NAT Policy Management

The following topics describe how to manage NAT policies for your Firepower System:

Requirements and Prerequisites for NAT Policies

Model Support

Any, but you must select the correct type of policy for the device model:

- **Firepower NAT** for 7000 & 8000 Series Series devices.
- **Threat Defense NAT** for FTD devices.

Supported Domains

Any

User Roles

Admin

Access Admin

Network Admin

Managing NAT Policies

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Administrators in ancestor domains can target NAT policies to devices in descendant domains, which descendant domains can use or replace with customized local policies. If a NAT policy targets devices in different descendant domains, administrators in the descendant domains can view information about target devices belonging to their domain only.

Procedure

Step 1 Choose **Devices** > **NAT** .

Step 2 Manage your NAT policies:

- Copy — Click **Copy** () next to the policy you want to copy; see Copying NAT Policies, on page 5.
- Create — Click **New Policy**; see Creating NAT Policies, on page 2.
- Delete — Click **Delete** () next to the policy you want to delete, then click **OK**. When prompted whether to continue, you are also informed if another user has unsaved changes in the policy.

  Caution After you have deployed a NAT policy to a managed device, you cannot delete the policy from the device. Instead, you must deploy a NAT policy with no rules to remove the NAT rules already present on the managed device. You also cannot delete a policy that is the last deployed policy on any of its target devices, even if it is out of date. Before you can delete the policy completely, you must deploy a different policy to those targets.

- Deploy—Click **Deploy**; see Deploy Configuration Changes.
- Edit — Click **Edit** (); see Configuring NAT Policies, on page 3.
- Report—Click **Report** (); see Generating Current Policy Reports.

Creating NAT Policies

When you create a new NAT policy you must, at minimum, give it a unique name. Although you are not required to identify policy targets at policy creation time, you must perform this step before you can deploy the policy. If you apply a NAT policy with no rules to a device, the system removes all NAT rules from that device.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Administrators in ancestor domains can target NAT policies to devices in descendant domains, which descendant domains can use or replace with customized local policies. If a NAT policy targets devices in different descendant domains, administrators in the descendant domains can view information about target devices belonging to their domain only.

Procedure

Step 1 Choose **Devices** > **NAT** .

Step 2 From the **New Policy** drop-down list, choose one of the following:

- **Firepower NAT** for 7000 & 8000 Series devices.
- **Threat Defense NAT** for Firepower Threat Defense devices.

Step 3 Enter a unique **Name**.

In a multidomain deployment, policy names must be unique within the domain hierarchy. The system may identify a conflict with the name of a policy you cannot view in your current domain.

Step 4 Optionally, enter a **Description**.

Step 5 Choose the devices where you want to deploy the policy:

- Choose a device in the **Available Devices** list, and click **Add to Policy**.
- Click and drag a device from the **Available Devices** list to the **Selected Devices** list.
- Remove a device from the **Selected Devices** list by clicking **Delete** ( ) next to the device.

Step 6 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Configuring NAT Policies

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Administrators in ancestor domains can target NAT policies to devices in descendant domains, which descendant domains can use or replace with customized local policies. If a NAT policy targets devices in different descendant domains, administrators in the descendant domains can view information about target devices belonging to their domain only.

If you change the type of an interface to a type that is not valid for use with a NAT policy that targets a device with that interface, the policy labels the interface as deleted. Click **Save** in the NAT policy to automatically remove the interface from the policy.

Note Rule attributes differ by NAT policy type. When adding or editing rules, click ? in the dialog box for more information, or see the relevant chapter: Network Address Translation (NAT) for Firepower Threat Defense or NAT for 7000 and 8000 Series Devices.

Procedure

Step 1 Choose **Devices** > **NAT** .

Step 2 Click **Edit** ( ) next to the NAT policy you want to modify.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Configure your NAT policies:

- To modify the policy name or description, click the **Name** or **Description** field, delete any characters as needed, then enter the new name or description. In a multidomain deployment, policy names must be unique within the domain hierarchy. The system may identify a conflict with the name of a policy you cannot view in your current domain.
- To manage policy targets, see Configuring NAT Policy Targets, on page 4.
- To save your policy changes, click **Save**.
- To add a rule to a policy, click **Add Rule**.
- To edit an existing rule, click **Edit** ( ) next to the rule.
- To delete a rule, click **Delete** ( ) next to the rule, then click **OK**.
- To enable or disable an existing rule, right-click a rule, choose **State**, and choose **Disable** or **Enable**.
- (Firepower NAT only) To display the configuration page for a specific rule attribute, click the name or value in the column for the condition on the row for the rule. For example, click the name or value in the **Source Networks** column to display the Source Network page for the selected rule.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Configuring NAT Policy Targets

You can identify the managed devices you want to target with your policy while creating or editing a policy. You can search a list of available devices, 7000 or 8000 Series stacks, and high-availability pairs, and add them to a list of selected devices.

You cannot target stacked devices running different versions of the Firepower System (for example, if an upgrade on one of the devices fails).

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Administrators in ancestor domains can target NAT policies to devices in descendant domains, which descendant domains can use or replace with customized local policies. If a NAT policy targets devices in different descendant domains, administrators in the descendant domains can view information about target devices belonging to their domain only.

Procedure

Step 1 Choose **Devices** > **NAT** .

Step 2 Click **Edit** ( ) next to the NAT policy you want to modify.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Click **Policy Assignments**.

Step 4 Do any of the following:

- To assign a device, stack, high-availability pair, or device group to the policy, select it in the **Available Devices** list and click **Add to Policy**. You can also drag and drop.
- To remove a device assignment, click **Delete** ( ) next to a device, stack, high-availability pair, or device group in the **Selected Devices** list.

Step 5 Click **OK**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Copying NAT Policies

You can make a copy of a NAT policy. The copy includes all policy rules and configurations.

In a multidomain deployment, you can copy policies from current and ancestor domains.

Procedure

Step 1 Choose **Devices** > **NAT** .

Step 2 Click **Copy** ( ) next to the NAT policy you want to copy.

Step 3 Enter a unique **Name** for the policy.

In a multidomain deployment, policy names must be unique within the domain hierarchy. The system may identify a conflict with the name of a policy you cannot view in your current domain.

Step 4 Click **OK**.