Overview of Cisco TrustSec

Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls. Cisco TrustSec is defined in three phases: classification, propagation and enforcement.

When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile.

After user traffic is classified, then the SGT is propagated from where classification took place, to where enforcement action is invoked. This process is called propagation. Cisco TrustSec has two methods of SGT propagation: inline tagging and SXP.

With inline tagging, the SGT is embedded into the ethernet frame. The ability to embed the SGT within an ethernet frame does require specific hardware support. Therefore network devices that do not have the hardware support use a protocol called SXP (SGT Exchange Protocol). SXP is used to share the SGT to IP address mapping. This allows the SGT propagation to continue to the next device in the path.

Finally an enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router, or switch. The enforcement device takes the source SGT and looks it up against the destination SGT to determine if the traffic should be allowed or denied. If the enforcement device is a Cisco firewall, then it also allows stateful firewall processing and IPS deep packet inspection using the same source SGT in a single firewall rule.

For more information about classification and enforcement, refer to Cisco TrustSec Quick Start Configuration Guide.

- SGT Inline Tagging, on page 1
- SGT Inline Tagging for IPv6 Traffic, on page 2
- CTS Credentials, on page 3
- Configuring SGT Inline Tagging, on page 3
- Configuring CTS Credentials, on page 5
- Example: Configuring SGT Inline Tagging, on page 6
- Feature Information for Overview of Cisco TrustSec, on page 6

SGT Inline Tagging

Each security group in a CTS domain is assigned a unique 16-bit tag called the “Scalable 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.

CTS-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L2) layer. This feature is called "L2-SGT Imposition." It allows Ethernet interfaces on the device to be enabled for L2-SGT imposition so that 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. Inline identity propagation is scalable, provides near line-rate performance and avoids control plane overhead.

The Cisco TrustSec with SXPv4 feature supports CTS Meta Data (CMD) based L2-SGT. When a packet enters a CTS 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 CTS 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, the access control can be applied. With CTS, 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, it is simply being sourced from a security group and destined for another security group.

SGT Inline Tagging for IPv6 Traffic

The following are the considerations for SGT inline tagging for IPv6 traffic:

- **Global Unicast IPv6 packet**: The SGT value corresponding to the unicast source IPv6 address is propagated and received in the CTS CMD header at various layers, that is, basic ethernet header, 802.1Q, Q-in-Q, IPSec header, and GRE header.
- **IPv6 Multicast Packet**: The SGT propagation of IPv6 source address in a IPv6 multicast packet is not a supported functionality on routing devices.

Restrictions for SGT Inline Tagging IPv6 Traffic

- SGT inline tagging for Tunneling of IPv6 packet over V4 transport & IPv4 packet over V6 transport is not supported.
- IPv6 IPSec inline SGT tagging is not supported on ISR4K based platforms. However, it works on ASR 1000 and CSR platforms.
- SGT Inline Tagging is not supported on IPv6 packets with link-local addresses, loopback address or unspecified addresses.

Restrictions for CTS in IPv6 Deployments

- Protected Access Credentials (PAC) provisioning over IPv6 RADIUS transport is not supported.
- CTS SGACL and environment data (ENV-data) download over IPv6 RADIUS is not supported.
- TrustSec server-list supports only IPv4 addresses and not IPv6.
- SXP peer-to-peer connections over IPv6 is not supported.

CTS Credentials

CTS requires each device in the network to identity itself uniquely. For use in TrustSec Network Device Admission Control (NDAC) authentication, use the **cts credentials** command to specify the Cisco TrustSec device ID and password for this device to use when authenticating with other Cisco TrustSec devices and for provisioning the PAC (Protected Access Credentials) with EAP-FAST. The CTS credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the CTS credential information is saved in the keystore, not in the startup-config. Those credentials are stored in the keystore, eliminating the need to save the running-config. To display the CTS device ID, use the **show cts credentials** command. The stored password is never displayed.

To change the device ID or the password, reenter the command. To clear the keystore, use the **clear cts credentials** command.

Note When the CTS device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because the PACs are associated with the old device ID and are not valid for a new identity.

Configuring SGT Inline Tagging

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**gigabitethernet** *port* | **vlan** *number*}
4. **cts manual**
5. **propagate sgt**
6. **policy static sgt** *tag* [**trusted**]
7. **end**
8. **show cts interface brief**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**interface** {**gigabitethernet** *port* | **vlan** *number*} **Example:** `Device(config)# interface gigabitethernet 0`	Enters the interface on which CTS SGT authorization and forwarding is enabled.
Step 4	**cts manual** **Example:** `Device(config-if)# cts manual`	Enables the interface for CTS SGT authorization and forwarding. Enters CTS manual interface configuration mode.
Step 5	**propagate sgt** **Example:** `Device(config-if-cts-manual)# propagate sgt`	Enables CTS SGT propagation on an interface. Use this command in situations where the peer device is not capable of receiving SGT over Ethernet packets (that is, when a peer device does not support Cisco Ethertype CMD 0x8909 frame format).
Step 6	**policy static sgt** *tag* [**trusted**] **Example:** `Device(config-if-cts-manual)# policy static sgt 77`	Configures a static SGT ingress policy on the interface and defines the trustworthiness of an SGT received on the interface. **Note** The **trusted** keyword indicates that the interface is trustworthy for CTS. The SGT value received in the Ethernet packet on this interface is trusted and will be used by the device for any SG-aware policy enforcement or for purpose of egress-tagging.
Step 7	**end** **Example:** `Device(config-if-cts-manual)# end`	Exits CTS manual interface configuration mode and enters privileged EXEC mode.

Step 8	**show cts interface brief**
	Example:
	`Device# show cts interface brief`
	`Interface GigabitEthernet0/0`
	`  CTS is enabled, mode:  MANUAL`
	`  Propagate SGT:  Enabled`
	`  Peer SGT assignment:  Trusted`
	`Interface GigabitEthernet0/1`
	`  CTS is enabled, mode:  MANUAL`
	`  Propagate SGT:  Disabled`
	`  Peer SGT assignment:  Untrusted`
	`Interface GigabitEthernet0/3`
	`  CTS is disabled.`
		Displays CTS configuration statistics for the interface.

Configuring CTS Credentials

SUMMARY STEPS

1. **enable**
2. **cts credentials id** *cts-id* **password** *cts-pwd*
3. **show cts credentials**
4. **show keystore**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cts credentials id** *cts-id* **password** *cts-pwd* **Example:** `Device# cts credentials id atlas password cisco123`	Specifies the Cisco TrustSec device ID and password for this device to use when authenticating with other CTS devices with EAP-FAST.
Step 3	**show cts credentials** **Example:** `Device# show cts credentials`	Displays the Cisco TrustSec (CTS) device ID.

Step 4	**show keystore**
	Example:
	****Note that the following is the sample output of the command till Cisco IOS XE Everest release 16.5.****
	`Device# show keystore`
	`Using software keystore emulation.`
	`Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):`
	`Index Type Name`
	`----- ---- ----`
	`0 S CTS-password`
	`1 P 57366898EEF9D71A6E33C3628CE7EEDE`
	Example:
	****Note that the following is the sample output of the command from Cisco IOS XE Everest release 16.6 and above.**
	The Protected Access Credentials (PAC) information is not displayed.**
		Display the contents of the software or hardware encryption keystore.

	Command or Action	Purpose
	Device# **show keystore** Using software keystore emulation. Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA): Index Type Name ----- ---- ---- 0 S CTS-password	

Example: Configuring SGT Inline Tagging

This example shows how to enable an interface on the device for L2-SGT tagging or imposition and defines whether the interface is trusted for CTS:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

Feature Information for Overview of Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.