Cisco TrustSec SGT Exchange Protocol

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 SXP. SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. 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

The SXP network needs to be established before implementing SXP. The 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.
- SXP software runs on all network devices

- Connectivity exists between all network devices

Restrictions for Cisco TrustSec SGT Exchange Protocol

- SXP does not support connections over IPv6.
- If the default password is configured on a switch, the connection on that switch should configure the password to use the default password. If the default password is not configured, the connection on that switch should be configured so as 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

Security Group Tagging

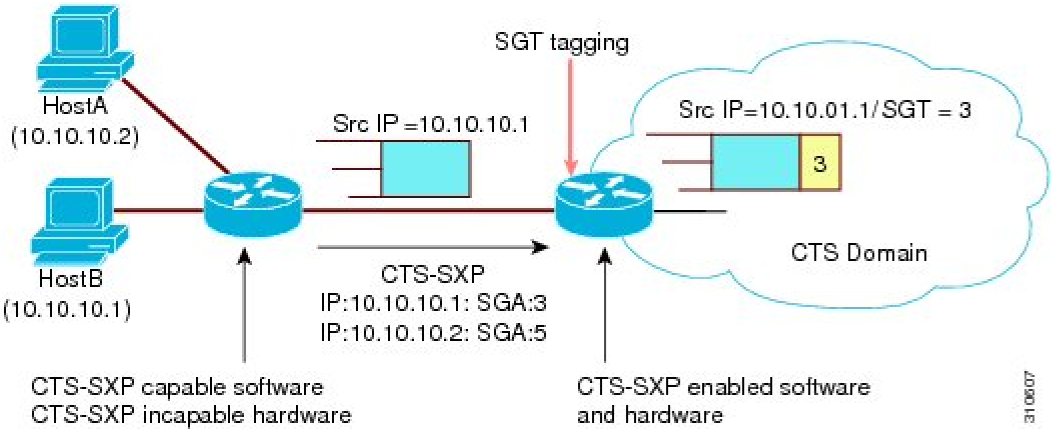
Cisco TrustSec (CTS) uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the CTS network so that they can be properly identified for 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 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 SXP is used, then these devices can pass IP-to-SGT mappings to a CTS peer device that has CTS-capable hardware.

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 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 SXP Propagates SGT Information



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

- If SXP data integrity and authentication are required, the same SXP password can be configured on both peer devices. The SXP password can be configured either explicitly for each peer connection or globally for the device. Although an SXP password is not required it is recommended.
- Each peer on the SXP connection can be configured as either an SXP speaker, or an SXP listener, or both. The speaker device distributes the IP-to-SGT mapping information to the listener device. If one peer on an SXP connection is configured as both speaker and listener, then the other peer on the connection must also be connected as both speaker and listener.
- 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.

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 an 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 an SXP listener for one SXP connection as an SXP speaker for another SXP connection.

A CTS device maintains connectivity with its 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.

How to Configure the Cisco TrustSec SGT Exchange Protocol

Enabling SXP

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp enable** **Example:** `Device(config)# cts sxp enable`	Enables an SXP connection to any peer connection that is configured. **Note** Ensure that peer connections are configured. If peer connections are not configured, then SXP connections cannot be established with them.

Configuring SXP Peer Connection

The 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 SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco TrustSec software derives the SXP source IP address from existing local IP addresses. The 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** | **both**]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief**]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker** | **both**]]
	Example:
	`Device(config)# cts sxp connection peer 10.20.2.2`
	` password default mode local speaker`
		Configures the SXP peer address connection.
		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.
		The **password** keyword specifies the password that SXP uses for the connection using the following options:
		• **default**—Use the default SXP password you configured using the **cts sxp default password** command.
		• **none**—A password is not used.
		The **mode** keyword specifies the role of the remote peer device:
		• **local**—The specified mode refers to the local device.
		• **peer**—The specified mode refers to the peer device.
		• **listener**—Specifies that the device is the listener in the connection.
		• **speaker**—Specifies that the device is the speaker in the connection. This is the default.
		• **both**—Specifies that the device is in bi-directional mode (listener and speaker).

Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show cts sxp** {**connections** | **sgt-map**} [**brief**] **Example:** `Device# show cts sxp connections`	(Optional) Displays SXP status and connections.

Configuring the Default 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp default password** [**0** | **6** | **7**] *password* **Example:** `Device(config)# cts sxp default password Cisco123`	Configures the 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. **Note** By default, SXP uses no password when setting up connections.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

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

Configuring the SXP Reconciliation Period

After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconciliation period timer starts. While the 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 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp reconciliation period** *seconds* **Example:** `Device(config)# cts sxp reconciliation period 150`	Sets the SXP reconciliation timer, in seconds. The range is from 0 to 64000. The default is 120.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and enters privileged EXEC mode.

Configuring the SXP Retry Period

The SXP retry period determines how often the CTS software retries an SXP connection. If an SXP connection is not established successfully, then the CTS software makes a new attempt to set up the connection after the SXP retry period timer expires. The default value is 2 minutes. Setting the 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp retry period** *seconds* **Example:** `Device(config)# cts sxp retry period 160`	Sets the SXP retry timer, in seconds. The range is from 0 to 64000. The default is 120.

	Command or Action	Purpose
Step 4	**exit** **Example:** `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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts sxp log binding-changes** **Example:** `Device(config)# cts sxp log binding-changes`	Enables logging for IP-to-SGT binding changes causing 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 SXP connection. **Note** This logging function is disabled by default.
Step 4	**exit** **Example:** `Device# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the SXP Connection

SUMMARY STEPS

1. **enable**
2. **show cts sxp connections** [**brief**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Switch# enable
```

Step 2 **show cts sxp connections** [**brief**]

Displays the SXP status and connections.

Example:

```
Switch# 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 1: Connection Status Output Scenarios

Node1	**Node2**	**Node1 CLI Output for Connection Status**	**Node2 CLI Output for Connection Status**
Both	Both	On (Speaker) On (Listener)	On (Speaker) On (Listener)
Speaker	Listener	On	On
Listener	Speaker	On	On

Note If one peer on an SXP connection is configured as both speaker and listener, then the other peer on the connection must also be connected as both speaker and listener.

Configuration Examples for Cisco TrustSec SGT Exchange Protocol IPv4

Example: Enabling and Configuring SXP Peer Connection

The following example shows how to enable SXP and configure the 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 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 example shows how to enable bidirectional 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
```

The following sample output for **show cts sxp connections** command displays 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
```