Enablement of Security Group ACL at Interface Level

The Enablement of Security Group ACL at Interface Level feature controls and manages the Cisco TrustSec access control on a network device based on an attribute-based access control list. When a security group access control list (SGACL) is enabled globally, the SGACL is enabled on all interfaces in the network by default; use the Enablement of Security Group ACL at Interface Level feature to disable the SGACL on a Layer 3 interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Restrictions for Enablement of Security Group ACL at Interface Level

- The Enablement of Security Group ACL at Interface Level feature is effective only if the security group access control list (SGACL) enforcement is enabled globally.
- Disabling per-interface SGACL enforcement also disables Security Group Tag (SGT) caching on the specific interface.
- Per-interface SGACL enforcement is not supported on Layer 3 port channel interfaces.
- Per-interface SGACL enforcement is not supported on Layer 2 interfaces.

Information About Enablement of Security Group ACL at Interface Level

Security Group ACL Overview

The attribute-based access control list organizes and manages the Cisco TrustSec access control on a network device. The security group access control list (SGACL) is a Layer 3-4 access control list to filter access based on the value of the security group tag (SGT). The filtering usually occurs at an egress port of the Cisco TrustSec domain. SGT is a Layer 2 tag that is used to classify traffic based on role, and SGT tagging occurs at ingress of the CTS domain.

The terms role-based ACL (RBACL) and SGACL can be used interchangeably, and they refer to a topology-independent ACL used in an attribute-based access control (ABAC) policy model. ABAC is an access control mechanism that uses subject attributes, resource attributes, and environment attributes.

- Subject attributes (S) are associated with a subject—be it a user or an application—that defines the identity and characteristics of that subject.
- Resource attributes (R) are associated with a resource, such as a web service, a system function, or data.
- Environment attributes (E) describe the operational, technical, or situational environment or context in which information is accessed.

ABAC policy rules are generated as Boolean functions of S, R, and E attributes, and these rules decide whether a subject S can access a resource R in a particular environment E. Access control policy is defined between security groups and consists of traditional security ACLs but without IP source and destination addresses.

Because networks are bidirectional, access control is applied both between the subject (user) and the object (resource or server) and between the object and the subject. This requires the subjects to be grouped together into security groups and the objects to be likewise grouped together into security groups. Rules based on subject and object attributes group the subjects and objects into security groups.

Once SGACL is enabled globally, it is automatically enabled on every Layer 3 interface on the device, and you can disable SGACL on specific Layer 3 interfaces. Granular disablement at interface level is effective

only if SGACL is enabled globally. This feature is applicable even if packets sent or received are not tagged with SGT at the source device of the packet.

Enabling or disabling per-interface SGACL enforcement enables or disables SGACL monitor mode on that interface.

Guidelines to Configure Security Group ACL

The security group access control list (SGACL) can be configured by the administrator in Cisco Identity Service Engine (ISE) or in Cisco Secure Access Control System (ACS).

You can also configure the SGACL in the device using the **ip access-list role-based** *sgacl-name* command in global configuration mode. Use the **show cts role-based permissions** command or the **show cts rbacl** command in privileged EXEC mode to view the SGACLs configured on the device. For more information about the security commands, see the *Cisco IOS Security Command Reference*.

Note Ensure that the SGACL name begins with an alphabetic character to prevent ambiguity with numbered access lists. These names cannot contain a space or quotation mark.

How to Configure Security Group ACL at Interface Level

Configuring Security Group ACL at Interface Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **cts role-based enforcement**
5. **end**
6. **show running-config interface** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 2/5/3`	Enters interface configuration mode.
Step 4	**cts role-based enforcement** **Example:** `Device(config-if)# cts role-based enforcement`	Enables a security group access control list (SGACL) for the interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show running-config interface** *type number* **Example:** `Device# show running-config interface gigabitethernet 2/5/3`	Displays whether the SGACL is disabled on a specific interface.

Configuration Examples for Enablement of Security Group ACL at Interface Level

Example: Configuring Security Group ACL at Interface Level

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

Example: Verifying Security Group ACL at Interface Level

```
Device# show running-config interface gigabitethernet 2/5/3

Building configuration...

Current configuration : 175 bytes
!
interface GigabitEthernet2/5/3
no switchport
ip address 192.0.2.2 255.255.255.0
```

```
load-interval 30
ipv6 address 2001:DB8::1
ipv6 enable
no cts role-based enforcement
end
```

Note The **no cts role-based enforcement** line in the command output indicates that the security group access control list (SGACL) is disabled at the interface level.

Additional References for Enablement of Security Group ACL at Interface Level

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cisco TrustSec switches	*Cisco TrustSec Switch Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Enablement of Security Group ACL at Interface Level

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 . An account on Cisco.com is not required.

Table 1: Feature Information for Enablement of Security Group ACL at Interface Level

Feature Name	Releases	Feature Information
Enablement of Security Group ACL at Interface Level	Cisco IOS XE 3.6E	The Enablement of Security Group ACL at Interface Level feature controls and manages the Cisco TrustSec access control on a network device based on an attribute-based access control policy. This feature provides the flexibility of enabling and disabling a security group access control list (SGACL) on specific Layer 3 interfaces with assigned security groups. In Cisco IOS XE Release 3.6E, this feature is supported on the following platforms: • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X Series Switches • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 3650 Series Switches The following command was introduced: **cts role-based enforcement**.