Security Group Tagging

Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag.

Cisco TrustSec-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L3) layer. This feature is called Layer 3 (L3)-SGT Imposition. It allows ethernet interfaces on the device to be enabled for L3-SGT imposition so that the device can insert an SGT in the packet to be carried to its next hop ethernet neighbor. SGT-over-Ethernet is a method of hop-by-hop propagation of SGT embedded in clear-text (unencrypted) ethernet packets. The inline identity propagation is scalable, provides near line-rate performance and avoids control plane overhead.

The Cisco TrustSec with SGT Exchange Protocol V4 (SXPv4) feature supports Cisco TrustSec metadata-based L3-SGT. When a packet enters a Cisco TrustSec-enabled interface, the IP-SGT mapping database (with dynamic entries built by SXP and/or static entries built by configuration commands) is analyzed to learn the SGT corresponding to the source IP address of the packet, which is then inserted into the packet and carried throughout the network within the Cisco TrustSec header.

As the tag represents the group of the source, the tag is also referred to as the Source Group Tag (SGT). At the egress edge of the network, the group assigned to the packet's destination becomes known. At this point, access control can be applied. With Cisco TrustSec, access control policies are defined between the security groups and are referred to as Security Group Access Control Lists (SGACL). From the view of any given packet, SGACL is simply being sourced from a security group and destined for another security group.

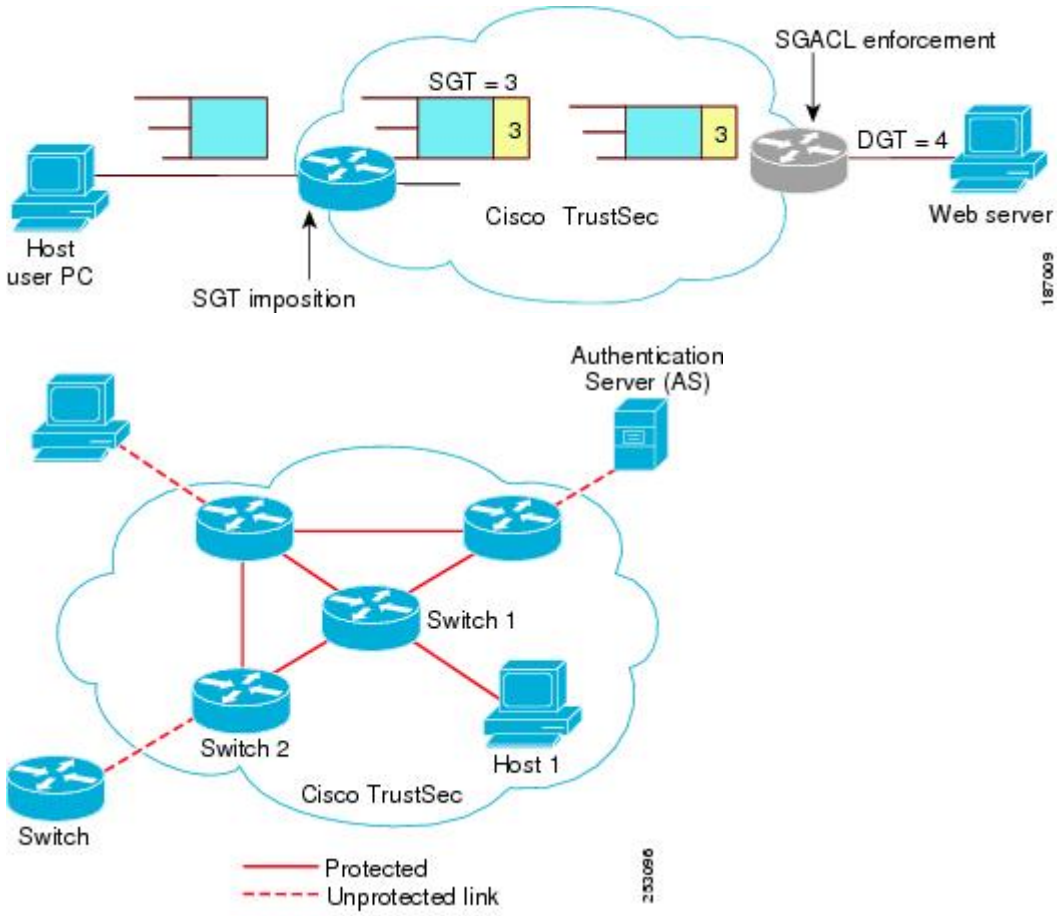
The SGT tag received in a packet from a trusted interface is propagated to the network, and is also be used for Identity firewall classification. When IPsec support is added, the received SGT tag is shared with IPSec for SGT tagging.

A network device at the ingress of Cisco TrustSec cloud needs to determine the SGT of the packet entering the Cisco TrustSec cloud so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec cloud. The SGT of a packet can be determined with these methods:

- SGT field on Cisco TrustSec header: If a packet is coming from a trusted peer device, it is assumed that the Cisco TrustSec header carries the correct SGT field. This situation applies to a network that is not the first network device in the Cisco TrustSec cloud for the packet.
- SGT lookup based on source IP address: In some cases, the administrator may manually configure a policy to decide the SGT of a packet based upon the source IP address. An IP address to SGT table can also be populated by the SXP protocol.

The following figures explains the topologies:

Figure 1: Cisco TrustSec Network



Limitations for Security Group Tag

The following are the limitations of the Cisco TrustSec feature:

- SGT and SGACL enforcement on switchport are not supported.
- Dynamic SGT and SGACL for ipv6 is not supported.
- The **cts manual** command is not support on SVI interface, while they are supported on on-board L3 interface.

Configuring Security Group Tagging for Dynamic SGT and SGACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aa new-model`	Enables AAA..
Step 4	**aaa authentication dot1x***{default | listname}* **group***group-name* **Example:** `Device(config)# aaa authentication dot1x default group ise`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 5	**aaa authorization network***{default | listname}***group** *group-name* **Example:** `Device(config)# aaa authentication network default group coa-ise`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 6	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.

	Command or Action	Purpose
Step 7	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 8	**aaa group server radius {radius | tacacs+}***group-name* **Example:** `Device(config)# aaa group server radius coa-ise`	Defines the AAA server group with a group name. Example: Device(config)# aaa group server radius group1 • All members of a group must be the same type, that is, RADIUS or TACACS+. This command puts the device in server group RADIUS configuration mode.
Step 9	**radius server** *server-name* **Example:** `Device(config)# radius server cts`	Specifies the name for the RADIUS server.
Step 10	**server** *ip-address***[auth-port***port-number***[acct-port***port-number* **Example:** `Device(config-sg-radius)# address ipv4 %{ise.ip} auth-port 1812 acct-port 1813`	Specifies the name for the RADIUS server.
Step 11	**pac key** *encyrption-key* **Example:** `Device(config-sg-radius)# pac key 0 cisco123`	Specifies the PAC encryption key (overrides the default). • The encryption-key can be **0** (specifies that an unencrypted keys follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
Step 12	**policy-map type control subscriber***control-policy-name* **Example:** `Device(config)# policy-map type control subscriber simple_dot1x`	Defines a control policy for subscriber sessions.
Step 13	**event** *event-name***[match-all | match-first]** **Example:**	Specifies the type of event that triggers actions in a control policy if conditions are met.

	Command or Action	Purpose
	`Device(config-event-control-policymap)# event session-started match-all`	• match-all is the default behavior.
Step 14	**priority-number class {control-class-name | always}[do-all | do-until-failure | do-until-success]** **Example:** `Device(config-event-control-policymap)# 10 class always do-until-failur`	Associates a control class with one or more actions in a control policy. • A named control class must first be configured before specifying it with the control-class-name argument.. • do-until-failure is the default behavior.
Step 15	**action-number authenticate using {dot1x | mab | webauth}aaa {authc-list authc-list-name | authz-list authz-list-name]} [merge] [parameter-map map-name] [priority priority-number] [replace | replace-all] [retries number {retry-time seconds}** **Example:** `Device(config-event-control-policymap)# 10 authenticate using dot1x`	Optional) Initiates the authentication of a subscriber session using the specified method.
Step 16	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet0/1`	Enter the interface to be added to the VLAN.
Step 17	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 22`	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094
Step 18	**switchport access mode** **Example:** `Device(config-if)# switchport mode access`	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094

	Command or Action	Purpose
Step 19	**access-session closed** **Example:** `Device(config-if)# access-session closed`	The **access-session closed** command closes access to a port, preventing clients or devices from gaining network access before authentication is performed.
Step 20	**access-session port-control {auto | force-authorized | force-unauthorized }** **Example:** `Device(config-if)# access-session port-control auto`	Sets the authorization state of a port.
Step 21	**policy-map type control subscriber***control-policy-name* **Example:** `Device(config-if)# policy-map type control subscriber simple_coa`	Defines a control policy for subscriber sessions.
Step 22	**dot1x pae [supplicant | authenticator | both]** **Example:** `Device(config-if)# dot1x pae authenticator`	[authenticator | Sets the Port Access Entity (PAE) type. • supplicant—The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator. • authenticator-—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant. • both—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.
Step 23	**end** **Example:** `Device(config-if)# end`	Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode.

Configuring SGT Tagging

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode. aaa authorization network cts-list group
Step 3	**aaa authorization network***{default | lcts-list}* **group***group-name* **Example:** `Device(config)# aaa authorization network cts-list group coa-ise`	Configures the device to use RADIUS authorization for all network-related service requests.
Step 4	**cts authorization list***mlist* **Example:** `Device(config)# cts authorization list cts-list`	Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator.
Step 5	**cts sgt** *{sgt_number}* **Example:** `Device(config)# cts sgt 4`	Enables Cisco TrustSec.
Step 6	**interface** *interface-id***VLAN***VLAN-id* **Example:** `Device(config)# interface Vlan32`	Enter the interface to be added to the VLAN.
Step 7	**cts role-based {sgt-map |sgt }** **Example:** `Device(config-if)# cts role-based sgt-map sgt`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces..

	Command or Action	Purpose
Step 8	**cts role-based enforcement** **Example:** `Device(configif)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.
Step 9	**ip access-list role-based** *rbacl-name* **Example:** `Device(configif)# ip access-list role-based sgacl1`	Creates a Role-based ACL and enters Role-based ACL configuration mode.
Step 10	**access-list permit icmp** **Example:** `Device(config-rb-acl)# 10 permit icmp`	
Step 11	**ipv6 access-list role-based** *rbacl-name* **Example:** `Device(configif-rb-acl)# ipv6 access-list role-based v6_acl`	Creates a Role-based ACL and enters Role-based ACL configuration mode.
Step 12	**sequence 10 permit icmp echo-reply** *ip-address* **Example:** `Device(configif-rb-acl)# sequence 10 permit icmp echo-reply`	
Step 13	**exit** **Example:** `Device(configif-rb-acl)# exit`	
Step 14	**cts role-based monitor enable** *from {sgt_num} to {dgt_num}***[ipv4 | ipv6]** **Example:** `Device(configif)# cts role-based monitor enable from 4 to 32 sgacl1`	Enables monitor mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4 | ipv6] Step 4 Group Tag (SGT)- Destination Group Tag (DGT) pair).

	Command or Action	Purpose
Step 15	**cts role-based permissions** *from {sgt_num} to {dgt_num}***[ipv4 | ipv6]** **Example:** `Device(configif)# cts role-based permissions from 4 to 32 ipv6 v6_acl`	Enables role-base permissions mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4 | ipv6] Step 4 Group Tag (SGT)-Destination Group Tag (DGT) pair).
Step 16	**end** **Example:** `Device(config-if)# end`	Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode.

Example 1: Static Security Group Tagging and Security Group ACL

This example shows how to enable an interface on the device for L3-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec.

```
Device# configure terminal
Device(config)# cts authorization list cts-list
Device(config)#cts sgt 4
Device(config)#interface Vlan32
Device(config-if)#ip address 192.168.32.2 255.255.255.0
Device(config-if)#ipv6 address 2001:DB8::1
Device(config-if)#cts role-based sgt-map sgt 32
Device(config-if)#cts role-based enforcement
Device(config-if)#ip access-list role-based sgacl1
Device(config-rb-acl#10 permit icmp
Device(config-rb-acl)#exit
Device(config)#ipv6 access-list role-based v6_acl
Device(config-rb-acl)#sequence 10 permit icmp echo-reply
Device(config-rb-acl)#cts role-based permissions from 4 to 32 sgacl1
Device(config-rb-acl)#cts role-based permissions from 4 to 32 ipv6 v6_acl
```

Example 2: Dynamic Security Group Tagging and Security Group ACL

This example shows how to enable an interface on the device for L3-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)#aaa authentication dot1x default group coa-ise
Device(config)#aaa authorization network default group coa-ise
Device(config)#dot1x system-auth-control
```

```
Device(config)#aaa group server radius coa-ise
Device(config)#server name coa
Device(config)#radius server coa
Device(config-sg-radius)#address ipv4 %{ise.ip} auth-port 1812 acct-port 1813
Device(config-sg-radius)#pac key 0 cisco123
Device(config-sg-radius)#exit
Device(config)#policy-map type control subscriber simple_coa
Device(config)#event session-started match-all
Device(config)#10 class always do-until-failure
Device(config)#10 authenticate using dot1x
Device(config)#interface gigabitethernet0/1
Device(config-if)#switchport access vlan 22
Device(config-if)#switchport mode access
Device(config-if)#access-session closed
Device(config-if)#access-session port-control auto
Device(config-if)#dot1x pae authenticator
Device(config-if)#service-policy type control subscriber simple_coa
```

Note The Dynamic Security Group Tagging and Security Group ACL are configured on ISE server, after the 802.1x client is authenticated by ISE server. Subsequently, the corresponding SGT and SGACL will be downloaded from ISE and applied to the client.

Troubleshoot the Security Group Tagging Configuration

You can use the following commands to troubleshoot the Cisco TrustSec configuration:

- **debug cts all**
- **debug rbm bindings debug**
- **debug condition interface <intf-name>**
- deb cts authorization events verbose
- **debug radius**

Feature History for Cisco TrustSec

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature Information for Cisco TrustSec

Feature Name	Releases	Feature Informatio
Cisco TrustSec Support on Cisco 1000 Series ISR SVI interface	IOS XE 17.5.1a	Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag. (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.