



SNEAK PEEK

Cisco Support Community Expert Series Webcast

Introduction to Cisco TrustSec Solution and Configuration

Dec 16, 2014

with Ankur Bajaj

Register Now: <http://bit.ly/decwebcast>

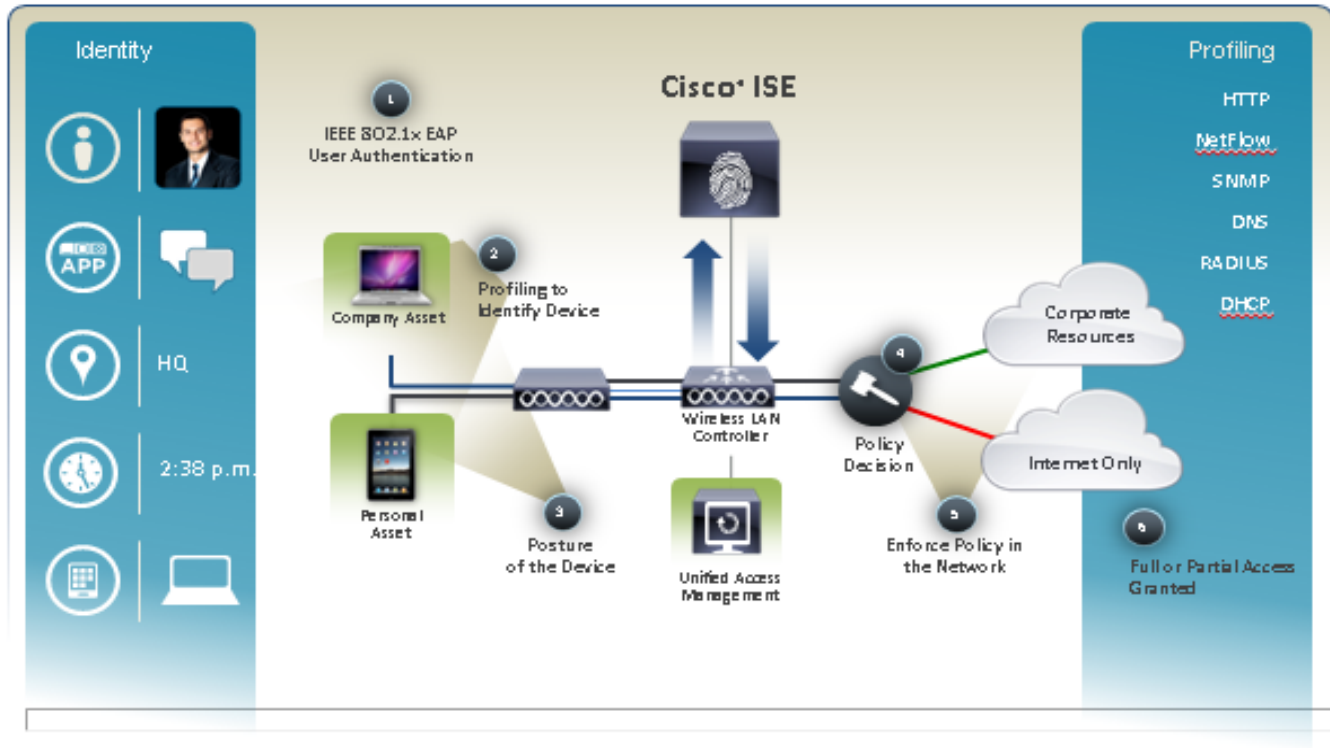
Goal of Cisco TrustSec

- 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.

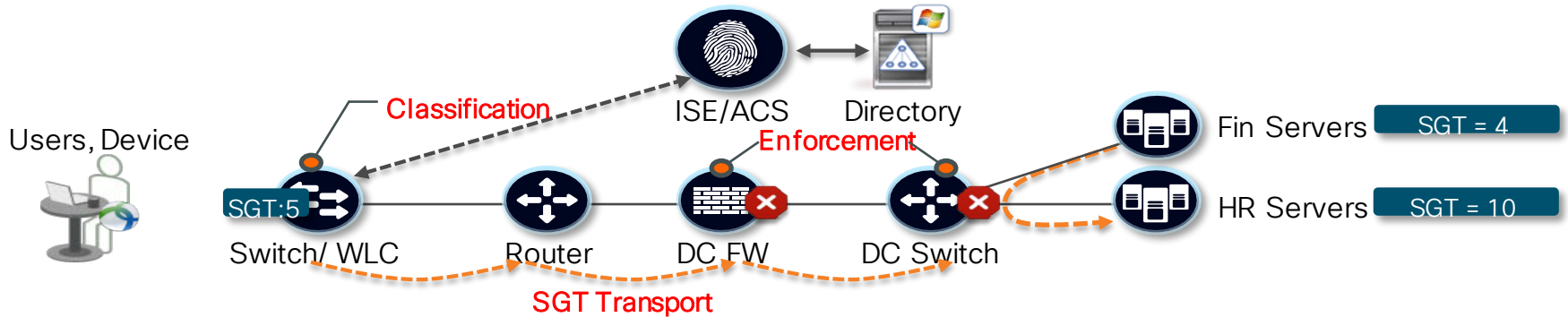
Policy: Who, What, Where, When, and How?

Network Access Workflow

Policy-governed Unified Access

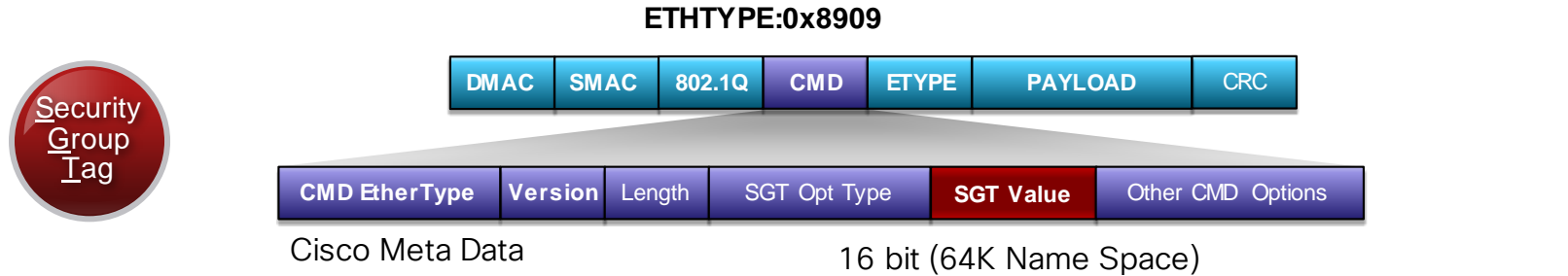




Why Not Just VLAN/DACL? SGT Travels!



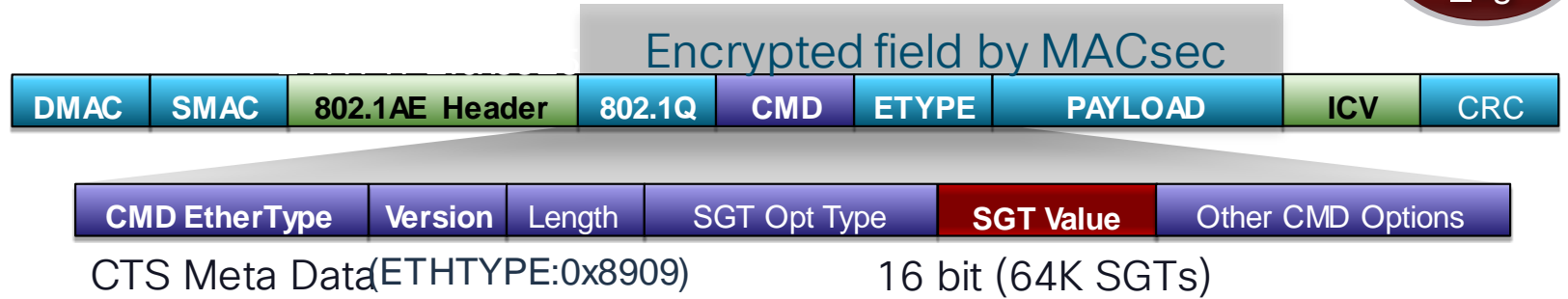
- TrustSec is a context-based firewall or access control solution:
- **Classification** of systems/users based on **context** (user role, device, location, access method) The context-based classification **propagates** using SGT
- SGT used by firewalls, routers and switches to make intelligent forwarding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

The Inline SGT without MACsec






-  Just SGT overhead  Ethernet Frame field
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 20 bytes = less than baby giant frame (~ 1600 bytes with 1552 bytes MTU)
- N5K support today. ISR/ASR support 1HCY13

The Inline SGT with MACsec



 Ethernet Frame field

-    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

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 (ISR2, ASR1K, N5K) only support cta manual/no encryption

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.

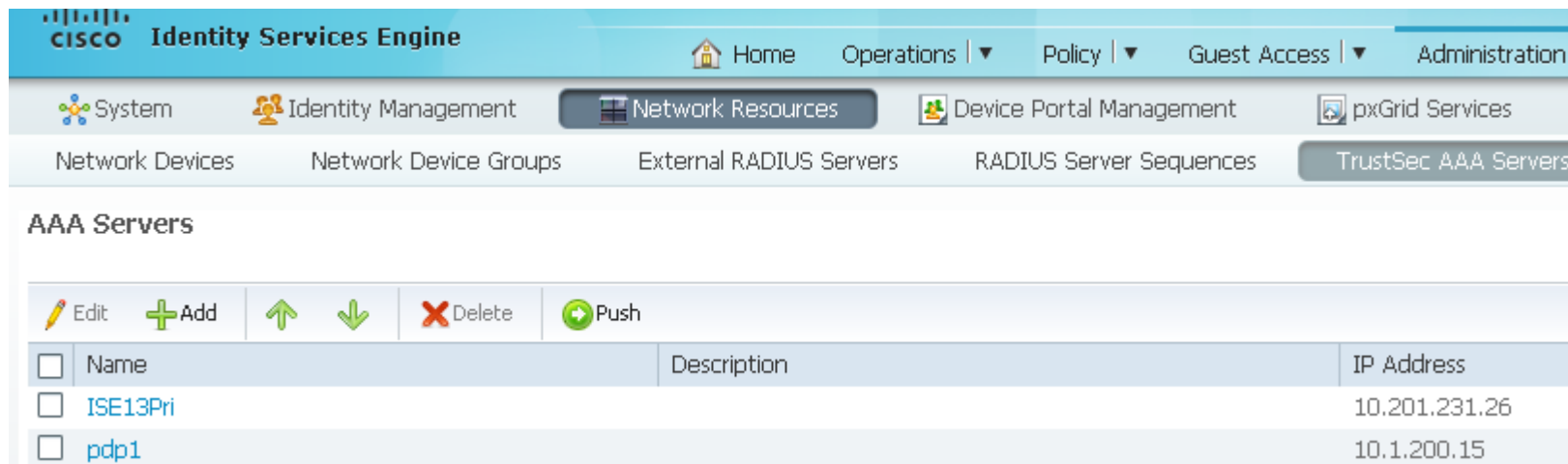
Enabling SGT/SGACL on ISE

- Following is a high-level overview of SGT/SGACL configuration on ISE 1.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)

The screenshot displays the Cisco ISE web interface. On the left, a navigation pane titled 'Results' shows a tree view of configuration categories: Authentication, Authorization, Profiling, Posture, Client Provisioning, and TrustSec. Under TrustSec, 'Security Groups' is selected and highlighted. The main content area shows the configuration for a specific Security Group named 'Device_SGT'. The breadcrumb path is 'Security Groups List > Device_SGT'. The configuration fields include: 'Name' set to 'Device_SGT', 'Generation Id' set to '0', and 'Description' set to 'SGT used for traffic sourced from Network Device'. Below these fields, the 'Security Group Tag (Dec / Hex)' is set to '2/0002'. At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

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

- 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 > TrustSec AAA Servers**. This data is available via CTS Environment Data (show cts environment-data)



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, the 'Network Resources' menu is expanded, showing 'TrustSec AAA Servers' as the selected option. The main content area is titled 'AAA Servers' and features a toolbar with 'Edit', 'Add', 'Move Up', 'Move Down', 'Delete', and 'Push' actions. A table lists the configured AAA servers:

<input type="checkbox"/>	Name	Description	IP Address
<input type="checkbox"/>	ISE13Pri		10.201.231.26
<input type="checkbox"/>	pdp1		10.1.200.15

Check out some additional information on Cisco TrustSec on the Cisco Support Community.

Community Tech-Talk : Understanding Cisco TrustSec (Secure Group Access) - presentation

<http://bit.ly/trustsec-doc-sneakpeek>

Community Tech-Talk : Understanding Cisco TrustSec (Secure Group Access) - video

<http://bit.ly/trustsec-sneakpeek-video>

If you are not yet a registered user on the community, [Click here](#) to register and become an active participant on the community.



Hope you enjoyed this little peek into the webcast.
Remember it was just a peek. Dec 16, you get a chance to see the whole thing.



Register Now: <http://bit.ly/decwebcast>

At the webcast you will be able to learn so much more and get a chance to submit questions for the expert to answer during the broadcast.
We'll see you there!