# Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

CHAPTER 1

# Cisco TrustSec Support for IOS

Cisco TrustSec (CTS) is a system that provides security for CTS-enabled network devices at each routing hop. In this system, each network device works to authenticate and authorize its neighbor devices and next applies some level of security (group tagging, role-based access control lists (ACLs), encryption, and so on) to traffic between the devices.

The Cisco TrustSec Support for IOS feature involves using Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic Protected Access Credential (PAC) provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling (EAP-FAST) to establish a Transport Layer Security (TLS) tunnel in which client credentials are verified.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

# Prerequisites for Cisco TrustSec Support for IOS

To use the Cisco TrustSec functionality on your existing router, ensure that you have purchased a Cisco TrustSec security license. If the router is being ordered and needs the Cisco TrustSec functionality, ensure that this license is preinstalled on your router before it is shipped to you.

The Cisco Identity Services Engine 1.0 is required for authentication. The Secure Access Control Server (ACS) Express Appliance server can also be used for authentication; however, not all ACS features are supported by CTS.

# Restrictions for Cisco TrustSec Support for IOS

- The Cisco TrustSec Support for IOS feature is supported on the Cisco Integrated Services Router Generation 2 (ISR G2) only.
- EAP-FAST only supports Phase 0 where the PAC is initially distributed to the client. EAP-FAST Phase 1 (the PAC is used to establish a secure tunnel) and Phase 2 (client is authenticated through the secure tunnel) are not supported.

# Information About Cisco TrustSec Support for IOS

## Cisco TrustSec Device Enrollment

Any device that participates in the CTS network requires it to be authenticated and trusted. New devices that connect to the CTS network use an enrollment process to obtain CTS authentication credentials and receive general information about the CTS environment to facilitate the authentication process. Device enrollment can happen either directly with an Authentication Server (AS) provided the device has L3 connectivity to AS or through a peer Authenticator (AT) device, such as a switch or router that facilitates enrollment with an AS.

Access switches or routers are the authentication points in typical branch access scenarios and have direct connectivity to the AS. They authenticate endpoints through EAP-FAST Phase 0 for dynamic PAC provisioning or RADIUS and EAP exchange. When endpoints are successfully authenticated, they receive user-specific AAA attributes that include the SGT, which in turn is relayed to a router using SXP. The router initiates EAP-FAST Phase 0 exchange with the available AS and obtains a PAC. This is accomplished by a local PAC-provisioning driver, which acts as a pass-through authenticator to the supplicant EAP-FAST engine running on the router.

## Secure RADIUS

The RADIUS protocol requires a secret to be shared between a client and a server. Shared secrets are used to verify that RADIUS messages are sent by a RADIUS enabled device that is configured with the same shared secret. Shared secrets also verify that the RADIUS message has not been modified in transit (message integrity). The message integrity is checked by including the Message Authenticator attribute in the RADIUS messages. This attribute is a Hash-based Message Authentication Code-Message Digest 5 (HMAC-MD5) of the entire

radius message using the shared secret as the key. The shared secret is also used to encrypt some RADIUS attributes, such as User-Password and Tunnel-Password.

# EAP-FAST

EAP-FAST is a publicly accessible IEEE 802.1X extensible authentication protocol type that is used to support customers who cannot enforce a strong password policy. EAP-FAST is used for the following reasons:

- Digital certificates are not required.
- A variety of database types for usernames and passwords are supported.
- Password expiration and change are supported.
- EAP-FAST is flexible, easy to deploy and manage.

**Note** Lightweight Directory Access Protocol (LDAP) users cannot be automatically PAC provisioned and must be manually provisioned.

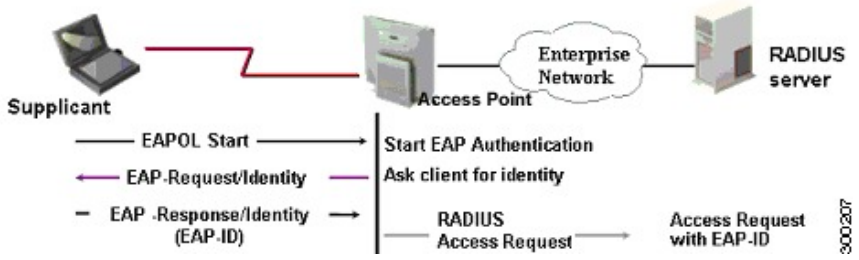
EAP-FAST comprises three basic phases, but only Phase 0 is supported. Phase 0 initially distributes the PAC to the client device.

**Note** Unsupported EAP-FAST Phase 1 uses the PAC to establish a secure tunnel and Phase 2 authenticates the client through a secure tunnel.

Phase 0 or auto-provisioning (also called in-band provisioning) component of EAP-FAST permits the secure distribution of the user PAC to each device. With some other authentication protocols, it is necessary to establish a network connection or manually install a file in order to distribute credentials to the device. Phase 0 in EAP-FAST permits a PAC to be distributed to the device during an encrypted session after the device's credentials are authenticated. This device authentication uses a challenge-handshake protocol to authenticate the device and to validate the server response. This authentication mechanism guards against potential interception and reforwarding of provisioning requests for the purpose of intercepting a user PAC.

The end result of Phase 0 is PAC distribution. After successful PAC distribution, the server issues an authentication failure to the access point and the device is disassociated from the network. Then the device reinitiates an EAP-FAST authentication with the network using the newly provisioned PAC and the device's credentials.

The figure below shows an overview of EAP-FAST authentication.



# Protected Access Credential (PAC)

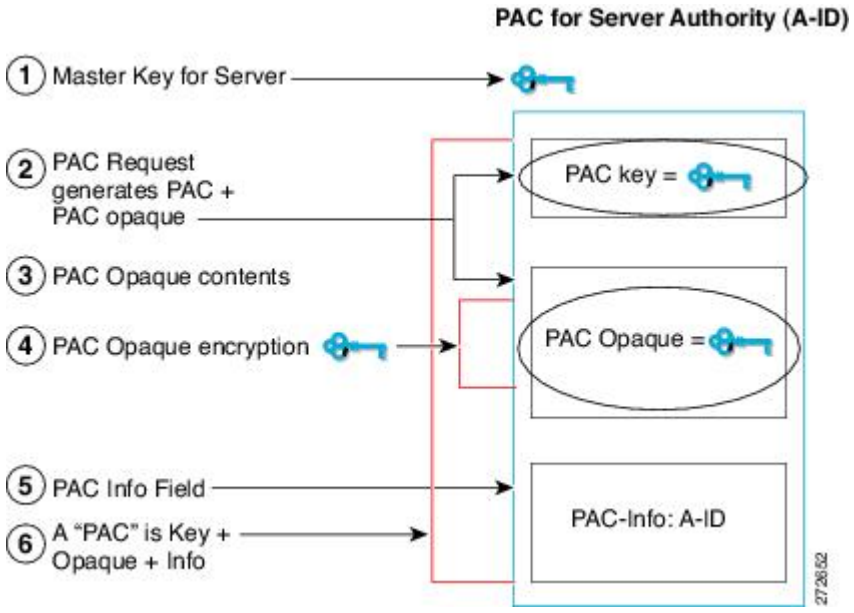
The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server authority identifier (A-ID). A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates.

Creating a PAC consists of the following steps:

1. Server A-ID maintains a local key (master key) that is only known by the server.
2. When a client, which is referred to in this context as an initiator identity (I-ID), requests a PAC from the server, the server generates a randomly unique PAC key and PAC-Opaque field for this client.
3. The PAC-Opaque field contains the randomly generated PAC key along with other information such as an I-ID and key lifetime.
4. PAC Key, I-ID, and Lifetime in the PAC-Opaque field are encrypted with the master key.
5. A PAC-Info field that contains the A-ID is created.
6. The PAC is distributed or imported to the client automatically.

**Note** The server does not maintain the PAC or the PAC key, enabling the EAP-FAST server to be stateless.

The figure below describes the PAC's construction. A PAC consists of the PAC-Opaque, PAC Key, and PAC-Info fields. The PAC-Info field contains the A-ID.



## PAC Provisioning

In Secure RADIUS, the PAC key is provisioned into each device during authentication to derive the shared secret. Since the RADIUS ACS does not store the PAC key for each device, the clients must also send an additional RADIUS attribute containing the PAC-Opaque field, which is a variable length field that can only be interpreted by the server to recover the required information and validate the peer's identity and authentication. For example, the PAC-Opaque field may include the PAC key and the PAC's peer identity.

The PAC-Opaque field format and contents are specific to the PAC server on which it is issued. The RADIUS server obtains the PAC Key from the PAC-Opaque field and derives the shared secret the same way clients do. Secure RADIUS only modifies the way shared secret is derived and not its usage.

EAP-FAST Phase 0 is used to automatically provision a client with a PAC.

## Deploying Devices in High Availability Setup

Perform the following steps when deploying devices in an HA setup:

1. Clear the credentials from all the devices which are part of the HA setup.
2. Boot the stack setup and establish the device roles (active, standby, and members).
3. Configure the credentials on the active device. Use the **cts credentials id** *id* **password** *password* command to configure the credentials.

**Note** While adding a new device to an existing stack, ensure that you clear the credentials on the fresh device and then add it to the existing stack setup.

# How to Provide Cisco TrustSec Support for IOS

## Installing the Cisco TrustSec Security License

To use the Cisco TrustSec functionality on your existing router, ensure that you have purchased a Cisco TrustSec security license. If the router is being ordered and needs the Cisco TrustSec functionality, ensure that this license is preinstalled on your router before it is shipped to you.

Perform this task to manually install the Cisco TrustSec security license:

### SUMMARY STEPS

1. **enable**
2. **license install** *stored-location-url*
3. **license boot module** *module-name* **technology-package** *package-name*
4. **reload**
5. **show license udi**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **license install** *stored-location-url*<br><br>**Example:**<br><br>`Router# license install tftp://mytftpserver/mylicensefile.lic` | Installs the license on the router. |
| **Step 3** | **license boot module** *module-name* **technology-package** *package-name*<br><br>**Example:**<br><br>`Router# license boot module c2900 technology-package securityk9` | Specifies the security software license to boot.<br><br>• The *module-name* argument is the router or module to be configured.<br><br>• The **technology-package** keyword and *package-name* argument upgrades the security software license package from which the router should boot.<br><br>• Accept the end-user license agreement when prompted. |
| **Step 4** | **reload**<br><br>**Example:**<br><br>`Router# reload` | Restarts the router to enable the new software with the securityk9 license containing the Cisco TrustSec license. |
| **Step 5** | **show license udi**<br><br>**Example:**<br><br>`Router# show license udi` | Displays all the UDI values that are licensed in the system, and verifies that your Cisco TrustSec security license has installed successfully. |

#### What to Do Next

See the "Configuring Cisco TrustSec Credentials" section to configure the basic parameters needed to make Cisco TrustSec operational on your router.

# Configuring Cisco TrustSec Credentials

Perform this task for CTS to work on your router.

## SUMMARY STEPS

1. **enable**
2. **cts credentials id** *cts-id* **password** *password*
3. **configure terminal**
4. **aaa new-model**
5. **aaa authentication dot1x default group radius**
6. **cts authorization list network** *list-name*
7. **aaa authorization network** *list-name* **group radius**
8. **exit**
9. **show cts server-list**
10. **show cts credentials**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **cts credentials id** *cts-id* **password** *password*<br><br>**Example:**<br>`Router# cts credentials id ctsid password abcd` | Specifies the CTS device ID for this device to use when authenticating with other CTS devices with EAP-FAST because CTS requires each device in the network to identity itself uniquely.<br>• The *cts-id* argument has a maximum length of 32 characters and is case sensitive.<br>• The *password* argument is the password for this device to use when authenticating with other CTS devices with EAP-FAST. |
| **Step 3** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 4** | **aaa new-model**<br><br>**Example:**<br>`Router(config)# aaa new-model` | Enables new RADIUS and AAA access control commands and functions and disables old commands. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **aaa authentication dot1x default group radius**<br><br>**Example:**<br><br>`Router(config)# aaa authentication dot1x default group radius` | Specifies that RADIUS servers are used for authentication on interfaces running IEEE 802.1X. |
| **Step 6** | **cts authorization list network** *list-name*<br><br>**Example:**<br><br>`Router(config)# cts authorization list network cts-mlist` | Specifies a list of AAA servers for the CTS seed device to use. |
| **Step 7** | **aaa authorization network** *list-name* **group radius**<br><br>**Example:**<br><br>`Router(config)# aaa authorization network cts-mlist group radius` | Specifies the CTS authorization list name for all network-related service requests from RADIUS servers. |
| **Step 8** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode. |
| **Step 9** | **show cts server-list**<br><br>**Example:**<br><br>`Router# show cts server-list` | Displays the RADIUS the server configurations for CTS seed devices. |
| **Step 10** | **show cts credentials**<br><br>**Example:**<br><br>`Router# show cts credentials` | Displays the CTS device ID. The stored password is never displayed. |

# Configuring Secure RADIUS Automatic PAC Provisioning

In seed devices, the PAC-Opaque field has to be provisioned so that all RADIUS exchanges can use the PAC-Opaque field to make the server it communicates with capable of automatic PAC provisioning. All non-seed devices obtain the PAC-Opaque field during the authentication phase of a link initialization.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius server** *name*
5. **address ipv4** *hostname* [**acct-port** *port* | **alias** *name* | **auth-port** *port* [**acct-port** *port*]]
6. **pac key** *encryption-key*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Router(config)# aaa new-model` | Enables new RADIUS and AAA access control commands and functions and disables old commands. |
| **Step 4** | **radius server** *name*<br><br>**Example:**<br>`Router(config)# radius server myserver` | Specifies a name for the RADIUS server PAC provisioning configuration and enters RADIUS server configuration mode. |
| **Step 5** | **address ipv4** *hostname* [**acct-port** *port* \| **alias** *name* \| **auth-port** *port* [**acct-port** *port*]]<br><br>**Example:**<br>`Router(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812` | Configures the RADIUS server accounting and authentication parameters for PAC provisioning.<br>• The *hostname* argument is the RADIUS server IPv4 address or Domain Name System (DNS) name.<br>• The **acct-port** keyword and *port* argument specify the UDP port for the RADIUS accounting server for accounting requests. The default port is 1646.<br>• The **alias** keyword and *name* argument specify an alias for this server. The alias can be an IPv4 address or host name. Up to 8 aliases can be configured for this server. |

| | Command or Action | Purpose |
|---|---|---|
| | | • The **auth-port** keyword and *port* argument specify the UDP port for RADIUS authentication server. The default port is 1645. |
| **Step 6** | **pac key** *encryption-key*<br><br>**Example:**<br>`Router(config-radius-server)# pac key 7 mypackey` | Specifies the PAC encryption key (overrides the default).<br>• 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. |

### What to Do Next

**Note** Automatic PAC Provisioning can also be triggered by Secure RADIUS when the server has no PAC or when an Access-Reject message is received from the Autonomous System (AS) says "PAC Expired".

# Configuration Examples for Cisco TrustSec Support for IOS

## Configuring the CTS Device ID and Password: Example

The following example configures himalaya and cisco as the CTS device ID and password:

```
Router# cts credentials id himalaya password cisco

CTS device ID and password have been inserted in the local keystore. Please make sure that
 the same ID and password are configured in the server database.
```

The following example changes the CTS device ID and password to atlas and cisco123:

```
Router# cts credentials id atlas password cisco123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y
TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following example displays the CTS device ID and password state:

```
Router# show cts credentials
CTS password is defined in keystore, device-id = atlas
```

# Configuring AAA for a CTS Seed Device and Automatic PAC Provisioning: Example

The following example configures the AAA configuration for a CTS seed device and automatic PAC provisioning on the router:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network cts-mlist group radius
Router(config)# cts authorization list cts-mlist
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Security commands | Cisco IOS Security Command Reference: Commands A to C<br>Cisco IOS Security Command Reference: Commands D to L<br>Cisco IOS Security Command Reference: Commands M to R<br>Cisco IOS Security Command Reference: Commands S to Z |
| EAP Flexible Authentication via Secured Tunnel (EAP-FAST) authentication protocol deployment in wireless networks | EAP-FAST Deployment Guide |
| Cisco TrustSec switches | Cisco TrustSec Switch Configuration Guide |

### MIBs

| Description | Link |
|---|---|
| CISCO-TRUSTSEC-SXP-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Cisco TrustSec Support for IOS

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 Cisco TrustSec Support for IOS*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Support for Cisco TrustSec Solution on ISR Platforms. | 12.2(33)SXI<br>15.2(2)T | This feature involves using secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic PAC provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with EAP-FAST to establish a TLS tunnel in which client credentials are verified.<br>In Cisco IOS Release 12.2(33)SXI, this feature was introduced on Cisco IOS software.<br>This feature was integrated into Cisco IOS Release 15.2(2)T software.<br>The following commands were introduced or modified: **address ipv4 (config-radius-server)**, **cts authorization list network**, **pac keyradius-server host**, **show cts credentials**, **show cts server-list**. |

CHAPTER 2

# Cisco TrustSec SGT Exchange Protocol IPv4

Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS and is referred to in this document as CTS-SXP. CTS-SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. CTS-SXP passes IP to SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

# Prerequisites for Cisco TrustSec SGT Exchange Protocol IPv4

The CTS-SXP network needs to be established before implementing SXP. The CTS-SXP network has the following prerequisites:

- To use the Cisco TrustSec functionality on your existing router, ensure that you have purchased a Cisco TrustSec security license. If the router is being ordered and needs the Cisco TrustSec functionality, ensure that this license is pre-installed on your router before it is shipped to you.
- CTS-SXP software runs on all network devices
- Connectivity exists between all network devices
- The Cisco Identity Services Engine 1.0 is required for authentication. The Secure Access Control Server (ACS) Express Appliance server can also be used for authentication, however not all ACS features are supported by CTS. ACS 5.1 operates with a CTS-SXP license
- Configure the **retry open timer** command to a different value on different routers.

# Restrictions for Cisco TrustSec SGT Exchange Protocol IPv4

- The Cisco TrustSec Support for IOS feature is supported on the Cisco Integrated Services Router Generation 2 (ISR G2) only.
- CTS-SXP is supported only on physical interfaces, not on logical interfaces.
- CTS-SXP does not support IPv6.
- If the default password is configured on a router, the connection on that router should configure the password to use the default password. If the default password is not configured, the connection on that router should configure to not use the password configuration. The configuration of the password option should be consistent across the deployment network.

# Information About Cisco TrustSec SGT Exchange Protocol IPv4

## Security Group Tagging

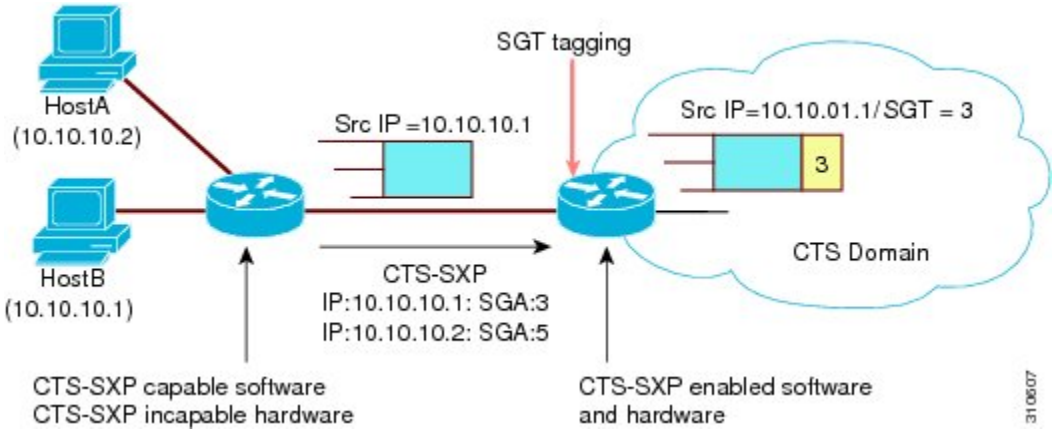
CTS-SXP uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the CTS-SXP network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The Security Group Tag (SGT) allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

# Using CTS-SXP for SGT Propagation Across Legacy Access Networks

Tagging packets with SGTs requires hardware support. There may be devices in the network that can participate in CTS authentication, but lack the hardware capability to tag packets with SGTs. However, if CTS-SXP is used, then these devices can pass IP-to-SGT mappings to a CTS peer device that has CTS-capable hardware.

CTS-SXP typically operates between ingress access layer devices at the CTS domain edge and distribution layer devices within the CTS domain. The access layer device performs CTS authentication of external source devices to determine the appropriate SGTs for ingress packets. The access layer device learns the IP addresses of the source devices using IP device tracking and (optionally) DHCP snooping, then uses CTS-SXP to pass the IP addresses of the source devices along with their SGTs to the distribution switches. Distribution switches with CTS-capable hardware can use this IP-to-SGT mapping information to tag packets appropriately and to enforce Security Group Access Control List (SGACL) policies as shown in the figure below. An SGACL associates an SGT with a policy. The policy is enforced when SGT-tagged traffic egresses the CTS domain.

***Figure 1: How CTS-SXP Propagates SGT Information***




You must manually configure a CTS-SXP connection between a peer without CTS hardware support and a peer with CTS hardware support. The following tasks are required when configuring the CTS-SXP connection:

- If CTS-SXP data integrity and authentication are required, the same CTS-SXP password can be configured on both peer devices. The CTS-SXP password can be configured either explicitly for each peer connection or globally for the device. Although a CTS-SXP password is not required it is recommended.
- Each peer on the CTS-SXP connection must be configured as either a CTS-SXP speaker or CTS-SXP listener. The speaker device distributes the IP-to-SGT mapping information to the listener device.
- A source IP address can be specified to use for each peer relationship or a default source IP address can be configured for peer connections where a specific source IP address is not configured. If no source IP address is specified, then the device uses the interface IP address of the connection to the peer.

CTS-SXP allows multiple hops. That is, if the peer of a device lacking CTS hardware support also lacks CTS hardware support, the second peer can have a CTS-SXP connection to a third peer, continuing the propagation of the IP-to-SGT mapping information until a hardware-capable peer is reached. A device can be configured as a CTS-SXP listener for one CTS-SXP connection as a CTS-SXP speaker for another CTS-SXP connection.

A CTS device maintains connectivity with its CTS-SXP peers by using the TCP keepalive mechanism. To establish or restore a peer connection, the device repeatedly attempts the connection setup by using the

configured retry period until the connection is successful or until the connection is removed from the configuration.

# VRF-Aware CTS-SXP

The CTS-SXP implementation of Virtual Routing and Forwarding (VRF) binds a CTS-SXP connection with a specific VRF. It is assumed that the network topology is correctly configured for Layer 2 or Layer 3 VPNs, and that all VRFs are configured before enabling CTS-SXP.

CTS-SXP VRF support can be summarized as follows:

- Only one CTS-SXP connection can be bound to one VRF.
- Different VRFs may have overlapping CTS-SXP peer or source IP addresses.
- IP-to-SGT mappings learned (added or deleted) in one VRF can be updated only in the same VRF domain. The CTS-SXP connection cannot update a mapping bound to a different VRF. If no SXP connection exits for a VRF, IP-SGT mappings for that VRF won't be updated by SXP.
- CTS-SXP does not support the establishment of connections with a source IPv6 address. However, multiple address families per VRF are supported where one CTS-SXP connection in a VRF domain can forward both IPv4 and IPv6 IP-to-SGT mappings.
- CTS-SXP has no limitation on the number of connections and number of IP-to-SGT mappings per VRF.

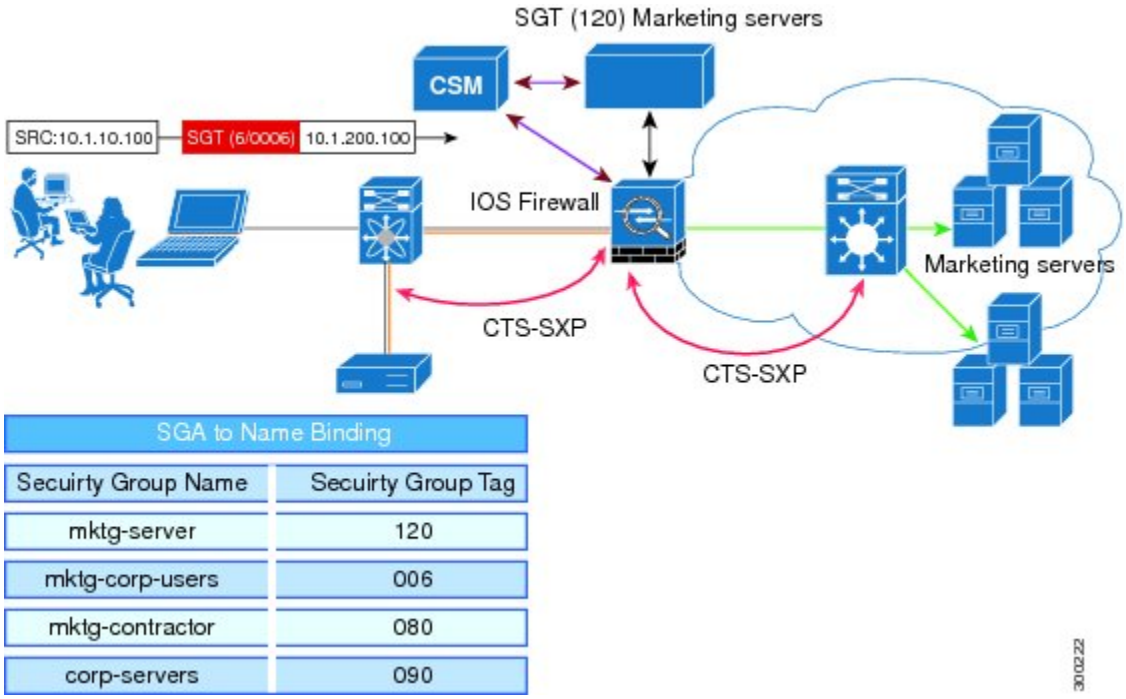
# Security Group Access Zone-Based Policy Firewall

CTS-SXP extends the deployment of network devices to additional places on the network by using the Security Group Access (SGA) Zone-Based Policy firewalls (ZBPFs). CTS-SXP is used for Identity distribution through inline devices where the identity information is learned from a primary communication path that exists across networks as shown in the figure below.

The Security Group Tag (SGT) is used by the SGA ZBPF to apply enforcement policy. IP-to-SGT mapping information is learned through CTS-SXP. When a packet arrives, source IP addresses in the packet are used

to derive source tags. The Identity firewall applies a policy to the received IP packets based on the configured policy where the SGT is one of the attributes.

***Figure 2: CTS-SXP SGA ZBPF Distribution Path Across Networks***




# How to Configure the Cisco TrustSec SGT Exchange Protocol IPv4

## Enabling CTS-SXP

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp enable**<br>**Example:**<br>`Device(config)# cts sxp enable` | Enables a CTS-SXP connection to any peer connection that is configured.<br>**Note** Ensure that peer connections are configured. If peer connections are not configured, then CTS-SXP connections cannot be established with them. |

# Configuring a CTS-SXP Peer Connection

The CTS-SXP peer connection must be configured on both devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.

**Note** If a default CTS-SXP source IP address is not configured and you do not configure a CTS-SXP source address in the connection, the Cisco TrustSec software derives the CTS-SXP source IP address from existing local IP addresses. The CTS-SXP source IP address might be different for each TCP connection initiated from the router.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp connection peer** *ipv4-address* {**source** \| **password**} {**default** \| **none**} **mode** {**local** \| **peer**} [[**listener** \| **speaker**] [**vrf** *vrf-name*]]<br>**Example:**<br>`Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker` | Configures the CTS-SXP peer address connection.<br>The **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address, if configured, or the address of the port.<br>The **password** keyword specifies the password that CTS-SXP uses for the connection using the following options:<br>• **default—**Use the default CTS-SXP password you configured using the **cts sxp default password** command.<br>• **none—**A password is not used.<br>The **mode** keyword specifies the role of the remote peer device:<br>• **local—**The specified mode refers to the local device.<br>• **peer—**The specified mode refers to the peer device.<br>• **listener—**Specifies that the device is the listener in the connection.<br>• **speaker—**Specifies that the device is the speaker in the connection. This is the default.<br>The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF. |
| **Step 4** | **exit**<br>**Example:**<br>`Device# exit` | Exits global configuration mode and returns to privileged EXEC mode. |
| **Step 5** | **show cts sxp** {**connections** \| **sgt-map**} [**brief** \| **vrf** *vrf-name*]<br>**Example:**<br>`Device# show cts sxp connections` | (Optional) Displays CTS-SXP status and connections. |

# Configuring the Default CTS-SXP Password

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp default password** [**0** | **6** | **7**] *password*
4. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp default password** [**0** \| **6** \| **7**] *password*<br><br>**Example:**<br>`Device(config)# cts sxp default password Cisco123` | Configures the CTS-SXP default password. You can enter either a clear text password (using the **0** or no option) or an encrypted password (using the **6** or **7** option). The maximum password length is 32 characters.<br>**Note** By default, CTS-SXP uses no password when setting up connections. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Device# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring the Default CTS-SXP Source IP Address

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp default source-ip** *src-ip-addr*
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp default source-ip** *src-ip-addr*<br><br>**Example:**<br>`Device(config)# cts sxp default source-ip 10.20.2.2` | Configures the CTS-SXP default source IP address that is used for all new TCP connections where a source IP address is not specified.<br>**Note** Existing TCP connections are not affected when the default CTS-SXP source IP address is configured. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Device# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring the CTS-SXP Reconciliation Period

After a peer terminates a CTS-SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the CTS-SXP reconciliation period timer starts. While the CTS-SXP reconciliation period timer is active, the CTS software retains the SGT mapping entries learned from the previous connection and removes invalid entries. The default value is 120 seconds (2 minutes). Setting the CTS-SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp reconciliation period** *seconds*
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp reconciliation period** *seconds*<br><br>**Example:**<br>`Device(config)# cts sxp reconciliation period 150` | Sets the CTS-SXP reconciliation timer, in seconds. The range is from 0 to 64000. The default is 120. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Device# exit` | Exits global configuration mode and enters privileged EXEC mode. |

# Configuring the CTS-SXP Retry Period

The CTS-SXP retry period determines how often the CTS software retries a CTS-SXP connection. If a CTS-SXP connection is not established successfully, then the CTS software makes a new attempt to set up the connection after the CTS-SXP retry period timer expires. The default value is 2 minutes. Setting the CTS-SXP retry period to 0 seconds disables the timer and retries are not attempted.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp retry period** *seconds*
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp retry period** *seconds*<br><br>**Example:**<br>`Device(config)# cts sxp retry period 160` | Sets the CTS-SXP retry timer, in seconds. The range is from 0 to 64000. The default is 120. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Device# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Creating Syslogs to Capture IP-to-SGT Mapping Changes

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp log binding-changes**
4. **exit**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp log binding-changes**<br><br>**Example:**<br>`Device(config)# cts sxp log binding-changes` | Enables logging for IP-to-SGT binding changes causing CTS-SXP syslogs (sev 5 syslog) to be generated whenever a change to IP-to-SGT binding occurs (add, delete, change). These changes are learned and propagated on the CTS-SXP connection.<br>**Note** This logging function is disabled by default. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Device# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring a Class Map for a Security Group Access Zone-Based Policy Firewall

Perform this task to configure a class map for classifying Security Group Access (SGA) zone-based policy firewall network traffic.

**Note** You must perform at least one match step.

The zone-based firewall policy uses the security group tag (SGT) ID for filtering. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
4. **match security-group source tag** *sgt-number*
5. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map type inspect** [**match-any** | **match-all**] *class-map-name*<br><br>**Example:**<br>`Router(config)# class-map type inspect match-all cmap-1` | Creates a Layer 3 or Layer 4 inspect type class map and enters class-map configuration mode. |
| **Step 4** | **match security-group source tag** *sgt-number*<br><br>**Example:**<br>`Router(config-cmap)# match security-group source tag 100` | Configures the match criterion for a class map based on the source SGT number. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-cmap)# exit` | Exits QoS class-map configuration mode and enters global configuration mode. |

# Creating a Policy Map for a Security Group Access Zone-Based Policy Firewall

Perform this task to create a policy map for a Security Group Access (SGA) zone-based policy firewall that is attached to zone pairs. This task also helps to configure Identity Firewall (IDFW) to work with Security Group Tag (SGT) Exchange Protocol (SXP) or L2-tagged traffic on the interfaces that belong to the security zones.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect**
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **cts manual**
13. **no propagate sgt**
14. **policy static sgt** *tag* [**trusted**]
15. **exit**
16. **show policy-map type inspect zone-pair session**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map type inspect** *policy-map-name* | Creates a Layer 3 or Layer 4 inspect type policy map. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# policy-map type inspect z1z2-policy` | • Enters policy map configuration mode. |
| **Step 4** | **class type inspect** *class-name*<br>**Example:**<br>`Device(config-pmap)# class type inspect cmap-1` | Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration mode. |
| **Step 5** | **inspect**<br>**Example:**<br>`Device(config-pmap-c)# inspect` | Enables packet inspection. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-pmap-c)# exit` | Exits policy-map class configuration mode and enters global configuration mode. |
| **Step 7** | **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*<br>**Example:**<br>`Device(config)# zone-pair security z1z2 source z1 destination z2` | Creates a zone pair and enters security zone configuration mode.<br>**Note** To apply a policy, you must configure a zone pair. |
| **Step 8** | **service-policy type inspect** *policy-map-name*<br>**Example:**<br>`Device(config-sec-zone)# service-policy type inspect z1z2-policy2` | Attaches a firewall policy map to the destination zone pair.<br>**Note** If a policy is not configured between a pair of zones, traffic is dropped by default. |
| **Step 9** | **end**<br>**Example:**<br>`Device(config-sec-zone)# end` | Exits security zone configuration mode and enters global configuration mode. |
| **Step 10** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/1/1` | Configures an interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **zone-member security** *zone-name*<br><br>**Example:**<br><br>`Device(config-if)# zone-member security Inside` | Assigns an interface to a specified security zone.<br>**Note** When you make an interface a member of a security zone, all traffic in and out of that interface (except traffic bound for the router or initiated by the router) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you should apply a policy. If the policy permits traffic, traffic can flow through that interface. |
| **Step 12** | **cts manual**<br><br>**Example:**<br><br>`Device(config-if)# cts manual` | Enables the interface for Cisco TrustSec Security (CTS) SGT authorization and forwarding, and enters CTS manual interface configuration mode. |
| **Step 13** | **no propagate sgt**<br><br>**Example:**<br><br>`Device(config-if-cts-manual)# no propagate sgt` | Disables SGT propagation at Layer 2 on CTS interfaces. |
| **Step 14** | **policy static sgt** *tag* [**trusted**]<br><br>**Example:**<br><br>`Device(config-if-cts-manual)# policy static sgt 100 trusted` | Configures a static authorization policy for a CTS security group with a tagged packet that defines the trustworthiness of the SGT. |
| **Step 15** | **exit**<br><br>**Example:**<br><br>`Device(config-if)# exit` | Exits security zone configuration mode and enters privileged EXEC mode. |
| **Step 16** | **show policy-map type inspect zone-pair session**<br><br>**Example:**<br><br>`Device# show policy-map type inspect zone-pair session` | (Optional) Displays the Cisco IOS stateful packet inspection sessions created because of the policy-map application on the specified zone pair.<br>**Note** The information displayed under the class-map field is the traffic rate (bits per second) of the traffic that belongs to the connection-initiating traffic only. Unless the connection setup rate is significantly high and is sustained for multiple intervals over which the rate is computed, no significant data is shown for the connection. |

**Example:**

The following sample output of the **show policy-map type inspect zone-pair session** command displays the information about the Cisco IOS stateful packet inspection sessions created because of the policy-map application on the specified zone pair:

```
Device# show policy-map type inspect zone-pair session

Zone-pair: in-out
 Service-policy inspect : test

   Class-map: test (match-any)
     Match: group-object security source sgt
     Inspect
       Established Sessions
        Session 113EF68C (192.2.2.1:8)=>(198.51.100.252:153) icmp SIS_OPEN
         Created 00:00:02, Last heard 00:00:02
         Bytes sent (initiator:responder) [360:360]


   Class-map: class-default (match-any)
     Match: any
     Drop (default action)
       310 packets, 37380 bytes
```

# Configuration Examples for Cisco TrustSec SGT Exchange Protocol IPv4

## Example: Enabling and Configuring a CTS-SXP Peer Connection

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

The following sample output for **show cts sxp connections** command displays CTS-SXP connections:

```
Device_B# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: 10.10.1.1
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.20.2.2
```

```
Source IP         : 10.10.1.1
Conn status       : On
Connection mode   : SXP Listener
Connection inst#  : 1
TCP conn fd       : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

# Example: Configuring a Security Group Access Zone-Based Policy Firewall

The following example shows the configuration of a class map and policy map for an SGA zone-based policy firewall.

```
Device> enable
Device# configure terminal
Device(config)# class-map type inspect match-all cmap-1
Device(config-cmap)# match security-group source tag 100
Device(config-cmap)# exit

Device(config)# policy-map type inspect z1z2-policy
Device(config-pmap)# class type inspect cmap-1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit

Device(config)# zone-pair security z1z2 source z1 destination z2
Device(config-sec-zone)# service-policy type inspect z1z2-policy2
Device(config-sec-zone)# end

Device(config)# interface GigabitEthernet 0/1/1
Device(config-if)# zone-member security Inside
Device(config-if)# exit
```

# Additional References for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | Cisco IOS Security Command Reference: Commands A to C |
| | Cisco IOS Security Command Reference: Commands D to L |
| | Cisco IOS Security Command Reference: Commands M to R |
| | Cisco IOS Security Command Reference: Commands S to Z |
| Cisco TrustSec switches | Cisco TrustSec Switch Configuration Guide |

### MIBs

| MIB | MIBs Link |
|---|---|
| CISCO-TRUSTSEC-SXP-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Cisco TrustSec SGT Exchange Protocol IPv4

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 2: Feature Information for Cisco TrustSec SGT Exchange Protocol IPv4*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco TrustSec SGT Exchange Protocol IPv4 | 12.2(53)SE2<br>12.2(50)SG5<br>12.2(33)SXI3<br>15.1(3)S<br>15.2(2)T | The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS and is referred to in this document as CTS-SXP. CTS-SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. CTS-SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This allows security services on switches, routers, or firewalls to learn identity information from access devices.<br>In Cisco IOS Release 12.2(53)SE2, this feature was introduced on the Cisco Catalyst 3500 and 3750 Series Switches.<br>In Cisco IOS Release 12.2(50)SG5, this feature was introduced on the Cisco Catalyst 4500 Series Switch.<br>In Cisco IOS Release 12.2(33)SXI3, this feature was introduced on the Cisco Catalyst 6500 Series Switches.<br>In Cisco NX-OS 4.2.1 Release, this feature was introduced on the Nexus 7000 Series Switches.<br>This feature was introduced in Cisco IOS Release 15.1(3)S.<br>The following commands were introduced or modified: **cts sxp enable, cts sxp connection peer**, **show cts sxp**, **cts sxp default source-ip, cts sxp reconciliation period, cts sxp retry period, cts sxp log binding-changes**.<br>This feature was integrated into Cisco IOS Release 15.2(2)T. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| Support for Cisco TrustSec Solution on ISR Platforms | 15.2(2)T | This feature helps CTS-SXP extend the deployment of network devices through Security Group Access (SGA) Zone-Based Policy firewalls (ZBPFs).<br>This feature was integrated into Cisco IOS Release 15.2(2)T.<br>The following commands were introduced or modified: **match security-group**. |

CHAPTER 3

# Cisco TrustSec with SXPv4

Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS. CTS SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection mechanism to prevent stale binding in the network. In addition, Cisco TrustSec with SXPv4 supports SGT inline tagging which allows propagation of SGT embedded in clear-text (unencrypted) Ethernet packets.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

# Information About Cisco TrustSec with SXPv4

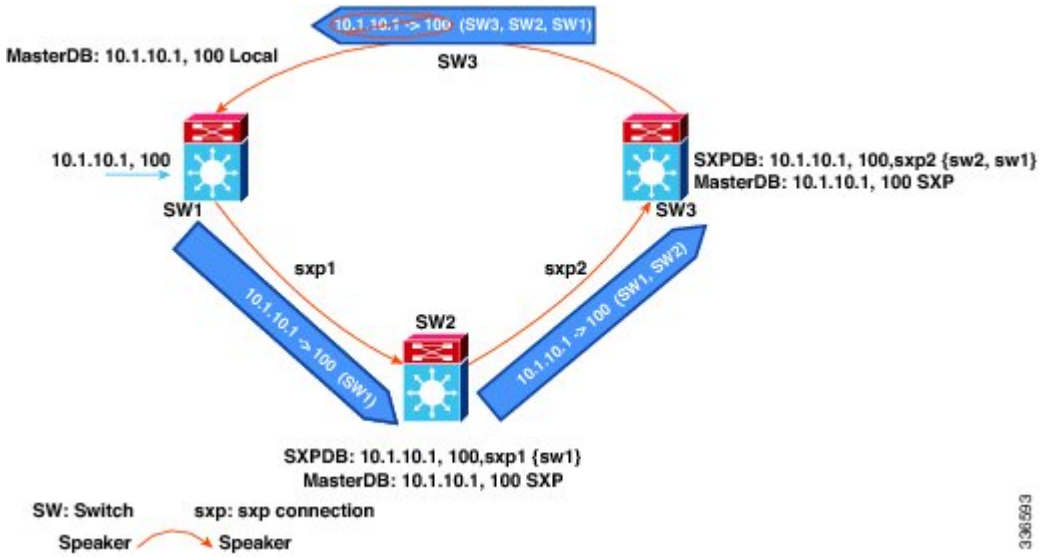
## Overview of Cisco TrustSec with SXPv4

Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol (SXP) (CTS-SXP) is a control protocol which propagates IP address to Security Group Tag (SGT) binding information across network devices. SGT is maintained by tagging packets on ingress to the CTS-SXP network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The Security Group Tag (SGT) allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

SXP connections can be enabled such that the binding forwarded by one switch for an SXP connection can be received from another SXP connection, resulting in SXP connection loops. SXP loop topology might, however, result in stale binding in the network. SXPv4's built-in loop detection and prevention mechanism addresses the stale binding issue whenever there is a loop between SXP nodes.

Loop prevention is achieved by adding SXP propagation path information when propagating (adding/deleting) bindings. Propagation path information keeps track of the network devices (via their node IDs) that the binding travels in an ordered manner. All nodes that participate in the network with looped SXP connections must run SXPv4 to function correctly. Loop detection is a mandatory capability in SXPv4.

***Figure 3: SXPv4 Loop Detection***




In the figure above there are three network devices: SW1, SW2, and SW3. There are also three SXP connections: SXP1, SXP2 and SXP3, together which create an SXP connection loop. A binding (10.1.10.1, 100) is learned at SW1 through local authentication. The binding is exported by SW1 to SW2 together with the path information (that is, SW1, from where the binding is forwarded).

Upon receiving the binding, SW2 exports it to SW3, again prepending the path information (SW2, SW1). Similarly, SW3 forwards the binding to SW1 with path information SW3, SW2, SW1. When SW1 receives the binding, the path information is checked. If its own path attribute is in the binding update received, then a propagation loop is detected. This binding is dropped and not stored in the SXP binding database.

If the binding is removed from SW1, (for example, if a user logs off), a binding deletion event is sent. The deletion event goes through the same path as above. When it reaches SW1, no action will be taken as no such binding exists in the SW1 binding database.

Loop detection is done when a binding is received by an SXP but before it is added to the binding database.

# SXP Node ID

An SXP node ID is used to identify the individual devices within the network. The node ID is a four-octet integer that can be configured by the user. If it is not configured by the user, SXP picks a node ID itself using the highest IPv4 address in the default VRF domain, in the same manner that EIGRP generates its node ID. The node ID has to be unique in the network that SXP connections traverse to enable SXP loop detection.

The SXP loop detection mechanism drops binding propagation packets based on finding its own node ID in the peer sequence attribute. Changing a node ID in a loop detection-running SXP network could break SXP loop detection functionality and therefore needs to be handled carefully.

The bindings that are associated with the original node ID have to be deleted in all SXP nodes before the new node ID is configured. This can be done by disabling the SXP feature on the network device where you desire to change the node ID.

**Note** Disabling the SXP feature brings down all SXP connections on the device.

Before you change the node ID, wait until the SXP bindings that are propagated with the particular node ID in the path attribute are deleted.

**Note** A syslog is generated when you change the node ID.

# Keepalive and Hold-Time Negotiation with SXPv4

SXP uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism within the protocol in order to provide more predictable and timely detection of connection loss.

SXP connections are asymmetric with almost all of the protocol messages (except for open/open_resp and error messages) being sent from an SXP speaker to an SXP listener. The SXP listener can keep a potentially large volume of state per connection, which includes all the binding information learned on a connection. Therefore, it is only meaningful to have a keepalive mechanism that allows a listener to detect the loss of connection with a speaker.

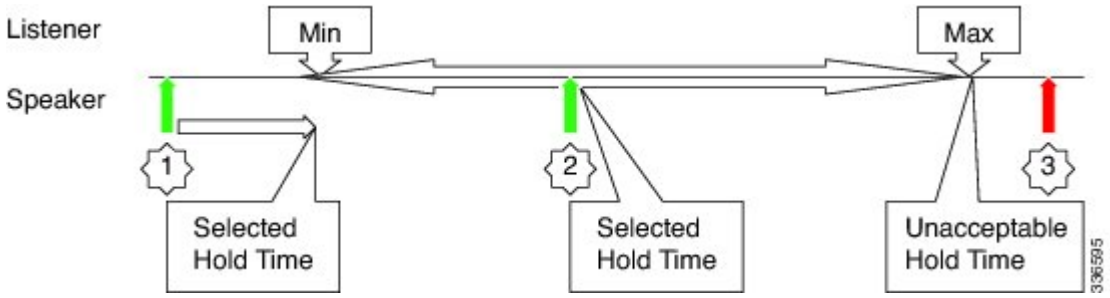
The mechanism is based on two timers:

- **Hold timer**: Used by a listener for detection of elapsing time without successive keepalive and/or update messages from a speaker.
- **Keepalive timer**: Used by a speaker to trigger the dispatch of keepalive messages during intervals when no other information is exported via update messages.

The hold-time for the keepalive mechanism may be negotiated during the open/open_resp exchange at connection setup. The following issues are important during the negotiation:

- A listener may have desirable range for the hold-time period locally configured or have a default of 90 to 180 seconds. A value of 0xFFFF..0xFFFF indicates that the keepalive mechanism is not used.
- A speaker may have a minimum acceptable hold-time period locally configured or have a default of 120 seconds. This is the shortest period of time a speaker is willing to send keepalive messages for keeping the connection alive. Any shorter hold-time period would require a faster keepalive rate than the rate the speaker is ready to support.
- A value of 0xFFFF implies that the keepalive mechanism is not used.
- The negotiation succeeds when the speaker's minimum acceptable hold-time falls below or within the desirable hold-time range of the listener. If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.
- The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.
- The selected hold-time period of a successful negotiation is the maximum of the speaker's minimum acceptable hold-time and the lower bound of the listener's hold-time range.
- The speaker calculates the keepalive time to one-third of the selected hold-time by default unless a different keepalive time is locally configured.

***Figure 4: Hold-time Negotiation Process***




The figure above illustrates the hold-time negotiation process. More detail on the listener's and speaker"s roles is given below.

**Connection Initiated by Listener**

- A listener may include a hold-time attribute in the open message with minimum and maximum values set to its configured range of the hold-time period. A hold-time attribute with just a minimum value set to 0xFFFF0 would indicate to the speaker that the keepalive mechanism is not used.
- When a speaker receives an open message, it will react as follows:
  - If the hold-time attribute is not present or if it contains a minimum value that is set to 0xFFFF0, the speaker will set its keepalive time to 0xFFFF0 to indicate that the keepalive mechanism is disabled.
  - If the received hold-time attribute contains a valid range, the speaker must include a hold-time attribute in its open_resp message with a minimum value set as follows:

- 0xFFFF0 if the speaker does not support the keepalive mechanism or if the mechanism is supported but disabled due to a local configuration, which sets the keepalive time to 0xFFFF0.
- If the speaker's minimum acceptable hold-time value is greater than the upper bound of the offered range, the speaker must send an open error message with the subcode set to "Unacceptable hold-time" and terminate the connection. Otherwise the speaker will set the selected hold-time to the maximum of its minimum acceptable hold-time value and the lower bound of the offered hold-time range.
- The speaker will calculate a new value for its keepalive time as one-third of that selected hold-time.
- The speaker will set the minimum hold-time value of the hold-time attribute to the selected hold-time.

- When the listener receives the open_resp message from the speaker, it will look for hold-time attribute:
  - If the hold-time attribute is present and contains a minimum hold-time value of 0xFFFF0, the speaker will set its hold-time value to 0xFFFF0 to indicate that the keepalive mechanism is not used.
  - If the minimum hold-time value is within the range offered by the listener, the listener will set its hold-time period to the selected value it has received in the open_resp message.
  - If the minimum hold-time value is outside the offered range, the listener will send an open error message with subcode set to "Unacceptable hold-time" and terminate the connection.

**Connection Initiated by Speaker**

- A speaker may include a hold-time attribute in the open message with minimum value set to its minimum acceptable hold-time period. A hold-time attribute with just a minimum value of 0xFFFF0 would indicate to the listener that the keepalive mechanism is not used.
- When a listener receives an open message, it will react as follows:
  - If the hold-time attribute is not present or if it contains a minimum value that is set to 0xFFFF0, the listener will set its hold-time to 0xFFFF0 to indicate that keepalive mechanism is disabled.
  - If the received hold-time attribute contains a valid value, the speaker must include hold-time attribute in its open_resp message with a minimum value set as follows:
    - 0xFFFF0 if the listener does not support the keepalive mechanism or if the mechanism is supported but disabled due to a local configuration, which sets the keepalive time to 0xFFFF0.
    - If the received hold-time value is greater than the upper bound of the listener's configured hold-time range, the speaker must send an open error message with subcode set to "Unacceptable hold-time" and terminate the connection.
    - If the received hold-time value falls within the listener's configured hold-time range, the listener will make it the selected hold-time.
    - If the received hold-time value is less than the lower bound of the listener's configured hold-time range, the listener will set the selected hold-time to the lower bound of its hold-time range.
    - The listener will set the minimum hold-time value of the hold-time attribute to the selected hold-time.

- When the speaker receives the open_resp message from the listener, it will look for the hold-time attribute:
  - If the hold-time attribute is present and contains a minimum hold-time value of 0xFFFF0. The speaker will set its hold-time value to 0xFFFF0 to indicate that the keepalive mechanism is not used.
  - If the received hold-time value is greater or equal to the speaker's minimum acceptable hold-time, the speaker will calculate a new value for its keepalive time as one-third of the received hold-time.
  - If the received hold-time value is lower than the minimum acceptable, the speaker must send an open error message with subcode set to "Unacceptable hold-time" and terminate the connection.

# SGT Inline Tagging

Each security group in a CTS 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.

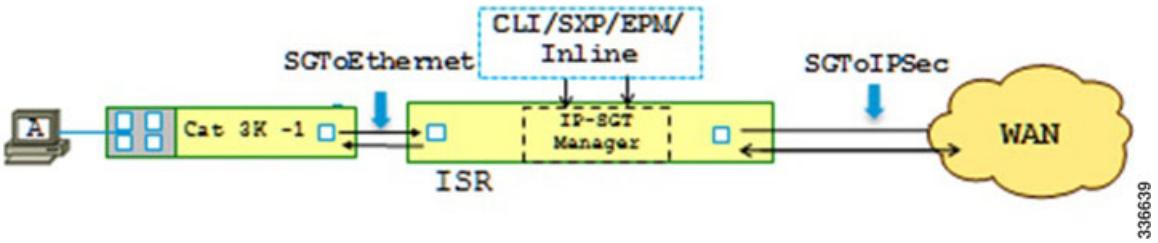
CTS-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L2) layer. This feature is called "L2-SGT Imposition." It allows Ethernet interfaces on the device to be enabled for L2-SGT imposition so that device can insert an SGT in the packet 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.

To complement CTS architecture of end-to-end identity enablement, Cisco ISR devices support inline propagation of SGT over Ethernet packets peer devices on the LAN. A typical branch deployment scenario for SGT over Ethernet is shown in the figure below:

***Figure 5: Cisco ISR Router with Routed Port SGT Over Ethernet***



- The end points are authenticated on a Cisco Catalyst switch and SGT-assigned. The switch tags native/802.1Q packets inline SGT on the egress.
- A Cisco ISR router sends/receives SGT over Ethernet (using EtherType 0x8909) on routed ports.
  - Ingress - receive SGToEthernet processes and makes SGT available to data-plane features (SGFW, IPsec).
  - Egress - send SGT over Ethernet from SGT learned from IP-SGT manager and/or IPsec. SGFW enforcements on Cisco ISR router using data-plane SGT.
- IPsec tags packets on WAN egress and vice-versa.

# How to Configure Cisco TrustSec with SXPv4

## Configuring the Hold-Time for the SXPv4 Protocol on a Network Device

Hold-time can be configured globally on a network device, which applies to all SXP connections configured on the device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp listener hold-time** *minimum-period maximum-period*
4. **cts sxp speaker hold-time** *minimum-period*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **cts sxp listener hold-time** *minimum-period maximum-period*<br><br>**Example:**<br><br>`Device(config)# cts sxp listener hold-time 750 1500` | Configures a minimum and maximum acceptable hold-time period in seconds for the listener device. The valid range is from 1 to 65534. The default hold-time range for a listener is 90 to 180 seconds.<br><br>**Note** The *maximum-period* value must be greater than or equal to the *minimum-period* value. |
| **Step 4** | **cts sxp speaker hold-time** *minimum-period*<br><br>**Example:**<br><br>`Device(config)# cts sxp speaker hold-time 950` | Configures a minimum acceptable hold-time period in seconds for the speaker device. The valid range is 1 to 65534. The default hold-time for a speaker is 120 seconds. |

# Configuring the Hold-Time for the SXPv4 Protocol for Each Connection

The peer connection must be configured on both devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**hold-time** *minimum-period maximum-period*] [**vrf** *vrf-name*]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **cts sxp connection peer** *ipv4-address* {**source** \| **password**} {**default** \| **none**} **mode** {**local** \| **peer**} [[**listener** \| **speaker**] [**hold-time** *minimum-period maximum-period*] [**vrf** *vrf-name*]]<br><br>**Example:**<br><br>`Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker` | Configures the CTS-SXP peer address connection.<br><br>The **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address, if configured, or the address of the port.<br><br>The **password** keyword specifies the password that CTS-SXP uses for the connection using the following options:<br><br>• **default—**Use the default CTS-SXP password you configured using the **cts sxp default password** command.<br><br>• **none—**A password is not used.<br><br>The **mode** keyword specifies the role of the remote peer device:<br><br>• **local—**The specified mode refers to the local device.<br><br>• **peer—**The specified mode refers to the peer device.<br><br>• **listener—**Specifies that the device is the listener in the connection.<br><br>• **speaker—**Specifies that the device is the speaker in the connection. This is the default.<br><br>The **hold-time** keyword allows you to specify the length of the hold-time period for the speaker or listener device.<br><br>**Note** A **hold-time** *maximum-period* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time** *minimum-period* value is required.<br>The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF. |
| **Step 4** | **exit**<br><br>**Example:**<br><br>`Device(config)# exit` | Exits global configuration mode. |
| **Step 5** | **show cts sxp** {**connections** \| **sgt-map**} [**brief** \| **vrf** *vrf-name*]<br><br>**Example:**<br><br>`Device# show cts sxp connections` | (Optional) Displays CTS-SXP status and connections. |

# Configuring the Node ID of a Network Device

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp node-id** {*sxp-node-id* | **interface** *interface-type* | *ipv4-address*}

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp node-id** {*sxp-node-id* | **interface** *interface-type* | *ipv4-address*}<br><br>**Example:**<br>`Device(config)# cts sxp node-id 172.16.1.3` | Configures the node ID of a network device. |

# 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**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** {**gigabitethernet** *port* \| **vlan** *number*}<br>**Example:**<br>`Device(config)# interface gigabitethernet 0` | Enters the interface on which CTS SGT authorization and forwarding is enabled. |
| **Step 4** | **cts manual**<br>**Example:**<br>`Device(config-if)# cts manual` | Enables the interface for CTS SGT authorization and forwarding. Enters CTS manual interface configuration mode. |
| **Step 5** | **propagate sgt**<br>**Example:**<br>`Device(config-if-cts-manual)# propagate sgt` | Enables CTS SGT propagation on an interface.<br>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**]<br>**Example:**<br>`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.<br>**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**<br>**Example:**<br>`Device(config-if-cts-manual)# end` | Exits CTS manual interface configuration mode and enters privileged EXEC mode. |
| **Step 8** | **show cts interface brief**<br>**Example:**<br>`Device# show cts interface brief` | Displays CTS configuration statistics for the interface. |

| | Command or Action | Purpose |
|---|---|---|
| | Interface GigabitEthernet0/0<br>CTS is enabled, mode: MANUAL<br>Propagate SGT: Enabled<br>Peer SGT assignment: Trusted<br><br>Interface GigabitEthernet0/1<br>CTS is enabled, mode: MANUAL<br>Propagate SGT: Disabled<br>Peer SGT assignment: Untrusted<br><br>Interface GigabitEthernet0/3<br>CTS is disabled. | |

# Configuration Examples for Cisco TrustSec with SXPv4

## Example: Configuring Cisco TrustSec with SXPv4

### Configuring the Hold-Time for the SXPv4 Protocol on a Network Device

```
Device(config)# cts sxp speaker hold-time 950
```

### Configuring the Hold-Time for the SXPv4 Protocol for Each Connection

```
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
hold-time 500
```

### Configuring the Node ID of a Network Device

```
Device(config)# cts sxp node-id 172.16.1.3
```

## Verifying Cisco TrustSec with SXPv4

### Display the SXP connections on a device

```
Device# show cts sxp connection

 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          : 2.2.2.1
Source IP        : 2.2.2.2
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
```

```
Conn hold time   : 0 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 32:00:41:31 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

### Displaying the current CST-SGT map database

In SXPv4, an SXP node ID is shown:

```
Device# show cts sxp sgt-map

SXP Node ID(generated):0x02020202(2.2.2.2)
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.0/29 , 29>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
Status  : Active;
Seq Num : 3
Peer Seq: 0B0B0B02,
IPv4,SGT: <12.12.133.1 , 12>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
Status  : Active;
Seq Num : 5
Peer Seq: 0B0B0B02,
Total number of IP-SGT Mappings: 2
```

## 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
```

# Additional References for Cisco TrustSec with SXPv4

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |

| Related Topic | Document Title |
|---|---|
| Security commands | • Cisco IOS Security Command Reference Commands A to C<br>• Cisco IOS Security Command Reference Commands D to L<br>• Cisco IOS Security Command Reference Commands M to R<br>• Cisco IOS Security Command Reference Commands S to Z |

### MIBs

| MIB | MIBs Link |
|---|---|
| CISCO-TRUSTSEC-SXP-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Cisco TrustSec with SXPv4

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 3: Feature Information for Cisco TrustSec with SXPv4***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco TrustSec with SXPv4 | 15.3(2)T | CTS SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection and prevention mechanism to prevent stale binding in the network. In addition, Cisco TrustSec with SXPv4 supports SGT inline tagging, which allows propagation of SGT embedded in clear-text (unencrypted) Ethernet packets.<br>The following commands were introduced:<br>**cts sxp listener hold-time**, **cts sxp node-id**, **cts sxp speaker hold-time**. |

CHAPTER 4

# Enabling Bidirectional SXP Support

The Bidirectional SXP Support feature enhances the functionality of Cisco TrustSec with SXP version 4 by adding support for Security Group Tag (SGT) Exchange Protocol (SXP) bindings that can be propagated in both directions between a speaker and a listener over a single connection.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

## Prerequisites for Bidirectional SXP Support

- Ensure that Cisco TrustSec is configured on the device. For more information, see the "Cisco TrustSec Support for IOS" chapter in the *Cisco TrustSec Configuration Guide*.
- To use the Cisco TrustSec functionality on your existing device, ensure that you have purchased one of the following security licenses:

- IP Base License
- LAN Base License

**Note** The LAN Base License is available from Cisco IOS XE Everest 16.5.1.

- IP Services License

- Connectivity must exist in all network devices.
- Cisco TrustSec SXP software must run on all network devices.

# Restrictions for Bidirectional SXP Support

- The peers at each end of the connection must be configured as a bidirectional connection using the **both** keyword. It is a wrong configuration to have one end configured as a bidirectional connection using the **both** keyword and the other end configured as a speaker or listener (unidirectional connection).
- The Bidirectional SXP Support feature only supports the scalability numbers for SXP connections and IP-SGT bindings provided in the following table.

*Table 4: Scalability Numbers for SXP Connections and IP-SGT Bindings*

| Platform | Unidirectional SXP Connections (Speaker only/Listener only) | Bidirectional SXP Connections | SXP Database IP-SGT Bindings<br>**Note** If the number of connections are increased, ensure that the number of bindings configured per box are reduced. The number of connections should not exceed the connections documented in this table.<br>**Note** The Role-Based IP-SGT database limit is 200K across all platforms. |
|---|---|---|---|
| ISR 2900, ISR 3900 | 250 | 125 | • 180K for unidirectional SXP connections<br>• 125K for bidirectional SXP connections |
| Catalyst 6000 series | 500 | 250 | 100K |

# Information About Bidirectional SXP Support

## Bidirectional SXP Support Overview

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. The peer that produces data is the speaker and the corresponding peer is the listener.

With the support for bidirectional Security Group Tag (SGT) Exchange Protocol (SXP) configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

The bidirectional SXP configuration is managed with one pair of IP addresses. On either end, only the listener initiates the SXP connection and the speaker accepts the incoming connection.

***Figure 6: Bidirectional SXP Connection***


In addition, SXP version 4 (SXPv4) continues to support the loop detection mechanism (to prevent stale binding in the network).

# How to Enable Bidirectional SXP Support

## Configuring Bidirectional SXP Support

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp enable**
4. **cts sxp default password**
5. **cts sxp default source-ip**
6. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*]
7. **cts sxp speaker hold-time** *minimum-period*
8. **cts sxp listener hold-time** *minimum-period maximum-period*
9. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp enable**<br><br>**Example:**<br><br>`Device(config)# cts sxp enable` | Enables the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) on a network device. |
| **Step 4** | **cts sxp default password**<br><br>**Example:**<br><br>`Device(config)# cts sxp default password Cisco123` | (Optional) Specifies the Cisco TrustSec SGT SXP default password. |
| **Step 5** | **cts sxp default source-ip**<br><br>**Example:**<br><br>`Device(config)# cts sxp default source-ip 10.20.2.2` | (Optional) Configures the Cisco TrustSec SGT SXP source IPv4 address. |
| **Step 6** | **cts sxp connection peer** *ipv4-address* {**source** \| **password**} {**default** \| **none**} **mode** {**local** \| **peer**} **both** [**vrf** *vrf-name*]<br><br>**Example:**<br><br>`Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both` | Configures the Cisco TrustSec SXP peer address connection for a bidirectional SXP configuration. The **both** keyword configures the bidirectional SXP configuration.<br><br>The **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address, if configured, or the address of the port.<br><br>The **password** keyword specifies the password that Cisco TrustSec SXP uses for the connection using the following options:<br><br>• **default—**Use the default Cisco TrustSec SXP password you configured using the **cts sxp default password** command.<br><br>• **none—**A password is not used.<br><br>The **mode** keyword specifies the role of the remote peer device:<br><br>• **local—**The specified mode refers to the local device.<br><br>• **peer—**The specified mode refers to the peer device.<br><br>• **both—**Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.<br><br>The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **cts sxp speaker hold-time** *minimum-period*<br><br>**Example:**<br><br>`Device(config)# cts sxp speaker hold-time 950` | (Optional) Configures the global hold time (in seconds) of a speaker network device for Cisco TrustSec SGT SXPv4. The valid range is from 1 to 65534. The default is 120. |
| **Step 8** | **cts sxp listener hold-time** *minimum-period maximum-period*<br><br>**Example:**<br><br>`Device(config)# cts sxp listener hold-time 750 1500` | (Optional) Configures the global hold time (in seconds) of a listener network device for Cisco TrustSec SGT SXPv4. The valid range is from 1 to 65534. The default is 90 to 180.<br><br>**Note** The *maximum-period* value must be greater than or equal to the *minimum-period* value. |
| **Step 9** | **exit**<br><br>**Example:**<br><br>`Device(config)# exit` | Exits global configuration mode. |

# Verifying Bidirectional SXP Support Configuration

## SUMMARY STEPS

1. **enable**
2. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

## DETAILED STEPS

**Step 1** **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

**Example:**

```
Device> enable
```

**Step 2** **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]
Displays Cisco TrustSec Exchange Protocol (SXP) status and connections.

**Example:**

```
Device# show cts sxp connections

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 running
------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)


Device# show cts sxp connection 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 running
-------------------------------------------------
Peer_IP Source_IP Conn Status Duration
-------------------------------------------------
2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19 (dd:hr:mm:sec)
```

The following table describes the various scenarios for the connection status output.

***Table 5: Connection Status Output Scenarios***

| Node1 | Node2 | Node1 CLI Output for Connection Status | Node2 CLI Output for Connection Status |
|---|---|---|---|
| Both | Both | On (Speaker)<br>On (Listener) | On (Speaker)<br>On (Listener) |
| Speaker | Listener | On | On |
| Listener | Speaker | On | On |

# Configuration Examples for Bidirectional SXP Support

## Example: Configuring Bidirectional SXP Support

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device_A to connect to Device_B:

```
Device_A> enable
Device_A# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device_A(config)# exit
```

The following example shows how to configure the bidirectional CTS-SXP peer connection on Device_B to connect to Device_A:

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Password123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device_B(config)# exit
```

# Additional References for Bidirectional SXP Support

**Related Documents**

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |
| Cisco TrustSec configuration | "Cisco TrustSec Support for IOS" chapter in the *Cisco TrustSec Configuration Guide* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Bidirectional SXP Support

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 6: Feature Information for Bidirectional SXP Support***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Bidirectional SXP Support | Cisco IOS 15.4(1)T<br>Cisco IOS 15.2(1)SY | The Bidirectional SXP Support feature enhances the functionality of Cisco TrustSec with SXP version 4 by adding support for Security Group Tag (SGT) Exchange Protocol (SXP) bindings that can be propagated in both directions between a speaker and a listener over a single connection.<br>The following command was introduced or modified: **cts sxp connection peer**. |

CHAPTER 5

# Cisco TrustSec Interface-to-SGT Mapping

The Cisco TrustSec Interface-to-SGT Mapping feature binds all traffic on a Layer 3 ingress interface to a security group tag (SGT). Once this mapping is implemented, Cisco TrustSec can use the SGT to segregate traffic from various logical Layer 3 ingress interfaces.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

## Information About Cisco TrustSec Interface-to-SGT Mapping

### Interface-to-SGT Mapping

The mapping between interfaces and security group tags (SGTs) is used to map SGTs to traffic of any of the following logical Layer 3 ingress interfaces, regardless of the underlying physical interface:

- Layer 3 (routed) Ethernet interfaces
- Layer 3 (routed) Ethernet 802.1Q subinterfaces

- Switch virtual interfaces (SVIs)
- Tunnel interfaces

The configured SGT tag is assigned to all traffic on the Layer 3 ingress interface and can be used for inline tagging and policy enforcement.

## Binding Source Priorities

Cisco TrustSec resolves conflicts among IP address to security group tag (IP-SGT) binding sources with a strict priority scheme. The current priority enforcement order, from lowest to highest, is as follows:

1 CLI—Bindings configured using the **cts role-based sgt-map sgt** command.

2 L3IF—Bindings added due to FIB forwarding entries that have paths through one or more interfaces with consistent Layer 3 Interface to SGT (L3IF-SGT) mapping or identity port mapping on routed ports.

3 SXP—Bindings learned from SGT Exchange Protocol (SXP) peers.

4 LOCAL—Bindings of authenticated hosts that are learned via Cisco Enterprise Policy Manager (EPM) and device tracking. This type of binding also includes individual hosts that are learned via Address Resolution Protocol (ARP) snooping on ports configured with the Layer 2 port mirroring feature.

5 INTERNAL—Bindings between locally configured IP addresses and the devices own SGT.

# How to Configure Cisco TrustSec Interface-to-SGT Mapping

## Configuring Layer 3 Interface-to-SGT Mapping

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **cts role-based sgt-map sgt** *sgt-number*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type slot/port*<br><br>**Example:**<br>`Device(config)# interface gigabitEthernet 0/0` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **cts role-based sgt-map sgt** *sgt-number*<br><br>**Example:**<br>`Device(config-if)# cts role-based sgt-map sgt 77` | An SGT is imposed on ingress traffic to the specified interface.<br>• *sgt-number*—Specifies the security group tag (SGT) number. Valid values are from 2 to 65519. |
| **Step 5** | **end**<br><br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Verifying Layer 3 Interface-to-SGT Mapping

## SUMMARY STEPS

1. **enable**
2. **show cts role-based sgt-map all**

## DETAILED STEPS

**Step 1** **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

**Example:**

```
Device> enable
```

**Step 2** **show cts role-based sgt-map all**
Displays the security group tag (SGT) mapping for the ingress traffic on the Layer 3 interface.

**Example:**

The following sample output from the **show cts role-based sgt-map all** command shows that once the Cisco TrustSec Interface-to-SGT Mapping feature is implemented, the traffic on the ingress interface is tagged appropriately with Layer 3 interface (L3IF). The output displays the priority scheme of the IP address to security group tag (IP-SGT) binding sources (for more information about the IP-SGT binding source priorities, see the "Binding Source Priorities" section).

```
Device# show cts role-based sgt-map all

IP Address              SGT     Source
============================================
192.0.2.1               4       INTERNAL
192.0.2.5/24            3       L3IF
192.0.2.10/8            3       L3IF
192.0.2.20              5       CLI
198.51.100.1            4       INTERNAL
IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 2
Total number of INTERNAL bindings = 2
Total number of active   bindings = 5
```

# Configuration Examples for Cisco TrustSec Interface-to-SGT Mapping

## Example: Configuring Layer 3 Interface-to-SGT Mapping

The following example shows the security group tag (SGT) mapping configuration for the Layer 3 ingress interface:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# cts role-based sgt-map sgt 77
Device(config-if)# end
```

# Additional References for Cisco TrustSec Interface-to-SGT Mapping

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |

| Related Topic | Document Title |
|---|---|
| Security commands | • Cisco IOS Security Command Reference Commands A to C<br>• Cisco IOS Security Command Reference Commands D to L<br>• Cisco IOS Security Command Reference Commands M to R<br>• Cisco IOS Security Command Reference Commands S to Z |
| Cisco TrustSec and SXP configuration | Cisco TrustSec Switch Configuration Guide |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Cisco TrustSec Interface-to-SGT Mapping

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 7: Feature Information for Cisco TrustSec Interface-to-SGT Mapping*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco TrustSec Interface-to-SGT Mapping | 15.4(2)T | The Cisco TrustSec Interface-to-SGT Mapping feature binds all traffic on a Layer 3 ingress interface to a security group tag (SGT). Once this mapping is implemented, Cisco TrustSec can use the SGT to segregate traffic from various logical Layer 3 ingress interfaces.<br>In Cisco IOS Release 15.4(2)T, support was added for the Cisco Integrated Services Router Generation 2 (Cisco ISR G2).<br>The following command was introduced or modified: **cts role-based sgt-map sgt**. |

CHAPTER 6

# Cisco TrustSec Subnet to SGT Mapping

Subnet to security group tag (SGT) mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address which belongs to the specified subnet.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

## Restrictions for Cisco TrustSec Subnet to SGT Mapping

- An IPv4 subnetwork with a /31 prefix cannot be expanded.
- Subnet host addresses cannot be bound to SGTs when the **cts sxp mapping network-map** command *bindings* argument is less than the total number of subnet hosts in the specified subnets or when the number of bindings is 0.

- IPv6 expansions and propagation only occurs when SXP speaker and listener are running SXPv3, or more recent versions.

# Information About Cisco TrustSec Subnet to SGT Mapping

In IPv4 networks, SXPv3, and more recent versions, can receive and parse subnet network address/prefix strings from SXPv3 peers. Earlier SXP versions convert the subnet prefix into its set of host bindings before exporting them to an SXP listener peer.

For example, the IPv4 subnet 198.1.1.0/29 is expanded as follows (only 3 bits for host addresses):

- Host addresses 198.1.1.1 to 198.1.1.7 are tagged and propagated to SXP peer.
- Network and broadcast addresses 198.1.1.0 and 198.1.1.8 are not tagged and not propagated.

**Note** To limit the number of subnet bindings SXPv3 can export, use the **cts sxp mapping network-map** global configuration command.

Subnet bindings are static, which means that active hosts are not learned. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet to SGT mapping can be propagated on Layer 2 or Layer 3 TrustSec links.

**Note** For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

# How to Configure Cisco TrustSec Subnet to SGT Mapping

## Configuring Subnet to SGT Mapping

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts sxp mapping network-map** *bindings*
4. **cts role-based sgt-map** *ipv4-address* **sgt** *number*
5. **cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number*
6. **exit**
7. **show running-config** | **include** *search-string*
8. **show cts sxp connections**
9. **show cts sxp sgt-map**
10. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts sxp mapping network-map** *bindings*<br><br>**Example:**<br>`Device(config)# cts sxp mapping network-map 10000` | Configures the subnet to SGT mapping host count constraint. The *bindings* argument specifies the maximum number of subnet IP hosts from 0 to 65,535 that can be bound to SGTs and exported to the SXP listener. The default is 0 (no expansions performed). |
| **Step 4** | **cts role-based sgt-map** *ipv4-address* **sgt** *number*<br><br>**Example:**<br>`Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234` | (IPv4) Specifies an IPv4 subnet in CIDR notation.<br>The number of bindings specified in step 3 should match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The **sgt** *number* keyword pair specifies the SGT number that is to be bound to every host address in the specified subnet.<br>• *ipv4-address*—Specifies the IPv4 network address in dotted decimal notation.<br>• *prefix*—(0 to 30). Specifies the number of bits in the network address.<br>• **sgt** *number* (0-65,535). Specifies the SGT number. |
| **Step 5** | **cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number*<br><br>**Example:**<br>`Device(config)# cts role-based sgt-map 2020::/64 sgt 1234` | (IPv6) Specifies an IPv6 subnet in hexadecimal notation.<br>The number of bindings specified in step 3 should match or exceed the number of host addresses in the subnet (excluding network and broadcast addresses). The **sgt** *number* keyword pair specifies the SGT number that is to be bound to every host address in the specified subnet.<br>• *ipv6-address*—Specifies the IPv4 network address in dotted decimal notation.<br>• *prefix*—(0 to 30). Specifies the number of bits in the network address.<br>• **sgt** *number*—(0-65,535). Specifies the SGT number. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Device(config)# exit` | Exits global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **show running-config \| include** *search-string*<br><br>**Example:**<br>`Device# show running-config \| include sgt 1234`<br>`Device# show running-config \| include network-map` | Verifies that the **cts role-based sgt-map** and the **cts sxp mapping network-map** commands are in the running configuration. |
| **Step 8** | **show cts sxp connections**<br><br>**Example:**<br>`Device# show cts sxp connections` | Displays the SXP speaker and listener connections with their operational status. |
| **Step 9** | **show cts sxp sgt-map**<br><br>**Example:**<br>`Device# show cts sxp sgt-map` | Displays the IP to SGT bindings exported to the SXP listeners. |
| **Step 10** | **copy running-config startup-config**<br><br>**Example:**<br>`Device# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

# Cisco TrustSec Subnet to SGT Mapping: Examples

The following example shows how to configure IPv4 Subnet to SGT Mapping between two devices running SXPv3 (Device 1 and Device 2):

Configure SXP speaker/listener peering between Device 1 (10.1.1.1) and Device 2 (10.2.2.2).

```
Device1# configure terminal
Device1(config)# cts sxp enable
Device1(config)# cts sxp default source-ip 10.1.1.1
Device1(config)# cts sxp default password 1syzygy1
Device1(config)# cts sxp connection peer 10.2.2.2 password default mode local speaker
```

Configure Device 2 as SXP listener of Device 1.

```
Device2(config)# cts sxp enable
Device2(config)# cts sxp default source-ip 10.2.2.2
Device2(config)# cts sxp default password 1syzygy1
Device2(config)# cts sxp connection peer 10.1.1.1 password default mode local listener
```

On Device 2, verify that the SXP connection is operating:

```
Device2# show cts sxp connections brief | include 10.1.1.1

     10.1.1.1          10.2.2.2          On                3:22:23:18 (dd:hr:mm:sec)
```

Configure the subnetworks to be expanded on Device 1.

```
Device1(config)# cts sxp mapping network-map 10000
Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Device1(config)# cts role-based sgt-map 10.11.11.0/29 sgt 11111
Device1(config)# cts role-based sgt-map 172.168.1.0/28 sgt 65000
```

On Device 2, verify the subnet to SGT expansion from Device 1. There should be two expansions for the 10.10.10.0/30 subnetwork, six expansions for the 10.11.11.0/29 subnetwork, and 14 expansions for the 172.168.1.0/28 subnetwork.

```
Device2# show cts sxp sgt-map brief | include 101|11111|65000

IPv4,SGT: <10.10.10.1 , 101>
IPv4,SGT: <10.10.10.2 , 101>
IPv4,SGT: <10.11.11.1 , 11111>
IPv4,SGT: <10.11.11.2 , 11111>
IPv4,SGT: <10.11.11.3 , 11111>
IPv4,SGT: <10.11.11.4 , 11111>
IPv4,SGT: <10.11.11.5 , 11111>
IPv4,SGT: <10.11.11.6 , 11111>
IPv4,SGT: <172.168.1.1 , 65000>
IPv4,SGT: <172.168.1.2 , 65000>
IPv4,SGT: <172.168.1.3 , 65000>
IPv4,SGT: <172.168.1.4 , 65000>
IPv4,SGT: <172.168.1.5 , 65000>
IPv4,SGT: <172.168.1.6 , 65000>
IPv4,SGT: <172.168.1.7 , 65000>
IPv4,SGT: <172.168.1.8 , 65000>
IPv4,SGT: <172.168.1.9 , 65000>
IPv4,SGT: <172.168.1.10 , 65000>
IPv4,SGT: <172.168.1.11 , 65000>
IPv4,SGT: <172.168.1.12 , 65000>
IPv4,SGT: <172.168.1.13 , 65000>
IPv4,SGT: <172.168.1.14 , 65000>
```

Verify the expansion count on Device 1:

```
Device1# show cts sxp sgt-map

IP-SGT Mappings expanded:22
There are no IP-SGT Mappings
```

Save the configurations on Device 1 and Device 2 and exit global configuration mode.

```
Device1(config)# copy running-config startup-config
Device1(config)# exit

Device2(config)# copy running-config startup-config
Device2(config)# exit
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Security commands | • Cisco IOS Security Command Reference Commands A to C<br>• Cisco IOS Security Command Reference Commands D to L<br>• Cisco IOS Security Command Reference Commands M to R<br>• Cisco IOS Security Command Reference Commands S to Z |

| Related Topic | Document Title |
|---|---|
| Cisco TrustSec and SXP configuration | Cisco TrustSec Switch Configuration Guide |
| IPsec configuration | Configuring Security for VPNs with IPsec |
| IKEv2 configuration | Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site |
| Cisco Secure Access Control Server | Configuration Guide for the Cisco Secure ACS |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Cisco TrustSec Subnet to SGT Mapping

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 8: Feature Information for Cisco TrustSec Subnet to SGT Mapping*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco TrustSec Subnet to SGT Mapping | 15.1(1)SY<br>15.4(2)T | Subnet to security group tag (SGT) mapping binds an SGT to all host addresses of a specified subnet. Once this mapping is implemented, Cisco TrustSec imposes the SGT on any incoming packet that has a source IP address which belongs to the specified subnet.<br>The following command was introduced: **cts sxp mapping network-map**. |

CHAPTER 7

# Flexible NetFlow Export of Cisco TrustSec Fields

The Flexible NetFlow Export of Cisco TrustSec Fields feature supports the Cisco TrustSec fields in the Flexible NetFlow (FNF) flow record and helps to monitor, troubleshoot, and identify non-standard behavior for Cisco TrustSec deployments.

This module describes the interaction between Cisco TrustSec and FNF and how to configure and export Cisco TrustSec fields in the NetFlow Version 9 flow records.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

## Restrictions for Flexible NetFlow Export of Cisco TrustSec Fields

- The security group tag (SGT) value exported in Flexible NetFlow (FNF) records is zero in the following scenarios:
  - The packet is received with an SGT value of zero from a trusted interface.

- The packet is received without an SGT.
- The SGT is not found during the IP-SGT lookup.

- For Cisco ISR 3900E, ISR 3900, ISR 2950, ISR 2900, ISR 1900, and ISR 890 Platforms, Cisco TrustSec fields are supported for both IPv4 and IPv6 FNF records.

# Information About Flexible NetFlow Export of Cisco TrustSec Fields

## Cisco TrustSec Fields in Flexible NetFlow

The Cisco TrustSec fields, source security group tag (SGT) and destination security group tag (DGT), in the Flexible NetFlow (FNF) flow records help administrators correlate the flow with identity information. It enables network engineers to gain a detailed understanding of the customer use of the network and application resources. This information can then be used to efficiently plan and allocate access and application resources and to detect and resolve potential security and policy violations.

The Cisco TrustSec fields are supported for ingress and egress FNF and for unicast and multicast traffic.

The following table presents Netflow v9 enterprise specific field types for Cisco TrustSec that are used in the FNF templates for the Cisco TrustSec source and destination source group tags.

| ID | Description |
|---|---|
| CTS_SRC_GROUP_TAG | Cisco Trusted Security Source Group Tag |
| CTS_DST_GROUP_TAG | Cisco Trusted Security Destination Group Tag |

The Cisco TrustSec fields are configured in addition to the existing match fields under the FNF flow record. The following configurations are used to add the Cisco TrustSec flow objects to the FNF flow record as key or non-key fields and to configure the source and destination security group tags for the packet.

- The **match flow cts {source | destination} group-tag** command is configured under the flow record to specify the Cisco TrustSec fields as key fields. The key fields differentiate flows, with each flow having a unique set of values for the key fields. A flow record requires at least one key field before it can be used in a flow monitor.
- The **collect flow cts {source | destination} group-tag** command is configured under flow record to specify the Cisco TrustSec fields as non-key fields. The values in non-key fields are added to flows to provide additional information about the traffic in the flows.

The flow record is then configured under flow monitor and the flow monitor is applied to the interface. To export the FNF data, a flow exporter needs to be configured and then added under the flow monitor.

# How to Configure Flexible NetFlow Export of Cisco TrustSec Fields

## Configuring Cisco TrustSec Fields as Key Fields in the Flow Record

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match** {**ipv4** | **ipv6**} **protocol**
5. **match** {**ipv4** | **ipv6**} **source address**
6. **match** {**ipv4** | **ipv6**} **destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **match flow direction**
10. **match flow cts source group-tag**
11. **match flow cts destination group-tag**
12. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow record** *record-name*<br><br>**Example:**<br>`Device(config)# flow record cts-record-ipv4` | Creates a new Flexible NetFlow (FNF) flow record, or modifies an existing FNF flow record, and enters Flexible NetFlow flow record configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **match {ipv4 \| ipv6} protocol**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 protocol` | (Optional) Configures the IPv4 protocol or IPv6 protocol as a key field for a flow record. |
| **Step 5** | **match {ipv4 \| ipv6} source address**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 source address` | (Optional) Configures the IPv4 or IPv6 source address as a key field for a flow record. |
| **Step 6** | **match {ipv4 \| ipv6} destination address**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 destination address` | (Optional) Configures the IPv4 or IPv6 destination address as a key field for a flow record. |
| **Step 7** | **match transport source-port**<br>**Example:**<br>`Device(config-flow-record)# match transport source-port` | (Optional) Configures the transport source port as a key field for a flow record. |
| **Step 8** | **match transport destination-port**<br>**Example:**<br>`Device(config-flow-record)# match transport destination-port` | (Optional) Configures the transport destination port as a key field for a flow record. |
| **Step 9** | **match flow direction**<br>**Example:**<br>`Device(config-flow-record)# match flow direction` | (Optional) Configures the direction in which the flow is monitored as a key field. |
| **Step 10** | **match flow cts source group-tag**<br>**Example:**<br>`Device(config-flow-record)# match flow cts source group-tag` | Configures the Cisco TrustSec source security group tag (SGT) in the FNF flow record as key fields. |
| **Step 11** | **match flow cts destination group-tag**<br>**Example:**<br>`Device(config-flow-record)# match flow cts destination group-tag` | Configures the Cisco TrustSec destination security group tag (DGT) in the FNF flow record as key fields. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 12** | **end**<br><br>**Example:**<br>`Device(config-flow-record)# end` | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |

# Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match** {**ipv4** | **ipv6**} **protocol**
5. **match** {**ipv4** | **ipv6**} **source address**
6. **match** {**ipv4** | **ipv6**} **destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **collect flow direction**
10. **collect flow cts source group-tag**
11. **collect flow cts destination group-tag**
12. **collect counter packets**
13. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **flow record** *record-name*<br><br>**Example:**<br><br>`Device(config)# flow record cts-record-ipv4` | Creates a new Flexible NetFlow (FNF) flow record, or modifies an existing FNF flow record, and enters Flexible NetFlow flow record configuration mode. |
| **Step 4** | **match** {**ipv4** \| **ipv6**} **protocol**<br><br>**Example:**<br><br>`Device(config-flow-record)# match ipv4 protocol` | (Optional) Configures the IPv4 protocol or IPv6 protocol as a key field for a flow record. |
| **Step 5** | **match** {**ipv4** \| **ipv6**} **source address**<br><br>**Example:**<br><br>`Device(config-flow-record)# match ipv4 source address` | (Optional) Configures the IPv4 or IPv6 source address as a key field for a flow record. |
| **Step 6** | **match** {**ipv4** \| **ipv6**} **destination address**<br><br>**Example:**<br><br>`Device(config-flow-record)# match ipv4 destination address` | (Optional) Configures the IPv4 or IPv6 destination address as a key field for a flow record. |
| **Step 7** | **match transport source-port**<br><br>**Example:**<br><br>`Device(config-flow-record)# match transport source-port` | (Optional) Configures the transport source port as a key field for a flow record. |
| **Step 8** | **match transport destination-port**<br><br>**Example:**<br><br>`Device(config-flow-record)# match transport destination-port` | (Optional) Configures the transport destination port as a key field for a flow record. |
| **Step 9** | **collect flow direction**<br><br>**Example:**<br><br>`Device(config-flow-record)# collect flow direction` | (Optional) Configures the flow direction as a non-key field and enables the collection of the direction in which the flow was monitored. |
| **Step 10** | **collect flow cts source group-tag**<br><br>**Example:**<br><br>`Device(config-flow-record)# collect flow cts source group-tag` | Configures the Cisco TrustSec source security group tag (SGT) in the FNF flow record as non-key fields. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **collect flow cts destination group-tag**<br><br>**Example:**<br><br>`Device(config-flow-record)# collect flow cts destination group-tag` | Configures the Cisco TrustSec destination security group tag (DGT) in the FNF flow record as non-key fields. |
| **Step 12** | **collect counter packets**<br><br>**Example:**<br><br>`Device(config-flow-record)# collect counter packets` | (Optional) Configures the number of packets seen in a flow as a non-key field and enables collecting the total number of packets from the flow. |
| **Step 13** | **end**<br><br>**Example:**<br><br>`Device(config-flow-record)# end` | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |

# Configuring a Flow Exporter

Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

### Before You Begin

Ensure that you create a flow record. For more information see the “Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record” section and the “Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record” section.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow exporter** *exporter-name*<br>**Example:**<br>`Device(config)# flow exporter EXPORTER-1` | Creates a flow exporter or modifies an existing flow exporter, and enters Flexible NetFlow flow exporter configuration mode. |
| **Step 4** | **destination** {*ip-address* \| *hostname*} [**vrf** *vrf-name*]<br>**Example:**<br>`Device(config-flow-exporter)# destination 172.16.10.2` | Specifies the IP address or hostname of the destination system for the exporter. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-flow-exporter)# end` | Exits Flexible NetFlow flow exporter configuration mode and returns to privileged EXEC mode. |

# Configuring a Flow Monitor

### Before You Begin

To add a flow exporter to the flow monitor for data export, ensure that you create the flow exporter. For more information see the “Configuring a Flow Exporter” section.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **record** *record-name*
5. **exporter** *exporter-name*
6. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow monitor** *monitor-name*<br>**Example:**<br>`Device(config)# flow monitor FLOW-MONITOR-1` | Creates a flow monitor or modifies an existing flow monitor, and enters Flexible NetFlow flow monitor configuration mode. |
| **Step 4** | **record** *record-name*<br>**Example:**<br>`Device(config-flow-monitor)# record FLOW-RECORD-1` | Specifies the record for the flow monitor. |
| **Step 5** | **exporter** *exporter-name*<br>**Example:**<br>`Device(config-flow-monitor)# exporter EXPORTER-1` | Specifies the exporter for the flow monitor. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-flow-monitor)# end` | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |

# Applying a Flow Monitor on an Interface

To activate a flow monitor, the flow monitor must be applied to at least one interface.

### Before You Begin

Ensure that you create a flow monitor. For more information see the “Configuring a Flow Monitor” section.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Device(config)# interface ethernet 0/0` | Specifies an interface and enters interface configuration mode. |
| **Step 4** | {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}<br><br>**Example:**<br>`Device (config-if)# ip flow monitor FLOW-MONITOR-1 input` | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| **Step 5** | **end**<br><br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Verifying Flexible NetFlow Export of Cisco TrustSec Fields

## SUMMARY STEPS

1. **enable**
2. **show flow record** *record-name*
3. **show flow exporter** *exporter-name*
4. **show flow monitor** *monitor-name*
5. **show flow monitor** *monitor-name* **cache**
6. **show flow interface** *type number*

## DETAILED STEPS

**Step 1** **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

**Example:**

```
Device> enable
```

**Step 2** **show flow record** *record-name*
Displays the details of the specified Flexible NetFlow (FNF) flow record.

**Example:**

```
Device> show flow record cts-recordipv4

flow record cts-recordipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  30 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    match interface output
    match flow direction
    match flow cts source group-tag
    match flow cts destination group-tag
    collect counter packets
```

**Step 3** **show flow exporter** *exporter-name*
Displays the current status of the specified FNF flow exporter.

**Example:**

```
Device> show flow exporter EXPORTER-1

Flow Exporter EXPORTER-1:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 100.100.100.1
    Source IP address:      3.3.3.2
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            65252
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

**Step 4** **show flow monitor** *monitor-name*
Displays the status and statistics of the specified FNF flow monitor.

**Example:**

```
Device> show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       cts-recordipv4
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:                normal (Platform cache)
    Status:              allocated
    Size:                200000 entries
    Inactive Timeout:    60 secs
    Active Timeout:      1800 secs
    Update Timeout:      1800 secs
    Synchronized Timeout: 600 secs
    Trans end aging:     off
```

**Step 5** **show flow monitor** *monitor-name* **cache**
Displays the contents of the specified FNF flow monitor cache.

**Example:**

```
Device> show flow monitor FLOW-MONITOR-1 cache

  Cache type:                                 Normal
  Cache size:                                 4096
  Current entries:                            2
  High Watermark:                             2

  Flows added:                                6
  Flows aged:                                 4
    - Active timeout      (1800 secs)         0
    - Inactive timeout    (15 secs)           4
    - Event aged                              0
    - Watermark aged                          0
    - Emergency aged                          0

  IPV4 SOURCE ADDRESS:                        10.1.0.1
  IPV4 DESTINATION ADDRESS:                   172.16.2.0
  TRNS SOURCE PORT:                           58817
  TRNS DESTINATION PORT:                      23
```

```
  FLOW DIRECTION:                         Input
  IP PROTOCOL:                            6
  SOURCE GROUP TAG:                       100
  DESTINATION GROUP TAG:                  200
  counter packets:                        10

  IPV4 SOURCE ADDRESS:                    172.16.2.0
  IPV4 DESTINATION ADDRESS:               10.1.0.1
  TRNS SOURCE PORT:                       23
  TRNS DESTINATION PORT:                  58817
  FLOW DIRECTION:                         Output
  IP PROTOCOL:                            6
  SOURCE GROUP TAG:                       200
  DESTINATION GROUP TAG:                  100
  counter packets:                        8
```

**Step 6** **show flow interface** *type number*

Displays the details of the FNF flow monitor applied on the specified interface. If a flow monitor is not applied on the interface, then the output is empty.

**Example:**

```
Device>  show flow interface GigabitEthernet0/0/3

Interface GigabitEthernet0/0/3
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on
```

# Configuration Examples for Flexible NetFlow Export of Cisco TrustSec Fields

## Example: Configuring Cisco TrustSec Fields as Key Fields in the Flow Record

The following example shows how to configure the Cisco TrustSec flow objects as key fields in an IPv4 Flexible NetFlow flow record:

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow direction
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# end
```

# Example: Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record

The following example shows how to configure the Cisco TrustSec flow objects as non-key fields in an IPv4 Flexible NetFlow flow record:

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect flow direction
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# end
```

# Example: Configuring a Flow Exporter

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# end
```

# Example: Configuring a Flow Monitor

```
Device> enable
Device# configure terminal
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
Device(config-flow-monitor)# exporter EXPORTER-1
Device(config-flow-monitor)# end
```

# Example: Applying a Flow Monitor on an Interface

The following example shows how to activate an IPv4 flow monitor by applying it to an interface to analyze traffic. To activate an IPv6 flow monitor, replace the **ip** keyword with the **ipv6** keyword.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# end
```

# Additional References for Flexible NetFlow Export of Cisco TrustSec Fields

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |
| Data export in Flexible NetFlow | "Flexible NetFlow Output Features on Data Export" chapter in the *Flexible Netflow Configuration Guide* publication |
| Flexible NetFlow flow records and flow monitors | "Customizing Flexible NetFlow Flow Records and Flow Monitors" chapter in the *Flexible Netflow Configuration Guide* publication |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Flexible NetFlow Export of Cisco TrustSec Fields

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 9: Feature Information for Flexible NetFlow Export of Cisco TrustSec Fields***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Flexible NetFlow Export of Cisco TrustSec Fields | Cisco IOS 15.4(3)M | The Flexible NetFlow Export of Cisco TrustSec Fields feature supports the Cisco TrustSec fields in the Flexible NetFlow (FNF) flow record and helps to monitor, troubleshoot, and identify non-standard behavior for Cisco TrustSec deployments.<br>The following commands were introduced by this feature: **match flow cts {source \| destination} group-tag** and **collect flow cts {source \| destination} group-tag**. |

CHAPTER 8

# Cisco TrustSec SGT Caching

The Cisco TrustSec SGT Caching feature enhances the ability of Cisco TrustSec to make Security Group Tag (SGT) transportability flexible. This feature identifies the IP-SGT binding and caches the corresponding SGT so that network packets are forwarded through all network services for normal deep packet inspection processing and at the service egress point the packets are re-tagged with the appropriate SGT.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

## Restrictions for Cisco TrustSec SGT Caching

The global Security Group Tag (SGT) caching configuration and the interface-specific ingress configuration are mutually exclusive. In the following scenarios, a warning message is displayed if you attempt to configure SGT caching both globally and on an interface:

- If an interface has ingress SGT caching enabled using the **cts role-based sgt-cache ingress** command in interface configuration mode, and a global configuration is attempted using the **cts role-based sgt-caching** command, a warning message is displayed as shown in this example:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# exit
Device(config)# cts role-based sgt-caching

There is at least one interface that has ingress sgt caching configured. Please remove
 all interface ingress sgt caching configuration(s) before attempting global enable.
```

- If global configuration is enabled using the **cts role-based sgt-caching** command, and an interface configuration is attempted using the **cts role-based sgt-cache ingress** command in interface configuration mode, a warning message is displayed as shown in this example:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress

Note that ingress sgt caching is already active on this interface due to global
sgt-caching enable.
```

# Information About Cisco TrustSec SGT Caching

## Identifying and Reapplying SGT Using SGT Caching

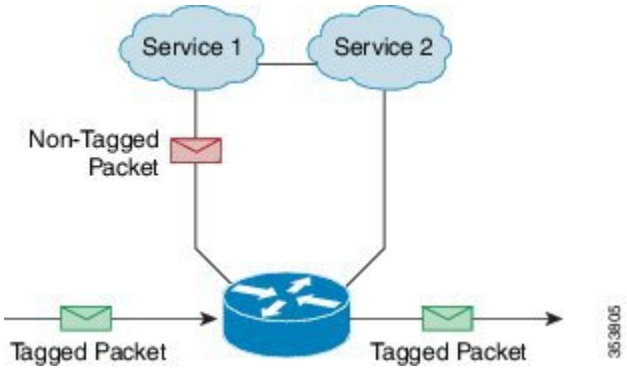
Cisco TrustSec uses Security Group Tag (SGT) caching to ensure that traffic tagged with SGT can also pass through services that are not aware of SGTs. Examples of services that cannot propagate SGTs are WAN acceleration or optimization, intrusion prevention systems (IPS), and upstream firewalls.

In one-arm mode, a packet tagged with SGT enters a device (where the tags are cached), and is redirected to a service. After that service is completed, the packet either returns to the device, or is redirected to another device as shown in the figure. In such a scenario:

1. The Cisco TrustSec SGT Caching feature enables the device to identify the IP-SGT binding information from the incoming packet and caches this information.
2. The device redirects the packet to the service or services that cannot propagate SGTs.
3. After the completion of the service, the packet returns to the device.
4. The appropriate SGT is reapplied to the packet at the service egress point.
5. Role-based enforcements are applied to the packet that has returned to the device from the service or services.

6 The packet with SGTs is forwarded to other Cisco TrustSec-capable devices downstream.

***Figure 7: SGT Caching in One-Arm Mode***




In certain instances, some services are deployed in a bump-in-the-wire topology. In such a scenario:

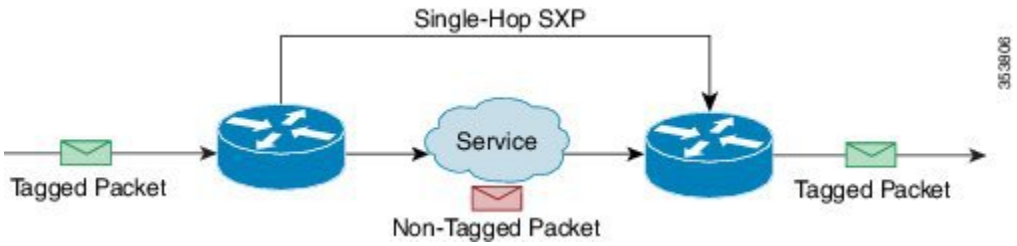
1 The packets that go through a service or services do not come back to the device.

2 Single-hop SGT Exchange Protocol (SXP) is used to identify and export the identified IP-SGT bindings.

3 The upstream device in the network identifies the IP-SGT bindings through SXP and reapplies the appropriate tags or uses them for SGT-based enforcement. During egress caching, the original pre-Network Address Translation (NAT) source IP address is cached as part of the identified IP-SGT binding information.

4 IP-SGT bindings that do not receive traffic for 300 seconds are removed from the cache.

***Figure 8: SGT Caching in Bump-in-the-wire Topology***



# How to Configure Cisco TrustSec SGT Caching

## Configuring SGT Caching Globally

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-caching**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cts role-based sgt-caching**<br><br>**Example:**<br>`Device(config)# cts role-based sgt-caching` | Enables SGT caching in ingress direction for all interfaces. |
| **Step 4** | **end**<br><br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

## Configuring SGT Caching on an Interface

When an interface is configured to be on a Virtual Routing and Forwarding (VRF) network, the IP-SGT bindings identified on that interface are added under the specific VRF. (To view the bindings identified on a corresponding VRF, use the **show cts role-based sgt-map vrf** *vrf-name* **all** command.)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **cts role-based sgt-cache** [**ingress** | **egress**]
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type slot/port*<br><br>**Example:**<br><br>`Device(config)# interface gigabitEthernet 0/1/0` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **cts role-based sgt-cache** [**ingress** | **egress**]<br><br>**Example:**<br><br>`Device(config-if)# cts role-based sgt-cache ingress` | Configures SGT caching on a specific interface.<br><br>• ingress—Enables SGT caching for traffic entering the specific interface (inbound traffic).<br><br>• egress—Enables SGT caching for traffic exiting the specific interface (outbound traffic). |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Verifying Cisco TrustSec SGT Caching

## SUMMARY STEPS

1. **enable**
2. **show cts**
3. **show cts interface**
4. **show cts interface brief**
5. **show cts role-based sgt-map all ipv4**
6. **show cts role-based sgt-map vrf**
7. **show cts platform sgt-caching**

## DETAILED STEPS

### Step 1 enable

Enables privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Device> enable
```

### Step 2 show cts

Displays Cisco TrustSec connections and the status of global SGT caching.

**Example:**

```
Device# show cts

Global Dot1x feature: Disabled
CTS device identity: ""
CTS caching support: disabled
CTS sgt-caching global: Enabled
Number of CTS interfaces in DOT1X mode:  0,    MANUAL mode: 0
Number of CTS interfaces in LAYER3 TrustSec mode: 0
Number of CTS interfaces in corresponding IFC state
  INIT            state:  0
  AUTHENTICATING  state:  0
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  0
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0
CTS events statistics:
  authentication success: 0
  authentication reject : 0
  authentication failure: 0
  authentication logoff : 0
  authentication no resp: 0
  authorization success : 0
  authorization failure : 0
  sap success           : 0
  sap failure           : 0
```

```
  port auth failure     : 0
```

**Step 3** **show cts interface**

Displays Cisco TrustSec configuration statistics for an interface and SGT caching information with mode details (ingress or egress).

**Example:**

```
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

    L2-SGT Statistics
        Pkts In                     : 16298041
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 5
        Pkts Drop (malformed packet): 0
        Pkts Drop (invalid SGT)     : 0
```

**Step 4** **show cts interface brief**

Displays SGT caching information with mode details (ingress or egress) for all interfaces.

**Example:**

```
Device# show cts interface brief

Interface GigabitEthernet0/0
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

Interface GigabitEthernet0/2
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             0
        Peer SGT assignment:  Untrusted

Interface GigabitEthernet0/3
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface Backplane-GigabitEthernet0/4
    CTS sgt-caching Ingress:  Enabled
```

```
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface RG-AR-IF-INPUT1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled
```

**Step 5** **show cts role-based sgt-map all ipv4**
Displays all the SGT-IPv4 bindings.

**Example:**

```
Device# show cts role-based sgt-map all ipv4

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                50      CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
192.0.2.5                3900    INTERNAL
192.0.2.6                3900    INTERNAL
192.0.2.7                3900    INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CACHED   bindings = 20
Total number of INTERNAL bindings = 3
Total number of active   bindings = 23
```

**Step 6** **show cts role-based sgt-map vrf**
Displays all the SGT-IP bindings for the specific Virtual Routing and Forwarding (VRF) interface.

**Example:**

```
Device# show cts role-based sgt-map vrf

%IPv6 protocol is not enabled in VRF RED
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                2007    CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
```

**Step 7** **show cts platform sgt-caching**
Displays SGT caching information for a platform, such as per-interface SGT caching configuration, global SGT caching configuration, timeout configuration, and IP-SGT bindings identified through SGT caching.

**Example:**

```
Device# show cts platform sgt-caching

Sgt-caching is Active
Total number of bindings = 20
```

```
=============================================================================
 IP Address      SGT     Interface        Age         Exptime   Mode    VRFID
                                       (hh:mm:ss)     (sec)
=============================================================================
192.0.2.1        50        Gi0/1          0:01:05       83     In      ---
192.0.2.2        50        Gi0/1          0:01:05       83     In      ---
192.0.2.3        50        Gi0/1          0:01:05       83     In      ---
192.0.2.4        50        Gi0/1          0:01:05       83     In      ---
192.0.2.5        2007      Gi0/1          0:01:05       83     In      ---
192.0.2.6        50        Gi0/1          0:01:11       77     In      ---
192.0.2.7        50        Gi0/1          0:01:11       77     In      ---
```

# Configuration Examples for Cisco TrustSec SGT Caching

## Example: Configuring SGT Caching Globally

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# end
```

## Example: Configuring SGT Caching for an Interface

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# end
```

## Example: Disabling SGT Caching on an Interface

The following example shows how to disable SGT caching on an interface and displays the status of SGT caching on the interface when caching is enabled globally, but disabled on the interface.

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet 0/1
Device(config-if)# no cts role-based sgt-cache ingress
Device(config-if)# end
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Disabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
```

```
  Static Ingress SGT Policy:
    Peer SGT:             200
    Peer SGT assignment:  Trusted

L2-SGT Statistics
    Pkts In                      : 200890684
    Pkts (policy SGT assigned)   : 0
    Pkts Out                     : 14
    Pkts Drop (malformed packet): 0
    Pkts Drop (invalid SGT)      : 0
```

# Additional References for Cisco TrustSec SGT Caching

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Cisco IOS Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |
| Cisco TrustSec configuration | "Cisco TrustSec Support for IOS" chapter in the *Cisco TrustSec Configuration Guide* |
| Cisco TrustSec overview | Overview of TrustSec |
| Cisco TrustSec solution | Cisco TrustSec Security Solution |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Cisco TrustSec SGT Caching

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 10: Feature Information for Cisco TrustSec SGT Caching*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco TrustSec SGT Caching | Cisco IOS 15.5(2)T | The Cisco TrustSec SGT Caching feature enhances the ability of Cisco TrustSec to make Security Group Tag (SGT) transportability flexible. This feature identifies the IP-SGT binding and caches the corresponding SGT so that network packets are forwarded through all network services for normal deep packet inspection processing and at the service egress point the packets are re-tagged with the appropriate SGT.<br>In Cisco IOS Release 15.5(2)T, support was added for Cisco Integrated Services Router Generation 2 (Cisco ISR G2).<br>The following commands were introduced or modified: **cts role-based sgt-caching**, **cts role-based sgt-cache** [**ingress** \| **egress**]. |