CHAPTER 4

Configuring SGT Exchange Protocol over TCP (SXP) and Layer 3 Transport

Revised: May 28, 2010, OL-22192-01

You can use the SGT Exchange Protocol (SXP) to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec. This section describes how to configure Cisco TrustSec SXP on switches in your network.

This section includes the following topics:

Cisco TrustSec SGT Exchange Protocol Feature Histories

For a list of supported TrustSec features per platform and the minimum required IOS release, see the *Cisco TrustSec Platform Support Matrix* at the following URL: (final URL posted with TS 4.0)

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.

Configuring Cisco TrustSec SXP

To configure Cisco TrustSec SXP, follow these steps:

Step 1 Enable the Cisco TrustSec feature (see the "Configuring Identities, Connections, and SGTs" chapter).

Step 2 Enable Cisco TrustSec SXP (see the "Enabling Cisco TrustSec SXP" section on page 4-2).

Step 3 Configure SXP peer connections (see the "Configuring an SXP Peer Connection" section on page 4-2).

Enabling Cisco TrustSec SXP

You must enable Cisco TrustSec SXP before you can configure peer connections. To enable Cisco TrustSec SXP, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# [no] cts sxp enable`	Enables SXP for Cisco TrustSec.
Step 3	`Router(config)# exit`	Exits configuration mode.

Configuring an SXP Peer Connection

You must configure the SXP peer connection on both of the 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 address might be different for each TCP connection initiated from the switch.

To configure the SXP peer connection, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# cts sxp connection peer peer-ipv4-addr [source src-ipv4-addr] password {default | none} mode {local | peer} {speaker | listener} [vrf vrf-name]`	Configures the SXP address connection. The optional **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection will use the default source address, if configured, or the address of the port. The **password** keyword specifies the password that SXP will use for the connection using the following options: • **default**—Use the default SXP password you configured using the **cts sxp default password** command. • **none**—Do not use a password. 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. • **speaker**—Default. Specifies that the device is the speaker in the connection. • **listener**—Specifies that the device is the listener in the connection. The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.
Step 3	`Router(config)# exit`	Exits configuration mode.
Step 4	`Router# show cts sxp connections`	(Optional) Displays the SXP connection information.

This example shows how to enable SXP and configure the SXP peer connection on Switch A, a speaker, for connection to Switch B, a listener:

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

This example shows how to configure the SXP peer connection on Switch B, a listener, for connection to Switch A, a speaker:

```
Router# configure terminal
Router(config)# cts sxp enable
Router(config)# cts sxp default password Cisco123
```

```
Router(config)# cts sxp default source-ip 10.20.2.2
Router(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

Configuring the Default SXP Password

By default, SXP uses no password when setting up connections. You can configure a default SXP password for the switch. In Cisco IOS Release 12.2(50)SY and later releases, you can specify an encrypted password for the SXP default password.

To configure a default SXP password, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# cts sxp default password [0 | 6 | 7] password`	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.
Step 3	`Router(config)# exit#`	Exits configuration mode.

This example shows how to configure a default SXP password:

```
Router# configure terminal
Router(config)# cts sxp default password Cisco123
```

Configuring the Default SXP Source IP Address

SXP uses the default source IP address for all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.

To configure a default SXP source IP address, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# cts sxp default source-ip src-ip-addr`	Configures the SXP default source IP address.
Step 3	`Router(config)# exit`	Exits configuration mode.

This example shows how to configure an SXP default source IP address:

```
Router# configure terminal
Router(config)# cts sxp default source-ip 10.20.2.2
```

Changing 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 Cisco TrustSec 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.

To change the SXP reconciliation period, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# cts sxp reconciliation period` *seconds*	Changes the SXP reconciliation timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 3	`Router(config)# exit`	Exits configuration mode.

Changing the SXP Retry Period

The SXP retry period determines how often the Cisco TrustSec software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco TrustSec software makes a new attempt to set up the connection after the SXP retry period timer expires. The default value is 120 seconds. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

To change the SXP retry period, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# cts sxp retry period` *seconds*	Changes the SXP retry timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 3	`Router(config)# exit`	Exits configuration mode.

Creating Syslogs to Capture Changes of IP Address to SGT Mapping Learned Through SXP

When the **cts sxp log binding-changes** global configuration command is executed, SXP syslogs (sev 5 syslog) are generated whenever a change to IP address to SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection.

The default is **no cts sxp log binding-changes**.

To enable logging of binding changes, perform the following task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# cts sxp log binding-changes`	Turns on logging for IP to SGT binding changes.

Verifying the SXP Connections

To view the SXP connections, perform this task:

	Command	Purpose
Step 1	`Router# show cts sxp connections [brief]`	Displays SXP status and connections.

This example shows how to view the SXP connections:

```
Router# 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
Conn Version     : 2
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
```

Configuring Layer 3 SGT Transport Between Cisco TrustSec Domains

Feature Name	Releases	Feature Information
L3 SGT Transport	12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.

You can configure Layer 3 SGT Transport on Cisco TrustSec gateway devices on the edges of a network domain that has no Cisco TrustSec-capable devices.

To configure Layer 3 SGT Transport, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# [no] cts policy layer3 {ipv4 | ipv6} traffic acl-name`	(Optional) Specifies the fallback traffic policy to be applied when the authentication server is not available for downloading the traffic policy. • *acl-name*—The name of a traditional interface ACL already configured on the device. See the additional usage notes following this task.
Step 3	`Router(config)# [no] cts policy layer3 {ipv4 | ipv6} exception acl-name`	(Optional) Specifies the fallback exception policy to be applied when the authentication server is not available for downloading the exception policy. See the additional usage notes following this task.
Step 4	`Router(config)# interface type slot/port`	Specifies an interface and enters interface configuration mode.
Step 5	`Router(config-if)# [no] cts layer3 {ipv4 | ipv6} trustsec forwarding`	(Configured on a Cisco TrustSec-capable physical port) Specifies that egress traffic on this interface will use Cisco TrustSec Layer 3 SGT transport encapsulation as determined by the traffic and exception policies.
	`Router(config-if)# [no] cts layer3 {ipv4 | ipv6} policy`	(Configured on a routed port or SVI) Specifies that egress traffic on this interface will use Cisco TrustSec Layer 3 SGT transport encapsulation as determined by the traffic and exception policies.
Step 6	`Router(config-if)# end` `Router(config)# end`	Exits interface configuration and global configuration modes.
Step 7	`Router# show cts policy layer3 {ipv4 | ipv6}`	(Optional) Displays the Layer 3 SGT transport configuration on the interfaces.

When configuring Cisco TrustSec Layer 3 SGT transport, consider these usage guidelines and restrictions:

- The Cisco TrustSec Layer 3 SGT transport feature can be configured only on ports that support hardware encryption.
- Traffic and exception policies for Cisco TrustSec Layer 3 SGT transport have the following restrictions:
  - The policies must be configured as IP extended or IP named extended ACLs.
  - The policies must not contain **deny** entries.
  - If the same ACE is present in both the traffic and exception policies, the exception policy takes precedence. No Cisco TrustSec Layer 3 encapsulation will be performed on packets matching that ACE.

- Traffic and exception policies can be downloaded from the authentication server (if supported by your Cisco IOS Release) or manually configured on the device. The policies will be applied based on these rules:
  - If a traffic policy or an exception policy is downloaded from the authentication server, it will take precedence over any manually configured traffic or exception policy.
  - If the authentication server is not available but both a traffic policy and an exception policy have been manually configured, the manually configured policies will be used.
  - If the authentication server is not available but a traffic policy has been configured with no exception policy, no exception policy is applied. Cisco TrustSec Layer 3 encapsulation will be applied on the interface based on the traffic policy.
  - If the authentication server is not available and no traffic policy has been manually configured, no Cisco TrustSec Layer 3 encapsulation will be performed on the interface.

This example shows how to configure Layer 3 SGT Transport to a remote Cisco TrustSec domain:

```
Router# configure terminal
Router(config)# ip access-list extended traffic-list
Router(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended exception-list
Router(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# cts policy layer3 ipv4 traffic traffic-sgt
Router(config)# cts policy layer3 ipv4 exception exception-list
Router(config)# interface gi2/1
Router(config-if)# cts layer3 trustsec ipv4 forwarding
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

Configuring Cisco TrustSec Reflector for Cisco TrustSec-Incapable Switching Modules

Note The Cisco TrustSec supervisor ingress reflector and the Cisco TrustSec egress reflector are mutually exclusive. Do not enable both functions.

Egress reflector should be disabled when ERSPAN is configured.

To configure the Cisco TrustSec supervisor ingress reflector function, perform this task.

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# [no] platform cts ingress`	Activates the Cisco TrustSec supervisor ingress reflector.

	Command	Purpose
Step 3	`Router(config)# exit`	Exits configuration mode.
Step 4	`Router# show platform cts`	Displays Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS).

This example shows how to configure a Cisco TrustSec ingress reflector:

```
Router# configure terminal
Router(config)# platform cts ingress
Router(config)# exit
Router# show platform cts
 CTS Ingress mode enabled
```

Note Before disabling the Cisco TrustSec ingress reflector, you must remove power from the Cisco TrustSec-incapable switching modules.

To configure the Cisco TrustSec egress reflector function, perform this task.

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# [no] platform cts egress`	Activates the Cisco TrustSec egress reflector.
Step 3	`Router(config)# exit`	Exits configuration mode.
Step 4	`Router# show platform cts`	Displays Cisco TrustSec reflector mode (Ingress, Egress, Pure, or No CTS).

This example shows how to configure a Cisco TrustSec egress reflector:

```
Router# configure terminal
Router(config)# platform cts egress
Router(config)# exit
Router# show platform cts
 CTS Egress mode enabled
```

Note Before disabling the Cisco TrustSec egress reflector, you must remove power from the Cisco TrustSec-incapable switching modules.

Configuring Cisco TrustSec Caching

Enabling Cisco TrustSec Caching

For quick recovery from brief outages, you can enable caching of authentication, authorization, and policy information for Cisco TrustSec connections. Caching allows Cisco TrustSec devices to use unexpired security information to restore links after an outage without requiring a full reauthentication

of the Cisco TrustSec domain. The Cisco TrustSec devices will cache security information in DRAM. If non-volatile (NV) storage is also enabled, the DRAM cache information will also be stored to the NV memory. The contents of NV memory populate DRAM during a reboot.

Note During extended outages, the Cisco TrustSec cache information is likely to become outdated.

To enable Cisco TrustSec caching, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode.
Step 2	`Router(config)# [no] cts cache enable`	Enables caching of authentication, authorization and environment-data information to DRAM. The default is disabled. The **no** form of this command deletes all cached information from DRAM and non-volatile storage.
Step 3	`Router(config)# [no] cts cache nv-storage {bootdisk: | bootflash: | disk0:} [directory dir-name]`	When DRAM caching is enabled, enables DRAM cache updates to be written to non-volatile storage. Also enables DRAM cache to be initially populated from non-volatile storage when the device boots.
Step 4	`Router(config)# exit`	Exits configuration mode.

This example shows how to configure Cisco TrustSec caching, including non-volatile storage:

```
Router# configure terminal
Router(config)# cts cache enable
Router(config)# cts cache nv-storage bootdisk:
Router(config)# exit
```

Clearing the Cisco TrustSec Cache

To clear the cache for Cisco TrustSec connections, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Router# clear cts cache [authorization-policies [peer] | environment-data | filename filename | interface-controller [type slot/port]]`	Clears the cache for Cisco TrustSec connection information.

This example shows how to clear the Cisco TrustSec cache:

```
Router# clear cts cache
```