

# 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.


- Information About Cisco TrustSec Interface-to-SGT Mapping, on page 1
- How to Configure Cisco TrustSec Interface-to-SGT Mapping, on page 2
- Configuration Examples for Cisco TrustSec Interface-to-SGT Mapping, on page 4
- Additional References for Cisco TrustSec Interface-to-SGT Mapping, on page 4
- Feature Information for Cisco TrustSec Interface-to-SGT Mapping, on page 5


# 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

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type slot/port*<br>**Example:**<br>`Device(config)# interface gigabitEthernet 0/0` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **cts role-based sgt-map sgt** *sgt-number*<br>**Example:**<br>`Device(config-if)# cts role-based sgt-map sgt 77` | An SGT is imposed on ingress traffic to the specified interface.<br>• *sgt-number*—Specifies the security group tag (SGT) number. Valid values are from 2 to 65519. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Verifying Layer 3 Interface-to-SGT Mapping

## SUMMARY STEPS

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

## DETAILED STEPS

### Procedure

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

### Technical Assistance

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

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

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

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

*Table 1: 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.<br>The following command was introduced or modified: **cts role-based sgt-map sgt**. |