Cisco Support Community Expert Series Webcast

Introduction to Cisco Trustsec Solution and Configuration

Ankur Bajaj
Engineer, Technical Services

Dec, 16 2014

Cisco Support Community – Expert Series Webcast

- Today's featured expert is Cisco Support Engineer Ankur Bajaj
- Ask questions now about Trustsec Solution and configuration

Ankur Bajaj
Customer Support Engineer

Topic: Troubleshooting SIP in Cisco Unified communications deployments

December 16, 2014

Panelists of Expert for Question Management

Fay-Ann Lee
Technical Marketing Engineer

Beau Wallace
TAC Support Engineer

Mrinal Jaiswal
TAC Support Engineer

January Expert Series Webcast

Ayodeji Okanlawon

CISCO DESIGNATED VIP

Expert VIP Webcast: Troubleshooting SIP in Cisco Unified communications deployments

Tuesday, January 13, 2015 at 2:00pm London.

6am Pacific Standard Time, 9am Eastern

Ayodeji Okanlawon

During the webcast, Deji will discuss how the Session Initiation Protocol (SIP) is redefining our UC world. The Session Initiation Protocol (SIP) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.

Registration for this live webcast:

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=E&SEMINAR_CODE=S21888&PRIORITY_CODE=

Thank You For Joining Us Today!

If you would like a copy of the presentation slides, click the PDF file link in the chat box on the right or go to:

- https://supportforums.cisco.com/document/12372471/expert-webcast-introduction-cisco-trustsec-solution-and-configuration-ankur-bajaj

Or, https://supportforums.cisco.com/expert-corner/knowledge-sharing

Ask the Expert Events – Current /Upcoming

Application Centric Infrastructure
with Daniel Pita

Learn and ask general questions about ACI fabric bringup, basic configuration, technical operation, and some options for integrating ACI with your existing network

Ends December 19, 2014

Digital Media Suite (DMM, SNS, DMP, Edge) Configuration & Troubleshooting
with Swati Chopra

This is an opportunity to learn and ask questions about configuring and troubleshooting the Digital Media Suite (DMM, SNS, DMP, Edge) with Cisco expert, Swati Chopra.

Ends December 19, 2014

Join the discussion for these Ask The Expert Events:
https://supportforums.cisco.com/expert-corner/knowledge-sharing

Continue the Questions on the Ask the Experts Event following today's Webcast

Introduction to Cisco Trustsec Solution and Configuration

Ankur, Mrinal, Fay Ann, and Beau

This is an opportunity to learn and ask more questions about Cisco Trustsec solution. The Trustsec solution is designed to flatten the network regardless of the access method but still provide fully distributed and differentiated access control no matter whether you are coming from wired or Wi-Fi or remote access, the Trustsec solution provides a consistent access control policy.

Security / AAA, Identity and NAC Community now through **December 19th, 2014**.

https://supportforums.cisco.com/discussion/12373686/ask-experts-introduction-cisco-trustsec-solution-and-configuration-webcast

Find more Events under the Expert Corner/Knowledge Sharing on the Cisco Support Community

Thank You For Joining Us Today!

Today's presentation will include audience polling questions.

We encourage you to participate!

Polling Question 1

What are the various ways of controlling network based access ?

a. VLAN Assignment

b. dACL assignment from RADIUS server

c. Role-Based Access Control

d. Security Group Tag

e. All of them

f. None

Submit Your Questions Now!

Use the Q & A panel to submit your questions and the panel of experts will respond. We have in the panel Ankur Bajaj, Mrinal Jaiswal and Beau Wallace

Agenda

- Introduction to Cisco TrustSec
- Classification and SGT Assignment
- Transporting the SGT
- Enforcement
- Network Device Admission Control
- MACSEC
- Common IOS configuration
- ISE Configuration
- Any connect VPN on ASA with SGT Assignment

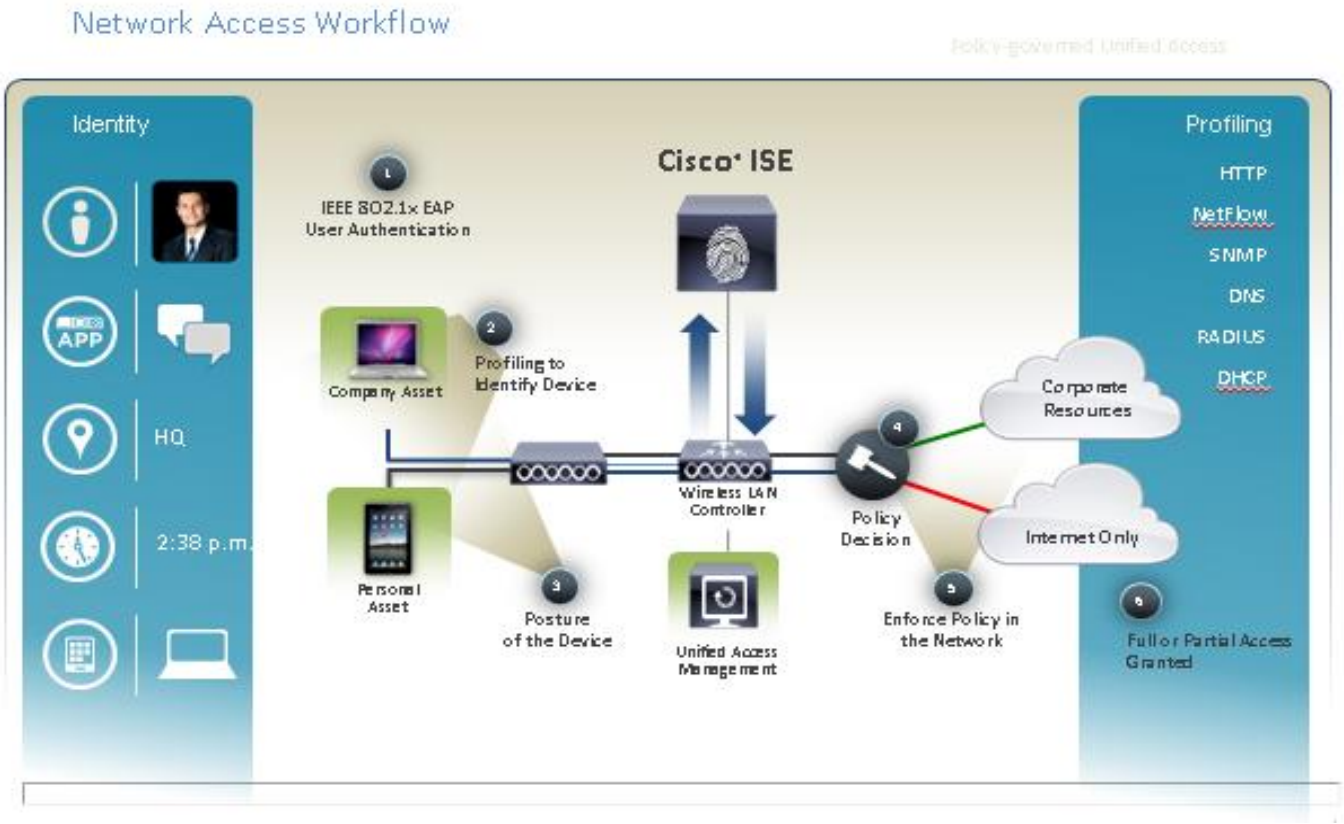
TrustSec Overview

- Introduction to TrustSec

Goal of Cisco TrustSec

- Provides Enhanced Network RBAC
- Context-Based Classification facilitating BYOD access control.
- Improved scale compared to IP-based ACL's.
- Provides Flexible Network Segmentation with Minimal Cost and operational impact.
- Introduce control to prevent user-to-user traffic (for threat defense)
- Provides access controls for Extranet Partners and differentiating Lines of Business.
- Simplify and Streamline Operation of Network-based Security Controls.
- Automate Firewall Policy Management.

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



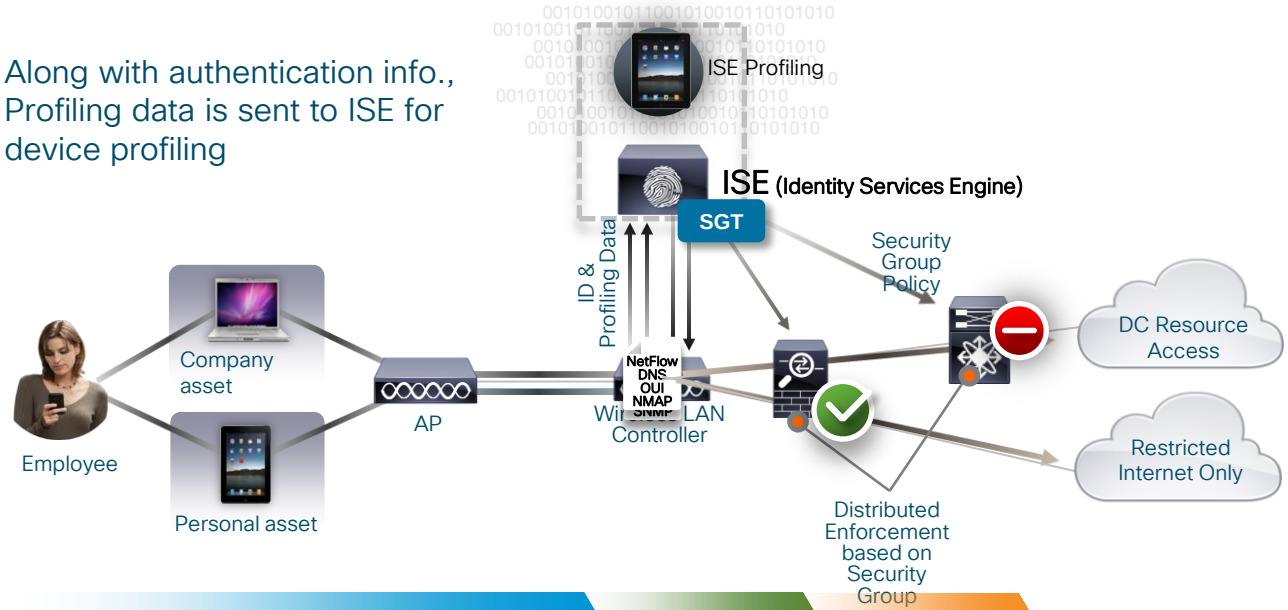
Key TrustSec functions: Classify, Propagate, Enforce

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

Classification Result:

Personal Asset SGT

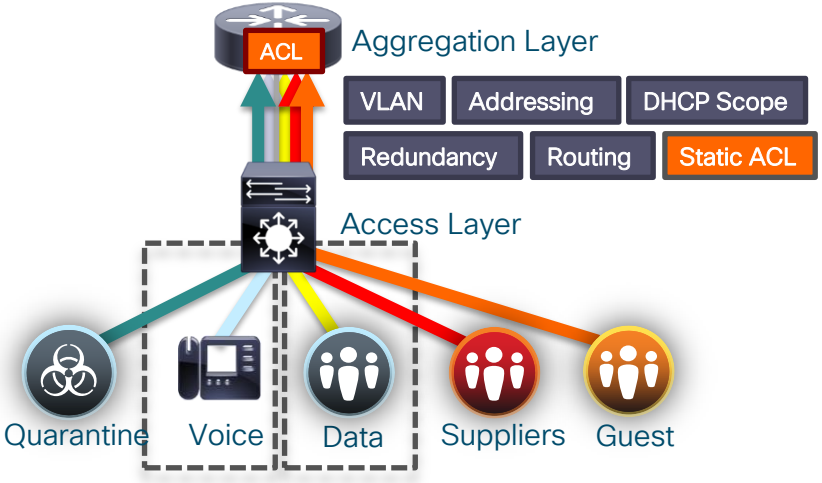
Along with authentication info., Profiling data is sent to ISE for device profiling



Classify → Propagate → Enforce

Traditional Segmentation

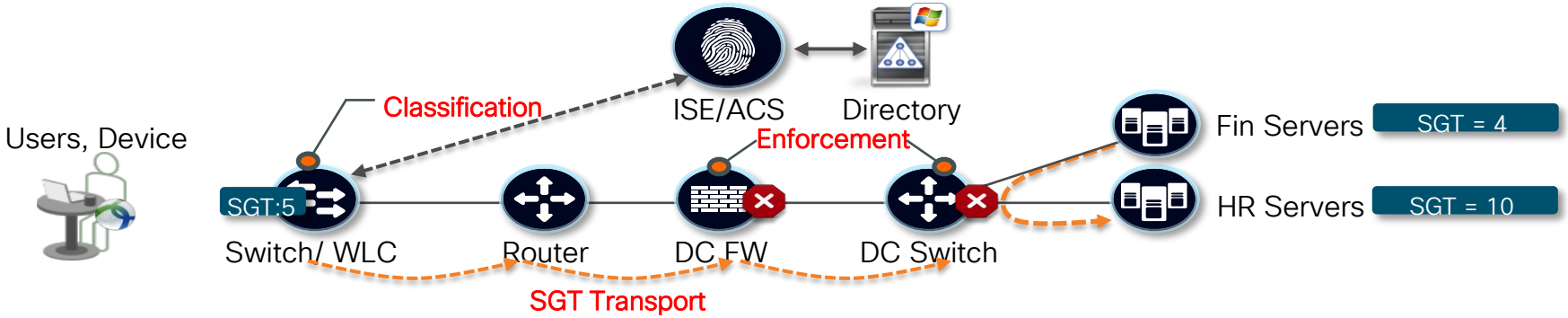
Steps replicated across floors, buildings and sites



Simple Segmentation with 2 VLANs

More Segmentation with 5 VLANs

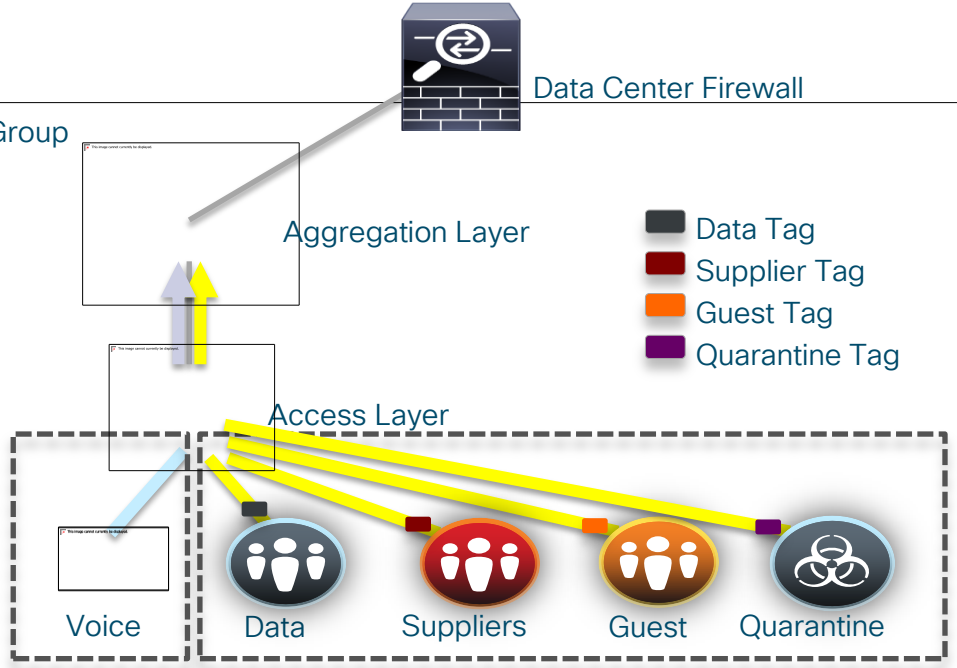
Why Not Just VLAN/DACL? SGT Travels!



- TrustSec is a context-based firewall or access control solution:
- **Classification** of systems/users based on **context**
  (user role, device, location, access method)The context-based classification **propagates** using SGT
- SGT used by firewalls, routers and switches to make intelligent forwarding or blocking decisions .
  Enforcement point needs to know "Source" SGT and Destination SGT to apply SGACL

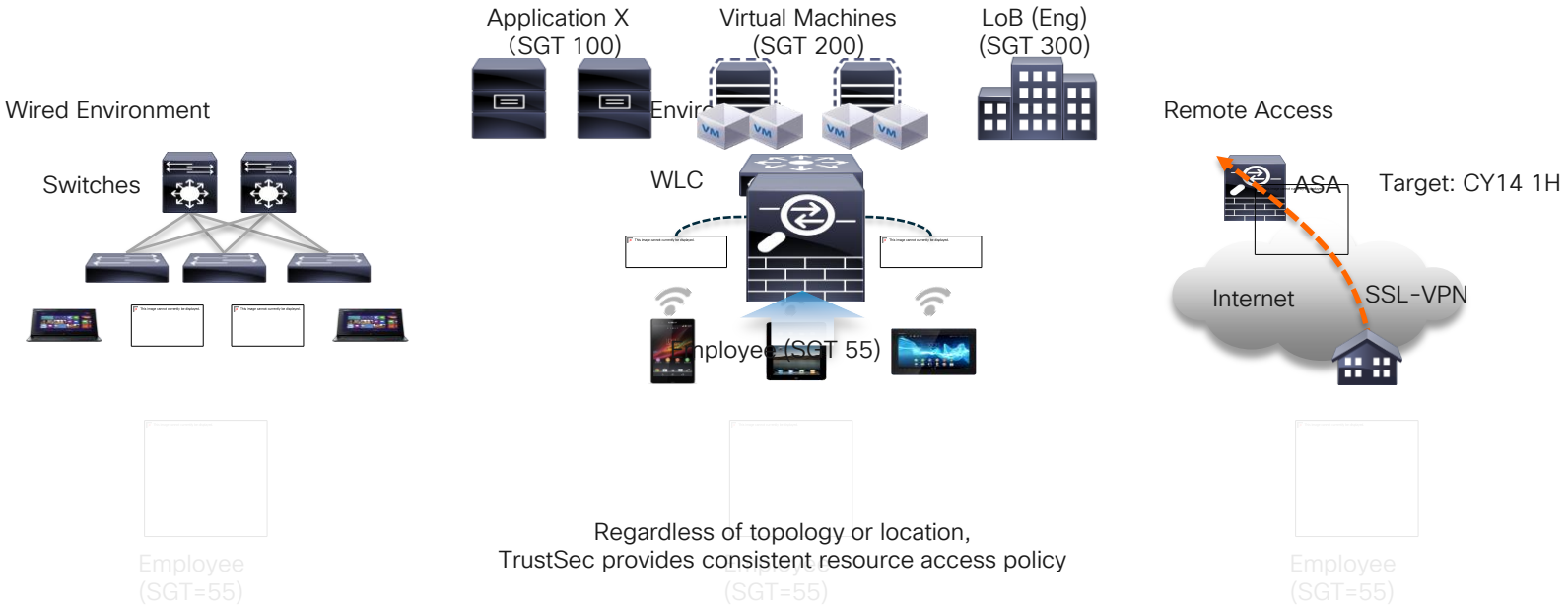
Policy and Segmentation with TrustSec

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



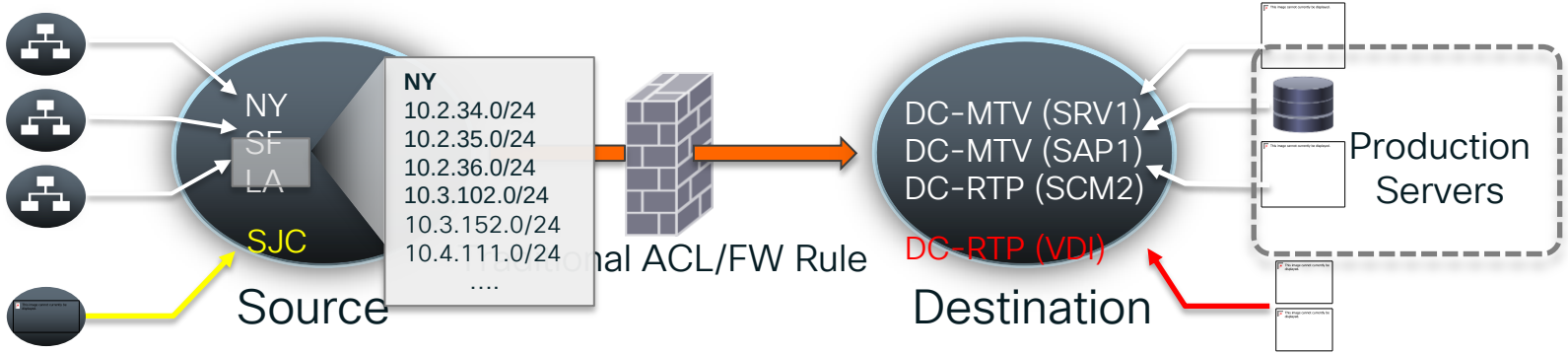
Retaining initial VLAN/Subnet Design

TrustSec = Consistent Policy!



Regardless of topology or location,
TrustSec provides consistent resource access policy

Traditional ACLs are High Overhead!



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

Complex Task and High OPEX continues

Key TrustSec functions: Classify, Propagate, Enforce

SGT Assignment Methods by Type

- Process to map SGT to IP Address
- Classification can be dynamic or static
- Not all platforms support all types of Static Classification!!! It is ***very important*** to verify support on hardware and software!!!

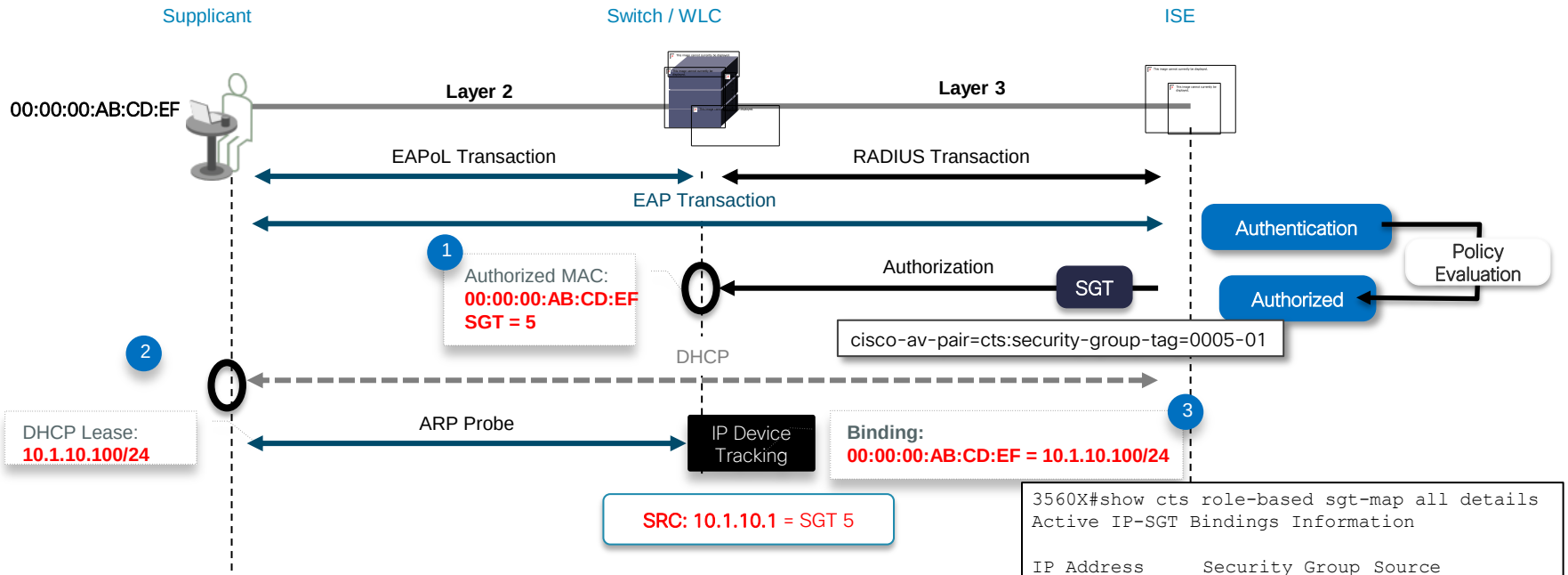
Dynamic Classification

- 802.1X
- MAC Authentication Bypass
- Web Authentication
- ASA VPN

Static Classification

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

Dynamic Classification Process in Detail




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

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

Make sure that IP Device Tracking is TURNED ON

Static Classification

IOS CLI Example

IP to SGT mapping

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

L2IF to SGT mapping*

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

VLAN to SGT mapping*

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

L3IF to SGT mapping**

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

Subnet to SGT mapping

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

L3 ID to Port Mapping**

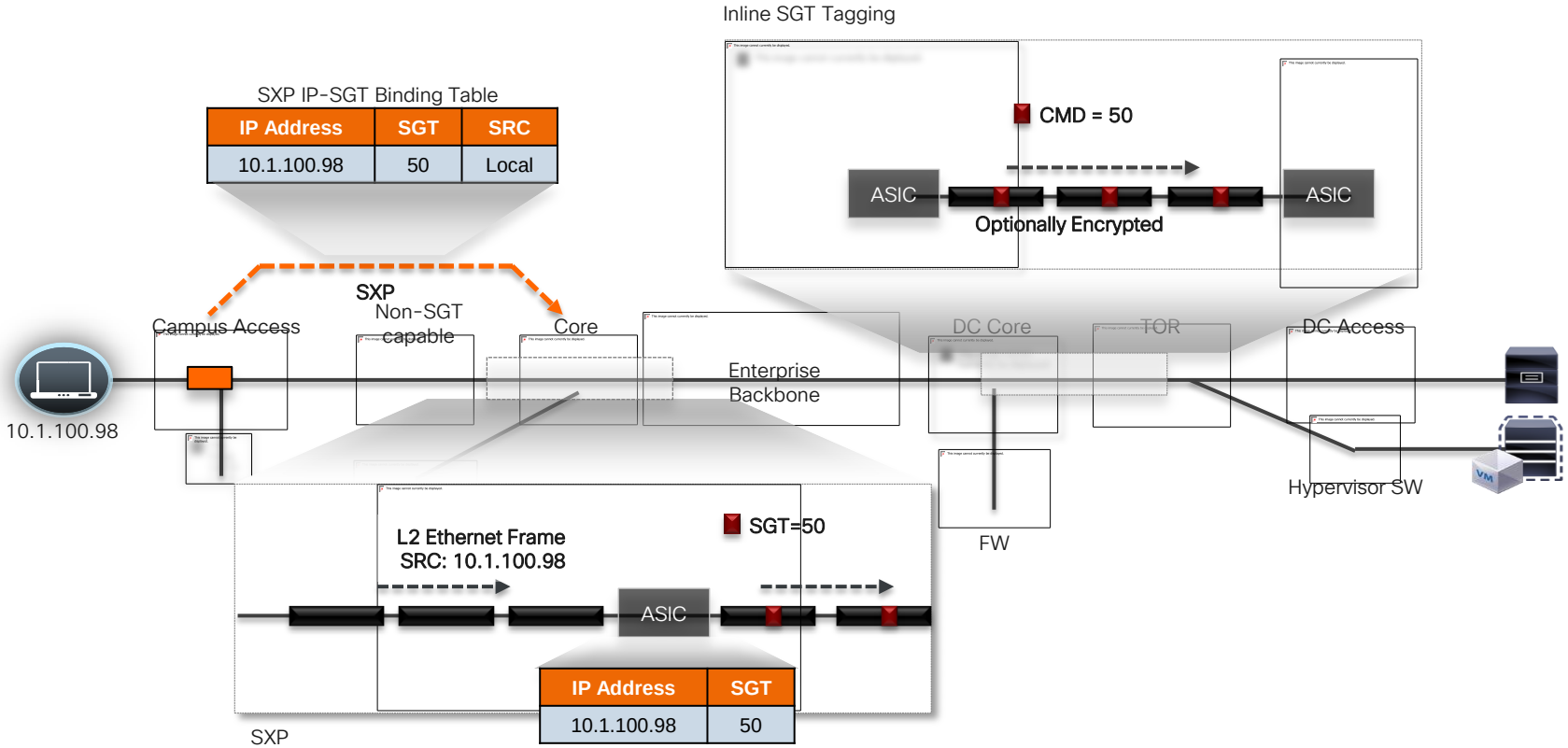
```
(config-if-cts-manual)#policy dynamic identity name
```

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

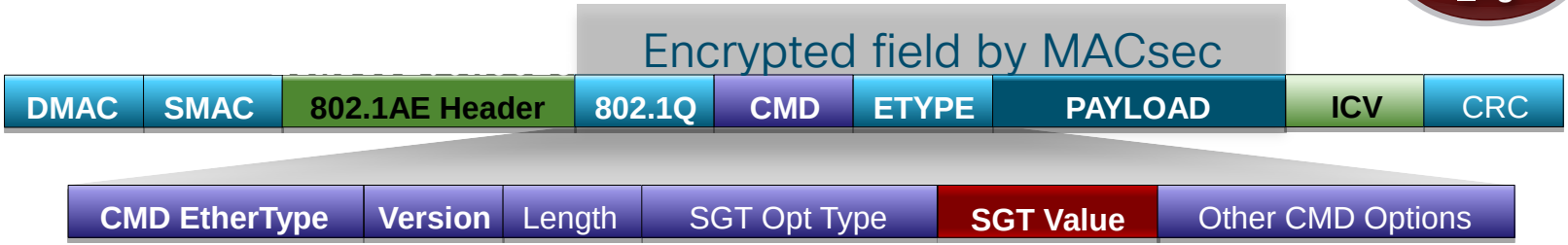
TrustSec Overview

- Transporting the SGT

More Than One Way to Transport the SGT!



The Inline SGT with MACsec



CTS Meta Data (`ETHTYPE:0x8909`)

16 bit (64K SGTs)

Ethernet Frame field

- 802.1AE Header | CMD | ICV are the L2 802.1AE + TrustSec overhead
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 40 bytes (~1600 bytes with 1552 bytes MTU)
- MACsec is optional for capable hardware

Polling Question 2

Is MACSEC a mandatory configuration for SGT propagation?

a. Yes

b. No

c. I'm not certain

Network Device Admission Control

- NDAC builds secure networks by establishing domains of trusted network devices preventing rogue switch connections
- Network devices are authenticated by their connected peer(s) via 802.1X
- There are three main roles within NDAC:
  - Supplicant: The role of an unauthenticated switch
  - Authentication server: The server that validates the identity of the supplicant and issues policies. This is the Cisco ISE server.
  - Authenticator: An authenticated device
- The first device to authenticate to ISE is known as the “Seed Device”

MACsec (802.1AE)

- MACsec provides Layer 2 Hop-by-Hop encryption on the LAN between endpoints and the switch as well as between the switches themselves
- Keying material for MACsec encryption can be statically defined or dynamically provided by ISE when using NDAC
- Some ethernet NIC vendors are beginning to include support for 802.1AE in hardware ASICs on the NIC

SGT link Authentication and Authorization

Mode	MACSEC	MACSEC Pairwise Master Key (PMK)	MACSEC Pairwise Transient Key (PTK)	Encryption Cipher Selection (no-encap, null, GCM, GMAC)	Trust and Propagation Policy for Tags
cts dot1x	Y	Dynamic	Dynamic	Negotiated	Dynamic from ISE/configured
cts manual – with encryption	Y	Static	Dynamic	Static	Static
cts manual – no encryption	N	N/A	N/A	N/A	Static

- CTS Manual is commonly used with SGT propagation
  - NDAC :“cts dot1x” takes link down with AAA down. Tight coupling of link state and AAA state
  - Some platforms (ISRG2, ASR1K, N5K) only support cta manual/no encryption

NDAC/MACsec dot1x

```
N7K-DST1# sho run int e 2/15

interface Ethernet2/15
  cts dot1x
  ip address 10.1.53.1/24
  ip router eigrp lab
  no shutdown

N7K-DST1# sho cts interface ethernet 2/15
CTS Information for Interface Ethernet2/15:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        C6K2T-CORE-2
      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:77d9058680000 an:2
      Current transmit SPI: sci:2498ea26fa0000 an:0
    Propagate SGT: Enabled
```

MACsec
CTS Manual Encryption

```
interface TenGigabitEthernet1/4
 cts manual
  sap pmk 1234ABCDEF mode-list gcm-encrypt null

6k-sup2t#sho cts int
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/4:
    CTS is enabled, mode:    MANUAL
    IFC state:               INIT
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              UNKNOWN
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE
```

Configuring an IOS Switch for SGT

- Following CLI is required to turn on NDAC (to authenticate device to ISE and receive policies including SGACL from ISE)

① Enabling AAA

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#aaa new-model
```

② Defining RADIUS server with PAC keyword

```
Switch(config)#radius-server host <ISE_PDP_IP> pac key
<RADIUS_SHARED_SECRET>
```

③ Define authorization list name for SGA policy download

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

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

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

Configuring an IOS switch for SGT(cont.)

⑤ Configure RADIUS server to use VSA in authentication request

```
Switch(config)#radius-server vsa send authentication
```

⑥ Enable 802.1X in system level

```
Switch(config)#dot1x system-auth-control
```

⑦ Define device credential (EAP-FAST I-ID), which must match ones in ISE AAA client configuration

```
Switch#cts credential id <DEVICE_ID> password <DEVICE_PASSWORD>
```

Note: remember that device credential under IOS is configured in Enable mode, not in config mode. This is different CLI command level between IOS and NX-OS, where you need to configure device credential in config mode.

Verification - PAC

Use show cts pac to verify whether PAC is provisioned or not. Key points are that A-ID matches to one that is found in environment data with IP address. Also check to see your I-ID is the one you setup in Device ID, and A-ID-Info matches one you configured on ISE (EAP-FAST configuration)

```
TS2-6K-DIST#show cts pacs
  AID: 04FB30FE056125FE90A340C732ED9530
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: 04FB30FE056125FE90A340C732ED9530
    I-ID: TS2-6K-DIST
    A-ID-Info: ISE PAP
    Credential Lifetime: 00:54:33 UTC Dec 21 2011
  PAC-Opaque:
000200B000030001000400100 4FB30FE056125FE90A340C732ED9530000600940003010098 0BC43B8BDAB7ECC3B12C04D2D3CA6E
000000134E7A69FD00093A80AD1F972E0C67757D29DBF9E8452EDC3E0A46858429C8E4714315533061DAD4FB2F31346FE4408579
D4F55B3813ADA9876F04ACC1656DE2F476ED3CBC96A0DB937403AC3B0CAB64EEC15A1BD6E351A005A8DE6E6F894DEE619F4EFFF0
31BC7E7BD9C8B230885093FF789BAECB152E3617986D3E0B
  Refresh timer is set for 12w0d
```

Verification Environment Data

Environment data shows more useful information. First you can see which SGT is assigned for Device SGT. Also you can see the server list downloaded from ISE. And this information should include SGT ID and Name table as well.

```
TS2-6K-DIST#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00
Server List Info:
Installed list: CTSServerList1-0004, 3 server(s):
 *Server: 10.1.100.3, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.1.100.4, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.1.100.6, port 1812, A-ID 04FB30FE056125FE90A340C732ED9530
          Status = ALIVE
          auto-test = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
  0001-30 :
    2-98 : 80 -> Device_SGT
    unicast-unknown-98 : 80 -> Unknown
    Any : 80 -> ANY
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 20:56:48 UTC Mon Sep 26 2011
Env-data expires in   0:23:59:59 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:59 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

Activating SGACL Enforcement on IOS switch

- After setting up SGT/SGACL on ISE, you can now enable SGACL Enforcement on IOS switch

Statically Defining IP to SGT mapping for servers

```
Switch(config)#cts role-based sgt-map 10.1.40.10 sgt 5
Switch(config)#cts role-based sgt-map 10.1.40.20 sgt 6
Switch(config)#cts role-based sgt-map 10.1.40.30 sgt 7
```

Enabling SGACL Enforcement Globally and for VLAN

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

IOS SXP Configuration

Example Shown: SXP between a 3750 and 6500

```
3750
cts sxp enable
cts sxp connection peer 10.1.44.1 source 10.1.11.44 password
 default mode local
! SXP Peering to Cat6K

6K
cts sxp enable
cts sxp default password cisco123
!
cts sxp connection peer 10.10.11.1 source 10.1.44.1 password
 default mode local listener hold-time 0 0
! ^^ Peering to Cat3K
cts sxp connection peer 10.1.44.44 source 10.1.44.1 password
 default mode local listener hold-time 0 0
! ^^ SXP Peering to WLC
```

IOS SXP configuration

Verification

Example Shown: SXP between a 3750 and 6500 (6500 output)

```
C6K2T-CORE-1#show cts sxp connections brief
 SXP                  : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running

-------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
-------------------------------------------------------------------------------
10.1.11.44       10.1.44.1        On                11:28:14:59 (dd:hr:mm:sec)
10.1.44.44       10.1.44.1        On                22:56:04:33 (dd:hr:mm:sec)

Total num of SXP Connections = 2
C6K2T-CORE-1#show cts role-based sgt-map all details
Active IP-SGT Bindings Information

IP Address         Security Group                         Source
========================================================================
10.1.40.10         5:PCI_Servers                           CLI
10.1.44.1          2:Device_sgt                            INTERNAL
--- snip ---
10.0.200.203       3:GUEST                                 SXP
10.10.11.100       8:EMPLOYEE_FULL                         SXP
```

TrustSec Debugging – Useful Commands

- debug CTS environment data all
- debug CTS authorization aaa
- debug CTS authorization events
- debug CTS aaa

Configuring ISE for TrustSec

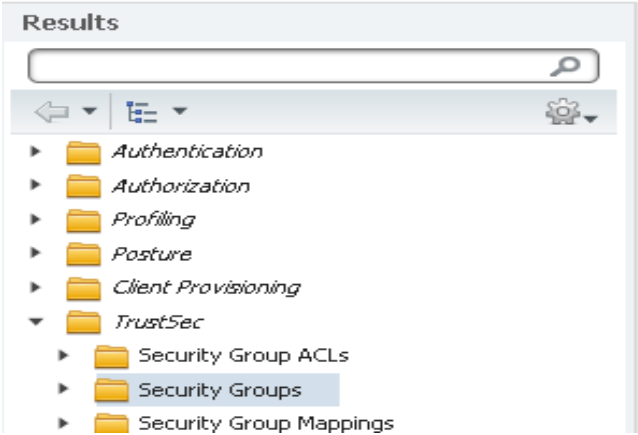
- Step-by-Step Instructions
  - ✓ Version 1.3 ISE Shown

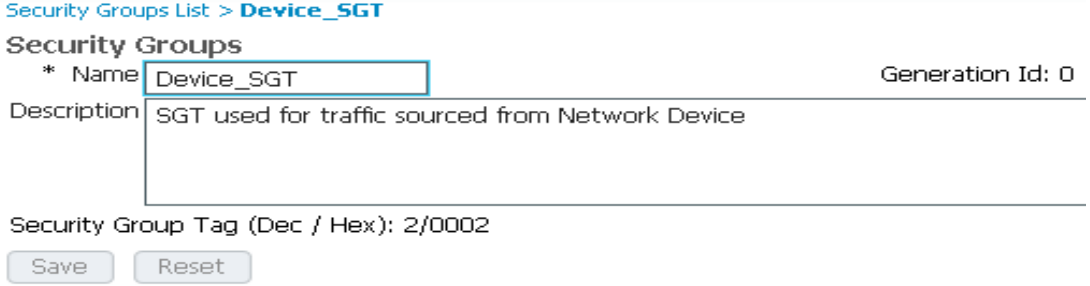
Enabling SGT/SGACL on ISE

- Following is a high-level overview of SGT/SGACL configuration on ISE1.x

① Configure ISE 1.x to the point where you can perform 802.1X authentication (bootstrap, certificate, AD integration, basic auths&authz rules)

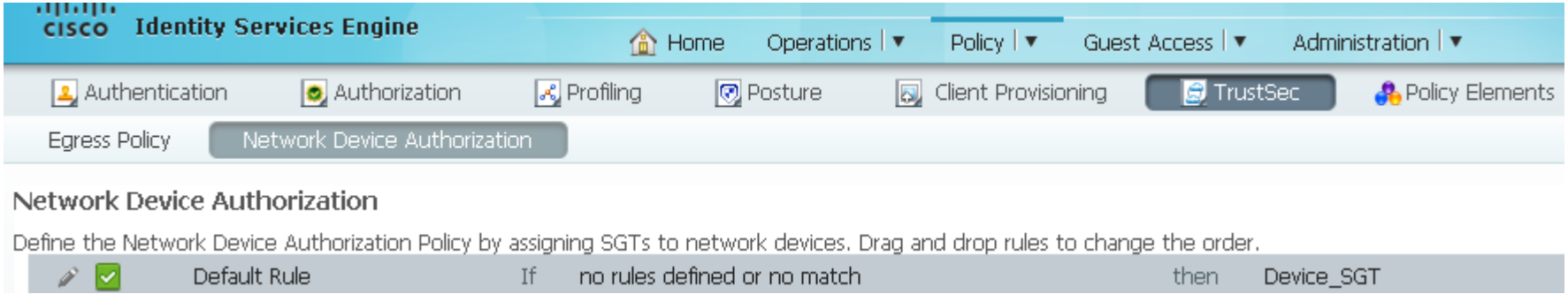
② Configure Device SGT (Policy > Policy Elements > Results > Trustsec> Security Group)



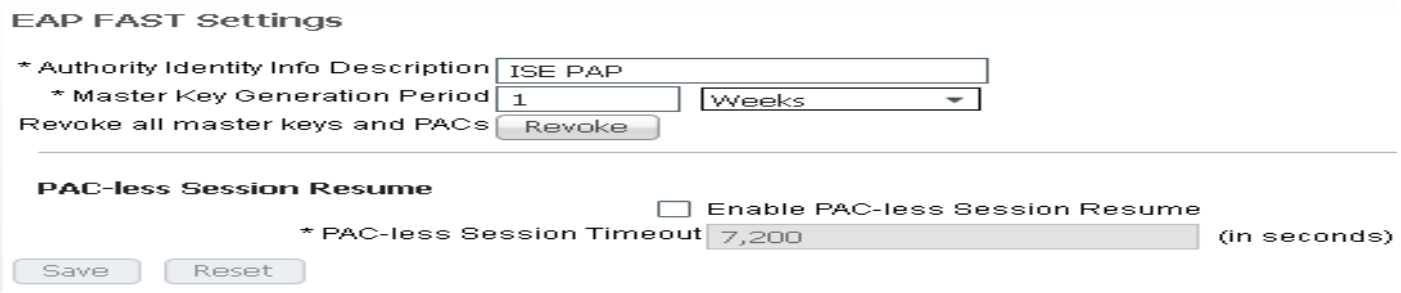


SGT Configuration for ISE

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

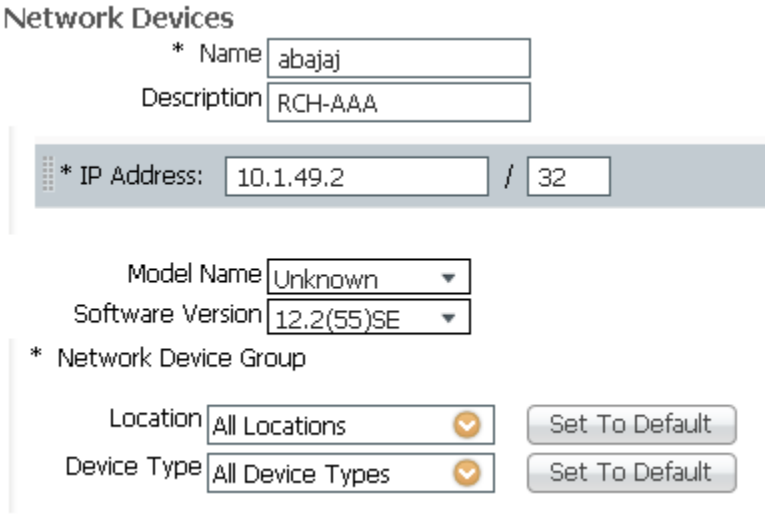


④ **Optionally** under **Admin > System > Settings > Protocols > EAP-FAST > EAP-FAST Settings**, change A-ID description to something meaningful, so that you can recognize which ISE you are receiving PAC file on the switch CLI.



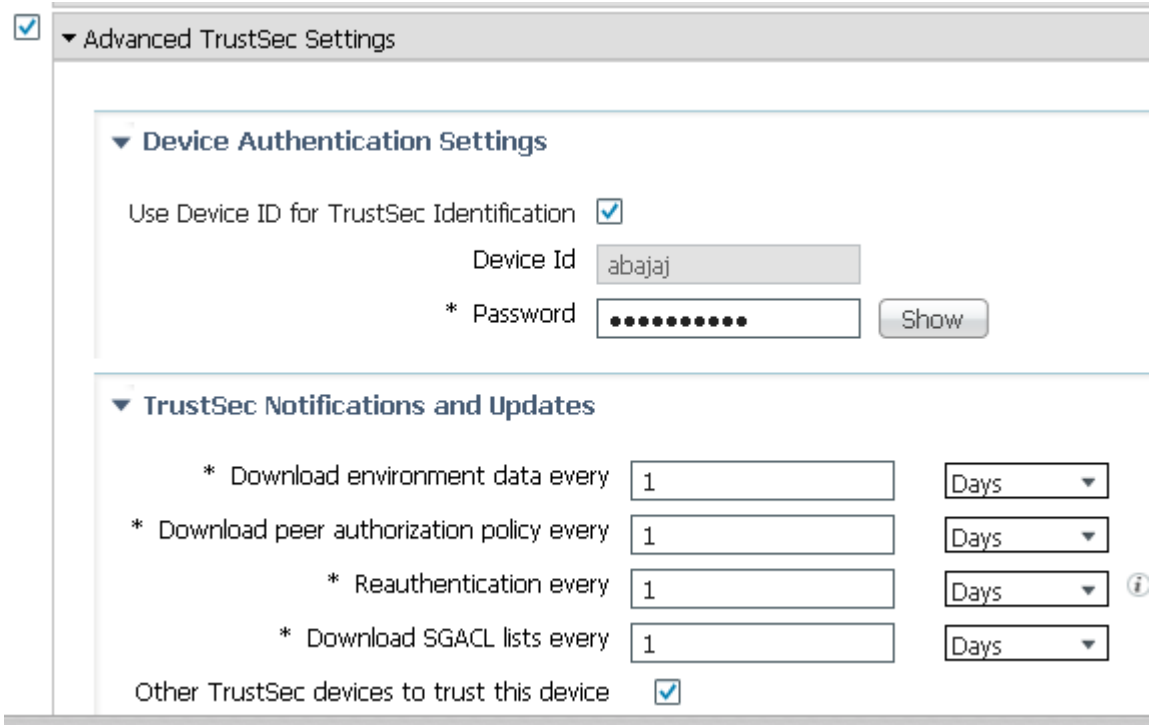
Configure ISE for TrustSec Devices

⑤ Under **Admin > Network Resources > Network Devices**, create AAA client entry for the device



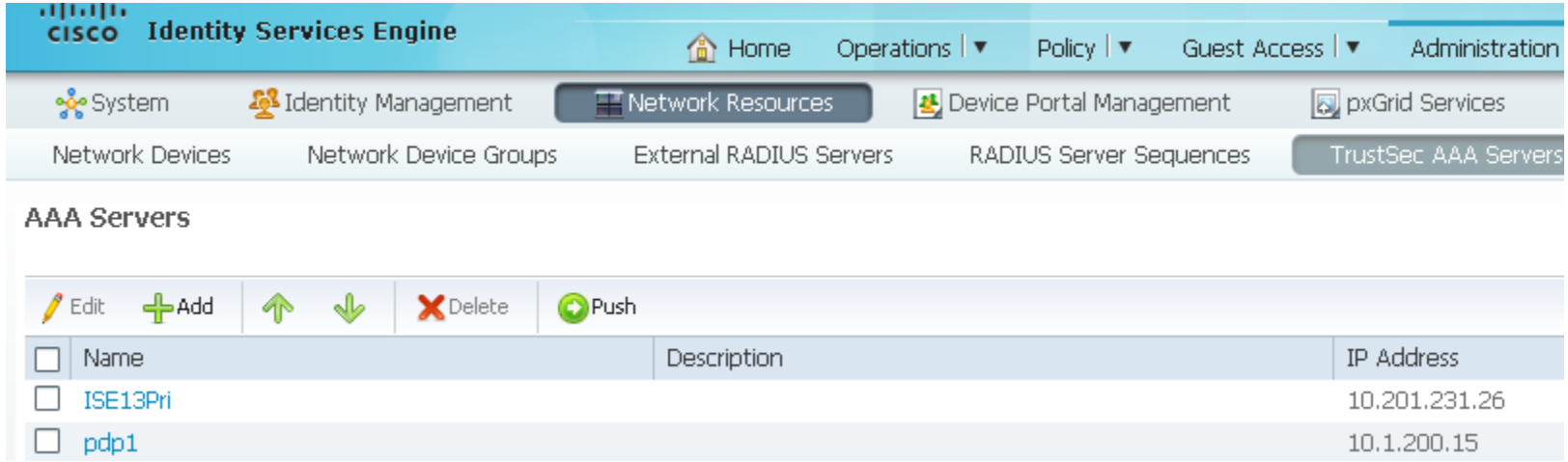
Configuration of an SGT Device

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



Extra Steps to setup Private Server List
For Network Device Admission Control (NDAC)

⑦ Update “seed” device (closest device to ISE) with list of multiple servers it can fall back to in case first PDP becomes unavailable. You can set such list under **Admin > Network Resources > TrustSecAAA Servers.** This data is available via CTS Environment Data (show cts environment-data)



Create a Security Group ACL (SGACL)

Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentication | Authorization | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

Dictionaries | Conditions | Results

Results

- Authentication
- Authorization
- Profiling
- Posture
- Client Provisioning
- TrustSec
  - Security Group ACLs
    - abajaj_ACL
  - Security Groups
  - Security Group Mappings

Security Groups ACLs List > **abajaj_ACL**

Security Group ACLs

* Name: abajaj_ACL

Description:

IP Version: (•) IPv4 ( ) IPv6 ( ) Agnostic

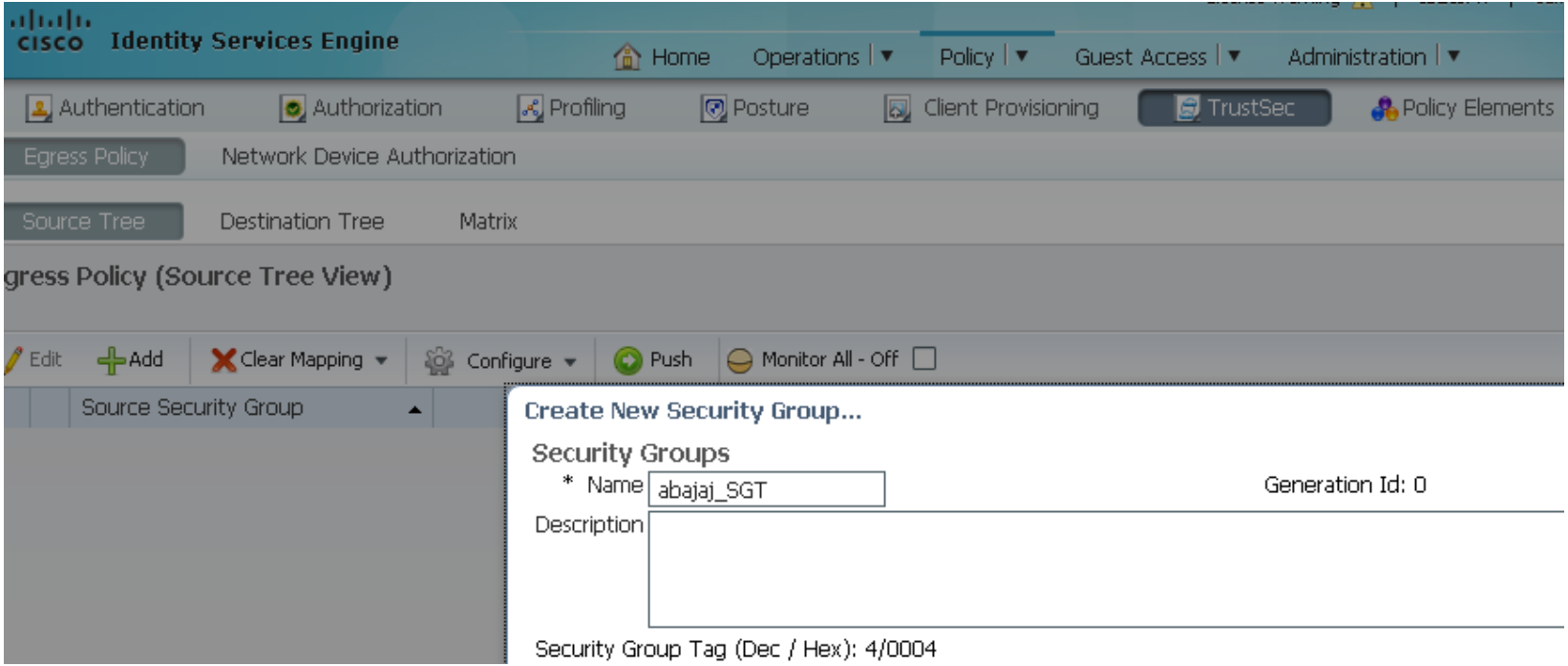
* Security Group ACL content:

```
permit tcp dst eq 443
permit tcp dst eq 80
permit tcp dst eq 1433
permit icmp
deny ip
```

Create Security Groups

- In order to provision SGACL policy automatically to network devices, ISE needs to be configured for SGT/SGACL and associated policies

Under Policy > Security Group Access > Egress Policy, create Security Group Tag for roles



Configure SGACL Mapping Enforcement

cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentication | Authorization | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

Egress Policy | Network Device Authorization

Source Tree | Destination Tree | Matrix

Egress Policy (Source Tree View)

Edit | Add | Clear Mapping | Configure | Push | Monitor All - Off

Source Security Group
abajaj_SGT (4/0004)

Create Security Group ACL Mapping...

Source Security Group:
abajaj_SGT

Destination Security Group:
SGT_abajaj

Status: Enabled

Description: SGACL to src to dst group mapping

Assigned Security Group ACLs

abajaj_ACL

Final Catch All Rule: None

SGACL Mapping vis Policy Matrix

cisco Identity Services Engine

Home

Authentication | Authorization | Profiling | Postu

Egress Policy | Network Device Authorization

Source Tree | Destination Tree | Matrix

Egress Policy (Matrix View)

Edit | Add | Clear Mapping | Configure | Push | Mo

Source \ Destination	abajaj_SGT (4/0004)
abajaj_SGT (4/0004)	
Device_SGT (2/0002)	
SGT_abajaj	

Edit Permissions...

Source Security Group **SGT_abajaj (3/0003)**

Destination Security Group **abajaj_SGT (4/0004)**

Status: Enabled

Description:

Assigned Security Group ACLs

abajaj_ACL

Final Catch All Rule: None

Configure an Authorization policy for SGT

cisco Identity Services Engine

Home | Operations | ▼ | Policy | ▼ | Guest Access | ▼ | Administration | ▼ | Setup Assist

Authentication | Authorization | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

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

First Matched Rule Applies ▼

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	abajaj_Authz	if	Employee	then	abajaj_SGT	Edit ▼

Polling Question 3

Does TRUSTSEC provides scalable and Enhanced Role Based Access Control?

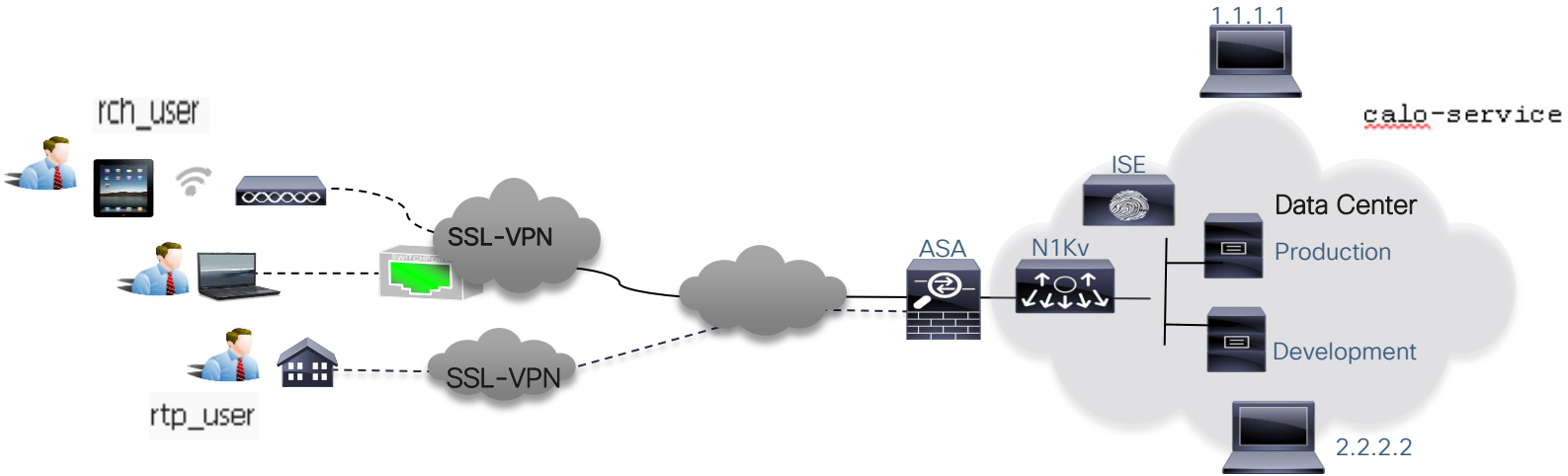
a. Yes

b. No

c. Not sure

TrustSec on ASA with VPN: Configuration

TrustSec on ASA with VPN



SGFW condition : Allow icmp from rtp-user to 1.1.1.1, Allow icmp from rch-user to 2.2.2.2, Deny access from rch-user to calo-service, Allow access from rtp-user to rch-user only, Allow everything else

Configuration on ASA

1) no sysopt connection permit-vpn

#Command to turn on traffic pass-through between two VPN users#

2) same-security-traffic permit intra-interface

Configuration on ASA (contd..)

#Command to create object groups, group name and tag for SGFW for two Users: rtp-user and rch-user and one Common services : calo#

```
3) object-group security RTP
 security-group name rtp-users
 security-group tag 105
object-group security RCH
security-group name rch-users
 security-group tag 103
object-group security CALO
security-group name calo-service
 security-group tag 301
```

Configuration on ASA (contd..)

4) access-list Outside_access_in extended permit icmp security-group name rtp-user any host 1.1.1.1

access-list Outside_access_in extended permit icmp security-group name rch-user any host 2.2.2.2

access-list Outside_access_in extended deny ip security-group name rch-user any security-group name calo-service any

access-list Outside_access_in extended permit ip security-group name rtp-user any security-group name rch-user any

access-list Outside_access_in extended permit ip any any

Create access-group with ACL created above and map it to outside interface

access-group Outside_access_in in interface Outside

Configuration on ASA (contd..)

#Configure AAA server for authorization, CoA and interim accounting update for web login #

5) aaa-server ISE protocol radius

authorize-only

interim-accounting-update

dynamic-authorization

aaa-server ISE (management) host <PSN_IP> key cisco

aaa-server ISE (management) host <PSN_IP> key cisco

#Configure CTS server group#

6) cts server-group ISE

Configuration on ASA (contd..)

#Turn on SXP to forward the IP-SGT bindings to device inside for Remote access users#

7) cts sxp enable

cts sxp default password cisco

cts sxp connection peer <inside_device_ip> password none mode peer listener

Configuration on ASA (contd..)

Configure tunnel group for authentication with ISE server

8) tunnel-group <name> type remote-access

tunnel-group <name> general-attributes

 address-pool <pool_name>

 authentication-server-group ISE

 authorization-server-group ISE

 accounting-server-group ISE

#Allow ASA to inspect the ICMP traffic to allow traffic between two VPN !users when SGFW is used#

9) policy-map global_policy

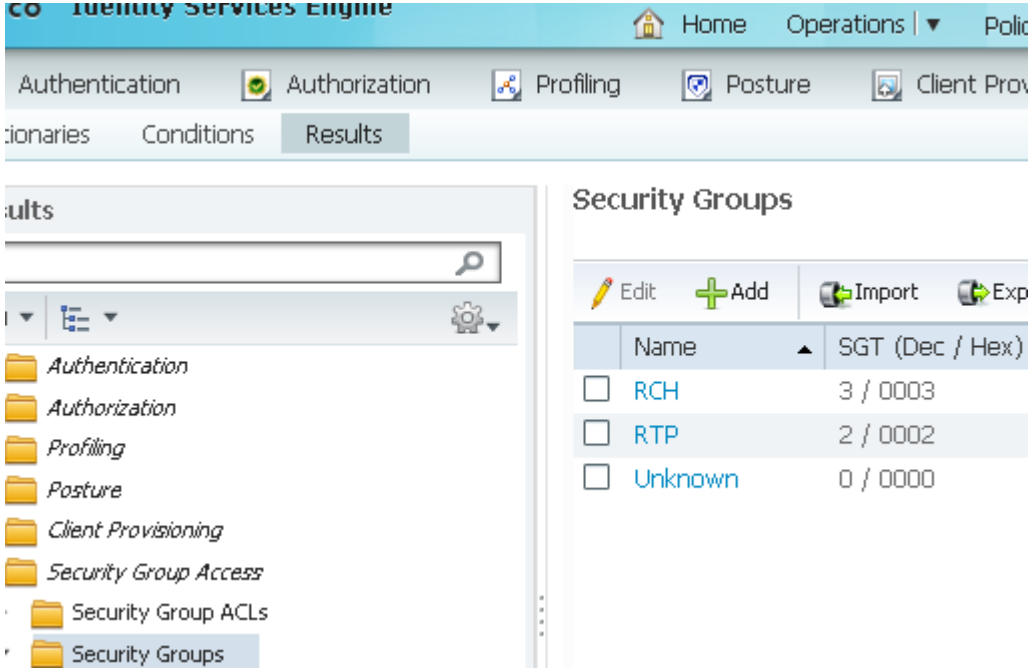
 class inspection_default

Inspect icmp

service-policy global_policy global

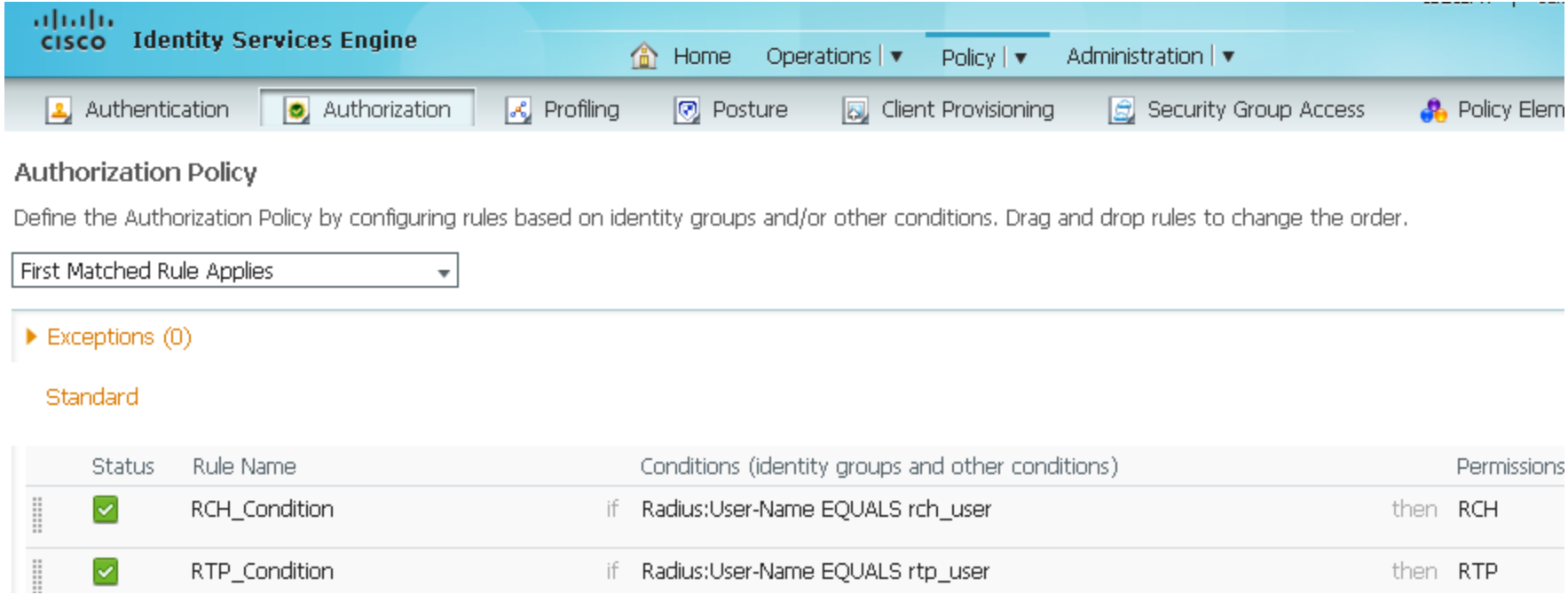
Configuration on ISE

Instead of defining the security-group name and value on step 3 we can define the same on ISE and push it using Authorization policy. Go **to Policy > Policy Elements> Results > Security Group Access > Security group > ADD**



Configuration on ISE (contd..)

Policy > Authorization. For rch_user there is SGT tag RCH and for rtp_user tag is RTP



Configuration on ISE (contd..)

System | Identity Management | Network Resources | Web Portal Management | Feed Service

Network Devices | Network Device Groups | External RADIUS Servers | RADIUS Server Sequences | SGA AAA Servers | NAC Managers | MDM

Network Devices

- Network Devices
- Default Device

Generate PAC

The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* Identity	ASA
* Encryption Key	••••••••
* PAC Time to Live	1 Years
Expiration Date	14 Dec 2015 21:01:26 GMT

Generate PAC | Cancel

Out Of Band (OOB) SGA PAC

Issue Date	
Expiration Date	
Issued By	

Generate PAC

Configuration on ASA (contd..)

Import the PAC to the ASA : The generated file could be put on an HTTP/FTP server. The ASA uses that to import the file.

```
ASA# cts import-pac http://1.1.1.1/ASA-CTS-2.pac password 12345678

!PAC Imported Successfully

ASA# show cts pac

  PAC-Info:

    Valid until: Dec 16 2015 17:40:25

    AID:        ea48096688d96ef7b94c679a17bdad6f

    I-ID:       ASA-CTS-2

    A-ID-Info:   Identity Services Engine

    PAC-type:    Cisco Trustsec

  PAC-Opaque:

    000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301

    0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555

    e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
```

Configuration on ASA (contd..)

```
ASA# show cts environment-data sg-table

Security Group Table:

Valid until: 17:48:12 CET Dec 17 2014

Showing 4 of 4 entries

SG Name                SG Tag    Type

-------                ------    -------------

ANY                    65535     unicast

Unknown                0         unicast

RTP                    2         unicast

RCH                    3         unicast
```

Configuration on ASA (contd..)

```
ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : rtp_user                Index        : 1
Assigned IP  : 100.100.100.100         Public IP    : 10.1.1.1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 11134                   Bytes Rx     : 12714
Group Policy : abajaj-SSL              Tunnel Group : RA
Login Time   : 17:49:15 CET Tue Dec 16 2014
Duration     : 0h:14m:21s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : c0a2100a000010002142d60b
Security Grp : 2:RTP
```

Configuration on ASA (contd..)

```
Username     : rch_user                Index        : 2
Assigned IP  : 100.100.100.101         Public IP    : 10.1.1.1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 86171                   Bytes Rx     : 122480
Group Policy : abajaj-SSL              Tunnel Group : RA
Login Time   : 17:52:27 CET Tue Dec 16 2014
Duration     : 0h:11m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : c0a2100a000010002142d6cb

Security Grp : 3:RCH
```

Submit Your Questions Now!

Use the Q & A panel to submit your questions and our expert will respond

Trivia Question (Select the correct answer)

What does your New Year's fitness resolution and Cisco's Trustsec share in common?

a. Fitness company BeachBody, partnered with Cisco to help install a next generation firewall to protect its data center and simplify security management.

b. Trustsec secures and maintains data applications and mobile devices from unauthorized access with corporate fitness equipment companies such as NordicTrack and Landice.

c. TrustSec engineers have an annual fitness competition around the holidays. The winner ironically gets an all-expense paid dinner of their choice.

d. National gyms such as 24 Hour Fitness and Gold's Gym use Trustsec for their corporate computer security as well as their in gym computer systems.

Join the Cisco Support Community

Participate in Live Interactive Technical Events and much more

http://bit.ly/1jlI93B

We invite you to actively collaborate in the Cisco Support Community & Social Media

http://www.facebook.com/CiscoSupportCommunity

http://twitter.com/#!/cisco_support

http://www.youtube.com/user/ciscosupportchannel

https://plus.google.com/110418616513822966153?prsrc=3#110418616513822966153/posts

http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019

Newsletter Subscription
https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=589&keyCode=146298_2&PHYSICAL%20FULFILLMENT%20Y/N=NO&SUBSCRIPTION%20CENTER=YES

http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8

https://play.google.com/store/apps/details?id=com.cisco.swtg_android

We have communities in other languages!

If you speak Spanish, Portuguese, Japanese, Russian or Chinese we invite you to participate and collaborate in your language

Spanish → https://supportforums.cisco.com/community/spanish

Portuguese → https://supportforums.cisco.com/community/portuguese

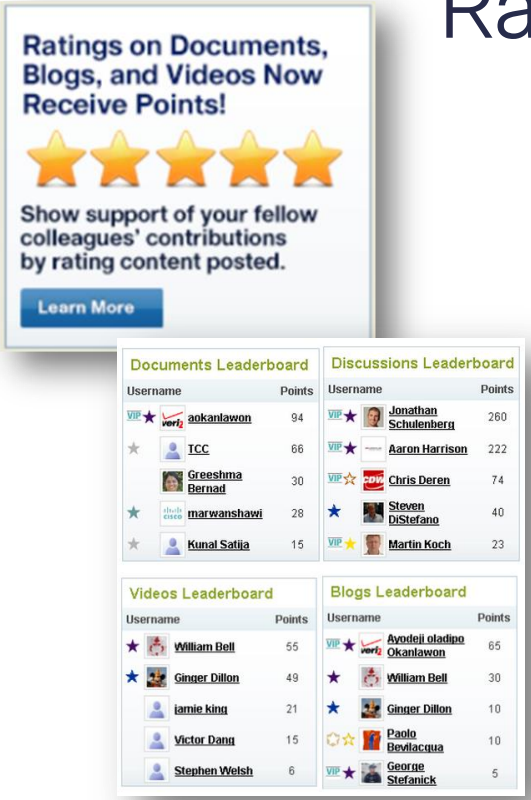
Japanese → https://supportforums.cisco.com/community/csc-japan

Russian → https://supportforums.cisco.com/community/russian

New Chinese Community!

Chinese → http://www.csc-china.com.cn/

Rate Support Community Content



Now your ratings on documents, videos, and blogs count give points to the authors!!!

So, when you contribute and receive ratings you now get the points in your profile.

Help us to recognize the quality content in the community and make your searches easier. Rate content in the community.

https://supportforums.cisco.com/blog/154746

More IT Training Videos & Tech Seminars

on the Cisco Learning Network

View Upcoming Sessions Schedule
cisco.com/go/techseminars

Trivia Question (Select the correct answer)

What does your New Year's fitness resolution and Cisco's Trustsec share in common?

a. Fitness company BeachBody, partnered with Cisco to help install a next generation firewall to protect its data center and simplify security management.

b. Trustsec secures and maintains data applications and mobile devices from unauthorized access with corporate fitness equipment companies such as NordicTrack and Landice.

c. TrustSec engineers have an annual fitness competition around the holidays. The winner ironically gets an all-expense paid dinner of their choice.

d. National gyms such as 24 Hour Fitness and Gold's Gym use Trustsec for their corporate computer security as well as their in gym computer systems.

The Answer is "a"

Thank you for Your Time!

Please take a moment to complete the evaluation

CISCO

Thank you.