Configuring Security Group ACL Policies

Using security group access control lists (SGACLs), you can control the operations that users can perform based on the security group assignments of users and destination resources. Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with source security group numbers on one axis and destination security group numbers on the other axis. Each cell in the body of the matrix can contain an ordered list of SGACLs, which specifies the permissions that should be applied to packets originating from the source security group and destined for the destination security group.

- Restrictions for Configuring Security Group ACL Policies, on page 1
- Information About Security Group ACL Policies, on page 2
- How to Configure Security Group ACL Policies, on page 3
- Configuration Examples for Security Group ACL Policies, on page 12
- Feature History for Security Group ACL Policies, on page 14

Restrictions for Configuring Security Group ACL Policies

- The following restrictions are applicable only to the Cisco Catalyst 9600 Series Supervisor 2 Module :
  - The same set of ACLs cannot be used for both regular SGACL cell permissions and SGACL default permissions. Use a unique set of ACLs for default permission instead.
  - Cell permit and deny counters are supported only for the first 511 cells.
  - Counters are not supported for default permissions.
- Due to hardware limitations, Cisco TrustSec SGACLs cannot be enforced for punt (CPU bound) traffic in hardware. SGACL enforcement in software is bypassed wfor CPU-bound traffic for switch virtual interface (SVI) and Layer 2 and Layer 3 Location Identifier Separation Protocol (LISP), and loopback interfaces.
- When configuring SGACL policies, if you change the IP version dynamically from **IPv4** or **IPv6** to **Agnostic** (applies to both IPv4 and IPv6) and vice-versa, the corresponding SGACL policies for IPv4 and IPv6 are not downloaded completely through the management VRF interface.
- When configuring SGACL policies, if you change the existing IP version to any other version (**IPv4**, **IPv6**, or **Agnostic**) and vice-versa, Change of Authorization (CoA) from Cisco Identity Services Engine (ISE) cannot be performed using RADIUS. Instead, use SSH and run the **cts refresh policy** command to perform a manual policy refresh.

- When using an allowed SGT model with default action as **deny all**, in some cases, Cisco TrustSec policies are only partially downloaded from the ISE server after a device reload.

  To prevent this, define a static policy on the device. Even if the **deny all** option is applied, the static policy permits traffic that allows the device to download policies from the ISE server and overwrite the defined static policies. For device SGT, configure the following commands in global configuration mode:

  - **cts role-based permissions from** <*sgt_num*> **to unknown**
  - **cts role-based permissions from unknown to** <*sgt_num*>

Information About Security Group ACL Policies

The following sections provide information about configuring SGACL policies.

SGACL Logging

A device can provide logging messages about packets that are permitted or denied by a standard IP access list. That is, any packet that matches an SGACL causes an informational logging message about the packet to be sent to the console. The limit of messages logged to the console is controlled by the **logging console** command that controls the syslog messages. In releases prior to Cisco IOS XE Amsterdam 17.3.1, SGACL logging was done as a CPU-intensive mechanism. From Cisco IOS XE Amsterdam 17.3.1 release, SGACL logging has been enhanced to use NetFlow hardware, which allows much larger logging rates.

Note SGACL logging in hardware is only supported for Role-Based access control list (RBACL).

The first packet that triggers the SGACL creates a flow, and logging is done at the NetFlow timeout of 30 seconds and 1 minute for inactive and active flows respectively. Subsequent packets are collected over 5-minute intervals before they are logged. The logging message includes the access list number, whether the packet was permitted or denied, the source and destination IP addresses of the packet, the interface on which the packet was ingressed, and the number of packets from that source permitted or denied in the previous 5-minute interval.

Note

- Because SGACL logging in the hardware is done using NetFlow, if a NetFlow-based feature is applied to an interface, logging for that interface falls back to the old mechanism. Logging through NetFlow hardware starts again for that interface after the NetFlow-based feature is removed. The rest of the interfaces continue logging through NetFlow hardware.
- Only 15 NetFlow monitors can be attached to the device at a given time. SGACL logging requires one NetFlow monitor each for IPv4 and IPv6 logging. If NetFlow monitors are not available for logging, SGACL logging is done through the earlier mechanism. Once the required number of NetFlow monitors are available, run the **cts role-based permissions** command to trigger logging through the NetFlow hardware again.
- If a log access control entry (ACE) has fields other than source port number, destination port number and the protocol in use, logging is done through the earlier mechanism.

How to Configure Security Group ACL Policies

The following sections provide information about various SGACL policy configurations.

SGACL Policy Configuration Process

Follow these steps to configure and enable SGACL policies:

1. Configuration of SGACL policies should be done primarily through the Policy Management function of the Cisco Secure Access Control Server (ACS) or the Cisco Identity Services Engine (ISE).

   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.

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

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

Enabling SGACL Policy Enforcement Globally

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

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

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 enforcement** **Example:** `Device(config)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

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:

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 6/2`	Configures an interface and enters interface configuration mode.
Step 4	**cts role-based enforcement** **Example:** `Device(config-if)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show cts interface** **Example:** `Device# show cts interface`	(Optional) Displays Cisco TrustSec states and statistics per interface.

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:

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 enforcement vlan-list** *vlan-list* **Example:** `Device(config)# cts role-based enforcement vlan-list 31-35,41`	Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring SGACL Monitor Mode

Before configuring SGACL monitor mode, ensure the following:

- Cisco TrustSec is enabled
- Counters are enabled

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 role-based monitor all** **Example:** `Device(config)# cts role-based monitor all`	Enables global monitor mode.
Step 4	**cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] **Example:** `Device(config)# cts role-based permissions from 2 to 3 ipv4`	Enables monitor mode for IPv4 or IPv6 Role-Based Access Control List (RBACL) (Security Group Tag-Destination Group Tag [SGT-DGT] pair).
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**show cts role-based permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] [**details**] **Example:** `Device# show cts role-based permissions from 2 to 3 ipv4 details`	(Optional) Displays the SGACL policies and details about the monitor mode functionality for each pair. The command output displays if per-cell monitor mode is enabled for the <*SGT-DGT*> pair.
Step 7	**show cts role-based counters** [**ipv4** | **ipv6**] **Example:** `Device# show cts role-based counters ipv4`	(Optional) Displays all the SGACL enforcement statistics for IPv4 and IPv6 events.

Manually Configuring SGACL Policies

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

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

Configuring and Applying IPv4 SGACL Policies

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

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	**ip access-list role-based** *rbacl-name* **Example:** `Device(config)# ip access-list role-based allow_webtraff`	Creates an RBACL and enters Role-based ACL configuration mode.
Step 4	{[*sequence-number*] | **default** | **permit** | **deny** | **remark**} **Example:** `Device(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. The following ACE keywords are not supported: • **reflect** • **evaluate** • **time-range**
Step 5	**exit** **Example:** `Device(config-rb-acl)# exit`	Exits role-based ACL configuration mode and returns to global configuration mode.
Step 6	**cts role-based permissions {default** | [**from** {*sgt_num* | **unknown**} **to** {*dgt_num* | **unknown** }] {*rbacls* | **ipv4** *rbacls*} **Example:** `Device(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 Cisco ISE or 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.

	Command or Action	Purpose
		• **ipv4**: Indicates the RBACLs are IPv4. • *rbacls*: Names of RBACLs.
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	**show cts role-based permissions** **Example:** `Device# show cts role-based permissions`	(Optional) Displays permission to RBACL configurations.
Step 9	**show ip access-lists** {*rbacls* | **ipv4** *rbacls*} **Example:** `Device# show ip access-lists allow_webtraff`	(Optional) Displays ACEs of all RBACLs or a specified RBACL.

Configuring IPv6 SGACL Policies

To manually configure IPv6 SGACL policies, perform this task:

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	**ipv6 access-list role-based** *sgacl-name* **Example:** `Device(config)# ipv6 access-list role-based sgaclname`	Creates a named IPv6 SGACL and enters IPv6 role-based ACL configuration mode.
Step 4	{**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*] **Example:**	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. The following ACE keywords are not supported:

	Command or Action	Purpose
	`Device(config-ipv6rb-acl)# permit 33 dest-option dscp af11`	• **reflect** • **evaluate** • **time-range**
Step 5	**end** **Example:** `Device(config-ipv6rb-acl)# end`	Exits IPv6 role-based ACL configuration mode and returns to privileged EXEC mode.

Manually Applying SGACL Policies

To manually apply SGACL policies, perform this task:

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 permissions default** [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]] **Example:** `Device(config)# cts role-based permissions default MYDEFAULTSGACL`	Specifies the default SGACL. The default policies are applied when no explicit policy exists between the source and destination security groups.
Step 4	**cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]] **Example:** `Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5`	Specifies the SGACLs to be applied for an SGT and a 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**

	Command or Action	Purpose
		An SGACL policy downloaded dynamically from the ACS will override conflicting manual policies, if any.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Displaying SGACL Policies

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

By using or omitting 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.

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**show cts role-based permissions default** [**ipv4** | **ipv6** | **details**] **Example:** `Device# show cts role-based permissions default MYDEFAULTSGACL`	Displays the list of SGACL, of the default policy.
Step 3	**show cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**}] [**ipv4** | **ipv6** | **details**] **Example:**	Specifies the SGACLs to be applied for an SGT and a 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.

	Command or Action	Purpose
	`Device# show cts role-based permissions from 3`	• **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 conflicting manual policies, if any.
Step 4	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode.

Refreshing the Downloaded SGACL Policies

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**cts refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]} **Example:** `Device# 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 the 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 the SGT policies, press **Enter** without specifying an SGT number. Select **default** to refresh the default policy. Select **unknown** to refresh an unknown policy.
Step 3	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode.

Configuration Examples for Security Group ACL Policies

The following sections provide examples of various SGACL policy configurations.

Example: Enabling SGACL Policy Enforcement Globally

The following example shows how to enable SGACL policy enforcement globally:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
```

Example: Enabling SGACL Policy Enforcement Per Interface

The following example shows how to enable SGACL policy enforcement per interface:

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

Example: Enabling SGACL Policy Enforcement on VLANs

The following example shows how to enable SGACL policy enforcement on VLANs:

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

Example: Configuring SGACL Monitor Mode

The following example shows how to configure SGACL monitor mode:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# 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

Device# 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

Device# 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
```

Example: Manually Configuring SGACL Policies

The following example shows how to manually configure SGACL policies:

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

Device# 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

Device# show cts role-based permissions from 2 to 5

Role-based permissions from group 2 to group 5:
srb2
srb5
```

Example: Manually Applying SGACLs

The following example shows how to manually apply SGACL policies:

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

Example: Displaying SGACL Policies

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

```
Device> enable
Device# 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
```

Feature History for Security Group ACL Policies

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

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

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.11.1	Security Group ACL Policies	Using SGACLs, you can control the operations that users can perform based on the security group assignments of users and destination resources.
Cisco IOS XE Amsterdam 17.3.1	Enhanced SGACL Logging	Enhanced ACL logging allows logging to be done at much higher rates than using the NetFlow hardware.
Cisco IOS XE Cupertino 17.7.1	Security Group ACL Policies	This feature was implemented on Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP-2)..

Use the 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.