

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.

- Restrictions for Cisco TrustSec SGT Caching, on page 1
- Information About Cisco TrustSec SGT Caching, on page 2
- How to Configure Cisco TrustSec SGT Caching, on page 4
- Configuration Examples for Cisco TrustSec SGT Caching, on page 9
- Additional References for Cisco TrustSec SGT Caching, on page 10
- Feature Information for Cisco TrustSec SGT Caching, on page 11

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.
- SGT caching is not supported on tunnel interfaces that have IPsec with IVRF configured.
- Configuring SGT caching on a virtual template interface is not supported on a Cisco ASR 1000 platform.

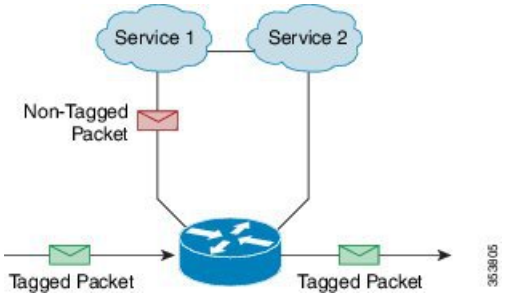
Information About Cisco TrustSec SGT Caching

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.

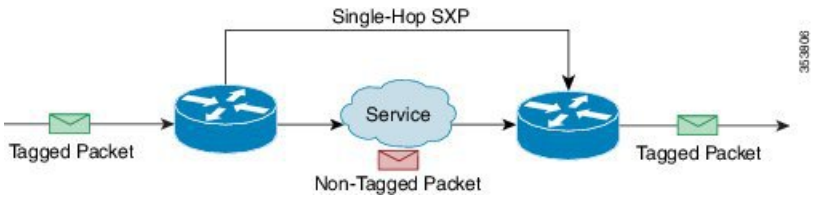
Figure 1: SGT Caching in One-Arm Mode



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 2: 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

Procedure

	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

Procedure

	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

Procedure

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 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 1: 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.