Access Control Rules: Custom Security Group Tags

The Security Group Tag (SGT) specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) automatically generates the SGT when a user adds a security group in TrustSec or ISE. SGA then applies the SGT attribute as packets enter the network. You can use SGTs for access control by configuring ISE as an identity source or creating custom SGT objects.

Custom SGT conditions allow you to configure access control rules based on custom SGT objects. You manually add custom SGT objects to the Firepower System, rather than obtaining SGTs via ISE.

You can only use custom SGT conditions if you disable ISE as an identity source.

The following topics describe how to use SGT conditions in access control rules:

ISE SGT v. Custom SGT Rule Conditions

You can use SGTs for access control by either configuring ISE as an identity source (*ISE SGT*) or creating custom SGT objects (*custom SGT*). The system handles ISE SGT and custom SGT rule conditions differently:

ISE SGT: ISE connection configured

You can use ISE SGTs as ISE attribute conditions in access control rules. When you choose **Security Group Tag** from the **Available Attributes** list in the **SGT/ISE Attributes** tab, the system populates the **Available Metadata** list by querying ISE for available tags. The presence or absence of an SGT attribute in a packet determines the system's response:

- If an SGT attribute is present in the packet, the system extracts that value and compares it to ISE SGT conditions in access control rules.
- If the SGT attribute is absent from the packet, the system queries ISE for the SGT associated with the packet's source IP address and compares the returned value to ISE SGT conditions in access control rules.

Custom SGT: No ISE connection configured

You can create custom SGT objects and use them as conditions in access control rules. When you choose **Security Group Tag** from the **Available Attributes** list in the **SGT/ISE Attributes** tab, the system populates the **Available Metadata** list with any SGT objects you have added. The presence or absence of an SGT attribute in a packet determines the system's response:

- If an SGT attribute is present in the packet, the system extracts that value and compares it to custom SGT conditions in access control rules.
- If the SGT attribute is absent from the packet, the system does not match the packet to custom SGT conditions in access control rules.

Automatic Transition from Custom SGT to ISE SGT Rule Conditions

If you create access control rules using custom SGT objects as conditions, then later configure ISE as an identity source, the system:

- Disables the **Security Group Tag** object option in the Object Manager. You cannot add new SGT objects, edit existing SGT objects, or add SGT objects as new conditions unless you disable the ISE connection.
- Retains existing SGT objects. You cannot modify these existing objects. You can view them only in the context of the existing access control rules that use them as conditions.
- Retains existing access control rules with custom SGT conditions. Because custom SGT objects can only be updated via manual editing, Cisco recommends that you delete or disable these rules. Instead, create rules using SGTs as ISE attribute conditions. The system automatically queries ISE to update SGT metadata for ISE attribute conditions, but you can only update custom SGT objects via manual editing.

Configuring Custom SGT Conditions

License: Any

To configure a custom Security Group Tag (SGT) condition:

Step 1 In the access control rule editor, click the **SGT/ISE Attributes** tab.

Step 2 Choose **Security Group Tag** from the **Available Attributes** list.

Step 3 In the **Available Metadata** list, find and choose a custom SGT object.

If you choose , the rule matches all traffic with an SGT attribute. For example, you might choose this value if you want the rule to block traffic from hosts that are not configured for TrustSec.

Step 4 Click **Add to Rule**, or drag and drop.

Step 5 Save or continue editing the rule.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Troubleshooting Custom SGT Conditions

If you notice unexpected rule behavior, consider tuning your custom SGT object configuration.

Security Group Tag objects unavailable

Custom SGT objects are only available if you do not configure ISE as an identity source. For more information, see Automatic Transition from Custom SGT to ISE SGT Rule Conditions, page 10-2.