Configuring Network Address Translation

These topics provide conceptual information about network address translation (NAT) in general, and about translation types and various implementations:

The following topics describe configuration and management of NAT rules on various Cisco devices:

Note From version 4.17, though Cisco Security Manager continues to support Cisco Catalyst switches, PIX, FWSM, and IPS, it does not support any enhancements.

Cisco IOS routers

PIX, FWSM, and ASA security devices

– Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43
– Per-Session NAT Rules: ASA 9.0(1)+
– Add and Edit Per Session NAT Rule Dialog Boxes, page 24-48

Understanding Network Address Translation

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.

One of the main functions of NAT is to enable private IP networks to connect to the Internet. Network address translation replaces a private IP address with a public IP address, translating the private addresses in the internal network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses; for example, NAT rules can be configured to utilize only one public address for the entire network in communications with the outside world.

Other functions of NAT include:

- Security – Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions – Overlapping IP addresses are not a problem.
- Flexibility – You can change internal IP addressing schemes without affecting the public addresses available externally. For example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.

Cisco devices support both NAT, which provides a globally unique address for each outbound host session, and Port Address Translation (PAT), which provides the same single 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.

The device translates an address when an existing NAT rule matches the specific traffic. 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.

Note In this document, all types of translation are generally referred to as NAT; see Types of Address Translation, page 24-3 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.

The release of ASA version 8.3 provides a simplified, interface-independent approach to configuring network address translation, as compared to earlier ASA versions and other devices. See About "Simplified" NAT on ASA 8.3+ Devices, page 24-4 for more information.

Related Topics

- Types of Address Translation, page 24-3
- About "Simplified" NAT on ASA 8.3+ Devices, page 24-4

Types of Address Translation

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

Table 24-1 Types of Address Translation

Static NAT	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.
Static PAT	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.
Policy Static NAT	Fixed translation of real source addresses to specific mapped addresses. Destination networks/hosts are also specified, and the service is always IP.
Policy Static PAT	Fixed translation of real source addresses with specific TCP or UDP port numbers, to specific mapped addresses and ports. Destination networks/hosts and services are also specified.
Dynamic NAT	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.
Dynamic PAT	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."
Policy Dynamic NAT	Dynamic translation of specific source-address/destination-address/service combinations on a given interface, using a pool of shared addresses. Translation direction—outbound or inbound—is also specified.
Identity NAT	The specified address is translated to itself—that is, it is effectively not translated; applies to outbound connections only. Identity NAT is a particular type of Static NAT.
NAT Exempt	Translation is bypassed for specified source/destination address combinations; connections can be initiated in both the outbound and inbound directions.

Note While certain of these types do not apply to ASA 8.3 and later devices, the ASA 8.3+ devices do provide a Dynamic NAT and PAT option, which is Dynamic NAT with a Dynamic PAT back-up feature.

About "Simplified" NAT on ASA 8.3+ Devices

The release of ASA version 8.3 provides 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.

All NAT rules on the device—static NAT, dynamic PAT, and dynamic NAT—are presented in a single table, and essentially the same dialog box is used to configure all NAT rules. The NAT rules are interface independent (that is, interfaces are optional), meaning the rules are independent of security levels also.

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.

Network Object NAT

You also can define NAT properties on Host, Address Range, and 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, ports, and optional interfaces only once. These automatically generated, object-based rules are referred to as "Network Object NAT" rules. Note that these rules cannot be created or deleted from the rules table; you must edit the appropriate objects in the Policy Object Manager. You can, however, edit these rules from the rules table after they have been defined for the network object. For more information, see Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43.

Note Network Object NAT rules are not displayed in the Translation Rules table in Policy View because these rules are device-specific.

The NAT Table

As mentioned, all NAT rules on a device are presented in a single table, which is divided into three sections: a "manual" section, the Network Object NAT rules section, and another manual-rules section. You can add, edit and order rules in both manual sections; the Network Object NAT rules are added and ordered automatically, and as mentioned, to edit these rules you must edit the related objects.

The NAT rules in the table are applied on a top-down, first-match basis. That is, a packet is translated only when it matches a NAT rule, and as soon as a match is made, regardless of its location or section, NAT rule processing stops.

You can use this table to organize and manage the manual rules—you can insert rules in any order, and you can re-order them. The two sections of manual rules are provided to let you order manual rules both before and after the automatic object rules.

Network Object NAT rules are automatically ordered such that static rules appear before dynamic rules. These two types are each further ordered as follows:

- Fewest number of IP addresses – Rules for objects with one IP address are listed before those for objects with two addresses, which are before those with three addresses, and so on.
- IP address numbers – For objects having the same number of IP addresses, the rules are arranged such that the IP addresses themselves are in numerical order, from lower to higher. For example, 10.1.1.1 rules are listed before 11.1.1.1 rules.
- Object names – If the IP address is the same, the rules are ordered by alphabetizing the object names.

And remember, translation is based on the first matching rule.

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 dialog box. Again, while source translation can be static or dynamic, destination translation is always static, and is only available with manual rules.

Bi-directional or Twice NAT

When creating a manual static rule, you can select the "Bi-directional" option, which 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.

For example, if Bi-directional is chosen when you create a static rule with Host1 in the Source field and Host2 in the Translated field, two lines are added to the rules table: one with Host1 being translated to Host2, and one with Host2 being translated to Host1.

This is sometimes referred to as "Twice NAT" because only one look-up is required to fetch and process what is in effect two rules.

Many-to-one Addressing

Generally, static NAT rules are configured with one-to-one address mapping. However, you can now define static NAT rules in which many IP addresses map to a few or one IP address. Functionally, many-to-few is the same as many-to-one, but because the configuration is more complicated, we recommend creating a many-to-one rule for each address as needed.

Many-to-one addressing might be useful, for example, in a situation where a range of public IP addresses is used to reach a load balancer which redirects requests to an internal network.

Related Topics

- Configuring NAT on ASA 8.3+ Devices, page 24-34
- Add and Edit NAT Rule Dialog Boxes, page 24-37
- Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43

NAT Policies on Cisco IOS Routers

You can configure NAT policies on a Cisco IOS router from the following tabs on the NAT policy page:

- NAT Page: Interface Specification, page 24-6
- NAT Page: Static Rules, page 24-6
- NAT Page: Dynamic Rules, page 24-10
- NAT Page: Timeouts, page 24-13

Network Address Translation (NAT) converts private, internal LAN addresses into globally routable IP addresses. NAT enables a small number of public IP addresses to provide global connectivity for a large number of hosts.

For more information, see Understanding Network Address Translation, page 24-2.

Navigation Path

- (Device view) Select **NAT** from the Policy selector.

- (Policy view) Select **NAT (Router)** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

NAT Page: Interface Specification

Before creating NAT rules, you must define the "direction" of the traffic to be translated by specifying the Inside and Outside interfaces. Inside interfaces typically connect to a LAN that the router serves. Outside interfaces typically connect to your organization's WAN or to the Internet. You must designate at least one Inside interface and one Outside interface to enable the router to perform network address translation.

The Inside and Outside designations are used when interpreting translation rules: addresses connected to the Inside interface are translated to addresses on the Outside interface. After these interfaces are defined, they are used in all static and dynamic NAT translation rules.

Use the Interface Specification tab of the NAT policy page to specify the Inside and Outside interfaces.

Navigation Path

- (Device view) Select **NAT** from the Policy selector, then click the **Interface Specification** tab.
- (Policy view) Select **NAT (Router) > Translation Rules** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Interface Specification** tab.

Defining the Inside and Outside Interfaces

In the **NAT Inside Interfaces** and **NAT Outside Interfaces** fields, enter or Select the names of the interfaces or interface roles for the Inside and Outside interfaces, respectively. Separate multiple names or roles with commas (for example, Ethernet1/1, Ethernet1/2). Note that you cannot enter the same name in both fields.

Related Topics

- NAT Policies on Cisco IOS Routers, page 24-5
- NAT Page: Static Rules, page 24-6
- NAT Page: Dynamic Rules, page 24-10
- NAT Page: Timeouts, page 24-13
- NAT Page: Timeouts, page 24-13

NAT Page: Static Rules

You define a static NAT rule by specifying a local address that must be translated, as well as the global address to which it is translated. This is a static or fixed mapping—the local address is always translated to the same global address.

You can define static NAT rules that translate the addresses of single hosts, as well as static rules that translate multiple addresses in a subnet. When multiple local addresses must use the same global address, you must define the necessary port redirection information, which defines a different port for each local address using the global address.

Note We strongly recommend that you do not perform NAT on traffic that will be transmitted over a VPN. Translating addresses on this traffic causes it to be sent out unencrypted instead of encrypted over the VPN.

The procedure for creating a static rule depends on whether the address being translated represents a port, a single host, or an entire subnet:

- You define a **static NAT rule for a single host** by entering the original address to translate and the global address to which it is translated. The global address may be taken from an interface on the device.
- You define a **static NAT rule for a subnet** by entering one of the addresses in the subnet (including the subnet mask) as the original address, and one of the global addresses that you want to use as the translated address. The router configures the remaining addresses based on the subnet mask you provide.
- You define a **static NAT rule for a port** by entering the original IP address and the global address to which it should be translated. The global address may be taken from an interface on the device. In addition, you must select the protocol used by the port, as well as the local and global port numbers.

The Add Static NAT Rule and Edit Static NAT Rule dialog boxes are used to add and edit these rules. Refer to NAT Static Rule Dialog Boxes, page 24-7 for descriptions of the fields displayed in the table on this page.

Before You Begin

- Define the inside and outside interfaces used for NAT. See NAT Page: Interface Specification, page 24-6.

Navigation Path

- (Device view) Select **NAT** from the Policy selector, then click the **Static Rules** tab.
- (Policy view) Select **NAT (Router) > Translation Rules** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Static Rules** tab.

Related Topics

- NAT Policies on Cisco IOS Routers, page 24-5
- NAT Page: Dynamic Rules, page 24-10
- NAT Page: Timeouts, page 24-13
- Standard Security Manager rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

NAT Static Rule Dialog Boxes

Use the Add/Edit NAT Static Rule dialog boxes to add or edit static address translation rules. Except for their titles, the two dialog boxes are identical.

Navigation Path

Go to the NAT Page: Static Rules, page 24-6 tab; click the **Add** button beneath the table to add a new rule, or select a rule in the table and click **Edit** to update that rule.

Related Topics

- Understanding Interface Role Objects, page 6-73

Field Reference

Table 24-2 Add/Edit NAT Static Rule Dialog Boxes

Element	Description
Static Rule Type	The type of local address to be translated by this static rule: • Static Host – A single host requiring static address translation. • Static Network – A subnet requiring static address translation. • Static Port – A single port requiring static address translation. If you select this option, you must define the Port Redirection parameters.
Original Address	An IP address, or the name of a network/host object representing the address(es) to be translated. You can enter or Select the object name. Network/host objects are logical collections of IP addresses that represent networks, hosts, or both. See Understanding Networks/Hosts Objects, page 6-80 for more information. **Note** Do not enter a local address belonging to this router, as it could cause Security Manager management traffic to be translated. Translating this traffic will cause a loss of communication between the router and Security Manager.
Translated Address	Use the options in this section of the dialog box to specify the address(es) to which the Original Address(es) are translated: • **Specify IP** – Select this option to specify an IP address, or the name of a network/host object that provides the translated address(es). Add an IP address, or the name of a network/host object, in the **Translated IP/Network** field. You can enter or Select the object name. • **Use Interface IP** – Select this option to specify that the IP address assigned to a particular interface be used as the translated address. Enter or Select the name of the desired **Interface**. (This is typically the interface from which translated packets leave the router.) **Note** This option is not available when Static Network is the chosen rule type. Only one static rule may be defined per interface.

Table 24-2 Add/Edit NAT Static Rule Dialog Boxes (continued)

Element	Description
Port Redirection	These parameters specify port information for the address translations. Port address translation lets you to use the same public IP address for multiple devices as long as the port specified for each device is different. **Note** These parameters are available only when Static Port is the chosen rule type. **Redirect Port** – When Static Port is chosen as the rule type, this box is automatically checked; it cannot be changed. Enter the appropriate information in the following fields: • **Protocol** – The communications protocol used for these ports: TCP or UDP. • **Local Port** – The port number on the source network. Valid values range from 1 to 65535. • **Global Port** – The port number on the destination network that the router is to use for this translation. Valid values range from 1 to 65535.
Advanced	This section contains optional, advanced translation options. **Note** The Advanced options are available only when the Specify IP option is the selected method for defining the translated address(es). • No Alias – When selected, disables automatic aliasing for the global IP address translation. If the NAT pool used as an inside global pool consists of addresses on an attached subnet, an alias is generated for that address so that the router can answer Address Resolution Protocol (ARP) requests for those addresses. When deselected, global address aliases are permitted. • No Payload – When selected, prohibits an embedded address or port in the payload from being translated. The payload option performs NAT between devices on overlapping networks that share the same IP address. When an outside device sends a DNS query to reach an inside device, the local address inside the payload of the DNS reply is translated to a global address according to the relevant NAT rule. You can disable this feature by selecting the No Payload option. Otherwise, embedded addresses and ports in the payload may be translated. See Disabling the Payload Option for Overlapping Networks, page 24-10 for more information. • Create Extended Translation Entry – When checked, extended translation entries (addresses and ports) are created in the translation table. This lets you associate multiple global addresses with a single local address. This is the default. When this option is deselected, simple translation entries are created, allowing association of a single global address with the local address. **Note** This option is not available when Static Port is the chosen rule type.

Disabling the Payload Option for Overlapping Networks

Overlapping networks result when you assign an IP address to a device on your network that is already legally owned and assigned to a different device on the Internet or outside network. Overlapping networks can also result after the merger of two companies using RFC 1918 IP addresses in their networks. These two networks need to communicate, preferably without your having to re-address all their devices.

This communication is achieved as follows. The outside device cannot use the IP address of the inside device because it is the same as the address assigned to itself (the outside device). Instead, the outside device sends a Domain Name System (DNS) query for the inside device's domain name. The source of this query is the IP address of the outside device, which is translated to an address from a designated address pool. The DNS server located on the inside network replies with the IP address associated with the inside device's domain name in the data portion of the packet. The destination address of the reply packet is translated back to the outside device's address, and the address in the data portion of the reply packet is translated to an address from a different address pool. In this way, the outside device learns that the IP address for the inside device is one of the addresses from that second address pool, and it uses this address when it communicates with the inside device. The router running NAT takes care of the translations at this point.

To disable the translation of the address inside the payload, check the **No Payload** option when you create a static NAT rule based on a global IP translation.

NAT Page: Dynamic Rules

Use the NAT Dynamic Rules tab of the router's NAT page to manage dynamic address translation rules. A dynamic address translation rule dynamically maps hosts to addresses, using either the IP address of a specific interface (with dynamic port translation), or the addresses included in an address pool that are globally unique in the destination network.

Defining Dynamic NAT Rules

You define a dynamic NAT rule by first selecting an access control list (ACL) whose rules specify the traffic requiring translation.

Then, you must either select an interface with an IP address to which the addresses should be translated, or define a pool of addresses to be used. You define the pool by specifying a range of addresses and giving the range a unique name; you can specify multiple ranges. The router uses the available addresses in the pool (those not used for static translations, or for its own WAN IP address) for connections to the Internet or another outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned later to another device.

If the addressing requirements of your network exceed the available addresses in your dynamic NAT pool, you can use the Port Address Translation (PAT) feature (also called Overloading) to associate many private addresses with one or a small group of public IP address, using port addressing to make each translation unique. With PAT enabled, the router chooses a unique port number for the IP address of each outbound translation slot. This feature is useful if you cannot allocate enough unique IP addresses for your outbound connections. Note that Port Address Translation does not occur until the address pool is depleted.

Note By default, Security Manager does not perform NAT on traffic that is meant to be transmitted over a VPN. Otherwise, any traffic appearing in both the NAT ACL and the crypto ACL defined on an interface would be sent out unencrypted because NAT is always performed before encryption. However, you can change this default setting.

Tip You can perform PAT on split-tunneled traffic on the spokes of your VPN topology directly from the Global VPN Settings page. There is no need to create a dynamic NAT rule for each spoke. Any NAT rules that you define on an individual device override the VPN setting. For more information, see Configuring VPN Global NAT Settings, page 26-42.

The Add Dynamic NAT Rule and Edit Static NAT Rule dialog boxes are used to add and edit these rules. Refer to NAT Dynamic Rule Dialog Box, page 24-11 for descriptions of the fields displayed in the table on this page.

Before You Begin

- Define the inside and outside interfaces used for NAT. See NAT Page: Interface Specification, page 24-6.

Navigation Path

- (Device view) Select **NAT** from the Policy selector, then click the **Dynamic Rules** tab.
- (Policy view) Select **NAT (Router) > Translation Rules** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Dynamic Rules** tab.

Related Topics

- NAT Policies on Cisco IOS Routers, page 24-5
- NAT Page: Static Rules, page 24-6
- NAT Page: Timeouts, page 24-13
- Standard Security Manager rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

NAT Dynamic Rule Dialog Box

Use the Add/Edit NAT Dynamic Rule dialog boxes to add or edit dynamic address translation rules. Except for their titles, the two dialog boxes are identical.

Navigation Path

Go to the NAT Page: Dynamic Rules, page 24-10 tab; click the **Add** button beneath the table to add a new rule, or select a rule in the table and click **Edit** to update that rule.

Related Topics

- Creating Access Control List Objects, page 6-53
- Understanding Interface Role Objects, page 6-73

Field Reference

Table 24-3 NAT Dynamic Rule Dialog Box

Element	Description
Traffic Flow	In the **Access List** field, enter or Select the name of the access control list (ACL) object whose entries define the addresses requiring dynamic translation. **Note** Make sure that the specified ACL does not permit the translation of Security Manager management traffic over any device address on this router. Translating this traffic will cause a loss of communication between the router and Security Manager.
Translated Address	Use the options in this section of the dialog box to specify the method and address(es) used for dynamic translation: • **Use Interface IP** – Select this option to specify that the globally registered IP address assigned to a particular interface be used as the translated address; port addressing ensures each translation is unique. (The Enable Port Translation (Overload) option is checked automatically when you select Use Interface IP.) Enter or Select the name of the desired **Interface**. This is typically the interface from which translated packets leave the router, meaning the interface or interface role must represent an outside interface on the router (see NAT Page: Interface Specification, page 24-6). • **Address Pool** – Select this option to base address translation on the addresses you specify in the **Network Ranges** pool. Enter one or more address ranges, including the prefix, using the format `min1-max1/prefix` (in CIDR notation), where "prefix" represents a valid netmask. For example, `172.16.0.0-172.31.0.223/12`. You can add as many address ranges to the address pool as required, but all ranges must share the same prefix. Separate multiple entries with commas.

Table 24-3 NAT Dynamic Rule Dialog Box (continued)

Element	Description
Settings	This section contains two options • **Enable Port Translation (Overload)** – When selected, the router uses port addressing (PAT) if supply of global addresses in the address pool is depleted; when deselected, PAT is not used. **Note** When you use select Use Interface IP in the Translated Address section, this box is checked automatically; it cannot be changed. • **Do Not Translate VPN Traffic (Site-to-Site VPN only)** – Deselect this option to allow address translation on traffic intended for a site-to-site VPN. When selected, address translation is not performed on VPN traffic. When deselected, the router performs address translation on VPN traffic in cases of overlapping addresses between the NAT ACL and the crypto ACL. **Note** We strongly recommend that you not deselect this option, or any traffic defined in both the NAT ACL and the crypto ACL will be sent unencrypted. When you perform NAT into IPsec, we also recommend that you leave this option selected; it does not interfere with the translation of addresses arriving from overlapping networks. This setting applies only in situations where the NAT ACL overlaps the crypto ACL used by the site-to-site VPN. Because the interface performs NAT first, any traffic arriving from an address within this overlap would get translated, causing the traffic to be sent unencrypted. Leaving this box checked prevents that from happening. **Note** This option does not apply to remote access VPNs.

NAT Page: Timeouts

Use the NAT Timeouts tab of the router's NAT page to manage the timeout values for port address (overload) translations. These timeouts cause a dynamic translation to expire after a specified period of inactivity. In addition, you can use options on this page to place a limit on the number of entries allowed in the dynamic NAT table, and to modify the default timeout on all dynamic translations that do not include PAT processing.

About Dynamic NAT Timeouts

Dynamic NAT translations have a timeout period for non-use, after which they expire and are purged from the translation table. If you enable the Overload feature for performing PAT, you can specify a variety of values that provide finer control over these timeouts, because each translation entry contains additional contextual information about the traffic using it.

For example, non-DNS translations time out by default after five minutes, but DNS translations time out after 1 minute. Further, TCP translations time out after 24 hours, unless an RST or FIN is seen on the stream, in which case they time out after one minute. You can change any of these timeout values.

Note If you disable the Port Translation (Overload) feature for all dynamic rules, you need not enter any PAT-related timeout values. However, you can still modify the default timeout value for non-PAT dynamic translations. (By default, all dynamic translations expire after 24 hours.) For more information about the Overload feature, see NAT Dynamic Rule Dialog Box, page 24-11.

Navigation Path

- (Device view) Select **NAT** from the Policy selector, then click the **Timeouts** tab.
- (Policy view) Select **NAT (Router) > Translation Rules** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Timeouts** tab.

Related Topics

- NAT Page: Interface Specification, page 24-6
- NAT Page: Static Rules, page 24-6
- NAT Page: Dynamic Rules, page 24-10

Field Reference

Table 24-4 NAT Timeouts Tab

Element	Description
Max Entries	The maximum number of entries allowed in the dynamic NAT table. You can enter a value between 1 and 2147483647, or you can leave the field blank (the default), which means that the number of entries in the table is unlimited.
Timeout (sec.)	The number of seconds after which dynamic translations expire; this does not apply to PAT (overload) translations. The default is 86400 seconds (24 hours).
UDP Timeout (sec.)	The timeout value applied to User Datagram Protocol (UDP) ports. The default is 300 seconds (5 minutes). **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.
DNS Timeout (sec.)	The timeout value applied to Domain Naming System (DNS) server connections. The default is 60 seconds. **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.
TCP Timeout (sec.)	The timeout value applied to Transmission Control Protocol (TCP) ports. The default is 86400 seconds (24 hours). **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.

Table 24-4 NAT Timeouts Tab (continued)

Element	Description
FINRST Timeout (sec.)	The timeout value applied when a Finish (FIN) packet or Reset (RST) packet (both of which terminate connections) is found in the TCP stream. The default is 60 seconds. **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.
ICMP Timeout (sec.)	The timeout value applied to Internet Control Message Protocol (ICMP) flows. The default is 60 seconds. **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.
PPTP Timeout (sec.)	The timeout value applied to NAT Point-to-Point Tunneling Protocol (PPTP) flows. The default is 86400 seconds (24 hours). **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.
SYN Timeout (sec.)	The timeout value applied to TCP flows after a synchronous transmission (SYN) message (used for precise clocking) is encountered. The default is 60 seconds. **Note** This value applies only when Port Translation (Overload) is enabled for a dynamic NAT rule; see NAT Dynamic Rule Dialog Box, page 24-11.

NAT Policies on Security Devices

The following topics describe configuring network address translation (NAT) options on managed security appliances: PIX firewalls, Firewall Service Modules (FWSMs) on Catalyst switches, pre-version-8.3 Adaptive Security Appliances (ASAs), and ASA 8.3+ devices. The topics are arranged as follows:

NAT in Transparent Mode

Using NAT on a security appliance operating in transparent mode eliminates the need for upstream or downstream routers to perform NAT for their networks. NAT in transparent mode has the following requirements and limitations:

- When the mapped addresses are not on the same network as the transparent firewall, you need to add a static route for the mapped addresses on the upstream router that points to the downstream router (through the security appliance).
- If the real destination address is not directly connected to the security appliance, you also need to add a static route on the security appliance for the real destination address that points to the downstream router. Without NAT, traffic from the upstream router to the downstream router does not need any routes on the security appliance because it uses the MAC address table. Using NAT, however, causes the security appliance to use a route look-up instead of a MAC address look-up, so it needs a static route to the downstream router.
- Because the transparent firewall does not have any interface IP addresses, you cannot use interface PAT.
- ARP inspection is not supported. Moreover, if for some reason a host on one side of the security appliance sends an ARP request to a host on the other side of the security appliance, and the initiating host real address is mapped to a different address on the same subnet, then the real address remains visible in the ARP request.

Global Options Page

Security Manager version 4.9 supports Carrier Grade NAT to configure the block size and maximum blocks per host limit for port block allocation, for ASA devices 9.5(1) or later. Use the Global Options page to configure these options.

Navigation Path

- (Device view) Select **NAT > Global Options** from the Device Policy selector.
- (Policy view) Select **NAT (PIX/ASA/FWSM) > Global Options** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **Global Options** to create a new policy.

Related Topics

- NAT Policies on Security Devices, page 24-15
- Add and Edit NAT Rule Dialog Boxes, page 24-37

Field Reference

Table 24-5 Global Options Page

Element	Description
xlate block-allocation size	Enter a value between 32 and 4096. The default value is 512.
xlate block-allocation maximum-per-host	Enter a value between 1 to 8. The default value is 4.

Table 24-5 Global Options Page (continued)

Element	Description
xlate block-allocation interim logging	Configure a timer interval to generate syslog for all the active port blocks allocated at that time for ASA 9.12(1) devices and later. Enter a value between 43200 to 604800.

Translation Options Page

Use the Translation Options page to set options that affect network address translation for the selected security appliance. These settings apply to all interfaces on the device.

Navigation Path

- (Device view) Select **NAT > Translation Options** from the Device Policy selector.
- (Policy view) Select **NAT (PIX/ASA/FWSM) > Translation Options** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **Translation Options** to create a new policy.

Related Topics

- NAT Policies on Security Devices, page 24-15

Field Reference

Table 24-6 Translation Options Page

Element	Description
Enable traffic through the firewall without address translation	When selected, lets traffic pass through the security appliance without address translation. If this option is not selected, any traffic that does not match a translation rule will be dropped. **Note** This option is available only on PIX 7.x, FWSM 3.x, and ASA devices.

Table 24-6 Translation Options Page (continued)

Element	Description
Enable xlate bypass	When selected, establishment of NAT sessions for untranslated traffic is disabled (this feature is called "xlate bypass"). **Note** This option is available only on FWSM 3.2 and later. By default, the FWSM creates NAT sessions for all connections even if NAT is not used. For example, a session is created for each untranslated connection even if NAT control is not enabled, if NAT exemption or identity NAT is used, or if you use same-security interfaces and do not configure NAT. Because there is a maximum number of NAT sessions (266,144 concurrent), these kinds of NAT sessions might cause you to run into the limit. To avoid reaching the limit, enable xlate bypass. If you disable NAT control and have untranslated traffic or use NAT exemption, or if you enable NAT control and use NAT exemption, then with xlate bypass, the FWSM does not create a session for those types of untranslated traffic. However, NAT sessions are still created in the following instances: • You configure identity NAT (with or without NAT control)—identity NAT is considered to be a translation. • You use same-security interfaces with NAT control. Traffic between same-security interfaces create NAT sessions even when you do not configure NAT for the traffic. To avoid NAT sessions in this case, disable NAT control, or use NAT exemption as well as xlate bypass.
Do not translate VPN traffic	When selected, VPN traffic passes through the security appliance without address translation.
Clear translates for existing connections	When selected, the translation slots assigned to dynamic translations and any associated connections are cleared following each session. Each session connecting through the security appliance, and undergoing some form of NAT or PAT, is assigned a translation slot known as an "xlate." These translation slots can persist after the session is complete, which can lead to a depletion of translation slots, unexpected traffic behavior, or both.

Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX and FWSM features/functions, it does not support any enhancements.

The following sections describe configuring network address translation on PIX and FWSM devices, and on pre-8.3-version ASAs. (See Configuring NAT on ASA 8.3+ Devices, page 24-34 for information about configuring NAT on ASA 8.3+ devices.)

- Address Pools, page 24-19
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20

– Translation Exemptions (NAT 0 ACL), page 24-21
– Dynamic Rules Tab, page 24-23
– Policy Dynamic Rules Tab, page 24-25
– Static Rules Tab, page 24-27
– General Tab, page 24-32

Address Pools

Use the Address Pools page to view and manage the global address pools used in dynamic NAT rules.

The Address Pool dialog box is used to add and edit these address pools. Refer to Address Pool Dialog Box, page 24-19 for descriptions of the fields displayed in the Global Address Pools table on this page.

Navigation Path

- (Device view) Select **NAT > Address Pools** from the Device Policy selector.
- (Policy view) Select **NAT (PIX/ASA/FWSM) > Address Pools** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **Address Pools** to create a new policy.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18

Address Pool Dialog Box

Use the Address Pool dialog box to add or edit a global address pool for use in dynamic NAT rules.

Navigation Path

You open the Address Pool dialog box by clicking the Add Row or Edit Row buttons on the Address Pools, page 24-19.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18

Field Reference

Table 24-7 Address Pools Dialog Box

Element	Description
Interface Name	Enter or Select the name of the device interface on which the mapped IP addresses will be used.
Pool ID	Enter a unique identification number for this address pool, an integer between 1 and 2147483647. When configuring a dynamic NAT rule, you select a Pool ID to specify the pool of addresses to be used for translation.

Table 24-7 Address Pools Dialog Box (continued)

Element	Description
IP address ranges	Enter or Select the addresses to be assigned to this address pool. You can specify these addresses as follows: • Address range for dynamic NAT (e.g., 192.168.1.1-192.168.1.15) • Subnetwork (e.g., 192.168.1.0/24) • List of addresses separated by commas (e.g., 192.168.1.1, 192.168.1.2, 192.168.1.3) • Single address to use for PAT (e.g., 192.168.1.1) • Combinations of the above (e.g., 192.168.1.1-192.168.1.15, 192.168.1.25) • Names of hosts on the connected network; these will be resolved to IP addresses.
Description	Enter a description for the address pool.
Enable Interface PAT	When checked, port address translation is enabled on the specified interface.

Translation Rules: PIX, FWSM, and pre-8.3 ASA

Note From version 4.17, though Cisco Security Manager continues to support PIX and FWSM features/functionality, it does not support any enhancements.

Use the Translation Rules page to define network address translation (NAT) rules on the selected device. The Translation Rules page consists of the following tabs:

- Translation Exemptions (NAT 0 ACL), page 24-21 – Use this tab to configure rules specifying traffic that is exempt from address translation.

  Note Translation exemptions are only supported by PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules.

- Dynamic Rules Tab, page 24-23 – Use this tab to configure dynamic NAT and PAT rules.

  Note Dynamic translation rules are only supported by PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules.

- Policy Dynamic Rules Tab, page 24-25 – Use this tab to configure dynamic translation rules based on source and destination addresses and services.

Note Policy dynamic rules are only supported by PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules.

- Static Rules Tab, page 24-27 – Use this tab to configure static translation rules for a security appliance or shared policy.
- General Tab, page 24-32 – Use this tab to view all current translation rules, listed in the order that they will be evaluated on the device.

Note The General tab is visible only for PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules and do not need to display summary information.

Navigation Path

To access the Translation Rules page, do one of the following:

- (Device view) Select **NAT > Translation Rules** from the Device Policy selector.
- (Policy view) Select **NAT (PIX/ASA/FWSM) > Translation Rules** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **Translation Rules** to create a new policy.

Translation Exemptions (NAT 0 ACL)

Use the Translation Exemptions (NAT 0 ACL) tab of the Translation Rules page to view and specify rules that exempt traffic from address translation. Rules are evaluated sequentially in the order listed. The row number indicates the rule's position in the ordering of the list. You can use the Up Row and Down Row buttons to change the position of the selected rule.

The Add/Edit Translation Exemption (NAT-0 ACL) Rule dialog box is used to add and edit these rules. Refer to Add/Edit Translation Exemption (NAT-0 ACL) Rule Dialog Box, page 24-22 for descriptions of the fields displayed in the table on this page.

Note Translation exemptions are only supported by PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules.

Navigation Path

You can access the Translation Exemptions (NAT 0 ACL) tab from the Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20 page.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Advanced NAT Options Dialog Box, page 24-30
- General Tab, page 24-32
- Standard Security Manager rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48

– Table Columns and Column Heading Features, page 1-49

Add/Edit Translation Exemption (NAT-0 ACL) Rule Dialog Box

Use the Add/Edit Translation Exemption (NAT-0 ACL) Rule dialog box to define and edit translation exemption rules on PIX, FWSM and pre-8.3 ASA devices in router mode, and FWSM 3.2 devices in transparent mode.

Navigation Path

You can access the Add/Edit Translation Exemption (NAT-0 ACL) Rule dialog box from the Translation Exemptions (NAT 0 ACL) tab. See Translation Exemptions (NAT 0 ACL), page 24-21 for more information.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20
- Advanced NAT Options Dialog Box, page 24-30

Field Reference

Table 24-8 Add/Edit Translation Exemption (NAT-0 ACL) Rule Dialog Box

Element	Description
Enable Rule	If checked, the rule is enabled. Deselect this option to disable the rule without deleting it.
Action	Select the action for this rule: • exempt – The rule identifies traffic that is exempt from NAT. • do not exempt – The rule identifies traffic that is not exempt from NAT.
Original: Interface	Enter the name of (or Select) the device interface to which the rule applies.
Original: Sources	Enter IP addresses for (or Select) the source hosts and network objects to which the rule applies. Multiple entries must be separated by commas. Note that this parameter is displayed in the Translation Exemptions (NAT 0 ACL) table under the column heading "Original Address."
Translated: Direction	The rule can be applied to Inbound or Outbound traffic, as specified with this option.
Traffic flow: Destinations	Enter IP addresses for (or Select) the destination hosts and network objects to which the rule applies. Multiple entries must be separated by commas.
Category	To assign the rule to a category, choose the category from this list. Categories can help identify rules and objects using labels and color-coding. See Using Category Objects, page 6-13 for more information. **Note** No commands are generated for the Category attribute.
Description	Enter a description of the rule.

Table 24-8 Add/Edit Translation Exemption (NAT-0 ACL) Rule Dialog Box (continued)

Element	Description
Advanced button (FWSM only)	Click to open the Advanced NAT Options Dialog Box, page 24-30 to configure advanced settings for this rule.

Dynamic Rules Tab

Use the Dynamic Rules tab of the Translation Rules page to view and configure dynamic NAT and PAT rules. Rules are evaluated sequentially in the order listed. The row number indicates the rule's position in the ordering of the list. You can use the Up Row and Down Row buttons to change the position of the selected rule.

With dynamic NAT, internal IP addresses are dynamically translated using IP addresses from a pool of global addresses. With dynamic PAT, internal IP addresses are translated to a single mapped address by using dynamically assigned port numbers with the mapped address. Dynamic translations are often used to map local RFC 1918 IP addresses to addresses that are Internet-routable.

The Add/Edit Dynamic Translation Rule dialog box is used to add and edit these rules. Refer to Add/Edit Dynamic Translation Rule Dialog Box, page 24-23 for descriptions of the fields displayed in the table on this page.

Note Dynamic translation rules are only supported by PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules.

Navigation Path

You can access the Dynamic Rules tab from the Translation Rules page. For more information about the Translation Rules page, see Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20.

Note By default, only standard Dynamic Rule elements are displayed in this table. Additional columns for elements defined in the Advanced NAT Options dialog box can be displayed by right-clicking any column heading. (All columns are displayed by default on the General Tab, page 24-32.)

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Advanced NAT Options Dialog Box, page 24-30
- Select Address Pool Dialog Box, page 24-24
- General Tab, page 24-32
- Standard rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

Add/Edit Dynamic Translation Rule Dialog Box

Use the Add/Edit Dynamic Translation Rule dialog box to define and edit dynamic NAT and PAT rules.

Navigation Path

You can access the Add/Edit Dynamic Translation Rule dialog box from the Dynamic Rules tab. See Dynamic Rules Tab, page 24-23 for more information.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20
- Advanced NAT Options Dialog Box, page 24-30
- Select Address Pool Dialog Box, page 24-24

Field Reference

Table 24-9 Add/Edit Dynamic Translation Rule Dialog Box

Element	Description
Enable Rule	If checked, the rule is enabled. Deselect this option to disable the rule without deleting it.
Original: Interface	Enter the name or Select the device interface to which the rule applies.
Original: Address	Enter IP addresses for (or Select) the source hosts and network objects to which the rule applies. Multiple entries must be separated by commas.
Translated: Pool	Enter (or Select) the ID number of the pool of addresses used for translation; clicking Select opens the Select Address Pool Dialog Box, page 24-24. Enter a value of zero to specify this as an identity NAT rule.
Translated: Direction	The rule can be applied to Inbound or Outbound traffic, as specified with this option.
Advanced button	Click to open the Advanced NAT Options Dialog Box, page 24-30 to configure advanced settings for this rule.

Select Address Pool Dialog Box

The Select Address Pool dialog box presents a list of global address pools; these pools are defined and managed via the Address Pools, page 24-19. Use this dialog box to select an address pool for use by a dynamic translation rule, or a policy dynamic translation rule.

Navigation Path

You can access the Select Address Pool dialog box from the Add/Edit Dynamic Translation Rule Dialog Box, page 24-23 when adding or editing a dynamic translation rule, or from the Add/Edit Policy Dynamic Rules Dialog Box, page 24-26 when adding or editing a policy dynamic translation rule.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20
- Address Pools, page 24-19

Field Reference

Table 24-10 Select Address Pool Dialog Box

Element	Description
Pool ID	The identification number of the address pool.
Interface	The name of the device interface to which the address pool applies.
IP Address Ranges	The IP addresses assigned to the pool; “interface” in this list indicates PAT is enabled on the specified Interface.
Description	The description provided for the address pool.
Selected Row	This field identifies the pool currently selected in the list. When you click OK to close the dialog box, this pool is assigned to the translation rule.

Policy Dynamic Rules Tab

Use the Policy Dynamic Rules tab of the Translation Rules page to view and configure dynamic translation rules based on source and destination addresses and services. Rules are evaluated sequentially in the order listed. The row number indicates the rule’s position in the ordering of the list. You can use the Up Row and Down Row buttons to change the position of the selected rule.

The Add/Edit Policy Dynamic Rule dialog box is used to add and edit these rules. Refer to Add/Edit Policy Dynamic Rules Dialog Box, page 24-26 for a description of the fields displayed in the table on this page.

Note Policy dynamic rules are only supported by PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules.

Navigation Path

You can access the Policy Dynamic Rules tab from the Translation Rules page. See Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20 for more information.

Note By default, only standard Policy Dynamic Rule elements are displayed in this table. Additional columns for elements defined in the Advanced NAT Options dialog box can be displayed by right-clicking any column heading. (All columns are displayed by default on the General Tab, page 24-32.)

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Add/Edit Policy Dynamic Rules Dialog Box, page 24-26
- Advanced NAT Options Dialog Box, page 24-30
- Select Address Pool Dialog Box, page 24-24
- General Tab, page 24-32
- Standard rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48

– Table Columns and Column Heading Features, page 1-49

Add/Edit Policy Dynamic Rules Dialog Box

Use the Add/Edit Policy Dynamic Rules dialog box to define and edit dynamic translation rules based on source and destination addresses and services.

Navigation Path

You can access the Add/Edit Policy Dynamic Rules dialog box from the Policy Dynamic Rules tab. See Policy Dynamic Rules Tab, page 24-25 for more information.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20
- Policy Dynamic Rules Tab, page 24-25
- Advanced NAT Options Dialog Box, page 24-30
- Select Address Pool Dialog Box, page 24-24

Field Reference

Table 24-11 Add/Edit Policy Dynamic Rules Dialog Box

Element	Description
Enable Rule	If checked, the rule is enabled. Deselect this option to disable the rule without deleting it.
Original: Interface	Enter the name of (or Select) the device interface to which the rule applies.
Original: Sources	Enter IP addresses for (or Select) the source hosts and network objects to which the rule applies. Multiple entries must be separated by commas. Note that this parameter is displayed in the Policy Dynamic Rules table under the column heading “Original Address.”
Translated: Pool	Enter (or Select) the ID number of the pool of addresses used for translation; clicking Select opens the Select Address Pool Dialog Box, page 24-24. Enter a value of zero to specify this as an identity NAT rule.
Translated: Direction	The rule can be applied to Inbound or Outbound traffic, as specified with this option.
Traffic flow: Destinations	Enter IP addresses for (or Select) the destination hosts and network objects to which the rule applies. Multiple entries must be separated by commas.
Traffic flow: Services	Enter (or Select) the services to which the rule applies. Multiple entries must be separated by commas.

Table 24-11 Add/Edit Policy Dynamic Rules Dialog Box (continued)

Element	Description
Category	To assign the rule to a category, choose the category from this list. Categories can help identify rules and objects using labels and color-coding. See Using Category Objects, page 6-13 for more information. **Note** No commands are generated for the Category attribute.
Description	Enter a description of the rule.
Advanced button	Click to open the Advanced NAT Options Dialog Box, page 24-30 to configure advanced settings for this rule.

Static Rules Tab

Use the Static Rules tab of the Translation Rules page to view and configure static translation rules for a security appliance or shared policy. Rules are evaluated sequentially in the order listed. The row number indicates the rule's position in the ordering of the list. You can use the Up Row and Down Row buttons to change the position of the selected rule.

With static translation, internal IP addresses are permanently mapped to a global IP address. These rules map a host address on a lower security-level interface to a global address on a higher security-level interface. For example, a static rule would be used for mapping the local address of a web server on a perimeter network to a global address that hosts on the outside interface would use to access the web server.

Caution The order of Static NAT rules on a security device is important, and Security Manager preserves this ordering during deployment. However, security appliances do not support in-line editing of Static NAT rules. This means that if you move, edit, or insert a rule anywhere above the end of the list, Security Manager will remove from the device all Static NAT rules that follow the new or modified rule, and then re-send the updated list from that point. Depending on the length of the list, this can require substantial overhead, and may result in traffic interruption. Whenever possible, add any new Static NAT rules to the end of the list.

The Add/Edit Static Rule dialog box is used to add and edit these rules. Refer to Add/Edit Static Rule Dialog Box, page 24-28 for descriptions of the fields displayed in the table on this page.

The "Nailed" Column in the Static Rules Table

In addition to the columns representing parameters specified in the Add/Edit Static Rule Dialog Box, page 24-28, the Static Rules table displays a column labeled "Nailed." This value is a product of device discovery; it cannot be changed in Security Manager.

The entry in the "Nailed" Column indicates whether TCP state tracking and sequence checking is skipped for the connection: true or false.

Navigation Path

You can access the Static Rules tab from the Translation Rules page. See Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20 for more information.

Note By default, only standard Static Rules elements are displayed in this table. Additional columns for elements defined in the Advanced NAT Options dialog box can be displayed by right-clicking any column heading. (All columns are displayed by default on the General Tab, page 24-32.)

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Add/Edit Static Rule Dialog Box, page 24-28
- Advanced NAT Options Dialog Box, page 24-30
- General Tab, page 24-32
- Standard rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

Add/Edit Static Rule Dialog Box

Use the Add/Edit Static Rule dialog box to add or edit static translation rules for a firewall device or shared policy.

Navigation Path

You can access the Add/Edit Static Rule dialog box from the Static Rules Tab, page 24-27.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20
- Advanced NAT Options Dialog Box, page 24-30

Field Reference

Table 24-12 Add/Edit Static Rule Dialog Box

Element	Description
Enable Rule	If checked, the rule is enabled. Deselect this option to disable the rule without deleting it.
Translation Type	Select the type of translation for this rule: NAT or PAT.
Original Interface	Enter (or Select) the device interface connected to the host or network with original addresses to be translated.
Original Address	Enter (or Select) the source address to be translated.
Translated Interface	Enter (or Select) the interface on which the translated addresses are to be used. To specify this as an identity NAT rule, enter the same interface in both this and the Original Interface fields.

Table 24-12 Add/Edit Static Rule Dialog Box (continued)

Element	Description
Use Interface IP/Use Selected Address	Specify the address used for the Translated Interface: select Use Interface IP (address), or select Use Selected Address and enter an address, or Select a network/host object.
Enable Policy NAT	Select this option to enable Policy NAT for this translation rule.
Dest Address	If Policy NAT is enabled, specify the destination addresses of the hosts or networks to which the rule applies.
Services	If Policy NAT is enabled, enter or Select the Services to which the rule applies. **Note** For Static Policy NAT, IP is the only Service that can be specified. The syntax for service and service-object specification is: {**tcp** | **udp** | **tcp&udp**}/{*source_port_number* | *port_list_object*}/{*destination_port_number* | *port_list_object*} Note that if you enter only one port parameter, it is interpreted as the destination port (with a source port of "any"). For example, **tcp/4443** means tcp, source port any, destination port 4443, while **tcp/4443/Default Range** means tcp, source port 4443, and destination port Default Range (generally 1-65535). As with all text-entry fields, Security Manager may display auto-complete options. For example, if you type **tcp/** in this field, an auto-complete list of all Port Lists objects defined in Security Manager is displayed. This list will include system-generated objects such as DEFAULT RANGE, HTTPS and WEBPORTS. Refer to Configuring Port List Objects, page 6-102 for more information about Port Lists, and Configuring Service Objects, page 6-103 for more information about defining Services.
Protocol	If PAT is the selected Translation Type, select the protocol, TCP or UDP, to which the rule applies.
Original Port	If PAT is the selected Translation Type, enter the port number to be translated. Note that this parameter is displayed in the Static Rules table under the column heading "Local Port."
Translated Port	If PAT is the selected Translation Type, enter the port number to which the original port number will be translated. Note that this parameter is displayed in the Static Rules table under the column heading "Global Port."
Category	To assign the rule to a category, choose the category from this list. Categories can help identify rules and objects using labels and color-coding. See Using Category Objects, page 6-13 for more information. **Note** No commands are generated for the Category attribute.
Description	Enter a description of the rule.
Advanced button	Click to open the Advanced NAT Options Dialog Box, page 24-30 to configure advanced settings for this rule.

Edit Translated Address Dialog Box

Use the Edit Translated Address dialog box to change just the translated address assigned to a static translation rule. The translated address is the address to which the original address is changed. The interface's IP address can be used, or you can enter a specific IP address. See Static Rules Tab, page 24-27 for more information about static rules and translated addresses.

For detailed information on editing firewall rules cells, see Editing Rules, page 12-10.

Navigation Path

Right-click the Translated Address cell in the Static Rules table (on the NAT > Translation Rules page) and choose **Edit Translated Address**.

Advanced NAT Options Dialog Box

Use the Advanced NAT Options dialog box to configure the advanced connection settings—DNS Rewrite, Maximum TCP and Maximum UDP Connections, Embryonic Limit, Timeout (PIX 6.x), and Randomize Sequence Number—for NAT and Policy NAT. You can also configure these options for Translation Exemption (NAT 0 ACL) rules on an FWSM.

Navigation Path

You can access the Advanced NAT Options dialog box by clicking the **Advanced** button when adding or editing a translation rule. See the following topics for more information:

- Add/Edit Translation Exemption (NAT-0 ACL) Rule Dialog Box, page 24-22
- Add/Edit Dynamic Translation Rule Dialog Box, page 24-23
- Add/Edit Policy Dynamic Rules Dialog Box, page 24-26
- Add/Edit Static Rule Dialog Box, page 24-28

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20

Field Reference

Table 24-13 Advanced NAT Options Dialog Box

Element	Description
Translate the DNS replies that match the translation rule	If checked, the security appliance rewrites DNS replies so an outside client can resolve the name of an inside host using an inside DNS server, and vice versa. For instance, if your NAT rule includes the real address of a host with an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host: one needs the mapped address and one needs the real address. This option rewrites the address in the DNS reply to the client. As an example, assume an inside web server, www.example.com, has the IP address 192.168.1.1, which is translated to 10.1.1.1 on the outside interface of the appliance. An outside client sends a DNS request to an inside DNS server, which will resolve www.example.com to 192.168.1.1. When the reply comes to the security appliance with DNS Rewrite enabled, the security appliance will translate the IP address in the payload to 10.1.1.1, so that the outside client will get the correct IP address. Note that the mapped host needs to be on the same interface as either the client or the DNS server. Typically, hosts that need to allow access from other interfaces use a static translation, so this option is more likely to be used with a static rule.
Max TCP Connections per Rule	Enter the maximum number of TCP connections allowed; valid values are 0 through 65,535. If this value is set to zero, the number of connections is unlimited.
Max UDP Connections per Rule	Enter the maximum number of UDP connections allowed; valid values are 0 through 65,535. If this value is set to zero, the number of connections is unlimited.
Max Embryonic Connections	Enter the number of embryonic connections allowed to form before the security appliance begins to deny these connections. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. Set this limit to prevent attack by a flood of embryonic connections. Valid values are 0 through 65,535. If this value is set to zero, the number of connections is unlimited. Any positive value enables the TCP Intercept feature. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP Intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.

Table 24-13 Advanced NAT Options Dialog Box (continued)

Element	Description
Timeout	For PIX 6.x devices, enter a timeout value for this translation rule, in the format *hh:mm:ss*. This value overrides the default translation timeout specified in Platform > Security > Timeouts, unless this value is 00:00:00, in which case translations matching this rule use the default translation timeout (specified in Platform > Security > Timeouts).
Randomize Sequence Number	If checked, the security appliance randomizes the sequence numbers of TCP packets. Each TCP connection has two Initial Sequence Numbers (ISNs): one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN in both the inbound and outbound directions. Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session. Disable this feature only if: • Another in-line security appliance is also randomizing initial sequence numbers and data is being scrambled. • You are using eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum. • You are using a WAAS device which requires that the security appliance not randomize the sequence numbers of connections. Disabling this option opens a security hole in the security appliance.

General Tab

Use the General tab of the Translation Rules page to view a summary of all translation rules defined for the current device or shared policy. The translation rules are listed in the order that they will be evaluated on the device.

Note The General tab is only visible for PIX, ASA and FWSM devices in router mode, and FWSM 3.2 devices in transparent mode. Other devices in transparent mode support only static translation rules and do not need to display summary information.

Navigation Path

You can access the General tab from the Translation Rules page. See Translation Rules: PIX, FWSM, and pre-8.3 ASA, page 24-20 for more information.

Related Topics

- Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18
- Translation Exemptions (NAT 0 ACL), page 24-21
- Dynamic Rules Tab, page 24-23
- Policy Dynamic Rules Tab, page 24-25
- Static Rules Tab, page 24-27

- Standard rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

Field Reference

Table 24-14 General Tab - Translation Rules Summary Table

Element	Description
Note Hatching (a series of slanted lines) across an entry in the table indicates that rule is currently disabled. (See Enable Rule in Add/Edit Dynamic Translation Rule Dialog Box, page 24-23 for information about enabling and disabling these rules.)	
No.	Rules are evaluated sequentially in the order listed. This number indicates the rule's position in the ordering of the list.
Type	The type of translation rule; for example, Static, Dynamic, Exemption, etc.
Action	Displays "exempt" if the rule is exempt from NAT.
Original Interface	The ID of the device interface to which the rule is applied.
Original Address	The object names or IP addresses of the source hosts and networks to which the rule applies.
Local Port	The port number supplied by the host or network (for static PAT).
Translated Pool	The ID number of the address pool used for translation.
Translated Interface	The interface on which the translated addresses are to be used.
Translated Address	The translated addresses.
Global Port	The port number to which the original port number will be translated (for static PAT).
Destination	The object names and IP addresses of the destination hosts or networks to which the rule applies.
Protocol	The protocol to which the rule applies.
Service	The services to which the rule applies.
Direction	The traffic direction (Inbound or Outbound) on which the rule is applied.
DNS Rewrite	Whether the DNS Rewrite option is enabled: Yes or No. This option is set in the Advanced NAT Options Dialog Box, page 24-30.
Maximum TCP Connections	The maximum number of TCP connections allowed to connect to the statically translated IP address. If zero, the number of connections is unlimited. This option is set in the Advanced NAT Options Dialog Box, page 24-30.
Embryonic Limit	The number of embryonic connections allowed to form before the security appliance begins to deny these connections. If zero, the number of connections is unlimited. A positive number enables the TCP Intercept feature. This option is set in the Advanced NAT Options Dialog Box, page 24-30.

Table 24-14 General Tab - Translation Rules Summary Table (continued)

Element	Description
Maximum UDP Connections	The maximum number of UDP connections allowed to connect to the statically translated IP address. If zero, the number of connections is unlimited. This option is set in the Advanced NAT Options Dialog Box, page 24-30.
Timeout	For PIX 6.x devices, this is the timeout value for a static translation rule. This value overrides the default translation timeout specified in Platform > Security > Timeouts. A Timeout value of 00:00:00 here means that translations matching this rule should use the default translation timeout specified in Platform > Security > Timeouts.
Randomize Sequence Number	Whether the security appliance will randomize the sequence number of TCP packets: Yes or No. This option is set in the Advanced NAT Options Dialog Box, page 24-30, and is enabled by default.
Category	The category to which the rule is assigned. Categories use labels and color-coding to help identify rules and objects. See Using Category Objects, page 6-13 for more information. **Note** No commands are generated for the Category attribute.
Description	The description of the rule, if provided.
Last Ticket(s)	Shows the ticket(s) associated with last modification to the rule. You can click the ticket ID in the Last Ticket(s) column to view details of the ticket and to navigate to the ticket. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page, page 11-72).

Configuring NAT on ASA 8.3+ Devices

The following section describes configuring network address translation on version 8.3 or later ASA devices:

- Translation Rules: ASA 8.3+, page 24-35
  - Add and Edit NAT Rule Dialog Boxes, page 24-37
  - Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43
- Per-Session NAT Rules: ASA 9.0(1)+

See Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18 for information about configuring NAT on other security appliances. Refer to About "Simplified" NAT on ASA 8.3+ Devices, page 24-4 for general information about NAT rules, and the changes to NAT configuration implemented on the ASA 8.3.

Note You can create a NAT object only if you have the Modify privilege mapped to your role. Cisco Security Manager displays error message for authorization.

Translation Rules: ASA 8.3+

Use the Translation Rules page to manage network address translation (NAT) rules on the selected ASA 8.3+ device. See NAT Policies on Security Devices, page 24-15 for information about configuring Translation Rules on other security devices.

Two types of NAT rules are displayed in this table: "manual" rules added by you and any other users, and "automatic" rules generated and applied by Security Manager when an object with NAT properties is assigned to the device. These are referred to as "NAT rules" and "Network Object NAT rules," respectively.

Some Features of the Translation Rules Table

This Translation Rules table is a standard Security Manager rules table, as described in Using Rules Tables, page 12-8. For example, you can move, show and hide columns; you can re-order the manual rules; and you can right-click certain table cells to edit that parameter. In addition, the following features are specific to this Translation Rules table:

- All rules are assigned to one of three pre-defined sections in the table:
  - **NAT Rules Before** – These are rules you or another user have "manually" defined on the device. You can specify that a rule be added to this section by clicking the section heading before adding the rule, although if you do not specify a section, the new rule will be added to this section by default.
  - **Network Object NAT Rules** – These are rules generated and ordered automatically by Security Manager when network objects that include NAT properties are assigned to the device. See Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43 for information about assigning NAT properties to objects. See the section "The NAT Table" in About "Simplified" NAT on ASA 8.3+ Devices, page 24-4 for information about how these rules are ordered.

    Note This section is not displayed in the Translation Rules table in Policy View because these rules are device-specific.

  - **NAT Rules After** – These also are rules you or another user have manually defined on the device. You can specify that a rule is added to this section by clicking the section heading before adding the rule.

  The NAT rules listed in this table are processed on a first-match basis; therefore, order is important. Providing a manual section both before and after the automatic rules lets you ensure all your rules are in the appropriate order, since you can re-order rules only within their section. The rules in each section take precedence over the rules in the section below it. For example, the rules in the top, "Before" section take precedence over the rules in the Network Object NAT section, and so on.
- The type of each rule—Static, Dynamic PAT, or Dynamic NAT and PAT— is indicated visually in the table by presenting ***(S)***, ***(DP)***, or ***(DNP)*** in blue following the Source parameter in the "Translated" column.
- A Bi-directional rule is a static rule that actually consists of two paired rules, one each for outgoing and incoming translation of the specified source and destination values. Each Bi-directional rule entry in the rules table is presented as two lines.

  For example, if Bi-directional is chosen when you create a static rule with Host1 in the Source field and Host2 in the Translated field, two lines are added to the rules table: one with Host1 being translated to Host2, and one with Host2 being translated to Host1.

Related Topics

- NAT Policies on Security Devices, page 24-15
- About "Simplified" NAT on ASA 8.3+ Devices, page 24-4
- Standard rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

Navigation Path

- (Device view) Select **NAT > Translation Rules** from the Device Policy selector.
- (Policy view) Select **NAT (PIX/ASA/FWSM) > Translation Rules** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **Translation Rules** to create a new policy.

The Translation Rules page is displayed. Note that in Policy View, the Network Object NAT Rules section is not displayed because those rules are device-specific.

Adding, Editing and Deleting Rules

To **add** a NAT rule:

1. Select the heading of the section to which the rule is to be added. If you do not select a heading, the rule will be added to *NAT Rules Before* by default.
2. Open the Add NAT Rule dialog box: either click the Add Row button at the bottom of the table, or right-click anywhere in the table (except on an existing rule entry) and choose Add Row from the pop-up menu.
3. Define the rule and then click OK to close the dialog box, adding the rule to the table.

To **edit** a NAT rule:

1. Open the Edit NAT Rule dialog box for the desired rule: either select the rule in the NAT rules table and then click the Edit Row button at the bottom of the table, or simply right-click the desired rule entry and choose Edit Row from the pop-up menu.
2. Edit the rule and then click OK to close the dialog box.

See Add and Edit NAT Rule Dialog Boxes, page 24-37 for a complete description of the Add NAT Rule dialog box.

To **delete** a NAT rule, select the rule in the table and click the Delete Row button at the bottom of the table, or simply right-click the desired rule entry and choose Delete Row from the pop-up menu.

Note To remove a Network Object NAT rule from this table, you must uncheck the Add Automatic Address Translation NAT Rule option, or change the device to which the rule is assigned, in the related Edit Network Host dialog box. See Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43 for additional information.

Enabling and Disabling Rules

You can disable one or more consecutive rules without removing them from the table, as follows:

1. Select the rule(s) to be disabled. If selecting a contiguous block of rules, click the first and then Shift-click the last rule of the block.
2. Right-click a selected rule, and choose **Disable** from the pop-up menu.

Disabled rules are grayed-out in the table.

To re-enable one or one or more consecutive disabled rules, repeat this process, choosing **Enable** from the pop-up menu.

Add and Edit NAT Rule Dialog Boxes

Use the Add NAT Rule dialog box to add a NAT rule to the selected ASA 8.3+ device; this dialog box is not available on earlier-version ASAs, nor on PIX or FWSM devices. Refer to Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices, page 24-18 for information about adding and editing NAT rules on those devices.

Note Except for their titles, the Add NAT Rule and Edit NAT Rule dialog boxes are identical, and the following descriptions apply to both.

Navigation Path

To add a rule, select the section to which you want the rule added (NAT Rules Before or NAT Rules After), and then click the Add Row button below the rules table, or right-click anywhere inside the table and choose **Add Row** to open the Add NAT Rule dialog box. Note that if you do not select a section, the new rule is added to the NAT Rules Before section.

To edit a rule, select the rule and click the Edit Row button, or simply right-click the rule and choose the Edit Row command, to open the Edit NAT Rule dialog box for that rule.

Related Topics

- Chapter 24, "Configuring Network Address Translation"
- Translation Rules: ASA 8.3+, page 24-35
- Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43

Field Reference

Table 24-15 Add and Edit NAT Rule Dialog Boxes

Element	Description
Source Interface	The name of the interface on which a packet may originate; this is the "real" interface. Defaults to "any," which represents all interfaces. Enter or Select the desired interface. **Note** In transparent firewall mode, you must set specific interfaces.
Destination Interface	**Destination Interface** – The name of the interface on which a packet may terminate; this is the "mapped" interface. Defaults to "any," which represents all interfaces. Enter or Select the desired interface. **Note** In transparent firewall mode, you must set specific interfaces.

Table 24-15 Add and Edit NAT Rule Dialog Boxes (continued)

Element	Description
Source NAT Type	The type of translation rule you are creating: • **Static** – Provides static assignment of real addresses to mapped addresses. • **Dynamic PAT (Hide)** – 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. • **Dynamic NAT and PAT** – Provides dynamic assignment of real addresses to mapped addresses, and real ports to mapped ports. Selecting this option adds the PAT Pool Address Translation options to the dialog box. On devices operating in routed mode, this option also provides the fallthrough option described below. **Note** This selection applies only to the specified source translation; destination translation is always static.
Source Translation	
Original Source	The source address the NAT rule will translate. If this is a range or network, all addresses in the range or network are translated.
Translated Source Address Interface	Whether the translation is based on an address or an interface on the device. Select either: • **Address** – Translate the original address using the Networks/Hosts object specified in the Translated Source field. This entry represents the pool of translation addresses: enter or Select the desired Networks/Hosts; defaults to the Original Source (which will produce an Identity NAT rule). • **Interface** – Translate the original address based on the interface specified in the Destination Interface field. For port address translation based on this interface, be sure to configure the options in the Service Translation section (in the Advanced panel of this dialog box). If the Destination Interface is not defined, the Address/Interface selection reverts to Address and the Original Source is inserted into the Address field. This produces an Identity NAT rule, meaning the specified address(es) are translated to themselves (effectively not translated); Identity NAT applies to outbound connections only. **Note** These options are not available when Dynamic NAT and PAT is the selected Type, nor are they available on devices operating in transparent mode.

Table 24-15 Add and Edit NAT Rule Dialog Boxes (continued)

Element	Description
PAT Pool Address Translation	This option is available when Dynamic NAT and PAT is the selected 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. Refer to PAT Pools and Round Robin Allocation, page 24-42 for additional information about these features. Check the PAT Pool Address Translation box to enable the following options: • **Address** or **Interface** – Select Address to indicate that the PAT Pool Address field contains networks/hosts (or networks/hosts objects) for use as the PAT pool. Select Interface to provide a Fallthrough Interface. • **Address** – Enter or Select the desired Networks/Hosts or desired Interface according to your Address or Interface selection above. • **Use Round Robin Allocation** – Check this box to map addresses/ports using a "round-robin" approach. See PAT Pools and Round Robin Allocation, page 24-42 for more information about this option. • **Extended PAT Table** (Available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1)) - Check this box 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. This option is available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1). • **Flat Port Range** (Available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1)) - Check this box 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 select **Include Reserve Ports**. • **Include Reserve Ports** (Available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1)) - Check this box to include the reserve ports, 1-1023, in the PAT range. • **Block Allocation** (Available for ASA 9.5(1) and later) – Check this box to allocate a block of ports per host. This feature is supported from Security Manager version 4.9 onwards for ASA devices 9.5(1) or later.

Table 24-15 Add and Edit NAT Rule Dialog Boxes (continued)

Element	Description
Destination Translation	
Use the options in this section to configure optional static translation of destination addresses: **Note** If defined, Destination Translation is always static, regardless of the rule Type. **Note** These options are not available on devices operating in transparent mode.	
Original Destination Address Interface	Whether the translation is based on an address or an interface on the device. Select either: • **Address** - Translate the original destination using the Networks/Hosts object specified in the Translated Destination field. If Address is selected, specify the Networks/Hosts object, whose original destination addresses should be translated, in the **Original Destination** entry field. • **Interface** – Translate the original destination using the Networks/Hosts object specified in the Translated Destination field. If Interface is selected, enter or select the desired interface in the Destination Interface field. The Interface Selector list contains all interfaces currently defined on the device.
Translated Destination	This entry represents the pool of destination addresses to use for translation: enter or select the desired Networks/Hosts object.
Service Translation	
Use the options in this section to configure port address translation. These service objects represent a service protocol (TCP or UDP), and one or more ports. The mapping of original ports to translated port is circular. That is, the first original value is mapped to the first translated value, and the second original value is mapped to the second translated value, and so on until all original values are translated. If the pool of translated port is exhausted before that point, mapping continues using the first translated value again. See Understanding and Specifying Services and Service and Port List Objects, page 6-100 for information about configuring service objects. **Note** Service Translation and the following **Translate DNS replies that match this rule** option cannot be used together.	
Original Service	Enter or select the Service object that defines the service(s) to be translated. Leave the Original Service field blank to configure translation of any service to the specified Translated Service. **Note** The protocol specified in both Service objects must be the same.
Translated Service	Enter or select the Service object that provides the service(s) to be used for translation.
Options	

Table 24-15 Add and Edit NAT Rule Dialog Boxes (continued)

Element	Description
Translate DNS replies that match this rule	When checked, 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.
Fallthrough to Interface PAT (Destination Interface)	When checked, 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 Use Address field. This option is available only when Dynamic NAT and PAT is the chosen Type on devices operating in routed mode.
IPv6	When selected, the IPv6 address of the interface is used.
Net to net mapping of IPv4 to IPv6	When checked, translates the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For a one-to-one translation, you must select this option.
Do not proxy ARP on Destination Interface	Check this box to disable proxy ARP on the specified Destination Interface. This option is available only when Static is the chosen rule Type. **Note** This option is available on ASA 8.4.2+ devices, only when Bidirectional is the chosen Direction. 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. (The NAT Exempt rules always take priority and appear above all other NAT rules in the Translation Rules table.) **Note** You also can disable Proxy ARP on individual interfaces, as described in Configuring No Proxy ARP, page 56-1.
Perform route lookup for Destination Interface	If this option is selected, the egress interface is determined using route look-up instead of using the specified Destination Interface. Be sure this box is checked for a NAT Exempt rule. This option is supported only for Static Identity NAT. **Note** This option is available on ASA 8.4.2+ devices, only when Bidirectional is the chosen Direction. The option is not available on devices operating in transparent mode.

Table 24-15 Add and Edit NAT Rule Dialog Boxes (continued)

Element	Description
Unidirectional	This feature lets you configure a static NAT rule in a single direction only; or dual rules, one each for both directions (forward and reverse). When selected, a single static NAT is created, as specified by the other options in this dialog box. Dynamic rules are uni-directional by default. If deselected, two linked static NAT rules are created, encompassing both directions of the translation, as specified by the other options in this dialog box. Note that each bi-directional rule entry in the rules table consists of two lines.
Description	(Optional) Provide a description of the rule.
Category	(Optional) Choose a category to assign to the rule. Categories can help you organize and identify rules and objects; see Using Category Objects, page 6-13 for more information. **Note** This option is not available when Dynamic NAT and PAT is the chosen rule Type.

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.

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 Translated Source field of the Add/Edit NAT Rule dialog boxes) to be used for translation. This pool could consist of individual IP addresses, ranges of addresses, Networks/Hosts objects, or Network/Host 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 Translated Source field) is considered the NAT Pool, while the PAT Pool addresses are specified in the PAT Pool Address Translation 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 Add and Edit NAT Rule Dialog Boxes, page 24-37 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 for PAT Pool—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. Note 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.

Add or Edit Network/Host Dialog Box: NAT Tab

Use the NAT tab in any of the dialog boxes used to add or edit host, network, or address range objects to create or update object NAT rules. This NAT configuration is used only for ASA 8.3+ devices; if you use the object on any other type of device, the NAT configuration is ignored.

The NAT configuration is created as a device override and is not kept in the global object. Therefore, you must select the **Allow Value Override per Device** option if you configure these NAT options. (This option is selected automatically when you close the dialog box.)

This topic describes the fields on the NAT tab. For information about the fields on the General tab, see Add or Edit Network/Host Dialog Box, page 6-83.

Navigation Path

Select the NAT tab on the Add or Edit Network/Host Dialog Box when creating or editing a host, network, or address range object.

Related Topics

- Chapter 24, "Configuring Network Address Translation"
- Creating Networks/Hosts Objects, page 6-82
- Understanding Networks/Hosts Objects, page 6-80
- Specifying IP Addresses During Policy Definition, page 6-87
- Policy Object Manager, page 6-4

Field Reference

Table 24-16 Network/Host Dialog Box NAT Tab

Element	Description
Add Automatic Address Translation NAT Rule	If checked, a network address translation (NAT) rule, as defined here, will be applied to the device specified in the Translated By field. The rule will appear in the Network Object NAT Rule section of the Translation Rules table for that device (see Translation Rules: ASA 8.3+, page 24-35).
Translated By	The device on which you are configuring the NAT rule. Click Select to select the device from a list. The list is filtered to show only ASA 8.3+ devices.
Source Interface	The name of the interface on which a packet may originate; this is the "real" interface. Defaults to **any**, which represents all interfaces.
Destination Interface	The name of the interface on which a packet may terminate; this is the "mapped" interface. Defaults to **any**, which represents all interfaces.
Type	The type of translation rule you are creating: • **Static** – Enables static assignment of real addresses to mapped addresses. • **PAT (Hide)** – Enables dynamic assignment of multiple local addresses to a single global IP address and a unique port number. • **Dynamic NAT and PAT** – Enables dynamic assignment of real addresses to mapped addresses, and real ports to mapped ports.
Source Translation	
Original value	Shows the address configured on the General tab of this dialog box. This is the source address the NAT rule will translate. If it is a range or network, all addresses in the range or network will be translated.
Translated Source Use Address Use Interface (available only for Static and PAT)	Whether the translation is based on an address or an interface on the device: • **Use Address**—Translate the original address using the specified address or network/host object. Enter the address or object name in the **Address** field, or click Select to select the object from a list. • **Use Interface** – Translate the original address based on the interface specified in the Destination Interface field. **Note** The Use Interface options are available only when either Static or PAT (Hide) is chosen as the Type.

Table 24-16 Network/Host Dialog Box NAT Tab (continued)

Element	Description
PAT Pool Address Translation	This option is available when Dynamic NAT and PAT is the selected 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. Refer to PAT Pools and Round Robin Allocation, page 24-42 for additional information about these features. Check the PAT Pool Address Translation box to enable the following options: • **Use Address** or **Use Interface** – Select Use Address to indicate that the PAT Pool Address field contains networks/hosts (or networks/hosts objects) for use as the PAT pool. Select Use Interface to provide a Fallthrough Interface. • **PAT Pool Address** – Enter or Select the desired Networks/Hosts or desired Interface according to your Address or Interface selection above. • **Use Round Robin Allocation for PAT Pool** – Check this box to map addresses/ports using a "round-robin" approach. See PAT Pools and Round Robin Allocation, page 24-42 for more information about this option. • **Extended PAT Table** (Available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1)) - Check this box 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. This option is available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1). • **Flat Port Range** (Available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1)) - Check this box 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 select **Include Reserve Ports**. • **Include Reserve Ports** (Available for ASA 8.4(3) and later, not including 8.5(1) or 8.6(1)) - Check this box to include the reserve ports, 1-1023, in the PAT range.

Table 24-16 Network/Host Dialog Box NAT Tab (continued)

Element	Description
Service Translation	
Use the options in this section of the Advanced panel to configure static port address translation: (Available for Static rules only.) **Note** Service Translation and the **Translate DNS replies that match this rule** option cannot be used together.	
Protocol	Whether a TCP or UDP port.
Original Port	The port on which the traffic enters the device.
Translated Port	The port number which is to replace the original port number.
Options	
Translate DNS replies that match this rule	When checked, 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. **Note** This option and Service Translation cannot be used together.
Fallthrough to Interface PAT (Destination Interface)	When checked, 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 Use Address field. This option is available only when Dynamic NAT and PAT is the chosen Type on devices operating in routed mode.
IPv6	When selected, the IPv6 address of the interface is used.
Net to net mapping of IPv4 to IPv6	When checked, translates the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For a one-to-one translation, you must select this option.
Do not proxy ARP on Destination Interface	Check this box to disable proxy ARP on the specified Destination Interface. This option is available only when Static is the chosen rule Type. 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. (The NAT Exempt rules always take priority and appear above all other NAT rules in the Translation Rules table.) **Note** You also can disable Proxy ARP on individual interfaces, as described in Configuring No Proxy ARP, page 56-1.

Table 24-16 Network/Host Dialog Box NAT Tab (continued)

Element	Description
Perform route lookup for Destination Interface	If this option is selected, the egress interface is determined using route look-up instead of using the specified Destination Interface. Be sure this box is checked 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.

Per-Session NAT Rules: ASA 9.0(1)+

Use the Per-Session NAT Rules page to configure per-session PAT rules on the selected ASA 9.0(1)+ device. By default, all TCP PAT traffic and all UDP DNS traffic uses per-session PAT. You can configure per-session rules to use multi-session PAT for specific traffic.

Per-Session PAT vs. Multi-Session PAT (Version 9.0(1) and Later)

The per-session PAT feature improves the scalability of PAT and, for clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the control unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For "hit-and-run" traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session feature, the connection rate for one address for an IP protocol is 65535/average-lifetime.

By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule.

Some Features of the Per-Session NAT Rules Table

This Translation Rules table is a standard Security Manager rules table, as described in Using Rules Tables, page 12-8. For example, you can move, show and hide columns; you can re-order the rules; and you can right-click certain table cells to edit that parameter.

The NAT rules listed in this table are processed on a first-match basis; therefore, order is important.

Related Topics

- Add and Edit Per Session NAT Rule Dialog Boxes, page 24-48
- NAT Policies on Security Devices, page 24-15
- About “Simplified” NAT on ASA 8.3+ Devices, page 24-4
- Standard rules table topics:
  - Using Rules Tables, page 12-8
  - Filtering Tables, page 1-48
  - Table Columns and Column Heading Features, page 1-49

Navigation Path

- (Device view) Select **NAT > Per-Session NAT Rules** from the Device Policy selector.

- (Policy view) Select **NAT (PIX/ASA/FWSM) > Per-Session NAT Rules** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **Translation Rules** to create a new policy.

The Per-Session NAT Rules page is displayed.

Adding, Editing and Deleting Rules

To **add** a per-session NAT rule:

1. Select the rule under which the rule is to be added. If you do not select a heading, the rule will be added to the end of the table by default.
2. Open the Add Per-Session NAT Rule dialog box: either click the **Add Row** button at the bottom of the table, or right-click anywhere in the table and choose **Add Row** from the pop-up menu.
3. Define the rule and then click **OK** to close the dialog box, adding the rule to the table.

See Add and Edit Per Session NAT Rule Dialog Boxes, page 24-48 for a complete description of the Add Per-Session NAT Rule dialog box.

To **edit** a per-session NAT rule:

1. Open the Edit Per-Session NAT Rule dialog box for the desired rule: either select the rule in the Per-Session NAT rules table and then click the **Edit Row** button at the bottom of the table, or simply right-click the desired rule entry and choose **Edit Row** from the pop-up menu.
2. Edit the rule and then click **OK** to close the dialog box.

See Add and Edit Per Session NAT Rule Dialog Boxes, page 24-48 for a complete description of the Edit Per-Session NAT Rule dialog box.

To **delete** a per-session NAT rule, select the rule in the table and click the **Delete Row** button at the bottom of the table, or simply right-click the desired rule entry and choose **Delete Row** from the pop-up menu.

Enabling and Disabling Rules

You can disable one or more consecutive rules without removing them from the table, as follows:

1. Select the rule(s) to be disabled. If selecting a contiguous block of rules, click the first and then Shift-click the last rule of the block.
2. Right-click a selected rule, and choose **Disable** from the pop-up menu.

   Disabled rules are grayed-out in the table.

To re-enable one or one or more consecutive disabled rules, repeat this process, choosing **Enable** from the pop-up menu.

Add and Edit Per Session NAT Rule Dialog Boxes

By default, all TCP PAT traffic and all UDP DNS traffic uses per-session PAT. To use multi-session PAT for traffic, you can configure per-session PAT rules: a permit rule uses per-session PAT, and a deny rule uses multi-session PAT.

For more information about per-session vs. multi-session PAT, see Per-Session NAT Rules: ASA 9.0(1)+.

Defaults

By default, the following rules are installed:

- Permit TCP from any (IPv4 and IPv6) to any (IPv4 and IPv6)

- Permit UDP from any (IPv4 and IPv6) to domain

These rules do not appear in the rule table.

Note You cannot remove these rules, and they always exist after any manually-created rules. Because rules are evaluated in order, you can override the default rules. For example, to completely negate these rules, you could add the following:

Deny TCP from any (IPv4 and IPv6) to any (IPv4 and IPv6)
Deny UDP from any (IPv4 and IPv6) to domain

Navigation Path

From the Per-Session NAT Rules: ASA 9.0(1)+ page, do one of the following:

- To add a rule, select the rule under which you want the rule added, and then click the **Add Row** button below the rules table, or right-click anywhere inside the table and choose **Add Row** to open the Add Per-Session NAT Rule dialog box.
- To edit a rule, select the rule and click the **Edit Row** button, or simply right-click the rule and choose **Edit Row** to open the Edit Per-Session NAT Rule dialog box for that rule.

Related Topics

- Per-Session NAT Rules
- Chapter 24, "Configuring Network Address Translation"
- Translation Rules: ASA 8.3+, page 24-35
- Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43

Field Reference

Table 24-17 Add and Edit NAT Rule Dialog Boxes

Element	Description
Action	The action for this rule: Permit or Deny. A permit rule uses per-session PAT; a deny rule uses multi-session PAT.
Original Network	The source address or addresses (or Networks/Hosts objects) to which the rule applies. If this is a range or network, all addresses in the range or network are translated.
Destination Network	The destination address or addresses (or Networks/Hosts objects) to which the rule applies.
Service (tcp/udp Only)	Enter or Select the Service object that defines the service(s) to be translated. These service objects represent a service protocol (TCP or UDP), and one or more ports. See Understanding and Specifying Services and Service and Port List Objects, page 6-100 for information about configuring service objects.

Table 24-17 Add and Edit NAT Rule Dialog Boxes (continued)

Element	Description
Category	(Optional) Choose a category to assign to the rule. Categories can help you organize and identify rules and objects; see Using Category Objects, page 6-13 for more information. **Note** This option is not available when Dynamic NAT and PAT is the chosen rule Type.
Description	(Optional) Provide a description of the rule.