CTS SGACL Support

CTS SGACL support feature provides state-less access control mechanism based on the security association or security group tag value instead of IP addresses.

Prerequisites for CTS SGACL Support

For CTS SGACL support, ensure that Protected Access Credential (PAC) and environmental data download is configured on the device for dynamic SGACL.

Restrictions for CTS SGACL Support

- For the 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
- SGACL enforcement is not supported on management interfaces.
- Dynamic SGACL download size is limited to 6 KB
- There is no validation of SGACL enforcement on Port-Channel interfaces.
- In a VRF aware SGT configuration, Cisco IOS XE Denali 16.3 supports ISE communication though non management VRF interface. ISE communication through management interface is not supported.
- Scale limit of 6 KB is only for dynamic SGACL. Static SGACL can support higher scale like 256*256 matrix.
- SGACL enforcement is by-passed for the IPv6 packets with link-local IPv6 source/destination address.
- The SGACL enforcement for IPv6 multicast traffic is by-passed.

- Starting with Cisco IOS XE Bengaluru 17.4.1, you can configure automated tester to be VRF aware. You can use the **vrf** keyword with the **automate-tester** command to enable automate-tester for a non-default VRF.

Note For VRF aware automate-tester to work, you must configure the **global config ipv4/ipv6 source interface** *interface-name* **vrf** *vrf-name* command.

Information About CTS SGACL Support

CTS SGACL Support

Security group access control lists (SGACLs) is a policy enforcement through which the administrator can control the operations performed by the user based on the security group assignments and destination resources. Policy enforcement within the Cisco Trustsec domain is represented by a permissions matrix, with source security group number on one axis and destination security group number on the other axis. Each cell in the matrix contains an ordered list of SGACLs which specifies the permissions that should be applied to packets originating from an IP belonging to a source security group and having a destination IP that belongs to the destination security group.

SGACL provides state-less access control mechanism based on the security association or security group tag value instead of IP addresses and filters the traffic based on match class. There are three ways to provision the SGACL policy:

- Static policy provisioning - The SGACL policies are defined by the user using the command **cts role-based permission**.
- Dynamic policy provisioning - Configuration of SGACL policies should be done primarily through the policy management function of the Cisco Secure ACS or the Cisco Identity Services Engine - Cisco Identity Services Engine User Guide
- Change of Authorization (CoA) - The updated policy is downloaded when the SGACL policy is modified on the ISE and CoA is pushed to the CTS device.

SGACL Monitor Mode

During the pre-deployment phase of Cisco TrustSec, an administrator will use the monitor mode to test the security policies without enforcing them to make sure that the policies function as intended. If the security policies do not function as intended, the monitor mode provides a convenient mechanism for identifying that and provides an opportunity to correct the policy before enabling SGACL enforcement. This enables administrators to have increased visibility to the outcome of the policy actions before they enforce it, and confirm that the subject policy meets the security requirements (access is denied to resources if users are not authorized).

The monitoring capability is provided at the SGT-DGT pair level. When you enable the SGACL monitoring mode feature, the deny action is implemented as an ACL permit on the line cards. This allows the SGACL counters and logging to display how connections are handled by the SGACL policy. Since all the monitored traffic is permitted, there is no disruption of service due to SGACLs while in the SGACL monitor mode.

How to Configure CTS SGACL Support

Enabling SGACL Policy Enforcement Globally

To enable SGACL policy enforcement on Cisco TrustSec-enabled routed interfaces, perform this task:

```
enable
configure terminal
cts role-based enforcement
```

Enabling SGACL Policy Enforcement Per Interface

You can enable SGACL enforcement globally and disable on a specific interface with **cts role-based enforcement** command. SGACL enforcement can also be enabled on specific interfaces without enabling it globally.

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

```
enable
configure terminal
interface GigabitEthernet 0/1/1
cts role-based enforcement
```

Configuring IPv6 SGACL Access Control Entries

An SGACL is defined similar to the extended named ACL using the following command:

```
Device(config)#ipv6 access-list role-based sgacl1
IPV6 Role-based Access List Configuration commands:
  default   Set a command to its defaults
  deny      Specify packets to reject
  exit      Exit from access-list configuration mode
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  remark    Access list entry comment
  sequence  Sequence number for this entry
```

Attaching SGACLs to Permission Matrix Cell

```
Device(config)#cts role-based permissions from 100 to 200
  WORD  Role-based Access-list name
  ipv4  Protocol Version - IPv4
  ipv6  Protocol Version - IPv6
```

This command defines, replaces, or deletes the list of RBACLs for a given <SGT, DGT> pair. This policy comes into an effect when there is no dynamic policy for the same SGT, DGT. By default, you can attach only an IPv4 type RBACL. To add an IPv6 SGACL, specify **ipv6** explicitly.

Manually Configuring SGACL Policies

To manually configure SGACL policies, perform the following tasks:

```
enable
configure terminal
ip access-list role-based allow_webtraff
10 permit tcp dst eq 80
20 permit tcp dst eq 443
cts role-based permissions from 55 to 66 allow_webtraff
end
```

Configuring Enhanced SGACL Logging

Starting from Cisco IOS XE Catalyst Routing Release 17.15.1a, SGACL logging uses the HSL capability for Cisco IOS XE Catalyst Routing devices. SGACL logging through HSL provides a logging method for security events that is more efficient and capable of scaling, which is useful in network environments experiencing high volumes of traffic.

This section provides sample CLI configurations to configure enhanced SGACL logging.

Enable SGACL logging for IPv4 traffic.

```
cts role-based sgt-map SGT value
cts role-based enforcement
cts role-based permissions from source-sgt to dest-sgt role-based_access_list_name

ip access-list access-list role_based_access_list_name
         sequence_number permit tcp log-input
         sequence_number permit icmp
         sequence_number permit ip
```

Enable SGACL logging for IPv6 traffic.

```
cts role-based sgt-map SGT value
cts role-based enforcement
cts role-based permissions from source-sgt to dest-sgt role-based_access_list_name

ipv6 role-based_access_list_name
        sequence sequence_number permit udp log
        sequence sequence_number permit tcp
```

Verify Enhanced SGACL Logging

The following is a sample output from the **show platform hardware qfp active feature acl dp hsl configuration** command. This output displays the configuration for SGACL HSL as set up on the device.

```
Device# show platform hardware qfp active feature acl dp hsl configuration
ACL DP HSL Config:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
SGACL HSL Setup:
Handle Session/Instance: 127/63
Version: 9
Dest Type: 3
HSL Enable: TRUE
HSL BackPressure Enable: FALSE
Base Memory Addr: <0xpXXXX>
Memory Size (bytes): 147560
Max Records: 1024
```

```
Record Threshold: 256
Memory Threshold (bytes): 32768
Record Timeout (ms): 512
Export Timeout (ms): 4
MTU Size (bytes): 1450
Template Refresh Timer: 0
Template Refresh Packets: 0
Source Id: 0x404”
Max Record Size (bytes): 104
```

The following is a sample output from the show platform hardware qfp active feature acl control command. This output displays whether SGACL logging is enabled or disabled. In this example, SGACL logging is enabled.

```
Device# show platform hardware qfp active feature acl control
Stats Poll Period: 0
Stats Entry Size: 16
Ha Init: 1
Fm Ready: 0
IPv4 Logging Threshold: 2147483647
IPv4 Logging Interval: 0
IPv6 Logging Threshold: 350000
IPv6 Logging Interval: 0
Maximum Aces Per Acl: 256000
Stats Update size: 180
Maximum Entries: 0
Maximum Entries per Classifier: 0
Result Bit Size: 0
Result Start Bit Pos: 0
Maximum Profiles: 0
Maximum Blocks per Profile: 0
Device Select: 0
Maximum Tree Depth: 0
Verify Enhanced SGACL Logging
Dimention: 0
Number Cuts: 0
HSL Support: TRUE // sgacl hsl logging is enabled
HSL Force Disable: FALSE
```

The following is a sample output from the show platform hardware qfp active feature acl dp hsl statistics command. In this example, the output displays the logging statistics for SGACL HSL from the device.

```
Device# show platform hardware qfp active feature acl dp hsl statistics
Router#show platform hardware qfp active feature acl dp hsl statistic
ACL DP HSL Statistics:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
SGACL Export Statistics
-----------------------
Records sent (to HSL): 2
Records dropped (before HSL): 0
Record alloc failures: 0
Records dropped flag: Off
Records sent (by HSL): 0
Records dropped (by HSL): 0
HSL packets dropped flag: Off
HSL buffer flow-on (count): 0
SGACL HSL Statistics
--------------------
Records exported: 2
Packets exported: 2
Bytes exported: 168
Dropped records: 0
```

```
Dropped packets (inc. Punt drops): 0
Dropped bytes: 0
```

Refreshing the Downloaded SGACL Policies

To refresh the downloaded SGACL policies, perform the following task:

```
enable
cts refresh policy
```

Or

```
enable
cts refresh policy sgt 10
```

Configuring SGACL Monitor Mode

Before configuring SGACL monitor mode, ensure that Cisco TrustSec is enabled.

Note The device level monitor mode is not enabled by default unless any one of the configurations are applied. In case of SGACL's downloaded from ISE, the monitor mode state from ISE takes precedence always. This is applicable for both per-cell monitor mode or global monitor mode which is applicable for all cell.

```
configure terminal
cts role-based monitor enable
cts role-based monitor permissions from 2 to 3 ipv4
show cts role-based permissions from 2 to 3 ipv4
show cts role-based counters ipv4
```

Configuring IPv6 SGACL ACE

The following CLI is used to define Access Control Entries (ACEs) of an IPv6 SGACL.

```
Device(config)#ipv6 access-list role-based sgacl1
Device(config-ipv6rb-acl)#permit ipv6
Device(config-ipv6rb-acl)#exit
Device(config)#cts role-based permissions from 100 to 200 ipv6 sgacl1
```

Note IPv6 ACL configuration is for static SGACL whereas for dynamic SGACL, ACEs are configured on the ISE.

Configuration Examples for CTS SGACL Support

Example: CTS SGACL Support

The following is a sample output of the show cts role-based permissions command.

```
Router# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-02
        Permit IP-00
IPv4 Role-based permissions from group 55:SGT_55 to group 66:SGT_66 (configured):
        allow_webtraff
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE



Router#sh cts role-based permissions ipv6
IPv6 Role-based permissions from group 2103:Cisco_UC_Servers to group 2104:Exchange_Servers:

        SGACL_5-10-ipv6
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

The following is a sample output, applicable only to dynamic SGACL, of the show cts policy sgt command.

```
Router# show cts policy sgt

CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0xc1408801
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-46:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = default_sgacl-02
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
```

```
  RBACL ACEs:
    permit icmp
    permit ip
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 2
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE
```

The following is a sample output, applicable only to dynamic SGACL, of the show cts rbacl command.

```
Router# show cts rbacl

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =multple_ace-16
  IP protocol version = IPV4
  refcnt = 4
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      deny tcp

  name   =default_sgacl-02
  IP protocol version = IPV4
  refcnt = 2
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      permit ip

  name   =SGACL_256_ACE-71
  IP protocol version = IPV4
```

Example: Configuring SGACL Monitor Mode

The following is a sample configuration example for SGACL Monitor Mode:

```
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 permissions ipv6
IPv6 Role-based permissions from group 201 to group 22 (configured):
        g6
IPv6 Role-based permissions from group 100 to group 200 (configured):
        sgacl1
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

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
100     200     0          0          0          0          0          0
101     201     0          0          0          0          0          0

Device# show cts role-based counters ipv6
Role-based IPv6 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
201     22      0          0          0          0          0          0
100     200     0          0          0          0          0          0
```

Example: Refreshing the Downloaded SGACL Policies

The following is a sample configuration example for refreshing the downloaded SGACL policies. The command is run in a privileged EXEC mode.

```
Router#cts refresh policy
Router#cts refresh policy sgt
```

Additional References for CTS SGACL Support

Related Documents

MIBs

MIB	MIBs Link
CISCO-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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/cisco/web/support/index.html

Feature Information for CTS SGACL Support

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 CTS SGACL Support

Feature Name	Releases	Feature Information
CTS SGACL Support	Cisco IOS Release 16.3	The CTS SGACL Support feature provides state-less access control mechanism based on the security association or security group tag value instead of IP addresses. In Cisco IOS Release 16.3, this feature was introduced for Cisco Aggregation Service Router 1000 series and Integrated Services Router 4000 series. The following commands were introduced by this feature: **cts role-based enforcement, ip access-list role-based, cts role-based permissions, show cts role-based permissions, show cts rbacl**.
TrustSec SGACL Monitor Mode	Cisco IOS XE Everest 16.4.1	TrustSec SGACL Monitor Mode feature monitors the security policies without enforcing that the policies function as intended. The monitor mode provides a convenient mechanism for identifying the security policies that do not function and provide an opportunity to correct the policy before enabling SGACL enforcement. The following commands were introduced by this feature: **cts role-based monitor enable, cts role-based monitor permissions**.
IPv6 enablement - SGACL Enforcement	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.
Enhanced SGACL Logging	Cisco IOS XE 17.15.1a	This feature enhances the Security Group Access Control List (SGACL) logging capability by using High Speed Logging (HSL) for Cisco IOS XE catalyst routing devices. SGACL logging through HSL provides a logging method for security events that is more efficient and capable of scaling, particularly useful in network environments experiencing high volumes of traffic.