Configuring SGACL Policies

Revised: January 13, 2016

This section includes the following topics:

- Cisco TrustSec SGACL Feature Histories, page 4-1
- Restrictions for Configuring SGACL Policies, page 4-1
- SGACL Policy Configuration Process, page 4-2
- Enabling SGACL Policy Enforcement Globally, page 4-2
- Enabling SGACL Policy Enforcement Per Interface, page 4-4
- Enabling SGACL Policy Enforcement on VLANs, page 4-5
- Configuring SGACL Monitor Mode, page 4-6
- Manually Applying SGACL Policies, page 4-10
- Refreshing the Downloaded SGACL Policies, page 4-12

Cisco TrustSec SGACL Feature Histories

For a list of supported TrustSec features per platform and the minimum required IOS release, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.

Restrictions for Configuring SGACL Policies

The following restrictions apply to IPv6 SGACL enforcement:

- SGACL enforcement will be bypassed for IPv6 multicast traffic.
- SGACL enforcement will be by-passed for IPv6 packets with Link-Local IPv6 source/destination addresses

The following restriction apply to the Cisco Catalyst 3750-X Series Switches while configuring SGACL policies:

- When SXP is configured between a Catalyst 3750-X switch and another switch, SGACL policies are not enforced on Catalyst 3750-X series switches. SGACL policies are downloaded for the destination SGT, but policy statements are not applied to the traffic that is initiated from the source SGT.

  IP device tracking must be enabled on both switches and these switches should have Layer2 adjacency configured between them so that Catalyst 3750-X can tag packets with the corresponding SGT learned via the SXP protocol.

  You can enable IP device tracking on Catalyst 3750-X switches by using the **ip device tracking maximum** <*number*> command. Based on your topology, configure the number of IP clients using the *number* argument. We do not recommend configuring a high number of IP clients on ports/interfaces.

  IP device tracking is enabled by default on all ports in Cisco IOS Release 15.2(1)E, and in Catalyst 3750-X switches using this release image, SGACL policy enforcement happens.

The following restriction apply to the Cisco Catalyst 6500 Series Switches:

- CTS SGACLs are enforced for punt (CPU bound) traffic by default.

The following restriction apply to the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches:

- CTS SGACLs cannot be enforced for punt (CPU bound) traffic due to hardware limitations.

SGACL Policy Configuration Process

Follow these steps to configure and enable Cisco TrustSec Security Group ACL (SGACL) policies:

Step 1 Configuration of SGACL policies should be done primarily through the Policy Management function of the Cisco Secure ACS or the Cisco Identity Services Engine (see the *Configuration Guide for the Cisco Secure ACS* or the *Cisco Identity Services Engine User Guide*).

If you are not using AAA on a Cisco Secure ACS or a Cisco ISE to download the SGACL policy configuration, you can manually configure the SGACL mapping and policies (see the "Manually Configuring SGACL Policies" section on page 4-7).

Note An SGACL policy downloaded dynamically from the Cisco Secure ACS or a Cisco ISE will override any conflicting locally-defined policy.

Step 2 To enable SGACL policy enforcement on egress traffic on routed ports, enable SGACL policy enforcement globally as described in the "Enabling SGACL Policy Enforcement Globally" section on page 4-2.

Step 3 To enable SGACL policy enforcement on switched traffic within a VLAN, or on traffic that is forwarded to an SVI associated with a VLAN, enable SGACL policy enforcement for specific VLANs as described in the "Enabling SGACL Policy Enforcement on VLANs" section on page 4-5.

Enabling SGACL Policy Enforcement Globally

You must enable SGACL policy enforcement globally for Cisco TrustSec-enabled routed interfaces.

The same configuration commands that are used for enforcement of IPv4 traffic apply for IPv6 traffic as well.

To enable SGACL policy enforcement on routed interfaces, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

Configuration Examples for Enabling SGACL Policy Enforcement Globally

```
Switch(config)# cts role-based enforcement
```

Enabling SGACL Policy Enforcement Per Interface

You must first enable SGACL policy enforcement globally for Cisco TrustSec-enabled routed interfaces. This feature is not supported on Port Channel interfaces.

To enable SGACL policy enforcement on Layer 3 interfaces, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface gigabitethernet 6/2`	Specifies interface on which to enable or disable SGACL enforcement.
Step 3	`Switch(config-if)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
Step 4	`Switch(config-if)# do show cts interface`	Verifies that SGACL enforcement is enabled.

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] cts role-based monitor enable`	Enables device level monitor mode. By default device level monitor mode is enabled. If device monitor mode is disabled, monitor mode information is still downloaded from ISE but not applied on device until this configuration is turned on.
Step 3	`Switch(config)# [no] cts role-based monitor permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6]`	Enables monitor mode for IPv4/IPv6 RBACL (SGT-DGT pair).
Step 4	`Switch(config)# show cts role-based permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6] [details]`	Displays the SGACL policies and details about the monitor mode feature for each pair. The command output displays `monitored` if per cell monitor mode is enabled for the <SGT-DGT> pair
Step 5	`Switch(config)# show cts role-based counters [ipv4 | ipv6]`	Displays all SGACL enforcement statistics for IPv4 and IPv6 events.

Configuration Examples for Enabling SGACL Policy Enforcement Per Interface

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# cts role-based enforcement
Switch(config-if)# end
```

Enabling SGACL Policy Enforcement on VLANs

You must enable SGACL policy enforcement on specific VLANs to apply access control to switched traffic within a VLAN, or to traffic that is forwarded to an SVI associated with a VLAN.

To enable SGACL policy enforcement on a VLAN or a VLAN list, perform this task:

Detailed Steps

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts role-based enforcement vlan-list` *vlan-list*	Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.

Configuration Examples for Enabling SGACL Policy Enforcement on VLANs

```
Switch# configure terminal
Switch(config)# cts role-based enforcement vlan-list 31-35,41
Switch(config)# exit
```

Configuring SGACLMonitor Mode

Before configuring SGACL monitor mode, ensure the following:

- Cisco TrustSec is enabled
- Counters are enabled

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] cts role-based monitor all`	Enables device level monitor mode. By default device level monitor mode is enabled. If device monitor mode is disabled, monitor mode information is still downloaded from ISE but not applied on device until this configuration is turned on.
Step 3	`Switch(config)# [no] cts role-based monitor permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6]`	Enables monitor mode for IPv4/IPv6 RBACL (SGT-DGT pair).
Step 4	`Switch(config)# show cts role-based permissions from {sgt_num} to {dgt_num}][ipv4 | ipv6] [details]`	Displays the SGACL policies and details about the monitor mode feature for each pair. The command output displays `monitored` if per cell monitor mode is enabled for the <SGT-DGT> pair
Step 5	`Switch(config)# show cts role-based counters [ipv4 | ipv6]`	Displays all SGACL enforcement statistics for IPv4 and IPv6 events.

Note The **show cts role-based counters** CLIs for IPv4 and IPv6 traffic are separate, but the displayed values for IPv4 and IPv6 are combined.

Configuration Example for Configuring SGACL Monitor Mode

```
Switch# conf t
Switch(config)# cts role-based monitor all
Switch(config)# cts role-based permissions from 2 to 3 ipv4
Switch# show cts role-based permissions from 2 to 3 ipv4
IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Switch# show cts role-based permissions from 2 to 3 ipv4 details
IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
    10 deny tcp
    20 deny udp
    30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
    10 permit ip
Switch# show cts role-based counters ipv4
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW_Permitt SW-Monitor HW-Monitor
*       *       0          0          8          18962      0          0
2       3       0          0          0          0          0          341057
```

Manually Configuring SGACL Policies

A role-based access control list bound to a range of SGTs and DGTs forms an SGACL, a TrustSec policy enforced on egress traffic. Configuration of SGACL policies are best done through the policy management functions of the Cisco ISE or the Cisco Secure ACS. To manually (that is, locally) configure SGACL policies, do the following:

1. Configure a role-based ACL.
2. Bind the role-based ACL to a range of SGTs.

Note An SGACL policy downloaded dynamically from the Cisco ISE or Cisco ACS overrides any conflicting manually configured policy.

Manually Configuring and Applying IPv4 SGACL Policies

Note When configuring SGACLs and Role-Based access control lists (RBACLs), the named access control lists (ACLs) must start with an alphabet.

Detailed Steps for Catalyst 3850,3650, 9300,9400,9500 switches:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list role-based** *rbacl-name* **Example:** `Switch(config)# ip access-list role-based allow_webtraff`	Creates a Role-based ACL and enters Role-based ACL configuration mode.
Step 3	{[*sequence-number*] | **default** | **permit** | **deny** | **remark**} **Example:** `Switch(config-rb-acl)#10 permit tcp dst eq 80 dst eq 20`	Specifies the access control entries (ACEs) for the RBACL. You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted. Press Enter to complete an ACE and begin the next. For full explanations of ACL configuration, keywords, and options, see, Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S. The following ACE commands or keywords are not supported: • **reflect** • **evaluate** • **time-range**
Step 4	`Switch(config-rb-acl)# exit`	Exits to global configuration mode.
Step 5	[**no**] **cts role-based permissions** {**default** | [**from** {*sgt_num* | **unknown**} **to** {*dgt_num* | **unknown**}]{*rbacls* | **ipv4** *rbacls*} **Example:** `Switch(config)# cts role-based permissions from 55 to 66 allow_webtraff`	Binds SGTs and DGTs to the RBACL. The configuration is analogous to populating the permission matrix configured on the Cisco ISE or the Cisco Secure ACS. • Default—Default permissions list • *sgt_num*—0 to 65,519. Source Group Tag • *dgt_num*—0 to 65,519. Destination Group Tag • unknown—SGACL applies to packets where the security group (source or destination) cannot be determined. • ipv4—Indicates the following RBACL is IPv4. • *rbacls*—Name of RBACLs
Step 6	`Switch(config)# end`	Exits to privileged EXEC mode.
Step 7	`Switch# show cts role-based permissions`	Displays permission to RBACL configurations.
Step 8	`Switch# show ip access-lists allow_webtraff`	Displays ACEs of all RBACLs or a specified RBACL.

Configuration Examples for Manually Configuring SGACL Policies

```
Switch(config)# ip access role allow_webtraff
Switch(config-rb-acl)# 10 permit tcp dst eq 80
Switch(config-rb-acl)# 20 permit tcp dst eq 443
Switch(config-rb-acl)# 30 permit icmp
Switch(config-rb-acl)# 40 deny ip
Switch(config-rb-acl)# exit
Switch(config)# cts role-based permissions from 55 to 66 allow_webtraff
Switch# show ip access allow_webtraff

Role-based IP access list allow_webtraff
    10 permit tcp dst eq www
    20 permit tcp dst eq 443
    30 permit icmp
    40 deny ip

Switch# show show cts role-based permissions from 50 to 70
```

Configuring IPv6 Policies

To manually configure IPv6 SGACL policies, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ipv6 access-list role-based` *sgacl-name*	Creates a named IPv6 SGACL and enters IPv6 role-based ACL configuration mode.
Step 3	`Switch(config-ipv6rb-acl)# [no] {permit | deny}` *protocol* `[dest-option | dest-option-type {`*doh-number* `|` *doh-type*`}] [dscp` *cp-value*`] [flow-label` *fl-value*`] [mobility | mobility-type {`*mh-number* `|` *mh-type*`}] [routing | routing-type` *routing-number*`] [fragments] [log | log-input] [sequence` *seqno*`]`	Specifies the access control entries (ACEs) for the IPv6 SGACL. You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted. The following ACE commands or keywords are not supported: • **reflect** • **evaluate** • **time-range**
Step 4	`Switch(config-ipv6rb-acl)# exit`	Exits IPv6 role-based ACL configuration mode.

Manually Applying SGACL Policies

To manually apply SGACL policies, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cts role-based permissions default [ipv4 | ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]]`	Specifies the default SGACLs. The default policies are applied when no explicit policy exists between the source and destination security groups.
Step 3	`Switch(config)# cts role-based permissions from {source-sgt | unknown} to {dest-sgt | unknown} [ipv4 | ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]]`	Specifies the SGACLs to be applied for a source security group (SGT) and destination security group (DGT). Values for *source-sgt* and *dest-sgt* range from 1 to 65533. By default, SGACLs are considered to be IPv4. • **from**—Specifies the source SGT. • **to**—Specifies the destination security group. • **unknown**—SGACL applies to packets where the security group (source or destination) cannot be determined. **Note** An SGACL policy downloaded dynamically from the ACS will override any conflicting manual policy.

Configuration Examples for Manually Applying SGACLs

Catalyst 6500—Apply default and custom SGACL policies:

```
Switch# configure terminal
Switch(config)# cts role-based permissions default MYDEFAULTSGACL
Switch(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Switch(config)# exit
```

Displaying SGACL Policies

After configuring the Cisco TrustSec device credentials and AAA, you can verify the Cisco TrustSec SGACL policies downloaded from the authentication server or configured manually. Cisco TrustSec downloads the SGACL policies when it learns of a new SGT through authentication and authorization on an interface, from SXP, or from manual IP address to SGT mapping.

To display the contents of the SGACL policies permissions matrix, perform this task:

Detailed Steps for Catalyst 6500

	Command	Purpose
Step 1	`Switch# show cts role-based permissions default [ipv4 | ipv6 | details]`	Displays the list of SGACL of the default policy.
	`Switch# show cts role-based permissions [from {source-sgt | unknown}] [to {dest-sg | unknown}] [ipv4 | ipv6] [details]`	Displays the contents of the permissions matrix, including SGACLs downloaded from the authentication server and manually configured on the switch.

Using the keywords, you can display all or part of the permissions matrix:

- If the **from** keyword is omitted, a column from the permissions matrix is displayed.
- If the **to** keyword is omitted, a row from the permissions matrix is displayed.
- If the **from** and **to** keywords are omitted, the entire permissions matrix is displayed.
- If the **from** and **to** keywords are specified, a single cell from the permissions matrix is displayed and the **details** keyword is available. When **details** is entered, the ACEs of the SGACL of the single cell are displayed.

This example shows how to display the content of the SGACL policies permissions matrix for traffic sourced from security group 3:

```
Switch# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
        SRB3
        SRB5
Role-based permissions from group 3 to group 7:
        SRB4
```

Refreshing the Downloaded SGACL Policies

Detailed Steps for Catalyst 6500, Catalyst 3850, Catalyst 3650

	Command	Purpose
Step 1	**cts refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number*| **default**|**unknown**]} `Switch3850# cts refresh policy peer my_cisco_ise`	Performs an immediate refresh of the SGACL policies from the authentication server. • If a *peer-id* is specified, only the policies related to the specified peer connection are refreshed. To refresh all peer policies, press Enter without specifying an ID. • If an SGT number is specified, only the policies related to that SGT are refreshed. To refresh all security group tag policies, press Enter without specifying an SGT number. Select default to refresh the default policy. Select unknown to refresh unknown policy.

Feature Information for SGACL Policies

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 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.

Table 1 Feature Information for SGACL Policies

Feature Name	Releases	Feature Information
Manual SGACL Configuration	Cisco IOS Release 12.2(50)SY Cisco IOS XE Release 3.3SE	This feature was introduced on the Catalyst 6500 series switches. This feature was introduced on the Catalyst 3650 and 3850 series switches.
SGACL Global Enforcement	Cisco IOS Release 12.2(50)SY	This feature was introduced on the Catalyst 6500 series switches.
SGACL Enforcement Per Interface	Cisco IOS Release 15.1(2)SY	This feature was introduced on the Catalyst 6500 series switches.
SGACL Enforcement on VLANs	Cisco IOS Release 12.2(50) SY	This feature was introduced on the Catalyst 6500 series switches.