Configuring SGACL Logging

SGACL Logging

Security group-based access control list (SGACL) Logging is supported on Cisco IE3400 and IE3400H Series Switches in Cisco IOS XE Release 17.8.1 and later. Support for SGACL Logging also requires that one of the following FPGA Profiles be activated on the switch:

- Default Profile
- CTS-IPv6 Profile

For information about FPGA Profile, see System Management Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches.

Security group access control lists (SGACLs) are a policy enforcement method through which the administrator can control operations performed by a user, based on security group assignments and destination resources. SGACL is a component of the Cisco TrustSec security architecture, which builds secure networks by establishing domains of trusted network devices. For comprehensive information about TrustSec, including TrustSec prerequisites, guidelines and limitations, and configuration procedures, see Cisco TrustSec Configuration Guide.

Logging-enabled access control lists (ACLs) provide insight into traffic as it traverses the network or is dropped by network devices. The device can provide logging messages about packets permitted or denied by a role-based IPv4/v6 access list. That is, any packet that matches the SGACL causes an informational logging message about the packet to be sent to the console. Logging is triggered only when the Access Control Entry (ACE) includes the log keyword. The level of messages logged to the console is controlled by the **logging console** command controlling the syslog messages.

Following is an example syslog message that is generated after a specific ACE that is configured for logging is matched:

```
*Jun 18 10:17:22.205: %RBM-6-SGACLHIT: ingress_interface='' sgacl_name='testv4'
action='Permit'
 protocol='udp' src-vrf='default' src-ip='25.1.1.1' src-port='96' dest-vrf='default'
```

```
dest-ip='25.1.1.2'
dest-port='0' sgt='100' dgt='200' logging_interval_hits='12'
```

The logging message includes the access list name, whether the packet was permitted or denied, the source and destination IP addresses of the packet, and information regarding the security group tag (SGT) and destination group tag (DGT).

The following table shows the types of ACE operations in IPv4/v6 role-based ACLs supported on the switch. The log keyword applies to individual ACEs and causes packets that match the ACE to be logged. The first packet logged by the **log** keyword generates a syslog message.

Note SGACL Logging is supported for ACEs with the OR logical operator. SGACL Logging is not supported for operations with the AND logical operator.

SGACL command	Description
permit/deny tcp src eq <src-port> or dst eq <dst-port> log	Matches TCP packets based on the specified source port or destination port.
permit/deny udp src eq <src-port> or dst eq <dst-port> log	Matches UDP packets based on the specified source port or destination port.
permit/deny tcp src range <start-port> <end-port> or dst range <start-port> <end-port> log	Matches TCP packets based on the range specified for source ports or destination ports.
permit/deny udp src range <start-port> <end-port> or dst range <start-port> <end-port> log	Matches UDP packets based on the range specified for source ports or destination ports.
Permit/deny tcp src gt/lt <src-port> or dst gt/lt <dst-port> log	Matches TCP packets that are greater than or lesser than the specified source port or greater than or lesser than the specified destination port.
Permit/deny udp src gt/lt <src-port> or dst gt/lt <dst-port> log	Matches UDP packets that are greater than or lesser than the specified source port or greater than or lesser than the specified destination port.

Prerequisites

- SGACL Logging requires that one of the following FPGA Profiles be activated on the switch:
  - Default Profile
  - CTS-IPv6 Profile

  For information about FPGA Profile, see System Management Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches.
- Configure Security Group ACL Policies as described in How to Configure Security Group ACL Policies

Guidelines and Limitations

- FPGA can support a maximum of 254 entries for an instance.
- Syslog entries for ingress interfaces are empty due to hardware limitations.

The SGACL logging features are available for the following IE3x00 switches running Network Advantage license:

- IE-3400-8P2S
- IE-3400-8T2S
- IE-3400H-8T
- IE-3400H-8FT
- IE-3400H-16T
- IE-3400H-16T
- IE-3400H-24T
- IE-3400H-24FT

The following IEM-3400 Expansion modules can be attached to IE-3400 and provide SGACL logging features:

- IEM-3400-8T
- IEM-3400-8P
- IEM-3400-8S

Note The expansion modules do not have a license. The license installed on base unit covers the expansion module.

Configuring SGACL Logging

To configure SGACL logging:

Step 1 Enter global configuration mode:

Example:

```
Switch# configure terminal
```

Step 2 Use the **cts role-based enforcement** command to globally enable or disable SGACL enforcement for Cisco TrustSec-enabled interfaces in the system.

Step 3 To configure a logging interval for an SGACL, enter:

cts role-based enforcement [logging-interval *interval*]

The valid values for the *interval* argument are from 5 to 86400 seconds. The default is 300 seconds.

Example:

```
Switch(config)# cts role-based enforcement logging-interval 90
```

Step 4 (Optional) Use the **logging rate-limit** command to limit the rate of messages logged per second.

Example:

```
Switch(config)# logging rate-limit <seconds>
```

Example

The following is a sample log, displaying source and destination SGTs. ACE matches for deny action. The **logging rate-limit** command can be used to limit the rate of messages logged per second.

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit 20
May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

Feature History

Feature Name	Release	Feature Information
SGACL Logging	Cisco IOS XE 17.8.1	Initial support on IE3400 and IE3400H