TrustSec Security Group Name Download

- TrustSec Security Group Name Download, on page 1

TrustSec Security Group Name Download

The TrustSec Security Group Name Download feature enhances the Security Group Tag (SGT) policy that downloads to the network access device to include the SGT name in addition to the SGT number and Security Group Access Control List (SGACL) policy.

Layer 3 Logical Interface to SGT Mapping

The TrustSec Security Group Name Download feature is used to directly map SGTs to traffic of any of the following Layer 3 interfaces regardless of the underlying physical interface:

- Routed port
- SVI (VLAN interface)
- Layer3 subinterface of a Layer2 port
- Tunnel interface

The **cts role-based sgt-map interface** global configuration command to specify either a specific SGT number, or a Security Group Name (whose SGT association is dynamically acquired from a Cisco ISE or a Cisco ACS access server).

Configuring TrustSec Security Group Name Download

Procedure

	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 role-based sgt-map interface** *type slot/port* [**security-group** *name* | **sgt** *number*] **Example:** `Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77`	An SGT is imposed on ingress traffic to the specified interface. • **interface** *type slot*/*port*—Displays list of available interfaces. • **security-group** *name*— Security Group name to SGT pairings are configured on the Cisco ISE or Cisco ACS. • **sgt** *number*—(0 to 65,535). Specfies the Security Group Tag (SGT) number.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 5	**show cts role-based sgt-map all** **Example:** `Device# show cts role-based sgt-map all`	Verify that ingressing traffic is tagged with the specified SGT.

Example: TrustSec Security Group Name Download

The following example shows the SGT download configuration for the ingress interface:

```
Device# config terminal
Device(config)# cts role-based sgt-map interface gigabitEthernet 6/3 sgt 3
Device(config)# exit
```

The following example shows that ingressing traffic for the ingress interface is tagged appropriately:

```
Device# show cts role-based sgt-map all

IP Address              SGT     Source

========================================

15.1.1.15               4       INTERNAL

17.1.1.0/24             3       L3IF

21.1.1.2                4       INTERNAL

31.1.1.0/24             3       L3IF

31.1.1.2                4       INTERNAL

43.1.1.0/24             3       L3IF
```

```
49.1.1.0/24             3       L3IF

50.1.1.0/24             3       L3IF

50.1.1.2                4       INTERNAL

51.1.1.1                4       INTERNAL

52.1.1.0/24             3       L3IF

81.1.1.1                5       CLI

102.1.1.1               4       INTERNAL

105.1.1.1               3       L3IF

111.1.1.1               4       INTERNAL

IP-SGT Active Bindings Summary

============================================

Total number of CLI      bindings = 1

Total number of L3IF     bindings = 7

Total number of INTERNAL bindings = 7

Total number of active   bindings = 15
```

Feature History for TrustSec Security Group Name Download

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	TrustSec Security Group Name Download	This feature enhances the SGT policy that downloads to the network access device to include the SGT name in addition to the SGT number and SGACL policy. Support for this feature was introduced on all the models of the Cisco Catalyst 9500 Series Switches.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.