Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Deploying Campus Security Group Tags

BRKCRS-2662

TOMORROW starts here.

Abstract

- This session provides an overview of the Cisco TrustSec Security Group Access (SGA) solution for Role-Based Access Control with focus on Campus Network. SGA allows for simplified network segmentation based on User Identity/Role and allows for secure access and consistent security policies across Wired/Wireless networks. SGA helps define BYOD policies through security policies based on User/Role/Device/Location.
- The session covers SGA on the Catalyst Switching platforms, including converged wired/wireless. The session covers an architectural overview of SGA and benefits of a converged wired/wireless network, elements of Cisco TrustSec such as user identification with 802.1x, device identification, role classification using Security Group Tagging (SGT) and enforcement using Security Group Access Control List (SGACL). We also discuss various SGA deployment use cases in a campus network. This session is for Network Architects, Pre-Sales Engineers and Technical Decision Makers.

Why Should You Care About TrustSec

- BYOD, IPv6 and Internet of Things require different approach to manageability
- Unified Security Policy across Wired and Wireless

Agenda

- TrustSec Overview
- Campus Deployment Use Cases
- Migration Path
- Wireless Integration
- How to Deploy

Session Objectives

TrustSec is ready to be deployed in campus networks today.

At the end of the session, the participants should be able to:

- Understand Components of TrustSec Solution
- Differentiate Campus Deployment Models
- Learn about Best Practices, Migration Paths and Caveats

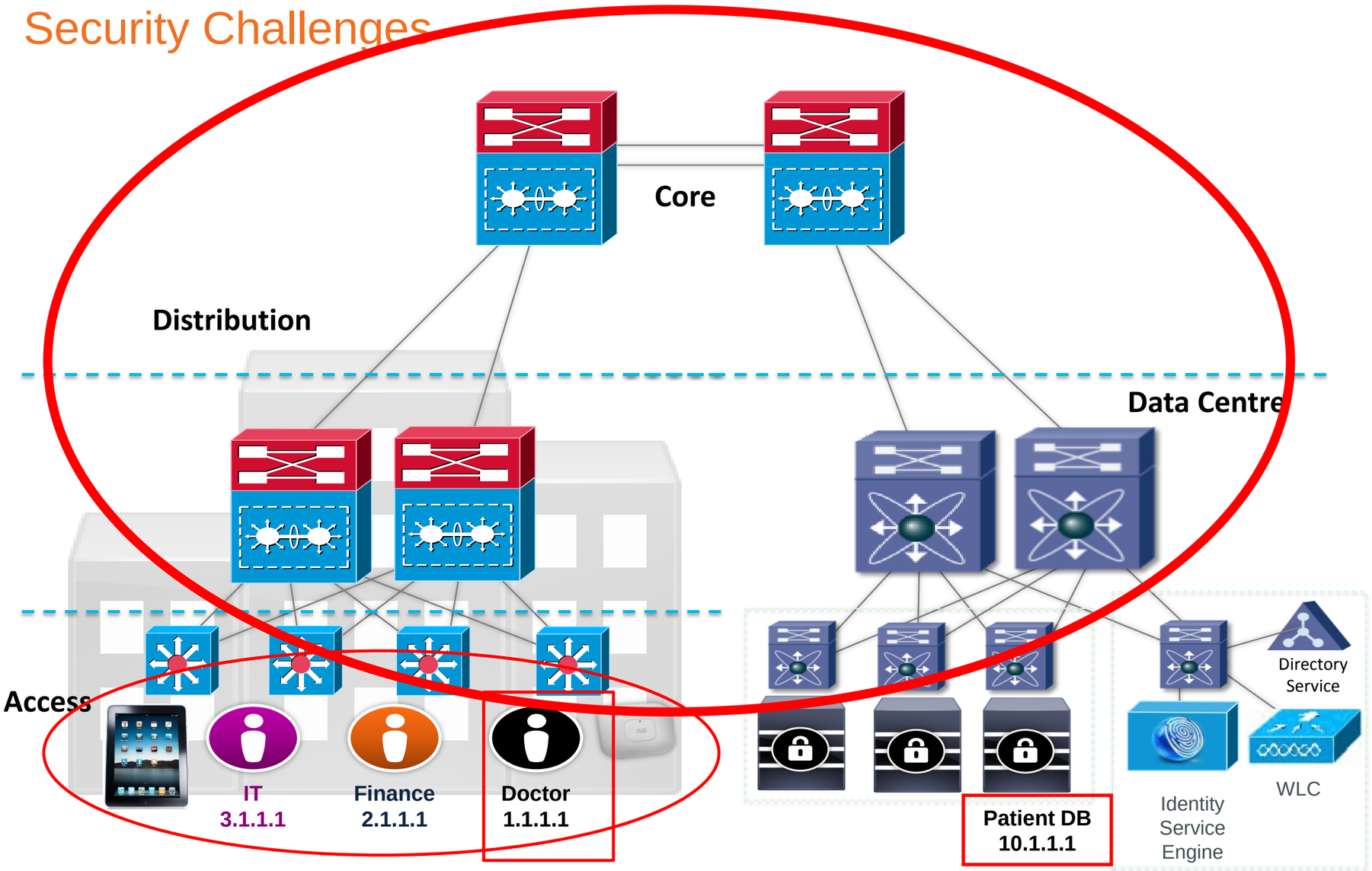
Not Covered

- ❑ Basic IEEE 802.1X concepts
- ❑ Branch Scenario
- ❑ ASA Firewall

TrustSec: An Overview

Traditional Campus Network

Security Challenges

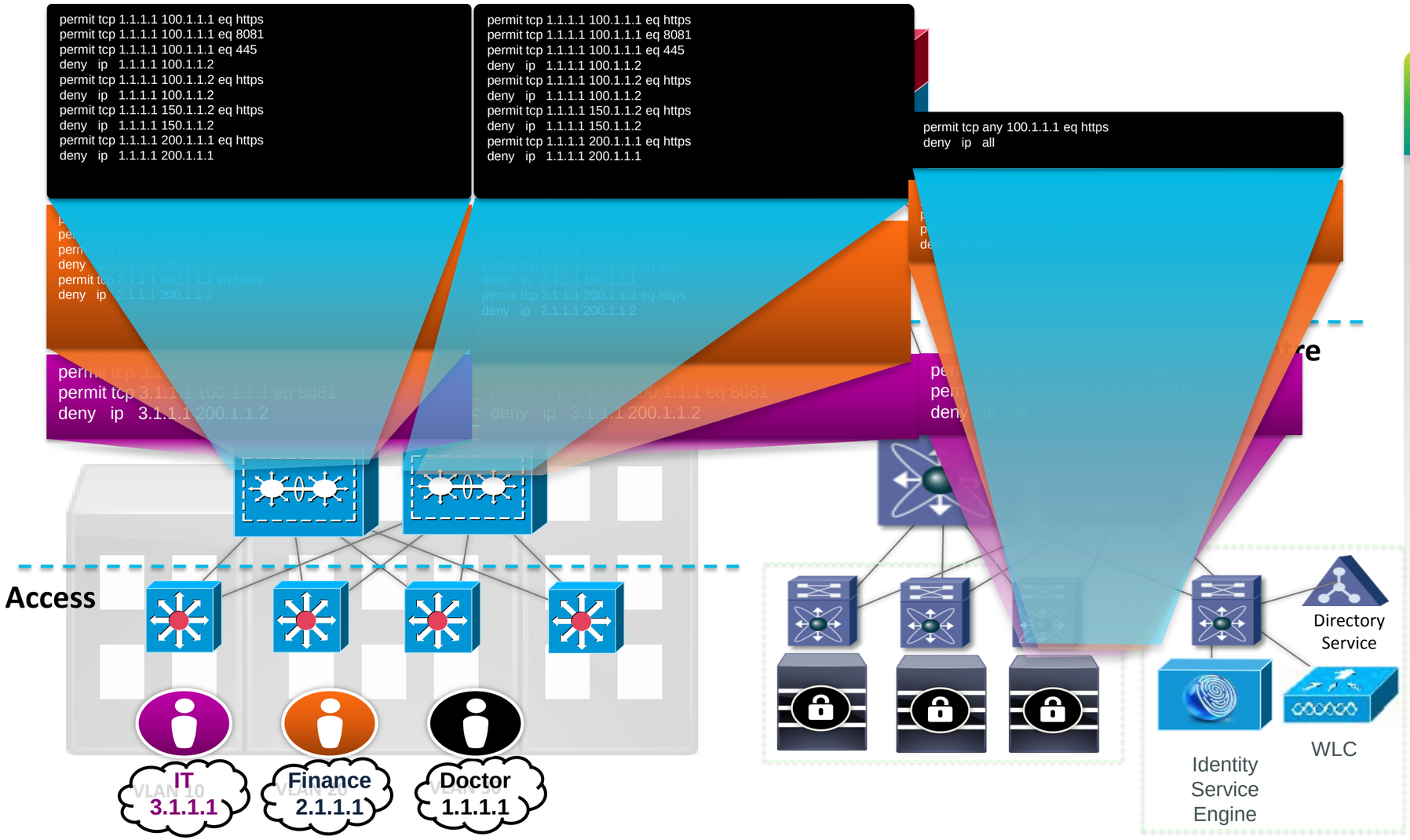


Security Challenges

- User Identification
- Device Identification
- Segmentation
- Unified Policy
- Central Policy Management
- Network Infrastructure Protection
- Scalable for future growth

Segmentation

The Challenge of Traditional Security Enforcement



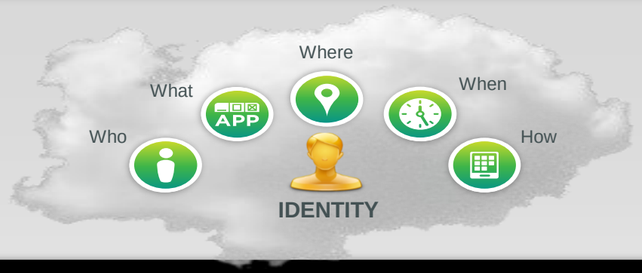
Access Control with IP Access Control Lists

- Topology-based
- Manual configurations
- Error prone
- Unscalable
- Difficult to maintain

Comprehensive End-to-End Security

Cisco TrustSec

Context-Aware Control

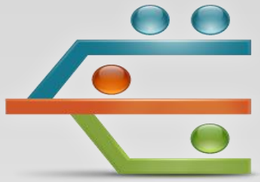


Role-Based Access Control with **Security Group Tagging** (SGT)

Identify, Profile Devices with **Device Sensor**

802.1X Authentication

Segmentation (Compliance)



Topology Independent Segmentation with **Secure Group Access** (SGA)

Protect Network Infrastructure

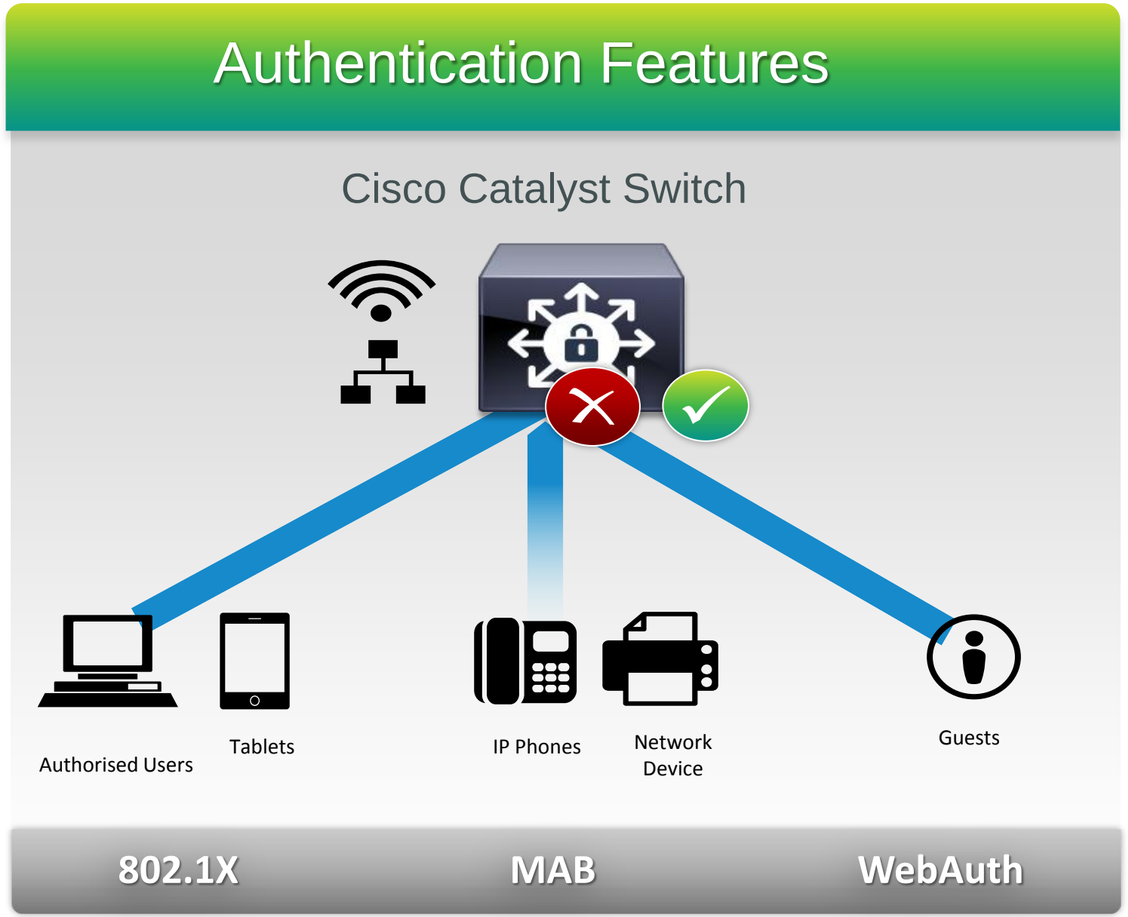
MACsec Encryption

Network Device Admission Control (NDAC)

Context-Aware Control

User Authentication: 802.1X

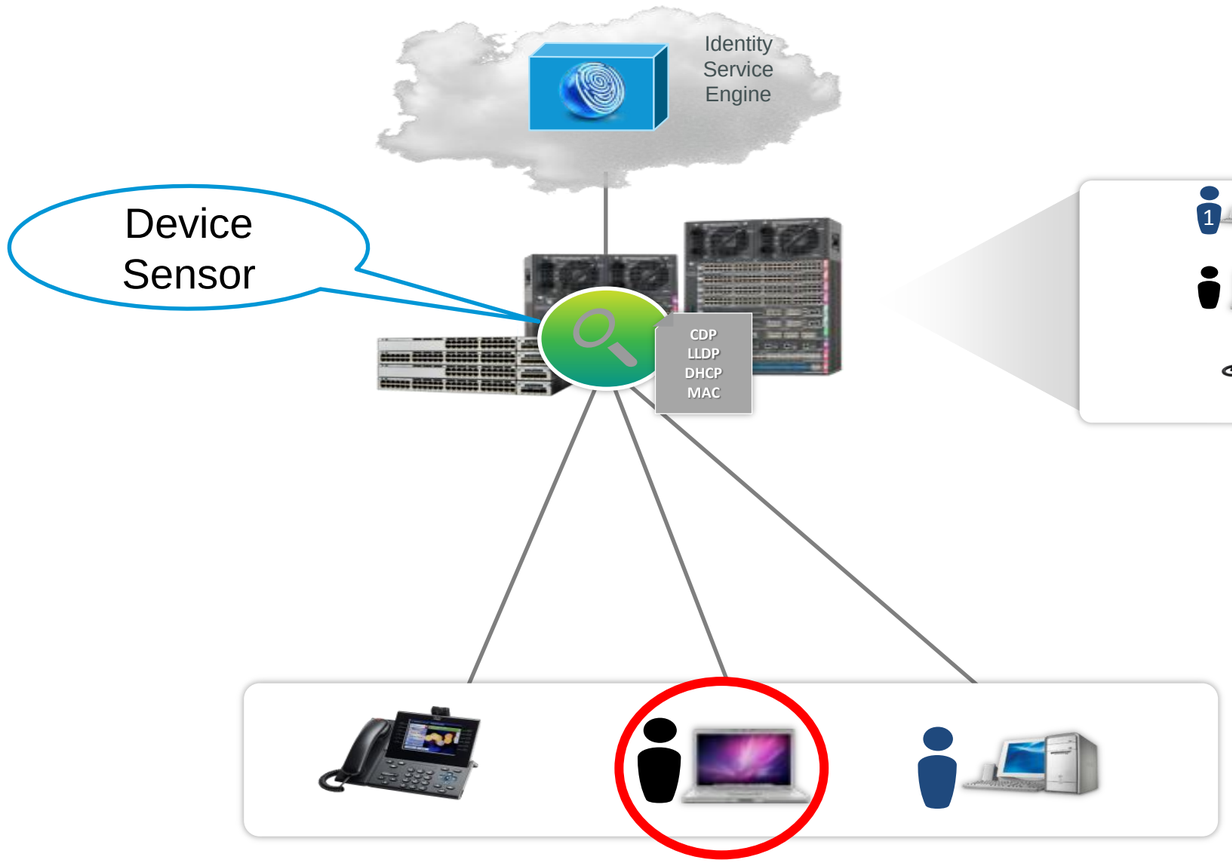
- Monitor Mode
  - Unobstructed access
  - No impact on productivity
  - Gain visibility



Context-Aware Control

Device Sensor

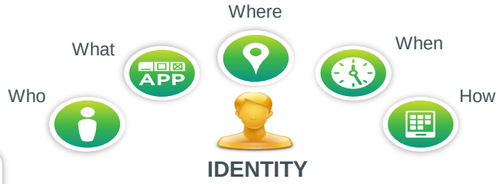
Identify Devices and set Device-based policies with Device Sensor



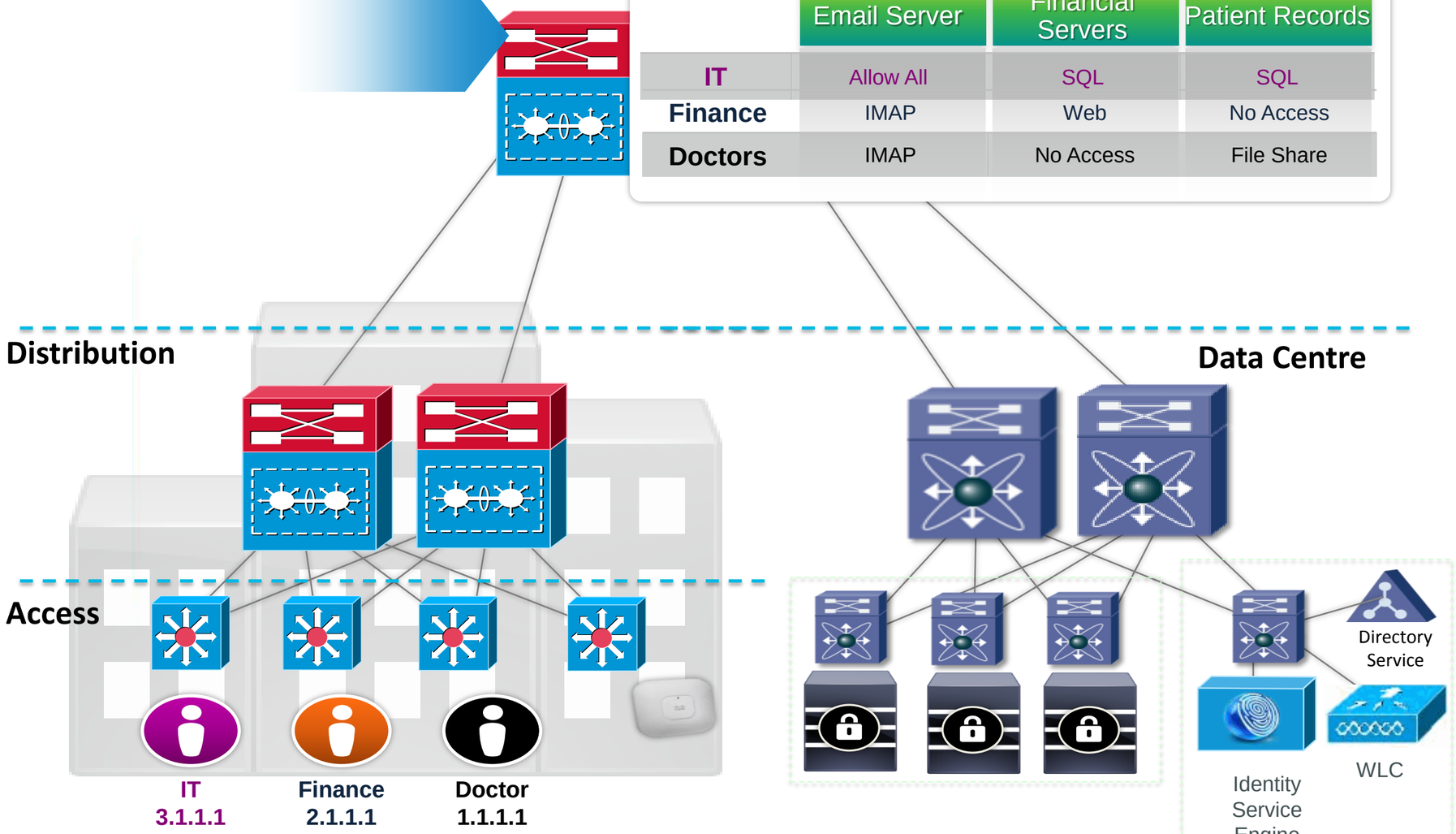
Device-Aware	Identity- Aware
Corp PC	Doctor
Personal Laptop	Doctor
IP Phone	N/A

Segmentation

Security Group Access



	Email Server	Financial Servers	Patient Records
IT	Allow All	SQL	SQL
Finance	IMAP	Web	No Access
Doctors	IMAP	No Access	File Share

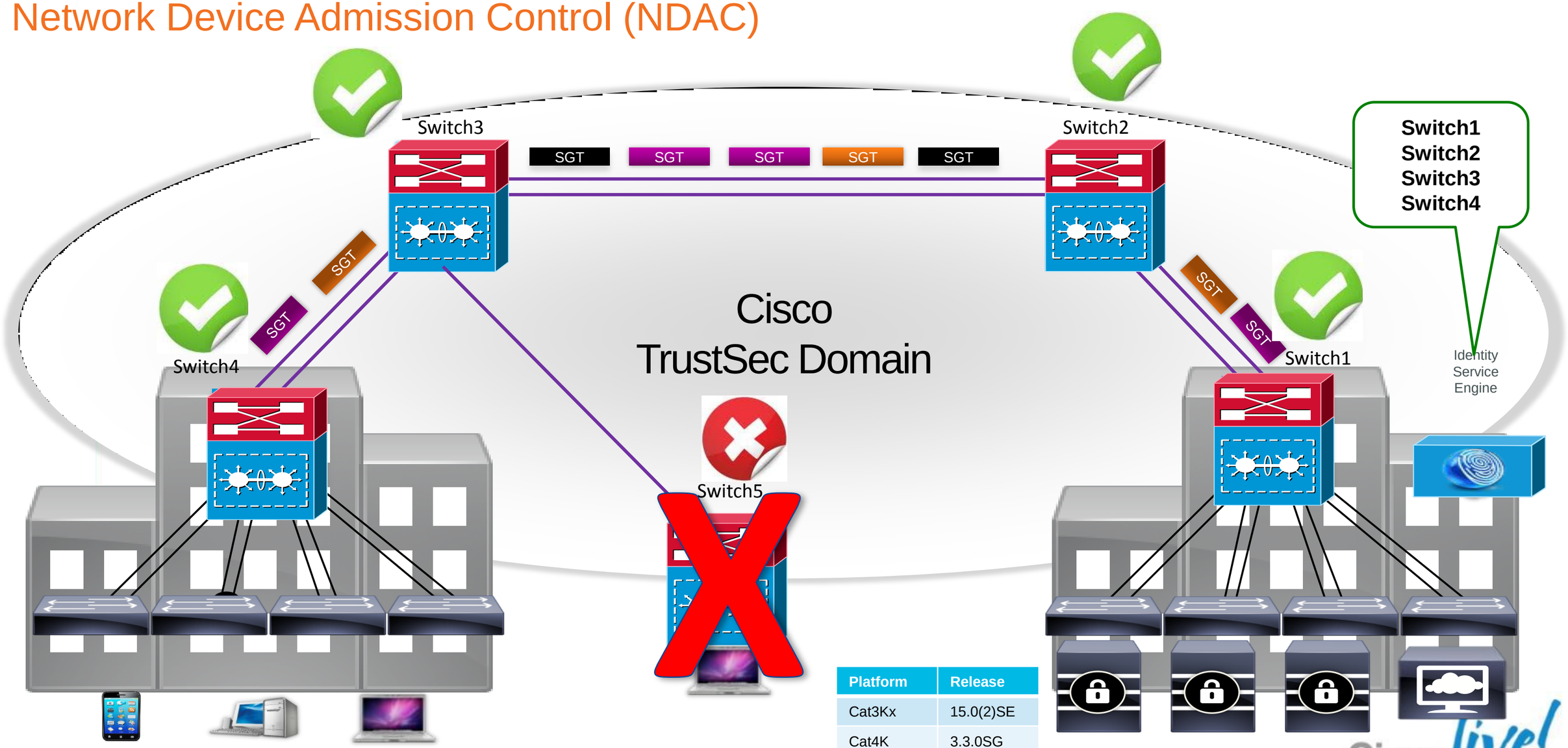


Access Control with Secure Group Access

- Context-based Classification
- Role-based Policies
- Topology-independent
- Network wide enforcement
- Scalable
- Easy to administer
- One Policy

Protect Network Infrastructure

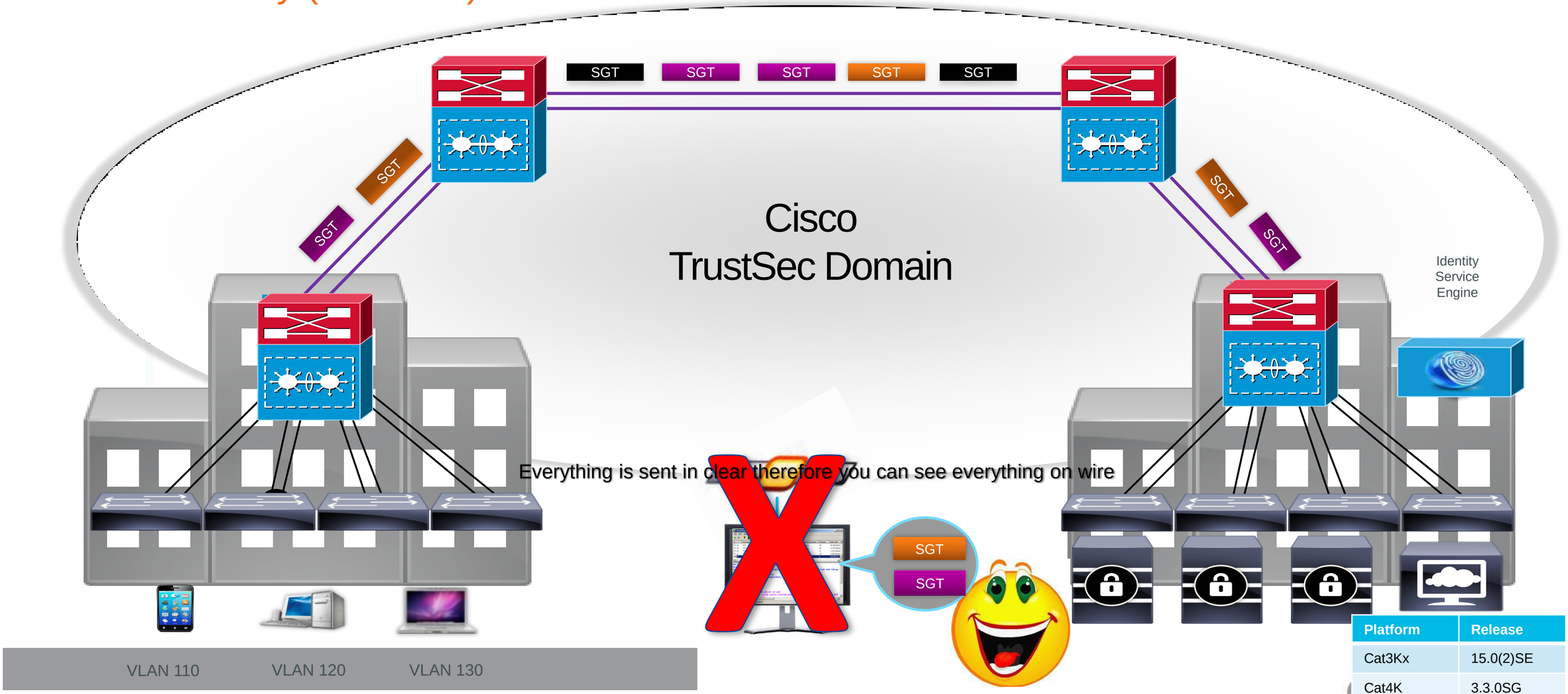
Network Device Admission Control (NDAC)



Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	3.3.0SG
Cat6K	15.0(1)SY

Protect Network Infrastructure

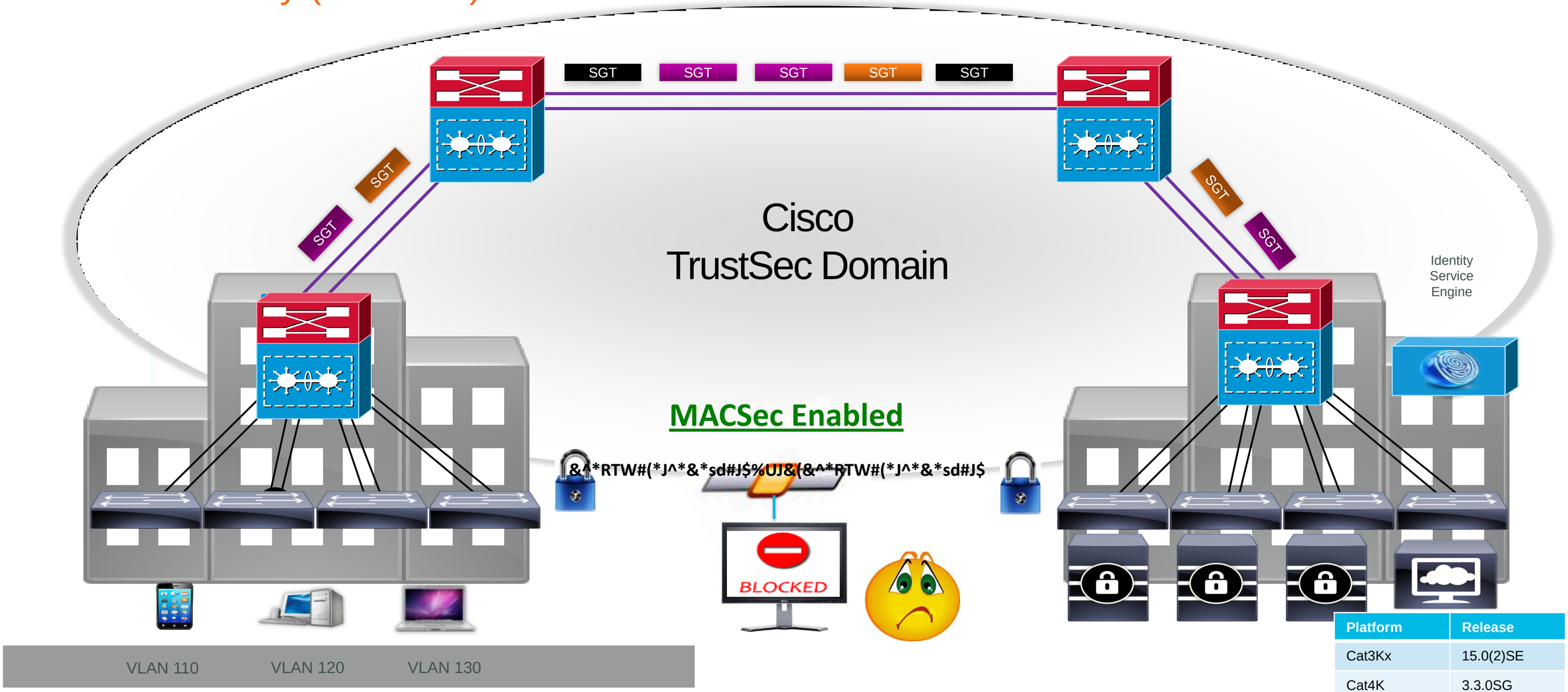
MAC Security (MACSec)



Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	3.3.0SG
Cat6K	15.0(1)SY

Protect Network Infrastructure

MAC Security (MACSec)



Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	3.3.0SG
Cat6K	15.0(1)SY

How Cisco TrustSec Works

Segmentation

Security Group Tagging (SGT) and SGACL

Dynamic Assignment or Map VLANs or IP Subnets to SGT Values

```
cts role-based sgt-map VLAN-list 10 sgt 10

cts role-based sgt-map 192.168.10.0/24 sgt 10
```

SGACL Enforcement

```
cts role-based permissions from 10 to 111
     permit tcp dst eq 443
     permit tcp dst eq 80
     deny ip
```

SGT SGT SGT SGT

Cisco TrustSec Domain

SGT

SGT

Identity Service Engine

Can Forward Existing SGT Traffic or Map SGTs Manually

SG Tag Imposed to Incoming Traffic

Device-Aware	Identity-Aware	Security Group
Corp PC	Doctor	Doctor
Personal PC	Doctor	Doctor
IP Phone	NA	Voice

Role Identification (SGT Assignment)

Campus/Mobile Endpoints

- via 802.1X Authentication
- via MAC Authentication Bypass
- via Web Authentication Bypass
- Or Static IP-to-SGT binding on SW

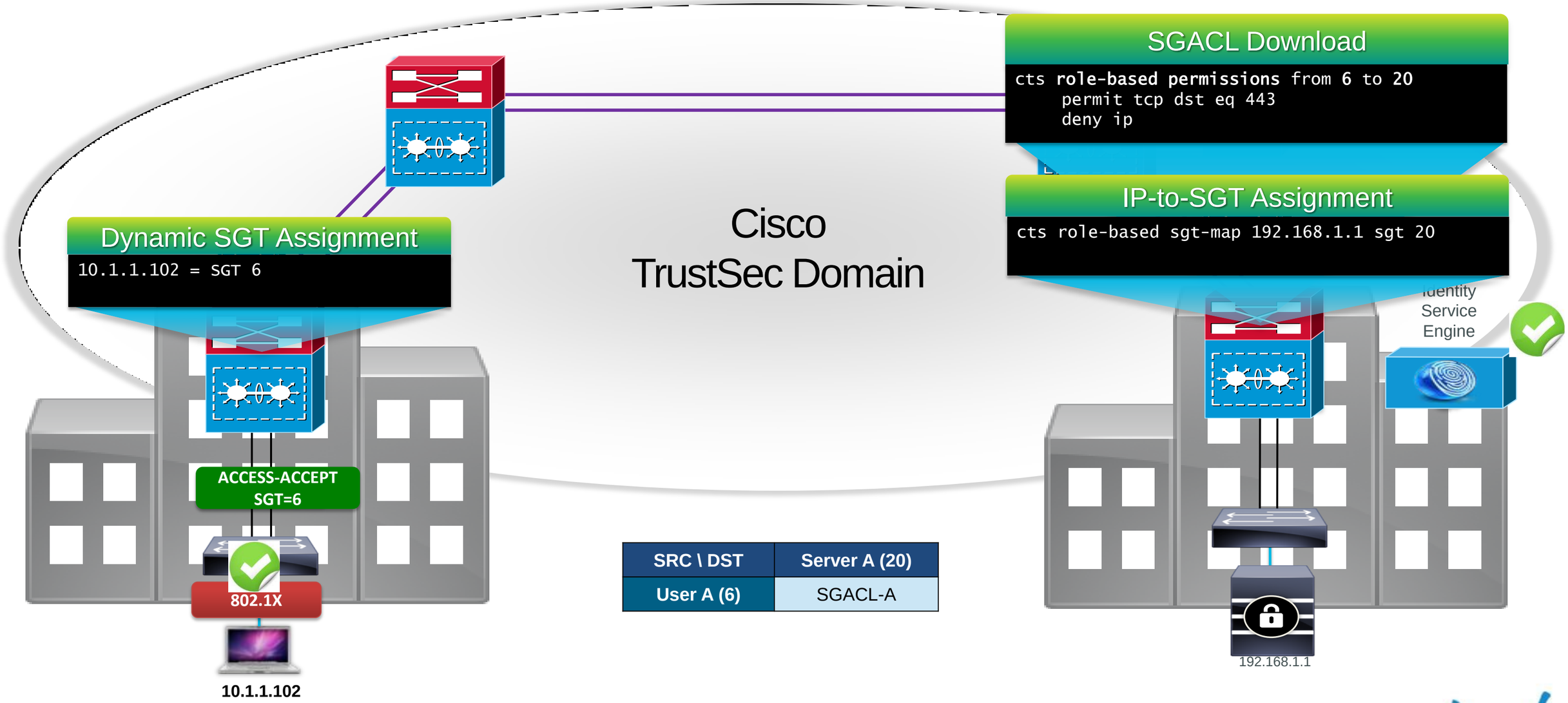
Full integration with Cisco Identity Solution

Just like VLAN Assignment or dACL, we assign SGT in authorisation process

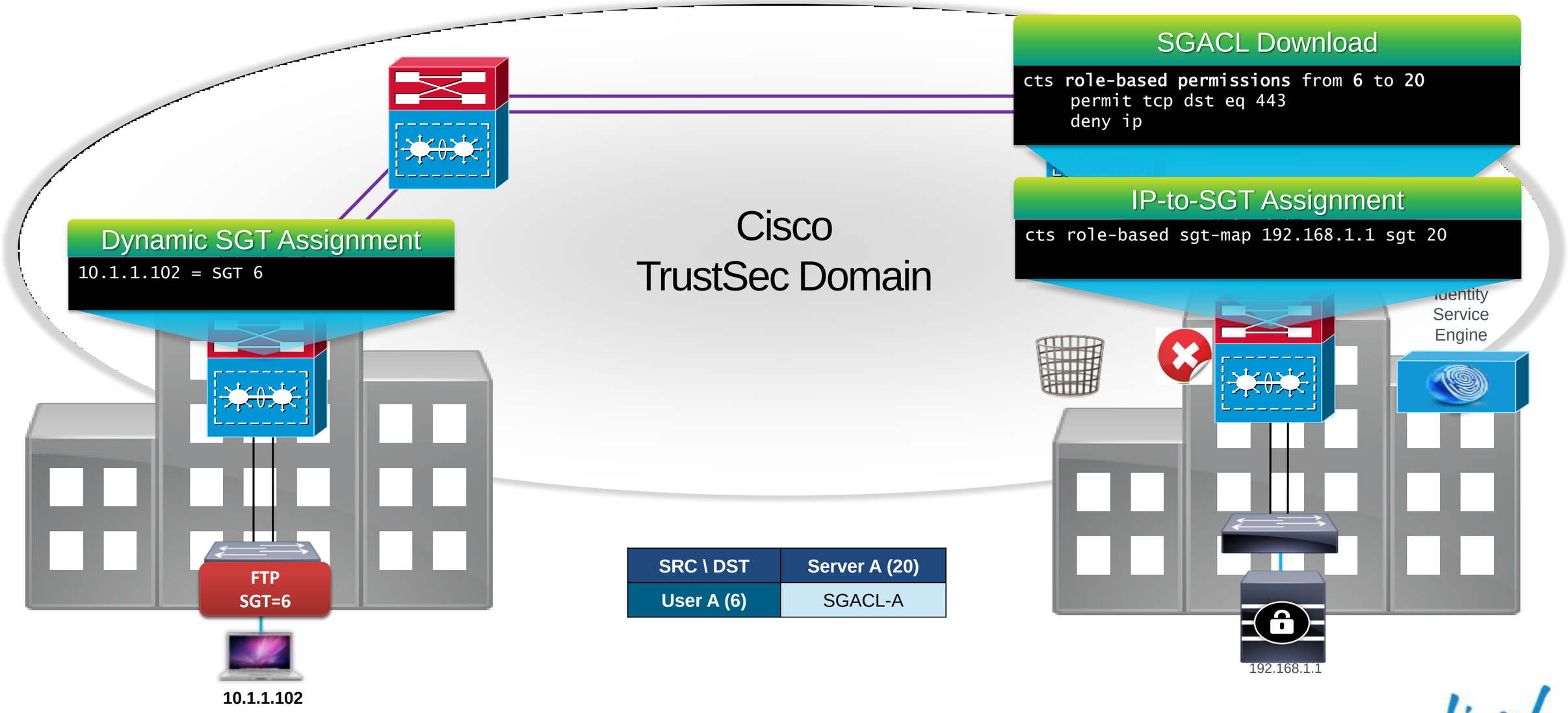
Data Centre/ Servers

- **via Manual IP-to-SGT binding on TrustSec device**
- **via IP-to-Port Mapping**

How SGT Assignment Works

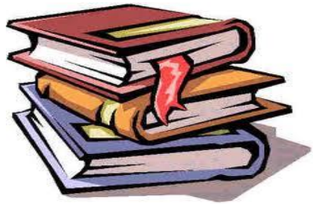


How SGACL Enforcement Works



SRC \ DST	Server A (20)
User A (6)	SGACL-A

RADIUS Access-Request Frame Format



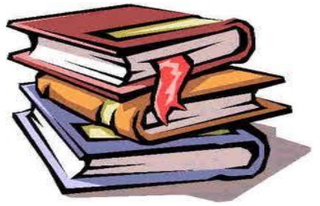
User Authentication Request

```
▽ User Datagram Protocol, Src Port: 1645 (1645), Dst Port: 1812 (1812)
    Source port: 1645 (1645)
    Destination port: 1812 (1812)
    Length: 280
  ▷ Checksum: 0x0e6b [validation disabled]
▽ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x5b (91)
    Length: 272
    Authenticator: e1a24213e4afaac4c0990a732f0e2ae0
    [The response to this request is in frame 71]
  ▽ Attribute Value Pairs
    ▽ AVP: l=203  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=197 t=Cisco-AVPair(1): cts-pac-opaque=\000\002\000X\000\003\000\C
          Cisco-AVPair: cts-pac-opaque=
    ▽ AVP: l=18  t=User-Password(2): Encrypted
        User-Password: XpX\235C\026\231Xk XX4XXX\202
    ▽ AVP: l=7  t=User-Name(1): user1
        User-Name: user1
    ▽ AVP: l=6  t=NAS-IP-Address(4): 172.28.103.210
        NAS-IP-Address: 172.28.103.210 (172.28.103.210)
    ▽ AVP: l=18  t=Message-Authenticator(80): f88ca523fbc3165dc403ece8bcf9cd01
        Message-Authenticator: f88ca523fbc3165dc403ece8bcf9cd01
```

```
Dist-3K#test aaa group radius user1 Cisco123 new-code
User successfully authenticated

USER ATTRIBUTES

username                0    "user1"
Termination-Action      0    True
Message-Authenticato    0    <hidden>
CiscoSecure-Defined-    0    "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406"
```

RADIUS Access-Accept Frame Format

User Authentication With Downloadable ACL



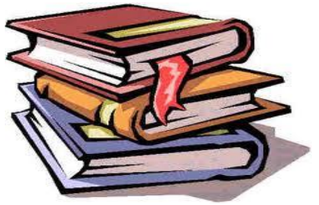
```
▽ User Datagram Protocol, Src Port: 1812 (1812), Dst Port: 1645 (1645)
    Source port: 1812 (1812)
    Destination port: 1645 (1645)
    Length: 226
  ▷ Checksum: 0x8a68 [validation disabled]
▽ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x5b (91)
    Length: 218
    Authenticator: 6efff45a8f5b4f2c361dab1e3f0f5d6d
    [This is a response to a request in frame 70]
    [Time from request: 0.006188000 seconds]
  ▽ Attribute Value Pairs
    ▽ AVP: l=7  t=User-Name(1): user1
        User-Name: user1
    ▽ AVP: l=40  t=State(24): 52656175746853657373696f6e3a6163316363762323030...
        State: 52656175746853657373696f6e3a6163316363762323030...
    ▽ AVP: l=52  t=Class(25): 434143533a6163316336376232303030333246313835304 1...
        Class: 434143533a6163316336376232303030333246313835304 1...
```

```
Dist-3K#test aaa group radius user1 Cisco123 new-code
User successfully authenticated

USER ATTRIBUTES

username                0   "user1"
Termination-Action      0   True
Message-Authenticato    0   <hidden>
CiscoSecure-Defined-    0   "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406"
```

```
5  t=Vendor-Specific(26) v=Cisco(9)
=69 t=Cisco-AVPair(1): ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_
o-AVPair: ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57
```

RADIUS Access-Accept Frame Format

User Authentication With SGT Assignment

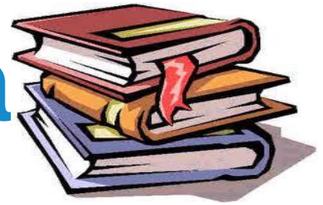


```
▽ User Datagram Protocol, Src Port: 1812 (1812), Dst Port: 1645 (1645)
    Source port: 1812 (1812)
    Destination port: 1645 (1645)
    Length: 188
  ▷ Checksum: 0x9356 [validation disabled]
▽ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x5d (93)
    Length: 180
    Authenticator: 543b6fedafe9f1b56afdf16a71937122
    [This is a response to a request in frame 27]
    [Time from request: 0.005731000 seconds]
  ▽ Attribute Value Pairs
    ▽ AVP: l=7  t=User-Name(1): user1
        User-Name: user1
    ▽ AVP: l=40  t=State(24): 526561757468536573736696f6e3a6163316336376232303030...
        State: 526561757468536573736696f6e3a6163316336376232303030...
    ▽ AVP: l=52  t=Class(25): 434143533a6163316336376232303030333246314135304 1...
        Class: 434143533a6163316336376232303030333246314135304 1...
    ▽ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
        Termination-Action: RADIUS-Request (1)
    ▽ AVP: l=18  t=Message-Authenticator(80): d0c61e9c3c7970ada598434df920e057
```

```
Dist-3K#test aaa group radius user1 Cisco123 new-code
User successfully authenticated

USER ATTRIBUTES

username                0   "user1"
Termination-Action      0   True
Message-Authenticato    0   <hidden>
security-group-tag      0   "0004-0"
Dist-3K#
```

```
▽ AVP: l=37  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=31 t=Cisco-AVPair(1): cts:security-group-tag=0004-0
      Cisco-AVPair: cts:security-group-tag=0004-0
```

RADIUS Access-Request Frame Forma



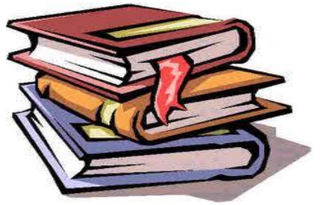
Device Authentication Request

```
▽ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x5e (94)
    Length: 368
    Authenticator: 92b69e3a453740eb1ded5448487624c2
    [The response to this request is in frame 92]
  ▽ Attribute Value Pairs
    ▽ AVP: l=203  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=197 t=Cisco-AVPair(1): cts-pac-opaque=\000\002\000[illegible]
          Cisco-AVPair: cts-pac-opaque=
    ▽ AVP: l=14  t=User-Name(1): #CTSREQUEST#
        User-Name: #CTSREQUEST#
    ▽ AVP: l=36  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=30 t=Cisco-AVPair(1): cts-environment-data=Dist-3K
          Cisco-AVPair: cts-environment-data=Dist-3K
    ▽ AVP: l=47  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=41 t=Cisco-AVPair(1): cts-device-capability=env-data-fragment
          Cisco-AVPair: cts-device-capability=env-data-fragment
    ▽ AVP: l=18  t=User-Password(2): Encrypted
        User-Password: c[illegible]\200\027[illegible]q\021\003[illegible]$s[illegible]\223\214\255\036
    ▷ AVP: l=6  t=Service-Type(6): Dialout-Framed-User(5)
    ▽ AVP: l=6  t=NAS-IP-Address(4): 172.28.103.210
        NAS-IP-Address: 172.28.103.210 (172.28.103.210)
    ▽ AVP: l=18  t=Message-Authenticator(80): 28f7e00c22fad4ea9a988a39cdb22419
        Message-Authenticator: 28f7e00c22fad4ea9a988a39cdb22419
```

Switch sends request to authenticate itself

RADIUS Access-Request Frame Format

Device Authentication & SGACL requests



```
▽ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=28 t=Cisco-AVPair(1): cts-rbacl-source-list=000A
      Cisco-AVPair: cts-rbacl-source-list=000A
```

Subsequent requests include SGTs found in the switch

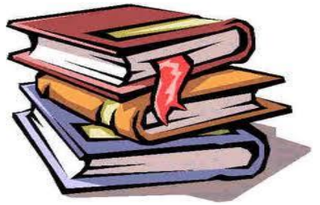
```
▽ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=28 t=Cisco-AVPair(1): cts-rbacl-source-list=0014
      Cisco-AVPair: cts-rbacl-source-list=0014
```

```
▽ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=28 t=Cisco-AVPair(1): cts-rbacl-source-list=0000
      Cisco-AVPair: cts-rbacl-source-list=0000
```

```
▽ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=28 t=Cisco-AVPair(1): cts-rbacl-source-list=0006
      Cisco-AVPair: cts-rbacl-source-list=0006
```

RADIUS Access-Accept Frame Format

Device Authentication

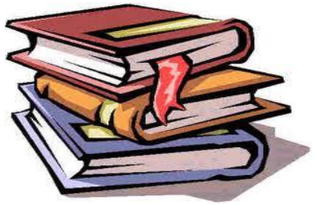


```
▽ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x60 (96)
    Length: 226
    Authenticator: e7743af587e4cc686b1522f78a412405
    [This is a response to a request in frame 79]
    [Time from request: 0.006261000 seconds]
  ▽ Attribute Value Pairs
    ▽ AVP: l=14  t=User-Name(1): #CTSREQUEST#
        User-Name: #CTSREQUEST#
    ▽ AVP: l=40  t=State(24): 526561757468536573736696f6e3a6163316336376232303...
        State: 526561757468536573736696f6e3a6163316336376232303...
    ▽ AVP: l=52  t=Class(25): 434143533a6163316336376232303030333246314435304 1...
        Class: 434143533a6163316336376232303030333246314435304 1...
    ▽ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
        Termination-Action: RADIUS-Request (1)
    ▽ AVP: l=18  t=Message-Authenticator(80): 6087cfbeb62cee11ef22b69fcc18ce44
        Message-Authenticator: 6087cfbeb62cee11ef22b69fcc18ce44
    ▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-00
          Cisco-AVPair: cts:security-group-tag=0000-00
    ▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
          Cisco-AVPair: cts:authorization-expiry=86400
```

Switch authenticated

RADIUS Access-Accept Frame Format

Device Authentication, SGACL & SGACL Matrix Download



SGACLs matching destination downloaded

```
▽ AVP: l=59  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=53 t=Cisco-AVPair(1): cts:src-dst-rbacl=ffff-00-00-ffff-00-00-Permit IP-0
       Cisco-AVPair: cts:src-dst-rbacl=ffff-00-00-ffff-00-00-Permit IP-0
```

```
▽ AVP: l=59  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=53 t=Cisco-AVPair(1): cts:src-dst-rbacl=0003-00-00-0005-06-00-PermitWeb-2
       Cisco-AVPair: cts:src-dst-rbacl=0003-00-00-0005-06-00-PermitWeb-2
```

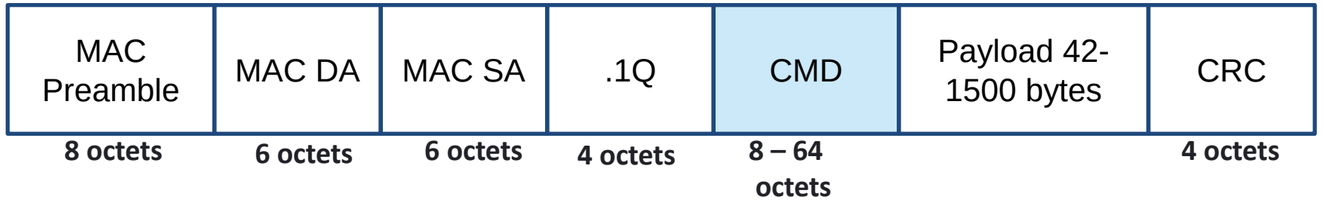
SGACLs downloaded

```
▽ AVP: l=29  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=23 t=Cisco-AVPair(1): cts:rbacl=PermitWeb-2
       Cisco-AVPair: cts:rbacl=PermitWeb-2
▽ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
  ▽ VSA: l=39 t=Cisco-AVPair(1): cts:rbacl-ace#1=permit tcp dst eq www
       Cisco-AVPair: cts:rbacl-ace#1=permit tcp dst eq www
```

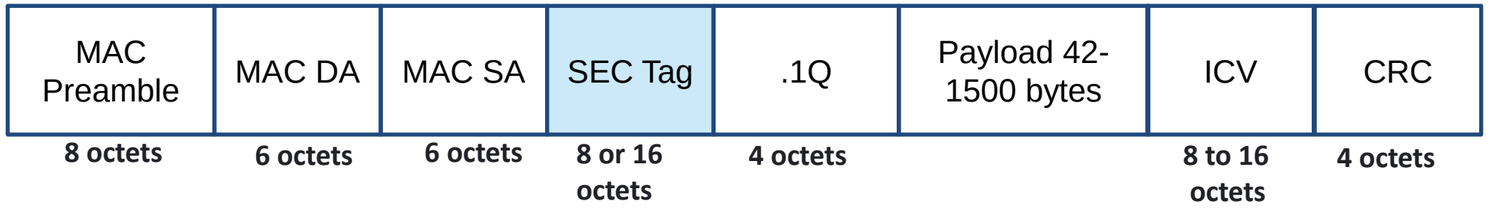
Cisco TrustSec Supported L2 Ethernet Frame Types

Ethernet

Cisco Meta Data (SGT) (gmac, propogate SGT) No encryption



MACsec only (gcm-encrypt) (SEC Tag)



MACsec with Cisco Meta (gcm-encrypt, propogate SGT) Data (SGT)

SGA Deployment Use Cases

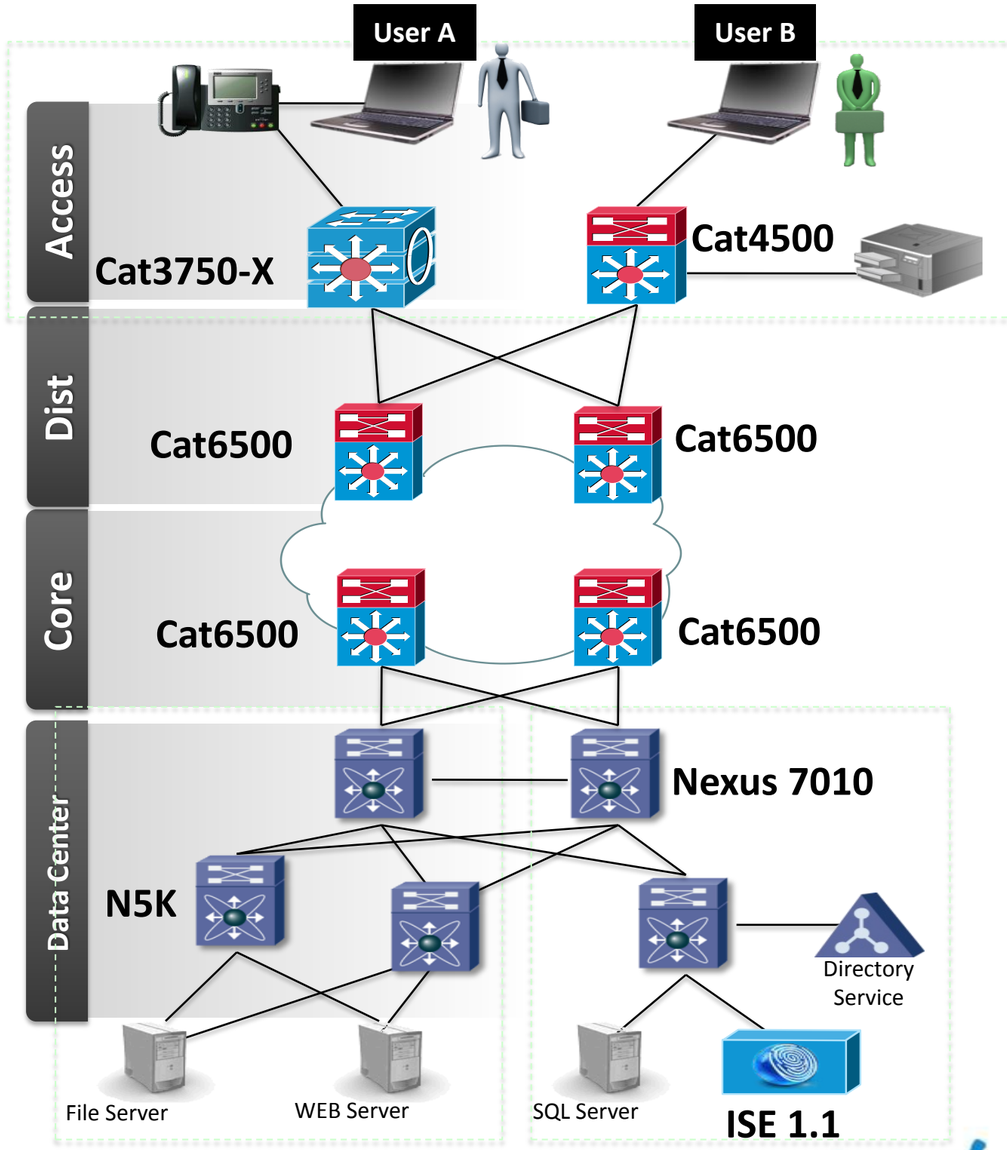
SGA Deployment Use Cases

Campus Reference Design

- Access, Distribution & Core
- Data Centre

Deployment Modes

- 802.1X based SGT Assignment
- Statically configured SGT Assignment
- Migration Scenarios



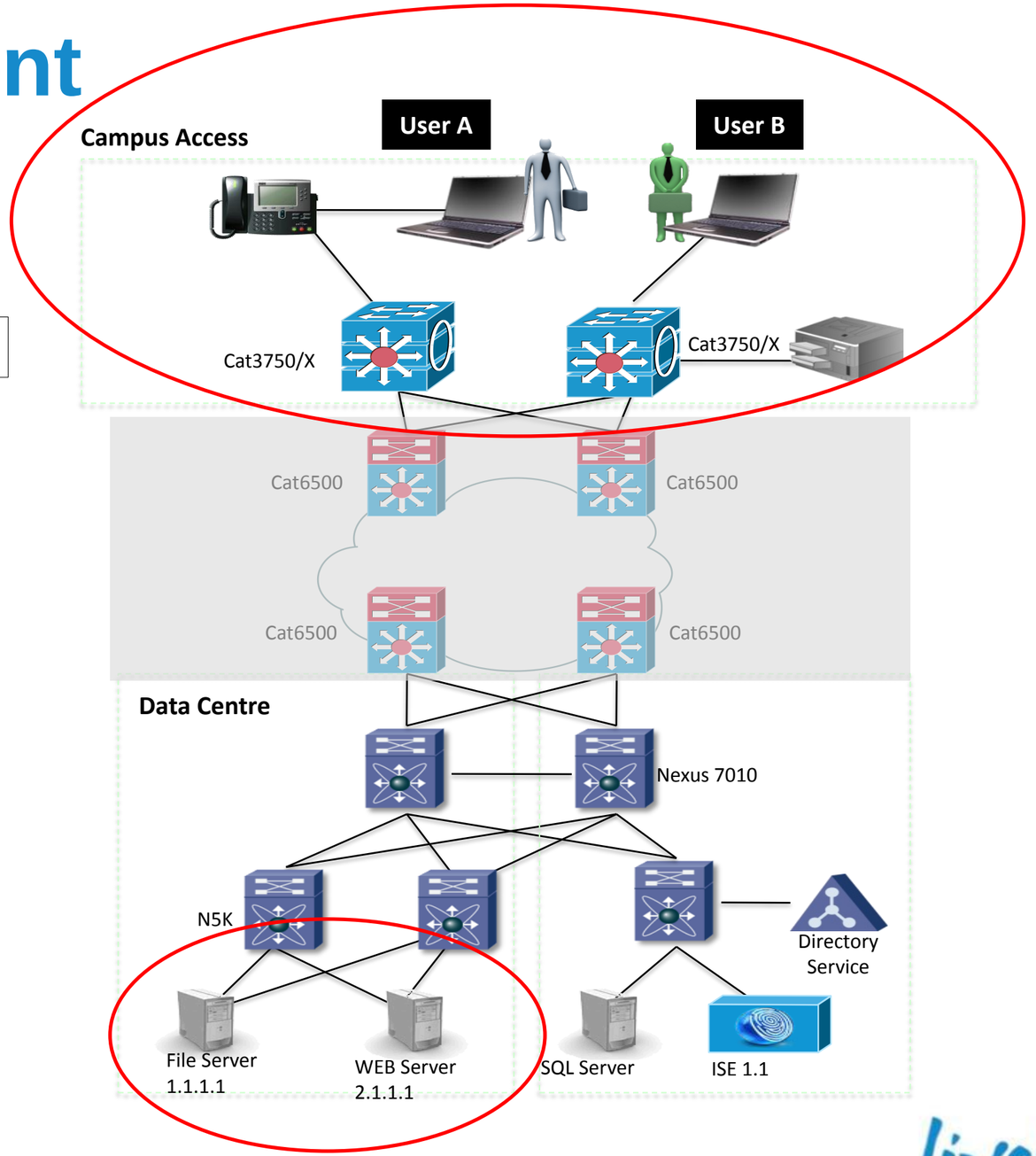
Campus LAN Deployment

Use Case

Campus users accessing resources in Data Centre

Requirement

- User A should be able to access File Server & Web Server
- User B should be denied access to File Server



Campus LAN Deployment

How is it done today without SGA

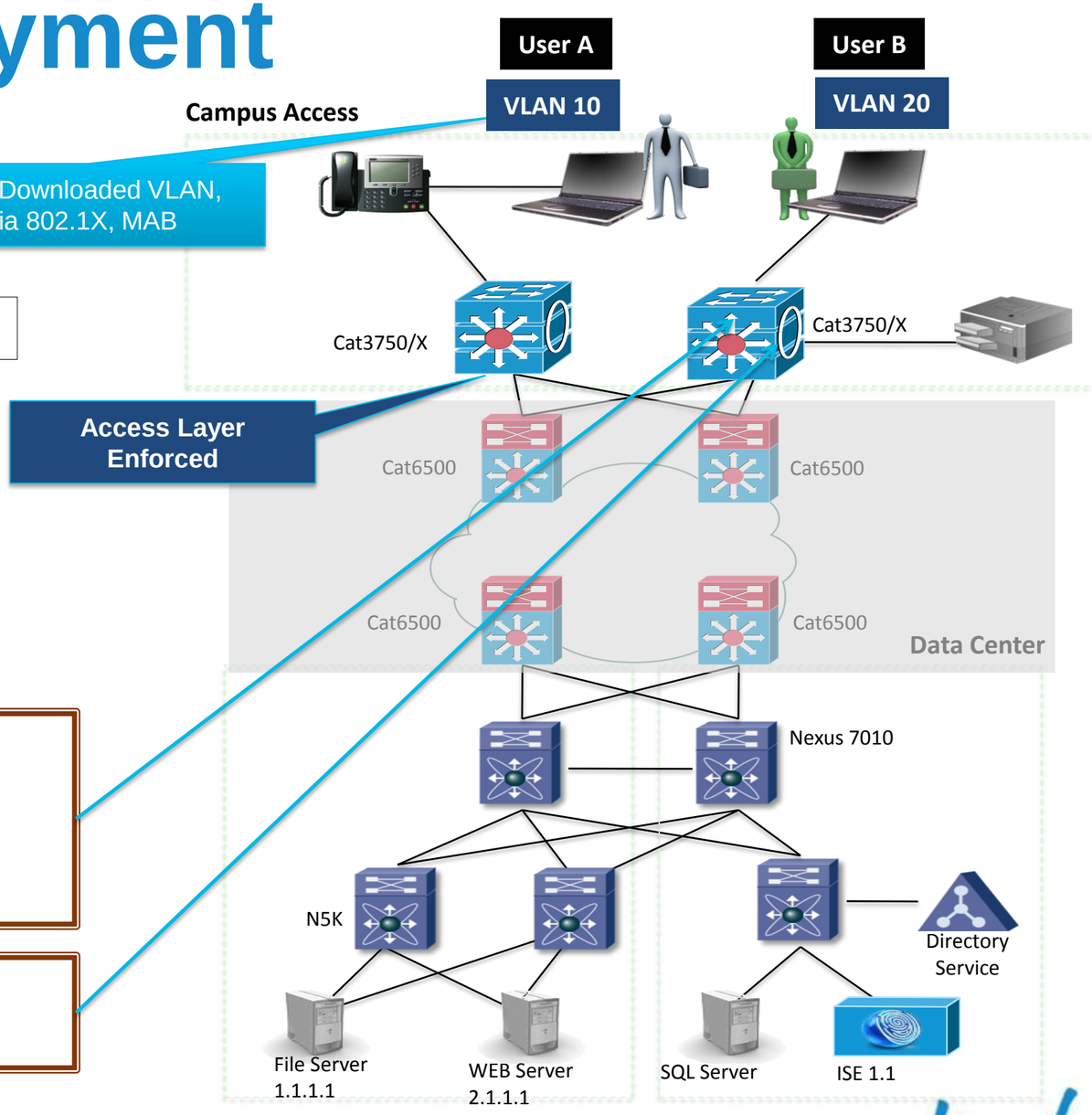
Use Case

Campus users accessing resources in Data Centre

- User VLAN statically defined or assigned during 802.1X or MAB Authentication
- ACL statically defined or downloaded during Authentication

```
Downloaded or Statically Defined ACL
!
Permit tcp any 1.1.1.1 eq 20
Permit tcp any 2.1.1.1 eq http
Permit tcp any 2.1.1.1 eq https
Deny ip any any
```

```
Statically Defined VLAN or Assignment from RADIUS
!
Vlan 10, 20
```



Campus LAN Deployment

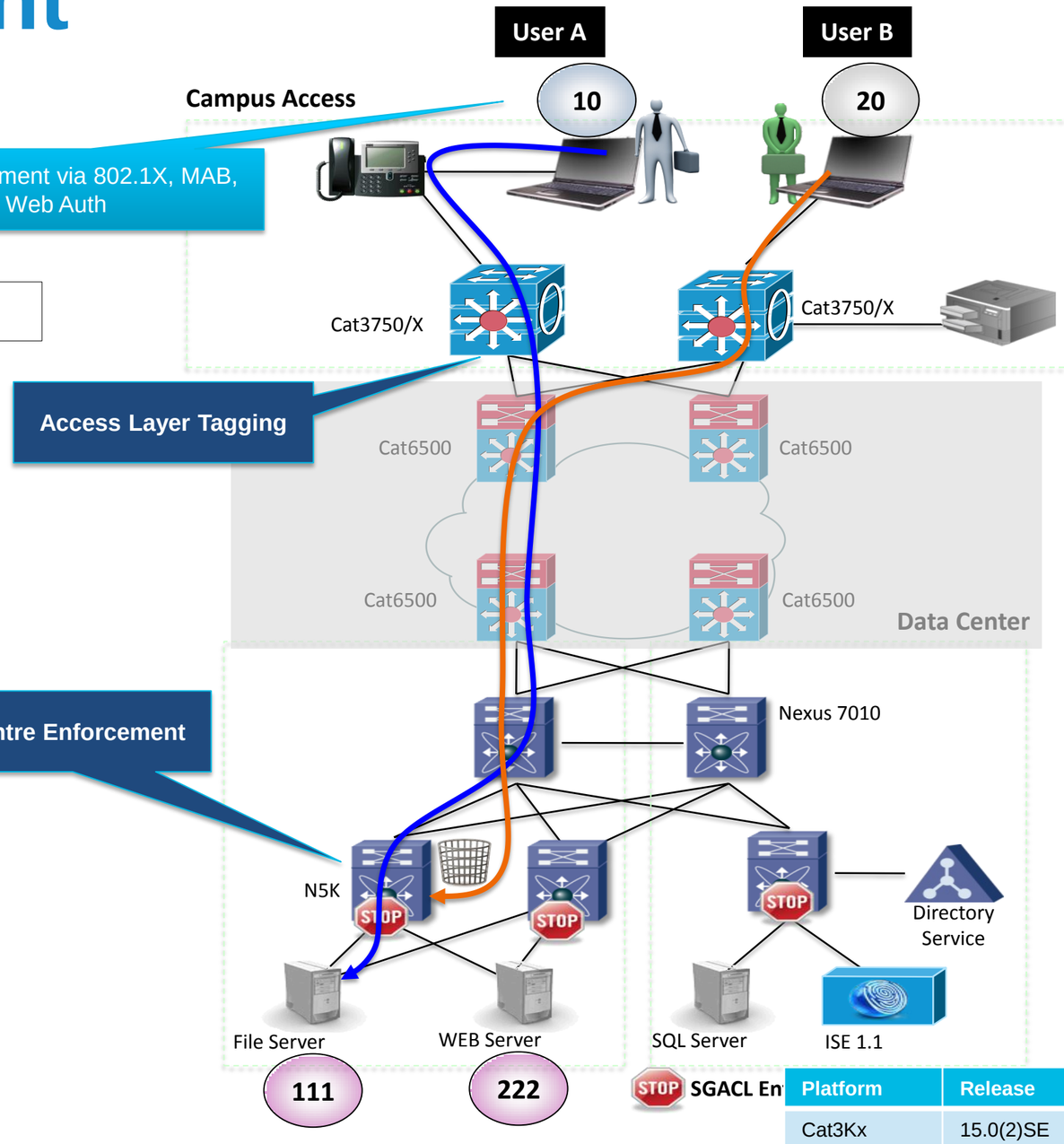
How is it done with SGA

Use Case

Campus users accessing resources in Data Centre

- User traffic SGTagged at access via 802.1X, MAB, or Web Authentication
- Server SGT assigned via static mapping
- SGTag propagated thru access, distribution to data centre
- SGACL enforcement at data centre egress switch

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



Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	Indus*
Cat6K	15.0(1)SY

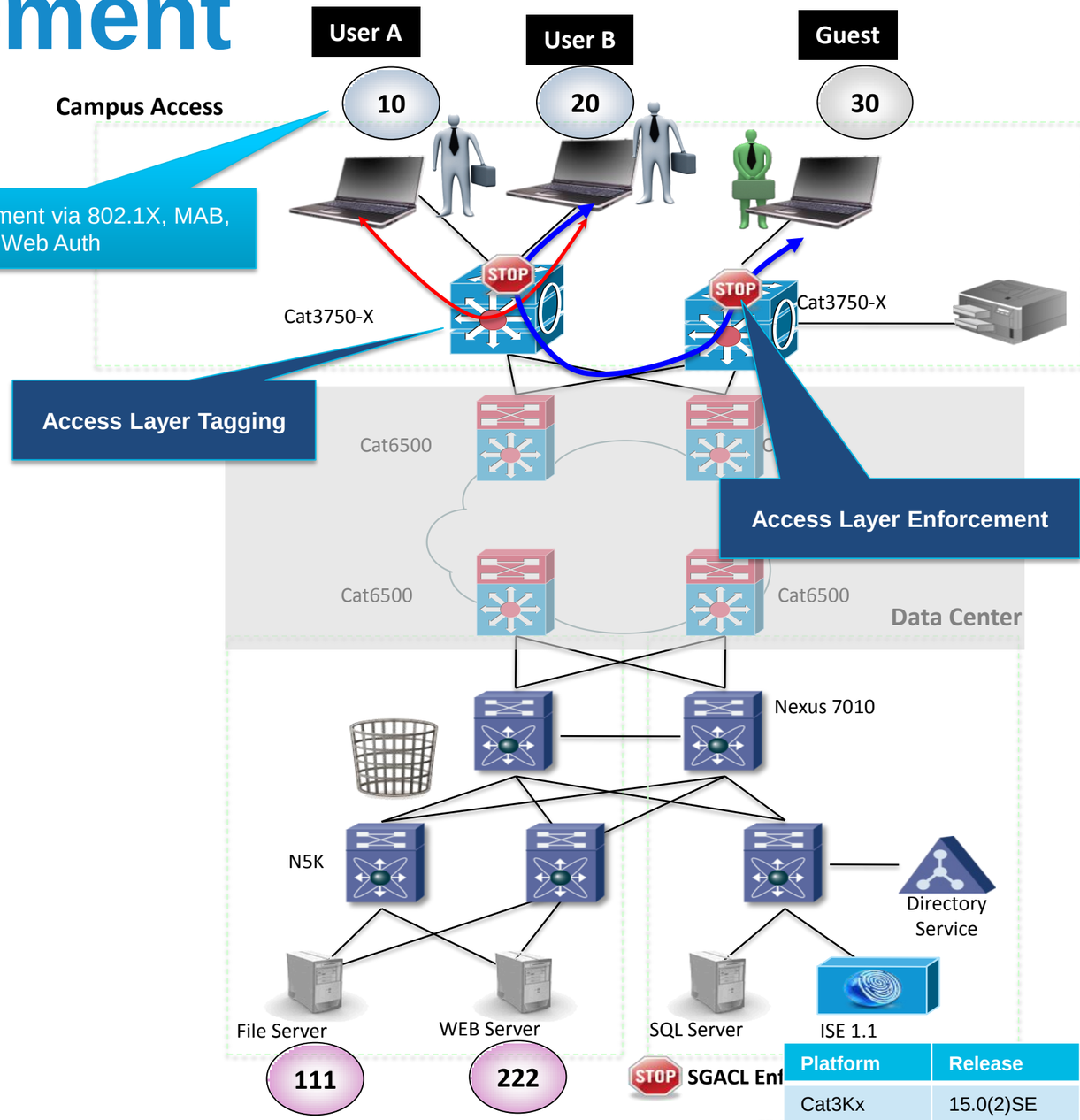
Access Layer Enforcement

Use Case

Segmentation between users/resources in campus

- User traffic SGTagged at access via 802.1X, MAB, or Web Authentication
- Resource SGTagged via 802.1X, MAB, or static mapping
- SGACL enforcement at egress access switch

SRC \ DST	User A (10)	User B (20)	Guest (30)
User A (10)	Permit all	Deny all	Deny all
User B (20)	Deny all	Permit all	Deny all
Guest (30)	Deny all	Deny all	Permit all



Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	Indus*
Cat6K	15.0(1)SY

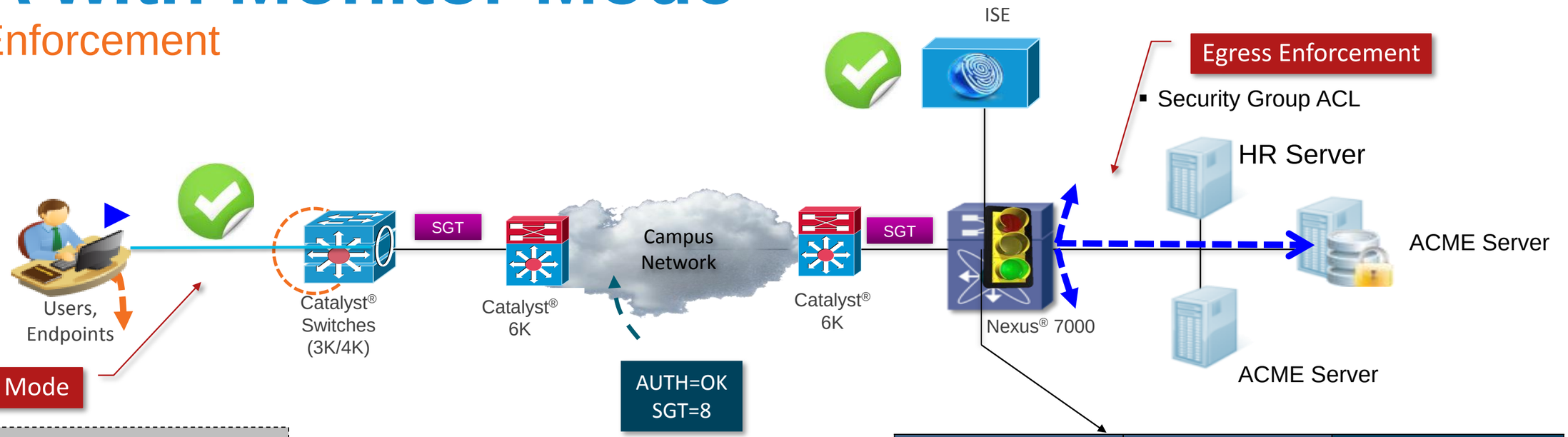
Campus Migration Path

Challenges Migrating to a TrustSec Network

- End device authentication
  - Different authentication mechanisms for device types
  - Multiple devices per per port
- Network device authentication
  - Prevent malicious or accidental changes in the network
- Partial support of TrustSec features in network devices
  - Many features require new or specific hardware

SGA with Monitor Mode

Zero Enforcement



authentication port-control auto

authentication open

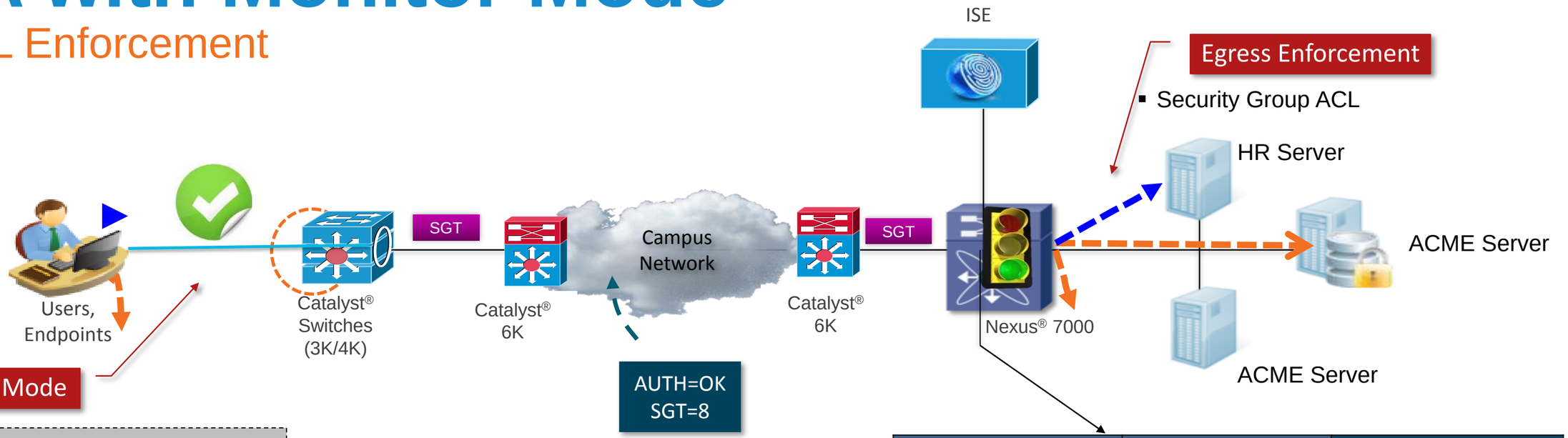
dot1x pae authenticator

SRC \ DST	HR Server (111)	ACME Server (222)
ACME-User(8)	Permit all	Permit all
HR-User (10)	Permit all	Permit all
Unknown (0)	Permit all	Permit 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 traverses to Data Centre and hits SGACL at egress enforcement point
5. All traffics are permitted with SGACL. No impact to the user traffic

SGA with Monitor Mode

SGACL Enforcement



authentication port-control auto

authentication open

dot1x pae authenticator

SRC \ DST	HR Server (111)	ACME Server (222)
ACME-User(8)	Deny all	Permit all
HR-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 traverses to Data Centre and hits SGACL at egress enforcement point
5. Only permitted traffic path (source SGT to destination SGT) is allowed

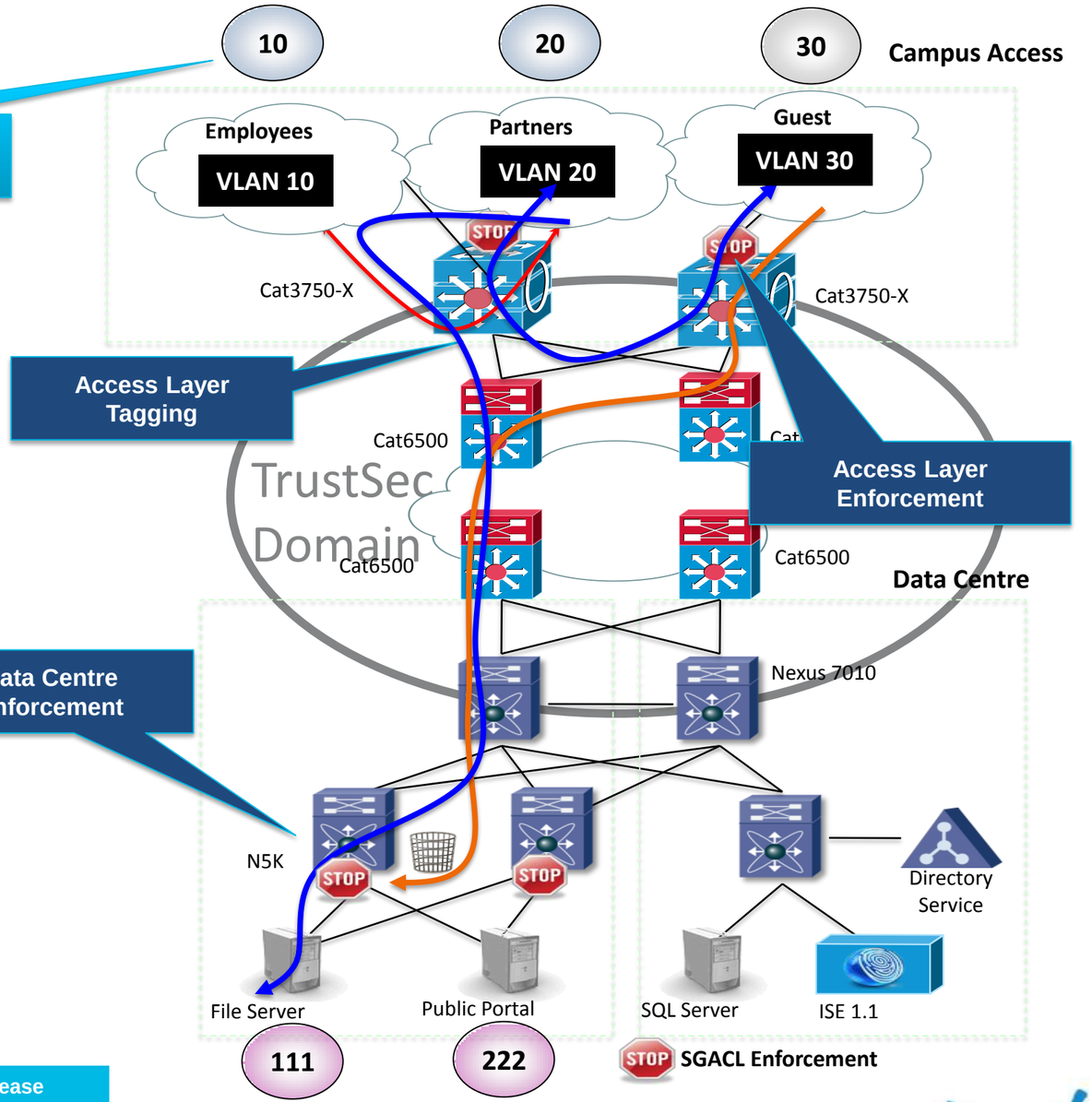
VLAN-to-SGT Mapping

SGT Assignment via VLAN-to-SGT mapping

Use Case

Migration path – VLAN-to-SGT mapping

- Source SGT assigned via VLAN-to-SGT mapping
- Server SGT assigned via static mapping
- SGACL enforcement at access switch & data centre egress switch
- IP Device Tracking must be enabled

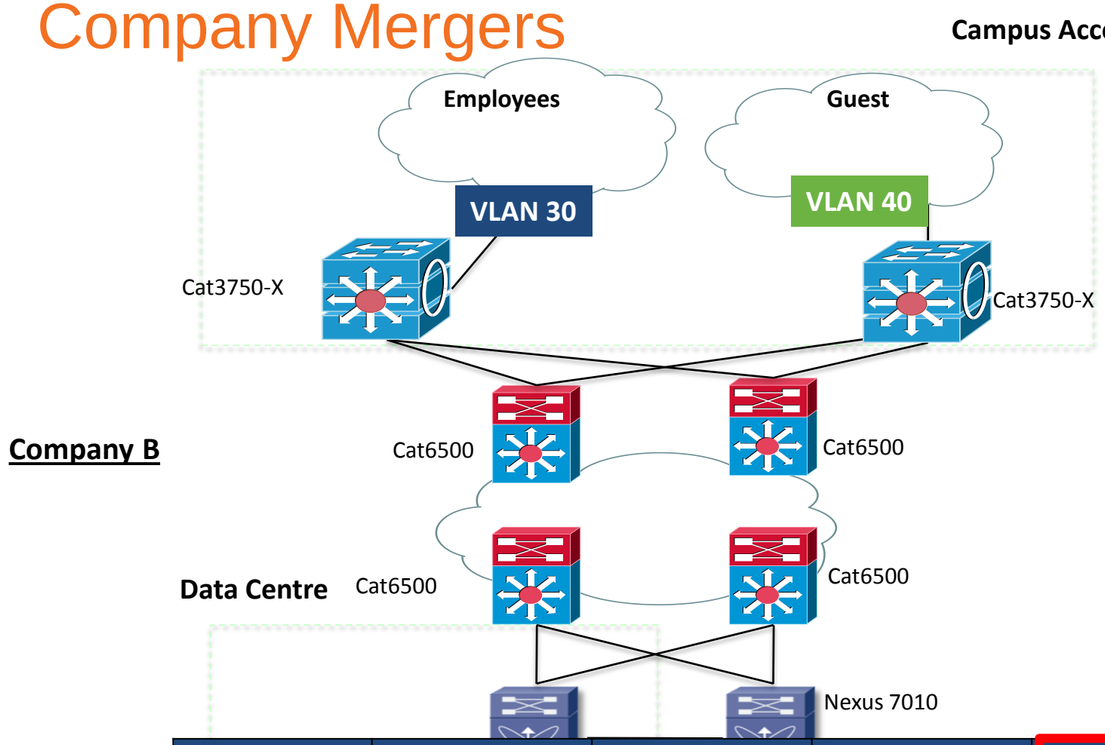


SRC(SGT) / DST(DGT)	File Server (111)	Public Portal (222)	Partners (20)	Guest (30)
Emp (10)	Permit all	Permit Web	SGACL-A	Deny all
Prtnr (20)	Permit Web	Permit Web	Deny all	Deny all
Guest (30)	Deny all	Permit Web	Deny all	SGACL-B

Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	Indus*
Cat6K	15.0(1)SY

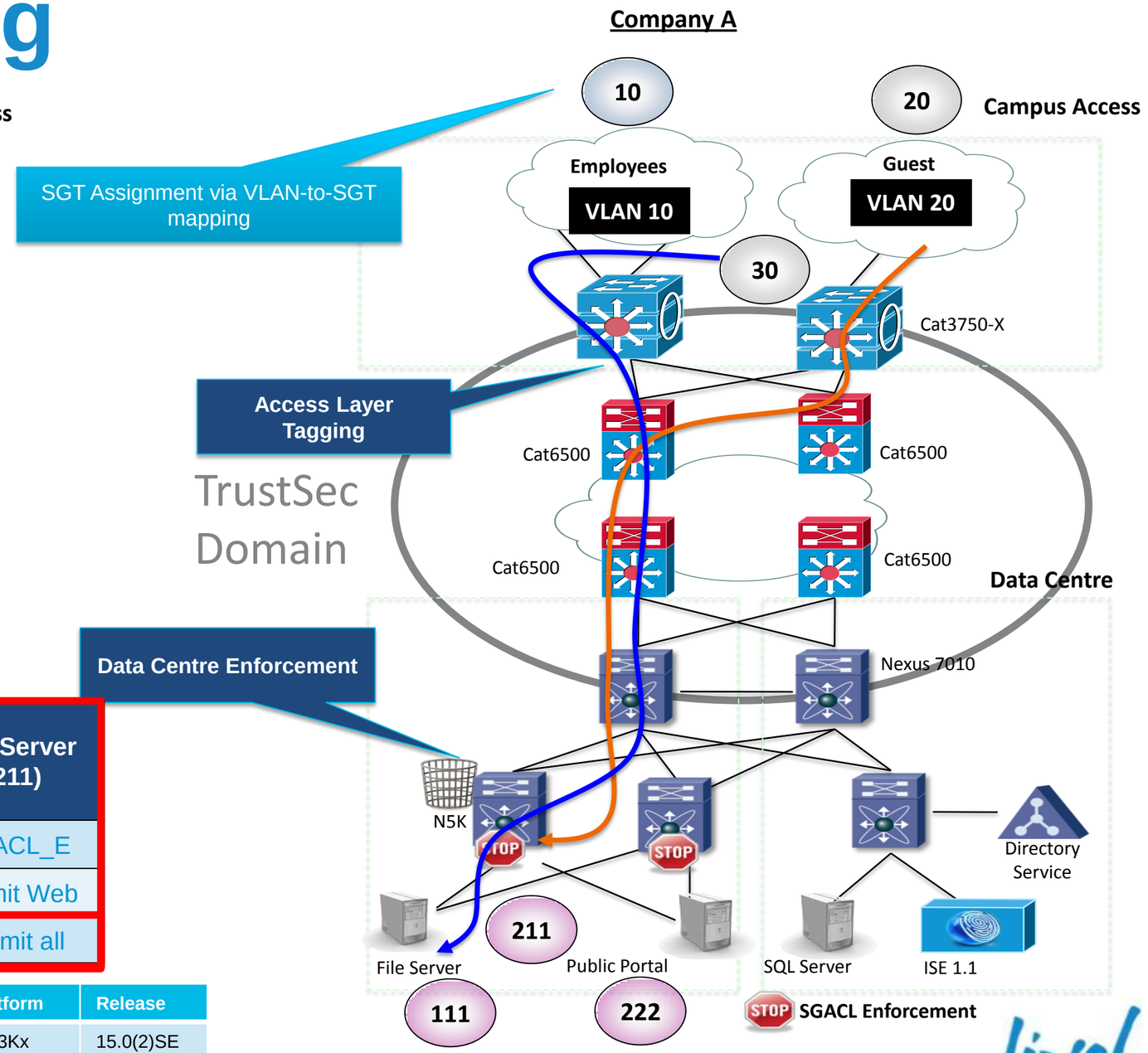
VLAN-to-SGT Mapping

Company Mergers



SRC(SGT) / DST(DGT)	File Server (111)	Public Portal (222)	Guest (30)	File Server (211)
Emp(10)	Permit all	Permit Web	Deny all	SGACL_E
Guest(20)	Deny all	Permit Web	SGACL-B	Permit Web
Emp_B(30)	Deny all	Deny all	Deny all	Permit all

Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	Indus*
Cat6K	15.0(1)SY



Subnet-to-SGT Mapping

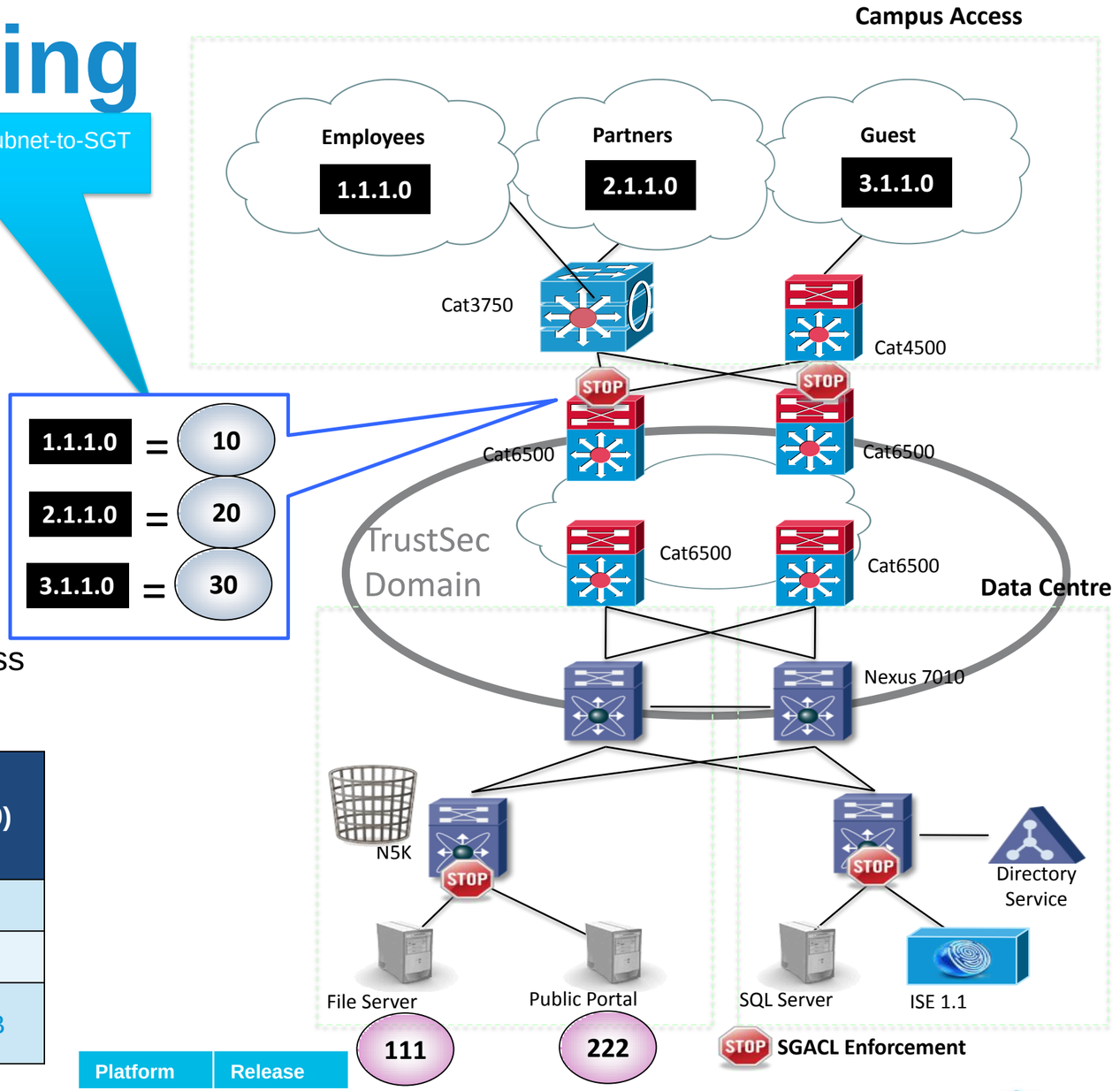
SGT Assignment via Subnet-to-SGT mapping

Use Case

Migration path – Subnet-to-SGT mapping

- Source SGT assigned via Subnet-to-SGT mapping
- Subnet bindings are static, no learning of active hosts
- Prefixes can be exported directly with SXPv3
- Server SGT assigned via static mapping
- SGACL enforcement at Dist switch & data centre egress switch

SRC(SGT) / DST(DGT)	File Server (111)	Public Portal (222)	Partners (20)	Guest (30)
Emp (10)	Permit all	Permit Web	SGACL-A	Deny all
Prtnr (20)	Permit Web	Permit Web	Deny all	Deny all
Guest (30)	Deny all	Permit Web	Deny all	SGACL-B



Platform	Release
Cat4K	Indus*
Cat6K	15.0(1)SY

IP-to-SGT Mapping

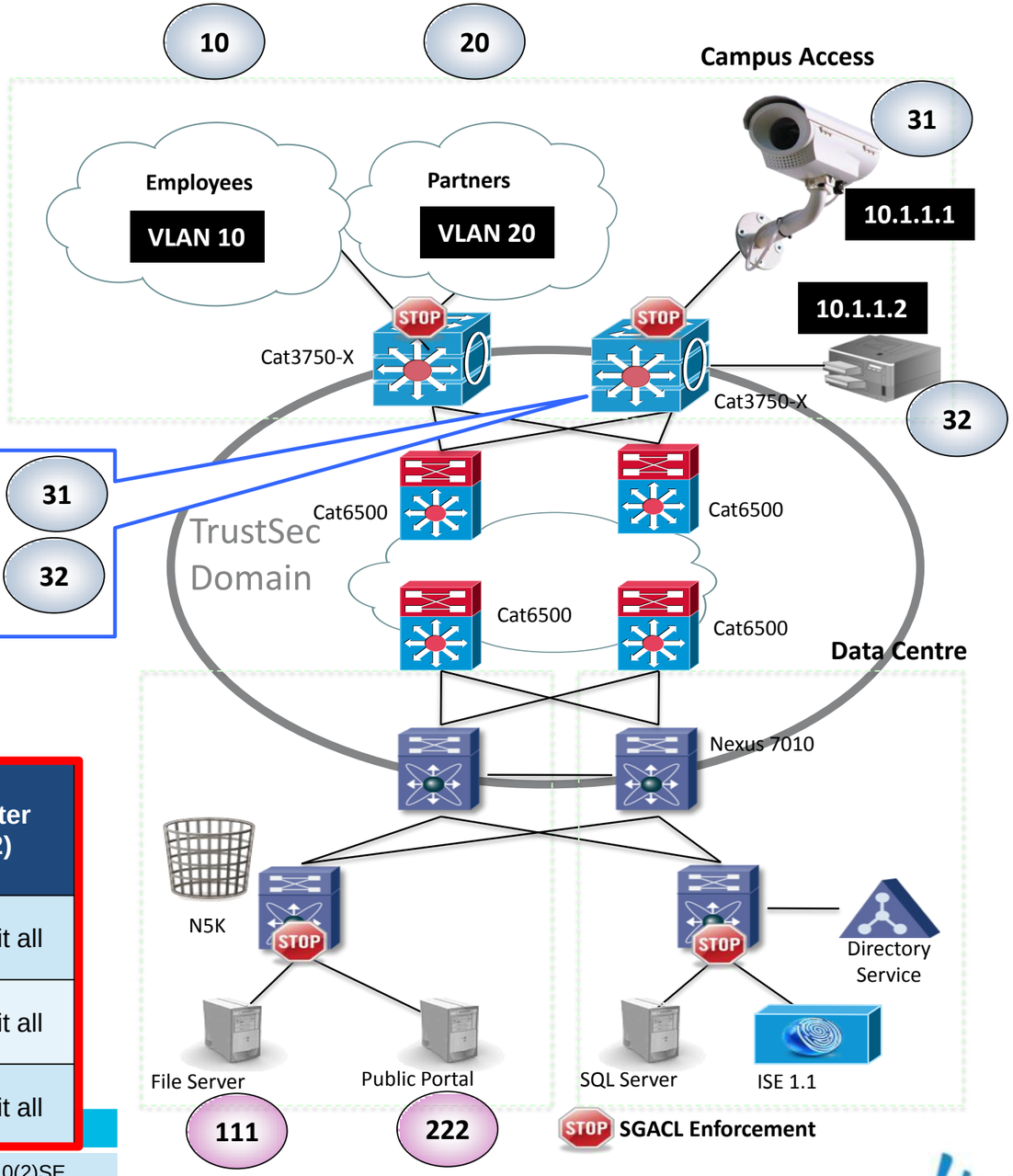
SGT Assignment via IP-to-SGT mapping

Use Case

IP-to-SGT mapping

- Source SGT assigned via IP-to-SGT mapping
- IP Device Tracking must be enabled
- Typically used for statically assigned IP devices
- Server SGT assigned via static mapping
- SGACL enforcement at access switch & data centre egress switch

10.1.1.1	=	31
10.1.1.2	=	32



SRC(SGT) / DST(DGT)	File Server (111)	Public Portal (222)	Partners (20)	Guest (30)	IPSVC (31)	Printer (32)
Emp (10)	Permit all	Permit Web	SGACL-A	Deny all	Permit all	Permit all
Prtnr (20)	Permit Web	Permit Web	Deny all	Deny all	Deny all	Permit all
Guest (30)	Deny all	Permit Web	Deny all	SGACL-B	Deny all	Permit all

Cat3Kx	15.0(2)SE
Cat4K	Indus*
Cat6K	15.0(1)SY

Port-to-SGT Mapping

SGT Assignment via Port-to-SGT mapping

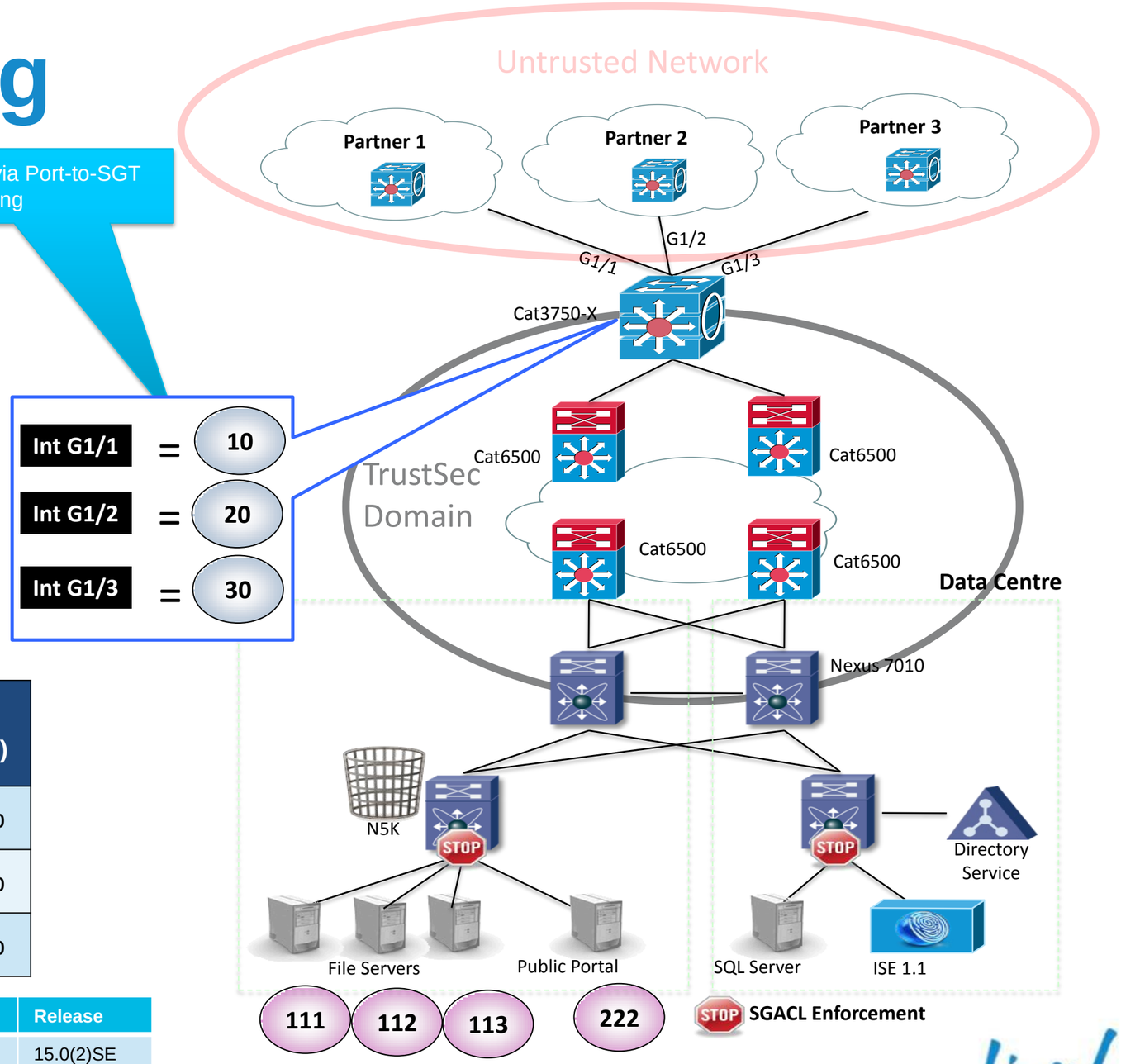
Use Case

Port-to-SGT mapping

- Source SGT assigned via Port-to-SGT mapping
- Typically used when connected to untrusted switches
- Server SGT assigned via static mapping
- SGACL enforcement at data centre switch

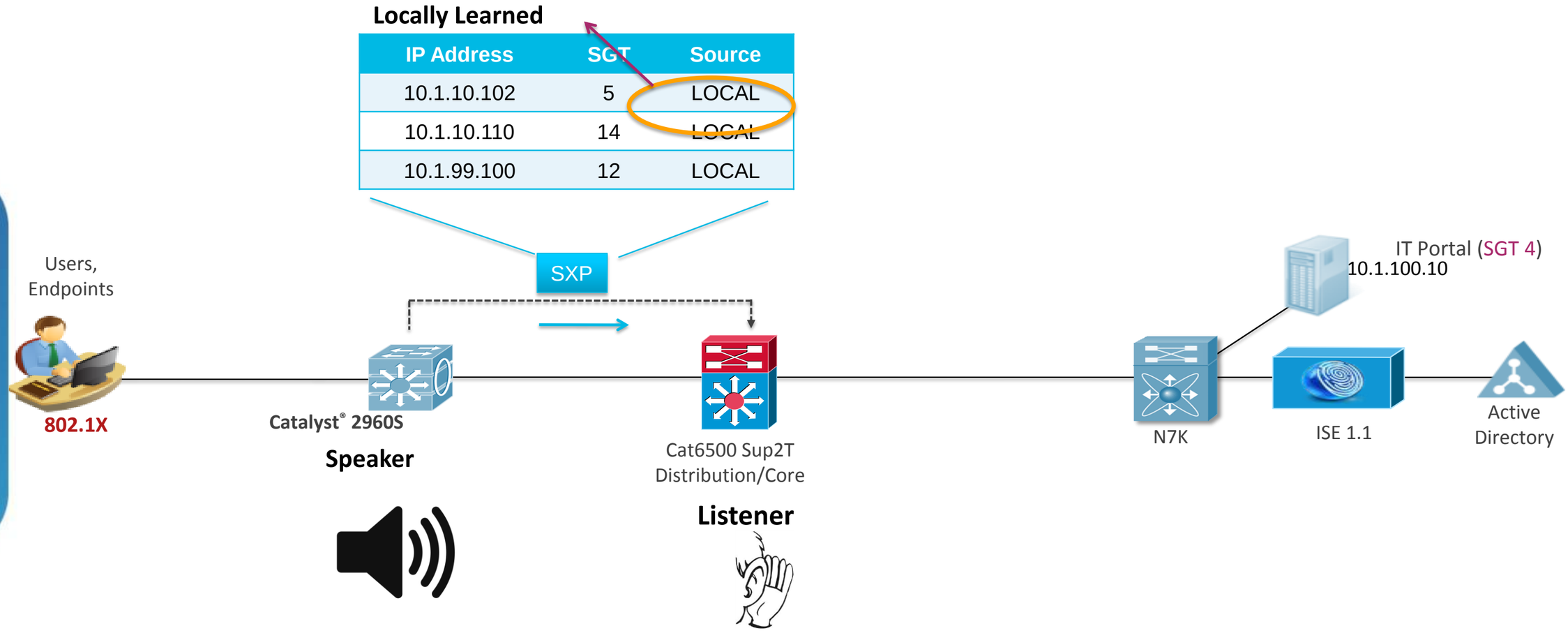
SRC(SGT) / DST(DGT)	File Server (111)	File Server (112)	File Server (113)	Public Portal (222)
Prtnr1 (10)	**Permit all**	Deny all	Deny all	Permit Web
Prtnr2 (20)	Deny all	**Permit all**	Deny all	Permit Web
Prtnr3 (30)	Deny all	Deny all	**Permit all**	Permit Web

Platform	Release
Cat3Kx	15.0(2)SE
Cat4K	Indus*
Cat6K	15.0(1)SY



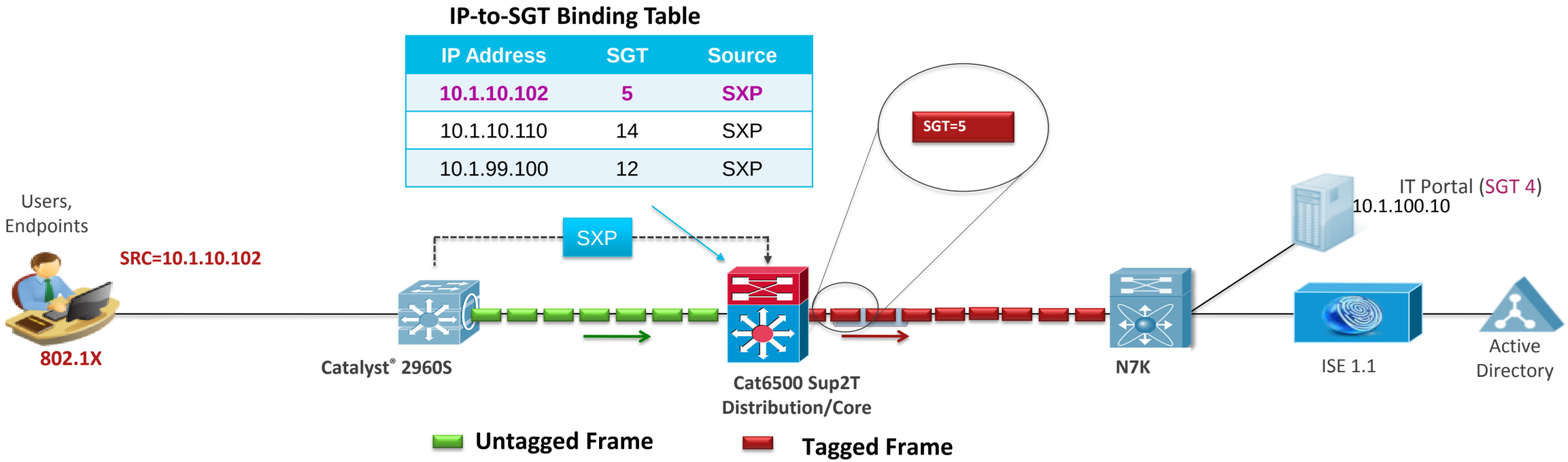
What if Scenarios

What if my Access Switch isn't capable of SGTagging



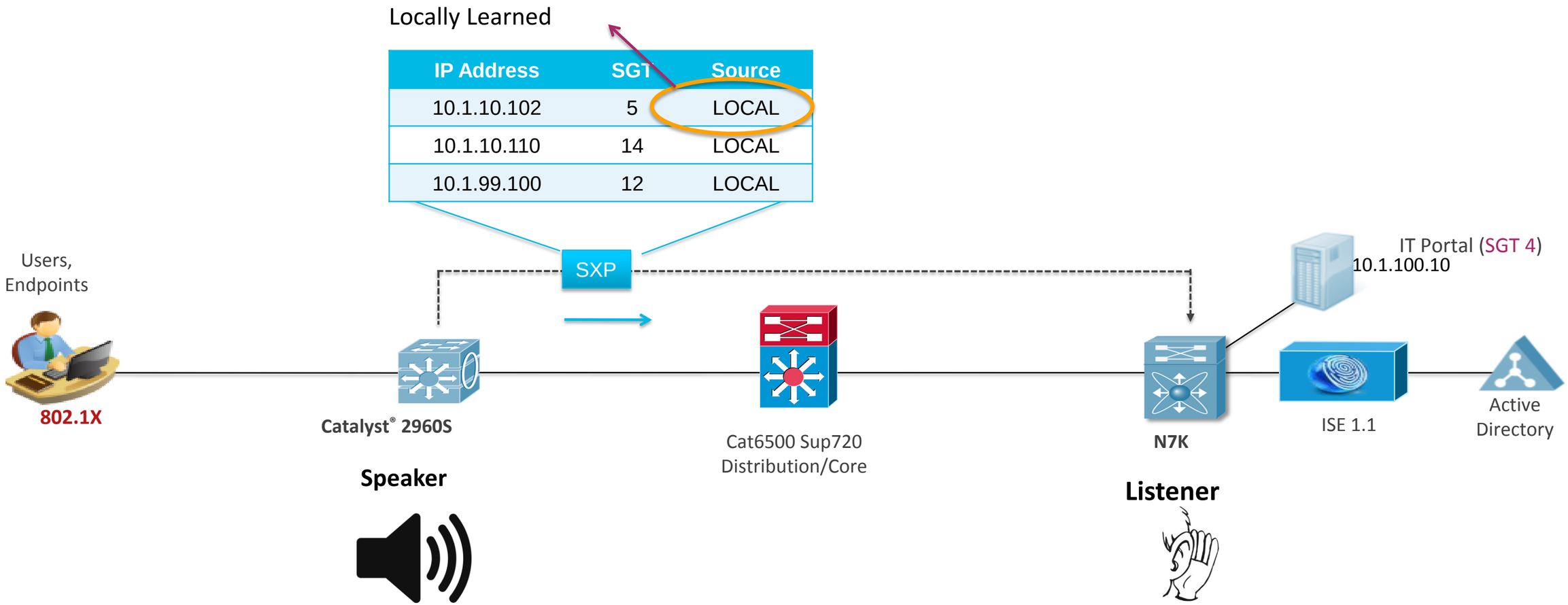
If the switch supports SXP, switch can send IP-to-SGT binding table to SGT capable device (e.g. Catalyst 6500 with Sup2T)

SGTagging based on SXP



When SGT capable device receives packet, it looks up SGT value in table, insert SGT tag to frame when it exits egress port

What if my Dist/Core Switch isn't Capable of SGTagging



If the switch supports SXP, switch can send IP-to-SGT binding table to SGT capable device (e.g. Nexus 7K)

What if I Received Multiple SGT Assignments

SGT Assignment Priorities

The current priority enforcement order, from highest to lowest:

INTERNAL—Bindings between locally configured IP addresses and the device own SGT

LOCAL—Bindings of authenticated hosts which are learned via IPM and device tracking. This type of binding also include individual hosts that are learned via ARP snooping on L2 [I]PM configured ports.

IP_ARP—Bindings learned when tagged ARP packets are received on a CTS capable link.

SXP—Bindings learned from SXP peers.

New

Layer 3 Interface—(L3IF) Bindings added due to FIB forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or Identity Port Mapping on routed ports.

CLI— Address bindings configured using the IP-SGT form of the cts role-based sgt-map global configuration command. (Hosts and subnets)

VLAN—Bindings learned from snooped ARP packets on a VLAN that has VLAN-SGT mapping configured.

SGT Transport over non-TrustSec Domain

Use Case

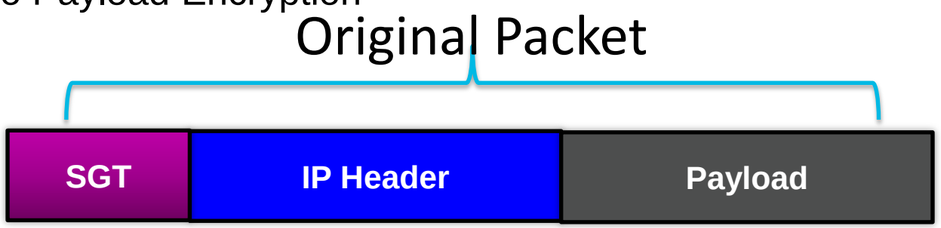
Connecting TrustSec Domains – L3 SGT Transport

Challenge

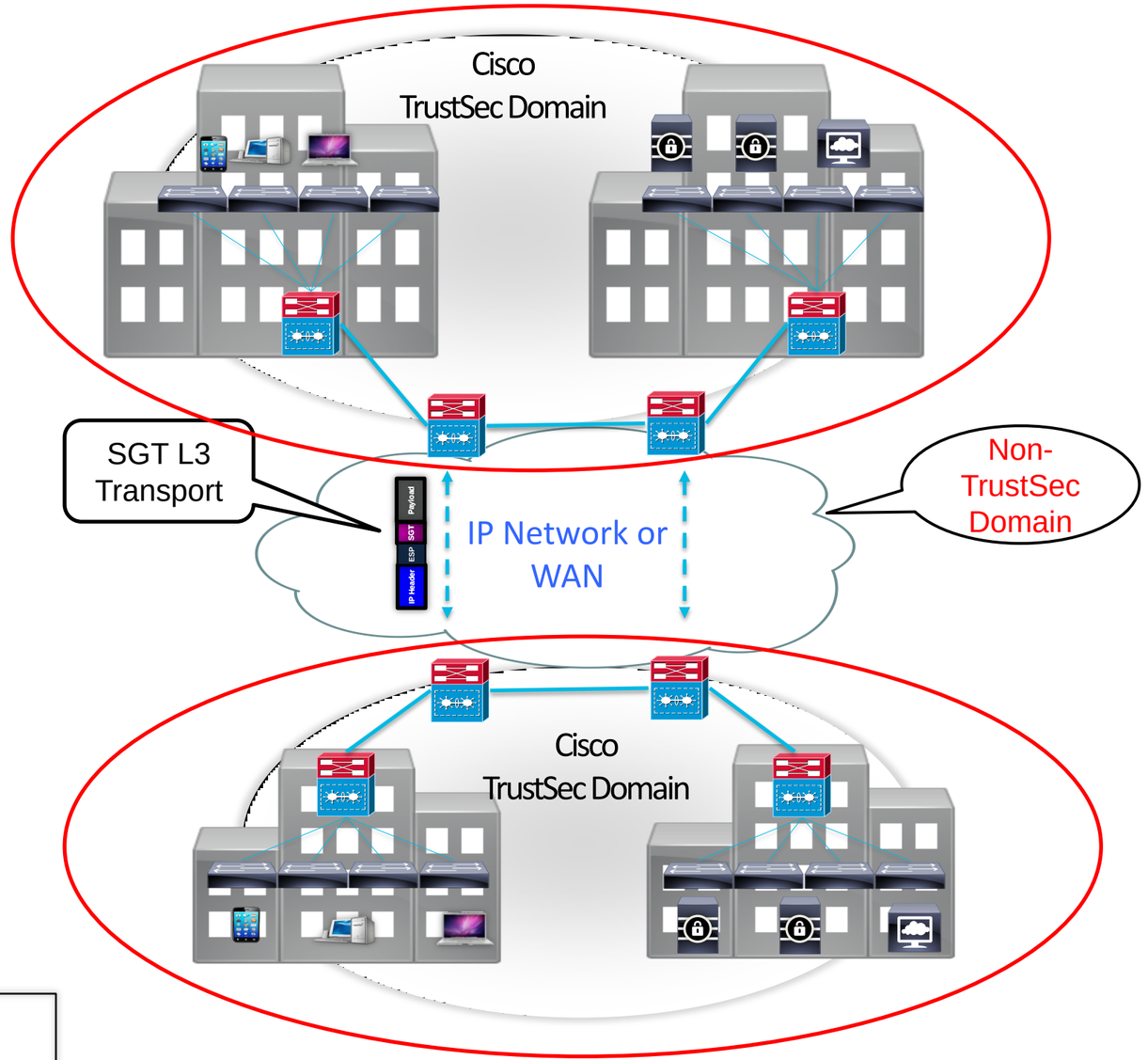
- Partial TrustSec infrastructure support

Solution

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



ESP – Encapsulating Security Payload



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

Platform	Release
Cat6K (Sup2T)	15.0(1)SY

Sup2T SGT L3 Transport

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

Configure L3 Transport on the interface

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

Policy for allowed Traffic

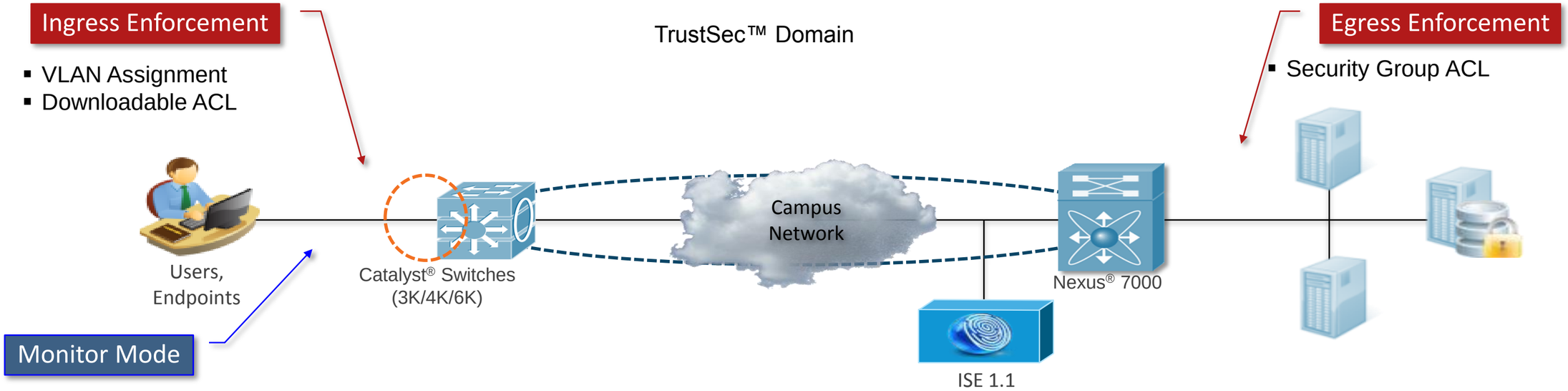
```
ip access-list extended l3-cts-policy
permit ip any 171.71.0.0/16
permit ip any 171.72.0.0/16
permit ip any 171.73.0.0/16
!
cts policy layer3 ipv4 traffic l3-cts-policy
```

Policy to for exception traffic

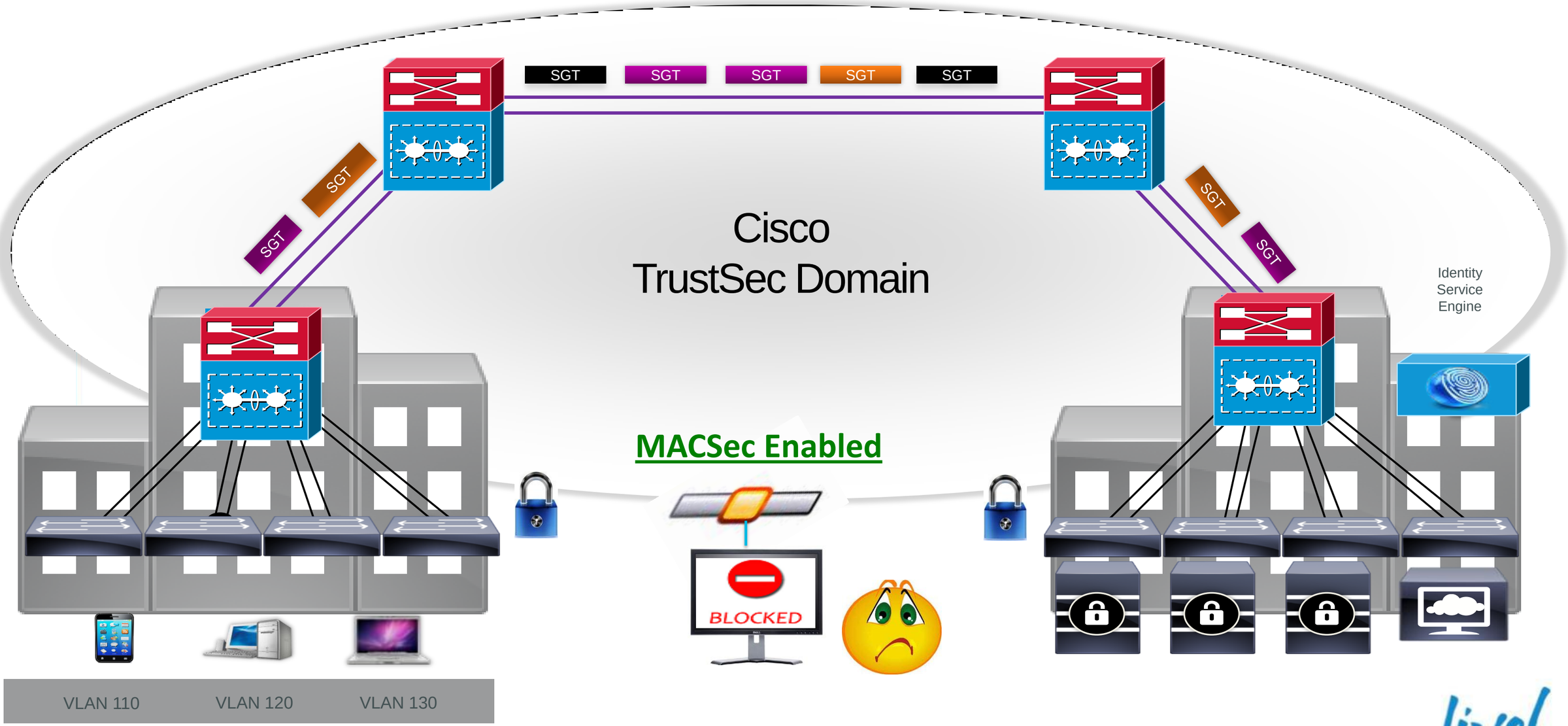
```
ip access-list extended l3-cts-exception
permit ip any 171.74.0.0/16
permit ip any 171.75.0.0/16
permit ip any 171.76.0.0/16
!
cts policy layer3 ipv4 exception l3-cts-policy
```

TrustSec: Best Practices

SGA and Monitor Mode

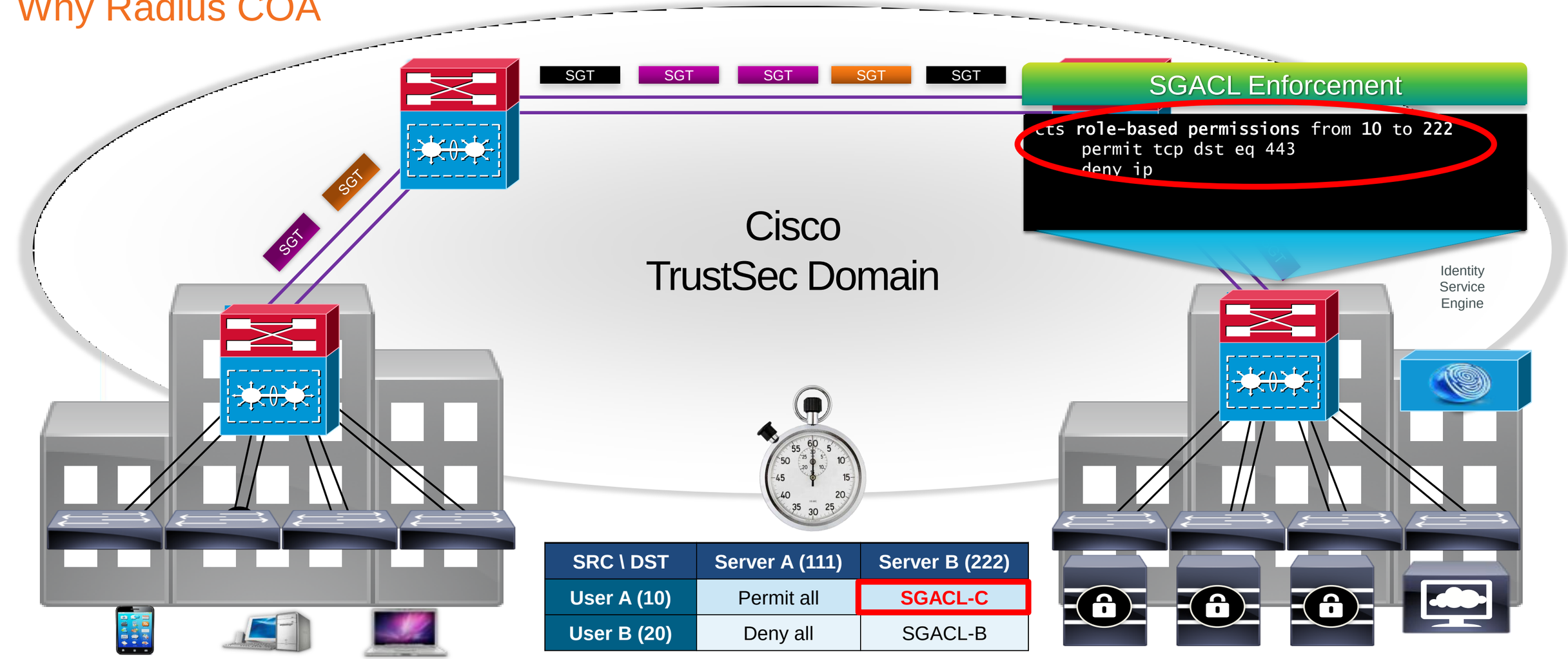


MACSec and SGA



SGA and RADIUS COA

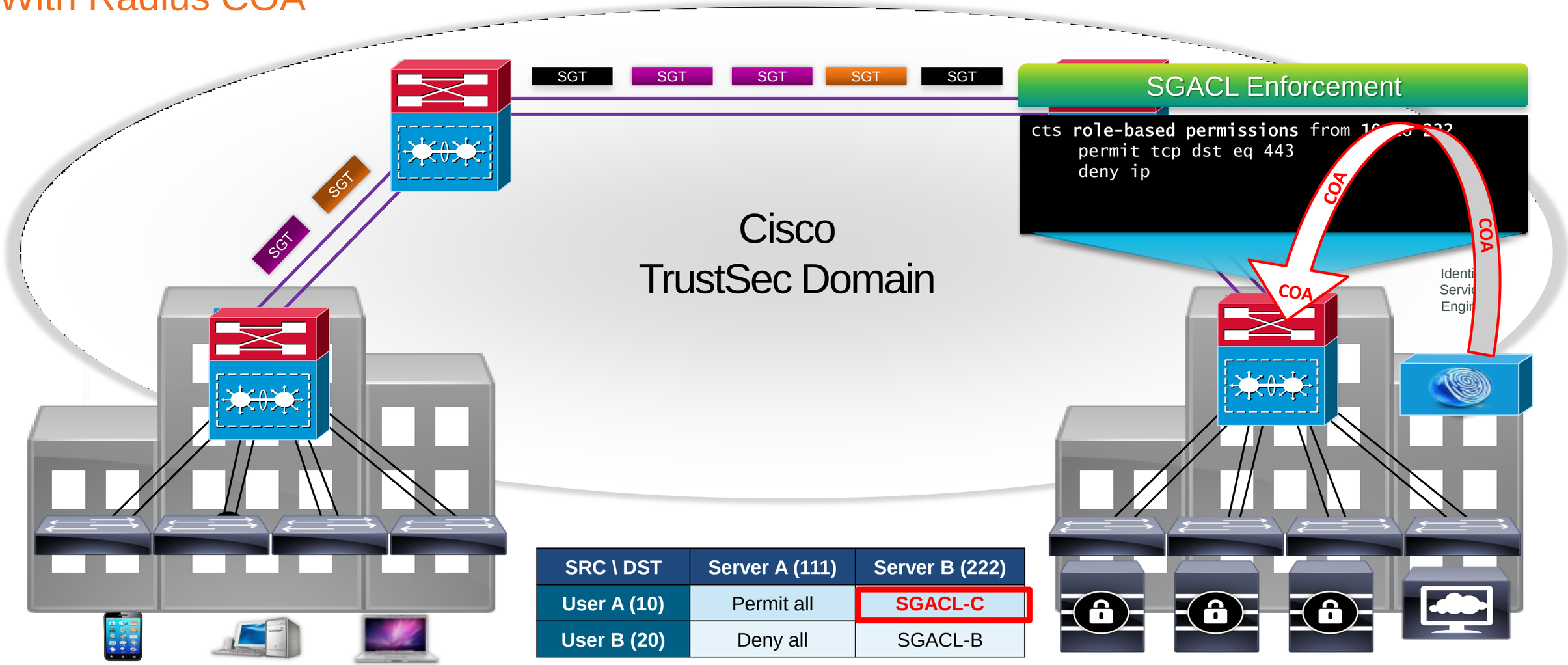
Why Radius COA



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

SGA and RADIUS COA

With Radius COA

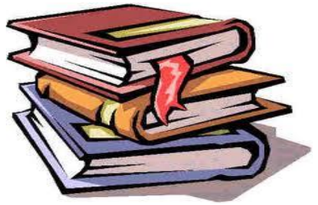


SRC \ DST	Server A (111)	Server B (222)
User A (10)	Permit all	SGACL-C
User B (20)	Deny all	SGACL-B

How to Deploy SGA

How To Deploy NDAC

NDAC – Seed Device Switch Configurations



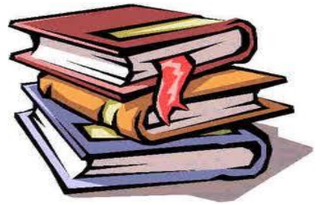
Configuration Commands:

```
aaa new-model
radius server ise
 address ipv4 <ip address> auth-port 1812 acct-port 1813
 pac key <password>
aaa authentication dot1x default group radius
aaa authorization network cts group radius
aaa session-id common
cts authorization list cts
dot1x system-auth-control
!
Interface t5/1
switchport mode trunk
cts dot1x
!
<exec mode> cts credentials id <userid> password <password>
```

Seed device includes RADIUS info

How To Deploy NDAC

NDAC – Non-Seed Device Switch Configurations

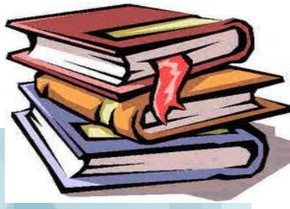


Configuration Commands:

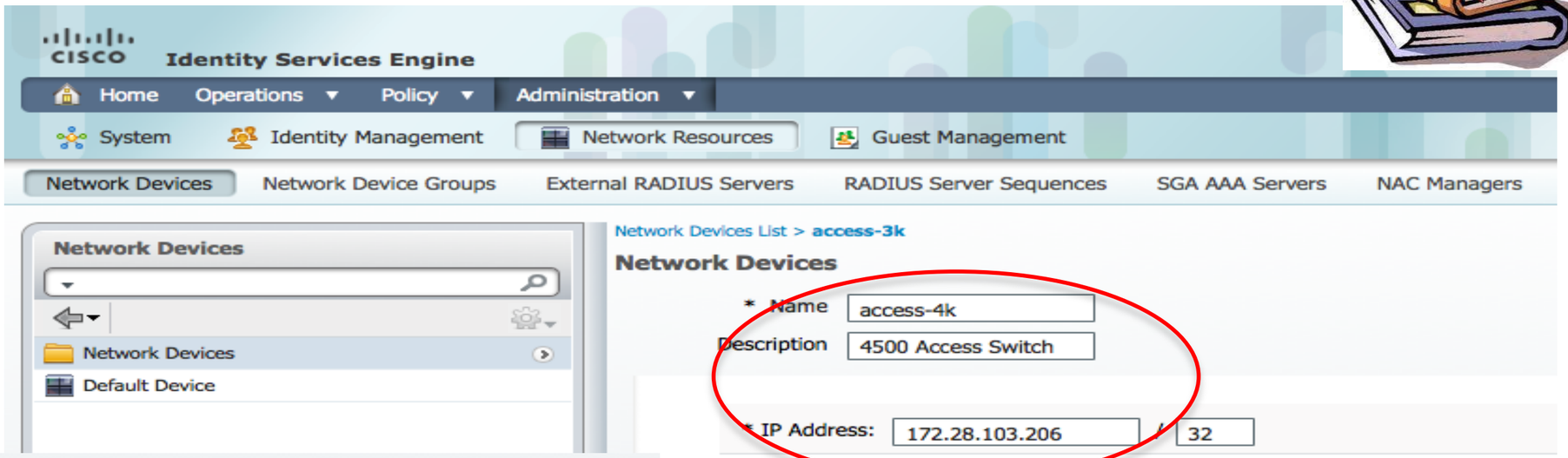
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa session-id common
dot1x system-auth-control
!
Interface t5/1
switchport mode trunk
cts dot1x
!
<exec mode> cts credentials id <userid> password <password>
```

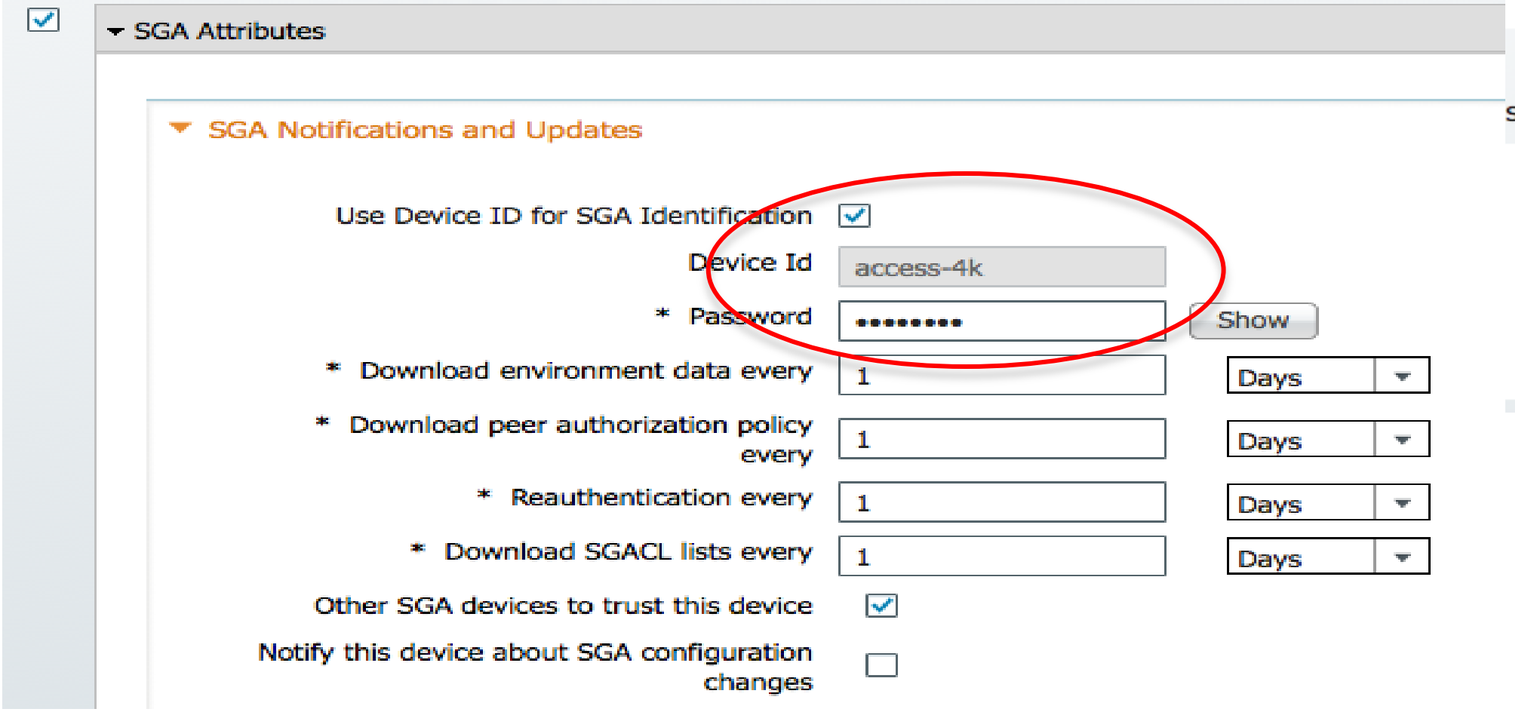
- ✓ Non-Seed device need not include RADIUS info
- ✓ Dynamically learns RADIUS info from Seed Device

Configuring Network Device Admission Control (NDAC) on ISE



Administration > Network Resources > Network Devices





SGT Assignment for Roles

Doctor (SGT 7)

IT Admin (SGT 6)

Users,
Endpoints

802.1X, MAB, LWA

Catalyst® 3750-X

Catalyst 6K
Core

Nexus® 7000
Distribution

Catalyst® 4948

ISE 1.1

Static
SGT Assignment
For
Servers

IT Portal (SGT 4)
10.1.100.10

Dynamic
SGT Assignment
For
Endpoint

Public Portal (SGT 8)
10.1.200.10

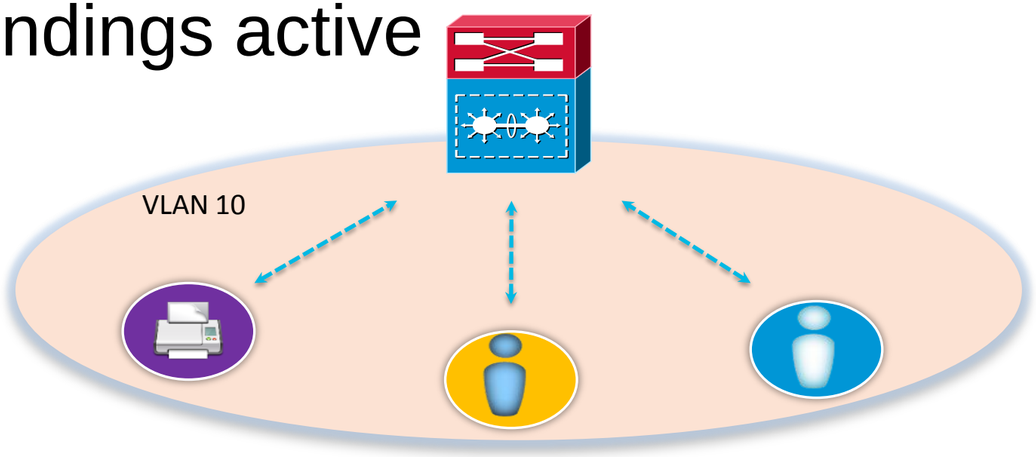
Internal Portal (SGT 9)
10.1.200.200

Patient Record DB (SGT 10)
10.1.200.100

VLAN to SGT Mapping

VLAN to SGT mapping uses IP Device Tracking mechanism to dynamically create IP to SGT bindings per VLAN

Once bindings are created IP device tracking uses periodic ARP Probe messages to keep IP to SGT bindings active




```
ip device tracking
!
cts role-based sgt-map vlan-list 10 sgt 10
cts role-based sgt-map vlan-list 20 sgt 20
cts role-based sgt-map vlan-list 30 sgt 30
cts role-based sgt-map vlan-list 40 sgt 40
cts role-based sgt-map vlan-list 200 sgt 200
```

```
SJC01#show cts role-based sgt-map summary

IP-SGT Active Bindings Summary
============================================
Total number of VLAN      bindings = 1012
Total number of CLI       bindings = 1
Total number of active    bindings = 1013
```

IP Subnet to SGT Mapping

Layer 3 interface mapping to SGT (L3IF) is supported on the following L3 logical or physical interfaces:

Routed port

SVI (VLAN interface)

L3 subinterface of L2 port

Tunnel interface

SGT-MAP CLI Example

```
cts role-based sgt-map 192.168.10.0/24 sgt 10
cts role-based sgt-map 192.168.20.0/24 sgt 20
cts role-based sgt-map 192.168.30.0/24 sgt 30
cts role-based sgt-map 192.168.40.0/24 sgt 40
cts role-based sgt-map 192.168.200.0/24 sgt 200
```

- Dynamically adds Destination Group Tag (DGT) to the FIB entries matching the SGT-MAP configured prefixes

```
SJC01#show platform hardware cef 192.168.10.10 detail
Codes: M - mask entry, V - value entry, A - adjacency index, NR- no_route bit
       LS - load sharing count, RI - router_ip bit, DF: default bit
       CP - copy_to_cpu bit, AS: dest_AS_number, DGTv - dgt_valid bit
       DGT: dgt/others value

Format:IPV4 (valid class vpn   prefix)
M(682    ):   1     F    3FFF 255.255.255.255
V(682    ):   1     0    0    192.168.10.10
                              (A:147497, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:1, DGT:10)
SJC01#
```

Sup2T SGT L3 Transport

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

Configure L3 Transport on the interface

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

Policy for allowed traffic

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

Policy for exception traffic

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

Monitoring SGT Mapping

```
SJC01#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address               SGT     Source
============================================
192.168.10.0/24           10     CLI
192.168.20.0/24           20     CLI
192.168.30.0/24           30     CLI
192.168.40.0/24           40     CLI
192.168.200.0/24         200     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI       bindings = 5
Total number of active    bindings = 5

SJC01#
```

```
SJC01#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address               SGT     Source
============================================
192.168.10.2              10     VLAN
192.168.10.3              10     VLAN
192.168.10.4              10     VLAN
192.168.10.5              10     VLAN
192.168.10.6              10     VLAN
192.168.10.7              10     VLAN
192.168.10.8              10     VLAN
192.168.10.9              10     VLAN
192.168.10.10             10     VLAN
192.168.10.11             10     VLAN
……
```

Monitoring SGACL Packet Drops with CLI

```
SJC01#show cts role-based permissions
IPv4 Role-based permissions from group 10 to group 200 (configured):
        rbac1
IPv4 Role-based permissions from group 20 to group 200 (configured):
        rbac1
IPv4 Role-based permissions from group 30 to group 200 (configured):
        rbac1
IPv4 Role-based permissions from group 40 to group 200 (configured):
        rbac1
SJC01#
```

```
SJC01#show ip access-lists rbac1
Role-based IP access list rbac1
    10 deny tcp dst eq www (104366 matches)
    20 deny tcp dst eq ftp (36402 matches)
    30 deny tcp dst eq ftp-data (232 matches)
SJC01#
```

Monitoring SGACL Packet Drops with Flexible Netflow

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

flow exporter EXP1
 destination 10.2.44.15
 source GigabitEthernet3/1

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

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

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

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

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

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

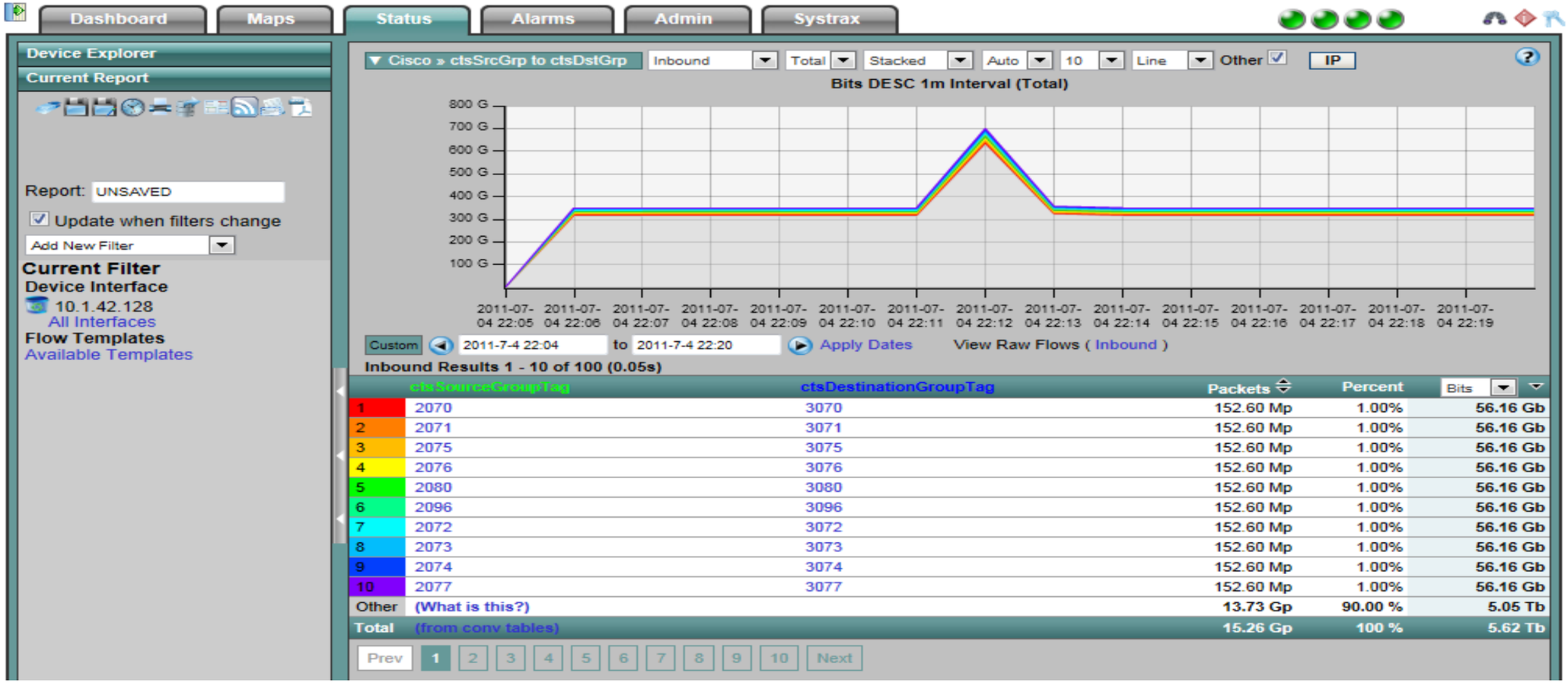
*Optional – will create flows for only Role-based ACL drops

Monitoring SGACL Packet Drops with Flexible Netflow

```
SJC01#show flow mon cts-mon cache
  Cache type:                                 Normal
  Cache size:                                   4096
  Current entries:                              1438
  High Watermark:                               1632
  Flows added:                                 33831
  Flows aged:                                  32393
    - Active timeout      (  1800 secs)            0
    - Inactive timeout    (    15 secs)        32393
    - Event aged                                    0
    - Watermark aged                                0
    - Emergency aged                                0

IPV4 SOURCE ADDRESS:              192.168.30.209
IPV4 DESTINATION ADDRESS:         192.168.200.156
TRNS SOURCE PORT:                 60952
TRNS DESTINATION PORT:            80
FLOW DIRECTION:                   Output
FLOW CTS SOURCE GROUP TAG:        30
FLOW CTS DESTINATION GROUP TAG:   200
IP PROTOCOL:                      6
counter bytes:                    56
counter packets:                  1

IPV4 SOURCE ADDRESS:              192.168.20.140
IPV4 DESTINATION ADDRESS:         192.168.200.104
TRNS SOURCE PORT:                 8233
TRNS DESTINATION PORT:            80
FLOW DIRECTION:                   Output
FLOW CTS SOURCE GROUP TAG:        20
FLOW CTS DESTINATION GROUP TAG:   200
IP PROTOCOL:                      6
counter bytes:                    56
counter packets:                  1
```

Monitoring SGT Traffic with Netflow

Plixer collector displays SGT information



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

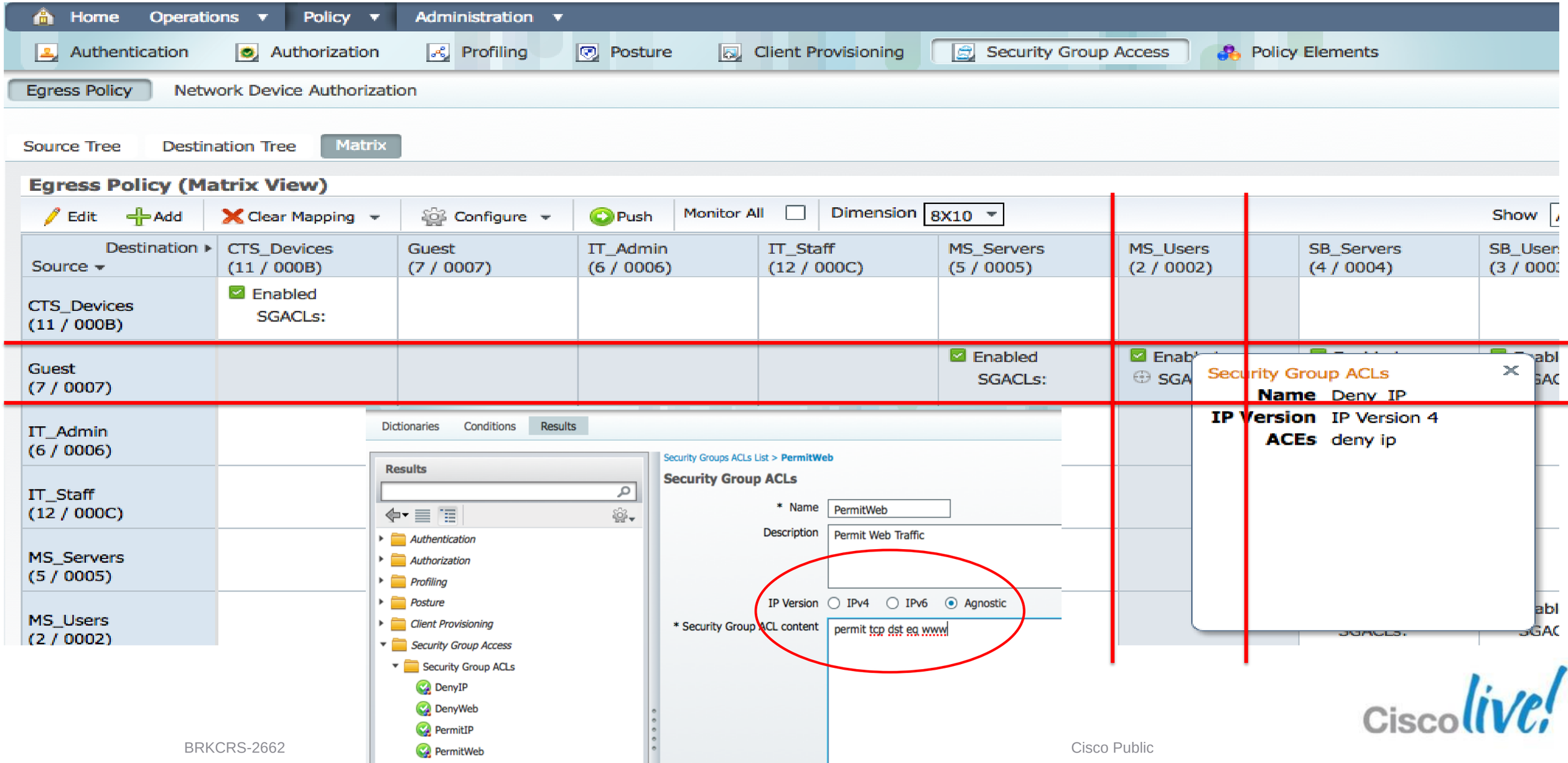
How To Create SGA Policy

Source SGT \ Destination SGT	Public Portal (SGT 8)	Internal Portal (SGT 9)	IT Portal (SGT 4)	Patient Record DB (SGT 10)
 Doctor (SGT 7)	Web	Web	No Access	Web File Share
 IT Admin (SGT 6)	We SSH RD File Sh		ccess	SSH RDP File Share

IT Maintenance 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
deny ip
```

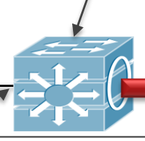
Configuring Security Group ACLs on ISE

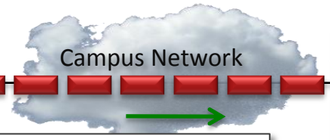


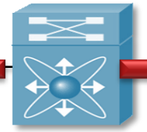
Security Group based Access Control

How Enforcement Works

```
Access-3K#show cts role-based permissions
IPv4 Role-based permissions default:
      Permit IP-00
IPv4 Role-based permissions from group 11:CTS_Devices to group
11:CTS_Devices:
      Permit_IP-30
IPv4 Role-based permissions from group 2:MS_Users to group
3:SB_Users:
      deny_ip
IPv4 Role-based permissions from group 10 to group 103 (configured):
      permit_web
Access-3K#
```







Catalyst 6K
Core

Nexus® 70
Distributi

```
Access-3K#show cts environment-data
CTS Environment Data
====================
<snip>
Security Group Name Table:
 0001-30 :
   0-7f:Unknown
   2-7f:MS_Users
   3-7f:SB_Users
   4-7f:IT_Portal
   5-7f:MS_Servers
   6-7f:IT_Admin
   7-7f:Guest
   9-7f:Internal_Portal
   11-7f:CTS_Devices
```

Public Portal (SGT 8)

10.1.200.10

agged Frame

10.1

```
CTS7K-DC# show cts role-based counters sgt 5

RBACL policy counters enabled
Counters last cleared: 04/20/2010 at 11:20:58 PM

sgt:5 dgt:4    [1555]
rbacl:Permit IP
      permit ip      [1555]

sgt:5 dgt:8    [1483]
rbacl:Permit IP
      permit ip      [1483]

sgt:5 dgt:9    [1541]
rbacl:Permit IP
      permit ip      [1541]

sgt:5 dgt:10   [1804]
rbacl:IT_Maintenance_ACL
      permit tcp dst eq 20 log       [0]
      permit tcp dst eq 21 log       [3]
      permit tcp dst eq 22 log       [3]
      permit tcp dst eq 445 log      [0]
      permit tcp dst eq 135 log      [0]
      permit tcp dst eq 136 log      [0]
      permit tcp dst eq 137 log      [0]
      permit tcp dst eq 138 log      [0]
      permit tcp dst eq 139 log      [0]
      permit tcp dst eq 3389 log     [251]
      permit icmp log [1547]
      deny ip [0]
```

Key Takeaways

Key Takeaways

- SGA provides easy way to manage and enforce policy in your networks
- Various mapping features enable SGA to be enabled without 802.1X
- Monitor Mode can be used with SGA for easy SGA deployment with Identity
- SGA can be deployed end-to-end today in Campus Networks

References

Cisco TrustSec

http://www.cisco.com/go/trustsec

Cisco Catalyst 6500 Series Switches
http://www.cisco.com/go/6500

Cisco Catalyst 4500 Series Switches

http://www.cisco.com/go/4500

Cisco Catalyst 3750X Series Switches

http://www.cisco.com/go/3750x

Cisco TechWise TV – Fundamentals of TrustSec

http://youtu.be/78-GV7Pz18I

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

Cisco live!