Configuring Cisco Security Group Access Policies

This chapter describes how to configure a Cisco Identity Services Engine (Cisco ISE) node as an authentication server, using Security Group Access (SGA) policies. This requires a Cisco SGA solution-enabled network.

This chapter contains the following topics:

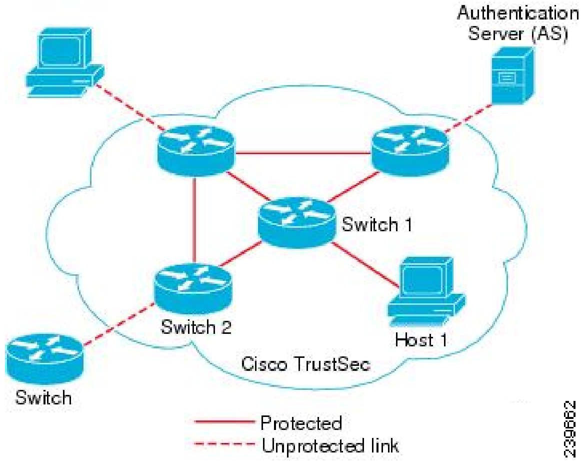
Security Group Access Architecture

The Cisco Security Group Access (SGA) solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco SGA cloud is authenticated by its neighbors (peers). Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. The SGA solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the SGA network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

You need an Advanced License Package for Cisco ISE to enable SGA services.

Figure 24-1 shows an example of an SGA network cloud.

Figure 24-1 SGA Architecture



Related Topics

- http://www.cisco.com/en/US/netsol/ns1051/index.html
- SGA Features, page 24-2
- SGA Terminology, page 24-3
- Supported Switches for SGA, page 24-4
- Components Required for SGA, page 24-5

SGA Features

The key features of the SGA solution include:

- Network Device Admission Control (NDAC)—In a trusted network, during authentication, each network device (for example Ethernet switch) in an SGA cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1x port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its Extensible Authentication Protocol (EAP) method. Successful authentication and authorization in the NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
- Endpoint Admission Control (EAC)—An authentication process for an endpoint user or a device connecting to the SGA cloud. EAC typically happens at the access level switch. Successful authentication and authorization in EAC process results in SGT assignment to the user or device. EAC access methods for authentication and authorization includes:
  - 802.1X port-based authentication
  - MAC authentication bypass (MAB)
  - Web authentication (WebAuth)
- Security Group (SG)—A grouping of users, endpoint devices, and resources that share access control policies. SGs are defined by the administrator in Cisco ISE. As new users and devices are added to the SGA domain, Cisco ISE assigns these new entities to the appropriate security groups.

- Security Group Tag (SGT)—SGA service assigns to each security group a unique 16-bit security group number whose scope is global within an SGA domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers. They are automatically generated, but you have the option to reserve a range of SGTs for IP-to-SGT mapping.
- Security Group Access Control List (SGACL)—SGACLs allow you to control the access and permissions based on the SGTs that are assigned. The grouping of permissions into a role simplifies the management of security policy. As you add devices, you simply assign one or more security groups, and they immediately receive the appropriate permissions. You can modify the security groups to introduce new privileges or restrict current permissions.
- Security Exchange Protocol (SXP)—SGT Exchange Protocol (SXP) is a protocol developed for SGA service to propagate the IP-to-SGT binding table across network devices that do not have SGT-capable hardware support to hardware that supports SGT/SGACL.
- Environment Data Download—The SGA device obtains its environment data from Cisco ISE when it first joins a trusted network. You can also manually configure some of the data on the device. The device must refresh the environment data before it expires. The SGA device obtains the following environment data from Cisco ISE:
  - Server lists—List of servers that the client can use for future RADIUS requests (for both authentication and authorization)
  - Device SG—Security group to which the device itself belongs
  - Expiry timeout—Interval that controls how often the SGA device should download or refresh its environment data
- SGT Reservation—An enhancement in Cisco ISE to reserve a range of SGTs to enable IP to SGT mapping.
- IP-to-SGT Mapping—An enhancement in Cisco ISE to bind an endpoint IP to an SGT and provision it to an SGA-capable device. Cisco ISE, Release 1.2 supports entering 1000 IP-to-SGT Mappings.
- Identity-to-Port Mapping—A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco ISE server.

SGA Terminology

Table 24-1 lists some of the common terms that are used in the SGA solution and their meaning in an SGA environment.

Table 24-1 SGA Terminology

Term	Meaning
Supplicant	A device that tries to join a trusted network.
Authentication	The process of verifying the identity of each device before allowing it to be part of the trusted network.
Authorization	The process of deciding the level of access to a device that requests access to a resource on a trusted network based on the authenticated identity of the device.
Access control	The process of applying access control on a per-packet basis based on the SGT that is assigned to each packet.

Table 24-1 SGA Terminology (continued)

Term	Meaning
Secure communication	The process of encryption, integrity, and data-path replay protection for securing the packets that flow over each link in a trusted network.
SGA device	Any of the Cisco Catalyst 6000 Series or Cisco Nexus 7000 Series switches that support the SGA solution.
SGA-capable device	An SGA-capable device will have SGA-capable hardware and software. For example, the Nexus 7000 Series Switches with the Nexus operating system.
SGA seed device	The SGA device that authenticates directly against the Cisco ISE server. It acts as both the authenticator and supplicant.
Ingress	When packets first encounter an SGA-capable device that is part of a network where the Cisco SGA solution is enabled, they are tagged with an SGT. This point of entry into the trusted network is called the ingress.
Egress	When packets pass the last SGA-capable device that is part of a network where the Cisco SGA solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

Supported Switches for SGA

To set up a Cisco ISE network that is enabled with the Cisco SGA solution, you need switches that support the SGA solution and other components. Table 24-2 lists the supported Cisco switch platforms.

Table 24-2 Supported Switches

Supported Cisco Switch Platforms		
Platform	**Operating System Version**	**Requirement**
Cisco Nexus 7000 Series	Cisco Nexus operating system, Release 5.0.2a. **Note** You would need Advanced Service Package license for Cisco SGA.	Mandatory as enforcement point
Cisco Catalyst 6500E Switch with Supervisor Engine 32 or 720 or Virtual Switching System (VSS) 720	Cisco IOS Software, Release 12.2(33) SXI3 or later	Optional as an access switch
Cisco Catalyst 4900 Series Switch	Cisco IOS Software, Release 2.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 4500E Switch with Supervisor 6L-E or 6-E	Cisco IOS Software, Release 12.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 3750-X or 3560-X Series Switches	Cisco IOS Software, Release 12.2(53) SE1 or later	Optional as an access switch

Table 24-2 Supported Switches

Supported Cisco Switch Platforms		
Cisco Catalyst 3750 or 3560 Series Switches	Cisco IOS Software, Release 12.2(53) SE1 or later	Optional as an access switch
Cisco Catalyst Blade Switch 3000 or 3100 Series	Cisco IOS Software, Release 12.2(53) SE1 or later	Optional as an access switch

Components Required for SGA

Apart from the switches listed in Table 24-2, you need other components for identity-based user access control using the IEEE 802.1X protocol. These include Microsoft Windows 2003 or 2008 Server running Microsoft Active Directory, certificate authority (CA) server, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server. An end host running the Microsoft Windows operating system can also be a part of this environment. Table 24-3 lists other components that may be required for your Cisco SGA environment.

Table 24-3 Components

Component	Description
User Identity Repository	Although you can use the Cisco ISE internal user database, we recommend that you use an external database for identity authentication. Cisco ISE supports connections to Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) service
DHCP Service	Any DHCP server that provides DHCP service. For example, Microsoft Windows Server 2008 DHCP server
DNS Service	Any DNS server that provides DNS service. For example, Microsoft Windows Server 2008 DNS server
Certificate Authority Server	Any certificate authority server that provides standalone CA service. For example, Microsoft Windows Server 2008 CA server
Target Servers	Servers that provide Internet services such as HTTP, FTP, Secure Shell (SSH), and even file sharing to test the SGACLs
Endpoint PC	SGA is a supplicant-agnostic solution and does not require any specific agent or IEEE 802.1X supplicant running on the endpoint PC. You can use the Cisco Secure Services Client supplicant, Microsoft Windows or another operating system-embedded supplicant, or other third-party supplicant

To enable Cisco ISE to interoperate with SGA deployments, you must configure SGA switch ports on your switches.

Related Topics

"Enable Cisco Security Group Access Switch Ports" section on page F-6

Enable SGA Solution

This section describes the tasks that you must perform to enable the SGA solution in your Cisco ISE network.

This section contains the following:

Configure SGA Settings on the Switches

To enable Cisco ISE to interoperate with SGA deployments, you must configure SGA switch ports on your switches. See "Enable Cisco Security Group Access Switch Ports" section on page F-6 for more information.

In addition to configuring SGA settings on Cisco ISE, you must also configure some settings on the SGA devices. These configurations vary for the Catalyst and Nexus switches and are described in the Catalyst and Nexus switch configuration guides that are available at the following URLs:

- For Catalyst 6500 Series Switches:
  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html
- For Nexus 7000 Series Switches:

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5.x.html
- Configuration Example Using Nexus 7000 Series Switches:

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/configuration_examples/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Configuration_Examples_Release_5.x_chapter4.html#con_1191129

Configuring SGA Devices

For Cisco ISE to process requests from SGA-enabled devices, you must define these SGA-enabled devices in Cisco ISE.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > Network Resources > Network Devices > Network Devices**.

Step 2 Add a network device to the deployment.

Step 3 Click **Submit** to save the SGA device definition.

What To Do Next

- Configuring Security Group Access Settings, page 24-7

Related Topics

- Network Device Definition Settings, page A-36
- SGA Device Attribute Settings, page A-39
- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Configuring Security Group Access Settings

For Cisco ISE to function as an SGA server and provide SGA services, you must define some global SGA settings.

Before You Begin

- Before you configure global SGA settings, ensure that you have defined global EAP-FAST settings (choose **Administration > System > Global Options > Protocol Settings > EAP-FAST > EAP-FAST Settings**).

  You must change the Authority Identity Info Description to your Cisco ISE server name. This description is a user-friendly string that describes the Cisco ISE server that sends credentials to an endpoint client. The client in a Cisco SGA architecture can be either the endpoint running EAP-FAST as its EAP method for IEEE 802.1X authentication or the supplicant network device performing NDAC. The client can discover this string in the protected access credentials (PAC) type-length-value (TLV) information. The default value is Cisco Identity Services Engine. You should change the value so that the Cisco ISE PAC information can be uniquely identified on network devices upon NDAC authentication.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > System > Settings > Security Group Access**.

Step 2 Enter the values in the fields.

Step 3 Click **Save**.

What To Do Next

- Configuring Security Group Access AAA Servers, page 24-8

Related Topics

- Map Security Groups to Devices, page 24-11
- Security Group Access Settings, page A-24
- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Configuring Security Group Access AAA Servers

You can configure a list of Cisco ISE servers in your deployment in the AAA server list to allow SGA devices to be authenticated against any of these servers. When you add Cisco ISE servers to this list, all these server details are downloaded to the SGA device. When an SGA device tries to authenticate, it chooses any Cisco ISE server from this list and, if the first server is down or busy, the SGA device can authenticate itself against any of the other servers from this list. By default, the primary Cisco ISE server is an SGA AAA server. We recommend that you configure additional Cisco ISE servers in this AAA server list so that if one server is busy, another server from this list can handle the SGA request.

This page lists the Cisco ISE servers in your deployment that you have configured as your SGA AAA servers.

You can click the **Push** button to initiate an environment CoA notification after you configure multiple SGA AAA servers. This environment CoA notification goes to all SGA network devices and provides an update of all SGA AAA servers that were changed.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > Network Resources > SGA AAA Servers**.

Step 2 Click **Add**.

Step 3 Enter the values as described:

- Name—Name that you want to assign to the Cisco ISE server in this AAA Server list. This name can be different from the hostname of the Cisco ISE server.
- Description—An optional description.
- IP—IP address of the Cisco ISE server that you are adding to the AAA Server list.
- Port—Port over which communication between the SGA device and server should take place. The default is 1812.

Step 4 Click **Submit**.

What To Do Next

Configure Security Groups, page 24-8

Related Topics

Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Configure Security Groups

A security Group (SG) or Security Group Tag (SGT) is an element that is used in SGA policy configuration. SGTs are attached to packets when they move within a trusted network. These packets are tagged when they enter a trusted network (ingress) and untagged when they leave the trusted network (egress).

SGTs are automatically generated in a sequential manner, but you have the option to reserve a range of SGTs for IP to SGT mapping. Cisco ISE skips the reserved numbers while generating SGTs.

If you have deleted a particular security group, the SGT assigned to this security group does not get reused until all the succeeding SGTs are deleted.

For example, if you have SGTs 2, 3, and 4 defined and you delete SGT 2, the next SGT that is generated would be SGT 5. If you want SGT 2 to be generated next, you must delete SGTs 3 and 4.

SGA service uses these SGTs to enforce the SGA policy at egress.

You can configure security groups from the following pages in the Admin portal:

- **Policy > Policy Elements > Results > Security Group Access > Security Groups**. See "Adding Security Groups" section on page 24-9.
- Directly from egress policy page. See "Configuring SGT from Egress Policy" section on page 24-16.
- Clicking the **Generate SGTs** button on the **Policy > Policy Elements > Results > Security Group Access > Security Groups** page. See "Adding Security Groups" section on page 24-9.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGTs. This environment CoA notification goes to all SGA network devices and provides an update of all SGTs that were changed.

Related Topics

- Adding Security Groups, page 24-9
- Configuring SGA Policy by Assigning SGTs to Devices, page 24-12

Adding Security Groups

Each security group in your SGA solution should be assigned a unique SGT. Even though Cisco ISE supports 65,535 SGTs, having fewer number of SGTs would enable you to deploy and manage the SGA solution easily. We recommend a maximum of 64000 SGTs.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy > Policy Elements > Results > Security Group Access > Security Groups**.

Step 2 Click **Add** to add a new security group.

Step 3 Enter the values in the fields.

Step 4 Click **Save** to save the security group.

What To Do Next

- Configure Security Group Access Control Lists, page 24-10
- Assigning Security Groups to Users and Endpoints, page 24-13

Related Topics

Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Configure Security Group Access Control Lists

Security group access control lists (SGACLs) are permissions that will be assigned after the SGA policy evaluation. SGACLs restrict the operations that a user can perform based on the role of the user instead of the IP address or subnet mask alone. You can configure SGACLs from the Admin portal.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGACLs. This environment CoA notification goes to all SGA network devices and provides an update of all SGACLs that were changed.

Related Topics

- Adding Security Group Access Control Lists, page 24-10
- Configuring SGT from Egress Policy, page 24-16

Adding Security Group Access Control Lists

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy > Policy Elements > Results** > **Security Group Access > Security Group ACLs**.

Step 2 Enter the following information:

- Name—Name of the SGACL
- Description—An optional description of the SGACL
- IP Version—IP version that this SGACL supports:
  - IPv4—Supports IP version 4 (IPv4)
  - IPv6—Supports IP version 6 (IPv6)
  - Agnostic—Supports both IPv4 and IPv6
- Security Group ACL Content—Access control list (ACL) commands. For example:

  permit icmp

  deny all

Step 3 Click **Submit**.

Access Control List Entries for Nexus 7000 Series

The Nexus 7000 Series with Cisco Nexus operating system 4.2 supports the following access control list entries:

deny all

deny icmp

deny igmp

deny ip

deny tcp [{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

deny udp[{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

permit all

permit icmp

permit igmp

permit ip

permit tcp [{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

permit udp[{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

When you change SGACL ACE, SGACL name, or IP version of an SGACL, all the accumulative changes can be pushed to the SGA network devices by clicking the **Push** button.

What To Do Next

Configuring SGA Policy by Assigning SGTs to Devices, page 24-12

Related Topics

- http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/command/reference/sec_cmds_d.html#wp1057446
- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Update RBACL Named List CoA, page 24-24

Map Security Groups to Devices

Cisco ISE allows you to assign an SGT to an SGA device if you know the device hostname or IP address. When a device with the specific hostname or IP address joins the network, Cisco ISE will assign the SGT before authenticating it. You can create this mapping from the Security Group Mappings page. Before you perform this action, ensure that you have reserved a range of SGTs. You can map the security groups to devices from the Admin portal.

Related Topics

- Adding Security Group Mappings, page 24-11
- Configuring Security Group Access Settings, page 24-7

Adding Security Group Mappings

You can add security group mappings from the Admin portal.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy > Policy Elements > Results > Security Group Mappings**.

Step 2 Click **Add** to add a new security group mapping.

Step 3 Enter the values in the fields.

Step 4 Check the check box next to an existing security group mapping that you want to reassign, and then click **Reassign Groups**.

Step 5 Check the check box next to an existing security group mapping that you want to deploy, and then click **Deploy**.

Step 6 Check the check box next to an existing security group mapping whose status you want to check, then choose **>>** and click **Check Status**.

Step 7 Click **Submit**.

Related Topics

Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Configuring SGA Policy by Assigning SGTs to Devices

You can configure the SGA policy by assigning SGTs to devices. You can assign security groups to devices by using the SGA device ID.

Before You Begin

- Ensure that you create the security groups for use in the policy. See "Configure Security Groups" section on page 24-8 for more information.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy > Security Group Access > Network Device Authorization**.

Step 2 Click the Action icon in the Default Rule row, and click **Insert New Row Above**.

Step 3 Enter the name for this rule.

Step 4 Click the plus sign (+) next to **Conditions** to add a policy condition.

Step 5 You can click **Create New Condition (Advance Option)** and create a new condition.

Step 6 From the **Security Group** drop-down list, select the SGT that you want to assign if this condition evaluates to true.

Step 7 Click the Action icon from this row to add additional rules based on device attributes either above or below the current rule. You can repeat this process to create all the rules that you need for the SGA policy. You can drag and drop the rules to reorder them by clicking the ⠿ icon. You can also duplicate an existing condition, but ensure that you change the policy name.

The first rule that evaluates to true determines the result of the evaluation. If none of the rules match, the default rule will be applied; you can edit the default rule to specify the SGT that must be applied to the device if none of the rules match.

Step 8 Click **Save** to save your SGA policy.

If an SGA device tries to authenticate after you have configured the network device policy, the device will get its SGT and the SGT of its peers and will be able to download all the relevant details.

Related Topics

Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Assigning Security Groups to Users and Endpoints

Cisco ISE allows you to assign a security group as the result of an authorization policy evaluation. Using this option, you can assign a security group to users and end points.

Before You Begin

- Read the "Cisco ISE Authorization Policies" section on page 20-1 for information on authorization policies.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Authorization** > **Standard**.

Step 2 Create a new authorization policy.

Step 3 For Permissions, instead of selecting an authorization profile, select a security group.

If the conditions specified in this authorization policy is true for a user or endpoint, then this security group will be assigned to that user or endpoint and all data packets that are sent by this user or endpoint will be tagged with this particular SGT.

Related Topics

- Configuring Authorization Policies, page 20-8
- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Egress Policy

The egress table lists the source and destination SGTs, both reserved and unreserved. This page also allows you to filter the egress table to view specific policies and also to save custom views. When the source SGT tries to reach the destination SGT, the SGA-capable device enforces the SGACLs based on the SGA policy as defined in the Egress Policy. Cisco ISE creates and provisions the policy.

After you create the SGTs and SGACLs, which are the basic building blocks required to create an SGA policy, you can establish a relationship between them by assigning SGACLs to source and destination SGTs.

Each combination of a source SGT to a destination SGT is a cell in the egress policy.

This section contains the following:

- View the Egress Policy, page 24-14
- Matrix Operations, page 24-15
- Configure Egress Policy Table Cells, page 24-15
- Configuring SGT from Egress Policy, page 24-16
- The Unknown Security Group, page 24-18

Related Topics

- Configure Security Groups, page 24-8
- Configure Security Group Access Control Lists, page 24-10

View the Egress Policy

You can view the Egress Policy in the **Policy** > **Security Group Access** > **Egress Policy** page.

You can view the Egress policy in three different ways:

- Source Tree, page 24-14
- Destination Tree, page 24-14
- Matrix View, page 24-14

Source Tree

The Source Tree view lists a compact and organized view of source SGTs in a collapsed state. You can expand any source SGT to see the internal table that lists all information related to that selected source SGT. This view displays only the source SGTs that are mapped to destination SGTs. If you expand a specific source SGT, it lists all destination SGTs that are mapped to this source SGT and their configurations in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Destination Tree

The Destination Tree view lists a compact and organized view of destination SGTs in a collapsed state. You can expand any destination SGTs to see the internal table that lists all information related to that selected destination SGT. This view displays only the destination SGTs that are mapped to source SGTs. If you expand a specific destination SGT, it lists all source SGTs that are mapped to this destination SGT and their configurations in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Matrix View

The Matrix View of the Egress policy looks like a spreadsheet. It contains two axis:

- Source Axis—The vertical axis lists all the source SGTs.
- Destination Axis—The horizontal axis lists all the destination SGTs.

The mapping of a source SGT to a destination SGT is represented as a cell. If a cell contains data, then it represents that there is a mapping between the corresponding source SGT and the destination SGT. There are two types of cells in the matrix view:

- Mapped cells—When a source and destination pair of SGTs is related to a set of ordered SGACLs and has a specified status.
- Unmapped cells—When a source and destination pair of SGTs is not related to any SGACLs and has no specified status.

The Egress Policy cell displays the source SGT, the destination SGT, and the Final Catch All Rule as a single list under SGACLs, separated by commas. The Final Catch All Rule is not displayed if it is set to None. An empty cell in a matrix represents an unmapped cell.

In the Egress Policy matrix view, you can scroll across the matrix to view the required set of cells. The browser does not load the entire matrix data at once. The browser requests the server for the data that falls in the area you are scrolling in. This prevents memory overflow and performance issues.

Related Topics

Matrix Operations, page 24-15

Matrix Operations

The Matrix view in Cisco ISE looks similar to a spreadsheet. It has source SGT as a row title and destination SGT as a column title. A cell is a crossing of source and destination SGTs. The cell in the matrix view contains the configuration information of source and destination pair to SGACLs. The Matrix view does not display all the fields in order to save the cell area.

Navigating through the Matrix

You can navigate through the matrix either by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can click and hold on a cell to drag it along with the entire matrix content in any direction. The source and destination bar moves along with the cells. The matrix view highlights the cell and the corresponding row (Source SGT) and column (Destination SGT) when a cell is selected. The coordinates (Source SGT and Destination SGT) of the selected cell are displayed below the matrix content area.

Selecting a Cell in the Matrix

To select a cell in the matrix view, click on it. The selected cell is displayed in different color, and the source and destination SGTs are highlighted. You can deselect a cell either by clicking it again or by selecting another cell. Multiple cell selection is not allowed in the matrix view. Double-click the cell to edit the cell configuration.

Configure Egress Policy Table Cells

Cisco ISE allows you to configure cells using various options that are available in the tool bar. Cisco ISE does not allow a cell configuration if the selected source and destination SGTs are identical to a mapped cell.

This section contains:

- Adding the Mapping of Egress Policy Cells, page 24-15
- Configuring SGT from Egress Policy, page 24-16

Adding the Mapping of Egress Policy Cells

You can add the mapping cell for Egress Policy from the Policy page.

Step 1 Choose **Policy** > **Security Group Access** > **Egress Policy**

Step 2 Click the appropriate view tab to see the matrix cells.

Step 3 To select the matrix cells, do the following:

- In the matrix view, click a cell to select it.
- In the Source and Destination tree view, check the check box of a row in the internal table to select it.

Step 4 Click **Add** to add a new mapping cell

Step 5 Select appropriate values for:

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

Step 6 Click **Submit** to save the configuration.

Configuring SGT from Egress Policy

You can create Security Groups directly from the Egress Policy page.

Step 1 Choose **Policy** > **Security Group Access** > **Egress Policy**.

Step 2 Choose **Create Security Group** from the Configure option drop-down list.

Step 3 Create a Security Group.

Related Topics

Configure Security Groups, page 24-8

Configuring SGACL from Egress Policy

You can create Security Group ACLs directly from the Egress Policy page.

Step 1 Choose **Policy** > **Security Group Access** > **Egress Policy**.

Step 2 Choose **Create Security Group ACLs** from the Configure option drop-down list.

Step 3 Create a Security Group ACLs.

Related Topics

Configure Security Group Access Control Lists, page 24-10

Push Button

The Push option in the egress policy initiates a CoA notification that calls the SGA devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy.

Related Topics

Update SGT Matrix CoA, page 24-25

Monitor Mode

The Monitor All option in the egress policy allows you to change the entire egress policy configuration status to monitor mode with a single click. Check the **Monitor All** check box in the egress policy page to change the egress policy configuration status of all the cells to monitor mode. When you check the Monitor All check box, the following changes take place in the configuration status:

- The cells whose status is Enabled will act as monitored but appears as if they are enabled.
- The cells whose status is Disable will not be affected.
- The cells whose status is Monitor will remain Monitored.

Uncheck the Monitor All check box to restore the original configuration status. It does not change the actual status of the cell in the database. When you deselect Monitor All, each cell in the egress policy regains its original configuration status.

Features of Monitor Mode

The monitoring functionality of the monitor mode helps you to:

- Know how much traffic is filtered but monitored by the monitor mode
- Know that SGT-DGT pair is in monitor mode or enforce mode, and observe if there is any unusual packet drop is happening in the network
- Understand that SGACL drop is actually enforced by enforce mode or permitted by monitor mode
- Create custom reports based on the type of mode (monitor, enforce, or both)
- Identify which SGACL has been applied on NAD and display discrepancy, if any

Related Topics

- Running Top N RBACL Drops by User
- Chapter 26, “Reporting.”

Running Top N RBACL Drops by User

You can run Top N RBACL Drops by User report as follows:

Step 1 From the Cisco ISE Admin dashboard, select **Operations > Reports > ISE Reports > Security Group Access**.

Step 2 Click **Top N RBACL Drops by User**.

Step 3 From the **Filters** drop-down menu, add the required monitor modes. The following options are available:

- Destination Name/Destination Address
- SGA SGT
- SGA DGT
- Enforcement Mode

Step 4 Enter the values for the selected parameters accordingly. You can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.

Step 5 From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.

Step 6 Click **Run** to run the report for a specific period, along with the selected parameters.

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the ox000 SGT.

The Cisco Security Group network devices request for cells that refer to the unknown SGT when they do not have a SGT of either source or destination. If only the source is unknown, the request applies to the <unknown, Destination SGT> cell. If only the destination is unknown, the request applies to the <source SGT, unknown> cell. If both the source and destination are unknown, the request applies to the <Unknown, Unknown> cell.

Default Policy

Default Policy refers to the <ANY,ANY> cell. Any source SGT is mapped to any destination SGT. Here, the ANY SGT cannot be modified and it is not listed in any source or destination SGTs. The ANY SGT can only be paired with ANY SGT. It cannot be paired with any other SGTs. A SGA network device attaches the default policy to the end of the specific cell policy.

- If a cell is empty, that means it contains the default policy alone.
- If a cell contains some policy, the resulting policy is a combination of the cell specific policy followed by the default policy.

According to Cisco ISE, the cell policy and the default policy are two separate sets of SGACLs that the devices get in response to two separate policy queries.

Configuration of the default policy is different from other cells:

- Status can take only two values, Enabled or Monitored.
- Security Group ACLs is an optional field for the default policy, so can be left empty.
- Final Catch All Rule can be either Permit IP or Deny IP. Clearly the None option is not available here because there is no safety net beyond the default policy.

OOB SGA PAC

All SGA network devices possess an SGA PAC as part of the EAP-FAST protocol. This is also utilized by the secure RADIUS protocol where the RADIUS shared secret is derived from parameters carried by the PAC. One of these parameters, Initiator-ID, holds the SGA network device identity, namely the Device ID.

If a device is identified using SGA PAC and there is no match between the Device ID, as configured for that device on Cisco ISE, and the Initiator-ID on the PAC, the authentication fails.

Some SGA devices (for example, Cisco firewall ASA) do not support the EAP-FAST protocol. Therefore, Cisco ISE cannot provision these devices with SGA PAC over EAP-FAST. Instead, the SGA PAC is generated on Cisco ISE and manually copied to the device; hence this is called as the Out of Band (OOB) SGA PAC generation.

When you generate a PAC from Cisco ISE, a PAC file encrypted with the Encryption Key is generated.

This section describes the following:

- SGA PAC Provisioning, page 24-19
- Monitoring SGA PAC, page 24-20

SGA PAC Provisioning

This section describes the following:

- Generating an SGA PAC from the Settings Screen, page 24-19
- Generating an SGA PAC from the Network Devices Screen, page 24-19
- Generating an SGA PAC from the Network Devices List Screen, page 24-20

Generating an SGA PAC from the Settings Screen

You can generate an SGA PAC from the Settings screen.

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-FAST > Generate PAC**.

Step 4 Generate SGA PAC.

Related Topics

Generating the PAC for EAP-FAST, page 19-12

Generating an SGA PAC from the Network Devices Screen

You can generate an SGA PAC from the Network Devices screen.

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Click **Add**. You can also click **Add new device** from the action icon on the Network Devices navigation pane.

Step 3 If you are adding a new device, provide a device name.

Step 4 Check the **Security Group Access (SGA)** check box to configure an SGA device.

Step 5 Under the **Out of Band (OOB) SGA PAC** sub section, click **Generate PAC**.

Step 6 Provide the following details:

- PAC Time to Live—Enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is ten years.

- Encryption Key—Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.

The Encryption Key is used to encrypt the PAC in the file that is generated. This key is also used to decrypt the PAC file on the devices. Therefore, it is recommended that the administrator saves the Encryption Key for later use.

The Identity field specifies the Device ID of an SGA network device and is given an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication will fail.

The expiration date is calculated based on the PAC Time to Live.

Step 7 Click **Generate PAC.**

Generating an SGA PAC from the Network Devices List Screen

You can generate an SGA PAC from the Network Devices list screen.

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Click **Network Devices**.

Step 3 Check the check box next to a device for which you want to generate the SGA PAC and click **Generate PAC**.

Step 4 Provide the details in the fields.

Step 5 Click **Generate PAC**.

Related Topics

Generating an SGA PAC from the Network Devices Screen, page 24-19

Monitoring SGA PAC

You can view SGA PAC provisioning data in the form of a PAC Provisioning Report.

Step 1 From the Cisco ISE Admin dashboard, select **Operations > Reports > ISE Reports** > **Security Group Access**.

Step 2 Click **PAC Provisioning**.

Step 3 From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.

Step 4 Click the **Run** button to run the report for a specific period.

Related Topics

Chapter 26, “Reporting.”

SGA CoA

Cisco ISE supports SGA Change of Authorization (CoA) which allows Cisco ISE to notify SGA devices about Security Group changes, so that the devices can reply with requests to get the relevant data.

A CoA notification can trigger a SGA network device to send either an Environment CoA or a Per Policy CoA.

This section contains:

CoA Supported Network Devices

Cisco ISE sends CoA notifications to the following network devices:

- Network device with single IP address (subnets are not supported)
- Network device configured as SGA device
- Network device set as CoA supported

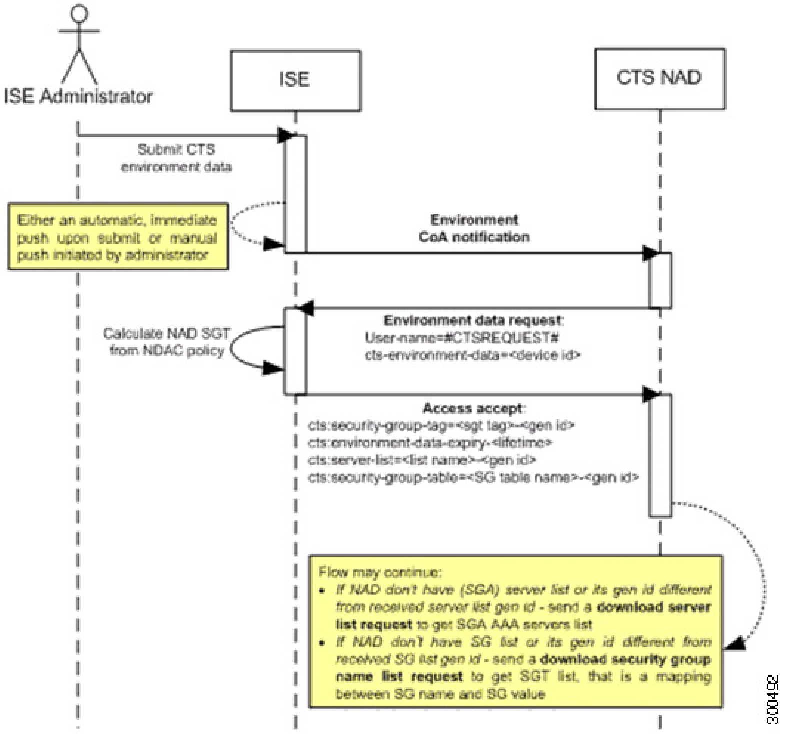
When Cisco ISE is deployed in a distributed environment where there are several secondaries that interoperate with different sets of devices, CoA requests are sent from Cisco ISE primary node to all the network devices. Therefore, SGA network devices need to be configured with the Cisco ISE primary node as the CoA client.

The devices return CoA NAK or ACK back to the Cisco ISE primary node. However, the SGA session that follows an SGA CoA is handled by the related Cisco ISE secondary node.

Environment CoA

Figure 24-2 depicts the Environment CoA notification flow.

Figure 24-2 Environment CoA Notification Flow


ISE Administrator
ISE
CTS NAD
Submit CTS environment data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Environment CoA notification
Environment data request:
User-name=#CTSREQUEST#
cts-environment-data=<device id>
Calculate NAD SGT from NDAC policy
Access accept:
cts:security-group-tag=<sgt tag>-<gen id>
cts:environment-data-expiry-<lifetime>
cts:server-list=<list name>-<gen id>
cts:security-group-table=<SG table name>-<gen id>
Flow may continue:
• If NAD don't have (SGA) server list or its gen id different from received server list gen id - send a download server list request to get SGA AAA servers list
• If NAD don't have SG list or its gen id different from received SG list gen id - send a download security group name list request to get SGT list, that is a mapping between SG name and SG value
300492

1. Cisco ISE sends an environment CoA notification to the SGA network device.
2. The device returns an environment request.
3. In response to the environment data request, Cisco ISE returns:
   a. The environment data of the device that sent the request—This includes the SGA device's SGT (as inferred from the NDAC policy) and download environment TTL.
   b. The name and generation ID of the SGA AAA server list.
   c. The names and generation IDs of (potentially multiple) SGT tables—These tables list SGT name versus SGT value, and together these tables hold the full list of SGTs.
4. If the device does not hold an SGA AAA server list, or the generation ID is different from the generation ID that is received, the device sends another request to get the AAA server list content.
5. If the device does not hold an SGT table listed in the response, or the generation ID is different from the generation ID that is received, the device sends another request to get the content of that SGT table.

Initiate Environment CoA

An Environment CoA can be triggered for:

- Triggering Environment CoA for Network Devices, page 24-23
- Triggering Environment CoA for Security Groups, page 24-23
- Triggering Environment CoA for SGA AAA Servers, page 24-23
- Triggering Environment CoA for NDAC Policy, page 24-24

Triggering Environment CoA for Network Devices

To trigger an Environment CoA for the Network devices, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Add or edit a network device.

Step 3 Update Security Group parameters under the SGA Attributes section.

Changing the environment TTL is notified only to the specific SGA network device where the change took place.

Because only a single device is impacted, an environmental CoA notification is sent immediately upon submission. The result is a device update of its environment TTL.

Triggering Environment CoA for Security Groups

To trigger an Environment CoA for the security groups, complete the following steps.

Step 1 Choose **Policy > Policy Elements > Results > Security Group Access > Security Groups**.

Step 2 In the security group page, change the name of an SGT, which will change the name of the mapping value of that SGT. This triggers an environmental change.

Step 3 Click the **Push** button to initiate an environment CoA notification after changing the names of multiple SGTs. This environment CoA notification goes to all SGA network devices and provides an update of all SGTs that were changed.

Triggering Environment CoA for SGA AAA Servers

To trigger an Environment CoA for the SGA AAA servers, complete the following steps.

Step 1 Choose **Administration > Network Resources > SGA AAA Servers**.

Step 2 In the SGA AAA Servers page create, delete or update the configuration of an SGA AAA server. This triggers an environment change.

Step 3 Click the **Push** button to initiate an environment CoA notification after you configure multiple SGA AAA servers. This environment CoA notification goes to all SGA network devices and provides an update of all SGA AAA servers that were changed.

Triggering Environment CoA for NDAC Policy

To trigger an Environment CoA for the NDAC Policies, complete the following steps.

In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

You can initiate an environment CoA notification by clicking the Push button in the NDAC policy page. This environment CoA notification goes to all SGA network devices and provides an update of network device own SGT, as described in the "Environment CoA" section on page 24-22.

Per Policy CoA

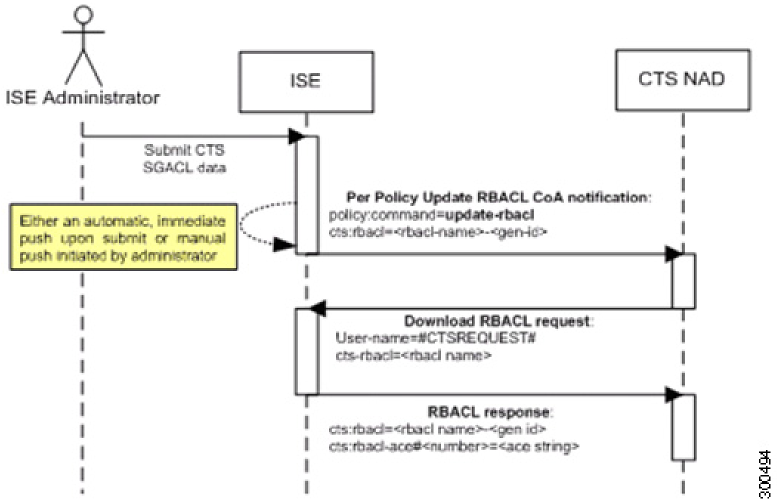
There are three types of Per Policy CoA notification:

- Update RBACL Named List CoA—Triggers a request to download SGACL (RBACL).
- Update SGT Matrix CoA—Triggers a request to download all egress policy cells related to a certain destination SGT (to an egress policy column).
- Policies Update CoA—This is an optimization that allows initiating multiple calls for both RBACL content and egress policy cells with a single CoA notification.

Update RBACL Named List CoA

Figure 24-3 depicts the Update RBACL Named List CoA flow.

Figure 24-3 Update RBACL Named List CoA Notification Flow


ISE Administrator
ISE
CTS NAD
Submit CTS SGACL data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update RBACL CoA notification:
policy:command=update-rbacl
cts:rbacl=<rbacl-name>-<gen-id>
Download RBACL request:
User-name=#CTSREQUEST#
cts-rbacl=<rbacl name>
RBACL response:
cts:rbacl=<rbacl name>-<gen id>
cts:rbacl-ace#<number>=<ace string>
300494

1. Cisco ISE sends an update RBACL named list CoA notification to a SGA network device. The notification contains the SGACL name and the generation ID.
2. The device may replay with an SGACL (RBACL) data request if both of the following terms are fulfilled:
   a. If the SGACL is part of an egress cell that the device holds. The device holds a subset of the egress policy data, which are the cells related to the SGTs of its neighboring devices and endpoints (egress policy columns of selected destination SGTs).

b. The generation ID in the CoA notification is different from the generation ID that the device holds for this SGACL.

3. In response to the SGACL data request, Cisco ISE returns the content of the SGACL (the ACE).

Initiating an Update RBACL Named List CoA

To trigger an Update RBACL Named List CoA, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the > button next to Security Group Access and click **Security Group ACLs**.

Step 3 Add or edit a SGACL as described in Configure Security Group Access Control Lists, page 24-10.

After you submit a SGACL, it promotes the generation ID of the SGACL.

Step 4 Click the **Push** button to initiate an Update RBACL Named List CoA notification after you change the content of multiple SGACLs. This notification goes to all SGA network devices, and provides an update of that SGACL content on the relevant devices.

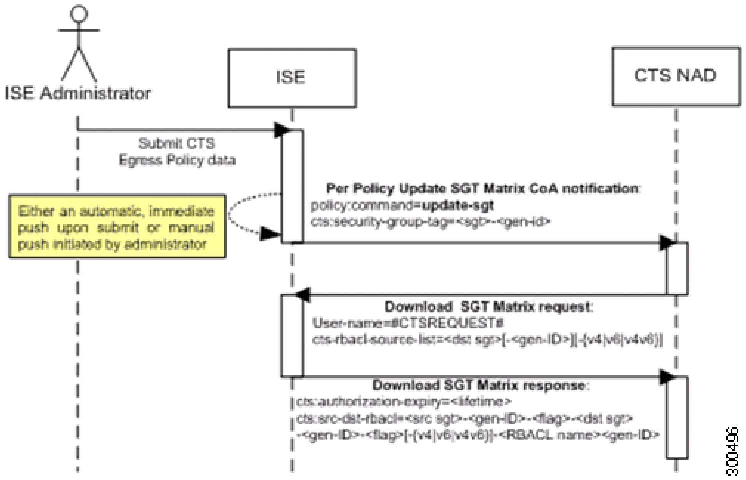
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update RBACL named list CoA notification.

However, changing the name or IP version of an SGACL that is in use in the egress policy indicates a change in the cell that contains that SGACL, and this changes the generation ID of the destination SGT of that cell. See Initiating Update SGT matrix CoA from Egress Policy, page 24-26 that deals with changes in the egress policy.

Update SGT Matrix CoA

Figure 24-4 depicts the Update SGT Matrix CoA flow.

Figure 24-4 Update SGT Matrix CoA flow


ISE Administrator
ISE
CTS NAD
Submit CTS Egress Policy data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update SGT Matrix CoA notification:
policy:command=update-sgt
cts:security-group-tag=<sgt>-<gen-id>
Download SGT Matrix request:
User-name=#CTSREQUEST#
cts-rbacl-source-list=<dst sgt>[-<gen-ID>][-{v4|v6|v4v6}]
Download SGT Matrix response:
cts:authorization-expiry=<lifetime>
cts:src-dst-rbacl=<src sgt>-<gen-ID>-<flag>-<dst sgt>
-<gen-ID>-<flag>[-{v4|v6|v4v6}]-<RBACL name><gen-ID>
300496

1. Cisco ISE sends an updated SGT matrix CoA notification to a SGA network device. The notification contains the SGT value and the generation ID.
2. The device may replay with an SGT data request if both the following terms are fulfilled:
   a. If the SGT is the SGT of a neighboring device or endpoint, the device downloads and hold the cells related to SGTs of neighboring devices and endpoints (a destination SGT).
   b. The generation ID in the CoA notification is different from the generation ID that the device holds for this SGT.
3. In response to the SGT data request, Cisco ISE returns the data of all egress cells, such as the source and destination SGTs, the status of the cell, and an ordered list of the SGACL names configured in that cell.

Initiating Update SGT matrix CoA from Egress Policy

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

Step 2 On the Egress Policy page, change the content of a cell (status, SGACLs).

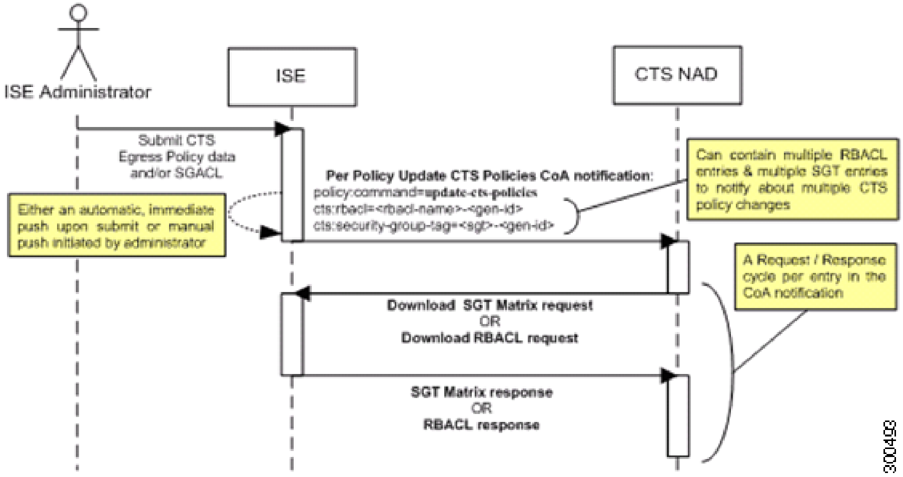
Step 3 After you submit the changes, it promotes the generation ID of the destination SGT of that cell.

Step 4 Click the **Push** button to initiate the Update SGT matrix CoA notification after you change the content of multiple egress cells. This notification goes to all SGA network devices, and provides an update of cells content on the relevant devices.

Policies Update CoA

Figure 24-5 depicts the Policies Update CoA flow.

Figure 24-5 Policies Update CoA flow


ISE Administrator
ISE
CTS NAD
Submit CTS Egress Policy data and/or SGACL
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update CTS Policies CoA notification:
policy:command=update-cts-policies
cts:rbacl=<rbacl-name>-<gen-id>
cts:security-group-tag=<sgt>-<gen-id>
Can contain multiple RBACL entries & multiple SGT entries to notify about multiple CTS policy changes
A Request / Response cycle per entry in the CoA notification
Download SGT Matrix request
OR
Download RBACL request
SGT Matrix response
OR
RBACL response
300493

1. Cisco ISE sends an update policies CoA notification to a SGA network device. The notification may contain multiple SGACL names and their generation IDs, and multiple SGT values and their generation IDs.

2. The device may replay with multiple SGACL data requests and/or multiple SGT data.
3. In response to each SGACL data request or SGT data request, Cisco ISE returns the relevant data.

SGA CoA Summary

Table 24-4 summarizes the various scenarios that may require initiating an SGA CoA, the type of CoA used in each scenario, and the related UI pages.

Table 24-4 SGA CoA Summary

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Network Device	Changing the environment TTL in the SGA section of the page	Upon successful Submit of SGA network device	Environment	The specific network device
SGA AAA Server	Any change in the SGA AAA server (create, update, delete, reorder)	Accumulative changes can be pushed by clicking the Push button on the SGA AAA servers list page.	Environment	All SGA network devices
Security Group	Any change in the SGT (create, rename, delete)	Accumulative changes can be pushed by clicking the Push button on the SGT list page.	Environment	All SGA network devices
NDAC Policy	Any change in the NDAC policy (create, update, delete)	Accumulative changes can be pushed by clicking the Push button on the NDAC policy page.	Environment	All SGA network devices
SGACL	Changing SGACL ACE	Accumulative changes can be pushed by clicking the Push button on the SGACL list page.	Update RBACL named list	All SGA network devices
	Changing SGACL name or IP version	Accumulative changes can be pushed by clicking the Push button on the SGACL list page or the policy push button in the Egress table.	Update SGT matrix	All SGA network devices
Egress Policy	Any operation that changes the generation ID of an SGT	Accumulative changes can be pushed by clicking the Push button on the egress policy page.	Update SGT matrix	All SGA network devices

Monitor SGA CoA

SGA CoA notifications can be viewed as alarms, logs, and reports.

This section describes how to view the following:

- SGA CoA Alarms, page 24-28
- Running SGA CoA Report, page 24-28

SGA CoA Alarms

When CoA returns CoA-NAK, an alarm is generated.

To view SGA CoA alarms, go to **Operations > Alarms > Rules**.

You can also view the SGA CoA alarms under Live Logs. To view live logs, go to **Operations > Alarms > Inbox .**

Running SGA CoA Report

You can run the SGA CoA Report as follows:

Step 1 From the Cisco ISE Admin dashboard, select **Operations > Reports > ISE Reports > Security Group Access**.

Step 2 From the **Run** drop-down menu, choose a time period over which the report data will be collected.

You can use the **Run** button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.