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.

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

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.

	Command or Action	Purpose
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.

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.

	Command or Action	Purpose
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
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
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 1: 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**.