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 1: 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 **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. **Note** The Role-Based IP-SGT database limit is 200K across all platforms.
ISR 2900, ISR 3900	250	125	• 180K for unidirectional SXP connections • 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 1: 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** **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 enable** **Example:** `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** **Example:** `Device(config)# cts sxp default password Cisco123`	(Optional) Specifies the Cisco TrustSec SGT SXP default password.
Step 5	**cts sxp default source-ip** **Example:** `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*] **Example:** `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. 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 Cisco TrustSec SXP uses for the connection using the following options: • **default—**Use the default Cisco TrustSec 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. • **both—**Specifies that the device is both the speaker and the listener in the bidirectional SXP connection. 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* **Example:** `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* **Example:** `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. **Note** The *maximum-period* value must be greater than or equal to the *minimum-period* value.
Step 9	**exit** **Example:** `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 2: 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

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 • 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 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. 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. 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 3: Feature Information for Bidirectional SXP Support

Feature Name	Releases	Feature Information
Bidirectional SXP Support	Cisco IOS 15.4(1)T 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. The following command was introduced or modified: **cts sxp connection peer**.