



CHAPTER 22

NAT

The security appliance supports both the Network Address Translation feature, which provides a globally unique address for each outbound host session, and the Port Address Translation feature, which provides a single, unique global address for up to 64,000 simultaneous outbound or inbound host sessions. The global addresses used for NAT come from a pool of addresses to be used specifically for address translation. The unique global address that is used for PAT can either be one global address or the IP address of a given interface.

The security appliance can perform NAT or PAT in 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. Outside NAT gives you the option to translate an outside host or network to an inside host or network, and it is sometimes referred to as bi-directional NAT. Just as when you translate outbound traffic with NAT, you may choose dynamic NAT, static NAT, dynamic PAT, and static PAT. If necessary, you may use outside NAT together with inside NAT to translate the both source and destination IP addresses of a packet.

NAT

The **NAT pane** lets you view all the address translation rules or Network Address Translation exemption rules applied to your network.

From the NAT pane you can also create a **Translation Exemption Rule**, which lets you specify traffic that is exempt from being translated or encrypted. The Exemption Rules are grouped by interface in the table, and then by direction. If you have a group of IP addresses that will be translated, you can exempt certain addresses from being translated using the Exemption Rules. You can use a previously configured access list to define your exemption rule. ASDM will write to the command-line interface a **nat 0** command. You can resort the view of your exemption by clicking the column heading.

You can also identify local traffic for address translation by specifying the source and destination addresses (or ports) in an access list using policy NAT. With policy NAT, you can create multiple NAT or static statements that identify the same local address as long as the source/port and destination/port combination is unique for each statement. You can then match different global addresses to each source/port and destination/port pair.

Prerequisites

- Before you can designate access and translation rules for your network, you must first define each host or server for which a rule will apply.



Caution

Review Important Notes about Object Groups regarding the naming of Network and Service Groups.

Restrictions

- You cannot use unavailable translation commands until you define networks or hosts. Unavailable commands appear dimmed on the menu.
- It is important to note that the order in which you apply translation rules can affect the way the rules operate. ASDM will list the static translations first and then the dynamic translations. When processing NAT, the security appliance will first translate the static translations in the order they are configured. You can use Insert or Insert After to determine the order in which static translations are processed. Because dynamically translated rules are processed on a best match basis, the option to insert a rule before or after a dynamic translation is disabled.
- It is necessary to run NAT even if you have routable IP addresses on your secure networks. When running NAT with routable IP addresses, translate the routable IP address to itself on the outside.
- A packet sourced on the more secure (inside) interface destined for an intermediate (DMZ) interface can not have the same translated address when it is outbound on a less secure (outside) interface. Furthermore, if one dynamic rule is deleted on either of the outbound interfaces, all outbound dynamic rules for translations originating on the same interface will be deleted.
- It is possible to create an Exemption Rule for traffic so that traffic is sent out to the Internet or a less secure interface unencrypted. This can be useful in a scenario where you want to encrypt some traffic to another remote VPN network, but would like traffic destined to anywhere else to remain unencrypted.

Fields

- **Add**—Adds a new NAT rule. Choose the type of rule you want to add from the drop-down list.
- **Edit**—Edits an NAT rule.
- **Delete**—Deletes a NAT rule.
- **Move Up**—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.
- **Move Down**—Moves a rule down.
- **Cut**—Cuts a rule.
- **Copy**—Copies the parameters of a rule so you can start a new rule with the same parameters using the Paste button.
- **Paste**—Opens an Add/Edit Rule dialog box with the copied or cut parameters of the rule prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.
- **Find**—Filters the display to show only matching rules. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
 - **Filter drop-down list**—Choose the criteria to filter on, either Interface, Source, Destination, Service, Action, or Rule Query. A rule query is a collection of multiple criteria that you can save and use repeatedly.
 - **Filter field**—For the Interface type, this field becomes a drop-down list so you can choose an interface name. For the Action type, the drop-down list includes Exempt, Static, and Dynamic. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type one manually, or browse for one by clicking the ... button and launching the Browse Address dialog box. The Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can type one manually, or browse for one by clicking the ... button and launching the Browse Service Groups dialog box.

- Filter—Runs the filter.
- Clear—Clears the Filter field.
- Rule Query—Opens the Rules Queries dialog box so you can manage named rule queries.
- Show Rule Flow Diagram—Shows the Rule Flow Diagram area under the rule table. This diagram shows the networks, type of traffic, interface name, direction of flow, and action.
- Packet Trace—Opens the Packet Tracer tool with the parameters pre-filled with the characteristics of the selected rule.

The following description summarizes the columns in the NAT Rules table. You can edit the contents of these columns by double-clicking on a table cell. Double-clicking on a column header sorts the table in ascending alphanumeric order, using the selected column as the sort key. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- **No**—Indicates the order of evaluation for the rule.
- **Type**—Displays the translation rule type applied to the given row, which can either be **dynamic** or **static**.
 - **Dynamic**—Internal IP addresses are dynamically translated using IP addresses from a pool of global addresses or, in the case of PAT, a single address. These rules translate addresses of hosts on a higher security level interface to addresses selected from a pool of addresses for traffic sent to a lower security level interface. Dynamic translations are often used to map local, RFC 1918 IP addresses to addresses that are Internet-routable addresses. They are represented with the dynamic icon.
 - **Static**—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. They are represented with the static icon.
- **Real**—Displays the original address with its associated interface before network translation is applied.
 - **Source Network**—The source network on which the traffic to be translated resides for policy NAT. For regular NAT, this displays any.
 - **Destination Network**—The destination network on which the traffic to be translated resides for policy NAT. For regular NAT, this displays any.
- **Translated**—Displays the translated addresses and the associated interfaces after network translation is applied.
 - **Interface**—The interface on which the translated addresses reside.
 - **Address**—The translated addresses.
- **Options**—Includes the following items:
 - **DNS Rewrite**—Lets the security appliance rewrite the DNS record so that an outside client can resolve name of an inside host using an inside DNS server, or vice versa. For example, assume an inside web server www.example.com has IP 192.168.1.1, it is translated to 10.1.1.1 on the outside interface. 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.

- **Maximum TCP Connections**—The maximum number of TCP connections that are allowed to connect to the statically translated IP address. Valid options are 0 through 65,535. If this value is set to zero, the number of connections is unlimited.
- **Embryonic Limit**—The number of embryonic connections allowed to form before the security appliance begins to deny these connections. Set this limit to prevent attack by a flood of embryonic connections. An embryonic connection is one that has been started but has not yet been established, such as a three-way TCP handshake state. Valid values are 0 through 65,535. If this value is set to zero, the number of connections is unlimited. A positive number enables the TCP Intercept feature.
- **Maximum UDP Connections**—The maximum number of UDP connections that are allowed to connect to the statically translated IP address. Valid options are 0 through 65,535. If this value is set to zero, the number of connections is unlimited.
- **Randomize Sequence Number**—With this check box checked, the security appliance will randomize the sequence number of TCP packets. Disable this feature only if another inline security appliance is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the security appliance. The default is selected.
- **Description (for Policy NAT only)**—If a description of the rule is available, it is displayed in this column.
- **Enable traffic through the firewall without address translation**—Allows traffic to pass through the security appliance without address translation.
- **Addresses**—Tab that lets you add, edit, delete, or find network objects or network object groups.
- **Services**—Tab that lets you add, edit, delete, or find services.
- **Global Pools**—Tab that lets you manage the Global address NAT pools, which are used for dynamic NAT configuration. These are the IP addresses the security appliance will present to the outside or less secure interface for which they are configured.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Static NAT Rule

The **Add/Edit Static NAT Rule** dialog box lets you add, edit, and paste translation rules for your security appliance, which are viewed in the **NAT Rules** table. A **Static NAT rule** specifies that the address translation is a static, one-to-one translation of an IP address from a private (non-valid) IP address to a global (valid) IP address. Static or Dynamic can be selected, but not both.



Note

Review Important Notes about Object Groups regarding the naming of Network and Service Groups.

Fields

- **Real Address**—The original address with its associated interface before network translation is applied.
 - **Interface**—Selects the security appliance network interface on which the original host or network resides.
 - **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
 - **Mask**—Select the network mask (netmask) for the address.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree for a predefined host or network.
- **Static Translation**—Lets you specify the static interface and IP address.
 - **Interface**—Selects the security appliance network interface for static translation.
 - **IP address**—Selects the IP address for the static translation.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree from a predefined host or network.
- **Enable Port Address Translation (PAT)**—Choose this option to specify the protocol, original port, and translated port for PAT.
 - Protocol—**TCP or UDP.**
 - Original Port—**Select from the list of ports.**
 - Translated Port—**Select from the list of ports.**
- **NAT Options**—Lets you configure the DNS Rewrite, Maximum Connections, Embryonic Limit and Randomize Sequence Number.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Dynamic NAT Rule

The **Add/Edit Dynamic NAT Rule** dialog box lets you add, edit, and paste translation rules for your security appliance, which are viewed in the **NAT Rules** table. A **Dynamic NAT rule** specifies either a predefined pool of IP addresses, or to perform PAT on a global IP address or the less secure interface for multiple hosts on the more secure interface. For example, if your inside network has multiple hosts, you can permit outbound access through a pool or a PAT address by using Dynamic NAT to dynamically assign an global IP address for each host requesting an outbound connection. Static or Dynamic can be selected, but not both.

**Note**

Review Important Notes about Object Groups regarding the naming of Network and Service Groups.

Fields

- **Real Address**—The original address with its associated interface before network translation is applied.
 - **Interface**—Selects the security appliance network interface on which the original host or network resides.
 - **IP Address**—Specifies the IP address of the host or network to which you would like to apply a rule.
 - **Mask**—Select the network mask (netmask) for the address.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree for a predefined host or network.
- **Dynamic Translation**—Lets you specify the dynamic interface and global address pool.
 - **Interface**—Selects the security appliance network interface for dynamic translation.
 - **Add**—Adds a global pool.
 - **Edit**—Edits a global pool.
 - **Delete**—Deletes a global pool.
- **NAT Options**—Lets you configure the DNS Rewrite, Maximum Connections, Embryonic Limit and Randomize Sequence Number.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

NAT Options

The **NAT Options** dialog box lets you configure the **DNS Rewrite**, **Maximum Connections**, **Embryonic Limit**, and **Randomize Sequence Number** for NAT and Policy NAT.

Fields

- **DNS Rewrite**—Lets the security appliance rewrite the DNS record so that an outside client can resolve name of an inside host using an inside DNS server, or vice versa. For example, assume an inside web server www.example.com has IP 192.168.1.1, it is translated to 10.1.1.1 on the outside interface. 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.
- **Maximum TCP Connections**—The maximum number of TCP connections that are allowed to connect to the statically translated IP address. Valid options are 0 through 65,535. If this value is set to zero, the number of connections is unlimited.
- **Maximum UDP Connections**—The maximum number of UDP connections that are allowed to connect to the statically translated IP address. Valid options are 0 through 65,535. If this value is set to zero, the number of connections is unlimited.

- **Embryonic Limit**—The number of embryonic connections allowed to form before the security appliance begins to deny these connections. Set this limit to prevent attack by a flood of embryonic connections. An embryonic connection is one that has been started but has not yet been established, such as a three-way TCP handshake state. Valid values are 0 through 65,535. If this value is set to zero, the number of connections is unlimited. A positive number enables the TCP Intercept feature.
- **Randomize Sequence Number**—With this check box checked, the security appliance will randomize the sequence number of TCP packets. Disable this feature only if another inline security appliance is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the security appliance. The default is selected.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Global Pools

The **Global Pools** dialog box lets you view, define new, or delete existing global address pools used in dynamic NAT rules. For more information on dynamic NAT rules and its uses, refer to Understanding Dynamic NAT.

Fields

- **Interface**—Identifies the interface name associated with the address pool used for dynamic address translation.
- **Pool ID**—Identifies the ID number of the address pool.
- **IP Address(es)**—Identifies the type and value of the address(es) for the pool. It can identify one of the following types:
 - A range of addresses
 - A PAT address
 - A PAT address associated with an interface

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Global Address Pool

The **Add/Edit Global Address Pool** dialog box lets you define the settings for a new global address pool or edit the settings of an existing pool.

Fields

- **Interface**—Specifies the interface name to associate with the new address pool. Select the name in the Interface drop-down list.
- **Pool ID**—Specifies the ID number that dynamic NAT rules use to reference this address pool. Enter the number in the Pool ID field.
- **Range**—Select this option to specify that a range of IP addresses be used with the new address pool. If you select this option, specify the following values:
 - Enter the start and end addresses used by the range in the **IP Address** fields. These addresses are the addresses to which the original addresses will be translated. If the security appliance is exposing the host or network to users on the Internet, these IP addresses must be valid IP addresses that are registered with the American Registry for Internet Numbers.
 - Enter the mask in the **Network Mask (optional)** field. This value identifies the mask of the network on which translated IP addresses are members.
- **Port Address Translation (PAT)**—Choose this option to specify that an IP address be used for Port Address Translation. If you select this option, specify the following value:
 - Enter the IP address used for PAT in the **IP Address** field. This value is the specific translated IP address to which you want to translate the original addresses of the translated host or network. If the security appliance is exposing the host or network to users on the Internet, this IP address must be a valid IP address that is registered with ARIN.
- **Port Address Translation (PAT) using the IP address of the interface**—Select this option to specify that the IP address assigned to the interface selected in the **Interface** drop-down list be used as the translated address for PAT.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Static Policy NAT Rule

The **Add/Edit Static Policy NAT Rule** dialog box lets you configure the protocol and service that policy NAT will use to translate traffic.

Fields

- **Real Address**—The original address with its associated interface before network translation is applied.

- **Interface**—Selects the security appliance network interface on which the original host or network resides.
- Source—**Choose type, IP address, and netmask.**
- Destination—**Choose type, IP address, and netmask**
- **Protocol and Service**—Lets you define the protocols and services to be used for policy NAT.
 - **TCP**—Select to define the TCP protocol types used for translation with policy NAT.
 - **UDP**—Select to define the UDP protocol types used for translation with policy NAT.
 - **ICMP**—Select to define the ICMP protocol types used for translation with policy NAT.
 - **IP**—Select to define the IP protocol types used for translation with policy NAT.
 - **IP Protocol**—Depending on your selection this displays the TCP, UDP, ICMP or IP protocol type. You can either enter the port or protocol number or select the protocol from a drop-down list using the browse (...) button.
- **Static Translation**—Lets you specify the static interface and IP address.
 - **Interface**—Selects the security appliance network interface for static translation.
 - **IP address**—Selects the IP address for the static translation.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree from a predefined host or network.
- **Enable Port Address Translation (PAT)**—Choose this option to specify the protocol, original port, and translated port for PAT.
 - Protocol—**TCP or UDP.**
 - Original Port—**Select from the list of ports.**
 - Translated Port—**Select from the list of ports.**
- **NAT Options**—Lets you configure the DNS Rewrite, Maximum Connections, Embryonic Limit and Randomize Sequence Number.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Dynamic Policy NAT Rule

The **Add/Edit Dynamic Policy NAT Rule** dialog box lets you configure the protocol and service that policy NAT will use to translate traffic.

Fields

- **Real Address**—The original address with its associated interface before network translation is applied.

- **Interface**—Selects the security appliance network interface on which the original host or network resides.
- Source—**Choose type, IP address, and netmask.**
- Destination—**Choose type, IP address, and netmask**
- **Protocol and Service**—Lets you define the protocols and services to be used for policy NAT.
 - **TCP**—Select to define the TCP protocol types used for translation with policy NAT.
 - **UDP**—Select to define the UDP protocol types used for translation with policy NAT.
 - **ICMP**—Select to define the ICMP protocol types used for translation with policy NAT.
 - **IP**—Select to define the IP protocol types used for translation with policy NAT.
 - **IP Protocol**—Depending on your selection this displays the TCP, UDP, ICMP or IP protocol type. You can either enter the port or protocol number or select the protocol from a drop-down list using the browse (...) button.
- **Dynamic Translation**—Lets you specify the dynamic interface and global address pool.
- **Real Address**—The original address with its associated interface before network translation is applied.
 - **Interface**—Selects the security appliance network interface on which the original host or network resides.
 - **IP Address**—Specifies the IP address of the host or network to which you would like to apply a rule.
 - **Mask**—Select the network mask (netmask) for the address.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree for a predefined host or network.
- **Dynamic Translation**—Lets you specify the dynamic interface and global address pool.
 - **Interface**—Selects the security appliance network interface for dynamic translation.
 - **Add**—Adds a global pool.
 - **Edit**—Edits a global pool.
 - **Delete**—Deletes a global pool.
- **NAT Options**—Lets you configure the DNS Rewrite, Maximum Connections, Embryonic Limit and Randomize Sequence Number.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit NAT Exempt Rule

The **Add/Edit NAT Exempt Rule** dialog box lets you add and edit Network Address Translation exemption rules for your security appliance. Depending upon which command you selected in the **Translation Rules** menu, the title for this dialog box will appear as **Add Address Exemption Rule** or **Edit Address Exemption Rule**.

Fields

- **Action**—The action drop-down list lets you select the action, exempt or do not exempt, that this exemption rule will take if the host/network meets the criteria defined. The Select an action list options are as follows:
 - **Exempt**—Specifies that the traffic defined will be exempted from NAT.
 - **Do Not Exempt**—Specifies that the traffic defined will not be exempted from NAT.
- **IP Address**—Selects the criteria of testing the IP address of the source host or network to determine if the action of the exemption rule will be applied. Selecting this option displays the following fields:
 - **Interface**—Selects the security appliance network interface name on which the original host or network resides.
 - **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree from a predefined host or network.
 - **Mask**—Select the network mask (netmask) for the address.
- **Name**—Selects the criteria of testing the name of the source host or network to determine if the action of the exemption rule will be applied. Selecting this option displays the following fields:
 - **Name**—Lets you select a previously defined name of a host or network to which you would like to apply the rule. The security appliance also automatically generates a hostname for each interface by using the interface name, such as inside or outside.
- **Group**—Selects the criteria of testing a group of the source host or network to determine if the action of the exemption rule will be applied. Selecting this option displays the following fields:
 - **Interface**—Selects the security appliance network interface name on which the original host or network resides.
 - **Group**—Selects the group of the host or network to which you would like to apply the rule.
- **When Connecting To**—The When Connecting To area lets you define the criteria which must be met for the action to be performed. The criteria may be defined by selecting an IP address, Name, Group, or by browsing a previously defined drop-down list of hosts/networks.
- **IP address**—Specifies the IP address of the destination host or network to which you would like to apply the exemption rule.
 - **Interface**—Selects the security appliance network interface name on which the original host or network resides.
 - **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree from a predefined host or network.
 - **Mask**—Select the network mask (netmask) for the address.

- **Name**—Selects the criteria of testing the name of the source host or network to determine if the action of the exemption rule will be applied. Selecting this option displays the following fields:
 - **Name**—Lets you select a previously defined name of a host or network to which you would like to apply the rule. The security appliance also automatically generates a hostname for each interface by using the interface name, such as inside or outside.
- **Group**—Selects the criteria of testing a group of the source host or network to determine if the action of the exemption rule will be applied. Selecting this option displays the following fields:
 - **Interface**—Selects the security appliance network interface name on which the original host or network resides.
 - **Group**—Selects the group of the host or network to which you would like to apply the rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Identity NAT Rule

The **Add/Edit Identity NAT Rule** dialog box lets you configure the identity NAT settings.

Fields

- **Real Address**—The original address with its associated interface before network translation is applied.
 - **Interface**—Selects the security appliance network interface on which the original host or network resides.
 - **IP address**—Specifies the IP address of the host or network to which you would like to apply a rule.
 - **Mask**—Select the network mask (netmask) for the address.
 - **Browse**—Lets you select the correct IP address and mask from the Network Objects/Groups tree for a predefined host or network.
- **Enable outside NAT**—Choose this option to enable outside NAT.
- **NAT Options**—Lets you configure the DNS Rewrite, Maximum Connections, Embryonic Limit and Randomize Sequence Number.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

