



NAT for 7000 and 8000 Series Devices

The following topics describe how to configure NAT for 7000 and 8000 Series devices:

- [NAT Policy Configuration, on page 1](#)
- [Rule Organization in a NAT Policy, on page 2](#)
- [Organizing NAT Rules, on page 3](#)
- [NAT Policy Rules Options, on page 4](#)

NAT Policy Configuration

You can configure NAT policies in different ways to manage specific network needs. You can:

- *Expose an internal server to an external network.*

In this configuration, you define a static translation from an external IP address to an internal IP address so the system can access an internal server from outside the network. Traffic sent to the server targets the external IP address or IP address and port, and is translated into the internal IP address or IP address and port. Return traffic from the server is translated back to the external address.

- *Allow an internal host/server to connect to an external application.*

In this configuration, you define a static translation from an internal address to an external address. This definition allows the internal host or server to initiate a connection to an external application that is expecting the internal host or server to have a specific IP address and port. Therefore, the system cannot dynamically allocate the address of the internal host or server.

- *Hide private network addresses from an external network.*

You can obscure your internal network addresses using either of the following configurations:

- If you have a sufficient number of external IP addresses to satisfy your internal network needs, you can use a block of IP addresses. In this configuration, you create a dynamic translation that automatically converts the source IP address of any outgoing traffic to an unused IP address from your externally facing IP addresses.
- If you have an insufficient number of external IP addresses to satisfy your internal network needs, you can use a limited block of IP addresses and port translation. In this configuration, you create a dynamic translation that automatically converts the source IP address and port of outgoing traffic to an unused IP address and port from your externally facing IP addresses.



Caution In 7000 or 8000 Series device high-availability pairs, only select an individual peer interface for a static NAT rule on a paired device if all networks affected by the NAT translations are private. Do **not** use configurations for static NAT rules affecting traffic between public and private networks.

NAT Policies Configuration Guidelines

To configure a NAT policy, you must give the policy a unique name and identify the devices, or *targets*, where you want to deploy the policy. You can also add, edit, delete, enable, and disable NAT rules. After you create or modify a NAT policy, you can deploy the policy to all or some targeted devices.

You can deploy NAT policies to a 7000 or 8000 Series device high-availability pair, including paired stacks, as you would a standalone device. However, you can define static NAT rules for interfaces on individual paired devices or the entire high-availability pair and use the interfaces in source zones. For dynamic rules, you can use only the interfaces on the whole high-availability pair in source or destination zones.



Caution In 7000 or 8000 Series device high-availability pairs, only select an individual peer interface for a static NAT rule on a paired device if all networks affected by the NAT translations are private. Do **not** use this configuration for static NAT rules affecting traffic between public and private networks.

If you configure dynamic NAT on a device high-availability pair without HA link interfaces established, both paired devices independently allocate dynamic NAT entries, and the system cannot synchronize the entries between devices.

You can deploy NAT policies to a device stack as you would a standalone device. If you establish a device stack from devices that were included in a NAT policy and had rules associated with interfaces from the secondary device that was a member of the stack, the interfaces from the secondary device remain in the NAT policy. You can save and deploy policies with the interfaces, but the rules do not provide any translation.

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.

Rule Organization in a NAT Policy

The Edit page for the NAT policy lists static NAT rules and dynamic NAT rules separately. The system sorts static rules alphabetically by name, and you cannot change the display order. You cannot create static rules with identical matching values. The system inspects static translations for a match before it inspects any dynamic translations.

Dynamic rules are processed in numerical order. The numeric position of each dynamic rule appears on the left side of the page next to the rule. You can move or insert dynamic rules and otherwise change the rule order. For example, if you move dynamic rule 10 under dynamic rule 3, rule 10 becomes rule 4 and all subsequent numbers increment accordingly.

A dynamic rule's position is important because the system compares packets to dynamic rules in the rules' numeric order on the policy Edit page. When a packet meets all the conditions of a dynamic rule, the system applies the conditions of that rule to the packet and ignores all subsequent rules for that packet.

You can specify a dynamic rule's numeric position when you add or edit a dynamic rule. You can also highlight a dynamic rule before adding a new dynamic rule to insert the new rule below the rule you highlighted.

You can select one or more dynamic rules by clicking a blank space in the row for the rule. You can drag and drop selected dynamic rules into a new location, thereby changing the position of the rules you moved and all subsequent rules.

You can cut or copy selected rules and paste them above or below an existing rule. You can only paste static rules in the Static Translations list and only dynamic rules in the Dynamic Translations list. You can also delete selected rules and insert new rules into any location in the list of existing rules.

You can display explanatory warnings to identify rules that will never match because they are preempted by preceding rules.


If you have access control policies in your deployment, the system does not translate traffic until it has passed through access control.


Organizing NAT Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin



Procedure

Step 1 Choose **Devices > NAT** .

Step 2 Click the edit icon () 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 Organize your NAT rules:

- To choose a rule, click a blank area in the row for a rule.
- To clear rule selections, click the reload icon () on the lower right side of the page. To clear individual rules, click a blank area in a rule's row while holding the Ctrl key.
- To cut or copy selected rules, right-click a blank area in the row for a selected rule, then select **Cut** or **Copy**.
- To paste rules you have cut or copied into the rule list, right-click a blank area in the row for a rule where you want to paste selected rules, then select **Paste above** or **Paste below**.
- To move selected rules, drag and drop selected rules beneath a new location, indicated by a horizontal blue line that appears above your pointer as you drag.
- To delete a rule, click the delete icon () next to the rule, then click **OK**.
- To show warnings, click **Show Warnings**.

NAT Rule Warnings and Errors

The conditions of a NAT rule may preempt a subsequent rule from matching traffic. Any type of rule condition can preempt a subsequent rule.





A rule also preempts an identical subsequent rule where all configured conditions are the same. A subsequent rule would not be preempted if any condition were different.

If you create a rule that causes the NAT policy to fail upon deploy, an error icon () appears next to the rule. An error occurs if there is a conflict in the static rules, or if you edit a network object used in the policy that now makes the policy invalid. For example, an error occurs if you change a network object to use only IPv6 addresses and the rule that uses that object no longer has any valid networks where at least one network is required. Error icons appear automatically; you do not have to click **Show Warnings**.

Showing and Hiding NAT Rule Warnings

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin

Procedure

-
- Step 1** Choose **Devices > NAT** .
- Step 2** Click the edit icon () 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** To show warnings, click **Show Warnings**.
- The page updates with a warning icon () next to each preempted rule.
- Step 4** To display the warning for a rule, hover your pointer over the warning icon () next to a rule. A message indicates which rule preempts the rule.
- Step 5** To clear warnings, click **Hide Warnings**.
- The page refreshes and the warnings disappear.
-

NAT Policy Rules Options

A NAT rule is simply a set of configurations and conditions that:

- qualifies network traffic
- specifies how the traffic that matches those qualifications is translated

You create and edit NAT rules from within an existing NAT policy. Each rule belongs to only one policy.

The web interface for adding or editing a rule is similar. You specify the rule name, state, type, and position (if dynamic) at the top of the page. You build conditions using the tabs on the left side of the page; each condition type has its own tab.

The following list summarizes the configurable components of a NAT rule.

Name

Give each rule a unique name. For static NAT rules, use a maximum of 22 characters. For dynamic NAT rules, use a maximum of 30 characters. You can use printable characters, including spaces and special characters, with the exception of the colon (:).

Rule State

By default, rules are enabled. If you disable a rule, the system does not use it to evaluate network traffic for translation. When viewing the list of rules in a NAT policy, disabled rules are grayed out, although you can still modify them.

Type

A rule's type determines how the system handles traffic that matches the rule's conditions. When you create and edit NAT rules, the configurable components vary according to rule type.

Position (Dynamic Rules Only)

Dynamic rules in a NAT policy are numbered, starting at 1. The system matches traffic to NAT rules in top-down order by ascending rule number.

When you add a rule to a policy, you specify its position by placing it **above** or **below** a specific rule, using rule numbers as a reference point. When editing an existing rule, you can **Move** the rule in a similar fashion.

Conditions

Rule conditions identify the specific traffic you want to translate. Conditions can match traffic by any combination of multiple attributes, including security zone, network, and transport protocol port.

Related Topics

[Creating and Editing NAT Rules](#), on page 5

Creating and Editing NAT Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin

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

Procedure

Step 1 Choose **Devices > NAT** .

Step 2 Click the edit icon (✎) next to the NAT policy where you want to add a rule.

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

Step 3 Add a new rule or edit an existing rule:

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click the edit icon (✎) next to the rule you want to edit.

Step 4 Enter a unique rule **Name**.

Step 5 Configure the following rule components:

- Specify whether the rule is **Enabled**.
- Specify a rule **Type**.
- Specify the rule position (dynamic rules only).
- Configure the rule's conditions.

Note Static rules must include an original destination network. Dynamic rules must include a translated source network.

Step 6 Click **Add**.

Step 7 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

NAT Rule Types

Every NAT rule has an associated type that:

- qualifies network traffic
- specifies how the traffic that matches those qualifications is translated

The following list summarizes the NAT rule types.

Static

Static rules provide one-to-one translations on destination networks and optionally port and protocol. When configuring static translations, you can configure source zones, destination networks, and destination ports. You cannot configure destination zones or source networks.

You **must** specify an original destination network. For destination networks, you can only select network objects and groups containing a single IP address or enter literal IP addresses that represent a single IP address. You can only specify a single original destination network and a single translated destination network.



Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

You can specify a single original destination port and a single translated destination port. You must specify an original destination network before you can specify an original destination port. In addition, you cannot specify a translated destination port unless you also specify an original destination port, and the translated value must match the protocol of the original value.



Caution For static NAT rules on a 7000 or 8000 Series device in a high-availability pair, only select an individual peer interface if all networks affected by the NAT translations are private. Do **not** use this configuration for static NAT rules affecting traffic between public and private networks.

Dynamic IP Only

Dynamic IP Only rules translate many-to-many source networks, but maintain port and protocol. When configuring dynamic IP only translations, you can configure zones, source networks, original destination networks, and original destination ports. You cannot configure translated destination networks or translated destination ports.

You **must** specify at least one translated source network. If the number of translated source network values is less than the number of original source networks, the system displays a warning on the rule that it is possible to run out of translated addresses before all original addresses are matched.

If there are multiple rules with conditions that match the same packet, the low priority rules become dead, meaning they can never be triggered. The system also displays warnings for dead rules. You can view tooltips to determine which rule supersedes the dead rule.



Note You can save and deploy policies with dead rules, but the rules cannot provide any translation.

In some instances, you may want to create rules with limited scope preceding rules with a broader scope. For example:

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

In this example, rule 1 matches some packets that also match rule 2. Therefore, rule 2 is not completely dead.

If you specify only original destination ports, you cannot specify translated destination ports.

Dynamic IP + Port

Dynamic IP and port rules translate many-to-one or many-to-many source networks and port and protocol. When configuring dynamic IP and port translations, you can configure zones, source networks, original

destination networks, and original destination ports. You cannot configure translated destination networks or translated destination ports.

You **must** specify at least one translated source network. If there are multiple rules with conditions that match the same packet, the low priority rules become dead, meaning they can never be triggered. The system also displays warnings for dead rules. You can view tool tips to determine which rule supersedes the dead rule.



Note You can save and deploy policies with dead rules, but the rules cannot provide any translation.

If you specify only original destination ports, you cannot specify translated destination ports.



Note If you create a dynamic IP and port rule, and the system passes traffic that does not use a port, no translation occurs for the traffic. For example, a ping (ICMP) from an IP address that matches the source network does not map, because ICMP does not use a port.

NAT Rule Condition Types

The following table summarizes the NAT rule condition types that can be configured based on the specified NAT rule type:

Table 1: Available NAT Rule Condition Types per NAT Rule Type

Condition	Static	Dynamic (IP Only or IP + Port)
Source Zones	Optional	Optional
Destination Zones	Not allowed	Optional
Original Source Networks	Not allowed	Optional
Translated Source Networks	Not allowed	Required
Original Destination Networks	Required	Optional
Translated Destination Networks	Optional; single address only	Not allowed
Original Destination Ports	Optional; single port only, and only allowed if you define the original destination network	Optional
Translated Destination Ports	Optional; single port only, and only allowed if you define the original destination port	Not allowed

NAT Rule Conditions and Condition Mechanics

You can add conditions to NAT rules to identify the type of traffic that matches the rule. For each condition type, you select conditions you want to add to a rule from a list of available conditions. When applicable, condition filters allow you to constrain available conditions. Lists of available and selected conditions may

be as short as a single condition or many pages long. You can search available conditions and display only those matching a typed name or value in a list that updates as you type.

Depending on the type of condition, lists of available conditions may be comprised of a combination of conditions provided directly by Cisco or configured using other Firepower System features, including objects created using the object manager (**Objects > Object Management**), objects created directly from individual conditions pages, and literal conditions.

NAT Rule Conditions

You can set a NAT rule to match traffic meeting any of the conditions described in the following table:

Table 2: NAT Rule Condition Types

Condition	Description
Zones	A configuration of one or more routed interfaces where you can deploy NAT policies. Zones provide a mechanism for classifying traffic on source and destination interfaces, and you can add source and destination zone conditions to rules.
Networks	Any combination of individual IP addresses, CIDR blocks, and prefix lengths, either specified explicitly or using network objects and groups. You can add source and destination network conditions to NAT rules.
Destination Ports	Transport protocol ports, including individual and group port objects you create based on transport protocols.

Adding Conditions to NAT Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin


Adding conditions to NAT rules is essentially the same for each type of condition. You choose from a list of available conditions on the left, and add the conditions you chose to one or two lists of selected conditions on the right.


For all condition types, you choose one or more individual available conditions by clicking on them to highlight them. You can either click a button between the two types of lists to add available conditions that you choose to your lists of selected conditions, or drag and drop available conditions that you choose into the list of selected conditions.

You can add up to 50 conditions of each type to a list of selected conditions. For example, you can add up to 50 source zone conditions, up to 50 destination zone conditions, up to 50 source network conditions, and so on, until you reach the upper limit for the appliance.

Procedure

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

Step 2 Click the edit icon () 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 **Add Rule**.

Step 4 Enter a **Name** for the rule.





Step 5 Specify a **Type** for the rule.

Step 6 Click the tab for the type of condition you want to add to the rule.

Step 7 Take any of the following actions:

- To choose available conditions to add to a list of selected conditions, click the available condition.
- To choose all listed available conditions, right-click the row for any available condition, then click **Select All**.
- To choose a list of available conditions or filters, click inside the **Search** field and enter a search string. The list updates as you type to display matching items.

You can search on object names and on the values configured for objects. For example, if you have an individual network object named `Texas Office` with the configured value `192.168.3.0/24`, and the object is included in the group object `US Offices`, you can display both objects by entering a partial or complete search string such as `Tex`, or by entering a value such as `3`.

- To clear a search when searching available conditions or filters, click the reload icon () above the Search field or the clear icon () in the Search field.
- To add selected zone conditions from a list of available conditions to a list of selected source or destination conditions, click **Add to Source** or **Add to Destination**.
- To add selected network and port conditions from a list of available conditions to a list of selected original or translated conditions, click **Add to Original** or **Add to Translated**.
- To drag and drop selected available conditions into a list of selected conditions, click a selected condition, then drag and drop into the list of selected conditions.
- To add a literal condition to a list of selected conditions using a literal field, click to remove the prompt from the literal field, enter the literal condition, and click **Add**. Network conditions provide a field for adding literal conditions.
- To add a literal condition to a list of selected conditions using a drop-down list, choose a condition from the drop-down list, then click **Add**. Port conditions provide a drop-down list for adding literal conditions.
- To add an individual object or condition filter so you can then choose it from the list of available conditions, click the add icon ()
- To delete a single condition from a list of selected conditions, click the delete icon () next to the condition.
- To delete a condition from a list of selected conditions, right-click to highlight the row for a selected condition, then click **Delete**.

Step 8 Click **Add** to save your configuration.

Literal Conditions in NAT Rules

You can add a literal value to the list of original and translated conditions for the following condition types:

- Networks
- Ports

For network conditions, you type the literal value in a configuration field below the list of original or translated conditions.

In the case of port conditions, you choose a protocol from a drop-down list. When the protocol is `ALL`, or `TCP` or `UDP`, you enter a port number in a configuration field.

Each relevant conditions page provides the controls needed to add literal values. Values you enter in a configuration field appear as red text if the value is invalid, or until it is recognized as valid. Values change to blue text as you type when they are recognized as valid. A grayed **Add** button activates when a valid value is recognized. Literal values you add appear immediately in the list of selected conditions.



Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

Objects in NAT Rule Conditions

Objects that you create in the object manager (**Objects > Object Management**) are immediately available for you to select from relevant lists of available NAT rule conditions.

You can also create objects on-the-fly from the NAT policy. A control on relevant conditions pages provides access to the same configuration controls that you use in the object manager.

Individual objects created on-the-fly appear immediately in the list of available objects. You can add them to the current rule, and to other existing and future rules. On the relevant conditions page, and also on the policy Edit page, you can hover your pointer over an individual object to display the contents of the object, and over a group object to display the number of individual objects in the group.


Zone Conditions in NAT Rules

The security zones on your system are comprised of interfaces on your managed devices. Zones that you add to a NAT rule target the rule to devices on your network that have routed or hybrid interfaces in those zones. You can only add security zones with routed or hybrid interfaces as conditions for NAT rules.

You can add either zones or standalone interfaces that are currently assigned to a virtual router to NAT rules.

If there are devices with un-deployed device configurations, the Zones page displays a warning icon (⚠) at the top of the available zones list, indicating that only deployed zones and interfaces are displayed. You can click the arrow icon (▾) next to a zone to collapse or expand the zone to hide or view its interfaces.

If an interface is on a 7000 or 8000 Series device in a high-availability pair, the available zones list displays an additional branch from that interface with the other interfaces in the high-availability pair as children of

the primary interface on the active device in the high-availability pair. You can also click the arrow icon () to collapse or expand the paired device interfaces to hide or view its interfaces.



Note You can save and deploy policies with disabled interfaces, but the rules cannot provide any translation until the interfaces are enabled.

The two lists on the right are the source and destination zones used for matching purposes by the NAT rules. If the rule already has values configured, these lists display the existing values when you edit the rule. If the source zones list is empty, the rule matches traffic *from* any zone or interface. If the destination zones list is empty, the rule matches traffic *to* any zone or interface.

The system displays warnings for rules with zone combinations that never trigger on a targeted device.



Note You can save and deploy policies with these zone combinations, but the rules will not provide any translation.

You can add individual interfaces by selecting an item in a zone or by selecting a standalone interface. You can only add interfaces in a zone if the zone it is assigned to has not already been added to a source zones or destination zones list. These individually selected interfaces are not affected by changes to zones, even if you remove them and add them to a different zone. If an interface is the primary member of a high-availability pair and you are configuring a dynamic rule, you can add only the primary interface to the source zones or destination zones list. For static rules, you can add individual high-availability pair member interfaces to the source zones list. You can only add a primary high-availability pair interface to a list if none of its children have been added, and you can only add individual high-availability pair interfaces if the primary has not been added.

If you add a zone, the rule uses all interfaces associated with the zone. If you add or remove an interface from the zone, the rule will not use the updated version of the zone until the device configuration has been re-deployed to the devices where the interfaces reside.





Note In a static NAT rule, you can add only source zones. In a dynamic NAT rule, you can add both source and destination zones.

Adding Zone Conditions to NAT Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin

Procedure

- Step 1** Choose **Devices > NAT** .
- Step 2** Click the edit icon () 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 **Add Rule**.

Step 4 Enter a **Name** for the rule.

Step 5 Specify a **Type** for the rule.

Step 6 Click the **Zones** tab.

Step 7 Click a zone or interface in the **Available Zones** list.

Step 8 You have the following choices:

- To match traffic by source zone, click **Add to Source**.
- To match traffic by destination zone, click **Add to Destination**.

Note You can add only source zones to static NAT rules. Additionally, while you can add disabled interfaces to a NAT rule, the rule does not provide any translation.

Step 9 Click **Add** to save the new rule.

Step 10 Click **Save** to save the changed policy.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Source Network Conditions in Dynamic NAT Rules

You configure the matching values and translation values of the source IP address for packets. If the original source network is not configured, then any source IP address matches the dynamic NAT rule. Note that you cannot configure source networks for static NAT rules. If a packet matches the NAT rule, the system uses the values in the translated source network to assign the new value for the source IP address. For dynamic rules, you must configure a translated source network with at least one value.



Caution If a network object or object group is being used by a NAT rule, and you change or delete the object or group, it can cause the rule to become invalid.

You can add any of the following kinds of source network conditions to a dynamic NAT rule:

- individual and group network objects that you have created using the object manager
- individual network objects that you add from the Source Network conditions page, and can then add to your rule and to other existing and future rules
- literal, single IP addresses, ranges, or address blocks






Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

Adding Network Conditions to a Dynamic NAT Rule

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin

When you update the network conditions in a dynamic rule in use in a deployed policy, the system drops any network sessions using the existing translated address pool.

Procedure

-
- Step 1** Choose **Devices > NAT** .
- Step 2** Click the edit icon () 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 **Add Rule**.
- Step 4** Enter a **Name** for the rule.
- Step 5** Specify a dynamic **Type** for the rule:
- **Dynamic IP Only**
 - **Dynamic IP + Port**
- Step 6** Click the **Source Networks** tab.
- Step 7** Optionally, add an individual network object to the **Available Networks** list by clicking the add icon () above the list.
- You can add multiple IP addresses, CIDR blocks, and prefix lengths to each network object.
- Step 8** Click a condition in the **Available Networks** list.
- Step 9** You have the following choices:
- To match traffic by original source network, click **Add to Original**.
 - To specify the translation value for traffic that matches the translated source network, click **Add to Translated**.
- Step 10** To add a literal IP address, range, or address block:
- a) Click the **Enter an IP address** prompt below the **Original Source Network** or **Translated Source Network** list.
 - b) Enter an IP address, range, or address block.

You add ranges in the following format: lower IP address-upper IP address. For example:
179.13.1.1-179.13.1.10.

Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

c) Click **Add** next to the value you entered.

Step 11 Click **Add** to save the rule.

Step 12 Click **Save** to save the changed policy.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Destination Network Conditions in NAT Rules

You configure the matching values and translation values of the destination IP address for packets. Note that you cannot configure translated destination networks for dynamic NAT rules.

Because static NAT rules are one-to-one translations, the **Available Networks** list contains only network objects and groups that contain only a single IP address. For static translations, you can add only a single object or literal value to both the **Original Destination Network** or **Translated Destination Network** lists.



Caution If a network object or object group is being used by a NAT rule, and you change or delete the object or group, it can cause the rule to become invalid.

You can add any of the following kinds of destination network conditions to a NAT rule:

- individual and group network objects that you have created using the object manager
- individual network objects that you add from the Destination Network conditions page, and can then add to your rule and to other existing and future rules
- literal, single IP addresses, range, or address blocks

For static NAT rules, you can add only a CIDR with subnet mask /32, and only if there is not already a value in the list.



Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

Adding Destination Network Conditions to NAT Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin

When you update the network conditions in a dynamic rule in use in a deployed policy, the system drops any network sessions using the existing translated address pool.

Procedure

-
- Step 1** Choose **Devices > NAT** .
- Step 2** Click the edit icon (✎) 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 **Add Rule**.
- Step 4** Enter a **Name** for the rule.
- Step 5** Specify a **Type** for the rule.
- Step 6** Click the **Destination Network** tab.
- Step 7** Optionally, add an individual network object to the **Available Networks** list by clicking the add icon (+) above the list.
- For dynamic rules, you can add multiple IP addresses, CIDR blocks, and prefix lengths to each network object. For static rules, you can add only a single IP address.
- Step 8** Click a condition or object in the **Available Networks** list.
- Step 9** You have the following choices:
- To match traffic by original destination network, click **Add to Original**.
 - To specify the translation value for traffic that matches the translated destination network, click **Add to Translated**.
- Step 10** Optionally, click the **Enter an IP address** prompt below the **Original Destination Network** or **Translated Destination Network** list, enter an IP address or address block, and click **Add**.
- Step 11** Click **Add**.
- Step 12** Click **Save** to save the changes to the policy.
-

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Port Conditions in NAT Rules

You can add a port condition to a rule to match network traffic based on the original and translated destination port and transport protocol for translation. If the original port is not configured, any destination port matches the rule. If a packet matches the NAT rule and a translated destination port is configured, the system translates the port into that value. Note that for dynamic rules, you can specify only the original destination port. For static rules, you can define a translated destination port, but only with an object with the same protocol as the original destination port object or literal value.

The system matches the destination port against the value of the port object or literal port in the original destination port list for static rules, or multiple values for dynamic rules.

Because static NAT rules are one-to-one translations, the **Available Ports** list contains only port objects and groups that contain only a single port. For static translations, you can add only a single object or literal value to both the **Original Port** or **Translated Port** lists.

For dynamic rules, you can add a range of ports. For example, when specifying the original destination port, you can add 1000-1100 as a literal value.



Caution If a port object or object group is being used by a NAT rule, and you change or delete the object or group, it can cause the rule to become invalid.

You can add any of the following kinds of port conditions to a NAT rule:

- individual and group port objects that you have created using the object manager
- individual port objects that you add from the Destination Ports conditions page, and can then add to your rule and to other existing and future rules
- literal port values, consisting of a TCP, UDP, or All (TCP and UDP) transport protocol and a port

Adding Port Conditions to NAT Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Any	Admin/Network Admin

Procedure

Step 1 Choose **Devices > NAT** .

Step 2 Click the edit icon (✎) 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 **Add Rule**.

Step 4 Enter a **Name** for the rule.

Step 5 Specify a **Type** for the rule.

- Step 6** Click the **Destination Port** tab.
- Step 7** Optionally, add an individual port object to the **Available Ports** list by clicking the add icon (+) above the list.
- You can identify a single port or a port range in each port object that you add. You can then choose objects you added as conditions for your rule. For static rules, you can use only port objects with single ports.
- Step 8** Click a condition in the **Available Ports** list.
- Step 9** You have the following choices:
- Click **Add to Original**.
 - Click **Add to Translated**.
 - Drag and drop available ports into a list.
- Step 10** To add a literal port:
- a) Choose an entry from the **Protocol** drop-down list beneath the **Original Port** or **Translated Port** lists.
 - b) Enter a port.
 - c) Click **Add**.
- For dynamic rules, you can specify a single port or a range.
- Step 11** Click **Add**.
- Step 12** Click **Save** to save the changes to the policy.
-

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).