Configuring Network Address Translation

The topics in this chapter describe defining and managing Network Address Translation (NAT) rules.

- Address Translation Overview, page 1
- Managing NAT Rules, page 5

Address Translation Overview

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. As part of the process, the device also records the substitution in a translation database; these records are known as “xlate” entries. The appropriate xlate entry must exist to allow address translation on return packets—the substitution of the original real address for the mapped address; this procedure is sometimes referred to as “untranslation.” Thus, network address translation (NAT) actually consists of two steps: the translation of a real address into a mapped address, and the reverse translation for returning traffic.

Cisco devices support both NAT, which provides a globally unique address for each outbound host session, and Port Address Translation (PAT), which provides one address combined with a unique port number, for up to 64,000 simultaneous outbound or inbound host sessions. The global addresses used for NAT come from a pool of addresses specifically designated for address translation. The unique global address that is used for PAT can be either one global address, or the IP address of a given interface.

A security device translates an address when an existing NAT rule matches a specific traffic flow. If no NAT rule matches, processing for the packet continues. The exception is when you enable NAT control—NAT control requires that packets traversing from a higher security interface (inside) to a lower security interface (outside) match a NAT rule, or processing for the packet stops.

Cisco devices can perform NAT or PAT on both inbound and outbound connections. This ability to translate inbound addresses is called “Outside NAT” because addresses on the outside, or less secure, interface are translated to a usable inside IP address. Just as when you translate outbound traffic, you may choose dynamic NAT, static NAT, dynamic PAT, or static PAT. If necessary, you can use outside NAT together with inside NAT to translate the both source and destination IP addresses of a packet.
In this document, all types of translation are generally referred to as NAT; see Address Translation Definitions, on page 2 for descriptions of the various types. When describing NAT, the terms inside and outside represent the security relationship between any two interfaces. The higher security level is inside and the lower security level is outside.

Address Translation Definitions

The release of ASA version 8.3 introduced a simplified approach to configuring network address translation (NAT), as compared to earlier ASA versions and other devices. Configuration of NAT was simplified by replacing the earlier flow-based scheme with an “original packet” to “translated packet” approach.

NAT rules are no longer dependent on security levels. A global address space consisting of all interfaces is available, and is specified using the keyword “any.” All Interface fields default to any, so unless a specific interface is provided, the rule is applicable to all interfaces.

The following table briefly describes the available types of address translation.

**Table 1: Types of Address Translation**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static NAT</td>
<td>Fixed translation of real source addresses to specific mapped addresses—each source address is always translated to the same mapped address, regardless of IP protocol and port number. A “bi-directional” rule is a static rule that operates as two paired rules, one each for outgoing and incoming translation of the specified source and destination values.</td>
</tr>
<tr>
<td>Static PAT</td>
<td>Fixed translation of real source addresses with specific TCP or UDP port numbers, to specific mapped addresses and ports. That is, each source address/port is always translated to the same mapped address/port.</td>
</tr>
<tr>
<td>Dynamic NAT</td>
<td>Dynamic translation of real source addresses to mapped addresses obtained from a pool of shared addresses. Each source address can be mapped to any available address in the pool.</td>
</tr>
<tr>
<td>Dynamic PAT</td>
<td>Translation of real source addresses to a single mapped address; singularity is provided by dynamic translation of related port numbers. That is, each real address/port combination is translated to the same mapped address, but assigned a unique port. This is sometimes referred to as “overloading.”</td>
</tr>
<tr>
<td>Policy Static NAT</td>
<td>Fixed translation of real source addresses to specific mapped addresses. Destination networks/hosts are also specified, and the service is always IP.</td>
</tr>
</tbody>
</table>
### Network Object NAT

You also can define NAT properties on Network objects, such that corresponding NAT rules are applied automatically to the designated security device. Using these objects means you need enter the necessary IP addresses, services, and interfaces only once. These automatically generated, object-based rules are referred to as "Network Object NAT" rules.

### Destination Translation

With manual static rules, in addition to source address translation, you also can configure destination address translation. Source and destination translation are defined at the same time, in the same screen. Again, while source translation can be static or dynamic, destination translation is always static, and is only available with manual rules.

### Twice NAT

Creating a manual static rule will produce an entry in the rules table that actually represents two static NAT rules, encompassing both translation directions. That is, a static rule is created for the specified source/translated address pairing, along with a mirror rule for the translated address/source pairing. This is referred to as "Twice NAT" because only one look-up is required to fetch and process what is in effect two rules.

### PAT Pools and Round Robin Allocation

Adaptive Security Appliances, version 8.4.2 and later, include two features that let you alter how port address translation (PAT) occurs: you can explicitly define a pool of IP addresses specifically for PAT, and you can select a "round robin" algorithm for port allocation during PAT processing.

These features simplify configuration of large numbers of PAT addresses, and help prevent a large number of connections from a single PAT address, which can appear to be part of a DoS attack.

### Explicit PAT Pool Definition
Prior to version 8.4.2, when you defined a Dynamic NAT and PAT rule, you provided a “pool” of IP addresses (in the Original packet Source field of the Twice NAT Rule Properties, on page 6) to be used for translation. This pool could consist of individual IP addresses, ranges of addresses, Network objects, or Network Group objects, and combinations thereof.

Ranges and objects with more than one IP address were considered to be in the “NAT Pool,” while individual IP addresses and group objects consisting of one or more individual addresses were considered to be part of the “PAT Pool.”

Address translation on the device would work its way through the NAT Pool until all available addresses were exhausted. Port address translation would then begin using the PAT Pool—assigning ports on the first IP address in the PAT Pool until all ports (approximately 64,000) are assigned, then assigning ports on the next address in the pool, and so on. When all ports are fully subscribed on all IP addresses in the PAT Pool, no further translation could occur.

On version 8.4.2 and later ASA devices, you can explicitly define a separate PAT Pool for a Dynamic NAT and PAT rule. If you do so, the first collection of addresses (defined in the Original packet Source field) is considered the NAT Pool, while the PAT Pool addresses are specified in the Translated packet Source field.

**Note**

If you do not explicitly specify a PAT Pool, address translation takes place as described for pre-8.4.2 devices.

Refer to Managing NAT Rules, on page 5 for more information about the defining translation rules.

**Round Robin Port Assignment**

On version 8.4.2 and later ASA devices, you also can specify an alternate method of port assignment during PAT processing. As mentioned earlier, PAT port numbers are assigned to a single IP address in succession until the final port number is assigned, and then the process begins again with the next available IP address in the pool.

However, a new parameter on 8.4.2 and later devices—Use round robin allocation—lets you specify "round robin" cycling through available IP addresses and port numbers. This method assigns an address/port combination using each successive address in the pool; it then uses the first address again with a different port, proceeds to the second address again, and so on.

Further, the round-robin algorithm incorporates two additional principles it will attempt to adhere to when assigning address/port combinations during PAT processing:

- If a specific source-to-destination mapping already exists, the algorithm attempts to use the existing translation for the new connection. If this is not possible (for example, when all ports for that IP address have been exhausted), the algorithm proceeds with standard round-robin cycling.

- If possible, the original source port number is used as the mapped port number. That is, if the port number of the address/port combination to be translated is 4904, for example, and 4904 is available with the next IP address in the PAT Pool, the translated address will be PAT_address/4904. If this is not possible (that port is not available with the next PAT address), the algorithm proceeds with standard round-robin cycling.

**Note**

If you do not explicitly specify Round Robin Allocation, port-allocation cycling occurs as described for pre-8.4.2 devices.
Managing NAT Rules

You can add, edit and delete NAT rules that are available to the entire device repository, and you can add, edit and delete the rules assigned to an individual device. Repository rules are assigned to all the devices in the inventory.

Procedure

Step 1  To manage NAT rules, select Configurations > Policies/Settings.
Step 2  Select the desired device: be sure Devices is chosen in the Policies/Settings view selector, and then select the device you want to manage from the Devices list.
Step 3  Click the NAT policies tab to view the NAT rules table. This table consist of three sections: the Twice NAT (Before Object NAT) rules, the Network Object rules (these are the "automatic" rules), and the Twice NAT (After Object NAT) rules. The Before and After rules are processed before and after the "automatic" rules, respectively.
Step 4  Add, edit, delete, duplicate, and enable/disable specific rules, as necessary. (General policy management is described in Policy Basics.)

  • To add a NAT rule, click the Add button to the left of the table and then choose Add Twice NAT (Before Object NAT), Add Network Object NAT, or Add Twice NAT (After Object NAT) to display the appropriate creation screen. See Twice NAT Rule Properties, on page 6 for descriptions of the Twice NAT (Before and After) options. See Object NAT Rules, on page 9 for descriptions of the Object NAT options.

  • To edit a NAT rule, select the rule and then click the Edit button to the left of the table to display the appropriate edit screen: Edit Twice NAT Policy (before), Edit Object NAT Policy, or Edit Twice NAT Policy (after).

  • To delete a NAT rule, select the rule and then click the Delete button to the left of the table. You are asked to confirm the deletion.

  • To duplicate a NAT rule, select the rule and then click the Duplicate button to the left of the table. The Duplicate NAT Rule screen opens, containing the same parameters as the selected rule. Change the parameters as necessary, and save the new rule. See Twice NAT Rule Properties, on page 6 for descriptions of the Twice NAT (Before and After) options. See Object NAT Rules, on page 9 for descriptions of the Object NAT options.

  • To enable or disable a rule in the Twice NAT Before or Twice NAT After sections, select the rule and then click the Enable/Disable button to the left of the table; the rule is enabled or disabled according to its current state, but it remains in the table. This is a shortcut to editing the rule and changing the Enable Rule option. This button is not available when a Network Object NAT rule is selected.

Step 5  If necessary, move the policy so that it is in priority order. Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.
Twice NAT Rule Properties

The following properties are presented when you add or edit a Twice NAT rule (that is, a Before Auto Rule or an After Auto Rule).

Twice NAT Properties

Description

An optional description of the rule of up to 200 characters.

Enable Rule

You can enable or disable this rule without removing it from the table: select On or Off.

Source NAT type

Specify the type of address translation for this override: choose Static or Dynamic.

- **Static** – Provides static assignment of real addresses to mapped addresses.

- **Dynamic** – Provides dynamic assignment of multiple local addresses to a single global IP address and a unique port number, in effect "hiding" the local addresses behind the one global address. Choosing this option also adds the PAT Pool option to the available properties. On devices operating in routed mode, this option also provides the fall-through option described below.

Note

This property applies only to the specified source translation; destination translation is always static.

Source interface

Enter or select the name of the interface on the specified device from which a packet may originate; this is the "real" interface. Defaults to Any, which represents all interfaces.

Note

In transparent firewall mode, you must specify this property.

Destination interface

Enter or select the name of the interface on which a packet may terminate; this is the "mapped" interface. Defaults to Any, which represents all interfaces. If Dynamic is the chosen Source NAT type, entering an interface name adds the Fallthrough to interface PAT option to the available properties.

Note

In transparent firewall mode, you must specify this property.
PAT Pool

The **PAT Pool** option appears when you choose **Dynamic** as the **Source NAT type**. The related parameters let you specify a “pool” of IP addresses to be used for specifically for port address translation, as well as change the algorithm used for PAT mapping. (See **PAT Pools and Round Robin Allocation**, on page 3 for more information.) If you select **On**, these options appear: **Translated address**, **Round Robin**, **Extended PAT table**, **Flat port range**, and **Include reserve ports**.

**Translated address**

Enter or select the name of one of more Network and Network Group objects to use as the PAT pool.

If you enter or select the name of an interface the **Fallthrough to interface PAT** and **IPv6 Source** options appear in the **Additional Information** section, and the **Extended PAT table** option disappears.

**Round Robin**

Available only when **PAT Pool** is **On**. Turn this option **On** to use a “round-robin” approach to mapping addresses/ports. See **PAT Pools and Round Robin Allocation**, on page 3 for more information about this option.

**Extended PAT table**

Available only when **PAT Pool** is **On**. Turn this option **On** to enable extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

**Flat port range**

Available only when **PAT Pool** is **On**. Turn this option **On** to enable use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also turn **On Include reserve ports**.

**Include reserve ports**

Available only when **PAT Pool** and **Flat port range** are **On**. Turn this option **On** to include the reserve ports, 1 to 1023, in the PAT range.
Additional Information

The following additional options related to NAT processing may be available depending on the type of rule you are creating and the chosen Source NAT type:

- Unidirection
- Translate DNS replies
- IPv6 Source
- One-to-one address translation
- Do not proxy ARP
- Fallthrough to interface PAT
- Perform route lookup

Unidirection

Available only when Static is the chosen Source NAT Type (dynamic rules are uni-directional by default). This feature lets you configure a static NAT rule in a single direction only, as specified by the other options in this screen. When Off, both directions of the translation are performed.

IPv6 Source

Available only when you enter a single interface into the Original Packet Destination field. Turn On to use an IPv6 destination interface address.

One-to-one address translation

Turn On to restrict translations to one-to-one mappings. Generally used for NAT 46 (IPv4 to IPv6 addresses).

Do not proxy ARP

Available only when Static is the chosen Source NAT type. Turn On to disable proxy ARP on the specified Destination Interface.

By default, all NAT rules include proxy ARP on the egress interface. A NAT Exempt rule is used to bypass NAT for both ingress and egress traffic, relying on route look-up to locate the egress interface. Thus, proxy ARP should be disabled for NAT Exempt rules. (NAT Exempt rules always take priority.)

Note  You also can disable Proxy ARP on individual interfaces.

Fallthrough to interface PAT

Available only when Dynamic is the chosen Source NAT Type on devices operating in routed mode, and it appears when you provide an interface name in the Translated address field. When On, dynamic PAT back-up is enabled. When the pool of dynamic NAT addresses is depleted, port address translation is performed, using the address pool specified in the Translated Address field.
Perform route lookup

Available only when Static is the chosen Source NAT type, and appears when you provide an interface name in the Destination Interface field. If this option is On, the egress interface is determined using route look-up instead of using the specified Destination Interface. Be sure this is On for a NAT Exempt rule. This option is supported only for Static Identity NAT.

**Note**

This option is not available on devices operating in transparent mode.

### Object NAT Rules

You can configure network address translation (NAT) overrides on a Network object in order to override the destination address of specific packets. This is referred to as "Object NAT," and it is considered a device-level override. NAT overrides apply to ASA devices only. Each network address translation (NAT) rule defined here will appear in the Network Object NAT Rule section of the NAT rules table for that device.

**Note**

You cannot configure NAT overrides on Network objects incorporating fully qualified domain names (FQDNs).

To configure a NAT rule on a Network object and assign it to the selected device, click the Add rule button on the NAT policies page, and choose Add Object NAT policy. The Create Object NAT Policy screen appears. Fill in the Object NAT Policy Properties.

You can edit an existing Object NAT rule by opening it (select the rule on the NAT policies page for the selected device and click the Edit NAT policy button) and updating the Object NAT policy properties.

To delete an existing Object NAT rule, select it and click the Delete NAT policy button.

### Object NAT Policy Properties

**Description**

An optional description of the rule of up to 200 characters.

**Network object**

Enter or select the name of the Network Object this rule is to be associated with; you also can create a new object from this field.
Source NAT type

Specify the type of address translation for this override: choose **Static** or **Dynamic**.

- **Static** – Provides static assignment of real addresses to mapped addresses.
- **Dynamic** – Provides dynamic assignment of multiple local addresses to a single global IP address and a unique port number, in effect "hiding" the local addresses behind the one global address. Choosing this option also adds the **PAT Pool** option to the available properties. On devices operating in routed mode, this option also provides the fall-through option described below.

**Note**
This property applies only to the specified source translation; destination translation is always static.

Source interface

Enter or select the name of the interface on the specified device from which a packet may originate; this is the “real” interface. Defaults to **Any**, which represents all interfaces.

**Note**
In transparent firewall mode, you must specify this property.

Destination interface

Enter or select the name of the interface on which a packet may terminate; this is the “mapped” interface. Defaults to **Any**, which represents all interfaces. If **Dynamic** is the chosen **Source NAT type**, entering an interface name adds the **Fallthrough to interface PAT** option to the available properties.

**Note**
In transparent firewall mode, you must specify this property.

Original packet

Available only when **Static** is the chosen **Source NAT type**. You can add Static port address translation (PAT) to the override by providing Original Packet information:

- **Service** – Enter a protocol/port combination for traffic entering the device.

Translated packet

Use these fields to add port address translation (PAT) to the rule—translation of specific source-address/destination-address/service combinations.

- **Source** – Enter or select the name of the interface, Network object, or Network Group object representing the PAT address pool.
- **Service** – Available only when Static is the chosen Source NAT type. Enter the port number which is to replace the original port number.
PAT Pool

The **PAT Pool** option appears when you choose **Dynamic** as the **Source NAT type**. The related parameters let you specify a “pool” of IP addresses to be used for specifically for port address translation, as well as change the algorithm used for PAT mapping. (See **PAT Pools and Round Robin Allocation**, on page 3 for more information.) If you select **On**, these options appear: **Translated address**, **Round Robin** and **Extended PAT table**.

**Translated address**

Enter or select the name of one or more Network and Network Group objects to use as the PAT pool.

**Round Robin**

Available only when **PAT Pool** is **On**. Turn this option **On** to use a “round-robin” approach to mapping addresses/ports. See **PAT Pools and Round Robin Allocation**, on page 3 for more information about this option.

**Extended PAT table**

Available only when **PAT Pool** is **On**. Turn this option **On** to enable extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

**Flat port range**

Available only when **PAT Pool** is **On**. Turn this option **On** to enable use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also turn **On Include reserve ports**.

**Include reserve ports**

Available only when **PAT Pool** and **Flat port range** are **On**. Turn this option **On** to include the reserve ports, 1 to 1023, in the PAT range.
Additional Information

The following additional options related to NAT processing may be available depending on the type of rule you are creating and the chosen Source NAT type:

- Unidirection
- Translate DNS replies
- IPv6 Source
- One-to-one address translation
- Do not proxy ARP
- Fallthrough to interface PAT
- Perform route lookup

Translate DNS replies

When On, addresses embedded in DNS replies that match this rule are rewritten.

For DNS replies traversing from a mapped interface to a real interface, the Address (or "A") record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the A record is rewritten from the real value to the mapped value. Note that DNS inspection must be enabled to support this functionality.

One-to-one address translation

Turn On to restrict translations to one-to-one mappings. Generally used for NAT 46 (IPv4 to IPv6 addresses).

Do not proxy ARP

Available only when Static is the chosen Source NAT type. Turn On to disable proxy ARP on the specified Destination Interface.

By default, all NAT rules include proxy ARP on the egress interface. A NAT Exempt rule is used to bypass NAT for both ingress and egress traffic, relying on route look-up to locate the egress interface. Thus, proxy ARP should be disabled for NAT Exempt rules. (NAT Exempt rules always take priority.)

Note: You also can disable Proxy ARP on individual interfaces.

Fallthrough to interface PAT

Available only when Dynamic is the chosen Source NAT Type on devices operating in routed mode, and it appears when you provide an interface name in the Translated address field. When On, dynamic PAT back-up is enabled. When the pool of dynamic NAT addresses is depleted, port address translation is performed, using the address pool specified in the Translated Address field.
Perform route lookup

Available only when Static is the chosen Source NAT type, and appears when you provide an interface name in the Destination Interface field. If this option is On, the egress interface is determined using route look-up instead of using the specified Destination Interface. Be sure this is On for a NAT Exempt rule. This option is supported only for Static Identity NAT.

Note
This option is not available on devices operating in transparent mode.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)
Object NAT Rules