Configuring Network Object NAT (ASA 8.3 and Later)

All NAT rules that are configured as a parameter of a network object are considered to be *network object NAT* rules. Network object NAT is a quick and easy way to configure NAT for a single IP address, a range of addresses, or a subnet. After you configure the network object, you can then identify the mapped address for that object.

This chapter describes how to configure network object NAT, and it includes the following sections:

Note For detailed information about how NAT works, see Chapter 32, "Information About NAT (ASA 8.3 and Later)."

Information About Network Object NAT

When a packet enters the ASA, both the source and destination IP addresses are checked against the network object NAT rules. The source and destination address in the packet can be translated by separate rules if separate matches are made. These rules are not tied to each other; different combinations of rules can be used depending on the traffic.

Because the rules are never paired, you cannot specify that a source address should be translated to A when going to destination X, but be translated to B when going to destination Y. Use twice NAT for that kind of functionality (twice NAT lets you identify the source and destination address in a single rule).

For detailed information about the differences between twice NAT and network object NAT, see the "How NAT is Implemented" section on page 32-15.

Network object NAT rules are added to section 2 of the NAT rules table. For more information about NAT ordering, see the "NAT Rule Order" section on page 32-20.

Licensing Requirements for Network Object NAT

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Prerequisites for Network Object NAT

Depending on the configuration, you can configure the mapped address inline if desired or you can create a separate network object or network object group for the mapped address. Network object groups are particularly useful for creating a mapped address pool with discontinous IP address ranges or multiple hosts or subnets. To create a network object or group, see the "Configuring Network Objects and Groups" section on page 25-2.

For specific guidelines for objects and groups, see the configuration section for the NAT type you want to configure. See also the "Guidelines and Limitations" section.

Guidelines and Limitations

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

- Supported in routed and transparent firewall mode.
- In transparent mode, you must specify the real and mapped interfaces; you cannot use --Any--.
- In transparent mode, you cannot configure interface PAT, because the transparent mode interfaces do not have IP addresses. You also cannot use the management IP address as a mapped address.
- In transparent mode, translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.

IPv6 Guidelines

- Supports IPv6. See also the "NAT and IPv6" section on page 32-15.
- For routed mode, you can also translate between IPv4 and IPv6.
- For transparent mode, translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.
- For transparent mode, a PAT pool is not supported for IPv6.
- For static NAT, you can specify an IPv6 subnet up to /64. Larger subnets are not supported.

- When using FTP with NAT46, when an IPv4 FTP client connects to an IPv6 FTP server, the client must use either the extended passive mode (EPSV) or extended port mode (EPRT); PASV and PORT commands are not supported with IPv6.

Additional Guidelines

- You can only define a single NAT rule for a given object; if you want to configure multiple NAT rules for an object, you need to create multiple objects with different names that specify the same IP address, for example, **object network obj-10.10.10.1-01**, **object network obj-10.10.10.1-02**, and so on.
- If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT configuration is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections that use translations.

Note If you remove a dynamic NAT or PAT rule, and then add a new rule with mapped addresses that overlap the addresses in the removed rule, then the new rule will not be used until all connections associated with the removed rule time out or are cleared using the **clear xlate** command. This safeguard ensures that the same address is not assigned to multiple hosts.

- Objects and object groups used in NAT cannot be undefined; they must include IP addresses.
- You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
- You can use the same mapped object or group in multiple NAT rules.
- The mapped IP address pool cannot include:
  - The mapped interface IP address. If you specify --Any-- interface for the rule, then all interface IP addresses are disallowed. For interface PAT (routed mode only), use the interface name instead of the IP address.
  - (Transparent mode) The management IP address.
  - (Dynamic NAT) The standby interface IP address when VPN is enabled.
  - Existing VPN pool addresses.
- For application inspection limitations with NAT or PAT, see the "Default Settings" section on page 57-4 in Chapter 57, "Getting Started with Application Layer Protocol Inspection."

Default Settings

- (Routed mode) The default real and mapped interface is Any, which applies the rule to all interfaces.
- (8.3(1), 8.3(2), and 8.4(1)) The default behavior for identity NAT has proxy ARP disabled. You cannot configure this setting. (8.4(2) and later) The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired. See the "Routing NAT Packets" section on page 32-21 for more information.
- If you specify an optional interface, then the ASA uses the NAT configuration to determine the egress interface. (8.3(1) through 8.4(1)) The only exception is for identity NAT, which always uses a route lookup, regardless of the NAT configuration. (8.4(2) and later) For identity NAT, the default behavior is to use the NAT configuration, but you have the option to always use a route lookup instead. See the "Routing NAT Packets" section on page 32-21 for more information.

Configuring Network Object NAT

This section describes how to configure network object NAT and includes the following topics:

Configuring Dynamic NAT or Dynamic PAT Using a PAT Pool

This section describes how to configure network object NAT for dynamic NAT or for dynamic PAT using a PAT pool. For more information, see the "Dynamic NAT" section on page 32-8 or the "Dynamic PAT" section on page 32-10.

Guidelines

For a PAT pool:

- If available, the real source port number is used for the mapped port. However, 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: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. (8.4(3) and later, not including 8.5(1) or 8.6(1)) If you have a lot of traffic that uses the lower port ranges, you can now specify for a PAT pool a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535.
- If you use the same PAT pool object in two separate rules, then be sure to specify the same options for each rule. For example, if one rule specifies extended PAT and a flat range, then the other rule must also specify extended PAT and a flat range.

For extended PAT for a PAT pool:

- Many application inspections do not support extended PAT. See the "Default Settings" section on page 57-4 in Chapter 57, "Getting Started with Application Layer Protocol Inspection," for a complete list of unsupported inspections.
- If you enable extended PAT for a dynamic PAT rule, then you cannot also use an address in the PAT pool as the PAT address in a separate static NAT with port translation rule. For example, if the PAT pool includes 10.1.1.1, then you cannot create a static NAT-with-port-translation rule using 10.1.1.1 as the PAT address.
- If you use a PAT pool and specify an interface for fallback, you cannot specify extended PAT.
- For VoIP deployments that use ICE or TURN, do not use extended PAT. ICE and TURN rely on the PAT binding to be the same for all destinations.

For round robin for a PAT pool:

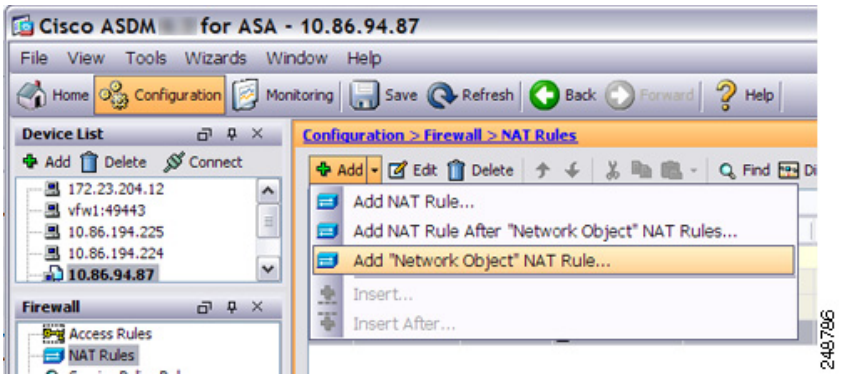
- If a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. **Note**: This "stickiness" does not survive a failover. If the ASA fails over, then subsequent connections from a host may not use the initial IP address.

- Round robin, especially when combined with extended PAT, can consume a large amount of memory. Because NAT pools are created for every mapped protocol/IP address/port range, round robin results in a large number of concurrent NAT pools, which use memory. Extended PAT results in an even larger number of concurrent NAT pools.

Detailed Steps

Step 1 Add NAT to a new or existing network object:

- To add a new network object, choose **Configuration > Firewall > NAT Rules**, then click **Add > Add Network Object NAT Rule**.



- To add NAT to an existing network object, choose **Configuration > Firewall > Objects > Network Objects/Groups**, and then double-click a network object.

For more information, see the "Configuring a Network Object" section on page 25-3.

The Add/Edit Network Object dialog box appears.

Step 2 For a new object, enter values for the following fields:

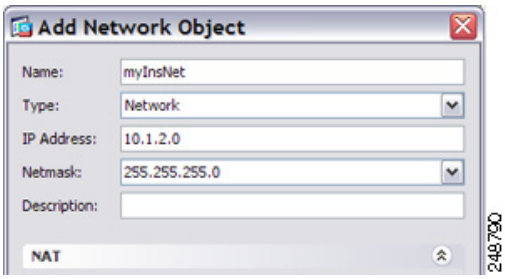
a. Name—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. Type—Host, Network, or Range.

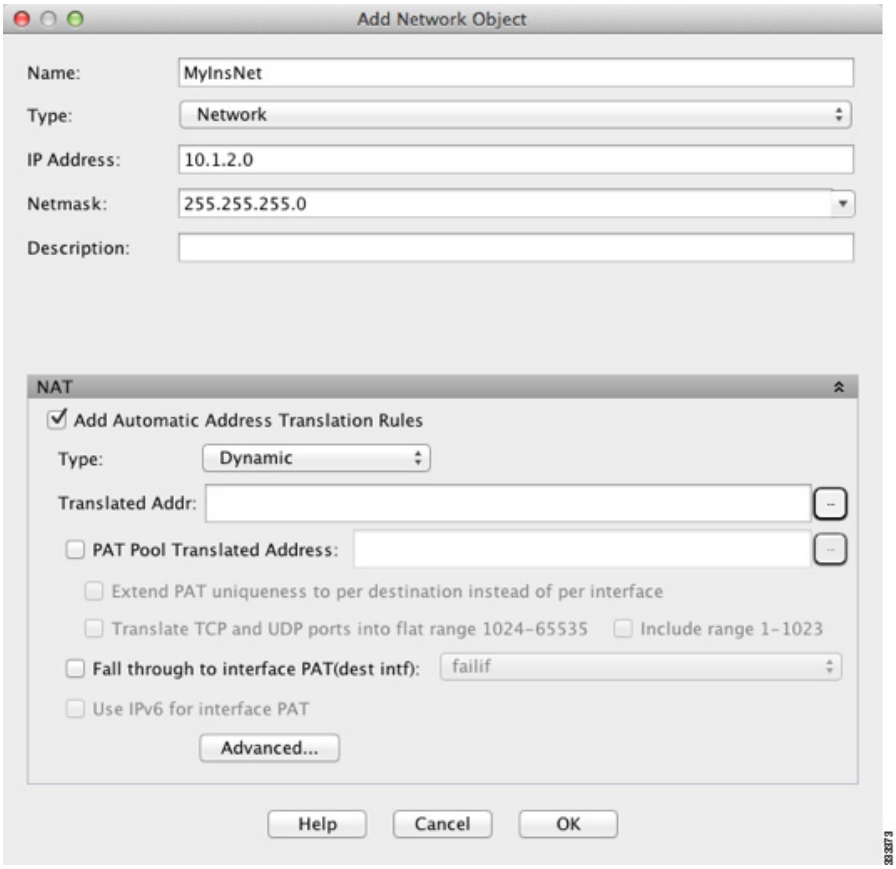
c. IP Address—An IPv4 or IPv6 address. If you select Range as the object type, the IP Address field changes to allow you to enter a Start Address and an End address.

d. Netmask/Prefix Length—Enter the subnet mask or prefix length.

e. Description—(Optional) The description of the network object (up to 200 characters in length).



Step 3 If the NAT section is hidden, click **NAT** to expand the section.

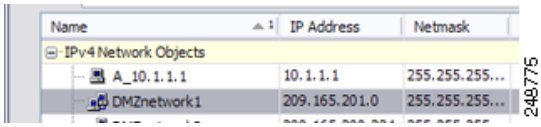


Step 4 Check the **Add Automatic Translation Rules** check box.

Step 5 From the Type drop-down list, choose **Dynamic**. Choose **Dynamic** even if you are configuring dynamic PAT with a PAT pool.

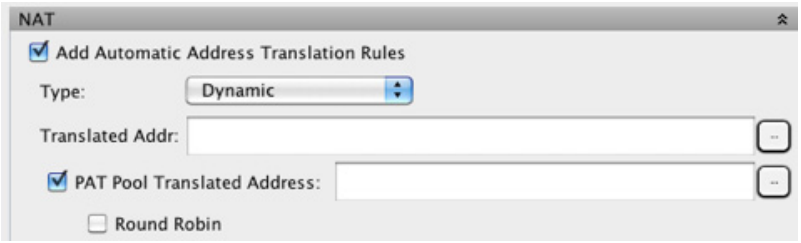
Step 6 Configure either dynamic NAT, or dynamic PAT with a PAT pool:

- Dynamic NAT—To the right of the Translated Addr field, click the browse button and choose an existing network object or create a new object from the Browse Translated Addr dialog box.



Note The object or group cannot contain a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

- Dynamic PAT using a PAT pool—Enable a PAT pool:



a. Do not enter a value for the Translated Addr. field; leave it blank.

b. Check the **PAT Pool Translated Address** check box, then click the browse button and choose an existing network object or create a new network object from the Browse Translated PAT Pool Address dialog box.

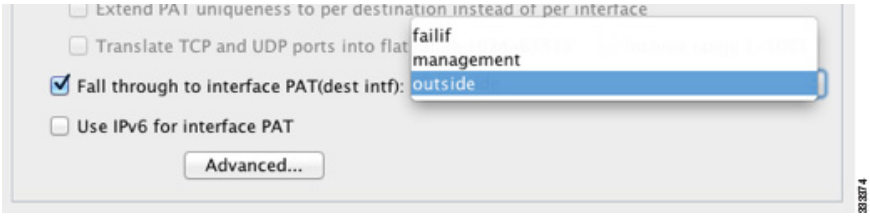
Note The PAT pool object or group cannot contain a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

c. (Optional) Check the **Round Robin** check box to assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.

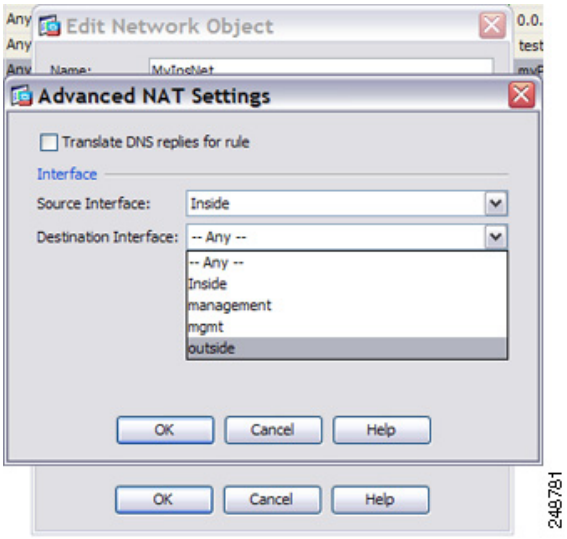
d. (Optional, 8.4(3) and later, not including 8.5(1) or 8.6(1)) Check the **Extend PAT uniqueness to per destination instead of per interface** check box to use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the 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.

e. (Optional, 8.4(3) and later, not including 8.5(1) or 8.6(1)) Check the **Translate TCP or UDP ports into flat range (1024-65535)** check box to use the 1024 to 65535 port range as a single flat 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 check the **Include range 1 to 1023** check box.

Step 7 (Optional, Routed Mode Only) To use the interface IP address as a backup method when the other mapped addresses are already allocated, check the **Fall through to interface PAT (dest intf)** check box, and choose the interface from the drop-down list. To use the IPv6 address of the interface, also check the **Use IPv6 for interface PAT** checkbox.



Step 8 (Optional) Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.



- Translate DNS replies for rule—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See the "DNS and NAT" section on page 32-30 for more information.
- (Required for Transparent Firewall Mode) Source Interface—Specifies the real interface where this NAT rule applies. By default, the rule applies to all interfaces.
- (Required for Transparent Firewall Mode) Destination Interface—Specifies the mapped interface where this NAT rule applies. By default, the rule applies to all interfaces.

When you are finished, click **OK**. You return to the Add/Edit Network Object dialog box.

Step 9 Click **OK**, and then **Apply**.

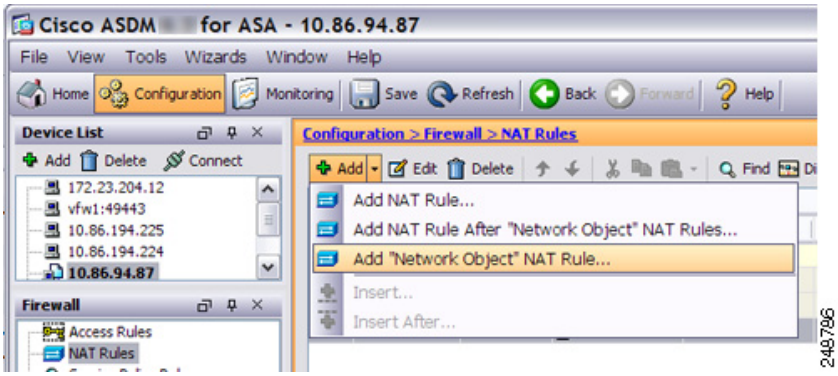
Configuring Dynamic PAT (Hide)

This section describes how to configure network object NAT for dynamic PAT (hide). For dynamic PAT using a PAT pool, see the "Configuring Dynamic NAT or Dynamic PAT Using a PAT Pool" section on page 33-4 instead of using this section. For more information, see the "Dynamic PAT" section on page 32-10.

Detailed Steps

Step 1 Add NAT to a new or existing network object:

- To add a new network object, choose **Configuration > Firewall > NAT Rules**, then click **Add > Add Network Object NAT Rule**.



- To add NAT to an existing network object, choose **Configuration > Firewall > Objects > Network Objects/Groups**, and then double-click a network object.

For more information, see the "Configuring a Network Object" section on page 25-3.

The Add/Edit Network Object dialog box appears.

Step 2 For a new object, enter values for the following fields:

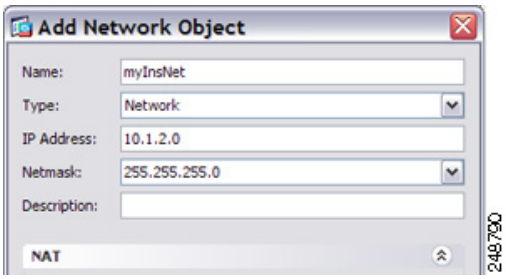
a. Name—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. Type—Host, Network, or Range.

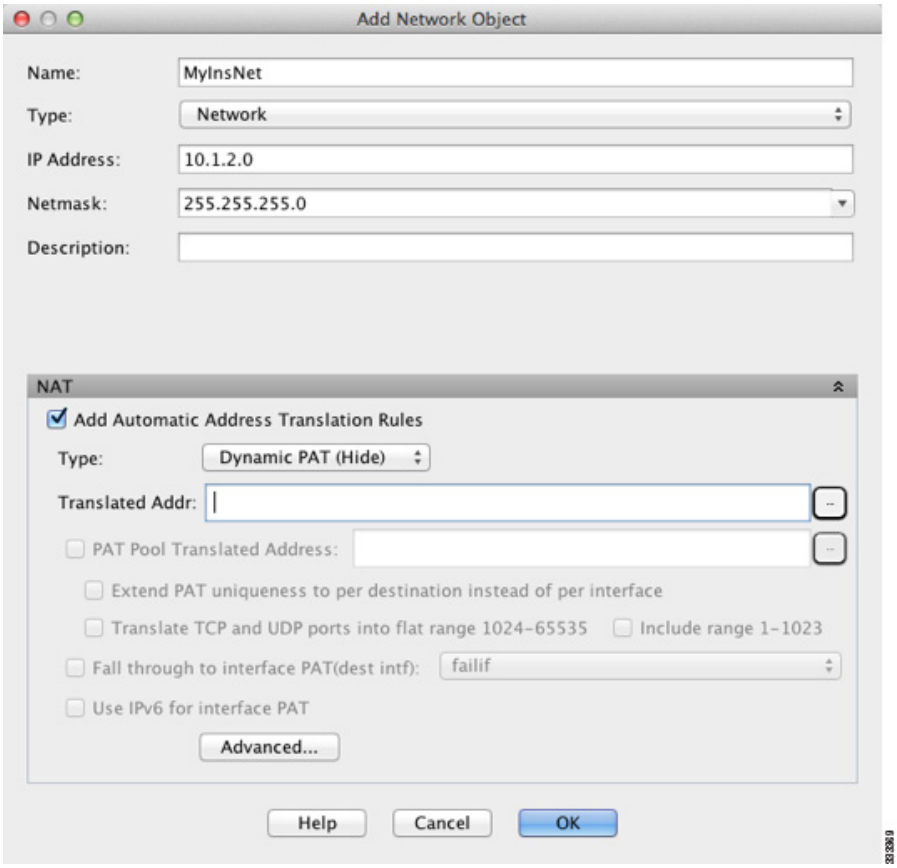
c. IP Address—An IPv4 or IPv6 address. If you select Range as the object type, the IP Address field changes to allow you to enter a Start Address and an End address.

d. Netmask/Prefix Length—Enter the subnet mask or prefix length.

e. Description—(Optional) The description of the network object (up to 200 characters in length).



Step 3 If the NAT section is hidden, click **NAT** to expand the section.



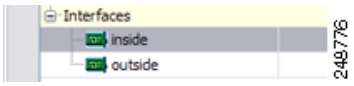
Step 4 Check the **Add Automatic Translation Rules** check box.

Step 5 From the Type drop-down list, choose **Dynamic PAT (Hide)**.

Note To configure dynamic PAT using a PAT pool instead of a single address, see the "Configuring Dynamic NAT or Dynamic PAT Using a PAT Pool" section on page 33-4.

Step 6 Specify a single mapped address. In the Translated Addr. field, specify the mapped IP address by doing one of the following:

- Type a host IP address.
- Type an interface name or click the browse button, and choose an interface from the Browse Translated Addr dialog box.

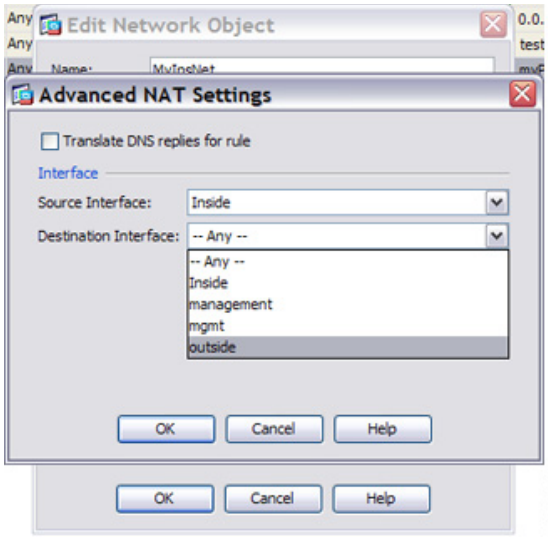


If you specify an interface name, then you enable *interface PAT*, where the specified interface IP address is used as the mapped address. To use the IPv6 interface address, you must also check the **Use IPv6 for interface PAT** checkbox. With interface PAT, the NAT rule only applies to the specified mapped interface. (If you do not use interface PAT, then the rule applies to all interfaces by default.) See Step 7 to optionally also configure the real interface to be a specific interface instead of --Any--.

Note You cannot specify an interface in transparent mode.

- Click the browse button, and choose an existing host address from the Browse Translated Addr dialog box.
- Click the browse button, and create a new named object from the Browse Translated Addr dialog box.

Step 7 (Optional) Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.



- Translate DNS replies for rule—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See the "DNS and NAT" section on page 32-30 for more information.
- (Required for Transparent Firewall Mode) Source Interface—Specifies the real interface where this NAT rule applies. By default, the rule applies to all interfaces.
- (Required for Transparent Firewall Mode) Destination Interface—Specifies the mapped interface where this NAT rule applies. By default, the rule applies to all interfaces.

When you are finished, click **OK**. You return to the Add/Edit Network Object dialog box.

Step 8 Click **OK**, and then **Apply**.

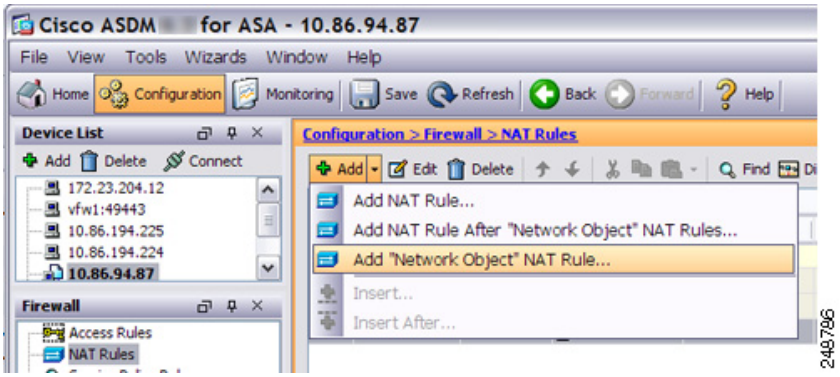
Configuring Static NAT or Static NAT-with-Port-Translation

This section describes how to configure a static NAT rule using network object NAT. For more information, see the "Static NAT" section on page 32-3.

Detailed Steps

Step 1 Add NAT to a new or existing network object:

- To add a new network object, choose **Configuration > Firewall > NAT Rules**, then click **Add > Add Network Object NAT Rule**.



- To add NAT to an existing network object, choose **Configuration > Firewall > Objects > Network Objects/Groups**, and then double-click a network object.

For more information, see the "Configuring a Network Object" section on page 25-3.

The Add/Edit Network Object dialog box appears.

Step 2 For a new object, enter values for the following fields:

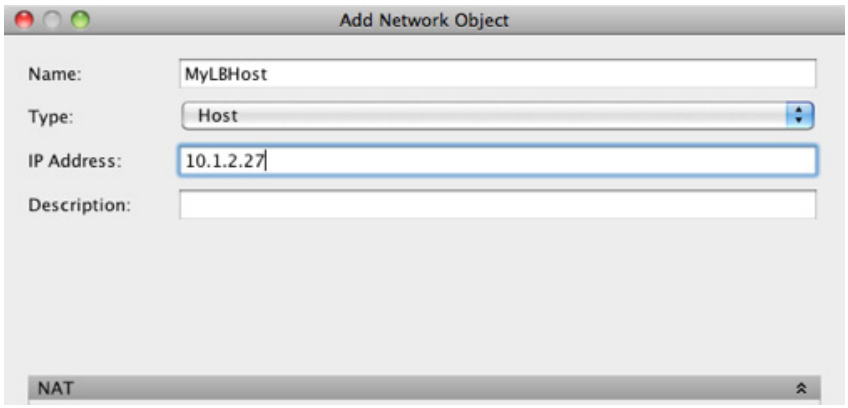
a. Name—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. Type—Network, Host, or Range.

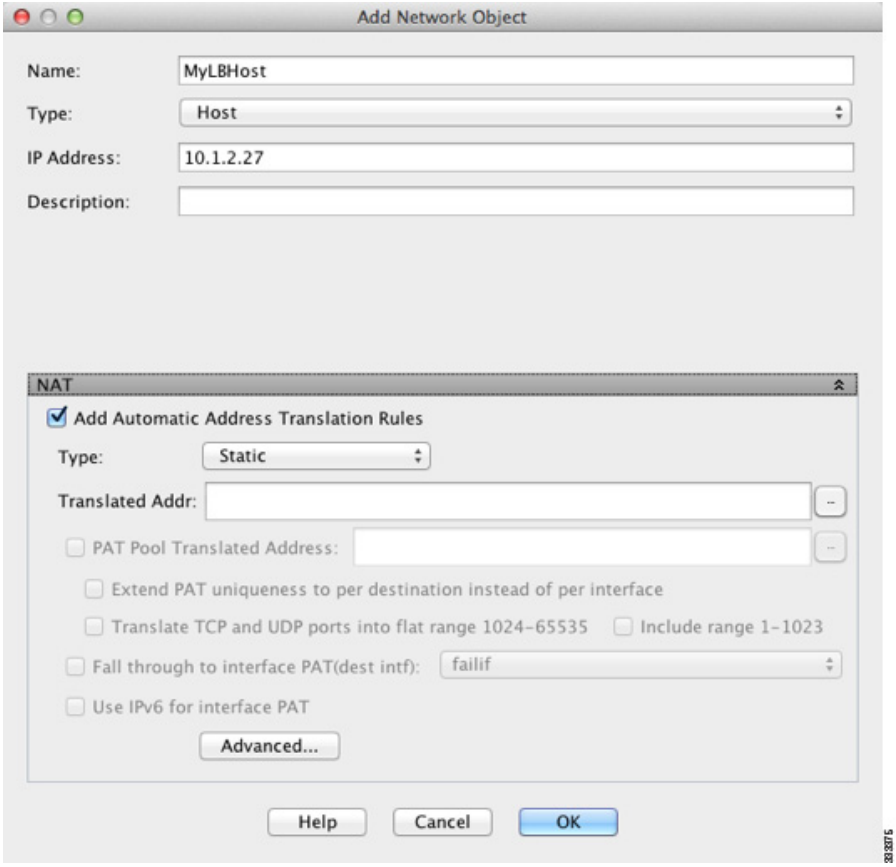
c. IP Address—An IPv4 or IPv6 address. If you select Range as the object type, the IP Address field changes to allow you to enter a Start Address and an End address.

d. Netmask/Prefix Length—Enter the subnet mask or prefix length.

e. Description—(Optional) The description of the network object (up to 200 characters in length).



Step 3 If the NAT section is hidden, click **NAT** to expand the section.



Step 4 Check the **Add Automatic Translation Rules** check box.

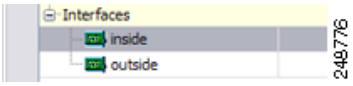
Step 5 From the Type drop-down list, choose **Static**.

Step 6 In the Translated Addr. field, do one of the following:

- Type an IP address.

  When you type an IP address, the netmask or range for the mapped network is the same as that of the real network. For example, if the real network is a host, then this address will be a host address. In the case of a range, then the mapped addresses include the same number of addresses as the real range. For example, if the real address is defined as a range from 10.1.1.1 through 10.1.1.6, and you specify 172.20.1.1 as the mapped address, then the mapped range will include 172.20.1.1 through 172.20.1.6.

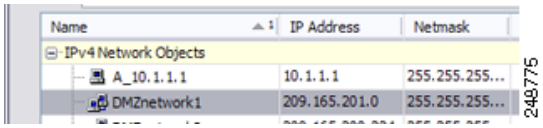
- (For static NAT-with-port-translation only) Type an interface name or click the browse button, and choose an interface from the Browse Translated Addr dialog box.



  To use the IPv6 interface address, you must also check the **Use IPv6 for interface PAT** checkbox. Be sure to also configure a service on the Advanced NAT Settings dialog box (see Step 8). (You cannot specify an interface in transparent mode).

- Click the browse button, and choose an existing address from the Browse Translated Addr dialog box.

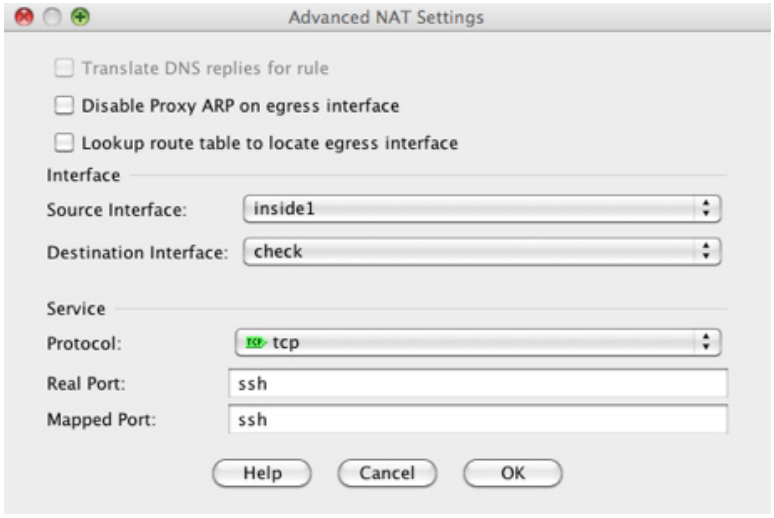
- Click the browse button, and create a new address from the Browse Translated Addr dialog box.



Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses. For more information, see the "Static NAT" section on page 32-3.

Step 7 (Optional) For NAT46, check **Use one-to-one address translation**. For NAT 46, specify one-to-one to translate 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. For a one-to-one translation, you must use this keyword.

Step 8 (Optional) Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.

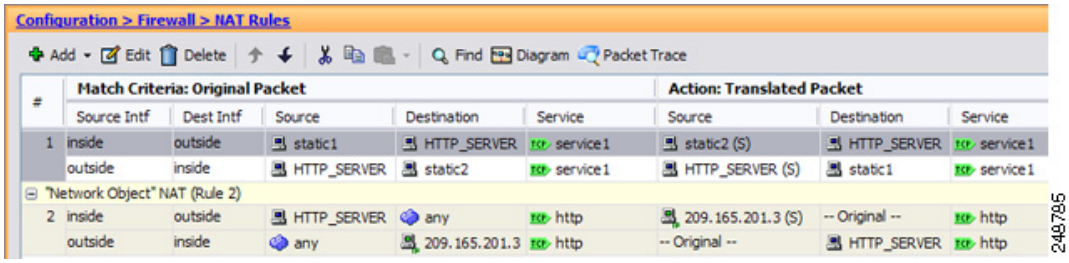


- Translate DNS replies for rule—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See the "DNS and NAT" section on page 32-30 for more information.
- Disable Proxy ARP on egress interface—Disables proxy ARP for incoming packets to the mapped IP addresses. See the "Mapped Addresses and Routing" section on page 32-22 for more information.
- (Required for Transparent Firewall Mode) Interface:
  - Source Interface—Specifies the real interface where this NAT rule applies. By default, the rule applies to all interfaces.
  - Destination Interface—Specifies the mapped interface where this NAT rule applies. By default, the rule applies to all interfaces.
- Service:
  - Protocol—Configures static NAT-with-port-translation. Choose **tcp** or **udp**.
  - Real Port—You can type either a port number or a well-known port name (such as "ftp").
  - Mapped Port—You can type either a port number or a well-known port name (such as "ftp").

When you are finished, click **OK**. You return to the Add/Edit Network Object dialog box.

Step 9 Click **OK**, and then **Apply**.

Because static rules are bidirectional (allowing initiation to and from the real host), the NAT Rules table show two rows for each static rule, one for each direction.



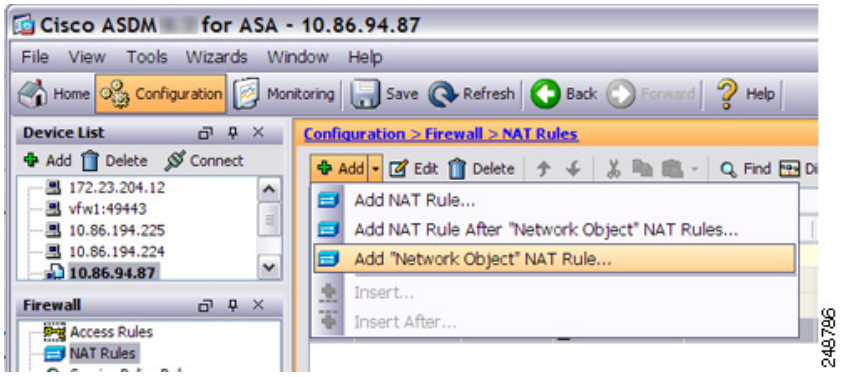
Configuring Identity NAT

This section describes how to configure an identity NAT rule using network object NAT. For more information, see the "Identity NAT" section on page 32-12.

Detailed Steps

Step 1 Add NAT to a new or existing network object:

- To add a new network object, choose **Configuration > Firewall > NAT Rules**, then click **Add > Add Network Object NAT Rule**.



- To add NAT to an existing network object, choose **Configuration > Firewall > Objects > Network Objects/Groups**, and then double-click a network object.

For more information, see the "Configuring a Network Object" section on page 25-3.

The Add/Edit Network Object dialog box appears.

Step 2 For a new object, enter values for the following fields:

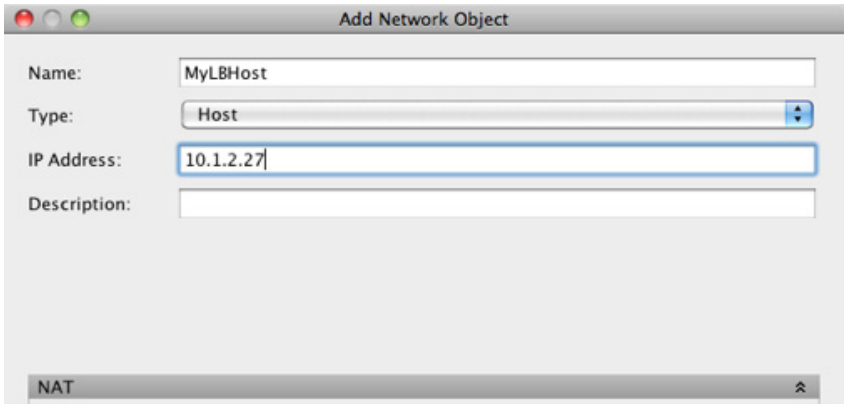
a. Name—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. Type—Network, Host, or Range.

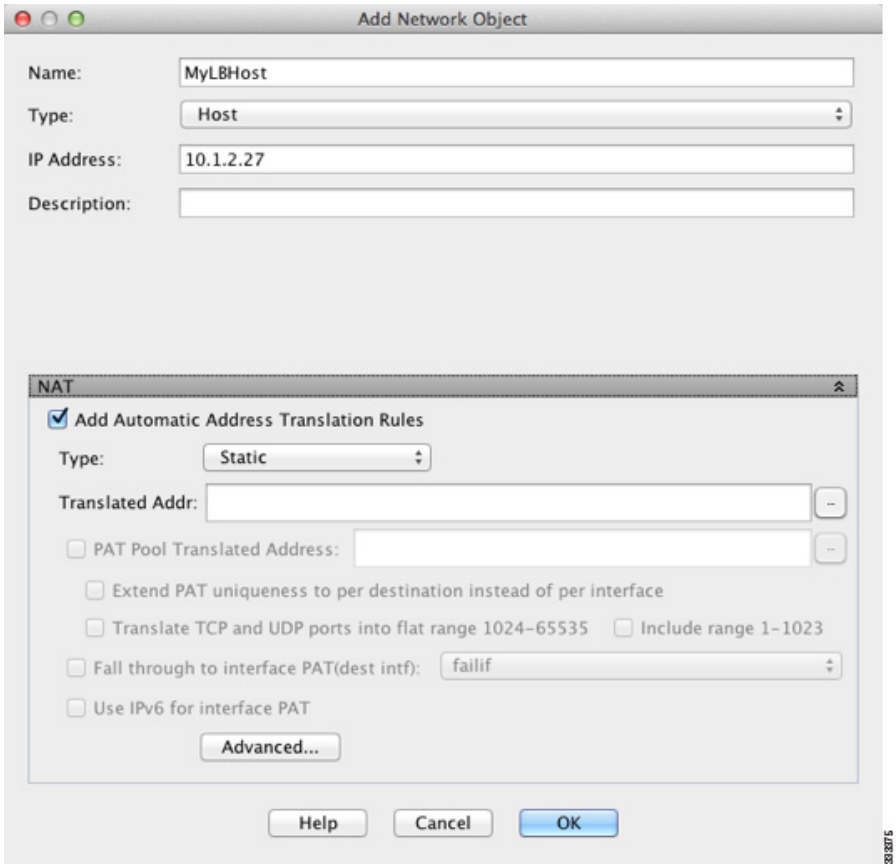
c. IP Address—An IPv4 or IPv6 address. If you select Range as the object type, the IP Address field changes to allow you to enter a Start Address and an End address.

d. Netmask/Prefix Length—Enter the subnet mask or prefix length.

e. Description—(Optional) The description of the network object (up to 200 characters in length).



Step 3 If the NAT section is hidden, click **NAT** to expand the section.

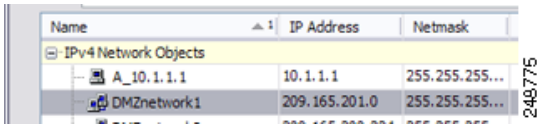


Step 4 Check the **Add Automatic Translation Rules** check box.

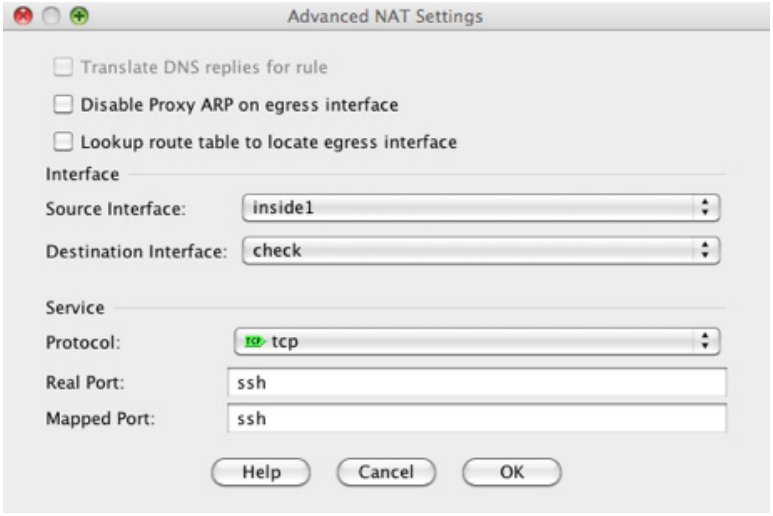
Step 5 From the Type drop-down list, choose **Static**.

Step 6 In the Translated Addr. field, do one of the following:

- Type the same IP address that you used for the real address.
- Click the browse button, and choose a network object with a matching IP address definition from the Browse Translated Addr dialog box.
- Click the browse button, and create a new network object with a matching IP address definition from the Browse Translated Addr dialog box.



Step 7 (Optional) Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.

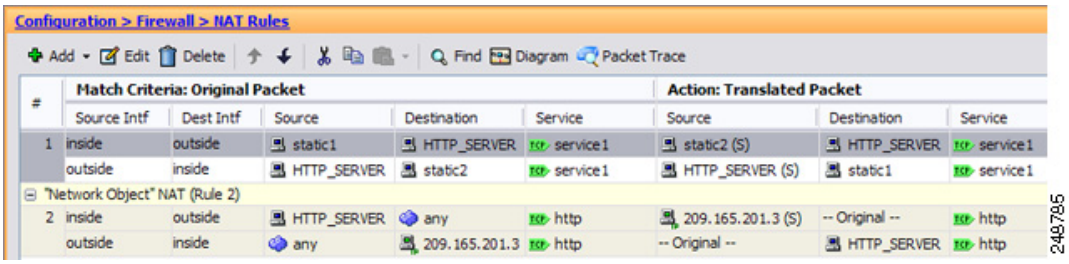


- Disable Proxy ARP on egress interface—Disables proxy ARP for incoming packets to the mapped IP addresses. See the "Mapped Addresses and Routing" section on page 32-22 for more information.
- (Routed mode; interface(s) specified) Lookup route table to locate egress interface—Determines the egress interface using a route lookup instead of using the interface specified in the NAT command. See the "Determining the Egress Interface" section on page 32-24 for more information.
- (Required for Transparent Firewall Mode) Interface:
  - Source Interface—Specifies the real interface where this NAT rule applies. By default, the rule applies to all interfaces.
  - Destination Interface—Specifies the mapped interface where this NAT rule applies. By default, the rule applies to all interfaces.

Do not configure any other options on this dialog box. When you are finished, click **OK**. You return to the Add/Edit Network Object dialog box.

Step 8 Click **OK**, and then **Apply**.

Because static rules are bidirectional (allowing initiation to and from the real host), the NAT Rules table show two rows for each static rule, one for each direction.



Configuring Per-Session PAT Rules

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 the "Per-Session PAT vs. Multi-Session PAT (Version 9.0(1) and Later)" section on page 32-11.

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.

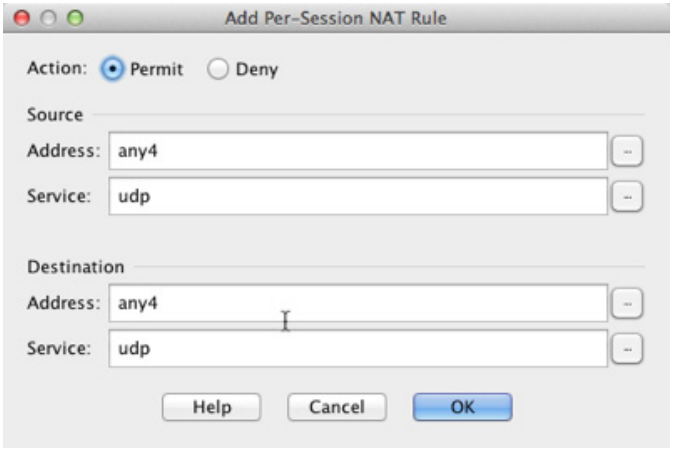
Note You cannot remove these rules, and they always exist after any manually-created rules. Because rules are evaluated in order, you can override the default rules. For example, to completely negate these rules, you could add the following:

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

Detailed Steps

Step 1 Choose **Configuration > Firewall > Advanced > Per-Session NAT Rules**, and click **Add > Add Per-Session NAT Rule**.

Step 2 Click **Permit** or **Deny**.



A permit rule uses per-session PAT; a deny rule uses multi-session PAT.

Step 3 Specify the Source Address either by typing an address or clicking the **...** button to choose an object.

Step 4 Specify the Source Service, UDP or TCP. You can optionally specify a source port, although normally you only specify the destination port. Either type in UDP/*port* or TCP/*port*, or click the **...** button to select a common value or object.

Step 5 Specify the Destination Address either by typing an address or clicking the **...** button to choose an object.

Step 6 Specify the Destination Service, UDP or TCP; this must match the source service. You can optionally specify a destination port. Either type in UDP/*port* or TCP/*port*, or click the **...** button to select a common value or object.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Monitoring Network Object NAT

The Monitoring > Properties > Connection Graphs > Xlates pane lets you view the active Network Address Translations in a graphical format. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
  - Xlate Utilization—Displays the ASA NAT utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected entry from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

The Monitoring > Properties > Connection Graphs > Perfmon pane lets you view the performance information in a graphical format. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
  - AAA Perfmon—Displays the ASA AAA performance information.
  - Inspection Perfmon—Displays the ASA inspection performance information.
  - Web Perfmon—Displays the ASA web performance information, including URL access and URL server requests.
  - Connections Perfmon—Displays the ASA connections performance information.
  - Xlate Perfmon—Displays the ASA NAT performance information.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

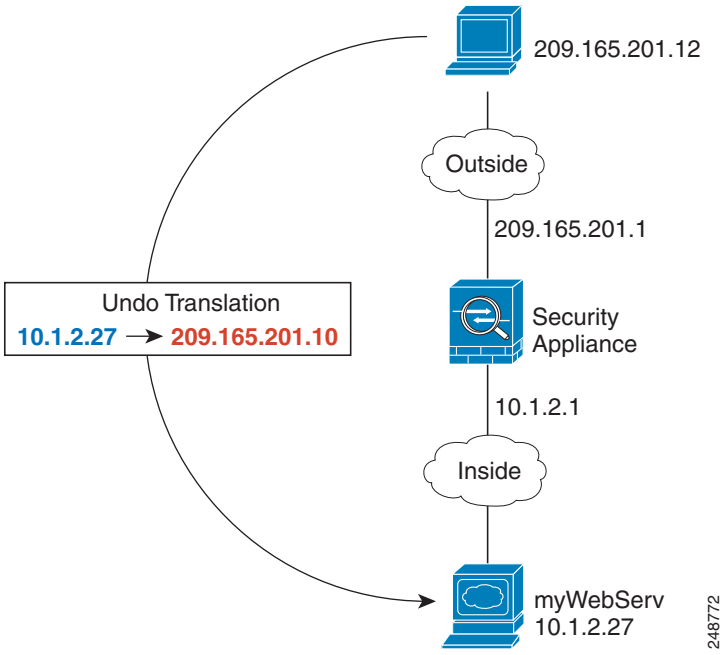
Configuration Examples for Network Object NAT

This section includes the following configuration examples:

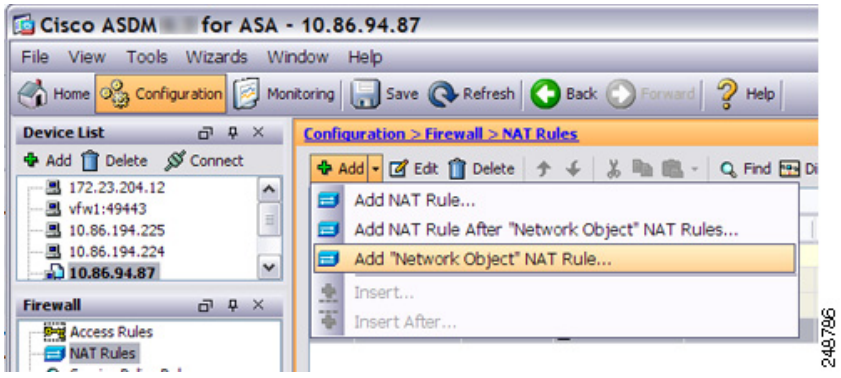
Providing Access to an Inside Web Server (Static NAT)

The following example performs static NAT for an inside web server. The real address is on a private network, so a public address is required. Static NAT is necessary so hosts can initiate traffic to the web server at a fixed address. (See Figure 33-1).

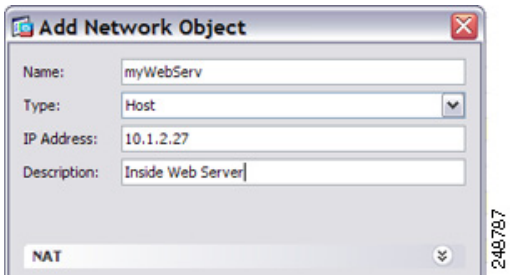
Figure 33-1 Static NAT for an Inside Web Server



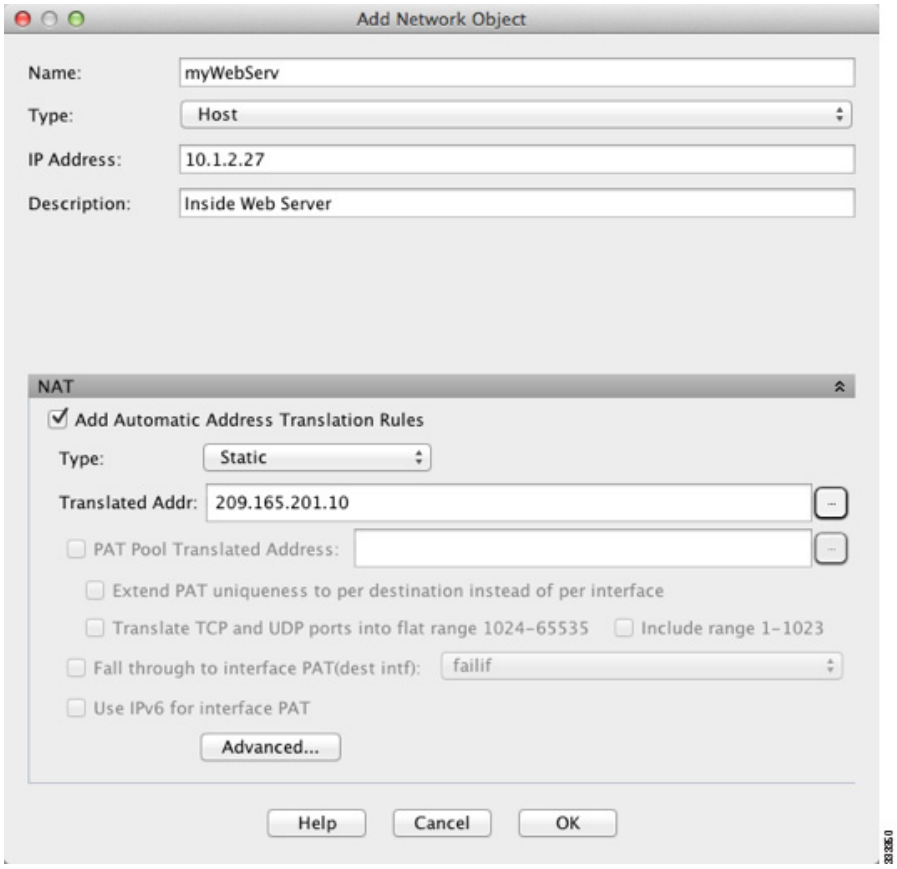
Step 1 Create a network object for the internal web server:



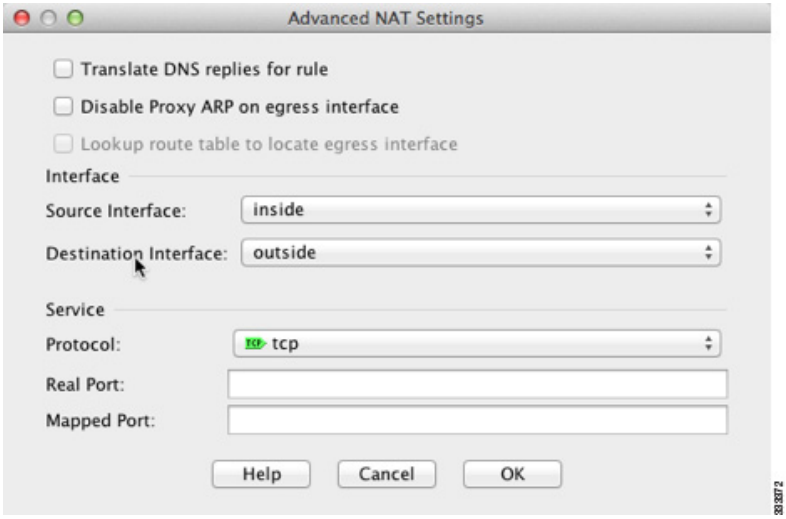
Step 2 Define the web server address:



Step 3 Configure static NAT for the object:



Step 4 Configure the real and mapped interfaces by clicking **Advanced**:

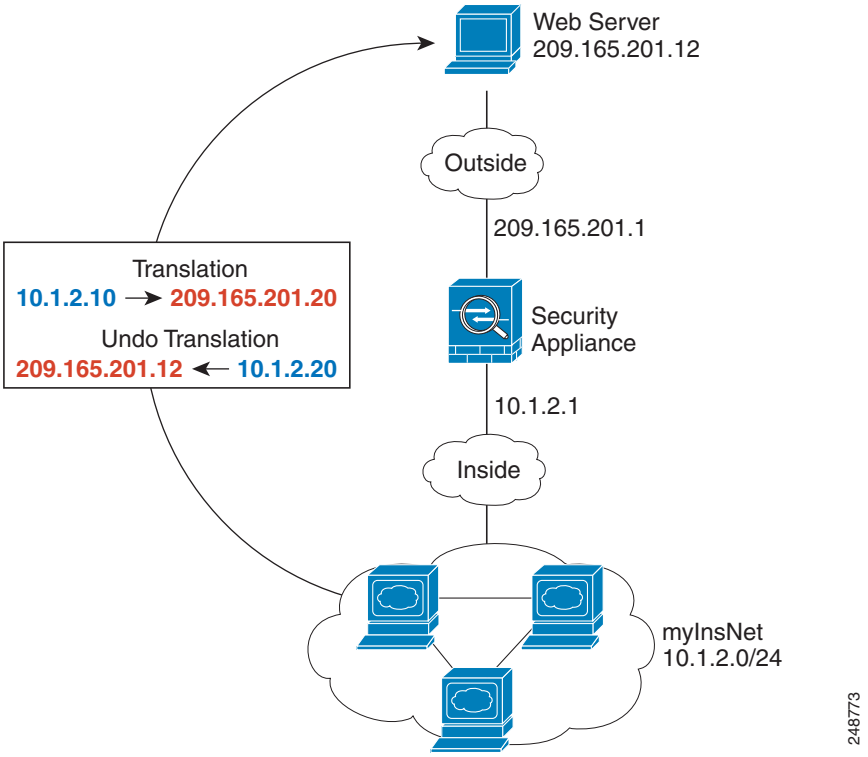


Step 5 Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

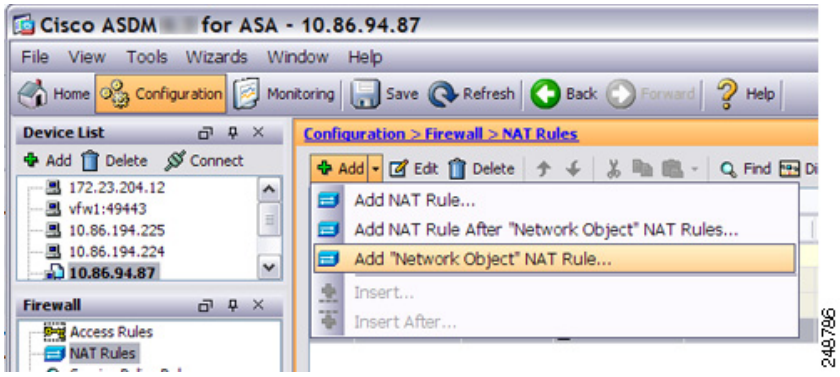
NAT for Inside Hosts (Dynamic NAT) and NAT for an Outside Web Server (Static NAT)

The following example configures dynamic NAT for inside users on a private network when they access the outside. Also, when inside users connect to an outside web server, that web server address is translated to an address that appears to be on the inside network. (See Figure 33-2).

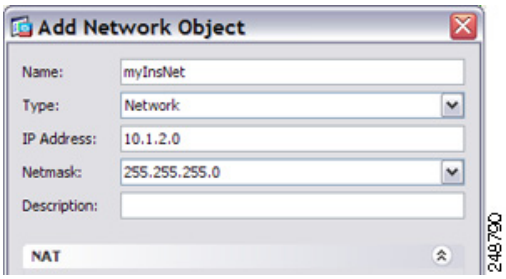
Figure 33-2 Dynamic NAT for Inside, Static NAT for Outside Web Server



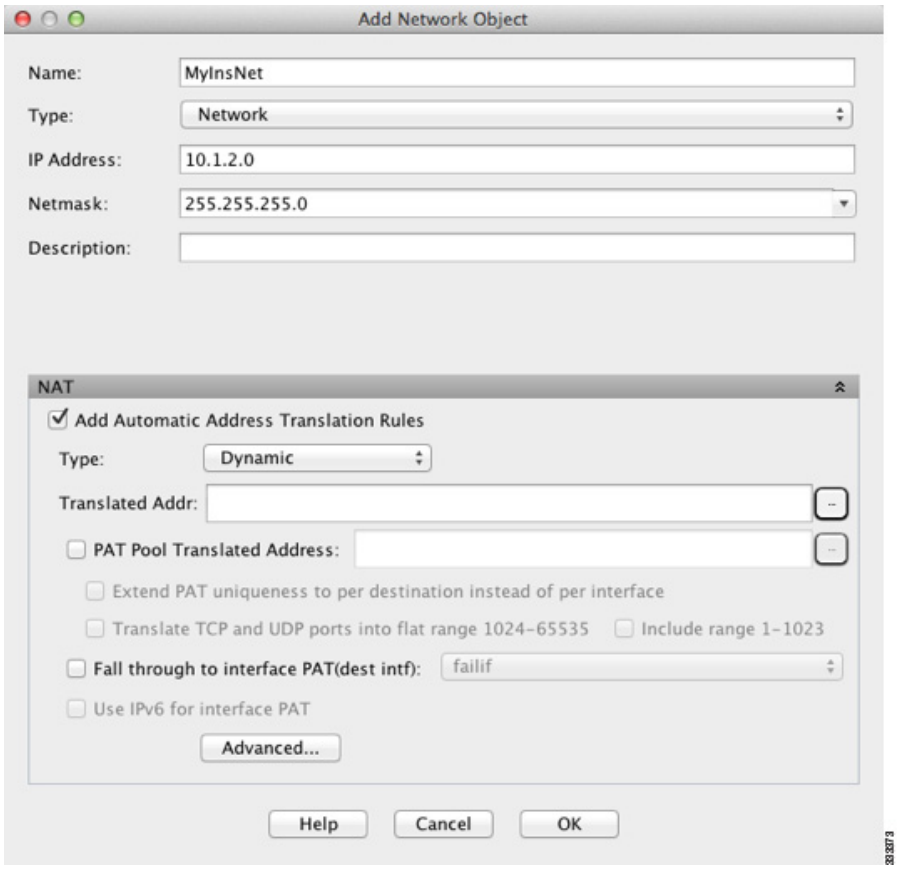
Step 1 Create a network object for the inside network:



Step 2 Define the addresses for the inside network:

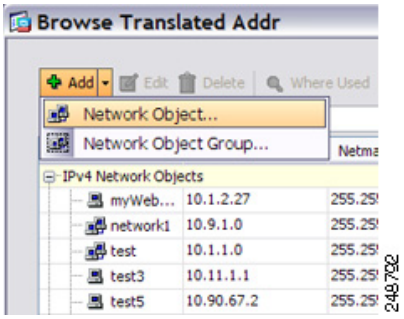


Step 3 Enable dynamic NAT for the inside network:

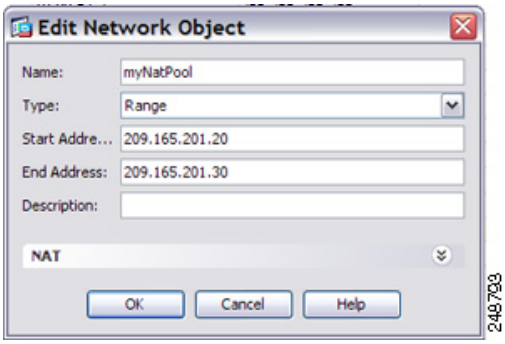


Step 4 For the Translated Addr field, add a new network object for the dynamic NAT pool to which you want to translate the inside addresses by clicking the browse button.

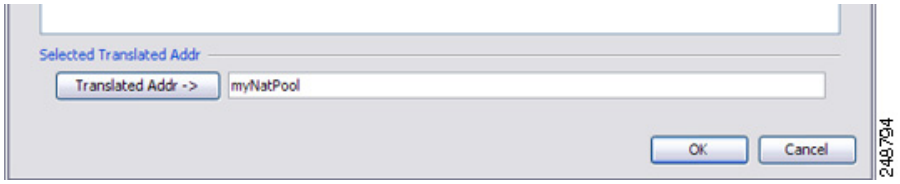
a. Add the new network object.



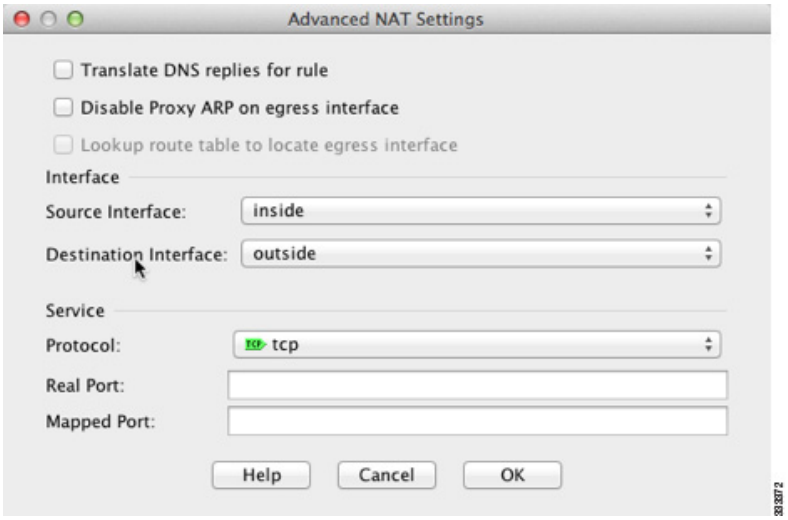
b. Define the NAT pool addresses, and click **OK**.



c. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.

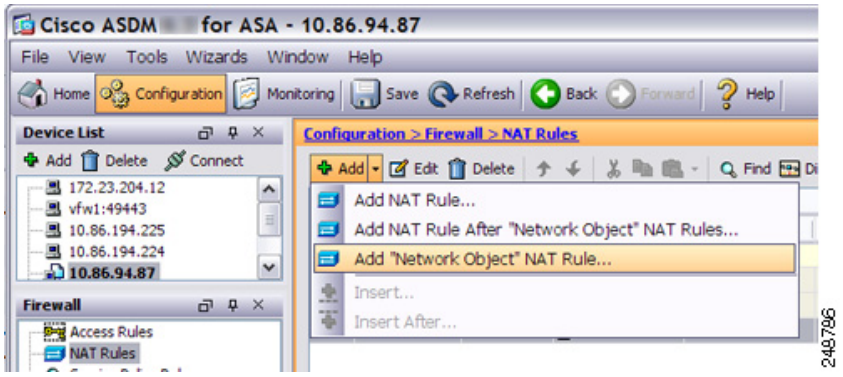


Step 5 Configure the real and mapped interfaces by clicking **Advanced**:

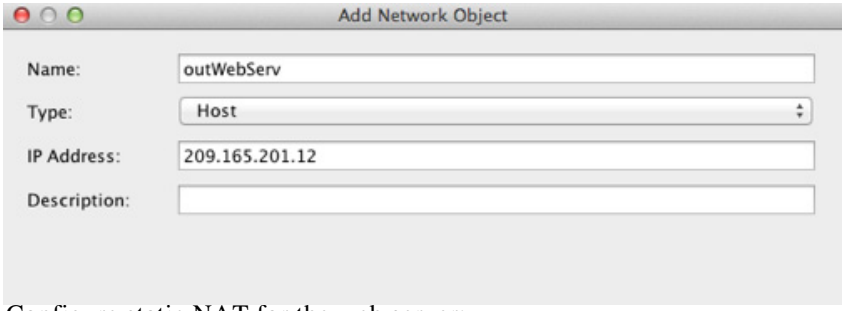


Step 6 Click **OK** to return to the Edit Network Object dialog box, click then click **OK** again to return to the NAT Rules table.

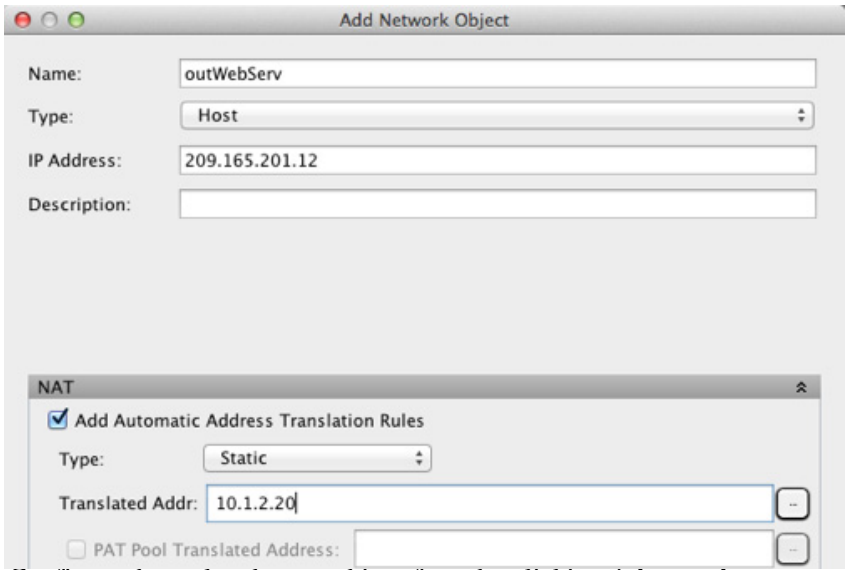
Step 7 Create a network object for the outside web server:



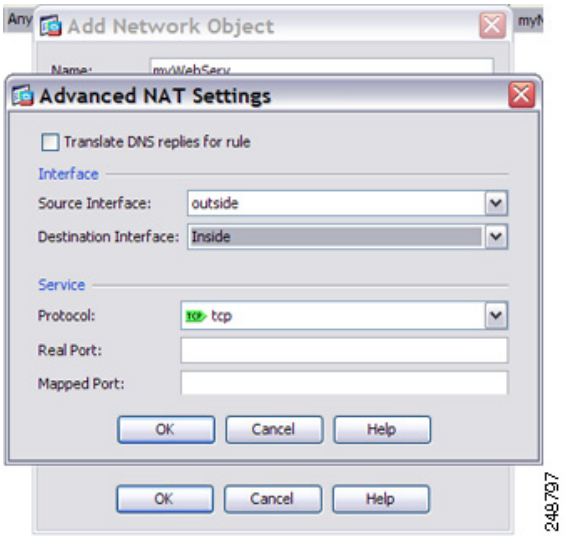
Step 8 Define the web server address:



Step 9 Configure static NAT for the web server:



Step 10 Configure the real and mapped interfaces by clicking **Advanced**:

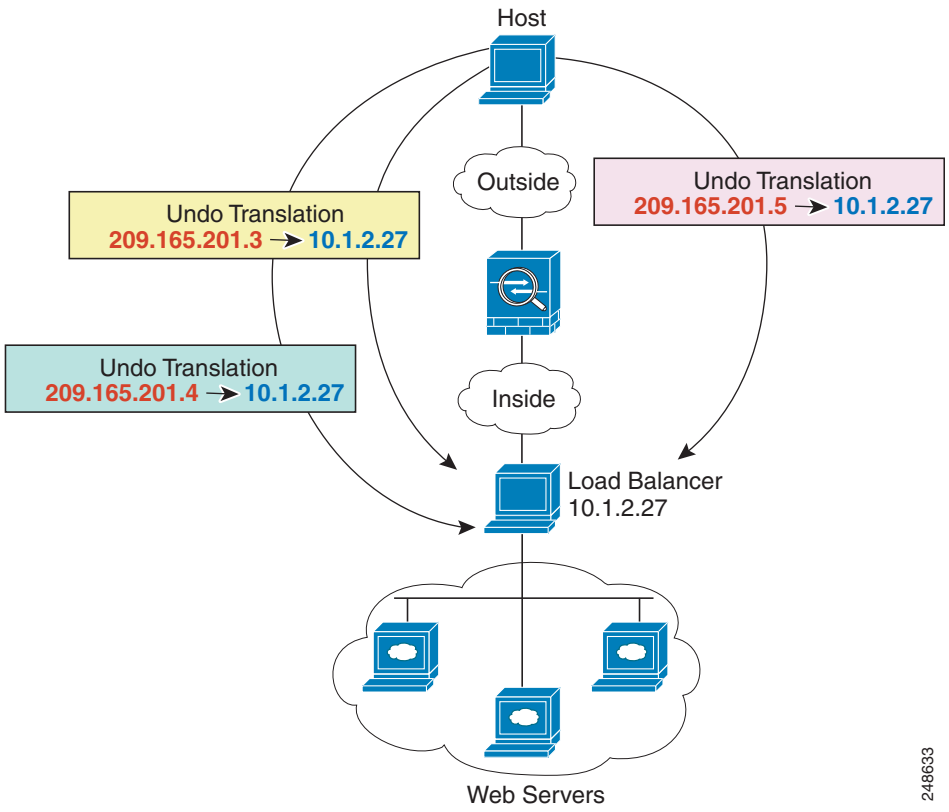


Step 11 Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

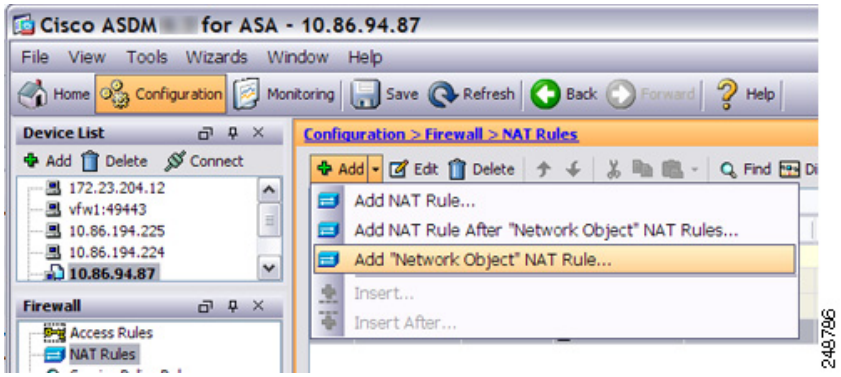
Inside Load Balancer with Multiple Mapped Addresses (Static NAT, One-to-Many)

The following example shows an inside load balancer that is translated to multiple IP addresses. When an outside host accesses one of the mapped IP addresses, it is untranslated to the single load balancer address. Depending on the URL requested, it redirects traffic to the correct web server. (See Figure 33-3).

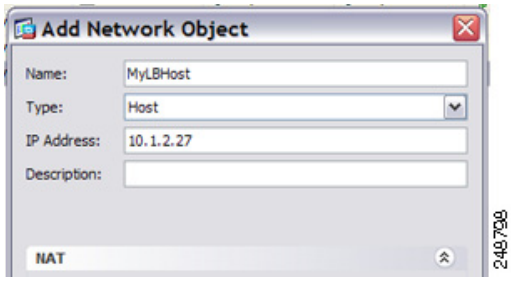
Figure 33-3 Static NAT with One-to-Many for an Inside Load Balancer



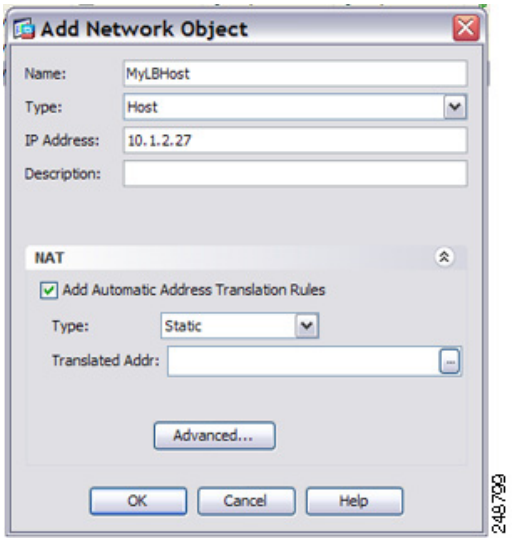
Step 1 Create a network object for the load balancer:



Step 2 Define the load balancer address:

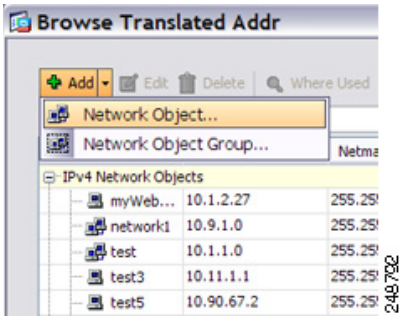


Step 3 Configure static NAT for the load balancer:

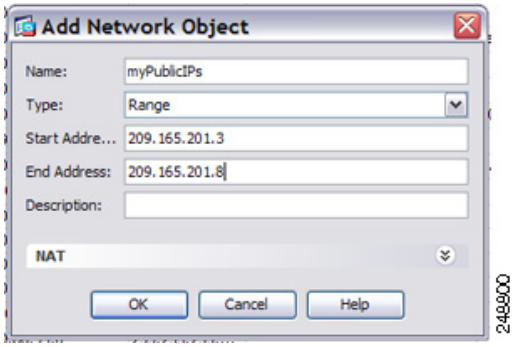


Step 4 For the Translated Addr field, add a new network object for the static NAT group of addresses to which you want to translate the load balancer address by clicking the browse button.

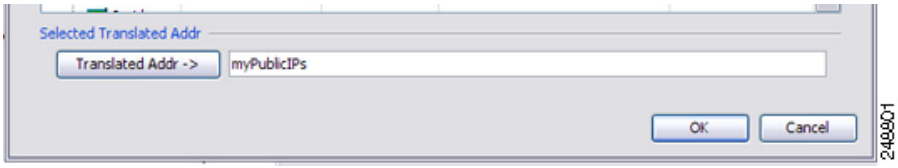
a. Add the new network object.



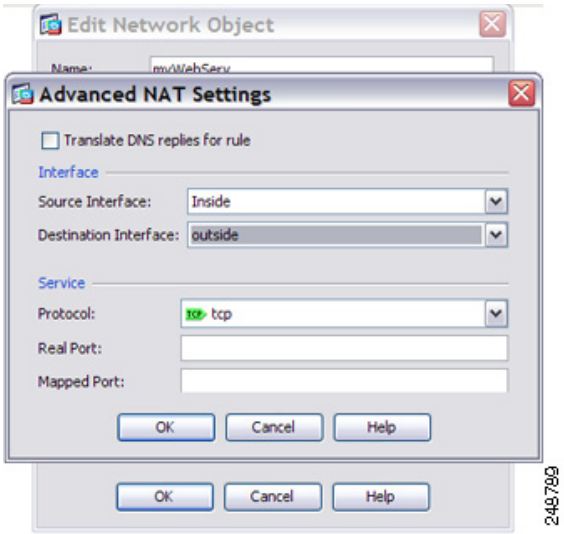
b. Define the static NAT group of addresses, and click **OK**.



c. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.



Step 5 Configure the real and mapped interfaces by clicking **Advanced**:

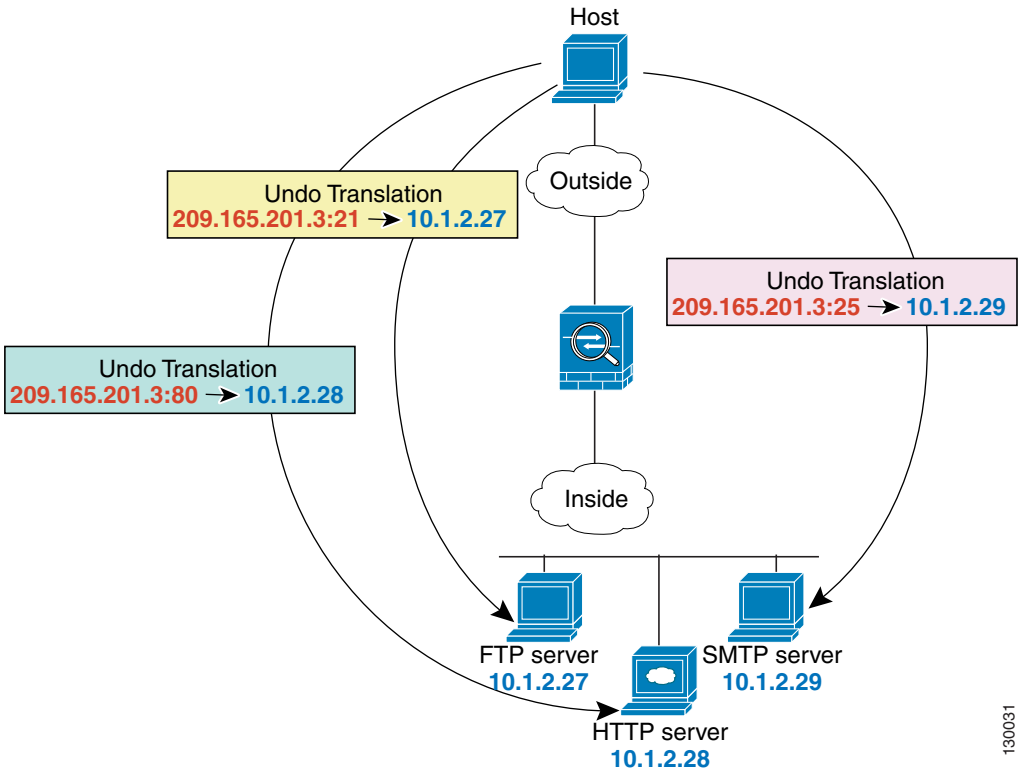


Step 6 Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

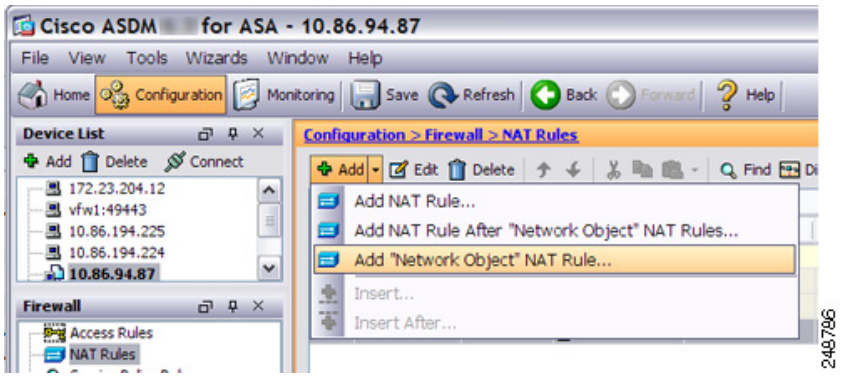
Single Address for FTP, HTTP, and SMTP (Static NAT-with-Port-Translation)

The following static NAT-with-port-translation example provides a single address for remote users to access FTP, HTTP, and SMTP. These servers are actually different devices on the real network, but for each server, you can specify static NAT-with-port-translation rules that use the same mapped IP address, but different ports. (See Figure 33-4.)

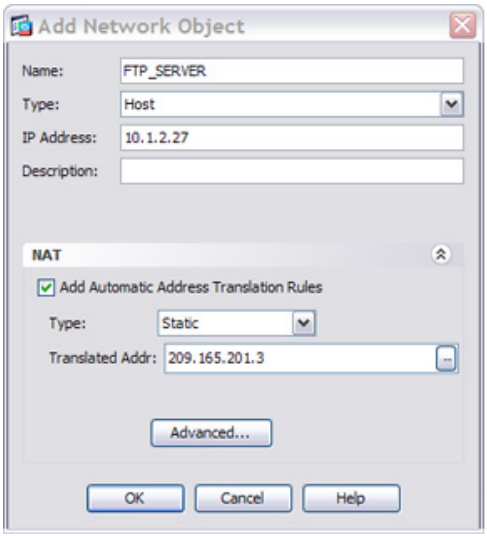
Figure 33-4 Static NAT-with-Port-Translation



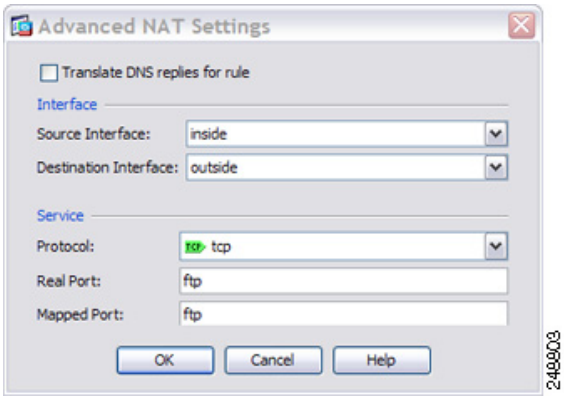
Step 1 Create a network object for the FTP server address:



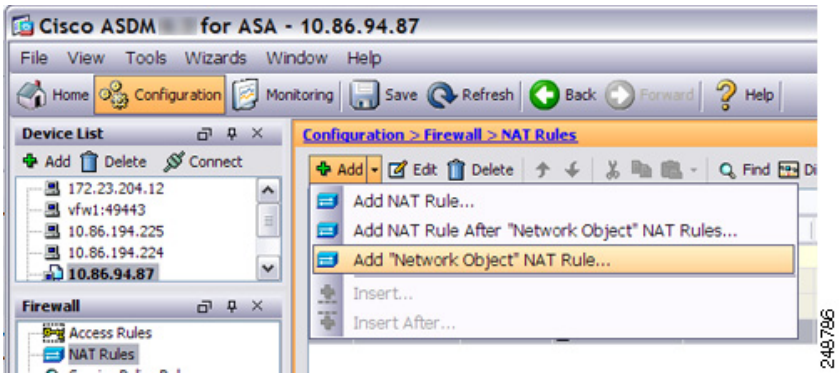
Step 2 Define the FTP server address, and configure static NAT with identity port translation for the FTP server:



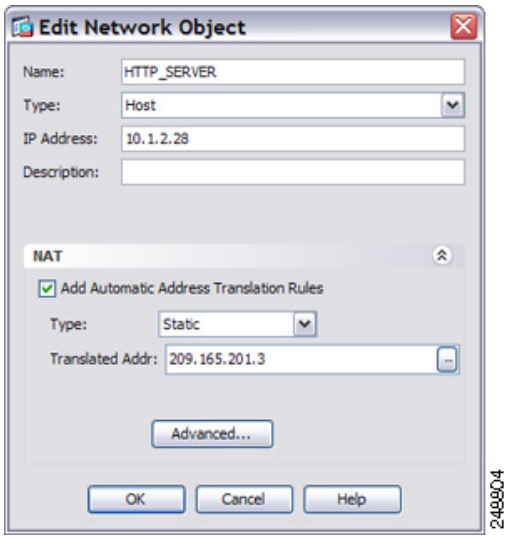
Step 3 Click **Advanced** to configure the real and mapped interfaces and port translation for FTP.



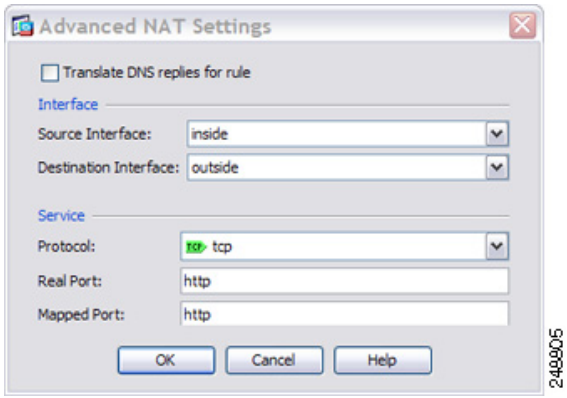
Step 4 Create a network object for the HTTP server address:



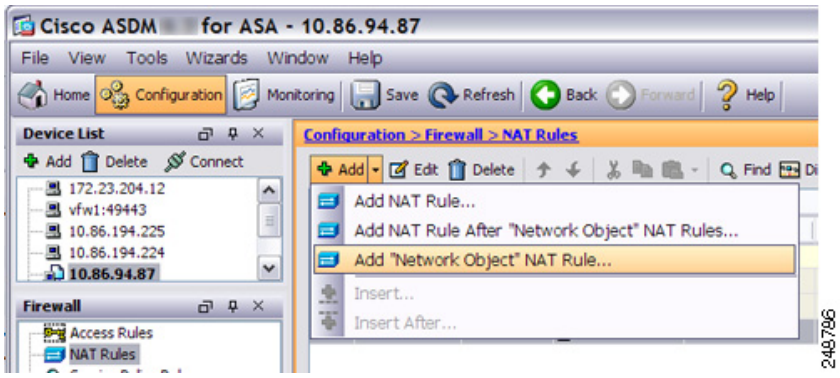
Step 5 Define the HTTP server address, and configure static NAT with identity port translation for the HTTP server:



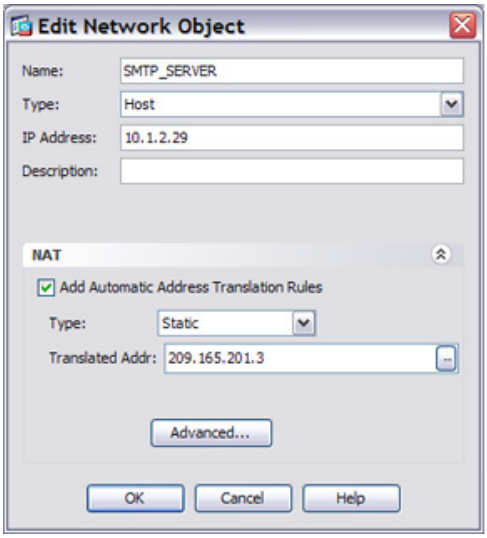
Step 6 Click **Advanced** to configure the real and mapped interfaces and port translation for HTTP.



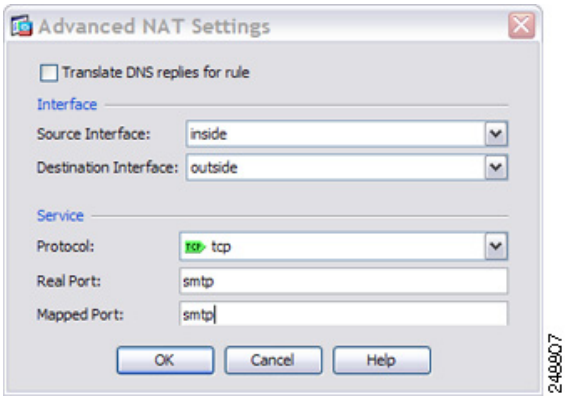
Step 7 Create a network object for the SMTP server address:



Step 8 Define the SMTP server address, and configure static NAT with identity port translation for the SMTP server:



Step 9 Click **Advanced** to configure the real and mapped interfaces and port translation for SMTP.



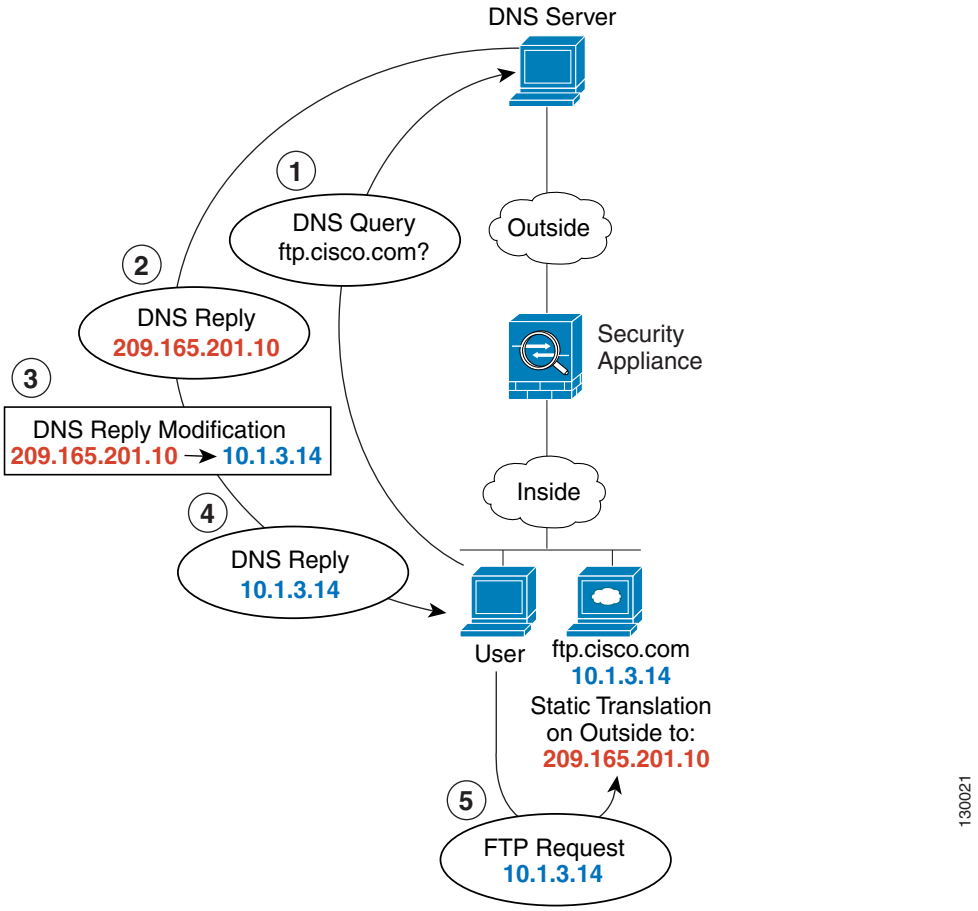
Step 10 Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

DNS Server on Mapped Interface, Web Server on Real Interface (Static NAT with DNS Modification)

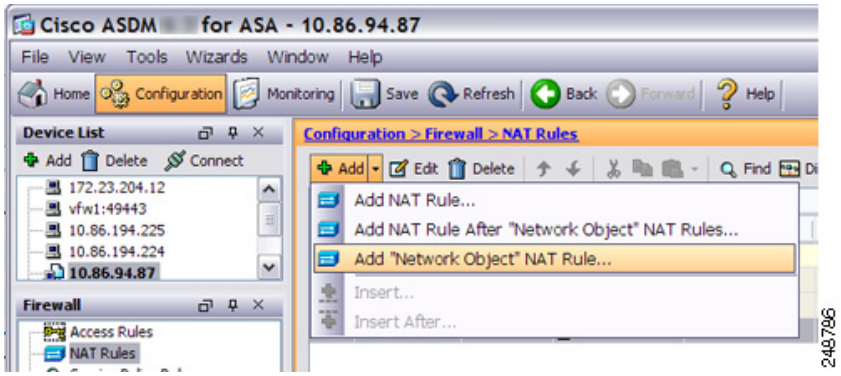
For example, a DNS server is accessible from the outside interface. A server, ftp.cisco.com, is on the inside interface. You configure the ASA to statically translate the ftp.cisco.com real address (10.1.3.14) to a mapped address (209.165.201.10) that is visible on the outside network. (See Figure 33-5.) In this case, you want to enable DNS reply modification on this static rule so that inside users who have access to ftp.cisco.com using the real address receive the real address from the DNS server, and not the mapped address.

When an inside host sends a DNS request for the address of ftp.cisco.com, the DNS server replies with the mapped address (209.165.201.10). The ASA refers to the static rule for the inside server and translates the address inside the DNS reply to 10.1.3.14. If you do not enable DNS reply modification, then the inside host attempts to send traffic to 209.165.201.10 instead of accessing ftp.cisco.com directly.

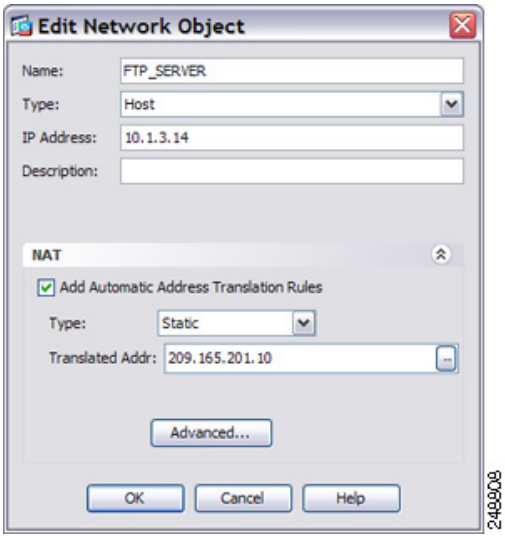
Figure 33-5 DNS Reply Modification



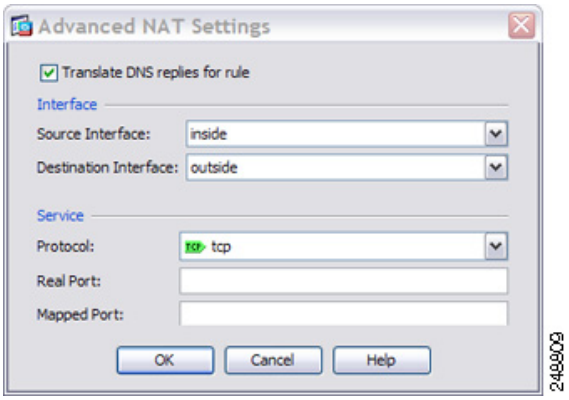
Step 1 Create a network object for the FTP server address:



Step 2 Define the FTP server address, and configure static NAT with DNS modification:



Step 3 Click **Advanced** to configure the real and mapped interfaces and DNS modification.

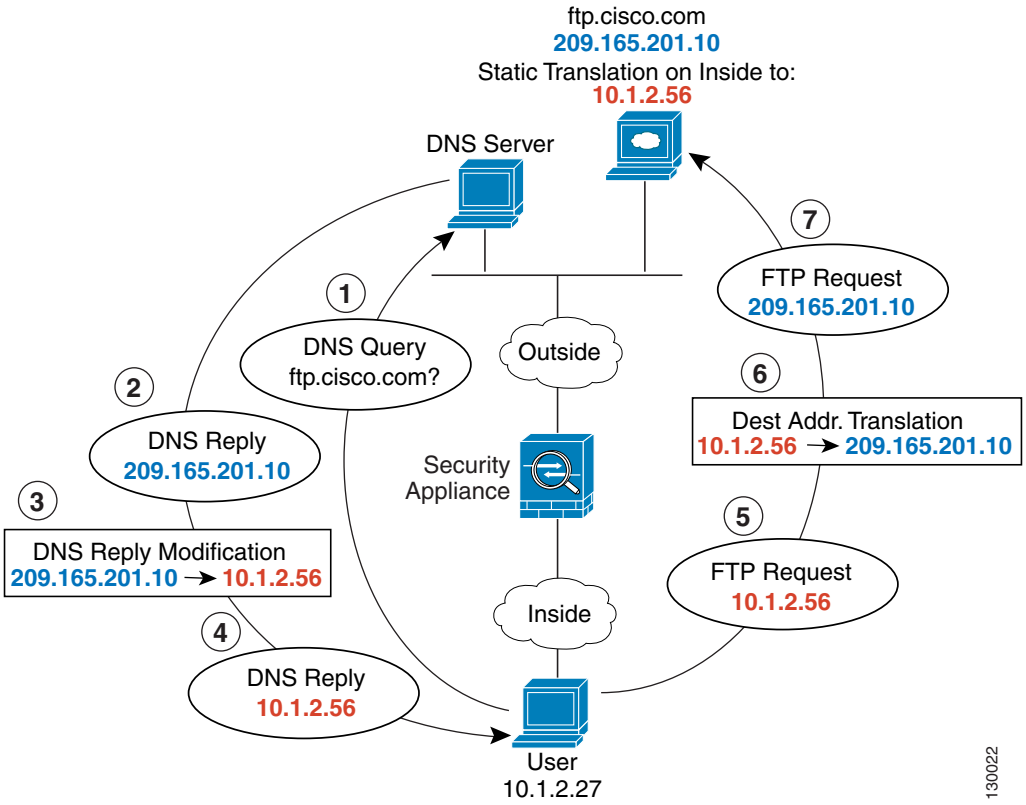


Step 4 Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

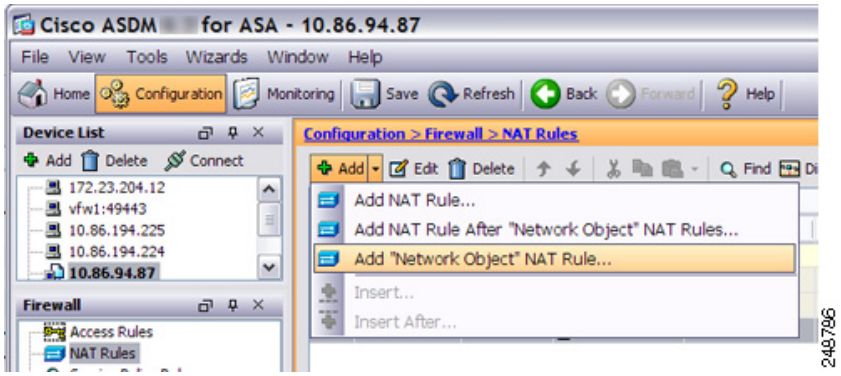
DNS Server and FTP Server on Mapped Interface, FTP Server is Translated (Static NAT with DNS Modification)

Figure 33-6 shows an FTP server and DNS server on the outside. The ASA has a static translation for the outside server. In this case, when an inside user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.201.10. Because you want inside users to use the mapped address for ftp.cisco.com (10.1.2.56) you need to configure DNS reply modification for the static translation.

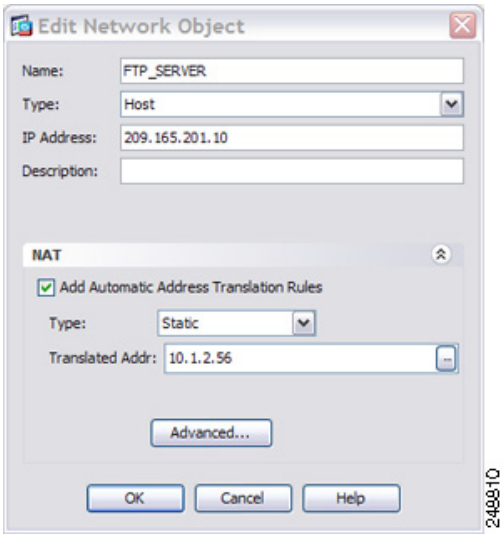
Figure 33-6 DNS Reply Modification Using Outside NAT



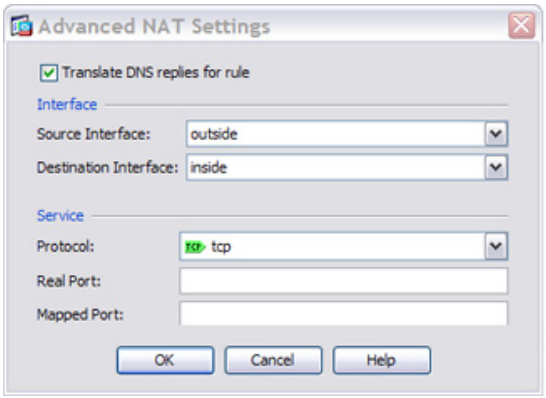
Step 1 Create a network object for the FTP server address:



Step 2 Define the FTP server address, and configure static NAT with DNS modification:



Step 3 Click **Advanced** to configure the real and mapped interfaces and DNS modification.

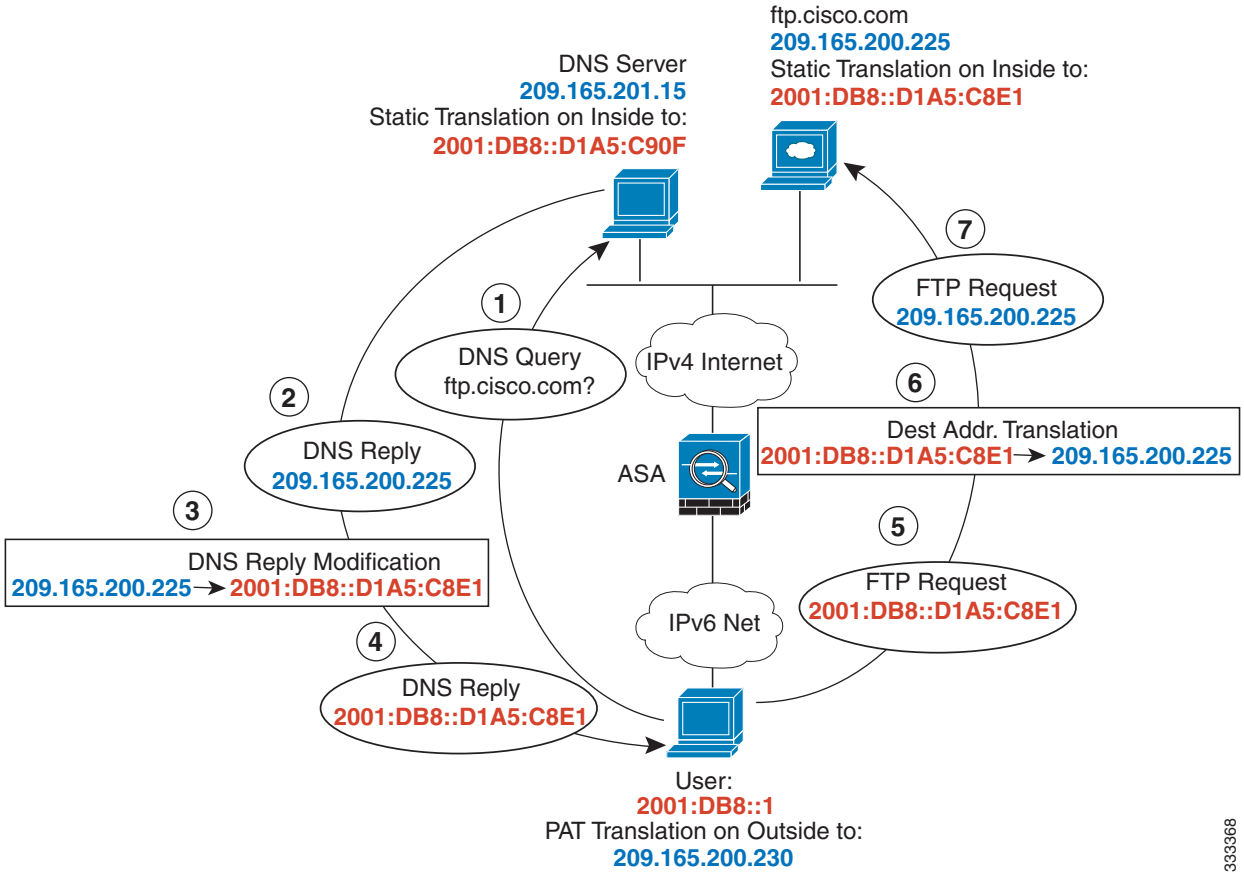


Step 4 Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

IPv4 DNS Server and FTP Server on Mapped Interface, IPv6 Host on Real Interface (Static NAT64 with DNS64 Modification)

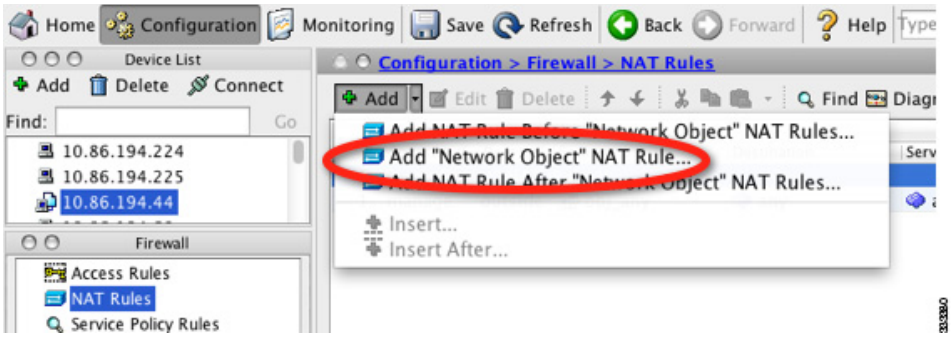
Figure 33-6 shows an FTP server and DNS server on the outside IPv4 network. The ASA has a static translation for the outside server. In this case, when an inside IPv6 user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.200.225. Because you want inside users to use the mapped address for ftp.cisco.com (2001:DB8::D1A5:C8E1) you need to configure DNS reply modification for the static translation. This example also includes a static NAT translation for the DNS server, and a PAT rule for the inside IPv6 hosts.

Figure 33-7 DNS Reply Modification Using Outside NAT

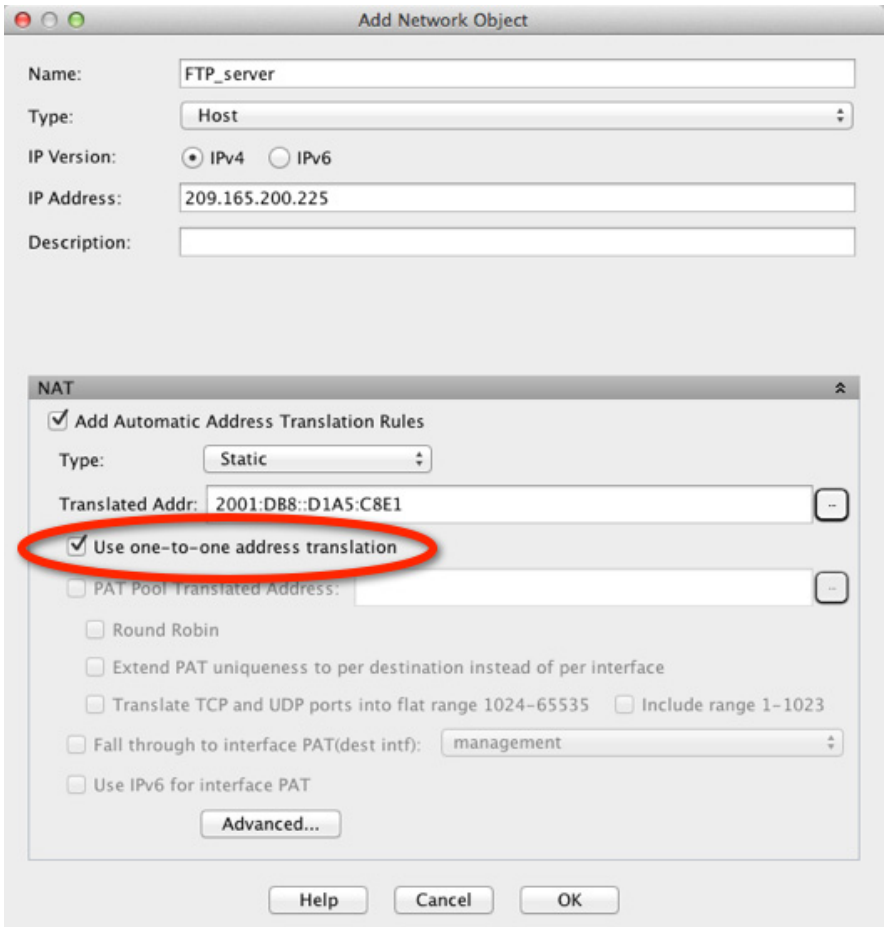


Step 1 Configure static NAT with DNS modification for the FTP server.

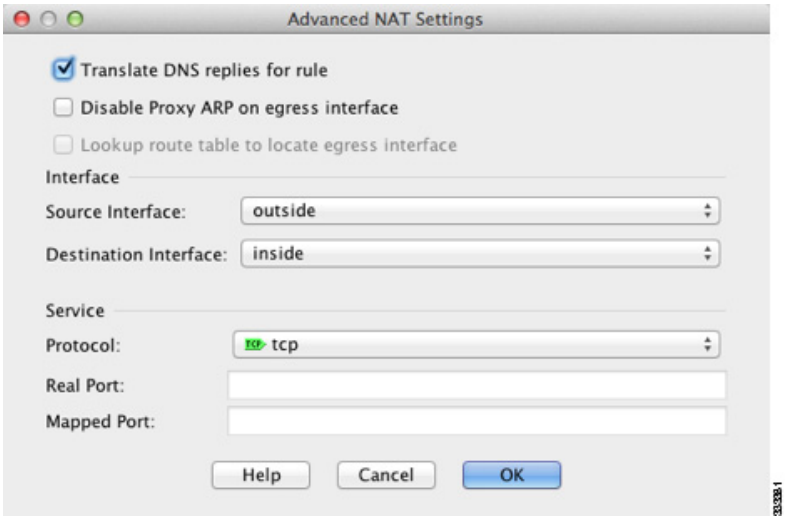
a. Create a network object for the FTP server address.



b. Define the FTP server address, and configure static NAT with DNS modification and, because this is a one-to-one translation, configure the one-to-one method for NAT46.



c. Click **Advanced** to configure the real and mapped interfaces and DNS modification.

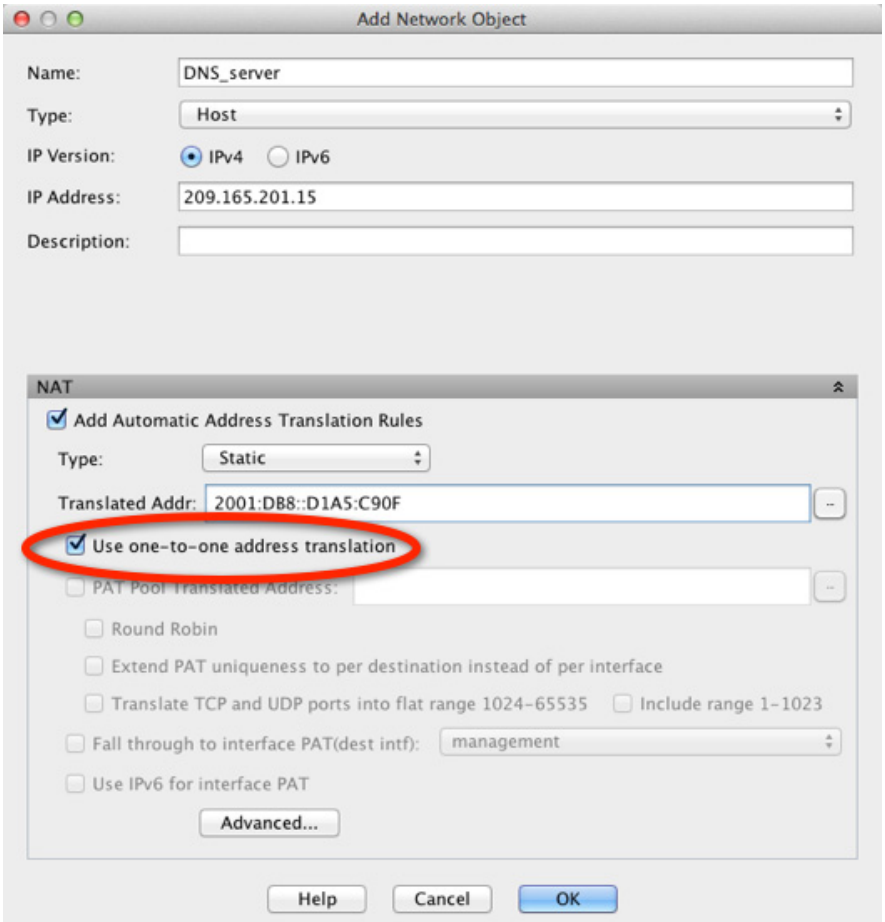


d. Click **OK** to return to the Edit Network Object dialog box.

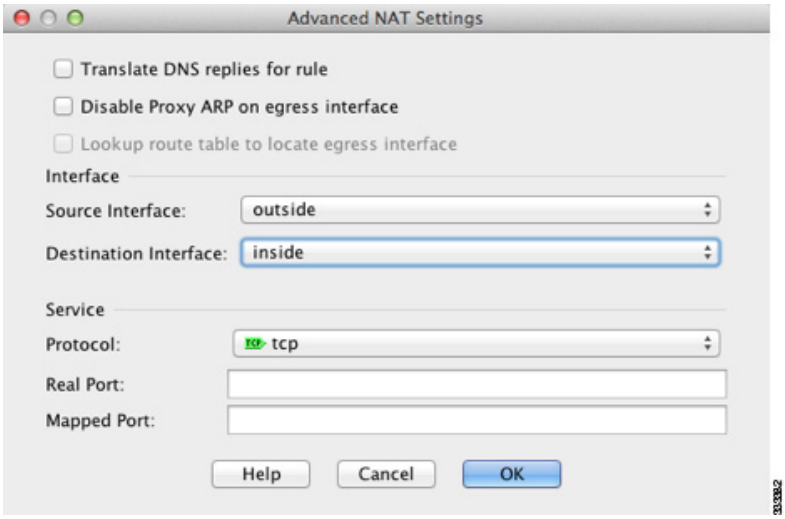
Step 2 Configure NAT for the DNS server.

a. Create a network object for the DNS server address.

b. Define the DNS server address, and configure static NAT using the one-to-one method.

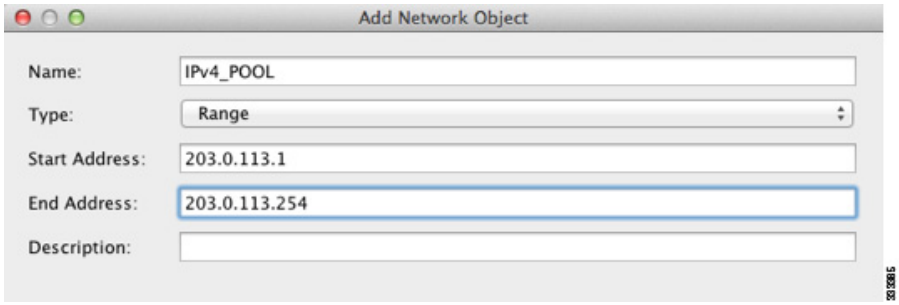


c. Click **Advanced** to configure the real and mapped interfaces.



d. Click **OK** to return to the Edit Network Object dialog box.

Step 3 Configure an IPv4 PAT pool for translating the inside IPv6 network.

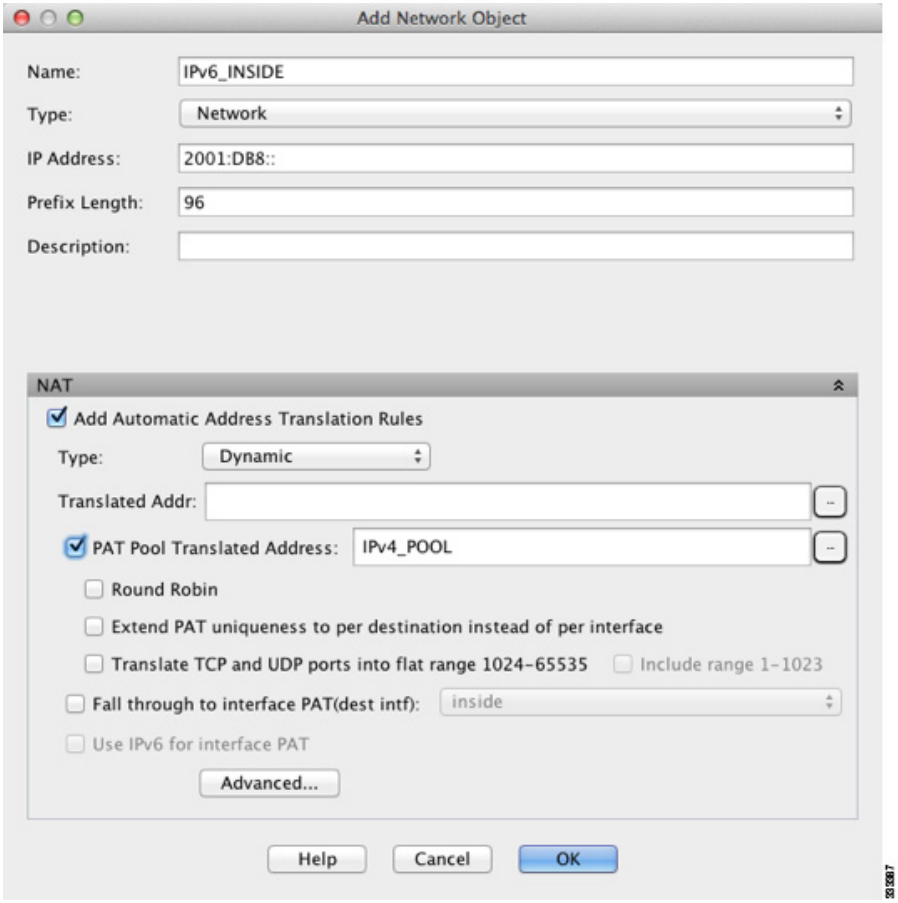


Under NAT, uncheck the **Add Automatic Address Translation Rules** check box.

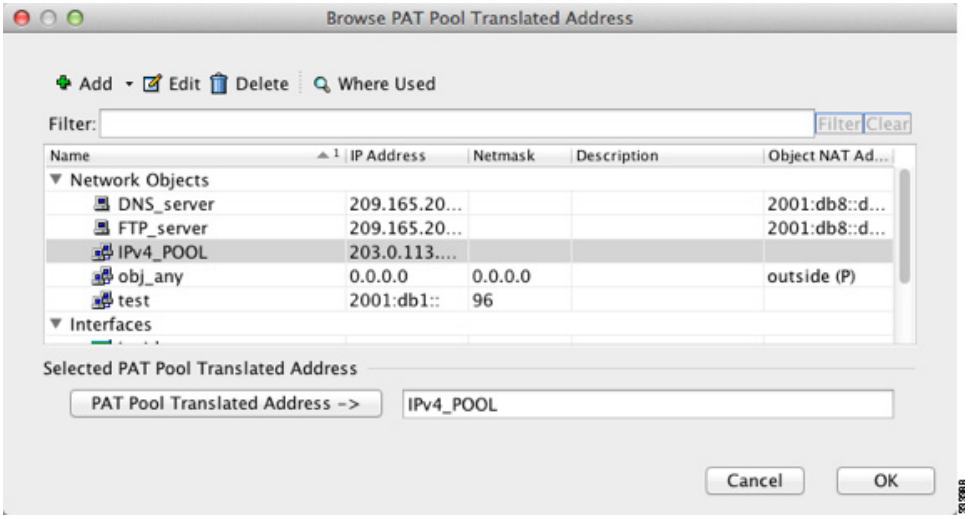
Step 4 Configure PAT for the inside IPv6 network.

a. Create a network object for the inside IPv6 network.

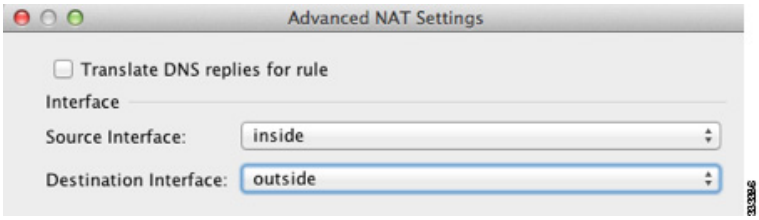
b. Define the IPv6 network address, and configure dynamic NAT using a PAT pool.



c. Next to the PAT Pool Translated Address field, click the **...** button to choose the PAT pool you created earlier, and click **OK**.



d. Click **Advanced** to configure the real and mapped interfaces.



e. Click **OK** to return to the Edit Network Object dialog box.

Step 5 Click **OK**, and then click **Apply**.

Feature History for Network Object NAT

Table 33-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 33-1 Feature History for Network Object NAT

Feature Name	Platform Releases	Feature Information
Network Object NAT	8.3(1)	Configures NAT for a network object IP address(es). We introduced or modified the following screens: Configuration > Firewall > NAT Rules Configuration > Firewall > Objects > Network Objects/Groups
Identity NAT configurable proxy ARP and route lookup	8.4(2)/8.5(1)	In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. We modified the following screen: Configuration > Firewall > NAT Rules > Add/Edit Network Object > Advanced NAT Settings.

Table 33-1 Feature History for Network Object NAT (continued)

Feature Name	Platform Releases	Feature Information
PAT pool and round robin address assignment	8.4(2)/8.5(1)	You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy. We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object.
Round robin PAT pool allocation uses the same IP address for existing hosts	8.4(3)	When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. We did not modify any screens. *This feature is not available in 8.5(1) or 8.6(1).*
Flat range of PAT ports for a PAT pool	8.4(3)	If available, the real source port number is used for the mapped port. However, 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: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool. If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535. We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object. *This feature is not available in 8.5(1) or 8.6(1).*
Extended PAT for a PAT pool	8.4(3)	Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough translations, you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object. *This feature is not available in 8.5(1) or 8.6(1).*

Table 33-1 Feature History for Network Object NAT (continued)

Feature Name	Platform Releases	Feature Information
Automatic NAT rules to translate a VPN peer's local IP address back to the peer's real IP address	8.4(3)	In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address. You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the **show nat** command. **Note** Because of routing issues, we do not recommend using this feature unless you know you need this feature; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations: • Only supports Cisco IPsec and AnyConnect Client. • Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied. • Does not support load-balancing (because of routing issues). • Does not support roaming (public IP changing). ASDM does not support this command; enter the command using the Command Line Tool.
NAT support for IPv6	9.0(1)	NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6. Translating between IPv4 and IPv6 is not supported in transparent mode. We modified the following screen: Configuration > Firewall > Objects > Network Objects/Group.

Table 33-1 Feature History for Network Object NAT (continued)

Feature Name	Platform Releases	Feature Information
NAT support for reverse DNS lookups	9.0(1)	NAT now supports translation of the DNS PTR record for reverse DNS lookups when using IPv4 NAT, IPv6 NAT, and NAT64 with DNS inspection enabled for the NAT rule.
Per-session PAT	9.0(1)	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 master 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 requires multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule. We introduced the following screen: Configuration > Firewall > Advanced > Per-Session NAT Rules.