Use Dynamic Objects in Access Control Policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the Secure Firewall Management Center as dynamic objects, in access control rules.

About Dynamic Objects in Access Control Rules

A *dynamic object* is automatically pushed from the dynamic attributes connector to the Secure Firewall Manager after you create connectors and save a dynamic attributes filter on the connector.

You can use these dynamic objects on the access control rule's **Dynamic Attributes** tab page, similarly to the way you used Security Group Tags (SGTs). You can add dynamic objects as source or destination attributes; for example, in an access control block rule, you can add a Finance dynamic object as a destination attribute to block access to Finance servers by whatever objects match the other criteria in the rule.

Note You cannot create dynamic attributes filters for AWS, AWS service tags, AWS service groups, Azure, Azure Service Tags, Cisco Cyber Vision, Generic Text, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create Access Control Rules Using Dynamic Attributes Filters

This topic discusses how to create access control rules using dynamic objects (these dynamic objects are named after the dynamic attributes filters you created previously).

Before you begin

Create dynamic attributes filters as discussed in Create Dynamic Attributes Filters.

Note You cannot create dynamic attributes filters for AWS, AWS service tags, AWS service groups, Azure, Azure Service Tags, Cisco Cyber Vision, Generic Text, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Procedure

Step 1 Log in to Secure Firewall Management Center .

Step 2 Click **Policies** > **Access Control heading** > **Access Control**.

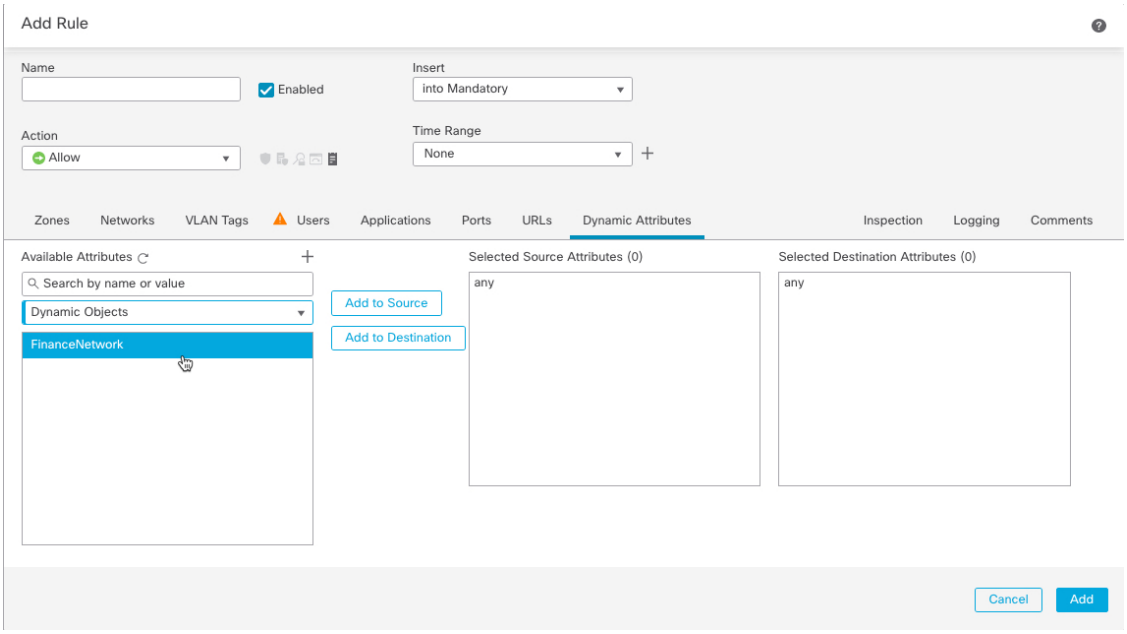
Step 3 Click **Edit** ( ) next to an access control policy.

Step 4 Click **Add Rule**.

Step 5 Click the **Dynamic Attributes** tab.

Step 6 In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.



The preceding example shows a dynamic object named `FinanceNetwork` that corresponds to the dynamic attribute filter created in the Cisco Secure Dynamic Attributes Connector.

Step 7 Add the desired object to source or destination attributes.

Step 8 Add other conditions to the rule if desired.

What to do next

Dynamic Attributes Rule Conditions in the *Cisco Secure Firewall Management Center Device Configuration Guide*.