Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Cisco Trustsec and Security Group Tagging

BRKSEC-2046

TOMORROW starts here.

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones

Agenda

Secure Access Overview – SGT Positioning

SGT Overview

Use Case Overview

Basic Customer Case Study Review

Summary

Top of Mind Concerns

- How do I classify so many devices coming onto my network every hour?
- Do we have an any visibility on those devices connecting to our application & data in Data Centre?
- Virtual Machine Sprawl! How should I manage security for all of those VMs we are being asked to provision everyday?
- My critical services are still running on physical servers. Do I maintain separate policies?

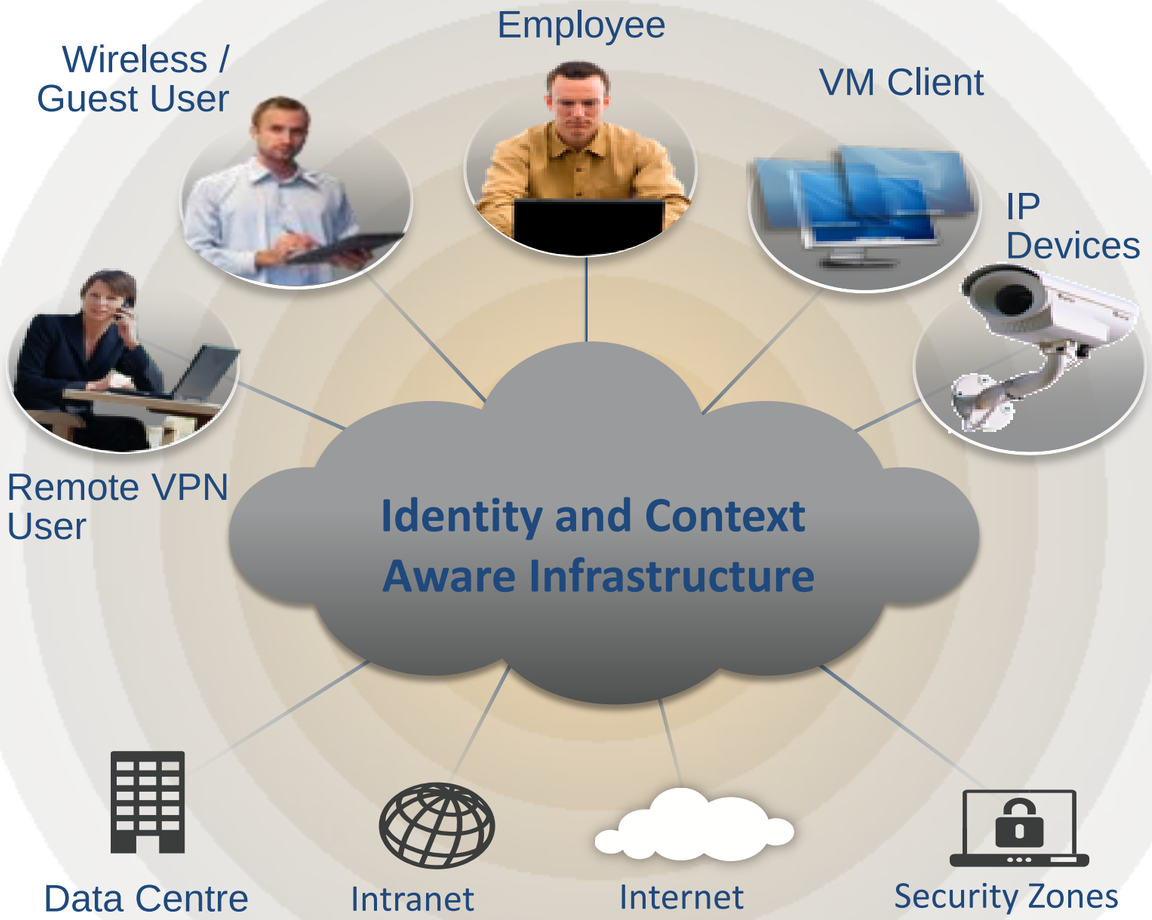
Cisco Secure Access Solution

Securely Enables Your Business with Policy Based Access Control

COMPREHENSIVE VISIBILITY

EXCEPTIONAL CONTROL

EFFECTIVE MANAGEMENT



Comprehensive Contextual Awareness of the Who, What, Where, When, How

Leverage Network to Secure Access to Your Critical Resources, Mitigating Risk and Ensuring Compliance

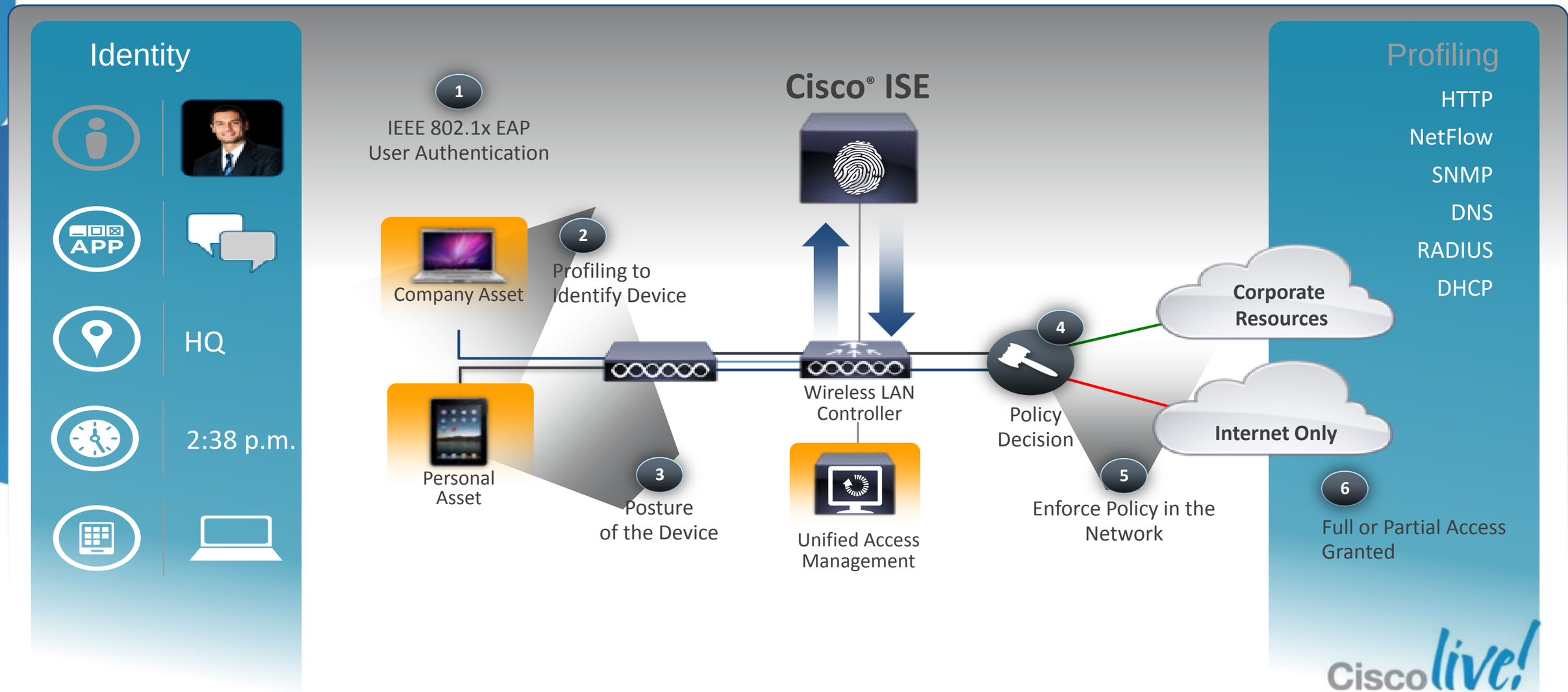
Centralised Management of Secure Access Services and Scalable Enforcement

Leveraging Your Infrastructure

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

Network Access Workflow

Policy-governed Unified Access



SGT Overview

Security Group Tag (SGT) Overview

Translating Business Policy to the Network

SGT lets you define policy
in meaningful business terms

Business Policy

Destination ▶ / Source ▼	HR Database	Prod HRMS	Storage
Exec BYOD	X	X	X
Exec PC	X	✓	X
Prod HRMS	✓	✓	X
HR Database	✓	✓	✓

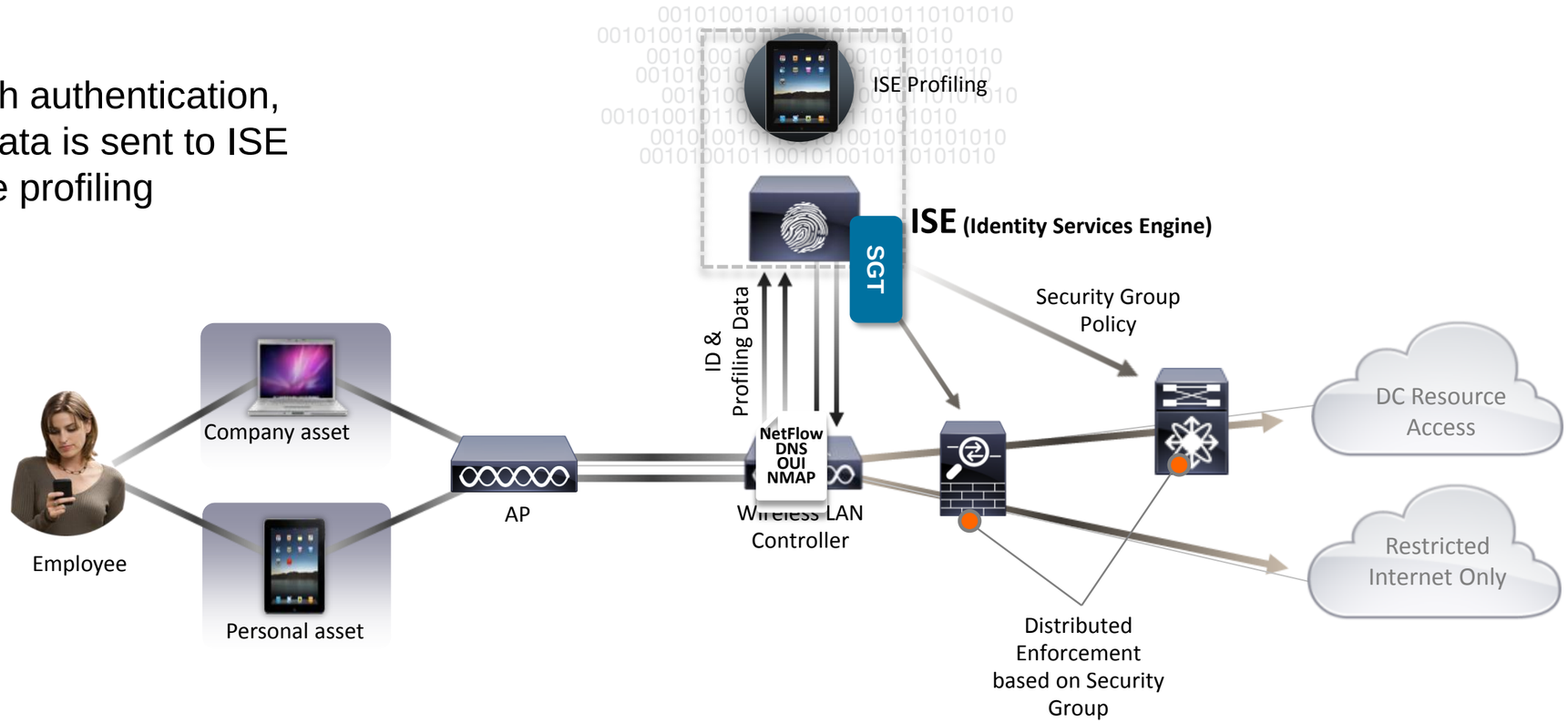
Rich Context Classification with ISE BYOD Use Case

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

Classification Result:

Personal Asset SGT

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

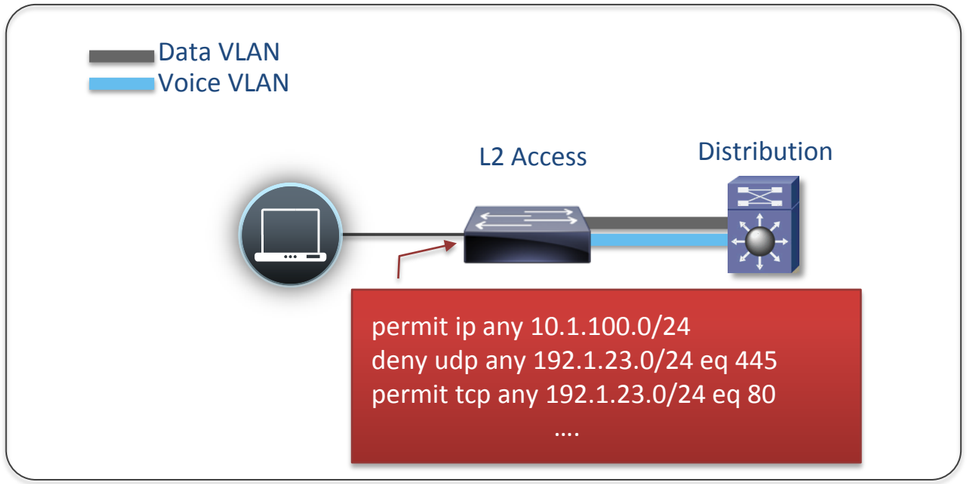


Traditional Ingress Authorisations

VLAN Segmentation

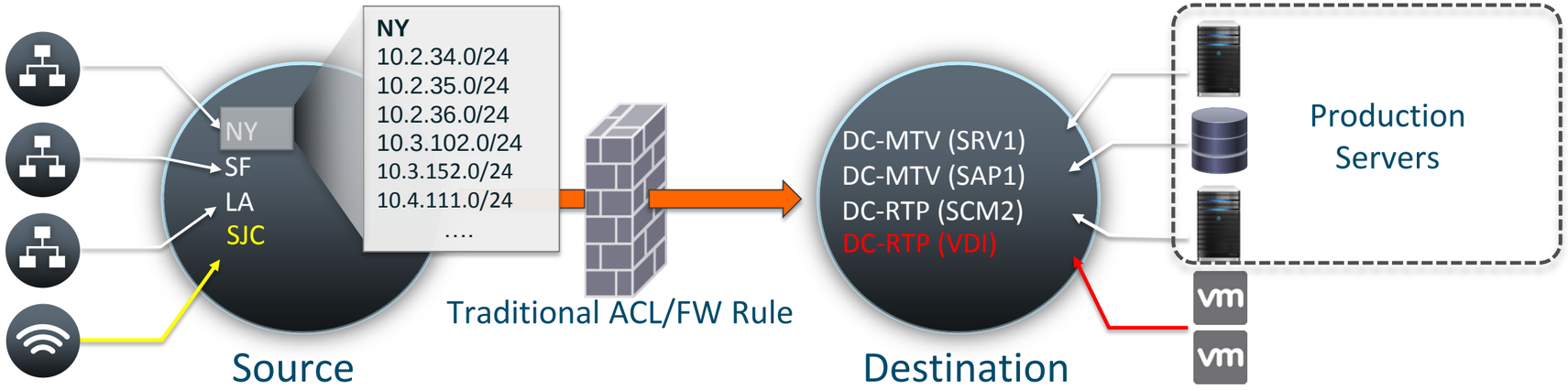
- Standard based (vendor agnostic)
- Easy implementation
- Hidden implementation costs
- Need new VLANs to everywhere
- Policy definition point and ACLs are still static
- Need to keep up with all destination change

dACL based ingress Filtering



- Access topology independent (Source Substitution)
- Centrally managed policy (Dynamic assignment)
- All protected destination needs to be defined
- Challenge to support many ACEs in TCAM
- Need to keep up with all destination changes

High OPEX Security Policy Maintenance




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

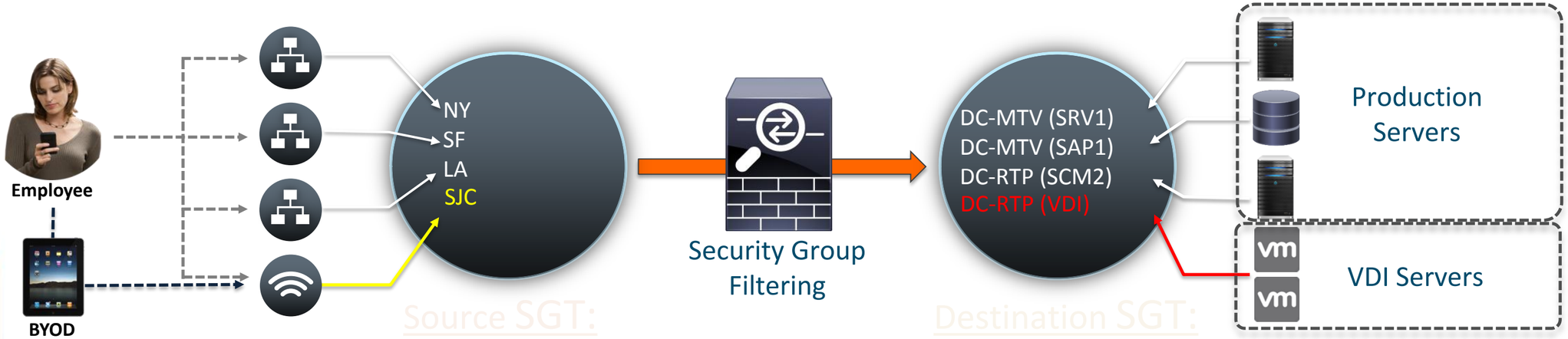
ACL for 3 source objects & 3 destination objects

Adding destination Object

A Global Bank dedicated 24 global resources to manage Firewall rules currently

Complex Task and High OPEX continues

Reduced OPEX in Policy Maintenance



Policy Stays with Users / Servers regardless of location or topology

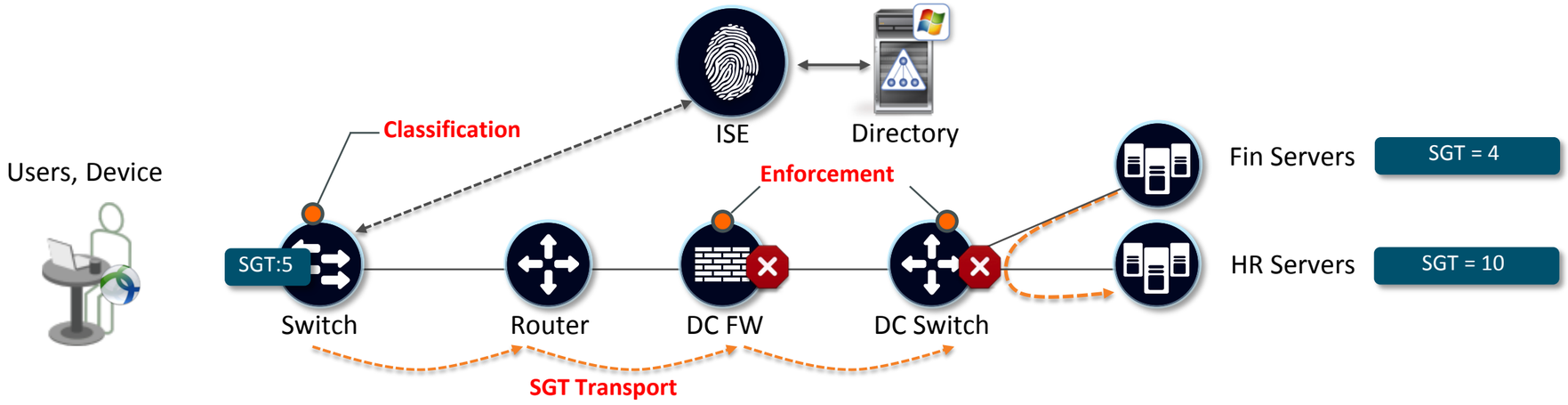
Simpler Auditing Process (Low Opex Cost)

Simpler Security Operation (Resource Optimisation)

(e.g. Bank now estimates 6 global resources)

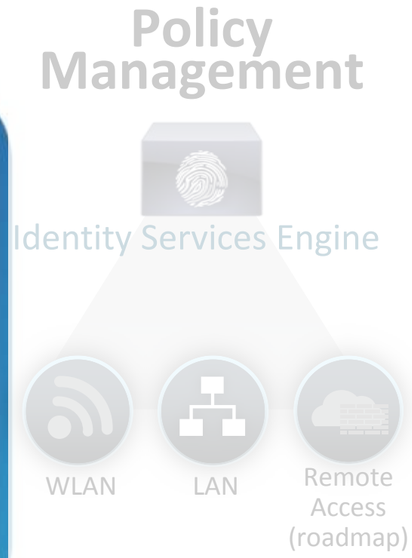
Clear ROI in OPEX

SGT In Action



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

SGT Platform Support



Classification

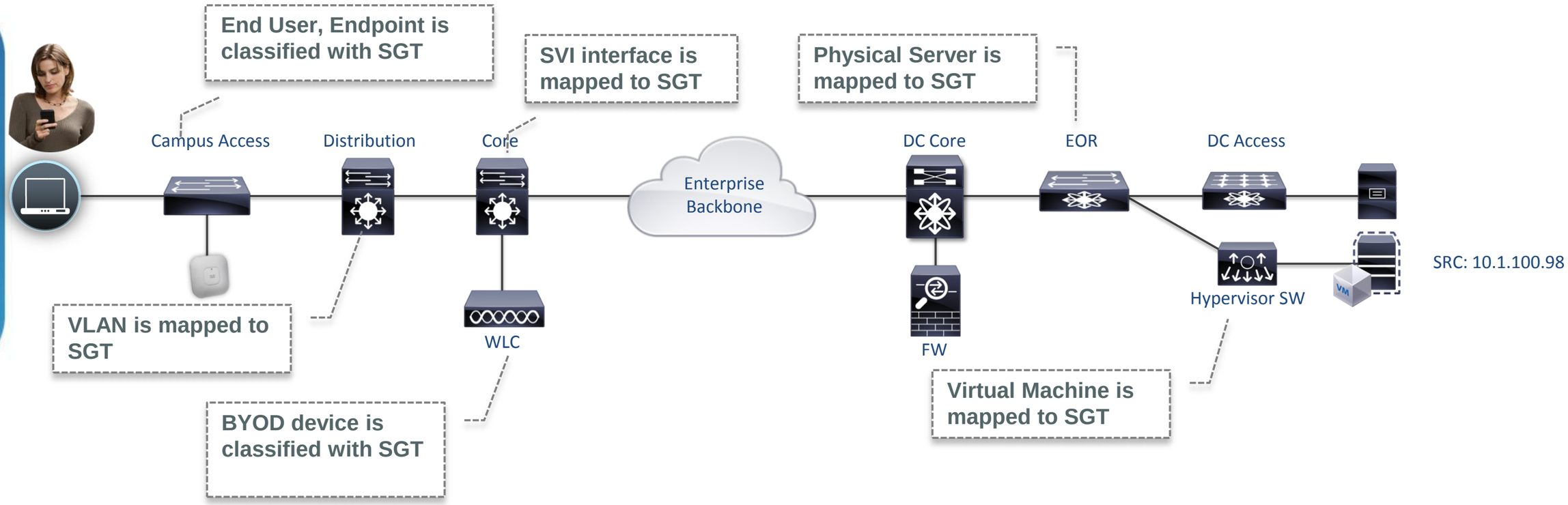
Transport

Cat 2K-S (SXP)	N7K (SXP/SGT)	ASR1K (SXP/SGT)
Cat 3K (SXP)	N5K (SGT)	ISR G2 (SXP)
Cat 3K-X (SXP/SGT)	N1Kv (SXP)	ASA (SXP)
Cat 4K (SXP)		
Cat 6K Sup720 (SXP)		
Cat 6K Sup2T (SXP/SGT)		

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

Enforcement

How SGT is Assigned (Tagged)?



SGT Classification

- Process to map SGT to IP Address
- Classification can be dynamic or static

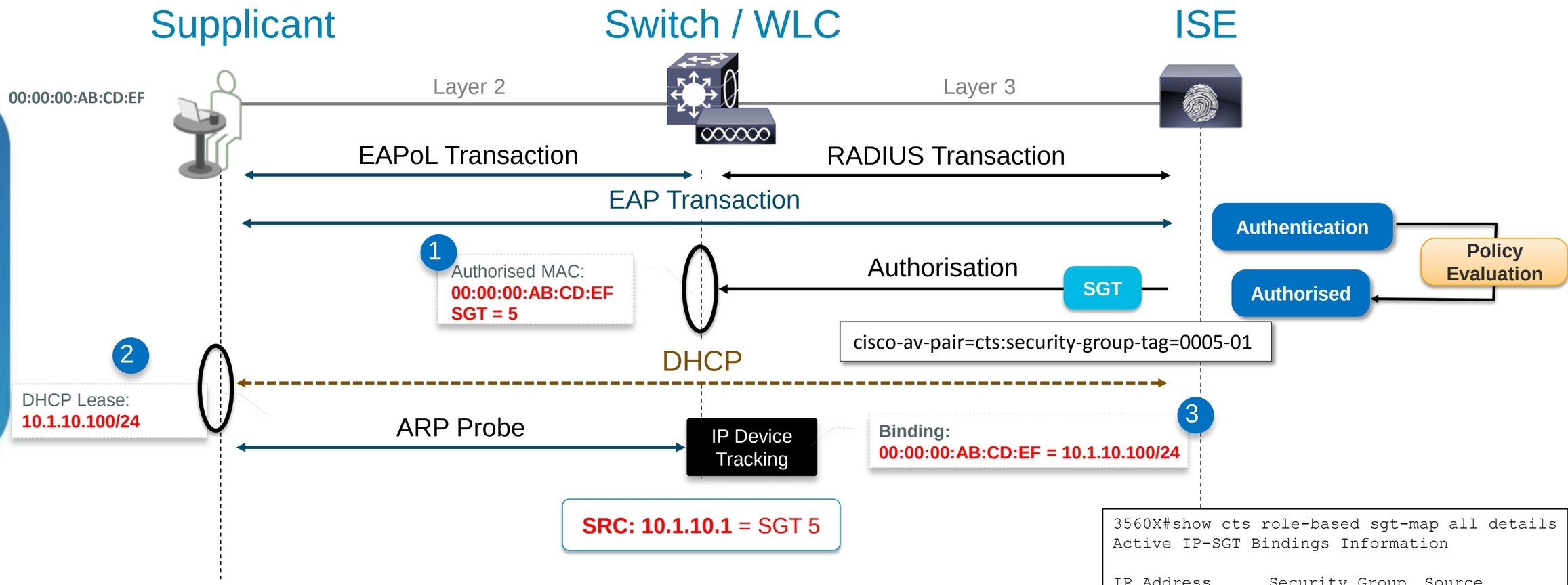
Dynamic Classification

- 802.1X
- MAC Authentication Bypass
- Web Authentication

Static Classification

- IP to SGT Mapping
- VLAN to SGT Mapping
- Subnet to SGT Mapping
- L2 Interface to SGT Mapping
- L3 Interface to SGT Mapping
- Nexus Port Profile to SGT Mapping
- Layer 2 IP to Port Mapping

Dynamic Classification Process in Detail




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

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

Make sure that IP Device Tracking is TURNED ON

ISE Being Centralised Policy Manager

Identity Services Engine

ise admin Logout Feedback

Home | Operations | Policy | Administration | Task Navigator

Authentication | Authorization | Profiling | Posture | Client Provisioning | Security Group Access | Policy Elements

Authorization Policy

Define the Authorization Policy by configuring

First Matched Rule Applies

if **RegisteredDevices** AND (Radius:Called-Station-ID MATCHES corporate-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD:ExternalGroups EQUALS cisco.com/Users/Employee) then Employee-Access AND Employee_SGT

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Black List Default	if **Blacklist**	then Blacklist_Access	Edit
✓	Employee Access	if **RegisteredDevices** AND (Radius:Called-Station-ID MATCHES corporate-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD:ExternalGroups EQUALS cisco.com/Users/Employee)	then Employee-Access AND Employee_SGT	Edit
✓	Management	if **RegisteredDevices** AND (Radius:Called-Station-ID MATCHES corporate-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD:ExternalGroups EQUALS cisco.com/Users /Management)	then Employee-Access AND Management_SGT	Edit
✓	Credit Card Scanner	if **Apple-iPhone** AND (Radius:Called-Station-ID MATCHES cc-secure-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Common Name STARTS_WITH cc-reader- AND AD:ExternalGroups EQUALS cisco.com/POS/Credit Card Scanners)	then CC-Reader-Profile AND CC_Scanner_SGT	Edit
✓	Default	if no matches, then Default-Guest-Access AND Unregist_Dev_SGT		Edit

Save | Reset

Static Classification

IOS CLI Example

IP to SGT mapping

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

L2IF to SGT mapping*

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

VLAN to SGT mapping*

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

L3IF to SGT mapping**

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

Subnet to SGT mapping

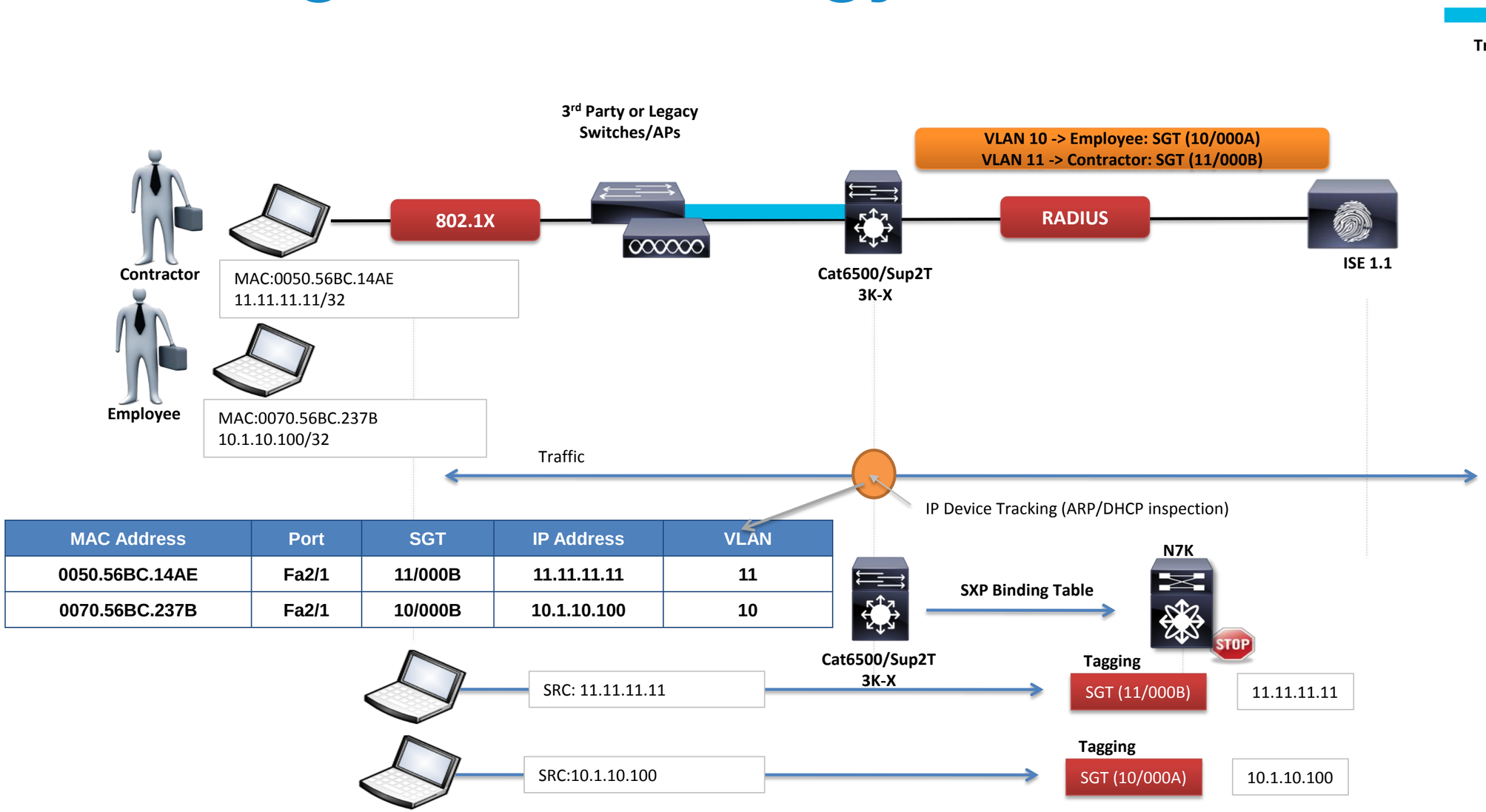
```
cts role-based sgt-map A.B.C.D/nn sgt SGT_Value
```

L3 ID to Port Mapping**

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

* - relies on IP Device Tracking
** - relies on route prefix snooping

SGT Migration Strategy – VLAN-SGT*



MAC Address	Port	SGT	IP Address	VLAN
0050.56BC.14AE	Fa2/1	11/000B	11.11.11.11	11
0070.56BC.237B	Fa2/1	10/000B	10.1.10.100	10

* - There are limits of the number of VLANs supported

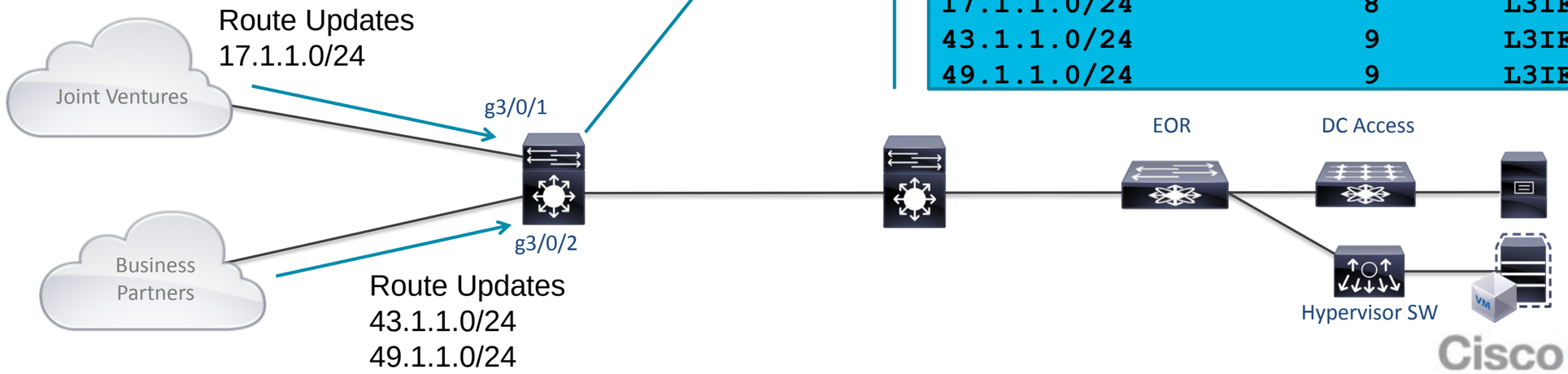
Layer 3 Interface to SGT mapping (L3IF-SGT) Sup2T 15.0(1)SY

- 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

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

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

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



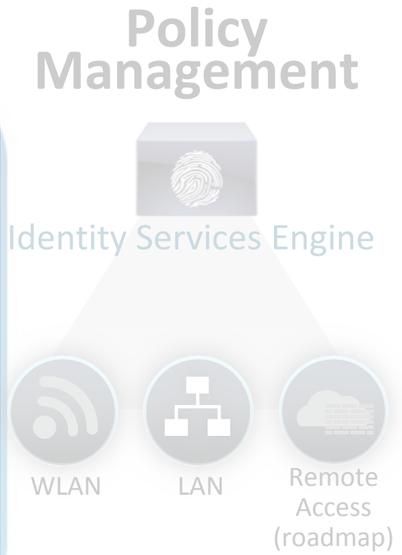
SGT Assignment

Access Layer Classification

		Cat2960-S	Cat3K	Cat4K	Cat6K	ISR	WLC	Notes
Dynamic	802.1X	X	X	X	X	X	X	
	MAB	X	X	X	X	X	X	
	Web Auth	X	X	X	X	X	X	
Static	Port Definition	X	X	-	X	-	-	
	Layer 2 Identity to Port Mapping	X	X	-	X	-	-	Dynamic query to ISE for SGT based “identity on port”
	VLAN/SGT	-	X*	-	X*	-	-	3K-X only for CY12
	Subnet/SGT	-	-	-	X	-	-	Via Sup2T
	Layer 3 Identity to Port Mapping	-	-	-	X	-	-	Based on routes learned from port via dynamic routing

* - limits on the number of VLANs per platform

SGT Platform Support



Classification

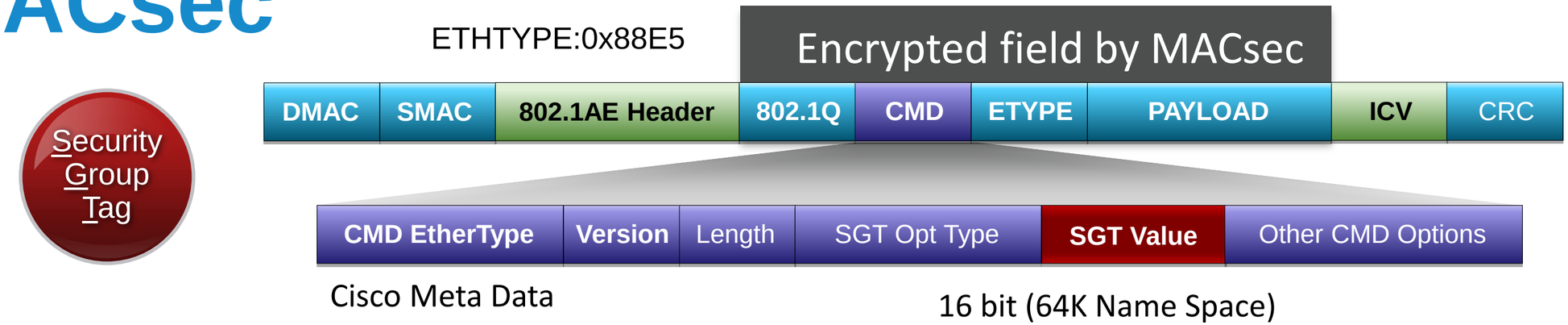
Transport

Cat 2K-S (SXP)	N7K (SXP/SGT)	ASR1K (SXP/SGT)
Cat 3K (SXP)	N5K (SGT)	ISR G2 (SXP)
Cat 3K-X (SXP/SGT)	N1Kv (SXP)	ASA (SXP)
Cat 4K (SXP)		
Cat 6K Sup720 (SXP)		
Cat 6K Sup2T (SXP/SGT)		

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

Enforcement

How Do We Want to Carry and SGT? – via MACsec



Security Group Tag

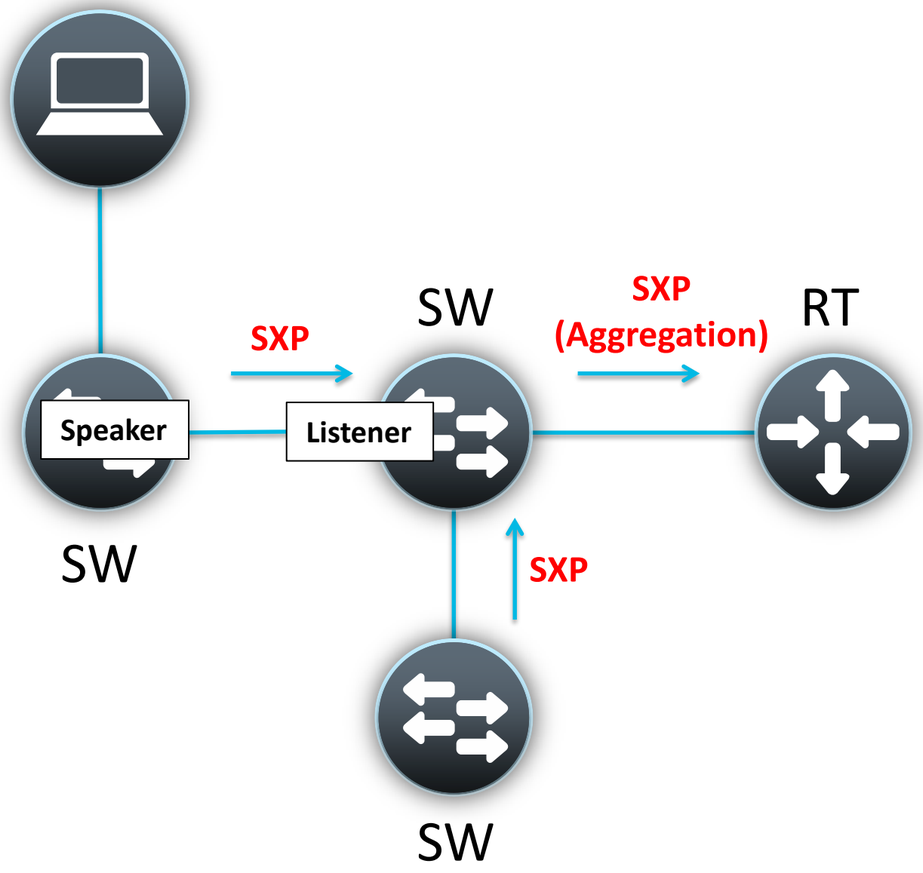
802.1AE Header | CMD | ICV are the L2 802.1AE + SGT overhead

Ethernet Frame field

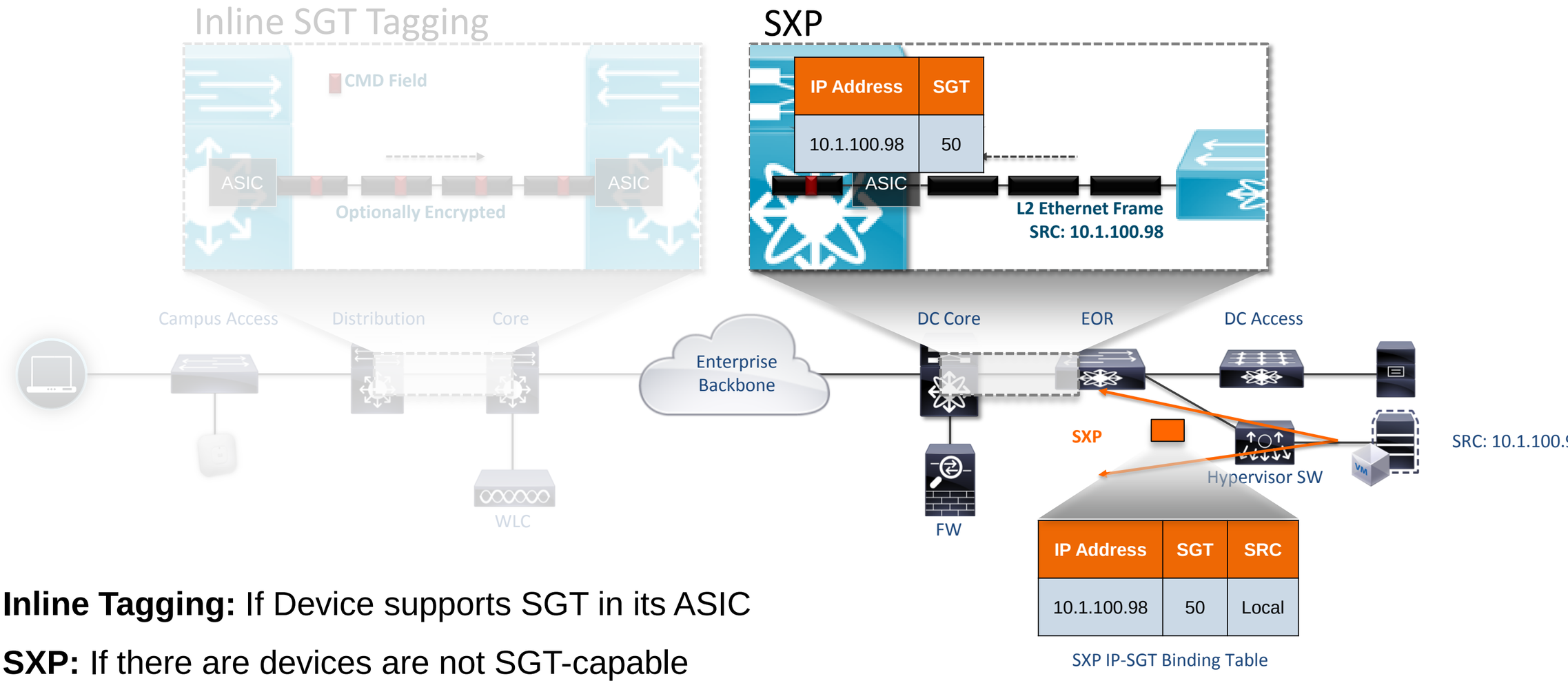
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 40 bytes = less than baby giant frame (~1600 bytes with 1552 bytes MTU)
- MACsec is optional for capable hardware

SGT Exchange Protocol (SXP)

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



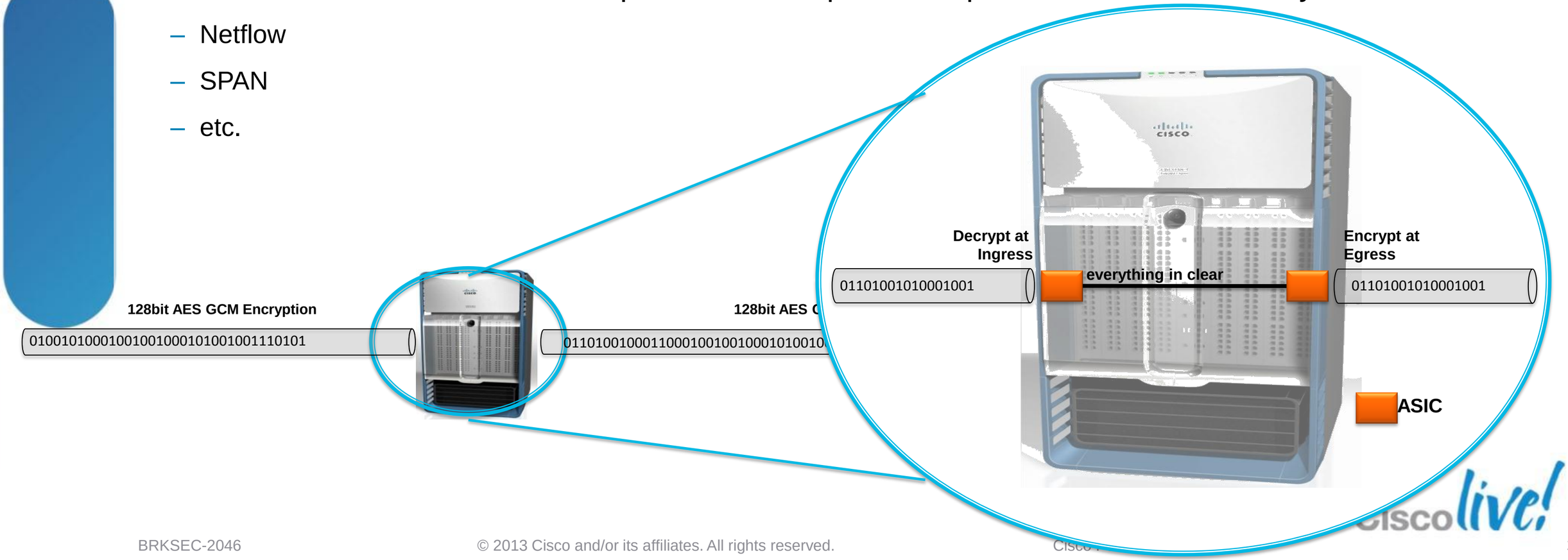
How SGT is Transported?



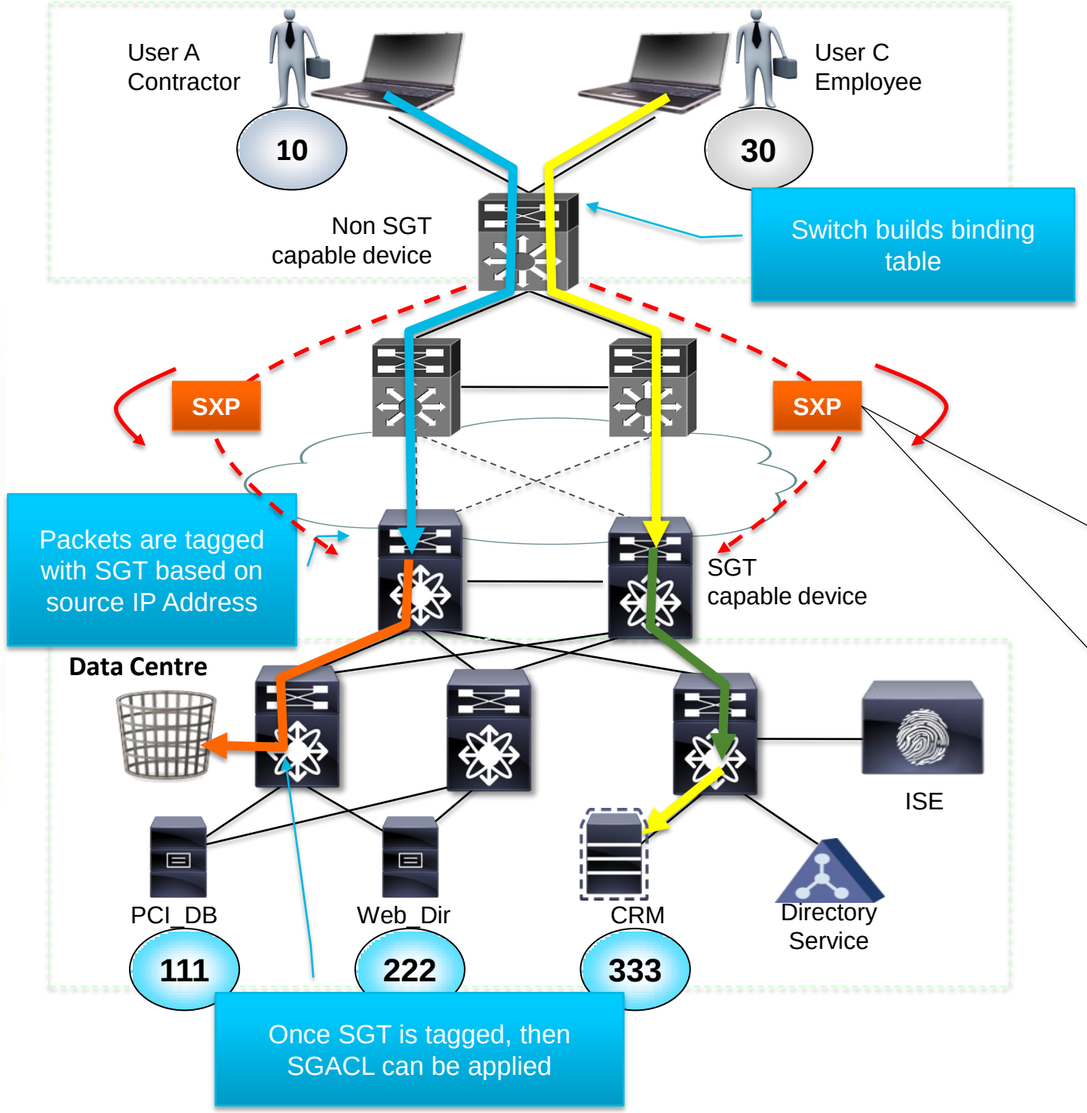
- **Inline Tagging:** If Device supports SGT in its ASIC
- **SXP:** If there are devices are not SGT-capable

Hop-by-Hop Encryption via IEEE802.1AE

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



IP-SGT Binding Exchange with SXP



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

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

SXP IP-SGT Binding Table

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

User A

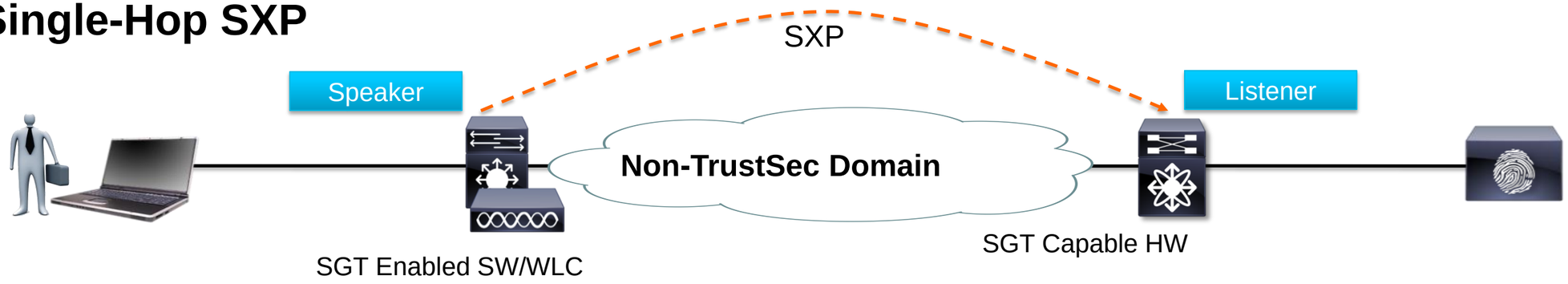
- Untagged Traffic
- CMD Tagged Traffic

User C

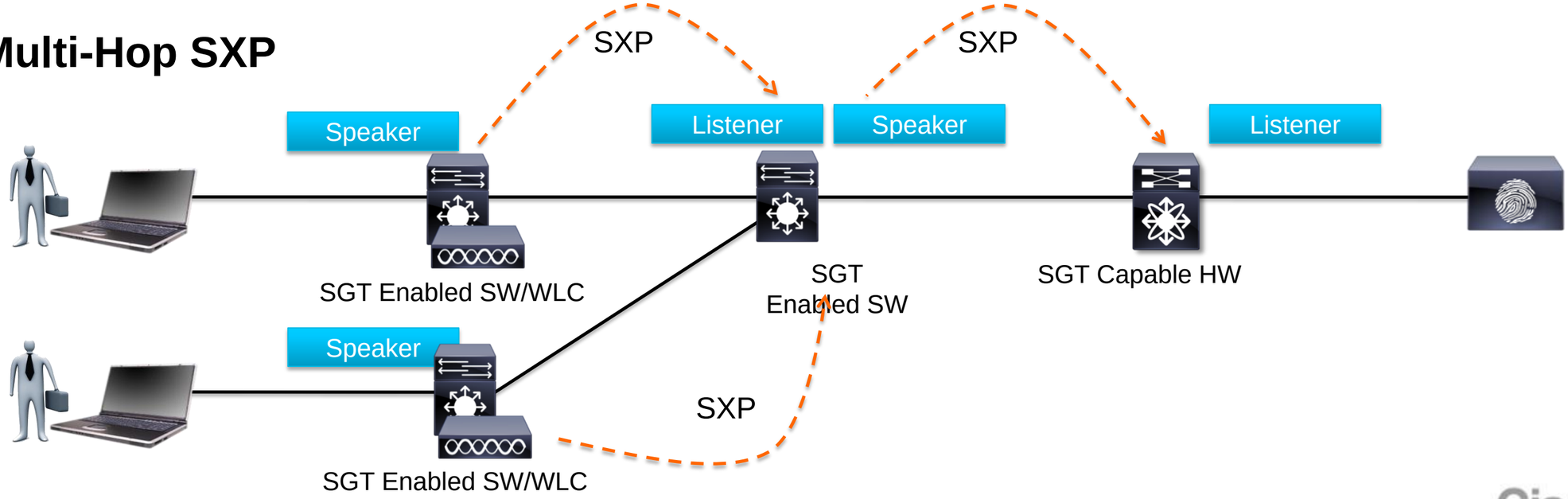
- Untagged Traffic
- CMD Tagged Traffic

SXP Connection Types

Single-Hop SXP



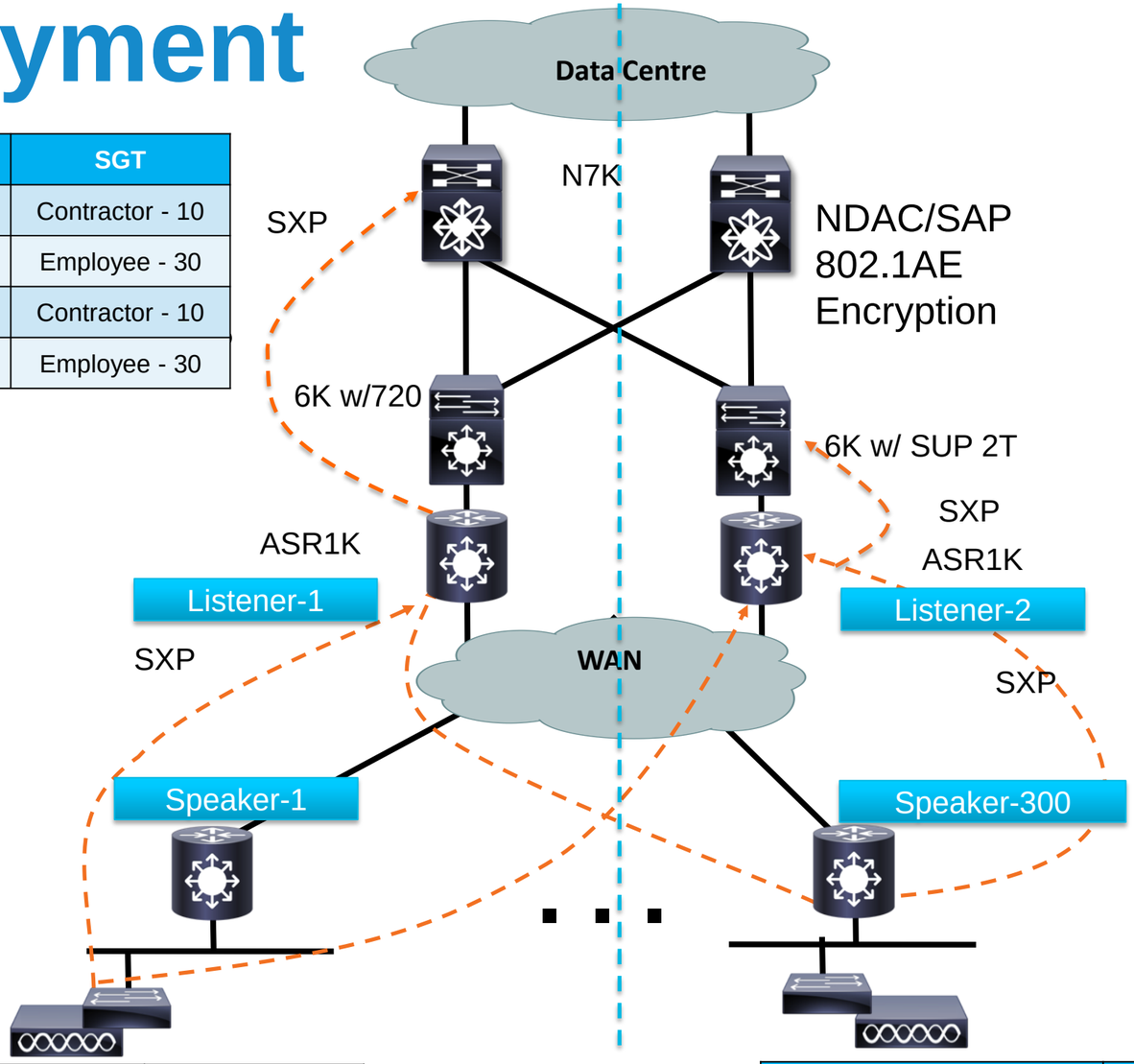
Multi-Hop SXP



SXP WAN Deployment

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

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



IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30

IP Address	SGT
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30

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

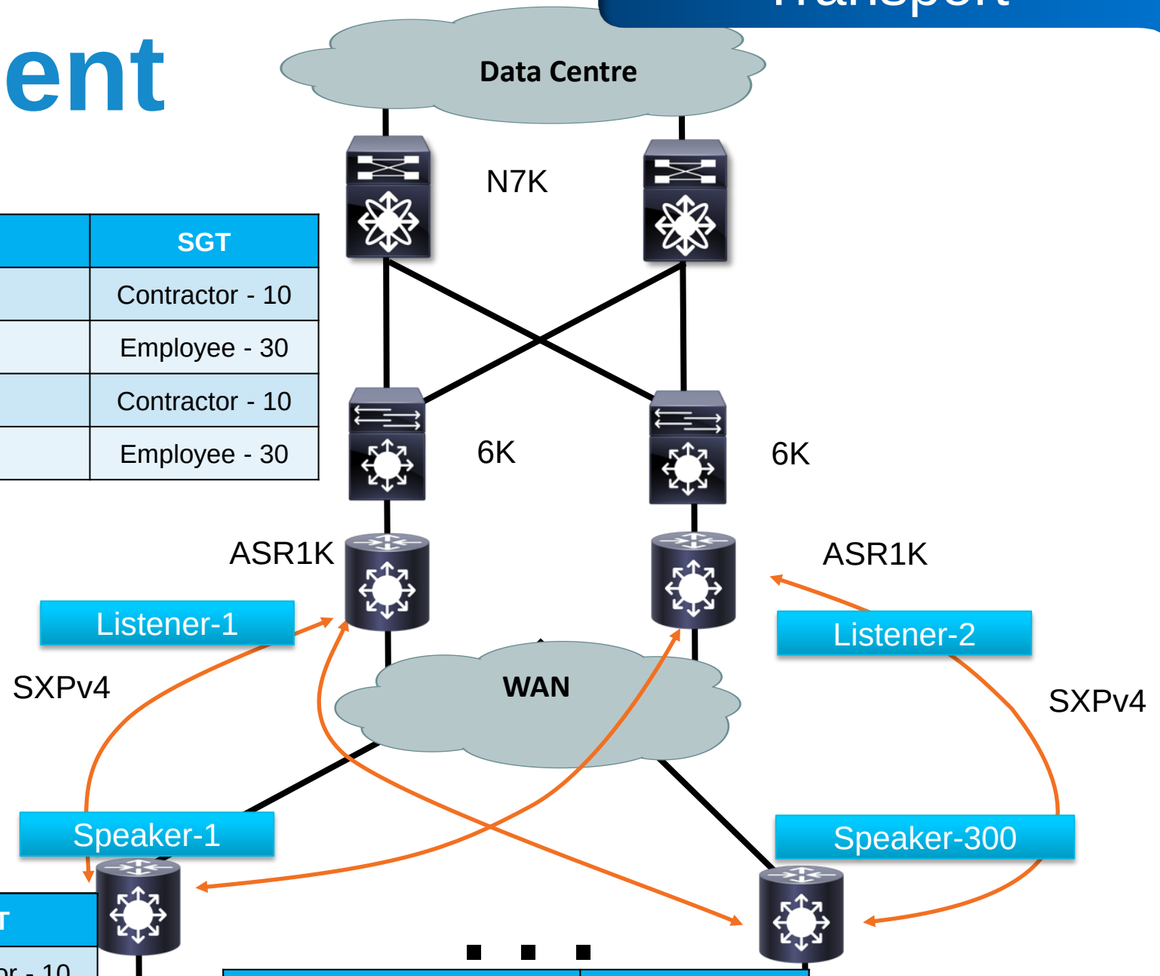
SGT/IPSEC WAN Deployment - ISRG2

- IPSEC inline Tagging – ESP Header
- SGT Capability exchange during IKEv2 negotiations
- Learn SGT from SXP or Auth-methods
- Site-to-Site IPSEC such as DMVPN, DVTI, SVTI methods supported

SXPv4 WAN Deployment

- ISRG2 – release numbering TBD
- ASR1K- 3.9
- Cat6K(SUP 2T) – MA2
- Bidirectional SXP with Loop Detection
- Allows ASR1K to be an IP/SGT relay from remote to remote
- Need to quantify scaling on ISRs since SXP is a fully replication model

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



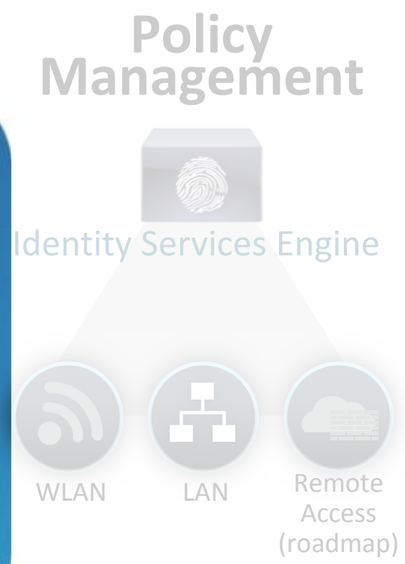
IP Address	SGT
10.1.10.1	Contractor - 10
10.1.10.4	Employee - 30
10.1.254.1	Contractor - 10
10.1.254.4	Employee - 30

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

SGT- GETVPN WAN Deployment ISRG2 15.(x)T and ASR 3.9*

- GETVPN inline Tagging – GET Header
- SGT Capability exchange during GET key negotiations
- Learn SGT from SXP, inline tag or Auth-methods
- Site-to-Site IPSEC such as DMVPN, DVTI, SVTI methods supported

SGT Platform Support



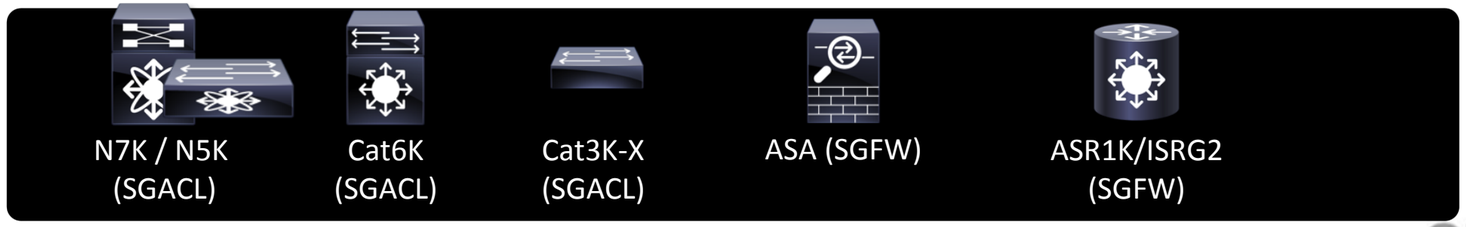
Classification

Transport

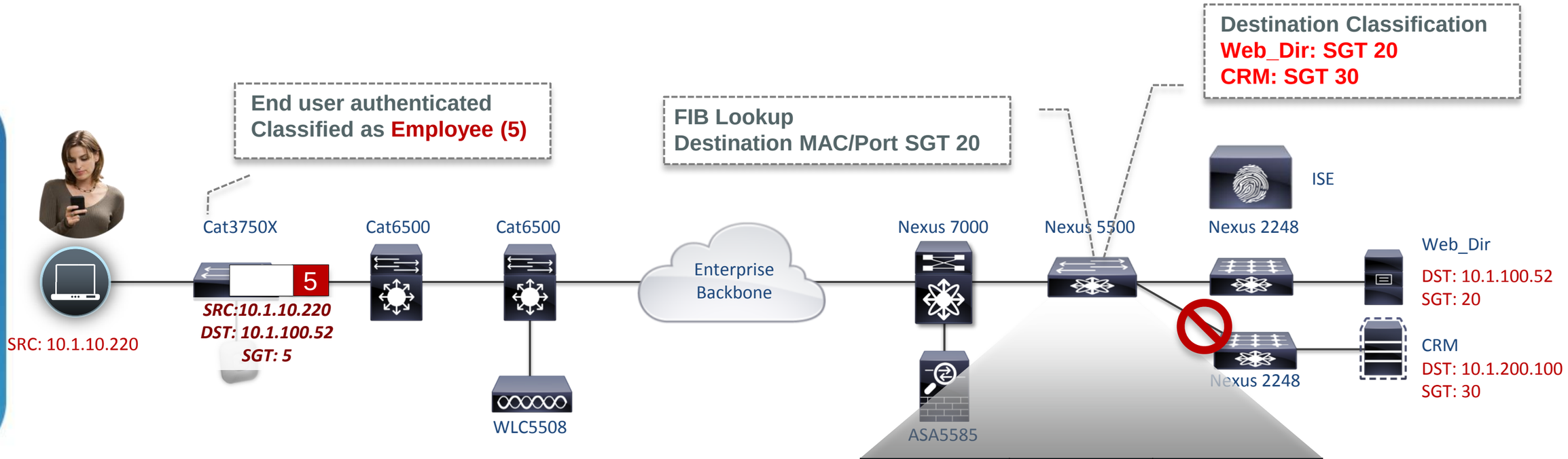
Cat 2K-S (SXP)	N7K (SXP/Inline)	ASR1K (SXP/Inline)
Cat 3K (SXP)	N5K (SXP Speaker/Inline)	ISR G2 (SXP)
Cat 3K-X (SXP/Inline)	N1Kv (SXP Speaker)	ASA (SXP)
Cat 4K (SXP)		
Cat 6K Sup720 (SXP)		
Cat 6K Sup2T (SXP/Inline)		

MACsec Capable with Tagging: Cat3K-X, Cat6K-Sup2T, N7K, N5K

Enforcement

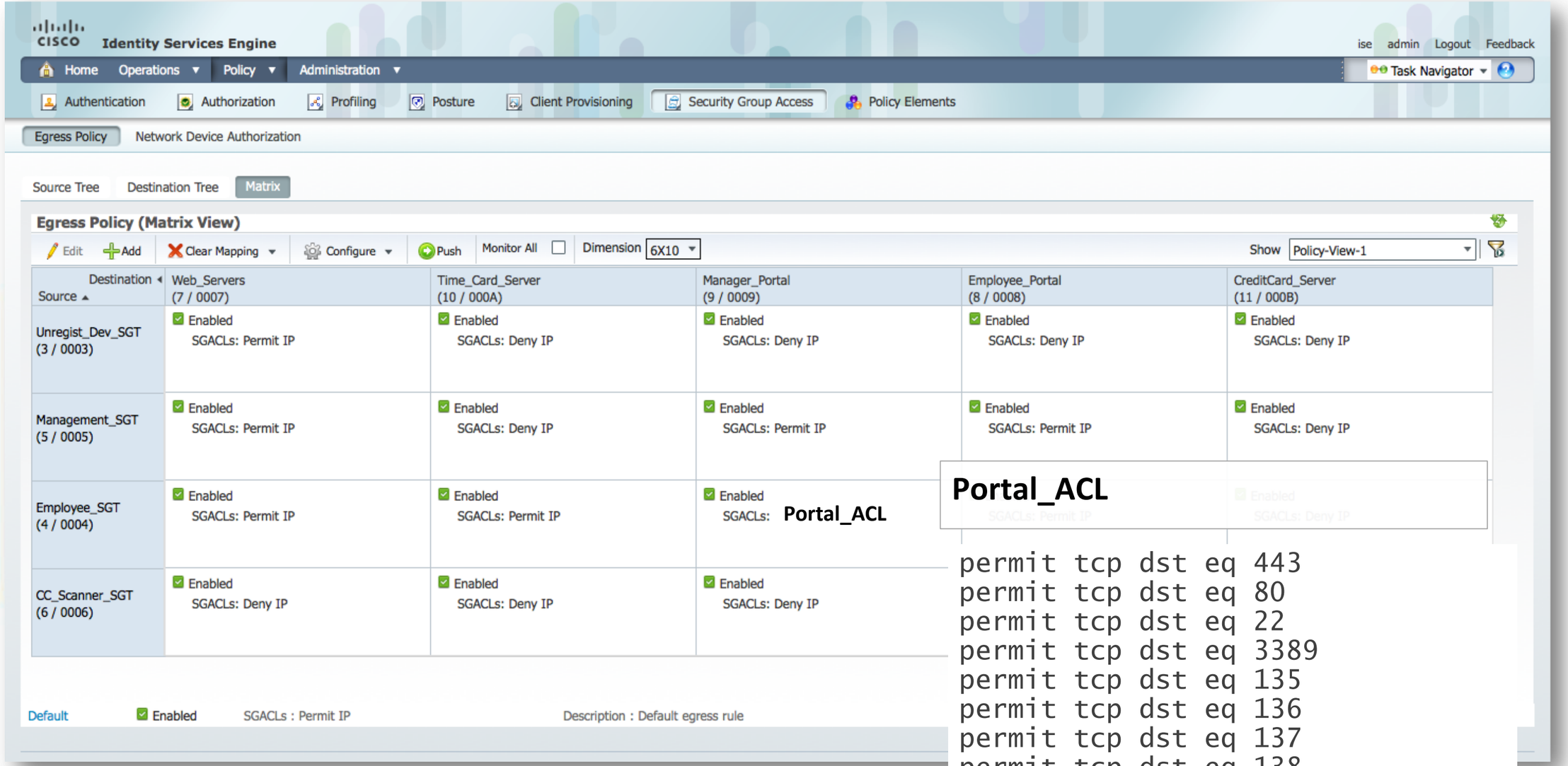


How is Traffic Enforced Using SGT?



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

Centralised Policy Management



Portal_ACL

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

Enforcing Traffic on Firewall (ASA) - SGFW

Cisco ASDM 6.7 for ASA - 10.1.201.2

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List: 10.1.201.2, 10.1.66.2

Firewall: Access Rules, NAT Rules, Service Policy Rules, AAA Rules, Filter Rules, Public Servers, URL Filtering Servers, Threat Detection, Identity Options, Identity By TrustSec, Objects, Unified Communications, Advanced

Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, Device Management

Configuration > Firewall > Access Rules

Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits	Logging	Time	Descript
inside (1 incoming rule)												
1	☑	any			any		ip	Permit				
outside (9 incoming rules)												
1	☑	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit	0			
2	☑	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny	0			
3	☑	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	Permit	0			
4	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	Deny	0			
5	☑	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit	0			
6	☑	any		Unregist_Dev_SGT Employee_SGT CC_Scanner_SGT	any	Manager_Portal	ip	Deny	0			
7	☑	any		Employee_SGT Management_SGT	any	Time_Card_Ser...	https	Permit	0			Time Card Application
8	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Time_Card_Ser...	https	Deny	0			Time Card Application
9	☑	any		CC_Scanner_SGT	any	CreditCard_Ser...	https	Permit	0			Credit Card Scan Communication
Global (1 implicit rule)												
1		any			any		ip	Deny				Implicit rule

Apply Reset Advanced...

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

SGACL Platform Support

	Cat3K-X	Cat4500E	Cat6500/Sup2T	Nexus 7000	Nexus 5000/2000
Software	15.0(2)SE	Spring, 2013	IOSIOS 12.2.50-SY	NXOS 5.2.1	NXOS 5.0(3)N2(2b)
Inline SGT Tagging	Catalyst 3750X Catalyst 3560X C3KX-SM-10G C3KX-NM-1G C3KX-NM-10G C3KX-NM-10GT	Catalyst 45xx-E WS-X45-Sup7-E WS-X4712-SFP+E WS-X4748-UPOE+E WS-X4748-RJ45V+E WS-X4748-RJ45-E	Catalyst 65xx-E VS-S2T-10G VS-S2T-10G-XL WS-X6908-10G-2T WS-X6908-10G-2TXL WS-X6904-40G-2T WS-X6904-40G-2TXL	N7K-C70xx N7K-SUP1 N7K-M108X2-12L N7K-M132XP-12 N7K-M132XP-12L N7K-M148GT-11 N7K-M148GT-11L N7K-M148GS-11 N7K-M148GS-11L N7K-M224XP-23L N7K-M206FQ-23L N7K-M202CF-22L N7K-F248XP-25	N5K-C5548P N5K-C5548UP N5K-C5596UP N5K-C5596T N2K-C2224TP N2K-C2248TP N2K-C2248TP-E N2K-C2232PP N2K-C2232TM N2K-C2148T-1GE N2K-C2224TP-1GE N2K-C2248TP-1GE N2K-C2232PP-10GE N2K-C2232TM-10GE
SGACL	15.0(2)SE	Spring, 2013	IOSIOS 12.2.50-SY	NXOS 5.2.1	NXOS 5.0(3)N2(2b)
Availability	Available Now	Available Now (requires Enterprise Services)	Available Now (requires Enterprise Services)	Available Now	Available Now

SGFW Platform Support

	ASR1000	ISR-G2	ASA
Software	IOS 15.2(1)S or IOS-XE3.5	IOS 15.2(1)T	ASA 9.0
Security Group based Firewall	PR1/PR2 ASR1001 ASR1002 ASR1004 ASR1006 ASR1000-ESP10 ASR1000-ESP20 ASR1000-ESP40 ASR1000-PR1 ASR1000-PR2 ASR1000-SIP10 ASR1000-SIP40	CISCO89x CISCO19xx CISCO29xx CISCO39xx	ASA5505 ASA5510 ASA5520 ASA5540 ASA5550 ASA5580 ASA5585-X ASASM ASA5512-X ASA5515-X ASA5525-X ASA5545-X ASA5555-X
Inline Tagging	Supported on built-in 1G interfaces	Not Supported	Not Supported
Availability	Available	Available Now	Available Now

Use Case Review

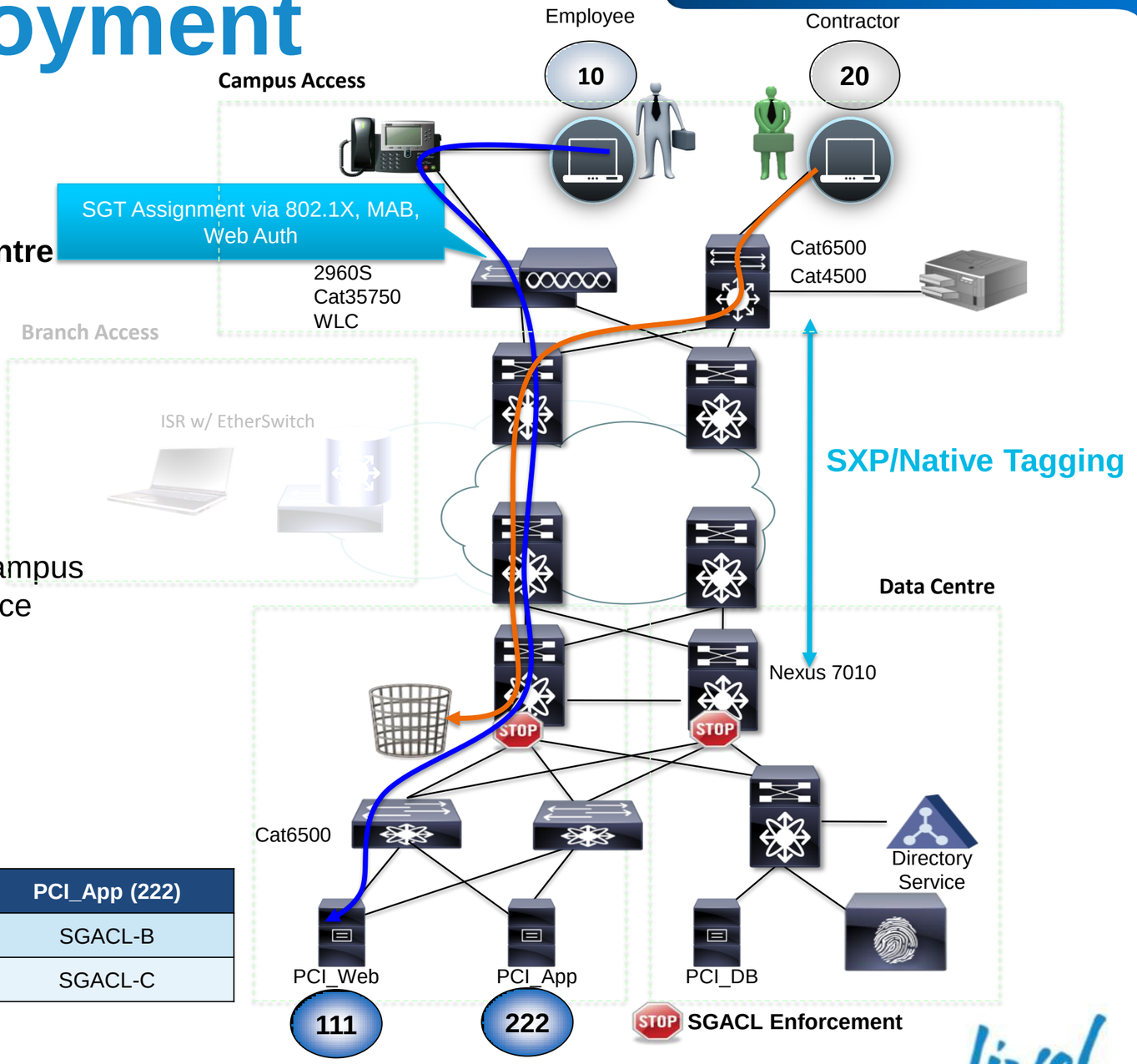
Common Deployment Questions

- What about all my other network devices that don't support SGT native tagging?
- How should I assign SGTs?
- What use cases are covered by SGTs?
- How should I phase a rollout with Identity/TrustSec/ISE services?
- How do I monitor and report on SGTs?
- How do firewalls fit with SGTs?

Campus LAN Deployment

SGT to cover campus network as well as Data Centre network

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

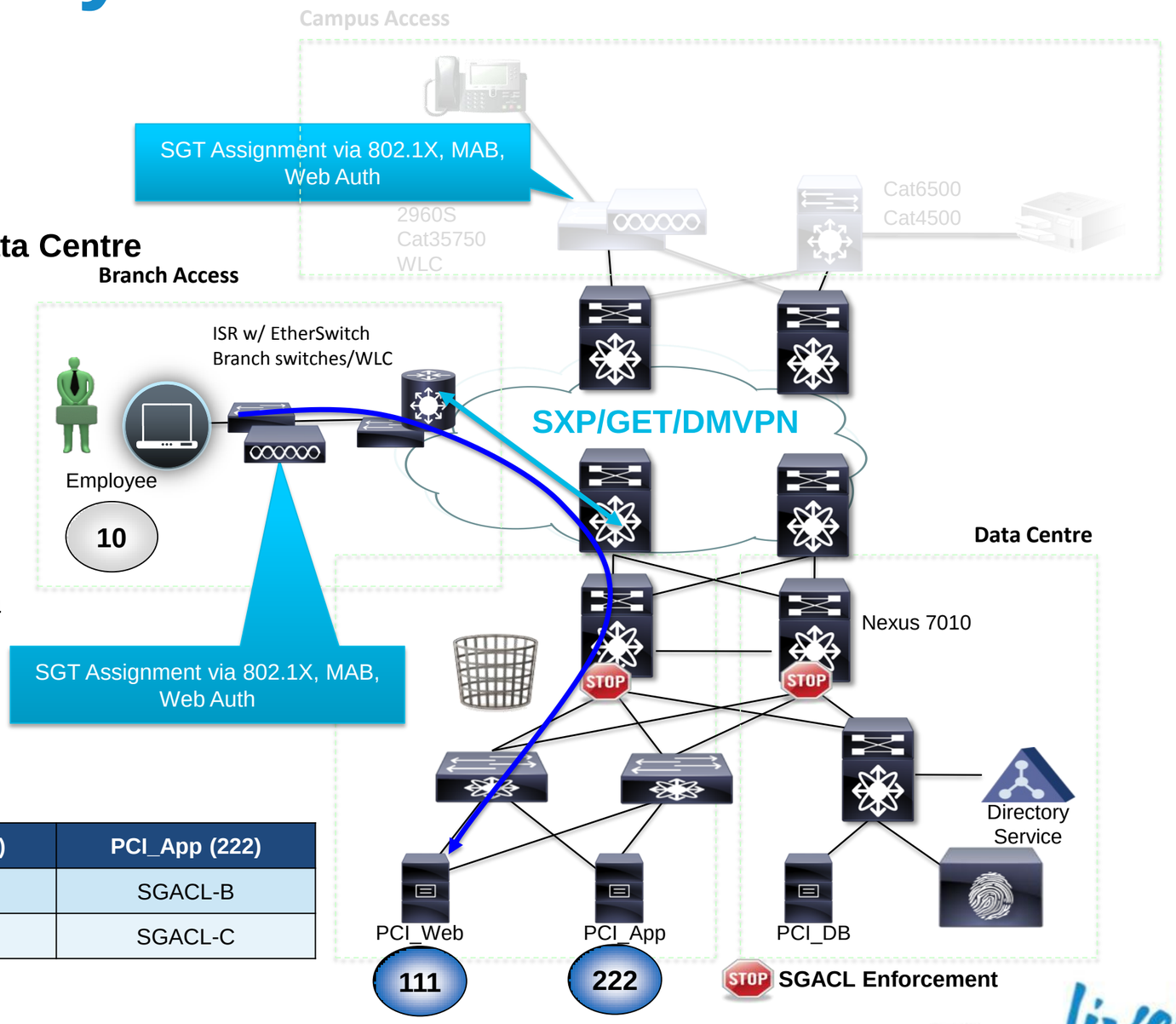


SRC \ DST	PCI_Web (111)	PCI_App (222)
Employee (10)	Permit all	SGACL-B
Contractor (20)	Deny all	SGACL-C

Branch LAN Deployment

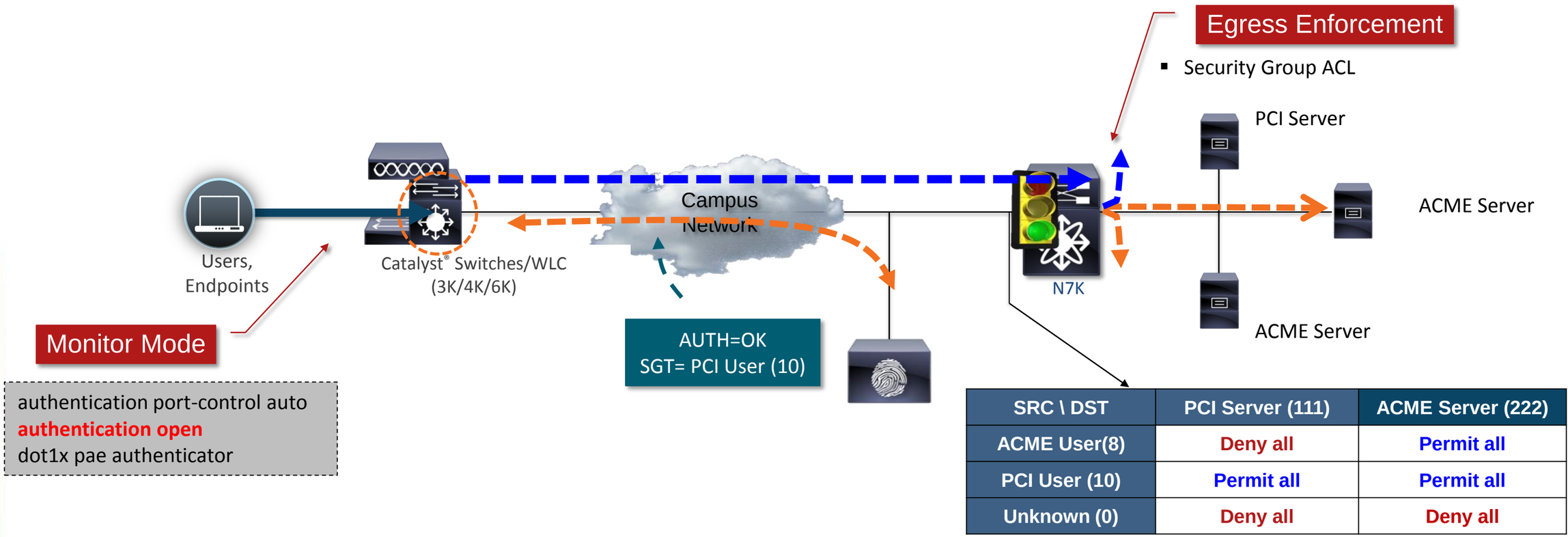
SGT to cover Branch office LAN as well as Data Centre network

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



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

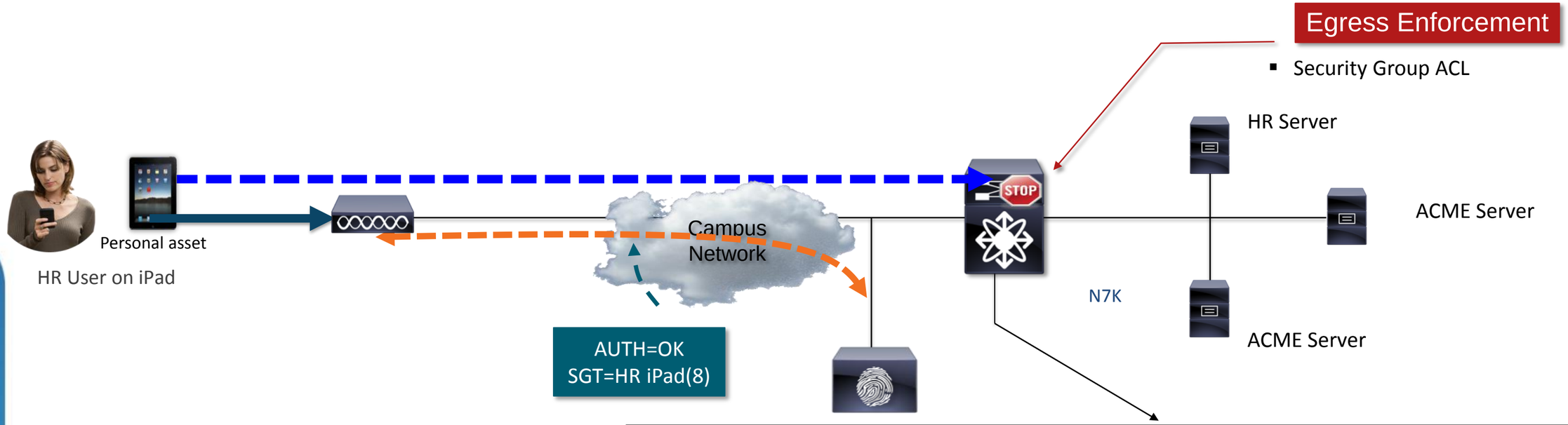
SGTs with Wired 802.1X Monitor Mode



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

1. User connects to network
2. Monitor mode allows traffic from endpoint before authentication
3. Authentication is performed and results are logged by ISE
4. Traffic traverse to Data Centre and hits SGACL at egress enforcement point
5. Only permitted traffic path (source SGT to destination SGT) is allowed

SGT with Identity – Device



SRC \ DST	HR Server (111)	ACME Server (222)	Unknown
HR iPad (8)	Deny all	Permit all	Permit all
HR User (10)	Permit all	Permit all	Permit all
Guest (30)	Deny all	Deny all	Permit all

1. User connects to network
2. Pre-Auth ACL only allows selective service before authentication
3. Authentication is performed and results are logged by ISE. dACL is downloaded along with SGT
4. Traffic traverse to Data Centre and hits SGACL at egress enforcement point
5. Traffic Denied Due to improper device of HR User

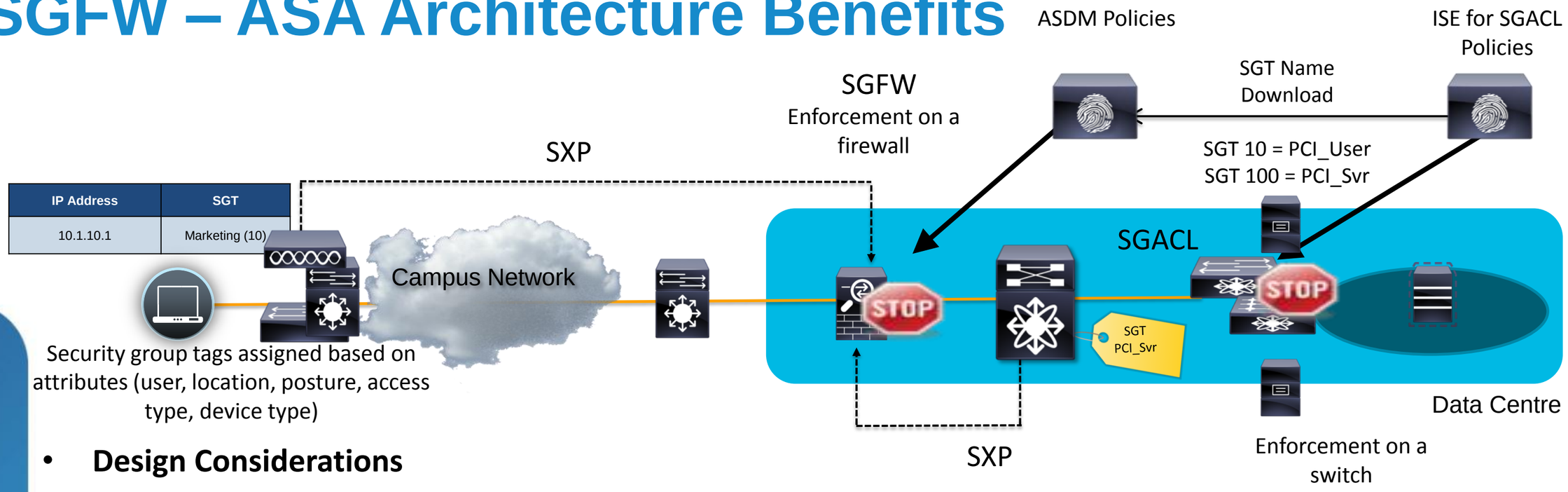
Security Group Firewall - SGFW

SGFW - Simplifying Policy and Operations

- Straight forward architecture for customers to understand
  - Policy addresses user roles and **server** roles.
  - Moves and changes do not require IP-address rule-changes.
  - New servers/users just require group membership to be established
- Enforcement scale and performance
- Common classification method for campus and data centre
- More accurate auditing for compliance

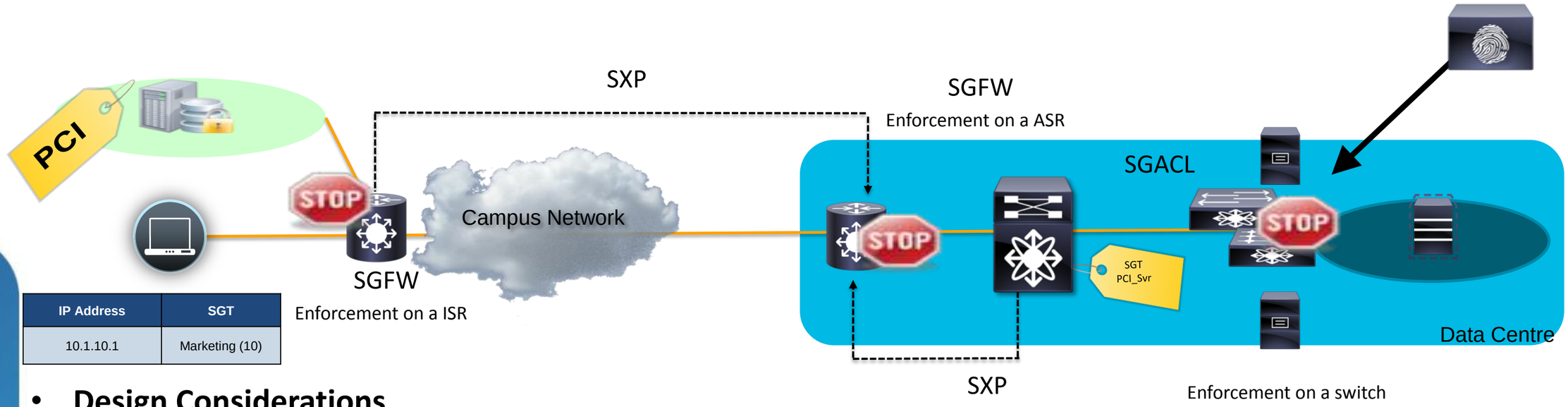
Source		Destination			Action
IP	SGT	IP	SGT	Port	Action
10.10.10.0/24	-		HIPAA Compliance Server	HTTP	Allow
Any	Web Server		PCI-Server	SQL	Allow
Any	Audit		PCI Servers	TCP	Allow
Any	Guest	Any	Any	Any	Deny

SGFW – ASA Architecture Benefits



- **Design Considerations**
  - **Consistent Classification/enforcement between FW and switching.**
  - **SGT Names will be sync'd ISE and ASDM**
  - **In general SGACL and SGFW policy should be sync'd via policy administration**
  - **Rich Logging requirements will be fulfilled on SGFW – URL logging, etc.**
  - **Switch logging is best effort via syslog (N7K/N5K) or netflow (Cat6K Sup2T)**
  - **SGACL counters vary per switch platform**
    - **Per SGT/DGT on N7K/Cat6K Sup2T**
    - **Per Platform on N5K**
  - **Future possibility to link physical switch policy with physical FW/virtual FW ppolicy**

SGFW ISR/ASR Use Case



IP Address	SGT
10.1.10.1	Marketing (10)

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

SGFW/AD Agent Policy Coexistence

- The combination also allows the FW admin to use the best technology for their requirements while still classifying consistently in the network and FWs.
- If ASA is Protecting and SGACL capable switching infrastructure SGACL Policy must equal SGACL policy
- ASA AD Agent and SGFW coexist in the ASA policy table
  - ASA AD agent rules must equal SGACL if protecting the same network
  - ASA AD agent rules can provide exceptions, but must be for non SGACL protected networks

Source			Destination			Action
IP	**AD Group/User**	**Sec Group**	**IP**	**Sec Group**	**Port**	**Action**
ANY	joeuser@cisco.com		foo.com			
ANY	ANY	**Marketing**	foo.com		http	Deny
ANY	ANY	**HR user on iPad**		**Corp-server**	http	Allow
ANY	ANY	**Audit**		**PCI servers**	https	Allow
ANY	ANY	**ANY**	ANY	**ANY**	ANY	DENY

Data Centre Policy
- SGT in the Data Centre

Security Group Access Controls in the Data Centre

Network-based functions to provide controls based on the role of the re

- Security policy defined by groups (instead of topology or design etc.)
- Resources are mapped into Security Groups
- Group-based policy rules do not change when resources are moved
- **Potential for much reduced SecOps effort** in the DC

Segmentation

- Logical separation of resources across common DC infrastructure
- Segment servers into logical zones
- Control access to these different logical DC entities based on role
- Apply controls to physical or virtual systems (Virtual servers, VDI…)

Use Case: Segmentation

Physical or VM server Segmentation for Compliance

Security Group Firewalling

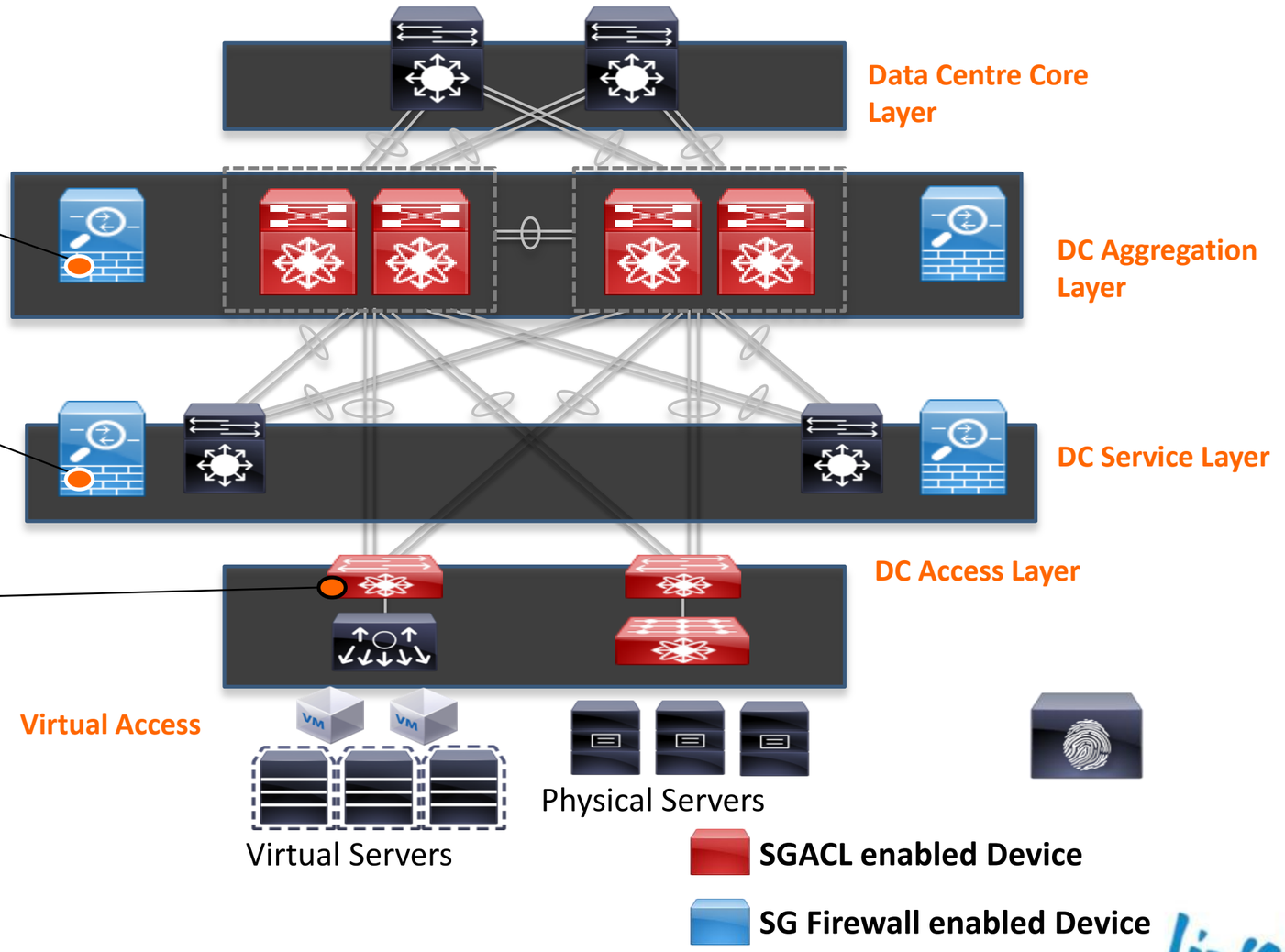
Firewall rule automation
using ASA SG-Firewall functions

Security Group Firewalling

Firewall rule automation
using ASA SG-Firewall functions

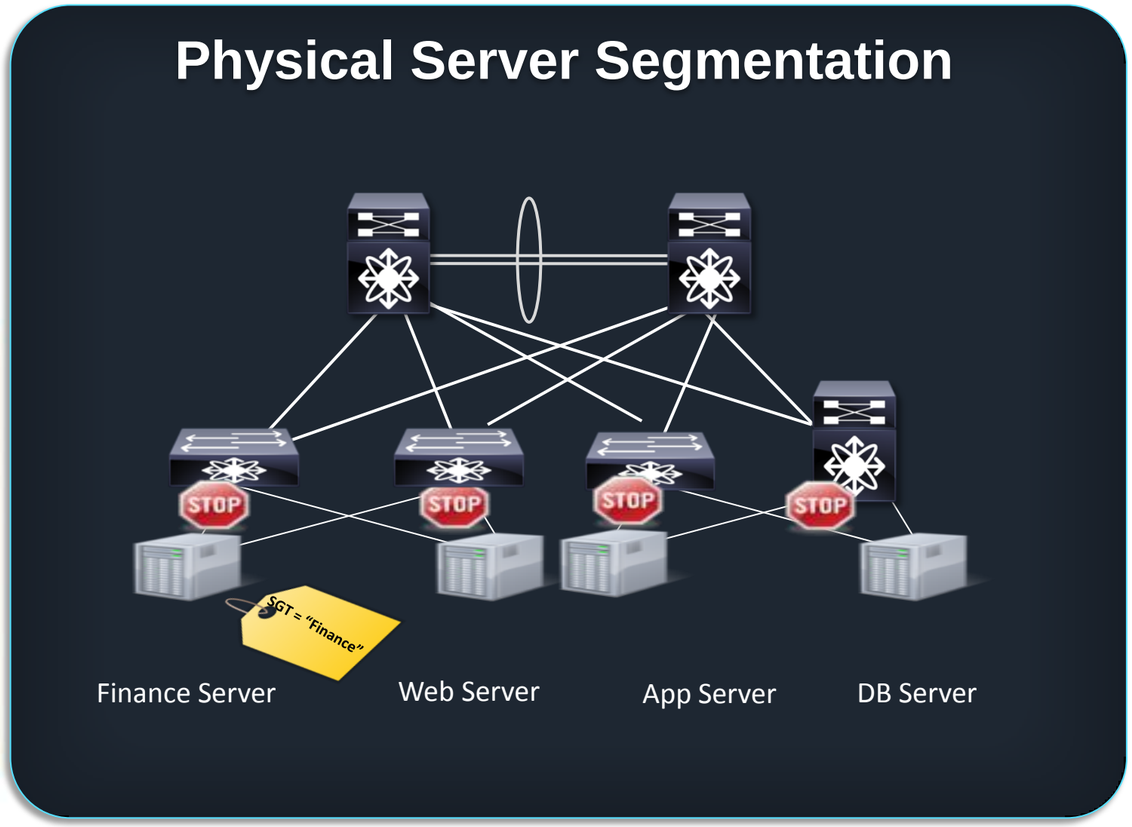
Security Group ACLs

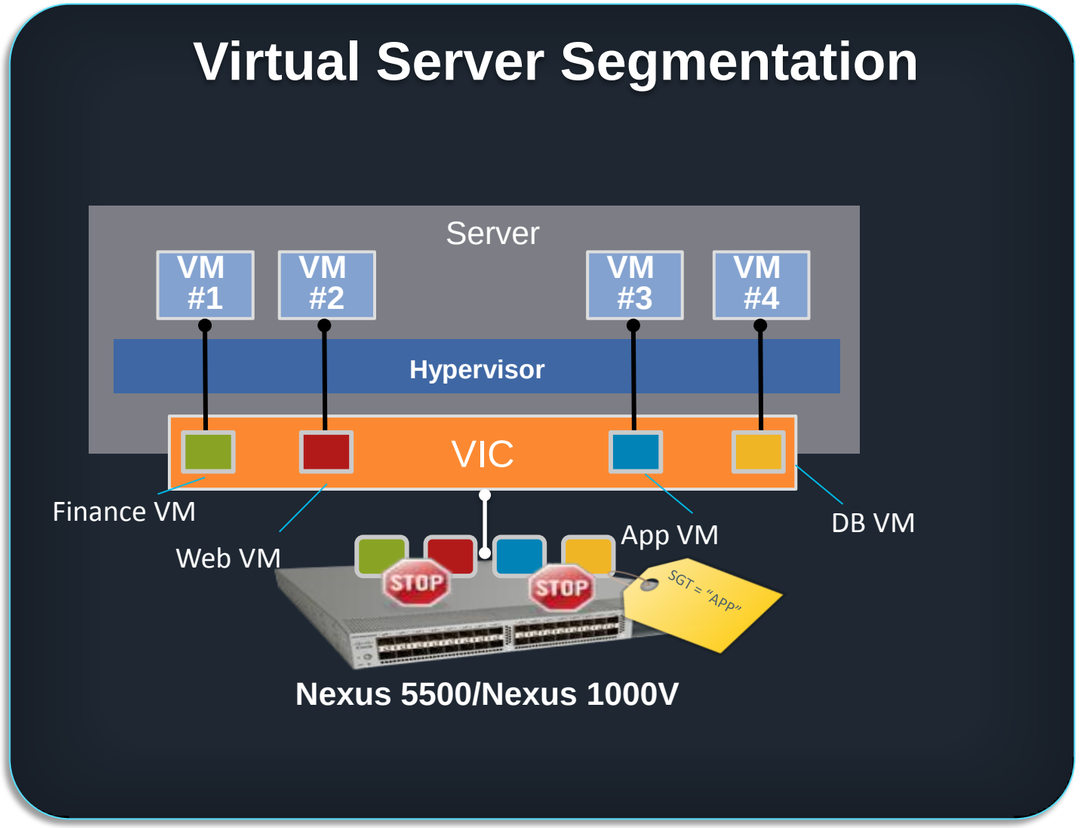
- Segmentation defined in a simple policy table or matrix
- Applied across Nexus 7000/5500/2000 independent of the topology



Use Case: Segmentation

Physical or VM Server Segmentation for Compliance





- Manually tag servers or using dynamic lookup (IPM, Port Profile, 802.1X, MAB)
- Use SGACL to enforce traffic between servers (VM, physical, VM-physical)
- Applicable for inter-security zone and intra-security zone (inside a VLAN)

Nexus 1000V 2.1

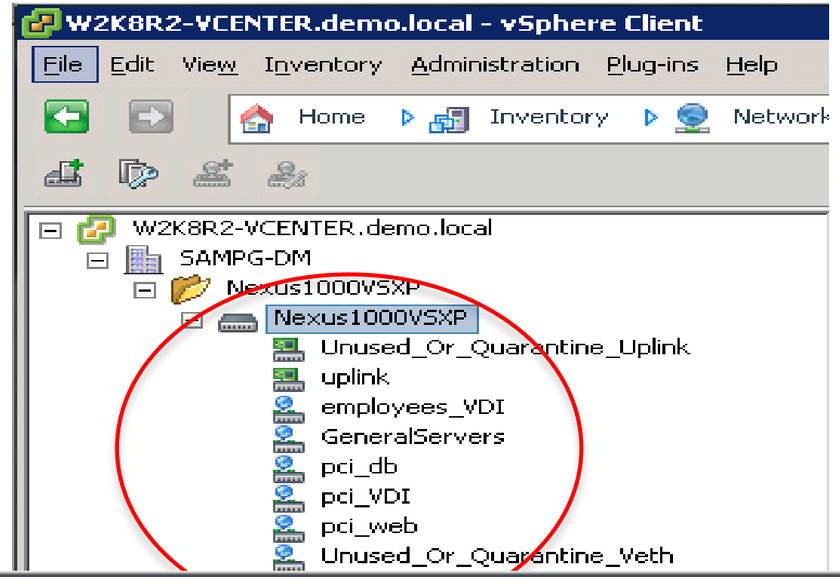
SGT Capabilities

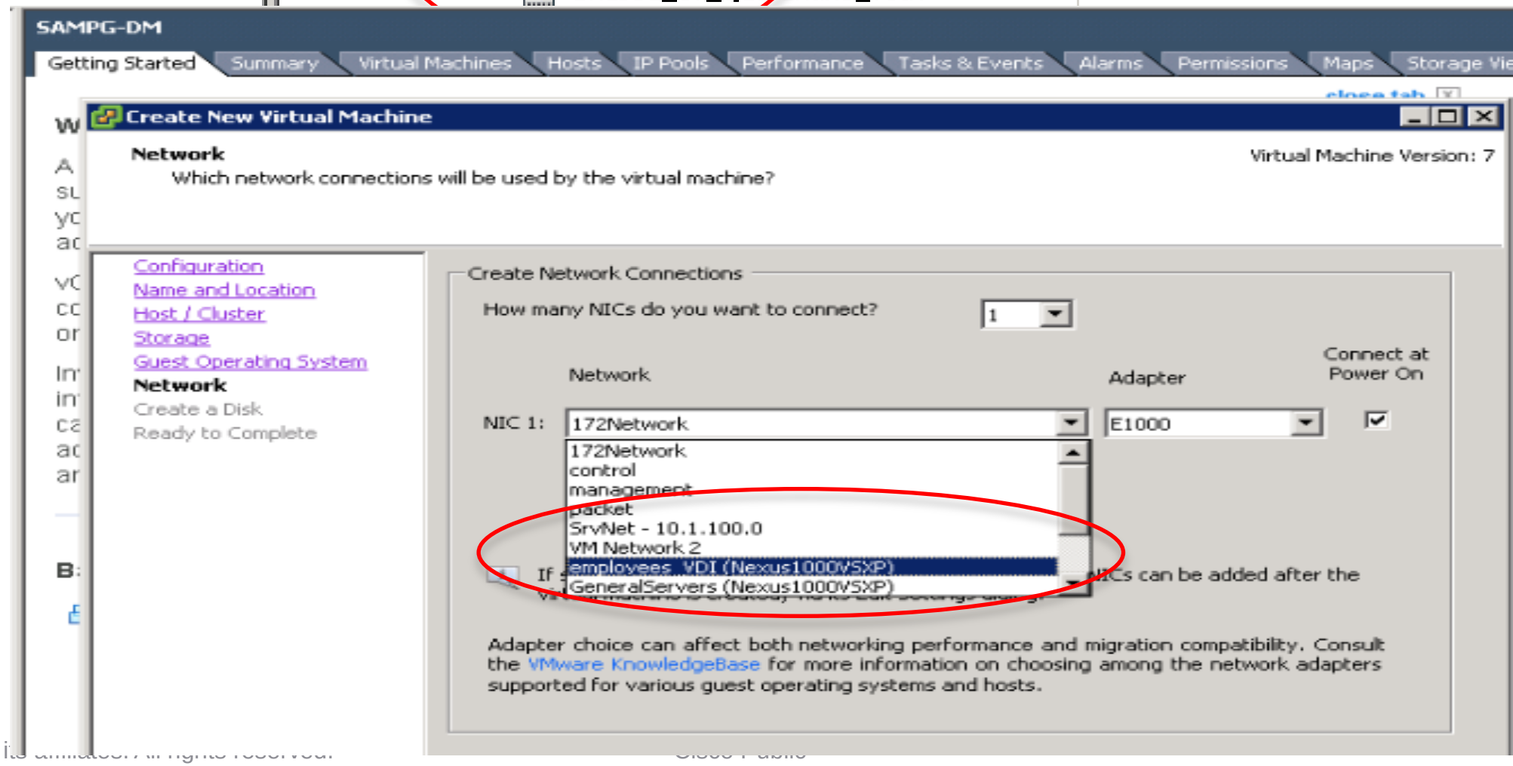
- Port Profile

  Container of network properties

  Applied to different interfaces

- VMs inherit network properties of the port-profile after vMotion has occurred





Nexus 1000V v2.1

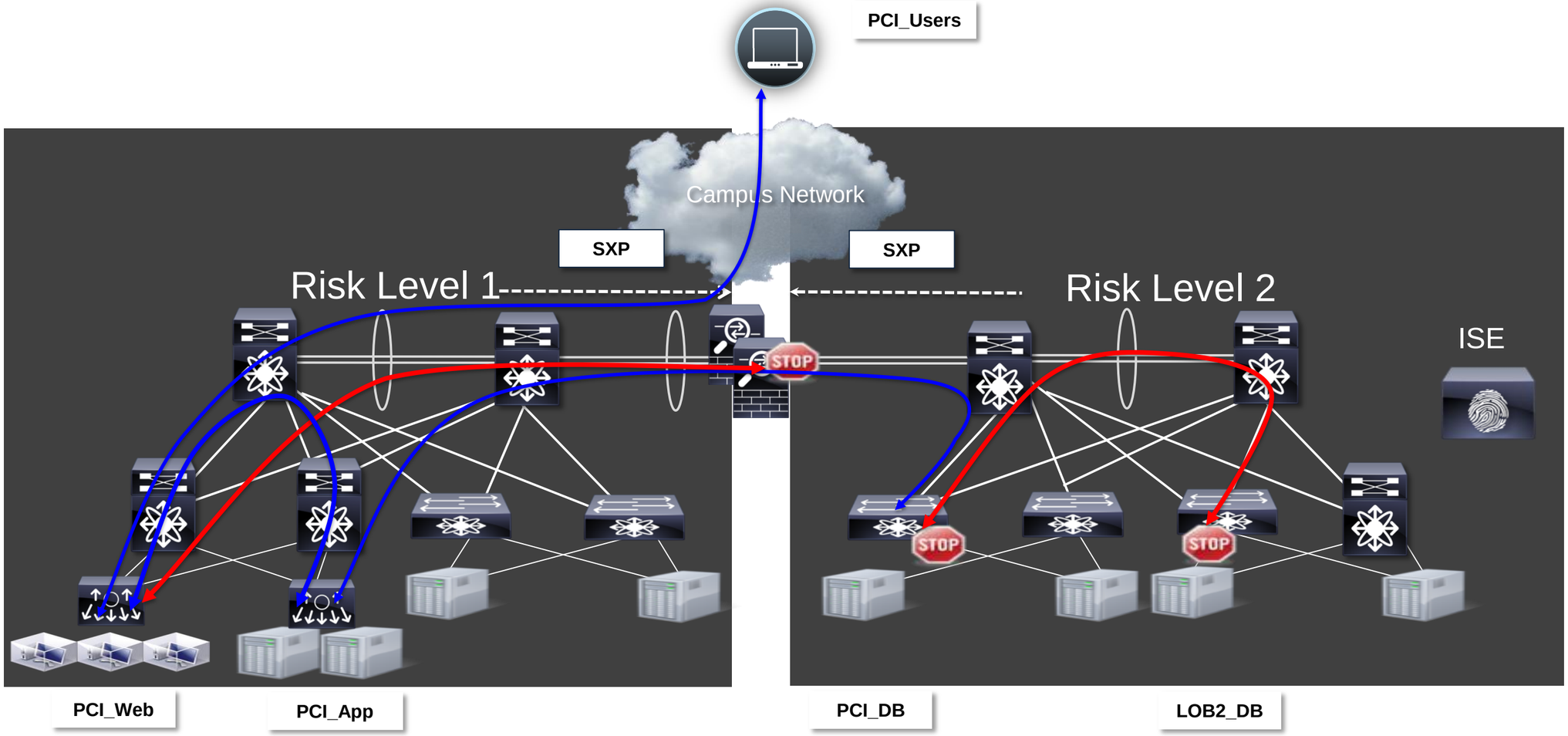
SGT Capabilities

- The port profiles are assigned to VMs

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

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

Customer End State in the DC

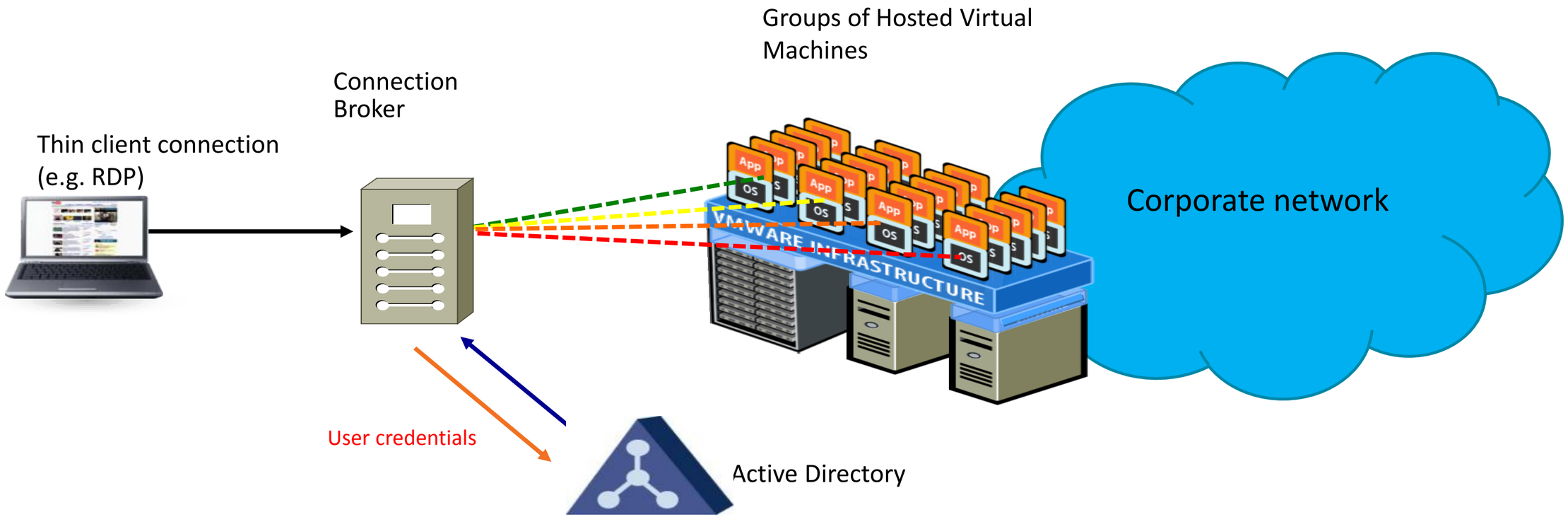


Data Centre Environment:

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

Virtual Desktop Infrastructure (VDI) with SGT

Background: Connection Brokers



Receives connection requests from thin-clients typically using RDP, PCoIP or ICA protocols

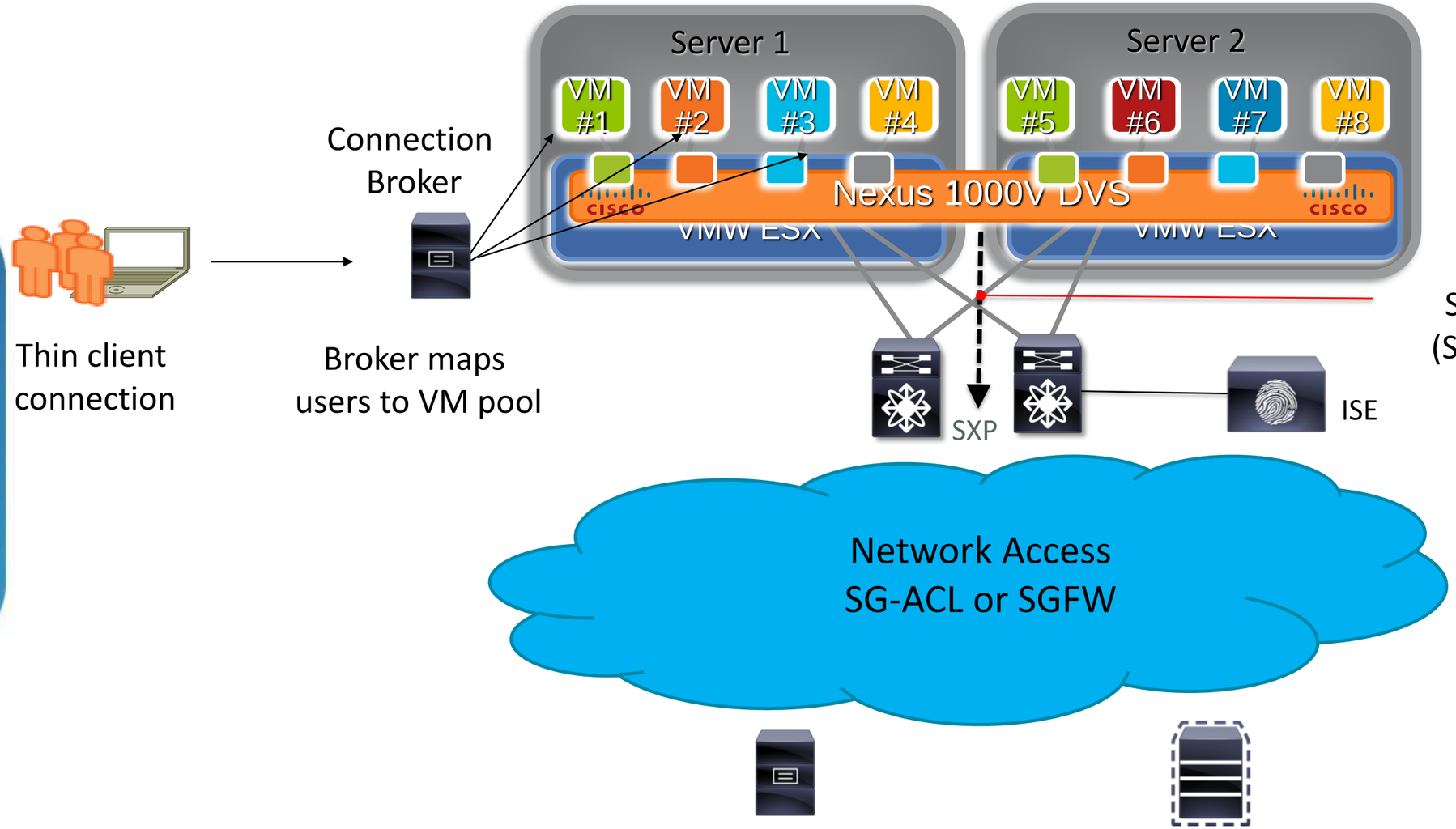
Authenticates the user, typically against AD

Maps the user to a pool of Virtual Machines or a specific VM

Hands off the user to the allocated VM

Using TrustSec SGA in a VDI/VXI Environment

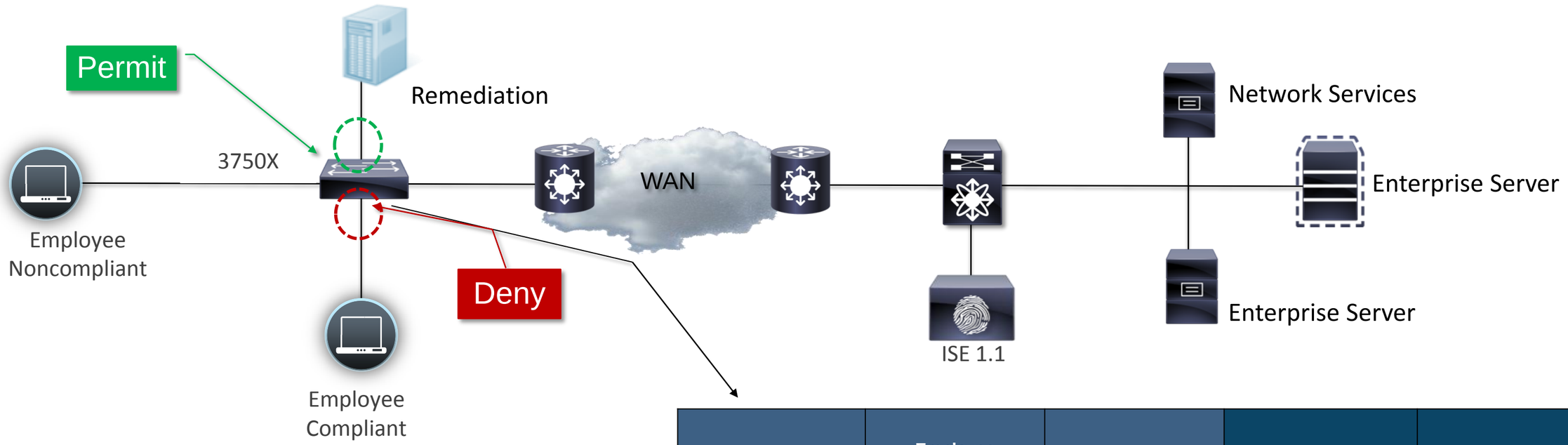
Nexus 1000V



SXP updates to N7k or ASA (SGTs defined in Port Profile)

Campus Security Overlay

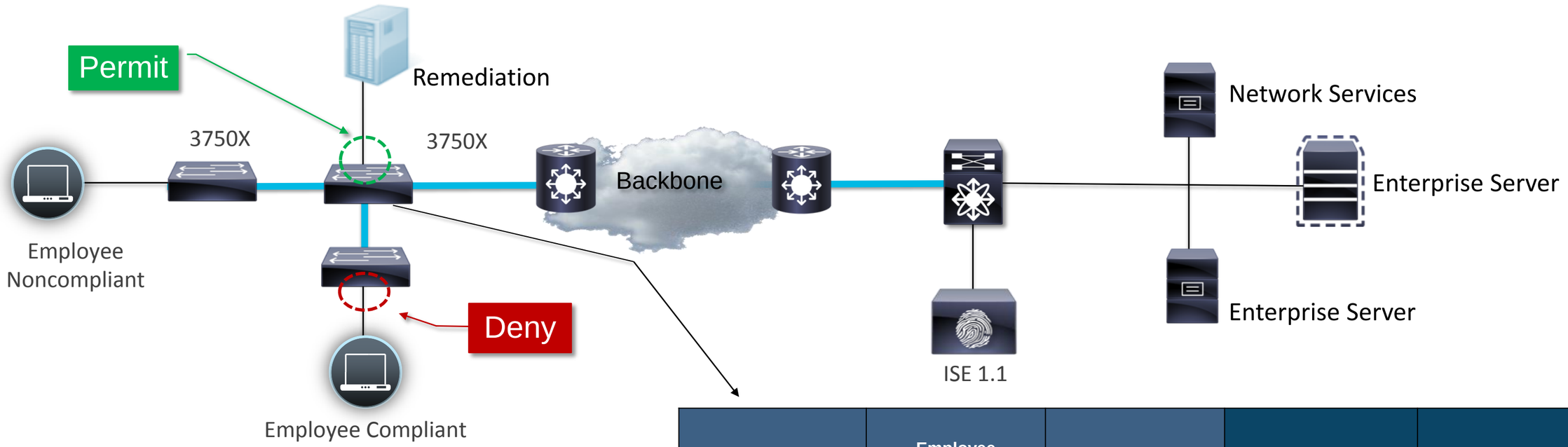
NAC – Pure Layer 2 SGACL



1. EmployeeNoncompliant is allowed to Remediation via intersecion of 20/222
2. EmployeeNoncompliant is denied access to EmployeeCompliant via intersecion of 20/10

SRC \ DST	Employee Compliant (10)	Network Services (111)	Remediation (222)	Enterprise Servers (333)
Employee Compliant (10)	Permit Any	Permit Any	Permit Any	Permit Any
Employee-Noncompliant (20)	Deny All	Permit DHCP Permit DNS	Permit Any	Deny All
Unknown (0)	Deny All	Permit DHCP Permit DNS	Deny All	Deny All

Security Overlay – Layer 2 /Layer 3 SGACL



1. Traffic from EmployeeNoncompliant must be tagged from 3750X to L3 Switch
2. L3-Switch implements SGACL.
3. EmployeeNoncompliant is allowed to Remediation via intersecion of 20/222
4. EmployeeNoncompliant is denied access to EmployeeCompliant via intersecion of 20/10

SRC \ DST	Employee Compliant (10)	Network Services (111)	Remediation (222)	Enterprise Servers (333)
Employee Compliant (10)	Permit Any	Permit Any	Permit Any	Permit Any
Employee-Noncompliant (20)	Deny All	Permit DHCP Permit DNS	Permit Any	Deny All
Unknown (0)	Deny All	Permit DHCP Permit DNS	Deny All	Deny All

L2 Tagged Traffic

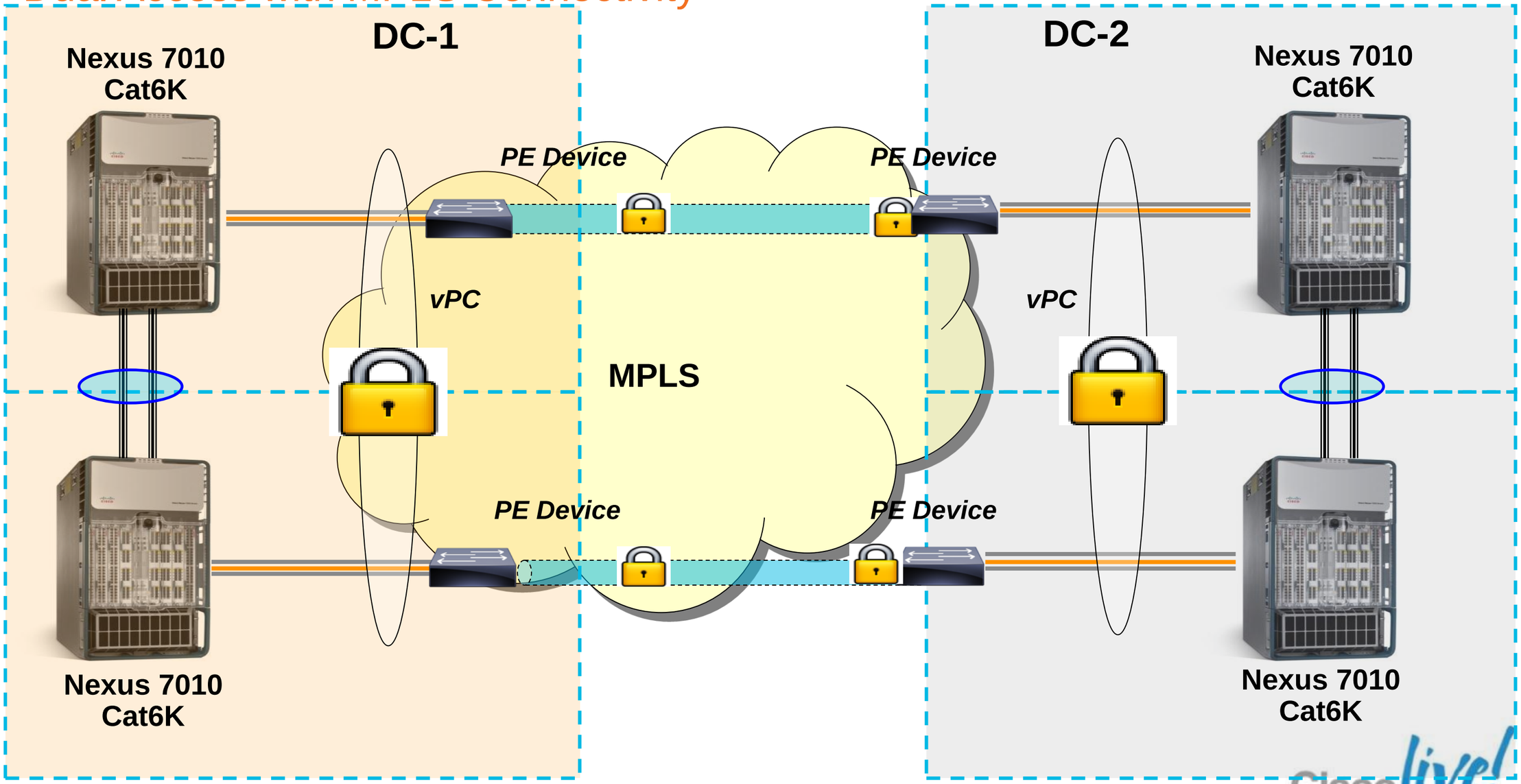
Secure Data Centre Interconnect

Encrypted Inter-DC Link with 802.1AE

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

SGT for Secure Data Centre Interconnect

Dual Access with MPLS Connectivity



Basic Customer Case Study Review

Customer Problem Statement

- Customer has several challenges for “network access”
- Regulatory Compliance
  - This requires compensating controls for to control traffic for different types of device/users on the network
- Business Strategy Support
  - The business is moving to a model where more contractors/vendors will be doing work
  - This requires that particular contractors have very specific and limited access to the network
- BYOD Trend
  - Support the mobile device BYOD
  - In addition it’s a stated goal to move the cost centre for general computing endpoints out of IT and into the employees hands

Customer Goals When Evaluating "Access Control"

- Customer has been evaluating "access control" solutions for over a decade to meet regulatory compliance. All have failed to address critical use cases
- The supporting criteria is that if they could dynamically identify the device/user that they could dynamically provision the necessary network controls to meet their regulatory compliance objectives.
- With the primary objective being device/user identification this same goal supports the business moving to more contractor/vendor support as well as BYOD

Customer Policy

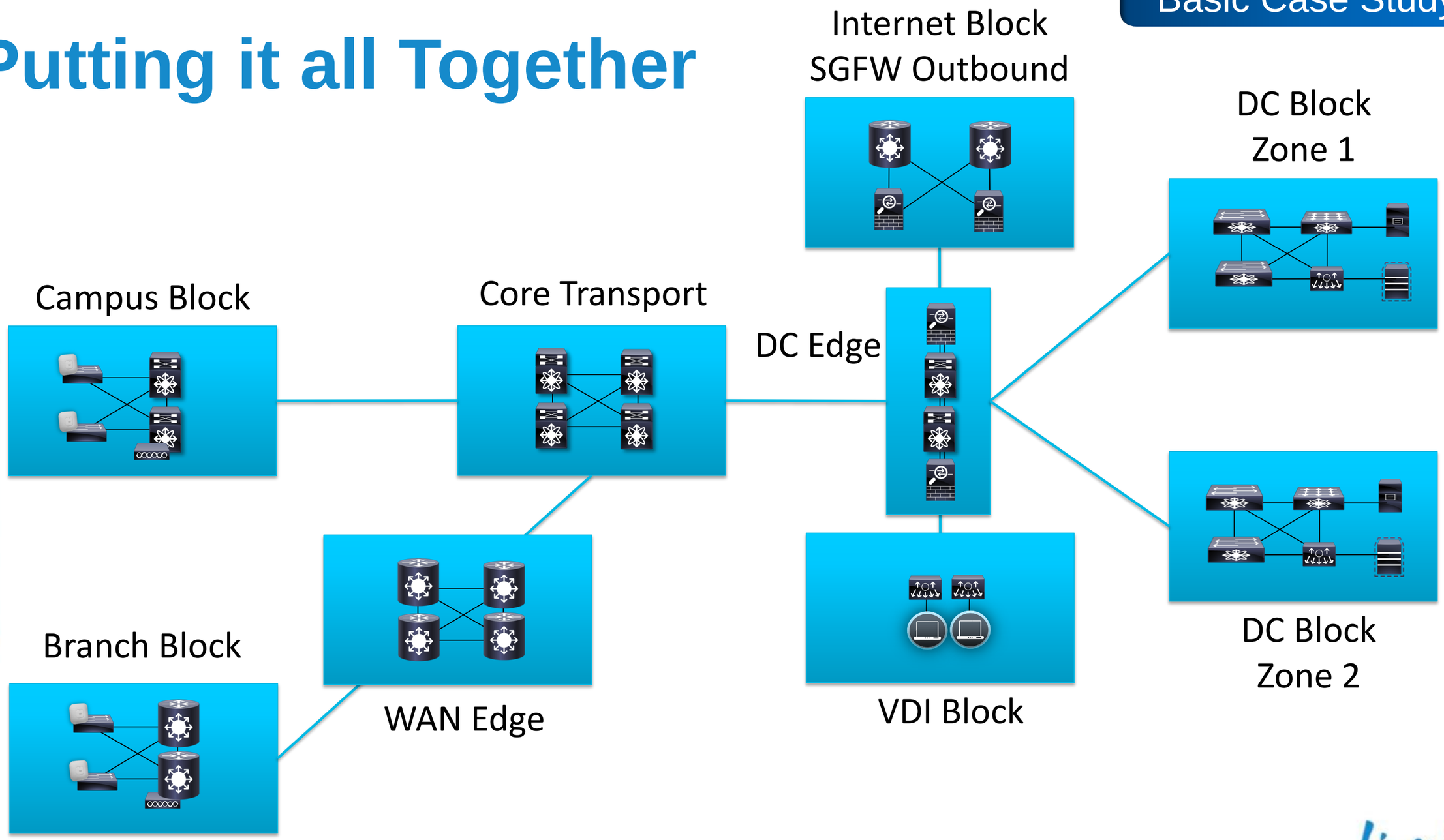
- Corporate Users with a corporate asset
  - full permissions at the access layer
  - restricted permissions based on role at the data centre and restricted area.
- Corporate users with a personal asset, or contractors/vendors that opt to use the asset for “work”
  - restricted permissions at the access layer
    - Internet only
    - VDI access
  - restricted permissions at the DC
    - Basic services like DNS/DHCP
    - VDI
- Guests or corporate with a personal asset that opt “out” and use the device for personal only use
  - Restricted permissions at the access layer
    - Internet only
- Restricted permissions at the DC

Role Based Classification and Filtering in the DC

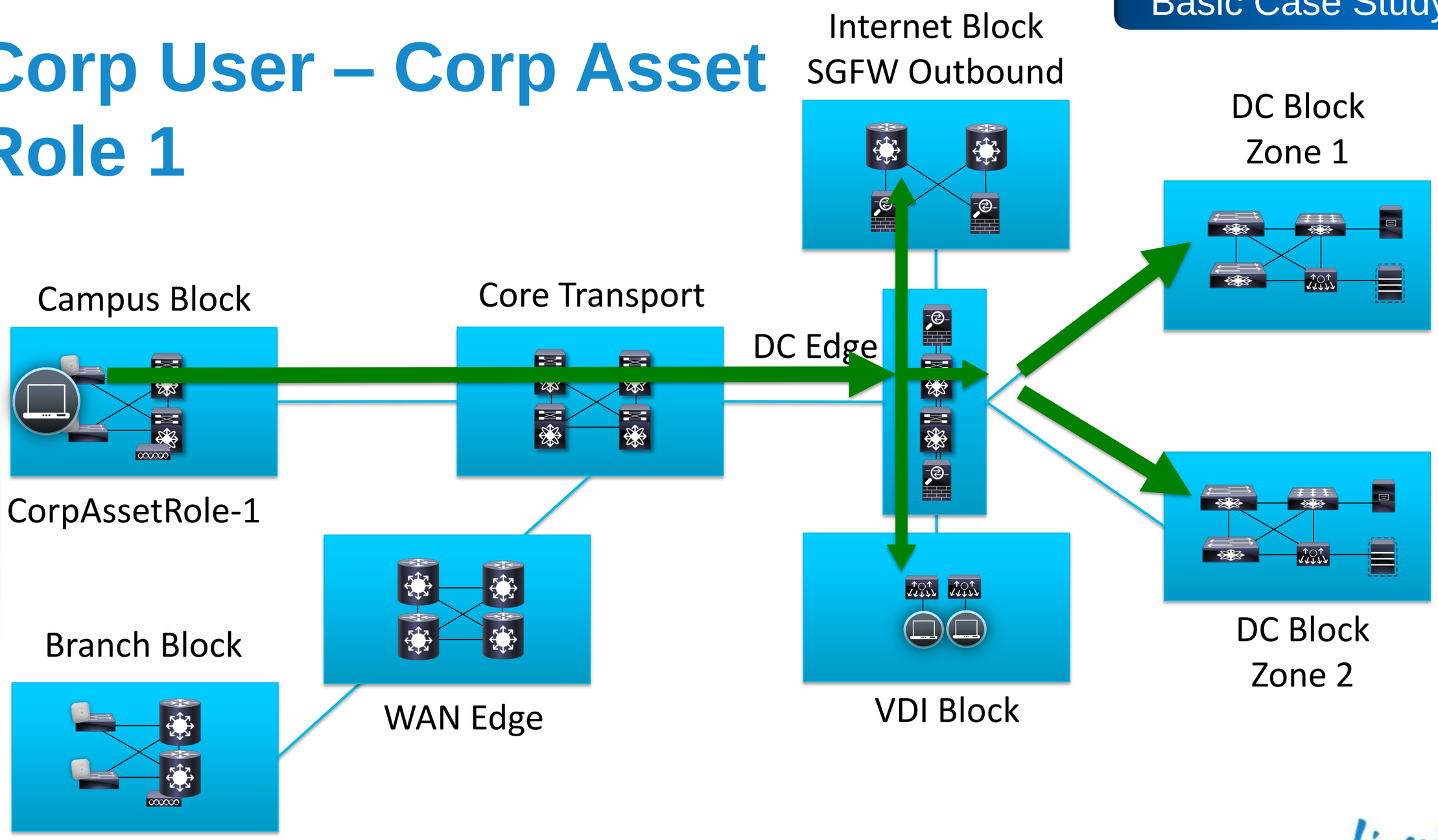
- The role based classification is used to isolate users from the different zones in the DC that are required to be isolated for regulatory compliance and services (DNS/DHCP/VDI)

SRC \ DST	CorpAsset (10)	……	Network Services (111)	Virtual Desktop Infraastructure (222)	Enterprise Zone 1 (333)	Enterprise Zone 2 (444)
CorpAsset-Role1 (10)	Permit Any	…..	Permit Any	Permit Any	Permit Any	Permit Any
CorpAsset-Role2 (20)	Permit Any	…..	Permit Any	Permit Any	Permit Any	Deny All
CorpNonAsset_VDI (30)	Deny All	…..	Permit DHCP Permit DNS	Permit_VDI	Permit Any	Deny All
Contractor (40)	Deny All	…..	Permit DHCP Permit DNS	Permit_VDI	Deny All	Deny All
Contractor_VDI (50)	Deny All	…..	Permit DHCP Permit DNS	Permit_VDI	Contractor ACL	Deny All
Corp_Contractor_InetOnly (60)	Deny All	…..	Permit DHCP Permit DNS	Deny All	Deny All	Deny All

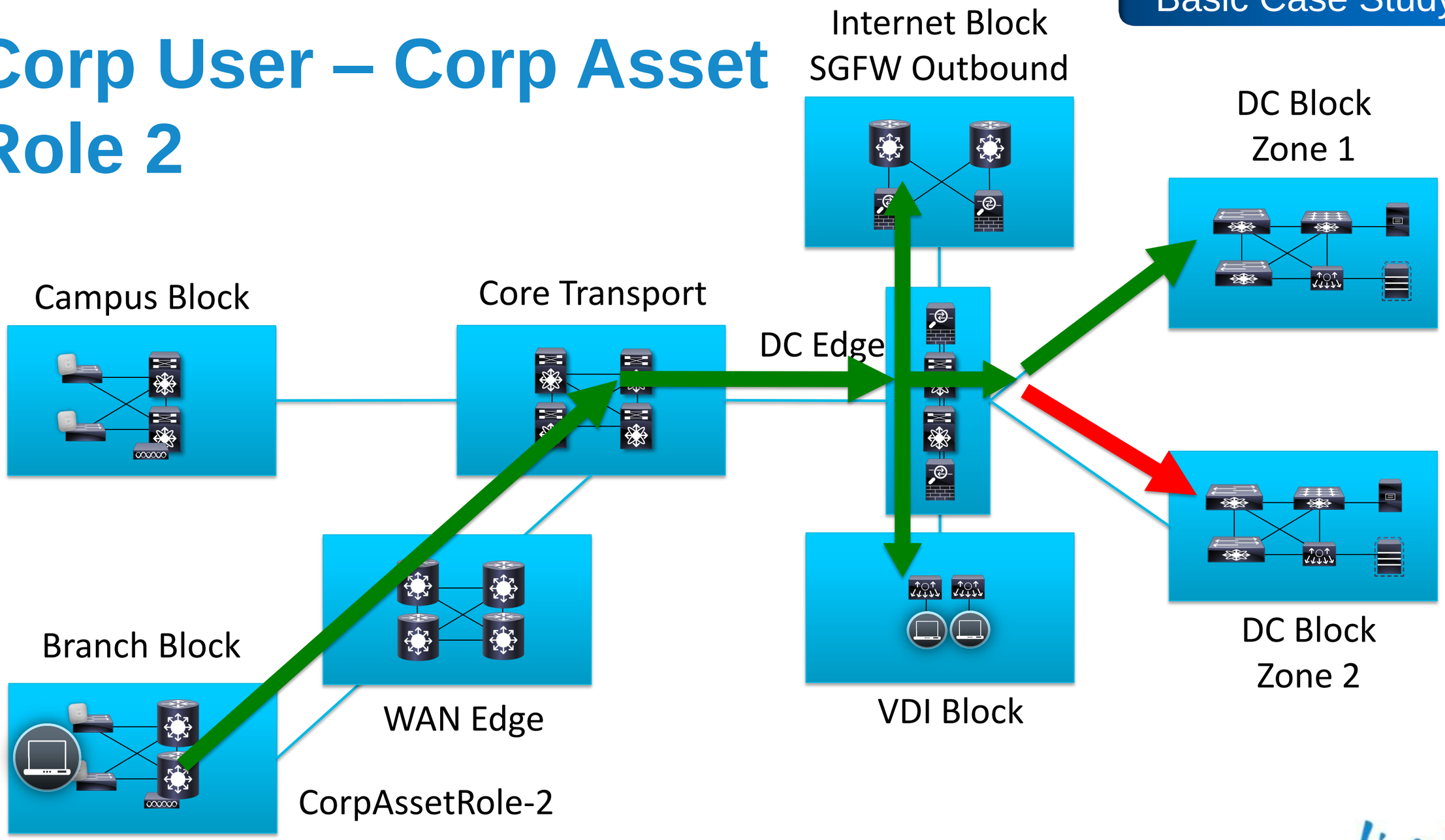
Putting it all Together



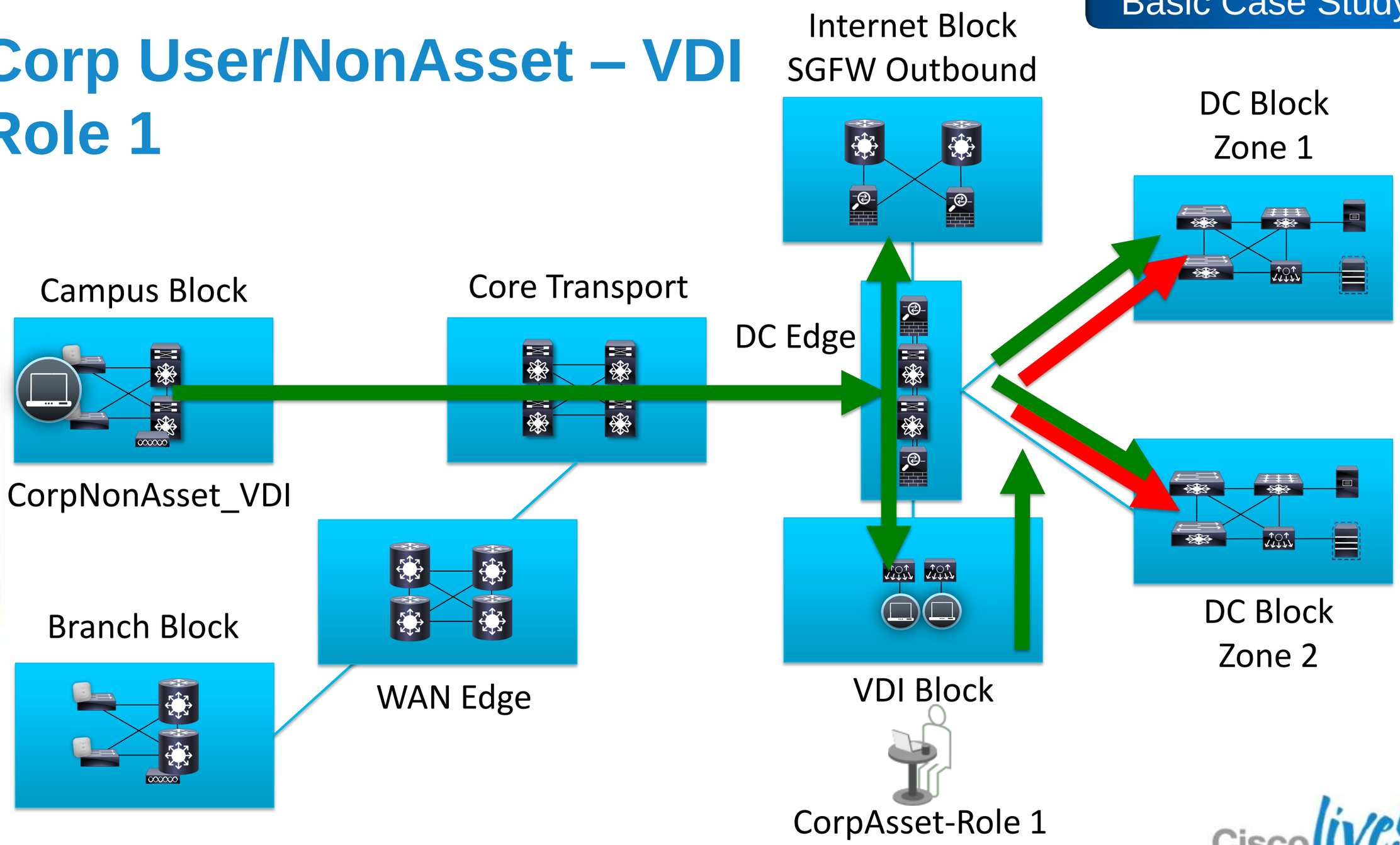
Corp User – Corp Asset Role 1



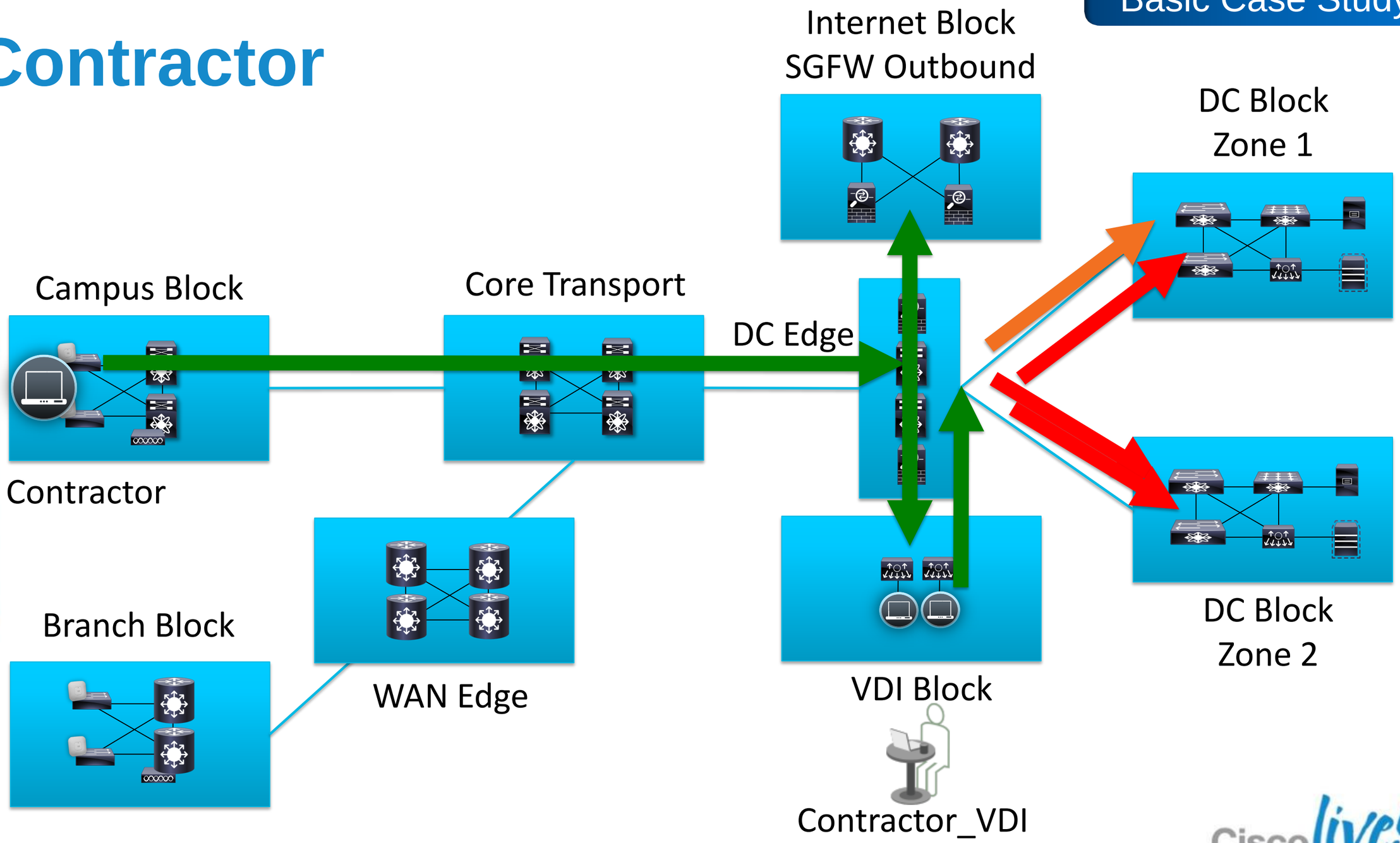
Corp User – Corp Asset Role 2



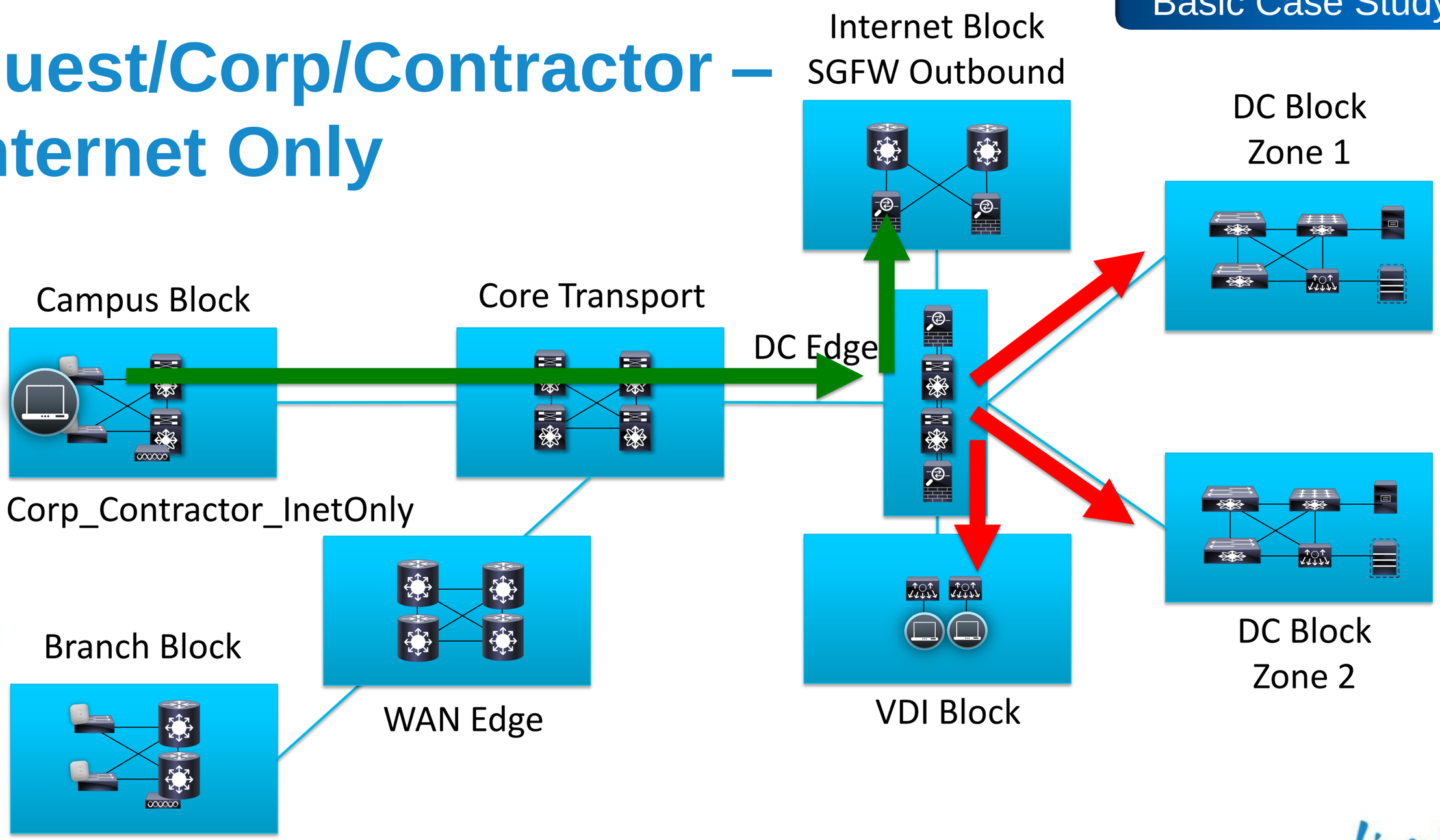
Corp User/NonAsset – VDI Role 1



Contractor



Guest/Corp/Contractor – Internet Only



Summary

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

- **Other sessions**
  - BRKSEC-2022 - Demystifying TrustSec, Identity, NAC and ISE
  - BRKCRS-2199 - Secure Converged Wired, Wireless Campus

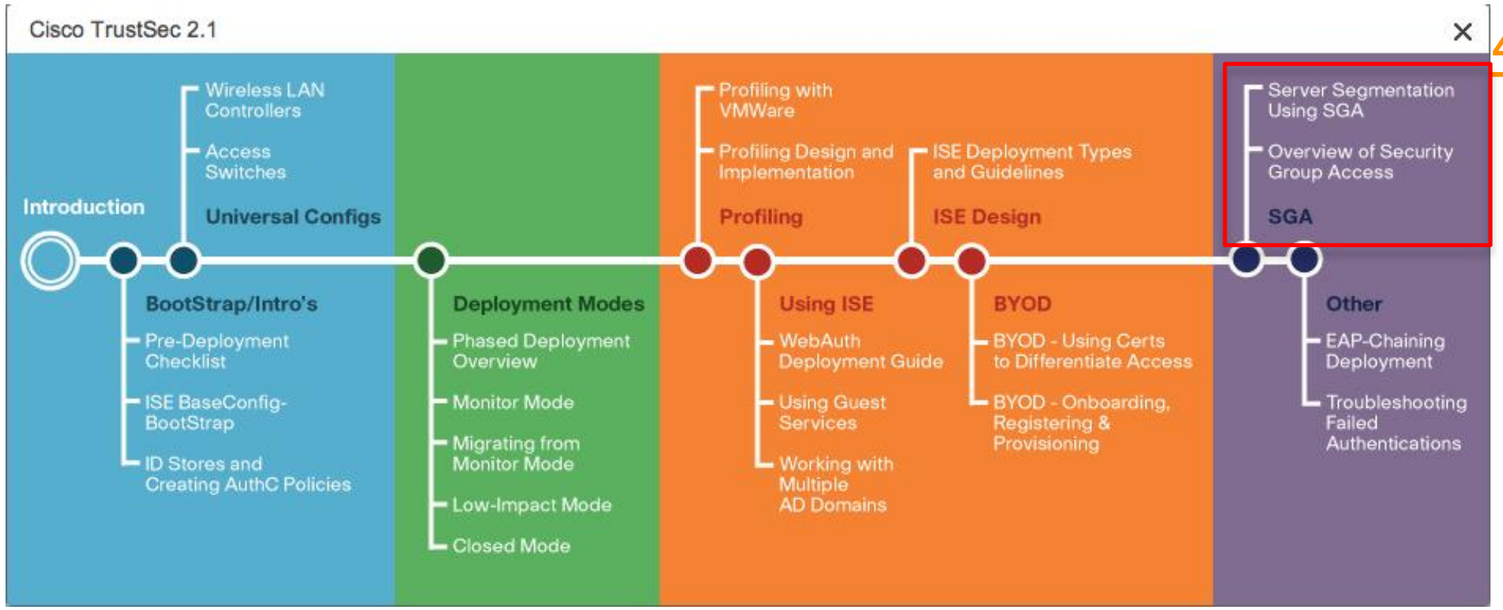
Recommended Reading

- Network Complexity - Michael H. Behringer: Classifying Network Complexity; slides; ACM ReArch'09 workshop; 2009
  http://networkcomplexity.org/wiki/index.php?title=References
- Cisco TrustSec 2.1 Design and Implementation Guide
  http://www.cisco.com/go/trustsec/
- Cisco Wireless LAN Security - http://www.ciscopress.com/bookstore/product.asp?isbn=1587051540
- Managing Cisco Network Security - http://www.ciscopress.com/bookstore/product.asp?isbn=1578701031
- Cisco Firewalls –http://www.ciscopress.com/bookstore/product.asp?isbn=1587141094
- Cisco LAN Switch Security: What Hackers Know About Your Switches - http://www.ciscopress.com/bookstore/product.asp?isbn=1587052563

Resources

- Main TrustSec Page
  - http://www.cisco.com/go/trustsec

- More Documents



4/ns742/ns744/landing_De

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww