The Transformation: The World Is Our New Workspace

Any Person
Any Place
Any Device
Any Resource

BORDERLESS NETWORKS

ANext Generation Architecture to Deliver the New Workspace Experience

Right Person
Right Device
Right Place
Right Resource
The Need for More Complex Access Control …

Who are the users in my network?
What devices are in my network?
How do I enforce role-based access control?
How do I scale my access policy across my network?

Complex workforce
User and Device Mobility
Device Proliferation
Cloud/Virtualization
Cisco TrustSec or Security Group-Based Access Control

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

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

- Encryption based on **IEEE802.1AE** (AES-GCM 128-Bit)
- **Wire rate** hop by hop layer 2 encryption (1Gbps, 10Gbps)
- Key management based on 802.11n (SAP, Today), awaiting for standardization in 802.1X-REV
Cisco TrustSec aka SGBAC
Tradition access authorization methods leave some deployment concerns:
- Detailed design before deployment is required, otherwise...
- Not so flexible for changes required by today’s business
- Access control project ends up with redesigning whole network
Security Group Based Access Control allows customers:

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

- Unique 16 bit (65K) tag assigned to unique role
- Represents privilege of the source user, device, or entity
- Tagged at ingress of TrustSec domain
- Filtered (SGACL) at egress of TrustSec domain
- No IP address required in ACE (IP address is bound to SGT)
- Policy (ACL) is distributed from central policy server (ISE/ACS) or configured locally on TrustSec device

Customer Benefits

- Provides topology independent policy
- Flexible and scalable policy based on user role
- Centralized Policy Management for Dynamic policy provisioning
- Egress filtering results to reduce TCAM impact
Layer 2 SGT Frame Format

- 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 = less than baby giant frame (~1600 bytes with 1552 bytes MTU)
Traditional Access Control

- (# of sources) * (# of Destinations) * permissions = # ACEs
- Source (S1) * Destination (S1~S6) * Permission (4) = 24 ACEs for S1
- Source (S1~S4) * Destination (S1~S6) * Permission (4) = 96 ACEs for S1~4

S1 to D1 Access Control
permit tcp S1 D1 eq https
permit tcp S1 D1 eq 8081
permit tcp S1 D1 eq 445
deny ip S1 D1

ACE # grows as # of permission statement increases
How SGACL Simplifies Access Control

- \((\text{# of Source SG}) \times (\text{# of Dest SG}) \times \text{Permissions} = \# \text{ACEs}\)
- SGT10 * Dest SGTs (3) * Permission (4) = 12 ACEs for MGMT A SGT
- SRC SGTs (4) * DST SGTs (3) * Permission (4) = 48 ACEs
SGACL Effectiveness in Operation

• Assume current Firewall technology that we don’t specify specific source (source = Any)

• 400 users accessing 30 network resources with 4 permissions each

With Traditional ACL on FW

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

Traditional ACL on VLAN interface on router or FW where we can use subnet ranges for source group

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

Per source IP on port with Downloadable ACL

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

With SGACL

4 SGT (src) * 3 SGT (dst) * 4 permission = 48 ACEs
802.1AE MAC Security
The Secure Network Fabric

- **NDAC**
  - Prevents rogue endpoints and network devices from connecting to the network
  - Network Device Admission Control (NDAC) enforces strong mutual authentication of network devices before joining the fabric

- **802.1AE**
  - Provides data confidentiality & integrity for wired Ethernet throughout the Enterprise
    - Mitigates packet eavesdropping, tampering, and injection
  - Standards-based technology
    - Strong (128-bit AES-GCM), NIST-approved, 10Gb line-rate encryption
    - Leverages IEEE standards including the MACSec Key Agreement (MKA) protocol
  - Deployment versatility
    - Hop-by-hop approach supports existing packet inspection technologies (IPS, Firewall, Caching, WAN optimization/acceleration, Network monitoring)
    - Works in shared media environments (IP Phones, Desktops)

- **802.1X-2010**
  - 802.1AE Encrypted on egress interface
  - Decrypt on ingress interface
  - Packets in the clear inside the system
Confidentiality and Integrity
Securing the Data Path with Media Access Control Security (MACSec)

- Provides “WLAN / VPN equivalent” encryption (128bit AES GCM) to LAN connection
- NIST approved* encryption (IEEE802.1AE) + Key Management (IEEE802.1X-2010/MKA)
- Allows the network to continue to perform auditing (Security Services)

* National Institute of Standards and Technology Special Publication 800-38D

Note: Cat3750-X currently supports MACSec on downlink only

802.1X

Supplicant with MACSec

Data sent in clear

Authenticated User

Guest User

TrustSec™ provides encrypted data path regardless your access methods (WLAN, Remote Access, and LAN!)

MACSec Capable Devices

Encrypt

Decrypt

Note: Cat3750-X currently supports MACSec on downlink only

MACSec Link
What is MACSec?

Media Access Control (MAC) Security

- Defined by the IEEE 802.1AE standard
- Builds on authentication framework provided by IEEE 802.1X
- Derives encryption keys using MACSec Key Agreement (MKA) protocol as defined in IEEE 802.1X-Rev-2010

Secures communication for trusted components on the LAN

Provides strong encryption on a hop-by-hop basis

Designed for incremental deployment

- Protect most vulnerable devices first
- Minimize impact to the network

© 2011 Cisco and/or its affiliates. All rights reserved.
802.1AE (MACSec) Tagging

SGA Frame Format

MACSec EtherType  TCI/AN  SL  Packet Number  SCI (optional)

 MACSec Tag Format

Frame 502 (287 bytes on wire, 287 bytes captured)

Ethernet II, Src: Cisco_c2:d4:42 (00:1b:54:c2:d4:42), Dst: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)

Destination: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
Address: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)

....1 ......... ...... = IG bit: Group address (multicast/broadcast)
....0 .......... ...... = LG bit: Globally unique address (factory default)

Source: Cisco_c2:d4:42 (00:1b:54:c2:d4:42)
Address: Cisco_c2:d4:42 (00:1b:54:c2:d4:42)

....0 .......... ...... = IG bit: Individual address (unicast)
....0 .......... ...... = LG bit: Globally unique address (factory default)

Type: Unknown (0x88e5)

Data (273 bytes)

Data: 2C000001000B001B54C1EFFA0000C655C93421ED794C9842...
Frame Format for 802.1AE + SGT

- **DMAC** | **SMAC** | **802.1AE Header** | **802.1Q** | **CMD** | **ETYPE** | **PAYLOAD** | **ICV** | **CRC**

- **CMD EtherType** | **Version** | **Length** | **SGT Opt Type** | **SGT Value** | **Other CMD Options**

Cisco Meta Data

- **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 = less than baby giant frame (~1600 bytes with 1552 bytes MTU)
# MACSec Benefits and Limitations

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Endpoint Support</td>
</tr>
<tr>
<td>Strong encryption at Layer 2 protects data.</td>
<td>Not all endpoints support MACSec</td>
</tr>
<tr>
<td>Integrity</td>
<td>Network Support</td>
</tr>
<tr>
<td>Integrity checking ensures data cannot be modified in transit</td>
<td>Line-rate encryption typically requires updated hardware on the access switch</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Technology Integration</td>
</tr>
<tr>
<td>Selectively enabled with centralized policy</td>
<td>MACSec may impact other technologies that connect at the access edge (e.g. IP Phones)</td>
</tr>
</tbody>
</table>

Network Intelligence
Hop-by-hop encryption enables the network to inspect, monitor, mark and forward traffic according to your existing policies.
Cisco TrustSec is a security solution that provides policy-based access control, identity-aware networking with data integrity and confidentiality services.
Technology Overview
Network Identity & Enforcement

- Authentication - (802.1x, MAB, Web, NAC)
- Authorization - (VLAN, DACL, SXP or SGT)
- Enforcement – (SGACL and Identity Firewall)

Cisco TrustSec Technology Overview:

- I want to allow guests into the network
- I need to allow/deny iPADs in my network
- I need to ensure my endpoints don’t become a threat vector
- I need to ensure data integrity and confidentiality for my users
- I need a scalable way of authorizing users or devices in the network
- How can I set my firewall policies based on identity instead of IP addresses?

Guest Access
Profiler
Posture
MACSec encryption
Security Group Access
Identity-based Firewall
Cisco TrustSec Architecture Overview

Overlay/Appliance Mode or Infrastructure Integrated Mode

Identity Context

User, Contractor, Guest, Device Type, Access Type, Location, Posture, Time of Day

802.1X, Web Authentication, MAB Authentication Bypass, Profiling

Authorization and Enforcement

Broad Access, Limited Access, Guest/Internet

VLAN, DACL, Security Group Access, Identity Firewall

Data Integrity and Confidentiality

MACSec (802.1AE)
Cisco TrustSec Authorization and Enforcement Points

Supplicant

Guest Users

802.1X

IP Phones

Cisco® Catalyst® Switch

PEP – Policy Enforcement Point

Nexus 7K Switch

NAC Guest Server

ACS/ISE

Directory Service

NAC Profiler Server

Protected Resources

Control Plane RADIUS

Controllers

NAC

Supplicant

Users, Endpoints

Network-Attached Device

Campus Network
SGT Assignment
SGT Assignment

Campus/Mobile endpoints

- Every endpoint that touches TrustSec domain is classified with SGT
- SGT can be sent to switch via RADIUS authorization after:
  - via 802.1X Authentication
  - via MAC Authentication Bypass
  - via Web Authentication Bypass
  - Or Static IP-to-SGT binding on SW

Data Center / Servers

- Every server that touches TrustSec domain is classified with SGT
- SGT is usually assigned to those servers:
  - via Manual IP-to-SGT binding on TrustSec device
  - via IP-to-Port Mapping
Creating the SGT Policy

<table>
<thead>
<tr>
<th>Source SGT</th>
<th>Destination SGT</th>
<th>Doctor (SGT x)</th>
<th>Finance (SGT x)</th>
<th>Global (SGT x)</th>
<th>Shared Services (SGT x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctor (SGT x)</td>
<td>IT Maintenance ACL</td>
<td>Web Access</td>
<td>Web File Share</td>
<td>Web File Share</td>
<td>SSH RDP File Share</td>
</tr>
<tr>
<td>Finance (SGT x)</td>
<td>Web</td>
<td>SSH RDP File Share</td>
<td>Full Access</td>
<td>SSH RDP File Share</td>
<td></td>
</tr>
<tr>
<td>Global (SGT x)</td>
<td>Web</td>
<td>SSH RDP File Share</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
permit tcp dst eq 136
permit tcp dst eq 137
permit tcp dst eq 138
permit tcp dst eq 139
deny ip
SGT Assignment for Roles

**Dynamic SGT Assignment For Endpoint**

**Static SGT Assignment For Servers**

- **IT Portal (SGT 4)** 10.1.100.10
- **IT Admin (SGT 5)**
- **Doctor (SGT 7)**
- **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

**Users, Endpoints**

- **802.1X, MAB, LWA**
- **Catalyst® 3750-E**
- **Nexus® 7000 Core**
- **Nexus® 7000 Distribution**
- **Catalyst® 4948**
- **ACS v5.1**

**For**

- **Endpoints**
- **Servers**
How To Assign SGT To Endpoint

MAC:0050.56BC.14AE

Port: 0050.56BC.14AE Gig1/0/1 5

IP Address: 10.1.10.102

Access Switch has IP to SGT Binding Now

cisco-av-pair=cts:security-group-tag=0005-01

<sgt-value-in-hex>-<rev#>
### Generating SGT for Role

<table>
<thead>
<tr>
<th>Name</th>
<th>SGT (Dec / Hex)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>0 / 0000</td>
<td>Unknown Security Group</td>
</tr>
<tr>
<td>CTS-Device-SGT</td>
<td>2 / 0002</td>
<td>Device SGT for all CTS capable device</td>
</tr>
<tr>
<td>HR Servers</td>
<td>3 / 0003</td>
<td>HR Server Group SGT</td>
</tr>
<tr>
<td>IT Servers</td>
<td>4 / 0004</td>
<td>IT Server Group SGT</td>
</tr>
<tr>
<td>IT Administrator</td>
<td>5 / 0005</td>
<td>IT Administrator SGT</td>
</tr>
<tr>
<td>HR Administrator</td>
<td>6 / 0006</td>
<td>HR Administrator SGT</td>
</tr>
<tr>
<td>Doctor</td>
<td>7 / 0007</td>
<td>Doctor Group SGT</td>
</tr>
<tr>
<td>Public Server</td>
<td>8 / 0008</td>
<td>SGT for Public Server (Portal) Group</td>
</tr>
<tr>
<td>Internal Server</td>
<td>9 / 0009</td>
<td>SGT for Internal Server Group</td>
</tr>
<tr>
<td>Record DB</td>
<td>10 / 000A</td>
<td>SGT for Confidential Database Server Group</td>
</tr>
<tr>
<td>Staff</td>
<td>11 / 000B</td>
<td>Hospital Staff Group SGT</td>
</tr>
<tr>
<td>IP Phone</td>
<td>12 / 000C</td>
<td>SGT for IP Phone Devices</td>
</tr>
<tr>
<td>Call Manager</td>
<td>13 / 000D</td>
<td>SGT for CUCM</td>
</tr>
<tr>
<td>Asset</td>
<td>14 / 000E</td>
<td>Hospital Asset Device SGT</td>
</tr>
<tr>
<td>Guest</td>
<td>15 / 000F</td>
<td></td>
</tr>
</tbody>
</table>

SGT value is automatically from 2~. SGT=0 is special SGT for Unknown
SGACL Policy on ACS / ISE

1. General
   - Name: IT_Maintenance_ACL
   - Description: Permit FTP, SSH, SMB, RDP, and ICMP

2. Configure Security Groups
   - Source Security Group: IT Administrator
   - Destination Security Group: Record DB

   General
   - Description: 

   ACLs
   - Select the set of Security Group ACLs for this cell. The ACLs are used at the egress point if the security group tag of the source and destination match the coordinates of the cell.

   Available: S2S_Permit_IT_Server
              Permit_ICMP Only
              TS_DHCP_Traffic
              Permit_Wb_On
              Permit_Wb_WinFile
              Permit_RDP_WinFile
              S2S_Deny_All
              Permit_ICMP_RDP
              S2S_Permit_Wb_Sec

   Selected: IT_Maintenance_ACL

   Apply a permit-ip or deny-ip ACL as a final catch all rule.
   - Permit IP
   - Deny IP
   - None (No closing ACL)

3. Access Policies > TrustSec Access Control > Egress Policy

   Destination Source
   Doctor (7 / 0007) Guest (15 / 000F)
   IT Administrator (5 / 0005) Staff (11 / 000B)

   Internal Server IT Servers Public Server Record DB
   (9 / 0009) (3 / 0004) (8 / 0008) (10 / 000A)
   Permit_Wb_On Deny IP Permit_Wb_On Permit_Wb_WinFileShare
   Permit_Wb_On Deny IP Permit_Wb_On Permit_Verb_Wb_WinFile
   Permit_IP Permit_IP Permit_IP Permit_IP
   Permit_Wb_On Deny IP Permit_Wb_On Deny IP

   IT_Maintenance_ACL
Sample 802.1X Authorization Policy for SGT Assignment

**Rule Name**
- Name: IT Admin Group

**Condition Statement**
- AD1:ExternalGroups:
  - contains any
  - cts.local/Users/IT Admin Group

**Authorization Profile**
- Permit Access

**SGT**
- Security Group: IT Administrator
Policy Download

CTS7K-DC# show cts role-based policy

sgt:5
dgt:4 rbact:Permit IP
  permit ip

sgt:5
dgt:8 rbact:Permit IP
  permit ip

sgt:5
dgt:9 rbact:Permit IP
  permit ip

sgt:5
dgt:10 rbact:IT_Maintenance_ACL
  permit tcp dst eq 20 log
  permit tcp dst eq 21 log
  permit tcp dst eq 22 log
  permit tcp dst eq 445 log
  permit tcp dst eq 135 log
  permit tcp dst eq 136 log
  permit tcp dst eq 137 log
  permit tcp dst eq 138 log
  permit tcp dst eq 139 log
  permit tcp dst eq 3389 log
  permit icmp log
  deny ip

<skip>
Security Group based Access Control
How Enforcement Works

NX-OS CLI
cts role-based enforcement

IT Admin (SGT 5)

Users, Endpoints

802.1X

Catalyst® 3750-E

Campus Network

Nexus® 7000 Core

Nexus® 7000 Distribution

Web

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

IT Portal (SGT 4)
10.1.100.10

ACS v5.1
Active Directory

VLAN100

VLAN200

SGT Enforcement

Untagged Frame
Tagged Frame
Security Group based Access Control
How Enforcement Works

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]
SGA High Level Overview

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

Use Case 1

TrustSec to cover campus network as well as Data Center network

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

<table>
<thead>
<tr>
<th>SRC \ DST</th>
<th>Server A (111)</th>
<th>Server B (222)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A (10)</td>
<td>Permit all</td>
<td>SGACL-B</td>
</tr>
<tr>
<td>User B (20)</td>
<td>Deny all</td>
<td>SGACL-C</td>
</tr>
</tbody>
</table>
SGA: Branch LAN Deployment

Use Case 2

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

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

<table>
<thead>
<tr>
<th>SRC \ DST</th>
<th>Server A (111)</th>
<th>Server B (222)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A (10)</td>
<td>Permit all</td>
<td>SGACL-B</td>
</tr>
<tr>
<td>User B (20)</td>
<td>Deny all</td>
<td>SGACL-C</td>
</tr>
</tbody>
</table>
**SGA: Intra Data Center Deployment**

### Use Case 3

**TrustSec to cover Intra Data Center for server traffic segmentation**

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

<table>
<thead>
<tr>
<th>SRC \ DST</th>
<th>Server A (111)</th>
<th>Server B (222)</th>
<th>Server C (333)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server A (111)</td>
<td>---</td>
<td>SGACL-A</td>
<td>Permit all</td>
</tr>
<tr>
<td>Server B (222)</td>
<td>Permit all</td>
<td>---</td>
<td>SGACL-B</td>
</tr>
<tr>
<td>Server C (333)</td>
<td>Deny all</td>
<td>Deny all</td>
<td>---</td>
</tr>
</tbody>
</table>
• Dynamic policy enforcement between servers within same isolated VLAN (Private VLAN)

• Dynamic policy enforcement between servers in different community VLANs
NDAC
Network Device Admission Control (NDAC) provides strong mutual authentication (EAP-FAST) to form trusted domain.

- Only SGT from trusted peer is honored.
- Authentication leads to Security Association Protocol (SAP) to negotiate keys and cipher suite for encryption automatically (mechanism defined in 802.11i).
- 802.1X-REV will succeed and replace SAP.
- Trusted device acquires trust and policies from ACS server.

**Customer Benefits**

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

- NDAC validates peer identity before peer becomes the circle of Trust!
  - The first device to authenticate against ACS is called TrustSec Seed Device
  - Seed Device becomes authenticator to its peer supplicant
  - Role determination process selects both Authenticator and Supplicant role
  - NDAC utilizes EAP-FAST/MSCHAPv2
- Credential (including PAC) is stored in hardware key store
As device connects to its peer, TrustSec domain expands its border of trust

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

- **Security Association Protocol (SAP)** to negotiate keys and cipher suite for encryption automatically
- Negotiation starts after successful authentication / authorization for NDAC
- Protocol communication only happens between Supplicant and Authenticator (No ACS involvement)
- At the end of SAP, both supplicant and authenticator have same session key
- Session key is used to encrypt traffic on the link
- Session key is derived from the PMK (learned by both device from ACS during authentication) and some random numbers shared during SAP
- Perform rekey periodically
SGT Exchange Protocol (SXP)

- SGT native tagging requires hardware (ASIC) support
- **SGT eXchange Protocol (SXP)** is used to exchange IP-to-SGT bindings between TrustSec capable and incapable device
- Currently supported on Catalyst 6500, 4500/4900, 3560/3750 and Nexus 7000 switch
- Based on TCP with MD5 authentication
- Support single hop or multi-hop SXP
- SXP accelerates initial deployment of SGT/SGACL without immediate hardware upgrade
Legacy Platform Support with SXP

- SGT native tagging requires hardware (ASIC) support
- Non-TrustSec hardware capable devices can still receive SGT attributes from ACS for authenticated users or devices, and then forward the IP-to-SGT binding to a TrustSec RBACL capable device for tagging & enforcement
- SGT eXchange Protocol (SXP) is used to exchange IP-to-SGT bindings between TrustSec capable and incapable device
- Currently Catalyst 6500 and 4500/4900 and Nexus 7000 switch platform support SXP
- SXP accelerates deployment of SGACL by without extensive hardware upgrade for TrustSec
Cisco TrustSec Milestones
TrustSec 1.0

Trustsec Launch at RSA 2010 introduced an identity-enabled network access architecture for the Borderless Network spanning multiple Cisco products and technologies.

**Infrastructure**
- Identity-enabled networking infrastructure:
  - Catalyst 3K/3K-X
  - Catalyst 4K
  - Catalyst 6K
  - Nexus 7K
  - ISR (integrated switch)

**Policy & Management**
- Cisco Secure Access Control System (ACS) Release 5.1

**Identity**
- Identity 4.1
- Authentication: 802.1x, MAB, Web
- Enforcement: DACL, VLANs, Security Group Access (SXP, SGT, SGACL)

**Security Services**
- Posture, Remediation and Guest Access
  - NAC Appliance
  - NAC Guest Server
  - NAC Profiler
- Link Encryption (MACSEC)

**Client**
- Cisco Secure Services Client (CSSC)
- Cisco NAC Agent
## TrustSec 1.99: 802.1x Features

<table>
<thead>
<tr>
<th>X-Platform Features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1x authentication</td>
<td>Open Access</td>
</tr>
<tr>
<td>MAC Authentication Bypass</td>
<td>Wake-on-LAN (WoL)</td>
</tr>
<tr>
<td>Local Web Authentication</td>
<td>Radius supplied time out</td>
</tr>
<tr>
<td>Flexible authentication</td>
<td>Critical port (IAB)</td>
</tr>
<tr>
<td>Multi-host</td>
<td>Inactivity timer (MAB and 802.1x)</td>
</tr>
<tr>
<td>Multi-domain Authentication (MDA)</td>
<td>CDP 2nd port disconnect</td>
</tr>
<tr>
<td>Multi-Authentication</td>
<td>Integration with DAI, IPSG, port security</td>
</tr>
<tr>
<td>VLAN assignment</td>
<td>Radius accounting</td>
</tr>
<tr>
<td>MDA with dynamic Voice VLAN assignment</td>
<td>Conditional logging/debugging</td>
</tr>
<tr>
<td>Guest VLAN, Auth-Fail VLAN</td>
<td>Single Host</td>
</tr>
<tr>
<td>Downloadable ACL</td>
<td>Filter ID</td>
</tr>
</tbody>
</table>
## TrustSec 2.0 - What’s New

<table>
<thead>
<tr>
<th>Business Problem</th>
<th>Available with TrustSec 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>I’d like to simplify my role-based access control deployment</td>
<td>Integrated policy manager and client:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Identity Services Engine</strong> with integrated profiling, guest, posture</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anyconnect 3.0</strong> with 802.1X/CSSC, MACSec, RDP and more</td>
</tr>
<tr>
<td>I need to ensure my endpoints don’t bring vulnerability into my network</td>
<td>• 802.1X with Posture</td>
</tr>
<tr>
<td></td>
<td>• Simplified Wireless with posture enforcement on WLC</td>
</tr>
<tr>
<td>I need to identify the wireless devices in my network (like iPADs)</td>
<td>Profiler with Wireless. Authorization supported with 802.1X (no MAB, Guest)</td>
</tr>
<tr>
<td>I am worried about confidentiality of data in my LAN</td>
<td>MACSec switch to switch encryption (Cat 3K and Cat 6K) with Cat 4K preview</td>
</tr>
<tr>
<td>I’d like to have scalable role-based access control in my network with enforcement in existing DC platforms</td>
<td>SGT/SGACL enforcement on the <strong>Cat 6K SUP 2T</strong></td>
</tr>
<tr>
<td>I’d like to have scalable role-based access control in my network with tagging for partner/contractor environment</td>
<td>TrustSec enabled <strong>ASR1K</strong> platforms (SXP/SGT) at WAN aggregation layer</td>
</tr>
<tr>
<td>I need my scalable role-based access control method to work in virtualized environment</td>
<td>SGA tested/validated in a <strong>VDI</strong> environment</td>
</tr>
</tbody>
</table>
Introducing Identity Services Engine 1.0

TrustSec 2.0

New Identity Use Cases
Endpoint Posture with 802.1X
Integrated Profiling for wired/wireless

Security Group Access Platform Enhancements
New platforms for enforcement and tagging
VDI Use Case Validation

MACSec Enhancements
Switch to Switch Encryption
Pre TrustSec 2.0:
Wired Use Cases - Authentication & Profiling
• Identity 4.1 (802.1X etc)
  • Monitor, low impact, security modes
  • NEAT
  • MAC move/replace
• CoA
• Profiling – NAC Profiler
• Auto Smartports

With TrustSec 2.0
Wired Use Case –
• Integrated services with ISE:
  • Profiling
  • Guest
  • (NEW!!) Posture with 802.1X
• Identity enhancements:
  • VLAN assignment in multi-auth
  • Critical voice VLAN
• AnyConnect 3.0
**Pre TrustSec 2.0:**

Wireless Use Case -
Authentication, profiling and posture with disparate elements
- 802.1X authentication
- Posture – NAC Posture
- Guest – NAC Guest

**With TrustSec 2.0**

Wireless Use Case –
- Unified services with ISE
- Profiling (after authentication, no MAB)
- Posture
  - Pre Wireless 7.0 MR1 – use inline PEP (no COA or URL redirect)
  - Post Wireless 7.0 MR1 – use with WLC
- Guest (Local Web Auth)
TrustSec 2.0
Security Group Access Expanded Platform Support

Cisco ASR 1000
- Ability to tag/propagate identity information at WAN aggregation layer for partner/contractor or site-to-site VPN use case
- Feature – SXP, SGT

Cisco Catalyst 6K (SUP-2T)
- Expands the ability to enforce based on TrustSec network identity on Nexus 7K and Cat 6K (SUP2T) SGACL enforcement now on Nexus 7K and Catalyst 6K (SUP-2T)
- Feature – SGACL

I’m a contractor. My group is HR.

802.1X/MAB/Web Auth.

SGACL

Finance (SGT=4)

HR (SGT=10)

Aggregation or Data Center

Contactor & HR SGT = 100

SXP

ISR

WAN

ASR

SGT 10
**VDI Solution Components**

- **SGT Role Assignment** – Any Catalyst switch with Multi-Auth
- **SGACL Enforcement Switch** – Catalyst 6K or Nexus 7K
- Two options:
  1. User mapped to “known” VM via static mapping to machine
     - Supplicant - Machine Auth via native supplicant on server
  2. User mapped to “any” VM
     - Anyconnect (with RDP) – intercepts user RDP credentials for 802.1X
VDI Security Group Access Use case

- Ituser SGT 12
- Doctor SGT 13
- Untagged Traffic
- SGT 12 Tagged Traffic
- SGT 13 Tagged Traffic
VDI Security Group Access UseCase

- Ituser SGT 12
- Doctor SGT 13

Diagram showing VDI Connection Broker, Control Plane, IT VM, Doc. VM, Record Server, IT Server, and AD with traffic types: Untagged Traffic, SGT 12 Tagged Traffic, SGT 13 Tagged Traffic.

Table showing SGACL Matrix with Source Groups and Destination Groups:
- DS: ☑️
- PS: ☒️
TrustSec 2.0
MACSec Encryption

Already supported:
• MACSec encryption supported in DC between Nexus 7000

TrustSec 2.0 adds:
• Switch to switch encryption: Catalyst 3K-X, 6500 or Nexus 7000
• Downlink encryption from AnyConnect to Catalyst 3KX (MKA)
• Note that encryption uses SAP, not MKA
TrustSec 2.0
Switch to Switch Encryption Enables End-to-End Data Integrity

Cisco Catalyst 3KX
• Switch-to-Switch Encryption
• 1G – use existing ports
• 10G – requires new 3KX services module (FCS July 2011)

Cisco Catalyst 6K (SUP-2T)
• Switch-to-Switch Encryption
• SUP 2T Module (FCS July 2011)

Cisco Catalyst 4K
• Switch-to-Switch Encryption
• 4500E : Sup7-E uplinks and 47xx series line cards (FCS 2H CY11)
Cisco TrustSec
Near Future :o)
Partner to Data Center (ID FW Integration)

Identity acquisition via IPsec, SSL VPN or Identity over EAPoUDP