Cisco TrustSec and Security Group Access

Presented by Fay-Ann Lee

Housekeeping

- Mobile phones - Please put on silent or vibrate mode
- Q&A – During Session Time Permitting and at End of Session
- Please Go Online and fill the evaluation form

Outline

- Introduction
  - Defining Network Access Management
  - Foundation Technology
- Security Group Access Overview
  - Source Group Tag (SGT)/ Source Group ACL (SGACL) Concepts
  - Network Device Access Control (NDAC) Concept
  - 802.1AE/SAP Concept
- SGT Use Cases
  - SGT with Identity Deployment Modes
  - SGT in the Data Center/VDI
- Monitoring and Troubleshooting

Introduction

Key Trustsec Functions

Policy-based access control for

- Users
- Endpoint devices
- Networking infrastructure

Identity-aware networking

- Identity information for granular controls
- Role-based business service delivery

Data integrity and confidentiality

- Securing data path in the switching environment
- IEEE 802.1AE standard encryption

Rule-Based Policies

Identity Information

Employee

Contractor

Guest

Device Types

+

Other Conditions

Time and Date

Posture

Location

Access Type

→

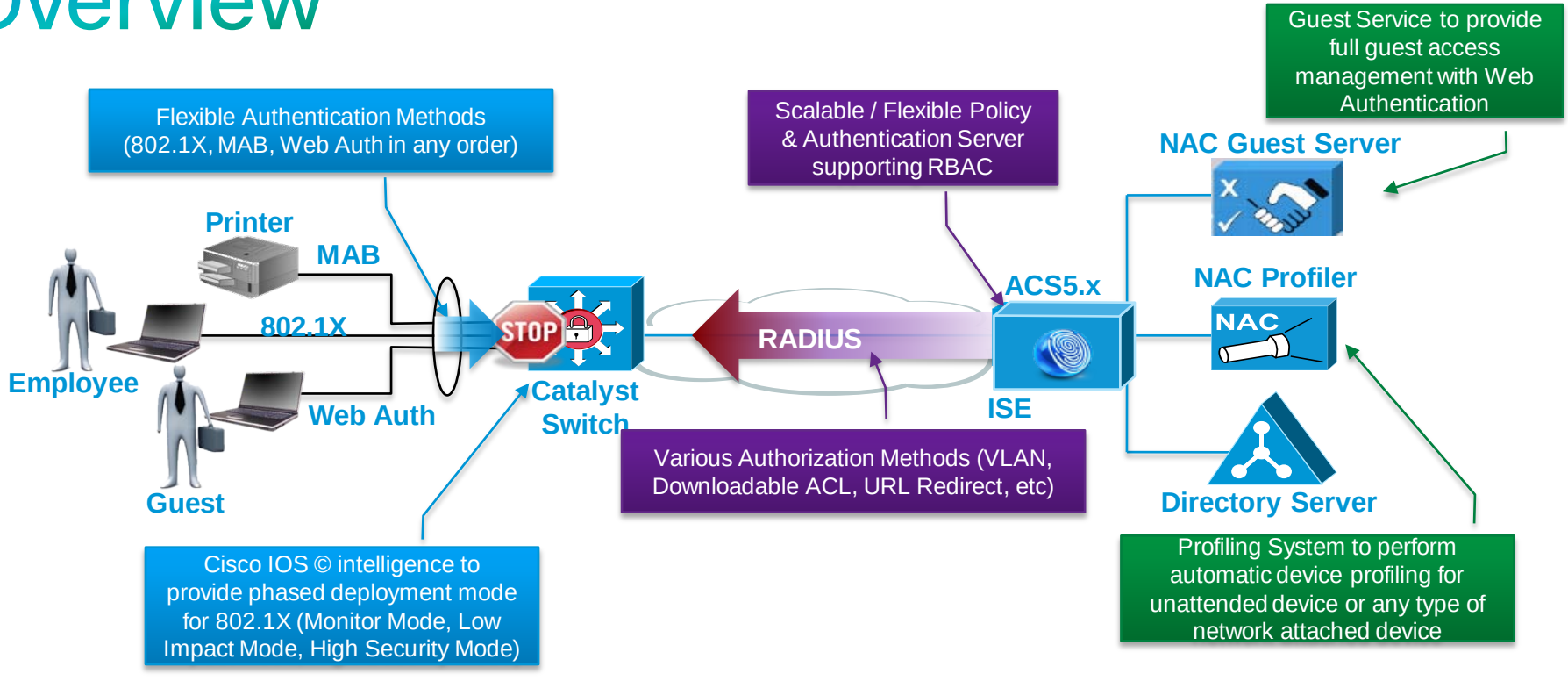
Authorization Profiles

- Broad Access
- Limited Access
- Guest/Internet
- Quarantine
- Deny Access

↓

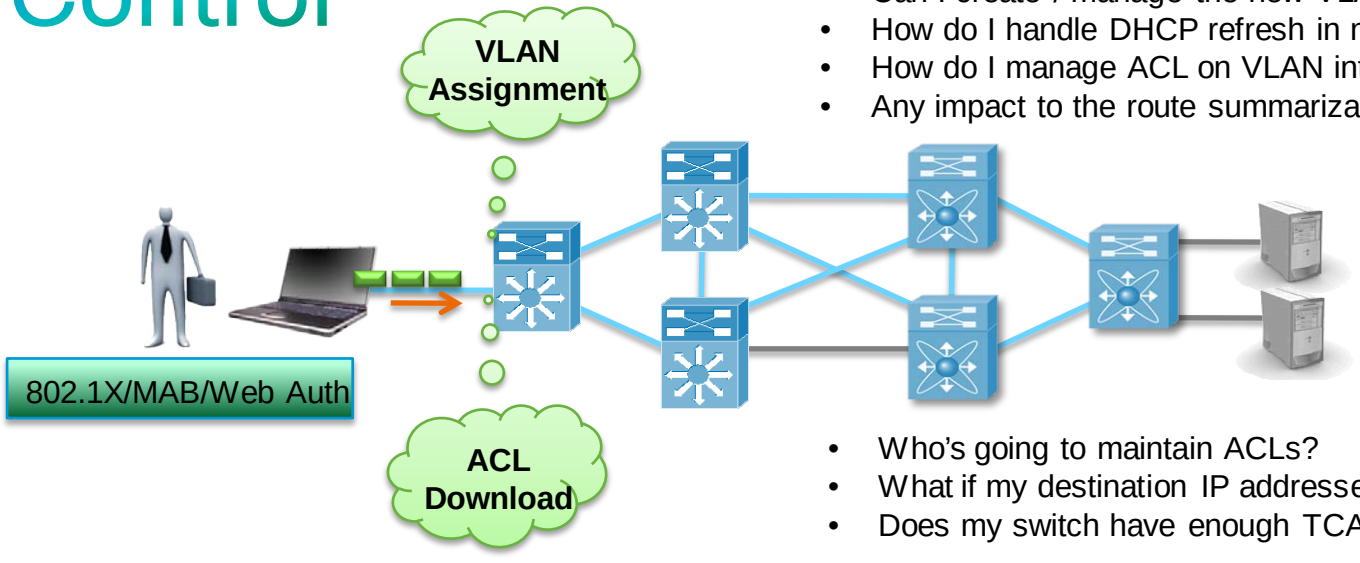
Track for Accounting

Cisco Identity Solution Overview



Challenges with Ingress Access Control

- Can I create / manage the new VLANs or IP Address scope?
- How do I handle DHCP refresh in new subnet?
- How do I manage ACL on VLAN interface?
- 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

Security Group Access Solution Overview

Security Group Access (SGA)

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

SGA 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

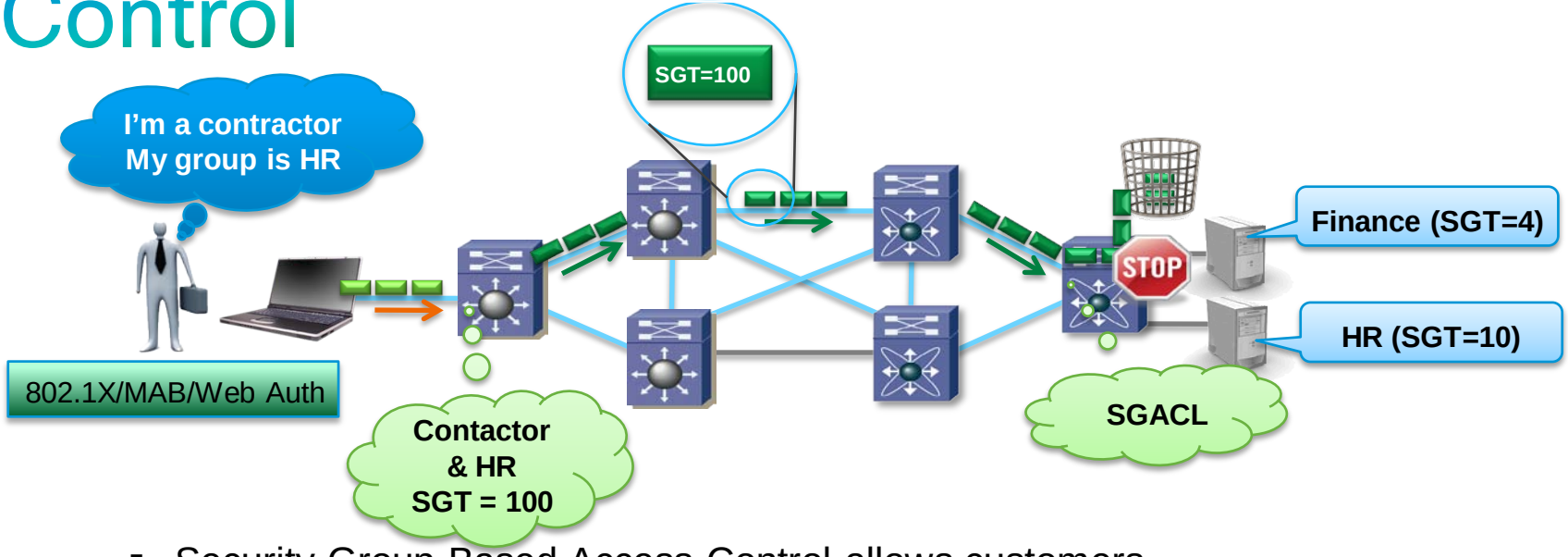
Authenticated Networking Environment

- 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), will migrate to standard based key management 802.1X-2010/MKA

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

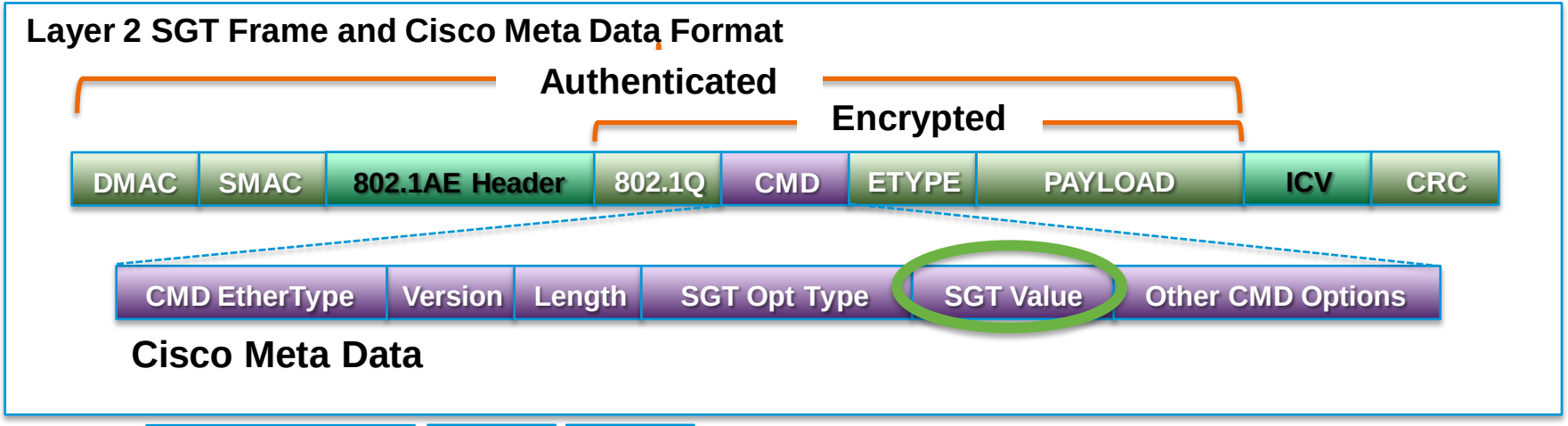
Security Group Based Access Control

- **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 (ISE)** or configured locally on TrustSec device

Customer Benefits

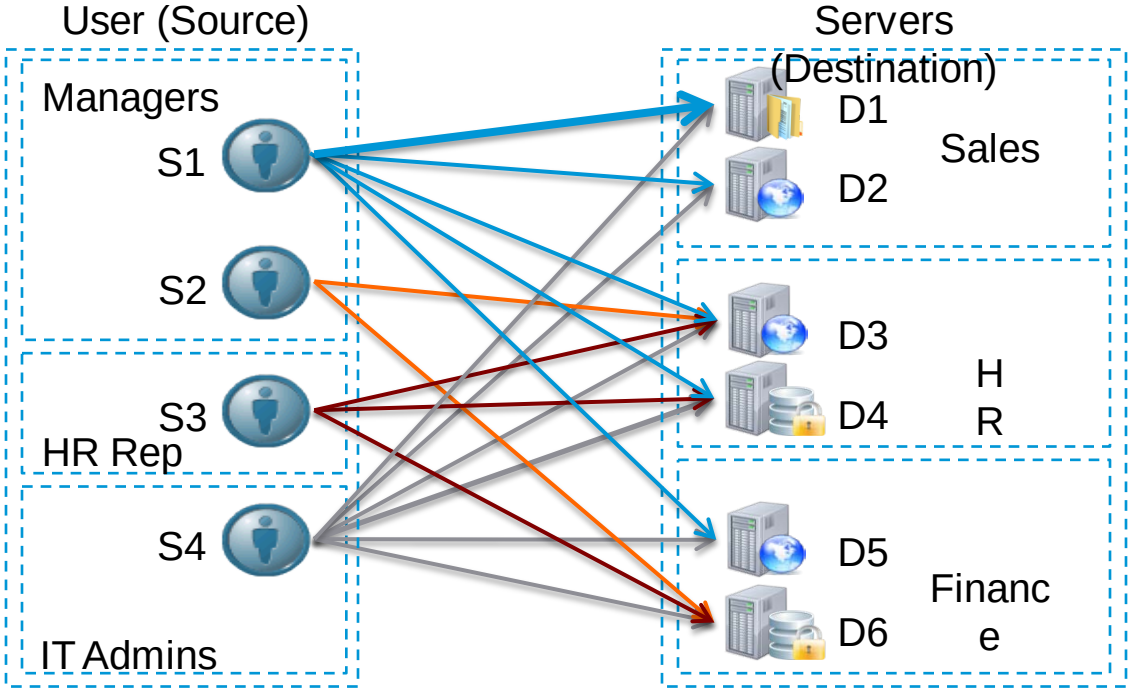
- Provides **topology independent** policy
- Flexible and scalable policy based on user role
- **Centralized Policy Management** for Dynamic policy provisioning
- Egress filtering **results to reduce TCAM impact**

SGT Frame Format



- 802.1AE Header | CMD | ICV are the L2 802.1AE + TrustSec overhead
- Frame is always tagged at ingress port of TrustSec capable device
- Tagging process prior to other L2 service such as QoS
- SGT namespace is managed on central policy server (ISE)
- No impact IP MTU/Fragmentation

Traditional Access Control



S1 to D1 Access Control

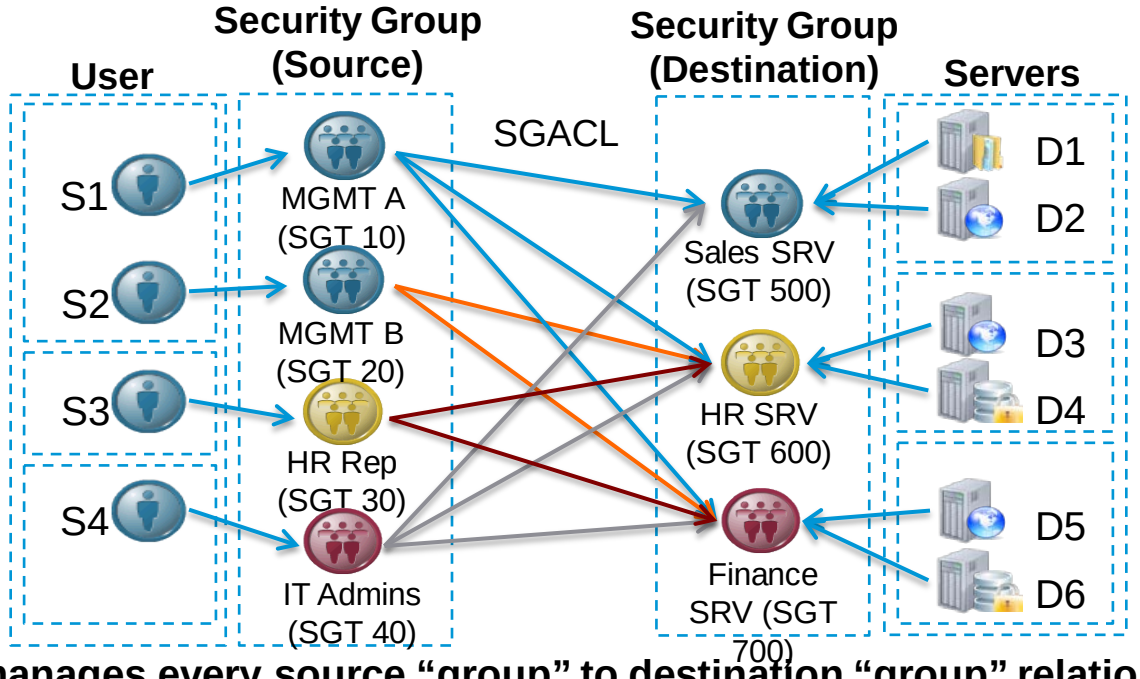
```
permit tcp S1 D1 eq https
permit tcp S1 D1 eq 8081
permit tcp S1 D1 eq 445
deny   ip   S1 D1
```

Access Control Entry -

ACE # grows as # of permission statement increases

- **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**
- ***Network Admin manages every IP source to IP destination relationship explicitly***

How SGACLs Simplifies Access Control



- **Network Admin manages every source “group” to destination “group” relationship**
- **This abstracts the network topology from the policy and reducing the number of policy rules necessary for the admin to maintain**
- **The network automates the alignment of users/servers to groups**

Role to SGT Binding and SGACL

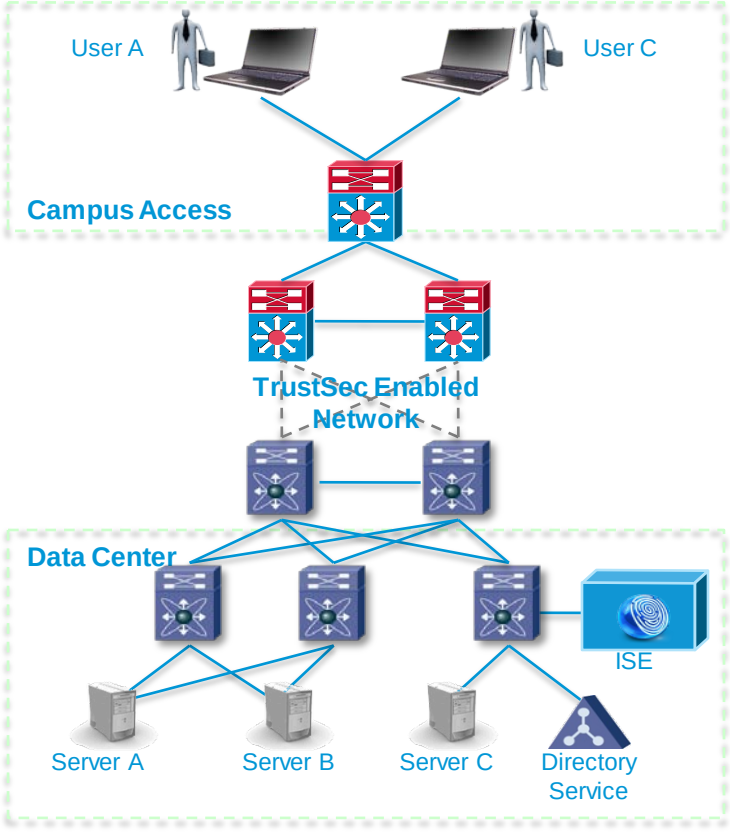
Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLS
Contractor (10/A)	Server A (111/6F)	Permit All
Contractor (10/A)	Server B (222/DE)	Deny All
Contractor (10/A)	Server C (333/14D)	Deny All
HR (30/1E)	Server A (111/6F)	Deny All
HR (30/1E)	Server B (222/DE)	SGACL-D
HR (30/1E)	Server C (333/14D)	Permit All

SGACL Details

SGACL-D
remark destination SQL permit permit tcp dst eq 1433 remark source SQL permit permit tcp src eq 1433 Remark http permit permit tcp dst eq 80 Remark https permit permit tcp dst eq 443 deny all

- No IP defined
- Downloaded from ISE
- Enforcement at Egress

SGACL Flow Step 1: Policy Population



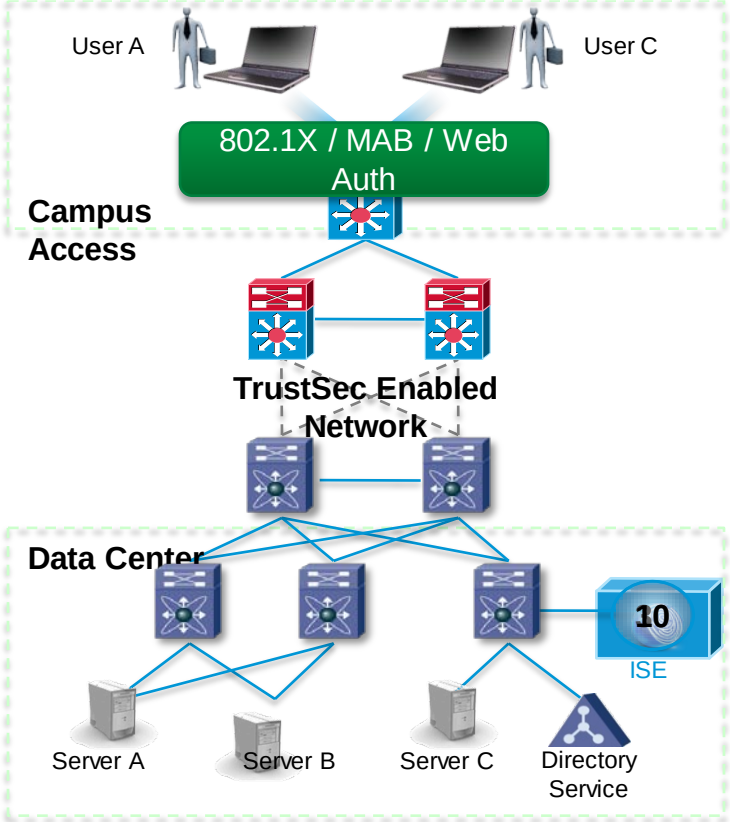
Step 1 **SGT Policy definition on ISE**

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

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 2: SGT Assignment



Step 2

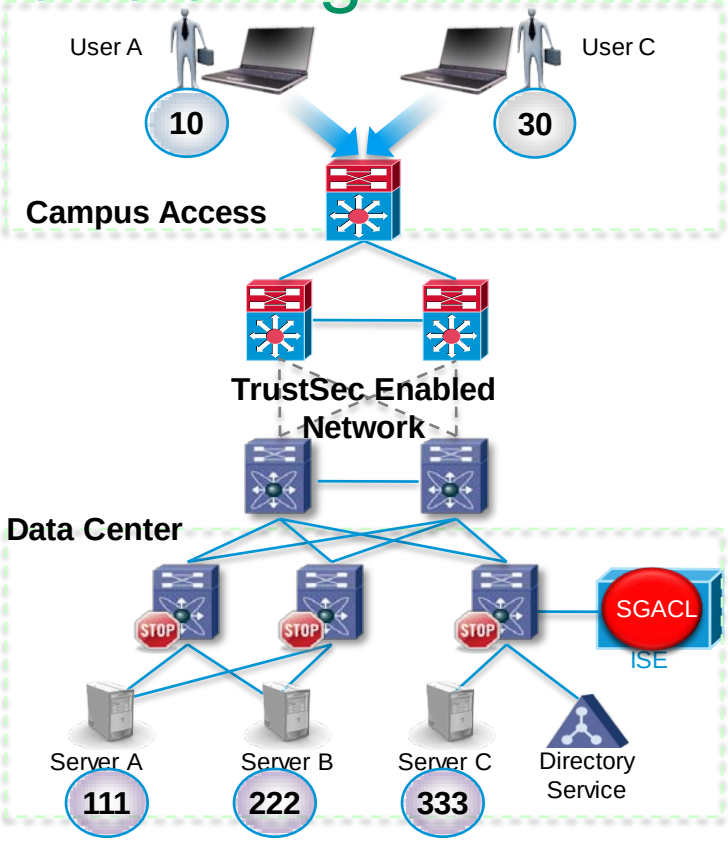
SGTs are assigned to role and bound to IP address

- 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
- Server IP address are bound to SGT statically on access switch or dynamically looked on ISE 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 **ISE provisions Egress Policy to TrustSec capable Device**

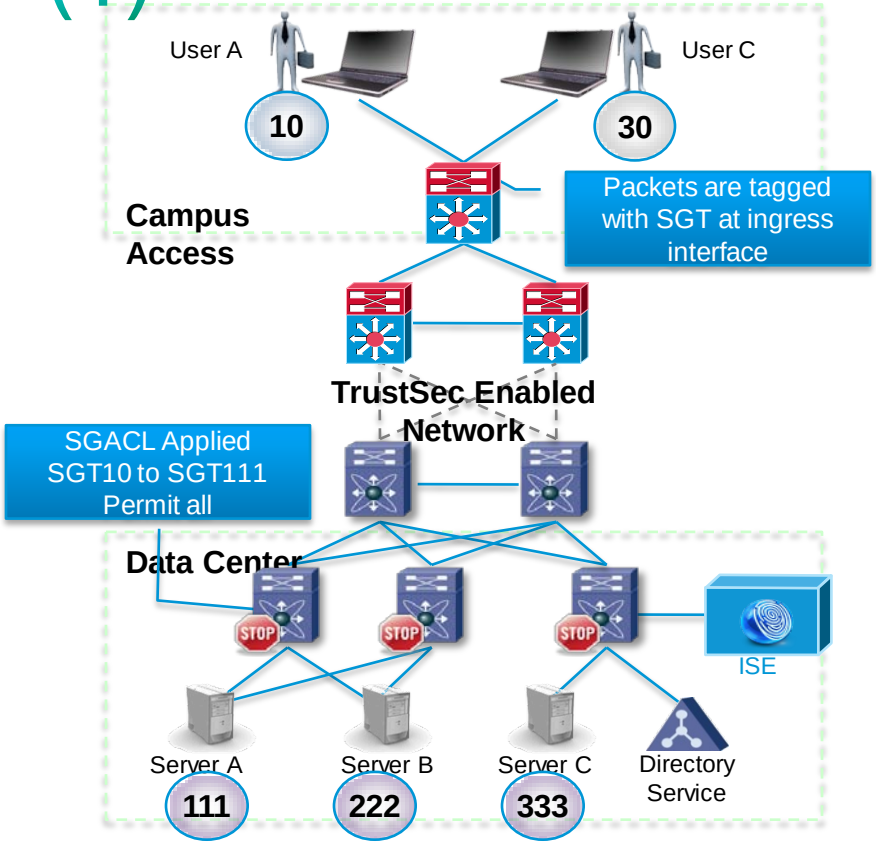
- Each Trustsec capable device downloads policy from ISE

Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
Contractor (10/A)	Server A (111/6F)	Permit All
Contractor (10/A)	Server B (222/DE)	Deny All
Contractor (10/A)	Server C (333/14D)	Deny All
HR (30/1E)	Server A (111/6F)	Deny All
HR (30/1E)	Server B (222/DE)	SGACL-D
HR (30/1E)	Server C (333/14D)	

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)



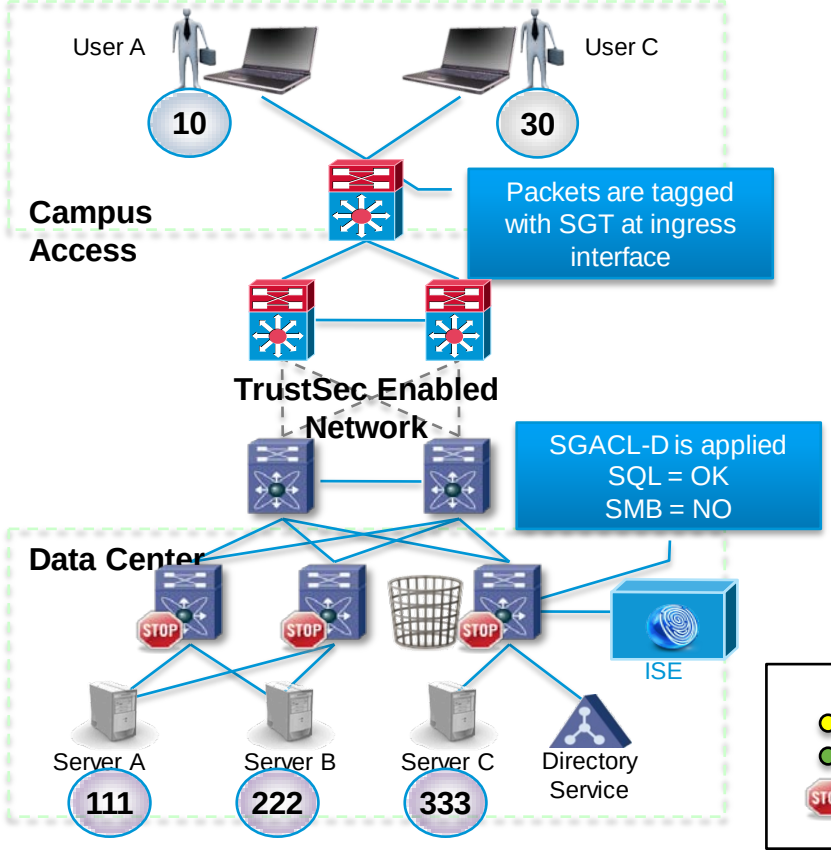
Step 4 **Policy enforcement begins**

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

Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
Contractor (10/A)	Server A (111/6F)	Permit All
Contractor (10/A)	Server B (222/DE)	Deny All
Contractor (10/A)	Server C (333/14D)	Deny All
HR (30/1E)	Server A (111/6F)	Deny All
HR (30/1E)	Server B (222/DE)	SGACL-D
HR (30/1E)	Server C (333/14D)	Permit All

- Untagged Traffic
- CMD Tagged Traffic

SGACL Flow: Final Step



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

Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
Contractor (10/A)	Server A (111/6F)	Permit All
Contractor (10/A)	Server B (222/DE)	Deny All
Contractor (10/A)	Server C (333/14D)	Deny All
HR (30/1E)	Server A (111/6F)	Deny All
HR (30/1E)	Server B (222/DE)	SGACL-D
HR (30/1E)	Server C (333/14D)	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
```

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
- SGT from distrusted device is tagged as “Unknown”, a special SGT (value is zero)
- A process of authenticating network device is called “Network Device Admission Control” or NDAC in short

Network Device Admission Control

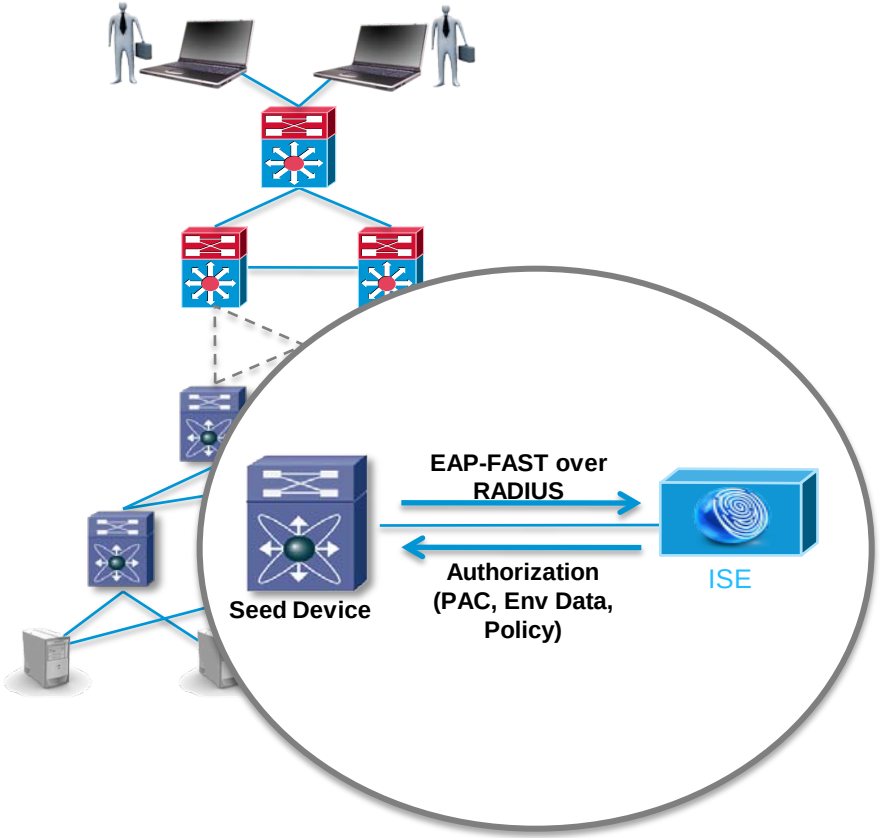
- Network Device Admission Control (NDAC) provides strong **mutual authentication (EAP-FAST) to form trusted domain**
- Only SGT from **trusted peer is honored**
- Authentication leads to **Security Association Protocol (SAP)** to negotiate keys and cipher suite for encryption automatically (mechanism defined in 802.11i)
- 802.1X-2010/MKA will replace SAP for switch to switch encryption in the future
- Trusted device acquires trust and policies from ISE 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**

TrustSec Domain Establishment

Seed Device Authentication

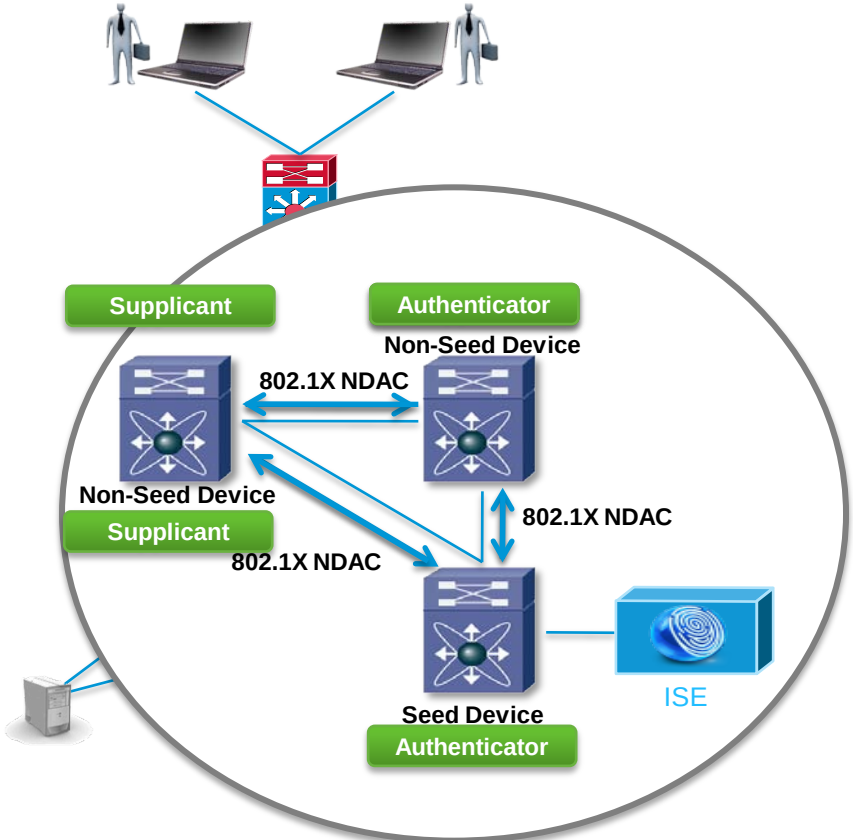


NDAC validates peer identity before peer becomes the circle of Trust!

- The first device to authenticate is called the Seed Device
- Seed Device becomes authenticator to is peer supplicant
- Role determination process selects both Authenticator and Suppicant roles
- NDAC utilizes EAP-FAST/MSCHAPv2
- Credential (including PAC) is stored in hardware key store

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 ISE directly, the device is called Non-Seed Device
- First peer to gain ISE connectivity wins authenticator role
- Lower MAC address is the tie breaker

NDAC Success Example


```
CTS7K-CORE# show cts interface ethernet 1/15
CTS Information for Interface Ethernet1/15:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        CTS7K-DC
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_SUP
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
SAP Status:                 CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:18bad853520000 an:2
      Current transmit SPI: sci:18bad853460000 an:2
```

```
CTS7K-DC# show cts interface ethernet 1/3
CTS Information for Interface Ethernet1/3:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        CTS7K-CORE
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_AUTH
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
SAP Status:                 CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:18bad853460000 an:2
      Current transmit SPI: sci:18bad853520000 an:2
```

Data Confidentiality and Integrity

- Trustsec provides layer 2 hop-by-hop encryption and integrity, based on IEEE 802.1AE standard
- 128bit AES-GCM- NIST Approved*
- Line rate encryption/decryption for both 10 GbE/1GbE interface
- Replay protection of each and every frame
- 802.1AE encryption to protect CMD field (SGT value)

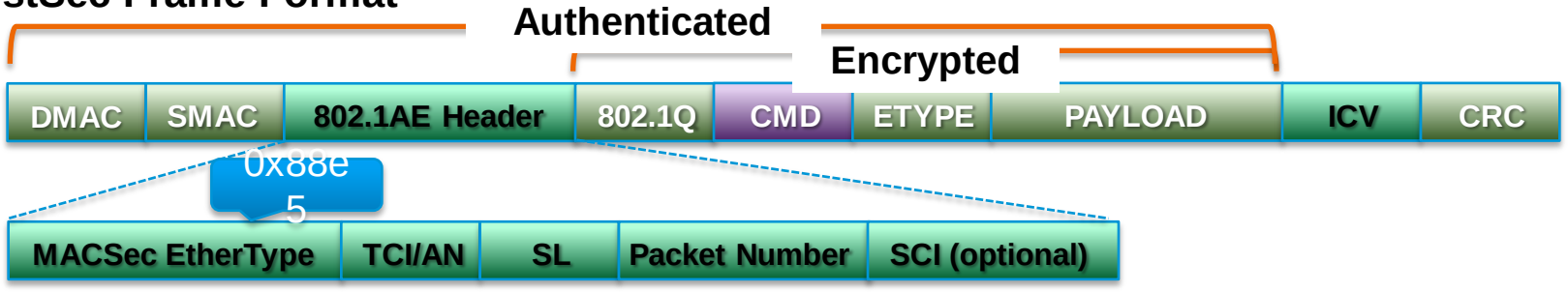
Customer Benefits

- Protects against man-in-the-middle attacks (snooping, tampering, replay)
- Standards based frame format and algorithm (AES-GCM)
- 802.1X-2010/MKA addition supports per-device security associations in shared media environments (e.g. PC vs. IP Phone) to provide secured communication
- Network service amenable 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

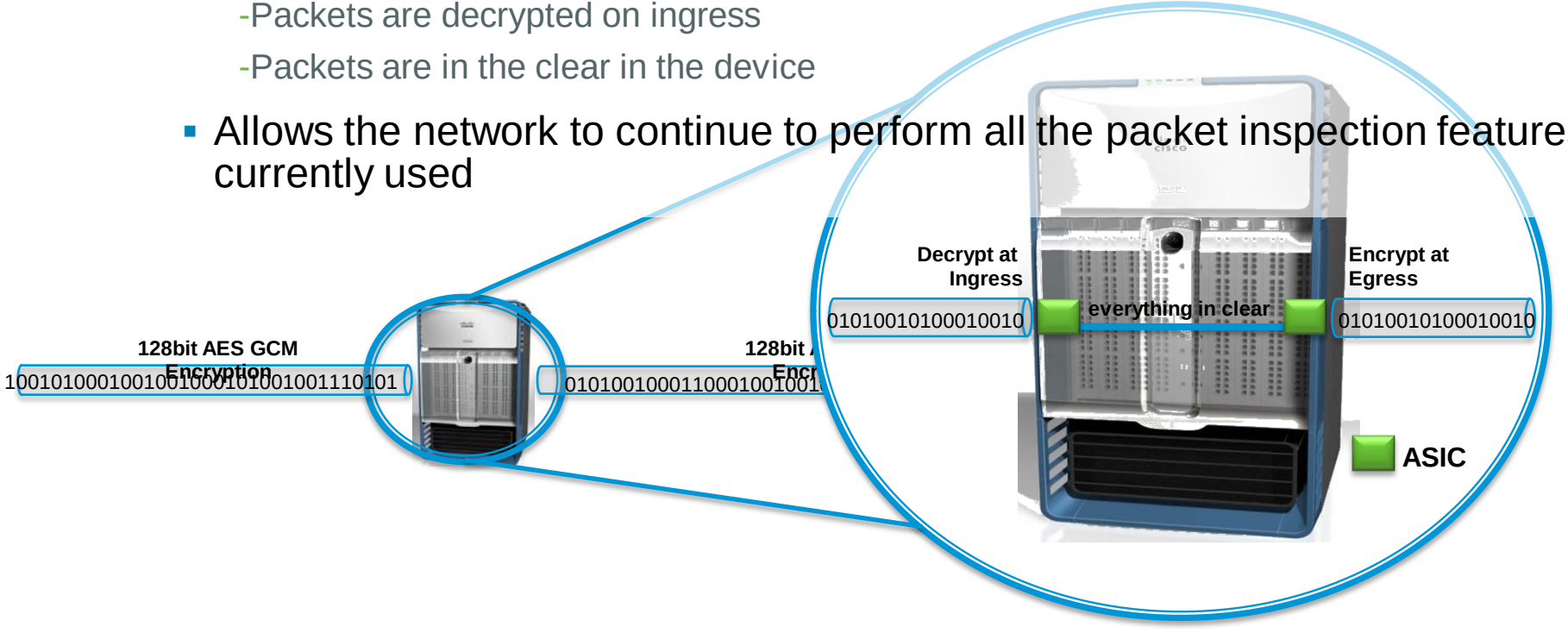


MACSec Tag Format

```
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 perform all the packet inspection features currently used



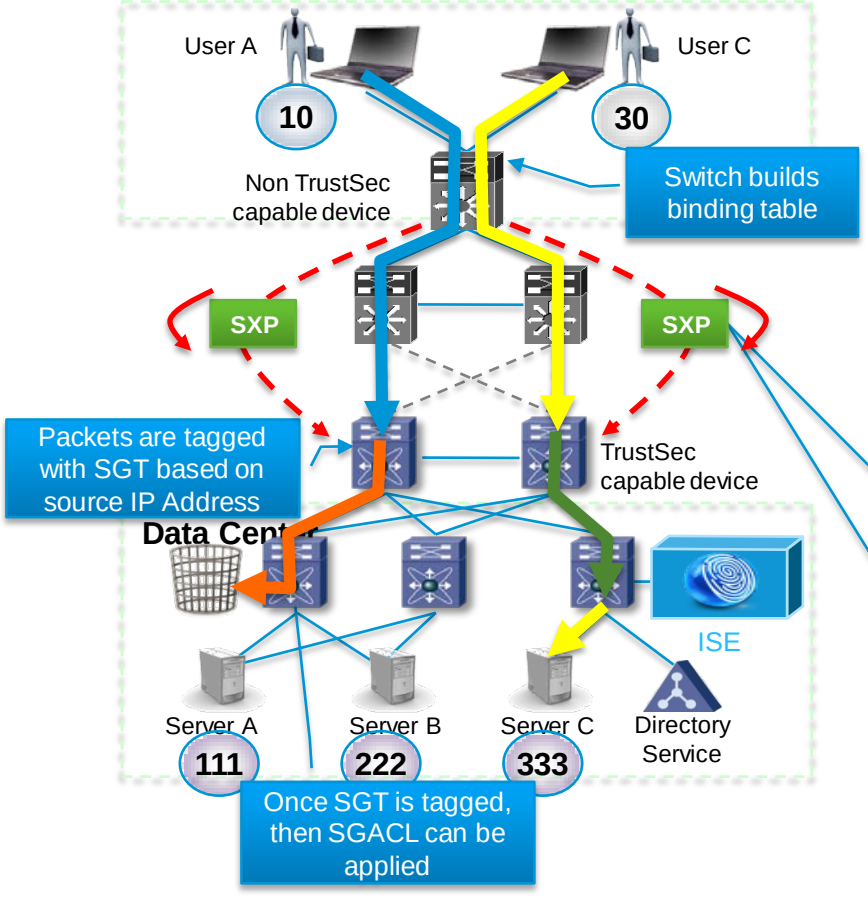
Common Deployment Questions

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

SXP Support for Non-SGT capable platforms

- SGT native tagging requires hardware (ASIC) support
- Non-TrustSec hardware capable devices can still receive SGT attributes from ISE 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 Nexus 7000 switch platform support SXP
- SXP accelerates deployment of SGACL by without extensive hardware upgrade for TrustSec

How SXP Exchanges the IP to SGT Binding



SXP enables communication between Non-TrustSec and TrustSec-capable devices

- SGT assigned to user
- Switch binds endpoint IP to SGT
- Switch uses SXP to send binding table to TrustSec capable device
- TrustSec capable device tags packet based on source IP 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

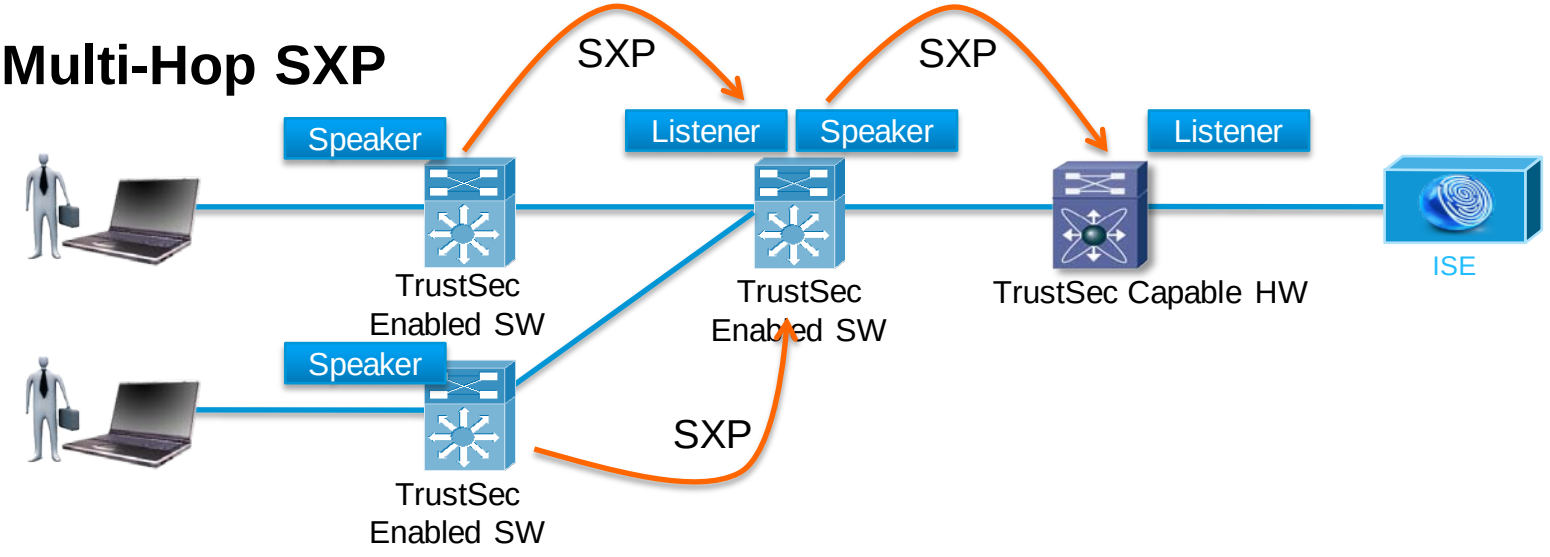
User C

- Untagged Traffic
- CMD Tagged Traffic

SXP Connection Types

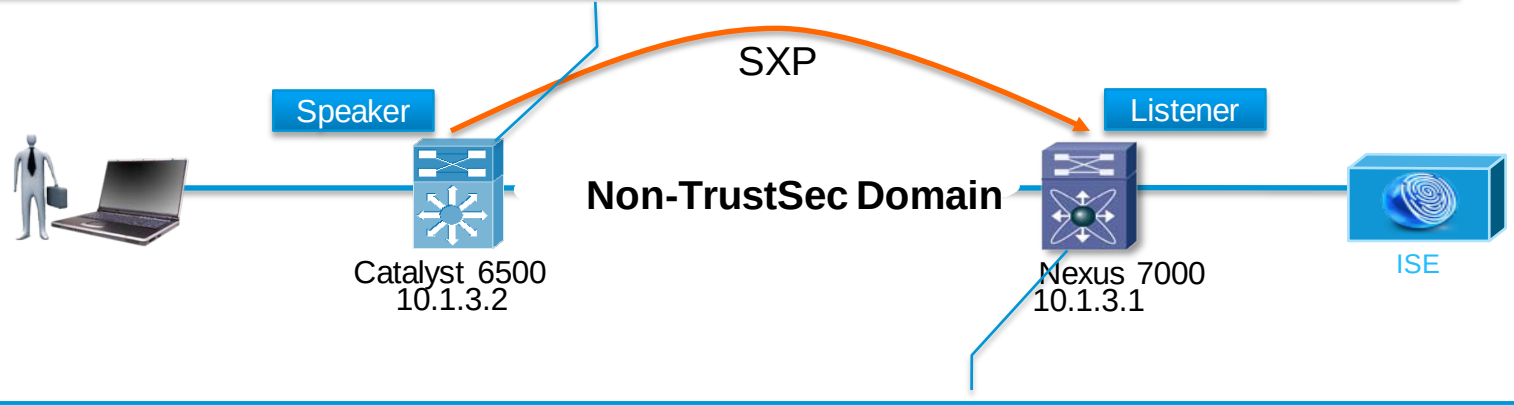
Single-Hop SXP

Multi-Hop SXP



SXP Configuration

```
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 10.1.2.3 source 10.1.2.1 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)

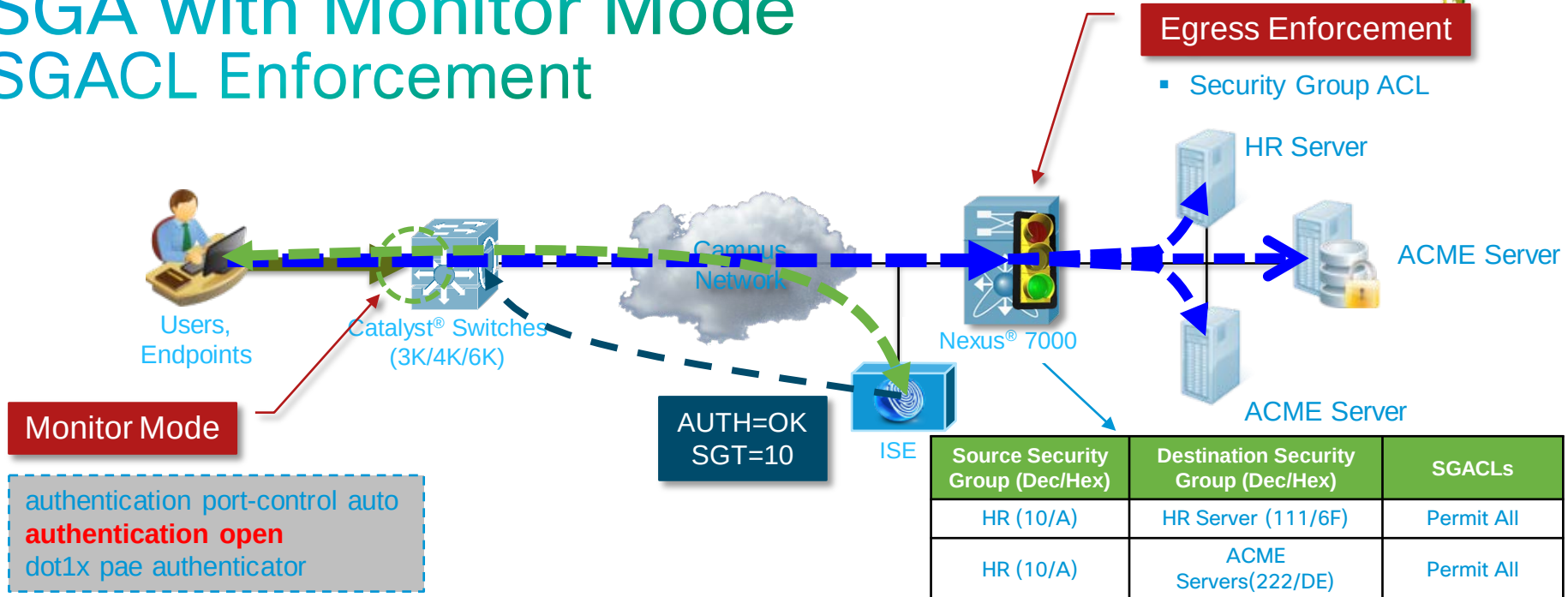
CTS7K-DC# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120

Applying SGA to Identity Deployment Modes

SGA and Monitor Mode Interoperability

- Open Mode and Multi-Auth at the access layer with Monitor and Reporting
- Assign SGTs to a session with permit any any for all flows
- Default for “unknown” SGTs is permit any any
- Does not have an impact on access layer functions (PXE, WoL, etc.)

SGA with Monitor Mode
SGACL Enforcement



Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
HR (10/A)	HR Server (111/6F)	Permit All
HR (10/A)	ACME Servers(222/DE)	Permit All
Employee (8/8)	HR Server (111/6F)	Deny All

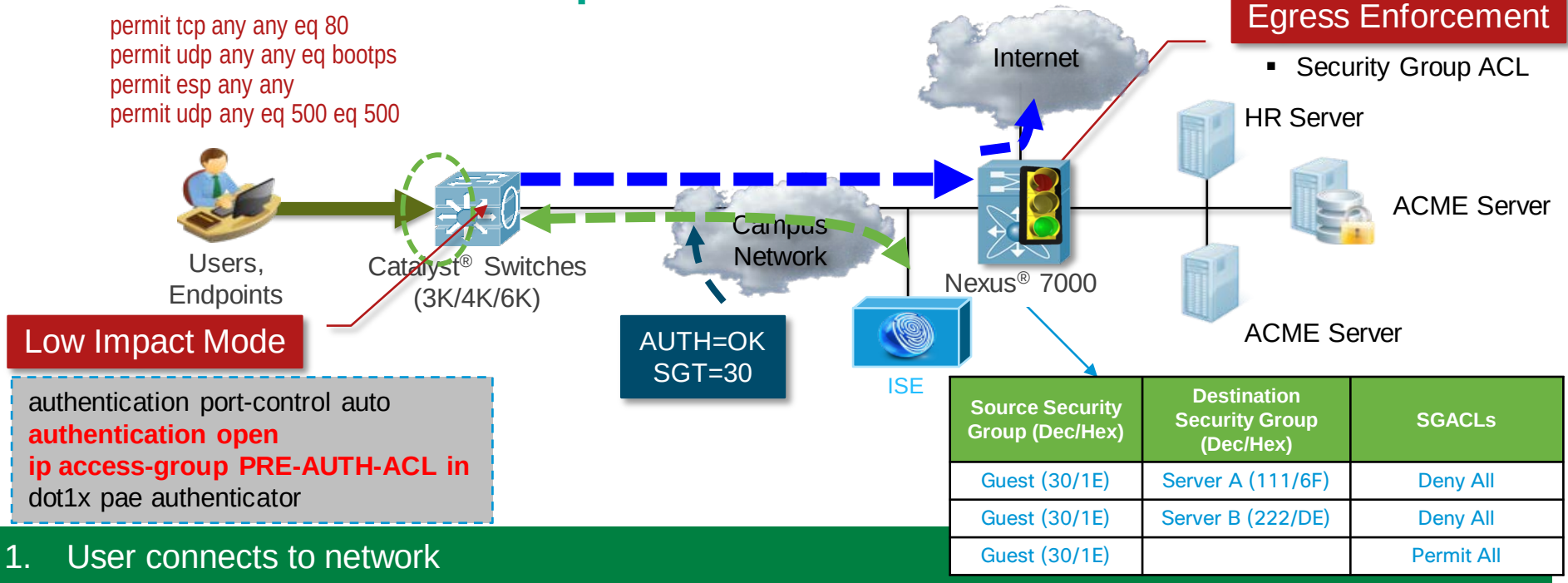
1. User connects to network
2. Monitor mode allows traffic from endpoint before authentication
3. Authentication is performed and results are logged by ISE
4. Traffic traverse to Data Centre and hits SGACL at egress enforcement point
5. Only permitted traffic path (source SGT to destination SGT) is allowed

SGA and Low Impact Mode Interoperability

- Eases dACL challenges by reducing the number of ACEs downloaded to ingress port
- Egress access control with SGT differentiates service among Employee group based on role

Difference between Monitor and Low Impact Mode is to enable very basic enforcement at ingress interface while keeping openness for easy deployment

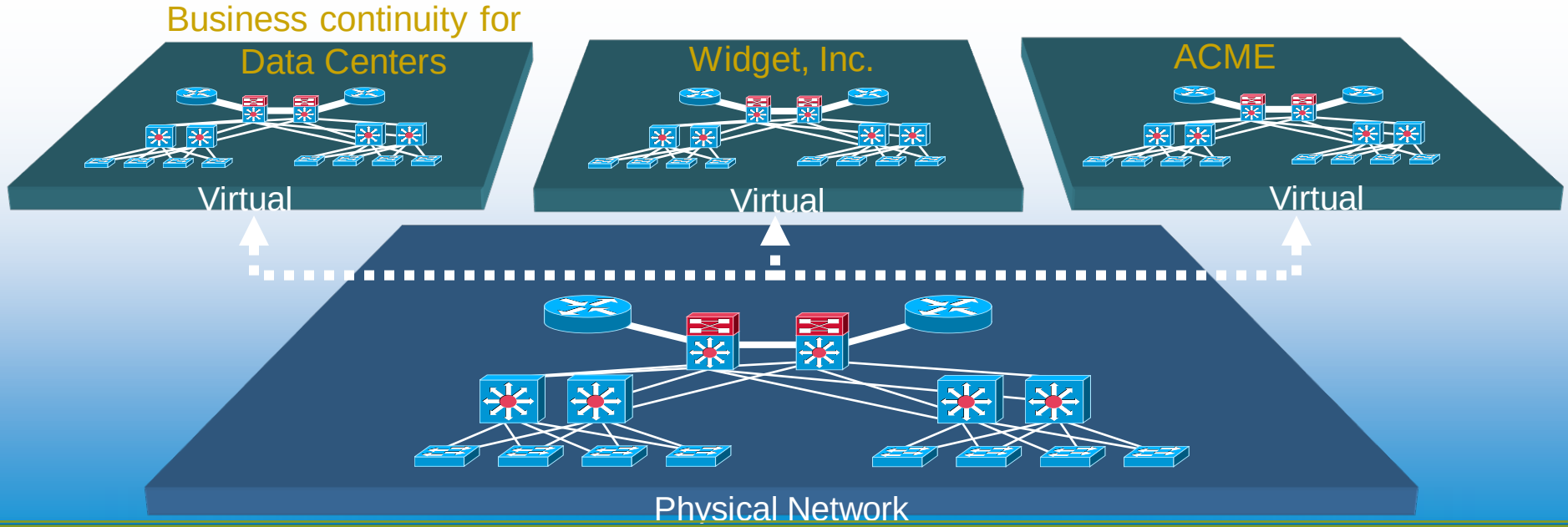
SGA and Low Impact Mode



Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
Guest (30/1E)	Server A (111/6F)	Deny All
Guest (30/1E)	Server B (222/DE)	Deny All
Guest (30/1E)		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 Center and hits SGACL at egress enforcement point
5. Only permitted traffic path (source SGT to destination SGT) is allowed

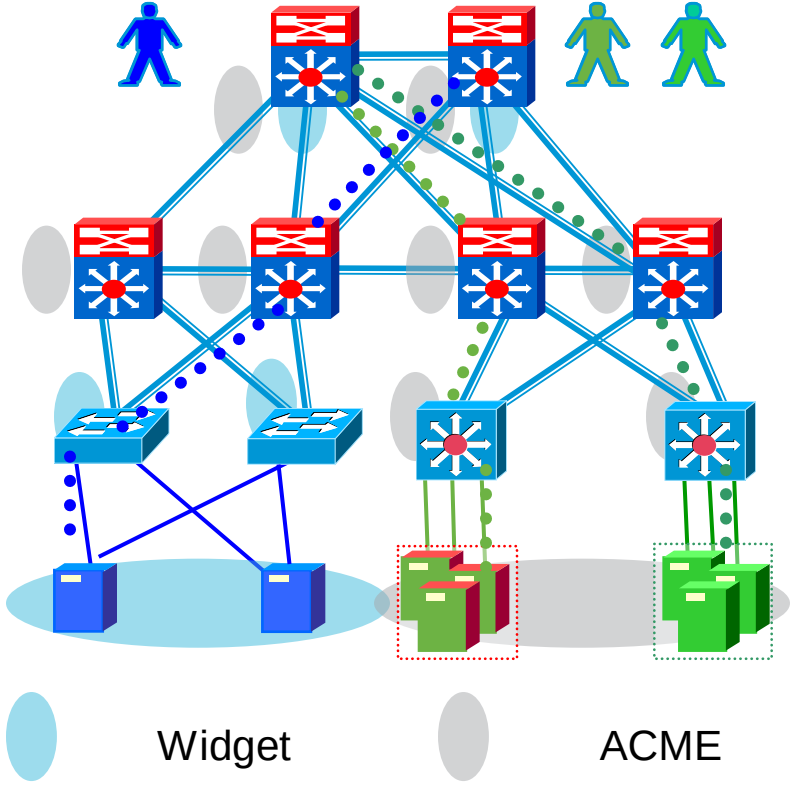
Network Virtualization with SGA



- Definition: 1 to Many. One network supports many virtual networks
- ACME High-level Technical Requirements
  - Separate Widget and ACME networks until regulatory agencies approve acquisition in multiple countries
  - Dynamic VLAN assignment allows Widget/ACME employees to be placed in the correct network

Network Virtualization with SGA

- Fine-tuning of network policy yields greater scalability
  - –Virtual Network used for coarse-grained virtualization of ACME vs. Widget networks
  - –SGA enhances policy control by providing fine-grained virtualization of user/groups within the existing virtual domains
  - –Servers are separated by color
  - –Traffic will gravitate towards correct server across integrated core
- One SGA namespace per network
- SGTs must be unique per virtual network
  - –"ACME employee" = SGT 10 while "Widget employee" = SGT 20



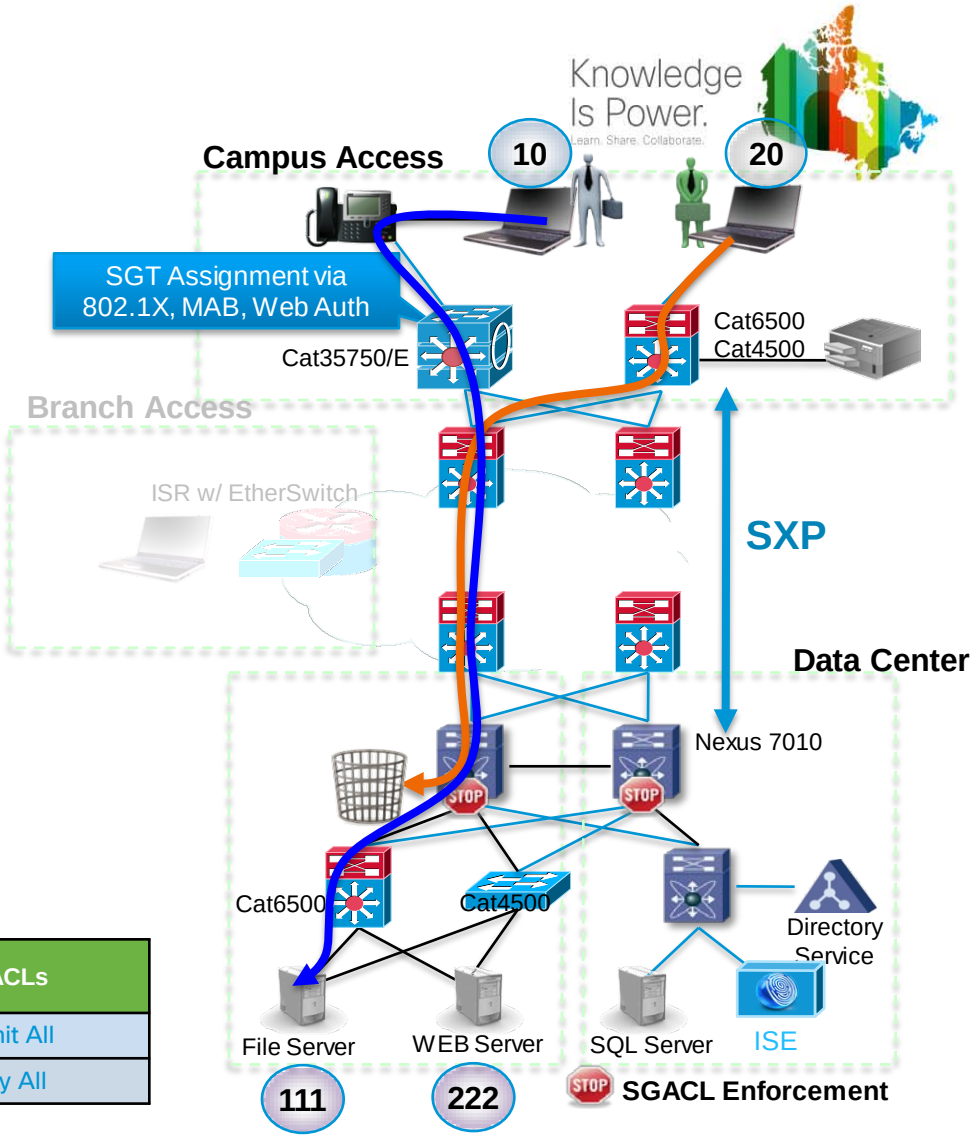
SGA Use Cases

Campus LAN Deployment

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

Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
Contractor (10/A)	Server A (111/6F)	Permit All
HR (30/1E)	Server A (111/6F)	Deny All

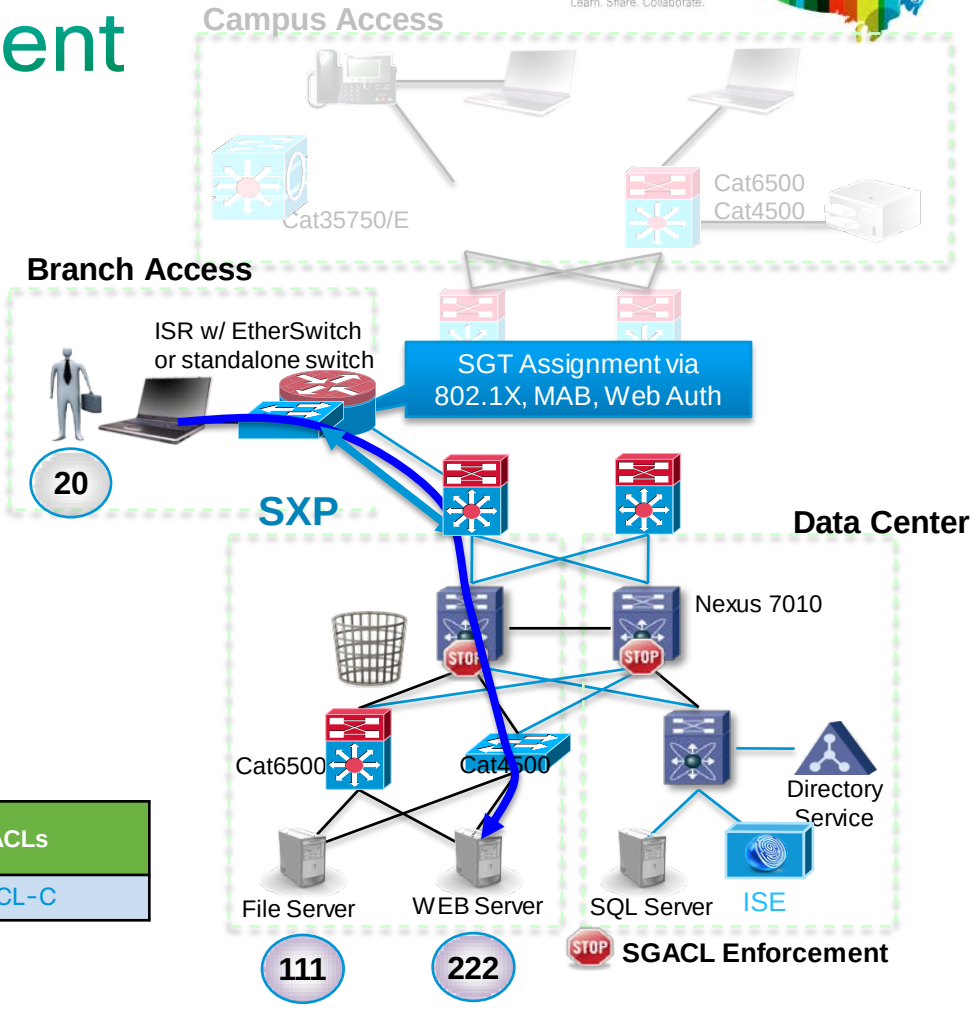


Branch LAN Deployment

TrustSec to cover Branch office LAN as well as Data Center network

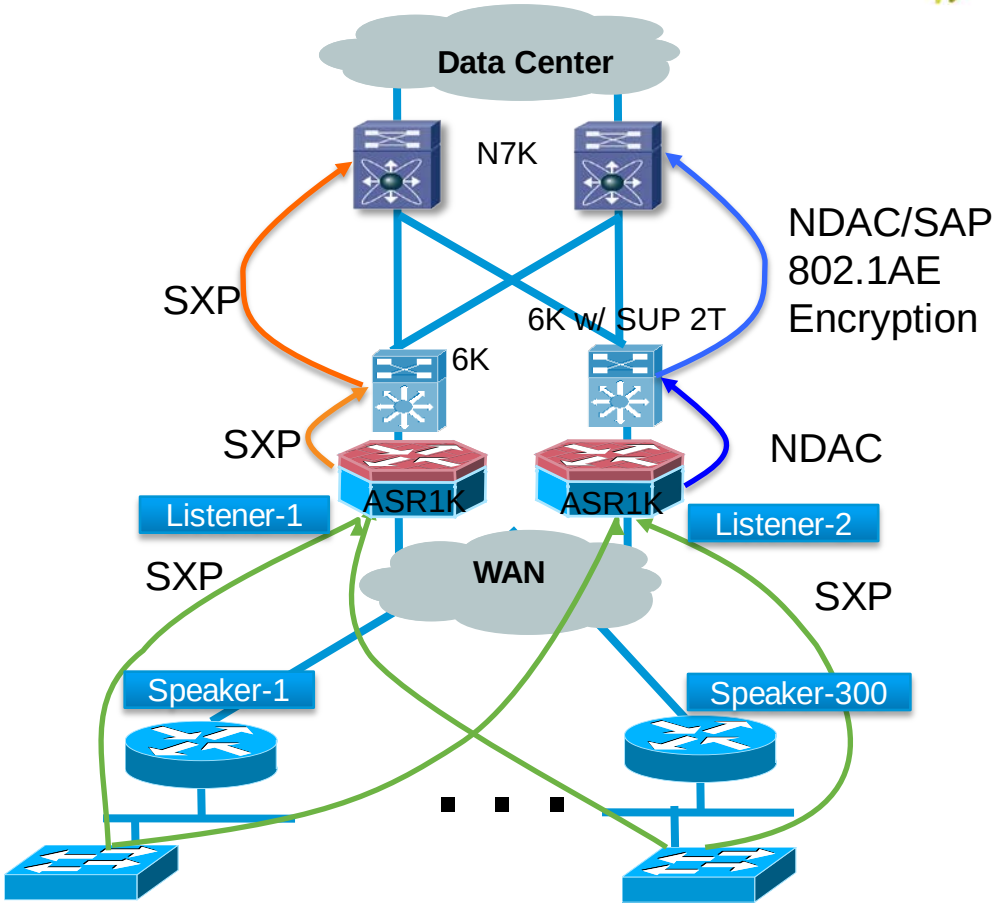
- Support for Branch access
- Source SGT assigned via 802.1X, MAB, or Web Authentication
- Server SGT assigned via IPM or statically
- IP-to-SGT binding table is exchanged between branch LAN access switch and Data Center TrustSec capable device

Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
User B (20/14)	Server B(222/DE)	SGACL-C



WAN Deployment

- ASR1K– avail. July
- 6K w/ SUP 2T –avail. July



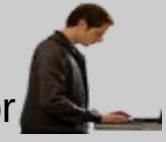
Note: For illustration purposes only

Location Based Access with SGA

More Flexible Policy with Role-Based Access Control

Identity Information

Identity:
Network Administrator



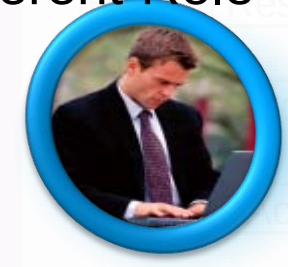
Identity:
Full-Time Employee

Identity:
Guest

Rossi Barks
Employee
HR

Everyone Has a Different Role

Employee



Francois Didier
Employee
Consultant

Vicky Sanchez
Employee
Marketing

Policy for Today's Business Requirement

Identity Information

Identity:
Network Administrator

Identity:
Full-Time Employee

Identity:
Guest

+

Other Conditions

Time and Date

Location

Access Type

Access Privilege

- Consultant
- Human Resources
- Finance
- Marketing
- Guest
- Deny Access

Role+Rule Based Access Control

Example 1: Human Resources Role

Identity Information

Identity:
Network Administrator

Identity:
Full-Time **Employee**

Identity:
Guest

+

Other Conditions

Time and Date

Location:Off Site

Access Type:
Wired

Access Privilege

- Engineering
- **Human Resources**
- Finance
- Home Access
- Guest
- Deny Access

Role+Rule Based Access Control

Example 2: Human Resources Role

Identity Information

Identity:
Network Administrator

Identity:
Full-Time **Employee**

Identity:
Guest

+

Other Conditions

Time and Date

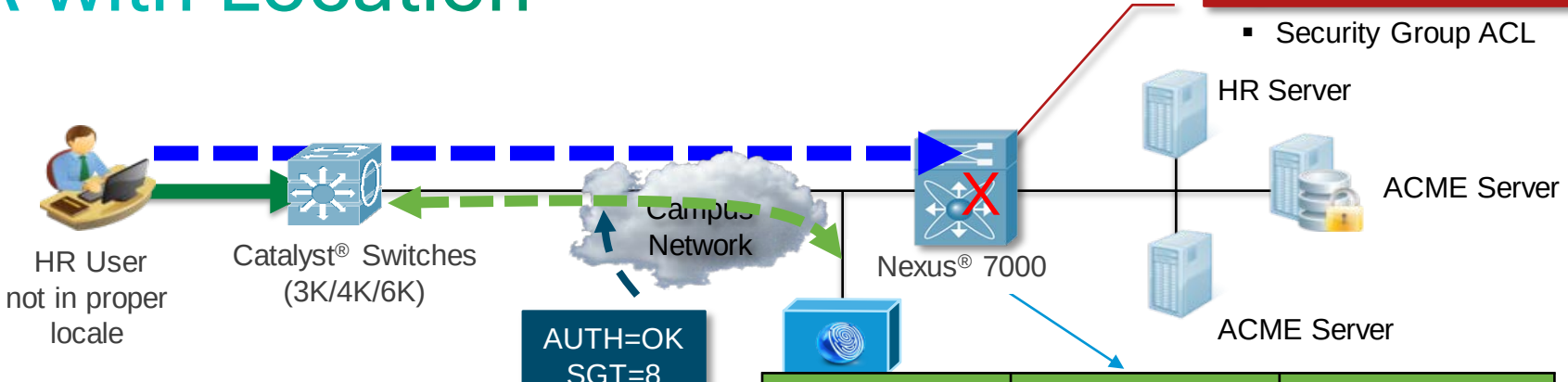
Location:Airport

Access Type:
VPN

Access Privilege

- Engineering
- Human Resources
- Finance
- Home Access
- Guest
- Deny Access

SGA with Location



Source Security Group (Dec/Hex)	Destination Security Group (Dec/Hex)	SGACLs
HR User (10/A)	HR Server (111/6F)	Permit All
HR User (10/A)	ACME Server (222/DE)	Permit All
HR Off Site (8/8)	HR Server (111/6F)	Deny All
HR Off Site (8/8)	ACME Server (222/DE)	Permit

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

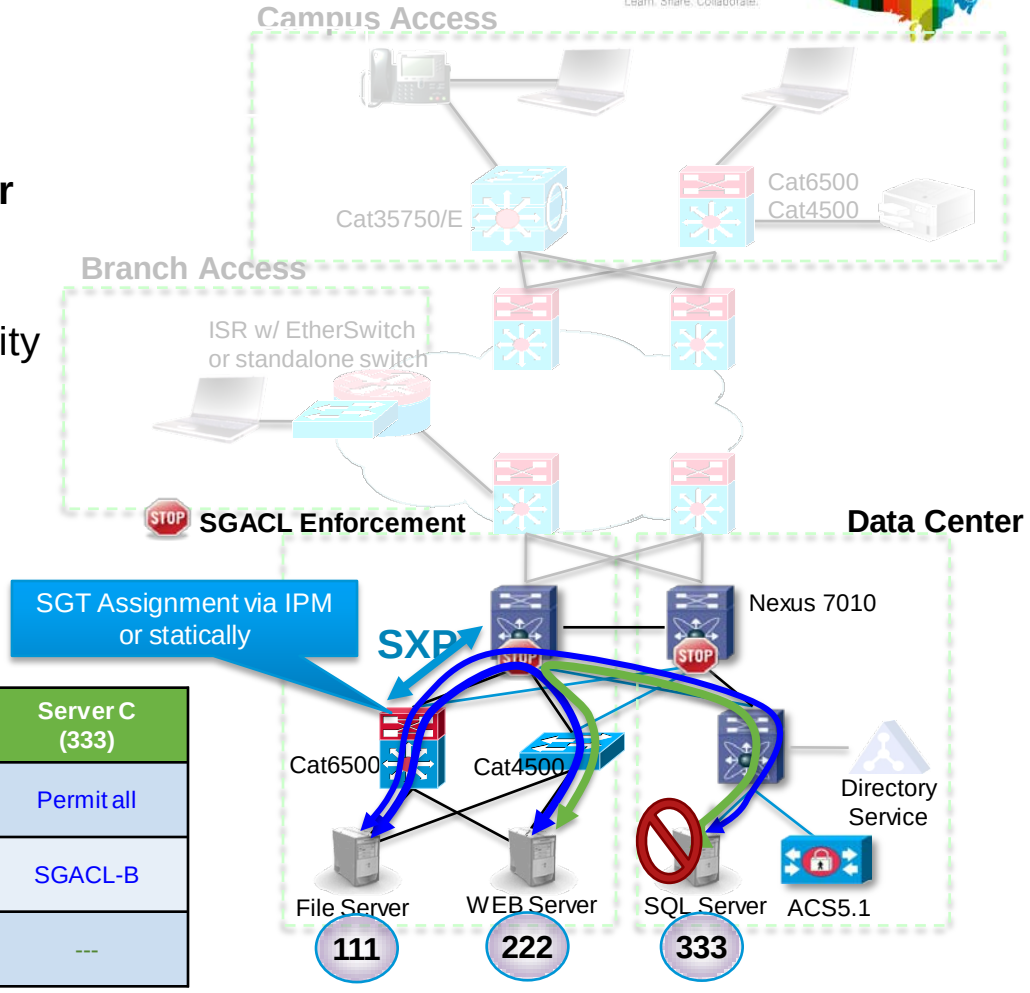
SGT in the Data Center

Intra Data Center Deployment

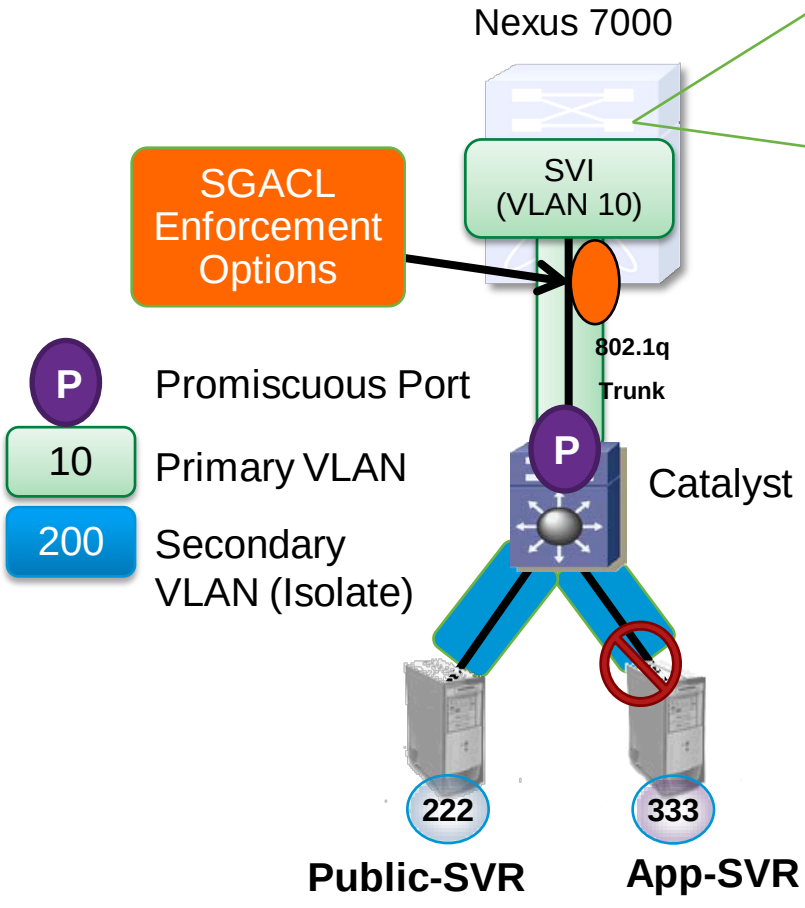
TrustSec to cover Intra Data Center for server traffic segmentation

- Manual server IP address to SGT binding on Nexus 7000 or IPM (Identity Port Mapping to ISE 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	---



Intra Data Center Deployment Detail



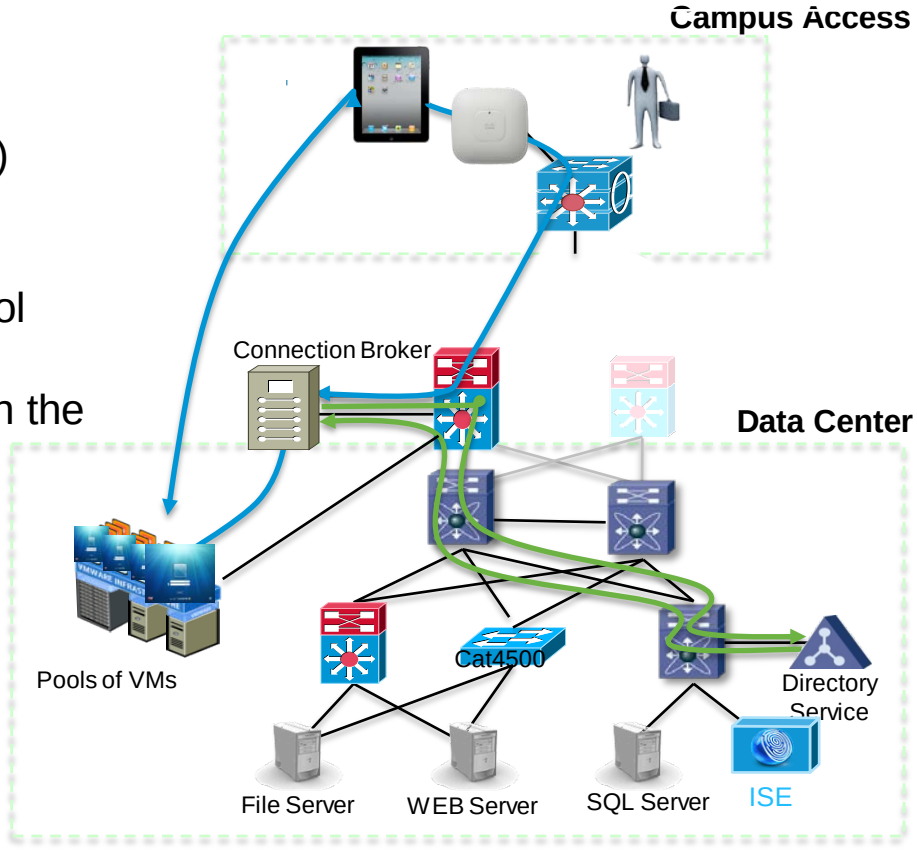
SGT/DGT	App-SVR (222)	Public-SVR (333)
App-SVR (222)	Permit	Deny
Public-SVR (333)	Deny	Permit

- Dynamic policy enforcement between servers within same isolated VLAN (Private VLAN)
- Dynamic policy enforcement between servers in different community VLANs

Virtual Desktop Infrastructure (VDI) with SGT

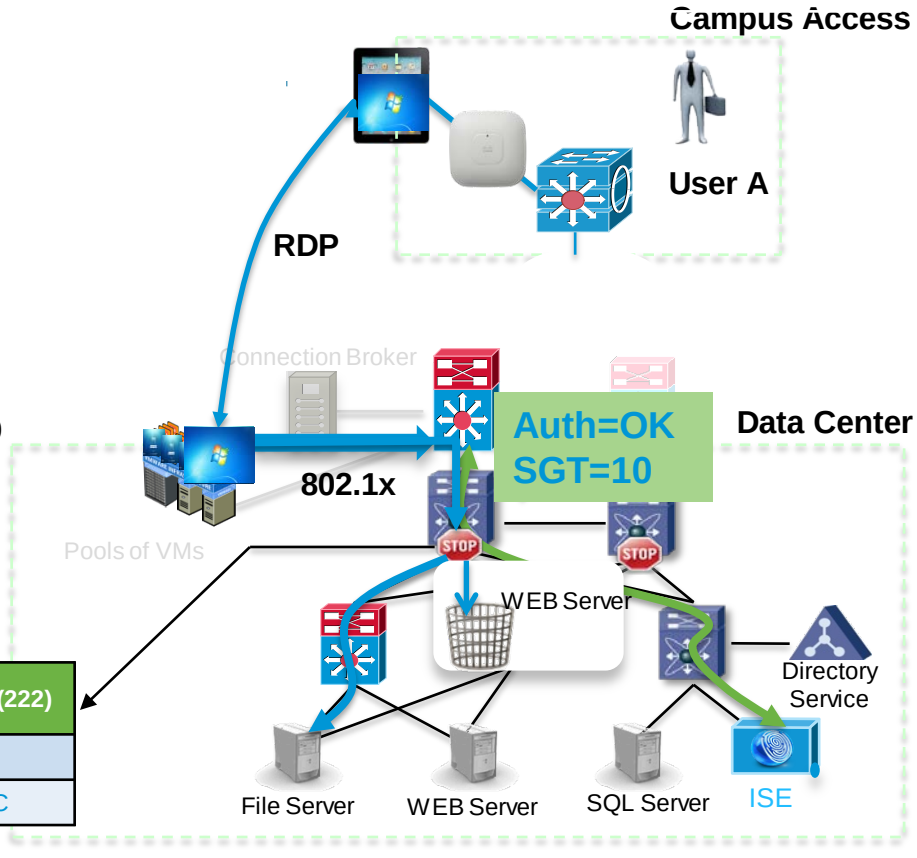
Background: Connection Brokers

- User logs into the thin client (no user authentication performed for this example)
- User initiates a connection to Connection Broker via RDP, PCoIP protocols
- Broker queries Active Directory for VM pool assignment
- Broker redirects user to an available VM in the VM pool
- User is now able to the remotely view and control the VM



Applying 802.1x and SGA to VDI

- User logs into VM which triggers 802.1x authentication
- Authentication succeeds. Authorization assigns the SGT for the user.
- Traffic hits the egress enforcement point
- Only permitted traffic path (source SGT to destination SGT) is allowed



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

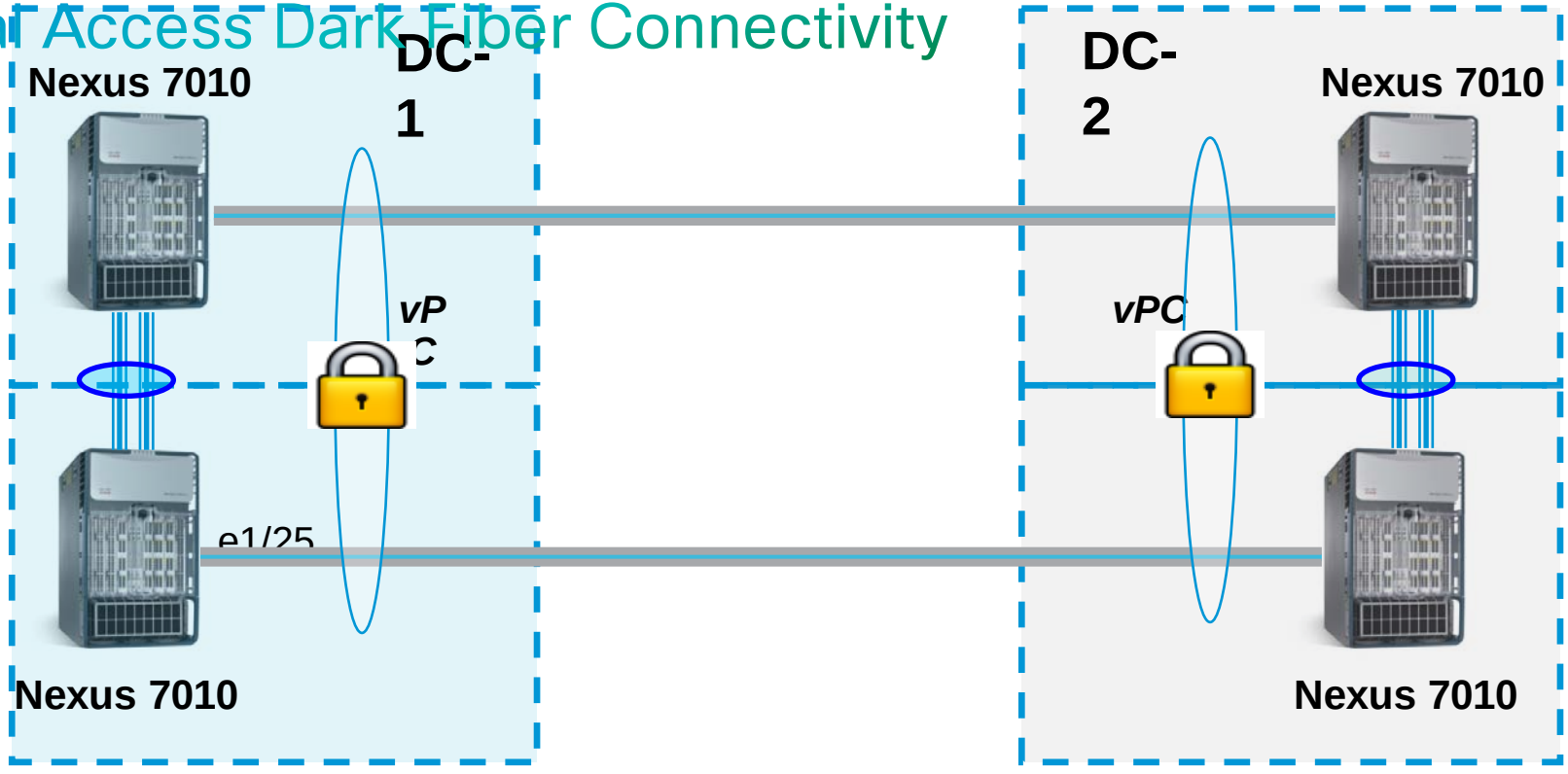
Secure Data Center Interconnect

TrustSec for Secure DataCenter Interconnect

Single Access Dark Fiber Connectivity

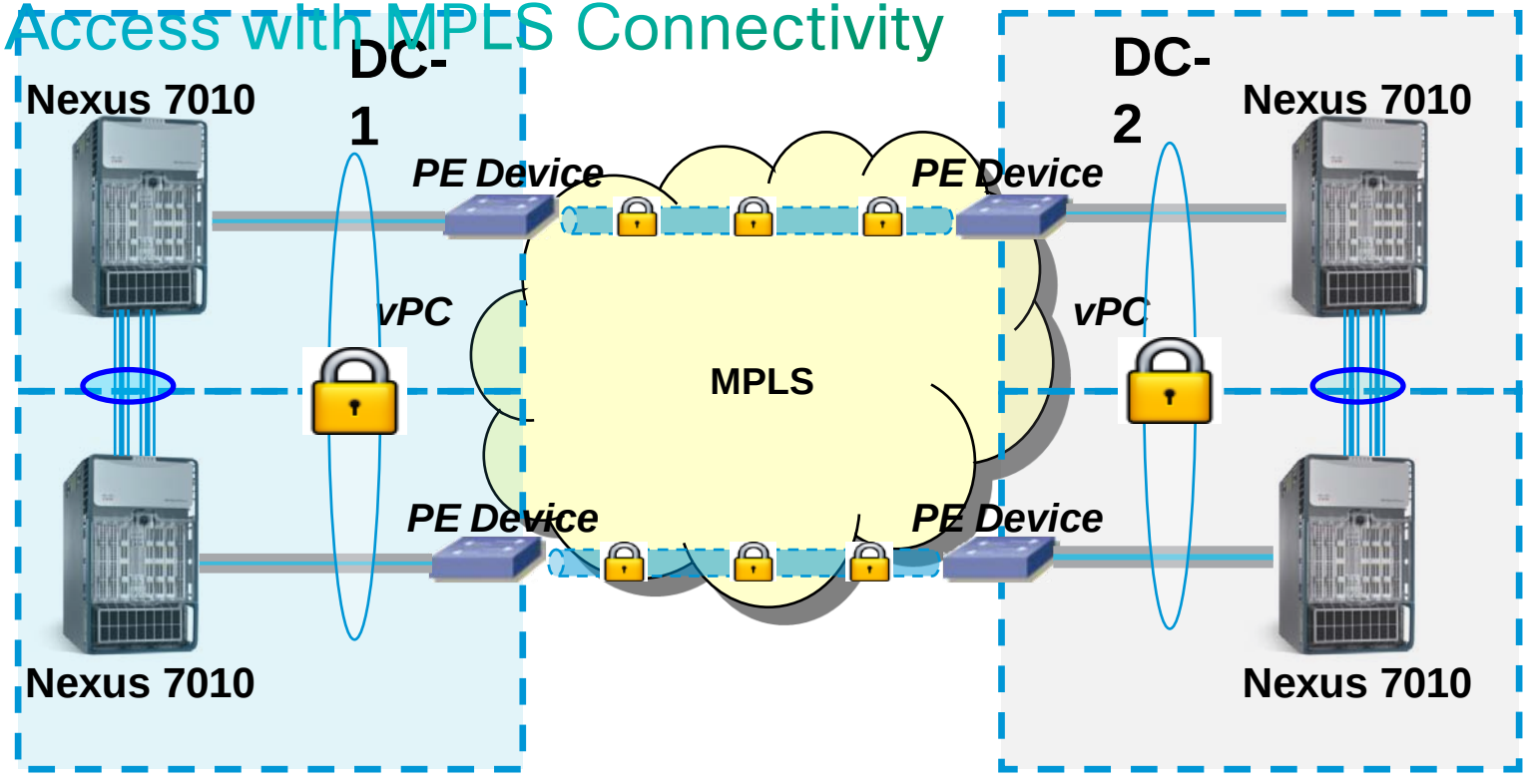
Trustsec for Secure DataCenter Interconnect

Dual Access Dark Fiber Connectivity



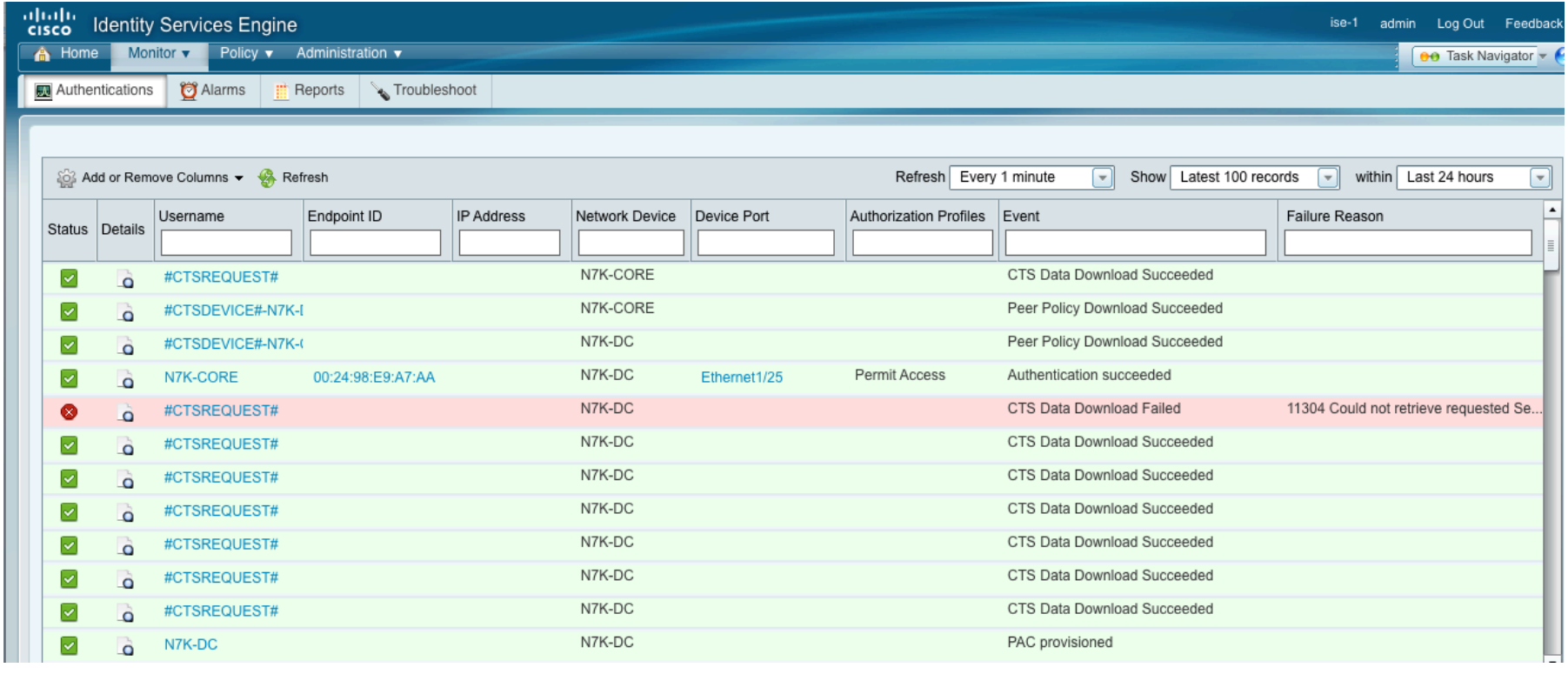
Trustsec for Secure DataCenter Interconnect

Dual Access with MPLS Connectivity



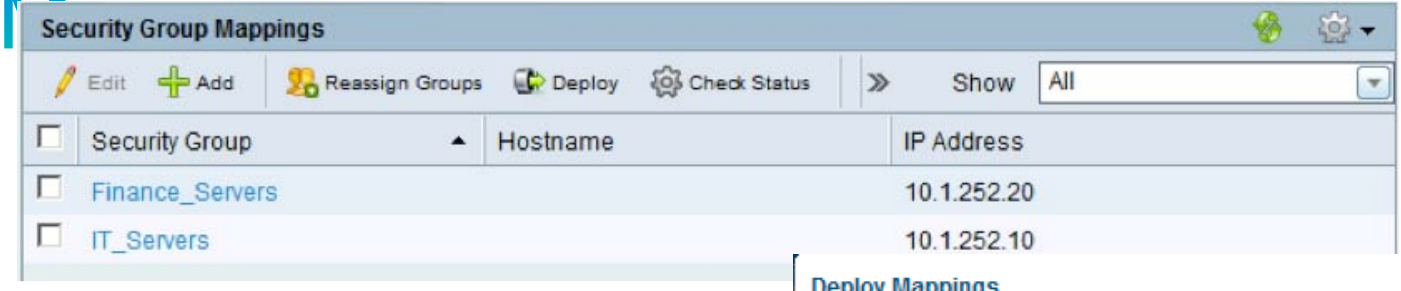
Monitoring and Reporting - SGT

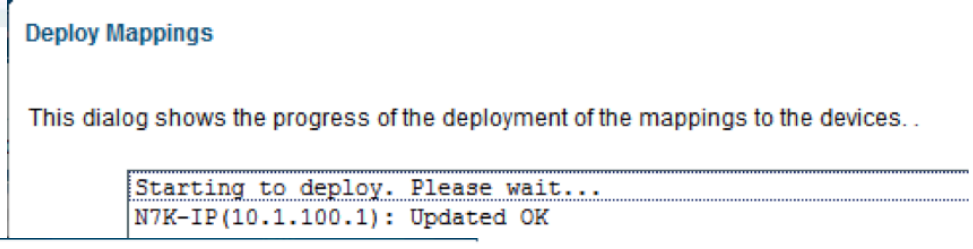
ISE Monitoring Authentications

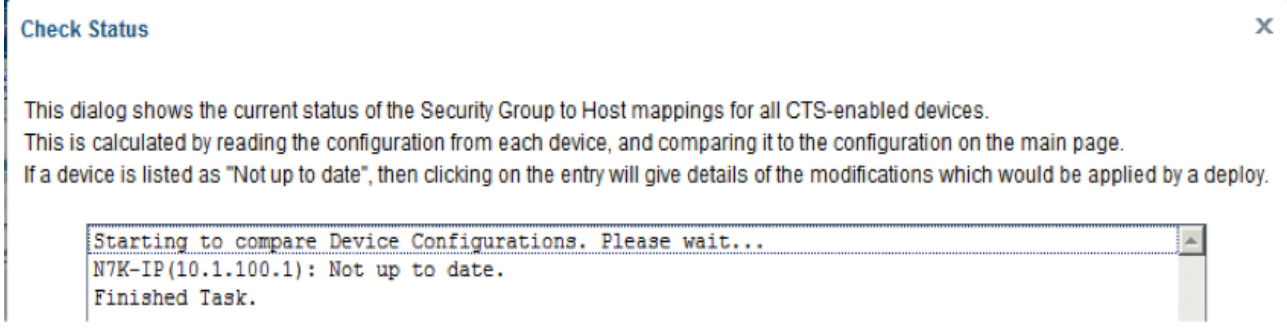


Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Event	Failure Reason
✓		#CTSREQUEST#			N7K-CORE			CTS Data Download Succeeded	
✓		#CTSDEVICE#-N7K-I			N7K-CORE			Peer Policy Download Succeeded	
✓		#CTSDEVICE#-N7K-(			N7K-DC			Peer Policy Download Succeeded	
✓		N7K-CORE	00:24:98:E9:A7:AA		N7K-DC	Ethernet1/25	Permit Access	Authentication succeeded	
✗		#CTSREQUEST#			N7K-DC			CTS Data Download Failed	11304 Could not retrieve requested Se...
✓		#CTSREQUEST#			N7K-DC			CTS Data Download Succeeded	
✓		#CTSREQUEST#			N7K-DC			CTS Data Download Succeeded	
✓		#CTSREQUEST#			N7K-DC			CTS Data Download Succeeded	
✓		#CTSREQUEST#			N7K-DC			CTS Data Download Succeeded	
✓		#CTSREQUEST#			N7K-DC			CTS Data Download Succeeded	
✓		#CTSREQUEST#			N7K-DC			CTS Data Download Succeeded	
✓		N7K-DC			N7K-DC			PAC provisioned	

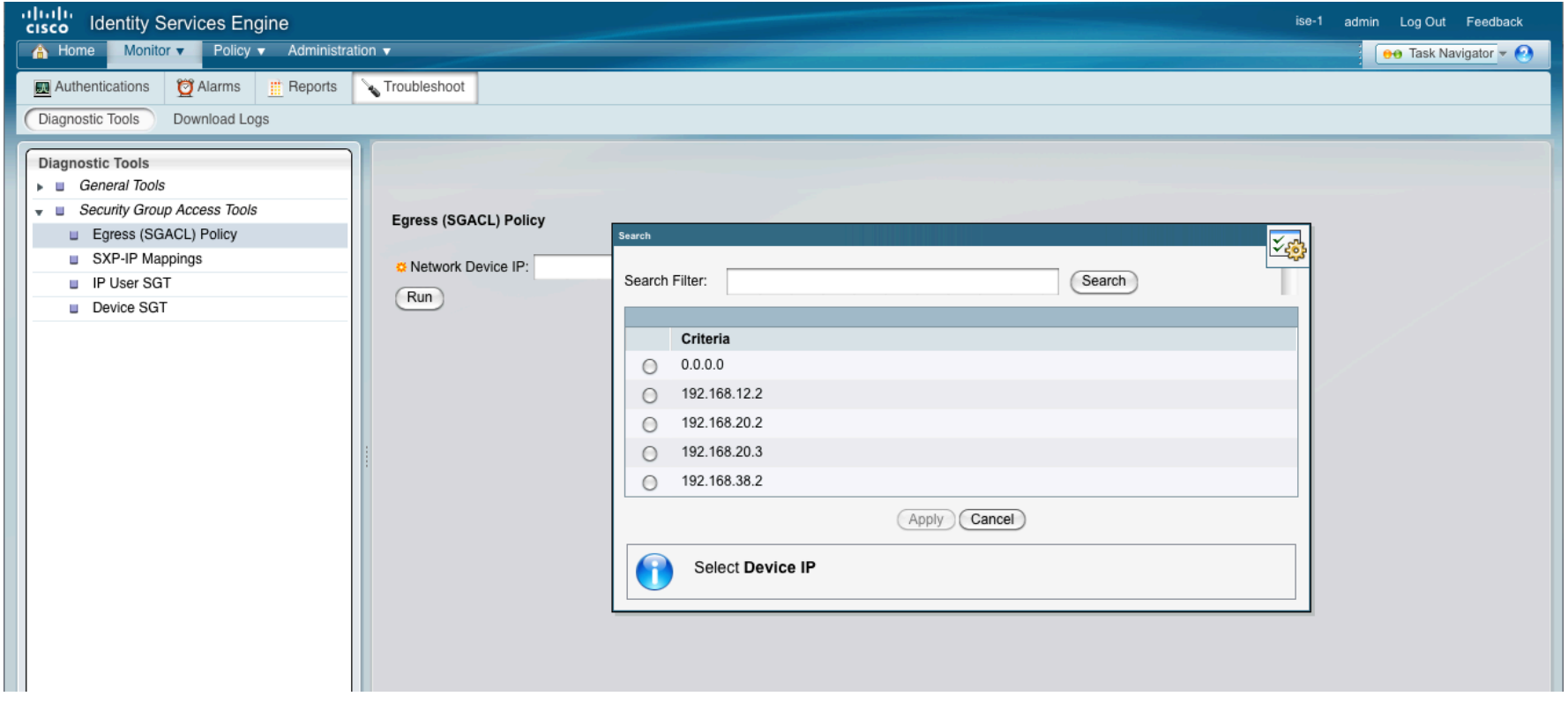
Using ISE to Deploy Security Group Mappings



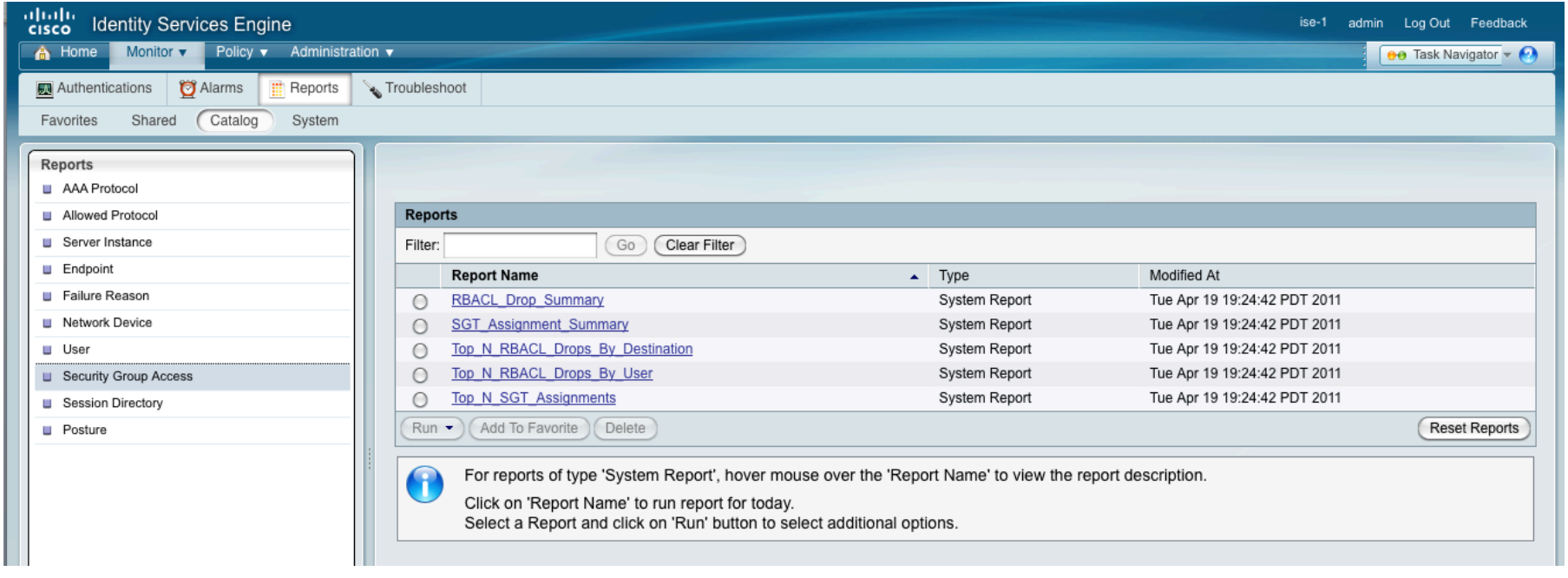




Diagnostic Tools for Troubleshooting SGA



TrustSec Reports



Session Summary

Summary

- SGA builds upon Identity services
- SGA provides a scalable Identity Access Control model
- SGA migration strategies allow customers to deploy with existing hardware
- SGA is deployable **today**

SGA Component Support Matrix

Platforms	Available Feature	OS Version	Notes
Nexus 7000 series Switch	SGACL, 802.1AE + SAP, NDAC, SXP, IPM, EAC	Cisco NX-OS®5.0.2a. **Advanced Service Package license is required**	Enforcement Device, DC Distribution
Catalyst 6500E Switch (Supervisor 32, 720, 720-VSS)	NDAC (No SAP), SXP, EAC	Cisco IOS® 12.2 (33) SXI3 or later release. IP Base K9 image required	Campus / DC Access switch
Catalyst 49xx switches	SXP, EAC	Cisco IOS® 12.2 (50) SG7 or later release.	DC Access switch
Catalyst 4500 Switch (Supervisor 6L-E or 6-E)	SXP, EAC	Cisco IOS® 12.2 (53) SG7 or later release.	Campus Access Switch
Catalyst 3560-X / 3750-X Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE2 or later release.	Campus Access Switch
Catalyst 3560(E) / 3750(E) Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE1 or later release.	Campus Access Switch
Catalyst Blade Module 3x00 Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE1 or later release.	DC Access Switch
Cisco EtherSwitch service module for ISR Routers	SXP, EAC	Cisco IOS® 12.2 (53) SE1 or later release. IP Base K9 image required.	Branch Access Switch
Cisco Secure ACS	Centralized Policy Management for TrustSec	ACS Version 5.1 with **TrustSec™ license required.** CSACS1120 appliance or ESX Server 3.5 or 4.0 is supported	Policy Server
Identity Services Engine	Centralized Policy Management for TrustSec	ISE 1.0 with Advanced license required.	Policy Server

For conference presentations visit:

www.networkerssolutionsforum.com

Please take a moment to complete the Networkers Conference Event Evaluation Form

Q & A

Thank you.