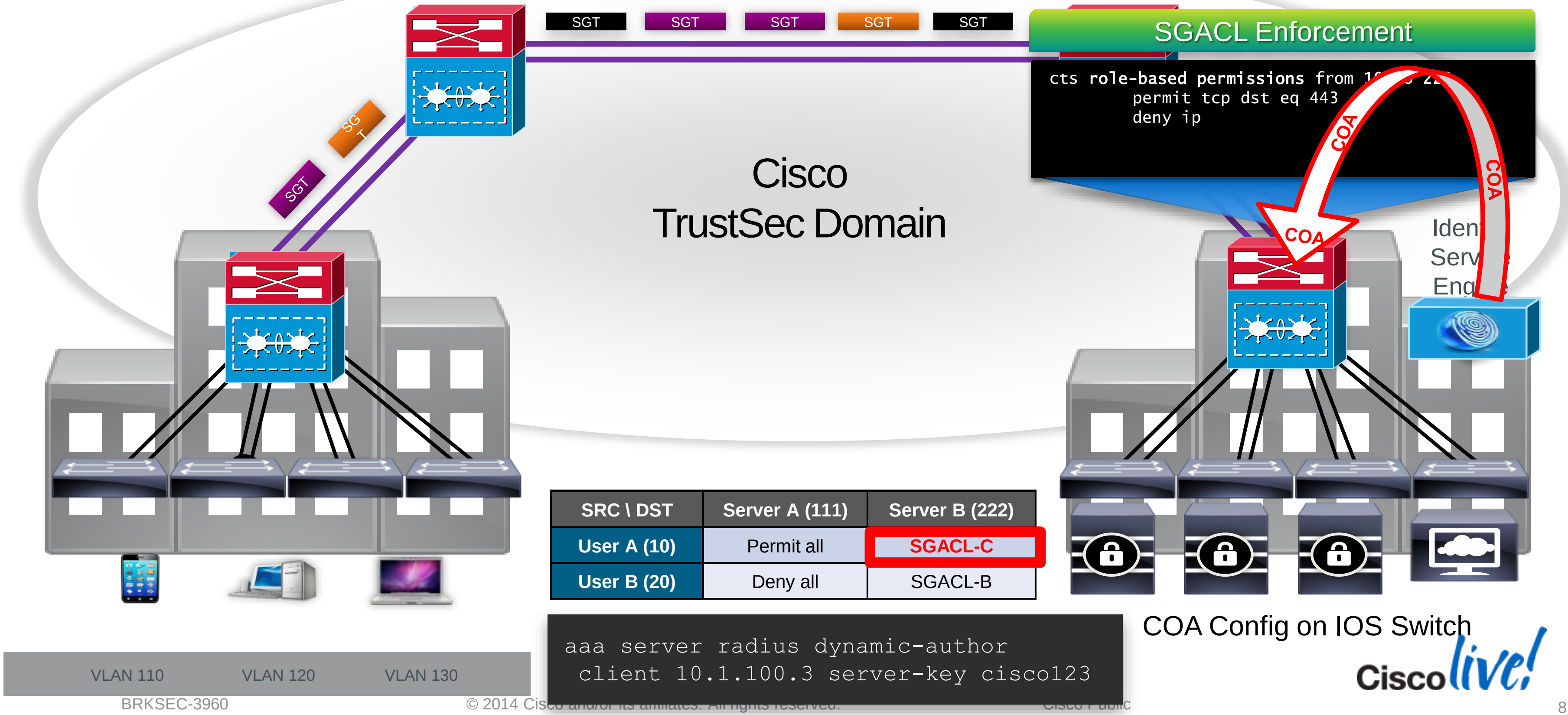
SGT and RADIUS COA



```
cts role-based permissions from 10 to 222
        permit tcp dst eq 443
        deny ip
```

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

SGT and RADIUS COA



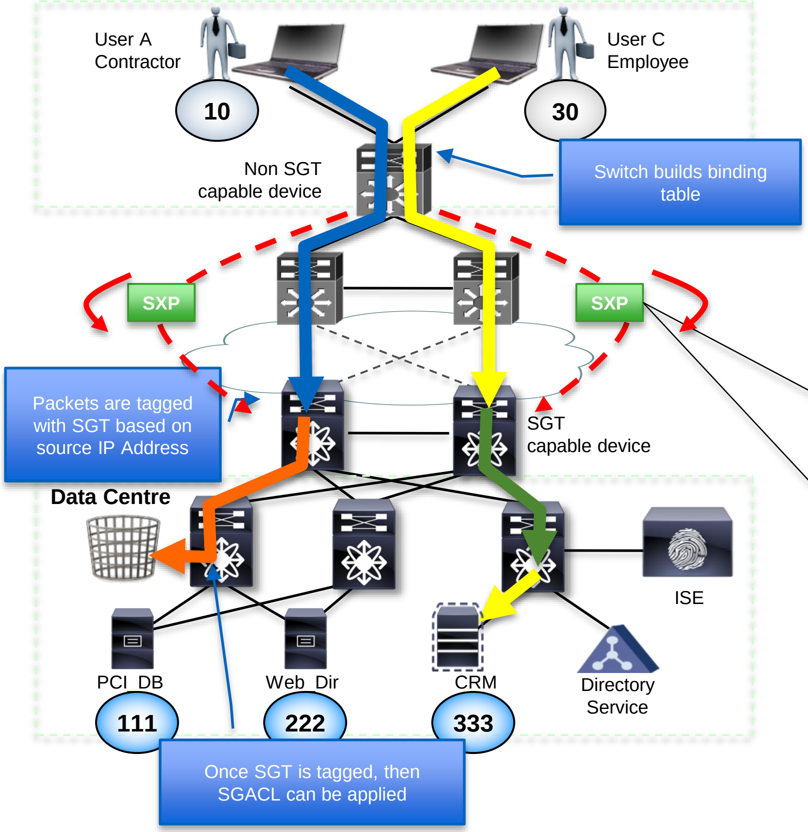
```
cts role-based permissions from 10 to 222
        permit tcp dst eq 443
        deny ip
```

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

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

COA Config on IOS Switch

IP-SGT Binding Exchange with SXP



Switch builds binding table

Packets are tagged with SGT based on source IP Address

Once SGT is tagged, then SGACL can be applied

TCP-based SXP is established between Non-TrustSec capable and TrustSec-Capable devices

- User is assigned to SGT
- Switch binds endpoint IP address and assigned SGT
- Switch uses SXP to send binding table to SGT capable device
- ***SGT capable device tags packet based on source IP address when packet appears on forwarding table***

SXP IP-SGT Binding Table

IP Address	SGT	Interface
10.1.10.1	Contractor - 10	Gig 2/10
10.1.30.4	Employee - 30	Gig 2/11

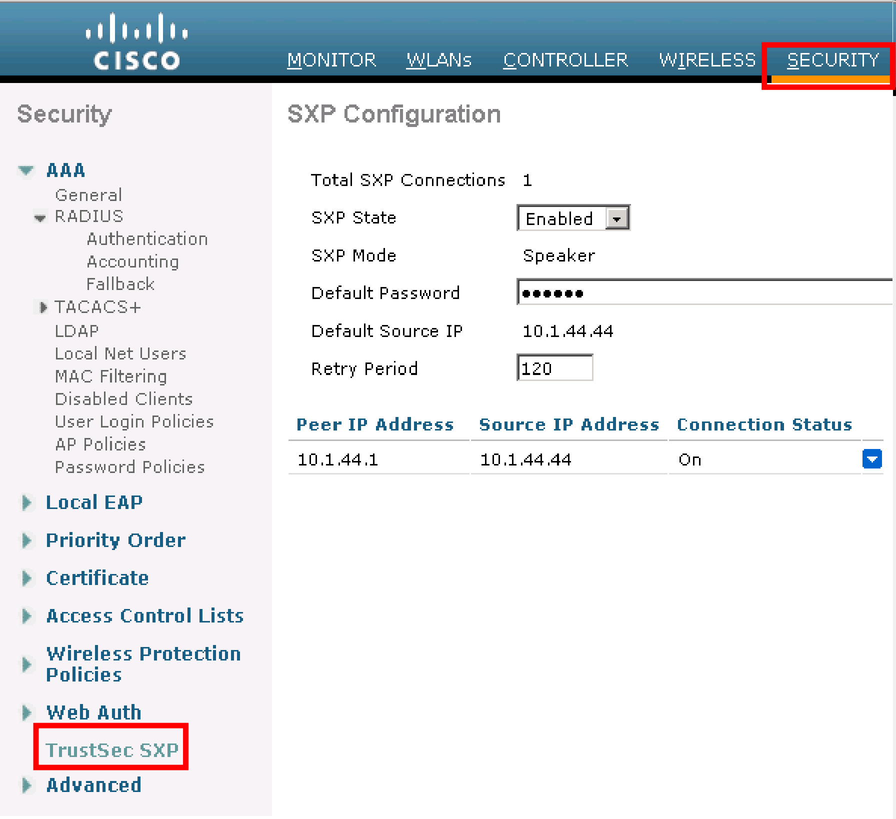
User A

● Untagged Traffic
● CMD Tagged Traffic

User C

● Untagged Traffic
● CMD Tagged Traffic

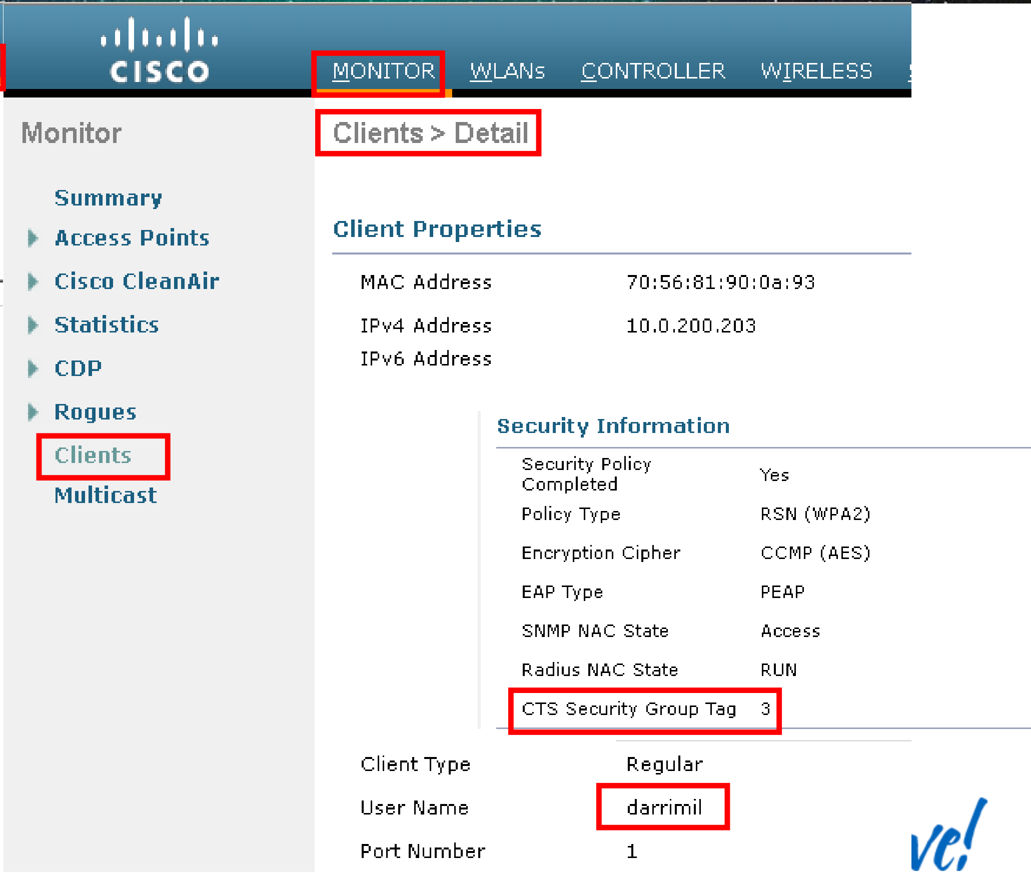
WLC SXP Configuration



SXP Configuration

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

Peer IP Address	Source IP Address	Connection Status
10.1.44.1	10.1.44.44	On



Clients > Detail

Client Properties

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

Security Information

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

Client Type	Regular
User Name	darrimil
Port Number	1

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

```
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
```

SGT Transport over non-TrustSec Domain

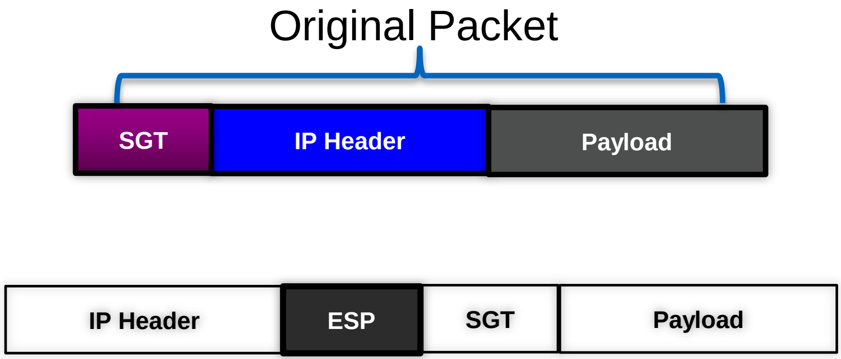
Connecting TrustSec Domains – L3 SGT Transport

Challenge

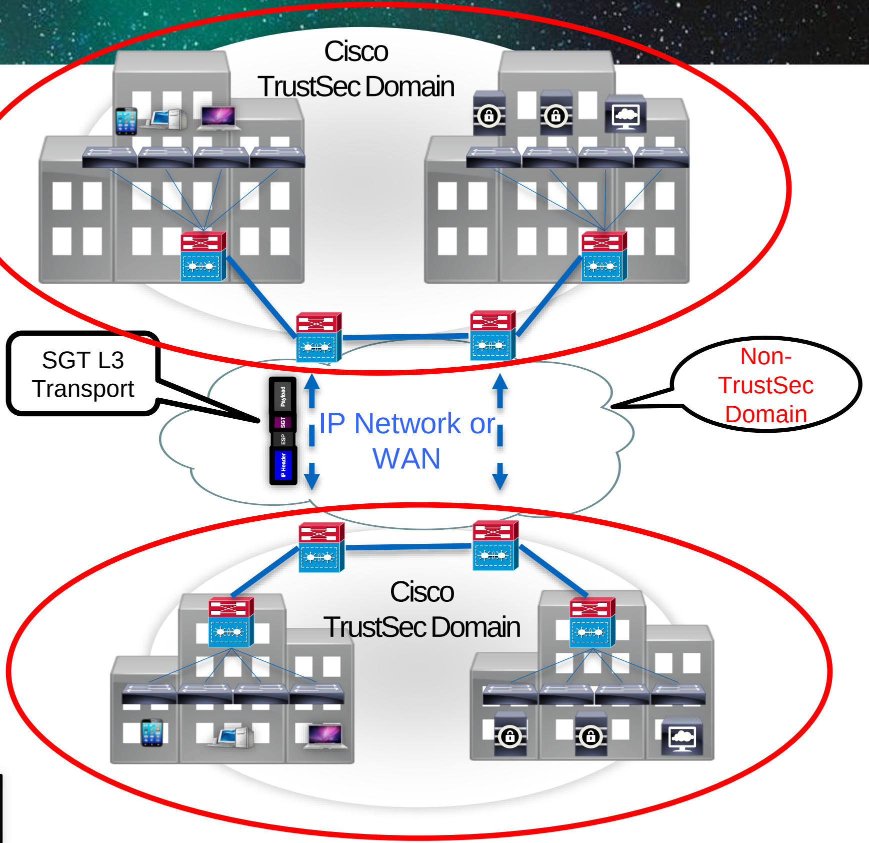
- Partial TrustSec infrastructure support

Solution

- Encap/Decap traffic in IP ESP header between sites
- SGT is carried in the ESP Payload
- No Payload Encryption



ESP – Encapsulating Security Payload

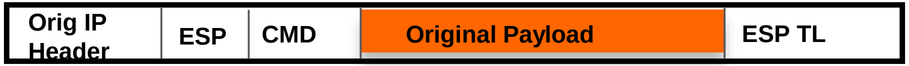


ESP overhead (42-45 bytes) impacts IP MTU/Fragmentation

Platform	Release
Cat6K (Sup2T)	15.0(1)SY

Crossing Non-SGT Capable Cores
6500/Sup2T SGT L3 Tag Forwarding (L3TF)

- Configure policy with explicit list of addresses in CTS domain to determine which packets need L3 CTS processing
- Packets sent with “transport mode” ESP to carry SGT without encryption or data authentication
- Simple H/W operations: encap/decap of ESP with NULL transform



Orig IP Header | ESP | CMD | Original Payload | ESP TL

Configure L3 Transport on the interface

```
Router(config)# interface TenGigabitEthernet 6/1
Router(config-if)# cts layer3 ipv4 trustsec forwarding
```

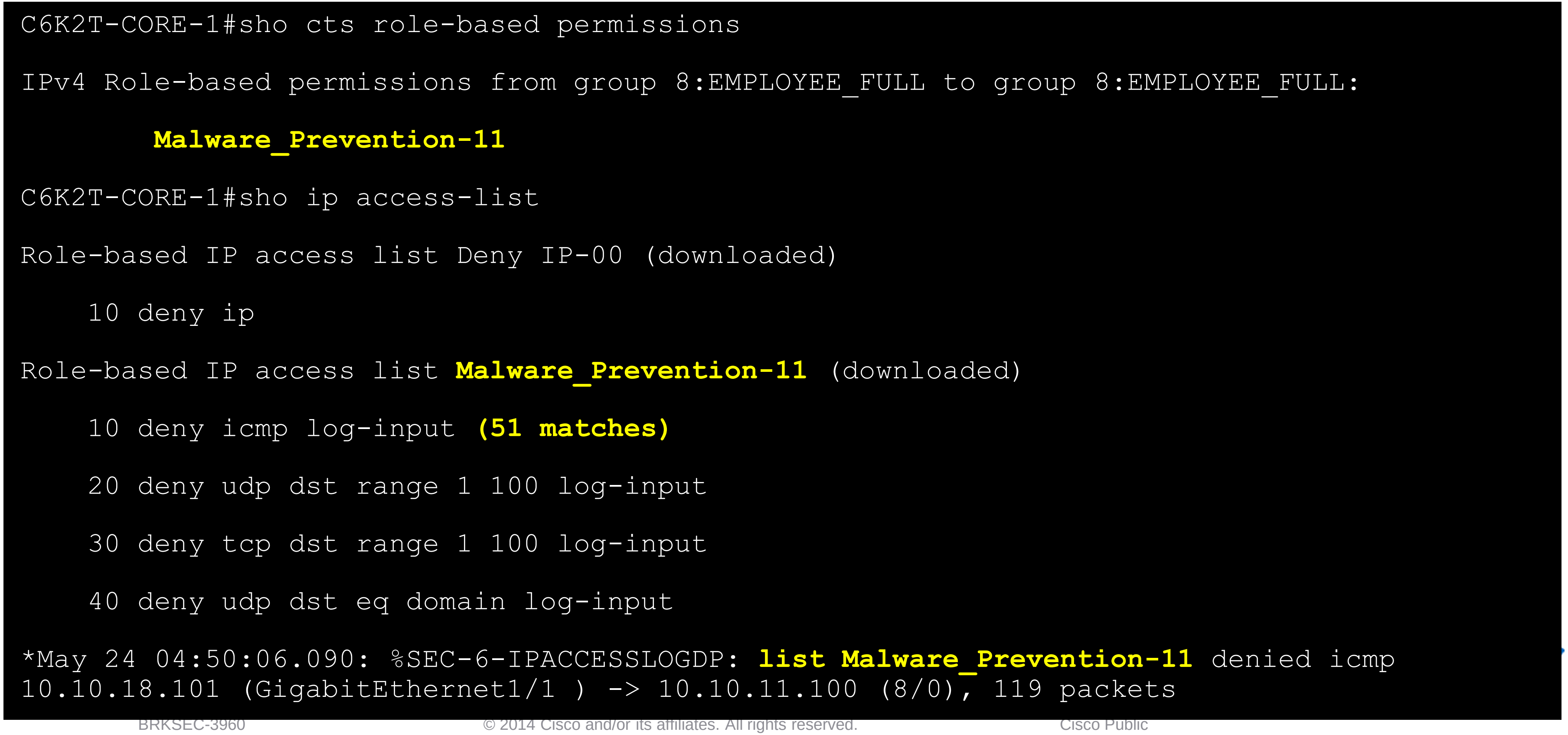
Policy for allowed Traffic

```
ip access-list extended l3-cts-policy
permit ip any 171.71.0.0/16
permit ip any 171.72.0.0/16
permit ip any 171.73.0.0/16
!
cts policy layer3 ipv4 traffic l3-cts-policy
```

Policy for exception traffic

```
ip access-list extended l3-cts-exception
permit ip any 171.74.0.0/16
permit ip any 171.75.0.0/16
permit ip any 171.76.0.0/16
!
cts policy layer3 ipv4 exception l3-cts-policy
```

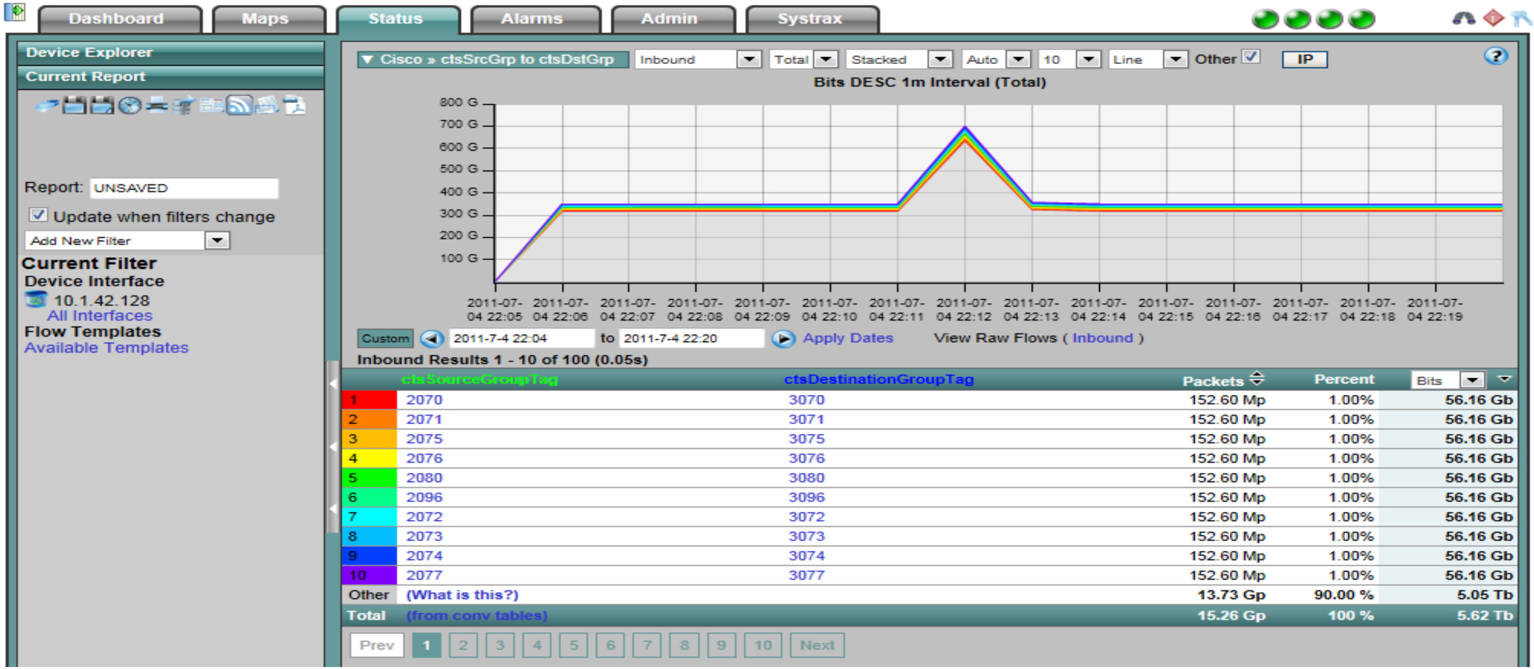
SGACL Monitoring – Best Effort Syslog



```
C6K2T-CORE-1#sho cts role-based permissions

IPv4 Role-based permissions from group 8:EMPLOYEE_FULL to group 8:EMPLOYEE_FULL:

        Malware_Prevention-11

C6K2T-CORE-1#sho ip access-list

Role-based IP access list Deny IP-00 (downloaded)

    10 deny ip

Role-based IP access list Malware_Prevention-11 (downloaded)

    10 deny icmp log-input (51 matches)

    20 deny udp dst range 1 100 log-input

    30 deny tcp dst range 1 100 log-input

    40 deny udp dst eq domain log-input

*May 24 04:50:06.090: %SEC-6-IPACCESSLOGDP: list Malware_Prevention-11 denied icmp
10.10.18.101 (GigabitEthernet1/1 ) -> 10.10.11.100 (8/0), 119 packets
```

Monitoring SGT Traffic with Netflow

Plixer collector displays SGT information



Report: UNSAVED

☑ Update when filters change

Add New Filter

Current Filter

Device Interface

10.1.42.128

All Interfaces

Flow Templates

Available Templates

2011-7-4 22:04 to 2011-7-4 22:20

Inbound Results 1 - 10 of 100 (0.05s)

	ctsSourceGroupTag	ctsDestinationGroupTag	Packets	Percent	Bits
1	2070	3070	152.60 Mp	1.00%	56.16 Gb
2	2071	3071	152.60 Mp	1.00%	56.16 Gb
3	2075	3075	152.60 Mp	1.00%	56.16 Gb
4	2076	3076	152.60 Mp	1.00%	56.16 Gb
5	2080	3080	152.60 Mp	1.00%	56.16 Gb
6	2096	3096	152.60 Mp	1.00%	56.16 Gb
7	2072	3072	152.60 Mp	1.00%	56.16 Gb
8	2073	3073	152.60 Mp	1.00%	56.16 Gb
9	2074	3074	152.60 Mp	1.00%	56.16 Gb
10	2077	3077	152.60 Mp	1.00%	56.16 Gb
Other	(What is this?)		13.73 Gp	90.00 %	5.05 Tb
Total	(from conv tables)		15.26 Gp	100 %	5.62 Tb

http://www.plixer.com/blog/netflow/cisco-trustsec-netflow-support/

Campus Design Notes

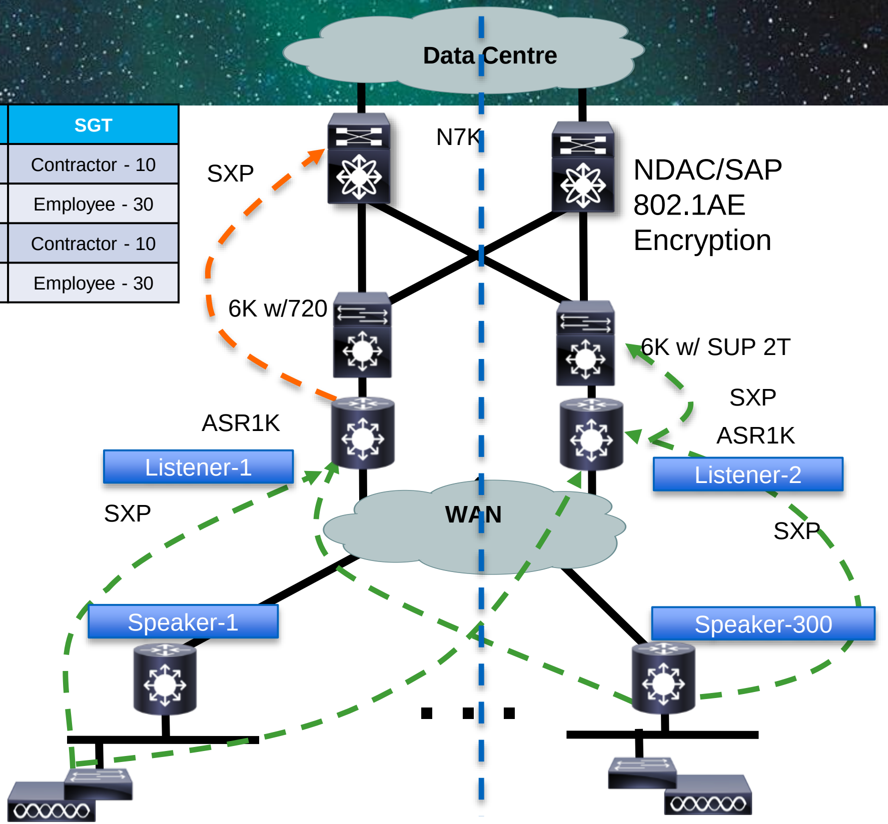
- Cat 3K-X “must” have “IP Device Tracking” (IPDT) enabled to be able to tag/filter
  - 802.1X/MAB/Web Auth or VLAN/SGT turn on IPDT by default
  - Static assignment on a port (server hanging off 3K-X stack) and 3K-X SXP does not have IPDT turned on by default
  - Enable IPDT on the port with the “ip device tracking maximum xx”
- Traffic destined for uplinks is subject to the “SGT/unknown SGT” policy in ISE egress matrix. Unknown SGT/unknown SGT in migration cases.
  - Make sure default policy is “permit ip” or
  - Turn off SGACL enforcement on the uplink with the CLI “no cts role-based enforcement” if the platform supports it
- Monitor Mode available – “match SGACL, but don’t enforce”

Branch Design Considerations

SXP WAN Deployment

- ISRG2 – 15.2(2)T
- ASR1K - IOS XE 3.4
- Cat6K(SUP 2T) - IOS 12.2(50)SY1
    - Unidirectional only
    - No loop detection
    - Branch to DC enforcement only

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



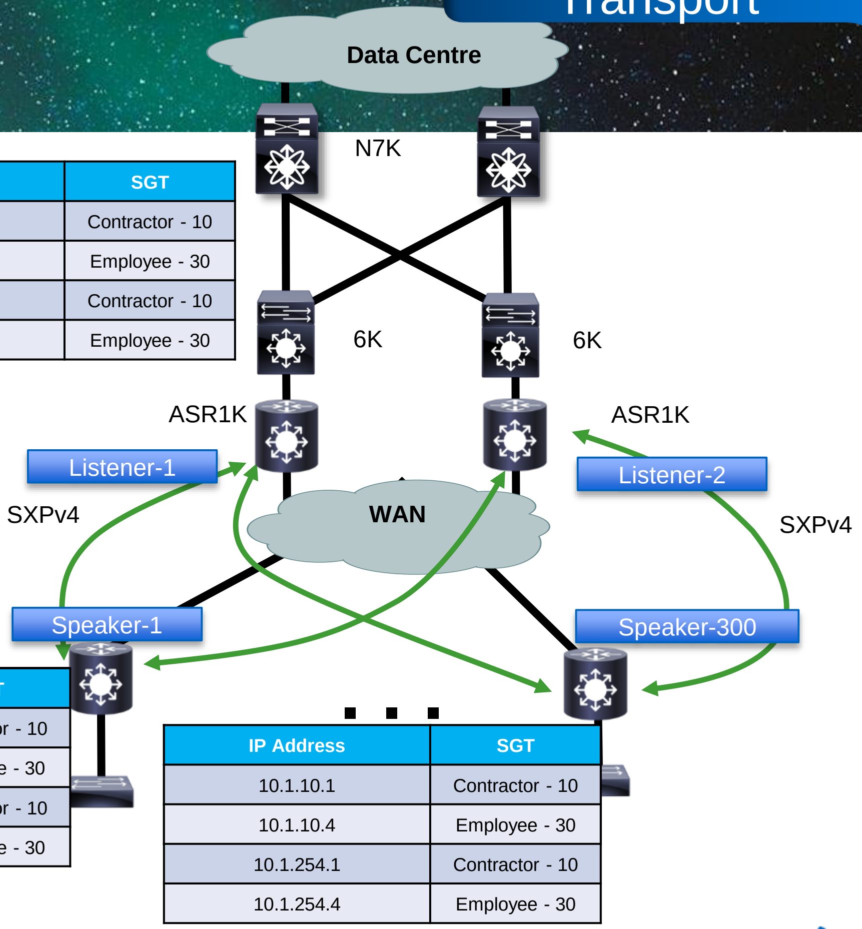
IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30

IP Address	SGT
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30

- Figure for Illustrations purposes only
- Don’t interpret as recommended topology

SXPv4 WAN Deployment

- ISRG2 – 15.3(2)T
- ASR1K- IOS XE 3.9
- Cat6K(SUP 2T) – 15.1(1)SY
- Bidirectional SXP with Loop Detection
- Allows ASR1K to be an IP/SGT relay from remote to remote
- Review scale for ISRs since SXP is a fully replication model

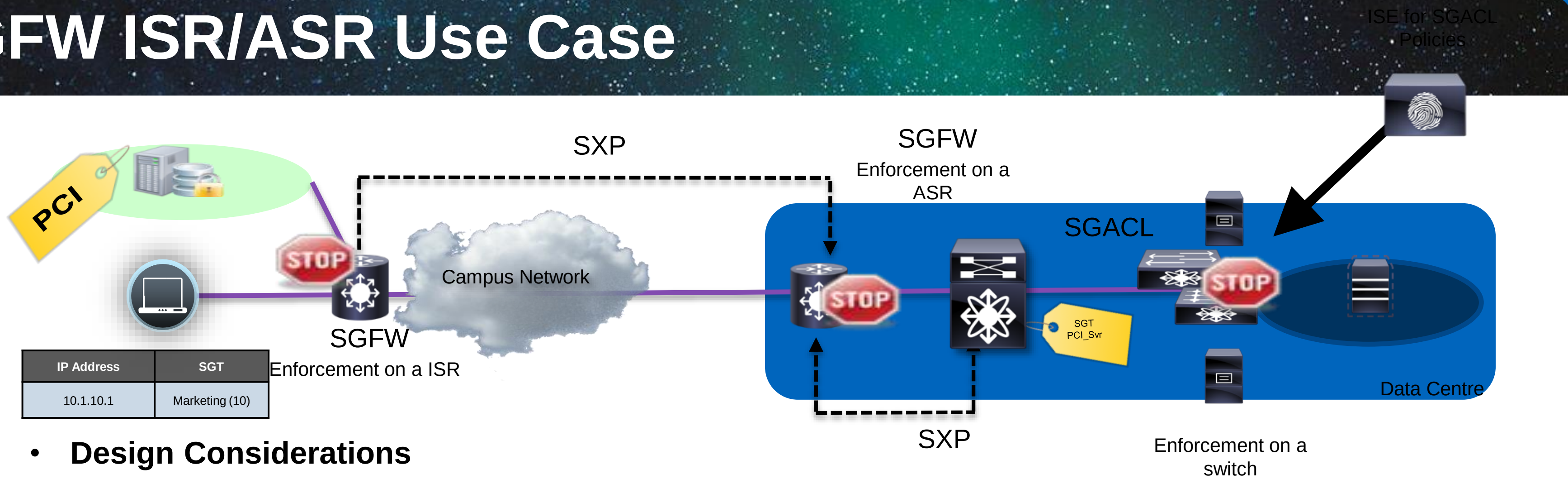


IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30

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

SGFW ISR/ASR Use Case

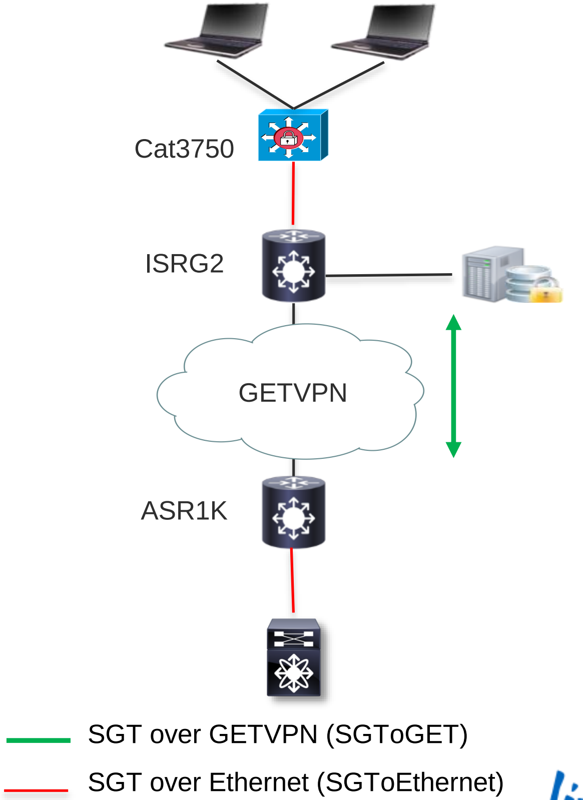


IP Address	SGT
10.1.10.1	Marketing (10)

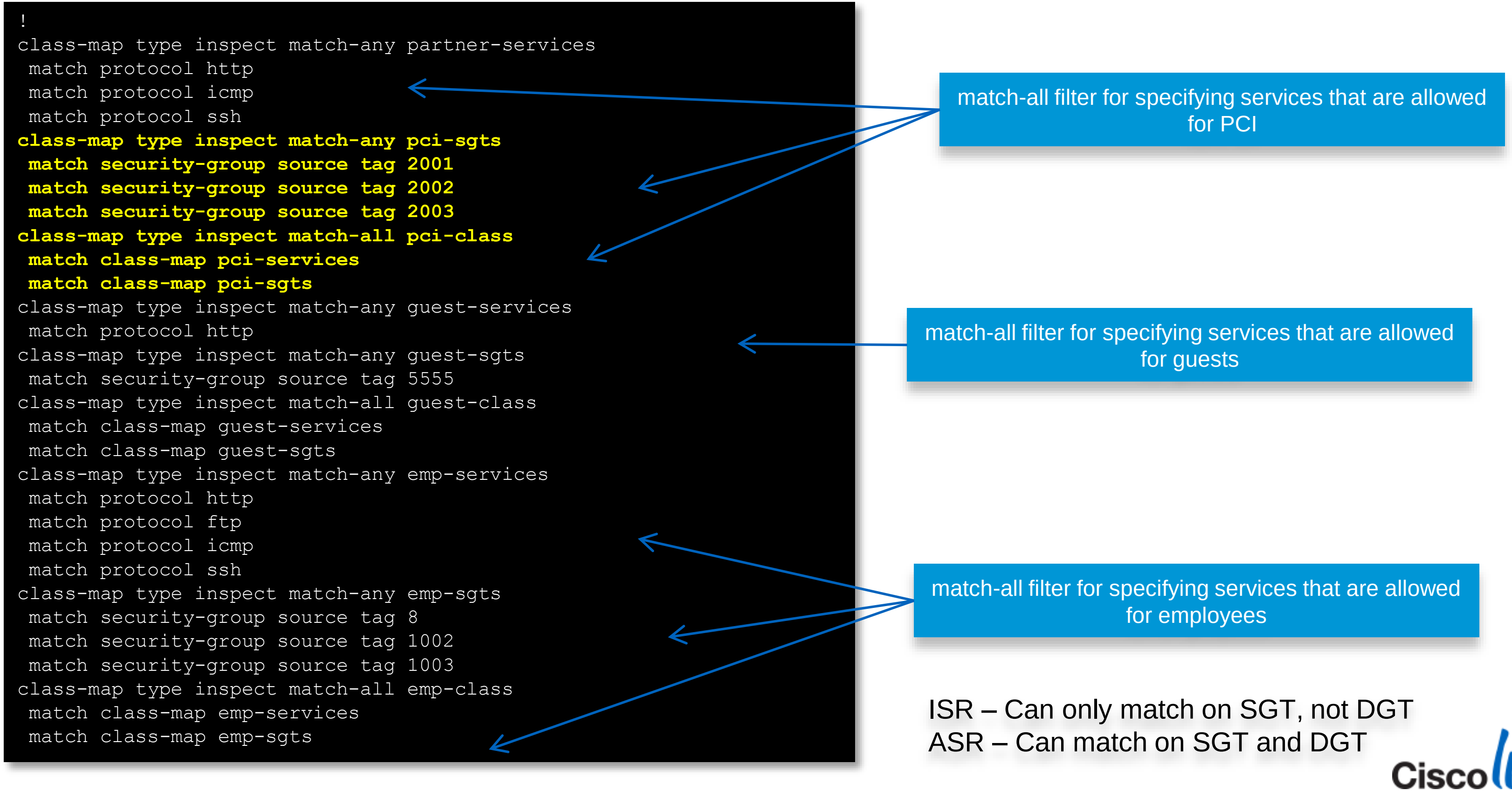
- **Design Considerations**
  - **Consistent Classification/enforcement between ISR/ASR SGFW and switching.**
  - ***In general SGACL and SGFW policy should be sync'd via policy administration UI***
  - **Normal positioning to justify ISR/ASR ZBFW in branch and DC WAN edge**
  - **SGT allows more dynamic classification in the branch and DC WAN edge**
    - **SGT only used in the source for ISR**
    - **SGT can be source and destination on ASR**
  - **Rich Logging requirements will be fulfilled on SGFW – URL logging, etc.**
  - **Active/Active support in ZBFW allows for async routing**
    - active/active assumes shared L3 subnet on router interfaces for redundancy groups

Simple Topology Enablement

- East-West traffic enforced via SGACL
  - From User 1 -> User 2 enforced on 3750X
  - From User 2 -> PCI_DB enforced on ISRG2
    - SGT from frame
    - SGT/PCI Subnet in ZBFW config
- North-South
  - From access layer 3KX to DC enforced in DC
  - From DC to access layer
    - DC -> 3KX enforced on 3KX
    - DC -> PCI Subnet enforced on ISRG2 ZBFW



ISR G2 SGFW Configuration Example



```
!
class-map type inspect match-any partner-services
 match protocol http
 match protocol icmp
 match protocol ssh
class-map type inspect match-any pci-sgts
 match security-group source tag 2001
 match security-group source tag 2002
 match security-group source tag 2003
class-map type inspect match-all pci-class
 match class-map pci-services
 match class-map pci-sgts
class-map type inspect match-any guest-services
 match protocol http
class-map type inspect match-any guest-sgts
 match security-group source tag 5555
class-map type inspect match-all guest-class
 match class-map guest-services
 match class-map guest-sgts
class-map type inspect match-any emp-services
 match protocol http
 match protocol ftp
 match protocol icmp
 match protocol ssh
class-map type inspect match-any emp-sgts
 match security-group source tag 8
 match security-group source tag 1002
 match security-group source tag 1003
class-map type inspect match-all emp-class
 match class-map emp-services
 match class-map emp-sgts
```

match-all filter for specifying services that are allowed for PCI

match-all filter for specifying services that are allowed for guests

match-all filter for specifying services that are allowed for employees

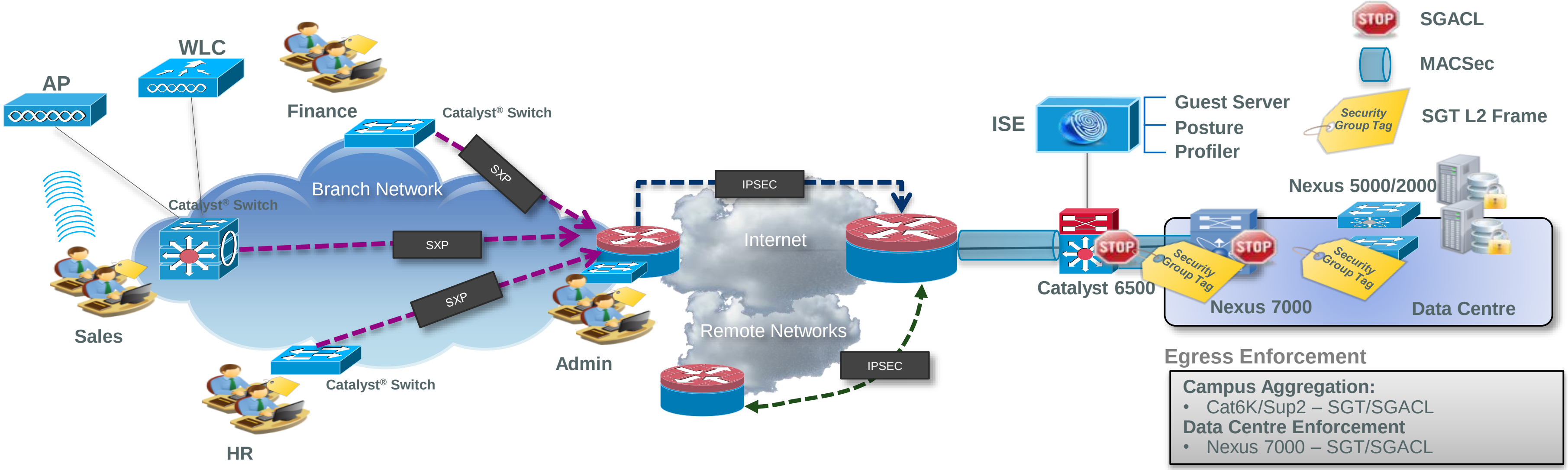
ISR – Can only match on SGT, not DGT
ASR – Can match on SGT and DGT

ISR G2 SGFW Configuration Example

```
!
policy-map type inspect branch-policy
 class type inspect emp-class
  inspect
 class type inspect pci-class
  inspect
 class type inspect guest-class
  inspect
 class class-default
  drop
!
zone security lan
zone security pci
zone-pair security lan-pci source lan destination pci
 service-policy type inspect branch-policy
!
interface GigabitEthernet0/1
 description Connection to Branch1 3750X
 ip address 172.16.11.1 255.255.255.0
 zone-member security lan
 cts manual
   policy static sgt 2 trusted
!
!
interface GigabitEthernet0/2
 description ***connection to pci***
 ip address 172.16.0.1 255.255.255.252
 zone-member security pci
 cts manual
   policy static sgt 2 trusted
!
```

Specific class filters are defined inside policy maps for each sgt groups

SGT Transport over IPSec VPN

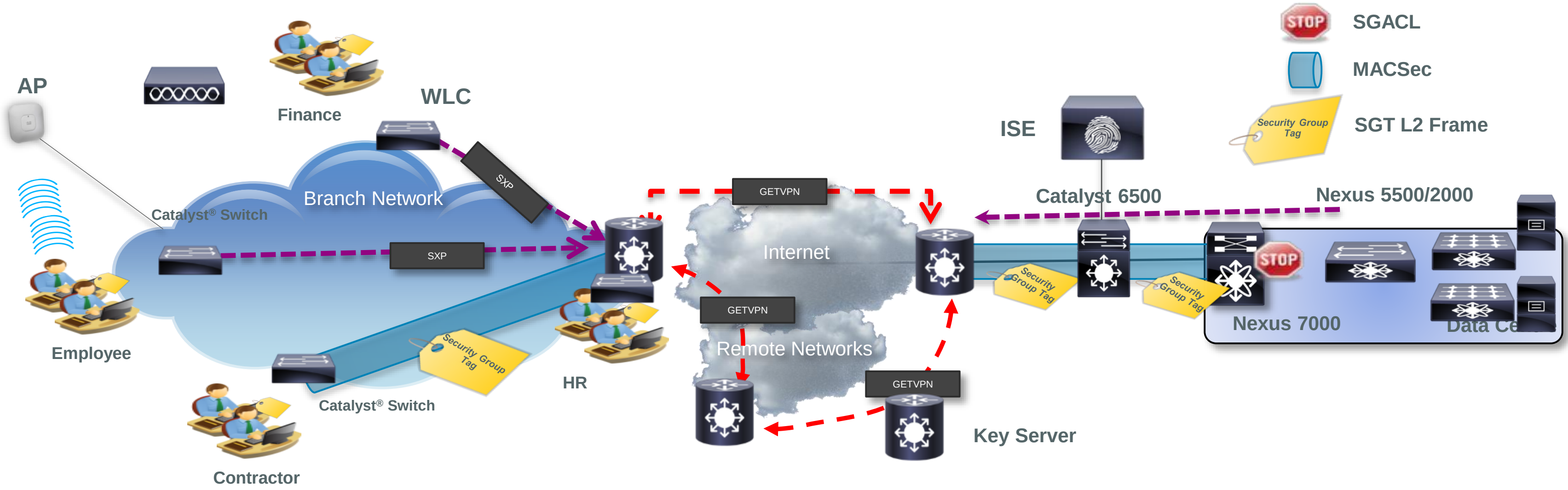


Campus Aggregation:
- Cat6K/Sup2 – SGT/SGACL

Data Centre Enforcement
- Nexus 7000 – SGT/SGACL

- IPSEC inline Tagging – ESP Header
- SGT Capability exchange during IKEv2 negotiations
- Learn SGT from SXP or Auth-methods
- Site-to-Site IPSEC such as DMVPN, DVTI, SVTI methods supported
- Failover is based on the underlying IPSec technology
- Scale is based on the underlying IPSec technology
- DMVPN – ISR to ISR now. ISR to ASR1K in middle CY14 – 15.4(1)T1 (ISR) and 15.4(1)S1 (ASR1K)

SGT- GETVPN WAN Deployment ISRG2 15.(3)2T and ASR IOS XE 3.9



- GETVPN inline Tagging – GET Header
- SGT Capability exchange during GET key negotiations
- Learn SGT from SXP, inline tag or Auth-methods
- Failover is the based on GET VPN failover
- Scale is based on GET VPN Scale

GET VPN Configuration (Key Server):

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.10.6
crypto isakmp key cisco123 address 172.16.10.1
!
!
crypto ipsec transform-set aes128 esp-aes esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile profile1
 set security-association lifetime seconds 7200
 set transform-set aes128
Crypto gdoi group GDOI
Identity number 12345
Server local
Rekey algorithm aes 256
Rekey transport unitcast
(cont…)
```

```
Sa ipsec 1
  profile profile1
  match address ipv4 getvpn-acl
  replay time window-size 5
  tag cts sgt  → This is what enables SGToGETVPN
Address ipv4 10.39.1.190

ip access-list extended getvpn-acl
 deny   udp any eq 848 any eq 848
 deny   tcp any any eq tacacs
 deny   tcp any eq tacacs any
 deny   tcp any any eq bgp
 deny   tcp any eq bgp any
 deny   ospf any any
 deny   eigrp any any
 deny   udp any any eq ntp
 deny   udp any eq ntp any
 deny   udp any any eq snmp
 deny   udp any eq snmp any
 deny   udp any any eq syslog
 deny   udp any eq syslog any
 permit ip any any
```

Group Member HQ – ASR1000:

- This configuration snippet shows just the GETVPN configuration piece and the configuration to natively carry the tag from the WAN natively to the next hop inside which is Nexus 7000 Switches.
- Note: To enable SGToGET VPN there is no configuration needed on the Group Members, as this configuration is pulled from the key Servers
- Note: To carry the TAG natively you must go into CTS manual mode on the interface, then set the static SGT to the device tag (2) in this case. The trusted keyword is entered after the SGT assignment telling the router to trust tags coming from the device down stream, and send tags downstream. That is all that’s need on the head-end ASRs to carry the tag natively

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 300
crypto isakmp key cisco123 address 10.39
!
!
!
!
crypto gdoi group GDOI
 identity number 12345
 server address ipv4 10.39.1.190
!
!
crypto map gdoimap 1 gdoi
 set group GDOI
Interface GigabitEthernet0/0/1
Description Connection to Carrier
Ip address 172.16.10.1 255.255.255.252
Cdp enable
Crypto map gdoimap
```

```
interface TenGigabitEthernet0/1/0
 description ***Connection to N7KA e1/17*
 ip address 172.16.1.5 255.255.255.252
 ip wccp 61 redirect in
 ip flow monitor lancope-mon input
 cts manual
  policy static sgt 2 trusted
 cdp enable
!
interface TenGigabitEthernet0/3/0
 description ***Connection to N7KB e1/17*
 ip address 172.16.1.1 255.255.255.252
 ip wccp 61 redirect in
 ip flow monitor lancope-mon input
 cts manual
  policy static sgt 2 trusted
 cdp enable
```

Group Member Branch1 – ISRG2:

- This configuration snippet shows just the GETVPN configuration piece and the configuration to natively carry the tag from the WAN natively to the next hop inside which is Catalyst 3750X branch switch.
- Note: To enable SGToGET VPN there is no configuration needed on the Group Members, as this configuration is pulled from the key Servers
- Note: To carry the TAG natively you must go into CTS manual mode on the interface, then set the static SGT to the device tag (2) in this case. The trusted keyword is entered after the SGT assignment telling the router to trust tags coming from the device down stream, and send tags downstream. That is all that’s need on the ISRG2 to carry the tag natively

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 300
crypto isakmp key cisco123 address 10.39
crypto gdoi group GDOI
 identity number 12345
 server address ipv4 10.39.1.190

crypto map gdoimap 1 gdoi
 set group GDOI

Int g0/0
Description Connection to WAN Carrier
Ip address 172.16.10.6 255.255.255.252
Crypto map gdoimap
```

```
interface GigabitEthernet0/1
 description Connection to Branch1 3750X
 ip address 172.16.11.1 255.255.255.252
 duplex auto
 speed auto
 cts manual
   policy static sgt 2 trusted
```

Switch Branch1 – Catalyst 3750X:

- This configuration snippet shows basic bootstrap config of ISE and whats needed for CTS on the 3750X
- Note: To carry the TAG natively you must go into CTS manual mode on the interface, then set the static SGT to the device tag (2) in this case. The trusted keyword is entered after the SGT assignment telling the router to trust tags coming from the device down stream, and send tags downstream. You should also do basic AAA bootstrapping of CTS and enable role-based enforcement
- Port g1/0/2 has basic setup for an 802.1X authenticated port

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting update periodic 5
aaa accounting dot1x default start-stop group rad
aaa accounting system default start-stop group
radius
aaa server radius dynamic-author
 client 10.39.1.120 server-key c1sc0
ip dhcp snooping
ip domain-name pghlab.cisco.com
ip device tracking
device-sensor accounting
device-sensor notify all-changes
cts authorization list default
cts role-based enforcement
dot1x system-auth-control
interface GigabitEthernet1/0/1
 description Connection to GETVPN_GM
 no switchport
 ip address 172.16.11.2 255.255.255.252
 cts manual
  policy static sgt 2 trusted
```

```
interface GigabitEthernet1/0/2
 description Desktop Port
 switchport access vlan 23
 switchport mode access
 ip access-group ACL-ALLOW in
 authentication host-mode multi-auth
 authentication port-control auto
 dot1x pae authenticator
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host 10.39.1.120 auth-port 1812 acct-
port 1813 key c1sc0
radius-server vsa send accounting
radius-server vsa send authentication
ip radius source-interface GigabitEthernet1/0/1
```

Verify Native SGT Tagging in Branch:

```
GET-BRANCH-SW#show cts platform interface ethernet 1/0 stats detail
Interface Ethernet1/0
    L2-SGT Statistics
        Pkts In                     : 8449
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 9413
        Pkts Drop (malformed packet): 0
        Pkts Drop (invalid SGT)     : 0
GET-BRANCH-SW#sho crypto ipsec sa detail

interface: GigabitEthernet0/0
    Crypto map tag: CM1, local addr 10.10.1.9

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: grp1
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 287738, #pkts encrypt: 287738, #pkts digest: 287738
    #pkts decaps: 195190, #pkts decrypt: 195190, #pkts verify: 195190
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
    #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
    #pkts invalid prot (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
    ##pkts replay failed (rcv): 0
    #pkts tagged (send): 287738, #pkts untagged (rcv): 101285
    #pkts not tagged (send): 0, #pkts not untagged (rcv): 93905
    #pkts internal err (send): 0, #pkts internal err (recv) 0
```

Command Semantics

L2-SGT Statistics => Statistics for interface configured with ‘cts manual’
Pkts In => Number of packets received (i.e SGT tagged or untagged)
Pkts Out => Number of packets transmitted (if the interface is enabled for ‘propagate sgt’
then it indicates the number packets transmitted with CMD-SGT tagged, else
it denotes packets sent without CMD-SGT.
Pkts Drop => Number of ingress packet drops due to mal-formed CMD packets or invalid
SGT (0xffff)
Pkts (policy SGT assigned) => Number of ingress packets assigned
with sgt as per ‘policy static sgt <num>’ policy on the interface.

Command Semantics

#pkts tagged (send) – SGT Tagged packets in IPSec
#pkts not tagged (send) – Bypassed in IPSec for SGT tagging
#pkts untagged (rcv) – packets from IPSec unencapped with SGT
#pkts not untagged (rcv) – packets from IPSec with no SGT

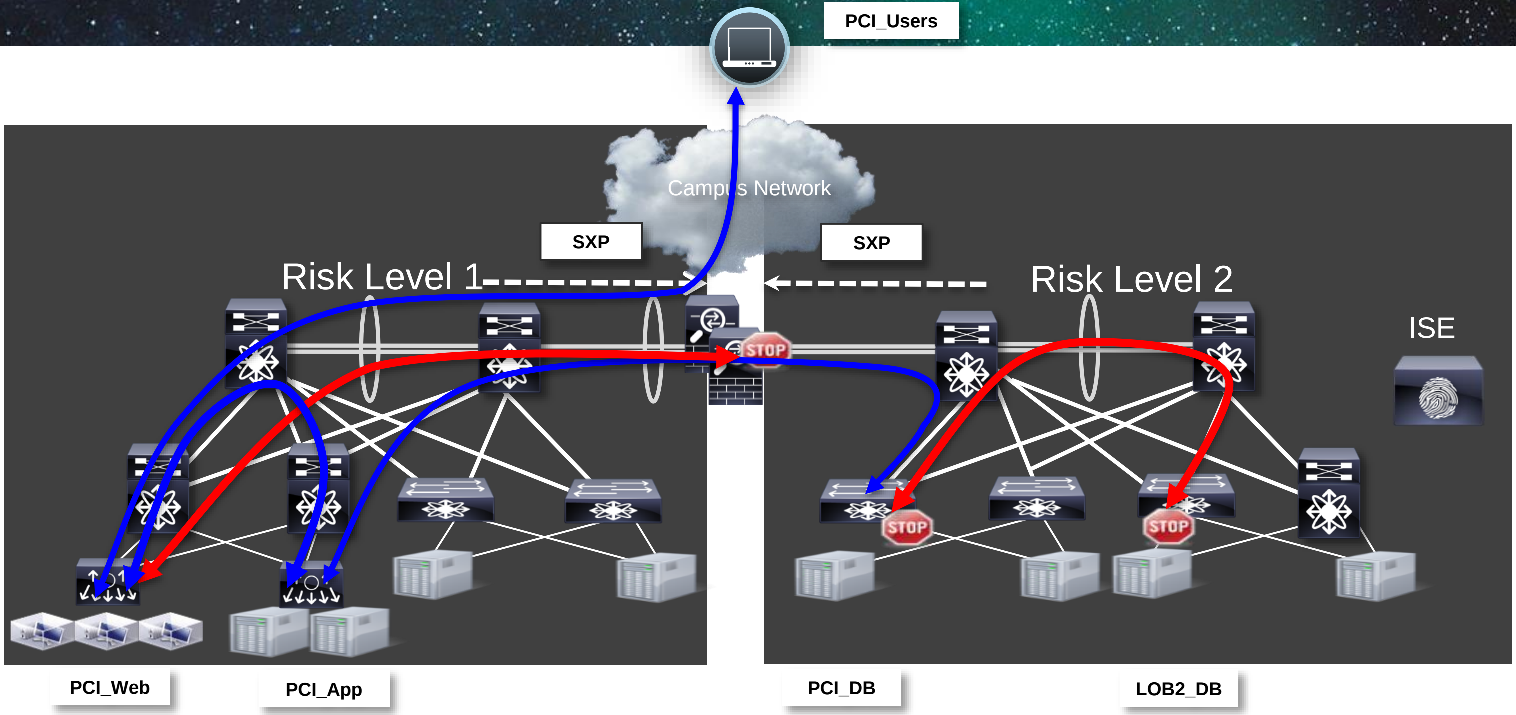
Verify Native SGT Tagging WAN HE:

- Run the following show platform command on the ASR router to verify IPSec SGT packets are coming in

```
Shauns_ASR_Headend#show platform hardware qfp act feature cts datapath stats
 Tagged Packets rcv: 33061543 xmt: 978506741      Def tag: 0
         Unknown SGT: 725160463         Unknown DGT: 0
 Invalid tags (drop): 0       Bad format (drop): 0
 No xmt buffer: 0
 IPSec SGT tagged packets received: 1854471
IPSec Invalid SGT tagged packets received: 0
```

Data Centre Design Considerations

Customer End State in the DC



Data Centre Environment:

- SGT classification of servers (N1KV Port Profile, N5K Port, N7K IP/SGT)
- SGACL on switches enforcement within Risk Level
- ASA between Risk Levels (sent IP/SGT from infrastructure)

Campus/Data Centre

North - South Traffic Flow

- ASA 9.x “only” supports SXP
- How do I handle an ASA fronting DC resources?
- How do I handle 3rd party services sitting in front of the DC
  - IPS
  - SLB
  - etc.
- Two options
  - Build SXP from access layer to DC
  - Use Native Tagging transport to DC services layer and use SGT Caching

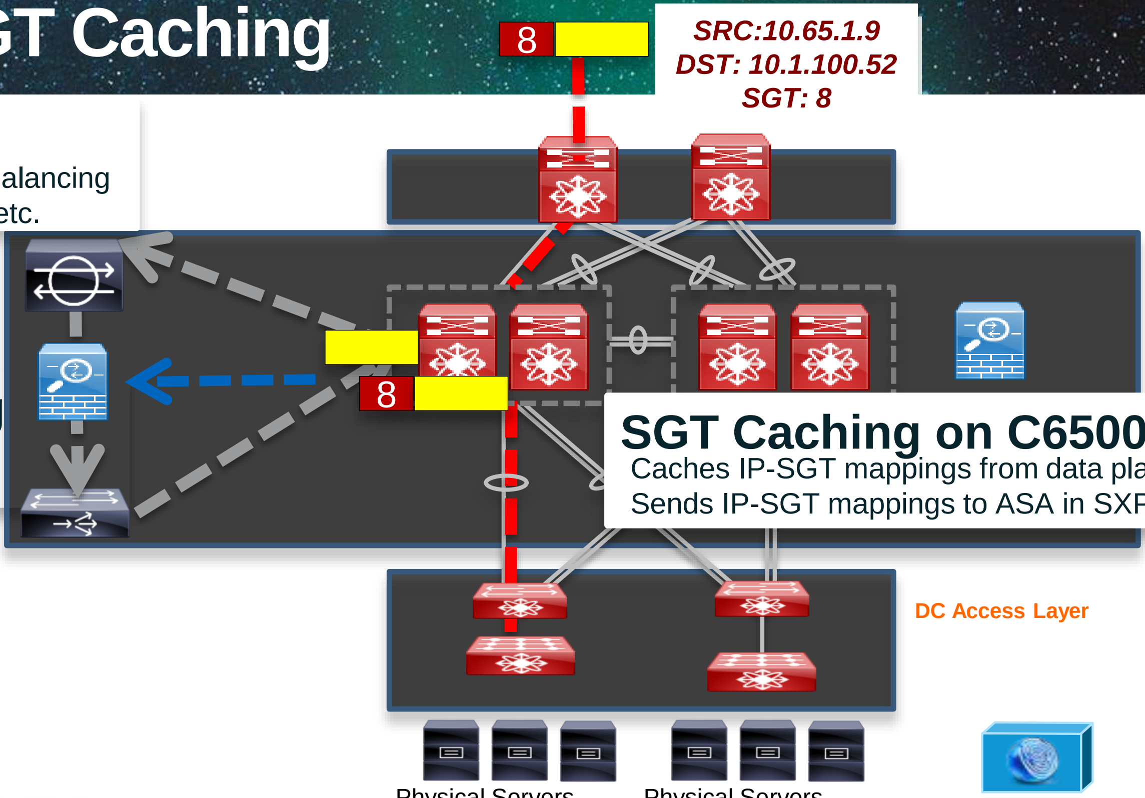
Services with SGT Caching

Service Chaining

Possible 3rd party devices for Server Load Balancing (SLB), Intrusion Prevention Services (IPS), etc.

Security Group Firewalling

Firewall rule automation
using ASA SG-Firewall functions



SRC:10.65.1.9
DST: 10.1.100.52
SGT: 8

SGT Caching on C6500/N7K

Caches IP-SGT mappings from data plane
Sends IP-SGT mappings to ASA in SXP

IP Address	SGT
10.65.1.9	8 (Employee_Full)

SGT Tagged Traffic

Untagged Traffic

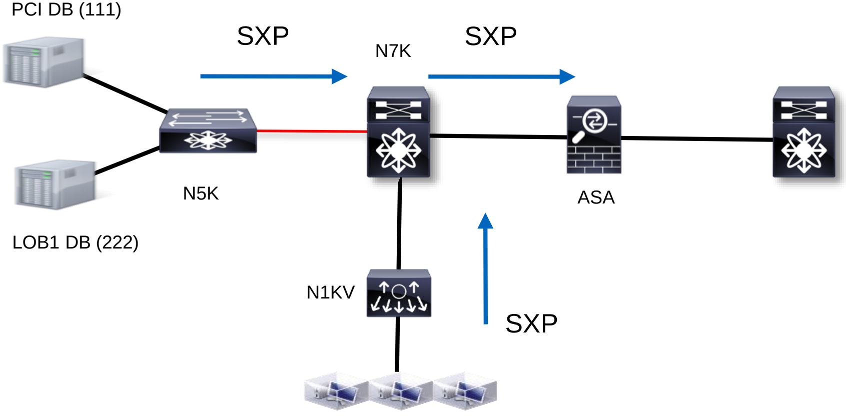
SXP

🟥 **SGACL enabled Device**

🟦 **SG Firewall enabled Device**

Example DC Topology

- East-West traffic enforced via SGACL
  - From PCI DB <-> LOB1 DB enforced on N5K
  - From N5K -> N1KV enforced N7K
    - SGT from frame
    - IP/SGT from SXP
  - N1KV -> N5K enforced on N7K
    - IP/SGT from SXP
    - IP/DGT from SXP
- North-South
  - From N5K/N1KV to Campus/Branch enforced on ASA
  - From Risk Level 1 -> Risk Level 2 enforced on ASA



SXP – Security eXchange Protocol

SGT over Ethernet (SGToEthernet)

N5K East-West Segmentation Configuration

```
pghlab-55ka(config)# feature cts                                    → Enables CTS feature
pghlab-55ka(config)# cts device-id N55KA password trustsec123      → Sets up device ID and password
                                                                      used in ISE NAD config
pghlab-55ka(config)# cts role-based counters enable                 → Turn on SGACL counters
pghlab-55ka(config)# vlan 118
pghlab-55ka(config-vlan)# cts role-based enforcement                → Enable Role Based enforcement on
                                                                      VLAN 118
pghlab-55ka(config-vlan)# int e 1/1
pghlab-55ka(config-vlan)# switchport trunk
pghlab-55ka(config-vlan)# switchport trunk native vlan 2
pghlab-55ka(config-vlan)# cts manual                                → Go into CTS manual mode for the
                                                                      port (other int CLI clipped)
pghlab-55ka(config-if-cts-manual)# policy static sgt 0x2 trusted → Set SGT and Trust for
          Trunk to N7KA  (for screen real estate)
```

N5K East-West Segmentation Configuration

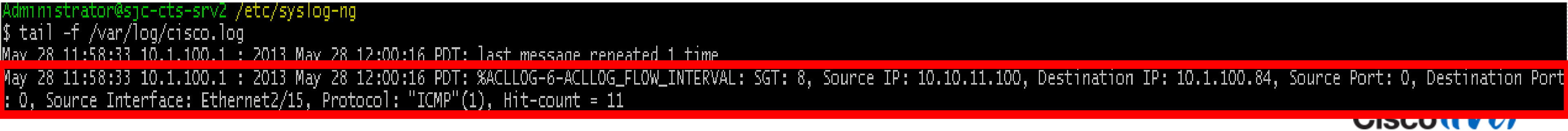
```
pghlab-55ka(config-vlan)# int e102/1/1
pghlab-55ka(config-vlan)# switchport
pghlab-55ka(config-vlan)# switchport access vlan 118
pghlab-55ka(config-vlan)# cts manual                          → Go into CTS manual mode for the port
pghlab-55ka(config-if-cts-manual)# policy static sgt 0x111    → Set SGT on the FEX port e102/1/1 to SGT 111
pghlab-55ka(config-if-cts-manual)# no propagate-sgt           → "Don't send the SGT to the server"
                                                                This would be bad. ☺
pghlab-55ka(config-if-cts-manual)# no shut
pghlab-55ka(config-vlan)# int e102/1/2
pghlab-55ka(config-vlan)# switchport
pghlab-55ka(config-vlan)# switchport access vlan 118
pghlab-55ka(config-vlan)# cts manual                          → Go into CTS manual mode for the port
pghlab-55ka(config-if-cts-manual)# policy static sgt 0x222    → Set SGT on the FEX port e102/1/1 to SGT 222
pghlab-55ka(config-if-cts-manual)# no propagate-sgt           → "Don't send the SGT to the server"
                                                                This would be bad. ☺
pghlab-55ka(config-if-cts-manual)# no shut
pghlab-55ka(config)# cts sxp enable                   → Enable SXP protocol for peering relationships
Pghlab-55ka(config)# cts sxp connection peer 10.49.1.2 source 10.49.1.10 password none mode listener →Peer with 7KA
Pghlab-55ka(config)# cts sxp connection peer 10.49.1.3 source 10.49.1.10 password none mode listener →Peer with 7KB
```

N7K East-West Configuration

```
feature cts
feature dot1x
cts device-id N7KA password 7 wnyxlszh123
cts role-based counters enable
cts role-based sgt-map 10.39.1.30 17
…….
cts role-based sgt-map 10.87.109.72 3
cts role-based enforcement

vlan 87
  cts role-based enforcement
vlan 118
  cts role-based enforcement
interface Ethernet1/25
  description N5K connection
  cts manual
    policy static sgt 0x0002 trusted
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 90,118-120,124
  spanning-tree port type normal
  channel-group 10 mode active
  no shutdown
```

Logging from N7K

```
pghlab-n7ka-n7k-shaun# show cts role-based policy
sgt:8
dgt:6    rbacl:PERMIT_MAIL
         deny icmp log
         permit tcp dst eq 110
         permit tcp dst eq 143
         permit tcp dst eq 25
         permit tcp dst eq 465
         permit tcp dst eq 585
         permit tcp dst eq 993
         permit tcp dst eq 995
         deny all log
pghlab-n7ka-n7k-shaun(config)# log level acllog 6   ← Recommended log levels
pghlab-n7ka-n7k-shaun(config)# log level cts 5
pghlab-n7ka-n7k-shaun(config)# log ip access-list include sgt
pghlab-n7ka-n7k-shaun# show logging ip access-list cache detail
SGT      Source IP         Destination IP      S-Port   D-Port     Interface    Protocol          Hits
-------------------------------------------------------------------------------------------------
8        10.10.11.100      10.1.100.84         0        0          Ethernet2/15  (1)ICMP           8
```

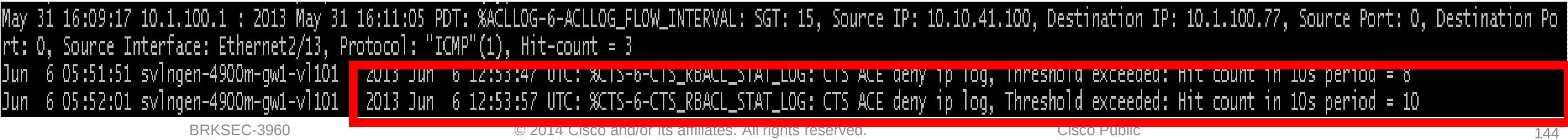


```
Administrator@sjc-cts-srv2 /etc/syslog-ng
$ tail -f /var/log/cisco.log
May 28 11:58:33 10.1.100.1 : 2013 May 28 12:00:16 PDT: last message repeated 1 time
May 28 11:58:33 10.1.100.1 : 2013 May 28 12:00:16 PDT: %ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 8, Source IP: 10.10.11.100, Destination IP: 10.1.100.84, Source Port: 0, Destination Port
: 0, Source Interface: Ethernet2/15, Protocol: "ICMP"(1), Hit-count = 11
```

Logging from N5K

```
pghlab-55ka# show cts role-based policy
sgt:8
dgt:6   rbacl:PERMIT_MAIL
        deny icmp log
        permit tcp dst eq 110
        permit tcp dst eq 143
        permit tcp dst eq 25
        permit tcp dst eq 465
        permit tcp dst eq 585
        permit tcp dst eq 993
        permit tcp dst eq 995
        deny all log
pghlab-55ka(config)# log level acllog 6   ← Log levels to make this work
pghlab-55ka(config)# log level cts 7
pghlab-55ka# show logging logfile duration 0:30:00
2013 Jun  6 12:27:06 pghlab-55ka last message repeated 6 times
2013 Jun  6 12:27:06 pghlab-55ka %CTS-6-CTS_RBACL_STAT_LOG: CTS ACE deny ip log, Threshold exceeded:
  Hit count in 10s period = 11
2013 Jun  6 12:27:16 pghlab-55ka %CTS-6-CTS_RBACL_STAT_LOG: CTS ACE deny ip log, Threshold exceeded:
  Hit count in 10s period = 10
2013 Jun  6 12:27:56 pghlab-55ka last message repeated 4 times
```

Threshold exceeded is a message about not overwhelming the CPU with log messages on the box.



```
May 31 16:09:17 10.1.100.1 : 2013 May 31 16:11:05 PDT: %ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 15, Source IP: 10.10.41.100, Destination IP: 10.1.100.77, Source Port: 0, Destination Po
rt: 0, Source Interface: Ethernet2/13, Protocol: "ICMP"(1), Hit-count = 3
Jun  6 05:51:51 svlngen-4900m-gw1-vl101  2013 Jun  6 12:53:47 UTC: %CTS-6-CTS_RBACL_STAT_LOG: CTS ACE deny ip log, Threshold exceeded: Hit count in 10s period = 8
Jun  6 05:52:01 svlngen-4900m-gw1-vl101  2013 Jun  6 12:53:57 UTC: %CTS-6-CTS_RBACL_STAT_LOG: CTS ACE deny ip log, Threshold exceeded: Hit count in 10s period = 10
```

NXOS Large Scale SGT

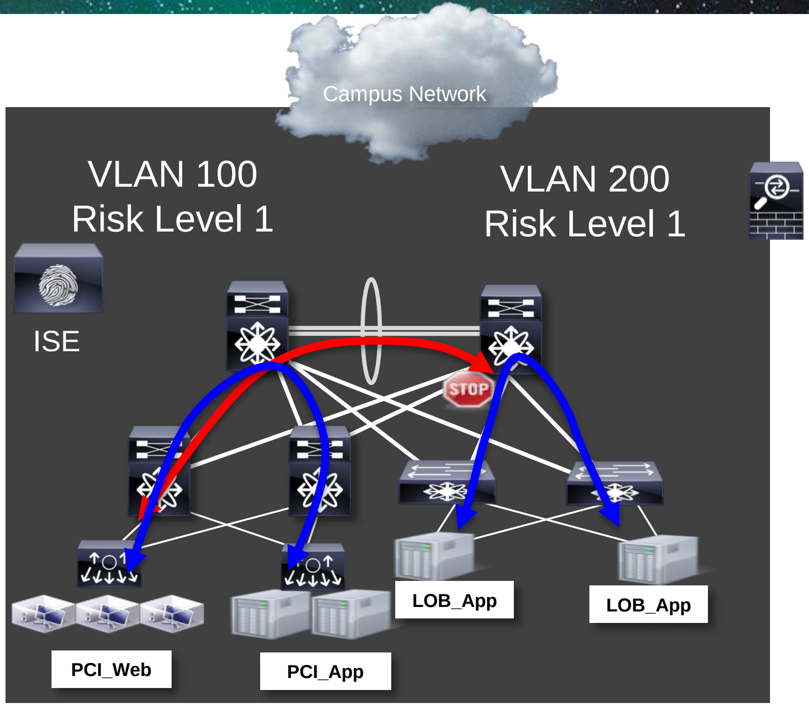
- Large numbers of SGT/DGT cells and SGACLs on N7K/N5K require new handling of SGACLs.
- Large policies can also exceed a single RADIUS packet, so the below releases introduce RADIUS SGACL fragmentation to spread the SGACL policies across multiple packets.
  - N7K – 6.2(6)
  - N5K – 6.0(2)N2
- N7K requires a batch programming command to scale above 50K IP/SGT for SXP and static classification (200K max.)

```
N7K-DST1(config-vlan)# cts role-based policy batched-programming enable
```

VLANs Designating Risk Levels/ Security Zones

- Often a VLAN is equal to a Risk Level/Security Zone
- In many cases ingress/egress ACLs are used to control flows between VLANs
- VLAN/SGT can be used on the Nexus 7000 to reduce TCAM usage substanitally
    - ACL conversion has shown 60% to 88% TCAM reduction
    - Distribution layer enforcement allows any computer layer
    - Does assume within a VLAN is permissible
- Flows to other risk levels/security zones still enforced on firewall
- NX-OS 6.2

```
N7K-DST1(config)# vlan 100
N7K-DST1(config-vlan)# cts role-based sgt 100
```



N1KV - Configuration

```
CTS-N1K(config)# feature cts
CTS-N1K(config)# port-profile type vethernet LOB2-VDI
CTS-N1K(config-port-prof)# vmware port-group
CTS-N1K(config-port-prof)# switch mode access
CTS-N1K(config-port-prof)# switch acc vlan 118
CTS-N1K(config-port-prof)# cts sgt 16
CTS-N1K(config-port-prof)# no shut
CTS-N1K(config-port-prof)# state enabled


SXP:
CTS-N1K(config)# cts device tracking
CTS-N1K(config)# cts sxp enable
CTS-N1K(config)# cts sxp connection peer 10.39.1.2 source 10.87.109.191
password none mode listener vrf management
CTS-N1K(config)# cts sxp connection peer 10.39.1.3 source 10.87.109.191
password none mode listener vrf management
```

N1KV - Verification

```
CTS-N1K(config)# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION
STATE
10.39.1.2       management      listener        speaker         connected
10.39.1.3       management      listener        speaker         connected

CTS-N1K(config)# show cts role-based sgt-map
  Interface       SGT           IP ADDRESS      VRF         Learnt
-------------- ------        ---------------- ----------   ---------
Vethernet1      14           10.39.1.92         -         Device Tracking
Vethernet2      16
Vethernet3      16           10.39.1.94         -         Device Tracking
CTS-N1K(config)#
```

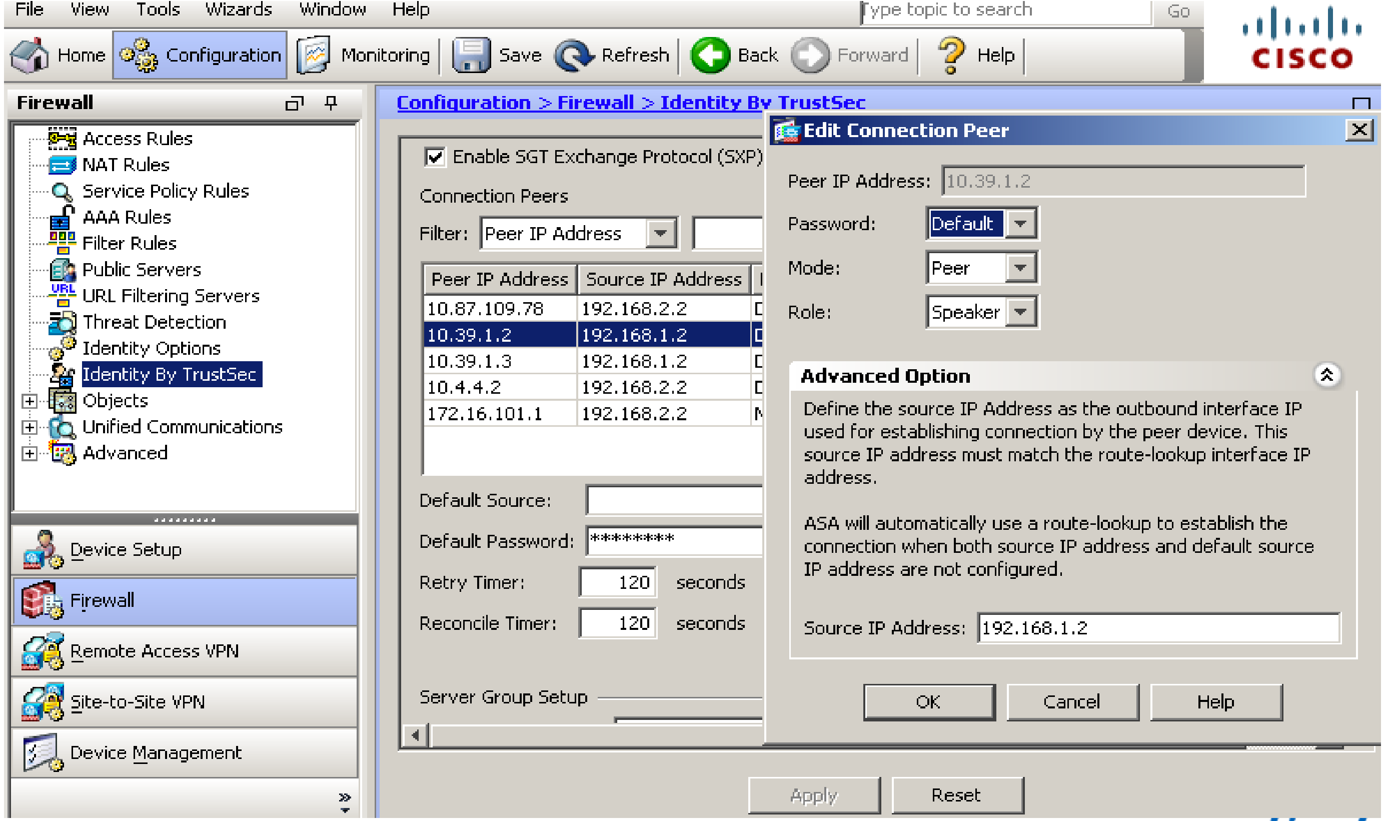
Configuration for ASA SGFW to Work

- First the DC switches must be configured to speak SXP to the SXP listening ASA to receive IP to Tag mappings

```
pghlab-n7kb-n7k-shaun(config)# cts sxp enable

pghlab-n7ka-n7k-shaun(config)# cts sxp connection peer 192.168.1.2 source
  10.39.1.2 password required trustsec123 mode listener

pghlab-n7kb-n7k-shaun(config)# cts sxp connection peer 192.168.1.2 source
  10.39.1.3 password required trustsec123 mode listener

pghlab-n7kb-n7k-shaun# sho cts sxp connection

PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE

172.16.1.20     default         speaker         listener        connected
```

Configuration for ASA SGFW to Work – Cont.

- Second Configure the ASA for SXP:



Configuration > Firewall > Identity By TrustSec

☑ Enable SGT Exchange Protocol (SXP)

Connection Peers

Filter: Peer IP Address

Peer IP Address	Source IP Address
10.87.109.78	192.168.2.2
10.39.1.2	192.168.1.2
10.39.1.3	192.168.1.2
10.4.4.2	192.168.2.2
172.16.101.1	192.168.2.2

Default Source:

Default Password: *********

Retry Timer: 120 seconds

Reconcile Timer: 120 seconds

Edit Connection Peer

Peer IP Address: 10.39.1.2

Password: Default

Mode: Peer

Role: Speaker

Advanced Option

Define the source IP Address as the outbound interface IP used for establishing connection by the peer device. This source IP address must match the route-lookup interface IP address.

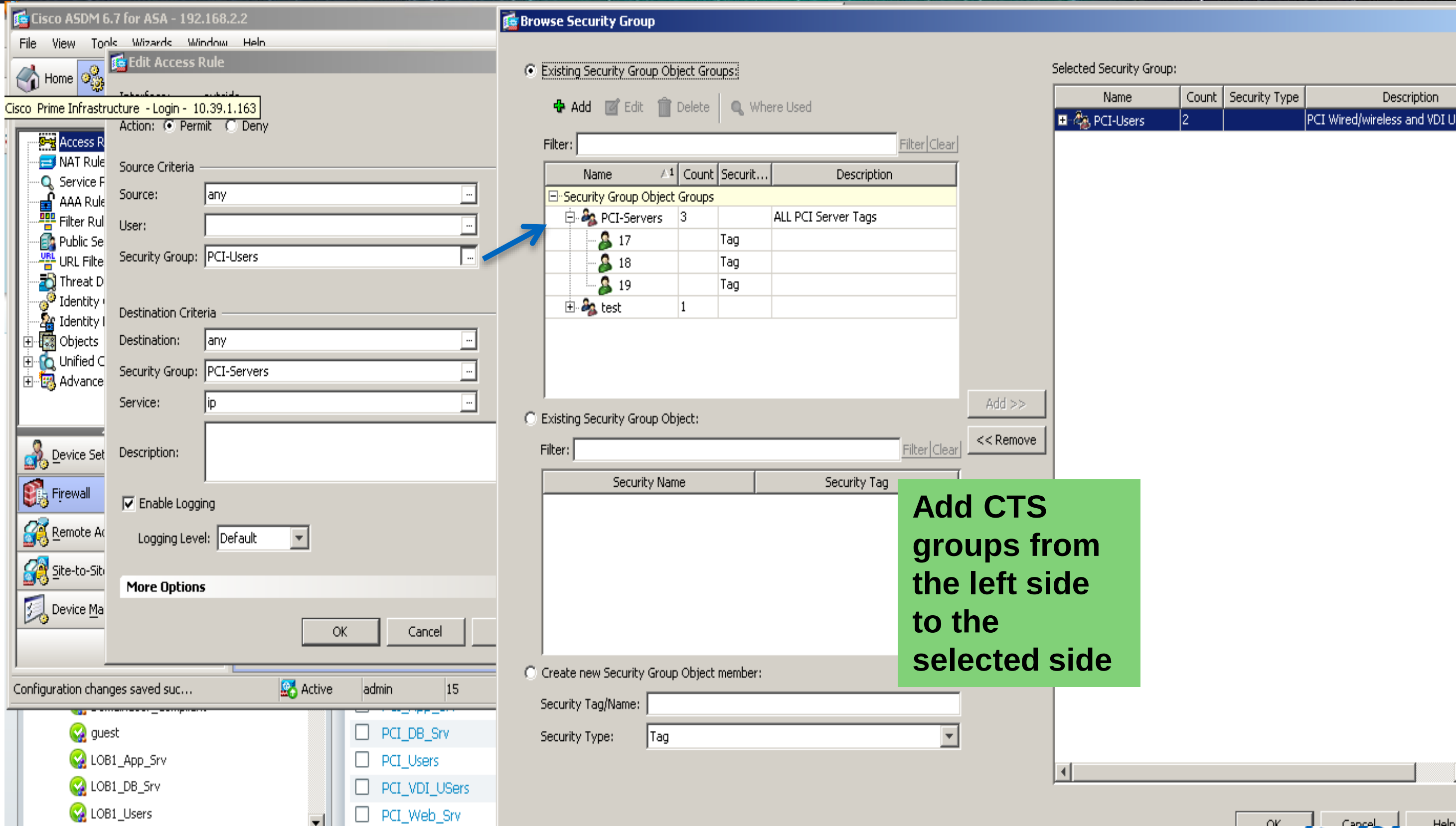
ASA will automatically use a route-lookup to establish the connection when both source IP address and default source IP address are not configured.

Source IP Address: 192.168.1.2

OK Cancel Help

Configuration for ASA SGFW to Work – Cont. (2)

- Finally configure your SGACL ACE entries in the firewall!



Cisco ASDM 6.7 for ASA - 192.168.2.2

Cisco Prime Infrastructure - Login - 10.39.1.163

Edit Access Rule

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group: PCI-Users

Destination Criteria

Destination: any

Security Group: PCI-Servers

Service: ip

Description:

☑ Enable Logging

Logging Level: Default

More Options

OK Cancel

Configuration changes saved suc... Active admin 15

Browse Security Group

● Existing Security Group Object Groups:

Add Edit Delete Where Used

Filter: Filter Clear

Name	Count	Securit...	Description
Security Group Object Groups			
PCI-Servers	3		ALL PCI Server Tags
17		Tag	
18		Tag	
19		Tag	
test	1		

○ Existing Security Group Object:

Filter: Filter Clear

Security Name	Security Tag

○ Create new Security Group Object member:

Security Tag/Name:

Security Type: Tag

Add >>

<< Remove

Selected Security Group:

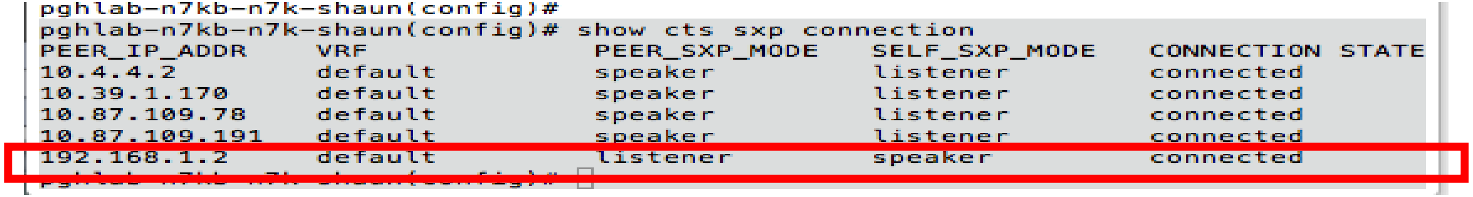
Name	Count	Security Type	Description
PCI-Users	2		PCI Wired/wireless and VDI U

OK Cancel Help

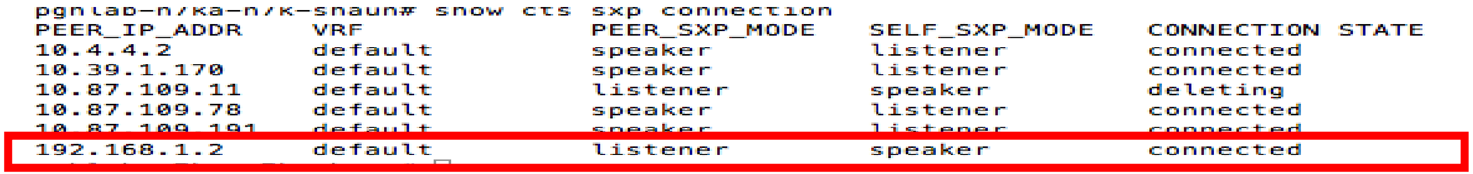
Add CTS groups from the left side to the selected side

ASA SGFW Verification:

- Check SXP peering on the DC switch side:



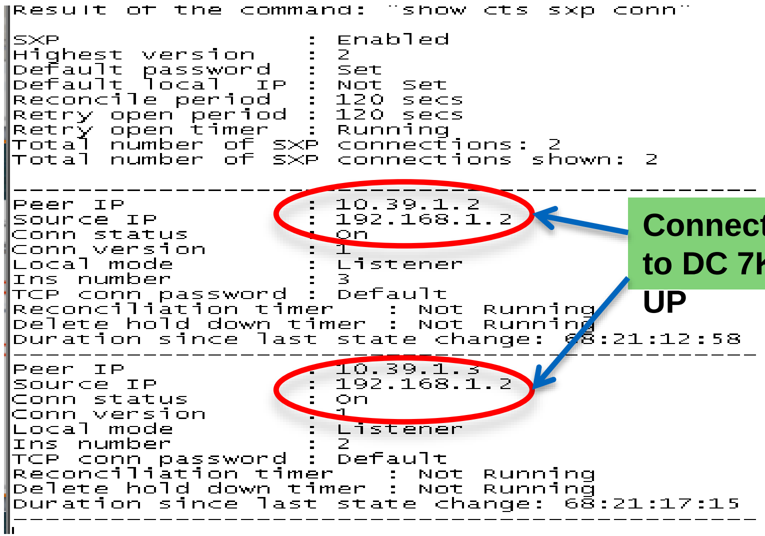
```
pghlab-n7kb-n7k-shaun(config)#
pghlab-n7kb-n7k-shaun(config)# show cts sxp connection
PEER_IP_ADDR     VRF              PEER_SXP_MODE    SELF_SXP_MODE    CONNECTION STATE
10.4.4.2         default          speaker          listener         connected
10.39.1.170      default          speaker          listener         connected
10.87.109.78     default          speaker          listener         connected
10.87.109.191    default          speaker          listener         connected
192.168.1.2      default          listener         speaker          connected
pghlab-n7kb-n7k-shaun(config)#
```



```
pghlab-n7ka-n7k-shaun# show cts sxp connection
PEER_IP_ADDR     VRF              PEER_SXP_MODE    SELF_SXP_MODE    CONNECTION STATE
10.4.4.2         default          speaker          listener         connected
10.39.1.170      default          speaker          listener         connected
10.87.109.11     default          listener         speaker          deleting
10.87.109.78     default          speaker          listener         connected
10.87.109.191    default          speaker          listener         connected
192.168.1.2      default          listener         speaker          connected
```

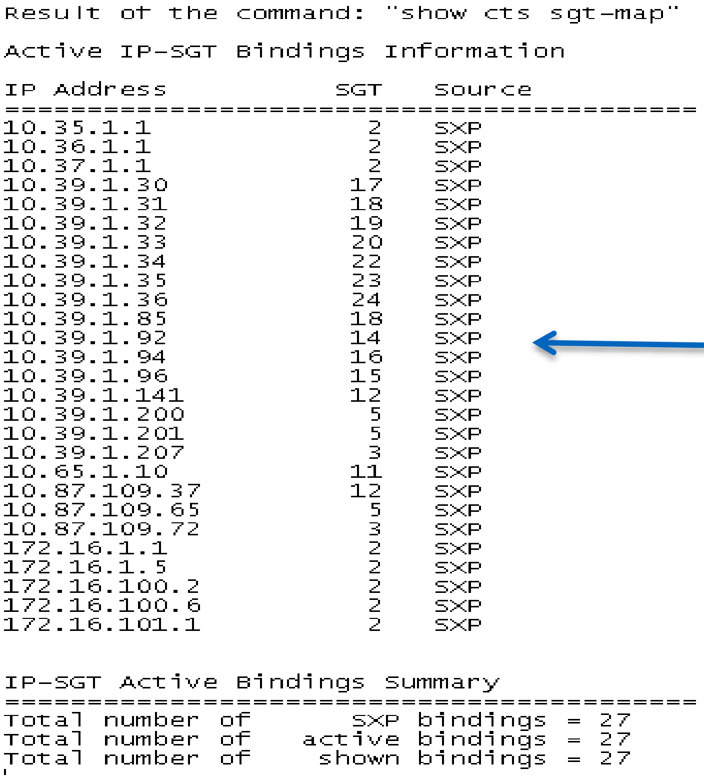
ASA SGFW Verification: Cont

- Check SXP peering on the ASA side and verify IP-SGT Bindings:



```
Result of the command: "show cts sxp conn"

SXP                    : Enabled
Highest version        : 2
Default password       : Set
Default local  IP      : Not Set
Reconcile period       : 120 secs
Retry open period      : 120 secs
Retry open timer       : Running
Total number of SXP connections: 2
Total number of SXP connections shown: 2

----------------------------------------------------------------------
Peer IP                : 10.39.1.2
Source IP              : 192.168.1.2
Conn status            : On
Conn version           : 1
Local mode             : Listener
Ins number             : 3
TCP conn password      : Default
Reconciliation timer       : Not Running
Delete hold down timer     : Not Running
Duration since last state change: 68:21:12:58
----------------------------------------------------------------------
Peer IP                : 10.39.1.3
Source IP              : 192.168.1.2
Conn status            : On
Conn version           : 1
Local mode             : Listener
Ins number             : 2
TCP conn password      : Default
Reconciliation timer       : Not Running
Delete hold down timer     : Not Running
Duration since last state change: 68:21:17:15
----------------------------------------------------------------------
```

Connection to DC 7Ks is UP



```
Result of the command: "show cts sgt-map"

Active IP-SGT Bindings Information

IP Address                 SGT    Source
============================================
10.35.1.1                    2    SXP
10.36.1.1                    2    SXP
10.37.1.1                    2    SXP
10.39.1.30                  17    SXP
10.39.1.31                  18    SXP
10.39.1.32                  19    SXP
10.39.1.33                  20    SXP
10.39.1.34                  22    SXP
10.39.1.35                  23    SXP
10.39.1.36                  24    SXP
10.39.1.85                  18    SXP
10.39.1.92                  14    SXP
10.39.1.94                  16    SXP
10.39.1.96                  15    SXP
10.39.1.141                 12    SXP
10.39.1.200                  5    SXP
10.39.1.201                  5    SXP
10.39.1.207                  3    SXP
10.65.1.10                  11    SXP
10.87.109.37                12    SXP
10.87.109.65                 5    SXP
10.87.109.72                 3    SXP
172.16.1.1                   2    SXP
172.16.1.5                   2    SXP
172.16.100.2                 2    SXP
172.16.100.6                 2    SXP
172.16.101.1                 2    SXP


IP-SGT Active Bindings Summary
============================================
Total number of     SXP bindings = 27
Total number of  active bindings = 27
Total number of   shown bindings = 27
```

IP-SGTs being received from DC Switches

Data Centre Server SGT Orchestration

Data Centre Server SGT Design Considerations

- Server SGTs can be assigned either statically or dynamically (less preferred)
  - Statically – Manual IP-SGT Binding must be entered onto the Data Centre Switches
  - Dynamically – Servers would have to run 802.1X to authenticate to the network and get assigned an SGT via ISE. Server admins do not like to run dot1x on their server platforms. Not all platforms support dot1x either

When Servers are decommissioned, Tags should be removed with the server during the decom process.

“Typical” Process Before SGT Orchestration

- Server Admin/LOB requests a new server.
- The network team, the server team and the security team meet and plan (sometimes multiple times) to plan VLAN, IP addressing, DNS, Security Profiles, etc.
  - The server is turned up by the server team.
  - Network Team must now go to the network devices add devices port to VLAN, etc.
  - The firewall team adds the destination IP address to appropriate firewall rules or firewall groups.
- All adds and deletes are a manual process!

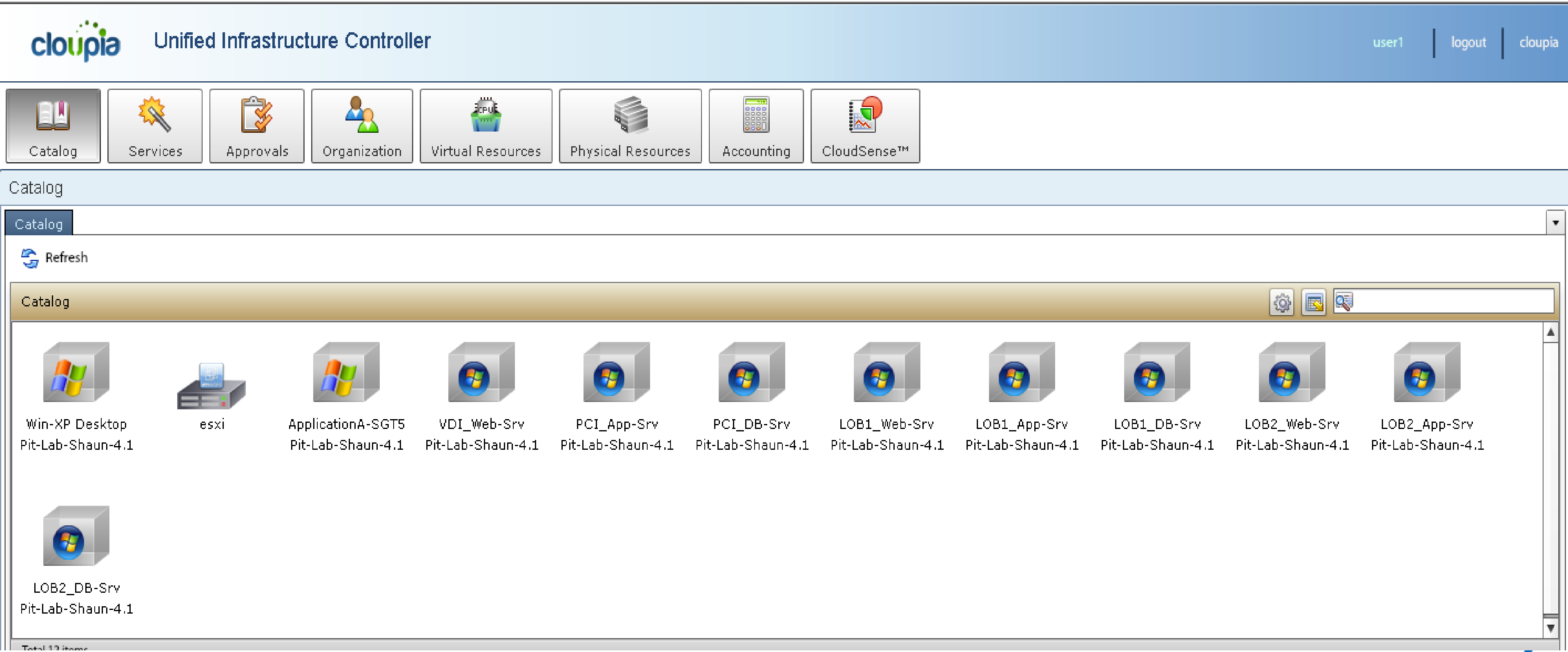
Data Centre Server SGT Orchestration

- Through the use of Data Centre orchestration tools we can fully automate the provisioning of server IP-SGT/port profile bindings for VMs and bare-metal machines based on the selected service catalog in the automation provisioning portal
- We can also automate the removal of IP-SGT bindings when the server is decommissioned from the network
- In our use case example we will show how to use UCS Director (UCSD) orchestration suite to automate the server IP-SGT provisioning process

Benefits of SGT Orchestration

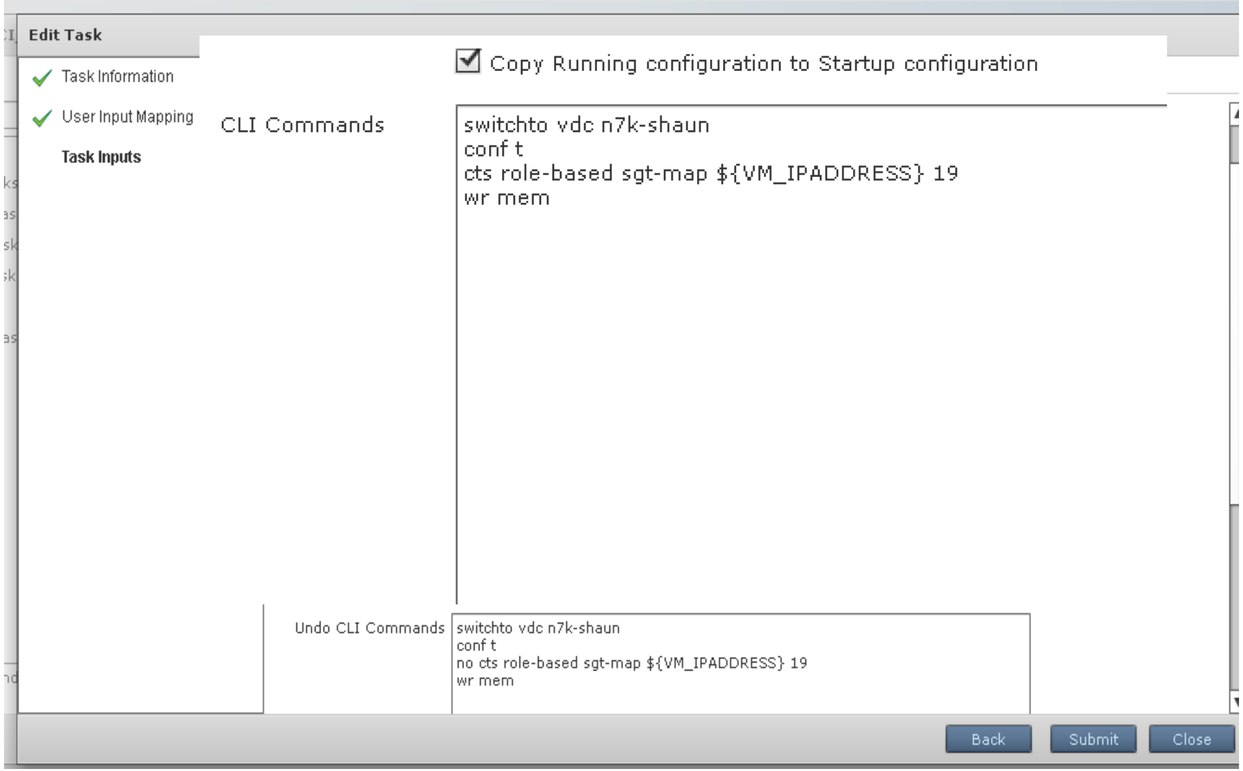
- Lower OPEX and time to provision: When deploying a server we reduce the amount of people that need to touch the
  - Network
  - Server
  - Security policies
- When a server is spun up from the provisioning portal, the IP-SGT binding is automatically provisioned to the network,
- Once a server has its SGT all SGACLs and SGFWs will begin enforcing without having to manually edit firewall rules everytime a server comes on-line or goes offline.

UCS Director Portal Screen


cloupia
Unified Infrastructure Controller
user1
logout
cloupia
Catalog
Services
Approvals
Organization
Virtual Resources
Physical Resources
Accounting
CloudSense™
Catalog
Catalog
Refresh
Catalog
Win-XP Desktop Pit-Lab-Shaun-4.1
esxi
ApplicationA-SGT5 Pit-Lab-Shaun-4.1
VDI_Web-Srv Pit-Lab-Shaun-4.1
PCI_App-Srv Pit-Lab-Shaun-4.1
PCI_DB-Srv Pit-Lab-Shaun-4.1
LOB1_Web-Srv Pit-Lab-Shaun-4.1
LOB1_App-Srv Pit-Lab-Shaun-4.1
LOB1_DB-Srv Pit-Lab-Shaun-4.1
LOB2_Web-Srv Pit-Lab-Shaun-4.1
LOB2_App-Srv Pit-Lab-Shaun-4.1
LOB2_DB-Srv Pit-Lab-Shaun-4.1
Total 12 items

UCSD Custom Task for Server SGT Deployment

- This assumes some knowledge of UCSD and workflow editing.
- Create a workflow that
  - IP address of the VM/Bare-metal machine
  - Logs into the DC switches
  - Adds the IP-SGT mapping based on the Service Catalog (IE: LOB1, LOB2, PCI)



☑ Copy Running configuration to Startup configuration

CLI Commands

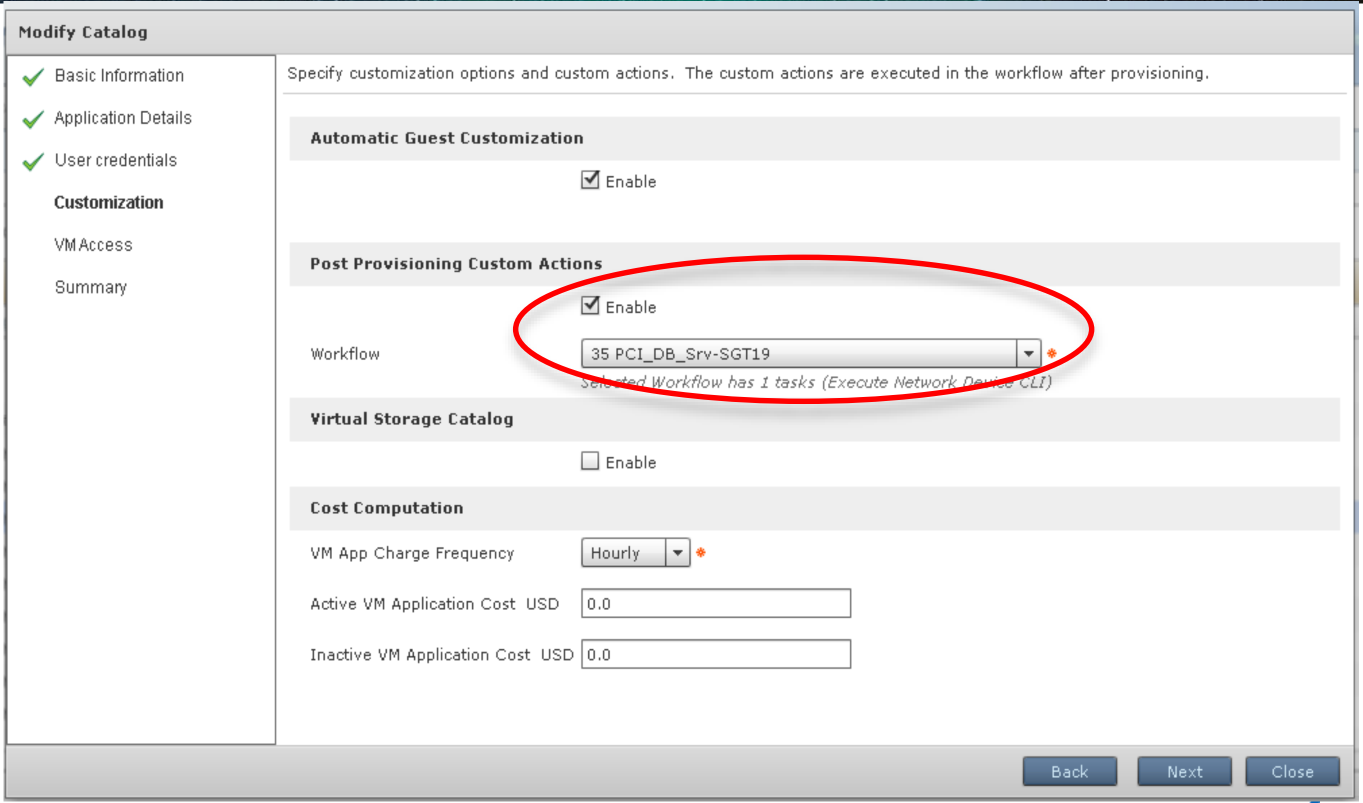
```
switchto vdc n7k-shaun
conf t
cts role-based sgt-map ${VM_IPADDRESS} 19
wr mem
```

Undo CLI Commands

```
switchto vdc n7k-shaun
conf t
no cts role-based sgt-map ${VM_IPADDRESS} 19
wr mem
```

How to Configure UCSD for Server SGT Deployment (continued)

- Add this workflow to each service catalog we want and SGT deployed when ordering the vm/bare metal machine



Modify Catalog

- ✓ Basic Information
- ✓ Application Details
- ✓ User credentials
- **Customization**
- VM Access
- Summary

Specify customization options and custom actions. The custom actions are executed in the workflow after provisioning.

Automatic Guest Customization

☑ Enable

Post Provisioning Custom Actions

☑ Enable

Workflow: 35 PCI_DB_Srv-SGT19 *

Selected Workflow has 1 tasks (Execute Network Device CLI)

Virtual Storage Catalog

□ Enable

Cost Computation

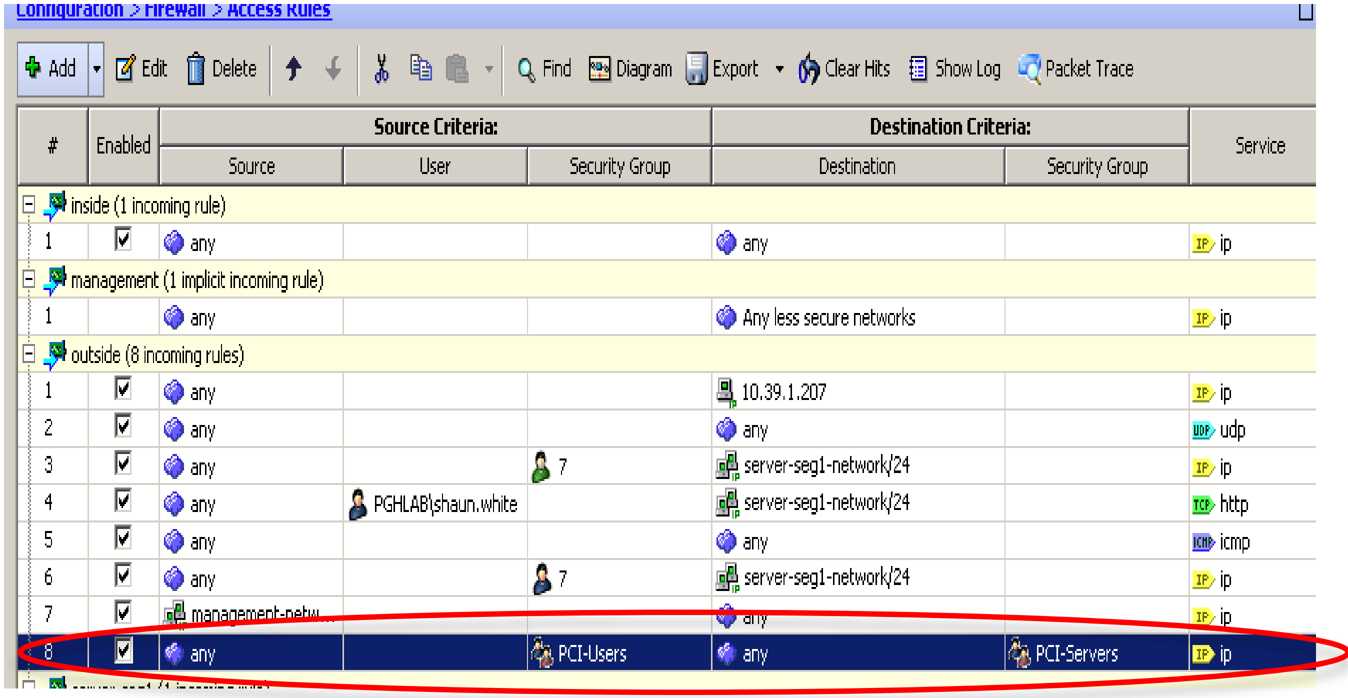
VM App Charge Frequency: Hourly *

Active VM Application Cost USD: 0.0

Inactive VM Application Cost USD: 0.0

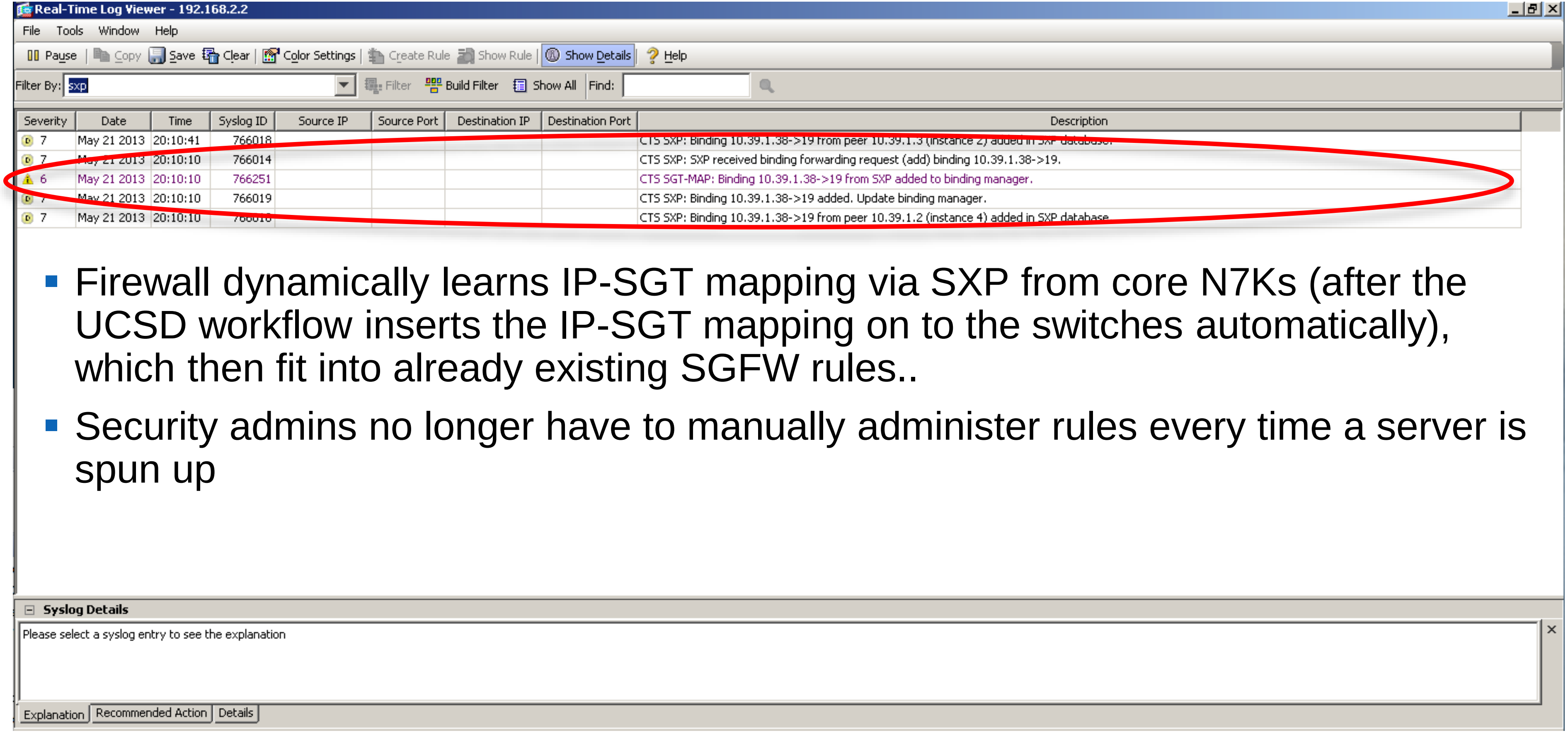
SGT Automates the Firewall Rule Process!!

- A PCI DB servers example
- When the server is provisioned the workflow runs
- Assigns the PCI DB SGT to the DC switches.
- The DC switches communicate via SXP to the firewall,
- Immediately the firewall can now enforce with no rule changes



#	Enabled	Source Criteria:			Destination Criteria:		Service
		Source	User	Security Group	Destination	Security Group	
inside (1 incoming rule)							
1	☑	any			any		ip
management (1 implicit incoming rule)							
1		any			Any less secure networks		ip
outside (8 incoming rules)							
1	☑	any			10.39.1.207		ip
2	☑	any			any		udp
3	☑	any		7	server-seg1-network/24		ip
4	☑	any	PGHLAB\shaun.white		server-seg1-network/24		http
5	☑	any			any		icmp
6	☑	any		7	server-seg1-network/24		ip
7	☑	management-netw...			any		ip
8	☑	any		PCI-Users	any	PCI-Servers	ip

ASA SGFW in Action



Filter By: sxp

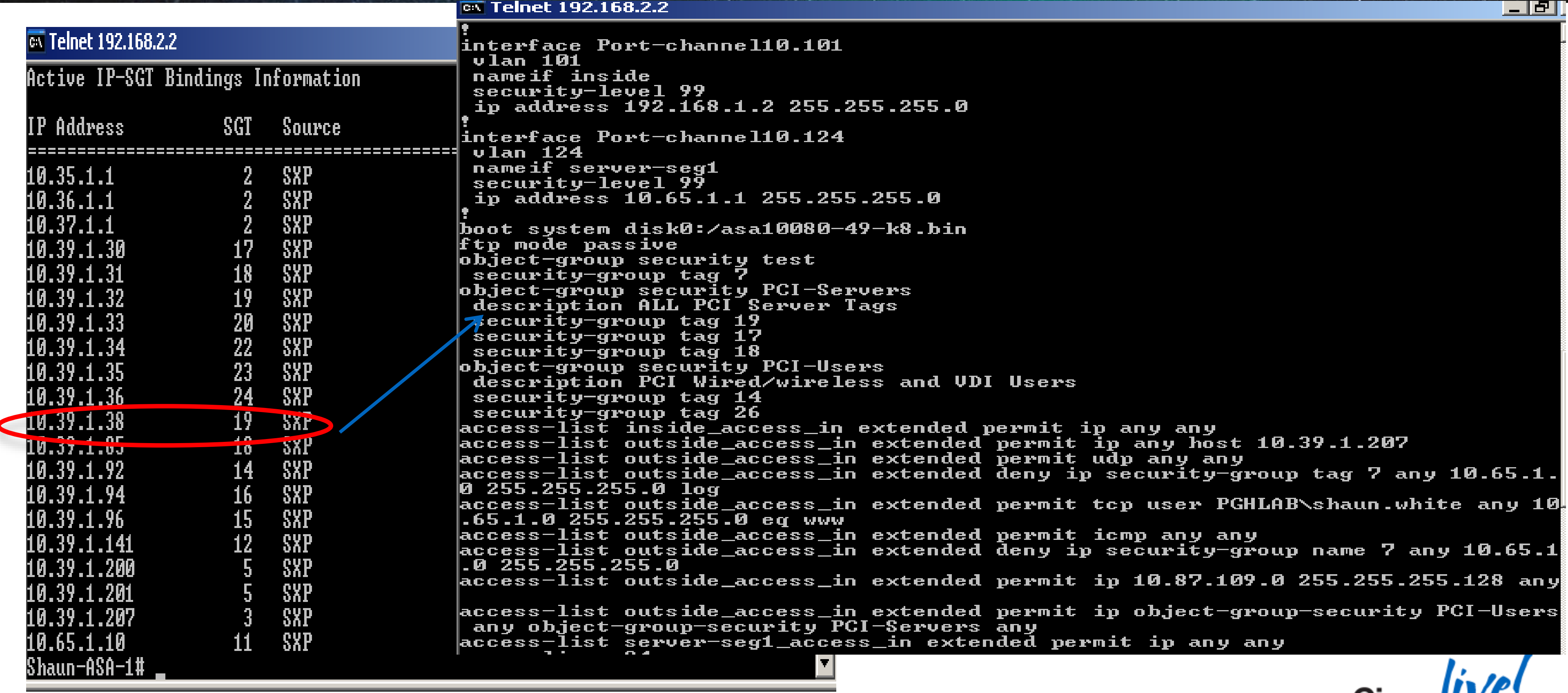
Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
7	May 21 2013	20:10:41	766018					CTS SXP: Binding 10.39.1.38->19 from peer 10.39.1.3 (instance 2) added in SXP database.
7	May 21 2013	20:10:10	766014					CTS SXP: SXP received binding forwarding request (add) binding 10.39.1.38->19.
6	May 21 2013	20:10:10	766251					CTS SGT-MAP: Binding 10.39.1.38->19 from SXP added to binding manager.
7	May 21 2013	20:10:10	766019					CTS SXP: Binding 10.39.1.38->19 added. Update binding manager.
7	May 21 2013	20:10:10	766016					CTS SXP: Binding 10.39.1.38->19 from peer 10.39.1.2 (instance 4) added in SXP database.

- Firewall dynamically learns IP-SGT mapping via SXP from core N7Ks (after the UCSD workflow inserts the IP-SGT mapping on to the switches automatically), which then fit into already existing SGFW rules..
- Security admins no longer have to manually administer rules every time a server is spun up

Syslog Details

Please select a syslog entry to see the explanation

ASA SGFW in Action (cont)



```
Active IP-SGT Bindings Information

IP Address            SGT    Source
==========================================
10.35.1.1               2    SXP
10.36.1.1               2    SXP
10.37.1.1               2    SXP
10.39.1.30             17    SXP
10.39.1.31             18    SXP
10.39.1.32             19    SXP
10.39.1.33             20    SXP
10.39.1.34             22    SXP
10.39.1.35             23    SXP
10.39.1.36             24    SXP
10.39.1.38             19    SXP
10.39.1.85             18    SXP
10.39.1.92             14    SXP
10.39.1.94             16    SXP
10.39.1.96             15    SXP
10.39.1.141            12    SXP
10.39.1.200             5    SXP
10.39.1.201             5    SXP
10.39.1.207             3    SXP
10.65.1.10             11    SXP
Shaun-ASA-1#
```

```
!
interface Port-channel10.101
 vlan 101
 nameif inside
 security-level 99
 ip address 192.168.1.2 255.255.255.0
!
interface Port-channel10.124
 vlan 124
 nameif server-seg1
 security-level 99
 ip address 10.65.1.1 255.255.255.0
!
boot system disk0:/asa10080-49-k8.bin
ftp mode passive
object-group security test
 security-group tag 7
object-group security PCI-Servers
 description ALL PCI Server Tags
 security-group tag 19
 security-group tag 17
 security-group tag 18
object-group security PCI-Users
 description PCI Wired/wireless and VDI Users
 security-group tag 14
 security-group tag 26
access-list inside_access_in extended permit ip any any
access-list outside_access_in extended permit ip any host 10.39.1.207
access-list outside_access_in extended permit udp any any
access-list outside_access_in extended deny ip security-group tag 7 any 10.65.1.
0 255.255.255.0 log
access-list outside_access_in extended permit tcp user PGHLAB\shaun.white any 10
.65.1.0 255.255.255.0 eq www
access-list outside_access_in extended permit icmp any any
access-list outside_access_in extended deny ip security-group name 7 any 10.65.1
.0 255.255.255.0
access-list outside_access_in extended permit ip 10.87.109.0 255.255.255.128 any

access-list outside_access_in extended permit ip object-group-security PCI-Users
 any object-group-security PCI-Servers any
access-list server-seg1_access_in extended permit ip any any
```

Summary

- SGTs builds upon Identity and Unified Access services
- SGTs provides a scalable Identity and Unified Access role based access control model
- SGTs has migration strategies allow customer to deploy with existing hardware
- Unified Access and SGTs are deployable **today**

Related Sessions on Cisco Live Online

- BRKSEC-2692 – Identity Based Networking: IEEE 802.1X and Beyond
  - Hariprasad Holla, Cisco Technical Marketing Engineer

Adv. 802.1X Topics

- BRKSEC-3698 – Advanced ISE and Secure Access Deployment
  - Aaron Woland, Cisco Technical Marketing Engineer

Adv. ISE Topics

- BRKSEC-2203 – Deploying TrustSec Security Group Tagging
  - Kevin Regan, Cisco Product Manager
- BRKSEC-3690 – Advanced Security Group Tags: The Detailed Walk Through
  - Darrin Miller, Cisco Distinguished Engineer

Intermediate and Adv TrustSec (SGA)

- BRKSEC-2045 – Mobile Devices and BYOD Security - Deployment and Best Practices
  - Sylvain Levesque, Consulting Systems Engineer
- BRKEWN-2020 – Wireless LAN Security, Policy and BYOD Best Practices
  - Federico Ziliotto, Senior Systems Engineer
- BRKSEC-3035 – Successful Designing and Deploying Cisco's ISE 1.2/MDM Integration
  - Christoph Altherr, Senior Systems Engineer
- PSOSEC-2001 – BYOD: Management and Control for the Use and Provisioning of Mobile Devices – Russell Rice, Director of Product Management

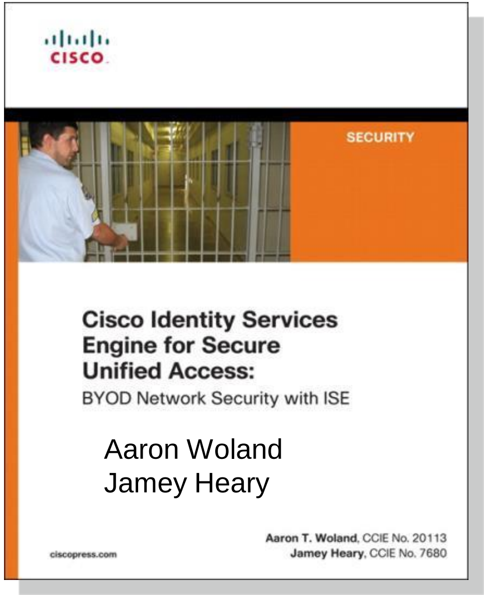
BYOD

MDM

Mobile Device Security

Recommended Reading

- For reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2014



CISCO

SECURITY

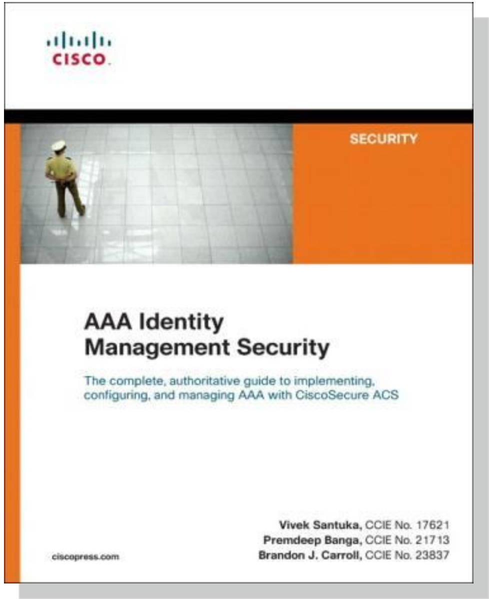
Cisco Identity Services Engine for Secure Unified Access:

BYOD Network Security with ISE

Aaron Woland
Jamey Heary

ciscopress.com

Aaron T. Woland, CCIE No. 20113
Jamey Heary, CCIE No. 7680



CISCO

SECURITY

AAA Identity Management Security

The complete, authoritative guide to implementing, configuring, and managing AAA with CiscoSecure ACS

ciscopress.com

Vivek Santuka, CCIE No. 17621
Premdeep Banga, CCIE No. 21713
Brandon J. Carroll, CCIE No. 23837

Links

- Secure Access, TrustSec, and ISE on Cisco.com
  - http://www.cisco.com/go/trustsec
  - http://www.cisco.com/go/ise
  - http://www.cisco.com/go/isepartner

- TrustSec and ISE Deployment Guides:
  - http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

- YouTube: Fundamentals of TrustSec:
  - http://www.youtube.com/ciscocin#p/c/0/MJJ93N-3Iew

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

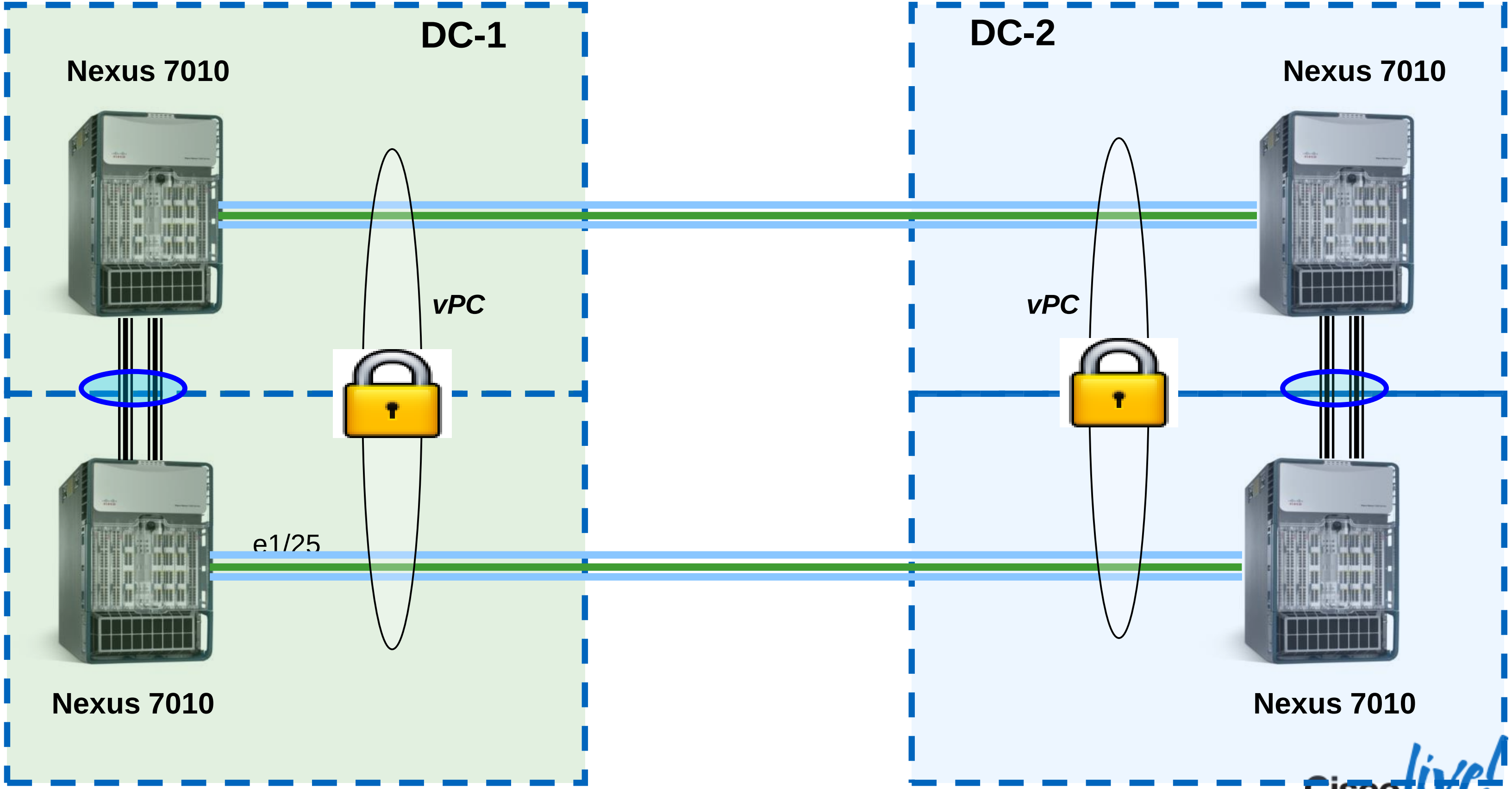
CISCO TM

Encrypted Inter-DC Link with 802.1AE

- Can SGT encrypt the link between multiple Data Centre for secure backup / DR purpose?
- 802.1AE technology can be used to encrypt point-to-point link with following conditions
  - 40 Gbps, 10Gbps or 1Gbps link between Nexus 7000s if both Nexus 7Ks are connected with dark fibre or passive repeater between DCs so that L2 frame is not manipulated
  - Or use EoMPLS Pseudowire to encapsulate 802.1AE frame between two Data Centres
- Catalyst 6500s with 69xx line cards as well

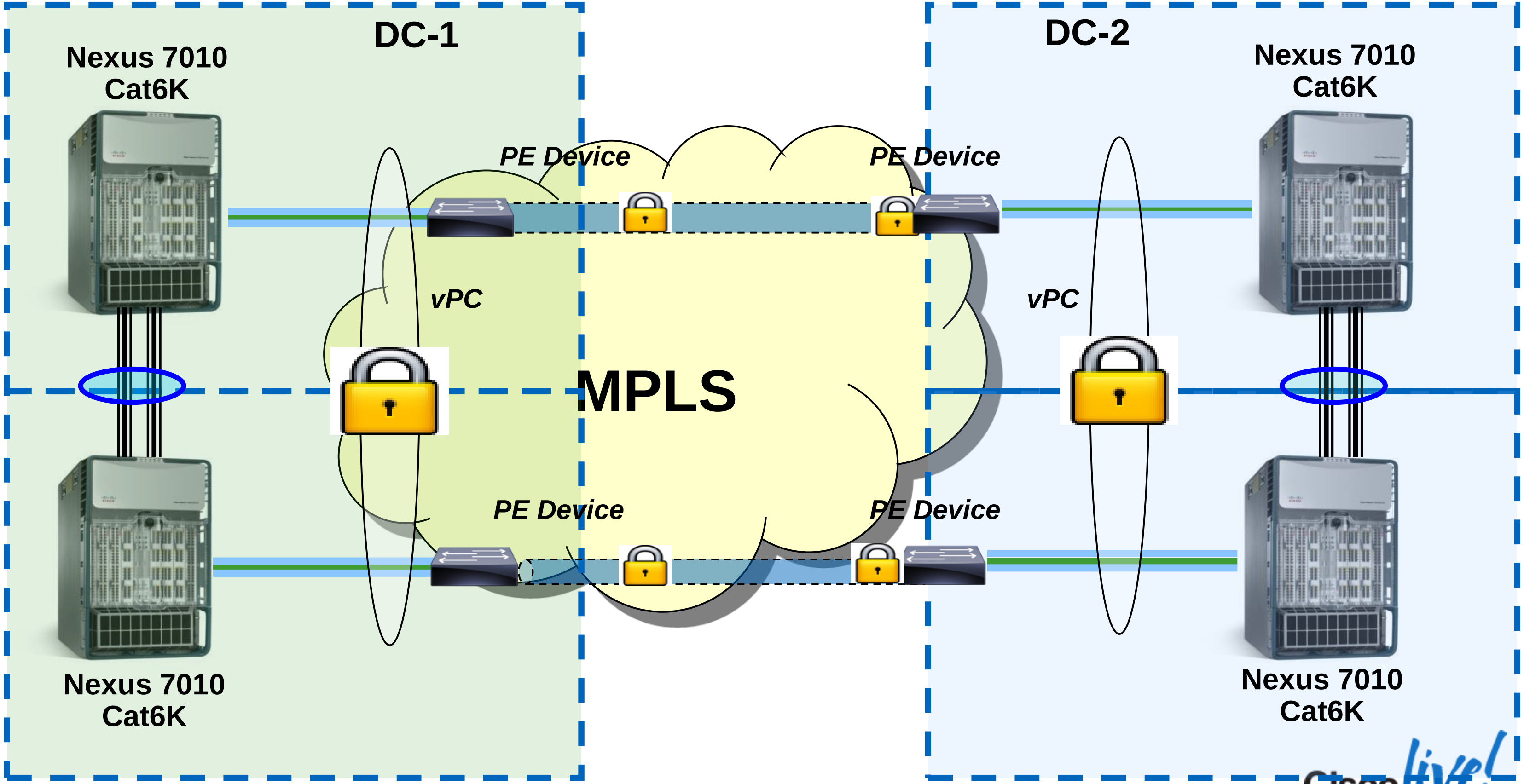
MACSEC for Secure Data Centre Interconnect

Dual Access with Dark Fibre Connectivity



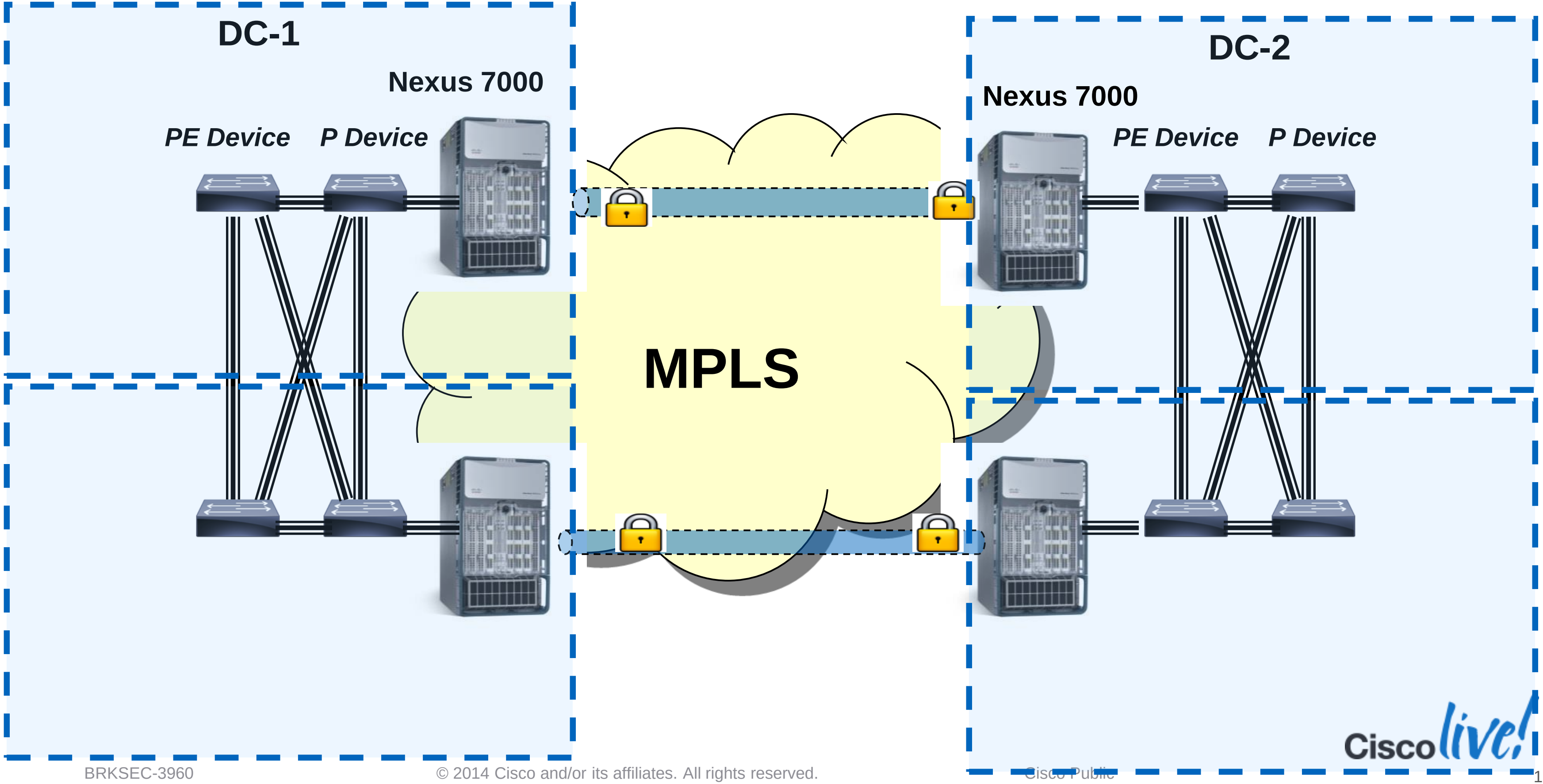
SGT for Secure Data Centre Interconnect

Dual Access with MPLS Connectivity



SGT for Secure Data Centre Interconnect

7Ks as bulk encrypters for Self managed MPLS DCI Cores – Bump in the wire



Configuring Point to Point DCI - PSK

- Configure DC-A
  - pghlab-n7ka-n7k-shaun(config)# int e1/22
  - pghlab-n7ka-n7k-shaun(config-if)# cts manual
  - pghlab-n7ka-n7k-shaun(config-if-cts-manual)# sap pmk 25241236789876543210 modelist gcm-encrypt
  - pghlab-n7ka-n7k-shaun(config-if-cts-manual)# policy static sgt 0x2 trusted

  - pghlab-n7kb-n7k-shaun(config)# int e1/22
  - pghlab-n7kb-n7k-shaun(config-if)# cts manual
  - pghlab-n7kb-n7k-shaun(config-if-cts-manual)# sap pmk 25241236789876543210 modelist gcm-encrypt
  - pghlab-n7kb-n7k-shaun(config-if-cts-manual)# policy static sgt 0x2 trusted

- Configure DC-B
  - pghlab-n7kc-n7k-shaun(config)# int e1/22
  - pghlab-n7kc-n7k-shaun(config-if)# cts manual
  - pghlab-n7kc-n7k-shaun(config-if-cts-manual)# sap pmk 25241236789876543210 modelist gcm-encrypt
  - pghlab-n7kc-n7k-shaun(config-if-cts-manual)# policy static sgt 0x2 trusted

  - pghlab-n7kd-n7k-shaun(config)# int e1/22
  - pghlab-n7kd-n7k-shaun(config-if)# cts manual
  - pghlab-n7kd-n7k-shaun(config-if-cts-manual)# sap pmk 25241236789876543210 modelist gcm-encrypt
  - pghlab-n7kd-n7k-shaun(config-if-cts-manual)# policy static sgt 0x2 trusted

Cisco TrustSec Nexus 7000

I/O Module Support

- Base Cisco TrustSec is supported on All Nexus 7000 Modules

I/O Module	Photo	SGACL Enforcement and SGT Propagation	802.1AE Support
N7K-M132XP-12	**M1 Series**	✓	✓
N7K-M148GT-11		✓	✓
N7K-M148GS-11 **N7K-M148GS-11L**		✓	✓
N7K-M108X2-12L		✓	✓
N7K-F132XP-15	**F1/F2 Series**	✓	X
N7K-F248XP-25		✓	X

- F2E has some macsec capable ports