

Use Dynamic Objects in Access Control Policies or DNS Policies

The dynamic attributes connector enables you to configure dynamic attributes filters, seen in the as dynamic objects, in access control rules or DNS policies.

- About dynamic objects in access control rules or DNS rules, on page 1
- Create dynamic attributes filters, on page 1
- Dynamic attributes rule conditions, on page 3
- View dynamic objects in the , on page 3
- Create access control rules or DNS rules using dynamic attributes filters, on page 5
- Use dynamic objects in DNS policies, on page 6
- How to use network object groups from Cisco APIC in ASA access rules, on page 7

About dynamic objects in access control rules or DNS 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 or DNS rule's **Dynamic Attributes** tab page. 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 dynamic attributes filters

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, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

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.

Before you begin

Create a connector

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Dynamic Attributes Filters**.

Step 3 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 4 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

Step 5 To add or edit a query, enter the following information.

Item	Description
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 6 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 7 When you're finished, click **Save**.

Step 8 (Optional.) Verify the dynamic object in the .

a) Log in to the as a user with the Network Admin role at minimum.

b) Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

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

Dynamic attributes rule conditions

Dynamic attributes include:

- (Source or destination.) Dynamic objects (such as from the dynamic attributes connector)

  The dynamic attributes connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the so they can be used in access control rules.

  For more information about the dynamic attributes connector, see .

- (Source only.) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source and Destination Security Group Tag (SGT) Matching and Security Group Tag.

- (Source only.) Location IP objects, defined by Cisco ISE

- (Source only.) Device type objects, defined by Cisco ISE (also referred to as endpoint profile objects)

Dynamic attributes can be used as source criteria and destination criteria in access control rules. Use the following guidelines:

- Objects of different types are ANDd together

- Objects of a similar type are ORd together

For example, if you choose source destination criteria SGT 1, SGT 2, and device type 1; the rule is matched if device type 1 is detected on either SGT 1 or SGT 2. As another example, if you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originates from (or is destined to) one of those IP addresses.

View dynamic objects in the

(Optional.) The following task discusses how you can view Cisco APIC network objects in the **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

Before you begin

Complete all of the previous tasks related to integrating Cisco APIC with the .

Procedure

Step 1 Log in to the

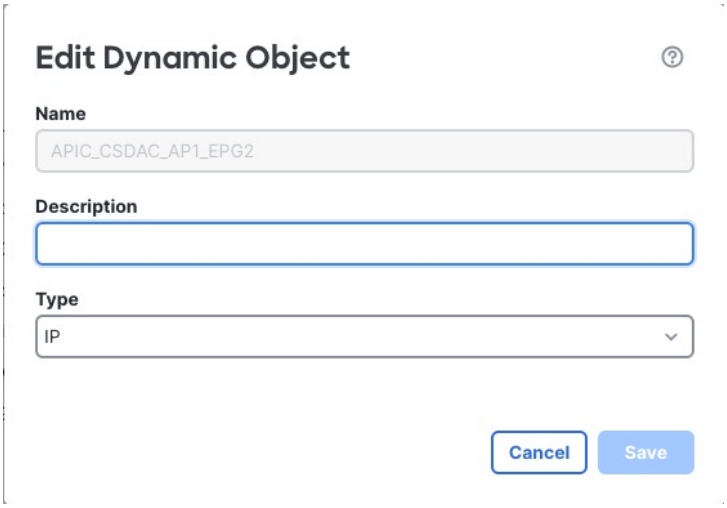
Step 2 Expand **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

Dynamic objects have their own naming conventions; for example, AWS dynamic objects have names like `aws_AMAZON`.

Dynamic objects created by the integration with Cisco APIC have names matching the pattern:

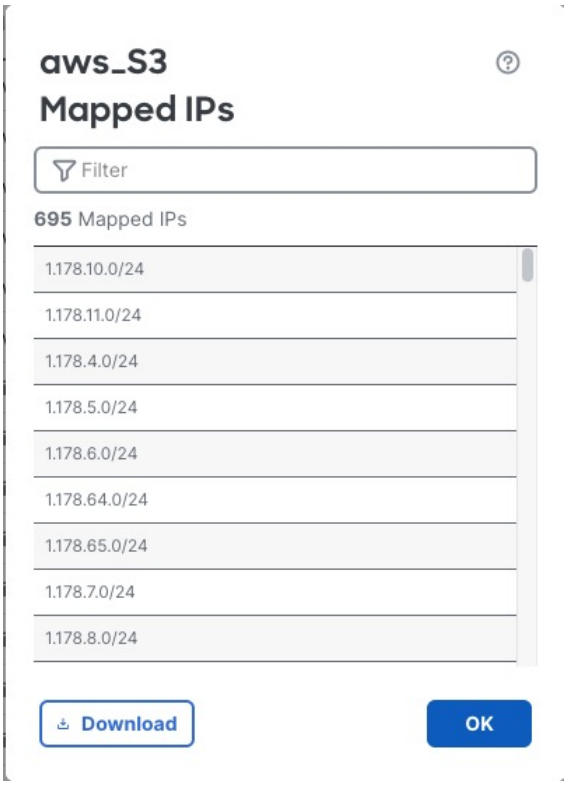
`APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name`

Example.



Step 3 To view IP addresses associated with each dynamic object, click (IPs) at the end of the row.

Example:



What to do next

See Create access control rules or DNS rules using dynamic attributes filters, on page 5.

Create access control rules or DNS 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).

To add dynamic attributes filters to DNS policies, see Creating Basic DNS Policies.

Before you begin

Create dynamic attributes filters as discussed in .

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 the

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

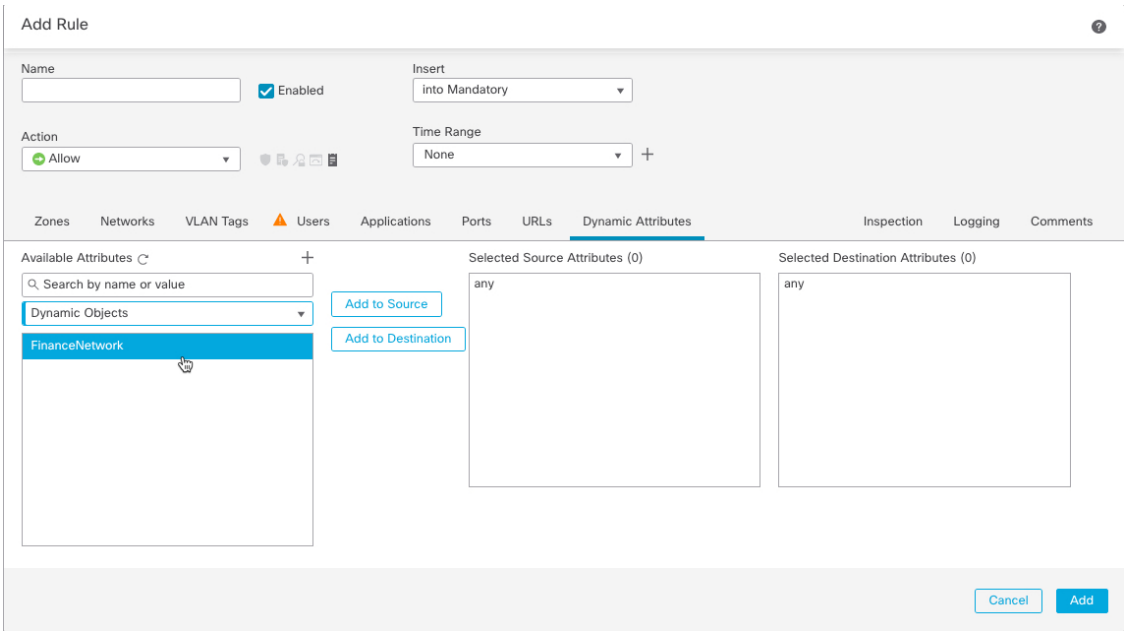
Step 3 Click **Edit** ( ) next to an access control policy.

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.



This example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the dynamic attributes connector.

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

Step 8 Add other conditions to the rule if desired.

Use dynamic objects in DNS policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the as dynamic objects, in DNS rules. For information about DNS policies, see .

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

You can use these dynamic objects on the DNS rule's Dynamic Attributes tab page, similarly to the way you use Security Group Tags (SGTs). You can add dynamic objects as source or destination attributes, except for endpoint device type objects, which are source only.

Procedure

Step 1 Click **Policies** > **Access Control heading** > **DNS** and create or edit a DNS policy.

Step 2 Add or edit a rule.

Step 3 Click the **Dynamic Attributes** tab.

Step 4 In the **Dynamic Attributes** list, select the objects you want to use, then add them to the source or destination lists as appropriate. Initially, all security group and dynamic objects are listed, by you can uncheck the Security Group option to see dynamic objects only.

Step 5 On the **DNS** tab, select the appropriate list or feed to match the DNS requests you are targeting.

Step 6 Add other conditions to the rule if desired and set the action.

Step 7 Click **Save**.

How to use network object groups from Cisco APIC in ASA access rules

The following topics show how to use network object groups from Cisco APIC in ASA access rules.

Related Topics

Add network object groups to access rules, on page 7
View network object groups in ASDM, on page 9

Add network object groups to access rules

To use dynamic network object groups from Cisco APIC to ASA access rules, you must add those objects as discussed in this task.

Before you begin

Complete all of the following tasks:

- Create a Cisco APIC connector
- Create an ASA adapter

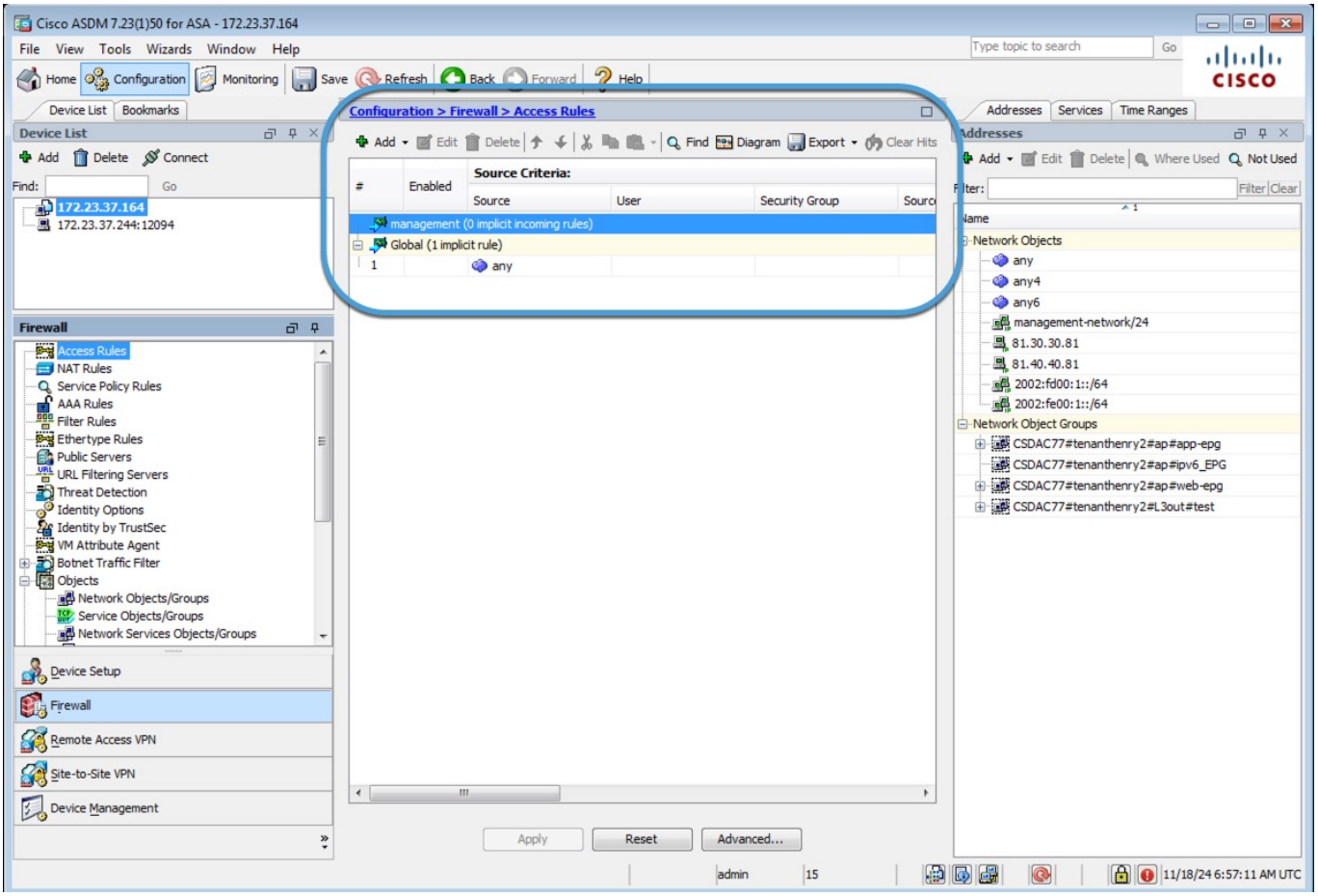
Procedure

Step 1 Log in to ASDM as a user with level 15 (administrator) privilege.

For more information about starting ASDM, see Start ASDM.

For more information about permissions, see Configure Management Remote Access.

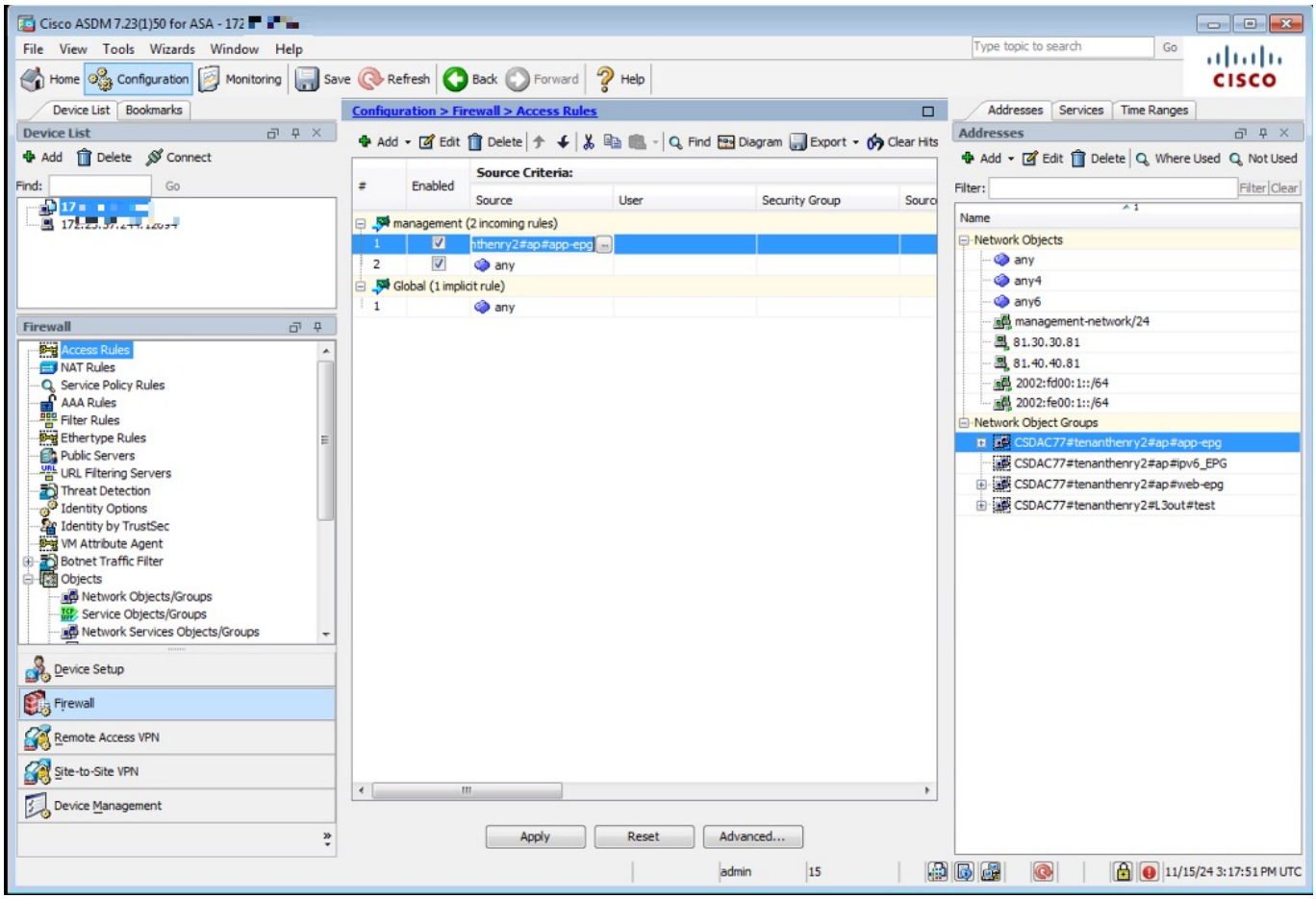
Step 2 Click **Configuration** > **Firewall** > **Access Rules** > **Network Objects/Groups**.
Access rules are displayed in the center pane as the following figure shows.



Step 3 Specify one or more network object groups as source criteria for the rule.

Double-click the **Source** field, then click to select a network object group for the rule.

The following figure shows an example.



Network object groups are named as follows: `SiteName#TenantName#ProfileName#EPGName`

Step 4 Follow the prompts on your screen to complete the action.

For more information, see Access Rules.

Related Topics

Add network object groups to access rules, on page 7
View network object groups in ASDM, on page 9

View network object groups in ASDM

This task is optional. To configure ASA access rules without viewing network object groups, see Add network object groups to access rules, on page 7.

Before you begin

Complete all of the following tasks:

- Create a Cisco APIC connector

- Create an ASA adapter

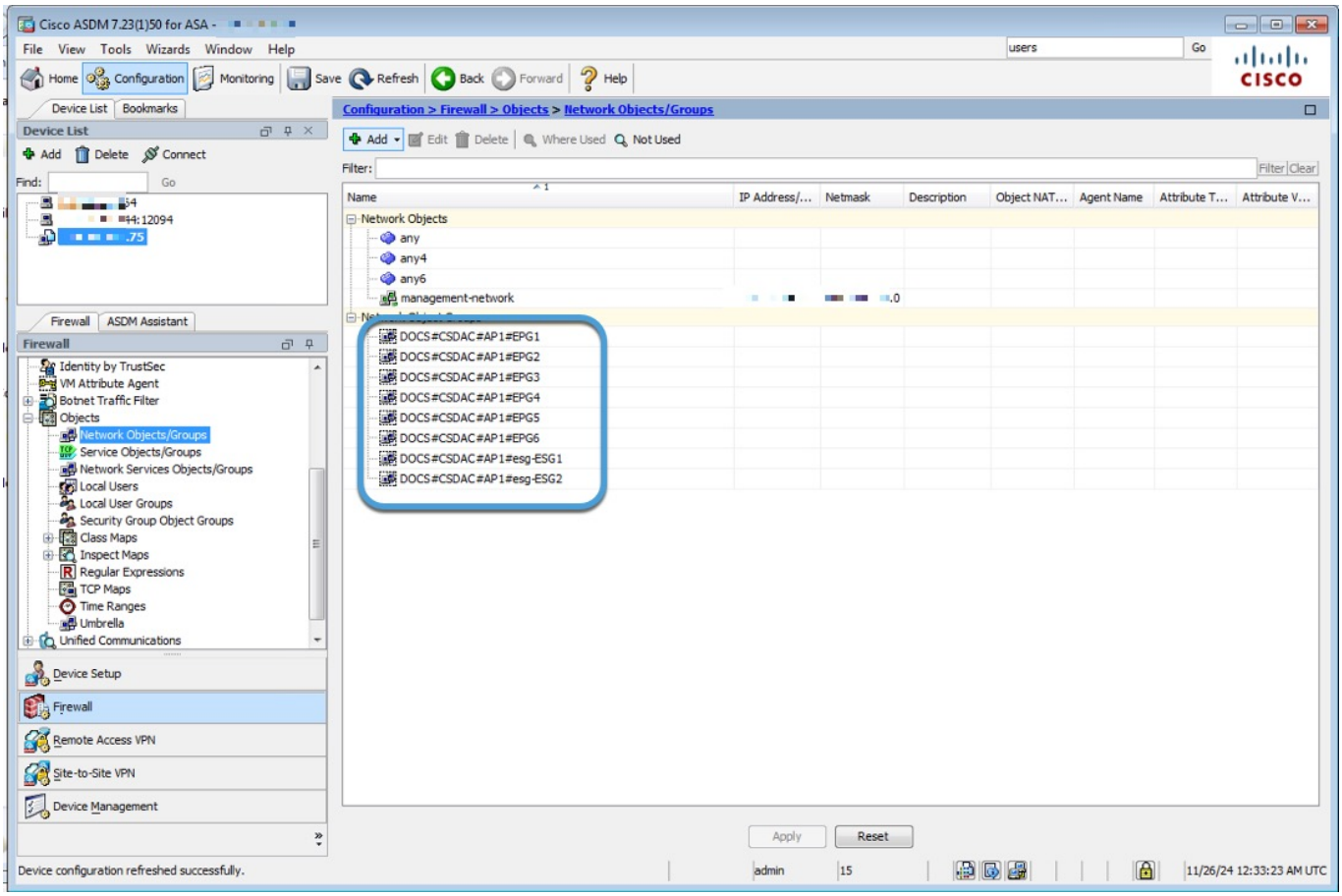
Procedure

Step 1 Log in to ASDM as a user with at least privilege level 15 (administrator).

For more information about starting ASDM, see Start ASDM.

For more information about permissions, see Configure Management Remote Access.

Step 2 Click **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**.
The network object groups are displayed in the right pane as the following figure shows.



Network object groups are named as follows: `SiteName#TenantName#ProfileName#EPGName`

What to do next

See Add network object groups to access rules, on page 7

Related Topics

Add network object groups to access rules, on page 7
View network object groups in ASDM, on page 9