IPv6 Support for SGT and SGACL

The IPv6 Support for SGT and SGACL feature facilitates the mapping between IPv6 addresses and Security Group Tags (SGTs). The mapped SGT is later used to drive the Security Group Access Control List (SGACL) enforcement.

This module describes how to configure this feature.

Information About IPv6 Support for SGT and SGACL

Components of IPv6 Dynamic Learning

Dynamic learning of IPv6 addresses require three components:

- Switch Integrated Security Features (SISF): An infrastructure built to take care of security, address assignment, address resolution, neighbor discovery, exit point discovery, and so on.
- Cisco Enterprise Policy Manager (EPM): A solution that registers to SISF to receive IPv6 address notifications. The Cisco EPM then uses these IPv6 addresses and Security Group Tags (SGTs) downloaded from the Cisco Identity Services Engine (ISE) to generate IP-SGT bindings.
- Cisco TrustSec: A solution that protects devices from unauthorized access. Cisco TrustSec assigns an SGT to the ingress traffic of a device and enforces the access policy based on the tag anywhere in the network.

Mapping of IPv6 addresses to SGT can be done using the following methods, which are listed starting from lowest priority (1) to highest priority (6):

1. VLAN: IPv6 addresses learnt through SISF on the VLAN that has an SGT-VLAN mapping. Bindings are learned through ICMPv6 Neighbor Discovery.
2. CLI: Address bindings configured using the IP-SGT form of the **cts role-based sgt-map** global configuration command.

3. Layer 3 Interface: Bindings added due to forwarding information base (FIB) forwarding entries that have paths through one or more interfaces with consistent Layer 3 interface-SGT mapping or identity port mapping (IPM) on routed ports.
4. SXP: Bindings learned from SGT Exchange Protocol (SXP) peers.
5. Local: Bindings of authenticated hosts that are learned via EPM and device tracking. Device tracking and SISF are the same.
6. Internal: Bindings between locally configured IP addresses and the device SGT.

How to Configure IPv6 Support for SGT and SGACL

Learning IPv6 Addresses for IP-SGT Bindings

Switch Integrated Security Features (SISF) is a feature that learns IPv6 addresses for use in IP-SGT bindings.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map** *host-address*/*prefix* **sgt** *sgt-value*
4. **device-tracking policy** *policy-name*
5. **tracking enable**
6. **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 role-based sgt-map** *host-address*/*prefix* **sgt** *sgt-value* **Example:** `Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120`	Manually maps a source IPv6 address to an SGT on either a host or a virtual routing and forwarding (VRF) instance.
Step 4	**device-tracking policy** *policy-name* **Example:** `Device(config)# device-tracking policy policy1`	Enables device tracking and enters device tracking configuration mode.

	Command or Action	Purpose
Step 5	**tracking enable** **Example:** `Device(config-device-tracking)# tracking enable`	Overrides the default tracking policy on a port.
Step 6	**exit** **Example:** `Device(config-device-tracking)# end`	Exits device tracking configuration mode and returns to privileged EXEC mode.

What to do next

Configure IPv6-SGT binding by using either local binding or a VLAN.

Configuring IPv6 IP-SGT Binding Using Local Binding

Before you begin

- In local binding, the SGT value is downloaded from the Identity Service Engine (ISE). For more information, see Configuring Cisco Security Group Access Policies document.
- SISF must be enabled and populated before IPv6 address can be generated.

This task uses Identity Based Networking Services (IBNS) Version 2.0.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *control-policy-name*
4. **event session-started match-all**
5. *priority-number* **class always do-until-failure**
6. *action-number* **authenticate using mab**
7. **end**
8. **interface gigabitethernet** *interface-number*
9. **description** *interface-description*
10. **switchport access vlan** *vlan-id*
11. **switchport mode access**
12. **device-tracking attach-policy** *policy-name*
13. **access-session port-control auto**
14. **mab eap**
15. **dot1x pae authenticator**
16. **service-policy type control subscriber** *policy-name*
17. **end**
18. **show cts role-based sgt-map all ipv6**

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	**policy-map type control subscriber** *control-policy-name* **Example:** `Device(config)# policy-map type control subscriber policy1`	Defines a control policy for subscriber sessions and enters control policy-map configuration mode.
Step 4	**event session-started match-all** **Example:** `Device(config-event-control-policymap)# event session-started match-all`	Specifies the type of event that triggers actions in a control policy if conditions are met.
Step 5	*priority-number* **class always do-until-failure** **Example:** `Device(config-class-control-policymap)# 10 class always do-until-failure`	Associates a control class with one or more actions in a control policy and enters action control policy-map configuration mode. • A named control class must first be configured before specifying it with the *control-class-name* argument.
Step 6	*action-number* **authenticate using mab** **Example:** `Device(config-action-control-policymap)# 10 authenticate using mab`	Initiates the authentication of a subscriber session using the specified method.
Step 7	**end** **Example:** `Device(config-action-control-policymap)# exit`	Exits action control policy-map configuration mode and returns to global configuration mode.
Step 8	**interface gigabitethernet** *interface-number* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Configures an interface and enters interface configuration mode.
Step 9	**description** *interface-description* **Example:** `Device(config-if)# description downlink to ipv6 clients`	Describes the configured interface.
Step 10	**switchport access vlan** *vlan-id* **Example:**	Sets access mode characteristics of the interface and configures VLAN when the interface is in access mode.

	Command or Action	Purpose
	`Device(config-if)# switchport access vlan 20`	
Step 11	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the trunking mode to access mode.
Step 12	**device-tracking attach-policy** *policy-name* **Example:** `Device(config-if)# device-tracking attach-policy snoop`	Applies a policy to the IPv6 snooping feature.
Step 13	**access-session port-control auto** **Example:** `Device(config-if)# access-session port-control auto`	Sets the authorization state of a port.
Step 14	**mab eap** **Example:** `Device(config-if)# mab eap`	Uses Extensible Authentication Protocol (EAP) for MAC authentication bypass.
Step 15	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables dot1x authentication on the port.
Step 16	**service-policy type control subscriber** *policy-name* **Example:** `Device(config-if)# service-policy type control subscriber policy`	Specifies the policy map that is used for sessions that come up on this interface. The policy map has rules for authentication and authorization.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 18	**show cts role-based sgt-map all ipv6** **Example:** `Device# show cts role-based sgt-map all ipv6`	Displays active IPv6 IP-SGT bindings.

Configuring IPv6 IP-SGT Binding Using a VLAN

In a VLAN, a network administrator assigns a Security Group Tag (SGT) value to a particular VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map vlan-list** *vlan-id* **sgt** *sgt-value*

4. **end**
5. **show cts role-based sgt-map all ipv6**

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-map vlan-list** *vlan-id* **sgt** *sgt-value* **Example:** `Device(config)# cts role-based sgt-map vlan-list 20 sgt 3`	Assigns an SGT value to the configured VLAN. **Note** The range of the *sgt-value* argument must be from 2 to 65519.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show cts role-based sgt-map all ipv6** **Example:** `Device# show cts role-based sgt-map all ipv6`	Displays active IPv6 IP-SGT bindings.

Verifying IPv6 Support for SGT and SGACL

SUMMARY STEPS

1. **enable**
2. **show cts role-based sgt-map all**
3. **show cts role-based sgt-map all ipv6**

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	**show cts role-based sgt-map all**
	Example:
	`Device# show cts role-based sgt-map all`
	
	`Active IPv4-SGT Bindings Information`
	
	`IP Address SGT Source`
	`==========`
	`192.0.2.1 8 INTERNAL`
	`192.0.2.2 8 INTERNAL`
	`192.0.2.3 11 LOCAL`
	
	`IP-SGT Active Bindings Summary`
	`==========`
	`Total number of LOCAL bindings = 1`
	`Total number of INTERNAL bindings = 2`
	`Total number of active bindings = 3`
	
	`Active IPv6-SGT Bindings Information`
	
	`IP Address SGT Source`
	`==========`
	`2001:DB8:0:ABCD::1 8 INTERNAL`
	`2001:DB8:1::1 11 LOCAL`
	`2001:DB8:1::1 11 LOCAL`
	
	`IP-SGT Active Bindings Summary`
	`==========`
	`Total number of LOCAL bindings = 2`
	`Total number of INTERNAL bindings = 1`
	`Total number of active bindings = 3`
		Displays active IPv4 and IPv6 IP-SGT bindings.

Step 3	**show cts role-based sgt-map all ipv6**
	Example:
	`Device# show cts role-based sgt-map all ipv6`
	
	`Active IP-SGT Bindings Information`
	
	`IP Address SGT Source`
	`==========`
	`2001:DB8:1::1 10 CLI`
	`2001:DB8:1:FFFF::1 27 VLAN`
	`2001:DB8:9798:8294:753F::1 5 LOCAL`
	`2001:DB8:8E99:DA94:8A6A::2 5 LOCAL`
	`2001:DB8:104:2001::139 27 VLAN`
	`2001:DB8:104:2001:14FE:9798:8294:753F 5 LOCAL`
		Displays active IPv6 IP-SGT bindings.

	Command or Action	Purpose
	IP-SGT Active Bindings Summary ========== Total number of VLAN bindings = 2 Total number of CLI bindings = 1 Total number of LOCAL bindings = 3 Total number of active bindings = 6	

Configuration Examples for IPv6 Support for SGT and SGACL

Example: Learning IPv6 Addresses for IP-SGT Bindings

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# end
```

Example: Configuring IPv6 IP-SGT Binding Using Local Binding

This examples uses Identity Based Networking Services (IBNS) Version 2.0.

```
Device> enable
Device# configure terminal
Device(config)# policy-map type control subscriber policy1
Device(config-event-control-policymap)# event session-started match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using mab
Device(config-action-control-policymap)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# description downlink to ipv6 clients
Device(config-if)# switchport access vlan 20
Device(config-if)# switchport mode access
Device(config-if)# device-tracking attach-policy snoop
Device(config-if)# access-session port-control auto
Device(config-if)# mab eap
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber policy
Device(config-if)# end
```

Example: Configuring IPv6 IP-SGT Binding Using a VLAN

```
Device> enable
Device# configure terminal
```

```
Device(config)# cts role-based sgt-map vlan-list 20 sgt 3
Device(config)# end
```

Additional References for IPv6 Support for SGT and SGACL

Related Documents

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

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 IPv6 Support for SGT and SGACL

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 IPv6 Support for SGT and SGACL

Feature Name	Releases	Feature Information
IPv6 Support for SGT and SGACL	Cisco IOS XE Fuji 16.9.1	The IPv6 Support for SGT and SGACL feature introduces dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is later used to derive the Security Group Access Control List (SGACL). In Cisco IOS XE Fuji 16.9.1, this feature was implemented on Cisco Catalyst 9500 Series High Performance Switches.