CHAPTER 5

Configuring SGACL Policies

Revised: August 15, 2013, OL-22192-02

This section includes the following topics:

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.

SGACL Policy Configuration Process

Follow these steps to configure and enable Cisco TrustSec 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 5-4 and the "Manually Configuring SGACL Policies" section on page 5-4).

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 5-2.

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 5-3.

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:

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

Configuration Examples for Enabling SGACL Policy Enforcement Globally

Catalyst 6500, Catalyst 3850:

```
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 Catalyst 6500

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

Configuration Examples for Enabling SGACL Policy Enforcement Per Interface

Catalyst 3850:

```
Switch# configure terminal
Switch(config)# interface gigabit 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 Catalyst 6500

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(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

Catalyst 3850:

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

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

Detailed Steps for Catalyst 3850

	Command	Purpose
Step 1	`Router# 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.

	Command	Purpose

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

Catalyst 3850 IPv4 Manual SGACL policy:

```
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
XXX need output XX
```

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	`Router# show cts role-based permissions default [ipv4 | ipv6 | details]`	Displays the list of SGACL of the default policy.
	`Router# 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:

```
Router# 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]}`	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.
	`Switch3850# cts refresh policy peer my_cisco_ise`	