

Network Address Translation (NAT)

The following topics explain Network Address Translation (NAT) and how to configure it.

- Why use NAT?, on page 1
- NAT basics, on page 2
- Guidelines for NAT, on page 8
- Configure NAT, on page 14
- Translating IPv6 networks, on page 40
- Monitoring NAT, on page 54
- Examples for NAT, on page 55

Why use NAT?

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private, not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of NAT is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

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

- Translating between IPv4 and IPv6 (Routed mode only)—If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

Note NAT is not required. If you do not configure NAT for a given set of traffic, that traffic will not be translated, but will have all of the security policies applied as normal.

NAT basics

The following topics explain some of the basics of NAT.

NAT terminology

This document uses the following terminology:

- Real address/host/network/interface—The real address is the address that is defined on the host, before it is translated. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the inside network would be the "real" network. Note that you can translate any network connected to the device, not just an inside network. Therefore if you configure NAT to translate outside addresses, "real" can refer to the outside network when it accesses the inside network.
- Mapped address/host/network/interface—The mapped address is the address that the real address is translated to. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the outside network would be the "mapped" network.

Note During address translation, IP addresses configured for the device interfaces are not translated.

- Bidirectional initiation—Static NAT allows connections to be initiated *bidirectionally*, meaning both to the host and from the host.
- Source and destination NAT—For any given packet, both the source and destination IP addresses are compared to the NAT rules, and one or both can be translated/untranslated. For static NAT, the rule is bidirectional, so be aware that "source" and "destination" are used in commands and descriptions throughout this guide even though a given connection might originate at the "destination" address.

NAT types

You can implement NAT using the following methods:

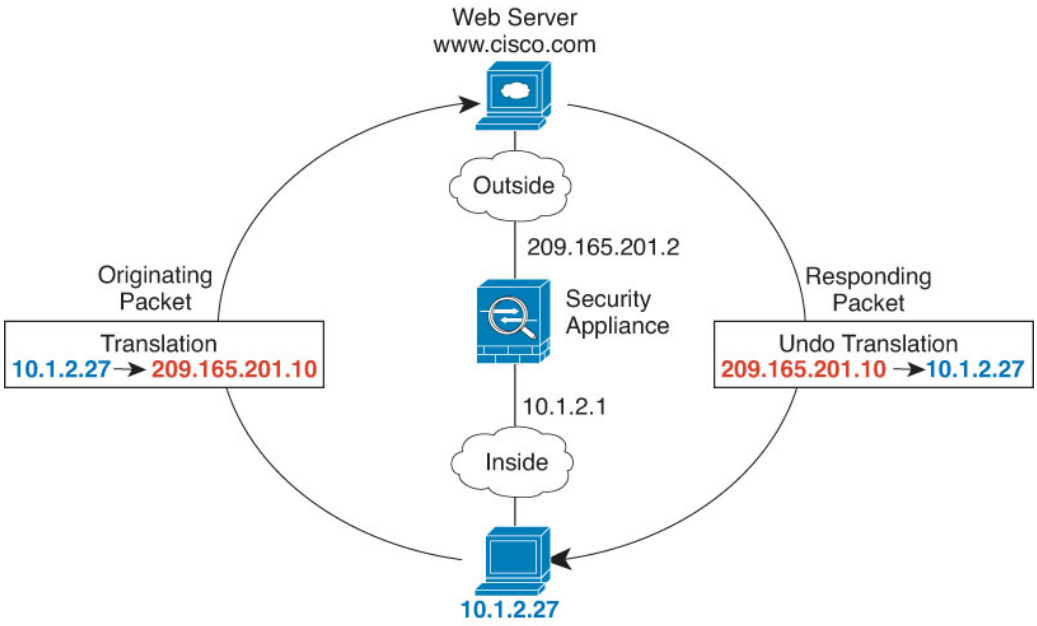
- Dynamic NAT—A group of real IP addresses are mapped to a (usually smaller) group of mapped IP addresses, on a first come, first served basis. Only the real host can initiate traffic. See Dynamic NAT, on page 14.
- Dynamic Port Address Translation (PAT)—A group of real IP addresses are mapped to a single IP address using a unique source port of that IP address. See Dynamic PAT, on page 19.

- Static NAT—A consistent mapping between a real and mapped IP address. Allows bidirectional traffic initiation. See Static NAT, on page 24.
- Identity NAT—A real address is statically translated to itself, essentially bypassing NAT. You might want to configure NAT this way when you want to translate a large group of addresses, but then want to exempt a smaller subset of addresses. See Identity NAT, on page 32.

NAT in routed mode

The following figure shows a typical NAT example in routed mode, with a private network on the inside.

Figure 1: NAT Example: Routed Mode



1. When the inside host at 10.1.2.27 sends a packet to a web server, the real source address of the packet, 10.1.2.27, is translated to a mapped address, 209.165.201.10.
2. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the Firewall Threat Defense receives the packet because the Firewall Threat Defense performs proxy ARP to claim the packet.
3. The Firewall Threat Defense then changes the translation of the mapped address, 209.165.201.10, back to the real address, 10.1.2.27, before sending it to the host.

Auto NAT and Manual NAT

You can implement address translation in two ways: *auto NAT* and *manual NAT*.

We recommend using auto NAT unless you need the extra features that manual NAT provides. It is easier to configure auto NAT, and it might be more reliable for applications such as Voice over IP (VoIP). (For VoIP, you might see a failure in the translation of indirect addresses that do not belong to either of the objects used in the rule.)

Auto NAT

All NAT rules that are configured as a parameter of a network object are considered to be *auto NAT* rules. This is a quick and easy way to configure NAT for a network object. You cannot create these rules for a group object, however.

Although these rules are configured as part of the object itself, you cannot see the NAT configuration in the object definition through the object manager.

When a packet enters an interface, both the source and destination IP addresses are checked against the auto 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 sourceA/destinationA should have a different translation than sourceA/destinationB. Use manual NAT for that kind of functionality, where you can identify the source and destination address in a single rule.

Manual NAT

Manual NAT lets you identify both the source and destination address in a single rule. Specifying both the source and destination addresses lets you specify that sourceA/destinationA can have a different translation than sourceA/destinationB.



Note For static NAT, the rule is bidirectional, so be aware that "source" and "destination" are used in commands and descriptions throughout this guide even though a given connection might originate at the "destination" address. For example, if you configure static NAT with port address translation, and specify the source address as a Telnet server, and you want all traffic going to that Telnet server to have the port translated from 2323 to 23, then you must specify the *source* ports to be translated (real: 23, mapped: 2323). You specify the source ports because you specified the Telnet server address as the source address.

The destination address is optional. If you specify the destination address, you can either map it to itself (identity NAT), or you can map it to a different address. The destination mapping is always a static mapping.

Comparing Auto NAT and Manual NAT

The main differences between these two NAT types are:

- How you define the real address.
  - Auto NAT—The NAT rule becomes a parameter for a network object. The network object IP address serves as the original (real) address.
  - Manual NAT—You identify a network object or network object group for both the real and mapped addresses. In this case, NAT is not a parameter of the network object; the network object or group is a parameter of the NAT configuration. The ability to use a network object *group* for the real address means that manual NAT is more scalable.
- How source and destination NAT is implemented.
  - Auto NAT— Each rule can apply to either the source or destination of a packet. So two rules might be used, one for the source IP address, and one for the destination IP address. These two rules cannot be tied together to enforce a specific translation for a source/destination combination.

- Manual NAT—A single rule translates both the source and destination. A packet matches one rule only, and further rules are not checked. Even if you do not configure the optional destination address, a matching packet still matches one manual NAT rule only. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example, sourceA/destinationA can have a different translation than sourceA/destinationB.

- Order of NAT Rules.
  - Auto NAT—Automatically ordered in the NAT table.
  - Manual NAT—Manually ordered in the NAT table (before or after auto NAT rules).

NAT rule order

Auto NAT and manual NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Note There is also a Section 0, which contains any NAT rules that the system creates for its own use. These rules have priority over all others. The system automatically creates these rules and clears xlates as needed. You cannot add, edit, or modify rules in Section 0.

Table 1: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Manual NAT	Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, manual NAT rules are added to section 1. By "specific rules first," we mean: • Static rules should come before dynamic rules. • Rules that include destination translation should come before rules with source translation only. If you cannot eliminate overlapping rules, where more than one rule might apply based on the source or destination address, be especially careful to follow these recommendations. If you do not follow the above recommendation, ensure that accurate routes are configured for the mapped addresses to match the correct NAT rule.

Table Section	Rule Type	Order of Rules within the Section
Section 2	Auto NAT	If a match in section 1 is not found, section 2 rules are applied in the following order: **1.** Static rules. **2.** Dynamic rules. **Within each rule type, the following ordering guidelines are used:** **1.** Quantity of real IP addresses—From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. **2.** For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. **3.** If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, abracadabra is assessed before catwoman.
Section 3	Manual NAT	If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object def)
- 172.16.1.0/24 (dynamic) (object abc)

The resultant ordering would be:

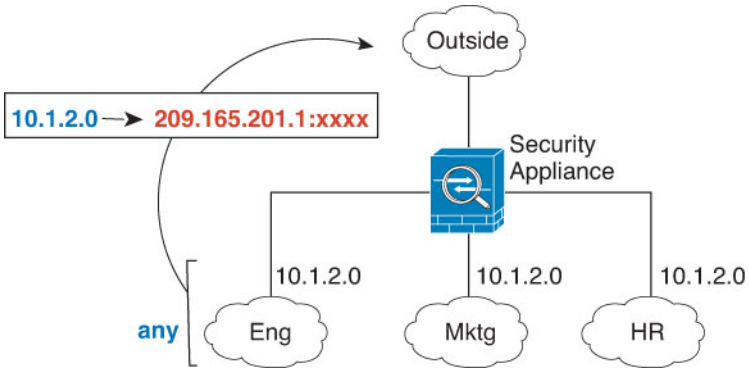
- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object abc)
- 172.16.1.0/24 (dynamic) (object def)
- 192.168.1.0/24 (dynamic)

NAT interfaces

Except for bridge group member interfaces, you can configure a NAT rule to apply to any interface (in other words, all interfaces), or you can identify specific real and mapped interfaces. You can also specify any interface for the real address, and a specific interface for the mapped address, or vice versa.

For example, you might want to specify any interface for the real address and specify the outside interface for the mapped address if you use the same private addresses on multiple interfaces, and you want to translate them all to the same global pool when accessing the outside.

Figure 2: Specifying Any Interface



However, the concept of "any" interface does not apply to bridge group member interfaces. When you specify "any" interface, all bridge group member interfaces are excluded. Thus, to apply NAT to bridge group members, you must specify the member interface. This could result in many similar rules where only one interface is different. You cannot configure NAT for the Bridge Virtual Interface (BVI) itself, you can configure NAT for member interfaces only.

Note You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes. When specifying interfaces, you do so indirectly by selecting the interface object that contains the interface.

Configuring Routing for NAT

The Firewall Threat Defense device needs to be the destination for any packets sent to the translated (mapped) address.

When sending packets, the device uses the destination interface if you specify one, or a routing table lookup if you do not, to determine the egress interface. For identity NAT, you have the option to use a route lookup even if you specify a destination interface.

The type of routing configuration needed depends on the type of mapped address, as explained in the following topics.

Addresses on the same network as the mapped interface

If you use addresses on the same network as the destination (mapped) interface, the Firewall Threat Defense uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the Firewall Threat Defense does not have to be

the gateway for any additional networks. This solution is ideal if the outside network contains an adequate number of free addresses, a consideration if you are using a 1:1 translation like dynamic NAT or static NAT. Dynamic PAT greatly extends the number of translations you can use with a small number of addresses, so even if the available addresses on the outside network is small, this method can be used. For PAT, you can even use the IP address of the mapped interface.

Addresses on a unique network

If you need more addresses than are available on the destination (mapped) interface network, you can identify addresses on a different subnet. The upstream router needs a static route for the mapped addresses that points to the Firewall Threat Defense.

The same address as the real address (identity NAT)

The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired. You can also disable proxy ARP for regular static NAT if desired, in which case you need to be sure to have proper routes on the upstream router.

Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues. For example, if you configure a broad identity NAT rule for “any” IP address, then leaving proxy ARP enabled can cause problems for hosts on the network directly connected to the mapped interface. In this case, when a host on the mapped network wants to communicate with another host on the same network, then the address in the ARP request matches the NAT rule (which matches “any” address). The Firewall Threat Defense will then proxy ARP for the address, even though the packet is not actually destined for the Firewall Threat Defense. (Note that this problem occurs even if you have a manual NAT rule; although the NAT rule must match both the source and destination addresses, the proxy ARP decision is made only on the “source” address). If the Firewall Threat Defense ARP response is received before the actual host ARP response, then traffic will be mistakenly sent to the Firewall Threat Defense.

Guidelines for NAT

The following topics provide detailed guidelines for implementing NAT.

Interface Guidelines

NAT is supported for standard routed physical or subinterfaces.

However, configuring NAT on bridge group member interfaces (interfaces that are part of a Bridge Virtual Interface, or BVI) has the following restrictions:

- When configuring NAT for the members of a bridge group, you specify the member interface. You cannot configure NAT for the bridge group interface (BVI) itself.
- When doing NAT between bridge group member interfaces, you must specify the source and destination interfaces. You cannot specify “any” as the interface.
- You cannot configure interface PAT when the destination interface is a bridge group member interface, because there is no IP address attached to the interface.
- You cannot translate between IPv4 and IPv6 networks (NAT64/46) when the source and destination interfaces are members of the same bridge group. Static NAT/PAT 44/66, dynamic NAT44/66, and dynamic PAT44 are the only allowed methods; dynamic PAT66 is not supported. However, you can do

NAT64/46 between members of different bridge groups, or between a bridge group member (source) and standard routed interface (destination).

IPv6 NAT guidelines

NAT supports IPv6 with the following guidelines and restrictions.

- For standard routed mode interfaces, you can also translate between IPv4 and IPv6.
- You cannot translate between IPv4 and IPv6 for interfaces that are members of the same bridge group. You can translate between two IPv6 or two IPv4 networks only. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.
- You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.
- 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.

IPv6 NAT best practices

You can use NAT to translate between IPv6 networks, and also to translate between IPv4 and IPv6 networks (routed mode only). We recommend the following best practices:

- NAT66 (IPv6-to-IPv6)—We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (manual NAT only).
- NAT46 (IPv4-to-IPv6)—We recommend using static NAT. Because the IPv6 address space is so much larger than the IPv4 address space, you can easily accommodate a static translation. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (manual NAT only). When translating to an IPv6 subnet (/96 or lower), the resulting mapped address is by default an IPv4-embedded IPv6 address, where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For example, if the IPv6 prefix is a /96 prefix, then the IPv4 address is appended in the last 32-bits of the address. For example, if you map 192.168.1.0/24 to 201b::0/96, then 192.168.1.4 will be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after the prefix, and a suffix of 0s is appended after the IPv4 address.
- NAT64 (IPv6-to-IPv4)—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

NAT Support for Inspected Protocols

Some application layer protocols that open secondary connections, or that embedded IP addresses in packets, are inspected to provide the following services:

- Pinhole creation—Some application protocols open secondary TCP or UDP connections either on standard or negotiated ports. Inspection opens pinholes for these secondary ports so that you do not need to create access control rules to allow them.
- NAT rewrite— Protocols such as FTP embed IP addresses and ports for the secondary connections in packet data as part of the protocol. If there is NAT translation involved for either of the endpoints, the inspection engines rewrite the packet data to reflect the NAT translation of the embedded addresses and ports. The secondary connections would not work without NAT rewrite.
- Protocol enforcement—Some inspections enforce some degree of conformance to the RFCs for the inspected protocol.

The following table lists the inspected protocols that apply NAT rewrite and their NAT limitations. Keep these limitations in mind when writing NAT rules that include these protocols. Inspected protocols not listed here do not apply NAT rewrite. These inspections include GTP, HTTP, IMAP, POP, SMTP, SSH, and SSL.



Note NAT rewrite is supported on the listed ports only. If you use these protocols on non-standard ports, do not use NAT on the connections.

Table 2: NAT Supported Application Inspection

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
DCERPC	TCP/135	No NAT64.	Yes
DNS over UDP	UDP/53	No NAT support is available for name resolution through WINS.	No
ESMTP	TCP/25	No NAT64.	No
FTP	TCP/21	No limitations.	Yes
H.323 H.225 (Call signaling) H.323 RAS	TCP/1720 UDP/1718 For RAS, UDP/1718-1719	No NAT64.	Yes
ICMP ICMP Error	ICMP (ICMP traffic directed to a device interface is never inspected.)	No limitations.	No
IP Options	RSVP	No NAT64.	No
NetBIOS Name Server over IP	UDP/137, 138 (Source ports)	No NAT64.	No
RSH	TCP/514	No PAT. No NAT64.	Yes

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
RTSP	TCP/554 (No handling for HTTP cloaking.)	No NAT64.	Yes
SIP	TCP/5060 UDP/5060	No extended PAT. No NAT64 or NAT46.	Yes
Skinny (SCCP)	TCP/2000	No NAT64, NAT46, or NAT66.	Yes
SQL*Net (versions 1, 2)	TCP/1521	No NAT64.	Yes
Sun RPC	TCP/111 UDP/111	No NAT64.	Yes
TFTP	UDP/69	No NAT64. Payload IP addresses are not translated.	Yes
XDMCP	UDP/177	No NAT64.	Yes

FQDN destination guidelines

You can specify the translated (mapped) destination in a manual NAT rule using a fully-qualified domain name (FQDN) network object instead of an IP address. For example, you can create a rule based on traffic that is destined for the www.example.com web server.

When using an FQDN, the system obtains the DNS resolution and writes the NAT rule based on the returned address. If more than one address is obtained from the DNS server, the address used is based on the following:

- If there is an address on the same subnet as the specified interface, that address is used. If there isn't one on the same subnet, the first address returned is used.
- The IP type for the translated source and translated destination must match. For example, if the translated source address is IPv6, the FQDN object must specify IPv6 as the address type. If the translated source is IPv4, the FQDN object can specify IPv4 or both IPv4 and IPv6. In this case, an IPv4 address is selected.

You cannot include an FQDN object in a network group that is used for manual NAT destination. In NAT, an FQDN object must be used alone, as only a single destination host makes sense for this type of NAT rule.

If the FQDN cannot be resolved to an IP address, the rule is not functional until a DNS resolution is obtained.

Additional guidelines for NAT

- NAT rules apply to through the device traffic only, they do not apply to traffic initiated by the device, such as a RADIUS authentication.
- For interfaces that are members of a bridge group, you write NAT rules for the member interfaces. You cannot write NAT rules for the Bridge Virtual Interface (BVI) itself.

- You cannot write NAT rules for a Virtual Tunnel Interface (VTI), which are used in site-to-site VPN. Writing rules for the VTI's source interface will not apply NAT to the VPN tunnel. To write NAT rules that will apply to VPN traffic tunneled on a VTI, you must use "any" as the interface; you cannot explicitly specify interface names.
- (Auto NAT only.) 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.
- If a VPN is defined on an interface, inbound ESP traffic on the interface is not subject to the NAT rules. The system allows the ESP traffic for established VPN tunnels only, dropping traffic not associated with an existing tunnel. This restriction applies to ESP and UDP ports 500 and 4500.
- If you define a site-to-site VPN on a device that is behind a device that is applying dynamic PAT, so that UDP ports 500 and 4500 are not the ones actually used, you must initiate the connection from the device that is behind the PAT device. The responder cannot initiate the security association (SA) because it does not know the correct port numbers.
- 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 in the device CLI. However, clearing the translation table disconnects all current connections that use translations.

  If you create a new NAT rule that should apply to an existing connection (such as a VPN tunnel), you need to use **clear conn** to end the connection. Then, the attempt to re-establish the connection should hit the NAT rule and the connection should be NAT'ed correctly.



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** or **clear conn** commands. This safeguard ensures that the same address is not assigned to multiple hosts.

- You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
- A network object used in NAT cannot include more than 131,838 IP addresses, either explicitly or implied in a range of addresses or a subnet. Break up the address space into smaller ranges and write separate rules for the smaller objects.
- (Manual NAT only.) When using **any** as the source address in a NAT rule, the definition of “any” traffic (IPv4 vs. IPv6) depends on the rule. Before the Firewall Threat Defense performs NAT on a packet, the packet must be IPv6-to-IPv6 or IPv4-to-IPv4; with this prerequisite, the Firewall Threat Defense can determine the value of **any** in a NAT rule. For example, if you configure a rule from “any” to an IPv6 server, and that server was mapped from an IPv4 address, then **any** means “any IPv6 traffic.” If you configure a rule from “any” to “any,” and you map the source to the interface IPv4 address, then **any** means “any IPv4 traffic” because the mapped interface address implies that the destination is also IPv4.
- 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), specify the interface name instead of the interface address.
  - The failover interface IP address.
  - (Dynamic NAT.) The standby interface IP address when VPN is enabled.

- Avoid using overlapping addresses in static and dynamic NAT policies. For example, with overlapping addresses, a PPTP connection can fail to get established if the secondary connection for PPTP hits the static instead of dynamic xlate.
- You cannot use overlapping addresses in the source address of a NAT rule and a remote access VPN address pool.
- If you specify a destination interface in a rule, then that interface is used as the egress interface rather than looking up the route in the routing table. However, for identity NAT, you have the option to use a route lookup instead.
- NAT applies to through traffic only. Traffic generated by the system is not subject to NAT.
- Do not name a network object or group pat-pool, using any combination of upper- or lower-case letters.
- You cannot use NAT on the internal payload of Protocol Independent Multicast (PIM) registers.
- (Manual NAT) When writing NAT rules for a dual ISP interface setup (primary and backup interfaces using service level agreements in the routing configuration), do not specify destination criteria in the rule. Ensure the rule for the primary interface comes before the rule for the backup interface. This allows the device to choose the correct NAT destination interface based on the current routing state when the primary ISP is unavailable. If you specify destination objects, the NAT rule will always select the primary interface for the otherwise duplicate rules.
- If you get the ASP drop reason nat-no-xlate-to-pat-pool for traffic that should not match the NAT rules defined for the interface, configure identity NAT rules for the affected traffic so the traffic can pass untranslated.
- If you configure NAT for GRE tunnel endpoints, you must disable keepalives on the endpoints or the tunnel cannot be established. The endpoints send keepalives to the original addresses.
- DHCP and BOOTP share ports UDP/67-68. Because BOOTP is obsolete, writing NAT rules for the bootps port can cause port allocation problems when also running DHCP. Consider using DHCP relay instead for transmitting DHCP requests between network segments.
- In rare cases, return traffic (server to client) with an existing translation (xlate) might be logged as a new flow in Connection Events. This can occur when the client has already terminated the connection and the server sends another packet that reaches the device during the brief interval between connection closure and xlate removal, often due to application behavior or TCP stack cleanup. Because the device removes the xlate only after deleting the connection, a server packet can arrive while the xlate still exists. If no valid connection entry is found, the device logs a separate connection event based on the matched Access Control Policy rule.

Configure NAT

Network address translation can be very complex. We recommend that you keep your rules as simple as possible to avoid translation problems and difficult troubleshooting situations. Careful planning before you implement NAT is critical. The following procedure provides the basic approach.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Decide what kinds of rules you need.

You can create dynamic NAT, dynamic PAT, static NAT, and identity NAT rules. For an overview, see NAT types, on page 2.

Step 3 Decide which rules should be implemented as manual or auto NAT.

For a comparison of these two implementation options, see Auto NAT and Manual NAT, on page 3.

Step 4 Create the rules as explained in the following sections.

- Dynamic NAT, on page 14
- Dynamic PAT, on page 19
- Static NAT, on page 24
- Identity NAT, on page 32

Step 5 Manage the NAT policy and rules.

You can do the following to manage the policy and its rules.

- To edit a rule, click the edit icon ( ) for the rule.
- To delete a rule, click the delete icon ( ) for the rule.

Dynamic NAT

The following topics explain dynamic NAT and how to configure it.

About dynamic NAT

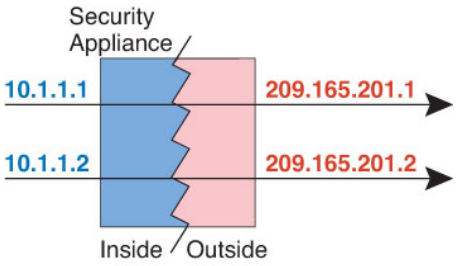
Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool typically includes fewer addresses than the real group. When a host you want to translate accesses the destination network, NAT assigns the host an IP address from the mapped pool. The translation is created only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation

times out. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, even if the connection is allowed by an access rule.

Note For the duration of the translation, a remote host can initiate a connection to the translated host if an access rule allows it. Because the address is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule. A successful connection from a remote host can reset the idle timer for the connection.

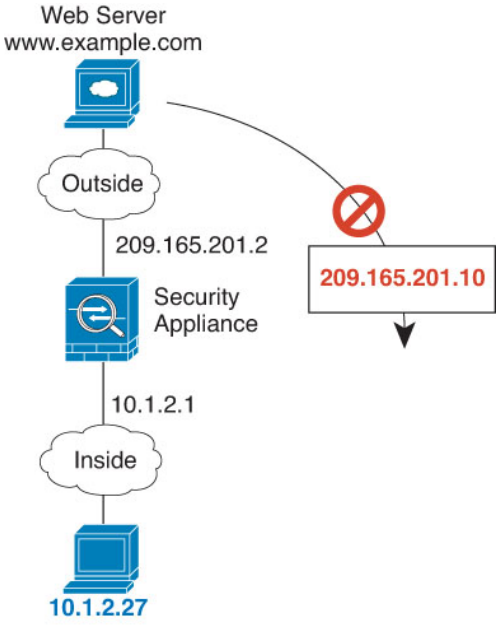
The following figure shows a typical dynamic NAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back.

Figure 3: Dynamic NAT



The following figure shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the packet is dropped.

Figure 4: Remote Host Attempts to Initiate a Connection to a Mapped Address



Dynamic NAT disadvantages and advantages

Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.

  Use PAT or a PAT fall-back method if this event occurs often because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool, and routable addresses may not be available in large quantities.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with the following:

- IP protocols that do not have a port to overload, such as GRE version 0.
- Some multimedia applications that have a data stream on one port, the control path on another port, and are not open standard.

Configure Dynamic Auto NAT

Use dynamic auto NAT rules to translate addresses to different IP addresses that are routable on the destination network.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Address**—This must be a network object (not a group), and it can be a host, range, or subnet.
- **Translated Address**—This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon () for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Auto NAT**.
- **Type**—Select **Dynamic**.

Step 4 Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the

device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

- **Original Address**—The network object that contains the addresses you are translating.
- **Translated Address**—The network object or group that contains the mapped addresses.

Step 5 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see Rewriting DNS queries and responses using NAT, on page 75.
- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group.

Step 6 Click **OK**.

Configure Dynamic Manual NAT

Use dynamic manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Dynamic NAT translates addresses to different IP addresses that are routable on the destination network.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source Address**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source Address**—This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.

You can also create network objects for the **Original Destination Address** and **Translated Destination Address** if you are configuring a static translation for those addresses in the rule.

For dynamic NAT, you can also perform port translation on the destination. In the Object Manager, ensure that there are port objects you can use for the **Original Destination Port** and **Translated Destination Port**. If you specify the source port, it will be ignored.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon ( ) for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

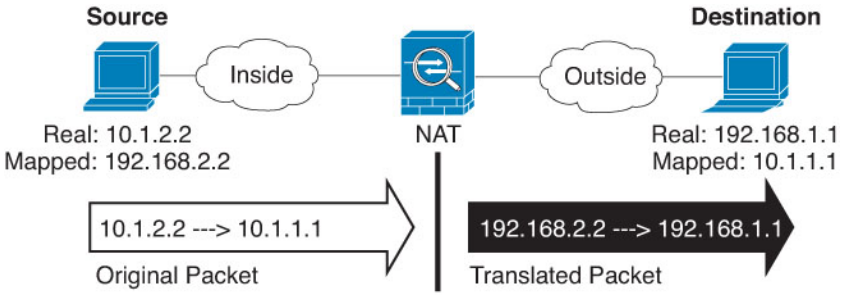
- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Manual NAT**.
- **Rule Placement**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule you select.
- **Type**—Select **Dynamic**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.

Step 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source Address**—The network object or group that contains the addresses you are translating.
- **Original Destination Address**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source Address**—The network object or group that contains the mapped addresses.
- **Translated Destination Address**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination Address**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the destination service ports for service translation: **Original Destination Port**, **Translated Destination Port**.

Dynamic NAT does not support port translation, so leave the **Original Source Port** and **Translated Source Port** fields empty. However, because the destination translation is always static, you can perform port translation for the destination port.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

Step 8 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see Rewriting DNS queries and responses using NAT, on page 75.
- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group.

Step 9 Click **OK**.

Dynamic PAT

The following topics describe dynamic PAT.

About dynamic PAT

Dynamic PAT translates multiple real addresses to a single mapped IP address by translating the real address and source port to the mapped address and a unique port.

Each connection requires a separate translation session because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The following figure shows a typical dynamic PAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back. The mapped address is the same for each translation, but the port is dynamically assigned.

Figure 5: Dynamic PAT



For the duration of the translation, a remote host on the destination network can initiate a connection to the translated host if an access rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

After the connection expires, the port translation also expires.

Note We recommend that you use different PAT pools for each interface. If you use the same pool for multiple interfaces, especially if you use it for "any" interface, the pool can be quickly exhausted, with no ports available for new translations.

Dynamic PAT disadvantages and advantages

Dynamic PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the Firewall Threat Defense interface IP address as the PAT address. However, you cannot use interface PAT for the IPv6 addresses on the interface.

You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group. This restriction does not apply between a bridge group member and a standard routed interface.

Dynamic PAT does not work with some multimedia applications that have a data stream that is different from the control path. For more information, see NAT Support for Inspected Protocols, on page 9.

Dynamic PAT might also create a large number of connections appearing to come from a single IP address, and servers might interpret the traffic as a DoS attack.

Configure Dynamic Auto PAT

Use dynamic auto PAT rules to translate addresses to unique IP address/port combinations, rather than to multiple IP addresses only. You can translate to a single address, either the destination interface's address or another address.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Address**—This must be a network object (not a group), and it can be a host, range, or subnet.
- **Translated Address**—You have the following options to specify the PAT address:
  - **Destination Interface**—To use the destination interface IPv4 address, you do not need a network object. You cannot use interface PAT for IPv6.

- **Single PAT address**—Create a network object containing a single host.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon ( ) for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Auto NAT**.
- **Type**—Select **Dynamic**.

Step 4 Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.
- **Original Address**—The network object that contains the addresses you are translating.
- **Translated Address**—One of the following:
  - (Interface PAT.) To use the IPv4 address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. You cannot use interface PAT for IPv6.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose.

Step 5 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. You cannot select this option if you already configured interface PAT as the translated address. You also cannot use this option with IPv6 networks.

Step 6 Click **OK**.

Configure Dynamic Manual PAT

Use dynamic manual PAT rules when auto PAT does not meet your needs. For example, if you want to do different translations based on the destination. Dynamic PAT translates addresses to unique IP address/port

combinations, rather than to multiple IP addresses only. You can translate to a single address, either the destination interface's address or another address.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source Address**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source Address**—You have the following options to specify the PAT address:
  - **Destination Interface**—To use the destination interface IPv4 address, you do not need a network object. You cannot use interface PAT for IPv6.
  - **Single PAT address**—Create a network object containing a single host.

You can also create network objects for the **Original Destination Address** and **Translated Destination Address** if you are configuring a static translation for those addresses in the rule.

For dynamic PAT, you can also perform port translation on the destination. In the Object Manager, ensure that there are port objects you can use for the **Original Destination Port** and **Translated Destination Port**. If you specify the source port, it will be ignored.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon () for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

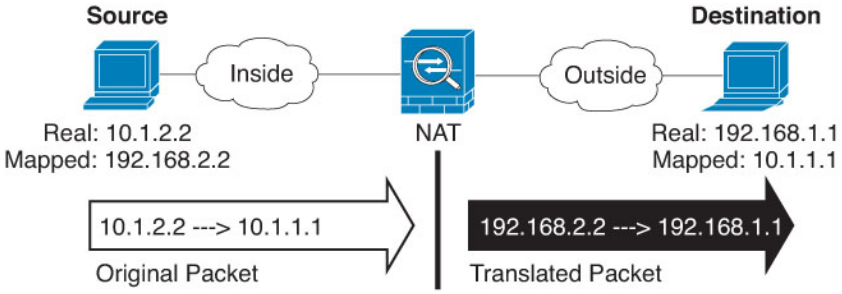
- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Manual NAT**.
- **Rule Placement**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule you select.
- **Type**—Select **Dynamic**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.

Step 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source Address**—The network object or group that contains the addresses you are translating.
- **Original Destination Address**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source Address**—One of the following:
  - (Interface PAT.) To use the IPv4 address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. You cannot use interface PAT for IPv6.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose.
- **Translated Destination Address**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the destination service ports for service translation: **Original Destination Port**, **Translated Destination Port**.

Dynamic NAT does not support port translation, so leave the **Original Source Port** and **Translated Source Port** fields empty. However, because the destination translation is always static, you can perform port translation for the destination port.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

Step 8 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. You cannot select this option if you already configured interface PAT as the translated address. You also cannot use this option with IPv6 networks.

Step 9 Click **OK**.

Static NAT

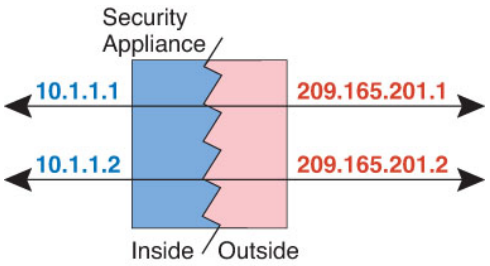
The following topics explain static NAT and how to implement it.

About static NAT

Static NAT creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if an access rule exists that allows it). With dynamic NAT and PAT, on the other hand, each host uses a different address or port for each subsequent translation, so bidirectional initiation is not supported.

The following figure shows a typical static NAT scenario. The translation is always active so both real and remote hosts can initiate connections.

Figure 6: Static NAT



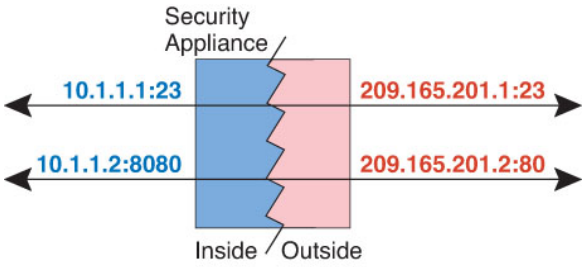
Static NAT with port translation

Static NAT with port translation lets you specify a real and mapped protocol and port.

When you specify the port with static NAT, you can choose to map the port and/or the IP address to the same value or to a different value.

The following figure shows a typical static NAT with port translation scenario showing both a port that is mapped to itself and a port that is mapped to a different value; the IP address is mapped to a different value in both cases. The translation is always active so both translated and remote hosts can initiate connections.

Figure 7: Typical Static NAT with Port Translation Scenario



Static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. In addition, for manual NAT, traffic that does not match the source IP address of the NAT rule will be dropped if it matches the destination IP address, regardless of the destination port. Therefore, you must add additional rules for all other traffic allowed to the destination IP address. For example, you can configure a static NAT rule for the IP address, without port specification, and place it after the port translation rule.

Note For applications that require application inspection for secondary channels (for example, FTP and VoIP), NAT automatically translates the secondary ports.

Following are some other uses of static NAT with port translation.

Static NAT with Identity Port Translation

You can simplify external access to internal resources. For example, if you have three separate servers that provide services on different ports (such as FTP, HTTP, and SMTP), you can give external users a single IP address to access those services. You can then configure static NAT with identity port translation to map the single external IP address to the correct IP addresses of the real servers based on the port they are trying to access. You do not need to change the port, because the servers are using the standard ones (21, 80, and 25 respectively).

Static NAT with Port Translation for Non-Standard Ports

You can also use static NAT with port translation to translate a well-known port to a non-standard port or vice versa. For example, if inside web servers use port 8080, you can allow outside users to connect to port 80, and then undo translation to the original port 8080. Similarly, to provide extra security, you can tell web users to connect to non-standard port 6785, and then undo translation to port 80.

Static Interface NAT with Port Translation

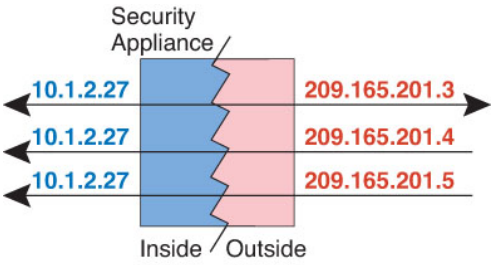
You can configure static NAT to map a real address to an interface address/port combination. For example, if you want to redirect Telnet access for the device's outside interface to an inside host, then you can map the inside host IP address/port 23 to the outside interface address/port 23.

One-to-many static NAT

Typically, you configure static NAT with a one-to-one mapping. However, in some cases, you might want to configure a single real address to several mapped addresses (one-to-many). When you configure one-to-many static NAT, when the real host initiates traffic, it always uses the first mapped address. However, for traffic initiated to the host, you can initiate traffic to any of the mapped addresses, and they will be untranslated to the single real address.

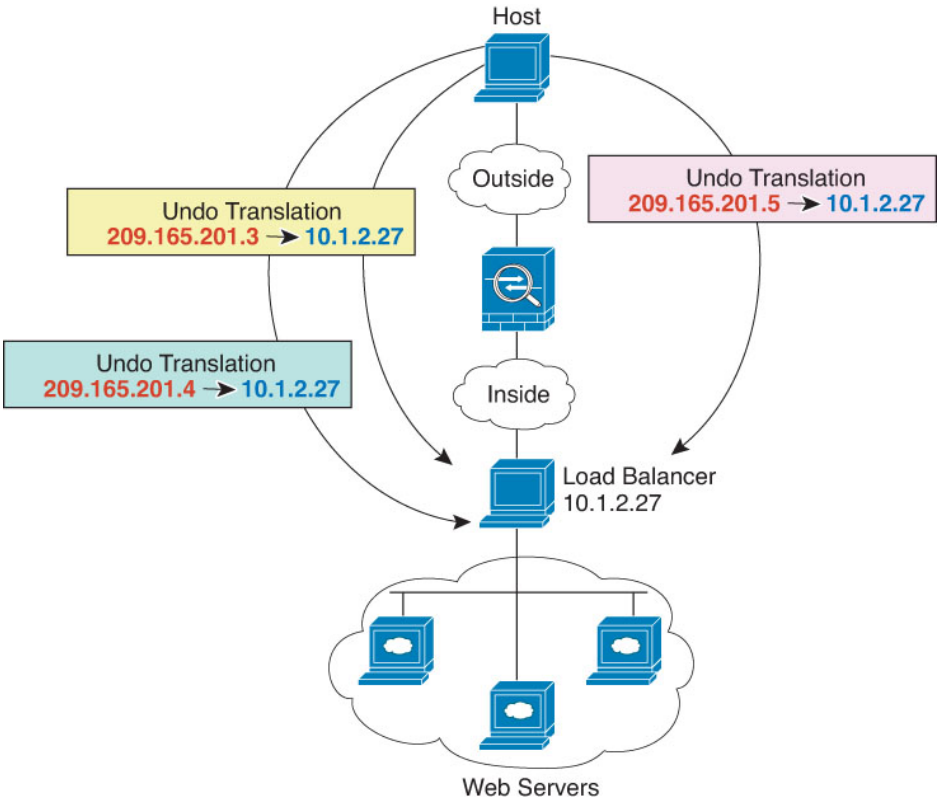
The following figure shows a typical one-to-many static NAT scenario. Because initiation by the real host always uses the first mapped address, the translation of real host IP/first mapped IP is technically the only bidirectional translation.

Figure 8: One-to-Many Static NAT



For example, you have a load balancer at 10.1.2.27. Depending on the URL requested, it redirects traffic to the correct web server.

Figure 9: One-to-Many Static NAT Example



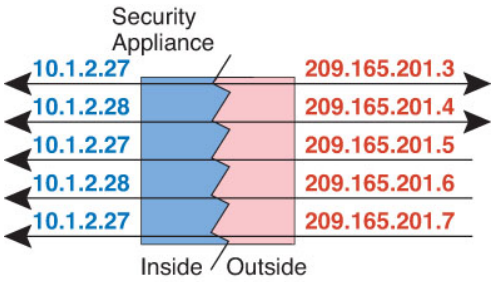
Other mapping scenarios (not recommended)

NAT has the flexibility to allow any kind of static mapping scenario: one-to-one, one-to-many, but also few-to-many, many-to-few, and many-to-one mappings. We recommend using only one-to-one or one-to-many mappings. These other mapping options might result in unintended consequences.

Functionally, few-to-many is the same as one-to-many; but because the configuration is more complicated and the actual mappings may not be obvious at a glance, we recommend creating a one-to-many configuration for each real address that requires it. For example, for a few-to-many scenario, the few real addresses are mapped to the many mapped addresses in order (A to 1, B to 2, C to 3). When all real addresses are mapped, the next mapped address is mapped to the first real address, and so on until all mapped addresses are mapped (A to 4, B to 5, C to 6). This results in multiple mapped addresses for each real address. Just like a one-to-many configuration, only the first mappings are bidirectional; subsequent mappings allow traffic to be initiated *to* the real host, but all traffic *from* the real host uses only the first mapped address for the source.

The following figure shows a typical few-to-many static NAT scenario.

Figure 10: Few-to-Many Static NAT

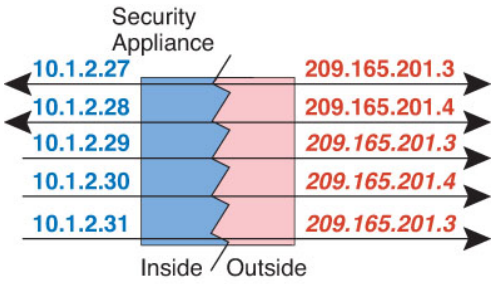


For a many-to-few or many-to-one configuration, where you have more real addresses than mapped addresses, you run out of mapped addresses before you run out of real addresses. Only the mappings between the lowest real IP addresses and the mapped pool result in bidirectional initiation. The remaining higher real addresses can initiate traffic, but traffic cannot be initiated to them (returning traffic for a connection is directed to the correct real address because of the unique 5-tuple (source IP, destination IP, source port, destination port, protocol) for the connection).

Note Many-to-few or many-to-one NAT is not PAT. If two real hosts use the same source port number and go to the same outside server and the same TCP destination port, and both hosts are translated to the same IP address, then both connections will be reset because of an address conflict (the 5-tuple is not unique).

The following figure shows a typical many-to-few static NAT scenario.

Figure 11: Many-to-Few Static NAT



Instead of using a static rule this way, we suggest that you create a one-to-one rule for the traffic that needs bidirectional initiation, and then create a dynamic rule for the rest of your addresses.

Configure Static Auto NAT

Use static auto NAT rules to translate addresses to different IP addresses that are routable on the destination network. You can also do port translation with the static NAT rule.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Address**—This must be a network object (not a group), and it can be a host, range, or subnet.
- **Translated Address**—You have the following options to specify the translated address:
  - **Destination Interface**—To use the destination interface IPv4 address, you do not need a network object. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number. You cannot use interface PAT for IPv6.
  - **Address**—Create a network object or group containing hosts, ranges, or subnets. A group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. 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.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon () for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Auto NAT**.
- **Type**—Select **Static**.

Step 4 Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.
- **Original Address**—The network object that contains the addresses you are translating.
- **Translated Address**—One of the following:
  - To use a set group of addresses, select the network object or group that contains the mapped addresses. 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.

- (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. You cannot use interface PAT for IPv6. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.

- (Optional.) **Original Port**, **Translated Port**—If you need to translate a TCP or UDP port, select the port objects that define the original and translated ports. The objects must be for the same protocol. Click the **Create New Object** link if the objects do not already exist. For example, you can translate TCP/80 to TCP/8080 if necessary.

Step 5 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see Rewriting DNS queries and responses using NAT, on page 75. This option is not available if you are doing port translation.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

Step 6 Click **OK**.

Configure Static Manual NAT

Use static manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Static NAT translates addresses to different IP addresses that are routable on the destination network. You can also do port translation with the static NAT rule.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source Address**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.

- **Translated Source Address**—You have the following options to specify the translated address:

  - **Destination Interface**—To use the destination interface IPv4 address, you do not need a network object. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number. You cannot use interface PAT for IPv6.

- **Address**—Create a network object or group containing hosts, ranges, or subnets. A group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. 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.

You can also create network objects for the **Original Destination Address** and **Translated Destination Address** if you are configuring a static translation for those addresses in the rule. If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses and specify the interface in the rule.

You can also perform port translation on the source, destination, or both. In the Object Manager, ensure that there are port objects you can use for the original and translated ports.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon ( ) for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

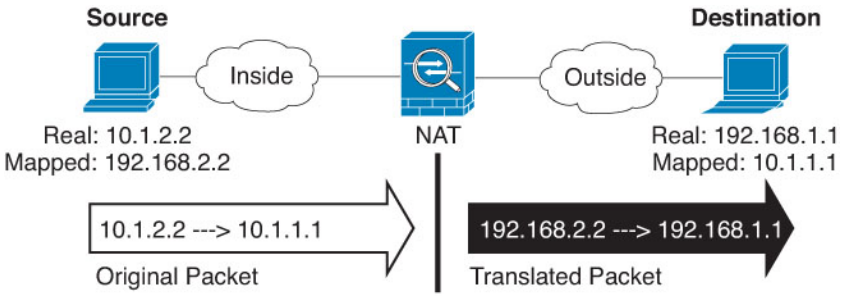
- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Manual NAT**.
- **Rule Placement**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule you select.
- **Type**—Select **Static**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.

Step 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source Address**—The network object or group that contains the addresses you are translating.
- **Original Destination Address**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source Address**—One of the following:
  - To use a set group of addresses, select the network object or group that contains the mapped addresses. 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.
  - (Static interface NAT with port translation.) To use the IPv4 address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number. You cannot use interface PAT for IPv6.
- **Translated Destination Address**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the source or destination service ports for service translation.

If you are configuring static NAT with port translation, you can translate ports for the source, destination, or both. For example, you can translate between TCP/80 and TCP/8080.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

- **Original Source Port**, **Translated Source Port**—Defines a port translation for the source address.
- **Original Destination Port**, **Translated Destination Port**—Defines a port translation for the destination address.

Step 8 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see Rewriting DNS queries and responses using NAT, on page 75. This option is not available if you are doing port translation.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

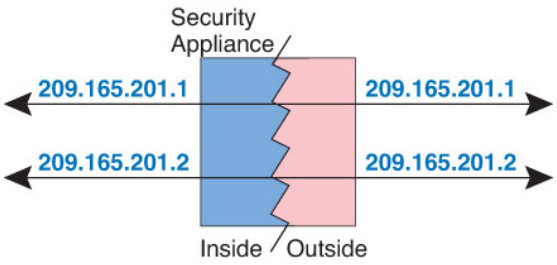
Step 9 Click **OK**.

Identity NAT

You might have a NAT configuration in which you need to translate an IP address to itself. For example, if you create a broad rule that applies NAT to every network, but want to exclude one network from NAT, you can create a static NAT rule to translate that network to itself.

The following figure shows a typical identity NAT scenario.

Figure 12: Identity NAT



The following topics explain how to configure identity NAT.

Configure Identity Auto NAT

Use static identity auto NAT rules to prevent the translation of an address. That is, to translate the address to itself.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Address**—This must be a network object (not a group), and it can be a host, range, or subnet.

- **Translated Address**—A network object or group with the exact same contents as the original source object. You can use the same object.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon () for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Auto NAT**.
- **Type**—Select **Static**.

Step 4 Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.
- **Original Address**—The network object that contains the addresses you are translating.
- **Translated Address**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Do not configure the **Original Port** and **Translated Port** options for identity NAT.

Step 5 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Translate DNS replies that match this rule**—Do not configure this option for identity NAT.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.
- **Perform Route Lookup for Destination Interface**— If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Step 6 Click **OK**.

Configure Identity Manual NAT

Use static identity manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Use static identity NAT rules to prevent the translation of an address. That is, to translate the address to itself.

Before you begin

Select **Objects** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source Address**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source Address**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

You can also create network objects for the **Original Destination Address** and **Translated Destination Address** if you are configuring a static translation for those addresses in the rule. If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses and specify the interface in the rule.

You can also perform port translation on the source, destination, or both. In the Object Manager, ensure that there are port objects you can use for the original and translated ports. You can use the same object for identity NAT.

Procedure

Step 1 Select **Policies** > **NAT**.

Step 2 Do one of the following:

- To create a new rule, click the + button.
- To edit an existing rule, click the edit icon () for the rule.

(To delete a rule you no longer need, click the trash can icon for the rule.)

Step 3 Configure the basic rule options:

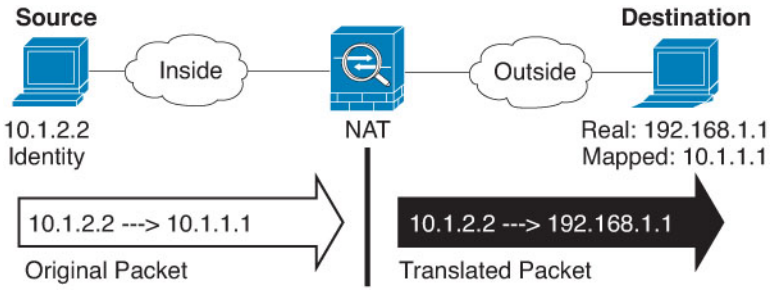
- **Title**—Enter a name for the rule.
- **Create Rule For**—Select **Manual NAT**.
- **Rule Placement**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule you select.
- **Type**—Select **Static**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.

Step 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet where you perform identity NAT on the inside host but translate the outside host.



- **Original Source Address**—The network object or group that contains the addresses you are translating.
- **Original Destination Address**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source Address**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.
- **Translated Destination Address**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination Address**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the source or destination service ports for service translation.

If you are configuring static NAT with port translation, you can translate ports for the source, destination, or both. For example, you can translate between TCP/80 and TCP/8080.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

- **Original Source Port**, **Translated Source Port**—Defines a port translation for the source address.
- **Original Destination Port**, **Translated Destination Port**—Defines a port translation for the destination address.

Step 8 (Optional.) Click the **Advanced Options** link and select the desired options:

- **Translate DNS replies that match this rule**—Do not configure this option for identity NAT.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy

ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

- **Perform route lookup for Destination interface**— If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Step 9 Click **OK**.

NAT Rule Properties

Use Network Address Translation (NAT) rules to translate IP addresses to other IP addresses. You would typically use NAT rules to convert private addresses to publically routable addresses. The translation can be from one address to another, or you can use Port Address Translation (PAT) to translate many addresses to one, using port numbers to distinguish among the source addresses.

NAT rules include the following basic properties. The properties are the same for auto NAT and manual NAT rules except where indicated.

Title

Enter a name for the rule. The name cannot include spaces.

Create Rule For

Whether the translation rule is **Auto NAT** or **Manual NAT**. Auto NAT is simpler than manual NAT, but manual NAT allows you to create separate translations for a source address based on the destination address.

Status

Whether you want the rule to be active or disabled.

Placement (Manual NAT only.)

Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule you select.

Type

Whether the translation rule is **Dynamic** or **Static**. Dynamic translation automatically chooses the mapped address from a pool of addresses, or an address/port combination when implementing PAT. Use static translation if you want to precisely define the mapped address/port.

The following topics describe the remaining NAT rules properties.

Packet Translation Properties for Auto NAT

Use the **Packet Translation** options to define the source addresses and the mapped translated addresses. The following properties apply to auto NAT only.

Source Interface, Destination Interface

(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Original Address (Always required.)

The network object that contains the source addresses you are translating. This must be a network object (not a group), and it can be a host, range, or subnet.

Translated Address (Usually required.)

The mapped addresses, the ones to which you are translating. What you select here depends on the type of translation rule you are defining.

- **Dynamic NAT**—The network object or group that contains the mapped addresses. This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.
- **Dynamic PAT**—One of the following:
  - (Interface PAT.) To use the IPv4 address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. You cannot use interface PAT for IPv6.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose.
- **Static NAT**—One of the following:
  - To use a set group of addresses, select the network object or group that contains the mapped addresses. The object or group can contain hosts, ranges, or subnets. 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.
  - (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number. You cannot use interface PAT for IPv6.
- **Identity NAT**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Original Port, Translated Port (Static NAT only.)

If you need to translate a TCP or UDP port, select the port objects that define the original and translated ports. The objects must be for the same protocol. For example, you can translate TCP/80 to TCP/8080 if necessary.

Packet Translation Properties for Manual NAT

Use the **Packet Translation** options to define the source addresses and the mapped translated addresses. The following properties apply to manual NAT only. All are optional except as indicated.

Source Interface, Destination Interface

(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Original Source Address (Always required.)

The network object or group that contains the addresses you are translating. This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can specify **Any** in the rule.

Translated Source Address (Usually required.)

The mapped addresses, the ones to which you are translating. What you select here depends on the type of translation rule you are defining.

- **Dynamic NAT**—The network object or group that contains the mapped addresses. This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.
- **Dynamic PAT**—One of the following:
  - (Interface PAT.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. You cannot use interface PAT for IPv6.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose.
- **Static NAT**—One of the following:
  - To use a set group of addresses, select the network object or group that contains the mapped addresses. The object or group can contain hosts, ranges, or subnets. 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.
  - (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface, which cannot be a bridge group member interface. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number. You cannot use interface PAT for IPv6.
- **Identity NAT**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Original Destination Address

The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Translated Destination Address

The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

You can use a network object that specifies a fully-qualified domain name as the translated destination; for more information, see FQDN destination guidelines, on page 11.

Original Source Port, Translated Source Port, Original Destination Port, Translated Destination Port

The port objects that define the source and destination services for the original and translated packets. You can translate the ports, or select the same object to make the rule sensitive to the service without translating the ports. Keep the following rules in mind when configuring services:

- (Dynamic NAT or PAT.) You cannot do translation on the **Original Source Port** and **Translated Source Port**. You can do translation on the destination port only.
- NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same object for both the real and mapped ports.

Advanced NAT Properties

When you configure NAT, you can configure properties that provide specialized services in the **Advanced** options. All of these properties are optional: configure them only if you need the service.

Translate DNS replies that match this rule

Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see Rewriting DNS queries and responses using NAT, on page 75. This option is not available if you are doing port translation in a static NAT rule.

Fallthrough to Interface PAT (Destination Interface) (Dynamic NAT only.)

Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. You cannot select this option if you already configured interface PAT as the translated address. You cannot use this option with IPv6 networks.

Do not proxy ARP on Destination Interface (Static NAT only.)

Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

Perform Route Lookup for Destination Interface (Static Identity NAT only. Routed mode only.)

If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Translating IPv6 networks

In cases where you need to pass traffic between IPv6-only and IPv4-only networks, you need to use NAT to convert between the address types. Even with two IPv6 networks, you might want to hide internal addresses from the outside network.

You can use the following translation types with IPv6 networks:

- NAT64, NAT46—Translates IPv6 packets into IPv4 and vice versa. You need to define two policies, one for the IPv6 to IPv4 translation, and one for the IPv4 to IPv6 translation. Although you can accomplish this with a single manual NAT rule, if the DNS server is on the external network, you probably need to rewrite the DNS response. Because you cannot enable DNS rewrite on a manual NAT rule when you specify a destination, creating two auto NAT rules is the better solution.



Note NAT46 supports static mappings only.

- NAT66—Translates IPv6 packets to a different IPv6 address. We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT.



Note NAT64 and NAT 46 are possible on standard routed interfaces only. NAT66 is possible on both routed and bridge group member interfaces.

NAT64/46: translating IPv6 addresses to IPv4

When traffic goes from an IPv6 network to an IPv4-only network, you need to convert the IPv6 address to IPv4, and return traffic from IPv4 to IPv6. You need to define two address pools, an IPv4 address pool to bind IPv6 addresses in the IPv4 network, and an IPv6 address pool to bind IPv4 addresses in the IPv6 network.

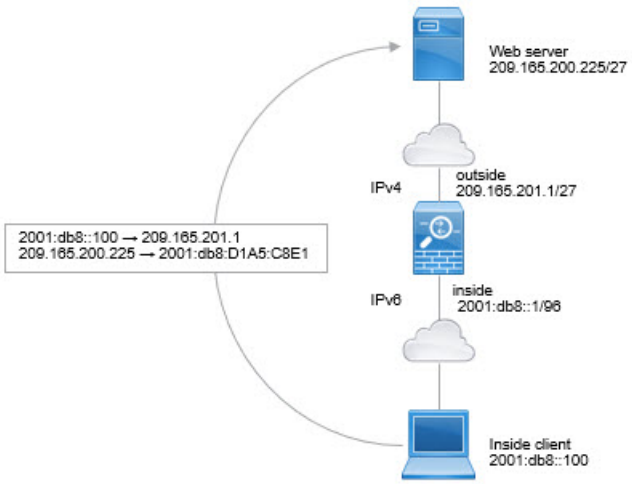
- The IPv4 address pool for the NAT64 rule is normally small and typically might not have enough addresses to map one-to-one with the IPv6 client addresses. Dynamic PAT might more easily meet the possible large number of IPv6 client addresses compared to dynamic or static NAT.

- The IPv6 address pool for the NAT46 rule can be equal to or larger than the number of IPv4 addresses to be mapped. This allows each IPv4 address to be mapped to a different IPv6 address. NAT46 supports static mappings only, so you cannot use dynamic PAT.

You need to define two policies, one for the source IPv6 network, and one for the destination IPv4 network. Although you can accomplish this with a single manual NAT rule, if the DNS server is on the external network, you probably need to rewrite the DNS response. Because you cannot enable DNS rewrite on a manual NAT rule when you specify a destination, creating two auto NAT rules is the better solution.

NAT64/46 Example: Inside IPv6 Network with Outside IPv4 Internet

Following is a straight-forward example where you have an inside IPv6-only network, and you want to convert to IPv4 for traffic sent to the Internet. This example assumes you do not need DNS translation, so you can perform both the NAT64 and NAT46 translations in a single manual NAT rule.



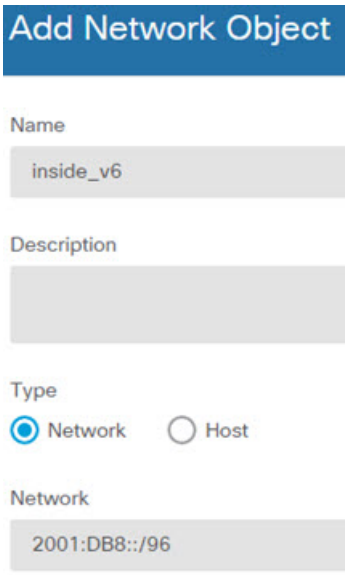
In this example, you translate the inside IPv6 network to IPv4 using dynamic interface PAT with the IP address of the outside interface. Outside IPv4 traffic is statically translated to addresses on the 2001:db8::/96 network, allowing transmission on the inside network.

Procedure

Step 1 Create a network object for the inside IPv6 network.

a) Choose **Objects**.
b) Select **Network** from the table of contents and click +.
c) Define the inside IPv6 network.

Name the network object (for example, inside_v6), select **Network**, and enter the network address, 2001:db8::/96.

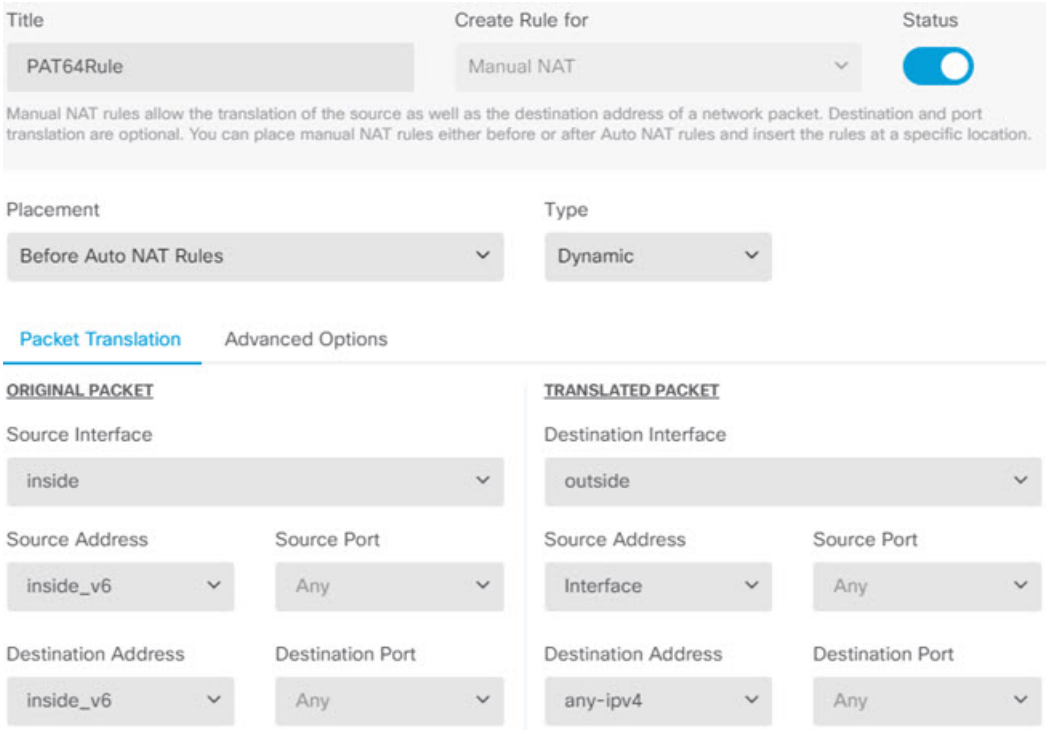


d) Click **OK**.

Step 2 Create the manual NAT rule to translate the IPv6 network to IPv4 and back again.

a) Select **Policies** > **NAT**.
b) Click the **+** button.
c) Configure the following properties:

- **Title** = PAT64Rule (or another name of your choosing).
- **Create Rule For** = **Manual NAT**.
- **Placement** = **Before Auto NAT Rules**
- **Type** = **Dynamic**.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Packet Source Address** = inside_v6 network object.
- **Translated Packet Source Address** = Interface. This option uses the IPv4 address of the destination interface as the PAT address.
- **Original Packet Destination Address** = inside_v6 network object.
- **Translated Packet Destination Address** = any-ipv4 network object.

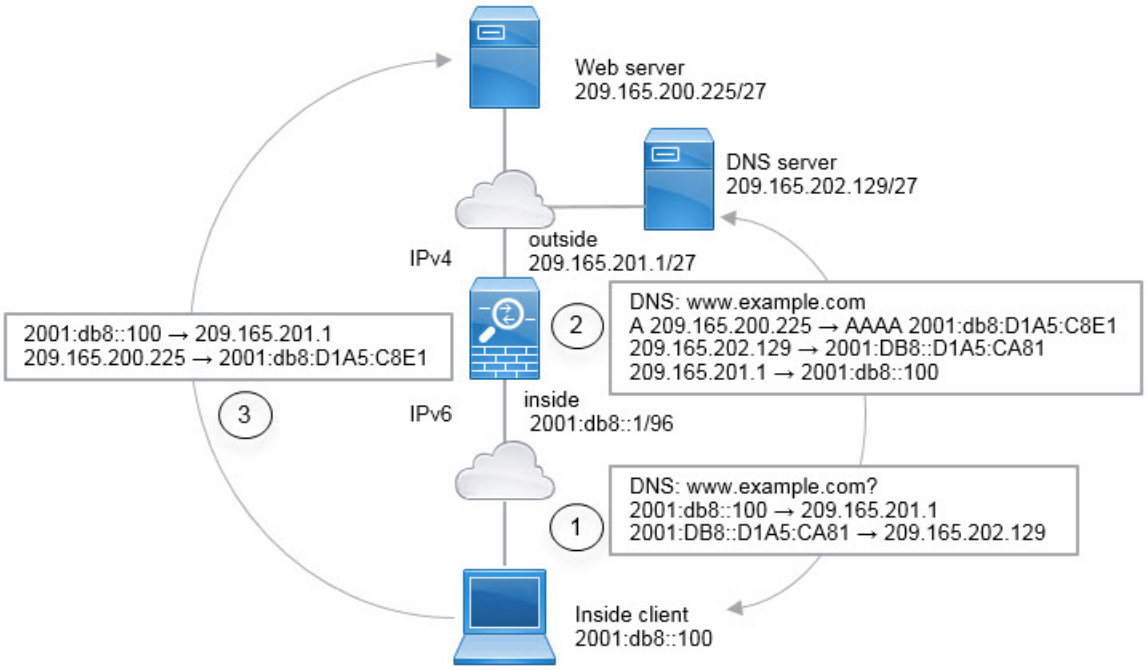


d) Click **OK**.

With this rule, any traffic from the 2001:db8::/96 subnet on the inside interface going to the outside interface gets a NAT64 PAT translation using the IPv4 address of the outside interface. Conversely, any IPv4 address on the outside network coming to the inside interface is translated to an address on the 2001:db8::/96 network using the embedded IPv4 address method.

NAT64/46 Example: Inside IPv6 Network with Outside IPv4 Internet and DNS Translation

Following is a typical example where you have an inside IPv6-only network, but there are some IPv4-only services on the outside Internet that internal users need.



In this example, you translate the inside IPv6 network to IPv4 using dynamic interface PAT with the IP address of the outside interface. Outside IPv4 traffic is statically translated to addresses on the 2001:db8::/96 network, allowing transmission on the inside network. You enable DNS rewrite on the NAT46 rule, so that replies from the external DNS server can be converted from A (IPv4) to AAAA (IPv6) records, and the addresses converted from IPv4 to IPv6.

Following is a typical sequence for a web request where a client at 2001:DB8::100 on the internal IPv6 network tries to open www.example.com.

1. The client's computer sends a DNS request to the DNS server at 2001:DB8::D1A5:CA81. The NAT rules make the following translations to the source and destination in the DNS request:
   - 2001:DB8::100 to a unique port on 209.165.201.1 (The NAT64 interface PAT rule.)
   - 2001:DB8::D1A5:CA81 to 209.165.202.129 (The NAT46 rule. D1A5:CA81 is the IPv6 equivalent of 209.165.202.129.)
2. The DNS server responds with an A record indicating that www.example.com is at 209.165.200.225. The NAT46 rule, with DNS rewrite enabled, converts the A record to the IPv6-equivalent AAAA record, and translates 209.165.200.225 to 2001:db8:D1A5:C8E1in the AAAA record. In addition, the source and destination addresses in the DNS response are untranslated:
   - 209.165.202.129 to 2001:DB8::D1A5:CA81
   - 209.165.201.1 to 2001:db8::100
3. The IPv6 client now has the IP address of the web server, and makes an HTTP request to www.example.com at 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) The source and destination of the HTTP request are translated:
   - 2001:DB8::100 to a unique port on 209.156.101.54 (The NAT64 interface PAT rule.)
   - 2001:db8:D1A5:C8E1 to 209.165.200.225 (The NAT46 rule.)

The following procedure explains how to configure this example.

Procedure

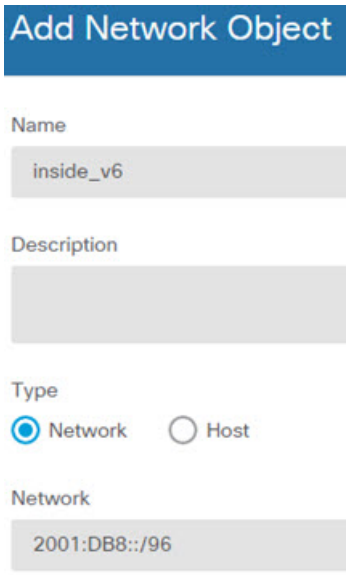
Step 1 Create the network objects that define the inside IPv6 and outside IPv4 networks.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the inside IPv6 network.

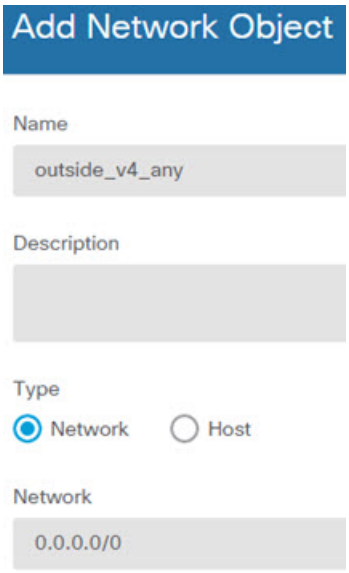
Name the network object (for example, inside_v6), select **Network**, and enter the network address, 2001:db8::/96.



d) Click **OK**.

e) Click + and define the outside IPv4 network.

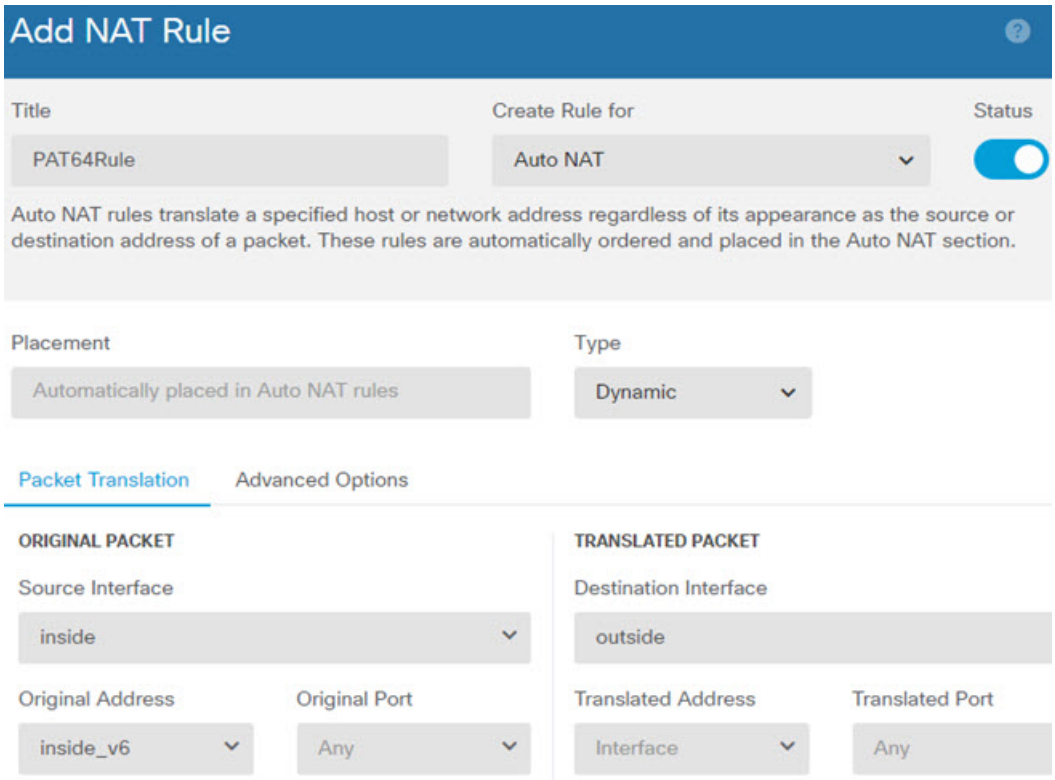
Name the network object (for example, outside_v4_any), select **Network**, and enter the network address 0.0.0.0/0.



Step 2 Configure the NAT64 dynamic PAT rule for the inside IPv6 network.

a) Select **Policies** > **NAT**.
b) Click the **+** button.
c) Configure the following properties:

- **Title** = PAT64Rule (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = inside_v6 network object.
- **Translated Address** = **Interface**. This option uses the IPv4 address of the destination interface as the PAT address.



d) Click **OK**.

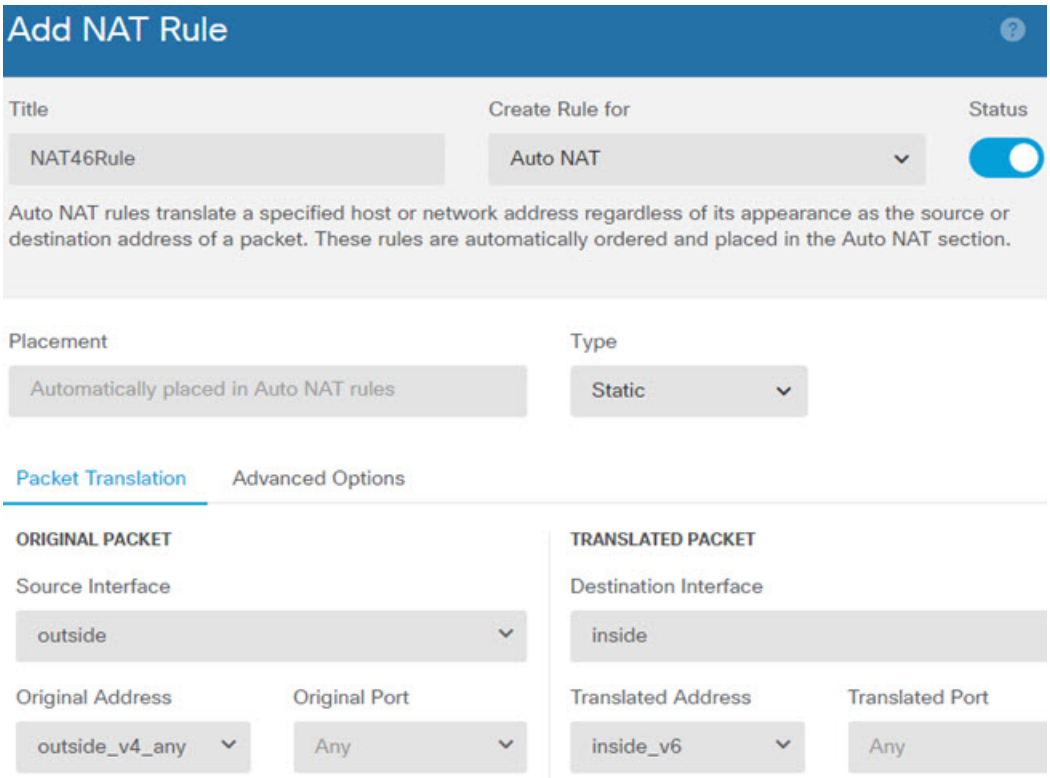
With this rule, any traffic from the 2001:db8::/96 subnet on the inside interface going to the outside interface gets a NAT64 PAT translation using the IPv4 address of the outside interface.

Step 3 Configure the static NAT46 rule for the outside IPv4 network.

a) Click the + button.

b) Configure the following properties:

- **Title** = NAT46Rule (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Static.
- **Source Interface** = outside.
- **Destination Interface** = inside.
- **Original Address** = outside_v4_any network object.
- **Translated Address** = inside_v6 network object.
- On the **Advanced Options** tab, select **Translate DNS replies that match this rule**.



c) Click **OK**.

With this rule, any IPv4 address on the outside network coming to the inside interface is translated to an address on the 2001:db8::/96 network using the embedded IPv4 address method. In addition, DNS responses are converted from A (IPv4) to AAAA (IPv6) records, and the addresses converted from IPv4 to IPv6.

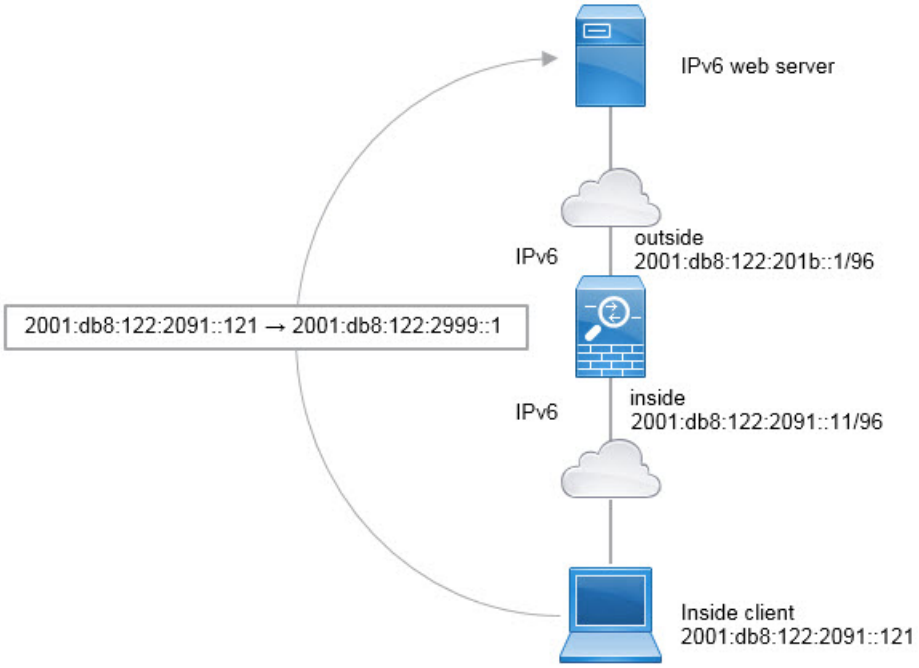
NAT66: translating IPv6 addresses to different IPv6 addresses

When going from an IPv6 network to another IPv6 network, you can translate the addresses to different IPv6 addresses on the outside network. We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT.

Because you are not translating between different address types, you need a single rule for NAT66 translations. You can easily model these rules using auto NAT. However, if you do not want to allow returning traffic, you can make the static NAT rule unidirectional using manual NAT only.

NAT66 Example, Static Translation between Networks

You can configure a static translation between IPv6 address pools using auto NAT. The following example explains how to convert inside addresses on the 2001:db8:122:2091::/96 network to outside addresses on the 2001:db8:122:2999::/96 network.



Note This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

Procedure

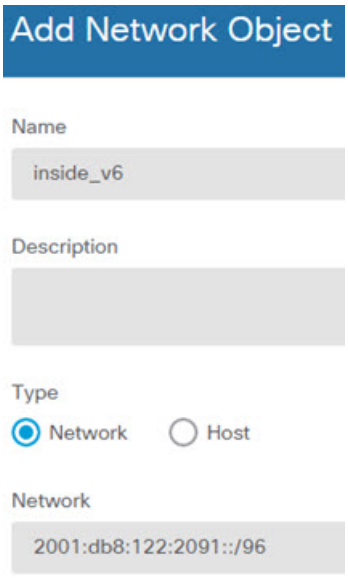
Step 1 Create the network objects that define the inside IPv6 and outside IPv6 NAT networks.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the inside IPv6 network.

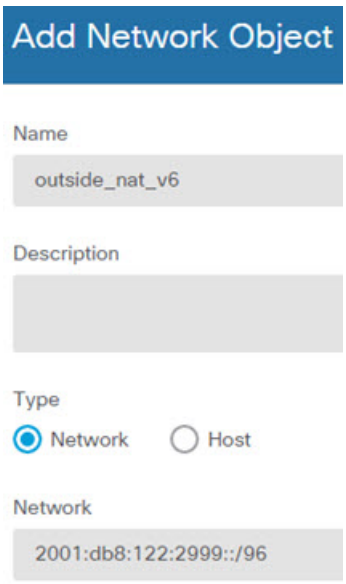
Name the network object (for example, inside_v6), select **Network**, and enter the network address, 2001:db8:122:2091::/96.



d) Click **OK**.

e) Click + and define the outside IPv6 NAT network.

Name the network object (for example, outside_nat_v6), select **Network**, and enter the network address 2001:db8:122:2999::/96.



Step 2 Configure the static NAT rule for the inside IPv6 network.

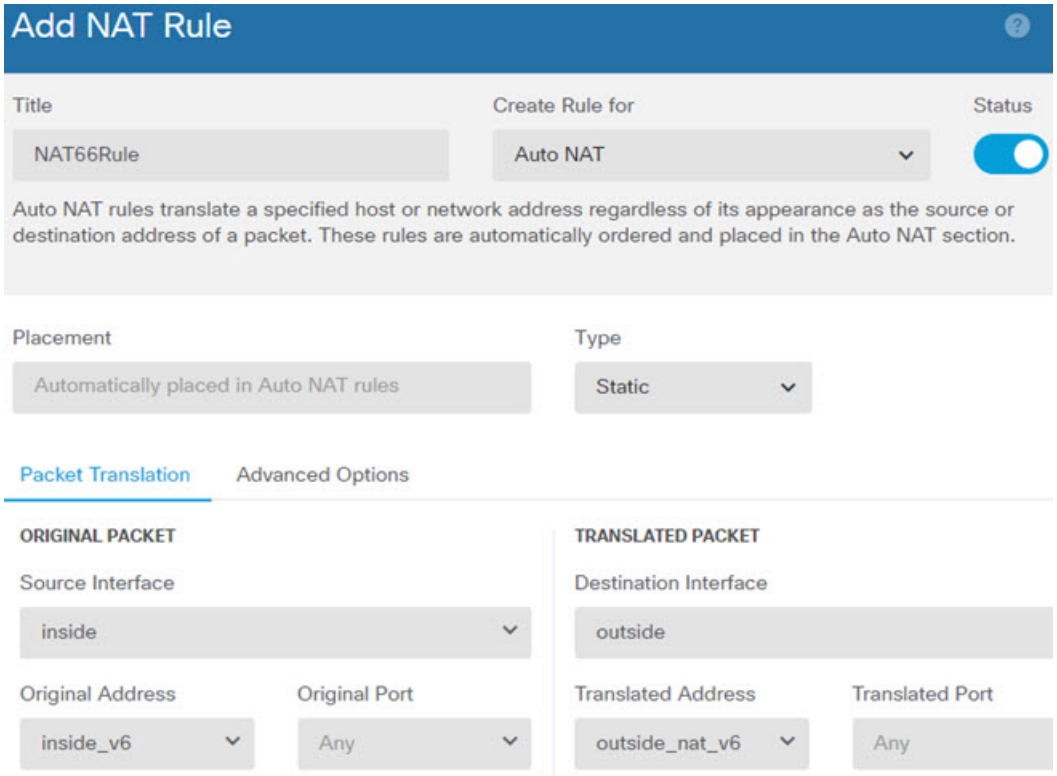
a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = NAT66Rule (or another name of your choosing).
- **Create Rule For** = Auto NAT.

- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = inside_v6 network object.
- **Translated Address** = outside_nat_v6 network object.



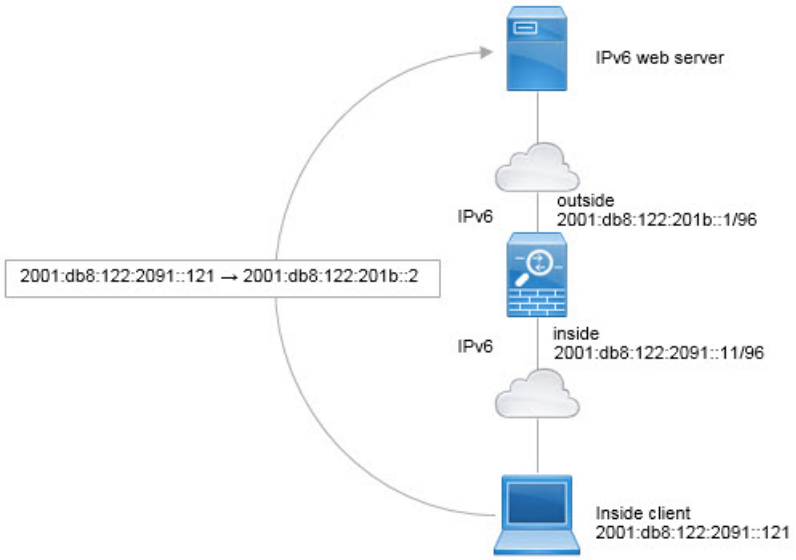
d) Click **OK**.

With this rule, any traffic from the 2001:db8:122:2091::/96 subnet on the inside interface going to the outside interface gets a static NAT66 translation to an address on the 2001:db8:122:2999::/96 network.

NAT66 Example, Simple IPv6 Interface PAT

A simple approach for implementing NAT66 is to dynamically assign internal addresses to different ports on the outside interface IPv6 address.

However, you cannot configure interface PAT using the IPv6 address of an interface using the Firewall Device Manager. Instead, use a single free address on the same network as a dynamic PAT pool.



Note This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

Procedure

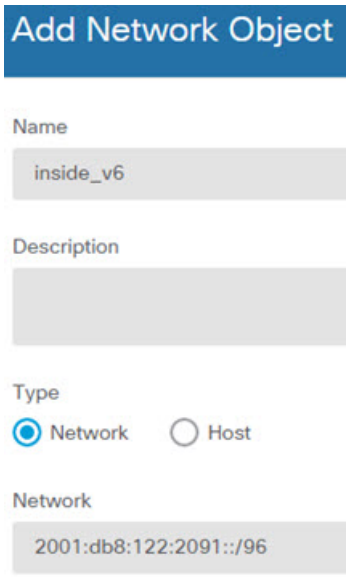
Step 1 Create the network objects that define the inside IPv6 network and the IPv6 PAT address.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the inside IPv6 network.

Name the network object (for example, inside_v6), select **Network**, and enter the network address, 2001:db8:122:2091::/96.



d) Click **OK**.

e) Click + and define the outside IPv6 PAT address.

Name the network object (for example, ipv6_pat), select **Host**, and enter the host address 2001:db8:122:201b::2.



Step 2 Configure the dynamic PAT rule for the inside IPv6 network.

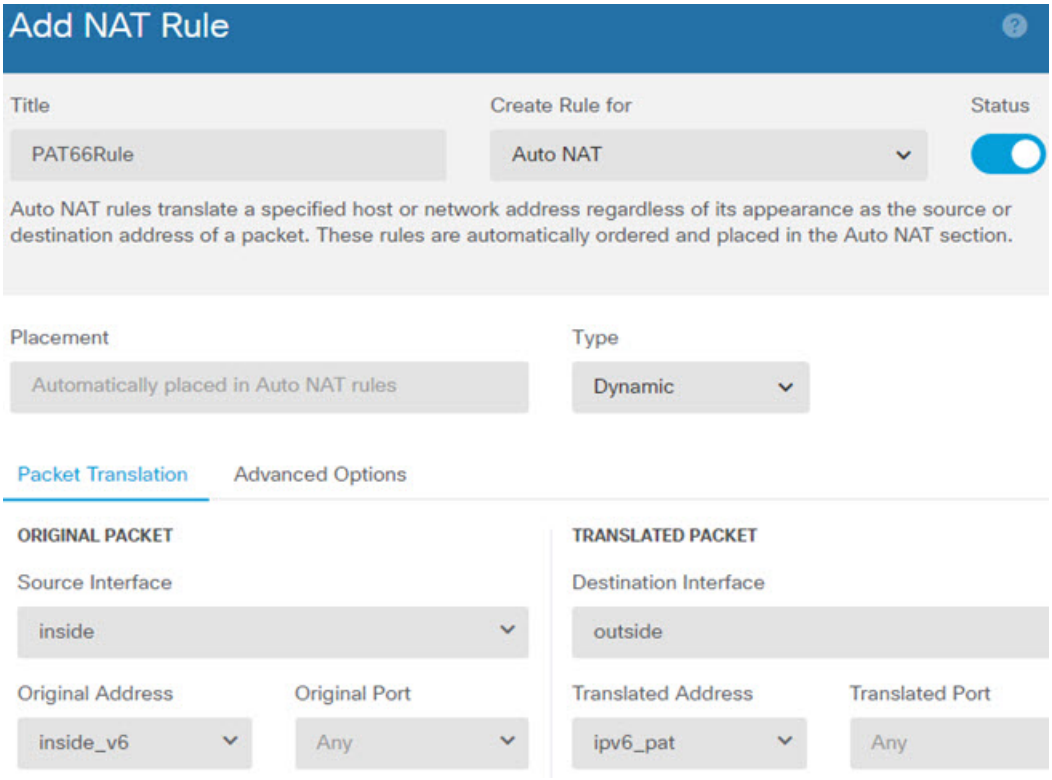
a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = PAT66Rule (or another name of your choosing).
- **Create Rule For** = Auto NAT.

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = inside_v6 network object.
- **Translated Address** = ipv6_pat network object.



d) Click **OK**.

With this rule, any traffic from the 2001:db8:122:2091::/96 subnet on the inside interface going to the outside interface gets a dynamic PAT66 translation to a port on 2001:db8:122:201b::2.

Monitoring NAT

To monitor and troubleshoot NAT connections, open the CLI console or log into the device CLI and use the following commands.

- **show nat** displays the NAT rules and per-rule hit counts. There are additional keywords to show other aspects of NAT.
- **show xlate** displays the actual NAT translations that are currently active.

- **clear xlate** lets you remove an active NAT translation. You might need to remove active translations if you alter NAT rules, because existing connections continue to use the old translation slot until the connection ends. Clearing a translation allows the system to build a new translation for a client on the client's next connection attempt based on your new rules. (You cannot use this command in the CLI console.)

Examples for NAT

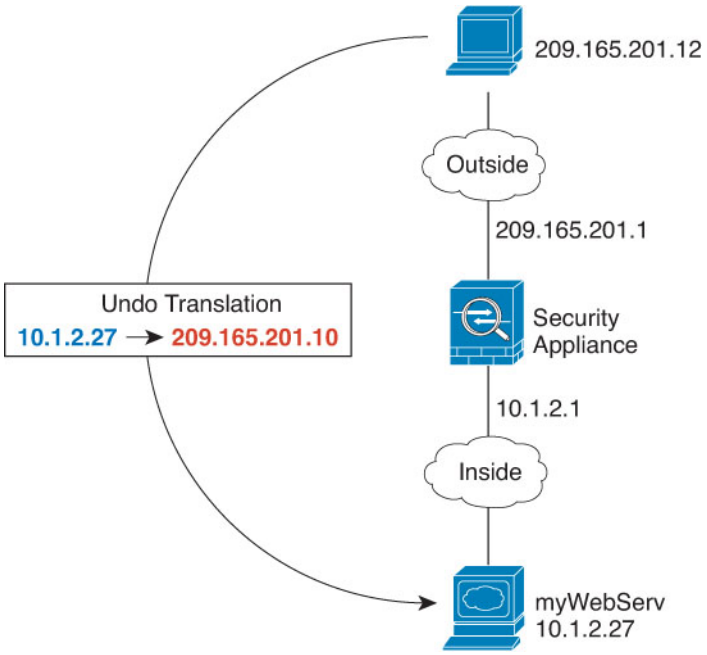
The following topics provide examples for configuring NAT on Threat Defense devices.

Providing Access to an Inside Web Server (Static Auto 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.

Note This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, select the specific bridge group member interface to which the web server is attached, for example, inside1_3.

Figure 13: Static NAT for an Inside Web Server



Procedure

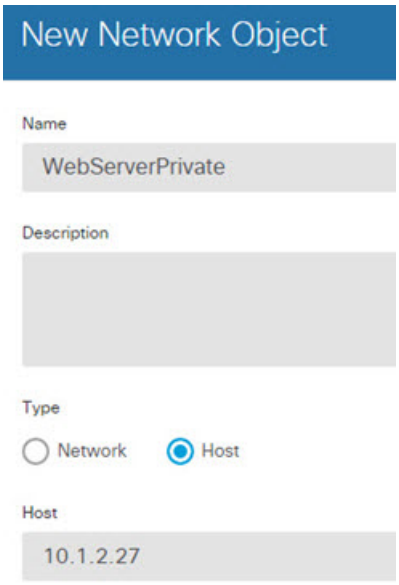
Step 1 Create the network objects that define the server's private and public host addresses.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the web server's private address.

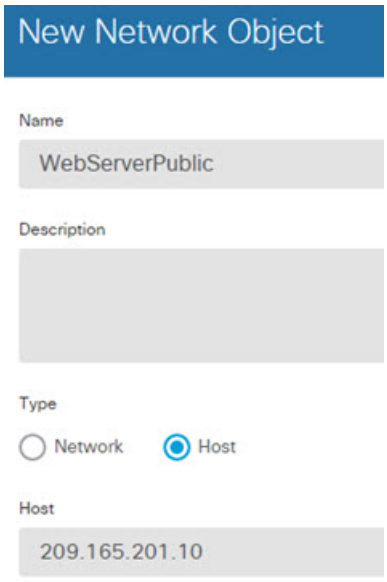
Name the network object (for example, WebServerPrivate), select **Host**, and enter the real host IP address, 10.1.2.27.



d) Click **OK**.

e) Click + and define the public address.

Name the network object (for example, WebServerPublic), select **Host**, and enter the host address 209.165.201.10.

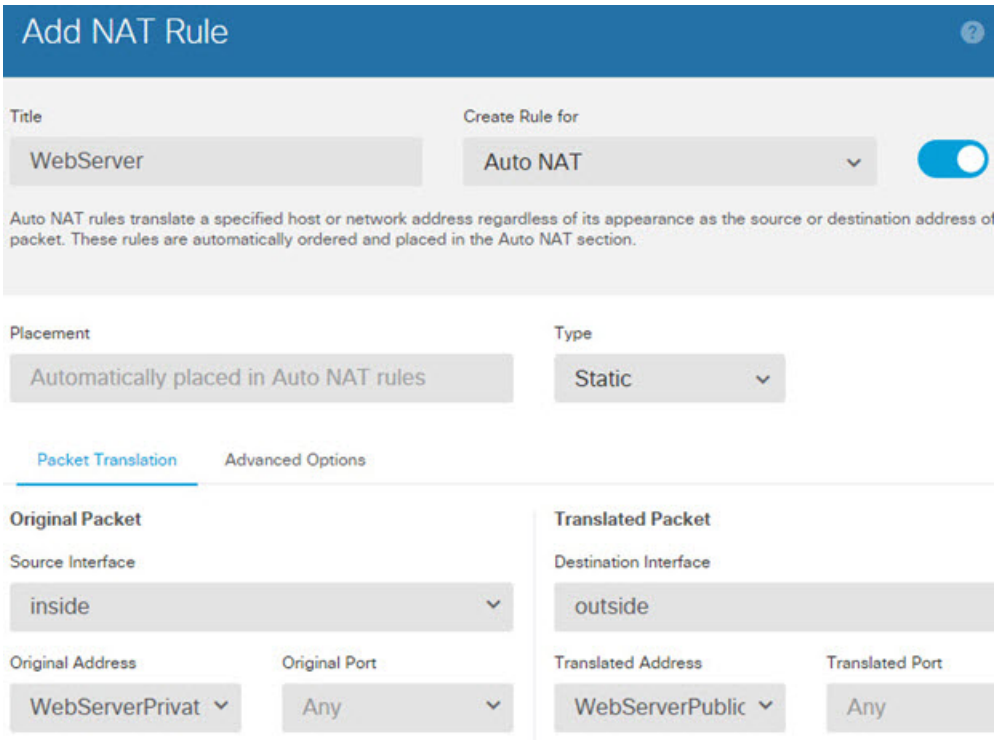


f) Click **OK**.

Step 2 Configure static NAT for the object.

a) Select **Policies** > **NAT**.
b) Click the + button.
c) Configure the following properties:

- **Title** = WebServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = WebServerPrivate network object.
- **Translated Address** = WebServerPublic network object.



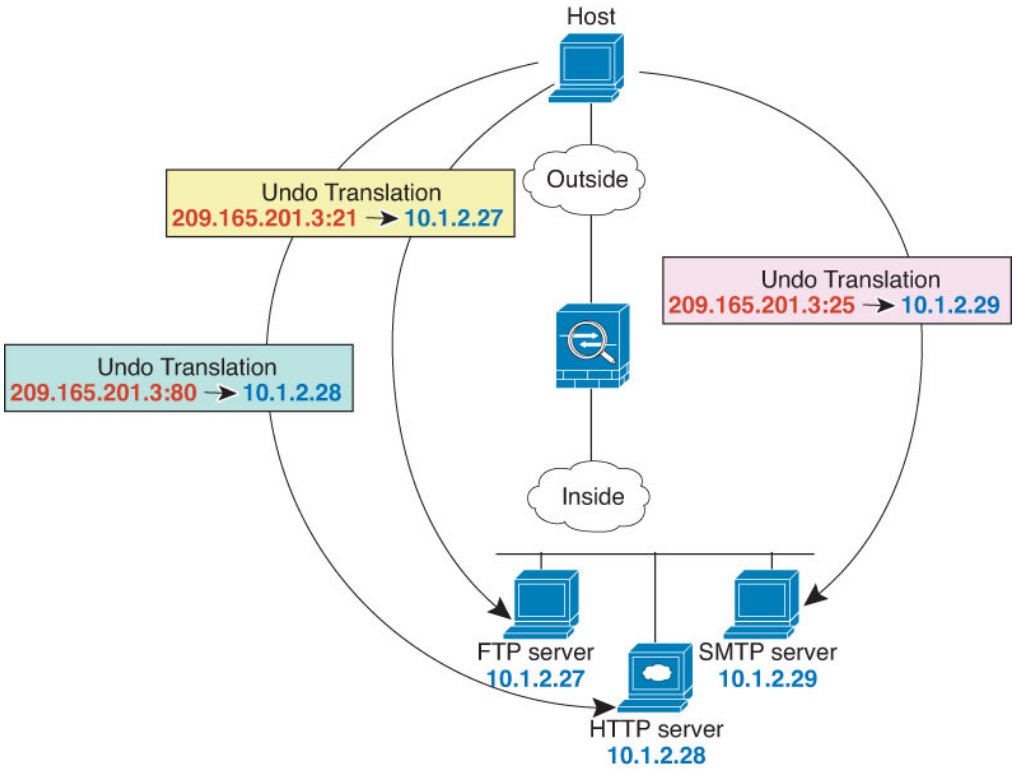
d) Click **OK**.

Single Address for FTP, HTTP, and SMTP (Static Auto 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.

Note This example assumes that the inside interface is a standard routed interface attached to a switch, with the servers attached to the switch. If your inside interface is a bridge group interface (BVI), and the servers are attached to separate bridge group member interfaces, select the specific member interface to which each server is attached for the corresponding rule. For example, the rules might have inside1_2, inside1_3, and inside1_4 for the source interface rather than inside.

Figure 14: Static NAT-with-Port-Translation



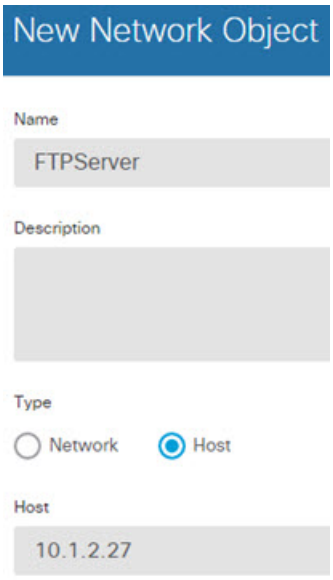
Procedure

Step 1 Create a network object for the FTP server.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Name the network object (for example, FTPserver), select **Host**, and enter the real IP address for the FTP server, 10.1.2.27.

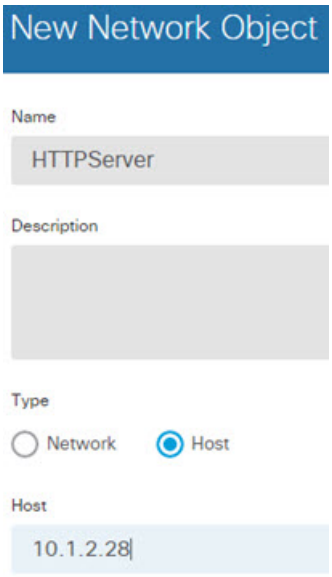


d) Click **OK**.

Step 2 Create a network object for the HTTP server.

a) Click **+**.

b) Name the network object (for example, HTTPserver), select **Host**, and enter the host address 10.1.2.28.

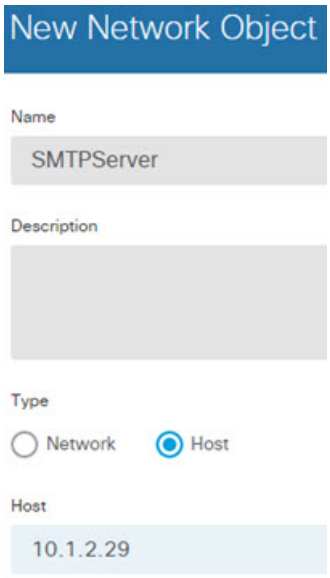


c) Click **OK**.

Step 3 Create a network object for the SMTP server.

a) Click **+**.

b) Name the network object (for example, SMTPserver), select **Host**, and enter the host address 10.1.2.29.

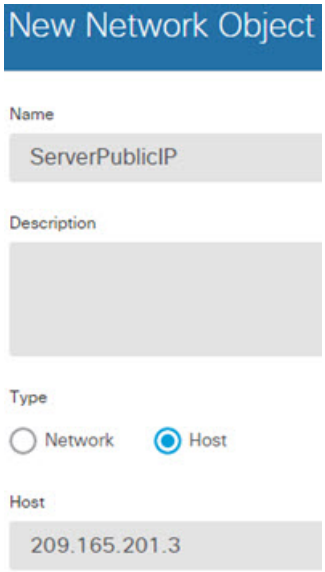


c) Click **OK**.

Step 4 Create a network object for the public IP address used for the three servers.

a) Click +.

b) Name the network object (for example, ServerPublicIP), select **Host**, and enter the host address 209.165.201.3.



c) Click **OK**.

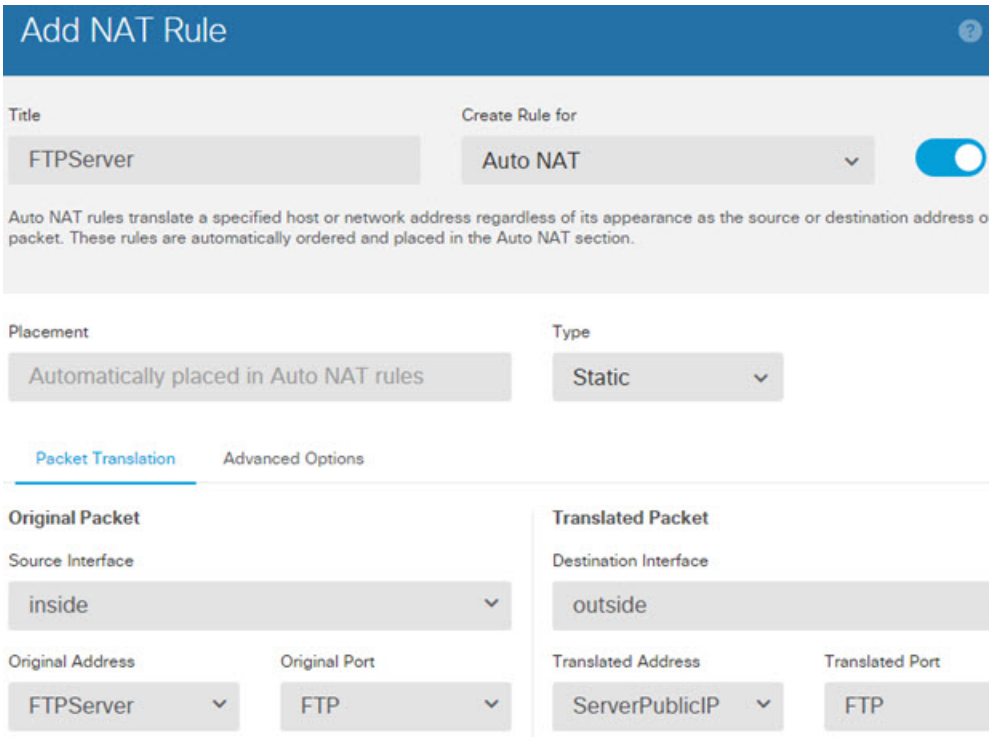
Step 5 Configure static NAT with port translation for the FTP server, mapping the FTP port to itself.

a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = FTPServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = FTPserver network object.
- **Translated Address** = ServerPublicIP network object.
- **Original Port** = FTP port object.
- **Translated Port** = FTP port object.



d) Click **OK**.

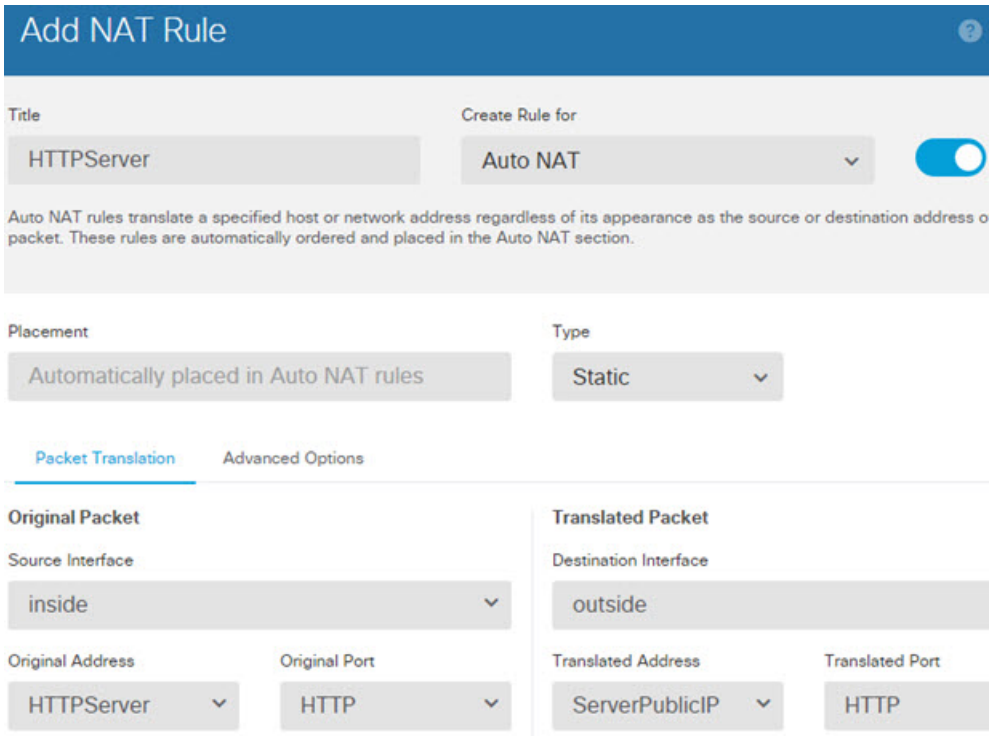
Step 6 Configure static NAT with port translation for the HTTP server, mapping the HTTP port to itself.

a) Click the + button.

b) Configure the following properties:

- **Title** = HTTPServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.

- **Original Address** = HTTPserver network object.
- **Translated Address** = ServerPublicIP network object.
- **Original Port** = HTTP port object.
- **Translated Port** = HTTP port object.



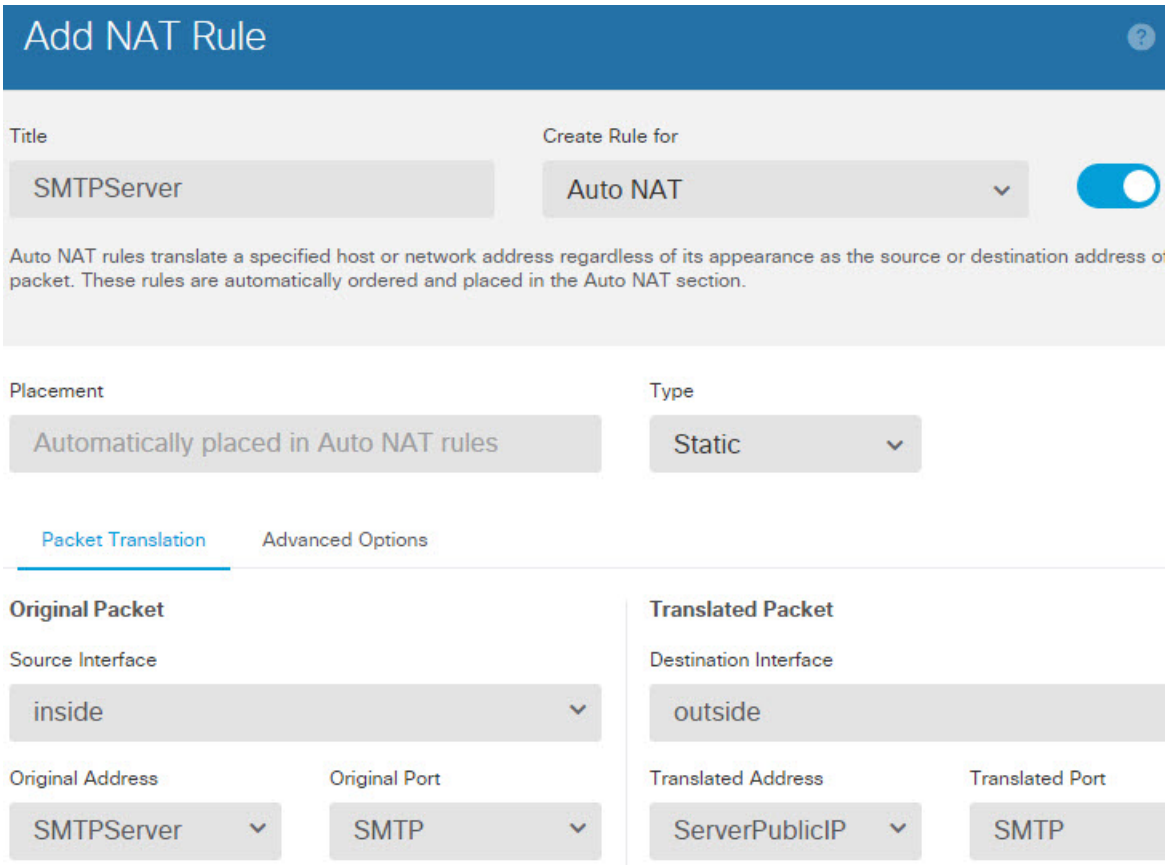
c) Click **OK**.

Step 7 Configure static NAT with port translation for the SMTP server, mapping the SMTP port to itself.

a) Click the + button.

b) Configure the following properties:

- **Title** = SMTPServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = SMTPserver network object.
- **Translated Address** = ServerPublicIP network object.
- **Original Port** = SMTP port object.
- **Translated Port** = SMTP port object.



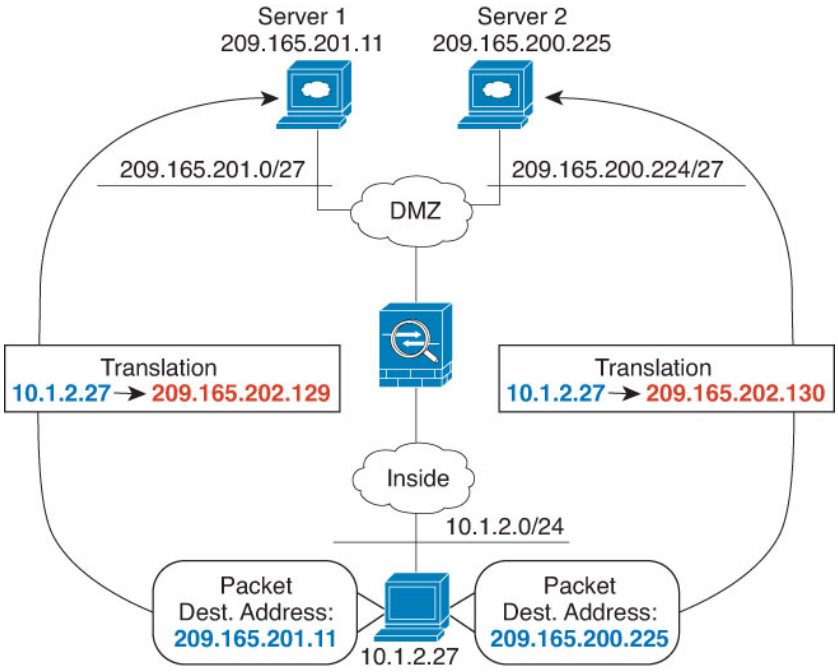
c) Click **OK**.

Different Translation Depending on the Destination (Dynamic Manual PAT)

The following figure shows a host on the 10.1.2.0/24 network accessing two different servers. When the host accesses the server at 209.165.201.11, the real address is translated to 209.165.202.129:*port*. When the host accesses the server at 209.165.200.225, the real address is translated to 209.165.202.130:*port*.

Note This example assumes that the inside interface is a standard routed interface attached to a switch, with the servers attached to the switch. If your inside interface is a bridge group interface (BVI), and the servers are attached to separate bridge group member interfaces, select the specific member interface to which each server is attached for the corresponding rule. For example, the rules might have inside1_2 and inside1_3 for the source interface rather than inside.

Figure 15: Manual NAT with Different Destination Addresses



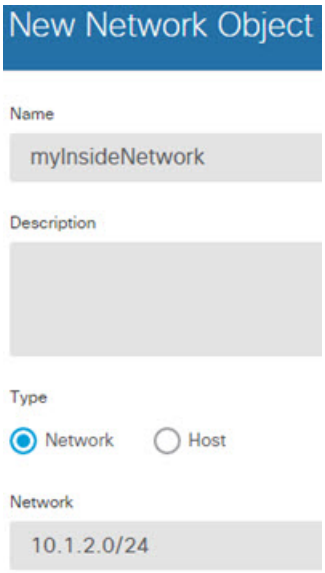
Procedure

Step 1 Create a network object for the inside network.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Name the network object (for example, myInsideNetwork), select **Network**, and enter the real network address, 10.1.2.0/24.

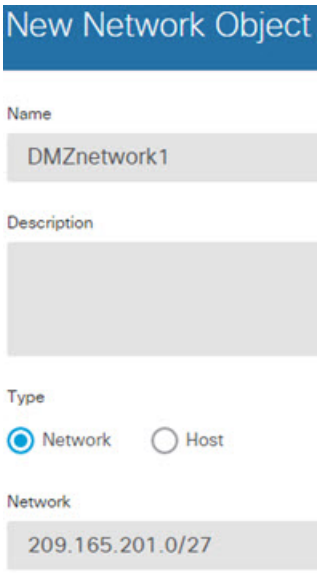


d) Click **OK**.

Step 2 Create a network object for the DMZ network 1.

a) Click +.

b) Name the network object (for example, DMZnetwork1), select **Network**, and enter the network address 209.165.201.0/27 (subnet mask of 255.255.255.224).

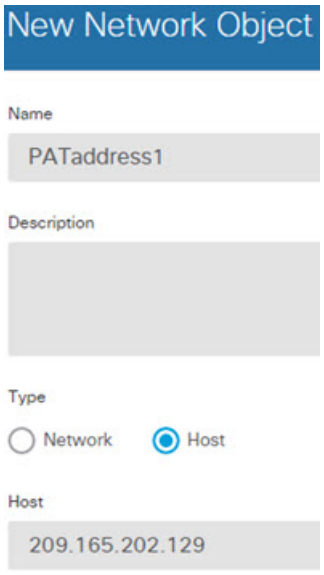


c) Click **OK**.

Step 3 Create a network object for the PAT address for DMZ network 1.

a) Click +.

b) Name the network object (for example, PATaddress1), select **Host**, and enter the host address 209.165.202.129.

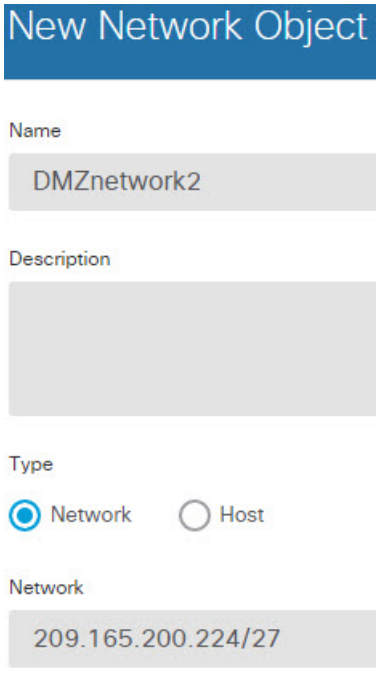


c) Click **OK**.

Step 4 Create a network object for the DMZ network 2.

a) Click +.

b) Name the network object (for example, DMZnetwork2), select **Network**, and enter the network address 209.165.200.224/27 (subnet mask of 255.255.255.224).

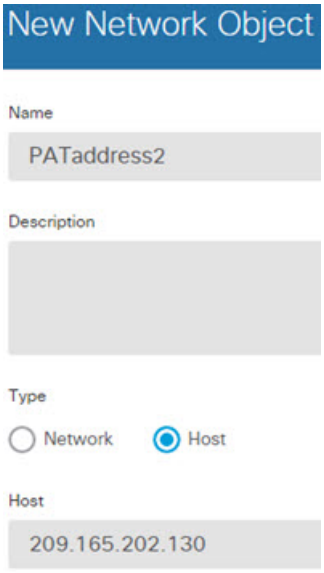


c) Click **OK**.

Step 5 Create a network object for the PAT address for DMZ network 2.

a) Click +.

b) Name the network object (for example, PATaddress2), select **Host**, and enter the host address 209.165.202.130.



c) Click **OK**.

Step 6 Configure dynamic manual PAT for DMZ network 1.

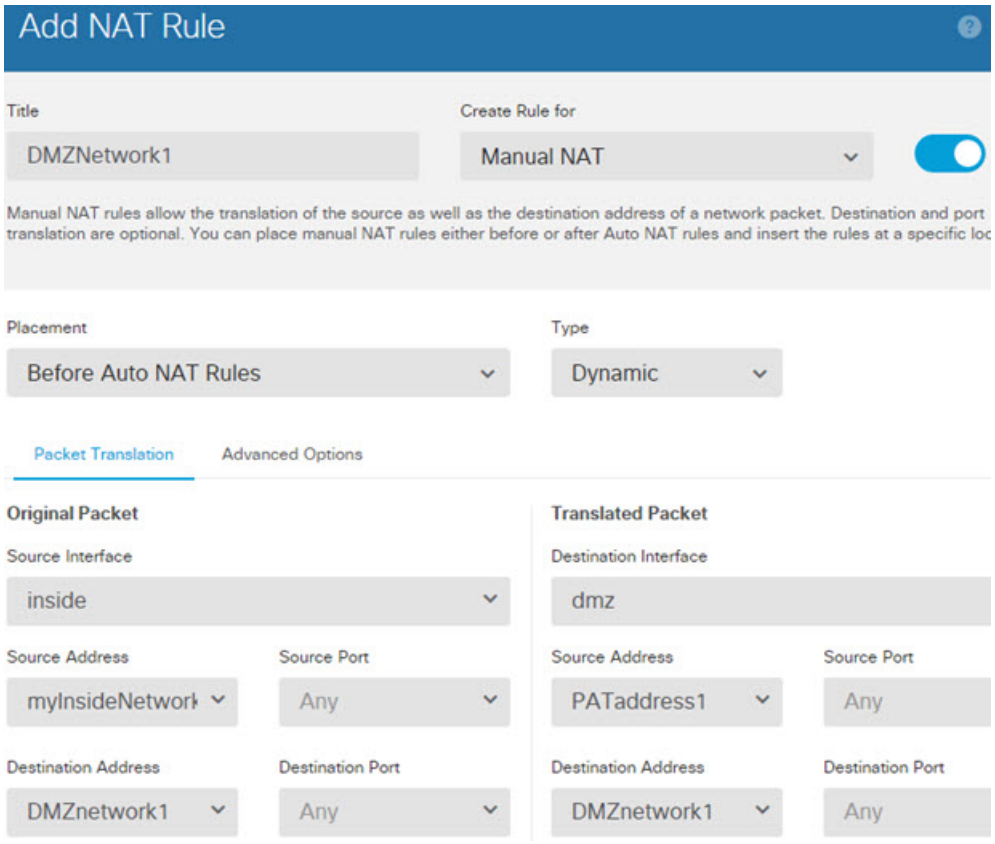
a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = DMZNetwork1 (or another name of your choosing).
- **Create Rule For** = Manual NAT.
- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source Address** = myInsideNetwork network object.
- **Translated Source Address** = PATaddress1 network object.
- **Original Destination Address** = DMZnetwork1 network object.
- **Translated Destination Address** = DMZnetwork1 network object.

Note
Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank.



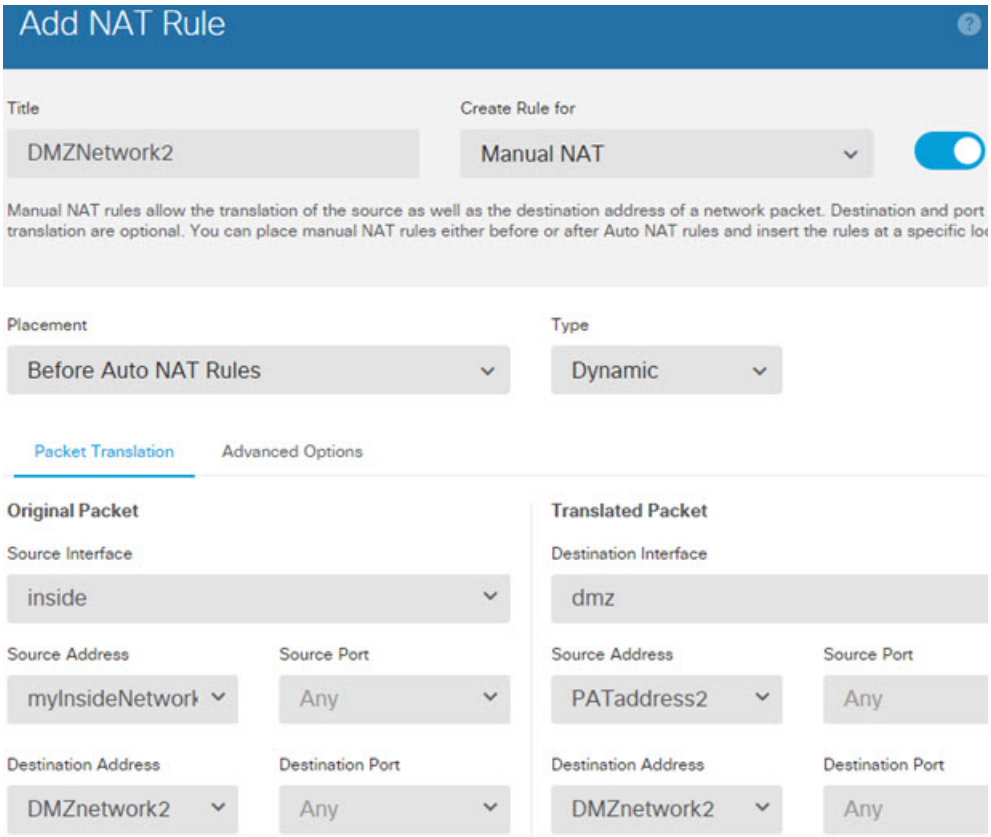
d) Click **OK**.

Step 7 Configure dynamic manual PAT for DMZ network 2.

a) Click the + button.

b) Configure the following properties:

- **Title** = DMZNetwork2 (or another name of your choosing).
- **Create Rule For** = Manual NAT.
- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source Address** = myInsideNetwork network object.
- **Translated Source Address** = PATaddress2 network object.
- **Original Destination Address** = DMZnetwork2 network object.
- **Translated Destination Address** = DMZnetwork2 network object.



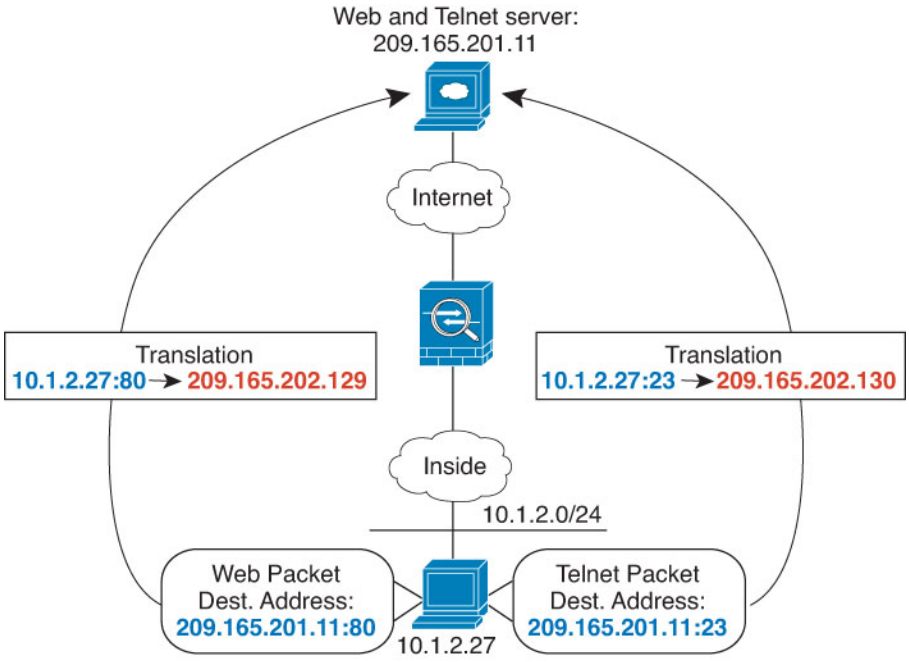
c) Click **OK**.

Different Translation Depending on the Destination Address and Port (Dynamic Manual PAT)

The following figure shows the use of source and destination ports. The host on the 10.1.2.0/24 network accesses a single host for both web services and Telnet services. When the host accesses the server for Telnet services, the real address is translated to 209.165.202.129:*port*. When the host accesses the same server for web services, the real address is translated to 209.165.202.130:*port*.

Note This example assumes that the inside interface is a standard routed interface attached to a switch, with the server attached to the switch. If your inside interface is a bridge group interface (BVI), and the server is attached to a bridge group member interface, select the specific member interface to which the server is attached. For example, the rule might have inside1_2 for the source interface rather than inside.

Figure 16: Manual NAT with Different Destination Ports



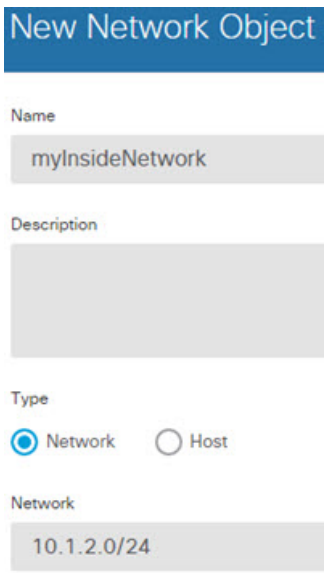
Procedure

Step 1 Create a network object for the inside network.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Name the network object (for example, myInsideNetwork), select **Network**, and enter the real network address, 10.1.2.0/24.

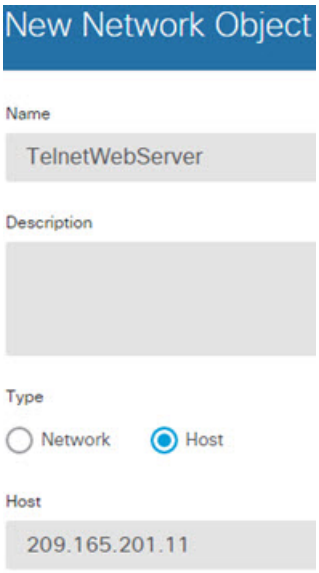


d) Click **OK**.

Step 2 Create a network object for the Telnet/Web server.

a) Click +.

b) Name the network object (for example, TelnetWebServer), select **Host**, and enter the host address 209.165.201.11.

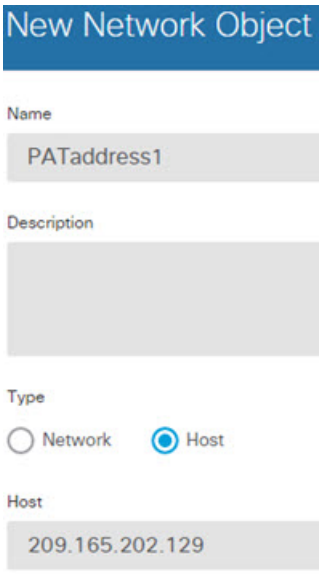


c) Click **OK**.

Step 3 Create a network object for the PAT address when using Telnet.

a) Click +.

b) Name the network object (for example, PATaddress1), select **Host**, and enter the host address 209.165.202.129.

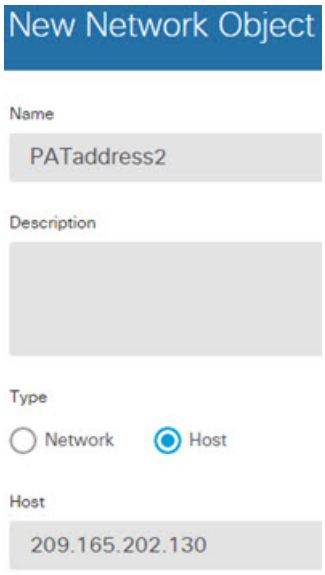


c) Click **OK**.

Step 4 Create a network object for the PAT address when using HTTP.

a) Click +.

b) Name the network object (for example, PATaddress2), select **Host**, and enter the host address 209.165.202.130.



c) Click **OK**.

Step 5 Configure dynamic manual PAT for Telnet access.

a) Select **Policies** > **NAT**.

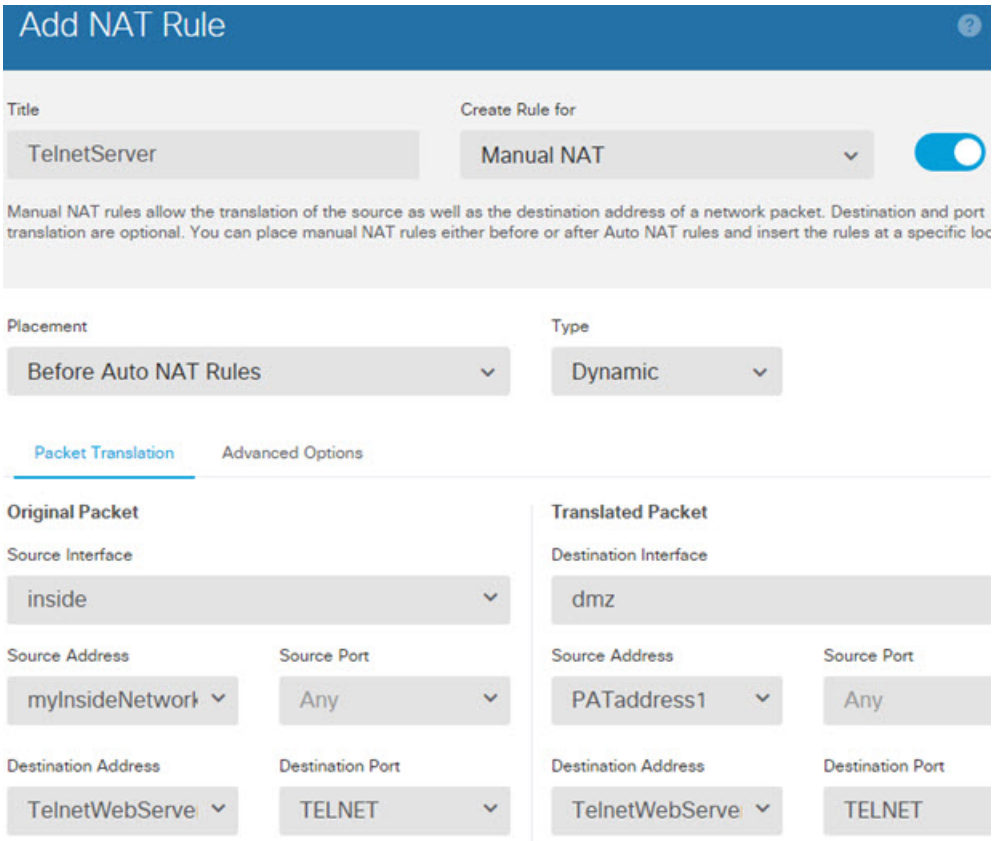
b) Click the + button.

c) Configure the following properties:

- **Title** = TelnetServer (or another name of your choosing).
- **Create Rule For** = Manual NAT.
- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source Address** = myInsideNetwork network object.
- **Translated Source Address**= PATaddress1 network object.
- **Original Destination Address** = TelnetWebServer network object.
- **Translated Destination Address** = TelnetWebServer network object.
- **Original Destination Port** = TELNET port object.
- **Translated Destination Port** = TELNET port object.

Note

Because you do not want to translate the destination address or port, you need to configure identity NAT for them by specifying the same address for the original and translated destination addresses, and the same port for the original and translated port.



d) Click **OK**.

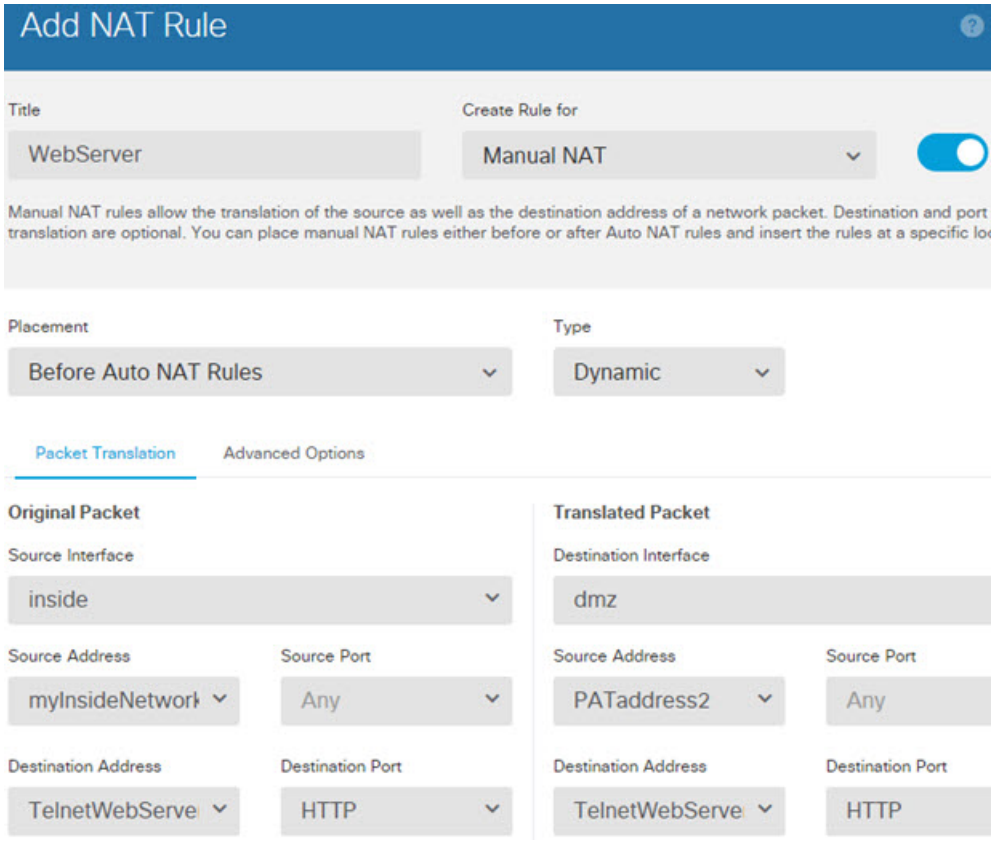
Step 6 Configure dynamic manual PAT for web access.

a) Click the + button.

b) Configure the following properties:

- **Title** = WebServer (or another name of your choosing).
- **Create Rule For** = Manual NAT.
- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source Address** = myInsideNetwork network object.
- **Translated Source Address** = PATaddress2 network object.
- **Original Destination Address** = TelnetWebServer network object.
- **Translated Destination Address** = TelnetWebServer network object.

- **Original Destination Port** = HTTP port object.
- **Translated Destination Port** = HTTP port object.



c) Click **OK**.

Rewriting DNS queries and responses using NAT

You might need to configure the Firewall Threat Defense to modify DNS replies by replacing the address in the reply with an address that matches the NAT configuration. You can configure DNS modification when you configure each translation rule. DNS modification is also known as DNS doctoring.

This feature rewrites the address in DNS queries and replies that match a NAT rule (for example, the A record for IPv4, the AAAA record for IPv6, or the PTR record for reverse DNS queries). For DNS replies traversing from a mapped interface to any other interface, the record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the record is rewritten from the real value to the mapped value. This feature works with NAT44,NAT 66, NAT46, and NAT64.

Following are the main circumstances when you would need to configure DNS rewrite on a NAT rule.

- The rule is NAT64 or NAT46, and the DNS server is on the outside network. You need DNS rewrite to convert between DNS A records (for IPv4) and AAAA records (for IPv6).

- The DNS server is on the outside, clients are on the inside, and some of the fully-qualified domain names that the clients use resolve to other inside hosts.
- The DNS server is on the inside and responds with private IP addresses, clients are on the outside, and the clients access fully-qualified domain names that point to servers that are hosted on the inside.

DNS rewrite limitations

Following are some limitations with DNS rewrite:

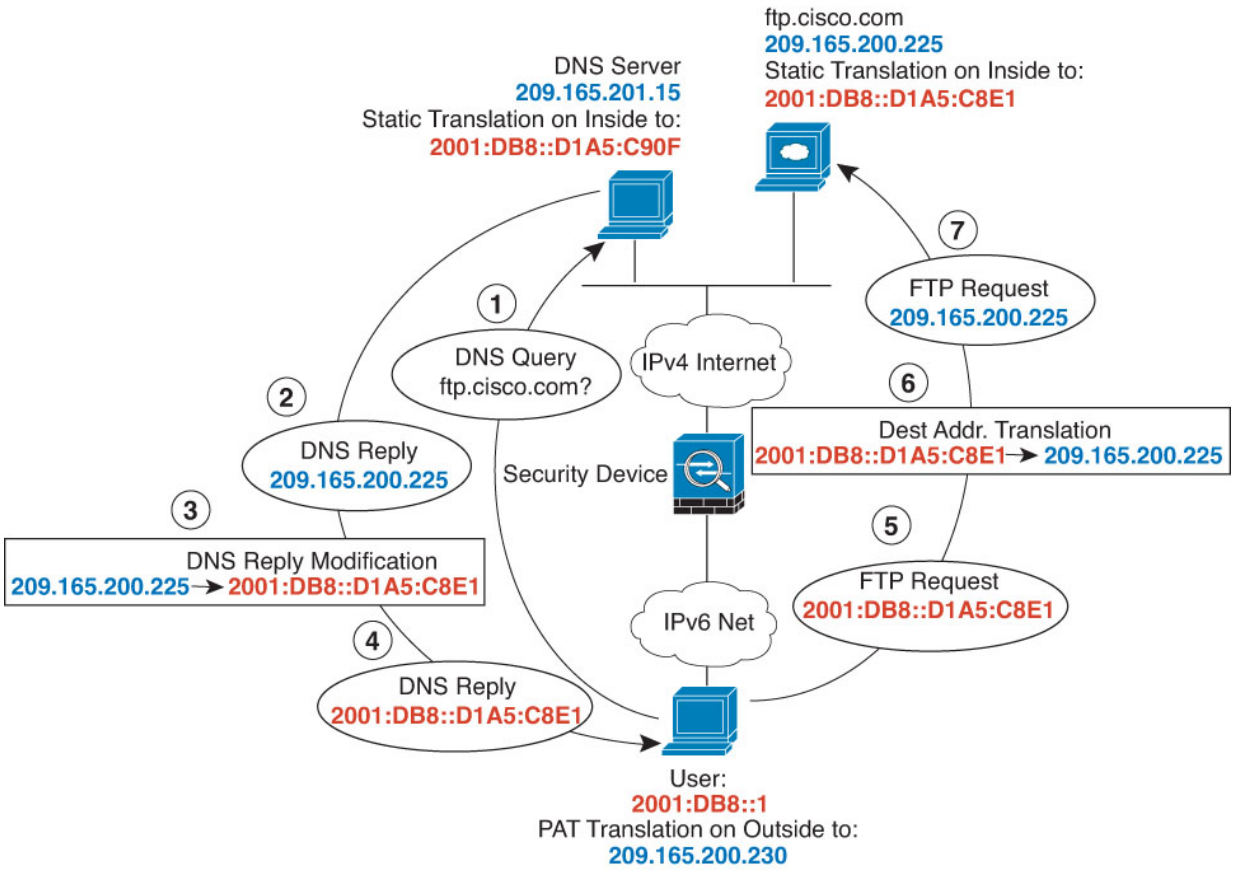
- DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A or AAAA record, and the PAT rule to use is ambiguous.
- If you configure a manual NAT rule, you cannot configure DNS modification if you specify the destination address as well as the source address. These kinds of rules can potentially have a different translation for a single address when going to A vs. B. Therefore, the can not accurately match the IP address inside the DNS reply to the correct twice NAT rule; the DNS reply does not contain information about which source/destination address combination was in the packet that prompted the DNS request.
- You must enable DNS application inspection with DNS NAT rewrite enabled for NAT rules to rewrite DNS queries and responses. By default, DNS inspection with DNS NAT rewrite enabled is globally applied, so you probably do not need to change the inspection configuration.
- DNS rewrite is actually done on the xlate entry, not the NAT rule. Thus, if there is no xlate for a dynamic rule, rewrite cannot be done correctly. The same problem does not occur for static NAT.
- DNS rewrite does not rewrite DNS Dynamic Update messages (opcode 5).

The following topics provide examples of DNS rewrite in NAT rules.

DNS 64 Reply Modification

The following figure shows an FTP server and DNS server on the outside IPv4 network. The system 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, where D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225) 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.



Note This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

Procedure

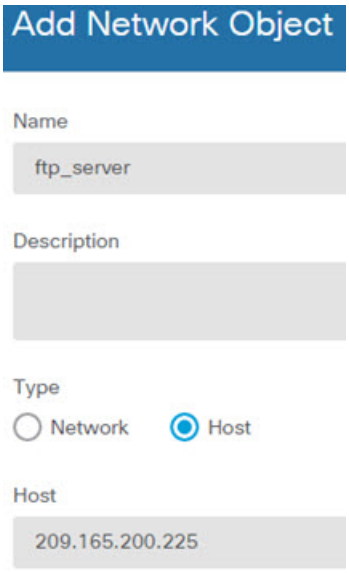
Step 1 Create the network objects for the FTP server, DNS server, inside network, and PAT pool.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the real FTP server address.

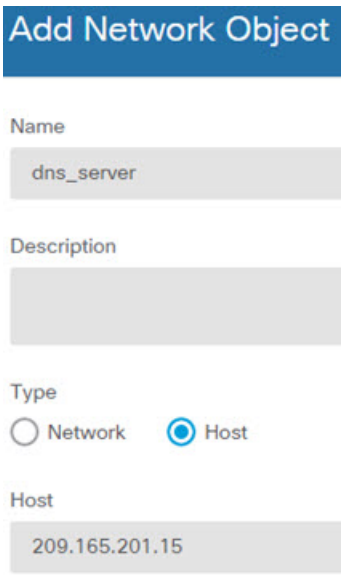
Name the network object (for example, ftp_server), select **Host**, and enter the real host IP address, 209.165.200.225.



d) Click **OK**.

e) Click + and define the DNS server's real address.

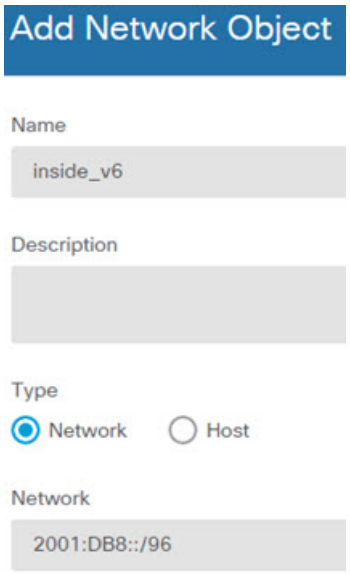
Name the network object (for example, dns_server), select **Host**, and enter the host address 209.165.201.15.



f) Click **OK**.

g) Click + and define the inside IPv6 network.

Name the network object (for example, inside_v6), select **Network**, and enter the network address, 2001:DB8::/96.



h) Click **OK**.

i) Click + and define the IPv4 PAT address for the inside IPv6 network.

Name the network object (for example, ipv4_pat), select **Host**, and enter the host address, 209.165.200.230.



j) Click **OK**.

Step 2 Configure the static NAT rule with DNS modification for the FTP server.

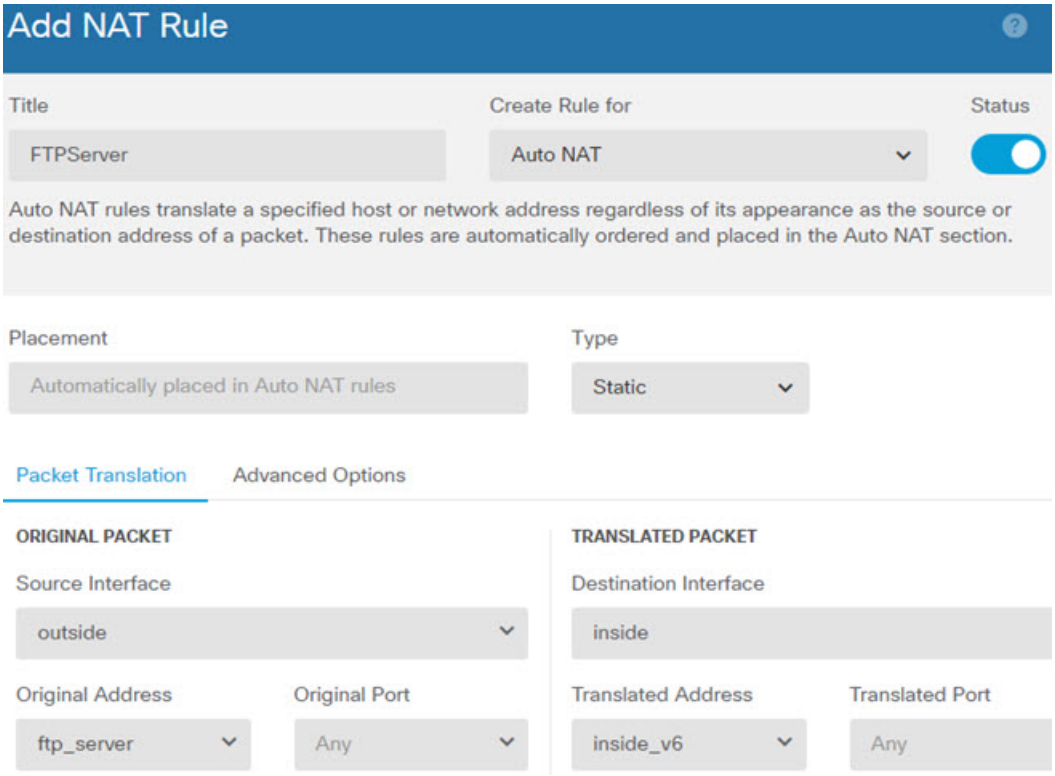
a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = FTPServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.

- **Type** = Static.
- **Source Interface** = outside.
- **Destination Interface** = inside.
- **Original Address** = ftp_server network object.
- **Translated Address** = inside_v6 network object. Because the IPv4 embedded address method is used when converting IPv4 to IPv6 addresses, 209.165.200.225 is converted to the IPv6 equivalent D1A5:C8E1 and the network prefix is added to get the full address, 2001:DB8::D1A5:C8E1.
- On the **Advanced Options** tab, select **Translate DNS replies that match this rule**.



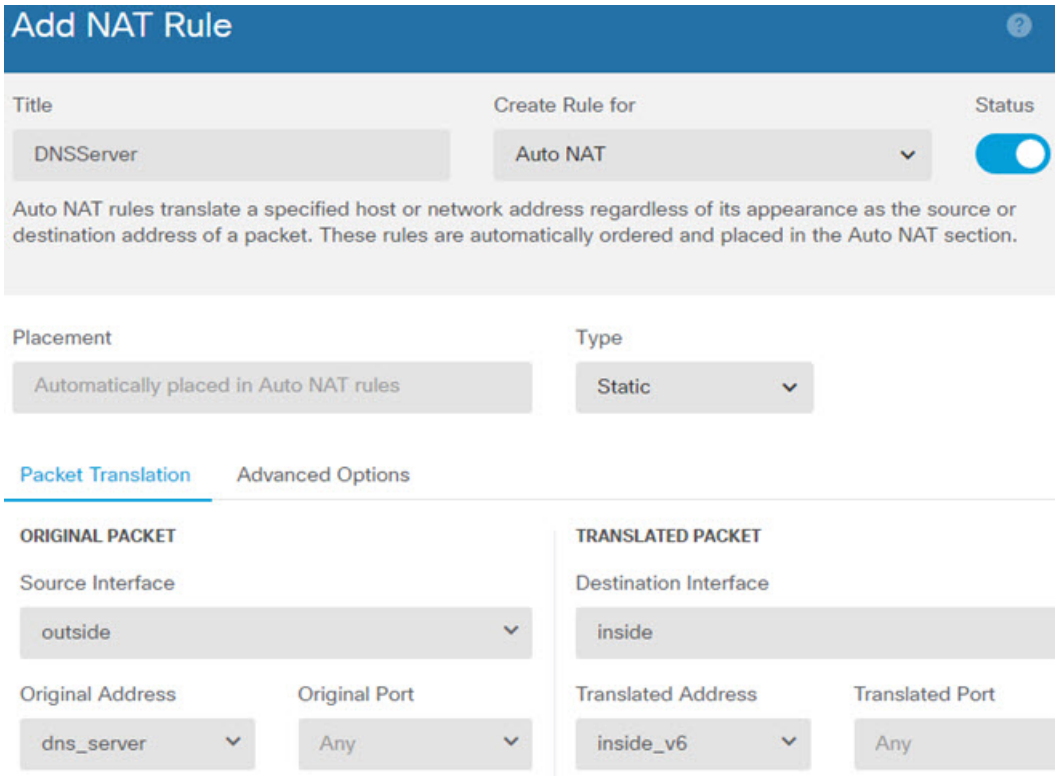
d) Click **OK**.

Step 3 Configure the static NAT rule for the DNS server.

a) Select **Policies** > **NAT**.
b) Click the + button.
c) Configure the following properties:

- **Title** = DNSServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Static.
- **Source Interface** = outside.
- **Destination Interface** = inside.

- **Original Address** = dns_server network object.
- **Translated Address** = inside_v6 network object. Because the IPv4 embedded address method is used when converting IPv4 to IPv6 addresses, 209.165.201.15 is converted to the IPv6 equivalent D1A5:C90F and the network prefix is added to get the full address, 2001:DB8::D1A5:C90F.

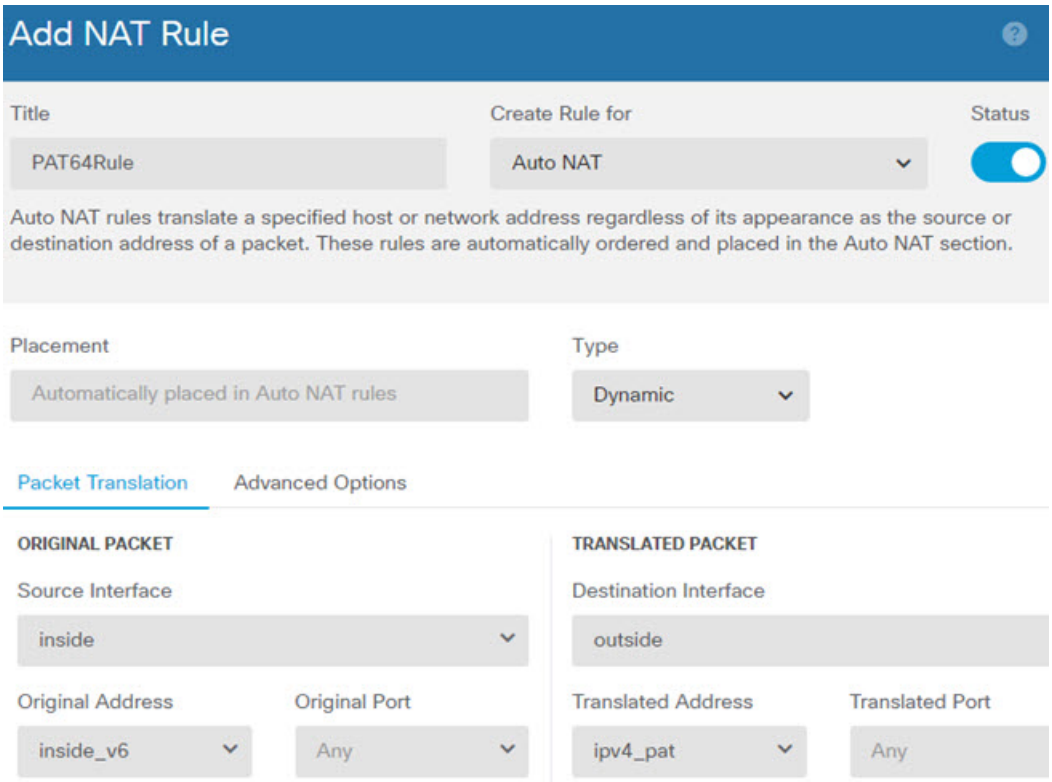


d) Click **OK**.

Step 4 Configure the dynamic PAT rule for the inside IPv6 network.

a) Select **Policies** > **NAT**.
b) Click the + button.
c) Configure the following properties:

- **Title** = PAT64Rule (or another name of your choosing).
- **Create Rule For** = Auto NAT.
- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = inside_v6 network object.
- **Translated Address** = ipv4_pat network object.



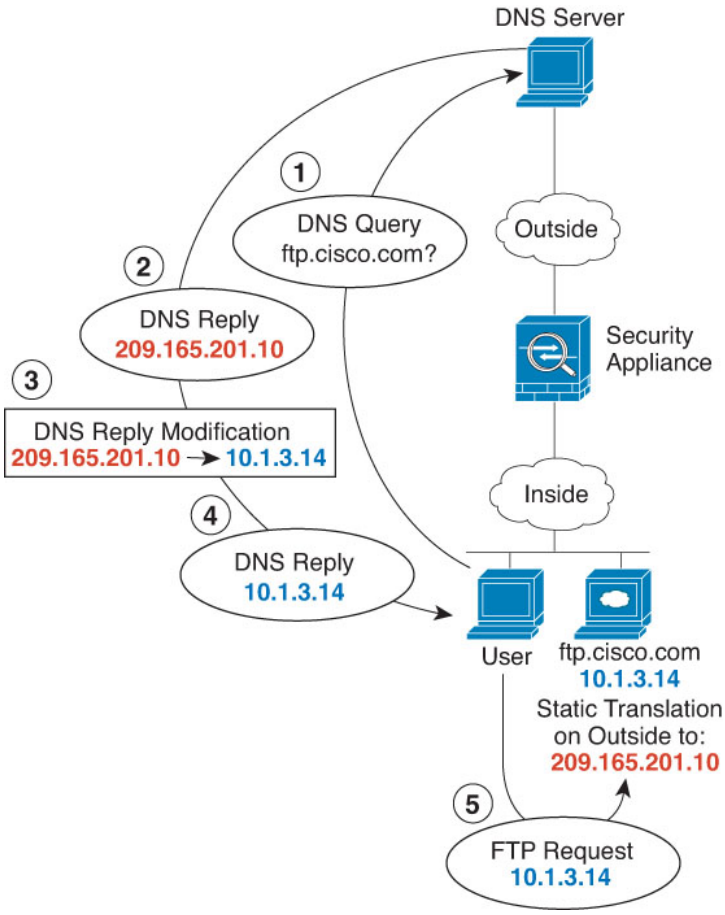
d) Click **OK**.

DNS Reply Modification, DNS Server on Outside

The following figure shows a DNS server that is accessible from the outside interface. A server, ftp.cisco.com, is on the inside interface. You configure NAT 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.

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 system 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.



Note This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

Procedure

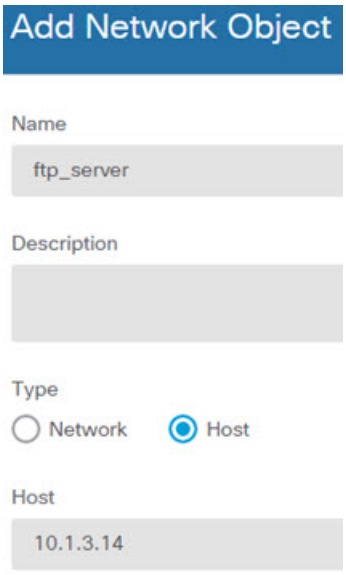
Step 1 Create the network objects for the FTP server.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the real FTP server address.

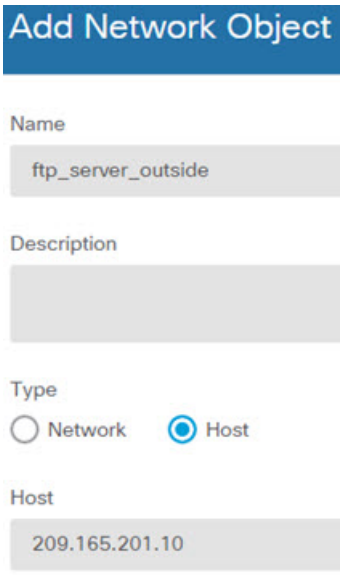
Name the network object (for example, ftp_server), select **Host**, and enter the real host IP address, 10.1.3.14.



d) Click **OK**.

e) Click + and define the FTP server's translated address.

Name the network object (for example, ftp_server_outside), select **Host**, and enter the host address 209.165.201.10.



Step 2 Configure the static NAT rule with DNS modification for the FTP server.

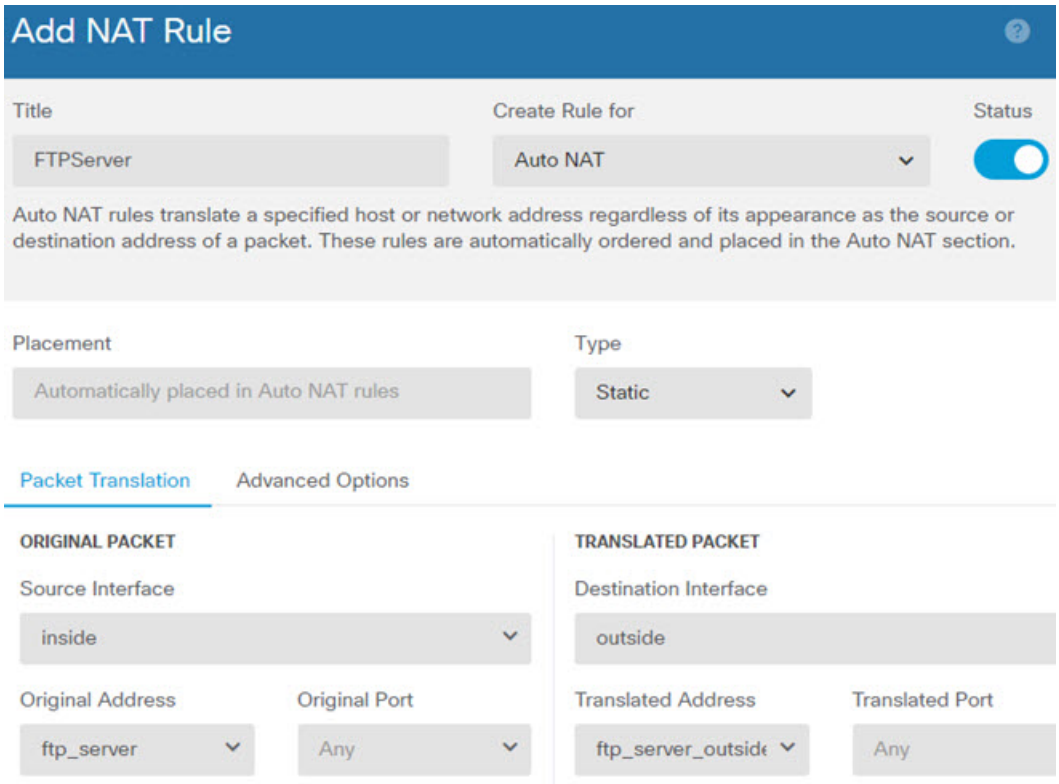
a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = FTPServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.

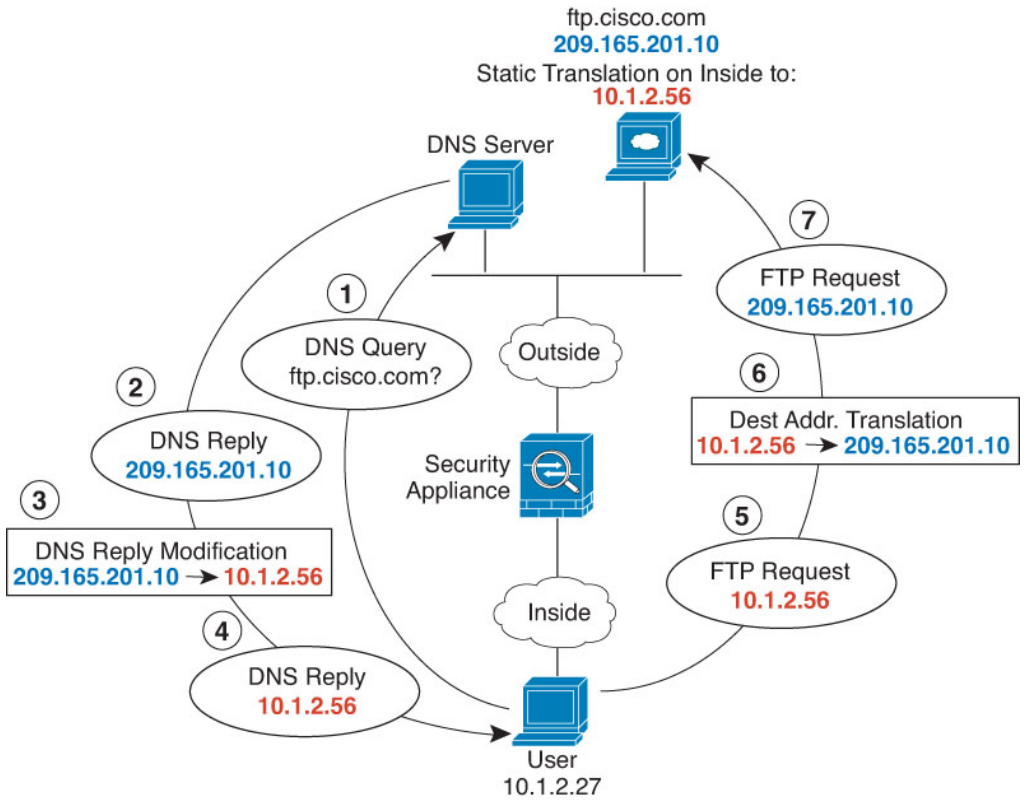
- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Address** = ftp_server network object.
- **Translated Address** = ftp_server_outside network object.
- On the **Advanced Options** tab, select **Translate DNS replies that match this rule**.



d) Click **OK**.

DNS Reply Modification, DNS Server on Host Network

The following figure shows an FTP server and DNS server on the outside. The system 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, 209.165.20.10. 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.



Note This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

Procedure

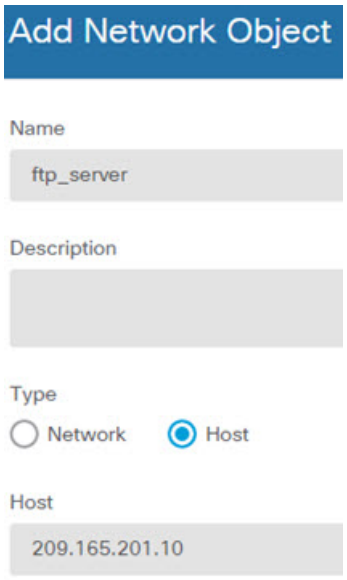
Step 1 Create the network objects for the FTP server.

a) Choose **Objects**.

b) Select **Network** from the table of contents and click +.

c) Define the real FTP server address.

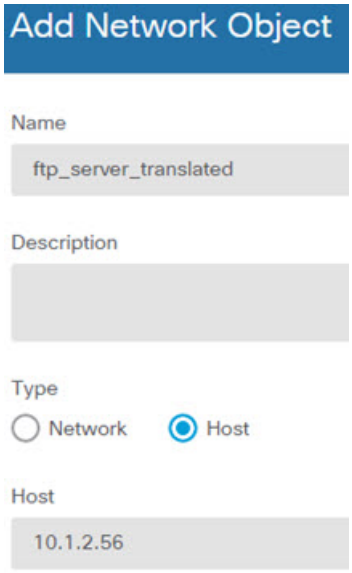
Name the network object (for example, ftp_server), select **Host**, and enter the real host IP address, 209.165.201.10.



d) Click **OK**.

e) Click + and define the FTP server's translated address.

Name the network object (for example, ftp_server_translated), select **Host**, and enter the host address 10.1.2.56.



Step 2 Configure the static NAT rule with DNS modification for the FTP server.

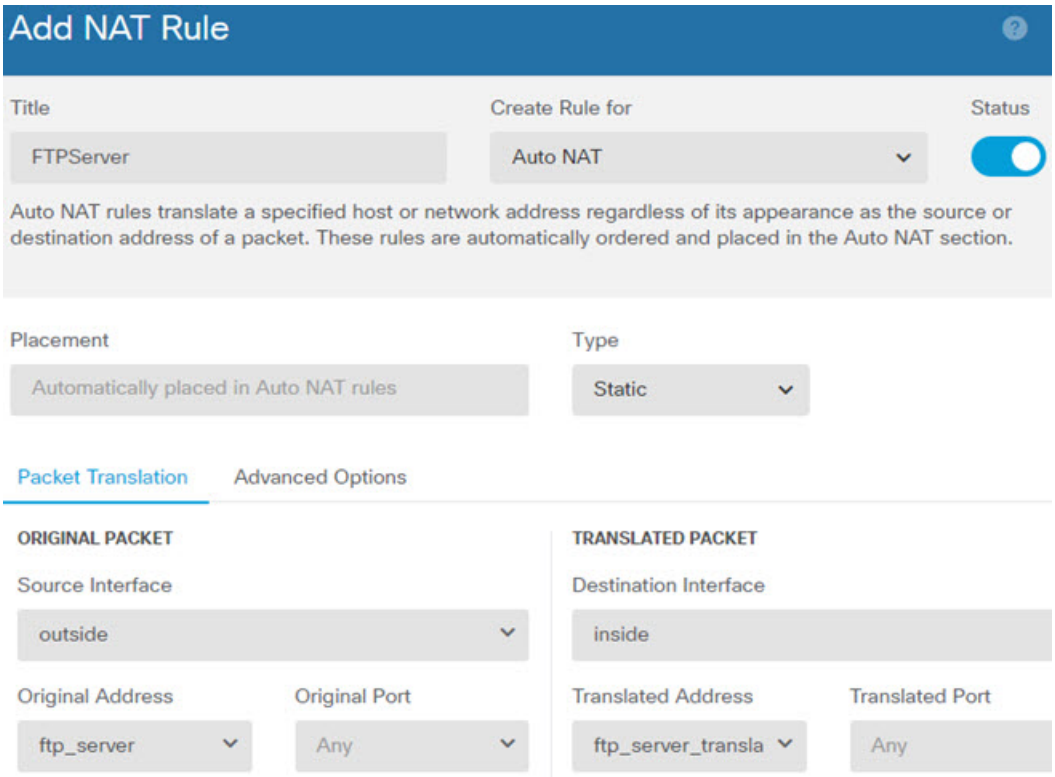
a) Select **Policies** > **NAT**.

b) Click the + button.

c) Configure the following properties:

- **Title** = FTPServer (or another name of your choosing).
- **Create Rule For** = Auto NAT.

- **Type** = Static.
- **Source Interface** = outside.
- **Destination Interface** = inside.
- **Original Address** = ftp_server network object.
- **Translated Address** = ftp_server_translated network object.
- On the **Advanced Options** tab, select **Translate DNS replies that match this rule**.



d) Click **OK**.