TOMORROW
starts here.

CISCO

Cisco live!

Advanced Security Group Tags: The Detailed Walk Through

BRKSEC-3690

Darrin Miller

Distinguished TME

#clmel

Cisco live!

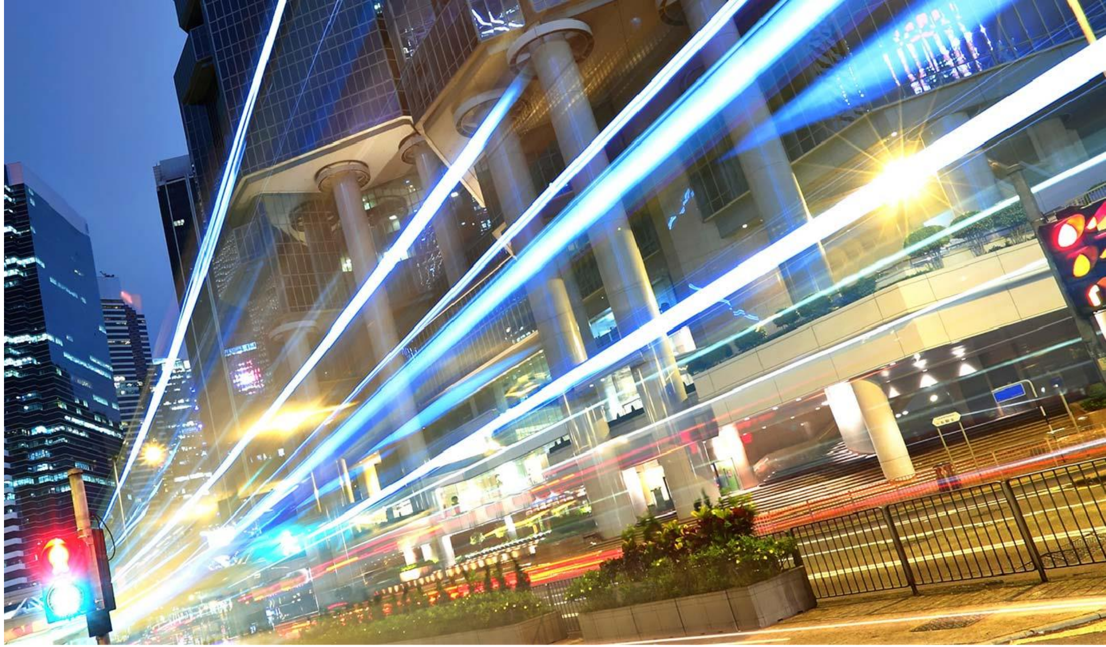
Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones
- After the event don’t forget to visit Cisco Live Virtual: www.ciscolivevirtual.com

© 2015 Cisco and/or its affiliates. All rights reserved.

Agenda

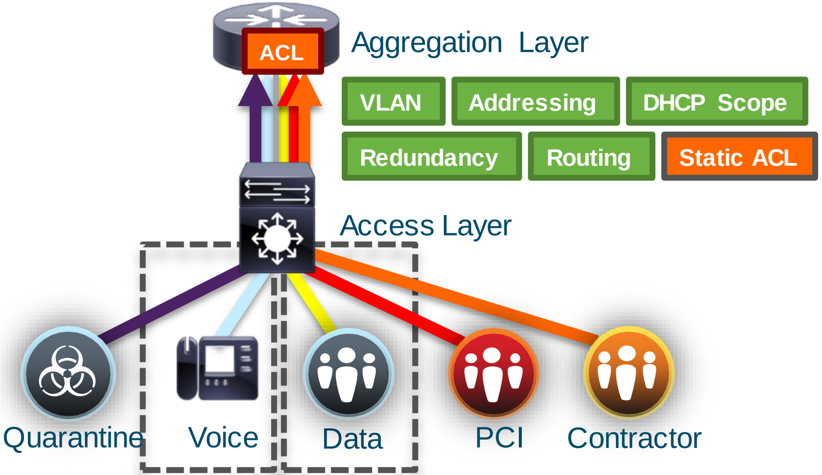
- Security Group Tag (SGT) Review
  - High Level Use Case Review
  - Technology Review
- Use Case Reviews with Design Consideration
  - WLAN Access Control
  - Partner/Vendor/Contractor Access Control
  - University VRF Enhancement
  - Health Care Access Control
  - Multi-Division Access Control
  - Retail Access Control
  - Data Centre Access Control/Segmentation
- Summary



Security Group Tag (SGT) Technology Review

Traditional Segmentation

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



ACL

Aggregation Layer

VLAN

Addressing

DHCP Scope

Redundancy

Routing

Static ACL

Access Layer

Quarantine

Voice

Data

PCI

Contractor

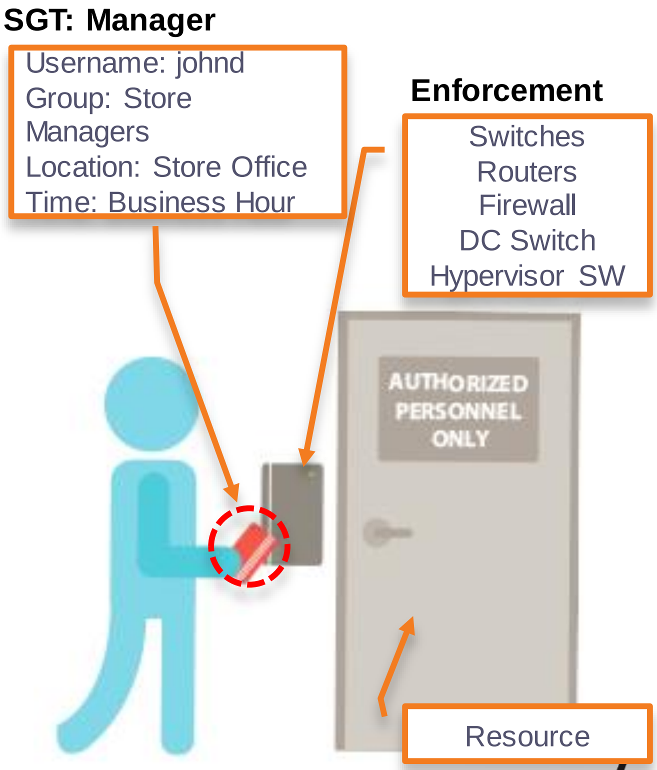
Simple Segmentation with 2 VLANs

More Policies using more VLANs

Network Segmentation with TrustSec

TrustSec Segmentation provides

- **Segmentation** based on **RBAC**, independent from address based topology
- Role based on AD, LDAP attributes, device type, location, time, access methods, etc…
- Use Tagging technology to represent logical group, traffic sent along with tag
- Tag based policy enforcement on switch, router, and firewall
- Centrally define segmentation policy, which can be invoked anywhere on the network



SGT: Manager

Username: johnd
Group: Store Managers
Location: Store Office
Time: Business Hour

Enforcement

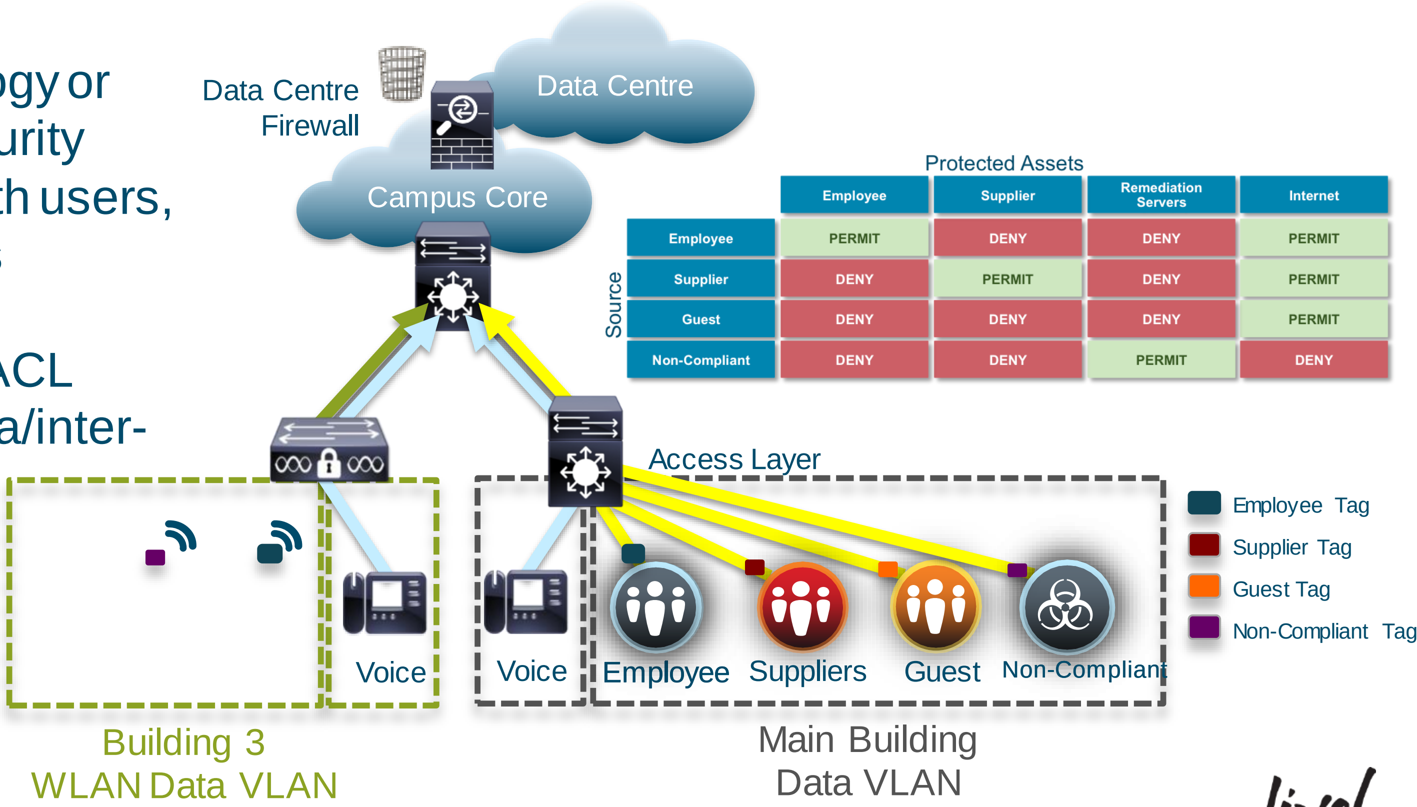
Switches
Routers
Firewall
DC Switch
Hypervisor SW

Resource

User to Data Centre Access Control with TrustSec

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

TrustSec simplifies ACL management for intra/inter-VLAN traffic



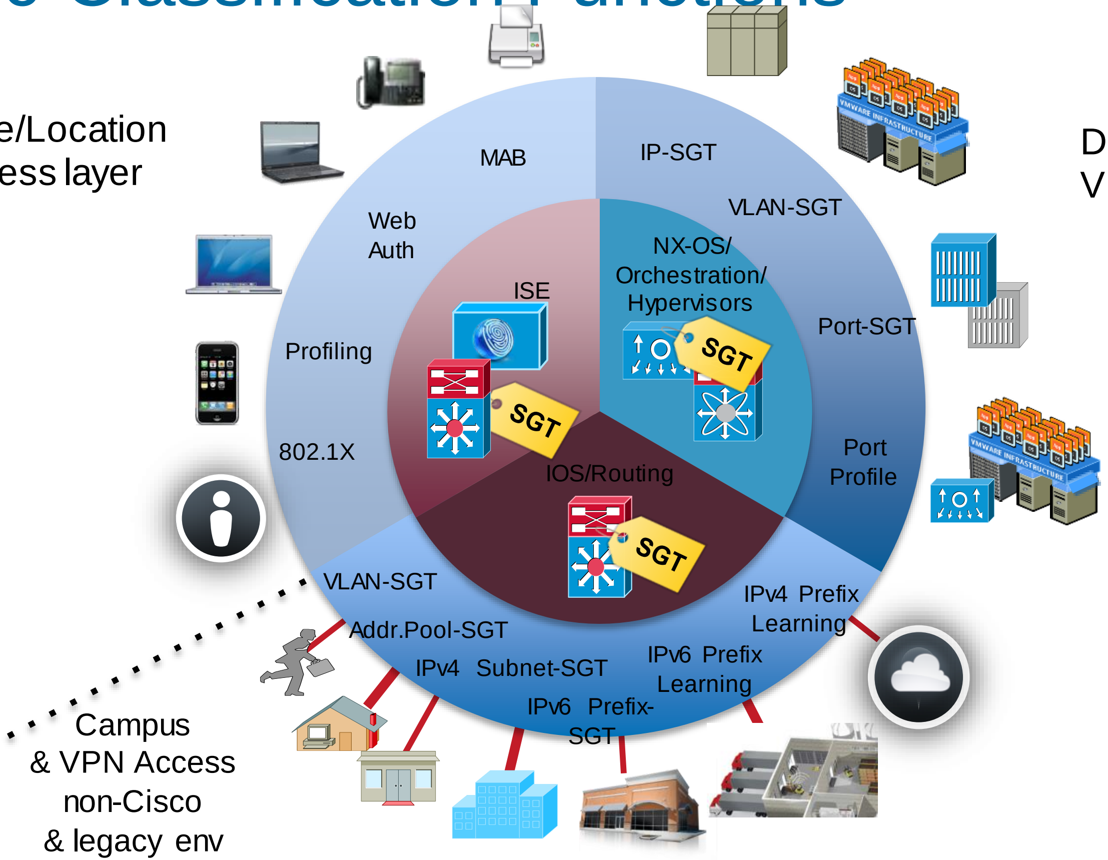
Protected Assets

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

- ■ Employee Tag
- ■ Supplier Tag
- ■ Guest Tag
- ■ Non-Compliant Tag

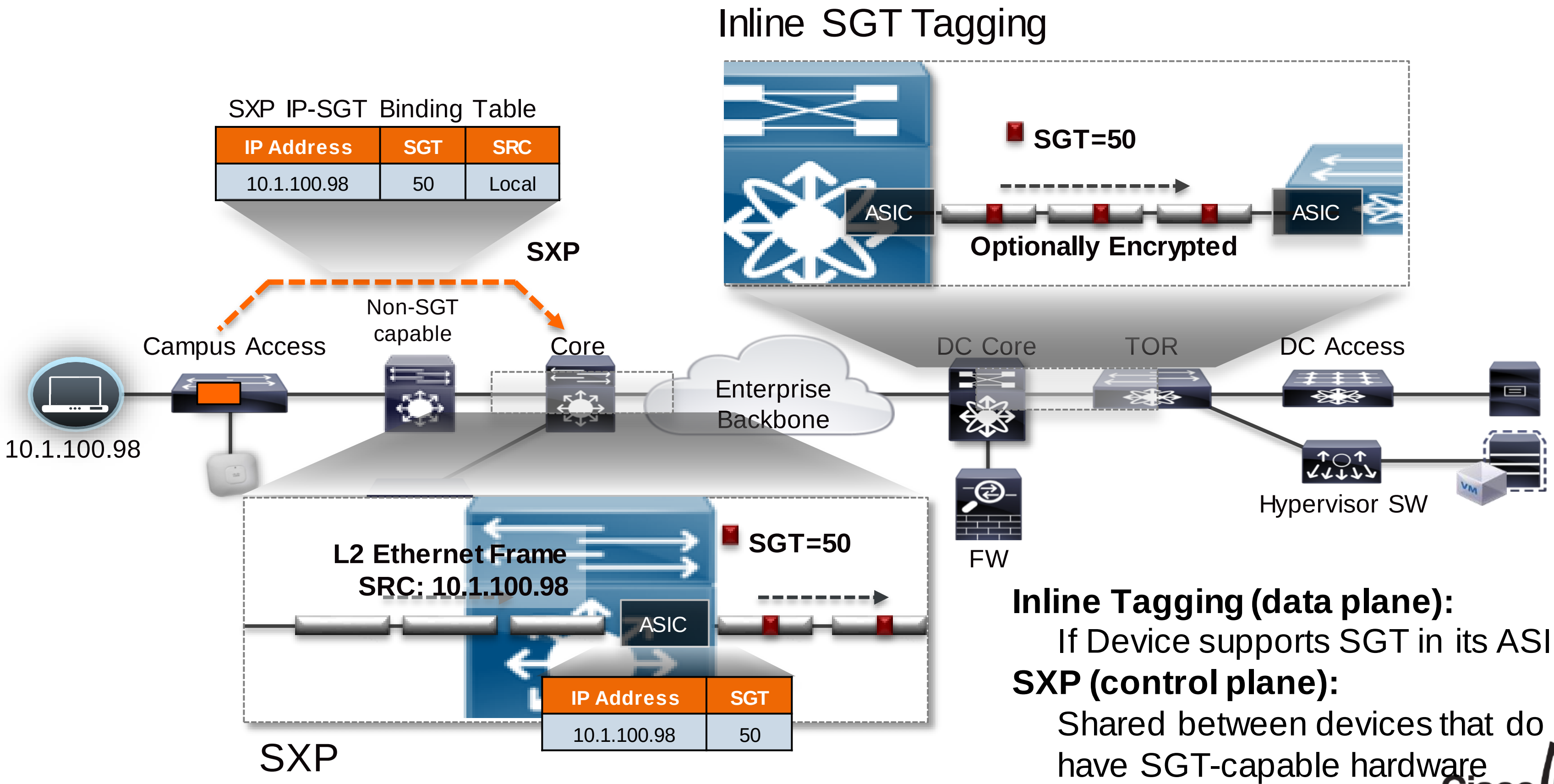
© 2015 Cisco and/or its affiliates. All rights reserved.

TrustSec Classification Functions



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

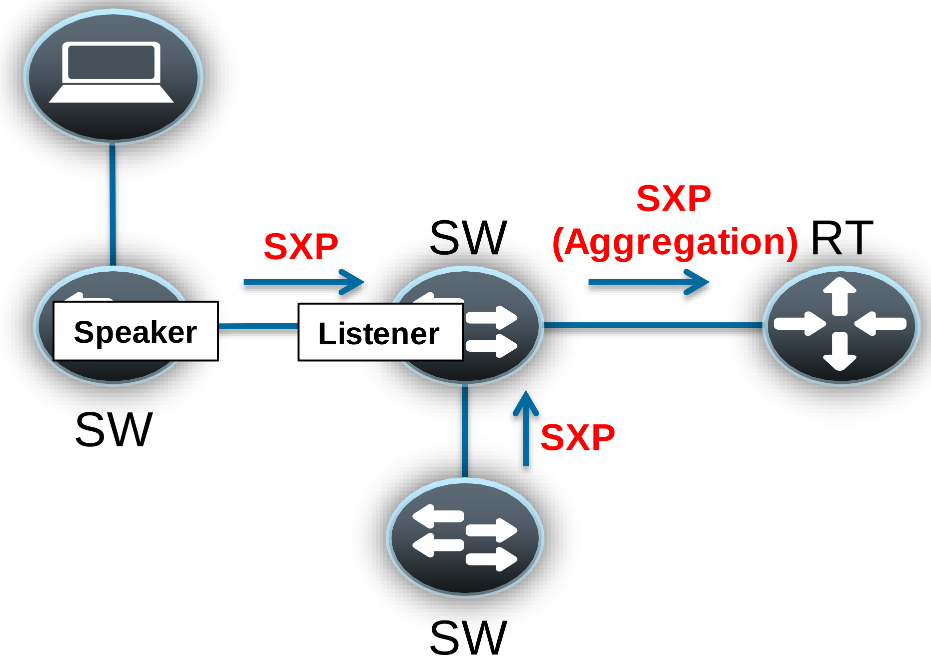
SXP (control plane):

Shared between devices that do not have SGT-capable hardware

© 2015 Cisco and/or its affiliates. All rights reserved.

SGT Exchange Protocol

- Control plane protocol that conveys the IP-SGT map of endpoints to enforcement point
- IP Traffic flows as normal – SXP is out of band to data flow
- 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

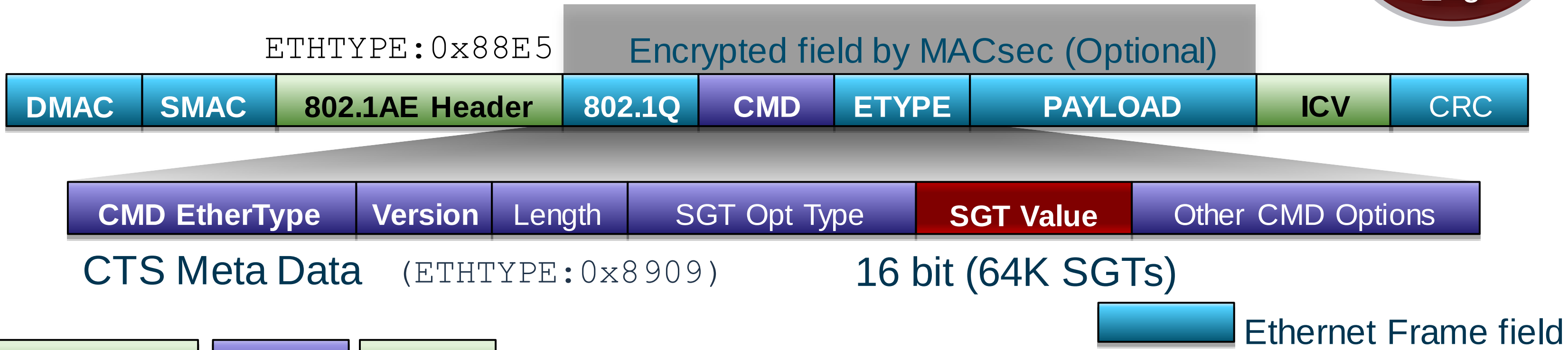


Open Implementations - SXP Informational Draft

- SXP now published as an Informational Draft to the IETF, based on customer requests – shipping partner implementations
- Draft called ‘Source-Group Tag eXchange Protocol’ because of likely uses beyond security
- Specifies SXP v4 functionality with backwards compatibility to SXP v2
- Includes the Cisco Meta Data (CMD) format for inclusion of the SGT with Ethernet frames (detailed on the next slides)
  - https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/
- Further alignment with other metadata carrying formats like the Network Services Header (NSH)
  - Allows for Source Group Tag to be mapped to Source Class
  - Allows for Source Group Tag to be mapped to Destination Class if available
- https://tools.ietf.org/html/draft-guichard-sfc-nsh-dc-allocation-01

Inline Security Group Tagging

Security **G**roup **T**ag


ETHTYPE:0x88E5

Encrypted field by MACsec (Optional)

DMAC | SMAC | 802.1AE Header | 802.1Q | CMD | ETYPE | PAYLOAD | ICV | CRC

CMD EtherType | Version | Length | SGT Opt Type | SGT Value | Other CMD Options

CTS Meta Data (ETHTYPE:0x8909)

16 bit (64K SGTs)

Ethernet Frame field

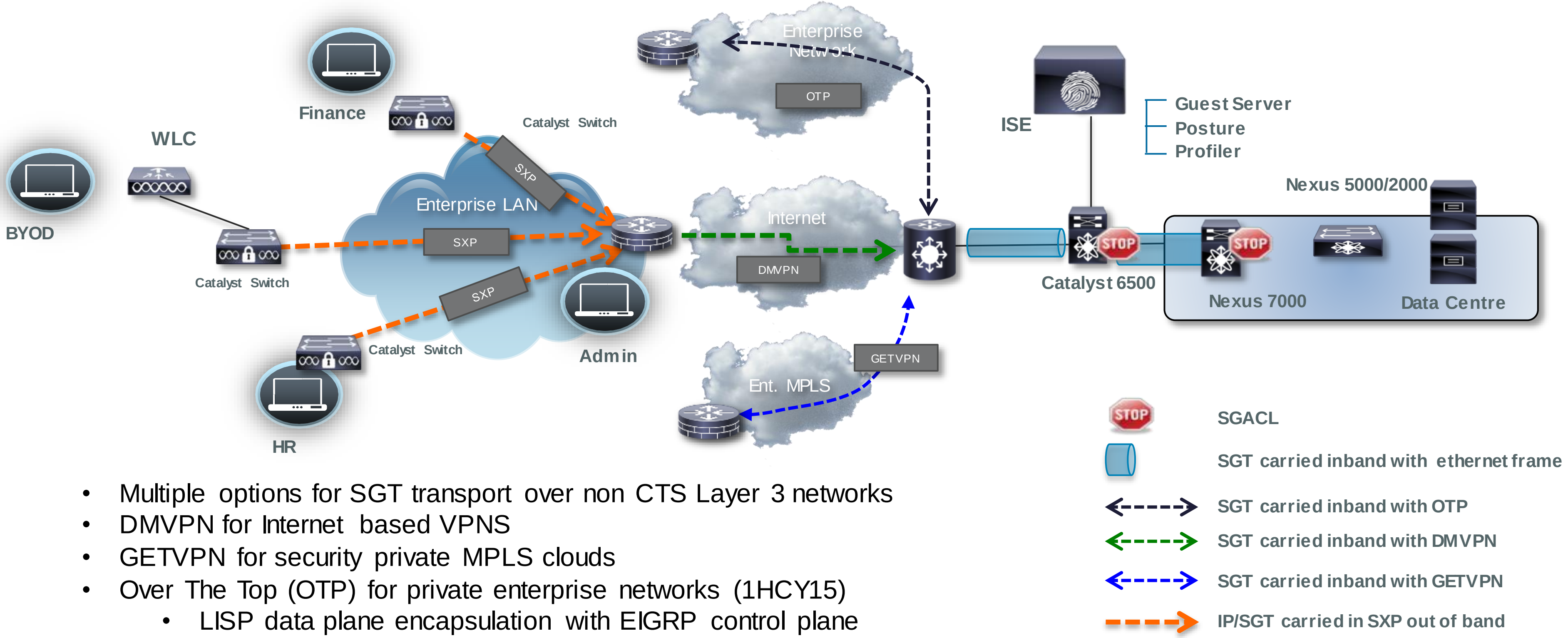
- 802.1AE Header CMD ICV are the L2 802.1AE + TrustSec overhead
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 40 bytes (~1600 bytes with 1552 bytes MTU)
- MACsec is optional 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 ***<u>strongly</u>*** recommended configuration for SGT propagation
  - "cts dot1x" takes link down with AAA down. Tight coupling of link state and AAA state
  - CTS "Critical Authentication" recently introduced on 3K/4K/6K only
- Some platforms (ISRG2, ASR1K, N5K, ASA, N1KV, etc.) only support cts manual/no encryption

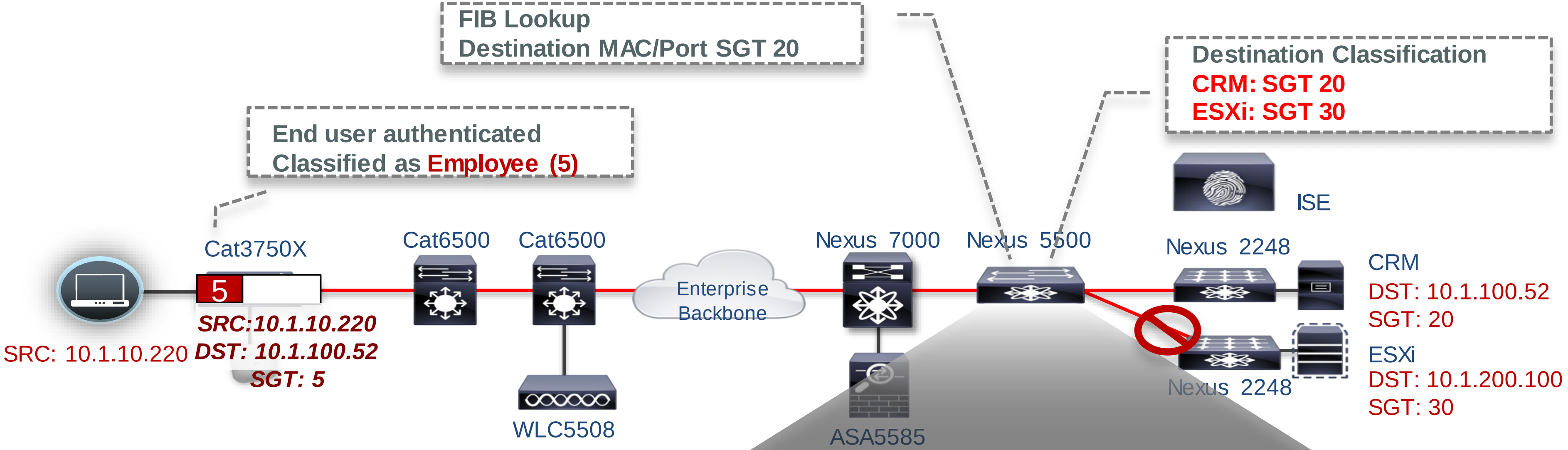
SGT Transport over L3 Networks



- Multiple options for SGT transport over non CTS Layer 3 networks
- DMVPN for Internet based VPNS
- GETVPN for security private MPLS clouds
- Over The Top (OTP) for private enterprise networks (1HCY15)
    - LISP data plane encapsulation with EIGRP control plane

© 2015 Cisco and/or its affiliates. All rights reserved.

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)**

L2 SGT Tagging

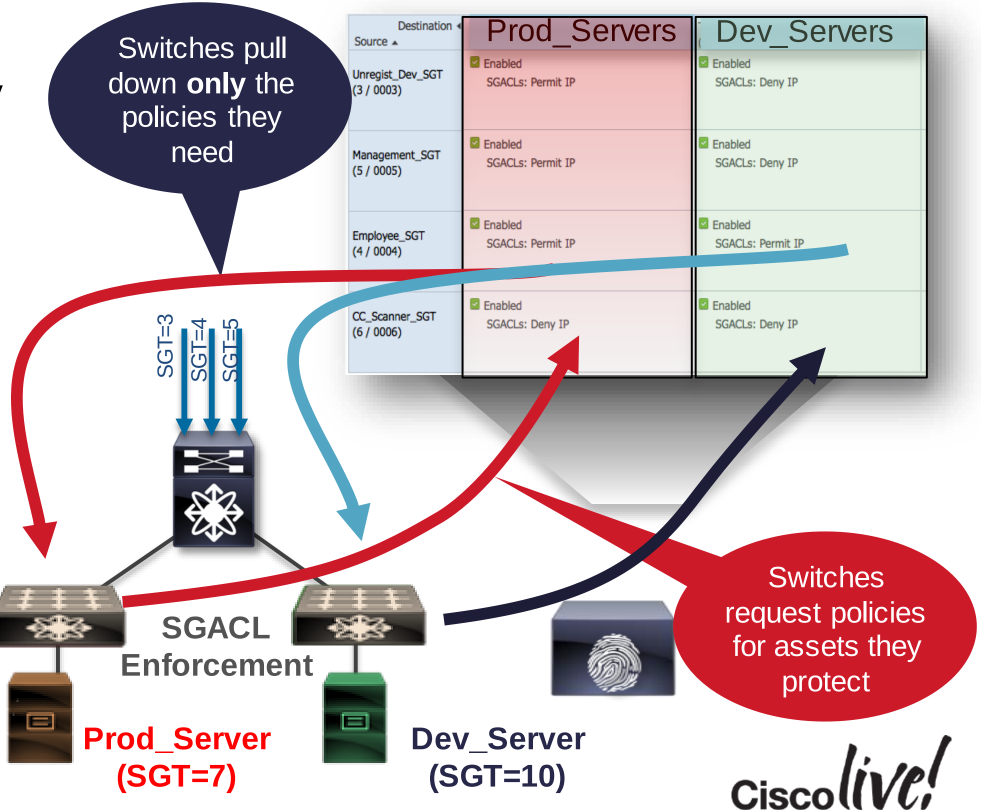
SRC\DST	CRM (20)	ESXi (30)
Employee (5)	SGACL-A	**Deny**
BYOD (7)	Deny	Deny

© 2015 Cisco and/or its affiliates. All rights reserved.

SGACL Scaling Segmentation

- New User/Device/Servers provisioned, e.g Prod Server & Dev Server Roles
- TrustSec switch requests policies for assets they protect
- Policies downloaded & applied dynamically
- Result: Software-Defined Segmentation
  - All controls centrally managed
  - Security policies de-coupled from network topology
  - **No switch-specific security** configs needed
  - One place to audit network-wide policies
  - Scales via two mechanisms
    - Put destination SGT in FIB, derive source SGT from frame/FIB
    - Only protocol/port information put into TCAM

Segmentation defined in ISE



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

Switches pull down **only** the policies they need

Prod_Server (SGT=7)

Dev_Server (SGT=10)

Switches request policies for assets they protect

Use Case Reviews with Design Consideration

TrustSec Platform Support

Tagging

- Catalyst 2960-S/-C/-Plus/-X/-XR
- Catalyst 3560-E/-C/-X
  Catalyst 3750-E/-X
- Catalyst 3850, 3650
  WLC 5760
- Catalyst 4500E (Sup6E/7E)
  Catalyst 4500E (8E)
  Catalyst 6500E (Sup720/2T), 6880X
- Wireless LAN Controller
  2500/5500/WiSM2
- Nexus 7000
- Nexus 6000
- Nexus 5600
  Nexus 5500
- Nexus 1000v (Port Profile)
- ISR G2 Router, CGR2000
- IE2000/3000, CGS2000
- ASA5500X, ASAv (VPN RAS)

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 3650, 3850
SXP	Catalyst 4500E (Sup6E)
SXP SGT	Catalyst 4500E (Sup 7E), 4500X
SXP SGT	Catalyst 4500E (Sup 8E)
SXP	Catalyst 6500E (Sup720)
SXP SGT	Catalyst 6500E (Sup 2T) / 6880X
SXP	WLC 2500, 5500, WiSM2
SXP SGT	WLC 5760
SXP SGT	Nexus 1000v
SXP SGT	Nexus 5500/22xx FEX
SXP SGT	Nexus 5600/6000/22xx FEX
SXP SGT	Nexus 7000/22xx FEX
SXP SGT GETVPN DMVPN	ISRG2, CGR2000
SXP SGT GETVPN DMVPN	ASR1000, CSR1000V, ISR 4400
SXP SGT	ASA5500(X), ASAv

- All ISRG2 Inline SGT (except C800): **Today**

Enforcement

SGACL	Catalyst 3560-X Catalyst 3750-X
SGACL	Catalyst 3850, 3650 WLC 5760
SGACL	Catalyst 4500E (Sup7E) Catalyst 4500E (Sup8E) Catalyst 6500E (Sup2T) / 6880X
SGACL	Nexus 7000
SGACL	Nexus 6000 Nexus 5600 Nexus 5500
SGACL	Nexus 1000v
SGFW	ISR G2 Router, CGR2000
SGFW	ASR 1000 Router, ISR 4400, CSR1000V
SGFW	ASA 5500/5500X Firewall ASAv Firewall

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to Start with TrustSec

- Find an appropriate use case that is straightforward and has realistic criteria for success and has demonstrable ROI.
  - Model potential group relationships and high level permissions for the use case
  - Develop detailed permissions (specific ACLs) off those relationships
- Apply details SGACLs to the use case in a monitoring function to detect items outside the security profile
  - Firewall ACE logging analysis (if available)
  - SGACL ACE logs and syslog analysis
  - ACE Log for unknown/SGT or SGT/unknown matches for the use case
  - Default permission of ACE log for anything that “missed” the explicit permission
  - Monitor mode SGACLs if available (Cat6K)
- Gather feedback from above analysis and iterate with the permissions
- Finalise final permissions and create completed TrustSec matrix.

© 2015 Cisco and/or its affiliates. All rights reserved.

WLAN Access Control

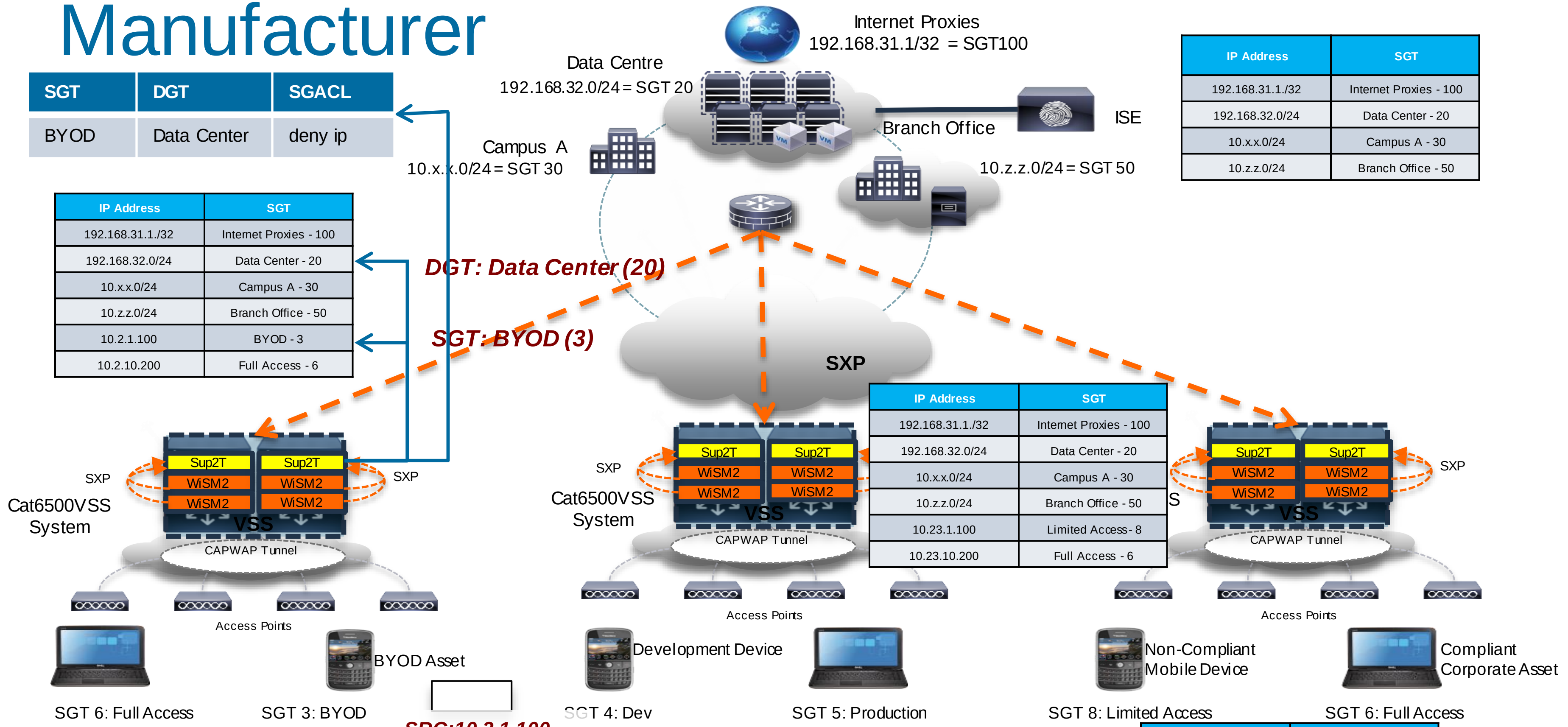
- Business Problem/Background
  - – BYOD assets require restricted access to Corp. network and Internet proxies
  - – Production vs. Development Users on Corp. WLAN
  - – Compliant vs. Noncompliant Users on Corp. WLAN
  - – Centralised compulsory tunnelling caused application performance degradation
  - – Scaling decentralised access control
    - WLC can't scale to ACL requirements - ACL needs to scale more than 64 lines of ACL (>1,500)
    - Capex concern on buying and distributing firewalls or switches
    - Opex concerns of operating distributed environment
- Solution Overview
  - – Use of SXP to communicate IP/SGT of all classes of users above to upstream SGACL switch
  - – Use subnet/SGT and IP/SGT definitions published to distributed SGACL switches via SXP, ISE 1.3 push, or CLI
  - – Upstream SGACL switch derives SGT/DGT matches from SXP, ISE 1.3, or CLI.
  - – Example - Reduced IOS ACE from approx 1500 lines to one ACE
    - permit tcp dst eq 443

WLAN Access Control

Manufacturer

SGT	DGT	SGACL
BYOD	Data Center	deny ip

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



SRC:10.2.1.100
DST: 10.x.x.100

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

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

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

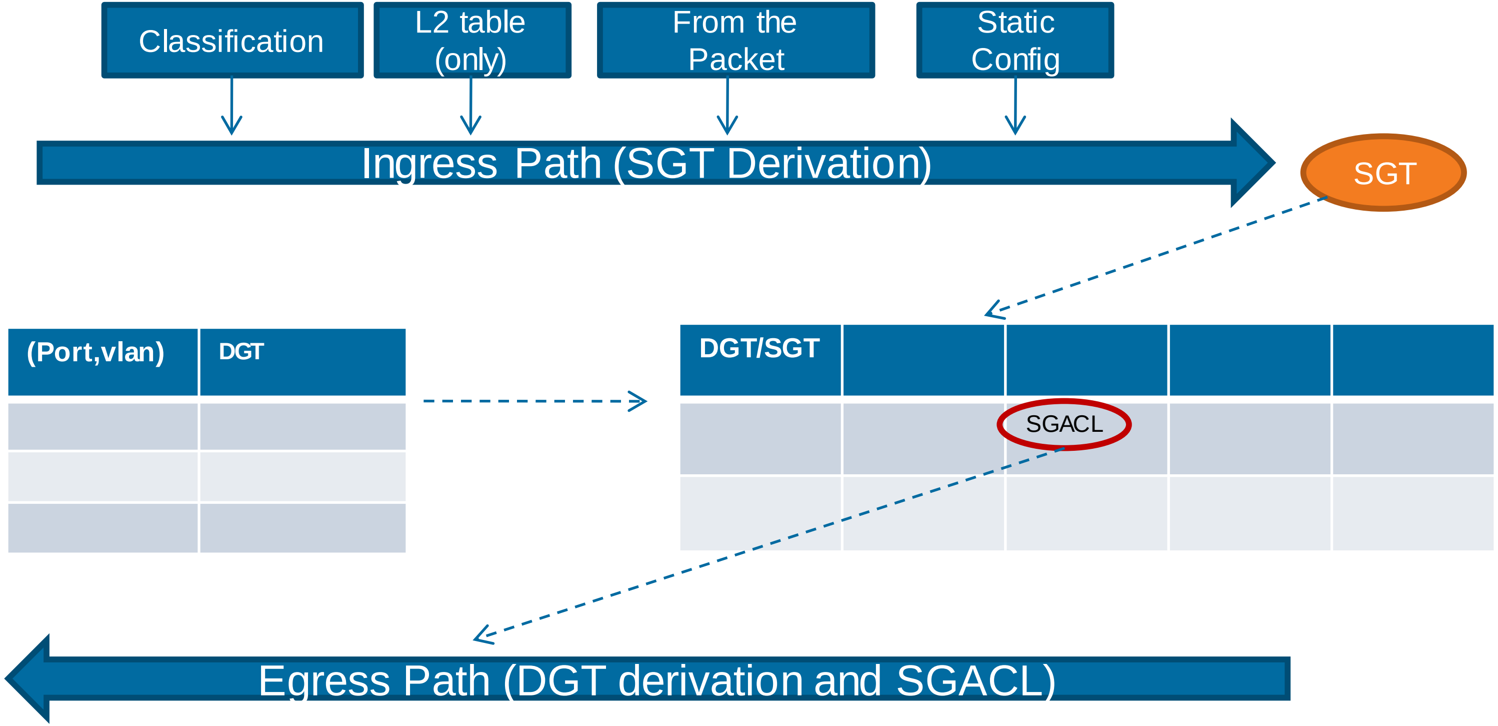
IP Address	SGT
10.23.1.100	Limited_Access - 8
10.23.10.200	Full Access - 6

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hardware Forwarding SGT/SGACL Today

- Two Groupings of Hardware Forwarding
- Port/VLAN based
  - Cat 3K-X
  - N5500
- 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

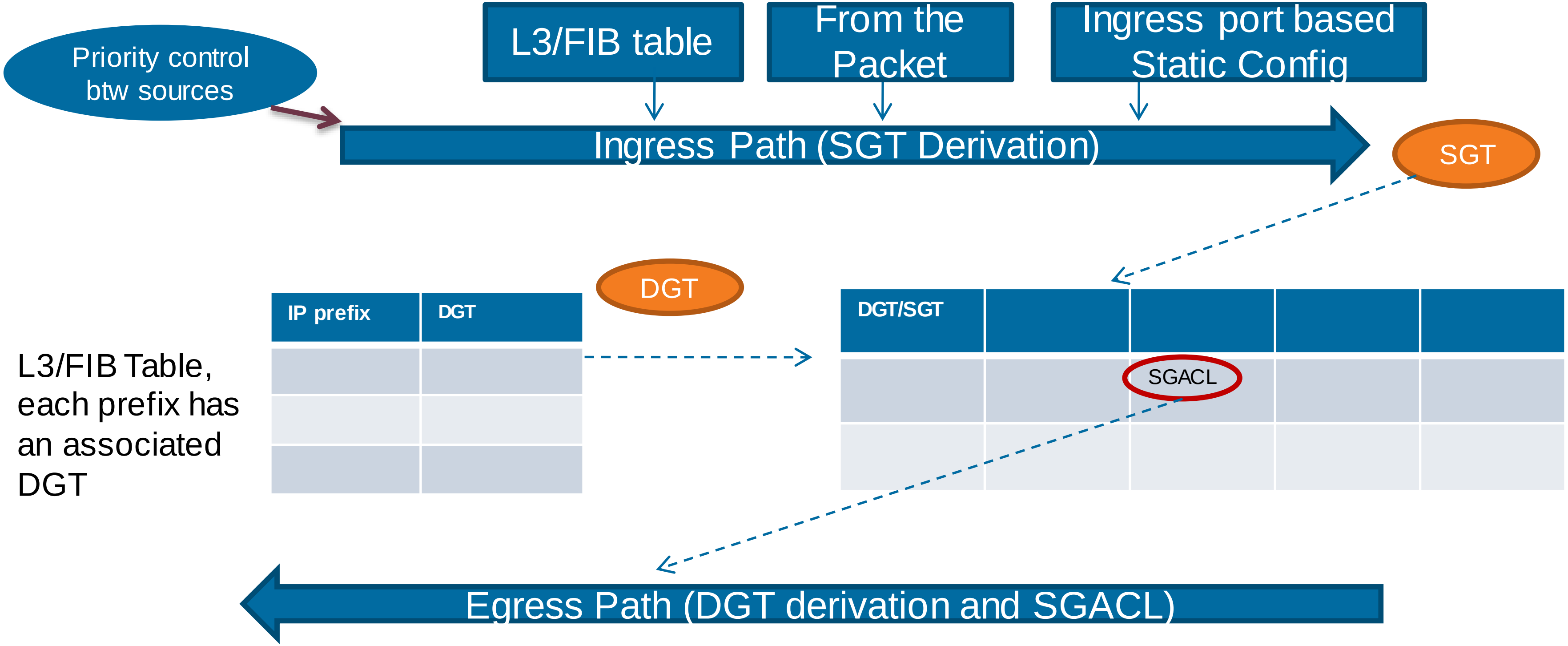

Classification
L2 table (only)
From the Packet
Static Config
Ingress Path (SGT Derivation)
SGT
Egress Path (DGT derivation and SGACL)

(Port,vlan)	DGT

DGT/SGT				
		SGACL		

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
Egress Path (DGT derivation and SGACL)

L3/FIB Table, each prefix has an associated DGT

IP prefix	DGT

DGT/SGT				
		SGACL		

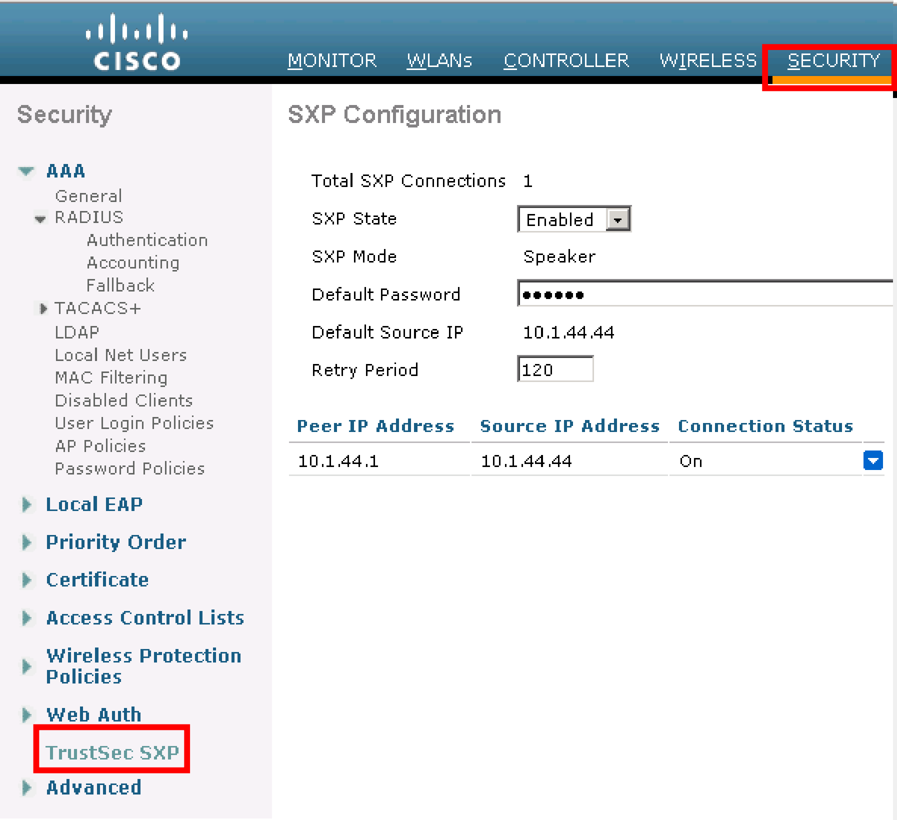
A number of SGT(DGT) assignment sources, e.g. SXP, VLAN-SGT, Subnet/Host SGT, will be evaluated by SGT software against a priority list, the winning result will be programmed into the L3/FIB table

Implications of Hardware Forwarding Capabilities

- Port/VLAN Based Hardware
  - Limited SXP applicability due to the SGT derivation on mac/port
  - Fine to be speakers/relays but not SGT/DGT derivation from SXP
  - Limited number of SGTs per port (one or per vlan/port)
  - Not appropriate for this WLAN access control use case
- 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)
  - As shown, very appropriate for this use case and others

© 2015 Cisco and/or its affiliates. All rights reserved.

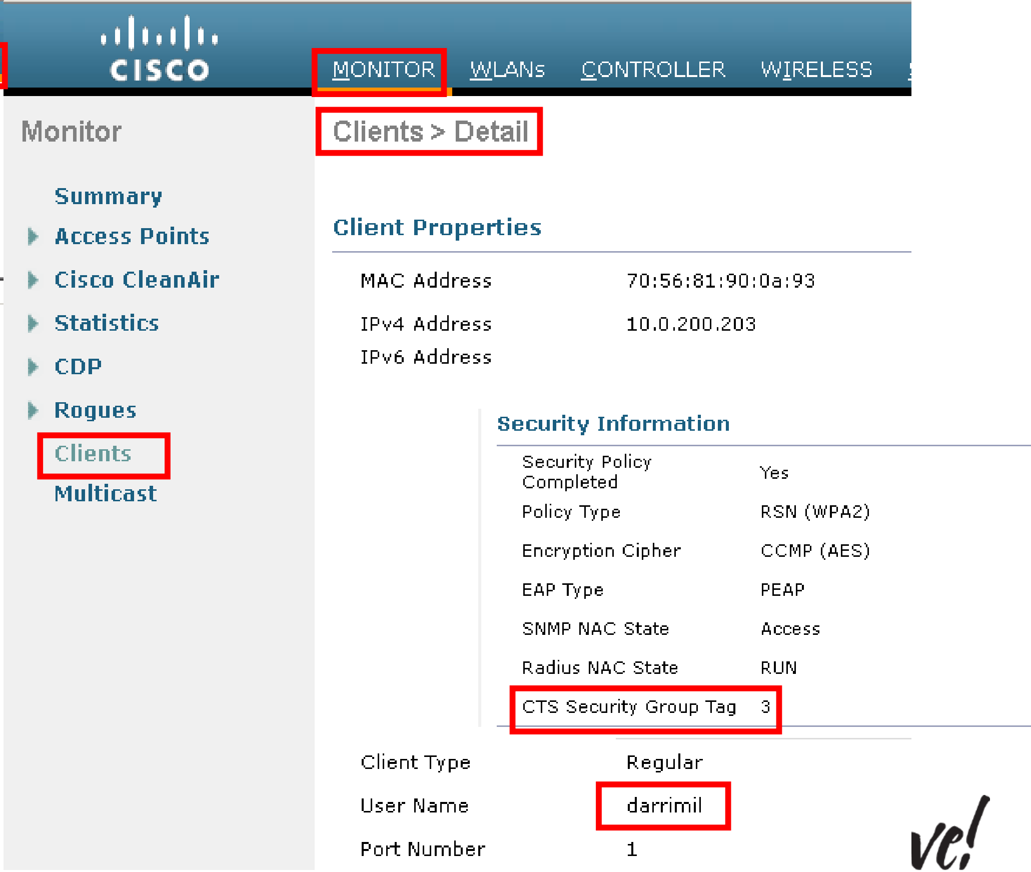
WLC SXP Configuration



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

© 2015 Cisco and/or its affiliates. All rights reserved.

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
```

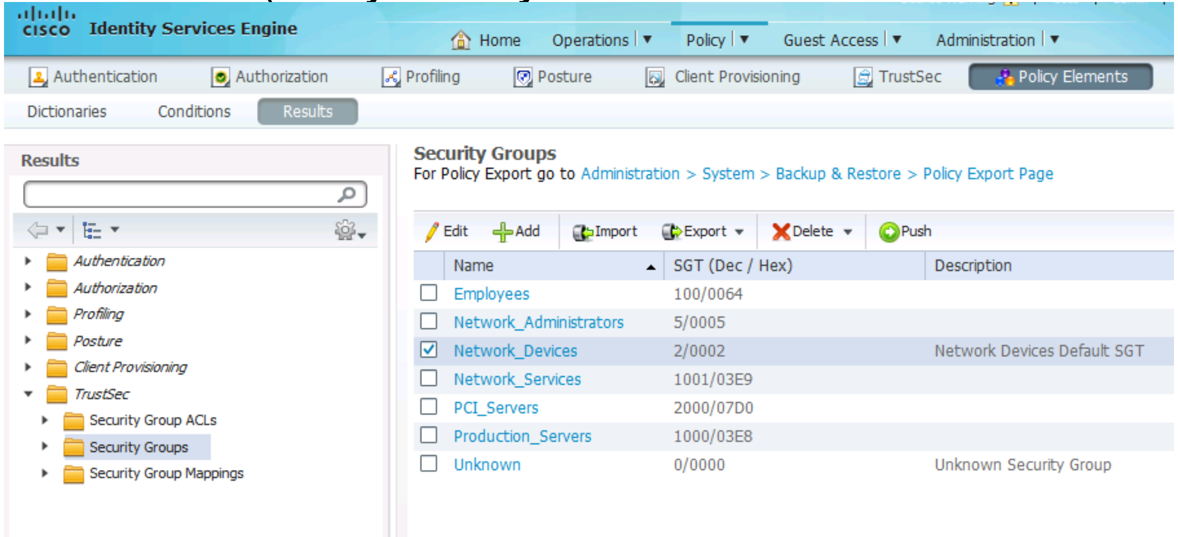
```
C3750#show cts role-based sgt-map all details
Active IP-SGT Bindings Information

IP Address            Security Group                                  Source
======================================================================
10.10.11.1            2:device_sgt                                     INTERNAL
10.10.11.100          6:Full_Access                                    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            2000:PCI_Servers                                 CLI
10.1.44.1             2:Device_sgt                                     INTERNAL
--- snip ---
10.0.200.203          3:BYOD                                           SXP
10.10.11.100          6:Full_Access                                    SXP
```

Enabling SGT/SGACL on IOS

- Following is a high-level overview of SGT/SGACL configuration on 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 > TrustSec > Security Group**)



Security Groups

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

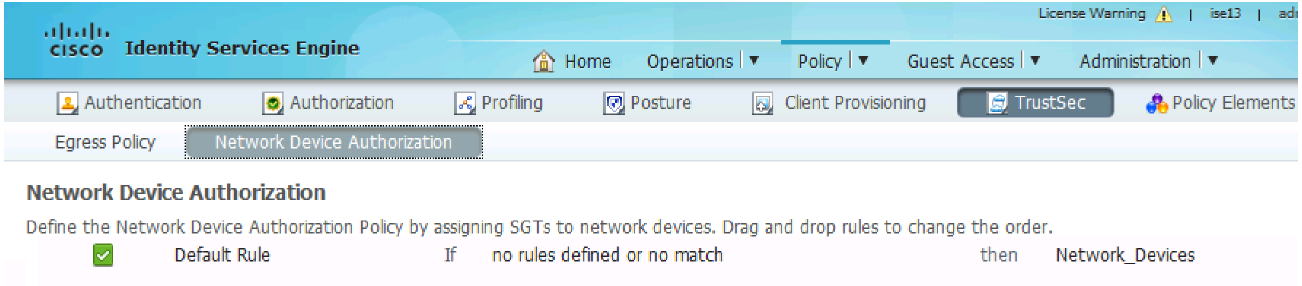
	Name	SGT (Dec / Hex)	Description
☐	Employees	100/0064	
☐	Network_Administrators	5/0005	
☑	Network_Devices	2/0002	Network Devices Default SGT
☐	Network_Services	1001/03E9	
☐	PCI_Servers	2000/07D0	
☐	Production_Servers	1000/03E8	
☐	Unknown	0/0000	Unknown Security Group

All SGTs should have access to an Network Device SGT by policy (ARP needs to work ☺)

© 2015 Cisco and/or its affiliates. All rights reserved.

SGT Configuration for ISE

③ Under **Policy > TrustSec > Network Device Authorisation**, assign Device SGT created in step (2) to default condition

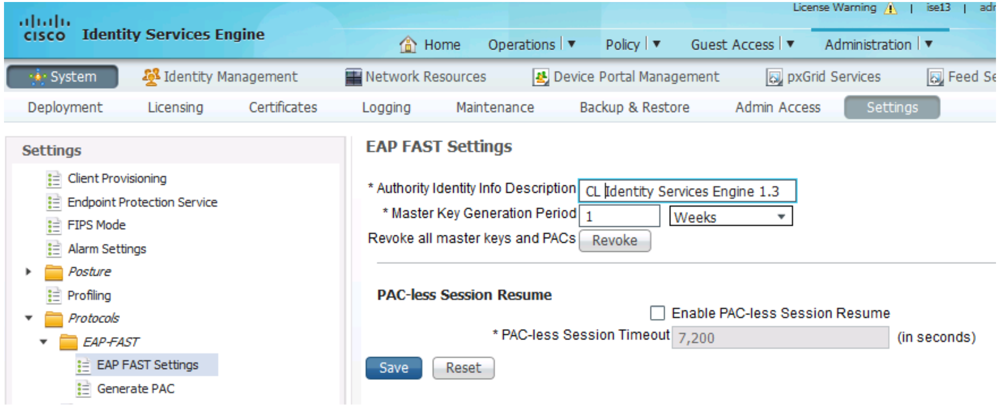


Network Device Authorization

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

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

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.



EAP FAST Settings

* Authority Identity Info Description: CL Identity Services Engine 1.3

* Master Key Generation Period: 1 Weeks

Revoke all master keys and PACs: Revoke

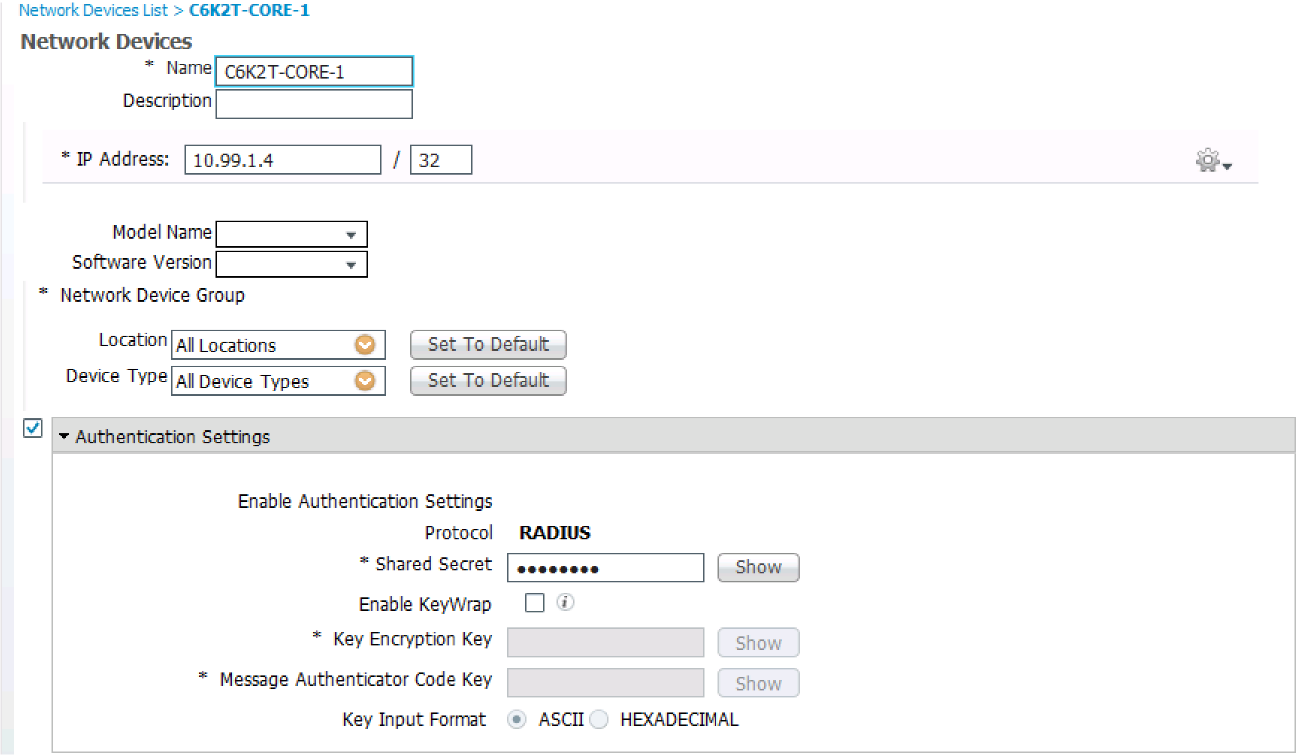
PAC-less Session Resume

□ Enable PAC-less Session Resume

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

Configuration Cat6K Sup2T as Seed Device

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



Network Devices List > C6K2T-CORE-1

Network Devices

* Name: C6K2T-CORE-1

Description:

* IP Address: 10.99.1.4 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations — Set To Default

Device Type: All Device Types — Set To Default

☑ Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: •••••••• — Show

Enable KeyWrap: □

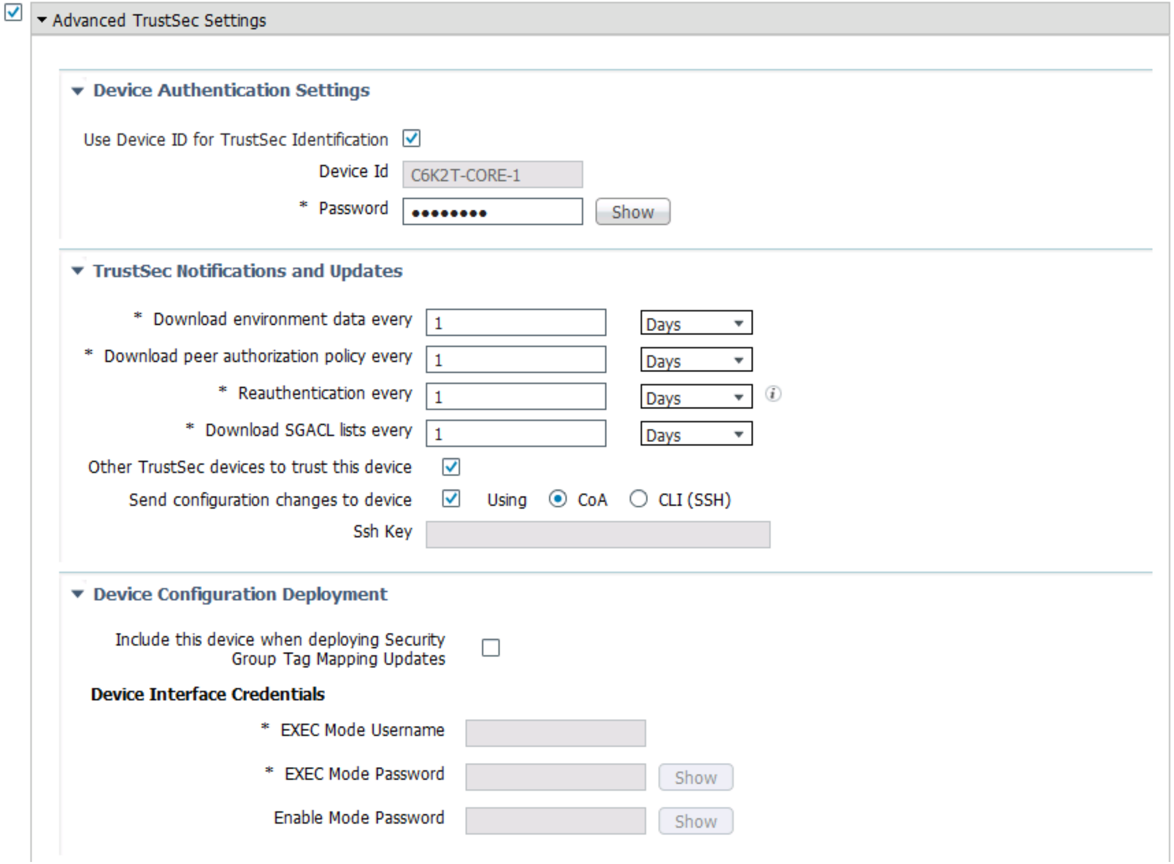
* Key Encryption Key: — Show

* Message Authenticator Code Key: — Show

Key Input Format: ● ASCII ○ HEXADECIMAL

Configuration an SGT Device

⑥ Configure RADIUS secret. Also Advanced TrustSec Settings, check Use Device ID for TrustSec, then type device password. This ID and Password needs to be exactly same as you define on network device CLI



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: C6K2T-CORE-1

* Password: ●●●●●●●●● [Show]

TrustSec 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 TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ● CoA ○ CLI (SSH)

Ssh Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates □

Device Interface Credentials

* EXEC Mode Username:

* EXEC Mode Password: [Show]

Enable Mode Password: [Show]

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 authorisation list name for Trustsec policy download

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

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

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

© 2015 Cisco and/or its affiliates. All rights reserved.

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

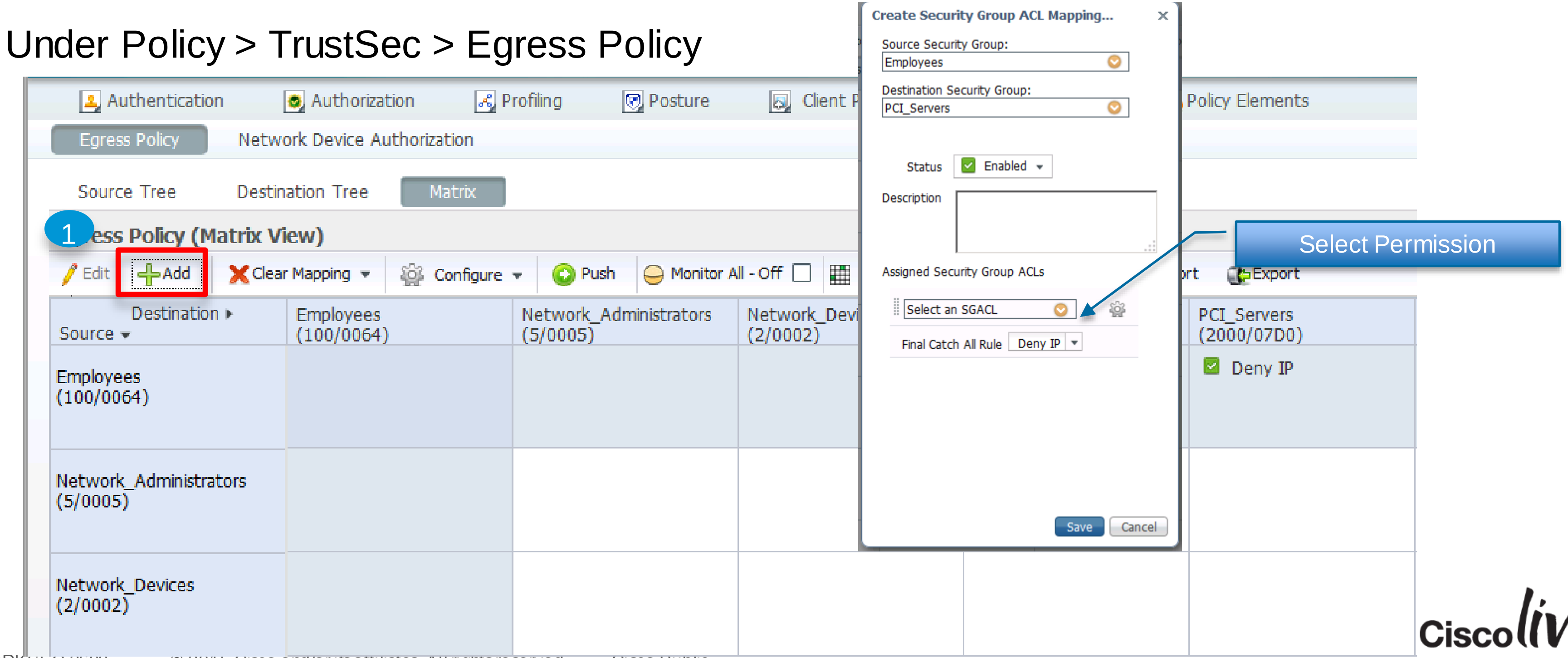
Verification – Environment Data

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

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 > TrustSec > Egress Policy



Destination ▸ Source ▾	Employees (100/0064)	Network_Administrators (5/0005)	Network_Devi (2/0002)	PCI_Servers (2000/07D0)
Employees (100/0064)				✓ Deny IP
Network_Administrators (5/0005)				
Network_Devices (2/0002)				

Create Security Group ACL Mapping... ×

Source Security Group: Employees

Destination Security Group: PCI_Servers

Status ☑ Enabled

Description

Assigned Security Group ACLs

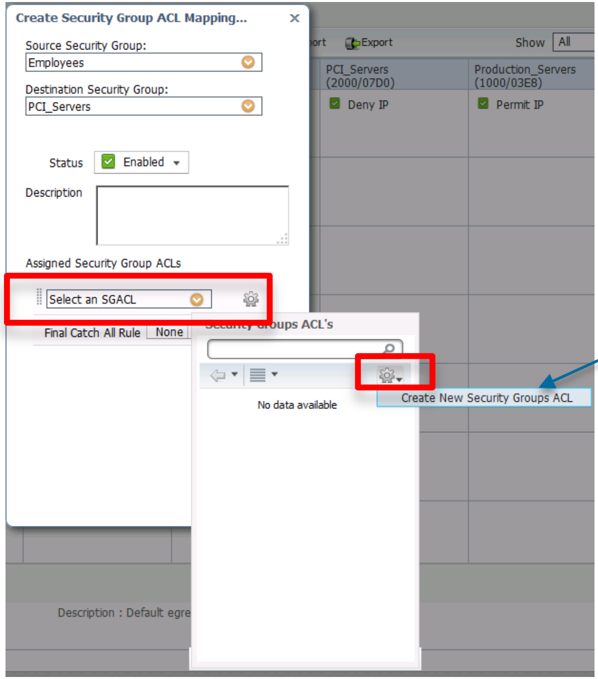
Select an SGACL

Final Catch All Rule Deny IP

Save Cancel

Preparing ISE for SGACL Enforcement

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



Create Security Group ACL Mapping...

Source Security Group: Employees

Destination Security Group: PCI_Servers

Status ☑ Enabled

Description

Assigned Security Group ACLs

Select an SGACL

Final Catch All Rule None

Security Groups ACL's

No data available

Create New Security Groups ACL

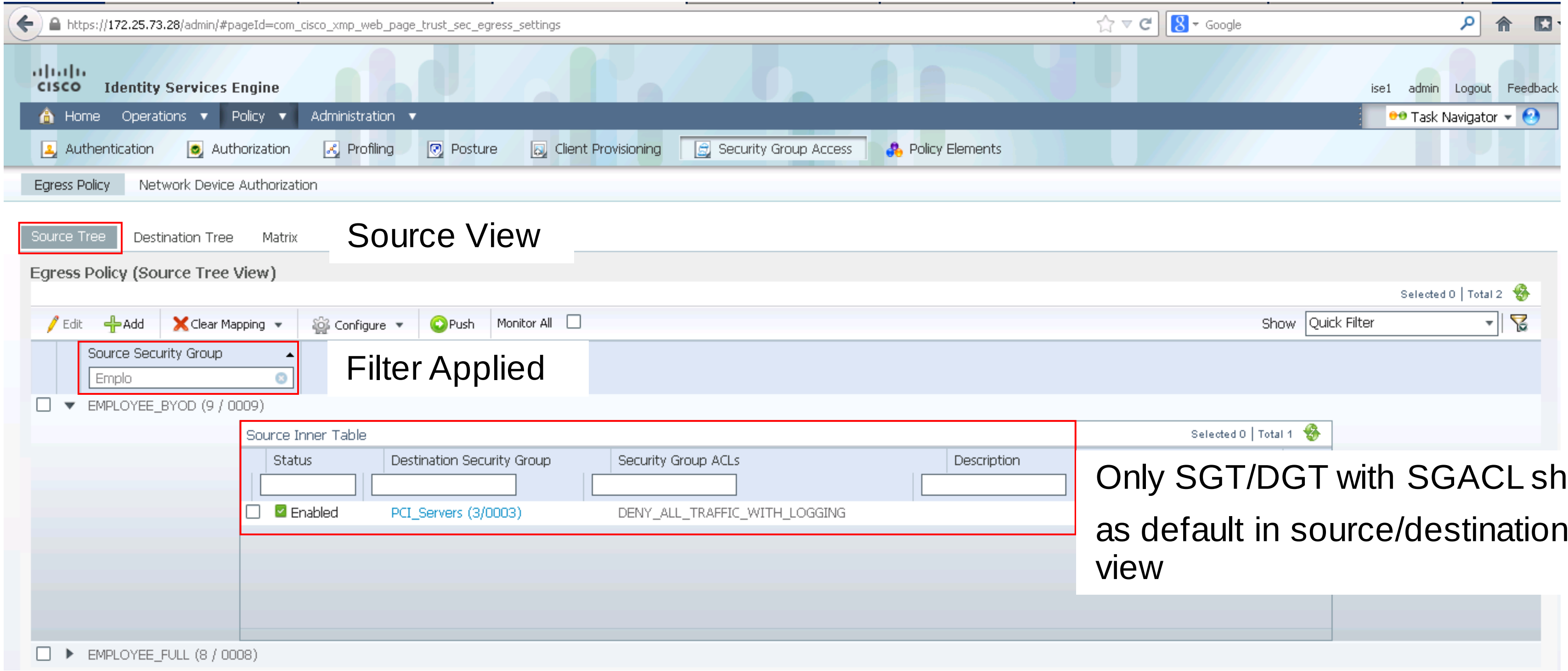
Create new SGACL if needed

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

Source View

Egress Policy (Source Tree View)

Selected 0 | Total 2

Edit Add Clear Mapping ▾ Configure ▾ Push Monitor All □
Show Quick Filter

Source Security Group: Emplo

Filter Applied

□ ▾ EMPLOYEE_BYOD (9 / 0009)

Source Inner Table — Selected 0 | Total 1

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

Only SGT/DGT with SGACL shown as default in source/destination tree view

□ ▸ 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 192.168.31.1 sgt 100
Switch(config)#cts role-based sgt-map 192.168.32.0/24 sgt 20
Switch(config)#cts role-based sgt-map 10.x.x.0 sgt 30
```

Enabling SGACL Enforcement Globally and for VLAN

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

© 2015 Cisco and/or its affiliates. All rights reserved.

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

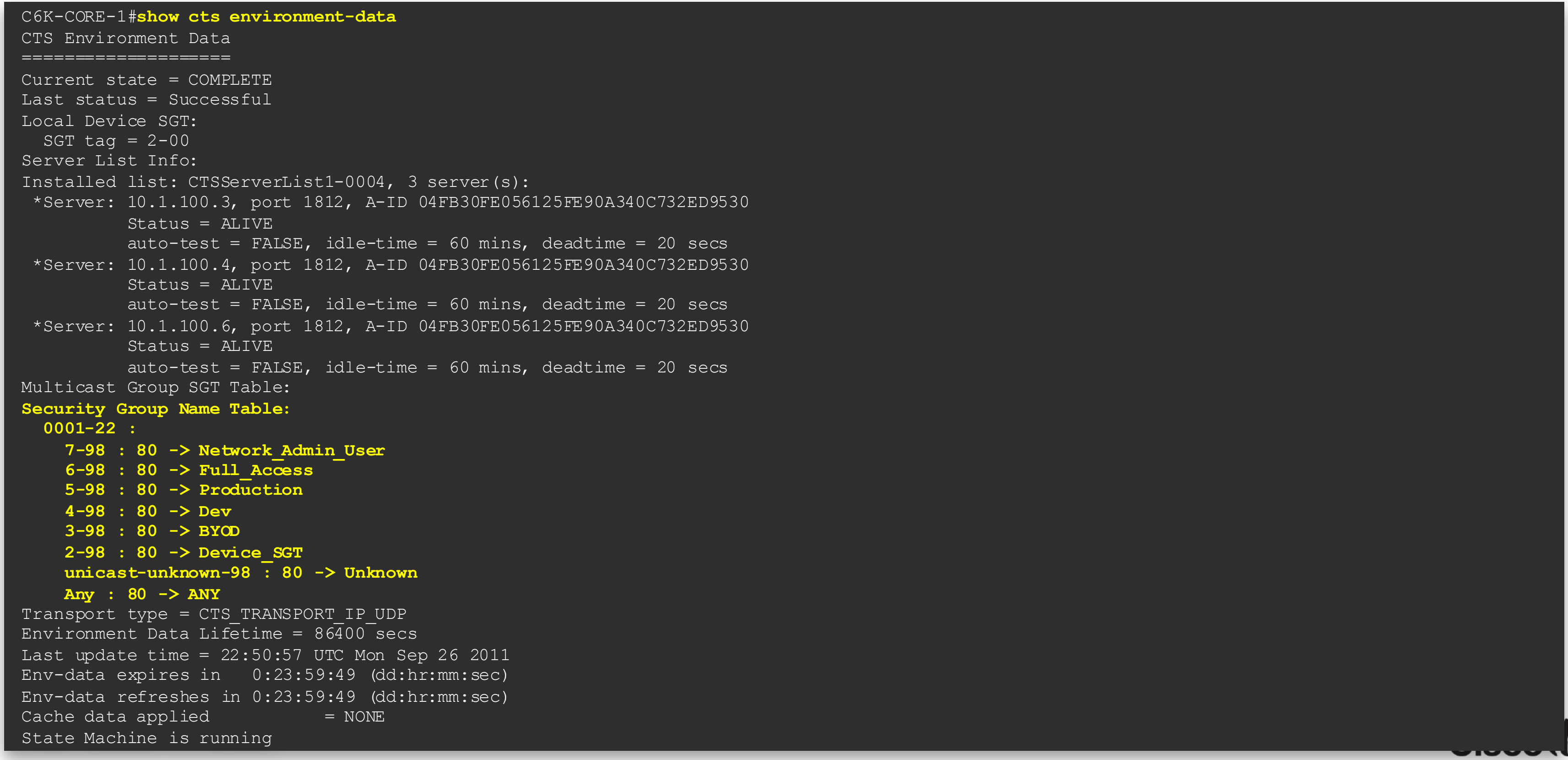
```
Switch#cts refresh environment-data
Environment data download in progress
```

Refresh Policy using cts refresh policy

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

Downloading Policy on IOS Switch

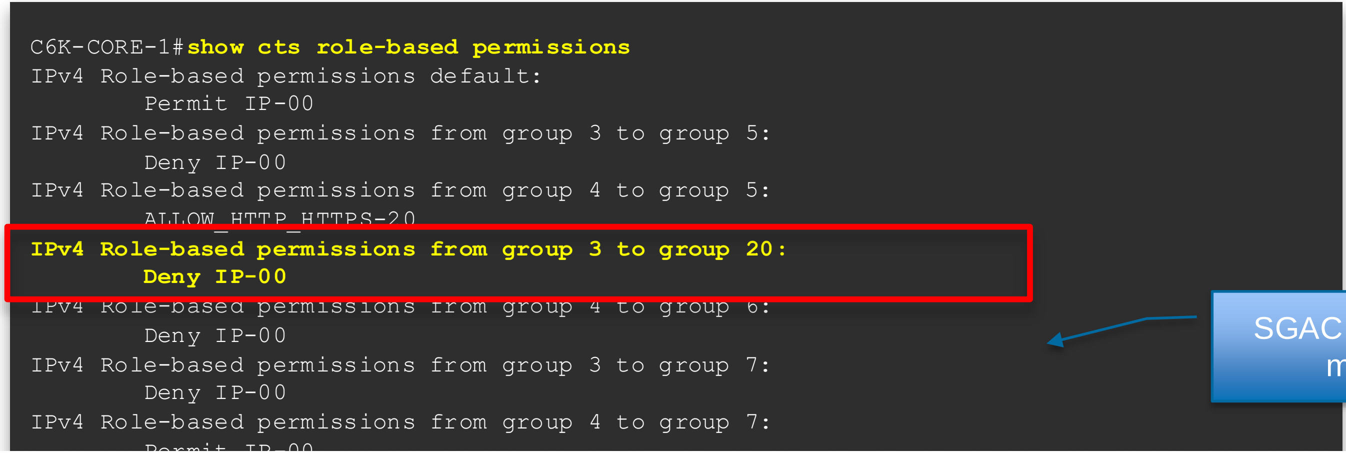
Verify Environment Data



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

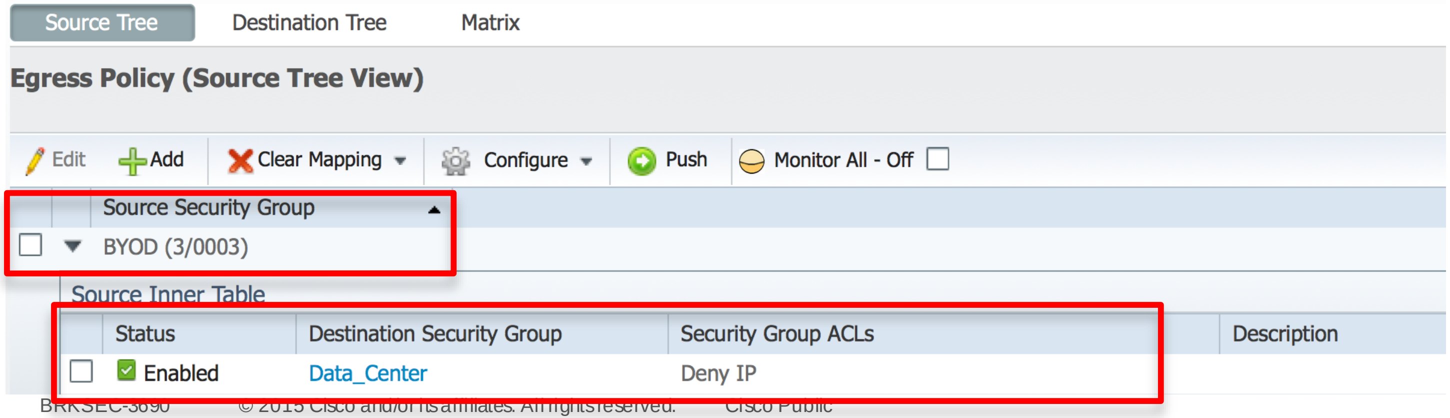
Downloading SGACL Policy on IOS Switch

Verify SGACL Content



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

SGACL Mapping Policy should match to one on ISE



Egress Policy (Source Tree View)

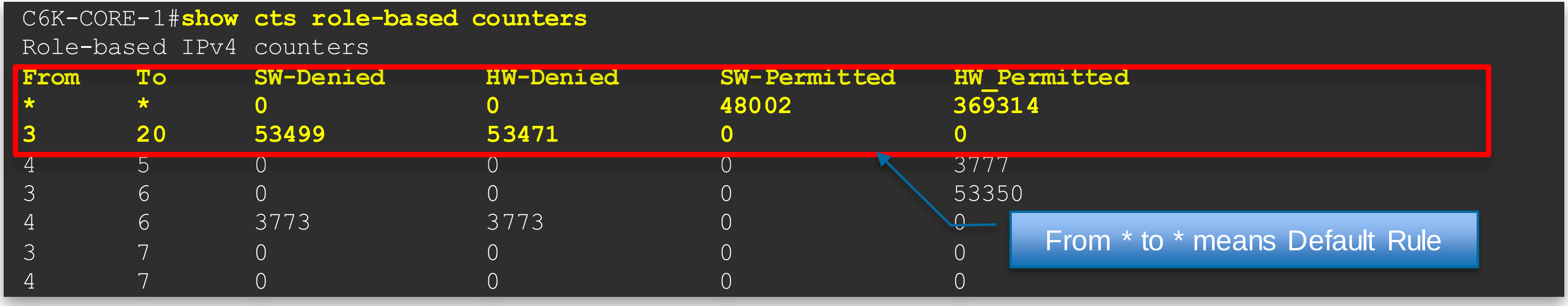
	Source Security Group
☐	BYOD (3/0003)

Source Inner Table

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

Verifying SGACL Drops

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



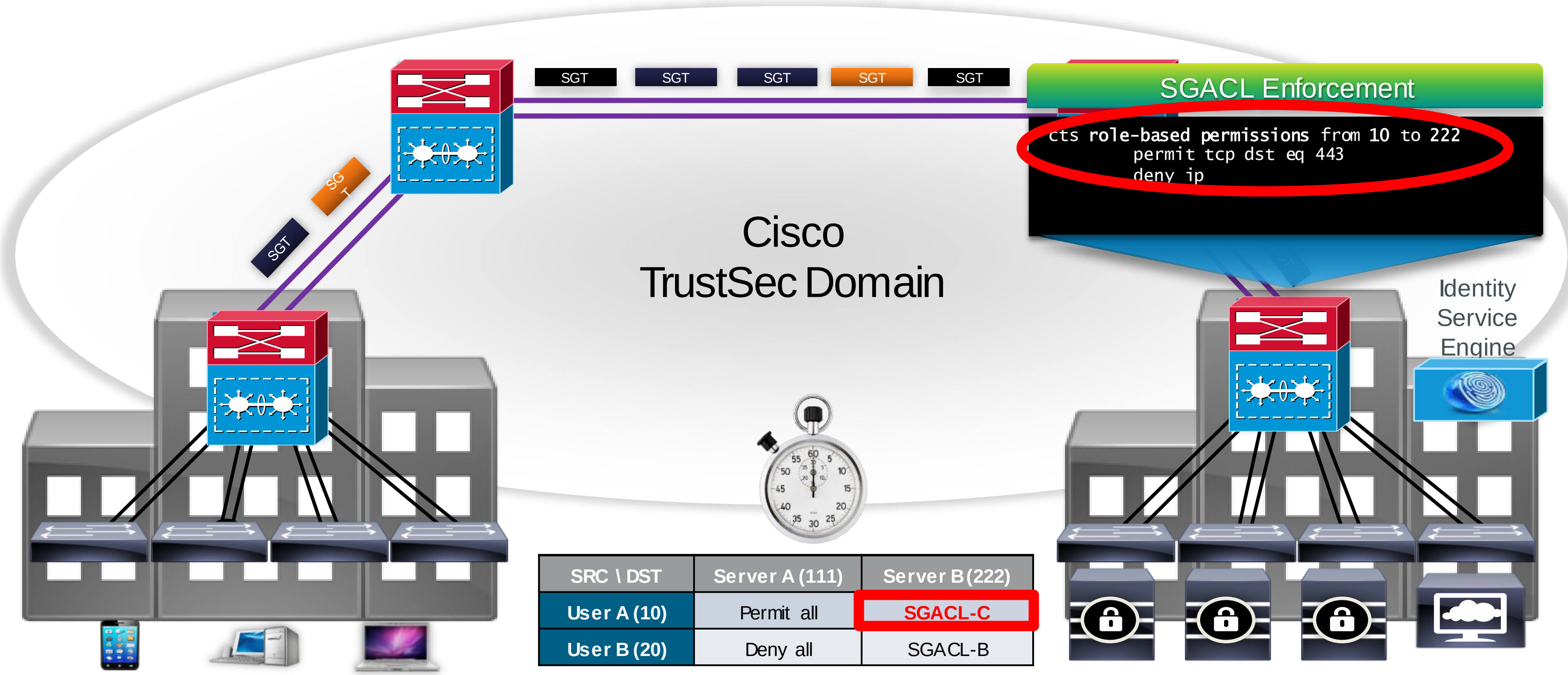
```
C6K-CORE-1#show cts role-based counters
Role-based IPv4 counters
From      To        SW-Denied          HW-Denied          SW-Permitted       HW_Permitted
*         *         0                  0                  48002              369314
3         20        53499              53471              0                  0
4         5         0                  0                  0                  3777
3         6         0                  0                  0                  53350
4         6         3773               3773               0                  0
3         7         0                  0                  0                  0
4         7         0                  0                  0                  0
```

From * to * means Default Rule

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

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

SGACL Policy Push

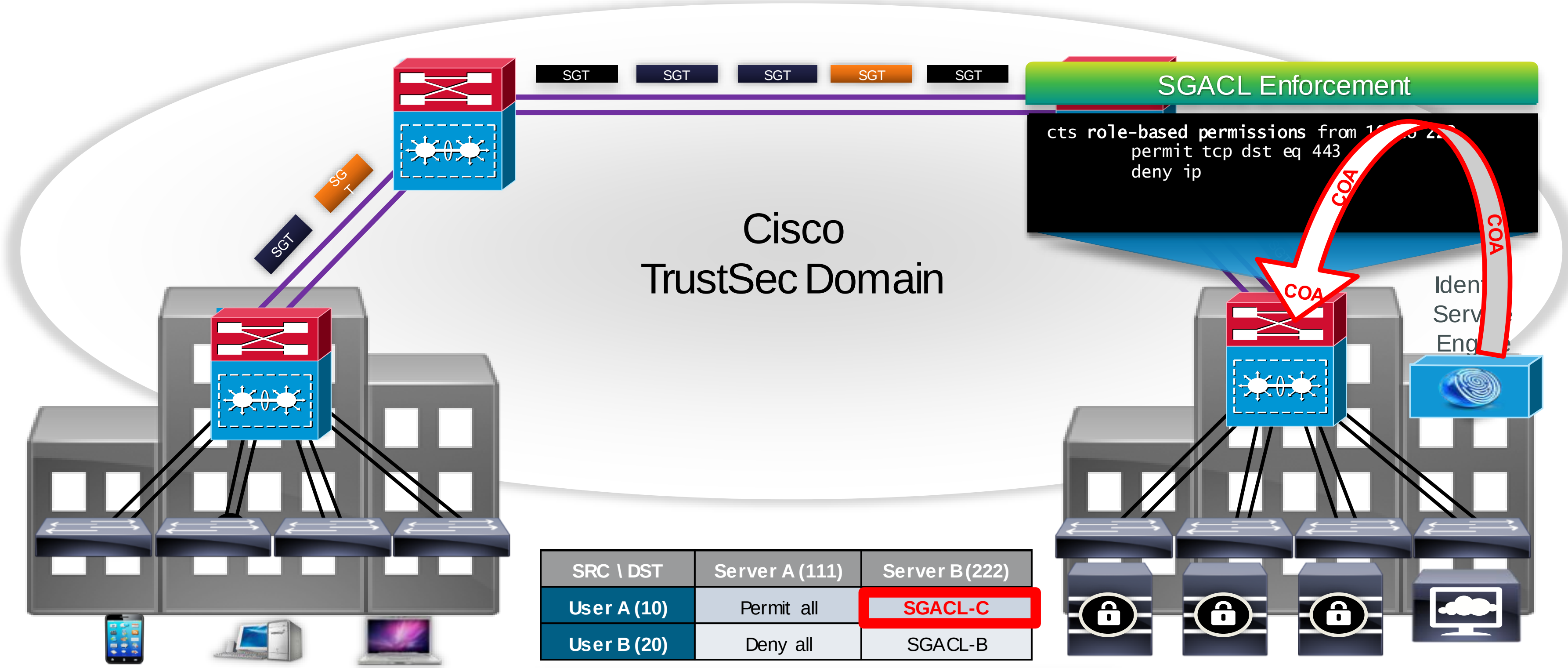


```
cts role-based permissions from 10 to 222
          permit tcp dst eq 443
          deny ip
```

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

© 2015 Cisco and/or its affiliates. All rights reserved.

SGACL Policy Push



```
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

COA Config on IOS Switch

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

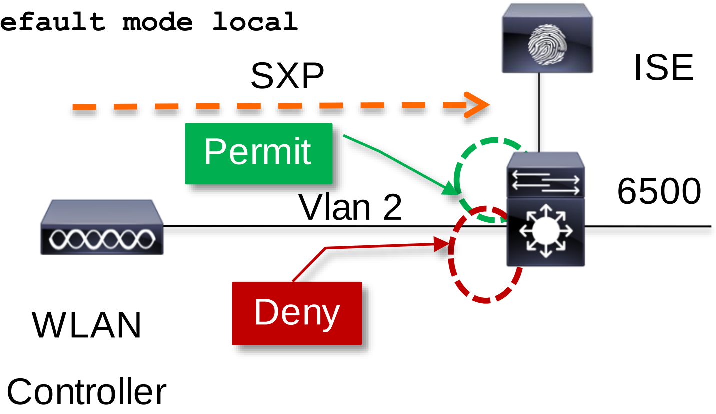
© 2015 Cisco and/or its affiliates. All rights reserved.

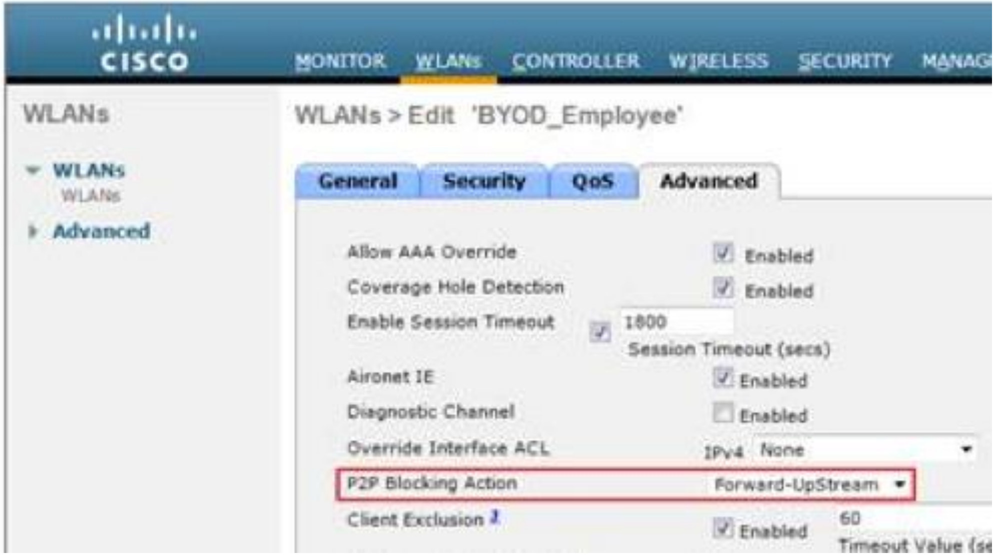
SGACL Monitoring – Best Effort Syslog

```
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
```

Shared Living Room/room Policy Enforcement

```
cts sxp connection peer 10.1.36.2 source 10.99.1.4 password default mode local
listener hold-time 0 0
!
interface Vlan2
  ip local-proxy-arp
  ip route-cache same-interface
!
cts role-based enforcement
cts role-based enforcement vlan-list 2
```





WLANs > Edit 'BYOD_Employee'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

Override Interface ACL IPv4 None

P2P Blocking Action Forward-UpStream

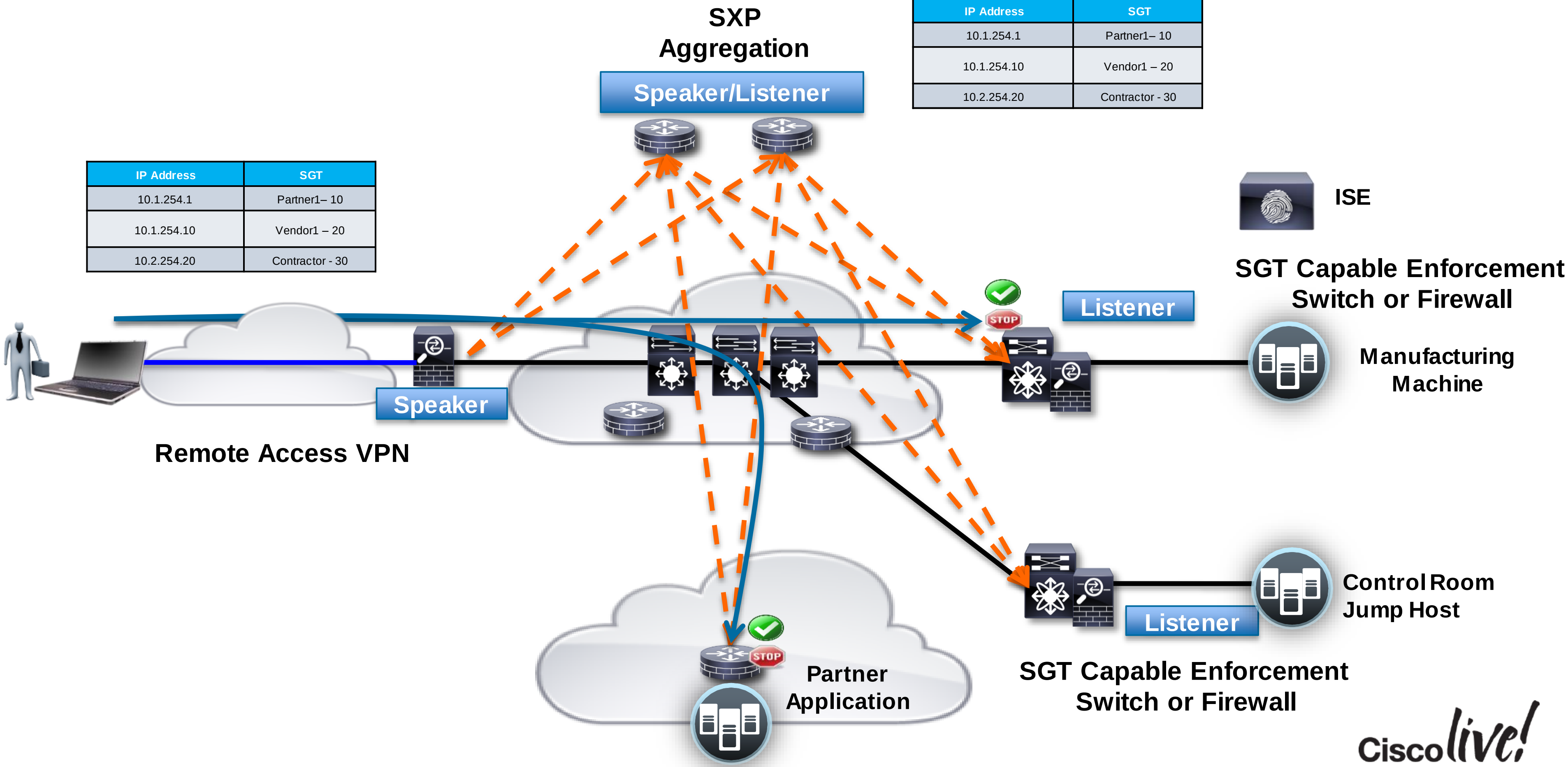
Client Exclusion ☑ Enabled 60 Timeout Value (se

SRC \ DST	Room 1 (10)	Room 2 (20)	Room 3 (30)	Room 4 (40)
Room 1 (10)	Permit	Deny	Deny	Deny
Room 2 (20)	Deny	Permit	Deny	Deny
Room 3 (30)	Deny	Deny	Permit	Deny
Room 4 (40)	Deny	Deny	Deny	Permit

Partner/Vendors/Contractor Access Control

- Business Problem/Background
  - Partners/Vendors/Contractors require access to control systems spread out geographically
  - Distributed Remote Access (RAS) VPN was not scaling and had inconsistent security policy applied
  - With RAS VPN a second level of control into the control system was required. Highly desired to not require “2nd” auth
  - Partners/Vendors/Contractors might have very different security access depending on control system
- Solution Overview
  - Centralised RAS VPN head ends were upgraded to support SXP
  - RAS VPNs communicate IP/SGT to reflector which shared it with each control system access control device (FW or switch depending on size/requirement)

Partner/Vendor/Contractor Access Control

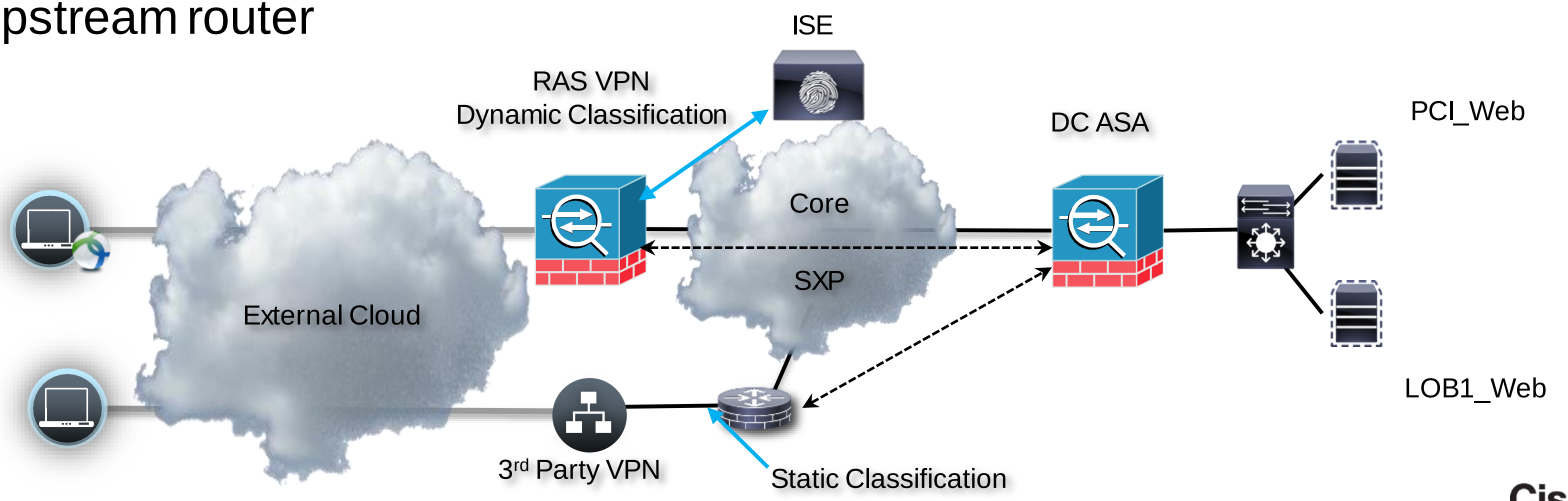


IP Address	SGT
10.1.254.1	Partner1– 10
10.1.254.10	Vendor1 – 20
10.2.254.20	Contractor - 30

IP Address	SGT
10.1.254.1	Partner1– 10
10.1.254.10	Vendor1 – 20
10.2.254.20	Contractor - 30

RAS VPN – Considerations

- ASA supports SGT classification for RAS VPN – Mix and match classifications in the same subnet/DHCP pool if you'd like
- "Most" concentrators allow users/groups to be mapped to specific DHCP pools or VLANs.
- ASA and 3rd party VPN concentrators are supported via Subnet/SGT or L3IF on upstream router



© 2015 Cisco and/or its affiliates. All rights reserved.

ASA RAS VPN Configuration:

- RAS VPN will assign a tag to the end user based on the authz policy matched in ISE when the user logs into the group.
- We then communicate the tag via SXP to the SXP reflector which communicates with enforcement ASA/switches across the company.
- Enforcement ASA/switches will then use the SGT via IP/SGT lookup

```
aaa-server cts-mlist protocol radius
 dynamic-authorization
aaa-server cts-mlist (inside) host 10.1.100.3
 timeout 5
 key TrustSec
 authentication-port 1812
 accounting-port 1813
 radius-common-pw TrustSec
cts server-group cts-mlist
cts sxp enable
cts sxp default password TrustSec
cts sxp default source-ip 10.1.100.20
cts sxp connection peer 10.3.99.2 source 10.1.100.20
password default mode local speaker
```

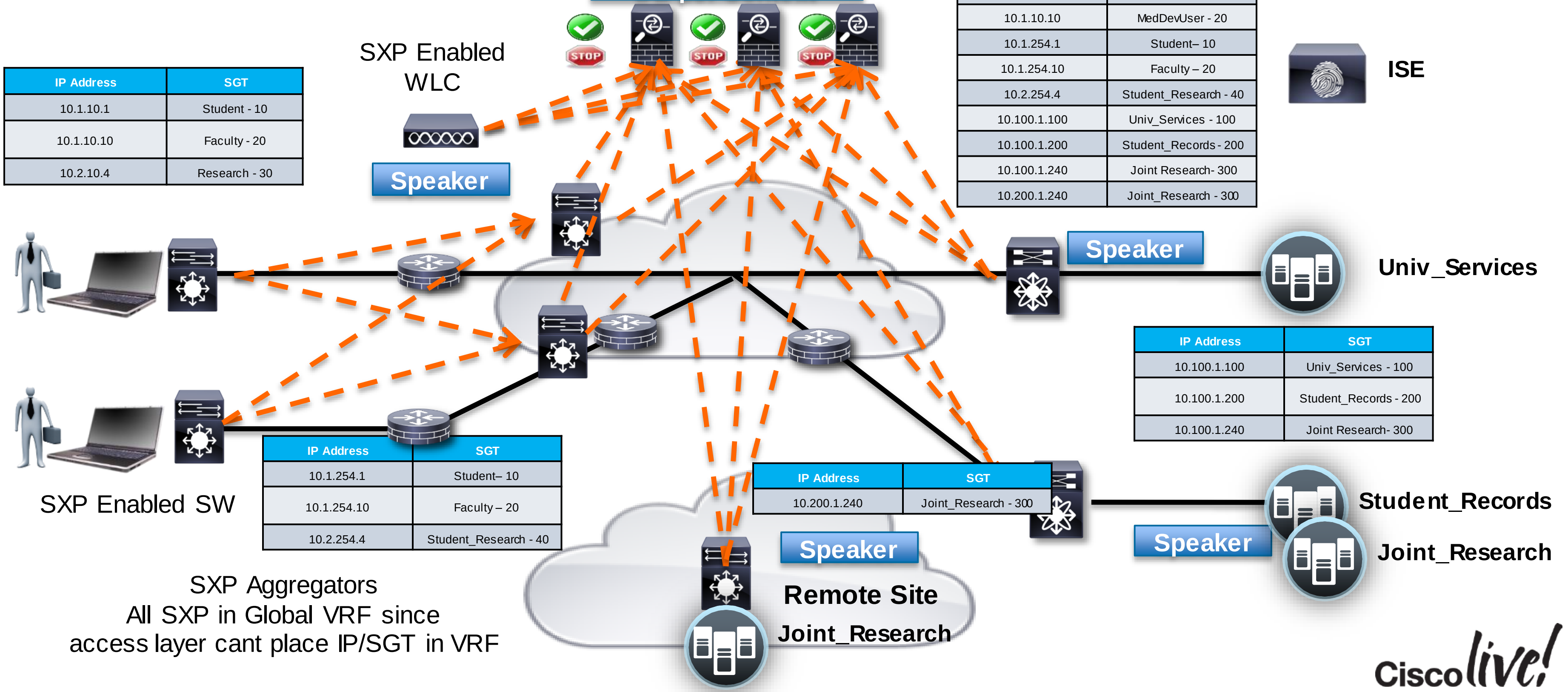
```
group-policy GroupPolicy_cts-local internal
group-policy GroupPolicy_cts-local attributes
 wins-server none
 dns-server value 10.1.100.100
 vpn-tunnel-protocol ssl-client
 default-domain value cts.local
tunnel-group cts-local general-attributes
 address-pool test
 authentication-server-group cts-mlist
 accounting-server-group cts-mlist
 default-group-policy GroupPolicy_cts-local
tunnel-group cts-local webvpn-attributes
 group-alias cts-local enable
```

© 2015 Cisco and/or its affiliates. All rights reserved.

University – Enhancing VRF Segmentation

- Business Problem/Background
  - Univ. policy requires more granular classifications of students, faculty, administration and visiting researchers
  - VRF Segmentation in place and operational with a centralised firewall cross connect
  - Adding more classifications is very costly with VRFs in design and operation
  - Desire to keep opex and design cost low while still providing more granular controls at centralised firewall
- Solution Overview
  - Access Layer of WLC/3750/4500 which can’t do SGACL
  - Cross connect firewall capable of SXP listener from access layer
  - Data Centre Nexus switches advertise application roles to cross connect firewall
- Cross Connect Firewall implements more granular policy via SGFW

University - Enhancing VRF Segmentation



Cross Connect Firewalls

Listener and IP/SGT DB per Context

IP Address	SGT
10.1.10.1	Student - 10
10.1.10.10	Faculty - 20
10.2.10.4	Research - 30
10.1.10.10	MedDevUser - 20
10.1.254.1	Student– 10
10.1.254.10	Faculty – 20
10.2.254.4	Student_Research - 40
10.100.1.100	Univ_Services - 100
10.100.1.200	Student_Records - 200
10.100.1.240	Joint Research- 300
10.200.1.240	Joint_Research - 300

SXP Enabled WLC

Speaker

IP Address	SGT
10.1.10.1	Student - 10
10.1.10.10	Faculty - 20
10.2.10.4	Research - 30

Speaker

Univ_Services

IP Address	SGT
10.100.1.100	Univ_Services - 100
10.100.1.200	Student_Records - 200
10.100.1.240	Joint Research- 300

SXP Enabled SW

IP Address	SGT
10.1.254.1	Student– 10
10.1.254.10	Faculty – 20
10.2.254.4	Student_Research - 40

IP Address	SGT
10.200.1.240	Joint_Research - 300

Speaker

Student_Records

Speaker

Joint_Research

Remote Site

Joint_Research

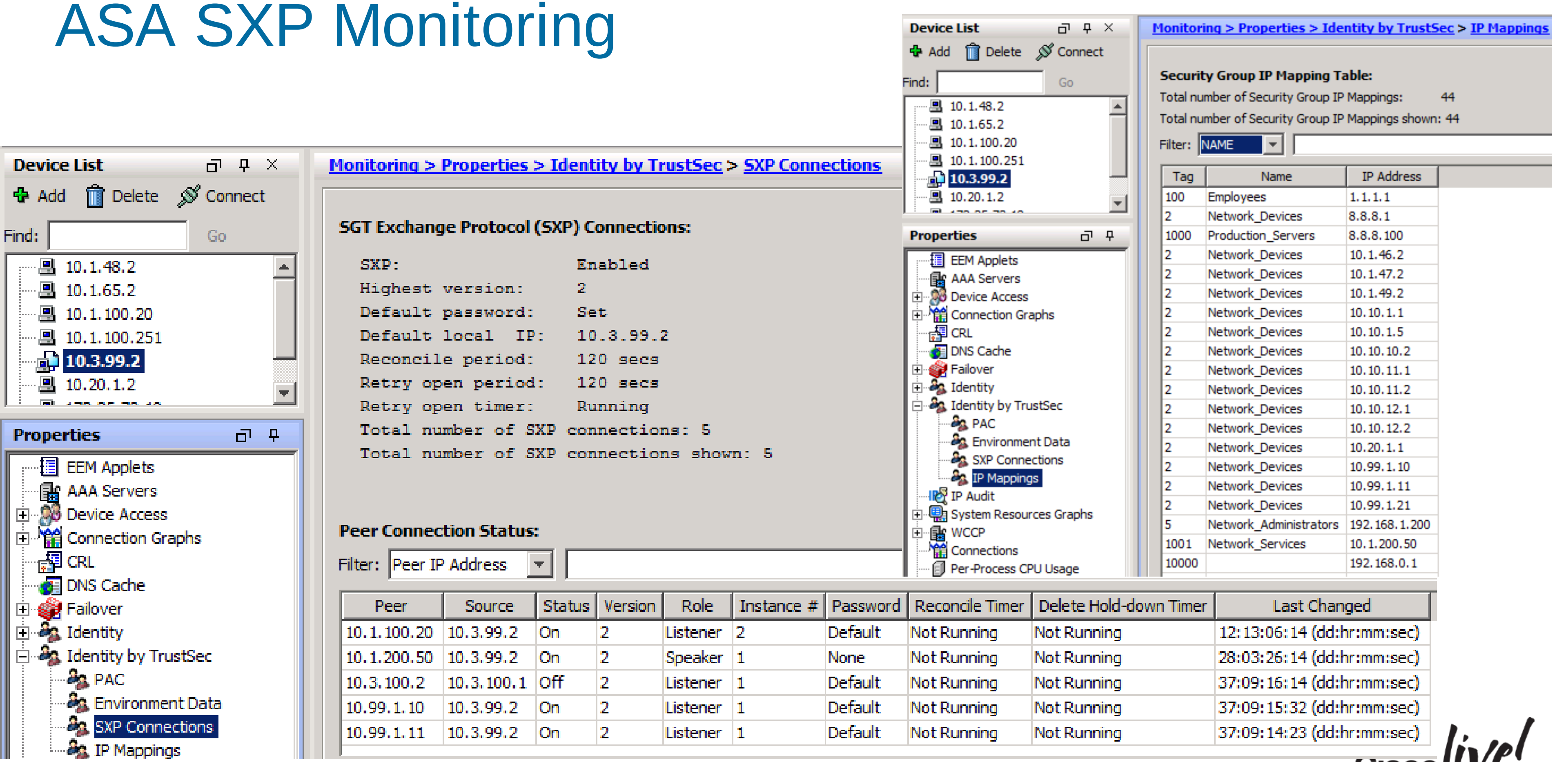
SXP Aggregators
All SXP in Global VRF since
access layer cant place IP/SGT in VRF

© 2015 Cisco and/or its affiliates. All rights reserved.

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 IPv4/IPv6 FW rules on ASA
- IPv6 Device Discovery
  - WLC - still being planned
  - 3750X, 3650, 3850, 5760, 4500
  - 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

ASA SXP Monitoring



Monitoring > Properties > Identity by TrustSec > SXP Connections

SGT Exchange Protocol (SXP) Connections:

```
SXP:                    Enabled
Highest version:        2
Default password:       Set
Default local  IP:      10.3.99.2
Reconcile period:       120 secs
Retry open period:      120 secs
Retry open timer:       Running
Total number of SXP connections: 5
Total number of SXP connections shown: 5
```

Peer Connection Status:

Filter: Peer IP Address

Peer	Source	Status	Version	Role	Instance #	Password	Reconcile Timer	Delete Hold-down Timer	Last Changed
10.1.100.20	10.3.99.2	On	2	Listener	2	Default	Not Running	Not Running	12:13:06:14 (dd:hr:mm:sec)
10.1.200.50	10.3.99.2	On	2	Speaker	1	None	Not Running	Not Running	28:03:26:14 (dd:hr:mm:sec)
10.3.100.2	10.3.100.1	Off	2	Listener	1	Default	Not Running	Not Running	37:09:16:14 (dd:hr:mm:sec)
10.99.1.10	10.3.99.2	On	2	Listener	1	Default	Not Running	Not Running	37:09:15:32 (dd:hr:mm:sec)
10.99.1.11	10.3.99.2	On	2	Listener	1	Default	Not Running	Not Running	37:09:14:23 (dd:hr:mm:sec)

Monitoring > Properties > Identity by TrustSec > IP Mappings

Security Group IP Mapping Table:

Total number of Security Group IP Mappings: 44

Total number of Security Group IP Mappings shown: 44

Filter: NAME

Tag	Name	IP Address
100	Employees	1.1.1.1
2	Network_Devices	8.8.8.1
1000	Production_Servers	8.8.8.100
2	Network_Devices	10.1.46.2
2	Network_Devices	10.1.47.2
2	Network_Devices	10.1.49.2
2	Network_Devices	10.10.1.1
2	Network_Devices	10.10.1.5
2	Network_Devices	10.10.10.2
2	Network_Devices	10.10.11.1
2	Network_Devices	10.10.11.2
2	Network_Devices	10.10.12.1
2	Network_Devices	10.10.12.2
2	Network_Devices	10.20.1.1
2	Network_Devices	10.99.1.10
2	Network_Devices	10.99.1.11
2	Network_Devices	10.99.1.21
5	Network_Administrators	192.168.1.200
1001	Network_Services	10.1.200.50
10000		192.168.0.1

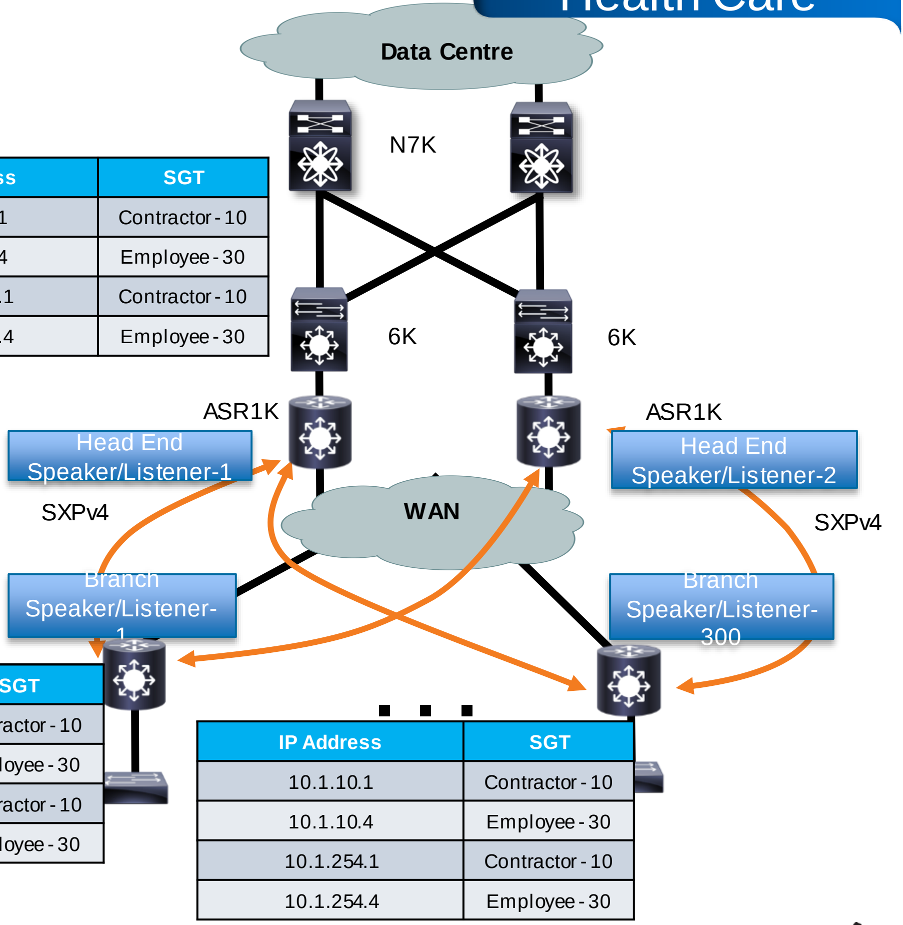
Health Care Access Control - Medical Devices

- Business Problem/Background
  - Isolate Medical Devices used for Patient Care
  - Only authorised users, devices, and servers access to the medical devices
- Solution Overview
  - Access Layer of 3650/3850 – Distribution/Core does not support SGT
  - Access Layer capable of bidirectional SXP and filtering on IP/SGT
  - 3650/3850 have limited resource for IP/SGT (12K) and can’t hold all users in the network
    - Resolved this by only applying SGT to users of medical device, and servers explicitly allowed access
    - All user or end devices on network that don’t get an SGT assigned do not populate the IP/SGT in SXP. This means only explicitly known users and end devices get an IP/SGT
    - This keeps the SXP total IP/SGT well under 12K for this particular network
  - This allows the policy to be Known_SGT <-> Known_SGT = Permit and all Unknown_SGT <-> Known_SGT = Deny (some times referred to as a Whitelist Model)

Health Care

SXPv4 Design Discussion

- Bidirectional SXP with Loop Detection
- Allows ASR1K to be an IP/SGT aggregator/reflector from remote to remote
- Review scale for remotes since SXP is a fully replication model
- Aggregator/Reflector can be inline of traffic
- ISRG2 – 15.3(2)T
- ASR1K- IOS XE 3.9
- ISR44xx – IOS XE at model introduc
- Cat6K(SUP 2T) – 15.1(1)SY
- 3650/3850/4500 – IOS XE 3.6


Data Centre
N7K
6K
6K
ASR1K
ASR1K
Head End Speaker/Listener-1
Head End Speaker/Listener-2
SXPv4
SXPv4
WAN
Branch Speaker/Listener-1
Branch Speaker/Listener-300
. . .

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

© 2015 Cisco and/or its affiliates. All rights reserved.

Bidirectional SXP WAN Scaling

- From previous slide - SXP is a full replication model – each remote router will learn all IP/SGT bindings with this approach
- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/asr1000/sec-usr-cts-xe-3s-asr-

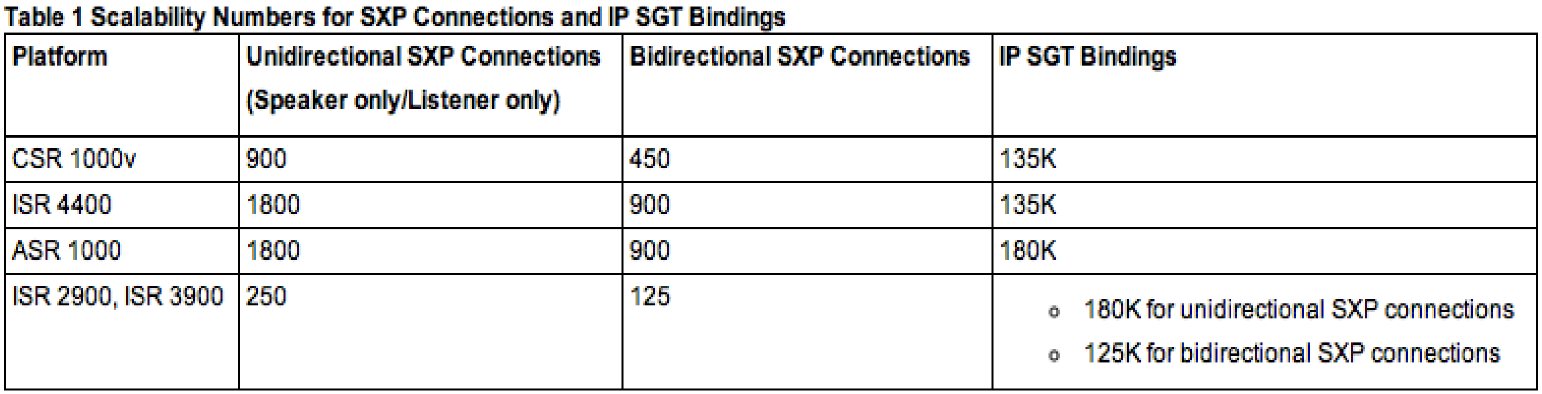


Table 1 Scalability Numbers for SXP Connections and IP SGT Bindings

Platform	Unidirectional SXP Connections (Speaker only/Listener only)	Bidirectional SXP Connections	IP SGT Bindings
CSR 1000v	900	450	135K
ISR 4400	1800	900	135K
ASR 1000	1800	900	180K
ISR 2900, ISR 3900	250	125	○ 180K for unidirectional SXP connections ○ 125K for bidirectional SXP connections

More SXP Scaling Information

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

* M series line cards - 200K expected in NX-OS 7.0

** Guideline – scaling higher is supported

*** - remember to halve for bidirectional

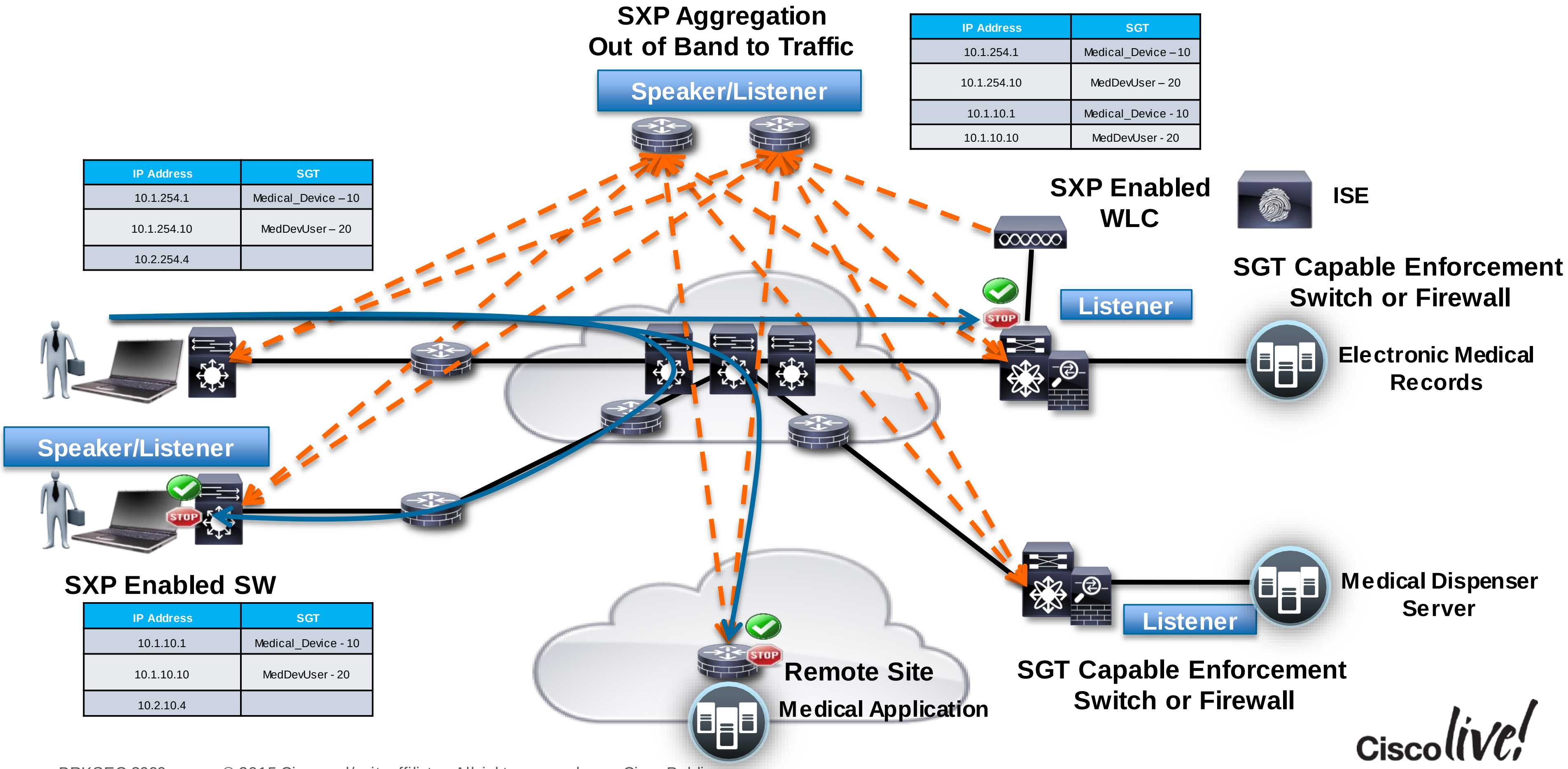
**** - 4000 reserved for Subnet/SGT

Nexus 7000 IP/SGT Scaling By Line Card

- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/verified_scalability/b_Cisco_Nexus_7000_Series_NX-OS_Verified_Scalability_Guide.html

Feature	Parameter	Verified Limit (Cisco NX-OS 6.2)	Verified Limit (Cisco NX-OS 6.1)	Verified Limit (Cisco NX-OS 6.0)	Verified Limit (Cisco NX-OS 5.2)
Cisco TrustSec	Number of IP-SGT mappings for M1/M2 I/O module	50,000	Not tested	Not tested	Not tested
	Number of IP-SGT mappings for F2/F2e I/O module	32,000	Not tested	Not tested	Not tested
	Number of IP-SGT mappings for F3 I/O module	64,000	Not tested	Not tested	Not tested
	Number of SXP connections	980	Not tested	Not tested	Not tested
	Number of IP-SGT mappings learned using SXP	50,000	Not tested	Not tested	Not tested
	Number of SGT Groups	3,000 SGT/DGT	Not tested	Not tested	Not tested

Access Control – Health Care Medical Devices



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

IP Address	SGT
10.1.254.1	Medical_Device – 10
10.1.254.10	MedDevUser – 20
10.2.254.4	

IP Address	SGT
10.1.10.1	Medical_Device - 10
10.1.10.10	MedDevUser - 20
10.2.10.4	

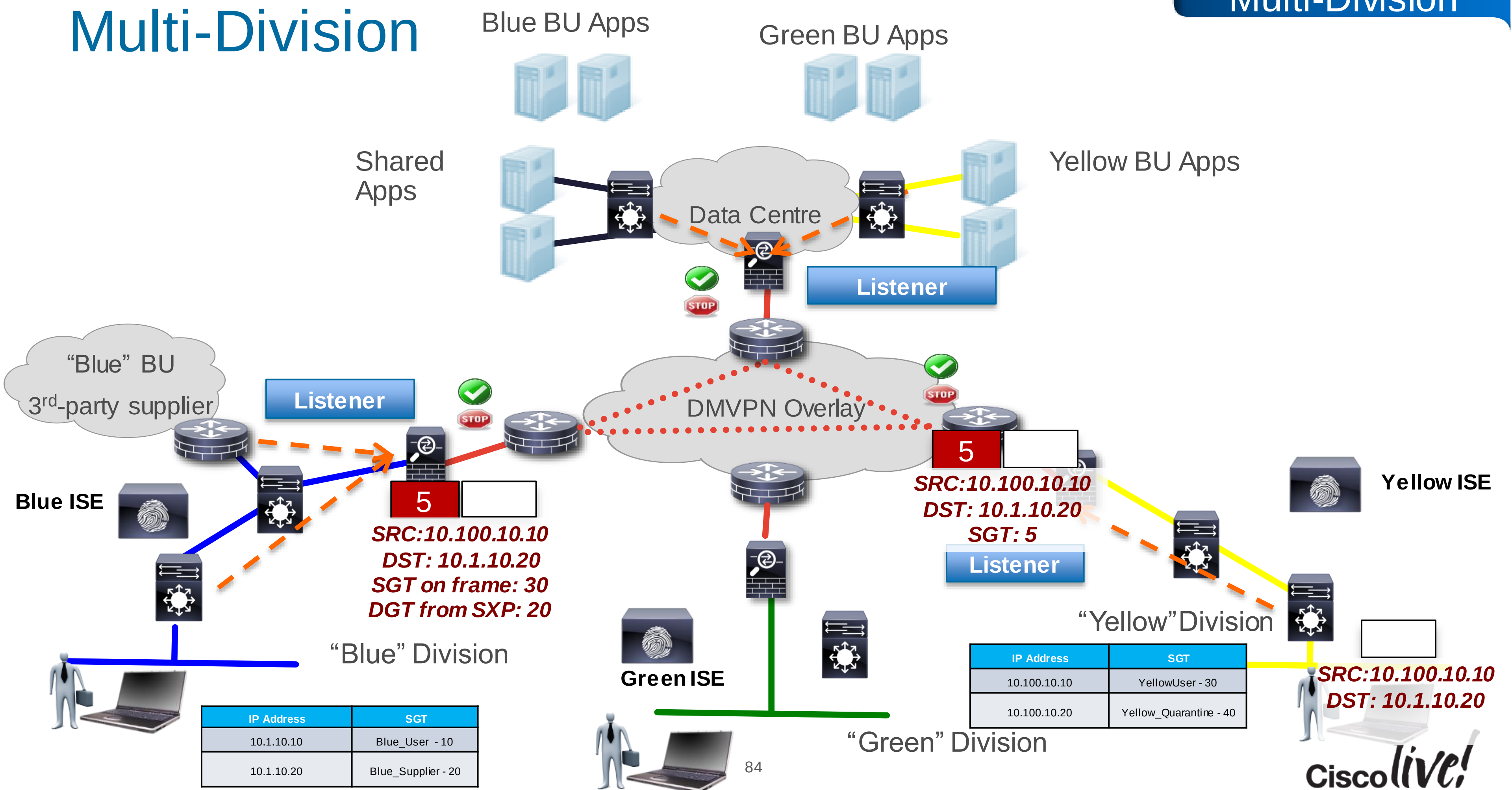
© 2015 Cisco and/or its affiliates. All rights reserved.

Multi-Division Organisation Access Control

- Business Case
  - Many labs had security incidents that exploited the open transit backbone of the organisation
  - Regulations for governments and financials required more segmentation of the network
  - Limit transit network for divisions on core;
  - Keep Isolated domains for network and security operations
- Solution
  - Use DMVPN isolation on backbone
  - Use ISE in divisions to classify in each division and across divisions
  - Use FWs at Divisions Edges to permit/deny division traffic
  - ASA receives SXP from Division switches
  - ASA tags to DMVPN router and DMVPN router carries SGT to destination division FW
    - Allows us to work around ASA needing src/dest match in rules
    - Allows Divisions to not upgrade all devices and still benefit

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multi-Division



SRC:10.100.10.10
DST: 10.1.10.20
SGT on frame: 30
DGT from SXP: 20

SRC:10.100.10.10
DST: 10.1.10.20
SGT: 5

SRC:10.100.10.10
DST: 10.1.10.20

IP Address	SGT
10.1.10.10	Blue_User - 10
10.1.10.20	Blue_Supplier - 20

IP Address	SGT
10.100.10.10	YellowUser - 30
10.100.10.20	Yellow_Quarantine - 40

© 2015 Cisco and/or its affiliates. All rights reserved.

ASA Native Tagging Configuration:

- Native Tag configuration need only on the OUTSIDE interface – Firewall rules are written to permit traffic from the outside to the inside (SGT->DGT). To get tags to the firewall for DGT we must still utilise SXP.

```
ASA5515X-A(config)# int g0/0
ASA5515X-A(config-if)# nameif outside
ASA5515X-A(config-if)# cts manual
ASA5515X-A(config-if)# policy static sgt 2 trusted
ASA5515X-A(config-if)# ip address 10.3.99.2 255.255.255.0

! SXP configuration doesn’t change for this use case
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 10.3.99.2
cts sxp connection peer 10.99.10.10 password default mode local listener
cts sxp connection peer 10.1.100.20 source 10.3.99.2 password default mode local listener
cts sxp connection peer 10.99.10.11 password default mode local listener
cts sxp connection peer 10.3.100.2 source 10.3.100.1 password default mode local listener
cts sxp connection peer 10.1.200.50 password none mode local listener
```

Configure Links for SGT Tagging

CTS Manual no encryption

```
Interface GigabitEthernet1/5
 mtu 9216*
 cts manual
  policy static sgt 2 trusted
```

- *increase MTU to take into account encryption and/or SGT overhead
- port-channel support - cts is configured on the physical interface then added to the port channel

```
ASR1K-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

Multi-Division

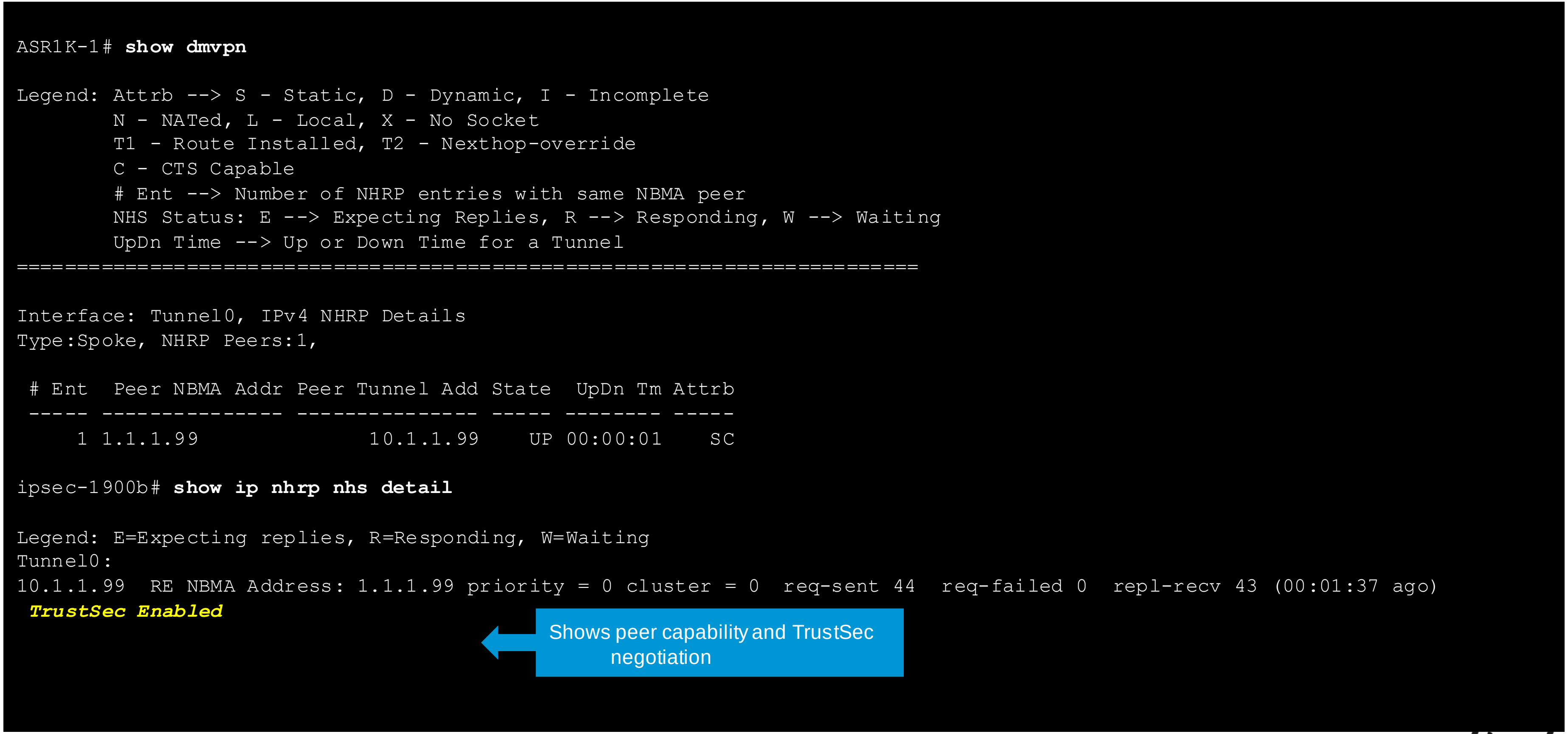
SGT DMVPN Inline Tagging Config

```
ASR1K-1#
cts role-based sgt-map 9.9.9.1 sgt 5000
cts role-based sgt-map 11.11.11.1 sgt 65533
!
crypto ikev2 proposal p1
 encryption 3des
 integrity md5
 group 2
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer v4
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof3
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
!
cts sgt inline
!
crypto ipsec transform-set trans esp-3des esp-sha-hmac
! (……………….continued in next slide)
```

CTS infra CLI used to configure IP->SGT mapping

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

SGT DMVPN – Show Commands



```
ASR1K-1# show dmvpn

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

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

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

ipsec-1900b# show ip nhrp nhs detail

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

Shows peer capability and TrustSec negotiation

© 2015 Cisco and/or its affiliates. All rights reserved.

Multi-Division

How do I know if I am Tagging? SGT and Flexible NetFlow (FNF)

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

flow exporter EXP1
 destination 10.2.44.15
 source GigabitEthernet3/1

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

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

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

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

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

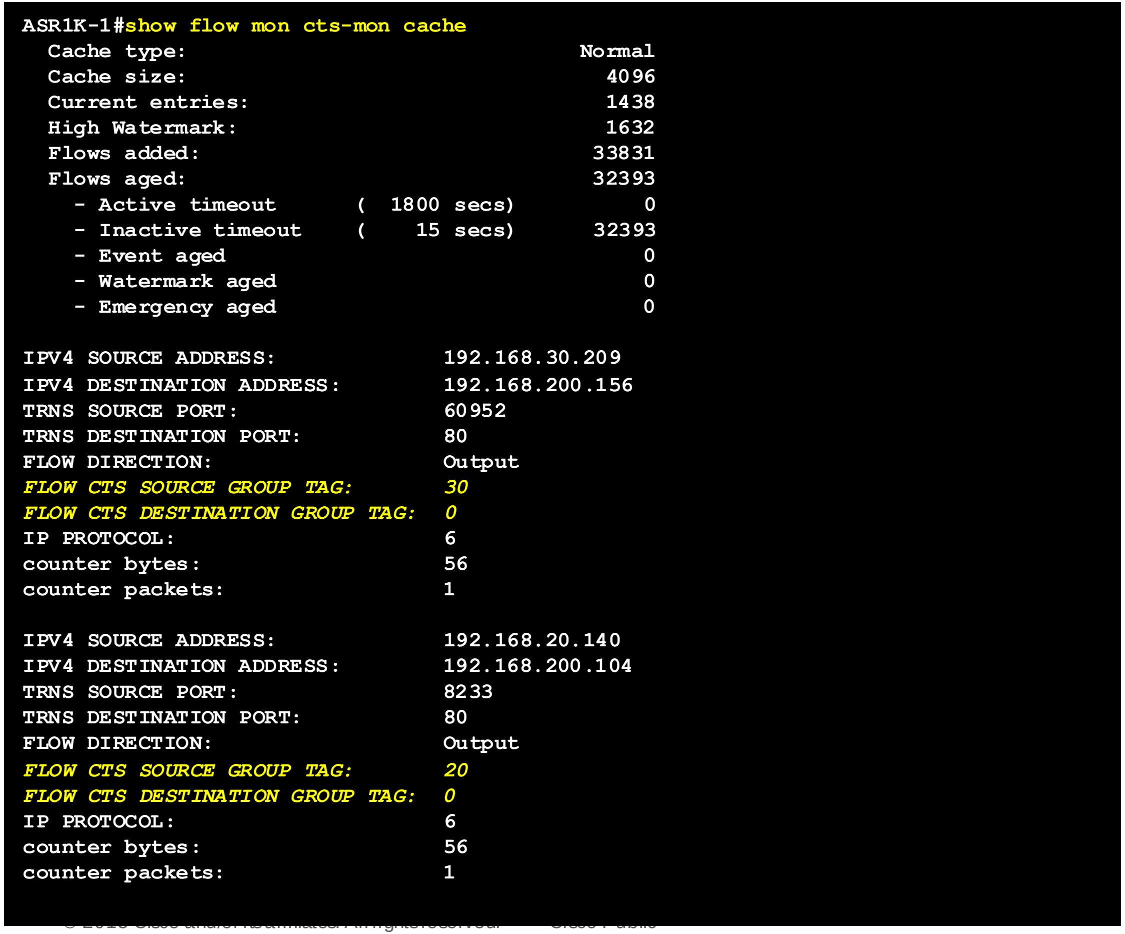
```
cts role-based ip flow mon cts-mon dropped
```

*Optional – will create flows for only Role-based ACL drops
Cat6K/Sup2T

© 2015 Cisco and/or its affiliates. All rights reserved.

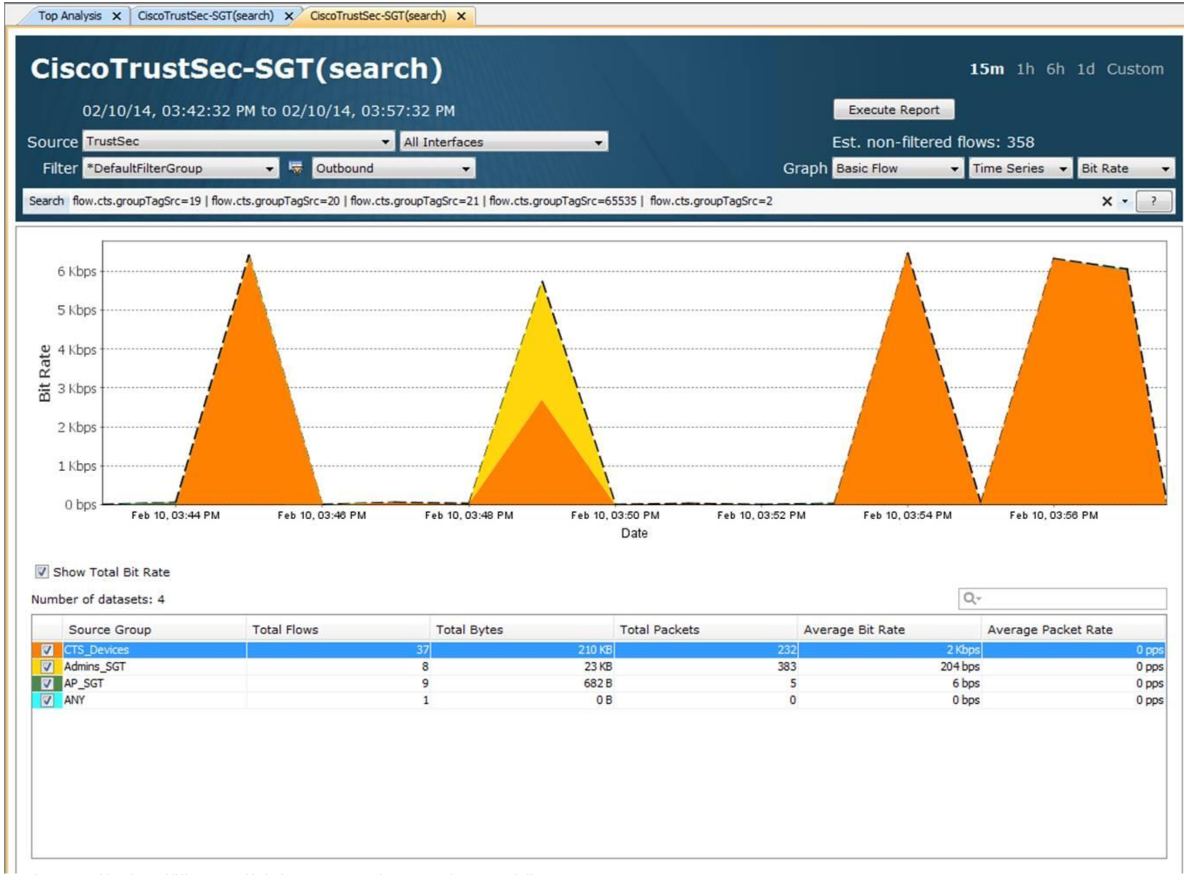
Multi-Division

Monitoring SGT/FNF Flow Cache Example



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

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

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

Live Action – Netflow with SGT Support



CiscoTrustSec-SGT(search)

02/10/14, 03:42:32 PM to 02/10/14, 03:57:32 PM

Source: TrustSec | All Interfaces

Filter: *DefaultFilterGroup | Outbound

Est. non-filtered flows: 358

Graph: Basic Flow | Time Series | Bit Rate

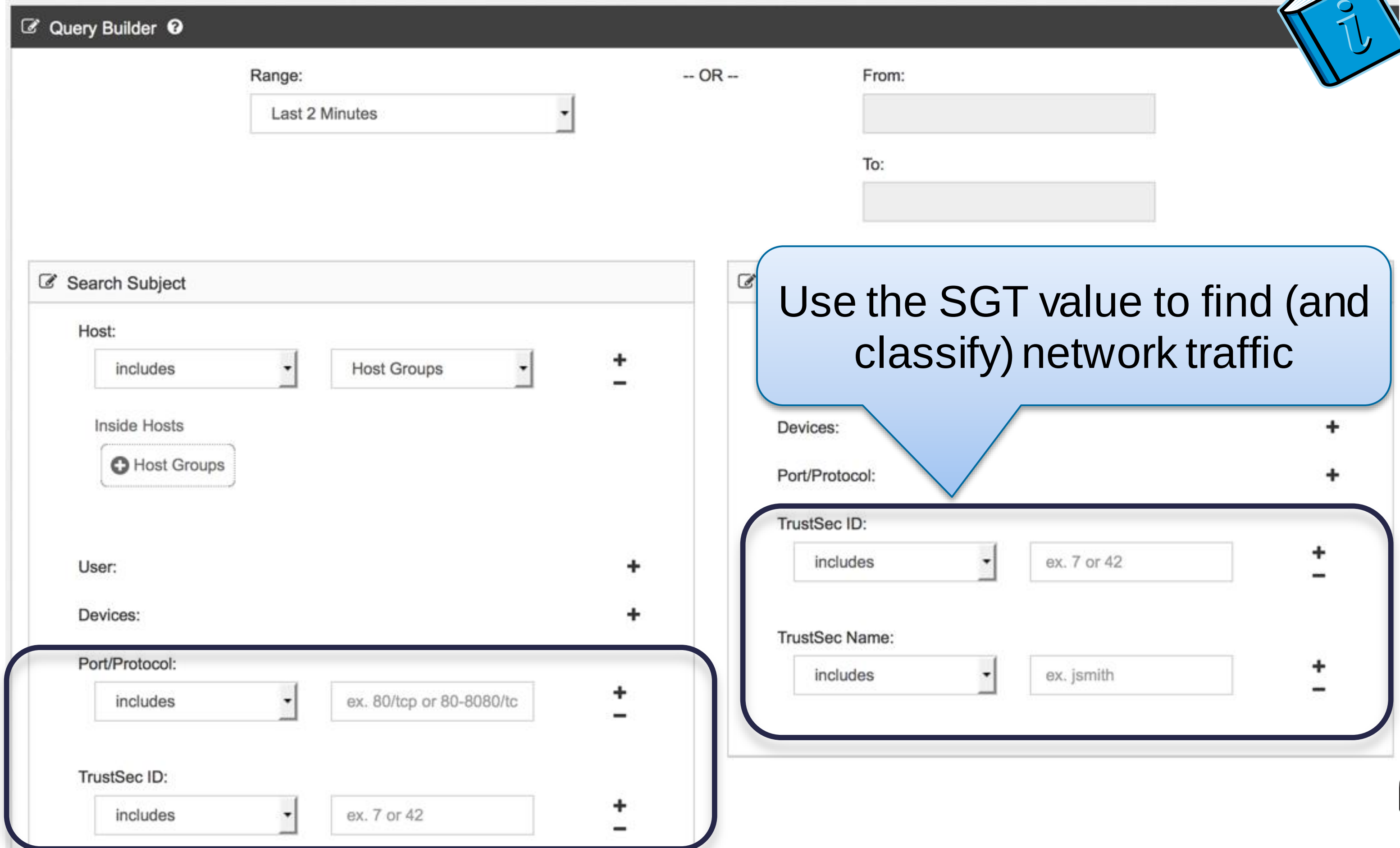
Search: flow.cts.groupTagSrc=19 | flow.cts.groupTagSrc=20 | flow.cts.groupTagSrc=21 | flow.cts.groupTagSrc=65535 | flow.cts.groupTagSrc=2

☑ Show Total Bit Rate

Number of datasets: 4

	Source Group	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate
☑	CTS_Devices	37	210 KB	232	2 Kbps	0 pps
☑	Admins_SGT	8	23 KB	383	204 bps	0 pps
☑	AP_SGT	9	682 B	5	6 bps	0 pps
☑	ANY	1	0 B	0	0 bps	0 pps

Lancope Flow Query



Query Builder

Range: Last 2 Minutes

-- OR --

From:

To:

Search Subject

Host: includes | Host Groups

Inside Hosts

Host Groups

User:

Devices:

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

TrustSec ID: includes | ex. 7 or 42

Devices:

Port/Protocol:

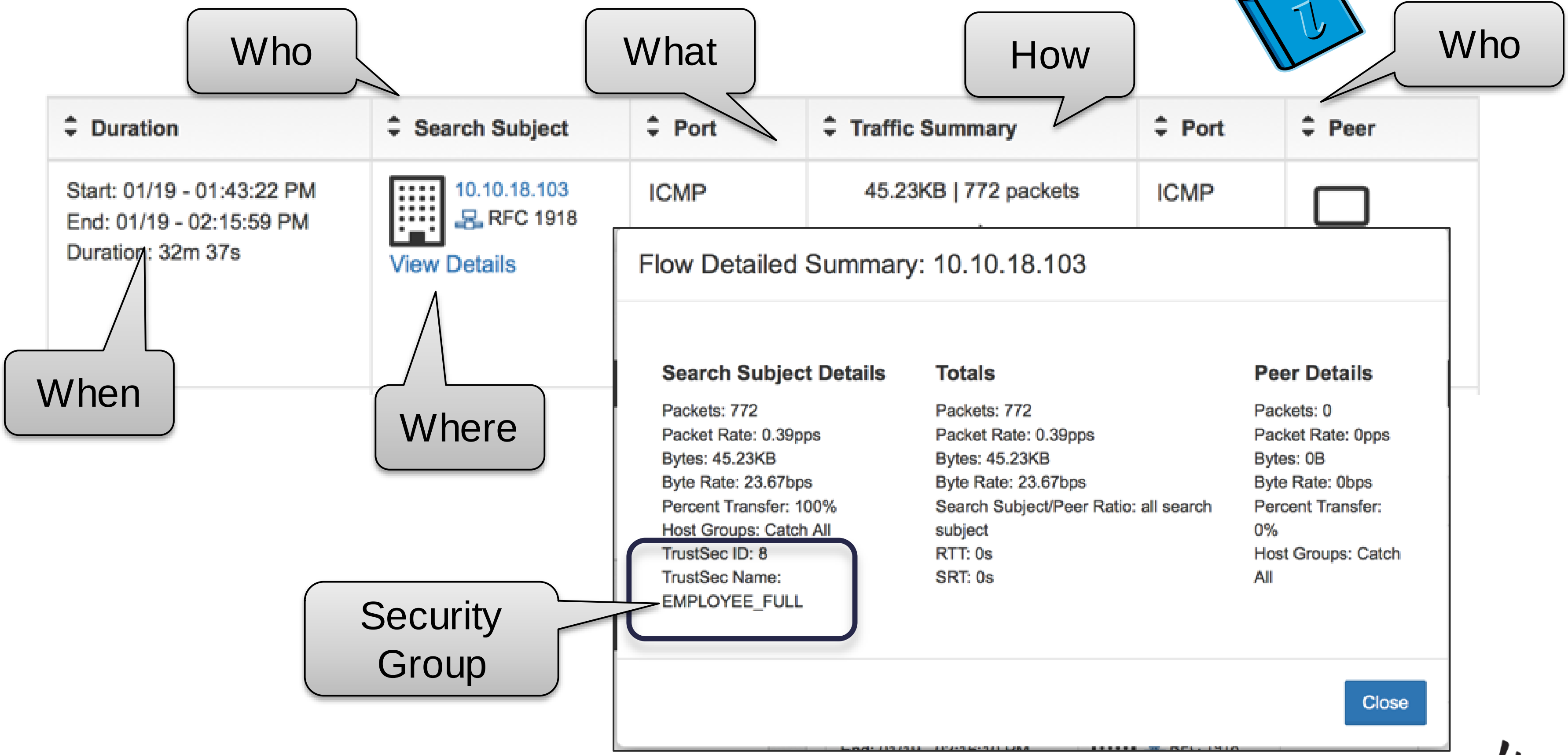
TrustSec ID: includes | ex. 7 or 42

TrustSec Name: includes | ex. jsmith

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

Multi-Division

Lancope Conversational Flow Record



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

Flow Detailed Summary: 10.10.18.103

Search Subject Details

Packets: 772
Packet Rate: 0.39pps
Bytes: 45.23KB
Byte Rate: 23.67bps
Percent Transfer: 100%
Host Groups: Catch All
TrustSec ID: 8
TrustSec Name: EMPLOYEE_FULL

Totals

Packets: 772
Packet Rate: 0.39pps
Bytes: 45.23KB
Byte Rate: 23.67bps
Search Subject/Peer Ratio: all search subject
RTT: 0s
SRT: 0s

Peer Details

Packets: 0
Packet Rate: 0pps
Bytes: 0B
Byte Rate: 0bps
Percent Transfer: 0%
Host Groups: Catch All

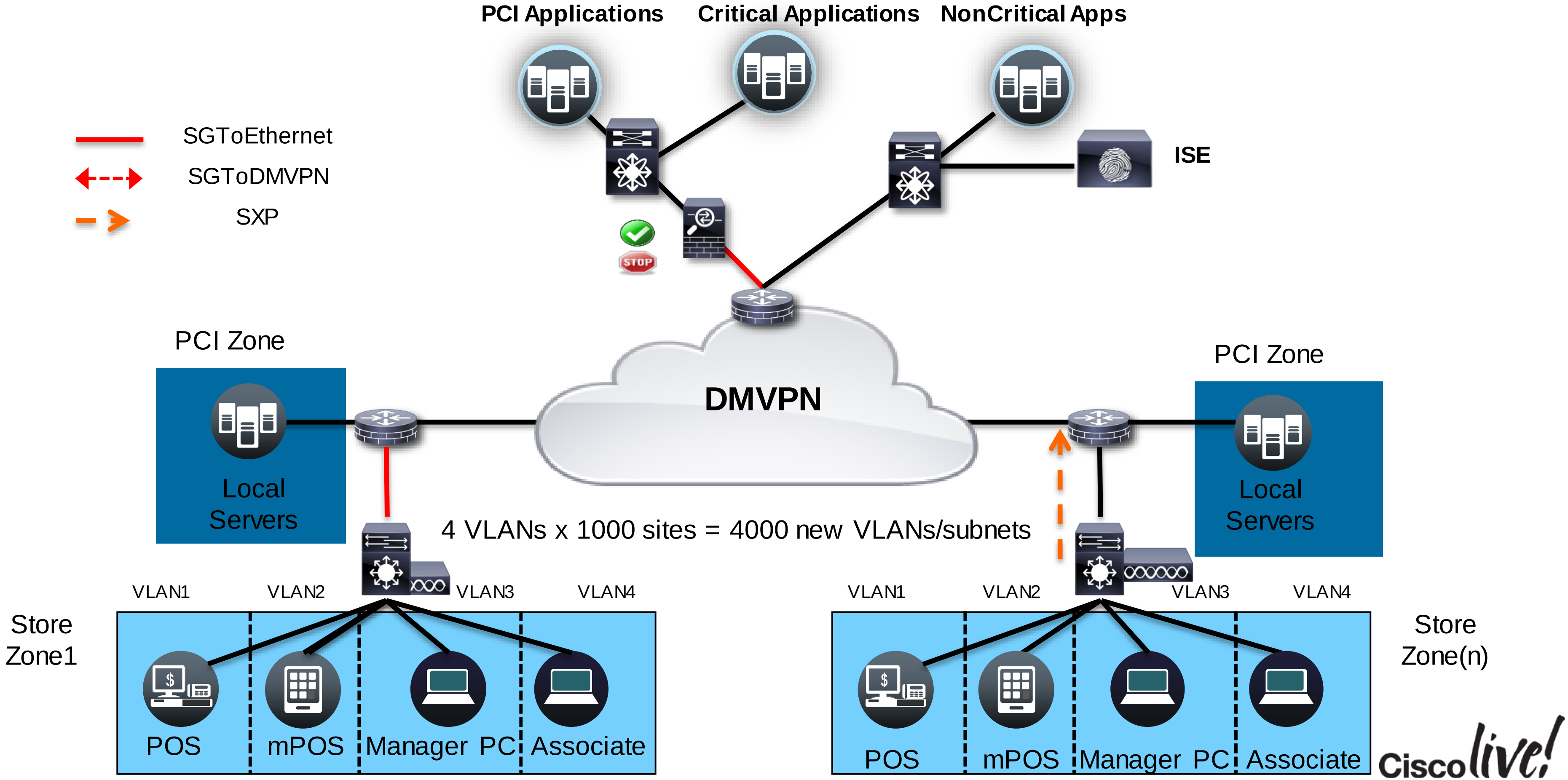
Close

© 2015 Cisco and/or its affiliates. All rights reserved.

Retail Access Control

- Business Problem/Background
  - Regulations for governments and financials required more segmentation of the network – PCI is the most notable branch requirement
  - Existing AD agent for users in main campus, but mobile proliferation requires better mobile classification
  - The branch environment is highly summarised and introducing new VLANs/subnets would require substantial capex/opex to redesign
  - Existing ACLs in branch opex needed to be lowered
- Solution Overview
  - Refreshed Network – All SGACL and Tagging Capable in the future
  - DMVPN for transport from store to data centre and store to store
  - Combination of SXP and inline SGT within store depending on rollout of new infrastrucutre
  - Store to DC would use SGT while campus would continue to use AD agent on ASA

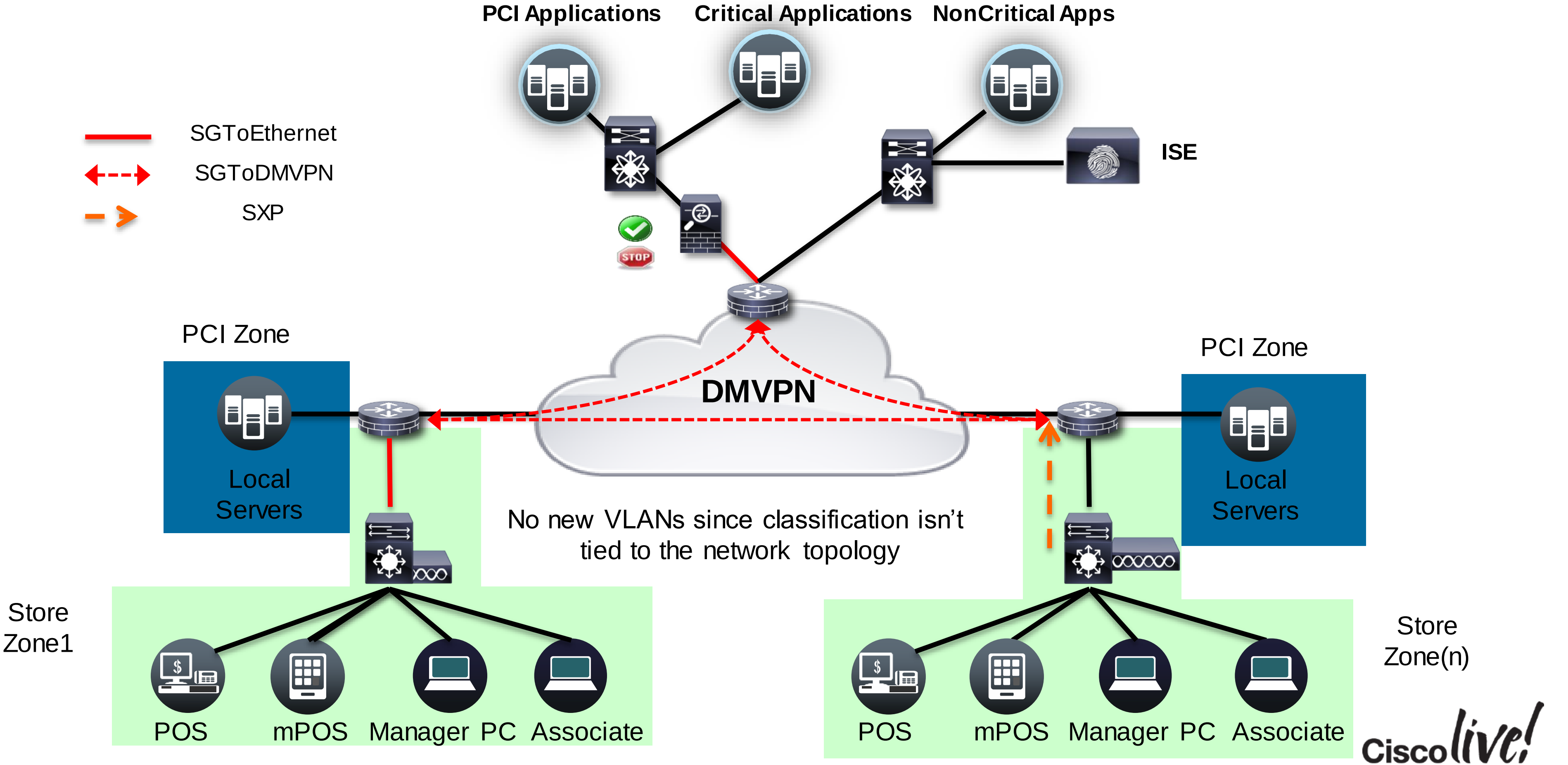
Retail Access Control – Traditional VLAN Structure



4 VLANs x 1000 sites = 4000 new VLANs/subnets

© 2015 Cisco and/or its affiliates. All rights reserved.

Retail Access Control - DMVPN

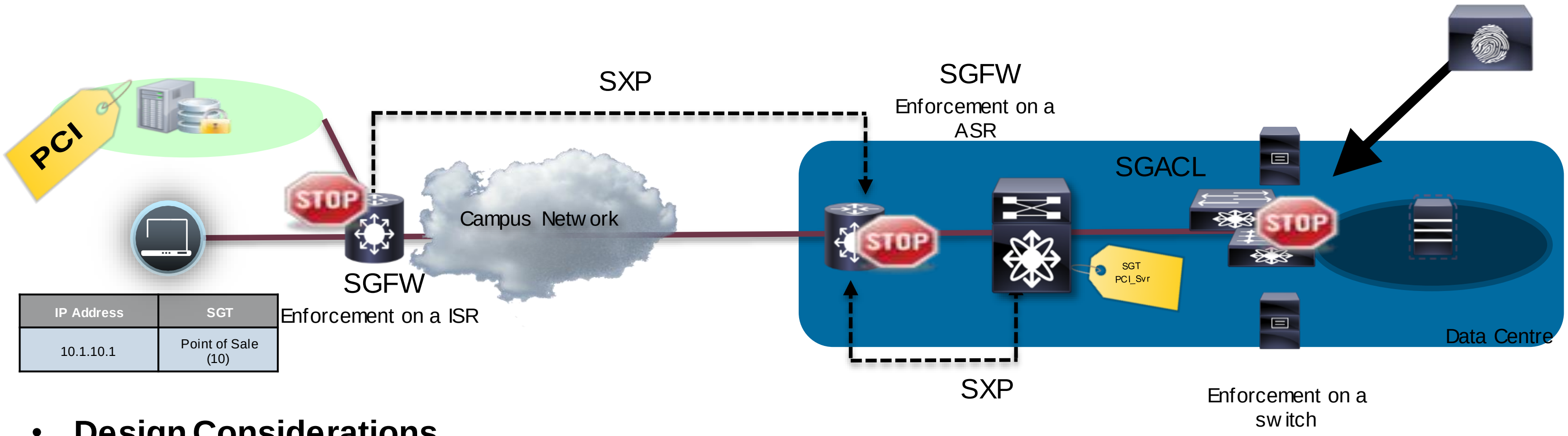


No new VLANs since classification isn't tied to the network topology

© 2015 Cisco and/or its affiliates. All rights reserved.

Retail

SGFW ISR/ASR Design Considerations

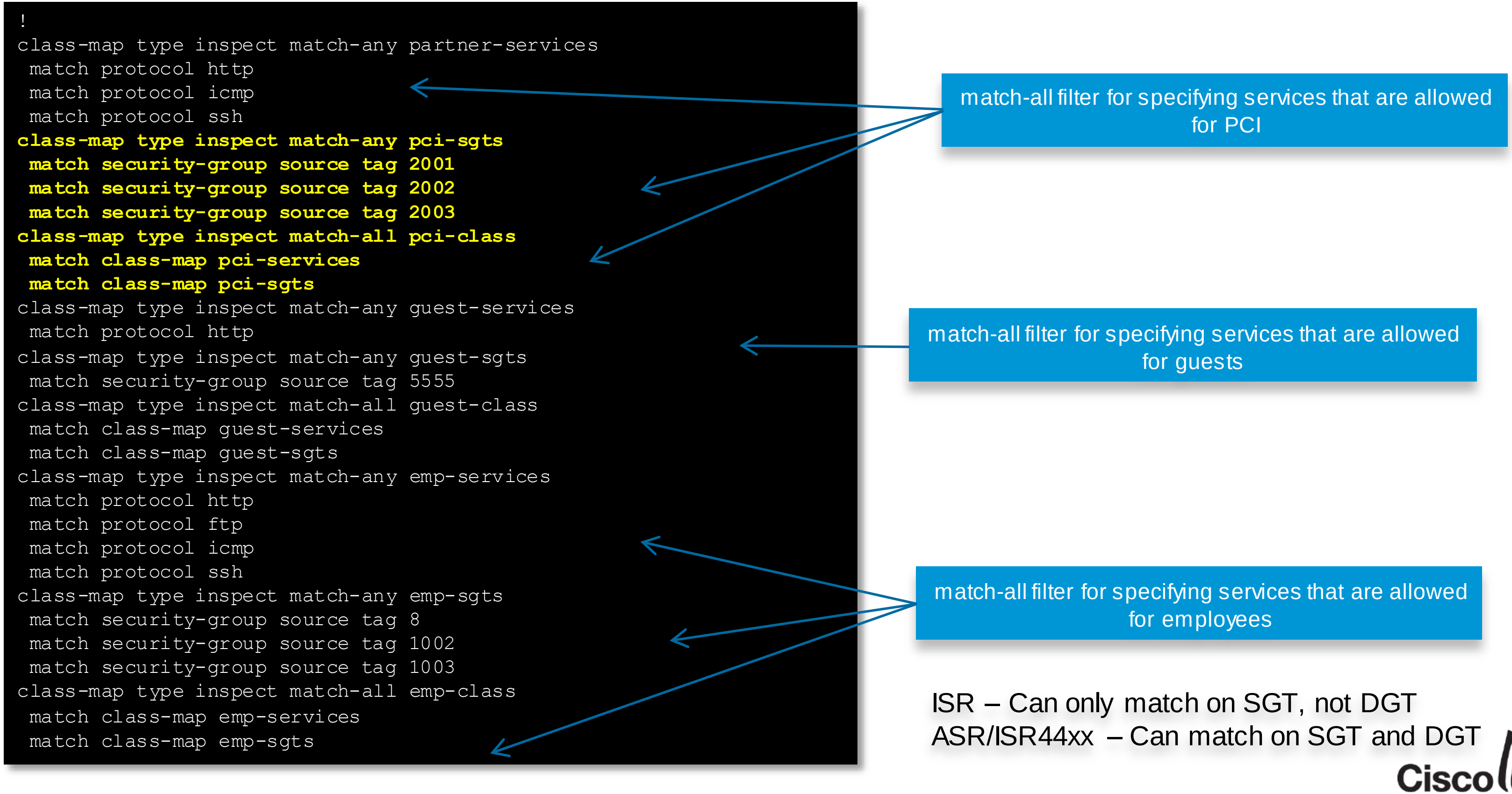


IP Address	SGT
10.1.10.1	Point of Sale (10)

- **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***
  - **SGT allows more dynamic classification in the branch and DC WAN edge**
    - **SGT only used in the *<u>source</u>* for ISR IOS Classic platforms**
    - **SGT can be <u>source and destination</u> on ASR/ISR44xx IOS-XE platforms**
  - **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

Retail

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/ISR44xx – Can match on SGT and DGT

ISR G2 SGFW Configuration

```
!
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
   no propagate sgt
!
```

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

On IOS-XE platforms (ASR1K, 44xx) "cts manual" is required on the interface for SGFW to function regardless of inline tagging.
** don't forget "no propagate sgt **

Data Centre Access Control/Segmentation

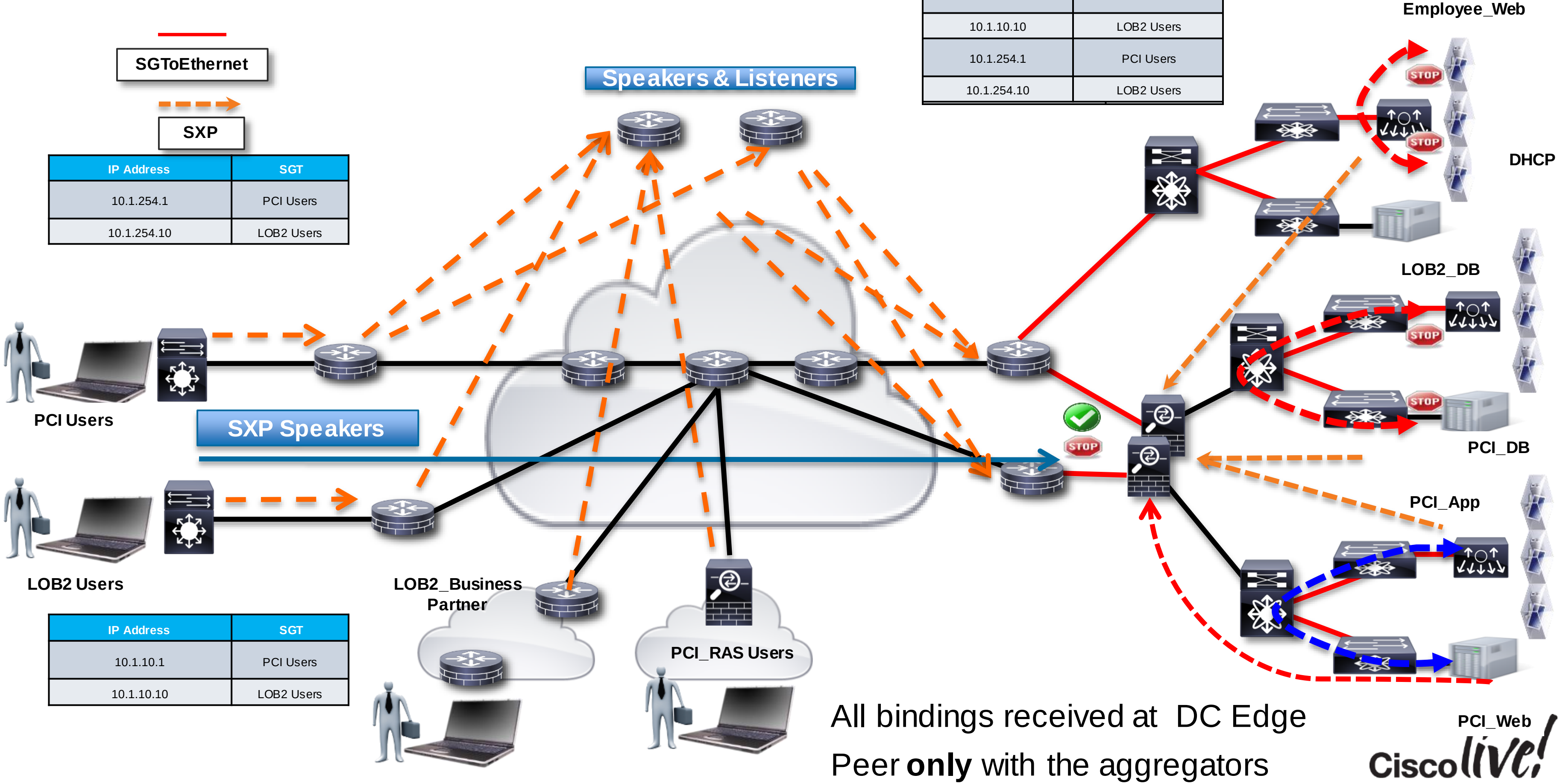
- Business Problem/Background
  - New Business Risk and regulatory concerns requires the business to implement security controls for users to the data centre and within the data centre
  - Users should only be allowed to base services and corresponding line of business applications
  - Applications should be segregated by Line of Business as well as restricted within the line of business.
  - Heavily leveraging partner/contractors/outsourcing for application and other services.
- Solution Overview
  - User to Data Centre Access is handles via SXP for wired, wireless, RAS VPN, and dedicated partner VPN
  - Line of Business (LOB) and PCI
    - Inter LOB handled at FW (between LOBs)
    - Intra LOB handed at N1KV/N7K/N5K (within the LOB)
  - Allow partner/contractors/outsourcing policies in a more automated fashion

Data Centre Details

- SXP scale on ASA and N7K is insufficient, so we need to change change from IP/SGT to SGToEthernet. SGToEthernet to ASA and N7K for shared services.
- ASA cannot do SGT caching, so in net effect it can only receive SGToEthernet on the outside interface for Source Group Tag derivation.
- ASA can do Destination Group Tag derivation by receiving SXP from the data centre switches
- ASA can optionally propagate the SGT to the DC switches – SGFW and SGACL need to be in sync
  - If ASA says “Employee is allowed to LOB1 Web App” then the SGACL needs to allow the same Access and vice versa
- N7K will enforce policy access to common_services (AD, DNS, DHCP)
  - VPC supported with IP/SGT received via IP/SGT CLI or SXP

© 2015 Cisco and/or its affiliates. All rights reserved.

Data Centre End State



IP Address	SGT
10.1.10.1	PCI Users
10.1.10.10	LOB2 Users
10.1.254.1	PCI Users
10.1.254.10	LOB2 Users

IP Address	SGT
10.1.254.1	PCI Users
10.1.254.10	LOB2 Users

IP Address	SGT
10.1.10.1	PCI Users
10.1.10.10	LOB2 Users

All bindings received at DC Edge

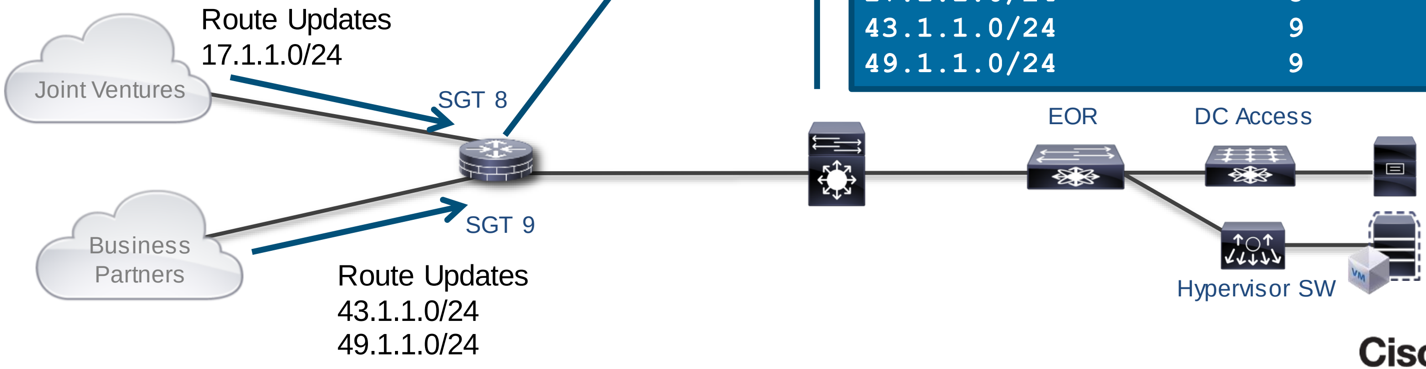
Peer **only** with the aggregators

© 2015 Cisco and/or its affiliates. All rights reserved.

Layer 3 Interface to SGT – L3IF

- Route Prefix Monitoring on a specific Layer 3 Port with mapping to the associate SGT
- Can be applied to Layer 3 interfaces regardless of the underlying physical interface:
  - Routed port, SVI (VLAN interface), Layer 3 subinterface of a Layer2 port , Tunnel interface
  - Makes the prefixes available for export in SXP
- ISR/ASR1K/Cat6K

```
ASR1K#show cts role-based sgt-map all
Active IP-SGT Bindings Information
IP Address                  SGT     Source
========================================
11.1.1.2                    2       INTERNAL
12.1.1.2                    2       INTERNAL
13.1.1.2                    2       INTERNAL
17.1.1.0/24                 8       L3IF
43.1.1.0/24                 9       L3IF
49.1.1.0/24                 9       L3IF
```

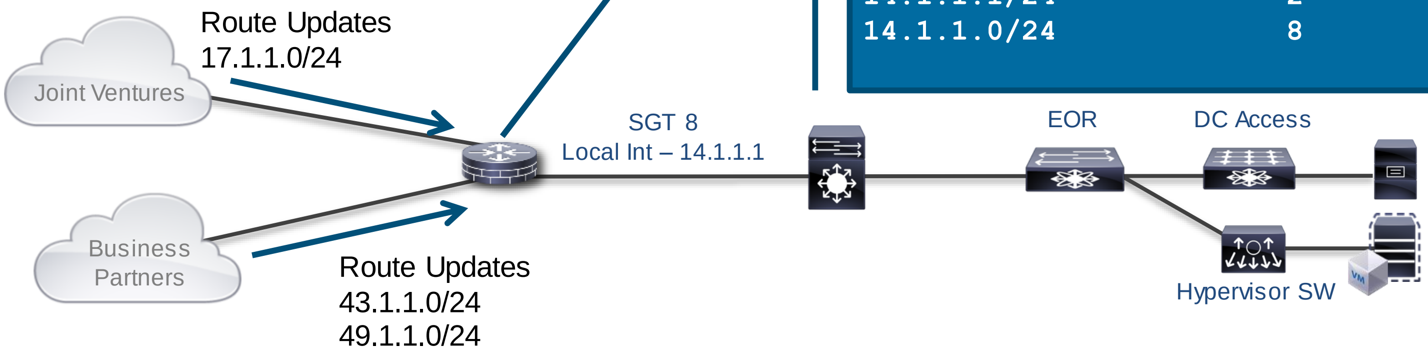


© 2015 Cisco and/or its affiliates. All rights reserved.

Layer 3 Interface to SGT – Port/SGT Mapping

- Port to Interface Mapping does not learn IP Prefixes via route learning
- All traffic coming into the interface is tagged with the SGT on the interface
- Will not make prefixes learned available in SXP

```
ASR1K#show cts role-based sgt-map all
Active IP-SGT Bindings Information
IP Address                  SGT      Source
========================================
11.1.1.2                    2        INTERNAL
12.1.1.2                    2        INTERNAL
13.1.1.2                    2        INTERNAL
14.1.1.1/24                 2        INTERNAL
14.1.1.0/24                 8        L3IF
```



Business Partner Router – Port Classification Options

- For our topology we're using SXP from the router to the data centre. We will use configuration on the right

- If we had to put into the frame we would use configuration on the left

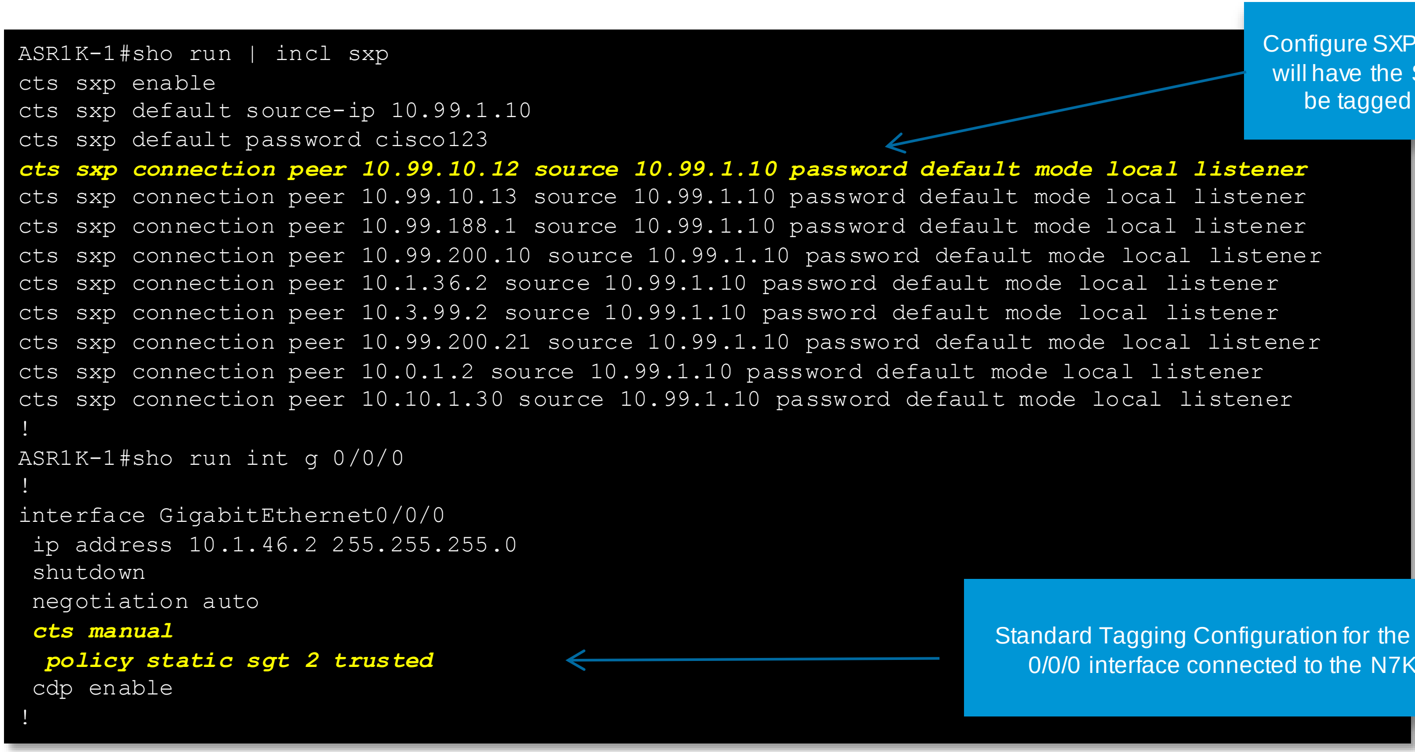
Port/SGT – Tag only transport

```
interface GigabitEthernet0/0/0
 ip address 10.1.47.2 255.255.255.0
 cts manual
  policy static sgt 2 trusted

interface GigabitEthernet0/0/2
 ip address 8.8.8.1 255.255.255.0
 cts manual
  policy static sgt 50
  no propagate-sgt
 cdp enable

ASR1K-2#sho cts role-based sgt-map all
Active IP-SGT Bindings Information
IP Address                SGT     Source
============================================
8.8.8.0/24                50      L3IF
8.8.8.1                   2       INTERNAL
```

Prefix Learning – SXP subnet/SGT

```
interface GigabitEthernet0/0/2
 ip address 8.8.8.1 255.255.255.0
 cts role-based sgt-map sgt 50

ASR1K-2#sho cts role-based sgt-map all
Active IP-SGT Bindings Information
IP Address                SGT     Source
============================================
8.8.8.0/24                50      L3IF
8.8.8.1                   2       INTERNAL
10.1.3.0/24               50      L3IF
10.1.47.2                 2       INTERNAL
10.254.100.0/24           50      L3IF
```

ASR1K Configuration – SXP to Inline SGT



```
ASR1K-1#sho run | incl sxp
cts sxp enable
cts sxp default source-ip 10.99.1.10
cts sxp default password cisco123
cts sxp connection peer 10.99.10.12 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.10.13 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.188.1 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.200.10 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.1.36.2 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.3.99.2 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.99.200.21 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.0.1.2 source 10.99.1.10 password default mode local listener
cts sxp connection peer 10.10.1.30 source 10.99.1.10 password default mode local listener
!
ASR1K-1#sho run int g 0/0/0
!
interface GigabitEthernet0/0/0
 ip address 10.1.46.2 255.255.255.0
 shutdown
 negotiation auto
 cts manual
  policy static sgt 2 trusted
 cdp enable
!
```

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

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

© 2015 Cisco and/or its affiliates. All rights reserved.

Services with SGT Caching

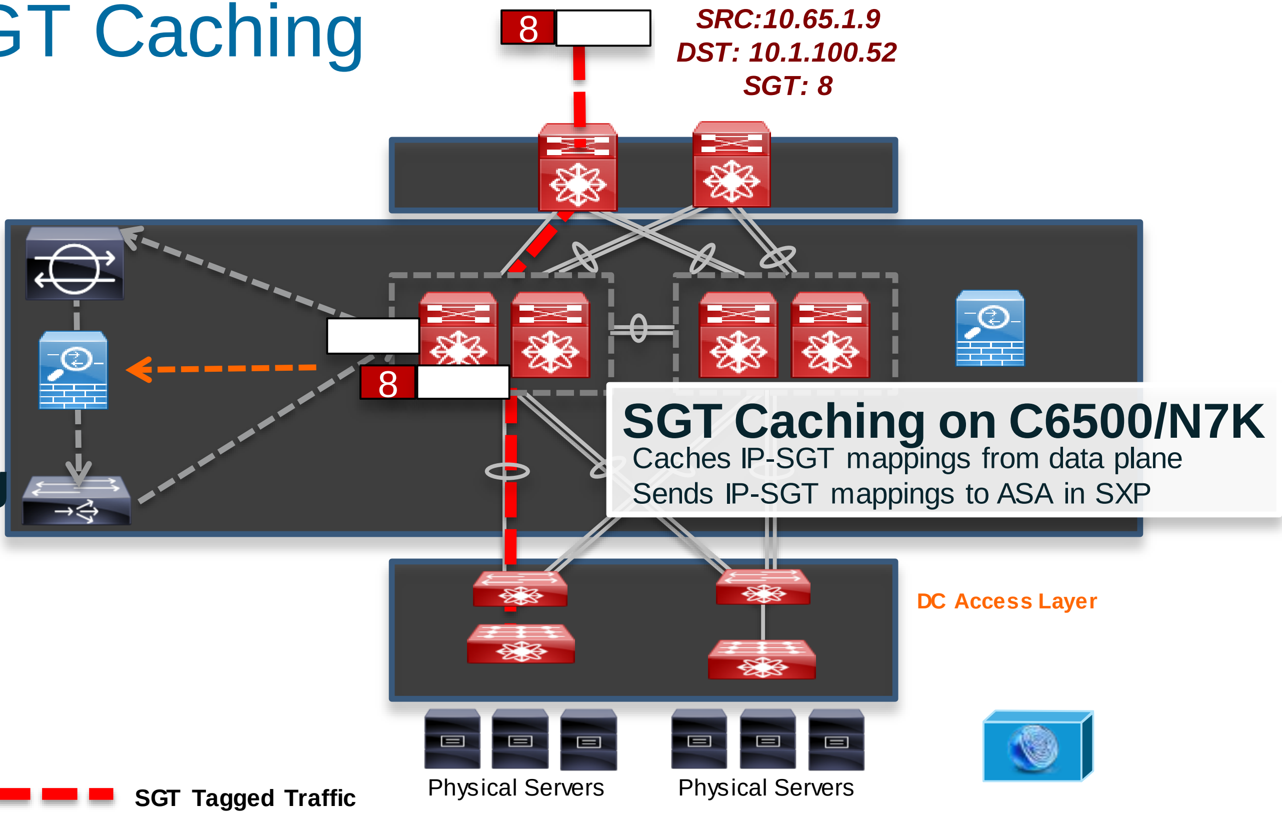
Service Chaining

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

IP Address	SGT
10.65.1.9	LOB1_User - 8



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

🟥 SGT Tagged Traffic

← Untagged Traffic

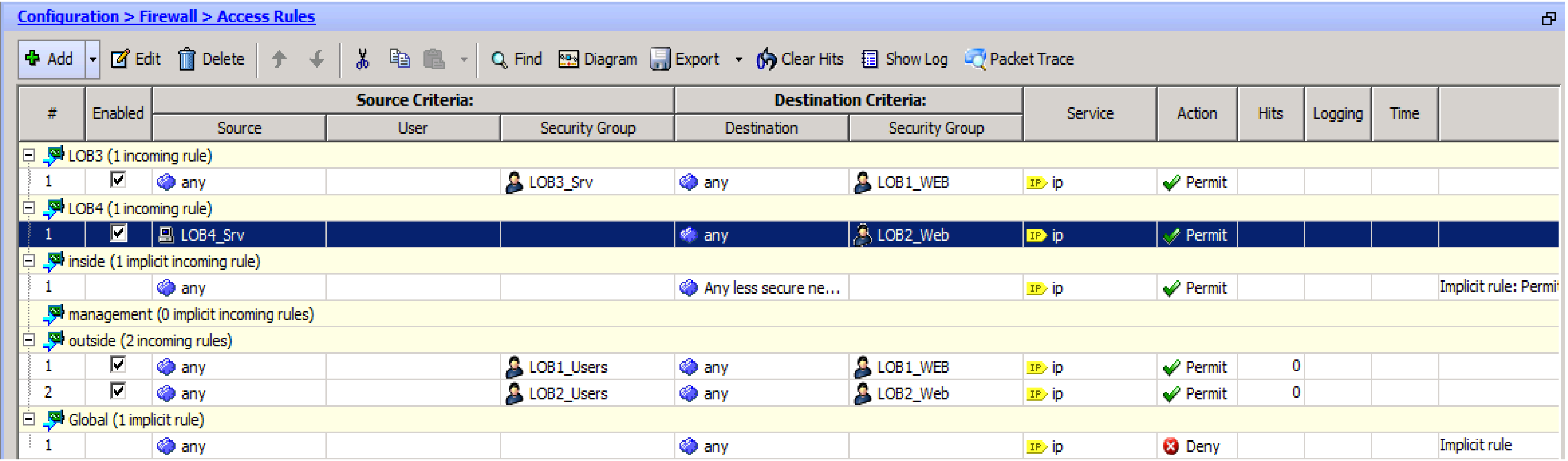
← SXP

🟥 SGACL enabled Device

🟦 SG Firewall enabled Device

© 2015 Cisco and/or its affiliates. All rights reserved.

ASA Policy Configuration Examples



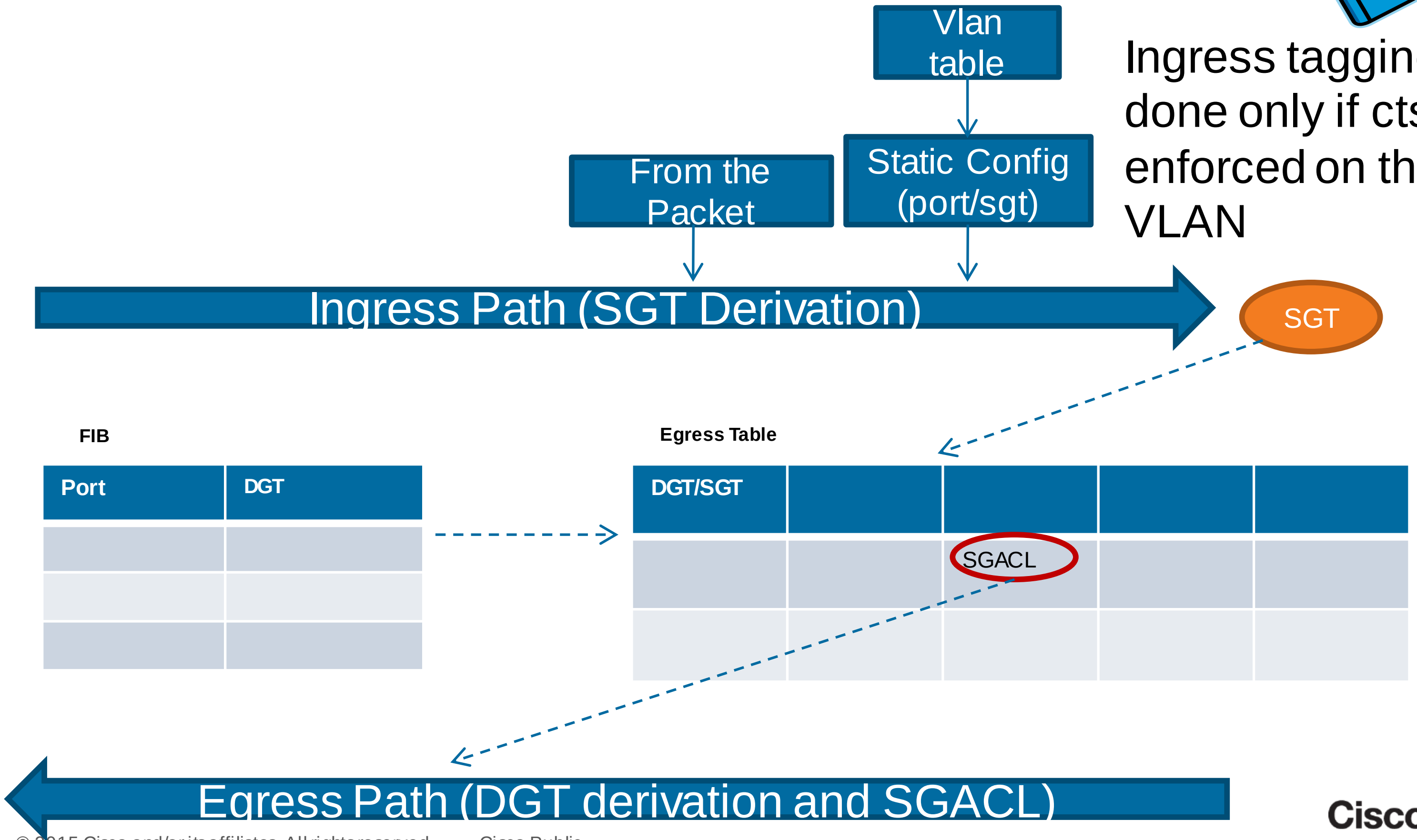
#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging	Time	
		Source	User	Security Group	Destination	Security Group						
⊟ LOB3 (1 incoming rule)												
1	☑	any		LOB3_Srv	any	LOB1_WEB	ip	Permit				
⊟ LOB4 (1 incoming rule)												
1	☑	LOB4_Srv			any	LOB2_Web	ip	Permit				
⊟ inside (1 implicit incoming rule)												
1		any			Any less secure ne...		ip	Permit				Implicit rule: Permi
management (0 implicit incoming rules)												
⊟ outside (2 incoming rules)												
1	☑	any		LOB1_Users	any	LOB1_WEB	ip	Permit	0			
2	☑	any		LOB2_Users	any	LOB2_Web	ip	Permit	0			
⊟ Global (1 implicit rule)												
1		any			any		ip	Deny				Implicit rule

Hardware Forwarding SGT/SGACL - Reminder

- Two Groupings of Hardware Forwarding for SGACL
- Port/VLAN based
  - Catalyst 3K-X
  - Nexus 5500
- IP/SGT Based
  - Nexus 7000 – M series and F series
  - Nexus 6000/5600
  - Cat 6K/Sup2T
  - 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
- Each type of hardware has different logging and monitoring capabilities
  - Counters
  - ACE Logging
  - Netflow with SGT/DGT

Nexus 5500 SGT and DGT Derivation

Each Port has one DGT (which is also used as SGT in the ingress) associated with it.


Vlan table
Static Config (port/sgt)
From the Packet
Ingress Path (SGT Derivation)
SGT
SGACL
Egress Path (DGT derivation and SGACL)

FIB

Port	DGT

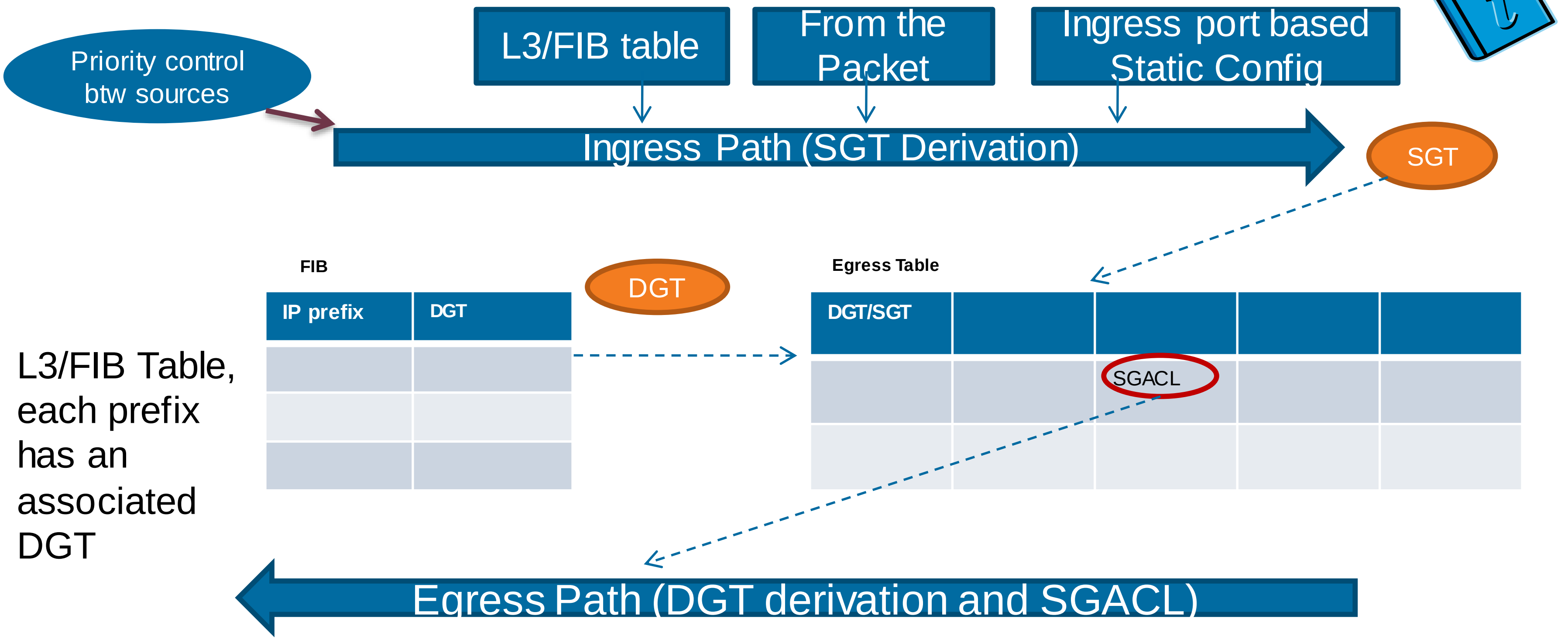
Egress Table

DGT/SGT				
		SGACL		

Ingress tagging is done only if cts is enforced on the VLAN

© 2015 Cisco and/or its affiliates. All rights reserved.

N7K M series SGT and DGT Derivation


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

FIB

IP prefix	DGT

Egress Table

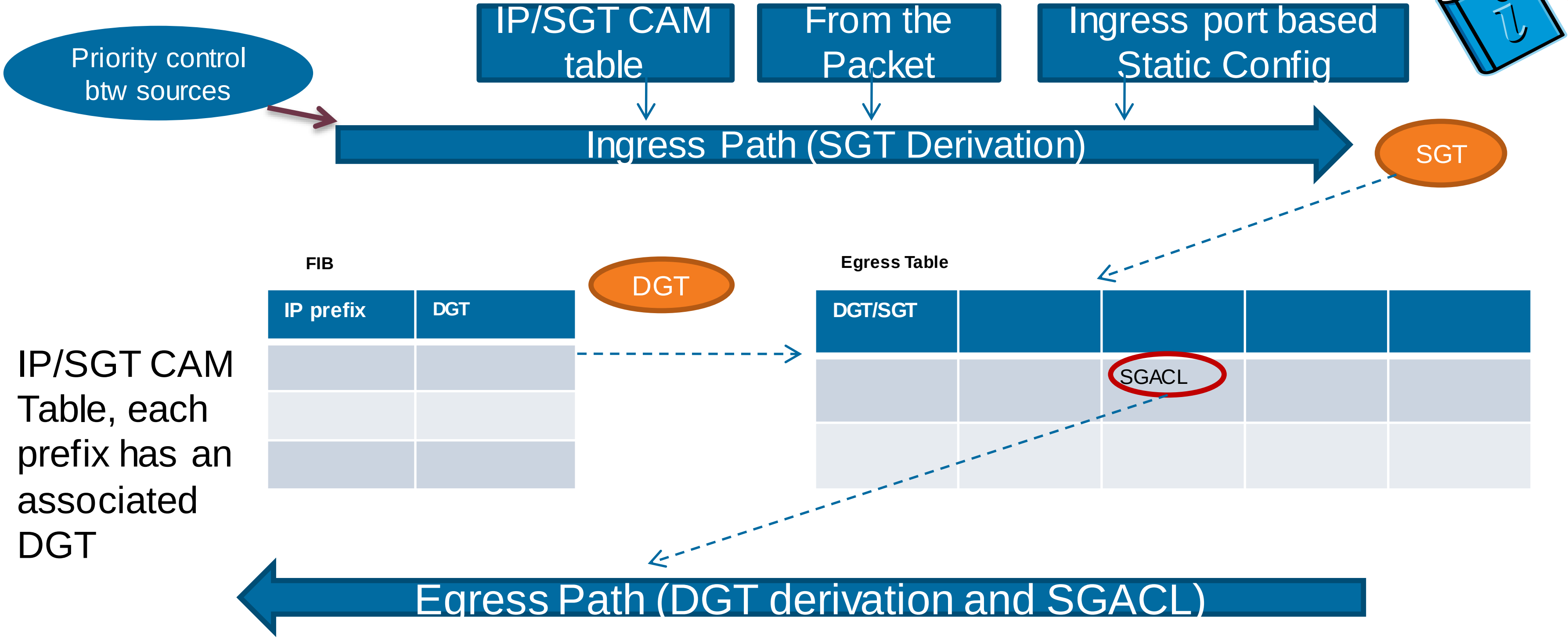
DGT/SGT				
		SGACL		

L3/FIB Table, each prefix has an associated DGT

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

© 2015 Cisco and/or its affiliates. All rights reserved.

N7K F Series SGT and DGT Derivation


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

FIB

IP prefix	DGT

Egress Table

DGT/SGT				
		SGACL		

IP/SGT CAM Table, each prefix has an associated DGT

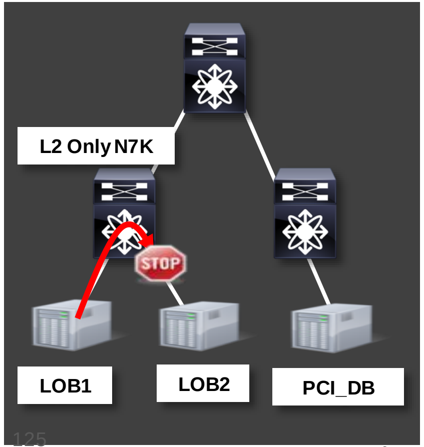
A number of SGT(DGT) assignment sources, e.g. SXP, VLAN-SGT,, will be evaluated by TrustSec software against a priority list, the winning result will be programmed into the L3/FIB table

© 2015 Cisco and/or its affiliates. All rights reserved.

Nexus 7000 TrustSec Capabilities -

- SGT/SGACL supported on M series, F1, F2, F2E cards as of 6.2(6a)
- SGT/SGACL support on F3 as of 6.2(10)
- N7K does all enforcement via IP/SGT programming in ASICs. This creates an interesting design case.
- In the case where the N7K is performing intra-VLAN policy (within the same VLAN)
  - The N7K MUST have an SVI on the VLAN
  - If N7K is L2 only then create an SVI w/o IP to be able to snoop ARP/DHCP to discover the IP
  - This allows the IP/SGT to be programmed properly for intra vlan filtering
- VPC and Fabric Path supported in 6.2(10) with IP/SGT only

```
N7K-DST1# sho run int vlan 3207
interface Vlan3207
  no shutdown
```

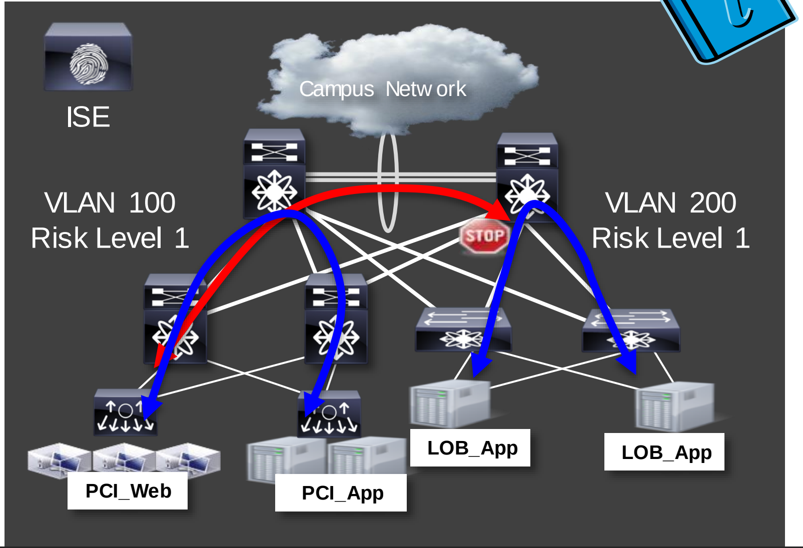


© 2015 Cisco and/or its affiliates. All rights reserved.

Data Centre

VLAN 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 substantially
  - ACL conversion has shown 60% to 88% TCAM reduction
  - Distribution layer enforcement allows any compute Does assume within a VLAN is permissible
- Flows to other risk levels/security zones still enforced on firewall
- No VPC or Fabric Path support until 7.x train



```
N7K-DST1(config)# vlan 100
N7K-DST1(config-vlan)# cts role-based sgt 100
N7K-DST1# sho cts role-based sgt-map
IP ADDRESS           SGT                 VRF/VLAN       SGT CONFIGURATION
10.1.200.10          2000(PCI_Servers)   vlan:200       Learnt through VLAN SGT configuration
10.1.200.77          2000(PCI_Servers)   vlan:200       Learnt through VLAN SGT configuration
10.1.100.26          2000(PCI_Servers)   vrf:1          CLI Configured
10.1.200.77          1000(Production_Servers)vrf:1      CLI Configured
```

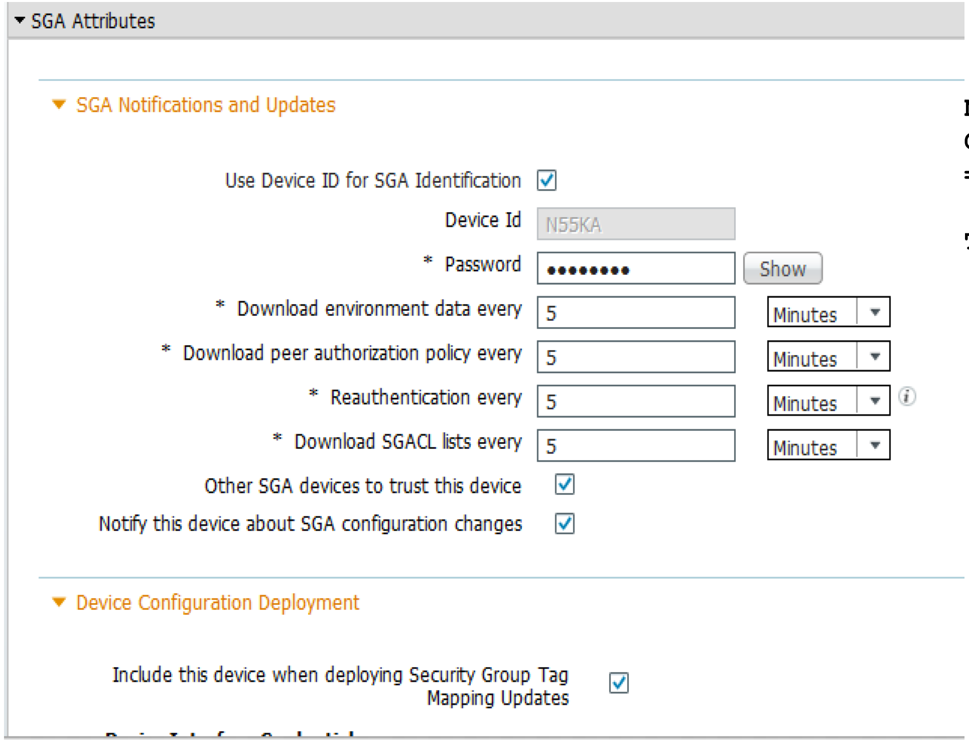
NX-OS Large Scale SGT

- Large numbers of SGT/DGT cells and SGACLs on N7K/N6K/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)
  - N6K – 7.0
  - N5K – 6.0(2)N2(6)
- N7K requires a batch programming command to scale large SGACLs

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

Configure ISE for Nexus Switch

Administration->Network Resources->Network Devices->+Add



▾ SGA Attributes

▾ SGA Notifications and Updates

Use Device ID for SGA Identification ☑

Device Id: N55KA

* Password: ●●●●●●●●● Show

* Download environment data every: 5 Minutes

* Download peer authorization policy every: 5 Minutes

* Reauthentication every: 5 Minutes

* Download SGACL lists every: 5 Minutes

Other SGA devices to trust this device ☑

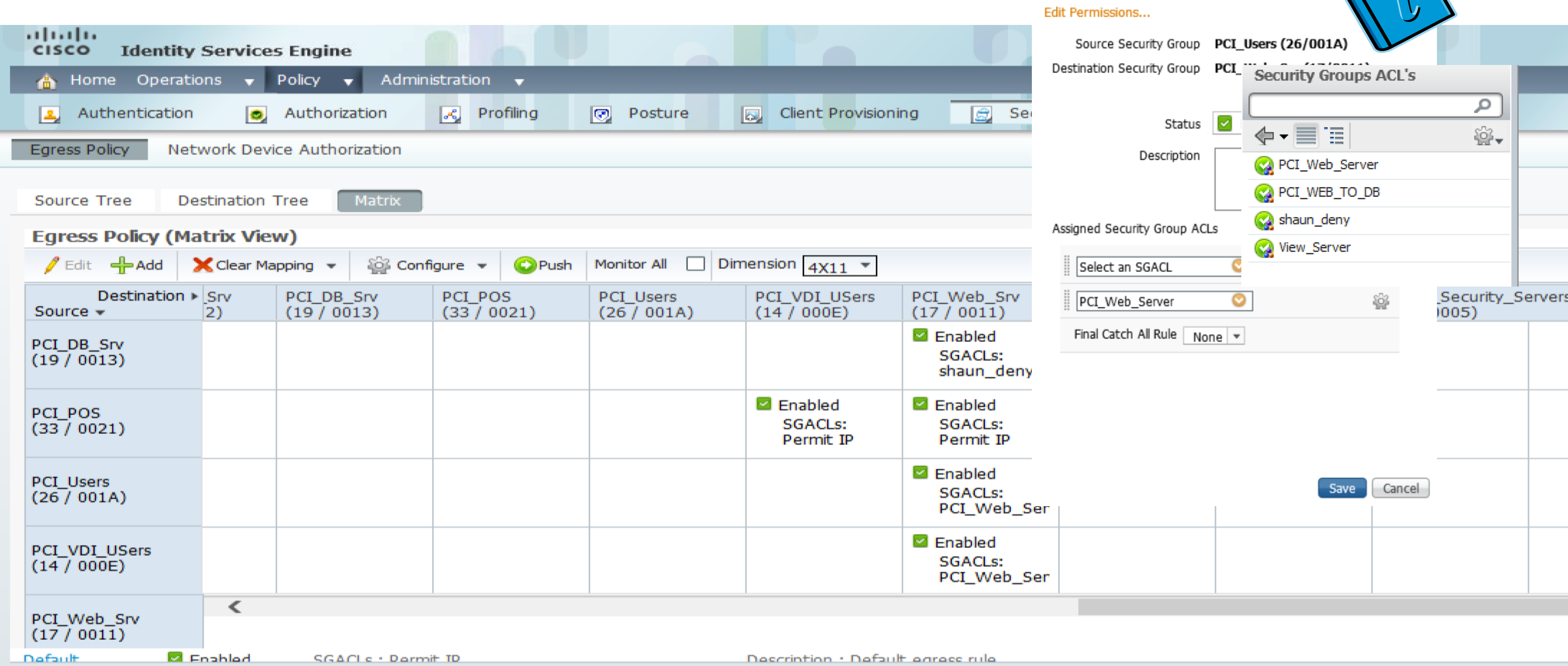
Notify this device about SGA configuration changes ☑

▾ Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

```
N55KAa# show cts environment-data
CTS Environment Data
==============================
  Current State            :
TS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
  Last Status              : CTS_ENV_SUCCESS
  Local Device SGT         : 0x0002
  Transport Type           : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache   : FALSE
  Env Data Lifetime        : 86400 seconds after last
  update
  Last Update Time         : Thu May 23 17:22:18 2013

  Server List              : CTSServerList1
     AID:a6f054a3856a15221714bba63e968867 IP:
     10.39.1.120 Port:1812
```

Configure ISE SGACL Policy Matrix



Egress Policy (Matrix View)

Destination ▸ Source ▾	Srv 2)	PCI_DB_Srv (19 / 0013)	PCI_POS (33 / 0021)	PCI_Users (26 / 001A)	PCI_VDI_USers (14 / 000E)	PCI_Web_Srv (17 / 0011)				Security_Servers)005)
PCI_DB_Srv (19 / 0013)						☑ Enabled SGACLs: shaun_deny				
PCI_POS (33 / 0021)					☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Permit IP				
PCI_Users (26 / 001A)						☑ Enabled SGACLs: PCI_Web_Ser				
PCI_VDI_USers (14 / 000E)						☑ Enabled SGACLs: PCI_Web_Ser				
PCI_Web_Srv (17 / 0011)										

Default ☑ Enabled SGACLs : Permit IP Description : Default egress rule

Edit Permissions...

Source Security Group PCI_Users (26/001A)

Destination Security Group PCI_Web_Srv (17/0011)

Status ☑

Description

Assigned Security Group ACLs

Select an SGACL

PCI_Web_Server

Final Catch All Rule None

Security Groups ACL's

- PCI_Web_Server
- PCI_WEB_TO_DB
- shaun_deny
- View_Server

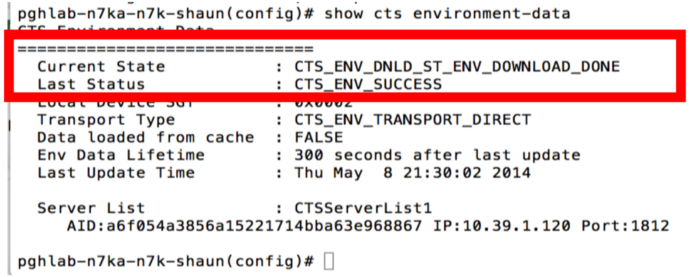
Reminder: NXOS can only handle one SGACL in a cell

Nexus 7000 CTS Interface Configuration

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

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

Verify Configuration

- Verify environmental data



```
pghlab-n7ka-n7k-shaun(config)# show cts environment-data
CTS Environment Data
==============================
  Current State            : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
  Last Status              : CTS_ENV_SUCCESS
  Local Device SGT         : 0x0002
  Transport Type           : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache   : FALSE
  Env Data Lifetime        : 300 seconds after last update
  Last Update Time         : Thu May  8 21:30:02 2014

  Server List              : CTSServerList1
     AID:a6f054a3856a15221714bba63e968867 IP:10.39.1.120 Port:1812

pghlab-n7ka-n7k-shaun(config)#
```

- If the N7K is protecting a host.
- Verify SGACLs downloaded and look at counters:

```
N5K-DST1# show cts role-based access-list
rbacl:Deny IP
        deny ip
rbacl:Permit IP
        permit ip
rbacl:PCI_Web_Server

N7K-DST1# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: 04/16/2014 at 06:28:11 PM

sgt:unknown dgt:19      [41677]
rbacl:Deny IP
        deny ip [41677]

sgt:unknown dgt:24      [13269]
rbacl:Deny IP
        deny ip [13269]

sgt:4 dgt:3     [0]
rbacl:Deny IP
        deny ip [0]

sgt:6 dgt:12    [0]
rbacl:Deny IP
        deny ip [0]

sgt:7 dgt:3     [53769]
rbacl:Deny IP
        deny ip [53769]
```

© 2015 Cisco and/or its affiliates. All rights reserved.

Nexus 5500 Server Segmentation Configuration: Initial Configuration

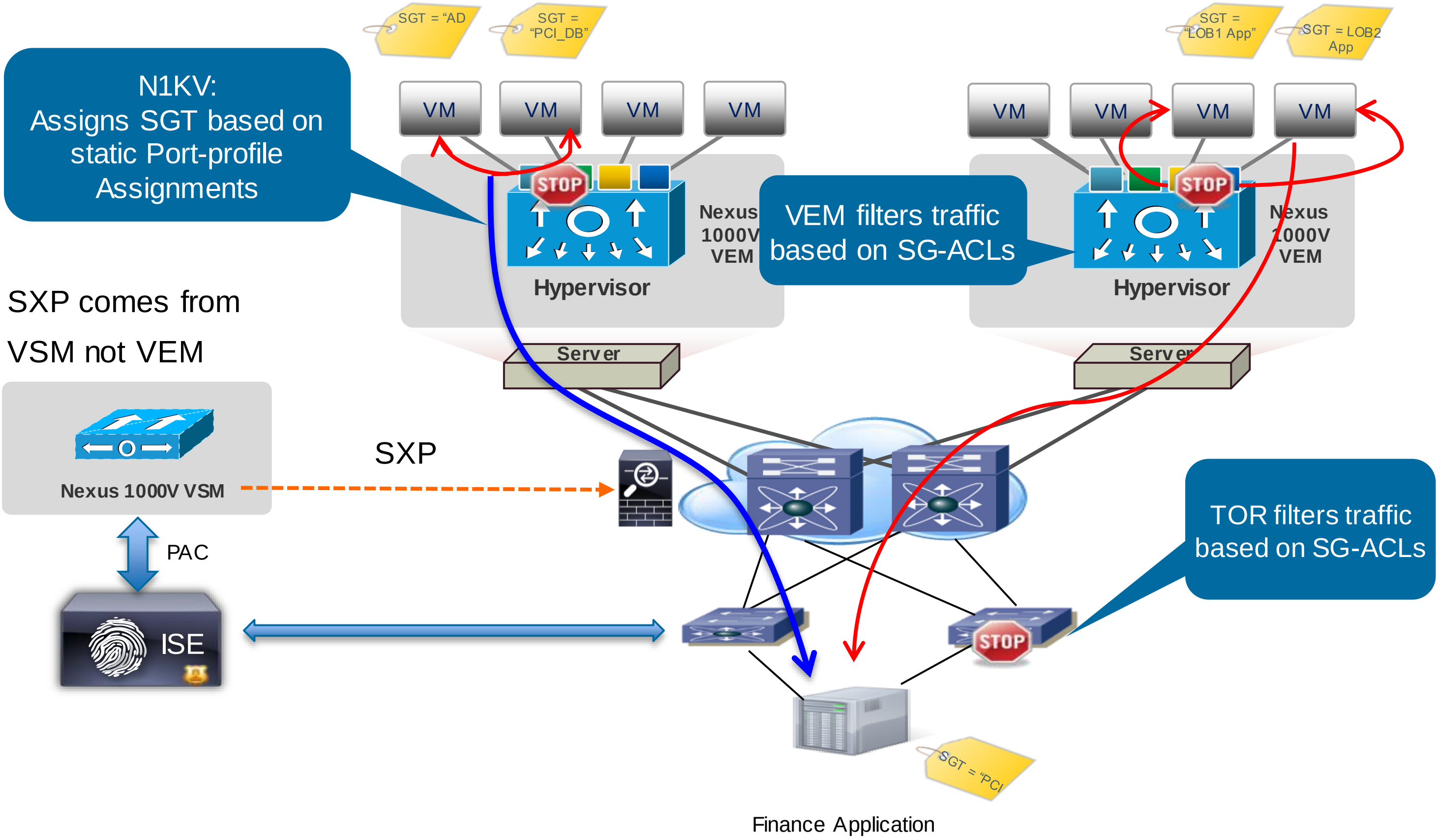
```
N55KA(config)# cts role-based counters enable      → Turn on SGACL counters

N55KA(config)# vlan 118

N55KA(config-vlan)# cts role-based enforcement     → Enable Role Based enforcement on
                                                      VLAN 118 – No Layer 3 Interface can be
                                                      attached to the VLAN!

N55KA(config-vlan)# int e 1/1

N55KA(config-vlan)# switchport trunk

N55KA(config-vlan)# switchport trunk native vlan 2

N55KA(config-vlan)# cts manual                               → Go into CTS manual mode for the
                                                                port (other int CLI clipped)

N55KA(config-if-cts-manual)# policy static sgt 0x2 trusted → Set SGT and Trust for Trunk
                                                                    to N7K-DST1
```

© 2015 Cisco and/or its affiliates. All rights reserved.

Nexus 5500 Server Segmentation Configuration

```
N55KA(config-vlan)# int e102/1/1
N55KA(config-vlan)# switchport
N55KA(config-vlan)# switchport access vlan 118
N55KA(config-vlan)# cts manual                          → Go into CTS manual mode for the port
N55KA(config-if-cts-manual)# policy static sgt 0x111          → Set SGT on the FEX port e102/1/1 to SGT 111
N55KA(config-if-cts-manual)# no propagate-sgt           → "Don't send the SGT to the server"
                                                              This would be bad. ☺
N55KA(config-if-cts-manual)# no shut
N55KA(config-vlan)# int e102/1/2
N55KA(config-vlan)# switchport
N55KA(config-vlan)# switchport access vlan 118
N55KA(config-vlan)# cts manual                          → Go into CTS manual mode for the port
N55KA(config-if-cts-manual)# policy static sgt 0x222          → Set SGT on the FEX port e102/1/1 to SGT 222
N55KA(config-if-cts-manual)# no propagate-sgt           → "Don't send the SGT to the server"
                                                              This would be bad. ☺
N55KA(config-if-cts-manual)# no shut
N55KA(config)# cts sxp enable                             → Enable SXP protocol for peering relationships
N55KA(config)# cts sxp connection peer 10.49.1.2 source 10.49.1.10 password none mode listener →Peer with ASA-A
N55KA(config)# cts sxp connection peer 10.49.1.3 source 10.49.1.10 password none mode listener →Peer with ASA-B
```

SGACL on Nexus 1000v Use Case



N1KV:
Assigns SGT based on static Port-profile Assignments

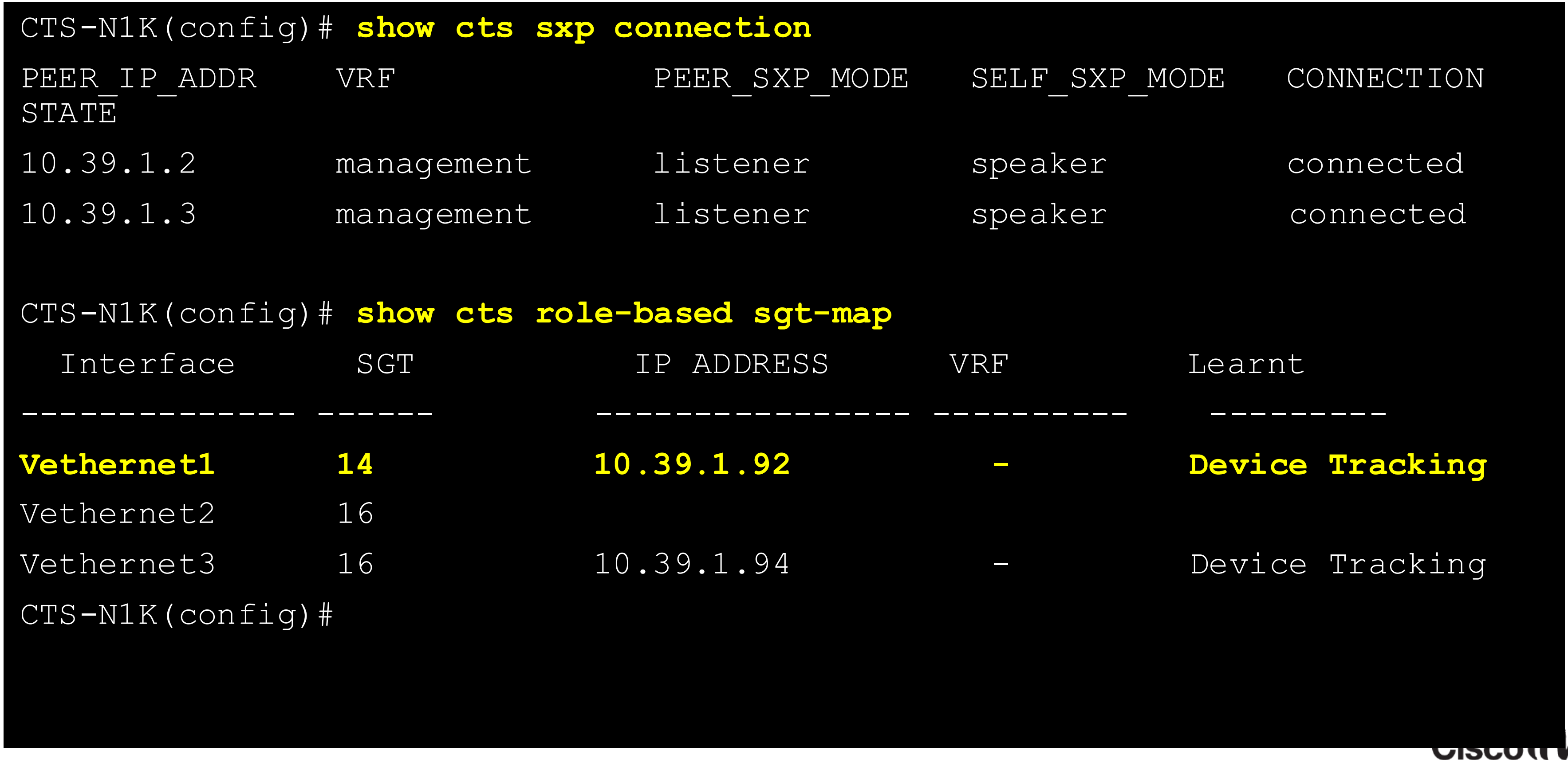
VEM filters traffic based on SG-ACLs

TOR filters traffic based on SG-ACLs

SXP comes from VSM not VEM

© 2015 Cisco and/or its affiliates. All rights reserved.

Nexus 1000v - 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)#
```

Nexus 1000v – SGACL Configuration

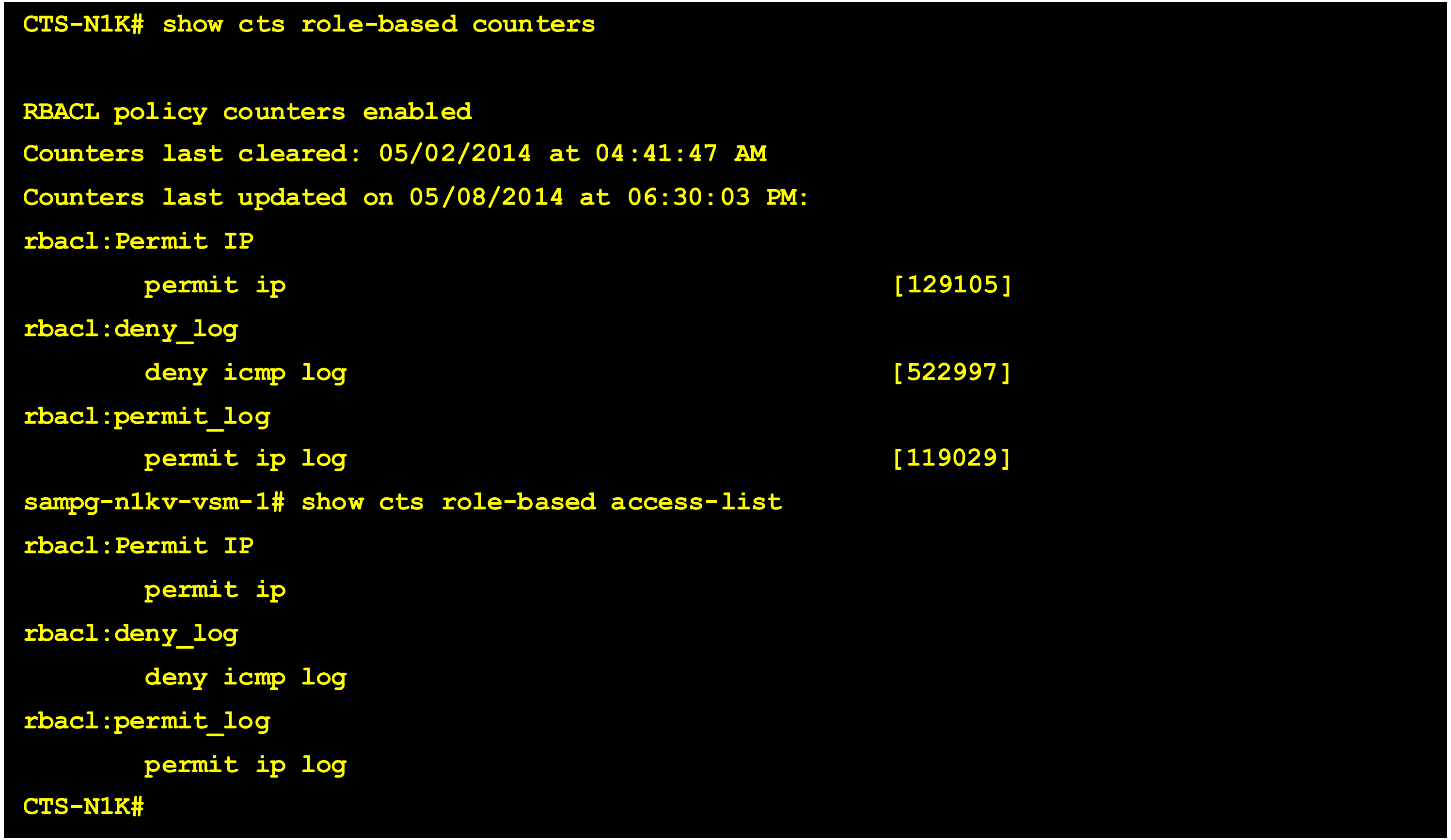
```
CTS-N1K(config)# feature cts
CTS-N1K(config)# cts device-id cts-n1k password 0 TrustSec
CTS-N1K(config)# radius-server host 10.39.1.120 key 0 TrustSec pac
authentication accounting
CTS-N1K(config)# aaa group server radius cts-ise
CTS-N1K(config)# server 10.39.1.120
CTS-N1K(config)# use-vrf management
CTS-N1K(config)# source-interface mgmt0
CTS-N1K(config)# aaa authentication cts default group cts-ise
CTS-N1K(config)# aaa authorization cts default group cts-ise
CTS-N1K(config)# cts role-based counters
```

Nexus 1000V – Port Profile Setup

```
Create UPLINK port-profile:

 CTS-N1K(config)# port-profile type ethernet uplink-vem
 CTS-N1K(config-port-prof)# switchport mode trunk
 CTS-N1K(config-port-prof)# switchport trunk allowed vlan 1-4000
 CTS-N1K(config-port-prof)# cts manual
 CTS-N1K(config-port-prof)#  policy static sgt 0x2 trusted  ->Set tag to device SGT (2) and trust
 CTS-N1K(config-port-prof)#  propagate-sgt                  ->Propogate the SGT to neighbor
 CTS-N1K(config-port-prof)# no shutdown
 CTS-N1K(config-port-prof)# state enabled
 CTS-N1K(config-port-prof)#  vmware port-group
```

```
Create PCI-Server port-profile:

CTS-N1K(config)# port-profile type vethernet PCI_Servers
CTS-N1K(config-port-prof)# switchport mode access
CTS-N1K(config-port-prof)# switchport access vlan 200
CTS-N1K(config-port-prof)# cts manual
CTS-N1K(config-port-prof)#  policy static sgt 0x7d0    ->Set the Tag to PCI-Servers
                                                       Hex 0x7d0 = 1000 Decimal
CTS-N1K(config-port-prof)#  role-based enforcement     ->Enable Role-based enforcement
CTS-N1K(config-port-prof)# no shutdown
CTS-N1K(config-port-prof)# state enabled
CTS-N1K(config-port-prof)# vmware port-group
```

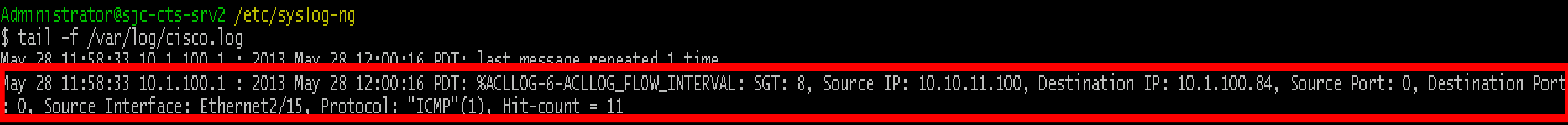
Nexus 1000v – SGACL Verification



```
CTS-N1K# show cts role-based counters


RBACL policy counters enabled
Counters last cleared: 05/02/2014 at 04:41:47 AM
Counters last updated on 05/08/2014 at 06:30:03 PM:
rbacl:Permit IP
        permit ip                                        [129105]
rbacl:deny_log
        deny icmp log                                    [522997]
rbacl:permit_log
        permit ip log                                    [119029]
sampg-n1kv-vsm-1# show cts role-based access-list
rbacl:Permit IP
        permit ip
rbacl:deny_log
        deny icmp log
rbacl:permit_log
        permit ip log
CTS-N1K#
```

Logging from Nexus 7000

```
N7K-DST1# 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
N7K-DST1(config)# log level acllog 6   ← Recommended log levels
N7K-DST1(config)# log level cts 5
N7K-DST1(config)# log ip access-list include sgt
N7K-DST1# 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
```

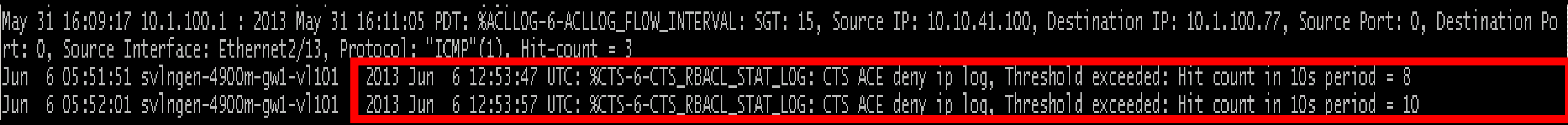


```
Administrator@sjc-cts-srv2 /etc/syslog-ng
$ tail -f /var/log/cisco.log
May 28 11:58:33 10.1.100.1 : 2013 May 28 12:00:16 PDT: last message repeated 1 time
May 28 11:58:33 10.1.100.1 : 2013 May 28 12:00:16 PDT: %ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 8, Source IP: 10.10.11.100, Destination IP: 10.1.100.84,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

Logging from Nexus 5500

```
N55KA# 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
N55KA(config)# log level acllog 6   ← Log levels to make this work
N55KA (config)# log level cts 7
N55KA# 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
```

N5500 - Monitoring SGACL Drops

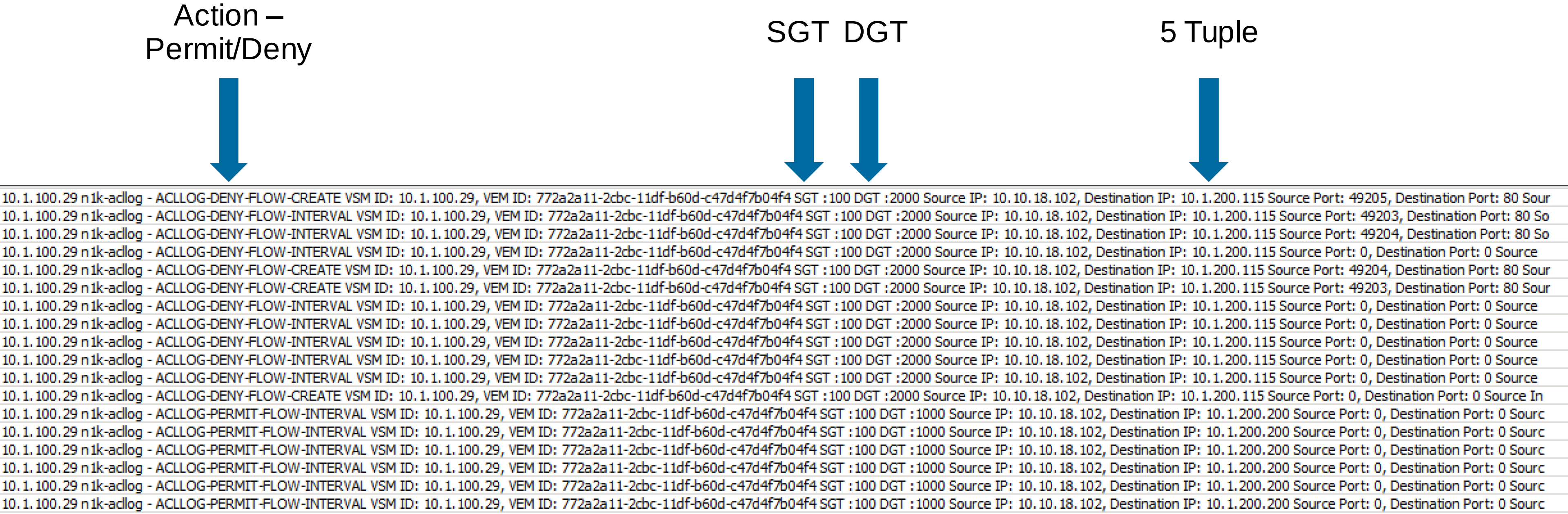
```
N55KA# show platform fwm info lif eth100/1/45 | grep good
Eth100/1/45 pd: rx frames: good 2755 drop 3; tx frames: good 2689 drop 106
```

Looking at the egress interface on the N5K protecting the server. It should show drops.

This correlated with counters increments shows what server and SGACL is being hit

```
N55KA# sho cts role-based counters

RBACL policy counters enabled
Counters last cleared: 11/16/2011 at 05:55:24 PM
rbacl:ALLOW_SQL
permit  tcp dst eq 1433                                 [0]
        permit icmp                                     [0]
        deny ip                                         [0]
rbacl:Deny IP
        deny ip                                         [6730]
rbacl:Deny_ICMP_Log
        deny icmp log                                   [106]
rbacl:Permit IP
        permit ip                                       [85730]
rbacl:test_deny
        deny icmp log                                   [0]
```

Nexus 1000V – Syslog for for ACE Logs



Action – Permit/Deny

SGT DGT

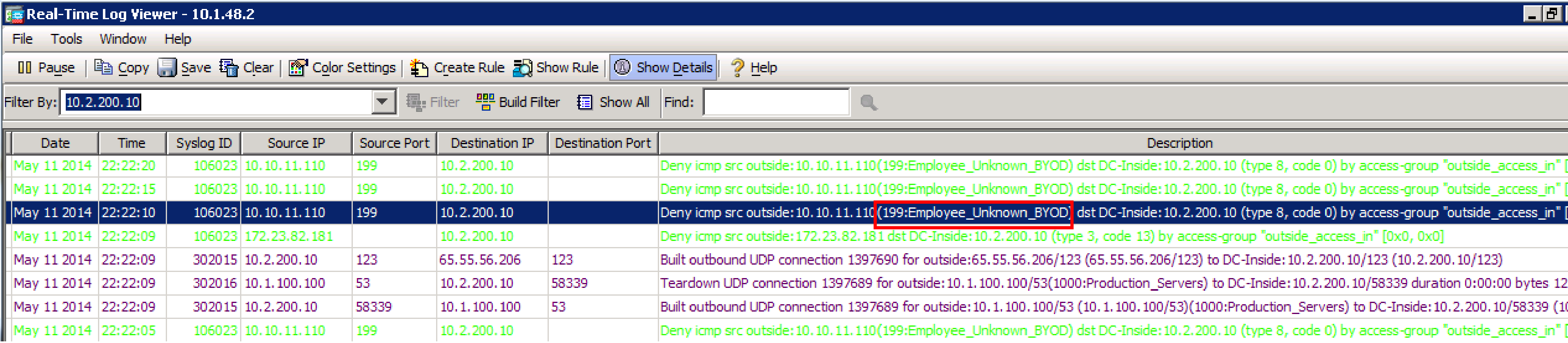
5 Tuple

```
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-CREATE VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 49205, Destination Port: 80 Sour
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 49203, Destination Port: 80 So
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 49204, Destination Port: 80 So
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-CREATE VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 49204, Destination Port: 80 Sour
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-CREATE VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 49203, Destination Port: 80 Sour
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source
10.1.100.29 n1k-acllog - ACLLOG-DENY-FLOW-CREATE VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :2000 Source IP: 10.10.18.102, Destination IP: 10.1.200.115 Source Port: 0, Destination Port: 0 Source In
10.1.100.29 n1k-acllog - ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :1000 Source IP: 10.10.18.102, Destination IP: 10.1.200.200 Source Port: 0, Destination Port: 0 Sourc
10.1.100.29 n1k-acllog - ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :1000 Source IP: 10.10.18.102, Destination IP: 10.1.200.200 Source Port: 0, Destination Port: 0 Sourc
10.1.100.29 n1k-acllog - ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :1000 Source IP: 10.10.18.102, Destination IP: 10.1.200.200 Source Port: 0, Destination Port: 0 Sourc
10.1.100.29 n1k-acllog - ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :1000 Source IP: 10.10.18.102, Destination IP: 10.1.200.200 Source Port: 0, Destination Port: 0 Sourc
10.1.100.29 n1k-acllog - ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :1000 Source IP: 10.10.18.102, Destination IP: 10.1.200.200 Source Port: 0, Destination Port: 0 Sourc
10.1.100.29 n1k-acllog - ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 10.1.100.29, VEM ID: 772a2a11-2cbc-11df-b60d-c47d4f7b04f4 SGT :100 DGT :1000 Source IP: 10.10.18.102, Destination IP: 10.1.200.200 Source Port: 0, Destination Port: 0 Sourc
```

Data Centre

ASA Firewall Logging

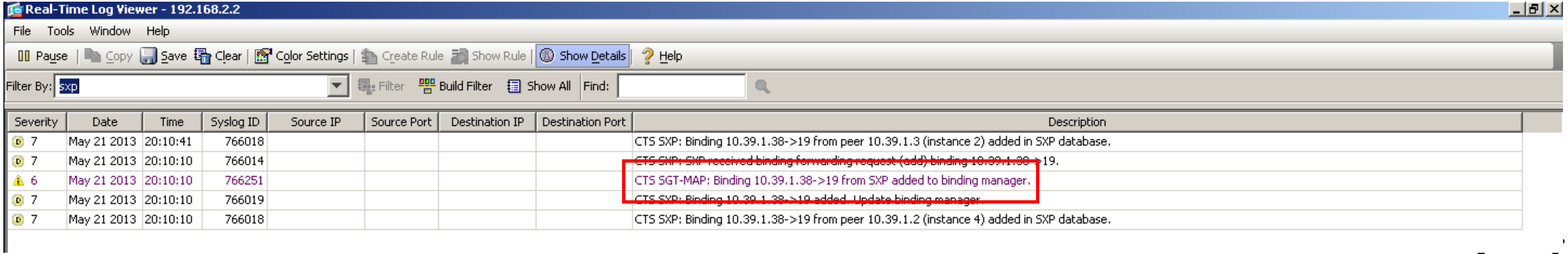
- Firewall logging will show the SGT/DGT in the logs if known by the firewall


Real-Time Log Viewer - 10.1.48.2
File Tools Window Help
Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help
Filter Build Filter Show All Find:

Filter By: 10.2.200.10

Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
May 11 2014	22:22:20	106023	10.10.11.110	199	10.2.200.10		Deny icmp src outside:10.10.11.110(199:Employee_Unknown_BYOD) dst DC-Inside:10.2.200.10 (type 8, code 0) by access-group "outside_access_in" [
May 11 2014	22:22:15	106023	10.10.11.110	199	10.2.200.10		Deny icmp src outside:10.10.11.110(199:Employee_Unknown_BYOD) dst DC-Inside:10.2.200.10 (type 8, code 0) by access-group "outside_access_in" [
May 11 2014	22:22:10	106023	10.10.11.110	199	10.2.200.10		Deny icmp src outside:10.10.11.110(199:Employee_Unknown_BYOD) dst DC-Inside:10.2.200.10 (type 8, code 0) by access-group "outside_access_in" [
May 11 2014	22:22:09	106023	172.23.82.181		10.2.200.10		Deny icmp src outside:172.23.82.181 dst DC-Inside:10.2.200.10 (type 3, code 13) by access-group "outside_access_in" [0x0, 0x0]
May 11 2014	22:22:09	302015	10.2.200.10	123	65.55.56.206	123	Built outbound UDP connection 1397690 for outside:65.55.56.206/123 (65.55.56.206/123) to DC-Inside:10.2.200.10/123 (10.2.200.10/123)
May 11 2014	22:22:09	302016	10.1.100.100	53	10.2.200.10	58339	Teardown UDP connection 1397689 for outside:10.1.100.100/53(1000:Production_Servers) to DC-Inside:10.2.200.10/58339 duration 0:00:00 bytes 12
May 11 2014	22:22:09	302015	10.2.200.10	58339	10.1.100.100	53	Built outbound UDP connection 1397689 for outside:10.1.100.100/53 (10.1.100.100/53)(1000:Production_Servers) to DC-Inside:10.2.200.10/58339 (1
May 11 2014	22:22:05	106023	10.10.11.110	199	10.2.200.10		Deny icmp src outside:10.10.11.110(199:Employee_Unknown_BYOD) dst DC-Inside:10.2.200.10 (type 8, code 0) by access-group "outside_access_in" [

- Firewall logging will show the IP/SGT as added and removed


Real-Time Log Viewer - 192.168.2.2
File Tools Window Help
Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help
Filter Build Filter Show All Find:

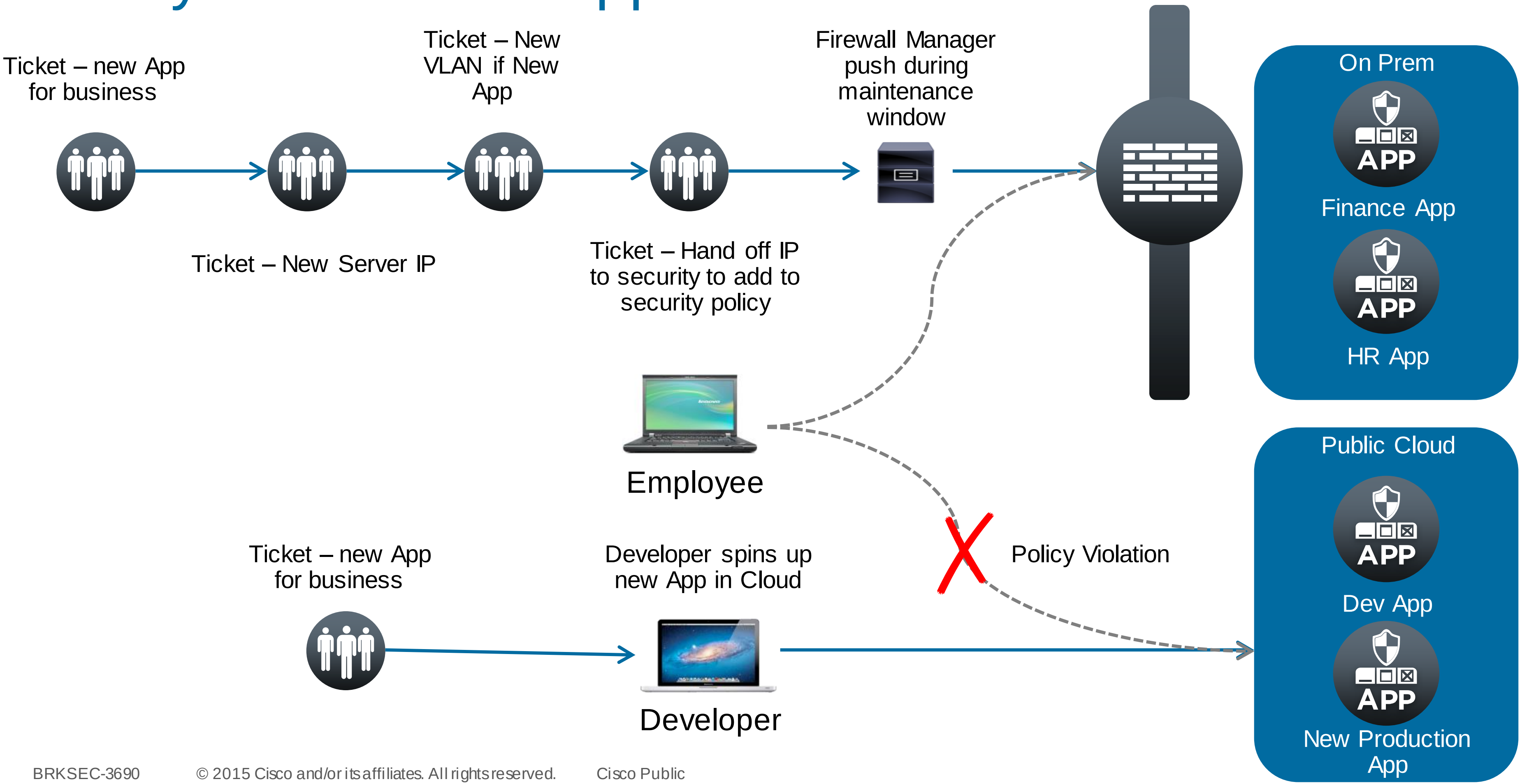
Filter By: sxp

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	766018					CTS SXP: Binding 10.39.1.38->19 from peer 10.39.1.2 (instance 4) added in SXP database.

Orchestrating Security Controls for Applications

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

Security Controls for Applications



Ticket – new App for business

Ticket – New Server IP

Ticket – New VLAN if New App

Ticket – Hand off IP to security to add to security policy

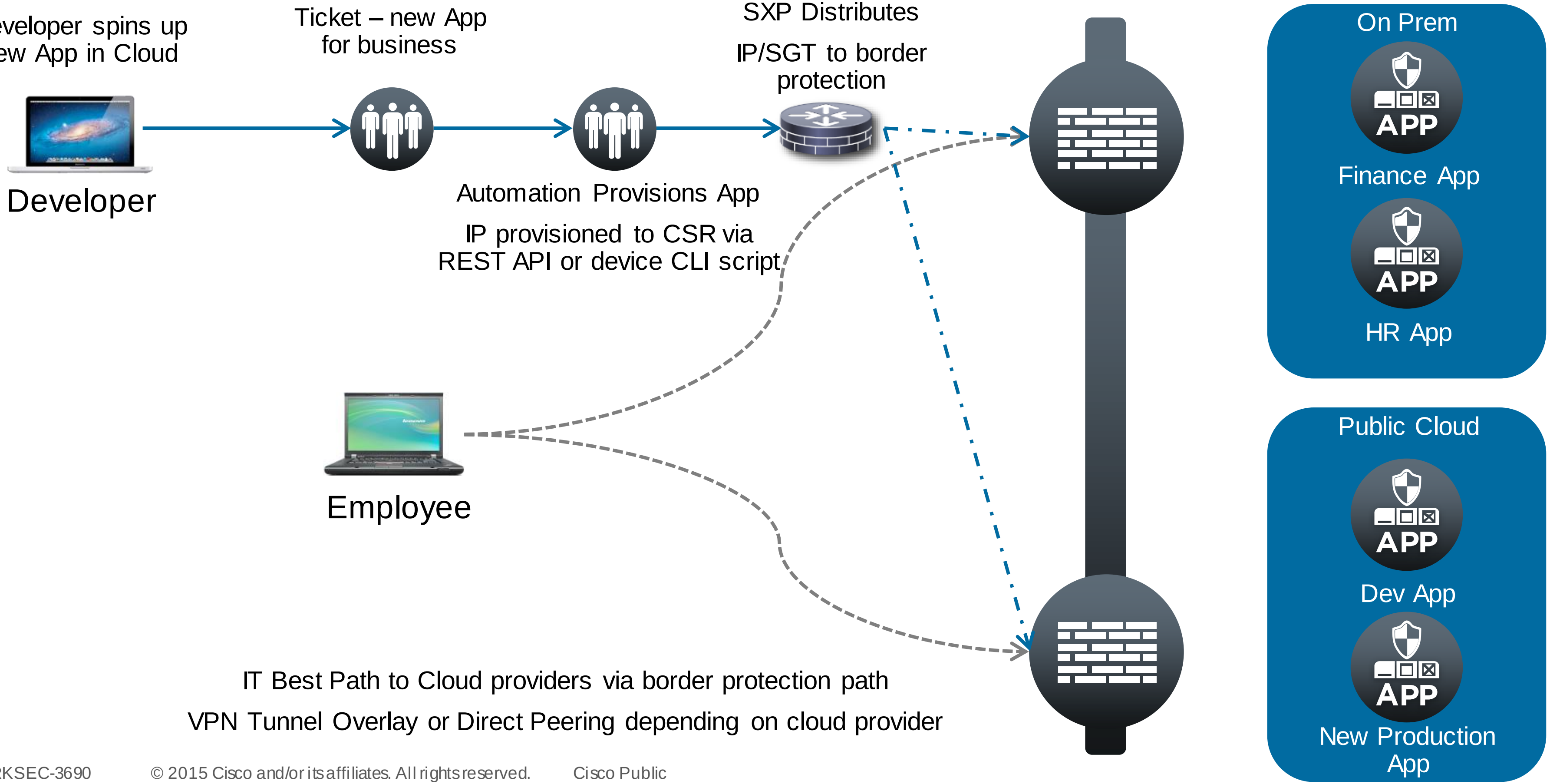
Firewall Manager push during maintenance window

Ticket – new App for business

Developer spins up new App in Cloud

© 2015 Cisco and/or its affiliates. All rights reserved.

Developer and Production Controls for Applications



Developer spins up new App in Cloud

Ticket – new App for business

SXP Distributes

IP/SGT to border protection

Developer

Automation Provisions App

IP provisioned to CSR via REST API or device CLI script

Employee

On Prem

Finance App

HR App

Public Cloud

Dev App

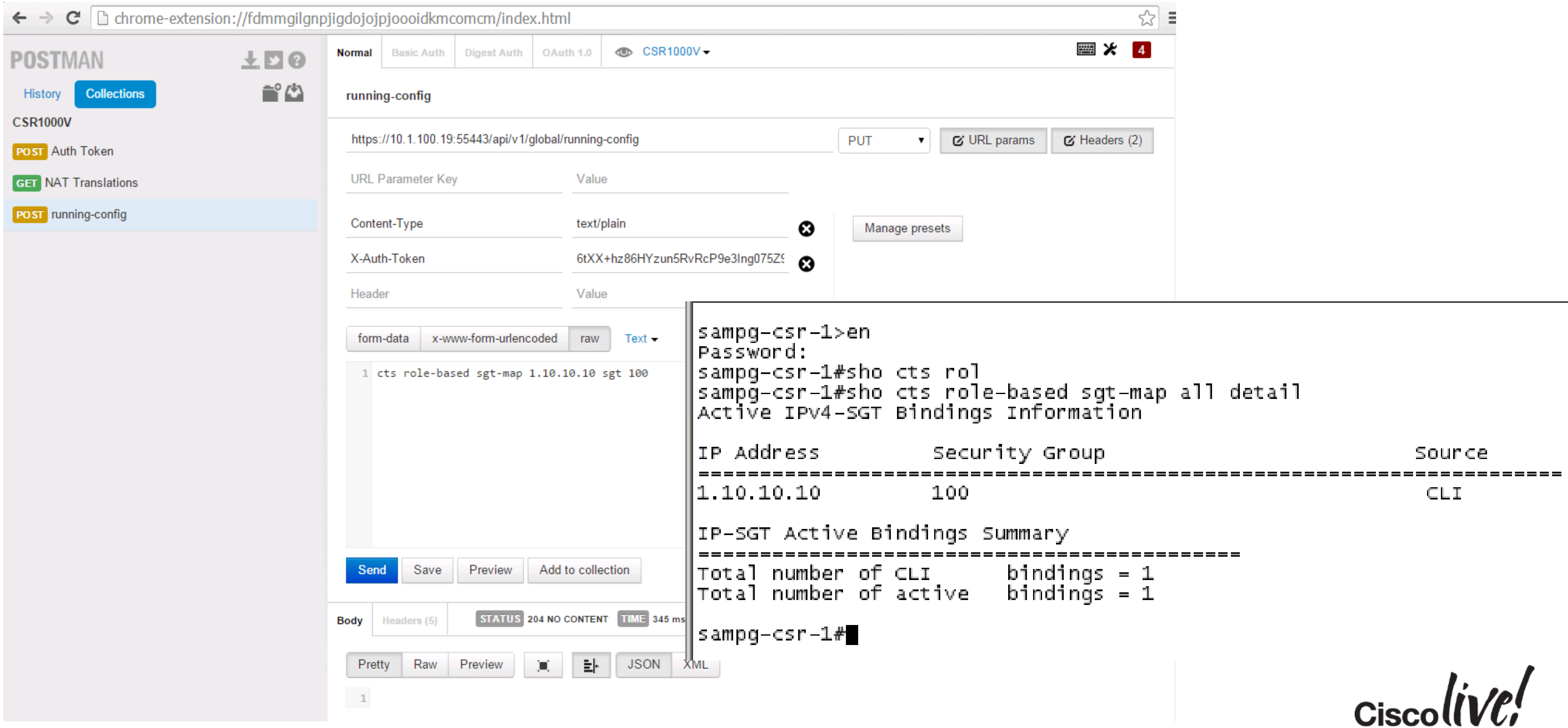
New Production App

IT Best Path to Cloud providers via border protection path

VPN Tunnel Overlay or Direct Peering depending on cloud provider

© 2015 Cisco and/or its affiliates. All rights reserved.

REST API – Cloud Services Router 1000V



CSR1000V

- POST Auth Token
- GET NAT Translations
- POST running-config

running-config

https://10.1.100.19:55443/api/v1/global/running-config — PUT

URL Parameter Key	Value
Content-Type	text/plain
X-Auth-Token	6tXX+hz86HYzun5RvRcP9e3Ing075Z
Header	Value

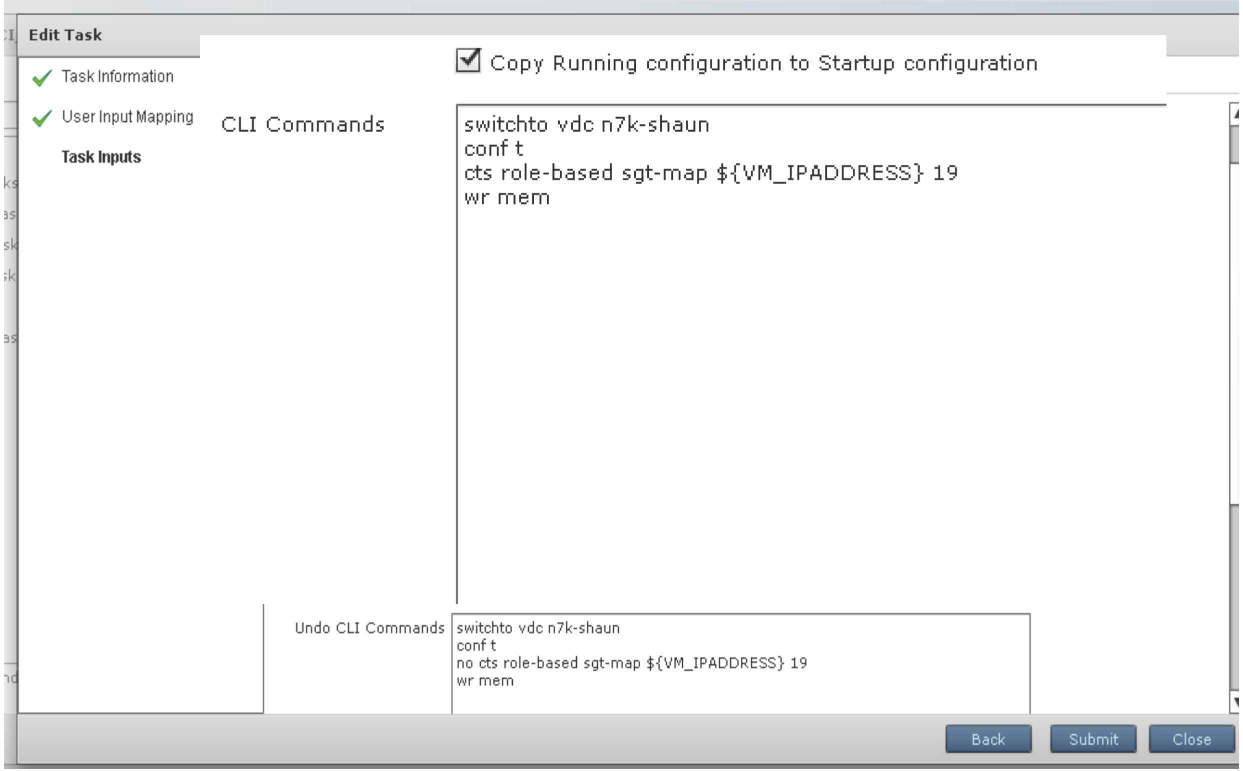
```
cts role-based sgt-map 1.10.10.10 sgt 100
```

STATUS 204 NO CONTENT TIME 345 ms

```
sampg-csr-1>en
Password:
sampg-csr-1#sho cts rol
sampg-csr-1#sho cts role-based sgt-map all detail
Active IPv4-SGT Bindings Information

IP Address              Security Group                                Source
=========================================================================
1.10.10.10              100                                            CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1

sampg-csr-1#
```

UCS Director 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
```

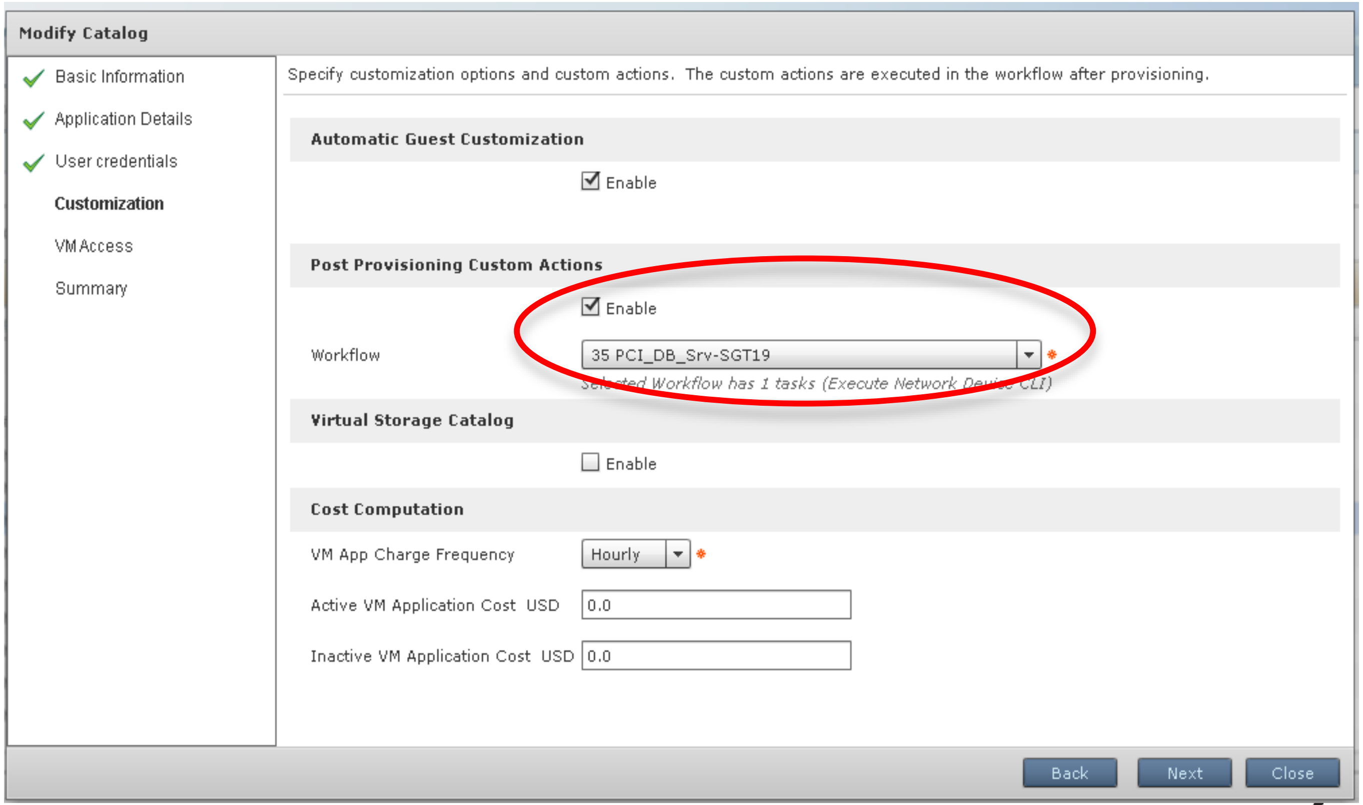
Undo CLI Commands

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

© 2015 Cisco and/or its affiliates. All rights reserved.

How to Configure UCSD for Server SGT Deployment – Cont.

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



Modify Catalog

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

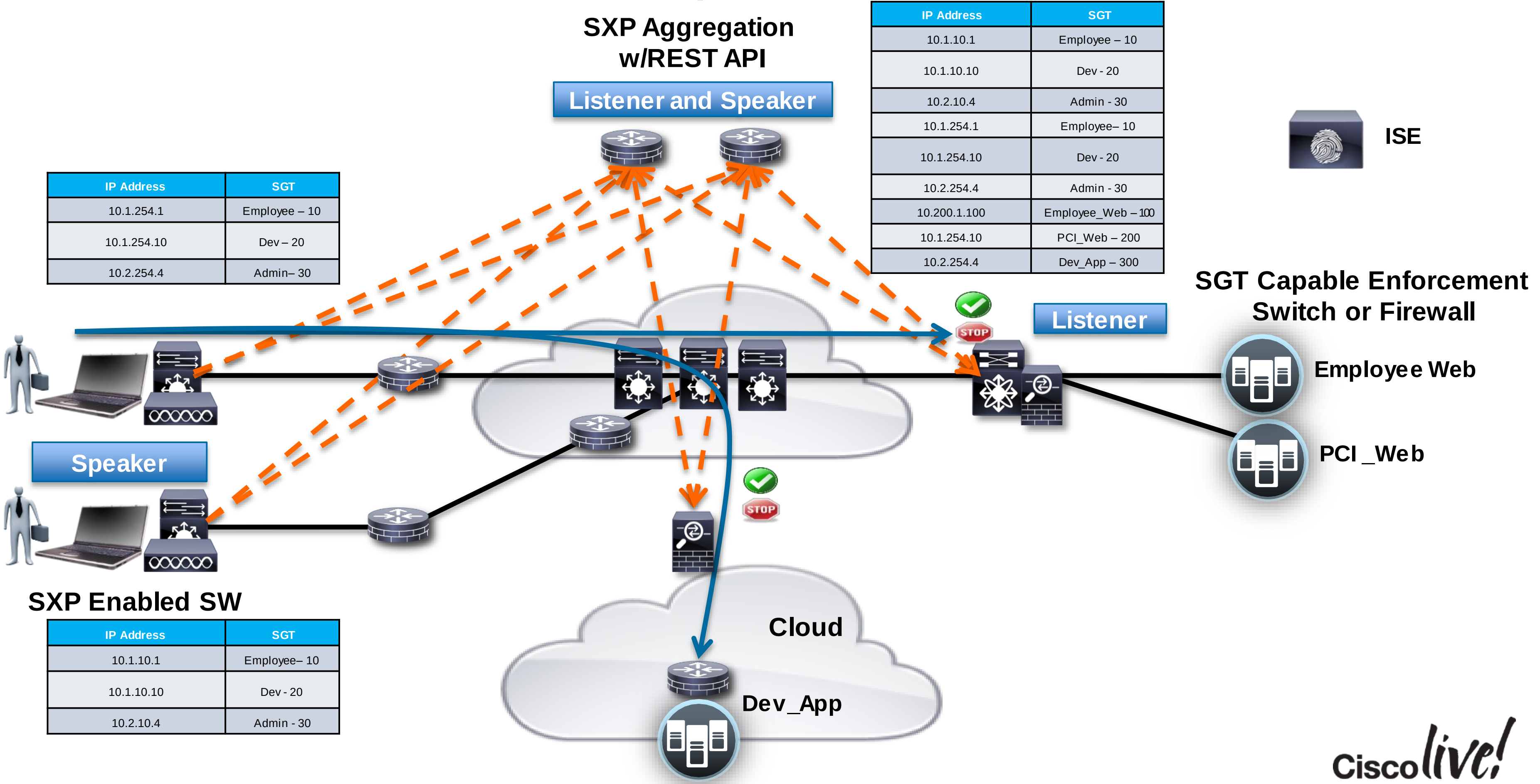
VM App Charge Frequency: Hourly *

Active VM Application Cost USD: 0.0

Inactive VM Application Cost USD: 0.0

© 2015 Cisco and/or its affiliates. All rights reserved.

Production and Dev Example



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

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

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

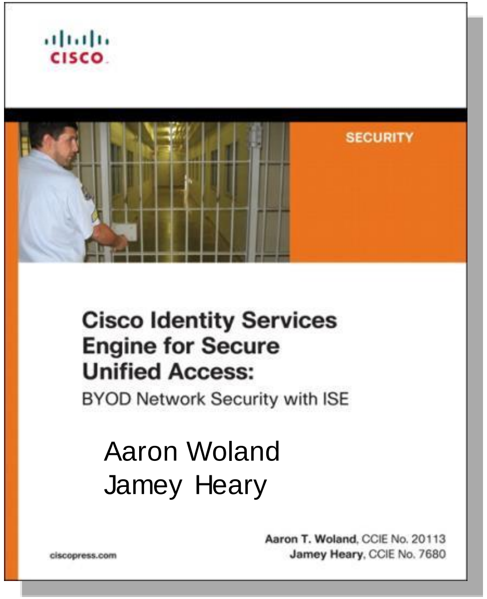
© 2015 Cisco and/or its affiliates. All rights reserved.

Summary

- TrustSec builds upon dynamic classification (802.1X), static classification (IP/SGT) and orchestration (REST, UCS Director)
- TrustSec provides a scalable Identity and Unified Access role based access control model
- TrustSec provides operational savings by decoupling security policy from the network topology
- TrustSec has broad software and hardware support and migration strategies for deployment
- TrustSec are deployed in customer environments today
- TrustSec is deployable **today in your network**

Recommended Reading

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



CISCO

SECURITY

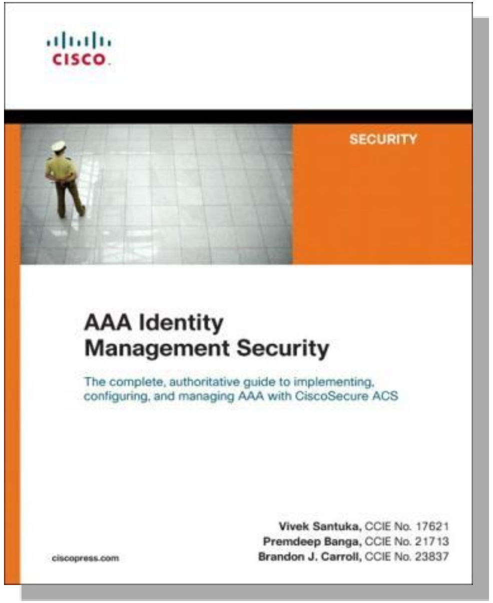
Cisco Identity Services Engine for Secure Unified Access:

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

TrustSec Related Sessions at CiscoLive Milan 2015

- TECSEC-2222 – Practical Securing Networks with Cisco TrustSec – Kevin Regan, Yuval Schrory, Darrin Miller
- TECSEC-2670 – Data Centre Security – Steinthor Bjarnason, Yves Louis, Andrew Ossipov, Fabien Gandola
- BRKSEC-2203 – Deploying Security Group Tags – Kevin Regan
- BRKSEC-1449 – Threat Defence for Enterprise Networks with Unified Access – Vaibhav Katkade
- PSOSEC-2003 – How ISE helps manage access, reach, and threat in an increasing uncontrolled environment – Kevin Skahill
- BRKSEC-3691 – Advanced ISE Services, Tips and Tricks – Aaron Woland
- BRKSEC-3502 – Advanced Enterprise Campus Design: Instant Access – Divya Rao
- BRKDCT-3578 – Building an End to End Policy Based Network: Multi-Tenant Networks using ACI Group Policy Model – Brenden Buresh
- CCSSEC-2500 – TrustSec – A Network Security Journey – Manfred Brabec, Thomas Vavra

Call to Action

- Visit the World of Solutions for
  - Cisco Campus – ISE and TrustSec, Enterprise Areas
  - Walk in Labs
  - Technical Solution Clinics
- Meet the Engineer
- Lunch time Table Topics
- DevNet zone related labs and sessions
- Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015

© 2015 Cisco and/or its affiliates. All rights reserved.

Q & A

Complete Your Online Session Evaluation

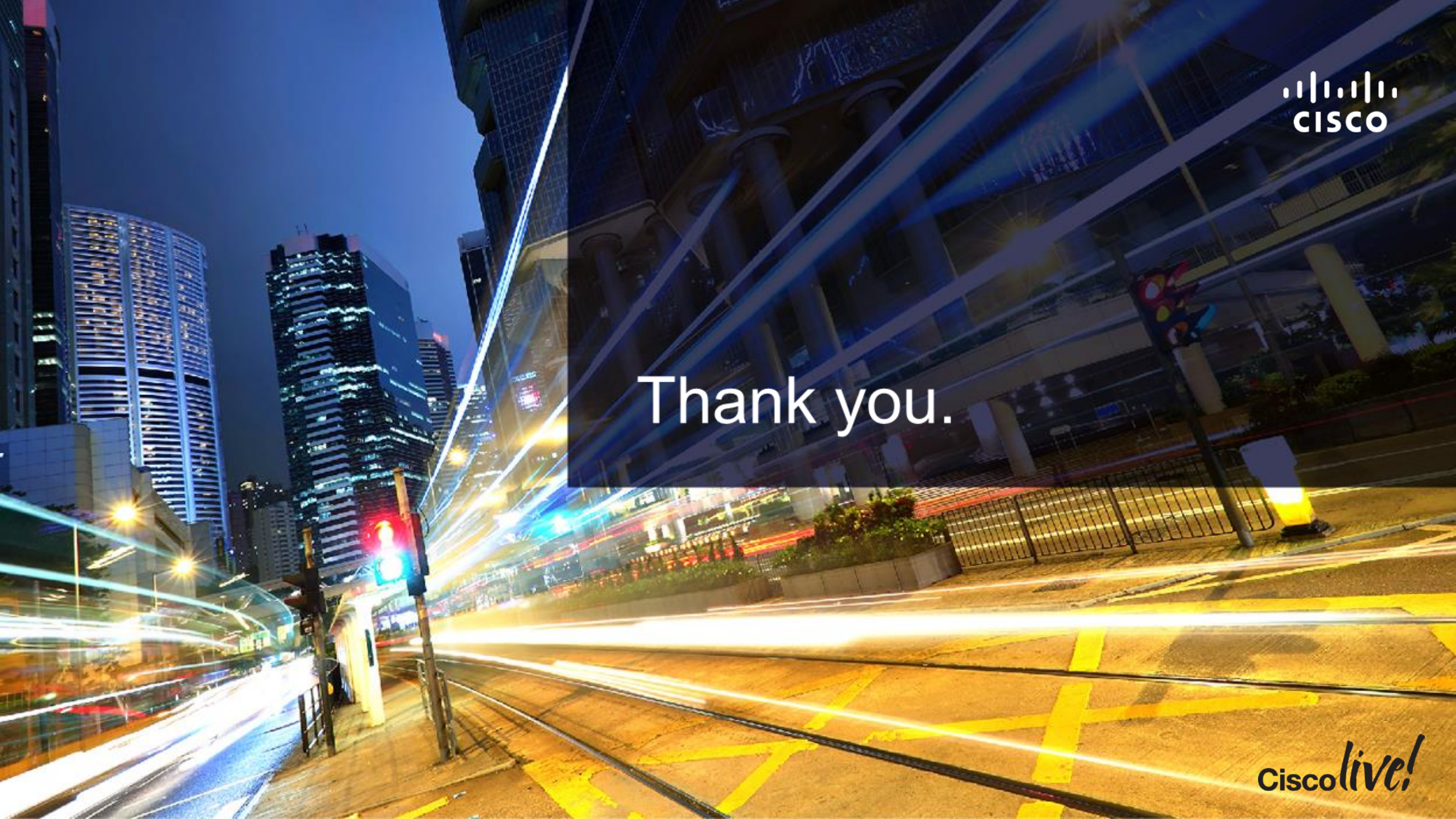
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

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

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

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



Thank you.

CISCO