Cisco TrustSec Configuration Guide, Cisco IOS XE Gibraltar 16.10.x

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **Overview of Cisco TrustSec** 3

- SGT Inline Tagging 3
- SGT Inline Tagging for IPv6 Traffic 4
- CTS Credentials 5
- Configuring SGT Inline Tagging 5
- Configuring CTS Credentials 7
- Example: Configuring SGT Inline Tagging 8
- Feature Information for Overview of Cisco TrustSec 8

CHAPTER 3 **Cisco TrustSec SGT Exchange Protocol IPv4** 9

- Finding Feature Information 9
- Prerequisites for Cisco TrustSec SGT Exchange Protocol IPv4 9
- Restrictions for Cisco TrustSec SGT Exchange Protocol IPv4 10
- Information About Cisco TrustSec SGT Exchange Protocol IPv4 10
  - Security Group Tagging 10
  - Using CTS-SXP for SGT Propagation Across Legacy Access Networks 10
  - VRF-Aware CTS-SXP 11
  - Security Group Access Zone-Based Policy Firewall 12
- How to Configure Cisco TrustSec SGT Exchange Protocol IPv4 13
  - Enabling CTS-SXP 13
  - Configuring a CTS-SXP Peer Connection 13
  - Configuring the Default CTS-SXP Password 15
  - Configuring the Default CTS-SXP Source IP Address 16
  - Configuring the CTS-SXP Reconciliation Period 16

Configuring the CTS-SXP Retry Period 17
Creating Syslogs to Capture IP-to-SGT Mapping Changes 18
Configuring a Class Map for a Security Group Access Zone-Based Policy Firewall 19
Creating a Policy Map for a Security Group Access Zone-Based Policy Firewall 21
Configuration Examples for Cisco TrustSec SGT Exchange Protocol IPv4 24
Example: Enabling and Configuring a CTS-SXP Peer Connection 24
Example: Configuring a Security Group Access Zone-Based Policy Firewall 25
Additional References for TrustSec SGT Handling: L2 SGT Imposition and Forwarding 26
Feature Information for Cisco TrustSec SGT Exchange Protocol IPv4 27

CHAPTER 4 **TrustSec SGT Handling: L2 SGT Imposition and Forwarding 29**
Finding Feature Information 29
Prerequisites for TrustSec SGT Handling: L2 SGT Imposition and Forwarding 29
Information about TrustSec SGT Handling: L2 SGT Imposition and Forwarding 30
Security Groups and SGTs 30
How to Configure TrustSec SGT Handling: L2 SGT Imposition and Forwarding 30
Manually Enabling TrustSec SGT Handling: L2 SGT Imposition and Forwarding on an Interface 30
Disabling CTS SGT Propagation on an Interface 32
Additional References for TrustSec SGT Handling: L2 SGT Imposition and Forwarding 34
Feature Information for TrustSec SGT Handling: L2 SGT Imposition and Forwarding 35

CHAPTER 5 **Cisco TrustSec with SXPv4 37**
Finding Feature Information 37
Information About Cisco TrustSec with SXPv4 37
Overview of Cisco TrustSec with SXPv4 37
SXP Node ID 38
Keepalive and Hold-time Negotiation with SXPv4 39
How to Configure Cisco TrustSec with SXPv4 41
Configuring the Hold-time for the SXPv4 Protocol on a Network Device 41
Configuring the Hold-Time for the SXPv4 Protocol for Each Connection 42
Configuring the Node ID of a Network Device 44
Configuration Examples for Cisco TrustSec with SXPv4 45
Example: Configuring Cisco TrustSec with SXPv4 45

Example: Verifying Cisco TrustSec with SXPv4 45
Additional References for Cisco TrustSec with SXPv4 46
Feature Information for Cisco TrustSec with SXPv4 47

CHAPTER 6 **Enabling Bidirectional SXP Support** 49
Finding Feature Information 49
Prerequisites for Bidirectional SXP Support 49
Restrictions for Bidirectional SXP Support 50
Information About Bidirectional SXP Support 50
Bidirectional SXP Support Overview 50
How to Enable Bidirectional SXP Support 51
Configuring Bidirectional SXP Support 51
Verifying Bidirectional SXP Support Configuration 53
Configuration Examples for Bidirectional SXP Support 54
Example: Configuring Bidirectional SXP Support 54
Additional References for Bidirectional SXP Support 55
Feature Information for Bidirectional SXP Support 55

CHAPTER 7 **SXP IP-Prefix and SGT based Filtering** 57
Restrictions for SXP IP-Prefix and SGT-based Filtering 57
Information about SXP IP-Prefix and SGT based Filtering 58
Feature Information for SXP IP-Prefix and SGT Based Filtering 58
Types of SXP Filtering 59
How to Configure an SXP Filter 59
Configuring an SXP Filter List 60
Configuring an SXP Filter Group 60
Enabling SXP Filtering 61
Configuring the Default or Catch-All Rule 61
Show Commands 62
show cts sxp filter-list 62
show cts sxp filter-group 62
Troubleshooting 63
debug cts sxp filter events 63
Syslog Messages for SXP Filtering 64

Syslog Messages for Filter Rules 64
Syslog Messages for Filter Lists 64

CHAPTER 8 Cisco TrustSec Interface-to-SGT Mapping 65
Finding Feature Information 65
Information About Cisco TrustSec Interface-to-SGT Mapping 65
Interface-to-SGT Mapping 65
Binding Source Priorities 66
How to Configure Cisco TrustSec Interface-to-SGT Mapping 66
Configuring Layer 3 Interface-to-SGT Mapping 66
Verifying Layer 3 Interface-to-SGT Mapping 67
Configuration Examples for Cisco TrustSec Interface-to-SGT Mapping 68
Example: Configuring Layer 3 Interface-to-SGT Mapping 68
Additional References for Cisco TrustSec Interface-to-SGT Mapping 68
Feature Information for Cisco TrustSec Interface-to-SGT Mapping 69

CHAPTER 9 Cisco TrustSec Subnet to SGT Mapping 71
Finding Feature Information 71
Restrictions for Cisco TrustSec Subnet to SGT Mapping 71
Information About Cisco TrustSec Subnet to SGT Mapping 72
How to Configure Cisco TrustSec Subnet to SGT Mapping 72
Configuring Subnet to SGT Mapping 72
Cisco TrustSec Subnet to SGT Mapping: Examples 74
Additional References 75
Feature Information for Cisco TrustSec Subnet to SGT Mapping 76

CHAPTER 10 Flexible NetFlow Export of Cisco TrustSec Fields 77
Finding Feature Information 77
Restrictions for Flexible NetFlow Export of Cisco TrustSec Fields 77
Information About Flexible NetFlow Export of Cisco TrustSec Fields 78
Cisco TrustSec Fields in Flexible NetFlow 78
How to Configure Flexible NetFlow Export of Cisco TrustSec Fields 79
Configuring Cisco TrustSec Fields as Key Fields in the Flow Record 79
Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record 81

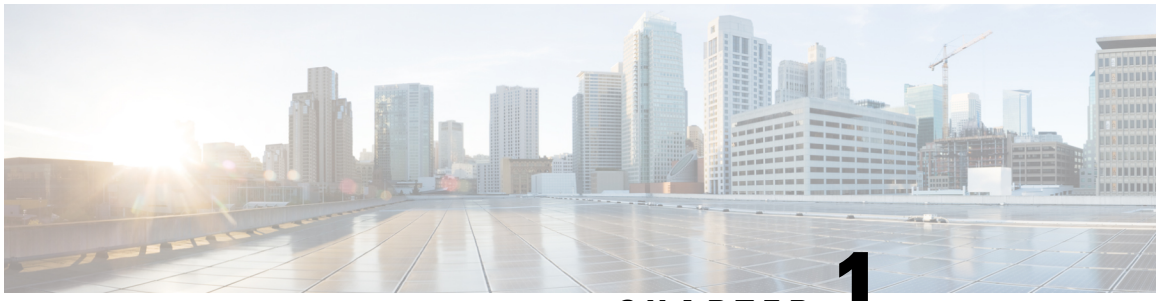
Configuring a Flow Exporter 83
Configuring a Flow Monitor 84
Applying a Flow Monitor on an Interface 85
Verifying Flexible NetFlow Export of Cisco TrustSec Fields 86
Configuration Examples for Flexible NetFlow Export of Cisco TrustSec Fields 89
Example: Configuring Cisco TrustSec Fields as Key Fields in the Flow Record 89
Example: Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record 89
Example: Configuring a Flow Exporter 89
Example: Configuring a Flow Monitor 90
Example: Applying a Flow Monitor on an Interface 90
Additional References for Flexible NetFlow Export of Cisco TrustSec Fields 90
Feature Information for Flexible NetFlow Export of Cisco TrustSec Fields 91

CHAPTER 11 **Cisco TrustSec SGT Caching** 93
Finding Feature Information 93
Restrictions for Cisco TrustSec SGT Caching 93
Information About Cisco TrustSec SGT Caching 94
Identifying and Reapplying SGT Using SGT Caching 94
SGT Caching for IPv6 Traffic 95
How to Configure Cisco TrustSec SGT Caching 96
Configuring SGT Caching Globally 96
Configuring SGT Caching on an Interface 96
Verifying Cisco TrustSec SGT Caching 97
Verifying IP-to-SGT Bindings 100
Configuration Examples for Cisco TrustSec SGT Caching 101
Example: Configuring SGT Caching Globally 101
Example: Configuring SGT Caching for an Interface 101
Example: Disabling SGT Caching on an Interface 101
Additional References for Cisco TrustSec SGT Caching 102
Feature Information for Cisco TrustSec SGT Caching 103

CHAPTER 12 **CTS SGACL Support** 105
Finding Feature Information 105
Prerequisites for CTS SGACL Support 105

Restrictions for CTS SGACL Support 105
Information About CTS SGACL Support 106
CTS SGACL Support 106
SGACL Monitor Mode 106
How to Configure CTS SGACL Support 107
Enabling SGACL Policy Enforcement Globally 107
Enabling SGACL Policy Enforcement Per Interface 107
Configuring IPv6 SGACL Access Control Entries 107
Attaching SGACLs to Permission Matrix Cell 107
Manually Configuring SGACL Policies 108
Refreshing the Downloaded SGACL Policies 108
Configuring SGACL Monitor Mode 108
Configuring IPv6 SGACL ACE 108
Configuration Examples for CTS SGACL Support 109
Example: CTS SGACL Support 109
Example: Configuring SGACL Monitor Mode 111
Example: Refreshing the Downloaded SGACL Policies 111
Additional References for CTS SGACL Support 112
Feature Information for CTS SGACL Support 112

CHAPTER 13 **Accessing TrustSec Operational Data Externally** 115
Prerequisites for Accessing Cisco TrustSec Operational Data Externally 115
Restrictions for Accessing Cisco TrustSec Operational Data Externally 116
Information About Cisco TrustSec Operational Data 116
How to Configure the External Device YTOOL 120
Accessing Operational Data 121



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

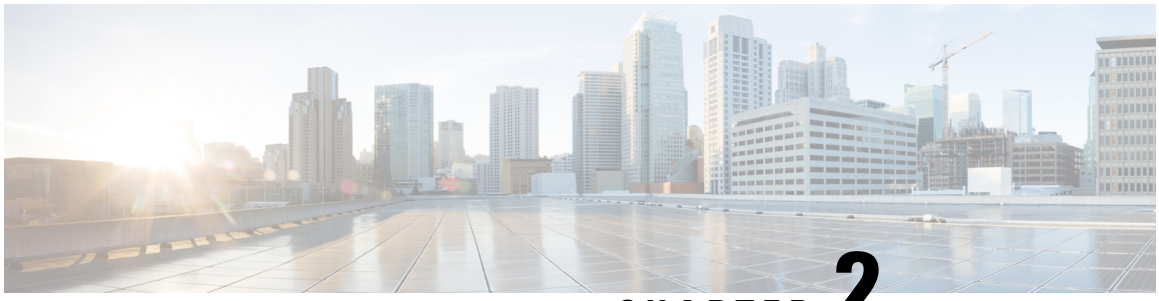
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

Overview of Cisco TrustSec

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

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

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

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

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

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

- SGT Inline Tagging, on page 3
- SGT Inline Tagging for IPv6 Traffic, on page 4
- CTS Credentials, on page 5
- Configuring SGT Inline Tagging, on page 5
- Configuring CTS Credentials, on page 7
- Example: Configuring SGT Inline Tagging, on page 8
- Feature Information for Overview of Cisco TrustSec, on page 8

SGT Inline Tagging

Each security group in a CTS domain is assigned a unique 16-bit tag called the “Scalable Group Tag” (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn

propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag.

CTS-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L2) layer. This feature is called "L2-SGT Imposition." It allows Ethernet interfaces on the device to be enabled for L2-SGT imposition so that device can insert an SGT in the packet to be carried to its next hop Ethernet neighbor. SGT-over-Ethernet is a method of hop-by-hop propagation of SGT embedded in clear-text (unencrypted) Ethernet packets. Inline identity propagation is scalable, provides near line-rate performance and avoids control plane overhead.

The Cisco TrustSec with SXPv4 feature supports CTS Meta Data (CMD) based L2-SGT. When a packet enters a CTS enabled interface, the IP-SGT mapping database (with dynamic entries built by SXP and/or static entries built by configuration commands) is analyzed to learn the SGT corresponding to the source IP address of the packet, which is then inserted into the packet and carried throughout the network within the CTS header.

As the tag represents the group of the source, the tag is also referred to as the Source Group Tag (SGT). At the egress edge of the network, the group assigned to the packet's destination becomes known. At this point, the access control can be applied. With CTS, access control policies are defined between the security groups and are referred to as Security Group Access Control Lists (SGACL). From the view of any given packet, it is simply being sourced from a security group and destined for another security group.

SGT Inline Tagging for IPv6 Traffic

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

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

Restrictions for SGT Inline Tagging IPv6 Traffic

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

Restrictions for CTS in IPv6 Deployments

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

CTS Credentials

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

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

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

Configuring SGT Inline Tagging

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Configuring CTS Credentials

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Example: Configuring SGT Inline Tagging

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

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

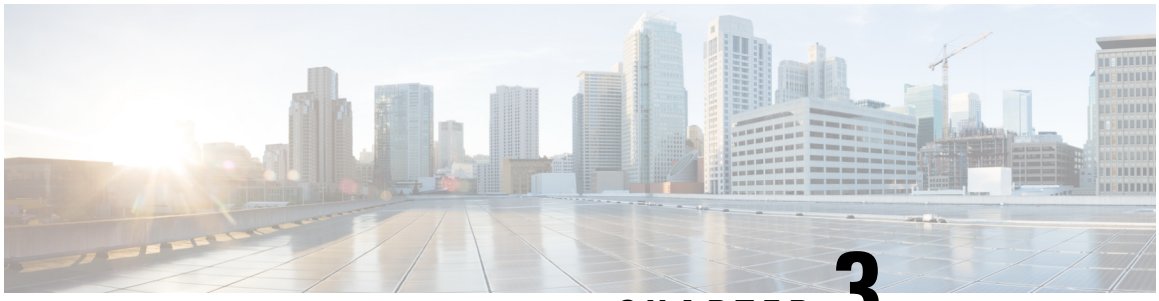
Feature Information for Overview of Cisco TrustSec

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

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

Table 1: Feature Information for Overview of Cisco TrustSec

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



CHAPTER 3

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, on page 9
- Prerequisites for Cisco TrustSec SGT Exchange Protocol IPv4, on page 9
- Restrictions for Cisco TrustSec SGT Exchange Protocol IPv4, on page 10
- Information About Cisco TrustSec SGT Exchange Protocol IPv4, on page 10
- How to Configure Cisco TrustSec SGT Exchange Protocol IPv4, on page 13
- Configuration Examples for Cisco TrustSec SGT Exchange Protocol IPv4, on page 24
- Additional References for TrustSec SGT Handling: L2 SGT Imposition and Forwarding, on page 26
- Feature Information for Cisco TrustSec SGT Exchange Protocol IPv4, on page 27

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.

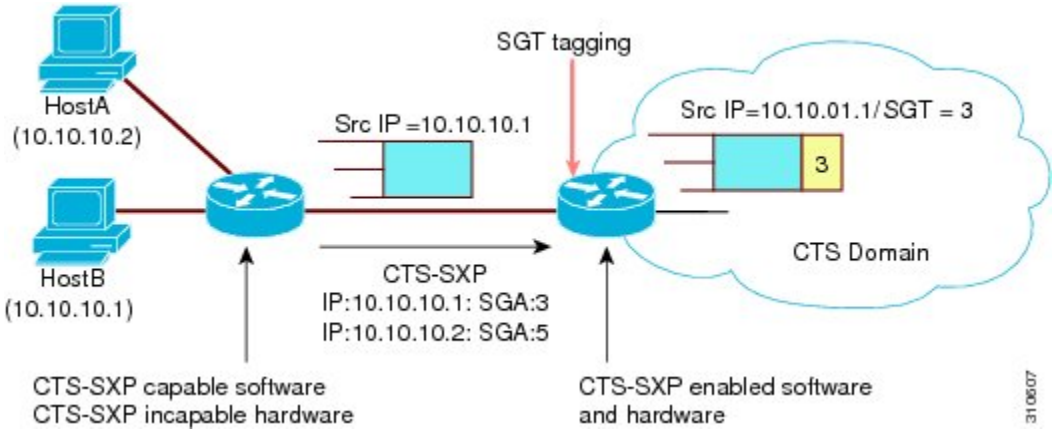
Using CTS-SXP for SGT Propagation Across Legacy Access Networks

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.

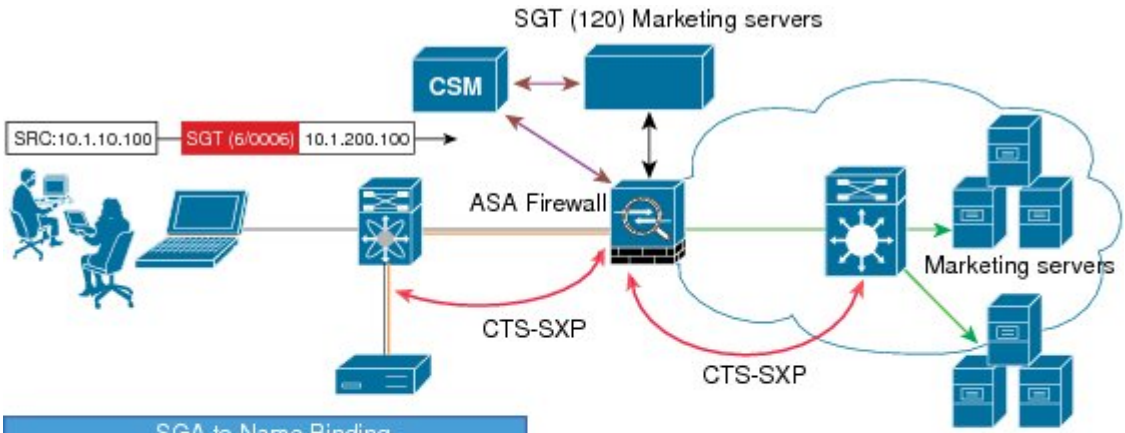
- Different VRFs may have overlapping CTS-SXP peer or source IP addresses.
- IP-to-SGT mappings learned (added or deleted) in one VRF can be updated only in the same VRF domain. The CTS-SXP connection cannot update a mapping bound to a different VRF. If no SXP connection exits for a VRF, IP-SGT mappings for that VRF will not 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 and destination IP addresses in the packet are used to derive source and destination 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



SGA to Name Binding	
Secuirty Group Name	Secuirty Group Tag
mktg-server	120
mktg-corp-users	006
mktg-contractor	080
corp-servers	090

How to Configure 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** **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 a CTS-SXP connection to any peer connection that is configured. **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** **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 connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]] **Example:** `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker`	Configures the CTS-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 CTS-SXP uses for the connection using the following options: • **default**—Use the default CTS-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. The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.

	Command or Action	Purpose
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** | **vrf** *vrf-name*] **Example:** `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** **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 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. **Note** By default, CTS-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 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** **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 CTS-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 CTS-SXP source IP address is configured.
Step 4	**exit** **Example:** `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** **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 reconciliation period** *seconds* **Example:** `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** **Example:** `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** **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 retry period** *seconds* **Example:** `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** **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 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. **Note** This logging function is disabled by default.

	Command or Action	Purpose
Step 4	**exit** **Example:** `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 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. **object-group security** *name*
4. **security-group tag-id** *sgt-id*
5. **group-object** *name*
6. **description** *text*
7. **exit**
8. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
9. **match group-object security source** *name*
10. **match group-object security destination** *name*
11. **end**
12. **show object-group** [*name*]

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**object-group security** *name* **Example:** `Device(config)# object-group security myobject1a`	Creates an object group to identify traffic coming from a specific user or endpoint and enters object-group identity mode.
Step 4	**security-group tag-id** *sgt-id* **Example:** `Device(config-object-group)# security-group tag-id 120`	Specifies the membership of a security group by using the SGT ID number. This number can be from 1 to 65535. Multiple security groups can be specified using this command.
Step 5	**group-object** *name* **Example:** `Device(config-object-group)# group-object admin`	(Optional) Specifies a nested reference to a type of user group. Multiple nested user groups can be specified using this command.
Step 6	**description** *text* **Example:** `Device(config-object-group)# description my sgtinfo`	(Optional) Defines information about the security group.
Step 7	**exit** **Example:** `Device(config-object-group)# exit`	Exits object-group identity mode and enters global configuration mode.
Step 8	**class-map type inspect** [**match-any** | **match-all**] *class-map-name* **Example:** `Device(config)# class-map type inspect match-any myclass1`	Creates a Layer 3 or Layer 4 inspect type class map and enters class-map configuration mode.
Step 9	**match group-object security source** *name* **Example:** `Device(config-cmap)# match group-object security source myobject1`	Matches traffic from a user in the security group.
Step 10	**match group-object security destination** *name* **Example:** `Device(config-cmap)# match group-object security destination myobject1`	Matches traffic for a user in the security group.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config-cmap)# end`	Exits class-map configuration mode and enters privileged EXEC mode.
Step 12	**show object-group** [*name*] **Example:** `Device# show object-group admin`	(Optional) Displays the content of all user groups. Optionally, use the *name* argument to show information for a single group.

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** **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	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect z1z2-policy`	Creates a Layer 3 or Layer 4 inspect type policy map. • Enters policy map configuration mode.
Step 4	**class type inspect** *class-name* **Example:** `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** **Example:** `Device(config-pmap-c)# inspect`	Enables packet inspection.
Step 6	**exit** **Example:** `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* **Example:** `Device(config)# zone-pair security z1z2 source z1 destination z2`	Creates a zone pair and enters security zone configuration mode. **Note** To apply a policy, you must configure a zone pair.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone)# service-policy type inspect z1z2-policy2`	Attaches a firewall policy map to the destination zone pair. **Note** If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 9	**end** **Example:** `Device(config-sec-zone)# end`	Exits security zone configuration mode and enters global configuration mode.
Step 10	**interface** *type number* **Example:** `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* **Example:** `Device(config-if)# zone-member security Inside`	Assigns an interface to a specified security zone. **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** **Example:** `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** **Example:** `Device(config-if-cts-manual)# no propagate sgt`	Disables SGT propagation at Layer 2 on CTS interfaces.
Step 14	**policy static sgt** *tag* [**trusted**] **Example:** `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** **Example:** `Device(config-if)# exit`	Exits security zone configuration mode and enters privileged EXEC mode.
Step 16	**show policy-map type inspect zone-pair session** **Example:** `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. **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(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# object-group security myobject2
Device(config-object-group)# security-group tag-id 2
Device(config-object-group)# exit
Device(config)# object-group security myobject3
Device(config-object-group)# security-group tag-id 3
Device(config-object-group)# exit
Device(config)# object-group security myobject4
Device(config-object-group)# security-group tag-id 4
Device(config-object-group)# exit

Device(config)# class-map type inspect match-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass2
Device(config-cmap)# match group-object security source myobject2
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass3
Device(config-cmap)# match group-object security source myobject3
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass4
Device(config-cmap)# match group-object security source myobject4
Device(config-cmap)# exit

Device(config)# policy-map type inspect InsideOutside
Device(config-pmap)# class type inspect myclass1
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass2
Device(config-pmap-c)# drop log
Device(config-pmap-c)# exit

Device(config)# policy-map type inspect OutsideInside
Device(config-pmap)# class type inspect myclass3
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass4
```

```
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit

Device(config)# zone-pair security Inside
Device(config-sec-zone)# description Firewall Inside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security Outside
Device(config-sec-zone)# description Firewall Outside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security InsideOutside source Inside destination Outside
Device(config-sec-zone)# description Firewall ZonePair Inside Outside
Device(config-sec-zone)# service-policy type inspect InsideOutside
Device(config-sec-zone)# exit

Device(config)# zone-pair security OutsideInside source Outside destination Inside
Device(config-sec-zone)# description Firewall ZonePair Outside Inside
Device(config-sec-zone)# service-policy type inspect OutsideInside
Device(config-sec-zone)# exit

Device(config)# interface Gigabit 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: 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

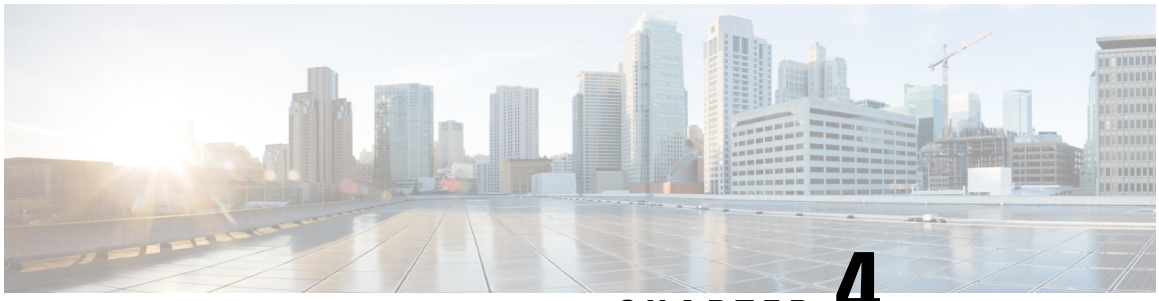
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

Feature Name	Releases	Feature Information
TrustSec SG Firewall Enforcement IPv4		This feature helps CTS-SXP extend the deployment of network devices through Security Group Access (SGA) Zone-Based Policy firewalls (ZBPFs). The following commands were introduced or modified: **group-object**, **match group-object security**, **object-group security**, **policy static sgt**, and **security-group**.



CHAPTER 4

TrustSec SGT Handling: L2 SGT Imposition and Forwarding

First Published: July 25, 2011

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 TrustSec SGT Handling: L2 SGT Imposition and Forwarding feature allows the interfaces in a router to be manually enabled for CTS so that the router can insert the Security Group Tag (SGT) in the packet to be carried throughout the network in the CTS header.

- Finding Feature Information, on page 29
- Prerequisites for TrustSec SGT Handling: L2 SGT Imposition and Forwarding , on page 29
- Information about TrustSec SGT Handling: L2 SGT Imposition and Forwarding, on page 30
- How to Configure TrustSec SGT Handling: L2 SGT Imposition and Forwarding, on page 30
- Additional References for TrustSec SGT Handling: L2 SGT Imposition and Forwarding, on page 34
- Feature Information for TrustSec SGT Handling: L2 SGT Imposition and Forwarding, on page 35

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 TrustSec SGT Handling: L2 SGT Imposition and Forwarding

The CTS network needs to be established with the following prerequisites before implementing the TrustSec SGT Handling: L2 SGT Imposition and Forwarding feature:

- Connectivity exists between all network devices
- Cisco Secure Access Control System (ACS) 5.1 operates with a CTS-SXP license
- Directory, DHCP, DNS, certificate authority, and NTP servers function within the network
- Configure the **retry open timer** command to a different value on different routers.

Information about TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Security Groups and SGTs

A security group is a grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the ACS. As new users and devices are added to the Cisco TrustSec (CTS) domain, the authentication server assigns these new entities to appropriate security groups. CTS assigns to each security group a unique 16-bit security group number whose scope is global within a CTS domain. The number of security groups in the router is limited to the number of authenticated network entities. Security group numbers do not need to be manually configured.

Once a device is authenticated, CTS tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT throughout the network within the CTS header. The SGT is a single label that determines the privileges of the source within the entire CTS domain. The SGT is identified as the source because it contains the security group of the source. The destination device is assigned a destination group tag (DGT).

Note The CTS packet tag does not contain the security group number of the destination device.

How to Configure TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Manually Enabling TrustSec SGT Handling: L2 SGT Imposition and Forwarding on an Interface

Perform the following steps to manually enable an interface on the device for Cisco TrustSec (CTS) so that the device can add Security Group Tag (SGT) in the packet to be propagated throughout the network and to implement a static authorization policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** {**GigabitEthernet** *port* | **Vlan** *number*}
4. **cts manual**
5. **policy static sgt** *tag* [trusted]
6. **end**
7. **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

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	**interface** {**GigabitEthernet** *port*	**Vlan** *number*} **Example:** `Device(config)# interface gigabitethernet 0`	Enters the interface on which CTS SGT authorization and forwarding is enabled
Step 4	**cts manual** **Example:** `Device(config-if)# cts manual`	Enables the interface for CTS SGT authorization and forwarding, and enters CTS manual interface configuration mode. **Note** To enable the **cts manual** command on a subinterface, you must increase the IP MTU size to accommodate the additional bytes for the Dot1Q tag. This is applicable only for releases earlier than Cisco IOS XE Release 3.17.
Step 5	**policy static sgt** *tag* [trusted] **Example:** `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 6	**end** **Example:** `Device(config-if-cts-manual)# end`	Exits CTS manual interface configuration mode and enters privileged EXEC mode.
Step 7	**show cts interface** [**GigabitEthernet** *port*	**Vlan** *number*	**brief**	**summary**] **Example:** `Device# show cts interface brief`	Displays CTS configuration statistics for the interface.

Example:

The following is sample output for the **show cts interface brief**command.

Cisco ASR 1000 Series Aggregation Services Routers and Cisco Cloud Services Router 1000V Series

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

Cisco 4400 Series Integrated Services Routers

```
Device# show cts interface brief

Interface GigabitEthernet0/1/0
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             100
        Peer SGT assignment:  Trusted
```

Disabling CTS SGT Propagation on an Interface

Follow these steps to disable CTS SGT Propagation on an interface in an instance when a peer device is not capable of receiving an SGT.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**GigabitEthernet***port* | **Vlan** *number*}
4. **cts manual**
5. **no propagate sgt**
6. **end**
7. **show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**GigabitEthernet***port* | **Vlan** *number*} **Example:** `Device(config)# interface gigabitethernet 0`	Enters the interface on which CTS SGT authorization and forwarding is enabled
Step 4	**cts manual** **Example:** `Device(config-if)# cts manual`	Enables the interface for CTS SGT authorization and forwarding. CTS manual interface configuration mode is entered where CTS parameters can be configured.
Step 5	**no propagate sgt** **Example:** `Device(config-if-cts-manual)# no propagate sgt`	Disables CTS SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT. **Note** CTS SGT propagation is enabled by default. The **propagate sgt** command can be used if CTS SGT propagation needs to be turned on again for a peer device. Once the **no propagate sgt** command is entered, the SGT tag is not added in the L2 header.
Step 6	**end** **Example:** `Device(config-if-cts-manual)# end`	Exits CTS manual interface configuration mode and enters privileged EXEC mode.

Step 7	**show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]
	Example:
	`Device# show cts interface brief`
	`Global Dot1x feature is Disabled`
	`Interface GigabitEthernet0:`
	`CTS is enabled, mode: MANUAL`
	`IFC state: OPEN`
	`Authentication Status: NOT APPLICABLE`
	`Peer identity: "unknown"`
	`Peer's advertised capabilities: ""`
	`Authorization Status: NOT APPLICABLE`
	`SAP Status: NOT APPLICABLE`
	`Propagate SGT: Disabled`
	`Cache Info:`
	`Cache applied to link : NONE`
		Displays CTS configuration statistics to verify that CTS SGT propagation was disabled on interface.

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: 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

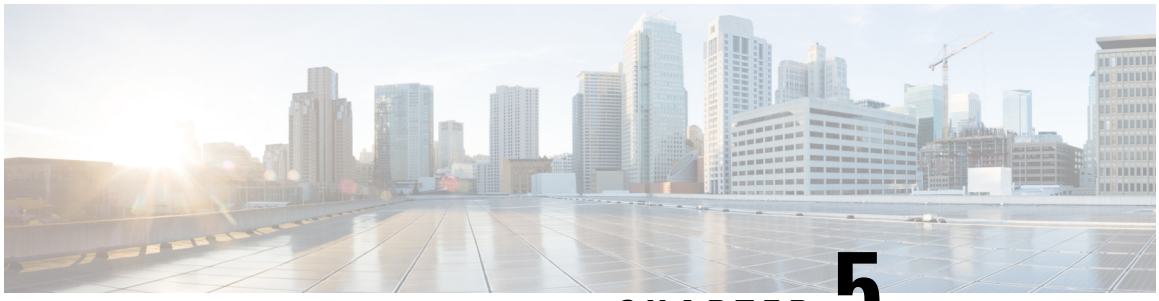
Feature Information for TrustSec SGT Handling: L2 SGT Imposition and Forwarding

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 TrustSec SGT Handling: L2 SGT Imposition and Forwarding

Feature Name	Releases	Feature Information
TrustSec SGT Handling: L2 SGT Imposition and Forwarding		This feature allows the interfaces in a router to be manually enabled for CTS so that the router can insert the Security Group Tag (SGT) in the packet to be carried throughout the network in the CTS header. The following commands were introduced or modified: **cts manual**, **policy static sgt**, **propagate sgt**, **show cts interface**.



CHAPTER 5

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 Scalable 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. SXPv4 is an alternative SGT transport mechanism to inline tagging. It enables the propagation of security group bindings between network devices that do not support carrying the SGT in the CMD field of Ethernet frames (inline tagging).

- Finding Feature Information, on page 37
- Information About Cisco TrustSec with SXPv4, on page 37
- How to Configure Cisco TrustSec with SXPv4, on page 41
- Configuration Examples for Cisco TrustSec with SXPv4, on page 45
- Additional References for Cisco TrustSec with SXPv4, on page 46
- Feature Information for Cisco TrustSec with SXPv4, on page 47

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

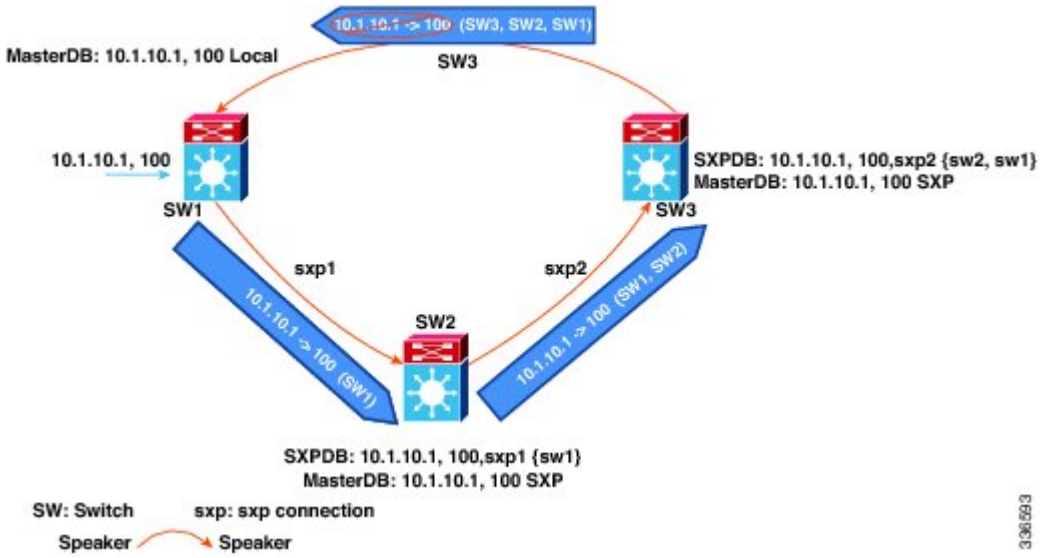
Overview of Cisco TrustSec with SXPv4

Cisco TrustSec (CTS) Scalable Group Tag (SGT) Exchange Protocol (SXP) (CTS-SXP) is a control plane protocol which propagates IP address to Security Group Tag (SGT) binding information across network devices. SGT is maintained by tagging packets (inline tagging) 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 versions prior to version 4 required careful attention to SXP traffic flow. For example, in Figure 1, SXP traffic flows in one direction (access layer to data center) and from the data center to the distribution layer. This unidirectional traffic pattern is done on purpose because if SXP traffic were to flow in the opposite direction, an SXP loop could be created. SXP version 4 prevents a loop from occurring.

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:

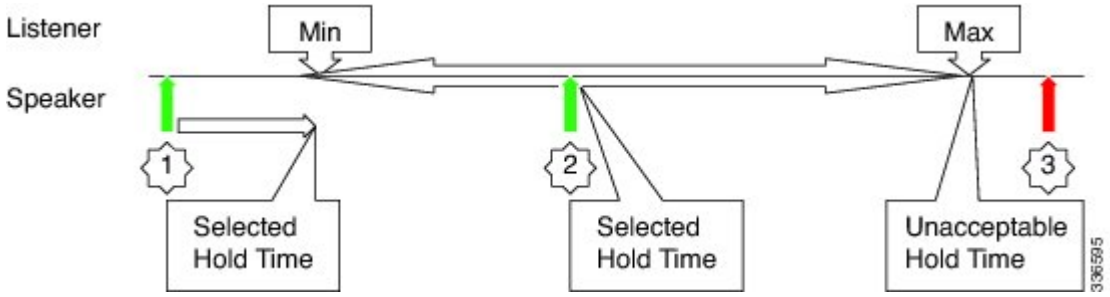
- **Hold timer**: Used by an SXP listener to detect when a connection is no longer live, that is, no KEEPALIVE or UPDATE message is received.
- **Keepalive timer**: Used by an SXP speaker to trigger the dispatch of keepalive messages during intervals when no other information is exported via update messages.

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.

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** **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 listener hold-time** *minimum-period maximum-period* **Example:** `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. **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* **Example:** `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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
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*]] **Example:** `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker`	Configures the CTS-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 CTS-SXP uses for the connection using the following options: • **default**—Use the default CTS-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. The **hold-time** keyword allows you to specify the length of the hold-time period for the speaker or listener device. **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. The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 5	**show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*] **Example:** `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** **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 node-id** {*sxp-node-id* | **interface** *interface-type* | *ipv4-address*} **Example:** `Device(config)# cts sxp node-id 172.16.1.3`	Configures the node ID of a network device.

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
```

Displaying the Platform Specific CTS Information

CTS does not maintain separate send and receive counters for IPv4 and IPv6 traffic. Hence, the below show command displays the combined statistics for IPv4 and IPv6.

```
Device# show platform hardware qfp active feature cts datapath stats

Tagged Packets rcv: 1055       xmt: 1048       Def tag: 0
         Unknown SGT: 109677    Unknown DGT: 0
 Invalid tags (drop): 34        Bad format (drop): 0
 No xmt buffer: 0
 IPSec SGT tagged packets received: 0
 IPSec Invalid SGT tagged packets received: 0
 GRE SGT tagged packets received: 0
 GRE Invalid SGT tagged packets received: 0
 GRE invalid next protocol 0
 LISP SGT tagged packets received: 0
 LISP Invalid SGT tagged packets received: 0
 VXLAN SGT tagged packets received: 0
 VXLAN Invalid SGT tagged packets: 0
```

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* • *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*

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: 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. 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

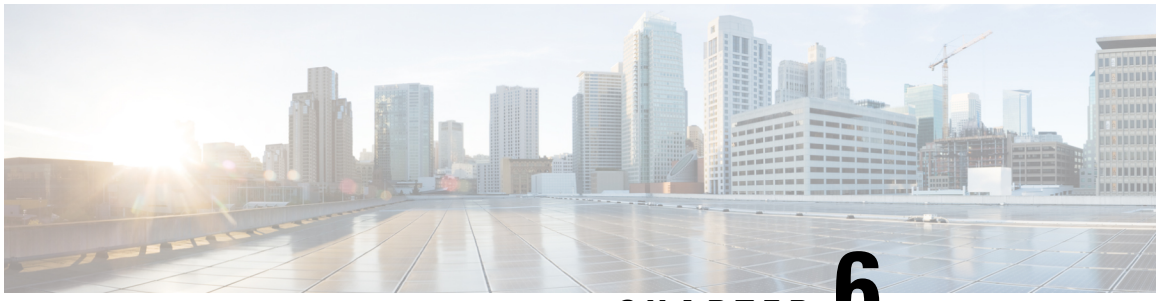
Feature Information for Cisco TrustSec with SXPv4

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 4: Feature Information for Cisco TrustSec with SXPv4

Feature Name	Releases	Feature Information
Cisco TrustSec with SXPv4	Cisco IOS XE Release 3.9S	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. In Cisco IOS XE Release 3.9S, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced: **cts sxp listener hold-time**, **cts sxp node-id**, **cts sxp speaker hold-time**.



CHAPTER 6

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, on page 49
- Prerequisites for Bidirectional SXP Support, on page 49
- Restrictions for Bidirectional SXP Support, on page 50
- Information About Bidirectional SXP Support, on page 50
- How to Enable Bidirectional SXP Support, on page 51
- Configuration Examples for Bidirectional SXP Support, on page 54
- Additional References for Bidirectional SXP Support, on page 55
- Feature Information for Bidirectional SXP Support, on page 55

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).

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 5: 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.
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.

	Command or Action	Purpose
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.
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 5: 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

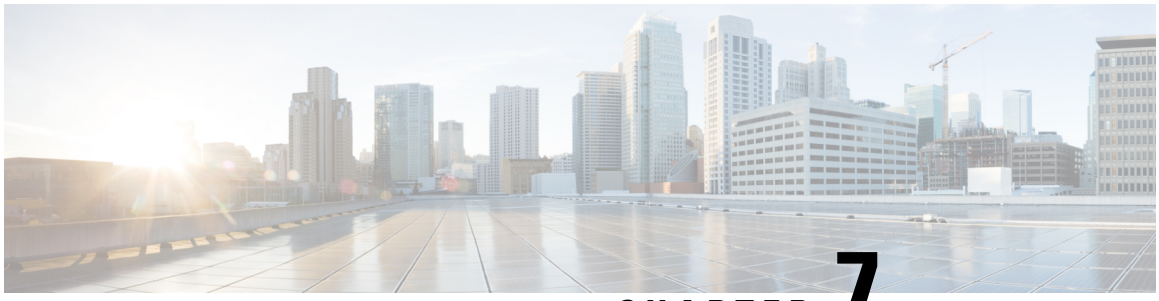
Feature Information for Bidirectional SXP Support

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 6: Feature Information for Bidirectional SXP Support

Feature Name	Releases	Feature Information
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. The following command was introduced or modified: **cts sxp connection peer**.



CHAPTER 7

SXP IP-Prefix and SGT based Filtering

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-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn user identity information from access devices.

The SXP IP-Prefix and SGT based Filtering feature allows IP-SGT bindings to be filtered when they are exported or imported. The filtering can be done based on IP prefix, SGT or a combination of both.

- Restrictions for SXP IP-Prefix and SGT-based Filtering, on page 57
- Information about SXP IP-Prefix and SGT based Filtering, on page 58
- Feature Information for SXP IP-Prefix and SGT Based Filtering, on page 58
- Types of SXP Filtering, on page 59
- How to Configure an SXP Filter, on page 59
- Show Commands, on page 62
- Troubleshooting, on page 63
- Syslog Messages for SXP Filtering, on page 64

Restrictions for SXP IP-Prefix and SGT-based Filtering

- High Availability (HA) is not supported for stateful synchronization of IP-SGT bindings in SXP database between active and standby devices. This is as per the existing behavior on routers and some switches.
- The applied filters to an existing connection takes effect only on the subsequent bindings that are exported/imported. Any bindings that have been imported/exported prior to applying the filters remains untouched.
- There is no VRF-specific filtering, and a filter specified for a peer IP is applicable across all VRFs on the device
- The SGT values taken in the filter rules will be a list of single SGT numbers. SGT ranges are not currently supported.

Information about SXP IP-Prefix and SGT based Filtering

Filtering IP-SGT bindings allows systems to selectively import or export only bindings of interest. In an SXP connection, a filter can be configured on a device that acts either as a speaker or a listener based on the filtering that happens during the export or import of bindings

In case of bi-directional SXP connections, the filters are applied in either of the directions based on whether a speaker or listener filter is configured. If a peer is a part of both the speaker and the listener filter groups, then filtering is applied in both directions.

The filters can be applied either on a peer-to-peer basis or globally (applicable to all SXP connections). In both the cases, the filter can be applied on the speaker or the listener.

How does SXP IP-Prefix and SGT based Filtering Work

A filter that needs to be applied on a device is created with a set of filter rules. Each filter rule specifies the action or actions to be taken for bindings with specific SGT values and/or IP-prefix values. Each binding is matched against the values specified in the filter rules; if a match is found, the corresponding action specified in the filter rule is taken. An action that can be executed on a selected binding is either a permit or a deny .

When a filter is enabled on the speaker or listener during the export or import of IP-SGT bindings, IP-SGT bindings are filtered based on the filter rules. If a rule is not specified for a binding in a filter list, the catch-all rule that is configured in the filter-list is executed. In the absence of a catch-all rule, the corresponding binding is implicitly denied.

Feature Information for SXP IP-Prefix and SGT Based Filtering

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.

Feature Information for SXP IP-Prefix and SGT Based Filtering

Feature Name	Releases	Feature Information
SXP IP-Prefix and SGT Based Filtering	Cisco IOS XE Everest 16.6.1	The SXP IP-Prefix and SGT based Filtering feature allows IP-SGT bindings to be filtered when they are exported or imported. The filtering can be done based on IP prefix, SGT or a combination of both. The following commands were introduced: **cts sxp filter-enable**, **cts sxp filter-group**, **cts sxp filter-list**, **debug cts sxp filter events**, **show cts sxp filter-group**, **show cts sxp filter-list**.

Types of SXP Filtering

IP-SGT bindings are filtered in one of the following ways:

- SGT-based filtering: Filter IP-SGT bindings in an SXP connection based on the SGT value.
- IP-prefix based filtering: Filter IP-SGT bindings in an SXP connection based on the IP-prefix value.
- SGT and IP-prefix based filtering: Filter IP-SGT bindings in an SXP connection based on the SGT value and IP-prefix value.

A filter rule is applied on each of the IP-SGT binding.

How to Configure an SXP Filter

1. **Configure an SXP filter list with filter rules:** In this step, a filter list is created to hold a set of rules. These rules filter the IP-SGT bindings by allowing bindings that are permitted and blocking bindings that are denied. Each rule can be based on SGT, IP prefix or a combination of both.

   If a filter list does not have a rule that matches a specific IP-SGT binding, the binding is implicitly denied unless a default or catch-all ruled is defined.

2. **Configure an SXP filter group:** In this step, a set of peers are grouped and a filter list is applied to the group. A filter-group can be either be defined as a speaker group or listener group. To apply the same filter list to all the speakers or all the listeners, you can create a global speaker filter group or a global listener filter group.

Note Only one filter list can be attached to a filter group.

3. **Enable SXP filtering:** The configured SXP filter list and filter group takes effect only after you enable filtering. Hence, you can configure all the required filters before executing them. You can also temporarily disable filters.

Configuring an SXP Filter List

The **cts sxp filter-list** command is used to create an SXP filter list.

cts sxp filter-list *filter_name*

When you issue this command, the filter lists is created and the device is placed in the filter list configuration mode. In this mode, you can define the filter rules.

A filter rule can be based on SGT or IP Prefix or a combination of both SGT and IP prefix. The command format to add rules to the filter list is a follows:

sequence-number **action(permit/deny) filter-type(ipv4/ipv6/sgt)** *value/values*

Given below is an example for creating a filter list and adding a filter rule:

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# 10 deny ipv4 1.1.1.0/24 permit sgt 100
```

Note that the sequence number is optional. If a sequence number is not mentioned, it is generated by the system. Sequence numbers are automatically incremented by a value of 10 from the last used/configured sequence number. A new rule can be inserted by specifying a sequence number in between two existing rules.

The range of valid SGT values is between 2 and 65519. To provide multiple SGT values in a rule, seperate the values using a space. A maximum of 8 SGT values are allowed in a rule.

In a SGT and IP prefix combination rule, if there is a match for the binding in both the parts of the rule, then the action specified in the second part of the rule takes precedence. For example, in the following rule, if the SGT value of the IP prefix 10.0.0.1 is 20, the corresponding binding will be denied even if the first part of the rule permits the binding.

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

Similarly, in the rule below the binding with the sgt value 20 will be permitted even if the sgt of the IP prefix 10.0.0.1 is 20, and the first action does not permit the binding.

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

Configuring an SXP Filter Group

The **cts sxp filter-group** command is used to create a filter group for grouping a set of devices and applying a filter list to them.

cts sxp filter-group {**listener** | **speaker**} [**global**] {*filter-group-name*]

When you issue this command, the filter group is created and the device is placed in a filter group configuration mode.

From this mode, you can do the following:

- Specify the peers to be grouped.
- Apply a filter list to the filter group.

The command format to add devices or peers to the group is a follows:

peer ipv4 *peer-IP*

In a single command, you can add a maximum a set of eight peers. To add more peers, repeat the command as many times as required.

The command format to apply a filter list to the group is as follows:

filter *filter-list-name*

The following example shows how to create a listener group called group_1 and assign peers to this group:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

The following example shows how to create a global listener group called group_2:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

There won't be a peer list option for the global listener and global speaker filter-group options because in this case the filter is applied for all SXP connections across the box that are either in the listener or speaker mode.

When both the global filter group and peer-based filter groups are applied, the global filter takes priority. If only a global listener or global speaker filter group is configured, then the global filtering takes precendence only in that specific direction. For the other direction, the peer-based filter group is implemented.

Enabling SXP Filtering

The configured SXP filter list and filter groups will take effect only after enabling filtering. The **cts sxp filter-enable** command is used to enable filtering.

cts sxp filter-enable

```
Device(config)# cts sxp filter-enable
```

Configuring the Default or Catch-All Rule

The default or catch-all rule is applied on IP-SGT bindings for which there was no match with any of the rules in the filter list. If a default rule is not specified, these IP-SGT bindings are denied.

Define the default or catch-all rule in the filter-list configuration mode of the corresponding filter list.

The following example shows how to create a default prefix rule that permits bindings corresponding to all IPv4 and IPv6 addresses:

```
Device(config)#cts sxp filter-list filter_1
```

```
Device(config-filter-list)# permit ipv4 0.0.0.0/0
Device(config-filter-list)# deny ipv6 00::/0
```

The following example shows how to create a default SGT rule that permits bindings corresponding to all SGTs :

```
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# permit sgt all
```

Show Commands

show cts sxp filter-list

The **show cts sxp filter-list** command displays the filter lists configured on the box along with the filter rules in each of the filter list. When this command is executed with a filter-list name, only the rules specific to that filter list is displayed.

cts sxp filter-list *filter-list-name*

The following example shows how to display the rules in a filter list:

```
Device# show cts sxp filter-list filter_1
   Filter-name: filter_1
   10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
```

Note The number within round barackets against each rule is the count of the number of times that rule has matched.

The following example shows how to display all the filter lists and their corresponding rules:

```
Device# show cts sxp filter-list
   Filter-name: filter_1 (0)
        10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Filter-name: filter_2 (0)
        10 permit sgt all (0)
        20 deny ipv4 5.5.5.0/24 (0)
        30 deny ipv6 ::/0 (0)
        40 permit ipv6 66:99::88/128 (0)
        50 permit sgt 100 200 300 (0)
        60 deny sgt 99 (0)
        90 permit ipv4 8.8.8.8/32 deny sgt 89 (0)
        100 deny ipv6 1::1/128 permit sgt 90 70 (0)
```

show cts sxp filter-group

The **sxp filter-group** command is used to display information about the configured filter groups along with their corresponding filter list name and peer list.

show cts sxp filter-group [**listener** | **speaker** | {**listener** | **speaker**} *filter-group-name*]
show cts sxp filter-group [**global**] [**detailed**]

The following example shows how to display the details of a specific speaker filter group:

```
Device# show cts sxp filter-group speaker group_1
   Filter-group: group_1
    Filter-name: filter_1
    peer 1.1.1.1
    peer 1.1.1.2
```

Note The number within round barackets against each rule is the count of the number of times that rule has matched.

The following example shows how to display the complete details of all the listener filter groups:

```
Device# show cts sxp filter-group listener detailed
    Global Listener Filter Name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0

    Global Speaker Filter Name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0

    Listener Groups:

    Filter-group: group_1
    Filter-name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0
    peer 1.1.1.1

    Speaker Groups:

    Filter-group: group_3
    peer 1.1.1.1
```

The following example shows how to display the brief details of the global filter group:

```
Device# show cts sxp filter-group global
   Global Listener Filter Name: filter_1
   Global Speaker Filter Name: filter_2
```

Troubleshooting

debug cts sxp filter events

The **debug cts sxp filter events** command is used to log events related to the creation, deletion, update of filter-lists and filter-groups. This command is also used to capture events related to the matching actions in a filtering process.

Syslog Messages for SXP Filtering

Syslog messages for SXP filtering are generated to indicate the various events related to filtering.

Syslog Messages for Filter Rules

The maximum number of rules that can be configured in a single filter is 128. The following message is generated everytime the number of filter rules that is configured in a single filter increases by 20% of this limit:

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in filter
 [filter-name].
```

The following message is generated when the number of rules configured in a single filter reaches 95% of the maximum number of rules allowed for a filter list:

```
CTS SXP filter rules exceed [ ] threshold. Reached count of [count] out of [max] in filter
 [filter-name].
```

The following message is generated when the number of rules configured in a single filter reaches the maximum number of allowed rules, and no more rules can be added.

```
Reached maximum filter rules. Could not add new rule in filter [filter-name]
```

Syslog Messages for Filter Lists

The maximum number of filter lists that can be configured is 256. The following message is generated everytime the number of filter lists that is configured increases by 20% of this limit:

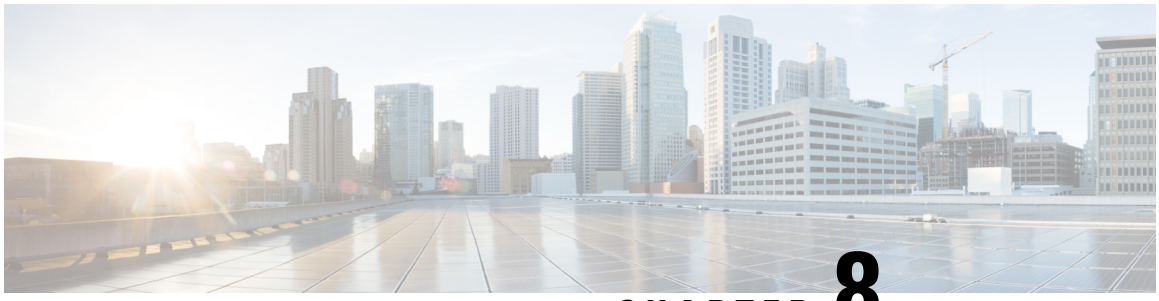
```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in filter
 [filter-name].
```

The following message is generated when the number of filter lists that is configured reaches 95% of the maximum number of allowed filter lists:

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max]
```

The following message is generated when the number of filter lists that is configured reaches the maximum number of allowed filter lists, and no more filter lists can be added:

```
Reached maximum filter count. Could not add new filter
```



CHAPTER 8

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, on page 65
- Information About Cisco TrustSec Interface-to-SGT Mapping, on page 65
- How to Configure Cisco TrustSec Interface-to-SGT Mapping, on page 66
- Configuration Examples for Cisco TrustSec Interface-to-SGT Mapping, on page 68
- Additional References for Cisco TrustSec Interface-to-SGT Mapping, on page 68
- Feature Information for Cisco TrustSec Interface-to-SGT Mapping, on page 69

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
- 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. 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** **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	**interface** *type slot/port* **Example:** `Device(config)# interface gigabitEthernet 0/0`	Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**cts role-based sgt-map sgt** *sgt-number* **Example:** `Device(config-if)# cts role-based sgt-map sgt 77`	An SGT is imposed on ingress traffic to the specified interface. • *sgt-number*—Specifies the security group tag (SGT) number. Valid values are from 2 to 65519.
Step 5	**end** **Example:** `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
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 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. 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/cisco/web/support/index.html

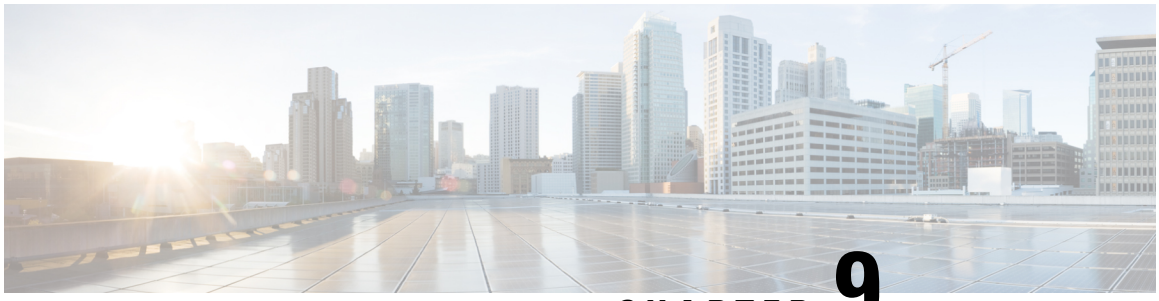
Feature Information for Cisco TrustSec Interface-to-SGT Mapping

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		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. The following command was introduced or modified: **cts role-based sgt-map sgt**.



CHAPTER 9

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, on page 71
- Restrictions for Cisco TrustSec Subnet to SGT Mapping, on page 71
- Information About Cisco TrustSec Subnet to SGT Mapping, on page 72
- How to Configure Cisco TrustSec Subnet to SGT Mapping, on page 72
- Cisco TrustSec Subnet to SGT Mapping: Examples, on page 74
- Additional References, on page 75
- Feature Information for Cisco TrustSec Subnet to SGT Mapping, on page 76

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** **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 mapping network-map** *bindings* **Example:** `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* **Example:** `Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	(IPv4) Specifies an IPv4 subnet in CIDR notation. 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. • *ipv4-address*—Specifies the IPv4 network address in dotted decimal notation. • *prefix*—(0 to 30). Specifies the number of bits in the network address. • **sgt** *number* (0-65,535). Specifies the SGT number.
Step 5	**cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number* **Example:** `Device(config)# cts role-based sgt-map 2020::/64 sgt 1234`	(IPv6) Specifies an IPv6 subnet in hexadecimal notation. 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. • *ipv6-address*—Specifies the IPv4 network address in dotted decimal notation. • *prefix*—(0 to 30). Specifies the number of bits in the network address. • **sgt** *number*—(0-65,535). Specifies the SGT number.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

	Command or Action	Purpose

Step 7	**show running-config** | **include** *search-string*
	Example:
	`Device# show running-config | include sgt 1234`
	`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** **Example:** `Device# show cts sxp connections`	Displays the SXP speaker and listener connections with their operational status.
Step 9	**show cts sxp sgt-map** **Example:** `Device# show cts sxp sgt-map`	Displays the IP to SGT bindings exported to the SXP listeners.
Step 10	**copy running-config startup-config** **Example:** `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 • 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 and SXP configuration	Cisco TrustSec Switch Configuration Guide
IPsec configuration	Configuring Security for VPNs with IPsec

Related Topic	Document Title
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

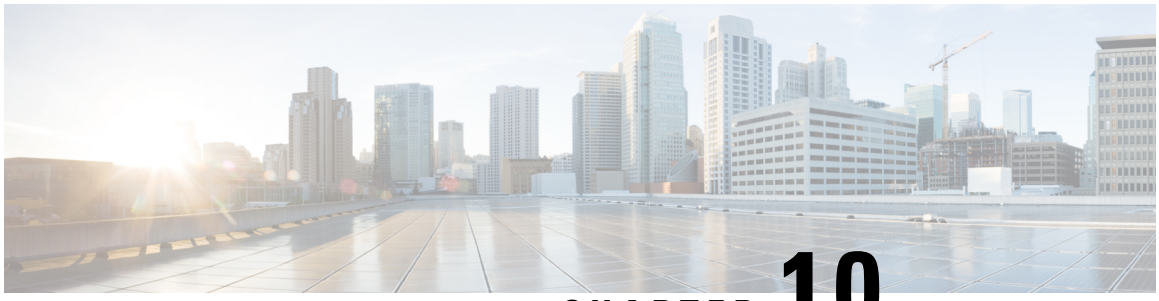
Feature Information for Cisco TrustSec Subnet to SGT Mapping

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		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. The following command was introduced: **cts sxp mapping network-map**.



CHAPTER 10

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, on page 77
- Restrictions for Flexible NetFlow Export of Cisco TrustSec Fields, on page 77
- Information About Flexible NetFlow Export of Cisco TrustSec Fields, on page 78
- How to Configure Flexible NetFlow Export of Cisco TrustSec Fields, on page 79
- Configuration Examples for Flexible NetFlow Export of Cisco TrustSec Fields, on page 89
- Additional References for Flexible NetFlow Export of Cisco TrustSec Fields, on page 90
- Feature Information for Flexible NetFlow Export of Cisco TrustSec Fields, on page 91

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.

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.

FNF can collect SGT tags of both IPv4 and IPv6 packets.

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** **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	**flow record** *record-name* **Example:** `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** **Example:** `Device(config-flow-record)# match ipv4 protocol`	(Optional) Configures the IPv4 protocol or IPv6 protocol as a key field for a flow record.

	Command or Action	Purpose
Step 5	**match {ipv4 | ipv6} source address** **Example:** `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** **Example:** `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** **Example:** `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** **Example:** `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** **Example:** `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** **Example:** `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** **Example:** `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.
Step 12	**end** **Example:** `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** **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	**flow record** *record-name* **Example:** `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** **Example:** `Device(config-flow-record)# match ipv4 protocol`	(Optional) Configures the IPv4 protocol or IPv6 protocol as a key field for a flow record. **Note** For Cisco CSR100V, ISR 4400, and ASR 1000 platforms, Cisco TrustSec fields are supported only in IPv4 FNF records.
Step 5	**match** {**ipv4**	**ipv6**} **source address** **Example:** `Device(config-flow-record)# match ipv4 source address`	(Optional) Configures the IPv4 or IPv6 source address as a key field for a flow record. **Note** For Cisco CSR100V, ISR 4400, and ASR 1000 platforms, Cisco TrustSec fields are supported only in IPv4 FNF records.

	Command or Action	Purpose
Step 6	**match {ipv4 | ipv6} destination address** **Example:** `Device(config-flow-record)# match ipv4 destination address`	(Optional) Configures the IPv4 or IPv6 destination address as a key field for a flow record. **Note** For Cisco CSR100V, ISR 4400, and ASR 1000 platforms, Cisco TrustSec fields are supported only in IPv4 FNF records.
Step 7	**match transport source-port** **Example:** `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** **Example:** `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** **Example:** `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** **Example:** `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.
Step 11	**collect flow cts destination group-tag** **Example:** `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** **Example:** `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** **Example:** `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** **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	**flow exporter** *exporter-name* **Example:** `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*] **Example:** `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** **Example:** `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** **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	**flow monitor** *monitor-name* **Example:** `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* **Example:** `Device(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 5	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	Specifies the exporter for the flow monitor.
Step 6	**end** **Example:** `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** **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	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip**	**ipv6**} **flow monitor** *monitor-name* {**input**	**output**} **Example:** `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** **Example:** `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 • 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
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. 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/cisco/web/support/index.html

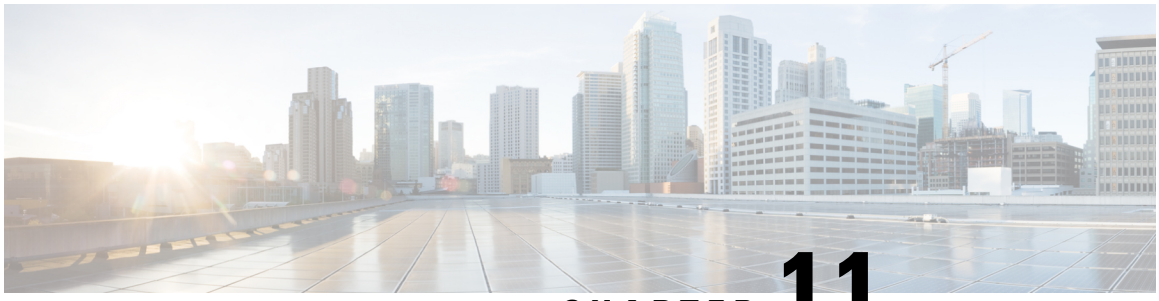
Feature Information for Flexible NetFlow Export of Cisco TrustSec Fields

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		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. The following commands were introduced by this feature: **match flow cts {source | destination} group-tag** and **collect flow cts {source | destination} group-tag**.



CHAPTER 11

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, on page 93
- Restrictions for Cisco TrustSec SGT Caching, on page 93
- Information About Cisco TrustSec SGT Caching, on page 94
- How to Configure Cisco TrustSec SGT Caching, on page 96
- Configuration Examples for Cisco TrustSec SGT Caching, on page 101
- Additional References for Cisco TrustSec SGT Caching, on page 102
- Feature Information for Cisco TrustSec SGT Caching, on page 103

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.
```

- SGT Caching for Tunneling of IPv6 packet over V4 transport & IPv4 packet over V6 transport is not supported.
- High availability and syncing of IPv6 SGACL policies on the routing platforms are not supported for IPv6-SGT caching.
- SGT caching is not supported for IPSec packets carrying SGT tags in ESP header on ISR4K based platforms.
- SGT caching is not performed for the link-local IPv6 source address.

  A link-local address is a network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to. Link-local addresses are not guaranteed to be unique beyond a single network segment. Therefore, routers do not forward packets with link-local addresses. Because they are not unique, SGT tags for the packets with source as link-local IPv6 address are not assigned.

Information About Cisco TrustSec SGT Caching

Identifying and Reapplying SGT Using SGT Caching

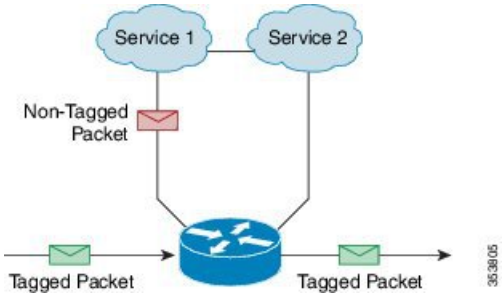
Cisco TrustSec uses Security Group Tag (SGT) caching to ensure that traffic tagged with SGT can also pass through services that are not aware of SGTs. Examples of services that cannot propagate SGTs are WAN acceleration or optimization, intrusion prevention systems (IPS), and upstream firewalls.

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.

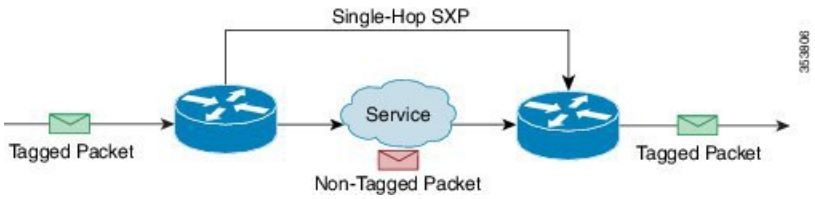
Figure 6: SGT Caching in One-Arm Mode



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 7: SGT Caching in Bump-in-the-wire Topology



SGT Caching for IPv6 Traffic

The following are the considerations for SGT caching for IPv6 traffic:

- **Global Unicast IPv6 Packet**: IPv6-SGT caching is performed for traffic coming in ingress and egress directions for IPv6 packets. The SGT tags come inline in the packet (ethernet header, IPSec header, GRE header). However, SGT caching for tag in IPSec packet is not supported on ISR4K based platforms.
- **Multicast IPv6 Address**: SGT caching is not supported for IPv6 multicast traffic and link local IPv6 addresses.

- **Export of Cached IPv6-SGT Binding Via SXP**: The IPv6-SGT binding learnt in the data-plane is notified to the RBM (RoleBased Manager) database in IOS. These bindings can then be exported to other trustsec devices using the SXP.

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** **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 role-based sgt-caching** **Example:** `Device(config)# cts role-based sgt-caching`	Enables SGT caching in ingress direction for all interfaces.
Step 4	**end** **Example:** `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** **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	**interface** *type slot/port* **Example:** `Device(config)# interface gigabitEthernet 0/1/0`	Configures an interface and enters interface configuration mode.
Step 4	**cts role-based sgt-cache** [**ingress**	**egress**] **Example:** `Device(config-if)# cts role-based sgt-cache ingress`	Configures SGT caching on a specific interface. • ingress—Enables SGT caching for traffic entering the specific interface (inbound traffic). • egress—Enables SGT caching for traffic exiting the specific interface (outbound traffic).
Step 5	**end** **Example:** `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**

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
```

Verifying IP-to-SGT Bindings

Displays the IP-to-SGT bindings learnt in the data-plane.

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.104.33.219           300     INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of INTERNAL bindings = 1
Total number of active   bindings = 1
```

```
Active IPv6-SGT Bindings Information

IP Address                                      SGT     Source
============================================================
100::/64                                        124     CLI
200::2                                          300     INTERNAL
300::1                                          300     INTERNAL
1000::2                                         300     INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of INTERNAL bindings = 3
Total number of active   bindings = 4
```

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 • 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*
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. 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/cisco/web/support/index.html

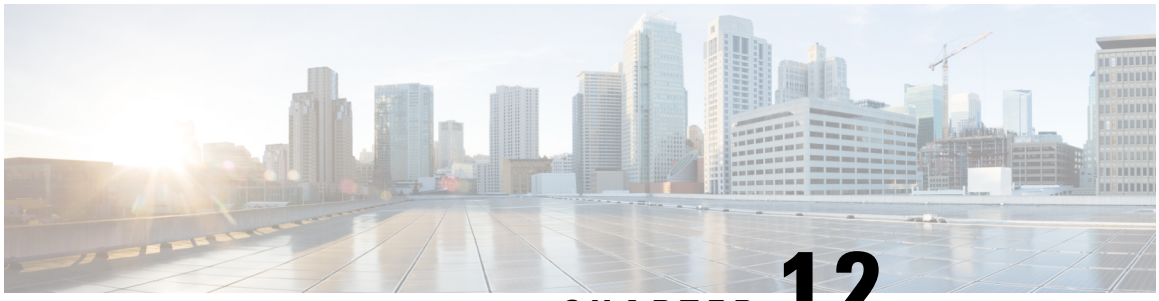
Feature Information for Cisco TrustSec SGT Caching

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		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. The following commands were introduced or modified: **cts role-based sgt-caching**, **cts role-based sgt-cache** [**ingress** | **egress**].
IPv6 enablement - SGT Caching	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.



CHAPTER 12

CTS SGACL Support

CTS SGACL support feature provides state-less access control mechanism based on the security association or security group tag value instead of IP addresses.

- Finding Feature Information, on page 105
- Prerequisites for CTS SGACL Support, on page 105
- Restrictions for CTS SGACL Support, on page 105
- Information About CTS SGACL Support, on page 106
- How to Configure CTS SGACL Support, on page 107
- Configuration Examples for CTS SGACL Support, on page 109
- Additional References for CTS SGACL Support, on page 112
- Feature Information for CTS SGACL Support, on page 112

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 CTS SGACL Support

For CTS SGACL support, ensure that Protected Access Credential (PAC) and environmental data download is configured on the device for dynamic SGACL.

Restrictions for CTS SGACL Support

- For the list of supported TrustSec features per platform and the minimum required IOS release, see the Cisco TrustSec Platform Support Matrix at the following URL: http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html
- SGACL enforcement is not supported on management interfaces.

- Dynamic SGACL download size is limited to 6 KB
- There is no validation of SGACL enforcement on Port-Channel interfaces.
- In a VRF aware SGT configuration, Cisco IOS XE Denali 16.3 supports ISE communication though non management VRF interface. ISE communication through management interface is not supported.
- Scale limit of 6 KB is only for dynamic SGACL. Static SGACL can support higher scale like 256*256 matrix.
- SGACL enforcement is by-passed for the IPv6 packets with link-local IPv6 source/destination address.
- The SGACL enforcement for IPv6 multicast traffic is by-passed.

Information About CTS SGACL Support

CTS SGACL Support

Security group access control lists (SGACLs) is a policy enforcement through which the administrator can control the operations performed by the user based on the security group assignments and destination resources. Policy enforcement within the Cisco Trustsec domain is represented by a permissions matrix, with source security group number on one axis and destination security group number on the other axis. Each cell in the matrix contains an ordered list of SGACLs which specifies the permissions that should be applied to packets originating from an IP belonging to a source security group and having a destination IP that belongs to the destination security group.

SGACL provides state-less access control mechanism based on the security association or security group tag value instead of IP addresses and filters the traffic based on match class. There are three ways to provision the SGACL policy:

- Static policy provisioning - The SGACL policies are defined by the user using the command **cts role-based permission**.
- Dynamic policy provisioning - Configuration of SGACL policies should be done primarily through the policy management function of the Cisco Secure ACS or the Cisco Identity Services Engine - Cisco Identity Services Engine User Guide
- Change of Authorization (CoA) - The updated policy is downloaded when the SGACL policy is modified on the ISE and CoA is pushed to the CTS device.

SGACL Monitor Mode

During the pre-deployment phase of Cisco TrustSec, an administrator will use the monitor mode to test the security policies without enforcing them to make sure that the policies function as intended. If the security policies do not function as intended, the monitor mode provides a convenient mechanism for identifying that and provides an opportunity to correct the policy before enabling SGACL enforcement. This enables administrators to have increased visibility to the outcome of the policy actions before they enforce it, and confirm that the subject policy meets the security requirements (access is denied to resources if users are not authorized).

The monitoring capability is provided at the SGT-DGT pair level. When you enable the SGACL monitoring mode feature, the deny action is implemented as an ACL permit on the line cards. This allows the SGACL counters and logging to display how connections are handled by the SGACL policy. Since all the monitored traffic is permitted, there is no disruption of service due to SGACLs while in the SGACL monitor mode.

How to Configure CTS SGACL Support

Enabling SGACL Policy Enforcement Globally

To enable SGACL policy enforcement on Cisco TrustSec-enabled routed interfaces, perform this task:

```
enable
configure terminal
cts role-based enforcement
```

Enabling SGACL Policy Enforcement Per Interface

You can enable SGACL enforcement globally and disable on a specific interface with **cts role-based enforcement** command. SGACL enforcement can also be enabled on specific interfaces without enabling it globally.

To enable SGACL policy enforcement on interfaces, perform this task:

```
enable
configure terminal
interface GigabitEthernet 0/1/1
cts role-based enforcement
```

Configuring IPv6 SGACL Access Control Entries

An SGACL is defined similar to the extended named ACL using the following command:

```
Device(config)#ipv6 access-list role-based sgacl1
IPV6 Role-based Access List Configuration commands:
  default   Set a command to its defaults
  deny      Specify packets to reject
  exit      Exit from access-list configuration mode
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  remark    Access list entry comment
  sequence  Sequence number for this entry
```

Attaching SGACLs to Permission Matrix Cell

```
Device(config)#cts role-based permissions from 100 to 200
  WORD  Role-based Access-list name
  ipv4  Protocol Version - IPv4
  ipv6  Protocol Version - IPv6
```

This command defines, replaces, or deletes the list of RBACLs for a given <SGT, DGT> pair. This policy comes into an effect when there is no dynamic policy for the same SGT, DGT. By default, you can attach only an IPv4 type RBACL. To add an IPv6 SGACL, specify **ipv6** explicitly.

Manually Configuring SGACL Policies

To manually configure SGACL policies, perform the following tasks:

```
enable
configure terminal
ip access-list role-based allow_webtraff
10 permit tcp dst eq 80
20 permit tcp dst eq 443
cts role-based permissions from 55 to 66 allow_webtraff
end
```

Refreshing the Downloaded SGACL Policies

To refresh the downloaded SGACL policies, perform the following task:

```
enable
cts refresh policy
```

Or

```
enable
cts refresh policy sgt 10
```

Configuring SGACL Monitor Mode

Before configuring SGACL monitor mode, ensure that Cisco TrustSec is enabled.

Note The device level monitor mode is not enabled by default unless any one of the configurations are applied. In case of SGACL's downloaded from ISE, the monitor mode state from ISE takes precedence always. This is applicable for both per-cell monitor mode or global monitor mode which is applicable for all cell.

```
configure terminal
cts role-based monitor enable
cts role-based monitor permissions from 2 to 3 ipv4
show cts role-based permissions from 2 to 3 ipv4
show cts role-based counters ipv4
```

Configuring IPv6 SGACL ACE

The following CLI is used to define Access Control Entries (ACEs) of an IPv6 SGACL.

```
Device(config)#ipv6 access-list role-based sgacl1
Device(config-ipv6rb-acl)#permit ipv6
Device(config-ipv6rb-acl)#exit
Device(config)#cts role-based permissions from 100 to 200 ipv6 sgacl1
```

Note IPv6 ACL configuration is for static SGACL whereas for dynamic SGACL, ACEs are configured on the ISE.

Configuration Examples for CTS SGACL Support

Example: CTS SGACL Support

The following is a sample output of the show cts role-based permissions command.

```
Router# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-02
        Permit IP-00
IPv4 Role-based permissions from group 55:SGT_55 to group 66:SGT_66 (configured):
        allow_webtraff
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE


Router#sh cts role-based permissions ipv6
IPv6 Role-based permissions from group 2103:Cisco_UC_Servers to group 2104:Exchange_Servers:

        SGACL_5-10-ipv6
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

The following is a sample output, applicable only to dynamic SGACL, of the show cts policy sgt command.

```
Router# show cts policy sgt

CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0xc1408801
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE
```

```
SGT: 65535-46:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = default_sgacl-02
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit icmp
    permit ip
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 2
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE
```

The following is a sample output, applicable only to dynamic SGACL, of the show cts rbacl command.

```
Router# show cts rbacl

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =multple_ace-16
  IP protocol version = IPV4
  refcnt = 4
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      deny tcp

  name   =default_sgacl-02
  IP protocol version = IPV4
  refcnt = 2
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      permit ip

  name   =SGACL_256_ACE-71
  IP protocol version = IPV4
```

Example: Configuring SGACL Monitor Mode

The following is a sample configuration example for SGACL Monitor Mode:

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

        IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

        IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
        Details:
        Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
        20 deny udp
        30 deny icmp
        Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip
Device# show cts role-based permissions ipv6
IPv6 Role-based permissions from group 201 to group 22 (configured):
        g6
IPv6 Role-based permissions from group 100 to group 200 (configured):
        sgacl1
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Device# show cts role-based counters ipv4
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
100     200     0          0          0          0          0          0
101     201     0          0          0          0          0          0

Device# show cts role-based counters ipv6
Role-based IPv6 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
201     22      0          0          0          0          0          0
100     200     0          0          0          0          0          0
```

Example: Refreshing the Downloaded SGACL Policies

The following is a sample configuration example for refreshing the downloaded SGACL policies. The command is run in a privileged EXEC mode.

```
Router#cts refresh policy
Router#cts refresh policy sgt
```

Additional References for CTS SGACL Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
CISCO-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: 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. 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/cisco/web/support/index.html

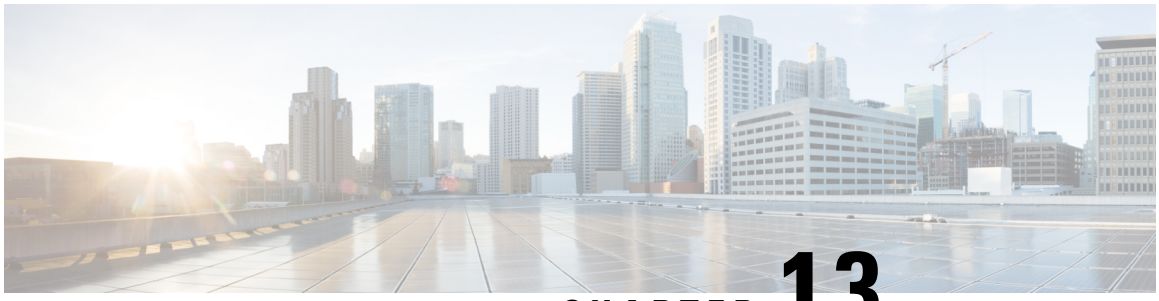
Feature Information for CTS SGACL Support

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 11: Feature Information for CTS SGACL Support

Feature Name	Releases	Feature Information
CTS SGACL Support	Cisco IOS Release 16.3	The CTS SGACL Support feature provides state-less access control mechanism based on the security association or security group tag value instead of IP addresses. In Cisco IOS Release 16.3, this feature was introduced for Cisco Aggregation Service Router 1000 series and Integrated Services Router 4000 series. The following commands were introduced by this feature: **cts role-based enforcement, ip access-list role-based, cts role-based permissions, show cts role-based permissions, show cts rbacl**.
TrustSec SGACL Monitor Mode	Cisco IOS XE Everest 16.4.1	TrustSec SGACL Monitor Mode feature monitors the security policies without enforcing that the policies function as intended. The monitor mode provides a convenient mechanism for identifying the security policies that do not function and provide an opportunity to correct the policy before enabling SGACL enforcement. The following commands were introduced by this feature: **cts role-based monitor enable, cts role-based monitor permissions**.
IPv6 enablement - SGACL Enforcement	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.



CHAPTER 13

Accessing TrustSec Operational Data Externally

Cisco TrustSec 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.

Cisco TrustSec also provides security using group-based access control - access policies within the Cisco TrustSec domain are topology-independent, and are based on the roles of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.

Cisco TrustSec produces two kinds of data - namely configuration data and operational data. Configuration data comes from the config programming model and the operational data comes from the operational data model.

It is possible to access TrustSec operational data from external applications that can handle data that is structured using YANG. Using the Netconf and Restconf protocol, the external device is able to extract operational information from Cisco devices - thereby providing programmability over an external interface.

- Prerequisites for Accessing Cisco TrustSec Operational Data Externally, on page 115
- Restrictions for Accessing Cisco TrustSec Operational Data Externally, on page 116
- Information About Cisco TrustSec Operational Data, on page 116
- How to Configure the External Device YTOOL, on page 120
- Accessing Operational Data, on page 121

Prerequisites for Accessing Cisco TrustSec Operational Data Externally

- An understanding of Cisco Trustsec, security tag propagation using SXP across network devices, and policy enforcement.
- Effective Cisco IOS XE Everest 16.5.1, Cisco TrustSec supports crypto k9 image with licenses for IP services or IP base only.
- The NETCONF or RESTCONF protocol should be enabled on the Cisco device. To enable the NETCONF protocol, use the command **netconf-yang** in the configuration mode.

Note The LANbase license supports only SXP; SGACL and IP-SGT operational data are not supported.

Restrictions for Accessing Cisco TrustSec Operational Data Externally

- Operation data limited to SGACL policy and IP-SGT & SXP connection can only be externally accessed.
- The below list of trustsec operational data is not supported in Cisco IOS XE Everest 16.5.1:
  - Cisco Trustsec PAC data, environment data and link-level operation data.
  - IPV6 based SGACL policy, IP-SGT mapping and SXP connection operational data.
  - VFR based IP-SGT mapping and SXP connection operational data.

Information About Cisco TrustSec Operational Data

Applications such as YTOOL provides users the flexibility to access Cisco TrustSec operational data from an external interface, without directly logging into Cisco devices to fetch the information using specific commands.

The following types of operational data can be accessed from an external device:

- The active SXP connections on a particular device.

  The following is a sample output to show SXP connections on a device:

```
Device# show cts sxp connections brief
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set

---------------------------------------------------------------------------------------------------
---------------
Peer_IP          Source_IP        Conn Status
 Duration
---------------------------------------------------------------------------------------------------
---------------
10.10.1.1        11.11.1.1        Off
 0:00:36:24 (dd:hr:mm:sec)
10.10.1.2        11.11.1.2        Off
 0:00:36:24 (dd:hr:mm:sec)
10.10.1.3        11.11.1.3        Off
 0:00:36:23 (dd:hr:mm:sec)
10.10.1.4        11.11.1.4        Off
 0:00:36:22 (dd:hr:mm:sec)
10.10.1.5        11.11.1.5        Off
 0:00:36:22 (dd:hr:mm:sec)
10.10.1.6        11.11.1.6        Off
 0:00:36:21 (dd:hr:mm:sec)
10.10.1.7        11.11.1.7        Off
 0:00:36:21 (dd:hr:mm:sec)
```

```
10.10.1.8        11.11.1.8        Off
 0:00:36:20 (dd:hr:mm:sec)
10.10.1.9        11.11.1.9        Off
 0:00:36:15 (dd:hr:mm:sec)
10.10.1.10       11.11.1.10       Off(Speaker)::Off(Listener)
 0:00:33:40 (dd:hr:mm:sec)::0:00:33:40 (
dd:hr:mm:sec)
```

- The IP-SGT mapping information.

  Every source IP is mapped with the corresponding SGT and an IP-SGT binding is created. This mapping information is stored in the Role-Based Manager (RBM) database.

  The following is a sample output to show IP-SGT mapping information:

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.10.10.10             10      CLI
20.20.20.20             20      CLI
30.30.30.30             30      CLI
32.1.1.32               40      CLI
45.1.1.45               100     CLI
69.1.1.1                103     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 6
Total number of active   bindings = 6

asr1k-cts-2006#
```

- Names of the policies that are currently applied for every data path.

  SGACL policies are enforced when SGT-tagged packets are transported between two trustsec-aware end points. A policy can either be static or dynamic. Policies that are configured on the device using the CLI command **cts role-based permissions** are static policies. Dynamic policies are configured on CISCO ISE (Identiy Services Engine). Dynamic policies take precedence over static policies. A static policy is enforced only in the absence of a dynamic policy.

  The following is a sample output to show policies for SGT-tagged traffic:

```
Device# show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 10:SGT_10:
        Collab1-10
IPv4 Role-based permissions from group 10:SGT_10 to group 20:SGT_20:
        SGACL_2-30
IPv4 Role-based permissions from group 11:SGT_11 to group 20:SGT_20:
        SGACL_2-30
        SGACL_3-10
        SGACL_4-90
IPv4 Role-based permissions from group 12:SGT_12 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 13:SGT_13 to group 20:SGT_20:
        SGACL_4-90
IPv4 Role-based permissions from group 14:SGT_14 to group 20:SGT_20:
        SGACL_5-20
IPv4 Role-based permissions from group 15:SGT_15 to group 20:SGT_20:
        SGACL_6-30
```

```
IPv4 Role-based permissions from group 16:SGT_16 to group 20:SGT_20:
        SGACL_101-90
IPv4 Role-based permissions from group 17:SGT_17 to group 20:SGT_20:
        SGACL_2-30
IPv4 Role-based permissions from group 18:SGT_18 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 19:SGT_19 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 10:SGT_10 to group 30:SGT_30:
        SGACL_6-30
IPv4 Role-based permissions from group 10:SGT_10 to group 40:SGT_40:
        SGACL_2-30
IPv4 Role-based permissions from group 10:SGT_10 to group 100:SGT_100:
        SGACL_4-90
IPv4 Role-based permissions from group 102:SGT_102 to group 100:SGT_100:
        Permit IP-00
IPv4 Role-based permissions from group 102:SGT_102 to group 103:SGT_103:
        SGACL_2-30
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

asr1k-cts-2006#
```

- The contents of each policy - which includes the ACEs (Access Control Entries) in the policy, and the lifetime and refresh time of the policy.

  A policy can have upto a combination of 256 ACEs. Lifetime and refresh time information is only applicable to dynamic policies. The lifetime and refresh time value for a static policy is 0.

  The following is a sample output to show policies for SGT-tagged traffic (only a part of the output is displayed):

```
Device# show cts policy sgt
CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0x41408001
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:42 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-52:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-52:ANY-0, Destination SGT: 65535-52:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 4
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
```

```
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 10-2770:SGT_10
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 10-2770:SGT_10-0, Destination SGT: 10-2770:SGT_10-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Collab1-10
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 20-44:SGT_20
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 10-2770:SGT_10-0, Destination SGT: 20-44:SGT_20-0
  rbacl_type = 80
  rbacl_index = 1
  name   = SGACL_2-30
  IP protocol version = IPV4
  refcnt = 8
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

  Source SGT: 12-17:SGT_12-0, Destination SGT: 20-44:SGT_20-0
  rbacl_type = 80
  rbacl_index = 2
  name   = SGACL_3-10
  IP protocol version = IPV4
  refcnt = 5
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

  Source SGT: 13-14:SGT_13-0, Destination SGT: 20-44:SGT_20-0
  rbacl_type = 80
  rbacl_index = 3
  name   = SGACL_4-90
  IP protocol version = IPV4
  refcnt = 5
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
```

```
  deny tcp

Source SGT: 14-14:SGT_14-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 4
name   = SGACL_5-20
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 15-1410:SGT_15-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 5
name   = SGACL_6-30
IP protocol version = IPV4
refcnt = 4
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit icmp log
  permit udp log
  permit tcp log

Source SGT: 16-14:SGT_16-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 6
name   = SGACL_101-90
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip
```

How to Configure the External Device YTOOL

Before you configure the YTOOL, ensure that the NETCONF or RESTCONF protocol is enabled on the Cisco device. One of these protocols is required for the YTOOL to communicate with the Cisco device.

Note To enable the NETCONF protocol, use the command **netconf-yang** in the configuration mode. After enabling NETCONF, execute the CLI **show onep session all** to check if the three processes that are needed to use Netconf are running. Netconf is usable only after these three processes are running.

Also, identify the IP address that you are going to use for communicating with the device.

Note YTOOL is also known as yang-explorer. You can download this application from the following location:

Yang Explorer at

To connect the YTOOL to a Cisco device, add the Cisco device in the YTOOL. Steps to add a Cisco device in the YTOOL:

1. Open YTOOL
2. Select **Admin**
3. On the **Ytool Utilities** page, select **Manage Profiles** (under **Manage Device Profiles**)
4. Choose **New Device** from the **Device Profile Name** dropdown
5. On the **Manage Device Profile** page, provide all the details of the device such as **Test Device IP Address, Test Device SSH Port Number, Netconf Username, NetConf Password** etc.

   Figure 8: Manage Device Profile

6. To check the connectivity to the device, navigate to **Build** > **Device Settings**. Select your device from **Profile** and click **Hello**. If you see a response under **Console**, it implies that the YTOOL is able to communicate with the device.

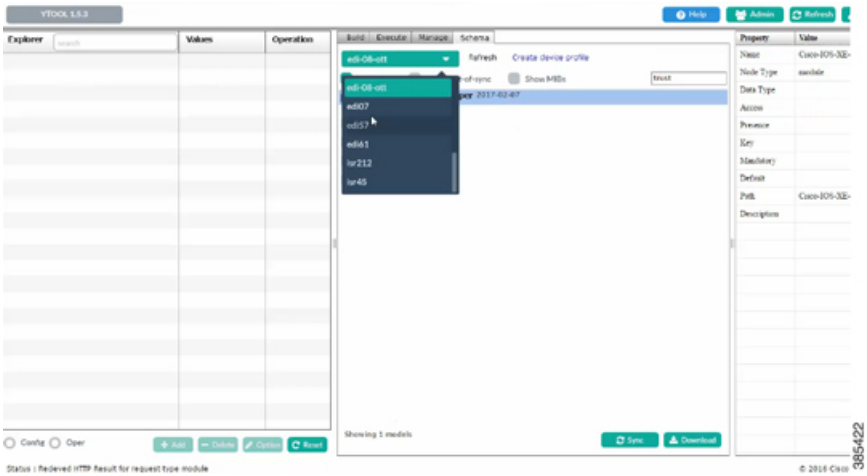
Note To communicate with Cisco devices, you can choose other external applications that can handle data that is structured using YANG. This section is relevant only if you have selected YTOOL to access Cisco devices.

Accessing Operational Data

Before you begin, ensure that the Cisco device from which you are going to extract operational data is configured on the YTOOL. See the "How to Configure the External Device YTOOL" section for details.

1. Download the Cisco TrustSec operational information schema from the Cisco device:
   1. Select **Schema**.
   2. Select the device. The list of schemas in the device will be displayed.

Figure 9: Select a Device

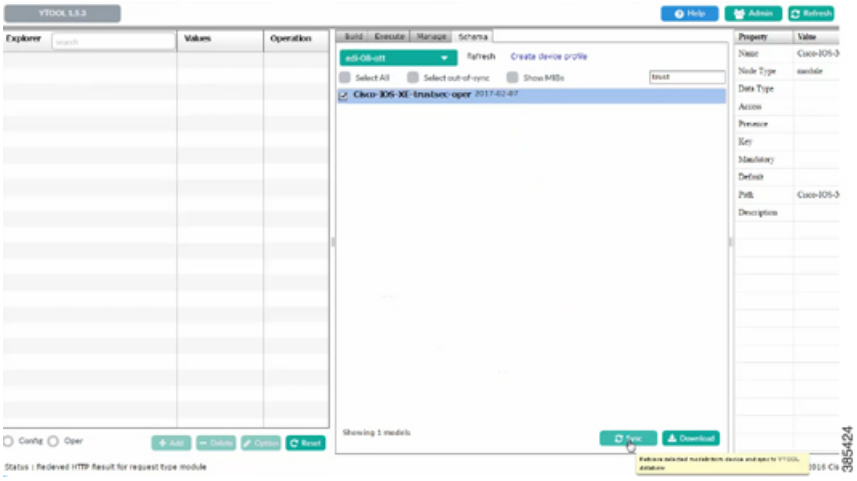


3. Select the Cisco TrustSec operational information schema. Use the search box to search for this schema.

Note The name of an operational information schema ends with **oper**.

4. Click **Sync**. The schema is downloaded into the YTOOL.

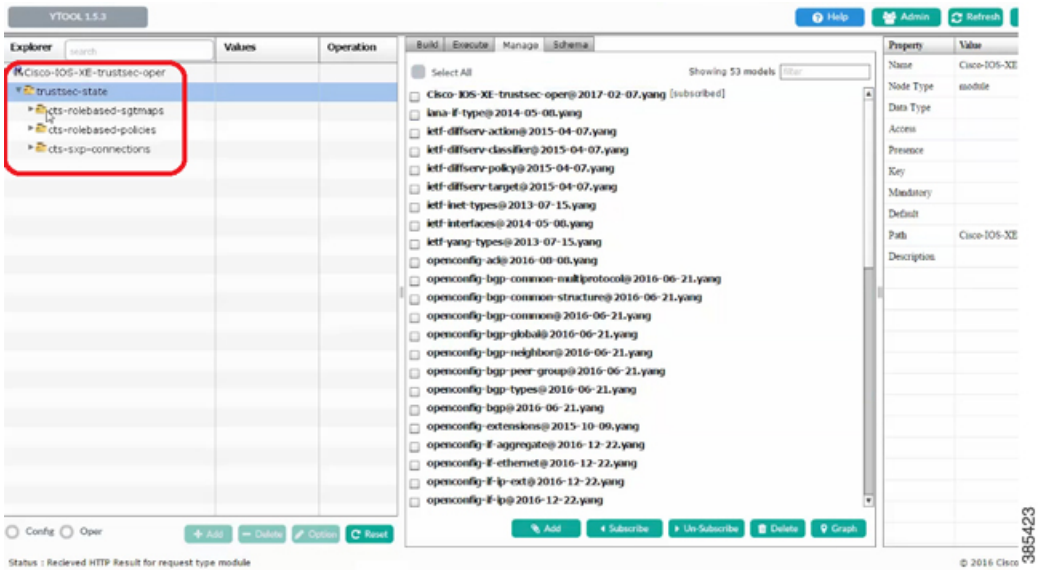
Figure 10: Download Schema



2. Subscribe to the downloaded operational information schema on YTOOL.
    1. Select **Manage**.
    2. From the list of schemas, select the operational information schema.
    3. Click **Subscribe**.

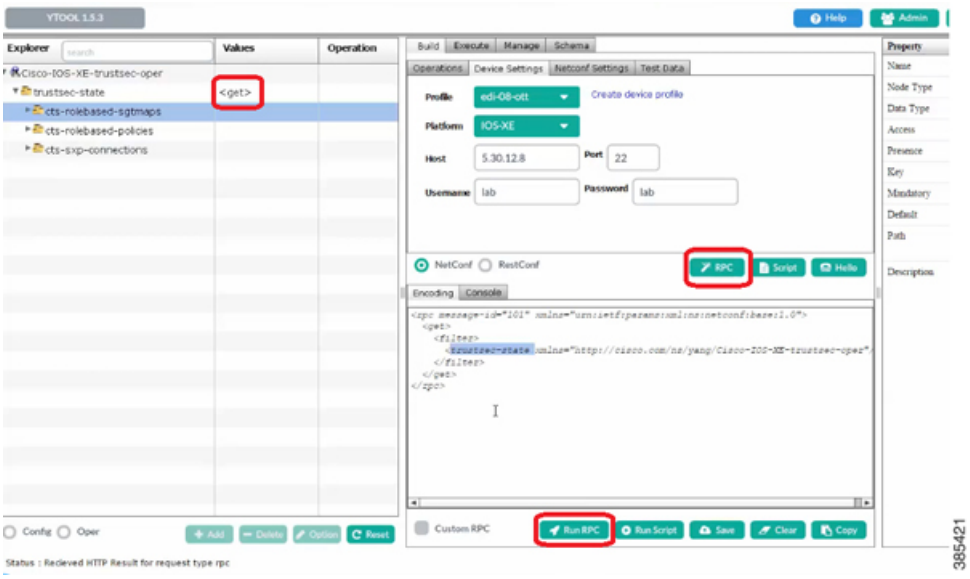
Note Once you have subscribed, the schema will be displayed under explorer.

Figure 11: Subscribe Schema



3. Retrieve selected operational data using the schema:
   1. Against the relevant information level of the operation information schema, select **get** under **values** .
   2. Click **RPC**. An XML generated RPC message will be generated.
   3. Click **Run RPC**. The operation data is retrieved from the Cisco device in the RPC-generated XML format.

Figure 12: Retrieve Operational Data



Note For information on the commands that are used to access operational data, see the section Information About Cisco TrustSec Operational Data, on page 116 .

Note To communicate with Cisco devices, you can choose other external applications that can handle data that is structured using YANG. This section is relevant only if you have selected YTOOL to access Cisco devices.