Implementacija 802.1x i Trustsec rešenja

György Ács, Regional security consultant

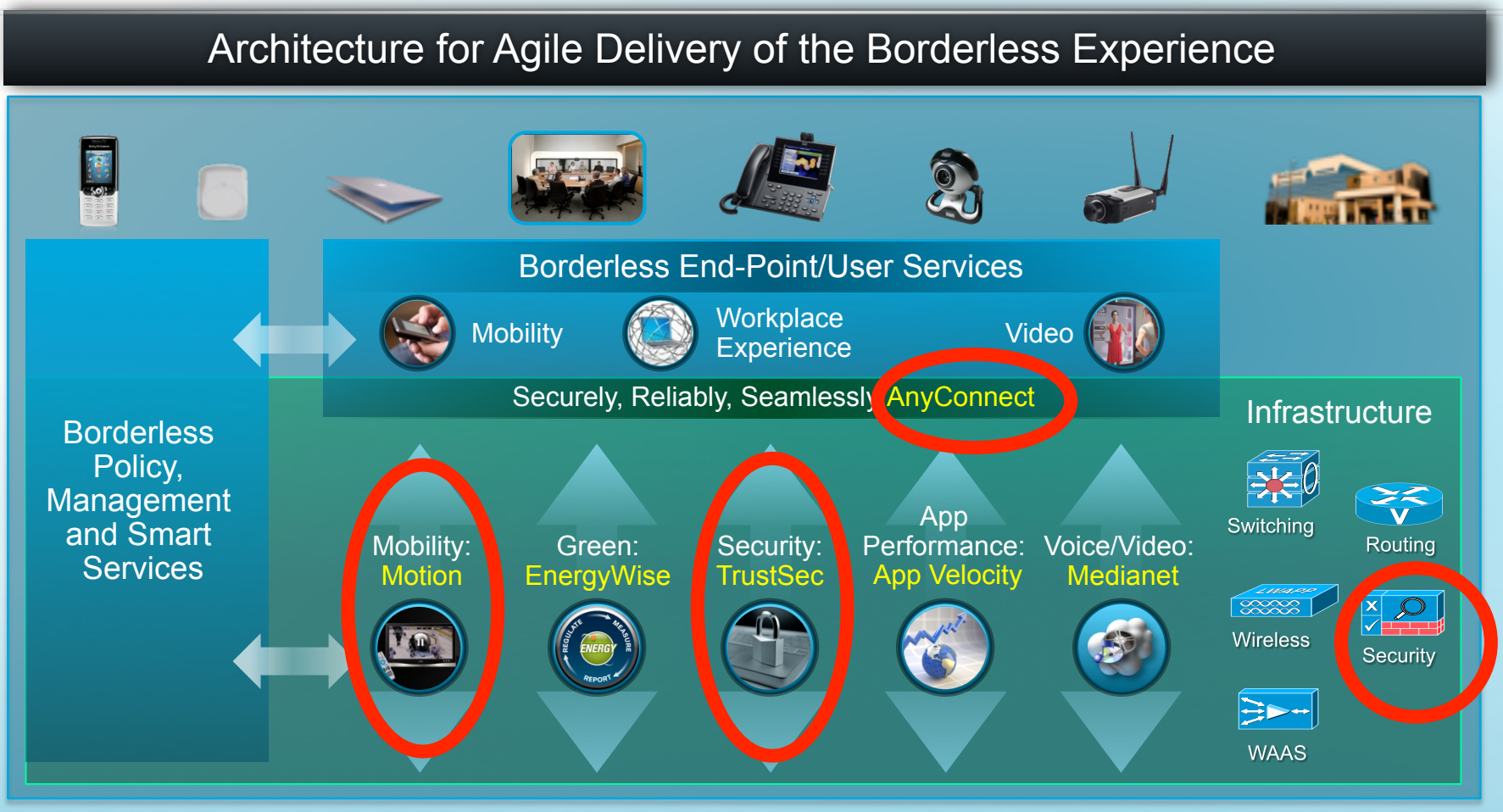
TrustSec

György Ács, Regional security consultant

Overview

- Introduction
  - Business Challenge
  - Defining Network Access Management
  - Foundation Technologies
- TrustSec Solution Overview
  - Source Group Tag (SGT) / Source Group ACL (SGACL) Concept
  - Network Device Access Control (NDAC) Concept
  - 802.1AE / SAP Concept
- Deployment Practice
  - SGT Assignment Practice
  - SXP
  - Use Case
    - Data Center Use Case
    - Campus to Data Center Use Case
  - Monitoring TrustSec, ACS

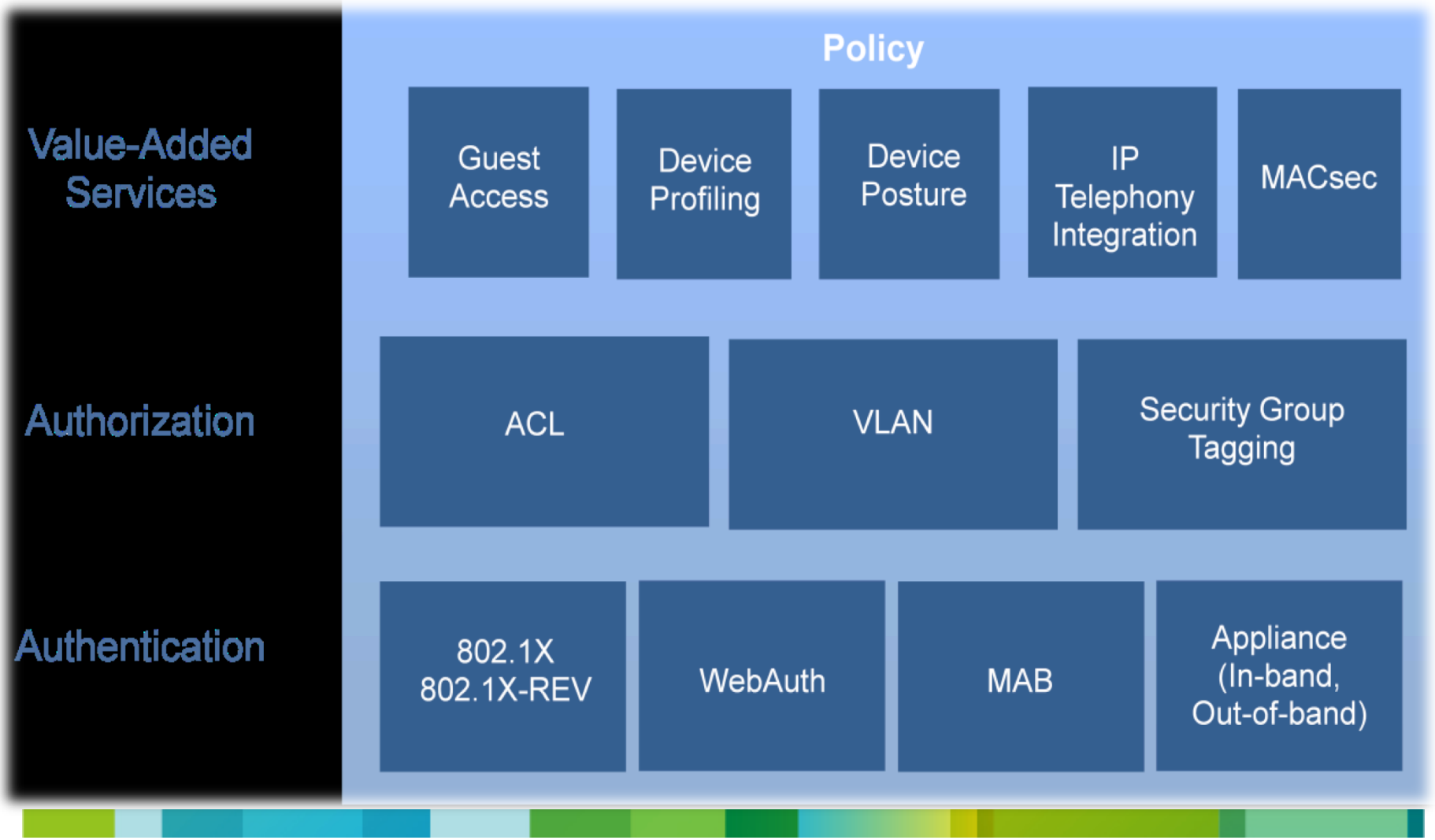
Borderless Network Architecture



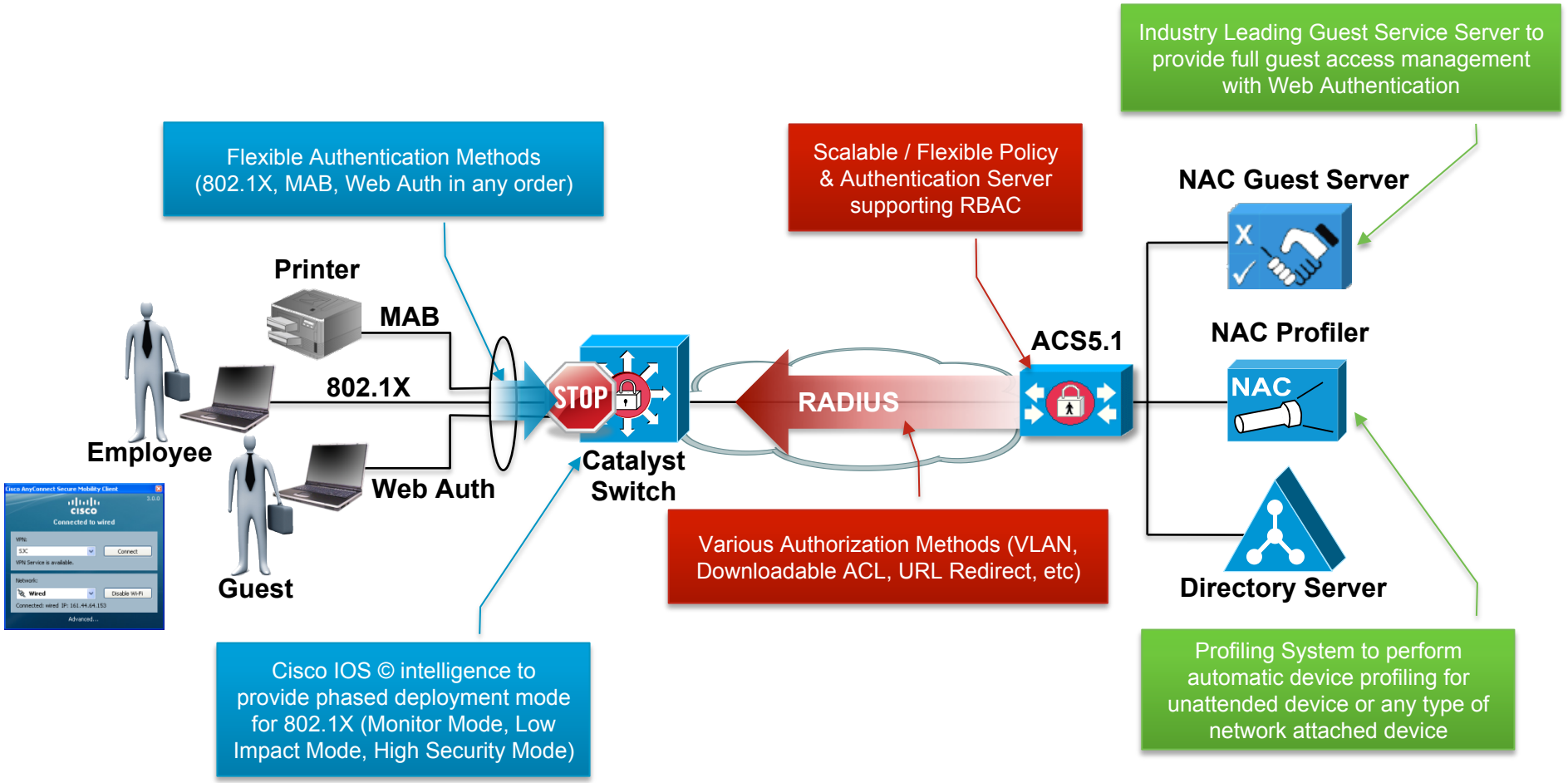
Security Challenges

Who?	Identify users and provide differentiated access in a dynamic, borderless environment
What ?	Devices are proliferating, including network capable purpose-built devices.
Where ?	Traditional borders are blurred. Access is possible from anywhere.
How ?	Establish, monitor, and enforce consistent global access policies

Cisco TrustSec architecture



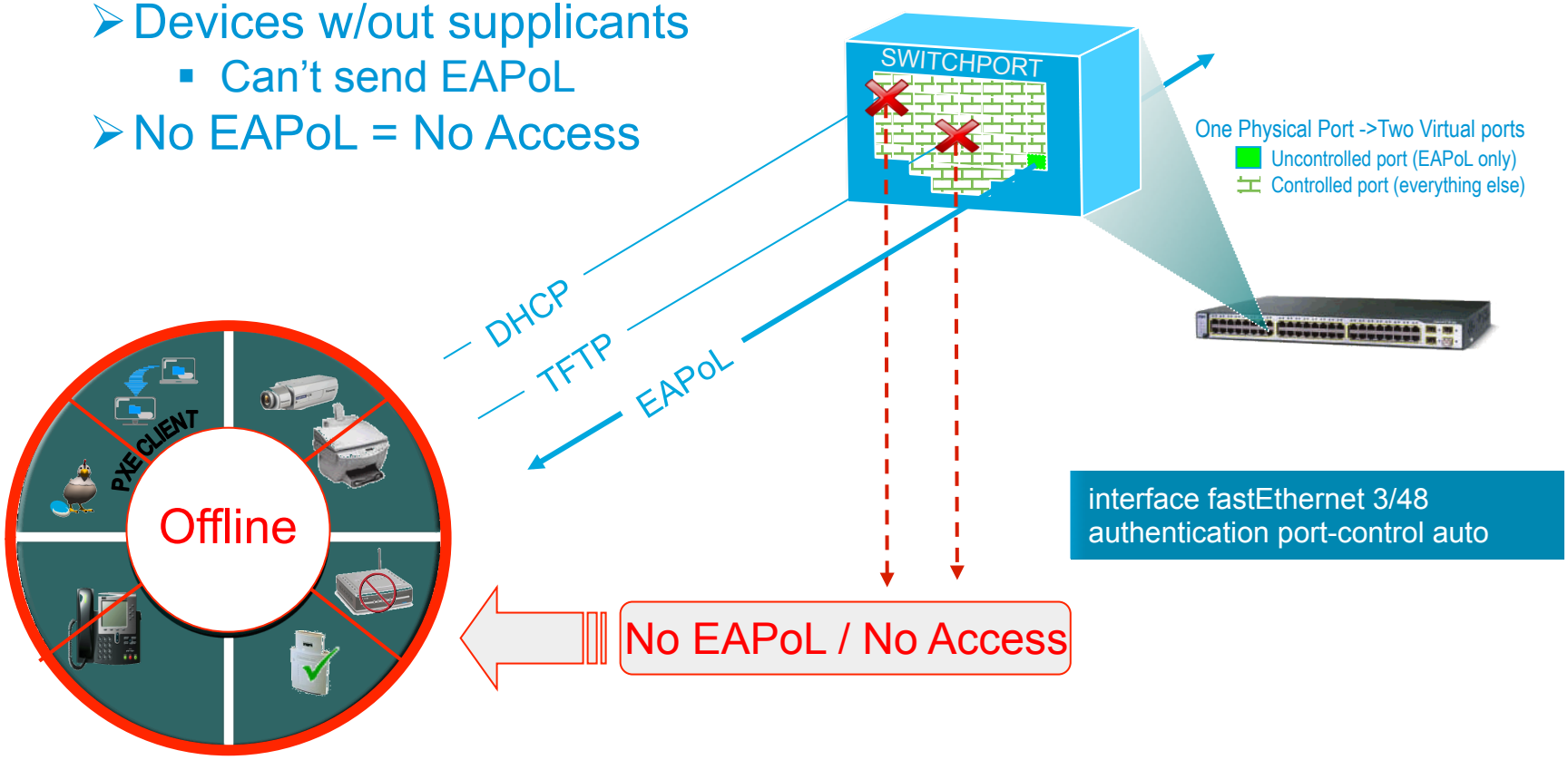
Cisco Identity Solution Overview



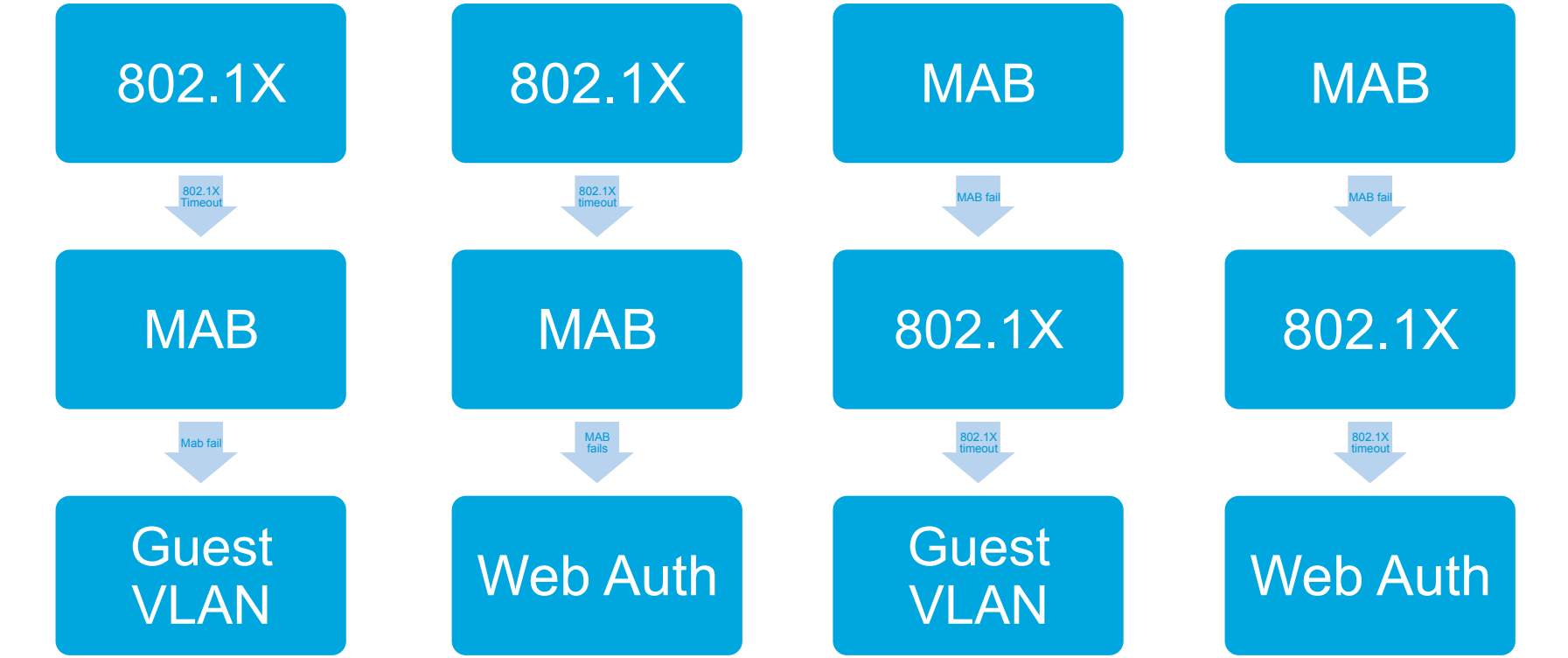
Default Security: Consequences

Default 802.1x Challenge

- Devices w/out supplicants
  - Can't send EAPoL
- No EAPoL = No Access



MAB, Web Auth, Guest VLAN interactions




```
interface GigabitE 3/13
 authentication port-control auto
 mab
authentication event no-response
      action authorize vlan 51
```

```
interface GigabitE 3/13
 authentication port-control auto
 mab
 authentication fallback WEB-AUTH
```

```
interface GigabitE 3/13
 authentication port-control auto
 mab
 authentication order mab dot1x
 authentication event no-response
      action authorize vlan 51
```

```
interface GigabitE 3/13
 authentication port-control auto
 authentication order mab dot1x
      webauth
 mab
 authentication fallback WEB-AUTH
```

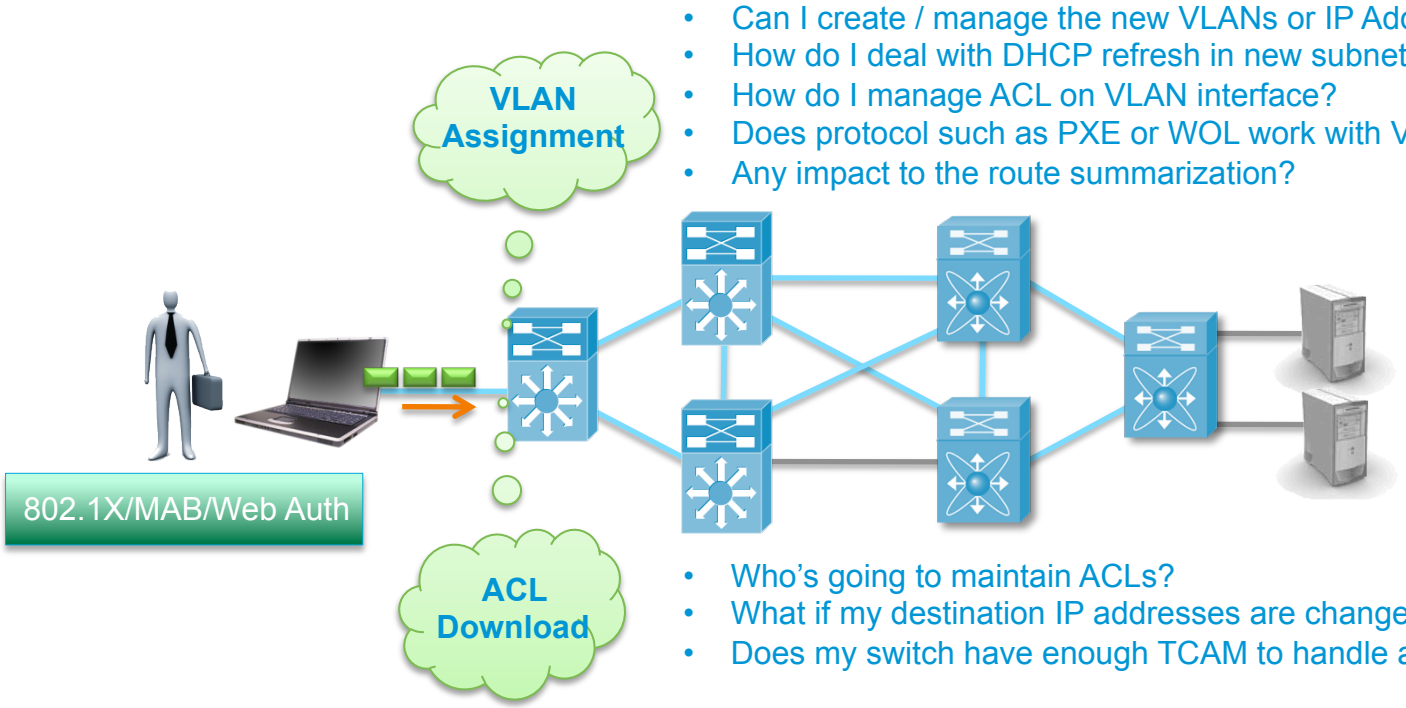
VLAN Assignment Pros and Cons

- Easiest way to segment traffic
- Most vendors supports dynamic VLAN assignment (RFC3580)
- Need to introduce new VLANs
- New VLAN => New IP scopes for subnet
- Changing VLAN in authorization means changing subnet for DHCP
- VLAN ID / Name design becomes very complicated
- policy is required for inter-VLAN communication
- Managing ACL on every L3 interface for VLAN becomes complicated

Downloadable ACL Pros and Cons

- ACLs managed centrally and provisioned per source IP address / authentication session
- No need to define endpoint IP address in ACL
- Scalable than per-user ACL download (more ACEs per RADIUS VSA)
- Pre-authentication interface ACL to integrate with services such as PXE Boot and Wake-On-LAN (WoL) for maintenance
- Destination IP address change needs to be reflected in every ACE
- Possible TCAM flooding if large amount of ACEs are configured

Challenge of Ingress Access Control



- Can I create / manage the new VLANs or IP Address scope?
- How do I deal with DHCP refresh in new subnet?
- How do I manage ACL on VLAN interface?
- Does protocol such as PXE or WOL work with VLAN assignment?
- Any impact to the route summarization?

- Who's going to maintain ACLs?
- What if my destination IP addresses are changed?
- Does my switch have enough TCAM to handle all request?

- Traditional access authorization methods leave some deployment concerns
  - Detailed design before deployment is required, otherwise…
  - Not so flexible for changes required by today's business
  - Access control project ends up with redesigning whole network

Cisco TrustSec Solution Overview

Cisco TrustSec

- **TrustSec is a broad umbrella** for security improvements based on the **capability to strongly identify users, hosts and network devices within a network**
- TrustSec provides **topology independent and scalable access controls** by uniquely classifying data traffic for a particular role
- TrustSec **ensures data confidentiality and integrity** by establishing trust among authenticated peer and encrypting links with those peers

TrustSec Key Features

Security Group Based Access Control

- Topology independent access control based on roles
- Scalable **ingress tagging via Source Group Tag (SGT) / egress filtering via Source Group ACL (SGACL)**
- Centralized Policy Management / Distributed Policy Enforcement

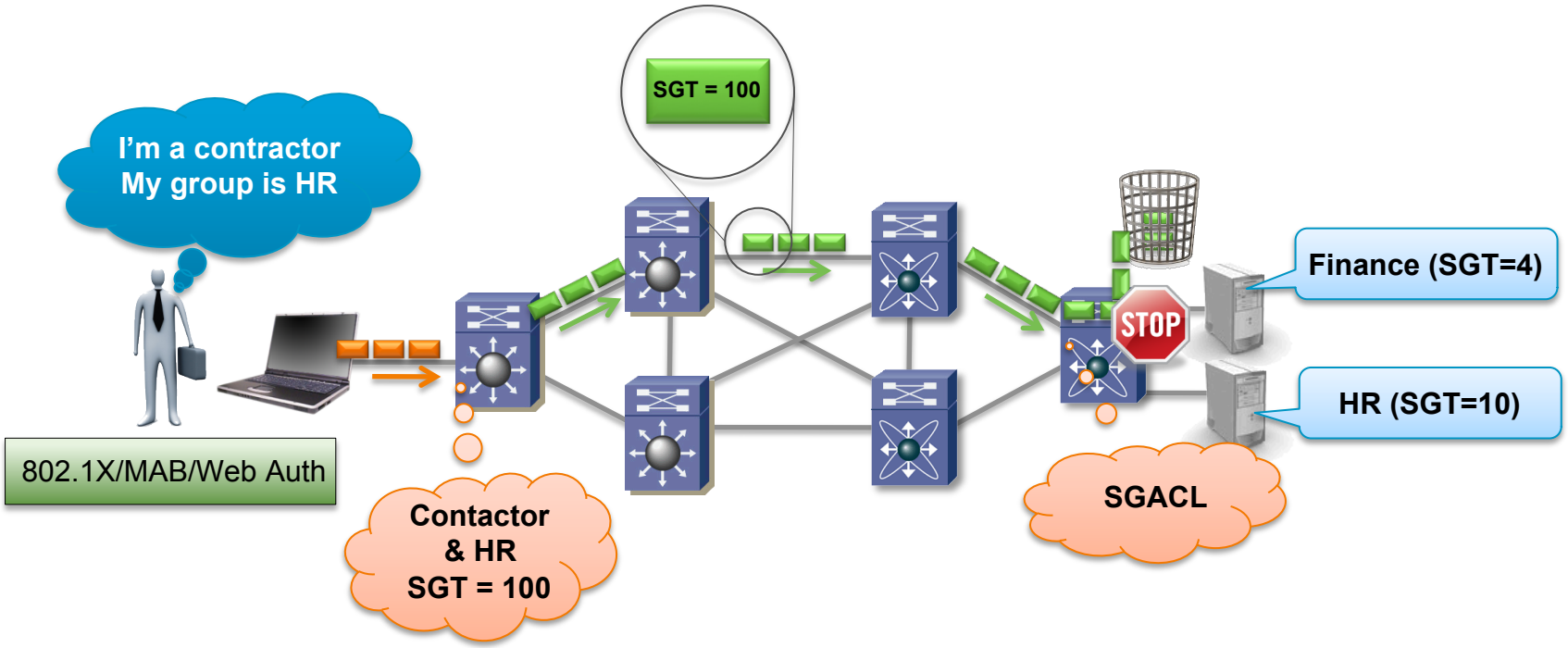
Authenticated Networking Environment

- Endpoint admission enforced via 802.1X authentication, MAB, Web Auth (Full IBNS compatibility)
- Network device admission control based on 802.1X creates trusted networking environment
- Only trusted network imposes Security Group TAG

Confidentiality and Integrity

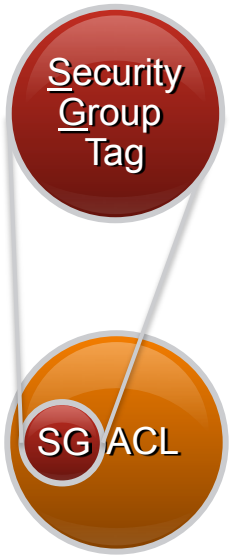
- Encryption based on **IEEE802.1AE** (AES-GCM 128-Bit)
- **Wire rate** hop to hop layer 2 encryption
- Key management based on 802.11n (SAP), and standard 802.1X-REV

Security Group Based Access Control



- Security Group Based Access Control allows customers
  - To keep existing logical design at access layer
  - To change / apply policy to meet today's business requirement
  - To distribute policy from central management server

Security Group Based Access Control



- **Unique 16 bit (65K)** tag assigned to **unique role**
- Represents **privilege of the source user, device, or entity**
- **Tagged at ingress** of TrustSec domain

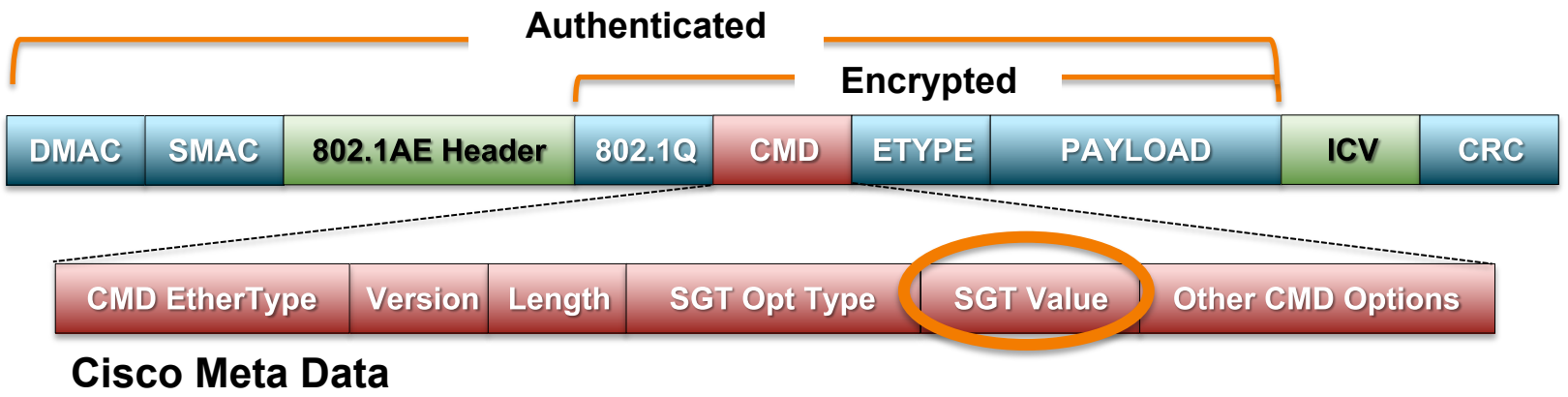
- **Filtered (SGACL) at egress** of TrustSec domain
- **No IP address required in ACE** (IP address is bound to SGT)
- Policy (ACL) is **distributed from central policy server (ACS)** or configured locally on TrustSec device

Customer Benefits

- Provides **topology independent** policy
- Flexible and scalable policy based on user role
- **Centralized Policy Management** for Dynamic policy provisioning
- Egress filtering **results to reduce TCAM impact**

Layer 2 SGT Frame Format

Layer 2 SGT Frame and Cisco Meta Data Format



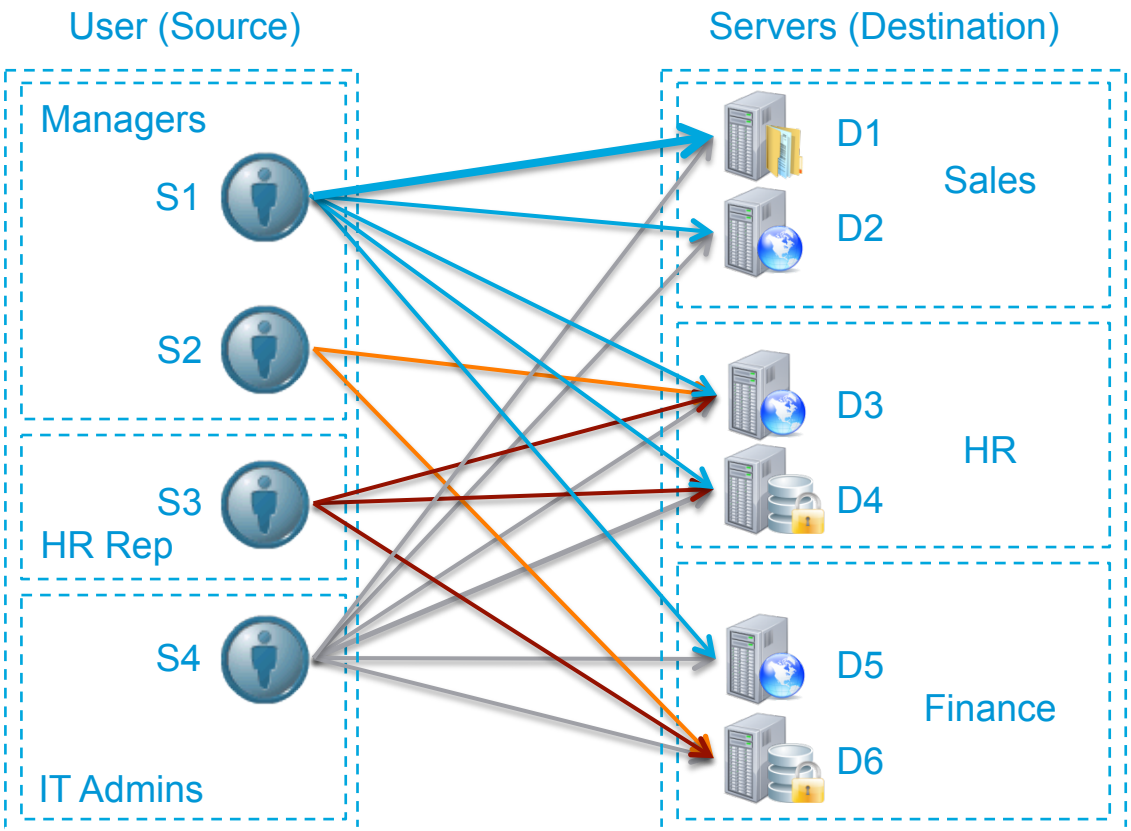
- 802.1AE Header | CMD | ICV are the L2 802.1AE + TrustSec overhead (=~40bytes)
- Tagging process prior to other L2 service such as QoS
- SGT namespace is managed on central policy server (ACS 5.x)
- No impact IP MTU/Fragmentation.

Normal Ethernet Frame

Evolution of Traditional Firewalls

- Traditional Firewall ACLs typically use an "any" for the source in their rules because they can't classify the source effectively
- Firewalls have started to evolve to use some extra mechanism to classify the source via identity
- Significant overhead can be created when using dynamic Identity classification for the source
  - More ACLs since each IP address is filled in for every rule on the FW
  - More resource consumption (TCAM, CPU, etc.)

Traditional Access Control List



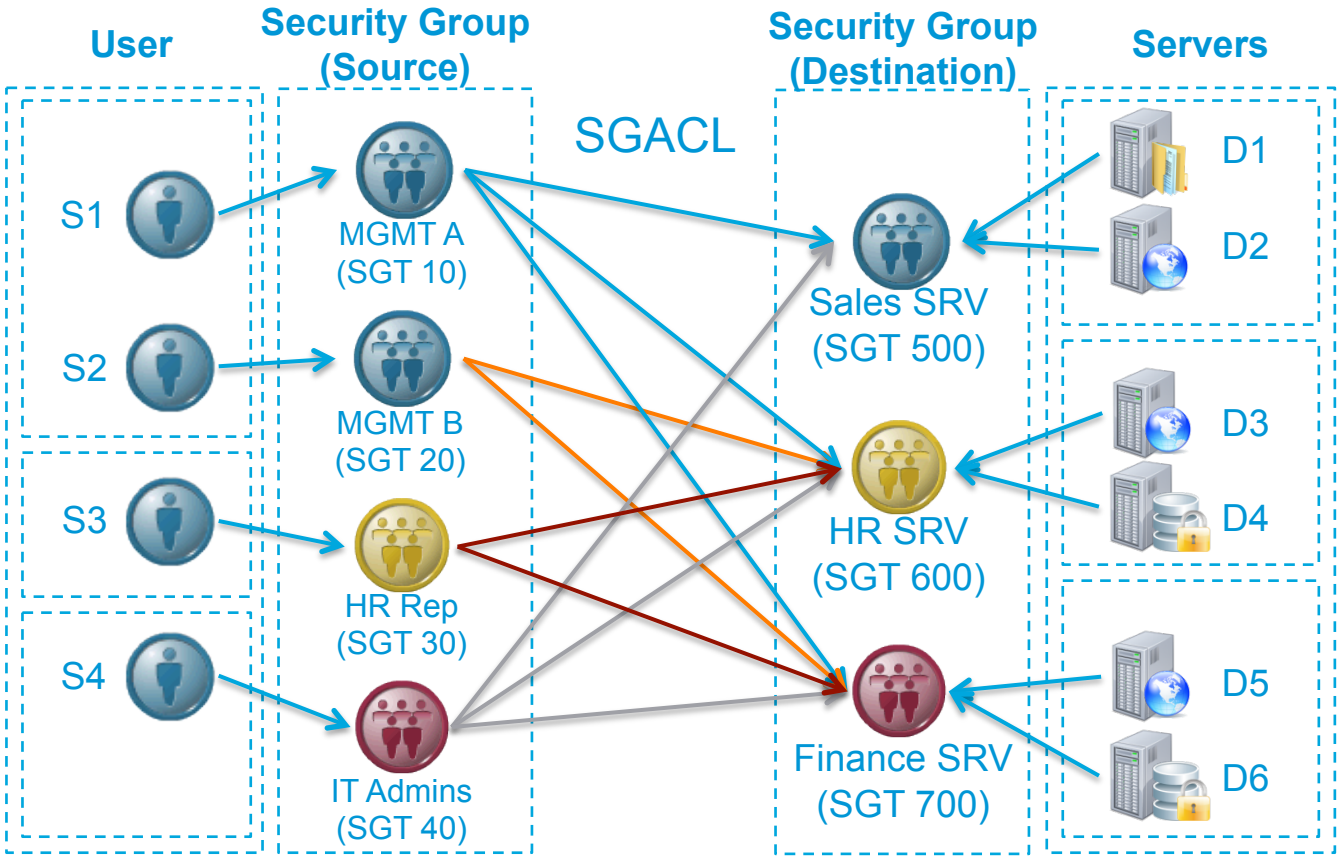
S1 to D1 Access Control

```
permit tcp S1 D1 eq https
permit tcp S1 D1 eq 8081
permit tcp S1 D1 eq 445
deny   ip  S1 D1
```

Access Control Entries (ACEs) grow as permission statements increase

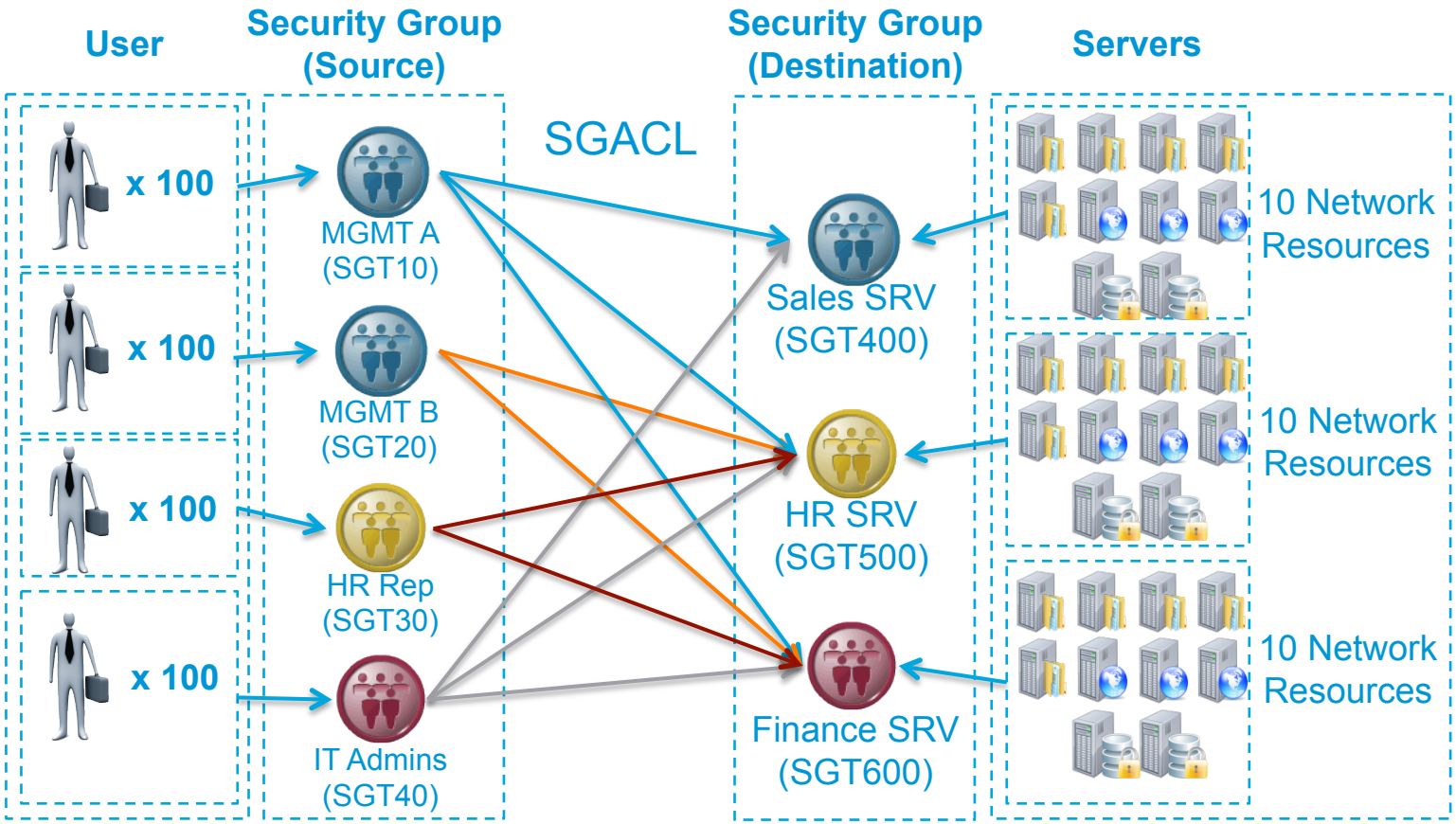
- **Sources x Destinations x Permissions = ACEs**
- **Source (S1) * Destination (S1~S6) * Permission (4) = 24 ACEs for S1**
- **Source (S1~S4) * Destination (S1~S6) * Permission (4) = 96 ACEs for S1~4**
- **The growing number of ACEs leads to resource comsumption on the enforcement point**

How SGACL Simplifies Access Control



- **(# of Source SG) * (# of Dest SG) * Permissions = # ACEs**
- **SGT10 * Dest SGTs (3) * Permission (4) = 12 ACEs for MGMT A SGT**
- **SRC SGTs (4) * DST SGTs (3) * Permission (4) = 48 ACEs**

SGACL Effectiveness in real world operation



SGACL Effectiveness in real world operation

- Assume current Firewall technology that we don't specify specific source (source = Any)
- 400 users accessing 30 network resources with 4 permissions each

With Traditional ACL on FW

Any (src) * 30 (dst) * 4 permission = **120 ACEs**

Traditional ACL on VLAN interface on router or FW - use subnet ranges for source group

4 VLANs (src) * 30 (dst) * 4 permission = **480 ACEs**

Per source IP on port with Downloadable ACL

1 Group (src) * 30 (dst) * 4 permission = **120 ACEs**

With SGACL

4 SGT (src) * 3 SGT (dst) * 4 permission = **48 ACEs**

Role to SGT Binding and SGACL

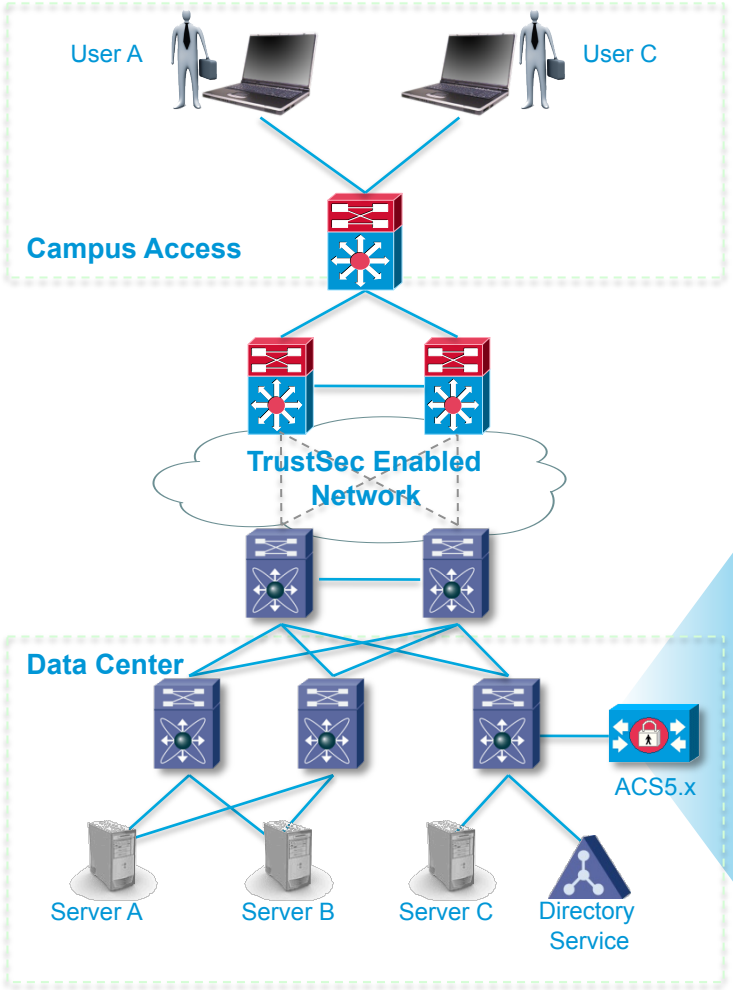
ACS SGACL Policy

SRC\ DST	SRVSGT 111	SRVSGT 222	SRVSGT 333
User SGT 10	Permit all	Deny all	Deny all
User SGT 20	SGACL-B	SGACL-C	Deny all
User SGT 30	Deny all	Permit all	SGACL-D

SGACL D

```
#remark destination SQL permit
  permit tcp  src  dst  eq 1433
#remark source SQL permit
  permit tcp src  eq 1433
# web permit
  permit tcp  src  dst eq 80
# secure web permit
  permit tcp  src  dst eq 443
  deny all
```

SGACL Flow
Step 1: Policy Population



Step 1 **ACS populates its SGT policy**

- ACS is configured for its policy and all endpoints need to be mapped to SGT in policy

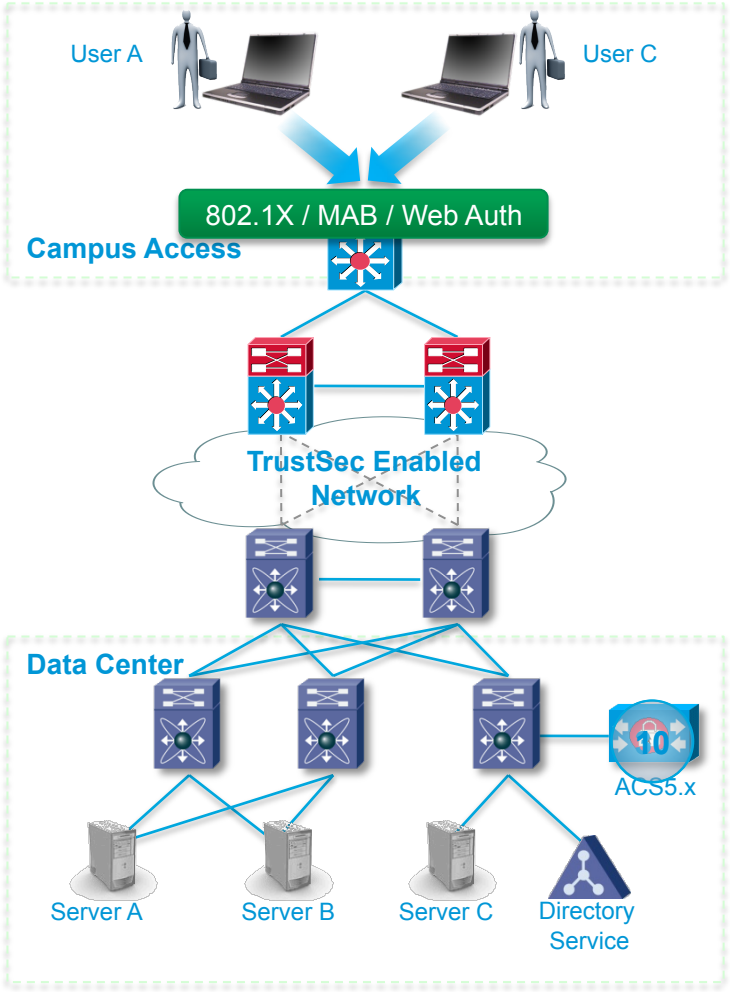
User to Role Mapping

AD User	Role	SGT
User A	Contractor	10
User B	Finance	20
User C	HR	30

Server to Role Mapping

Server	Role	IP	SGT
HTTP Server	Server Group A	10.1.100.111	111
File Server	Server Group B	10.1.100.222	222
SQL Server	Server Group C	10.1.200.3	333

SGACL Flow
Step 2: SGT Assignment



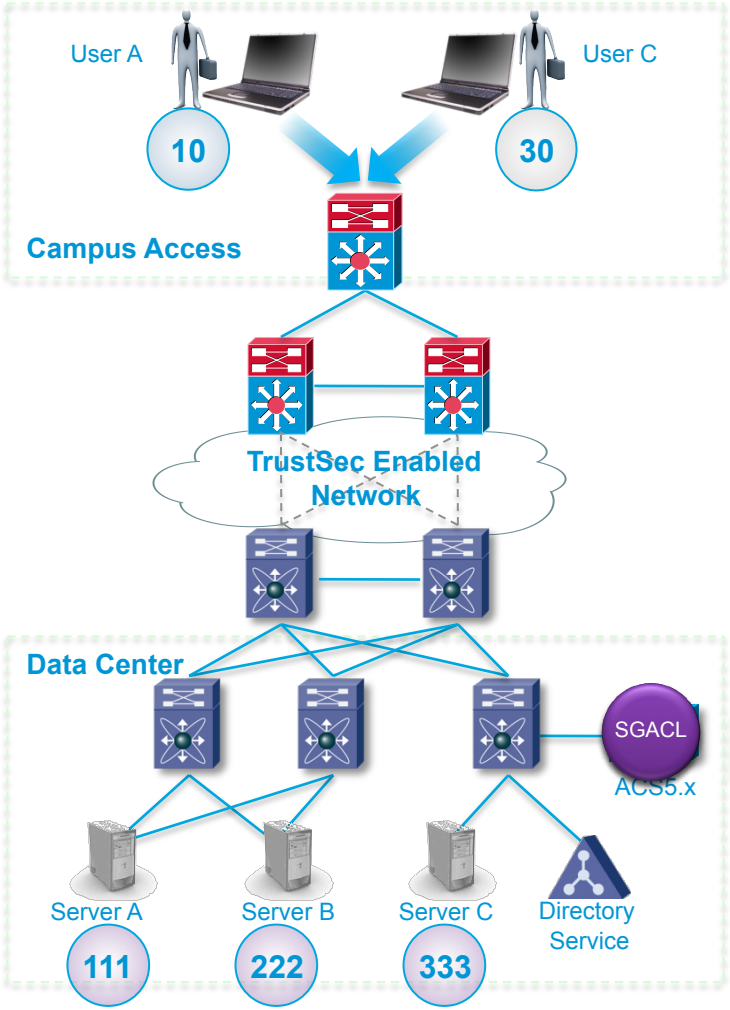
Step 2 **SGTs are assigned to role and bound to IP address**

- With 802.1X / MAB / Web Authentication, SGTs are assigned in an authorization policy via RADIUS
- Access devices snoops ARP and / or DHCP for authenticated MAC Address, then bind assigned SGT to snooped IP Address
- For Servers IP addresses are bound to SGT statically on access switch or dynamically looked up on ACS using IPM feature

AD User	Role	SGT
User A	Contractor	10
User B	Finance	20
User C	HR	30

Server	Role	IP	SGT
HTTP Server	Server Group A	10.1.100.111	111
File Server	Server Group B	10.1.100.222	222
SQL Server	Server Group C	10.1.200.3	333

SGACL Flow
Step 3: SGACL Policy Provisioning



Step 3 **ACS provisions Egress Policy (SGT Matrix) to TrustSec capable Device**

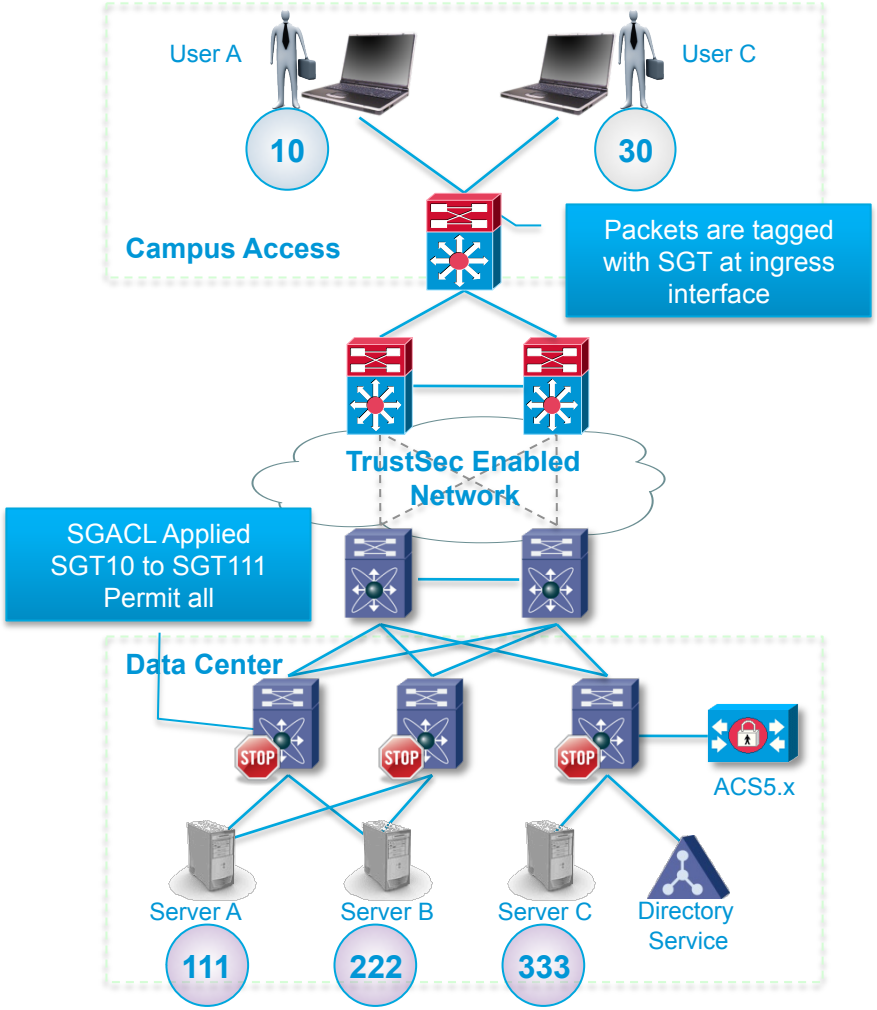
- Each TrustSec capable device downloads policy from central policy server, that is, ACS server

SRC\ DST	Server A (111)	Server B (222)	Server C (333)
User A (10)	Permit all	Deny all	Deny all
User B (20)	SGACL-B	SGACL-C	Deny all
User C (30)	Deny all	**SGACL-D**	Permit all

SGACL-D

```
permit tcp  src  dst  eq 1433
#remark destination SQL permit
permit tcp src  eq 1433  dst
#remark source SQL permit
permit tcp  src  dst eq 80
# web permit
permit tcp  src  dst eq 443
# secure web permit
deny all
```

SGACL Flow
Step 4: SGACL Enforcement (1)

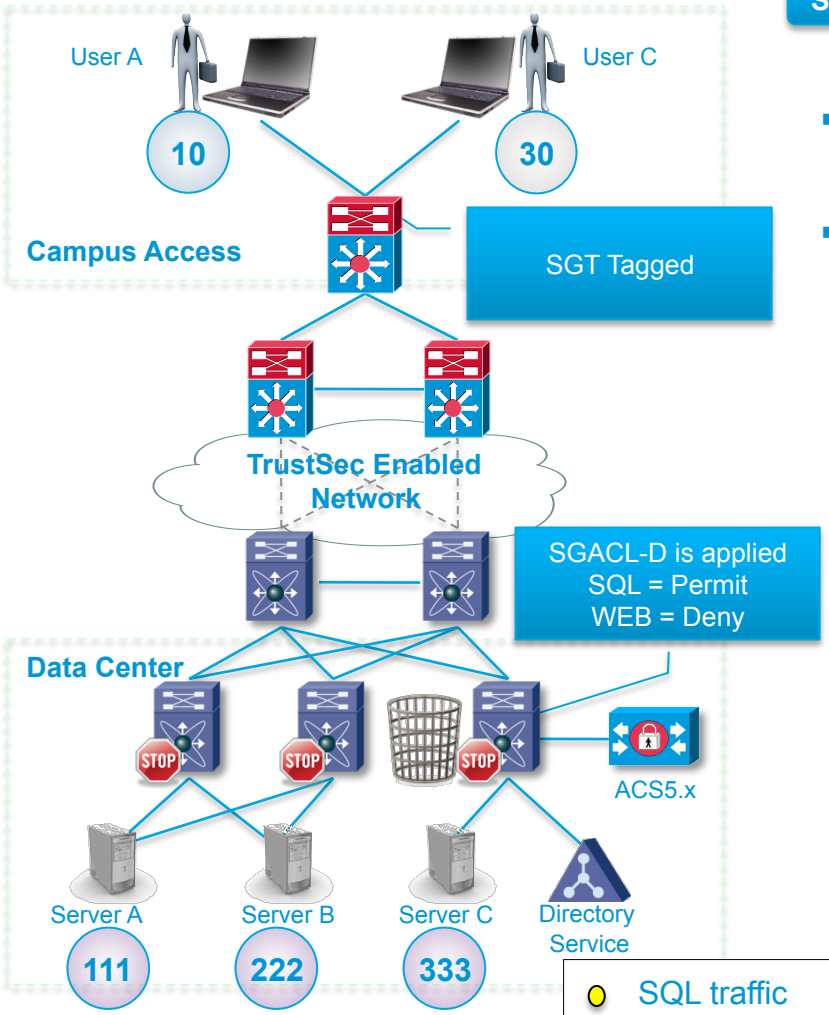


Step 4 **Now TrustSec network is ready to enforce the policy**

- User's traffic is tagged at ingress of TrustSec domain
- SGT is carried when packet traverses within domain
- At egress port, TrustSec device looks up local policy and drops packet if needed

SRC\ DST	Server A (111)	Server B (222)	Server C (333)
User A (10)	Permit all	Deny all	Deny all
User B (20)	SGACL-B	SGACL-C	Deny all
User C (30)	Deny all	**SGACL-D**	Permit all

SGACL Flow
Step 5: SGACL Enforcement (2)



Step 5 **SGACL allows topology independent access control**

- Even another user accesses on same VLAN as previous example, his traffic is tagged differently
- If traffic is destined to restricted resources, packet will be dropped at egress port of TrustSec domain

SRC\ DST	Server A (111)	Server B (222)	Server C (333)
User A (10)	Permit all	Deny all	Deny all
User B (20)	SGACL-B	SGACL-C	Deny all
User C (30)	Deny all	Permit all	**SGACL-D**

SGACL-D

```
permit tcp  src  dst  eq 1433
#remark destination SQL permit
permit tcp src  eq 1433  dst
#remark source SQL permit
deny tcp  src  dst eq 80
# web deny
deny tcp  src  dst eq 443
# secure web deny
deny all
```

TrustSec is based on “Trust”

- Any member of TrustSec domain needs to establish trust relationship to its peer, otherwise not trusted
- Only SGT from trusted member can be “trusted” and processed by its peer
- A process of authenticating is called “Endpoint Admission Control” (e.g. SGT tagging via 802.1X)
- A process of authenticating network device is called “Network Device Admission Control” or NDAC in short

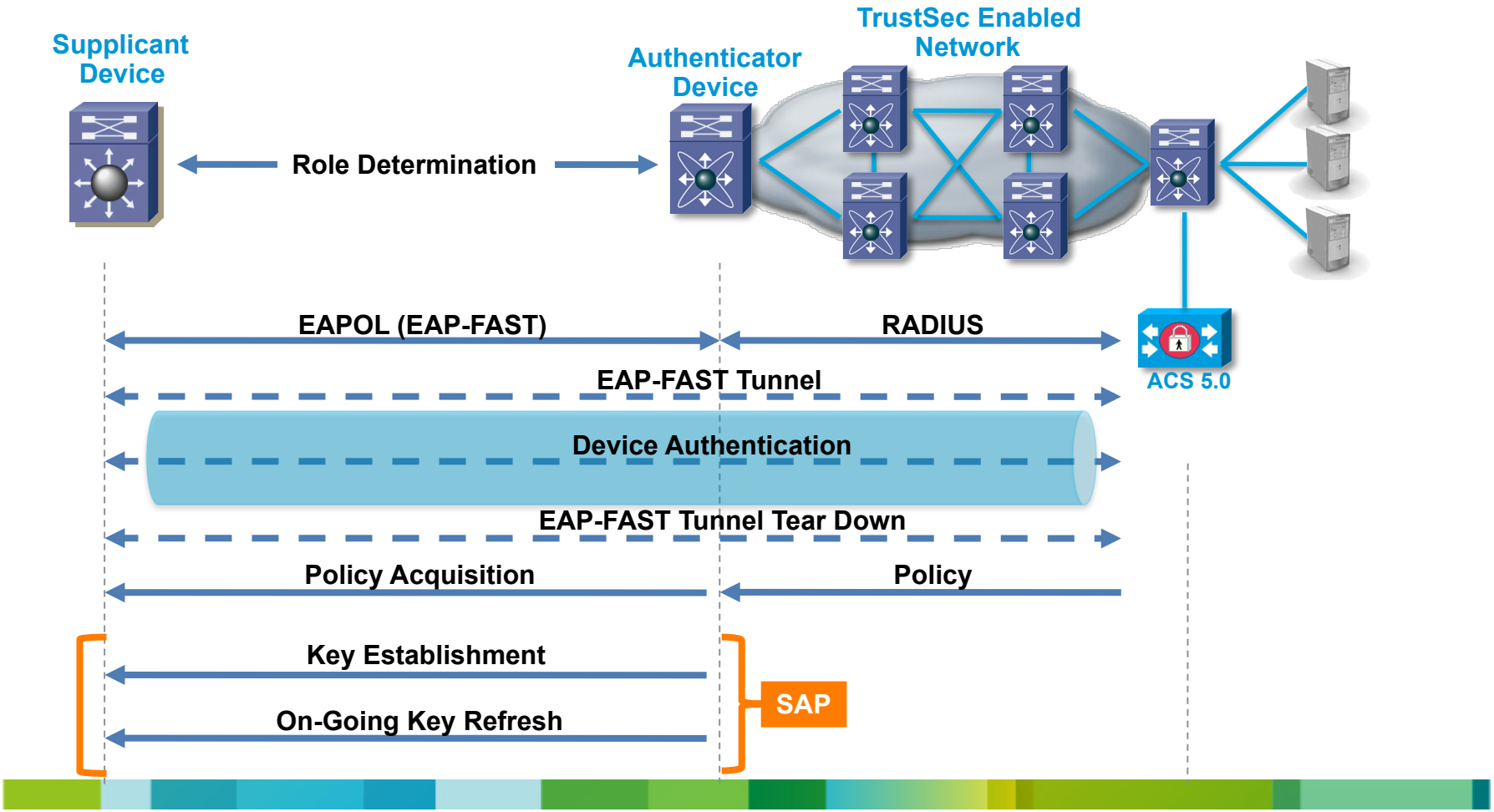
Network Device Admission Control

- Provides strong **mutual authentication (EAP-FAST) to form trusted domain**
- Only SGT from **trusted peer is honored**
- **Security Association Protocol (SAP)** is used to negotiate keys and cipher suite for encryption automatically as defined in 802.11i
- 802.1X-2010 redefines key negotiation and will replace SAP
- Authentication and policy provisioning provided by ACS server

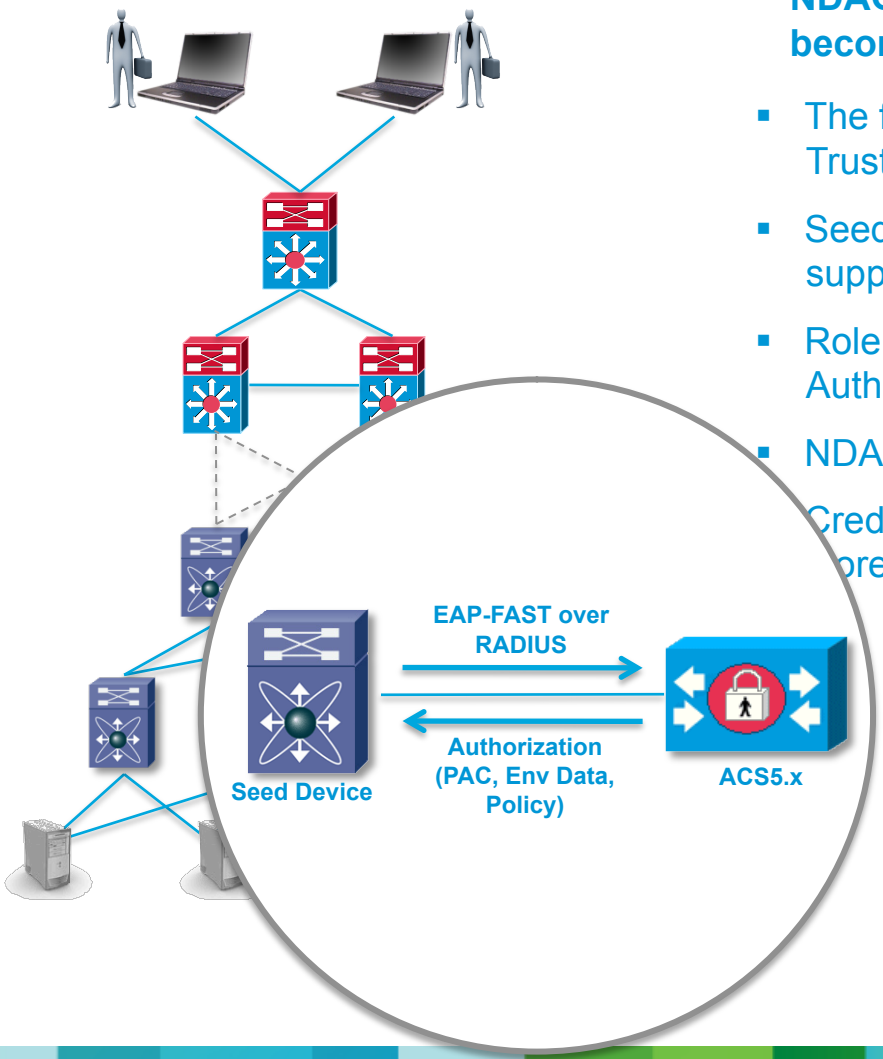
Customer Benefits

- Mitigate rogue network devices, **establish trusted network fabric** to ensure SGT integrity and its privilege
- Automatic key and cipher suite negotiation for **strong 802.1AE based encryption**

NDAC Authentication / SAP



TrustSec Domain Establishment
Seed Device Authentication

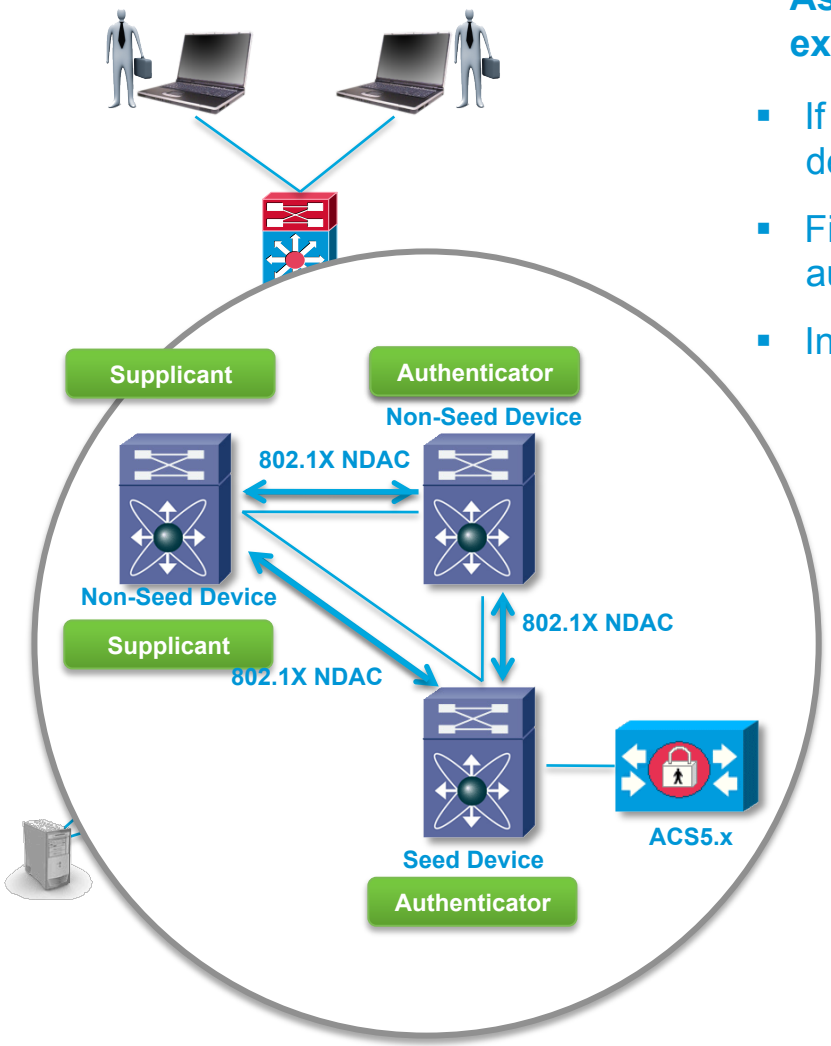


NDAC validates peer identity before peer becomes the circle of Trust!

- The first device to authenticate against ACS is called TrustSec Seed Device
- Seed Device becomes authenticator to its peer supplicant
- Role determination process selects both Authenticator and Supplicant role
- NDAC utilizes EAP-FAST/MSCHAPv2

Credential (including PAC) is stored in hardware key
ore

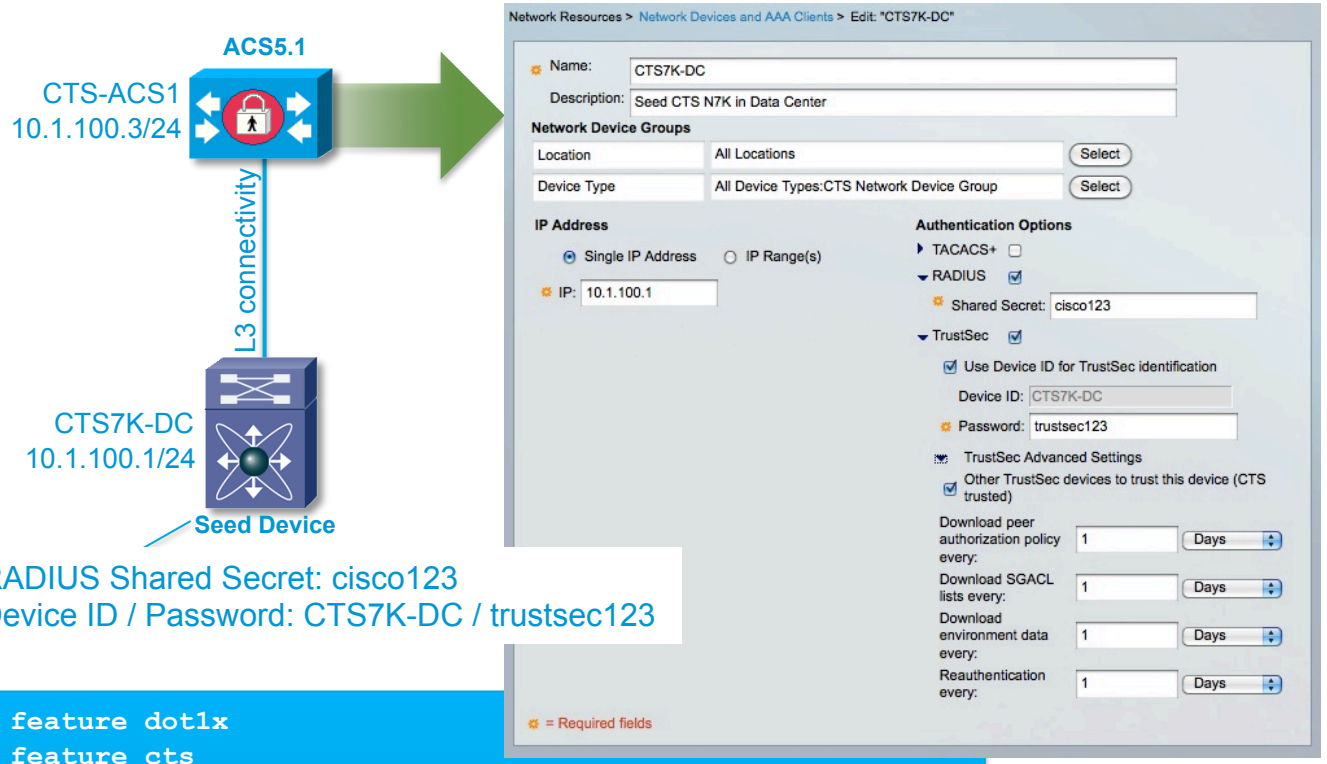
TrustSec Domain Establishment
Non-Seed Device Authentication



As device connects to its peer, TrustSec domain expands its border of trust

- If the device is not connected to ACS directly, the device is called non-Seed Device
- First peer to gain ACS server connectivity wins authenticator role
- In case of tie, lower MAC address wins

Sample Seed Device Configuration




```
CTS7K-DC(config)# feature dot1x
CTS7K-DC(config)# feature cts
CTS7K-DC(config)# cts device-id CTS7K-DC password trustsec123
CTS7K-DC(config)# radius-server host 10.1.100.3 key cisco123 pac
CTS7K-DC(config)# aaa group server radius cts-radius-grp
CTS7K-DC(config-radius)# server 10.1.100.3
CTS7K-DC(config-radius)# use-vrf default
CTS7K-DC(config-radius)# exit
CTS7K-DC(config)# aaa authentication dot1x default group cts-radius-grp
CTS7K-DC(config)# aaa authorization cts default group cts-radius-grp
CTS7K-DC(config)# aaa accounting dot1x default group cts-radius-grp
```

Confidentiality and Integrity 802.1AE based Encryption

- TrustSec provides Layer 2 hop-by-hop encryption and integrity, based on IEEE 802.1AE standard
- 128bit AES-GCM (Galois/Counter Mode) – NIST Approved *
- Line rate Encryption / Decryption for both 10GbE/1GbE interface
- Replay Protection of each and every frame
- 802.1AE encryption to protect CMD field (SGT value)

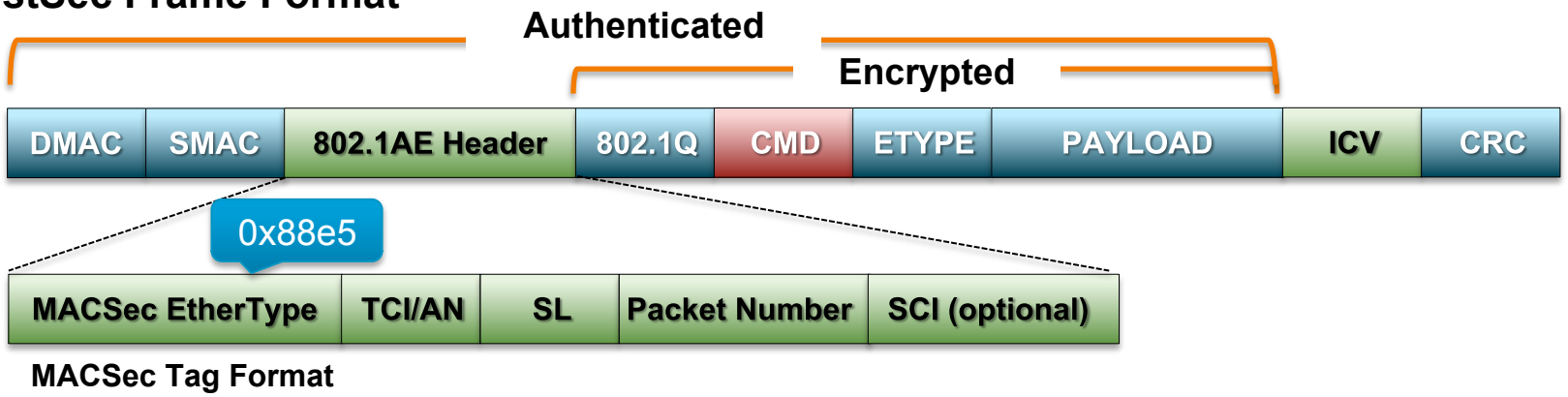
Customer Benefits

- Protects against man-in-the-middle attacks (snooping, tampering, replay)
- Standards based frame format and algorithm (AES-GCM)
- 802.1X-REV/MKA addition supports per-device security associations in shared media environments (e.g. PC vs. IP Phone) to provide secured communication
- hop-by-hop approach compared to end-to-end approach (e.g. Microsoft Domain Isolation/IPsec)

- * NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

802.1AE (MACSec) Tagging

TrustSec Frame Format

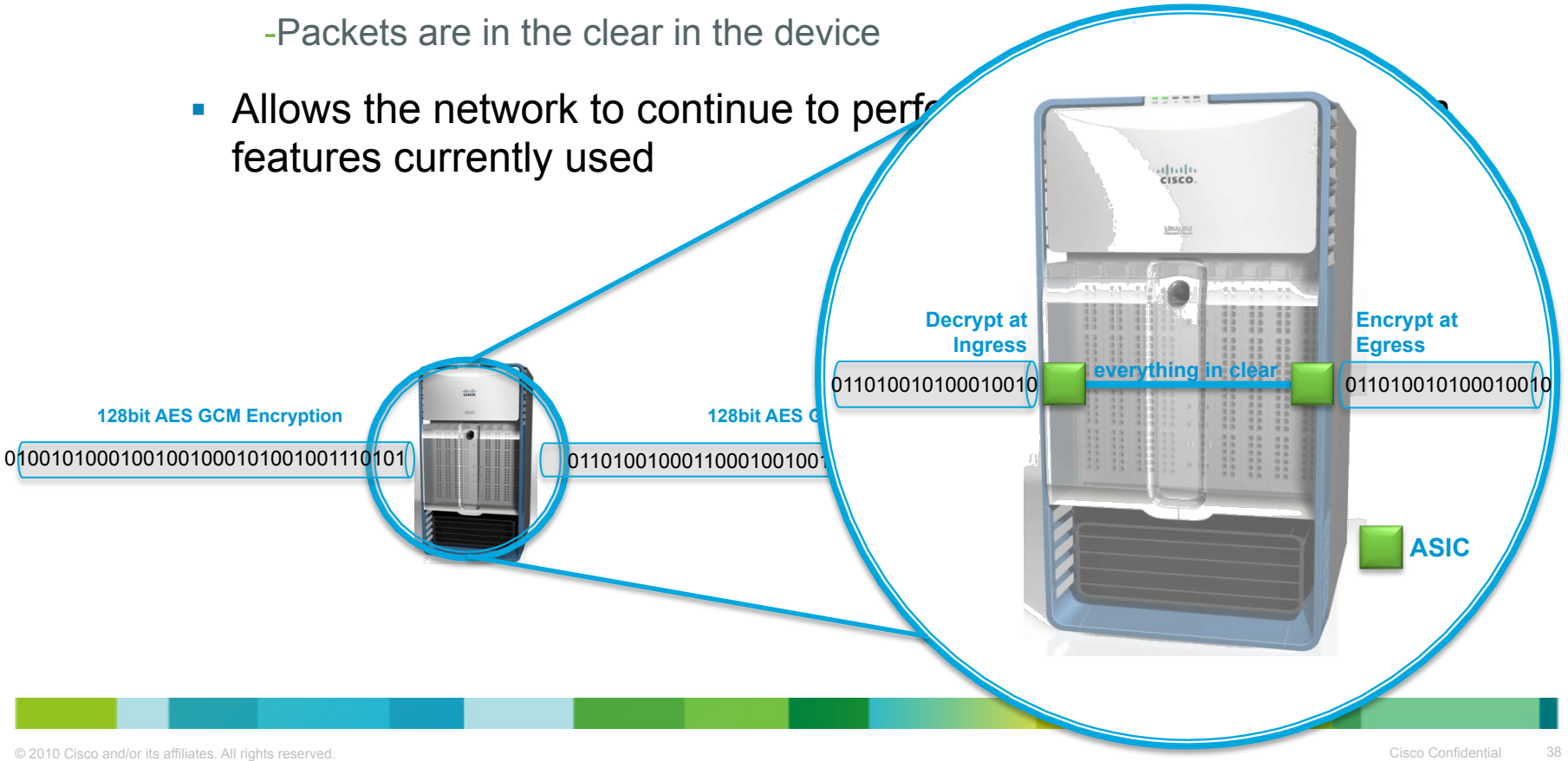


MACSec Tag Format

```
Frame 502 (287 bytes on wire, 287 bytes captured)
Ethernet II, Src: Cisco_c2:d4:42 (00:1b:54:c2:d4:42), Dst: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
  Destination: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
      Address: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Source: Cisco_c2:d4:42 (00:1b:54:c2:d4:42)
      Address: Cisco_c2:d4:42 (00:1b:54:c2:d4:42)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: Unknown (0x88e5)
Data (273 bytes)
    Data: 2C000001000B001B54C1EFFA0000C655C93421ED794C9842...
```

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 perf… features currently used



Cisco TrustSec Deployment Practice

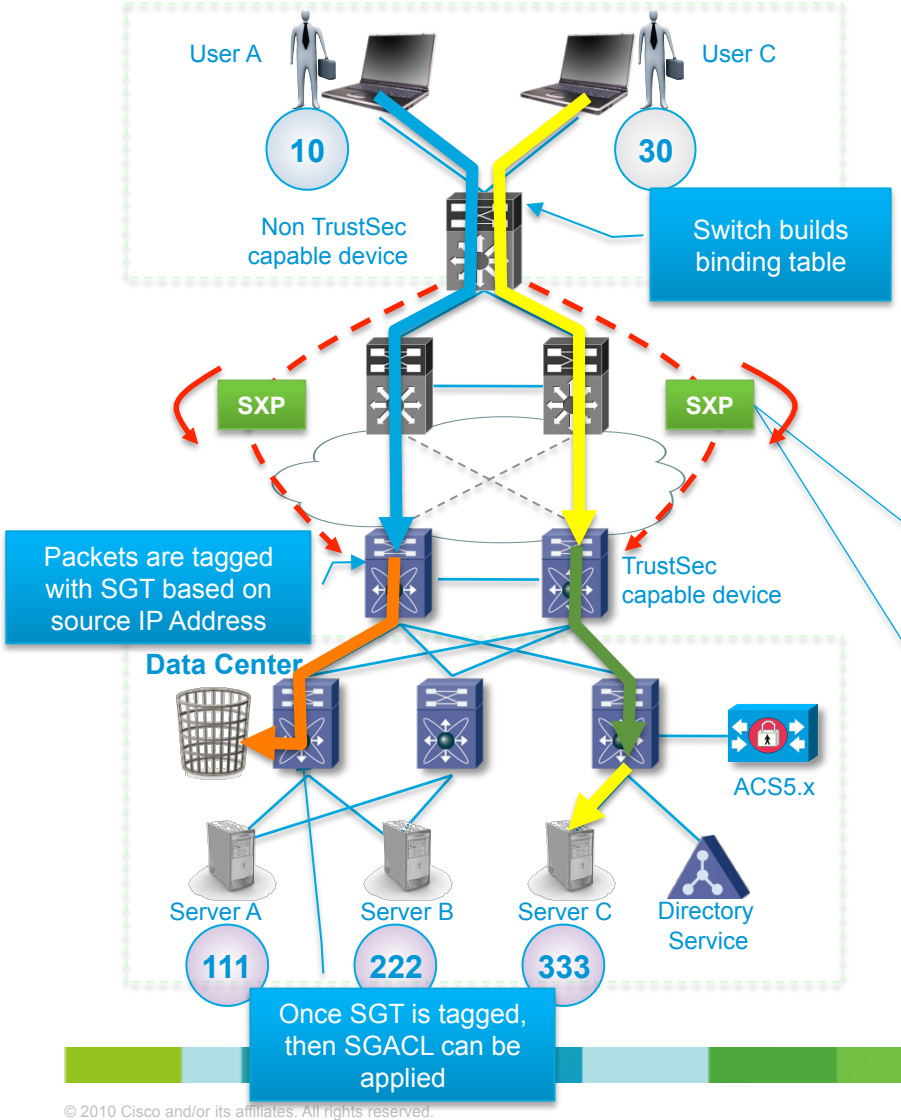
Deployment Flow

- What about all my other network devices that don’t support TrustSec hardware?
- How should I assign SGTs at different points in the network?
- What use cases are covered by TrustSec
- How should I phase a rollout with Identity services?
- How do I monitor and report on TrustSec?
- What platforms support SXP?

Legacy Platform Support with SXP

- SGT native tagging requires hardware (ASIC) support
- Non-TrustSec hardware capable devices can still receive SGT attributes from ACS for authenticated users or devices, and then forward the IP-to-SGT binding to a TrustSec SGACL capable device for tagging & enforcement
- SGT eXchange Protocol (SXP) is used to exchange IP-to-SGT bindings between TrustSec capable and incapable device
- Currently Catalyst 6500, 4500/4900, 3750, 3560 (and new access switches) and Nexus 7000 switch platform support SXP
- SXP accelerates deployment of SGACL by without extensive hardware upgrade for TrustSec

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 TrustSec capable device
- TrustSec 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	10	Gig 2/10
10.1.30.4	30	Gig 2/11

User A

- Untagged Traffic
- CMD Tagged Traffic

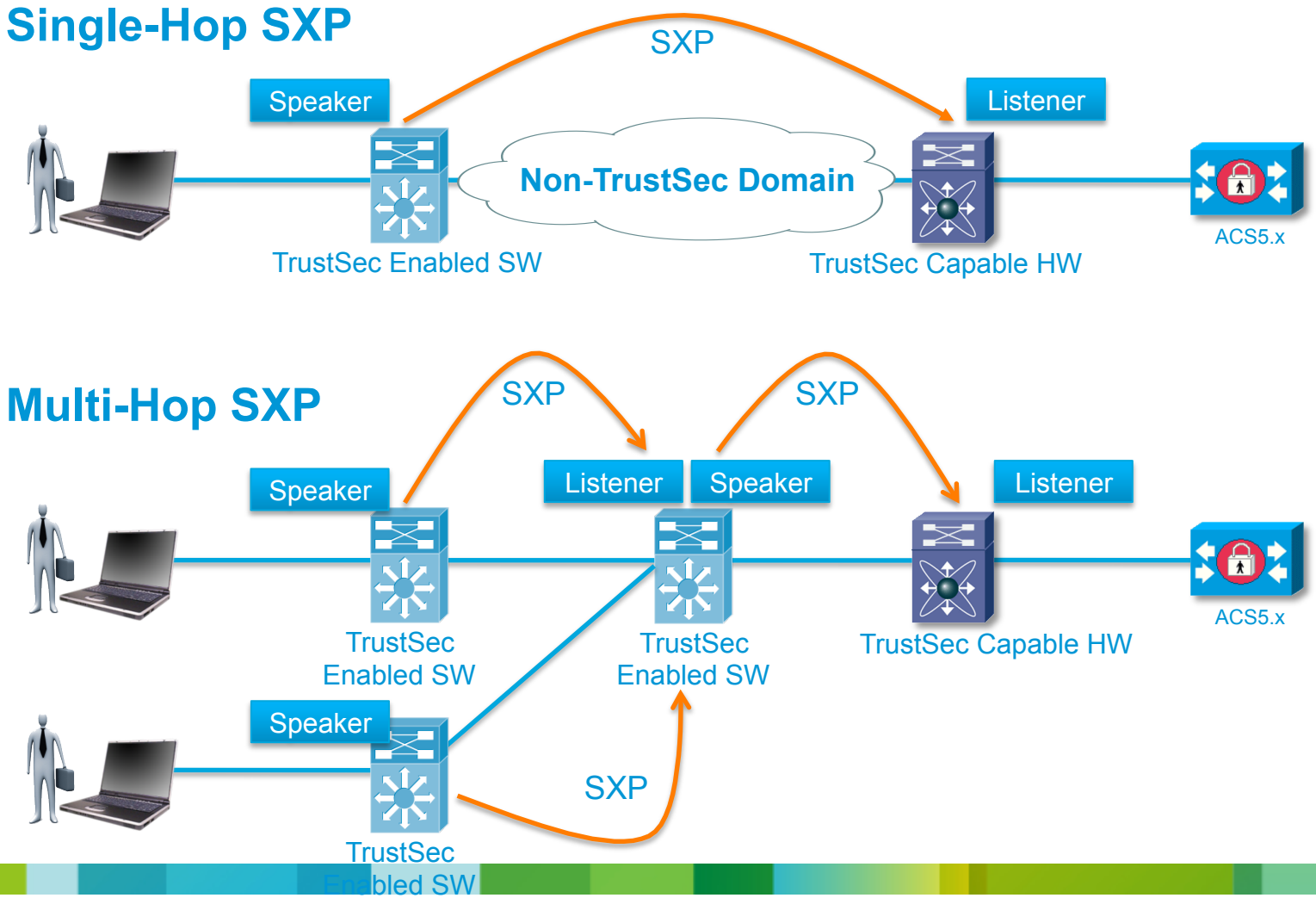
User C

- Untagged Traffic
- CMD Tagged Traffic

SGT Exchange Protocol Detail (1)

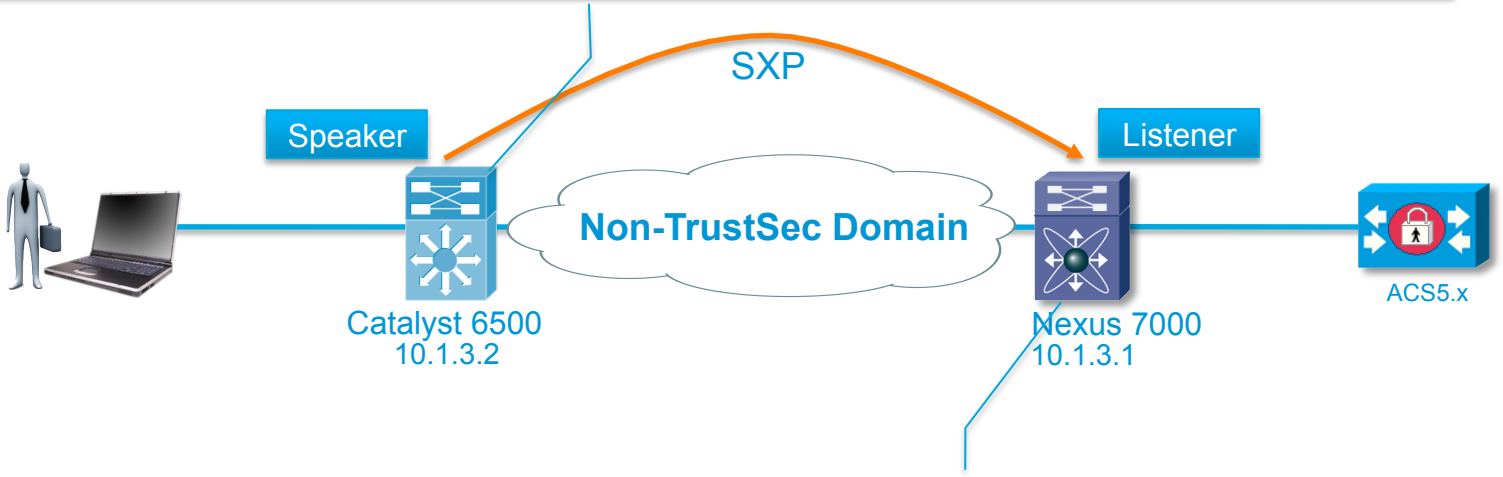
- Uses TCP for transport protocol
- TCP port 64999 for connection initiation
- Support Single/Multi-Hop (SXP relay) SXP connection
- Use MD5 for authentication and integrity check
- Two roles: Speaker (initiator) and Listener (receiver)

SXP Connection Types



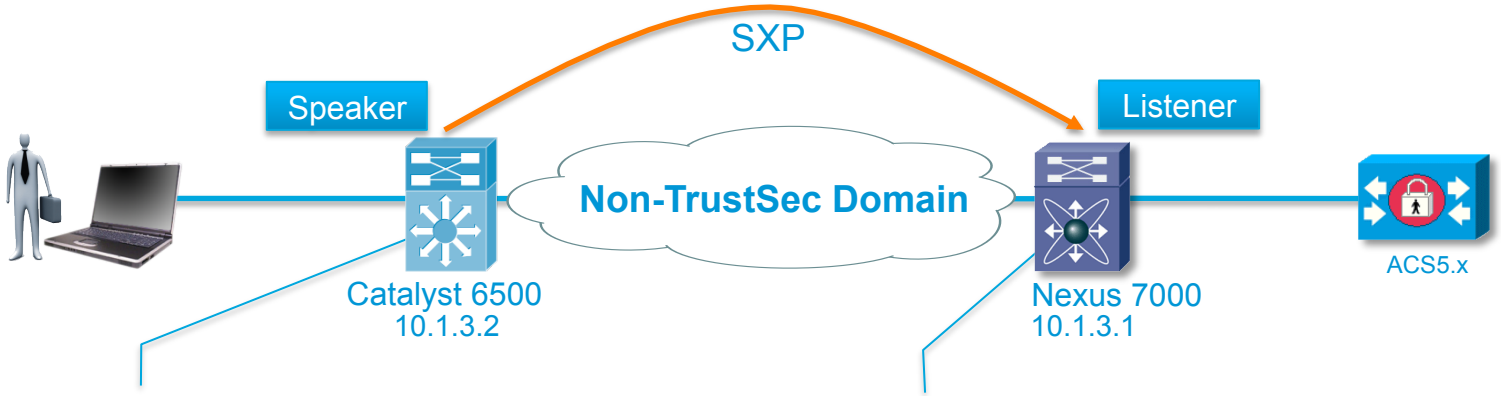
SXP Configuration Sample

CTS6K-AS(config)#**cts sxp enable**
CTS6K-AS(config)#**cts sxp default password <password>**
CTS6K-AS(config)#**cts sxp connection peer 10.1.3.1 source 10.1.3.2 password default mode peer listener**



CTS7K-DC(config)#**cts sxp enable**
CTS7K-DC(config)#**cts sxp connection peer 10.1.3.2 source 10.1.3.1 password required <password> mode speaker**

SXP Connection Verification



CTS6K-AS#show cts sxp connections
SXP : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running

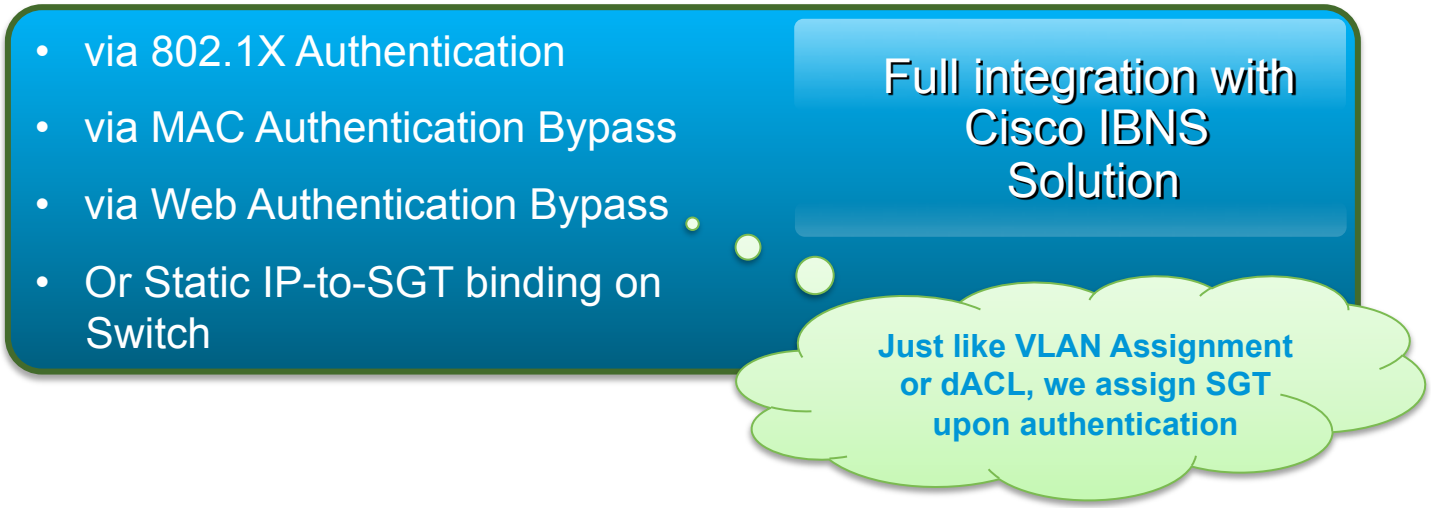
Peer IP : 10.1.3.1
Source IP : 10.1.3.2
Conn status : On
Local mode : SXP Speaker
Connection inst# : 1
TCP conn fd : 1
TCP conn password: default SXP password
Duration since last state change: 5:21:56:26 (dd:hr:mm:sec)

CTS7K-DC# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120

SGT Assignment Practice – Campus

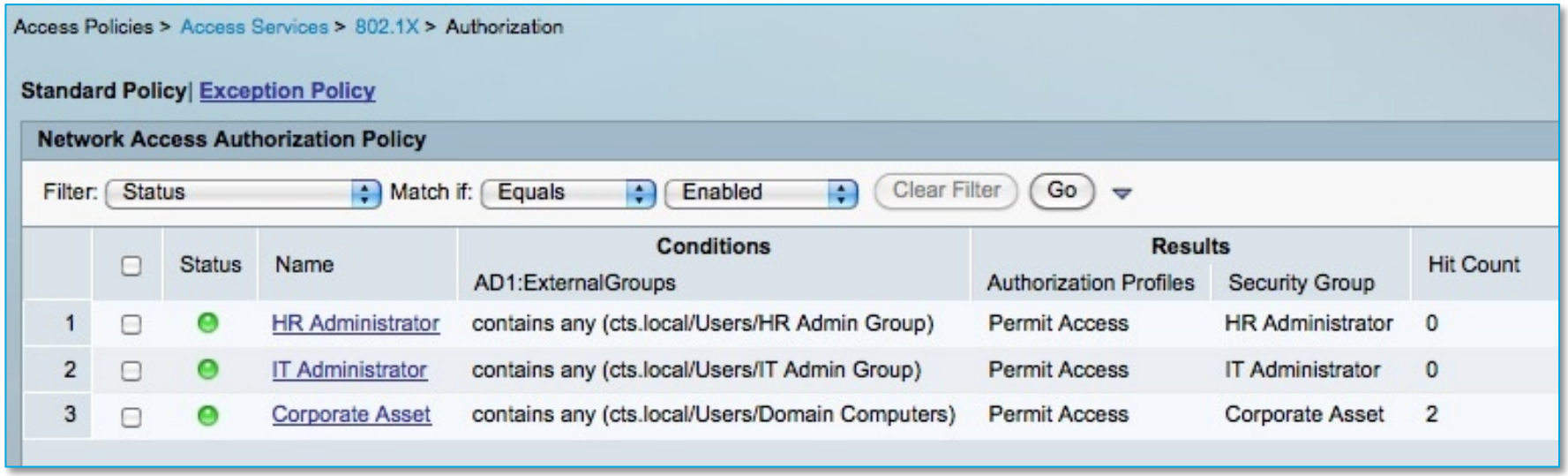
Campus/Mobile endpoints

- **Every endpoint that touches TrustSec domain is classified with SGT**
- **SGT can be sent to switch via RADIUS authorization after:**



Sample SGT Assignment Policy

- Sample 802.1X authorization policy to assign Security Group to individual role



Access Policies > Access Services > 802.1X > Authorization

Standard Policy | Exception Policy

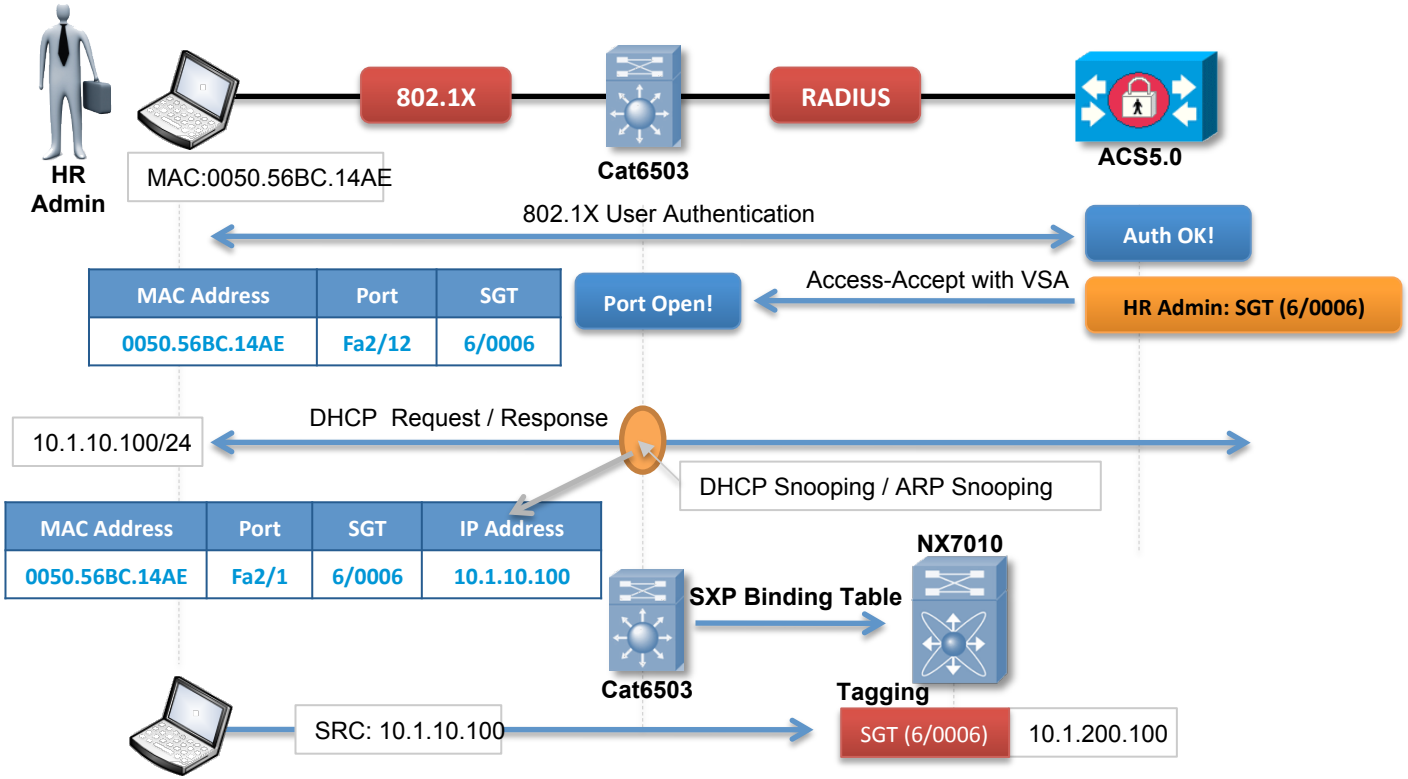
Network Access Authorization Policy

Filter: Status | Match if: Equals | Enabled | Clear Filter | Go

		Status	Name	Conditions	Results		Hit Count
				AD1:ExternalGroups	Authorization Profiles	Security Group	
1	☐	●	HR Administrator	contains any (cts.local/Users/HR Admin Group)	Permit Access	HR Administrator	0
2	☐	●	IT Administrator	contains any (cts.local/Users/IT Admin Group)	Permit Access	IT Administrator	0
3	☐	●	Corporate Asset	contains any (cts.local/Users/Domain Computers)	Permit Access	Corporate Asset	2

SGT Assignment - Campus

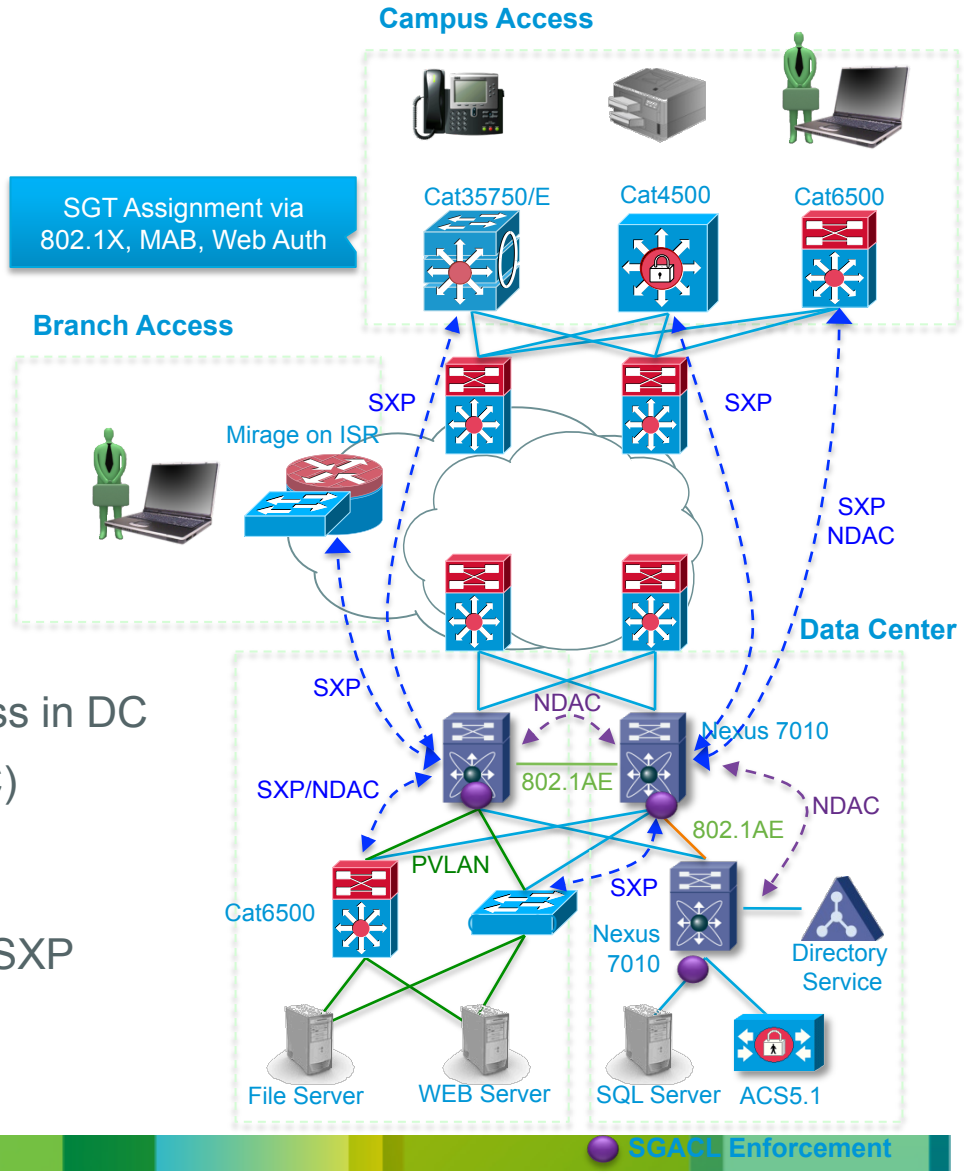
- How the SGT is assigned to role dynamically



Cisco TrustSec Deployment Use Cases

TrustSec Technology High Level Overview

- SGT Assignment (Endpoint)
  - 802.1X based
  - MAB based
  - Web Auth based
- SGT Assignment (Data Center)
  - Static IP-to-SGT mapping
  - Port to SGTmapping
- SGACL Enforcement
  - User role based enforcement at egress in DC
  - Server group based enforcement (DC)
- Network Device Admission Control
- IP-to-SGT binding table forwarding via SXP
- 802.1AE based L2 encryption
  - Network and endpoint based

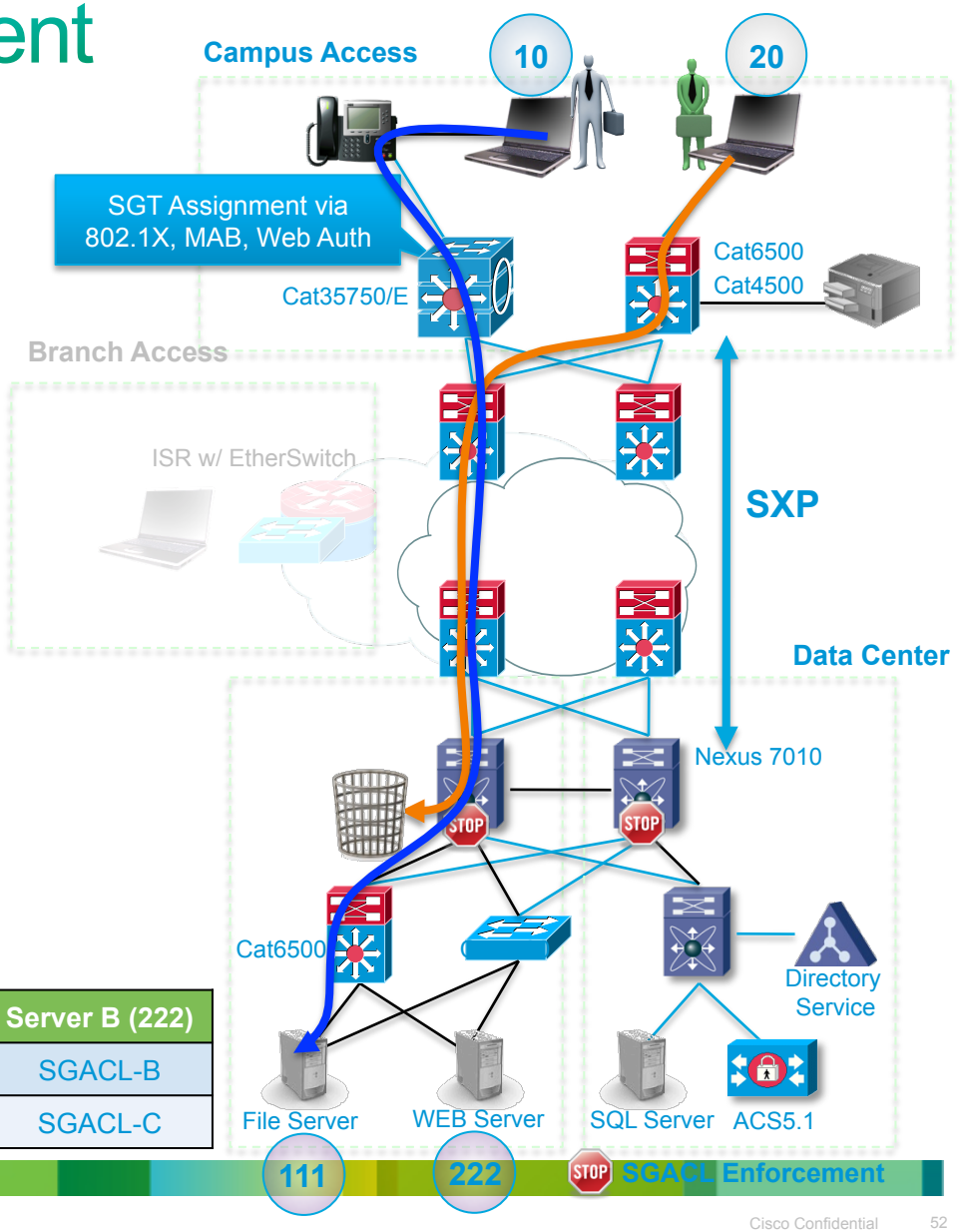


Use Case 1: Campus LAN Deployment

Use Case 1

TrustSec to cover campus network as well as Data Center 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 center TrustSec capable device



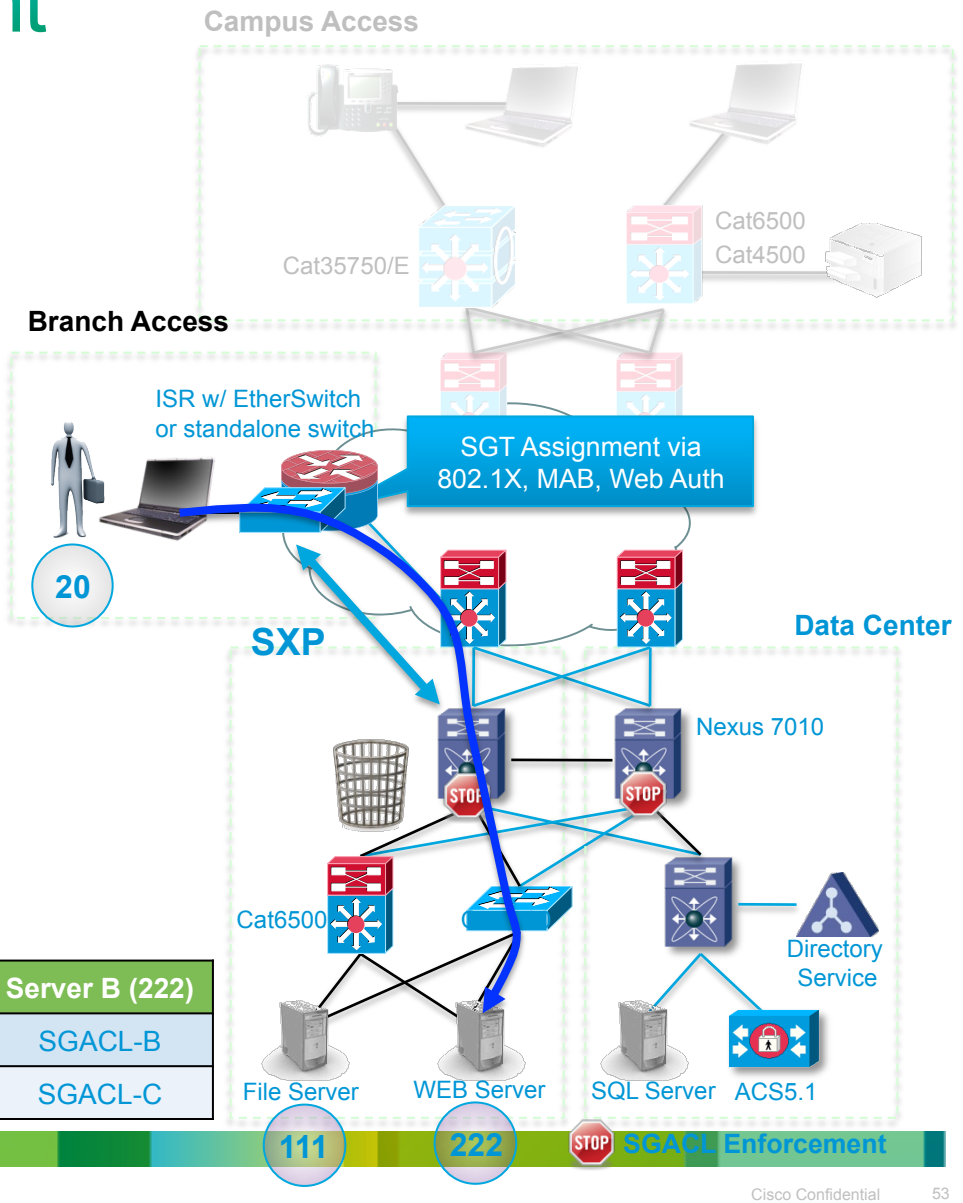
SRC \ DST	Server A (111)	Server B (222)
User A (10)	Permit all	SGACL-B
User B (20)	Deny all	SGACL-C

Use Case 2: Branch LAN Deployment

Use Case 2

TrustSec to cover Branch office LAN as well as Data Center 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 center TrustSec capable device



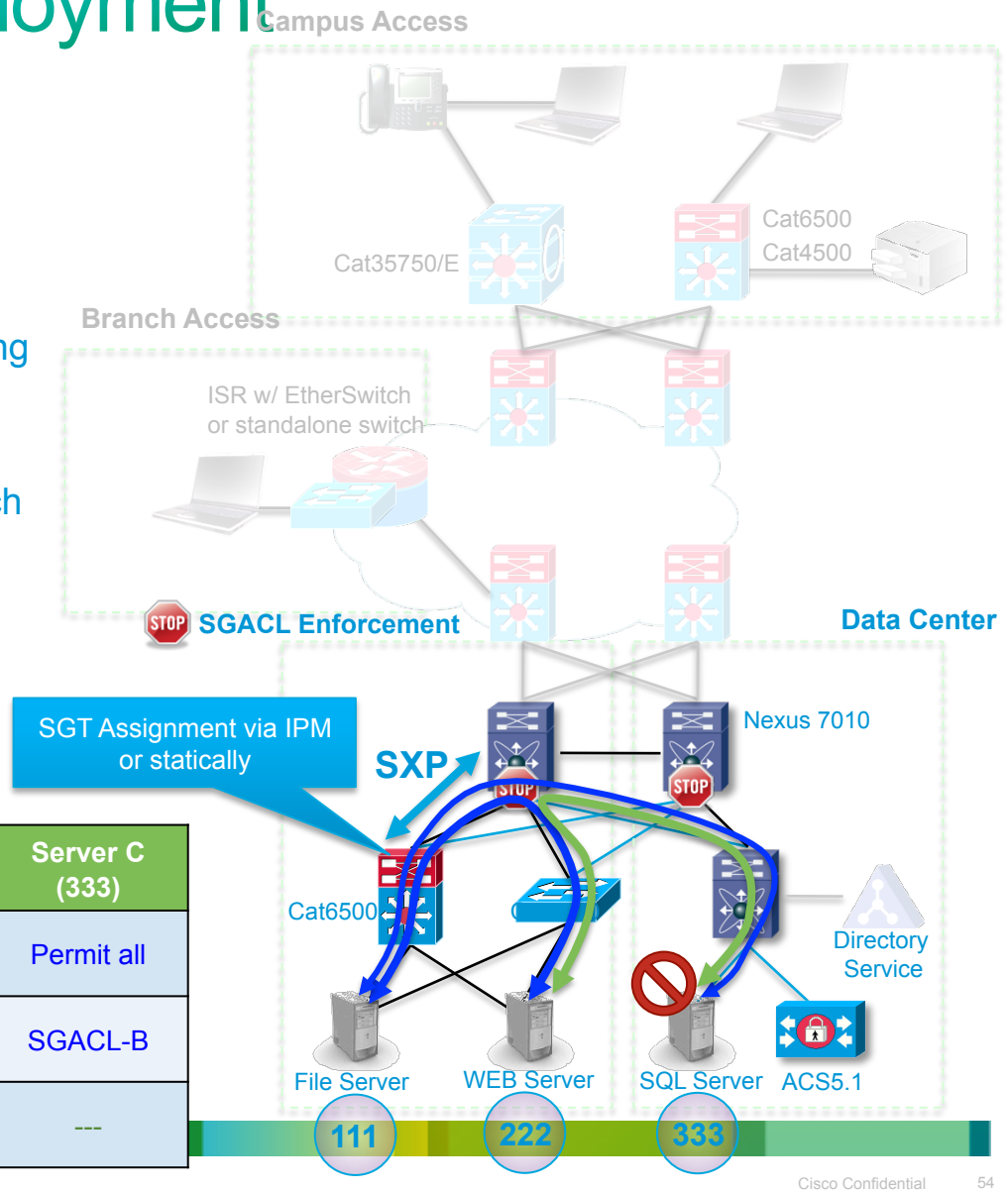
SRC \ DST	Server A (111)	Server B (222)
User A (10)	Permit all	SGACL-B
User B (20)	Deny all	SGACL-C

Use Case 3: Intra Data Center Deployment

Use Case 3

TrustSec to cover Intra Data Center for server traffic segmentation

- Manual server IP address to SGT binding on Nexus 7000 or IPM to ACS for centralized SGT management
- Server connected to same access switch can be segmented using Private VLAN feature to distribution switch

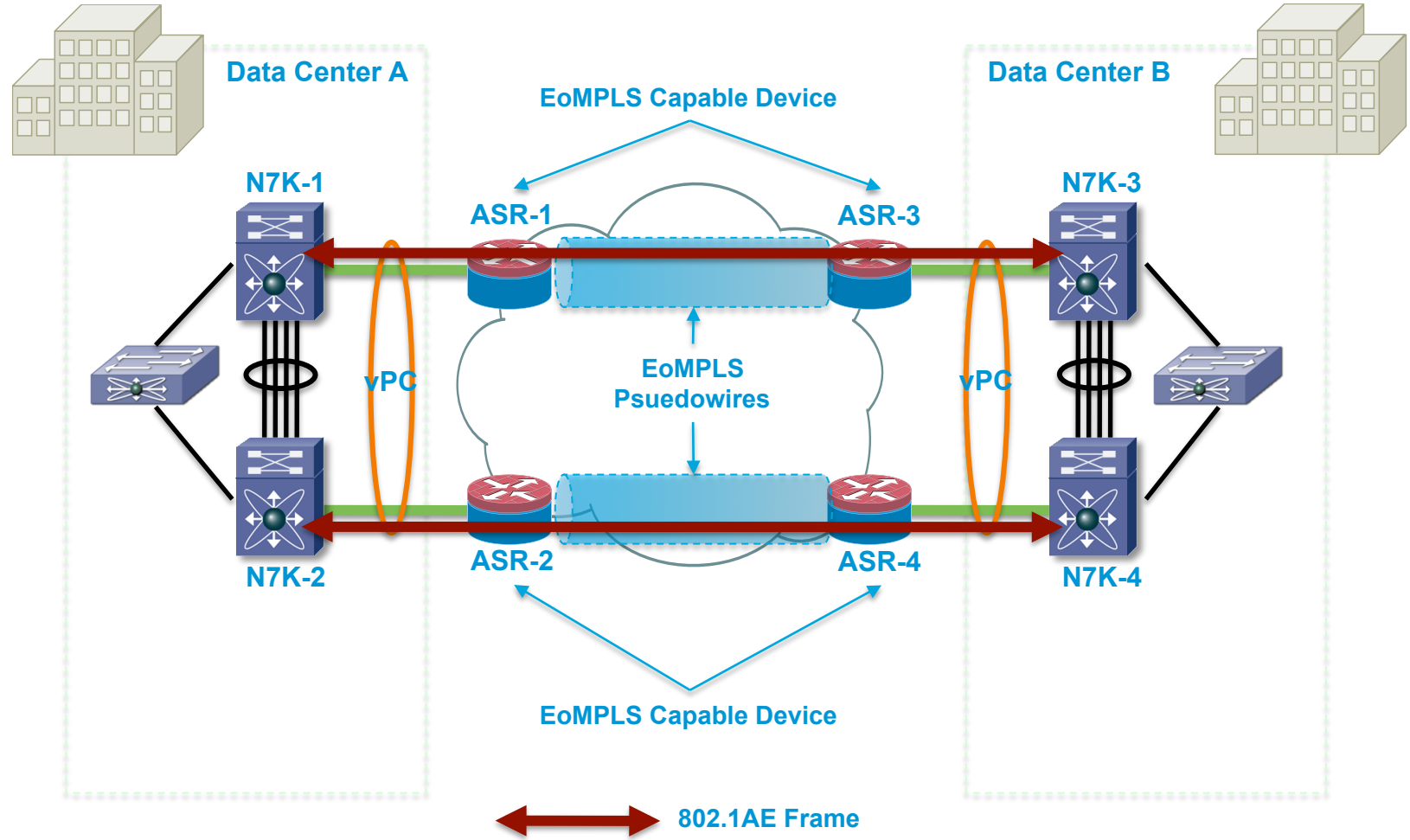


SRC \ DST	Server A (111)	Server B (222)	Server C (333)
Server A (111)	---	SGACL-A	Permit all
Serer B (222)	Permit all	---	SGACL-B
Server C (333)	Deny all	Deny all	---

Encrypted Inter-DC Link with 802.1AE

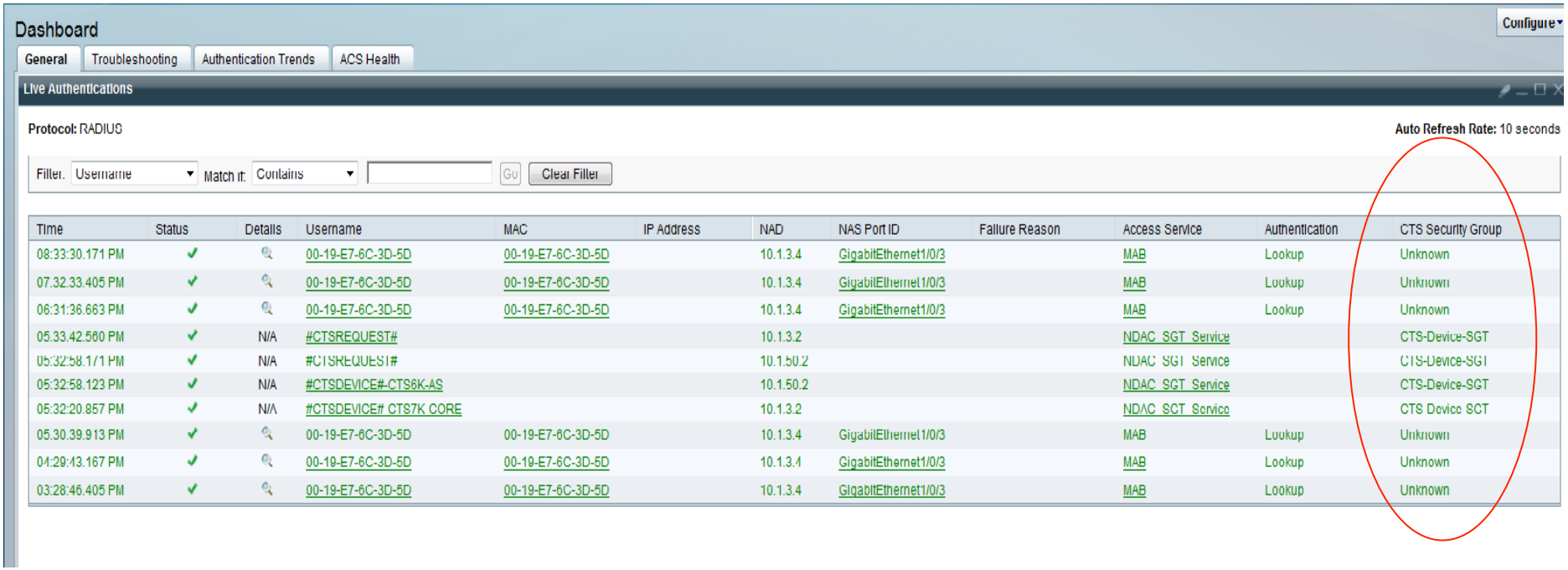
- Can TrustSec encrypt the link between multiple Data Center for secure backup / DR purpose?
- 802.1AE technology can be used to encrypt point-to-point link with following conditions
  - 10Gbps or 1Gbps link between Nexus 7000s if both Nexus 7Ks are connected with dark fiber or passive repeater between DCs so that L2 frame is not manipulated
  - Or use EoMPLS Pseudowire to encapsulate 802.1AE frame between two Data Centers

Sample Topology for 802.1AE over EoMPLS



Monitoring and Reporting Cisco TrustSec

TrustSec Information in Basic Reports



TrustSec Reports

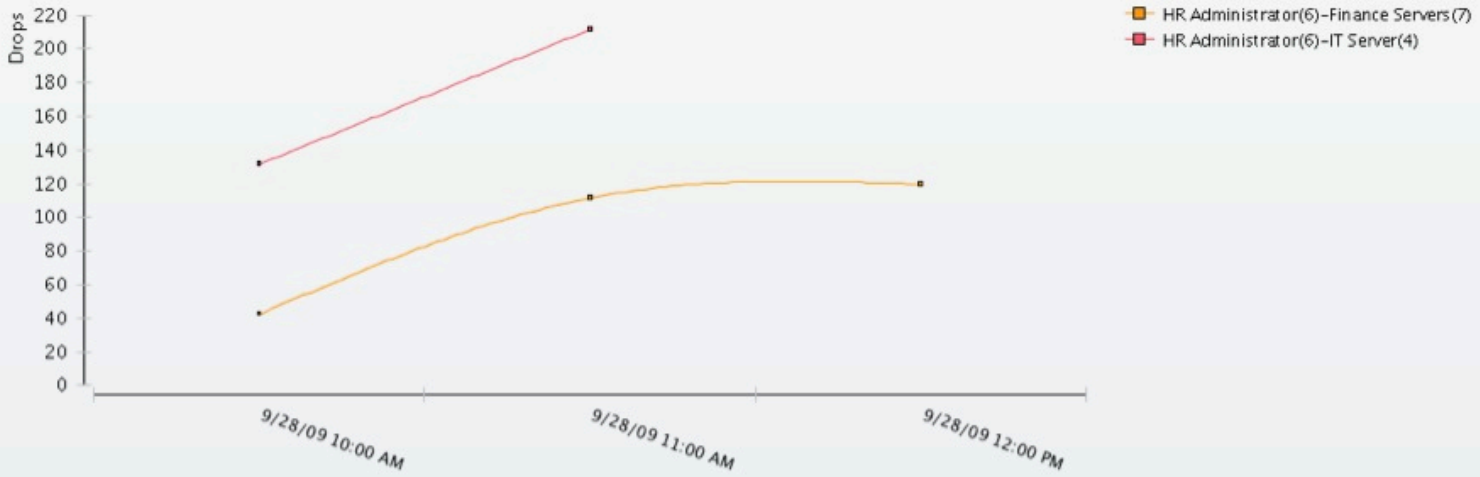
Monitoring SGACL Drops

TrustSec > RBACL Drop Summary

Date : September 28, 2009

Generated on : September 28, 2009 2:12:09 PM PDT

Reload



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

TrustSec Tools

- Native Tools in ACS 5.1 to compare ACS/Switch Information
- Validate SXP bindings on differing switches
- Validate User/Device SGT assignment

Trust Sec Tools	
Egress (SGACL) Policy	Compare Egress Policy (SGACL Policy) in Network Device and ACS.
SXP-IP Mappings	Compare SXP Mappings in Device versus Peers.
IP User SGT	Compare IP-SGTs on a device with ACS assigned SGT records.
Device SGT	Compare Device SGT to ACS assigned Device SGT.

ACS 5.1/5.2 Platform Options

1121 Hardware Appliance

One rack-unit (1RU) security-hardened, Linux-based appliance

VMware Appliance

Complete appliance image for installation on VMware ESX 3.5 or 4.0

vmware

Session Summary

Reference Slide

TrustSec Component Support Matrix

Platforms	Available Feature	OS Version	Notes
Nexus 7000 series Switch	SGACL, 802.1AE + SAP, NDAC, SXP, IPM, EAC	Cisco NX-OS® 4.2.2. Advanced Service Package license is required	Mandatory as enforcement point
Catalyst 6500E Switch (Supervisor 32, 720, 720-VSS)	NDAC (No SAP), SXP, EAC	Cisco IOS® 12.2 (33) SXI3 or later release. IP Base w/ K9 image required	Campus access / distribution switch, DC access switch
Catalyst 49xx switches	SXP, EAC	Cisco IOS® 12.2 (53) SG or later release. IP Base w/ K9 image required.	Optional as an DC access switch
Catalyst 4500 Switch (Supervisor 6L-E or 6-E)	SXP, EAC	Cisco IOS® 12.2 (53) SG or later release. IP Base w/ K9 image required.	Optional as Campus access switch
Catalyst 3760(E) / 3750(E) Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE or later release. IP Base w/ K9 image required.	Optional as Campus access switch
Catalyst Blade Module 3x00 Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE or later release. IP Base w/ K9 image required.	Optional as DC access switch
Cisco EtherSwitch service module for ISR Routers	SXP, EAC	Cisco IOS® 12.2 (53) SE or later release. IP Base w/ K9 image required.	Optional as Branch access
Cisco Secure ACS	Centralized Policy Management for TrustSec / NDAC + EAC Authentication Server	ACS Version 5.1 with TrustSec license required. CSACS1120 appliance or ESX Server 3.5 or 4.0 is supported	Mandatory as main policy server

What is new in CTS now?

- **Launched March 17, Next Generation Fixed Switches: Catalyst 3750-X, 3560-X, 2960-S**

  802.1ae (MACSec) encryption on the 3750-X and 3560-X : only the user/down-link ports (links between the switch and endpoint devices such as a PC or IP phone) can be secured using MACsec

- Supervisor Engine 7-E on Catalyst 4500-E, 48G/slot

  Gigabit and 10 Gigabit line cards

  TrustSec with 802.1ae (MACSec) encryption and Security Group Tags

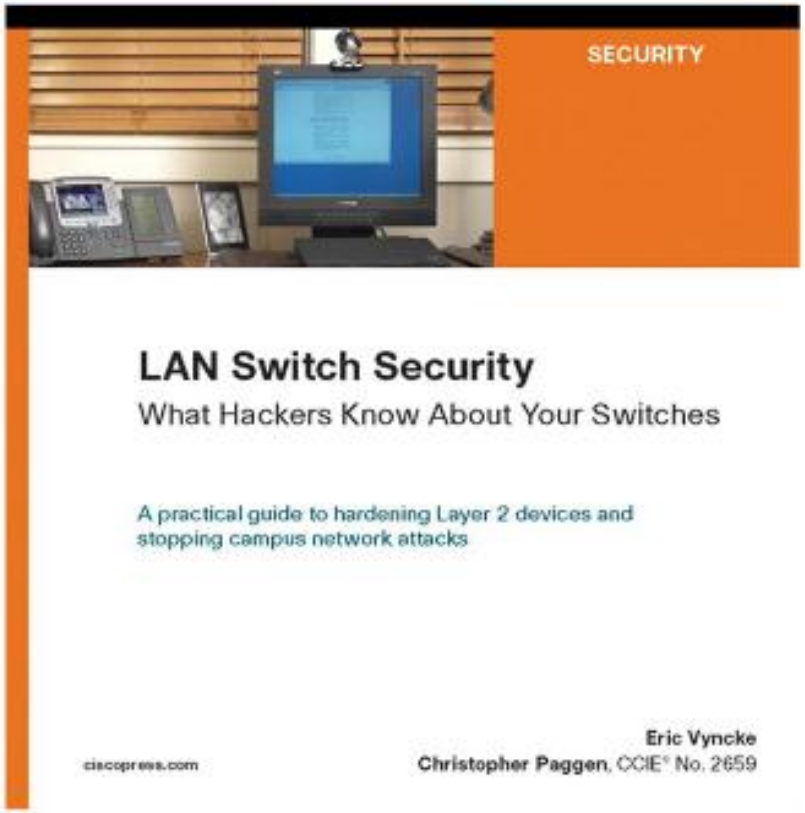
  hardware : ready, software: end of 2011

Summary

- TrustSec builds upon Identity services
- TrustSec provides a scalable Identity access control model
- TrustSec migration strategies allow customer to deploy with existing hardware
- TrustSec is deployable today

Recommended Reading

- Continue your Cisco Live learning experience with further reading from Cisco Press
- Check the Recommended Reading flyer for suggested books

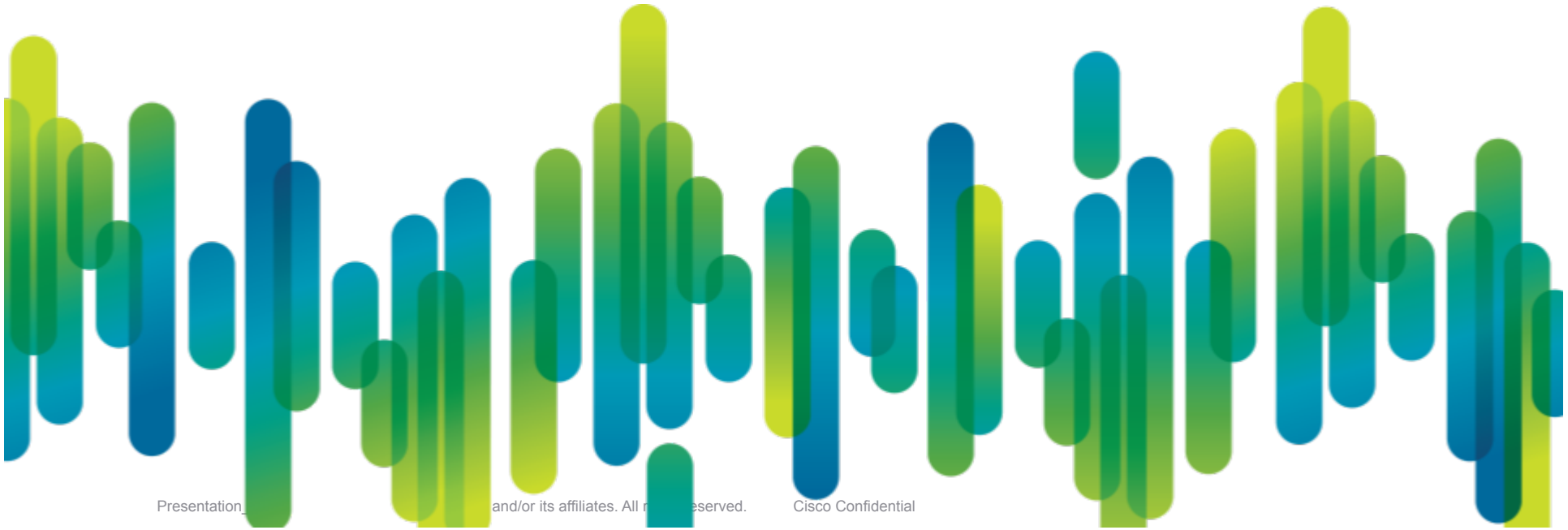


Recommended Reading

- Cisco Wireless LAN Security - http://www.ciscopress.com/bookstore/product.asp?isbn=1587051540
- Cisco Internetwork Troubleshooting - http://www.ciscopress.com/bookstore/product.asp?isbn=1578700922
- Cisco Secure Internet Security Solutions - http://www.ciscopress.com/bookstore/product.asp?isbn=1587050161
- Managing Cisco Network Security - http://www.ciscopress.com/bookstore/product.asp?isbn=1578701031
- Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design - http://www.ciscopress.com/bookstore/product.asp?isbn=1587052415
- Cisco LAN Switch Security: What Hackers Know About Your Switches - http://www.ciscopress.com/bookstore/product.asp?isbn=1587052563

Cisco live!

Registrujte se za Cisco Live Networkers u Londonu ili Bahreinu!
Više informacija na:
http://www.ciscolive.com/



Thank you.