Dynamic firewall

A dynamic firewall integrates user identity data with user trust data provided by Identity Intelligence to enhance your ability to detect identity-based exploits in your network.

Identity data integration

The dynamic firewall integrates user identity data from Microsoft AD and ISE with user trust data.

Dynamic Firewall

A dynamic firewall integrates identity sources with Identity Intelligence to provide user and device trust information.

Enhanced identity information

Previously, the collected information about users exclusively from the configured identity sources, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address.

The dynamic firewall enables you to pair user identity with intelligence and use that information in reporting and access control policies.

To use the dynamic firewall, you must:

- Have an Identity Intelligence tenant

  See Duo Identity Security with Cisco Identity Intelligence.

- Enable the Dynamic Attributes Connector
- Set up an identity source:
  - Cisco Identity Services Engine (Cisco ISE)
  - pxGrid Cloud

    pxGrid Cloud combines identity and posture in the same feed

    More information: What is pxGrid?

In addition to providing authentication information, Cisco ISE and pxGrid Cloud can provide the following:

- SGT Exchange Protocol (SXP) over TCP binding and directory session information if desired. For more information, see the *Cisco Identity Services Engine Administrator Guide*
- Posture and mobile device management compliance. For more information, see Compliance.

- Set up an identity realm:
  -

The *identity source* provides authentication information (login, logout) as well as posture. The identity source can also provide SXP binding and session directory information if desired.

The *identity realm* provides user, group, and IP address information.

How to configure the dynamic firewall

This topic helps you understand the concepts and options to configure the dynamic firewall discussed in Dynamic Firewall, on page 1.

Summary

The dynamic firewall integrates an identity source (such as Cisco ISE) with Cisco Identity Intelligence, which provides user trust information to the Secure Firewall Management Center.

1. Configure Cisco Identity Intelligence to collect user trust information.
2. Configure a supported Secure Firewall Management Center identity source.
3. Configure a supported identity realm.
4. Enable the dynamic attributes connector.
5. Configure the dynamic firewall.

Workflow

The following procedure provides a high-level overview of how to configure the dynamic firewall.

1. As a Duo user with the Owner role, provision a Cisco Identity Intelligence tenant.

   You can provision a tenant from Duo Advantage as discussed in *Provision Your Cisco Identity Intelligence Tenant*.

2. In Cisco Identity Intelligence, create an API integration and use the information to set up the dynamic firewall.

   We use Cisco Identity Intelligence to find user and device risk information in your network.

   For more information about Cisco Identity Intelligence, see How-to Guides.

   For more information about this task, see Get required information for Identity Intelligence, on page 4.

3. (Microsoft Azure AD realm only.) In Identity Intelligence, create a Microsoft Entra ID integration.

For more information, see Microsoft Entra ID (Azure AD) Data Integration.

4. Create an identity source. (If you already have an identity source, continue with the next step.)

   You can do this in any of the following ways:

   - The Configure Dynamic Firewall dialog box displays **Configure** links to start setting up your identity source.
   - Click **System** (⚙) > **Integration** > **Identity Sources**.

   For more information about creating identity sources, see:

5. Create an identity realm.

   We support the following realms:

   - Only Microsoft AD is supported; LDAP realms are not supported.
   -

6. Enable the dynamic attributes connector.

   The dynamic attributes connector is required to use the dynamic firewall. It enables your identity source to integrate with Identity Intelligence to provide enhanced insights into user activity.

   See .

7. Create the dynamic firewall instance. (If you already have a dynamic firewall instance, continue with the next step.)

   Click **Integration** > **Dynamic Attributes Connector** and click **Configure Dynamic Firewall**.

   See Create a dynamic firewall instance, on page 6.

8. Associate your identity source with Cisco Identity Intelligence.

   See Associate an identity source with Identity Intelligence, on page 7.

9. View system-defined filters.

   We create dynamic attributes filters for the following:

   - Untrusted device
   - Trusted device
   - Untrusted user
   - Questionable user

   You can edit or replace these dynamic attributes filters as discussed in Create dynamic attributes filters, on page 14.

10. View system-defined access control rules.

    We create an access control policy named Dynamic Firewall Policy (or similar) with the following rules:

    - Block an untrusted user from any source network to any destination network.
    - Monitor a questionable user from any source network to any destination network.

- Block an untrusted device from any source network to any destination network.

You can edit or delete the access control policy and rules as discussed in View and edit the system-created access control policy, on page 13.

Enable the dynamic attributes connector

Enable the dynamic attributes connector to allow objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

This task discusses how to enable the dynamic attributes connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integration** > **Dynamic Attributes Connector**.

Step 3 Slide to **Enabled**.

Step 4 The system displays messages when the dynamic attributes connector is enabled.

In the event of errors, try again. If errors persist, contact Cisco TAC.

See Connectors.

Get required information for Identity Intelligence

Get the necessary credentials and configuration values from Identity Intelligence to enable integration with the dynamic firewall.

This task discusses how to create an API client, which provides all the get required information to set up Identity Intelligence in the dynamic firewall.

If you already have an API client and you know the values of all these parameters, you can skip this procedure and continue with :

- **Client ID**
- **API URL**
- **Token URL**
- **Client Secret**

Before you begin

Integrating with the dynamic firewall requires you to create an *API client integration* in Identity Intelligence.

Among the values you must know about your API client integration is the client secret, which is displayed when you create the API client only. For that reason you might need to create the API integration first.

For more information about creating an API cilent integration, see Public API.

Follow these steps to get required information for Identity Intelligence:

Procedure

Step 1 Log in to your Identity Intelligence tenant.

Step 2 Click (**Integrations**).

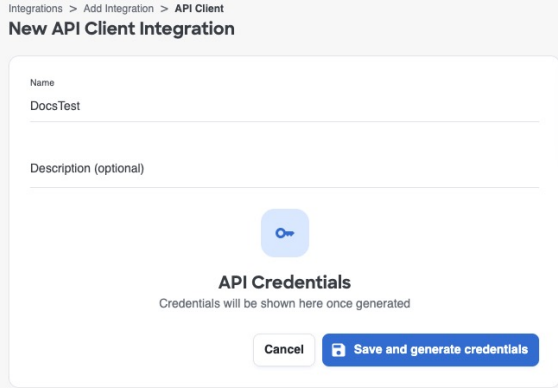
Step 3 Click **Add Integration**.

Step 4 On the next page, under API Clients, click **Add API Client**.

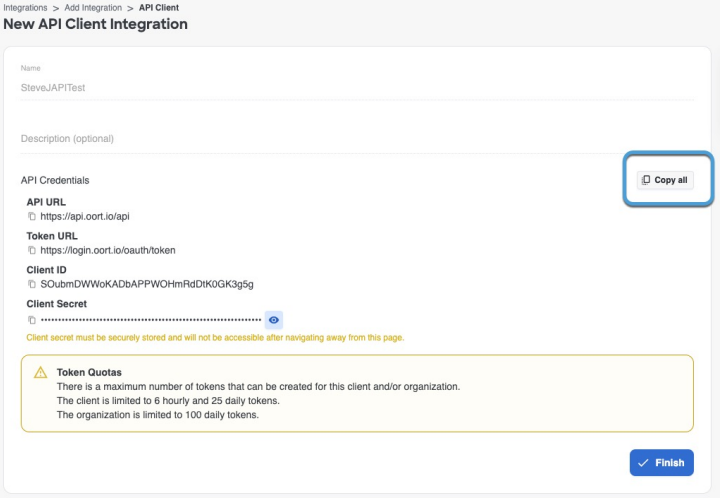
Step 5 Enter a **Name** and an optional **Description**.

Step 6 Click **Save and Generate Credentials**.

This figure shows an example.



Step 7 On the next page, click **Copy all** as this figure shows.



Step 8 Save the credentials for later use.

Step 9 Click **Finish**.

Create an identity source and realm for the dynamic firewall

Before you configure the dynamic firewall, you must configure a supported identity realm and identity source.

Configure an identity realm

These identity realms are supported:

- Only Microsoft AD is supported; LDAP realms are not supported.
-

Configure an identity source

These identity sources are supported:

Create a dynamic firewall instance

Create a new instance of the dynamic firewall to establish an association between an identity source and Identity Intelligence.

This task discusses how to create a new instance of the dynamic firewall, which is an association between an identity source and Identity Intelligence.

Before you begin

Complete all these steps:

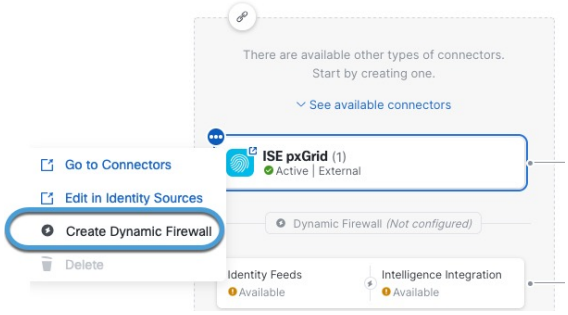
- Enable the dynamic attributes connector as discussed in .
- Create an identity source:

Follow these steps to create a dynamic firewall instance:

Procedure

Step 1 Click  next to the name of the identity source with which to add the dynamic firewall.

The following figure shows an example.



Note
If you do not see an identity source, create one before continuing:

Step 2 Click **Create Dynamic Firewall**.

Step 3 Continue with .

Associate an identity source with Identity Intelligence

Associate a supported identity source with Identity Intelligence to enable user and device trust ratings for dynamic firewall configuration.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device trust ratings to the .

For more information, see User Trust Level.

Before you begin

Before you begin, make sure you:

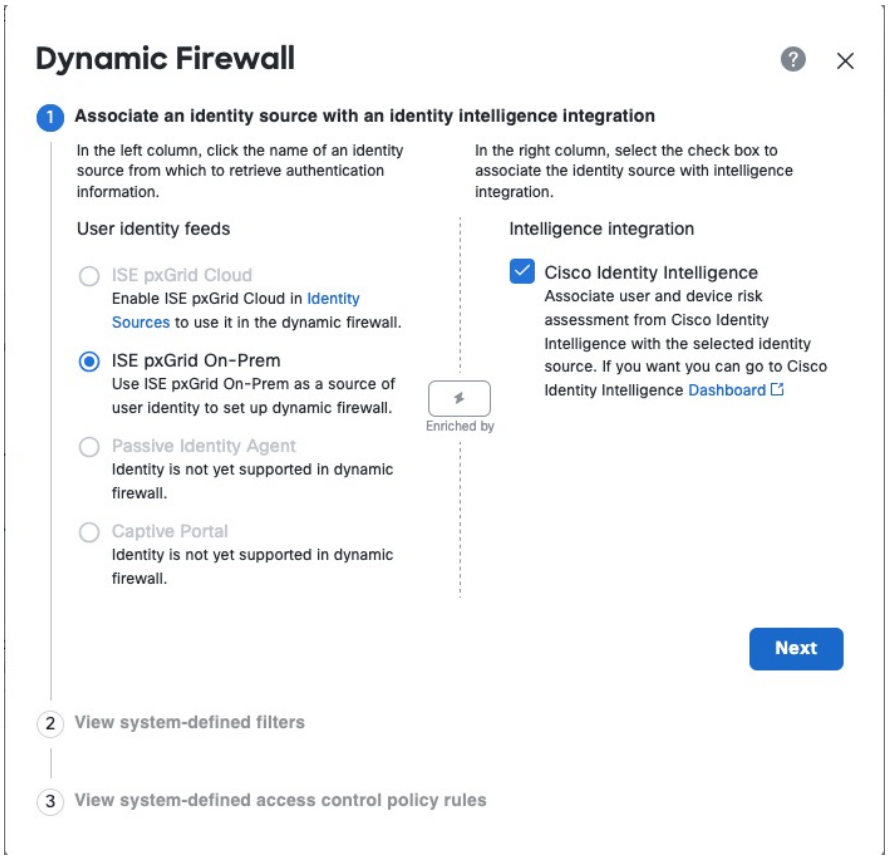
- Understand how the identity realm, identity source, and Identity Intelligence work together as discussed in Dynamic Firewall, on page 1.
- Completed the tasks discussed in Create a dynamic firewall instance, on page 6.

Procedure

Step 1 Start with .

Step 2 On the next page, from the left column, click your identity source. Then, in the right column, select the **Cisco Identity Intelligence** check box to add user intelligence, including user and device risk.

The following figure shows an example.



Step 3 Click **Next**.

Step 4 Continue with Configure Identity Intelligence, on page 8.

Configure Identity Intelligence

This task enables integration between the dynamic firewall and Identity Intelligence.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device risk ratings to the .

Before you begin

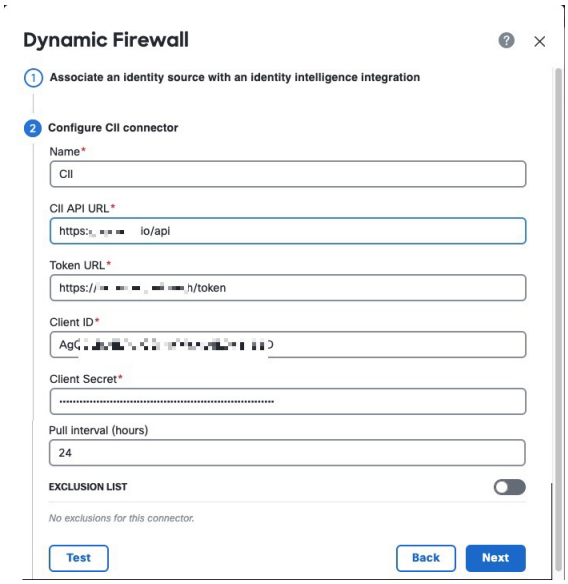
Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 7.

Procedure

Step 1 Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 7.

Step 2 If you selected the **Cisco Identity Intelligence** check box, enter the information you found for Identity Intelligence as described in Get required information for Identity Intelligence, on page 4.

The following figure shows an example.



Step 3 (Optional.) For Identity Intelligence to consider a specific set of users as trusted, slide **Exclusion List** to **Slider enabled** ( ).

Enter one user name per line in **username@domain.com** format. Users in this list are considered trusted by Identity Intelligence.

Step 4 Click **Test**.

Only if the test succeeds, continue with the next step.

If any errors are displayed, check all of your Identity Intelligence values and try again.

Step 5 Click **Next**.

Step 6 Continue with View system-defined filters, on page 9.

View system-defined filters

This task allows you to examine and understand the system-defined dynamic attributes filters that are automatically created during the configuration process.

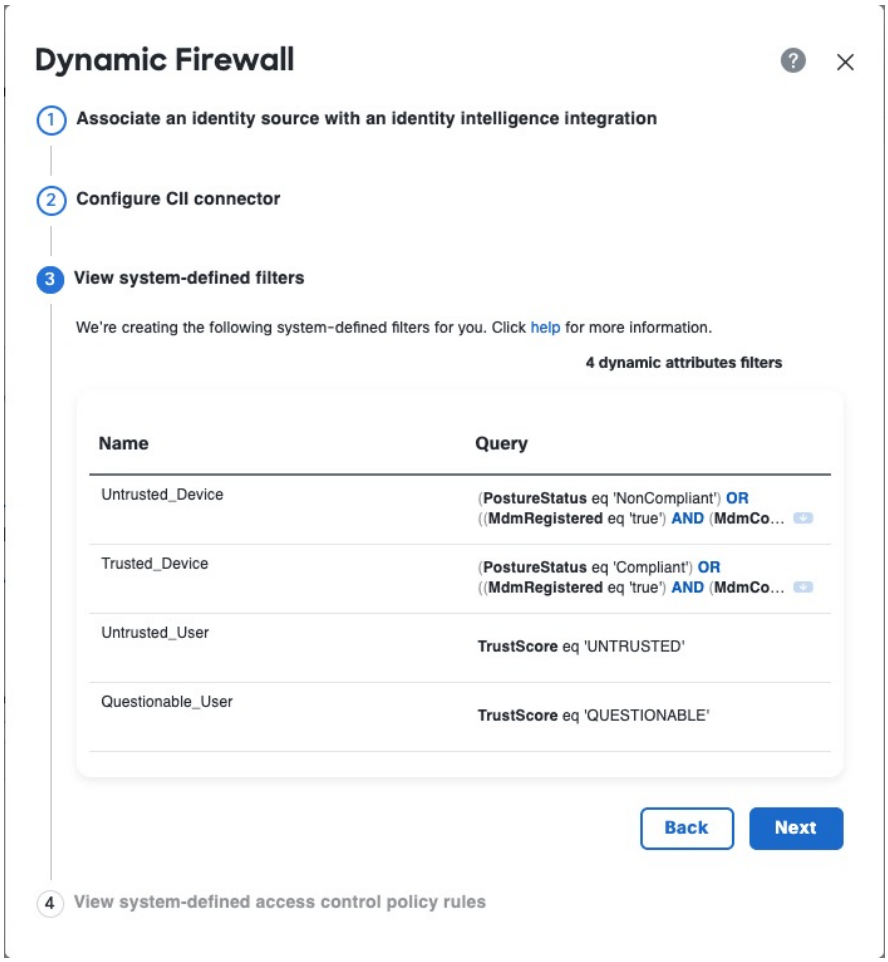
This task discusses how you associate an identity source with Cisco Identity Intelligence, which provides user and device risk ratings to the .

Before you begin

See .

Procedure

Step 1 The system displays a set of system-defined dynamic attributes filters, as shown in the following figure.



Step 2 View the system-created filters. Click on any row to expand the filter so you can view the filter and see its details.

Step 3 Click **Next**.

Step 4 Continue with View system-defined access control rules, on page 10.

View system-defined access control rules

This task allows you to review and decide whether to create system-defined access control rules for your dynamic firewall instance.

This task discusses access control rules created by the dynamic firewall.

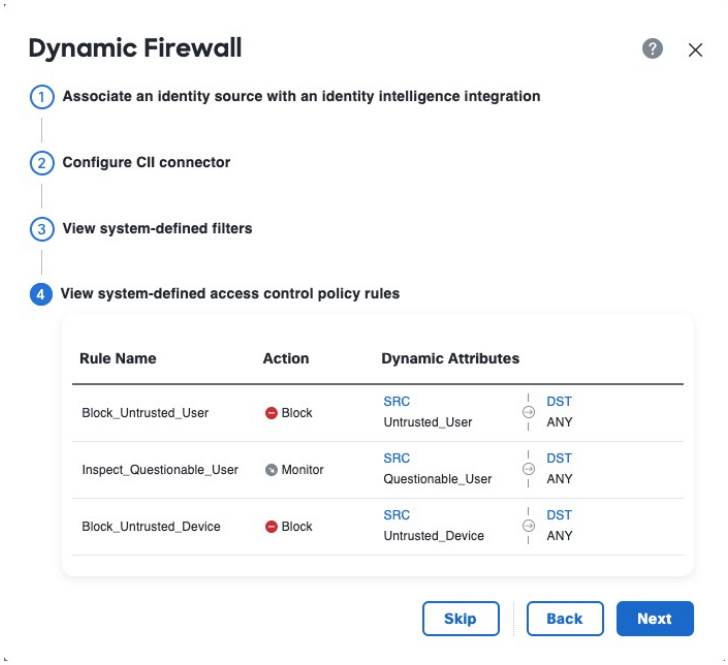
Before you begin

See View system-defined filters, on page 9.

Procedure

Step 1 View the system-created access control rules.

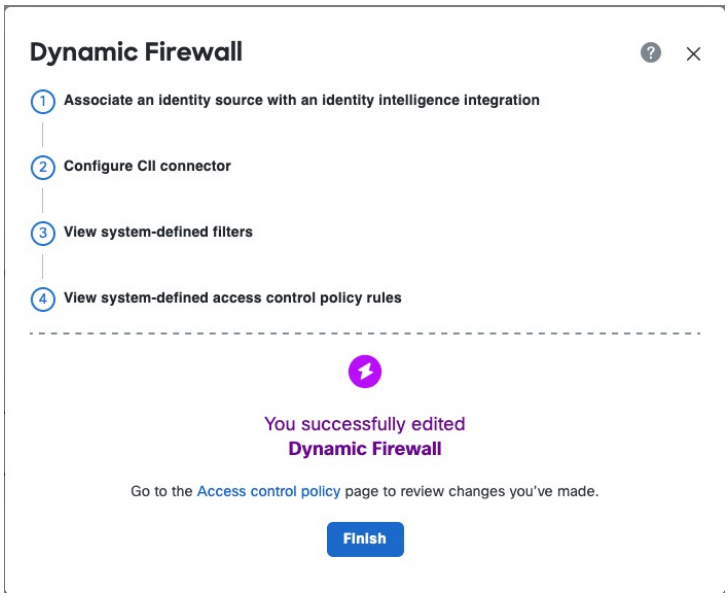
The following figure shows an example.



Step 2 Choose one of these options:

- Click **Skip** to skip creating these access control rules. You can create your own anytime.
- Click **Next** to create an access control policy named Dynamic Firewall Policy with the rules shown in the preceding figure.
- Click **Back** to return to system-created filters.

Step 3 After you click **Next**, if you created access control rules successfully, the following page is displayed:



Edit the user exclusion list

Specify users provided by Identity Intelligence as always being trusted.

You can instruct Identity Intelligence to treat specific users as trusted.

Before you begin

Configure the dynamic firewall as discussed in Create a dynamic firewall instance, on page 6.

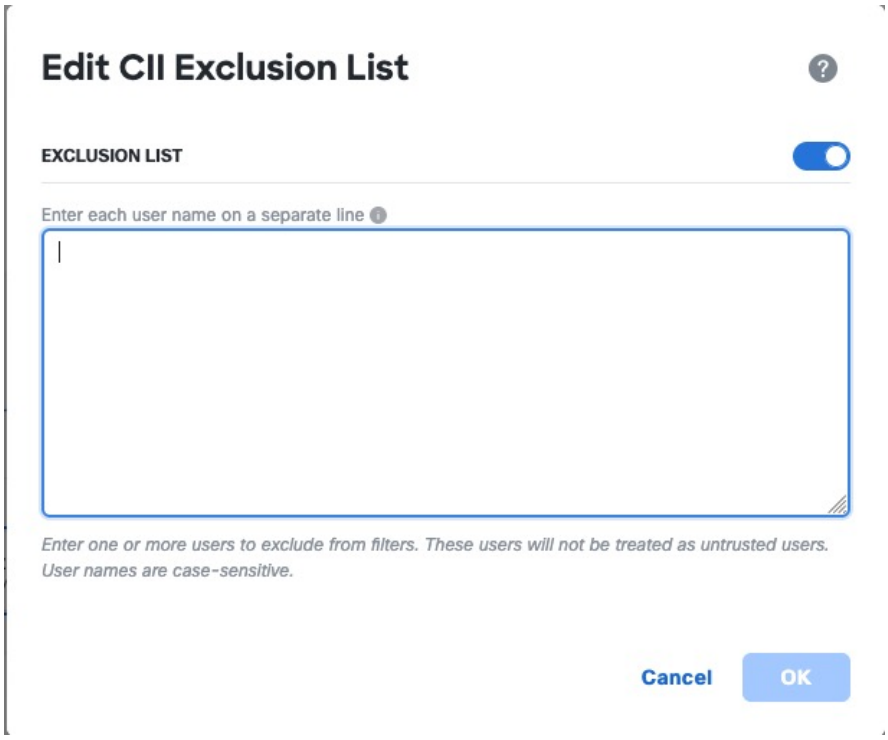
Procedure

Step 1 Click **Integration** > **Dynamic Attributes Connector**.

Step 2 Click next to the name of the identity source.

Step 3 Click **Edit CII Exclusion List**.

The following dialog box is displayed.



Step 4 In the provided field, enter one user name in `username@domain.com` format on a line, press Enter, and enter another user name.

Each user name is considered as trusted by Identity Intelligence.

View and edit the system-created access control policy

Customize the system-created access control policy by adding devices, changing rules, reordering rules, or deleting rules to meet your specific network security requirements.

This topic discusses how you can edit the system-created access control rules and policy. Initially, the policy isn't associated with any devices but if you want to use it you can add devices, change rules, reorder rules, or delete rules.

Before you begin

Complete the tasks described in View system-defined access control rules, on page 10.

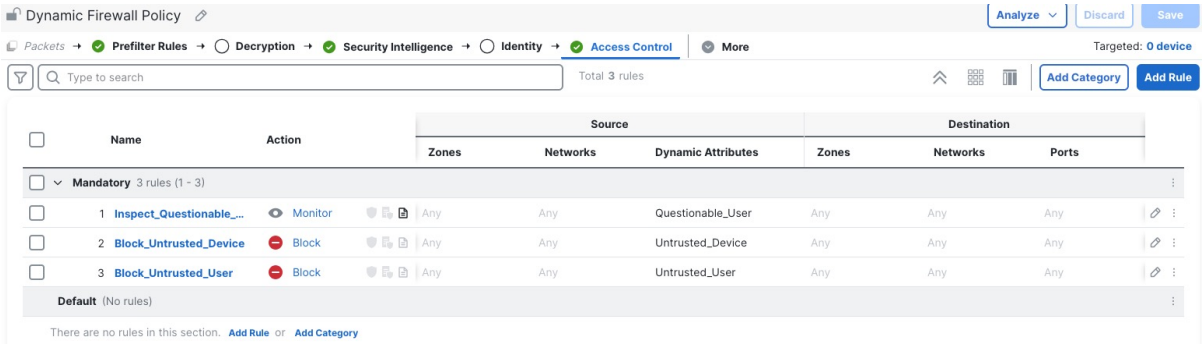
Follow these steps to view and edit the system-created access control policy:

Procedure

Step 1 Click **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** ( ) next to the policy named Dynamic Firewall Policy (or similar).

The following figure shows a sample access control policy.



Note that in this access control policy, only the rule set to monitor questionable users logs anything. To adjust the logging settings, see .

Step 3 Do any of the following:

- Target the access control policy at devices: .
- Edit the policy, including adding logging: .
- Edit access control rules: .
- Set advanced policy options: .
- Associate other policies with this access control policy: .

Create dynamic attributes filters

Create dynamic attributes filters that can be used as dynamic objects in access control policies to restrict access based on specific criteria such as group membership.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the as dynamic objects that can be used in access control policies. For example, you could restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

Procedure

Step 1 Do any of the following:

- Add a new filter: click **Add** ( ).
- Edit or delete a filter: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

Step 2 Enter the following information.

- **Name**: Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the Object Manager (**External Attributes** > **Dynamic Object**).
- **Connector**: From the list, click the name of a connector to use.

Step 3 To add a query, enter the following information.

- **Key**: Click a key from the list. Keys are fetched from the connector.
- **Operation**: Click one of the following:
  - **Equals** to exactly match the key to the value.
  - **Contains** to match the key to the value if any part of the value matches.
- **Values**: Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

Step 4 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

When you're finished, click **Save**.

What to do next

Verify the dynamic object in the .

1. Log in to the .
2. Click **Policies** > **Firewall Threat Defense**.
3. Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.