Access Control Rules: Realms and Users

The following topics describe how to control user traffic on your network:

Realm, User, User Group, and ISE Attribute Access Control Rule Conditions

License: Control

Before you can perform user control (create access control rule conditions based on entire realms, individual users, user groups, or ISE attributes), you must:

- Configure a realm for each Microsoft Active Directory or LDAP server you want to monitor. If you enable user download for the realm, the Firepower Management Center regularly and automatically queries the server to download metadata for newly or already-reported authoritative users and user groups.
- Create an identity policy to associate the realm with an authentication method.
- Configure one or more User Agents or ISE devices, or captive portal. If you want to use an ISE attribute condition, you must configure ISE.

  User Agents, ISE, and captive portal collect authoritative user data that can be used for user control in access control rule conditions. The identity sources monitor specified users as they log in or out of hosts or authenticate using LDAP or AD credentials.

Note If you configure a User Agent or ISE device to monitor a large number of user groups, or if you have a very large number of users mapped to hosts on your network, the system may drop user mappings based on groups, due to your Firepower Management Center user limit. As a result, access control rules with realm, user, or user group conditions may not fire as expected.

You can add a maximum of 50 realms, users, and groups to the Selected Users in a single user condition. Conditions with user groups match traffic to or from any of the group's members, including members of any sub-groups, with the exception of individually excluded users and members of excluded sub-groups.

Including a user group automatically includes all of that group's members, including members of any secondary groups. However, if you want to use the secondary group in access control rules, you must explicitly include the secondary group.

Note Hardware-based fast-path rules, Security Intelligence-based traffic filtering, SSL inspection, user identification, and some decoding and preprocessing occur before access control rules evaluate network traffic.

Troubleshooting Issues with User Access Control Rules

License: Control

If you notice unexpected user access control rule behavior, consider tuning your rule, identity source, or realm configurations.

Access control rules targeting realms, users, or user groups are not firing

If you configure a User Agent or ISE device to monitor a large number of user groups, or if you have a very large number of users mapped to hosts on your network, the system may drop user records due to your Firepower Management Center user limit. As a result, access control rules with realm or user conditions may not fire as expected.

Access control rules targeting user groups or users within user groups are not firing as expected

If you configure an access control rule with a user group condition, your LDAP or Active Directory server must have user groups configured. The Firepower Management Center cannot perform user group control if the server organizes the users in basic object hierarchy.

Access control rules targeting users in secondary groups are not firing as expected

If you configure an access control rule with a user group condition that includes or excludes users who are members of a secondary group on your Active Directory server, your server may be limiting the number of users it reports.

By default, Active Directory servers limit the number of users they report from secondary groups. You must customize this limit so that all of the users in your secondary groups are reported to the Firepower Management Center and eligible for use in access control rules with user conditions.

Access control rules are not matching users when seen for the first time

After the system detects activity from a previously-unseen user, the system retrieves information from the server. Until the system successfully retrieves this information, activity seen by this user is not handled by matching access control rules. Instead, the user session is handled by the next access control rule it matches (or the access control policy default action).

For example, this may explain when:

- Users who are members of user groups are not matching access control rules with user group conditions.
- Users who were reported by ISE or the User Agent are not matching access control rules, when the server used for user data retrieval is an Active Directory server.

Note that this may also cause the system to delay the display of user data in event views and analysis tools.

Adding a Realm, User, or User Group Condition to an Access Control Rule

License: Control

Before You Begin

- Configure one or more authoritative user identity sources as described in User Identity Sources, page 33-1.
- Configure a realm as described in Creating a Realm, page 32-4. A user download (automatic or on-demand) must be performed before you can configure realm, user, or user group conditions in an access control rule.

Step 1 In the access control rule editor, select the **Users** tab.

Step 2 Search by name or value above the **Available Realms** list and select a realm.

Step 3 Search by name or value above the **Available Users** list and select a user or group.

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.

Configuring ISE Attribute Conditions

License: Control

Before You Begin

- Configure ISE as described in Configuring an ISE Connection, page 33-6.

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

Step 2 Search by name or value above the **Available Attributes** list and choose an attribute.

Step 3 Search by name or value above the **Available Metadata** list and choose metadata.

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

You can also use the **Add a Location IP Address** field to add a Location IP attribute to the condition.

Note You can use ISE-assigned Security Group Tags (SGTs) to constrain ISE attribute conditions. To use custom SGTs in access control rules, see ISE SGT v. Custom SGT Rule Conditions, page 10-1.

Step 5 Save or continue editing the rule.

What to Do Next

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