Network Address Translation (NAT)

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

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.

✎

（注） 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.

✎

（注） 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 （13 ページ） .

- 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 （19 ページ） .

- Static NAT—A consistent mapping between a real and mapped IP address. Allows bidirectional traffic initiation. See Static NAT （24 ページ） .

- 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 （33 ページ） .

NAT in Routed Mode

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

図 *1 : NAT Example: Routed Mode*
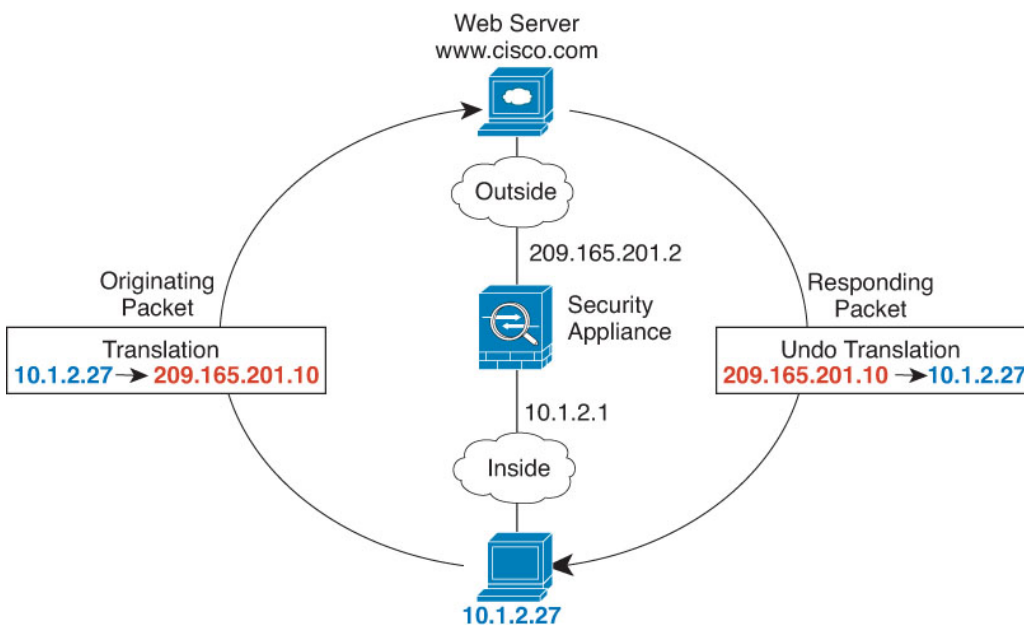
1. When the inside host at 10.1.2.27 sends a packet to a web server, the real source address of the packet, 10.1.2.27, is translated to a mapped address, 209.165.201.10.

2. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the FTD デバイス receives the packet because the FTD デバイス performs proxy ARP to claim the packet.

3. The FTD デバイス 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.

自動 NAT and 手動 NAT

You can implement address translation in two ways: 自動 *NAT* and 手動 *NAT*.

We recommend using 自動 NAT unless you need the extra features that 手動 NAT provides. It is easier to configure 自動 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.)

自動 **NAT**

All NAT rules that are configured as a parameter of a network object are considered to be 自動 *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 自動 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 手動 NAT for that kind of functionality, where you can identify the source and destination address in a single rule.

手動 **NAT**

手動 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.

（注） 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 自動 **NAT and** 手動 **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.

  • 手動 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 手動 NAT is more scalable.

• How source and destination NAT is implemented.

- 自動 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.

- 手動 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 手動 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.

  - 自動 NAT—Automatically ordered in the NAT table.

  - 手動 NAT—Manually ordered in the NAT table (before or after 自動 NAT rules).

NAT Rule Order

自動 NAT and 手動 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.

表 *1 : NAT Rule Table*

Table Section	Rule Type	Order of Rules within the Section
Section 1	手動 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, 手動 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.

Table Section	Rule Type	Order of Rules within the Section
Section 2	自動 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	手動 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.

図 *2 : Specifying Any Interface*
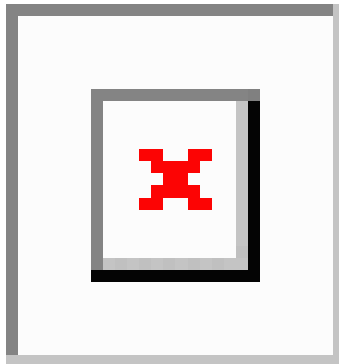
However, the concept of "any" interface does not apply to bridge group member interfaces. When you specify "any" interface, all bridge group member interfaces are excluded. Thus, to apply NAT to bridge group members, you must specify the member interface. This could result in many similar rules where only one interface is different. You cannot configure NAT for the Bridge Virtual Interface (BVI) itself, you can configure NAT for member interfaces only.

You cannot configure NAT on passive interfaces.

Configuring Routing for NAT

The FTD 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 FTD デバイス 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 FTD デバイス 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 FTD デバイス.

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 FTD デバイス will then proxy ARP for the address, even though the packet is not actually destined for the FTD デバイス. (Note that this problem occurs even if you have a 手動 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 FTD デバイス ARP response is received before the actual host ARP response, then traffic will be mistakenly sent to the FTD デバイス.

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.

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 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 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 (手動 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 (手動 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.

（注）　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.

表 *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
RTSP	TCP/554 (No handling for HTTP cloaking.)	No NAT64.	Yes
SIP	TCP/5060 UDP/5060	No extended PAT. No NAT64 or NAT46.	Yes

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
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

Additional Guidelines for NAT

- 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.

- (自動 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.

    （注）　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.

- (手動 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 FTD デバイス performs NAT on a packet, the packet must be IPv6-to-IPv6 or IPv4-to-IPv4; with this prerequisite, the FTD デバイス 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.

- (手動 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.

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.

手順

ステップ **1** Select **Policies** > **NAT**.

ステップ **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 （2 ページ）.

ステップ **3** Decide which rules should be implemented as manual or auto NAT.

For a comparison of these two implementation options, see 自動 NAT and 手動 NAT （3 ページ）.

ステップ **4** Create the rules as explained in the following sections.

- Dynamic NAT （13 ページ）

- Dynamic PAT （19 ページ）

- Static NAT （24 ページ）

- Identity NAT （33 ページ）

ステップ **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.

（注）　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.

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

図 **3 : Dynamic NAT**
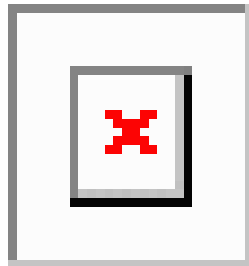
The following figure shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the packet is dropped.

図 **4 : Remote Host Attempts to Initiate a Connection to a Mapped Address**
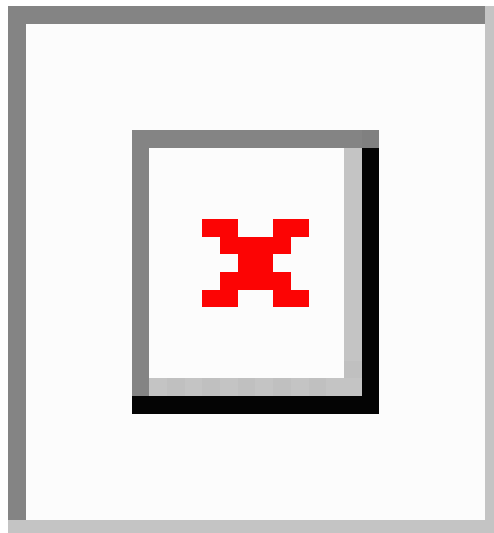
Dynamic NAT Disadvantages and Advantages

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.

始める前に

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.

手順

ステップ **1** Select **Policies** > **NAT**.

ステップ **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.)

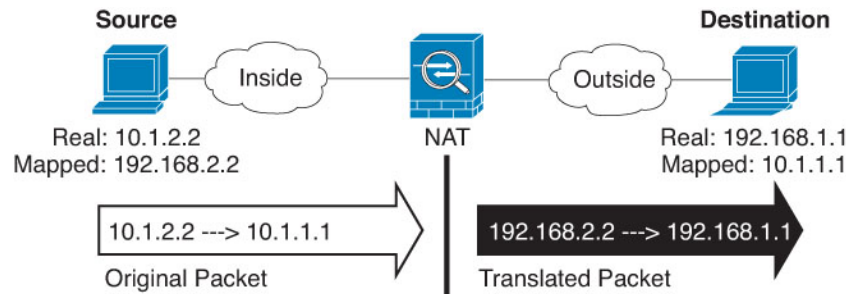ステップ **3** Configure the basic rule options:

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

ステップ **4** Configure the following packet translation options:

- **Source Interface**, **Destination Interface—**（ブリッジ グループ メンバー インターフェイス
  に必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のイ
  ンターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入りま
  す。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイ
  スを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグ
  ループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用され
  ます。
- **Original Address**—The network object that contains the addresses you are translating.
- **Translated Address**—The network object or group that contains the mapped addresses.

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

- **Translate DNS replies that match this rule**—DNS 応答の IP アドレスを変換するかどうかを
  指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS
  応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から
  実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインター
  フェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書
  き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと
  AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳
  細については、「NAT を使用した DNS クエリと応答の書き換え （76 ページ）」を参照
  してください。
- **Fallthrough to Interface PAT (Destination Interface)**—その他のマッピングアドレスがすで
  に割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式
  として使用するかどうかを指定します（インターフェイス PAT フォールバック）。この
  オプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場
  合にのみ使用できます。

ステップ 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.

始める前に

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.

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.

手順

ステップ 1 Select **Policies** > **NAT**.

ステップ 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.)

ステップ 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. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- **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.

ステップ 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。

- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、または
ネットワークグループ。

- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワークオブ
ジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されま
す。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単に
アイデンティティ NAT を使用できます。

[インターフェイス（Interface）][送信元インターフェイスIP（Source Interface IP）] を選択
して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにで
きます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要が
あります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を
実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択
します。

ステップ **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.

ステップ **7** （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original
Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original
Source Port）] フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空
白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポー
トに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービ
ス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じ
になるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実
際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

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

- **Translate DNS replies that match this rule**—DNS 応答の IP アドレスを変換するかどうかを
指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS
応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から

実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え（76 ページ）」を参照してください。

- **Fallthrough to Interface PAT (Destination Interface)**—その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 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.

図 **5 : Dynamic PAT**
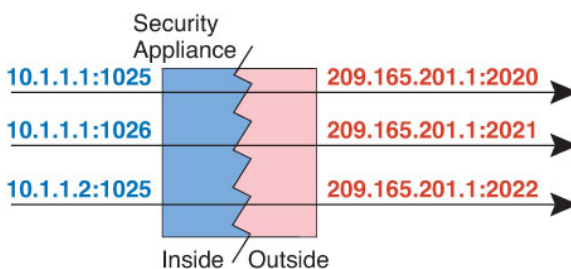
For the duration of the translation, a remote host on the destination network can initiate a connection to the translated host if an access rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

After the connection expires, the port translation also expires.

（注）　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 FTD デバイス 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 （9 ページ） .

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.

始める前に

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.

手順

ステップ 1 Select **Policies** > **NAT**.

ステップ 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.)
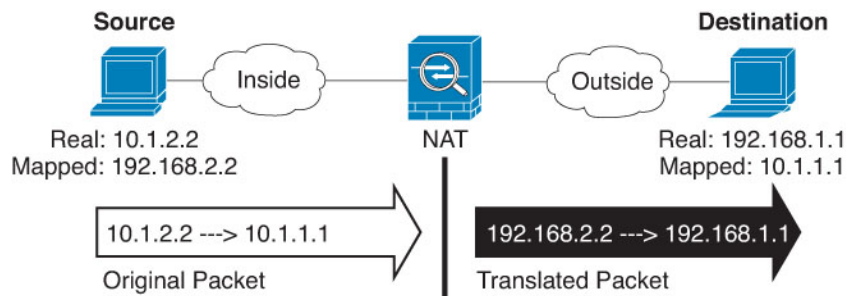
ステップ 3 Configure the basic rule options:

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

ステップ 4 Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイス に必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のイ ンターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入りま す。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイ スを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグ ループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用され ます。
- **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.

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

- **Fallthrough to Interface PAT (Destination Interface)**—その他のマッピングアドレスがすで に割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式 として使用するかどうかを指定します（インターフェイス PAT フォールバック）。この オプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場 合にのみ使用できます。 You cannot select this option if you already configured interface PAT as the translated address. You also cannot use this option with IPv6 networks.

ステップ 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.

始める前に

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.

手順

ステップ 1 Select **Policies** > **NAT**.

ステップ 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.)

ステップ 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. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- **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.

ステップ 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。

- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、または ネットワークグループ。

- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワークオブ ジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されま す。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単に アイデンティティ NAT を使用できます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）] を選択 して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにで きます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要が あります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を 実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択 します。

ステップ 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.

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）] フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空 白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポー トに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービ ス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じ

になるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

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

- **Fallthrough to Interface PAT (Destination Interface)**—その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。 You cannot select this option if you already configured interface PAT as the translated address. You also cannot use this option with IPv6 networks.

ステップ **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.

図 *6 : Static NAT*
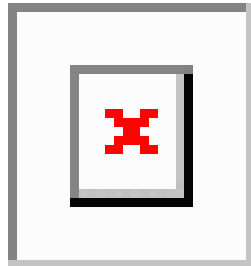
Static NAT with Port Translation

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.

図 *7 : Typical Static NAT with Port Translation Scenario*
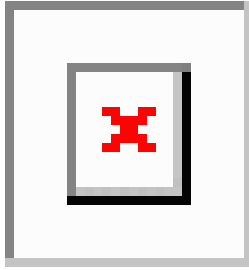
Static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. In addition, for 手動 NAT, traffic that does not match the source 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.

（注）   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.

図 *8 : One-to-Many Static NAT*
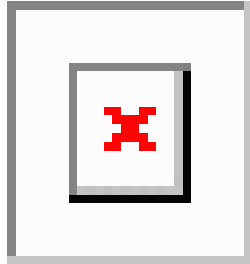
For example, you have a load balancer at 10.1.2.27. Depending on the URL requested, it redirects traffic to the correct web server.

図 *9 : One-to-Many Static NAT Example*
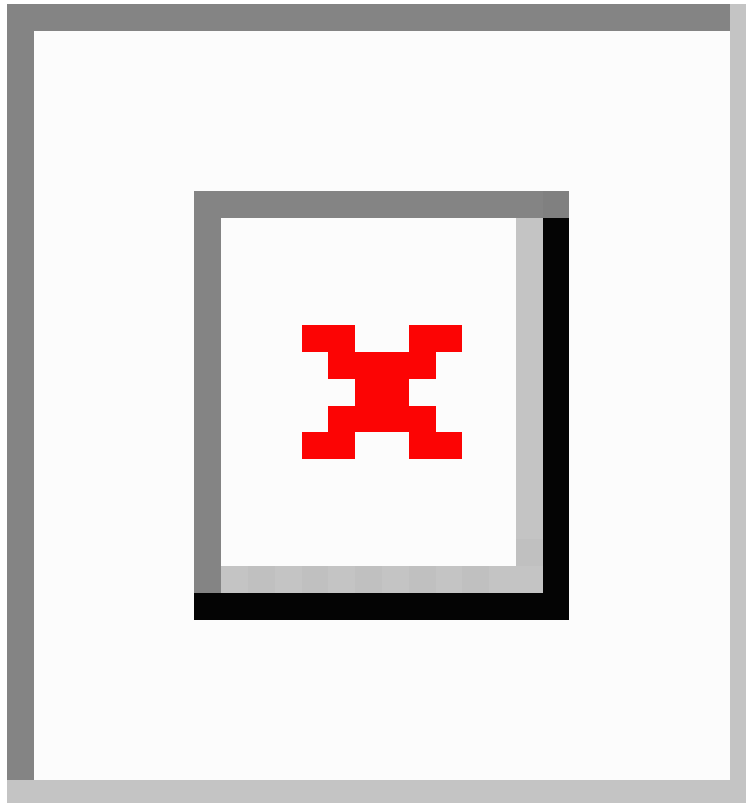
Other Mapping Scenarios (Not Recommended)

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.

図 *10 : Few-to-Many Static NAT*
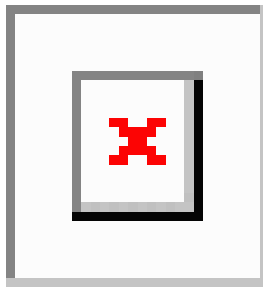
For a many-to-few or many-to-one configuration, where you have more real addresses than mapped addresses, you run out of mapped addresses before you run out of real addresses. Only the mappings between the lowest real IP addresses and the mapped pool result in bidirectional initiation. The remaining 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).

（注）　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.

図 *11 : Many-to-Few Static NAT*
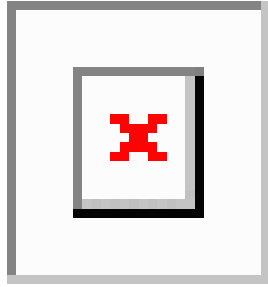
Instead of using a static rule this way, we suggest that you create a one-to-one rule for the traffic that needs bidirectional initiation, and then create a dynamic rule for the rest of your addresses.

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.

始める前に

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.

手順

ステップ **1** Select **Policies** > **NAT**.

ステップ **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.)

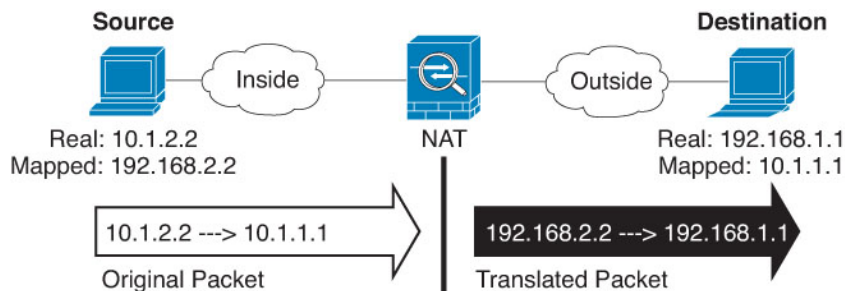ステップ **3** Configure the basic rule options:

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

ステップ 4 Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- **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.

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

- **Translate DNS replies that match this rule**—DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え （76 ページ）」を参照してください。 This option is not available if you are doing port translation.
- **Do not proxy ARP on Destination Interface**—マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があり

ます。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ **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.

始める前に

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.

手順

ステップ **1** Select **Policies** > **NAT**.

ステップ **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.)

ステップ **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. ルールはカテゴリ内（自動 NAT のルール
  の前後）、または選択するルールの上下に挿入できます。
- **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.

ステップ **4** Configure the following interface options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイス
  に必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のイ
  ンターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入りま
  す。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイ
  スを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグ
  ループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用され
  ます。

ステップ **5** 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットア
ドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。

- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、または
  ネットワークグループ。

- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワークオブ
  ジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されま
  す。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単に
  アイデンティティ NAT を使用できます。

  [インターフェイス（Interface）][送信元インターフェイスIP（Source Interface IP）] を選択
  して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにで
  きます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要が
  あります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を
  実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択
  します。

ステップ **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.

ステップ **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.

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

- **Translate DNS replies that match this rule**—DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え（76 ページ）」を参照してください。 This option is not available if you are doing port translation.

- **Do not proxy ARP on Destination Interface**—マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ **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 an address to itself.

The following figure shows a typical identity NAT scenario.

図 **12 : Identity NAT**
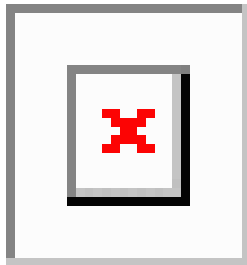
The following topics explain how to configure identity NAT.

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.

始める前に

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.

手順

ステップ **1** Select **Policies** > **NAT**.

ステップ **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.)

ステップ **3** Configure the basic rule options:

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

ステップ **4** Configure the following packet translation options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイス に必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のイ ンターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入りま す。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイ スを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグ ループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用され ます。
- **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.

ステップ **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**—マッピング IP アドレスへの着信パケットのプ ロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアド レスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべて の ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受 信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要が ないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできま す。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があり ます。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接 続性に関する問題を引き起こす可能性があります。
- **Perform Route Lookup for Destination Interface**—元の送信元アドレスと変換後の送信元ア ドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先イン ターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されてい る宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先イン ターフェイスを決めさせることができます。

ステップ **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.

始める前に

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.

手順

ステップ 1 Select **Policies** > **NAT**.

ステップ 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.)

ステップ 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. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- **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.

ステップ 4 Configure the following interface options:

- **Source Interface**, **Destination Interface**—（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ **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.
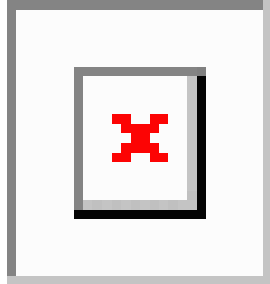
- **Original Source Address**—The network object or group that contains the addresses you are translating.

- **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.

ステップ **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.

ステップ **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.

ステップ **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**—マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

- **Perform route lookup for Destination interface**—元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 9 Click **OK**.

NAT Rule Properties for FTD

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. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。

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

（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

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.

- **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

（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用される インターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

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.

- **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.

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

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え（76 ページ）」を参照してください。 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.)

その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。 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.)

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

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

元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

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 手動 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 手動 NAT rule when you specify a destination, creating two 自動 NAT rules is the better solution.

✎

（注）　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.

（注） 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 手動 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 手動 NAT rule when you specify a destination, creating two 自動 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 手動 NAT rule.
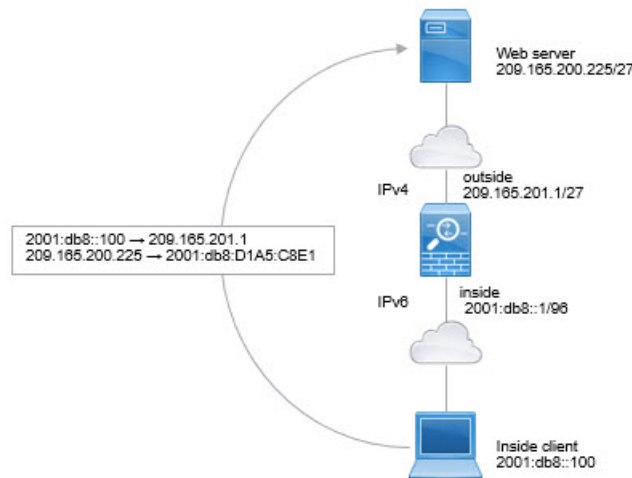

```
Web server
209.165.200.225/27

IPv4        outside
            209.165.201.1/27

2001:db8::100 → 209.165.201.1
209.165.200.225 → 2001:db8:D1A5:C8E1

IPv6        inside
            2001:db8::1/96

Inside client
2001:db8::100
```

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.

手順

ステップ 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.

Add Network Object

Name

inside_v6

Description

Type

⦿ Network   ◯ Host

Network

2001:DB8::/96

    d) Click **OK**.

ステップ 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.
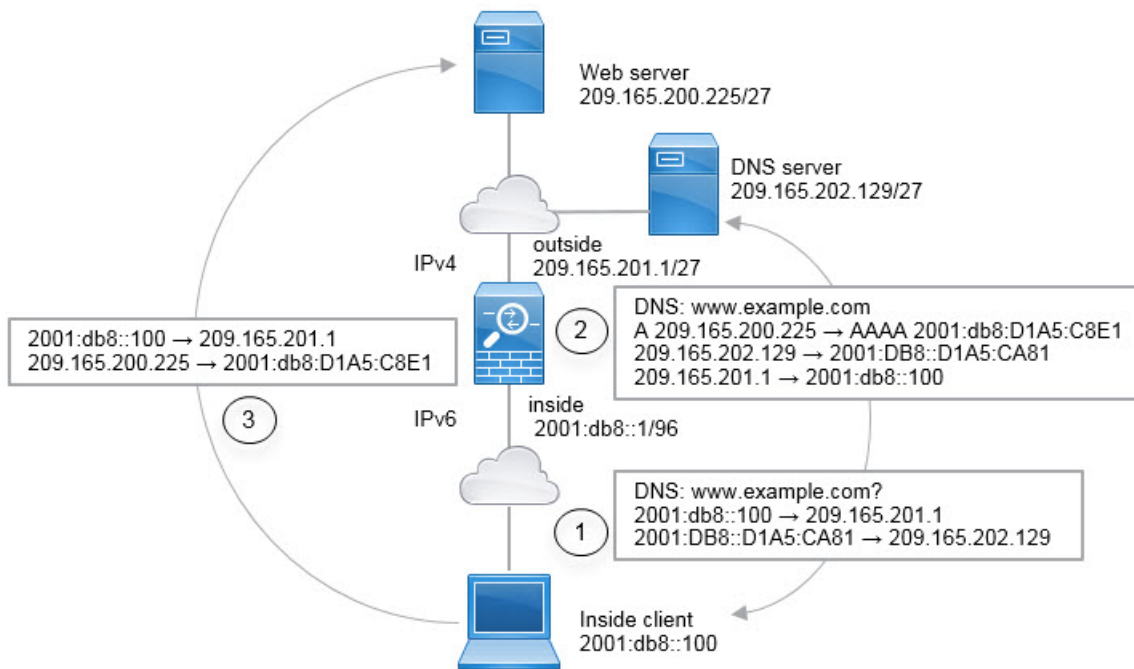
In this example, you translate the inside IPv6 network to IPv4 using dynamic interface PAT with the IP address of the outside interface. Outside IPv4 traffic is statically translated to addresses on the 2001:db8::/96 network, allowing transmission on the inside network. You enable DNS rewrite on the 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.)
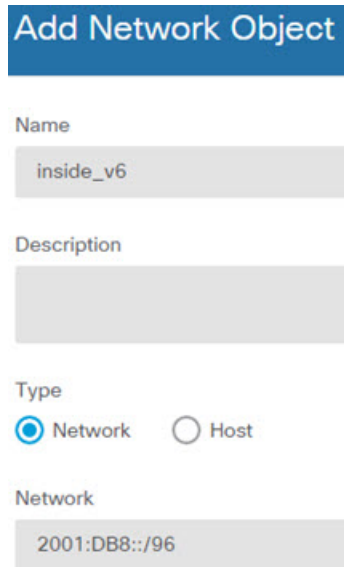
The following procedure explains how to configure this example.

手順

ステップ**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.

Add Network Object

Name

inside_v6

Description

Type
● Network   ○ Host

Network

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.

Add Network Object

Name

outside_v4_any

Description

Type

◉ Network ○ Host

Network

0.0.0.0/0

ステップ**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.

ステップ **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**.

Add NAT Rule

Title	Create Rule for	Status
NAT46Rule	Auto NAT	

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Automatically placed in Auto NAT rules

Type

Static

Packet Translation   Advanced Options

ORIGINAL PACKET

Source Interface

outside

Original Address	Original Port
outside_v4_any	Any

TRANSLATED PACKET

Destination Interface

inside

Translated Address	Translated Port
inside_v6	Any

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 自動 NAT. However, if you do not want to allow returning traffic, you can make the static NAT rule unidirectional using 手動 NAT only.

NAT66 Example, Static Translation between Networks

You can configure a static translation between IPv6 address pools using 自動 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.
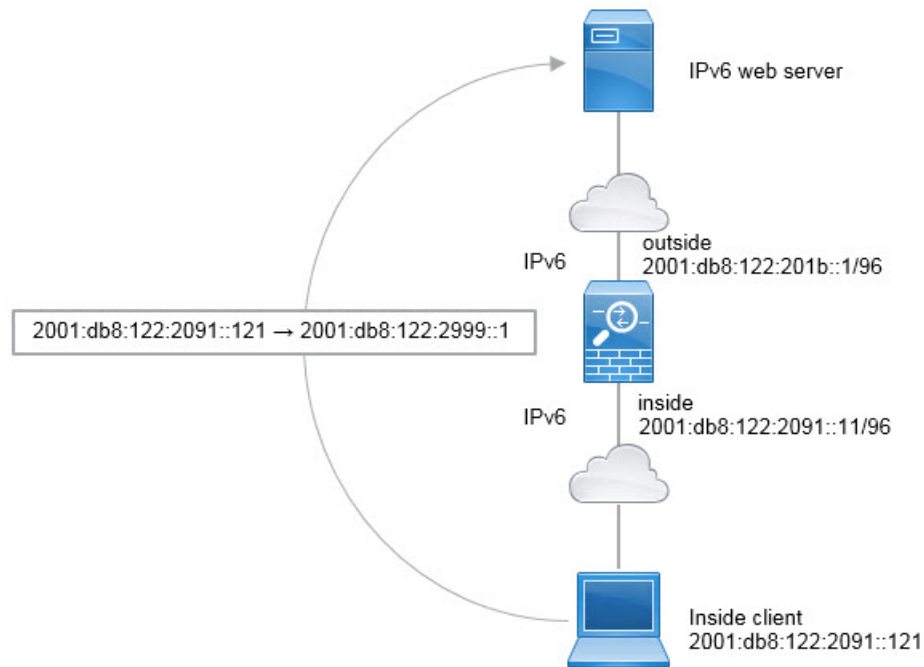
(注) This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

手順

ステップ 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.

Add Network Object

Name

inside_v6

Description

Type

◉ Network   ○ Host

Network

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.

Add Network Object

Name

outside_nat_v6

Description

Type

◉ Network   ○ Host

Network

2001:db8:122:2999::/96

ステップ **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 FDM. Instead, use a single free address on the same network as a dynamic PAT pool.
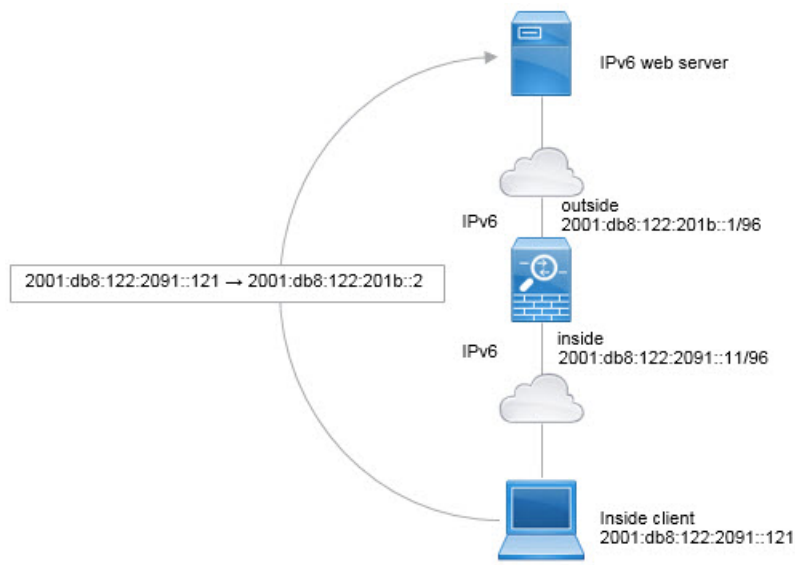
IPv6 web server

outside
IPv6   2001:db8:122:201b::1/96

2001:db8:122:2091::121 → 2001:db8:122:201b::2

inside
IPv6   2001:db8:122:2091::11/96

Inside client
2001:db8:122:2091::121

（注）　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.

手順

ステップ **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.

Add Network Object

Name

inside_v6

Description

Type

◉ Network   ○ Host

Network

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.

Add Network Object

Name

ipv6_pat

Description

Type

○ Network   ◉ Host

Host

2001:db8:122:201b::2

ステップ **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.

Add NAT Rule

Title	Create Rule for	Status
PAT66Rule	Auto NAT	

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Dynamic

Packet Translation   Advanced Options

ORIGINAL PACKET

Source Interface
inside

Original Address   Original Port
inside_v6   Any

TRANSLATED PACKET

Destination Interface
outside

Translated Address   Translated Port
ipv6_pat   Any

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.

✎

（注） 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.

図 **13 : Static NAT for an Inside Web Server**

手順
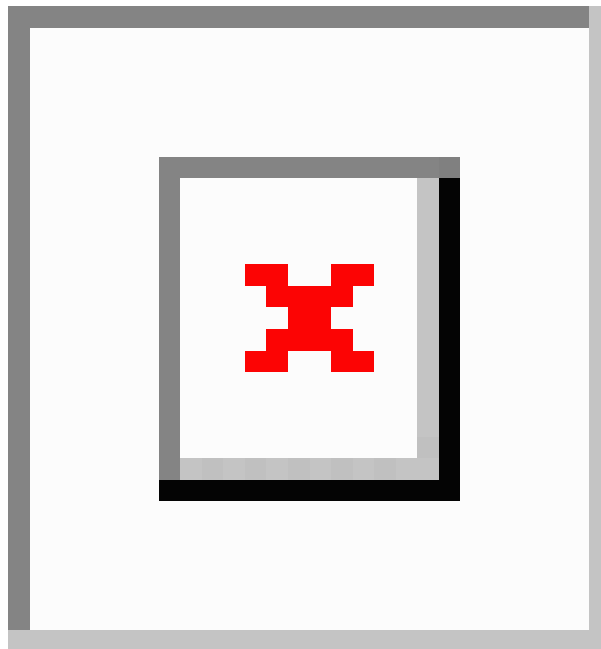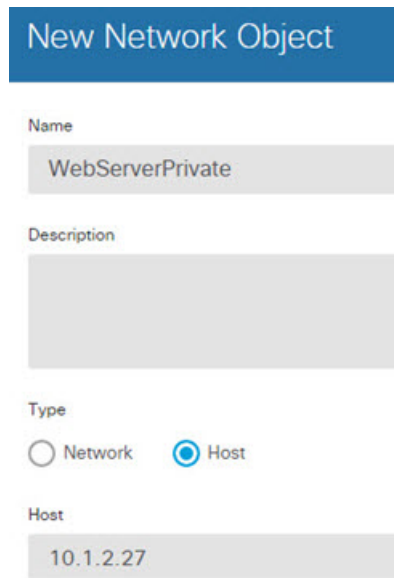
ステップ**1** Create the network objects that define the server's private and public host addresses.

   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**.

ステップ **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.
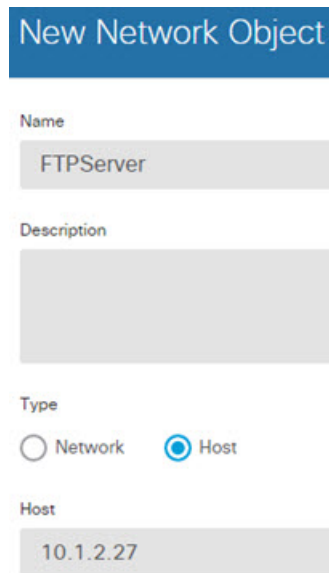
（注） This example assumes that the inside interface is a standard routed interface attached to a switch, with the servers attached to the switch. If your inside interface is a bridge group interface (BVI), and the servers are attached to separate bridge group member interfaces, select the specific member 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.

図 *14 : Static NAT-with-Port-Translation*

手順
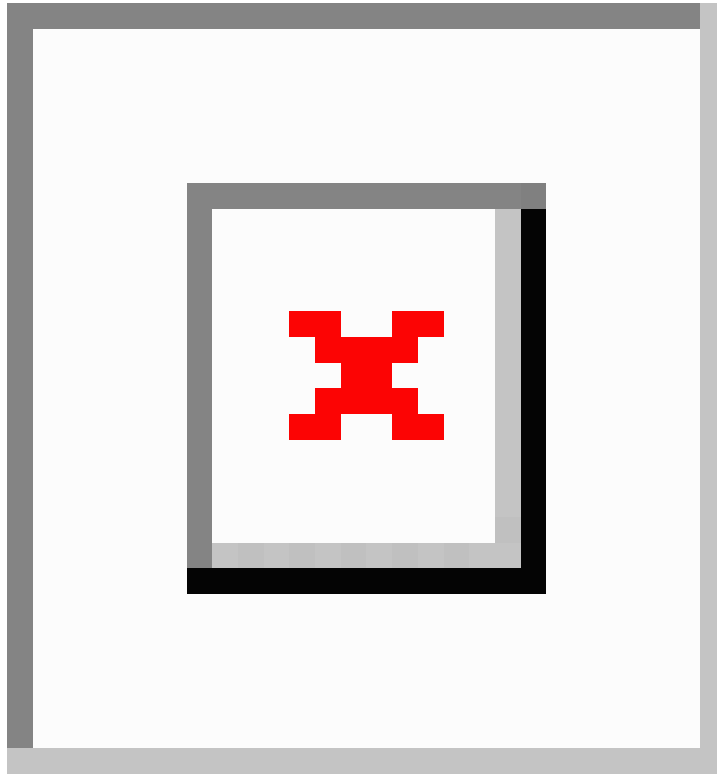
ステップ **1** Create a network object for the FTP server.

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.
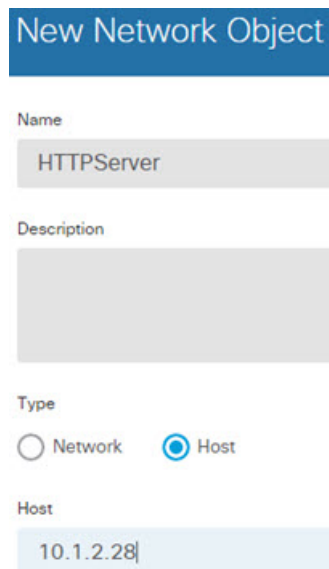
New Network Object

Name

FTPServer

Description

Type

○ Network   ⦿ Host

Host

10.1.2.27

    d)   Click **OK**.

ステップ 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.

New Network Object

Name

HTTPServer

Description

Type

○ Network   ⦿ Host

Host

10.1.2.28

    c)   Click **OK**.

ステップ 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.

New Network Object

Name

SMTPServer

Description

Type

○ Network ● Host

Host

10.1.2.29

    c)   Click **OK**.

ステップ **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.

New Network Object

Name

ServerPublicIP

Description

Type

○ Network ● Host

Host

209.165.201.3

    c)   Click **OK**.

ステップ **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**.

ステップ **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.

Add NAT Rule

Title
HTTPServer

Create Rule for
Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address o packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement
Automatically placed in Auto NAT rules

Type
Static

Packet Translation   Advanced Options

Original Packet

Source Interface
inside

Translated Packet

Destination Interface
outside

Original Address
HTTPServer

Original Port
HTTP

Translated Address
ServerPublicIP

Translated Port
HTTP

c) Click **OK**.

ステップ **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.

Add NAT Rule

Title

SMTPServer

Create Rule for

Auto NAT ⌄ 🔵

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Automatically placed in Auto NAT rules

Type

Static ⌄

Packet Translation   Advanced Options

Original Packet

Source Interface

inside ⌄

Original Address   Original Port

SMTPServer ⌄   SMTP ⌄

Translated Packet

Destination Interface

outside

Translated Address   Translated Port

ServerPublicIP ⌄   SMTP

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*.

✎

（注）   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.

図 *15 : Manual NAT with Different Destination Addresses*
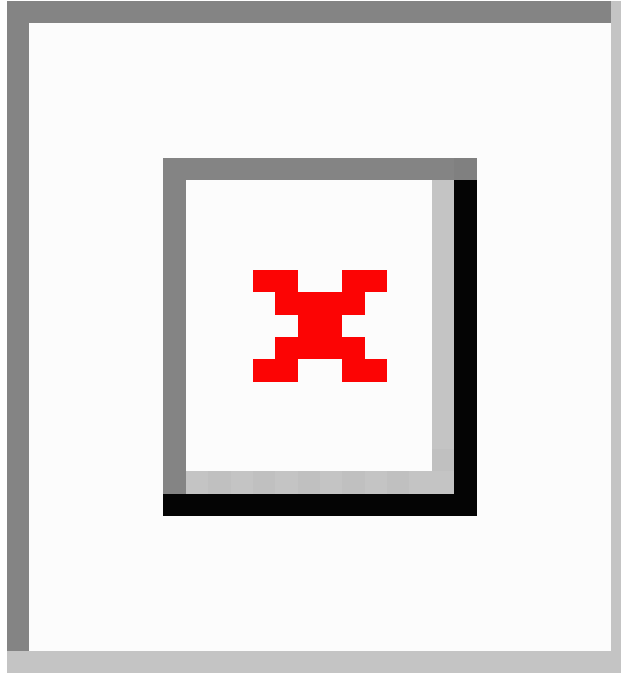
手順

ステップ**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**.

ステップ **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).

New Network Object

Name

DMZnetwork1

Description

Type

◉ Network   ○ Host

Network

209.165.201.0/27

        c)   Click **OK**.

ステップ **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.

New Network Object

Name

PATaddress1

Description

Type

○ Network   ◉ Host

Host

209.165.202.129

        c)   Click **OK**.

ステップ **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**.

ステップ **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**.

ステップ **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.

   （注） 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**.

ステップ**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*.

（注） 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.

図 *16 : Manual NAT with Different Destination Ports*
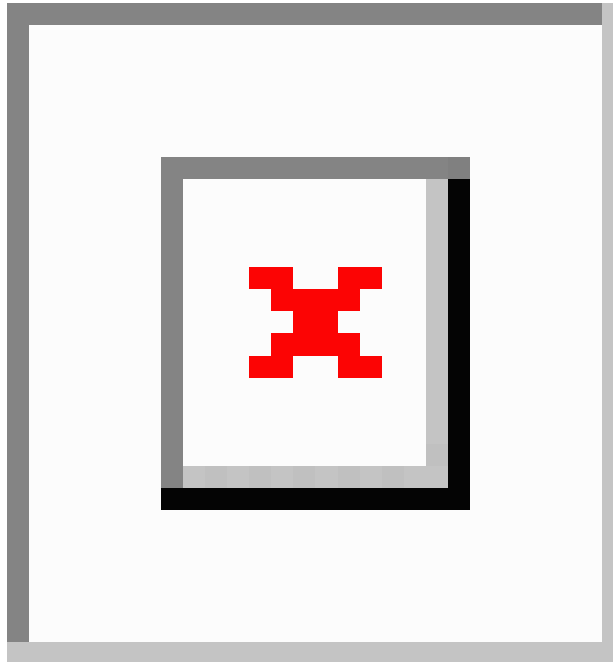
手順

ステップ **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.
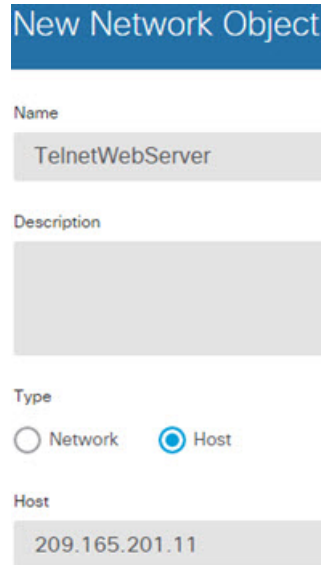
    d)   Click **OK**.

ステップ **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.

New Network Object

Name

TelnetWebServer

Description
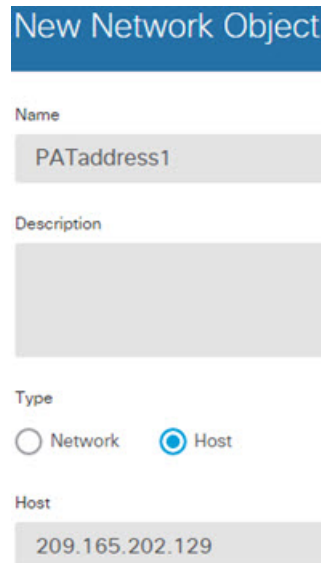
Type

○ Network   ◉ Host

Host

209.165.201.11

    c)   Click **OK**.

ステップ **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.

New Network Object

Name

PATaddress1

Description

Type

○ Network   ◉ Host

Host

209.165.202.129

    c)   Click **OK**.

ステップ **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**.

ステップ **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.

    （注）   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**.

ステップ **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**.

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT 設定と一致するアドレスに置き換えて、DNS 応答を修正するように FTD デバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーション ルールを設定するときに設定できます。DNS 修正は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へ書き換えられます。逆に、任意のインターフェイスからマッピン インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。この機能は、NAT44、NAT66、NAT46、および NAT64 と連動します。

以下に、NAT ルールで DNS の書き換えを設定する必要が生じる主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード（IPv4 用）と AAAA レコード（IPv6 用）を変換するために DNS の書き換えが必要です。

- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。

- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS の書き換えの制限事項

次に DNS の書き換えの制限事項を示します。

- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS の書き換えは PAT には適用されません。

- 手動 NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。

- 実際には、DNS の書き換えは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、書き換えが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。

- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ（オペレーション コード 5）は書き換えられません。

次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

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.
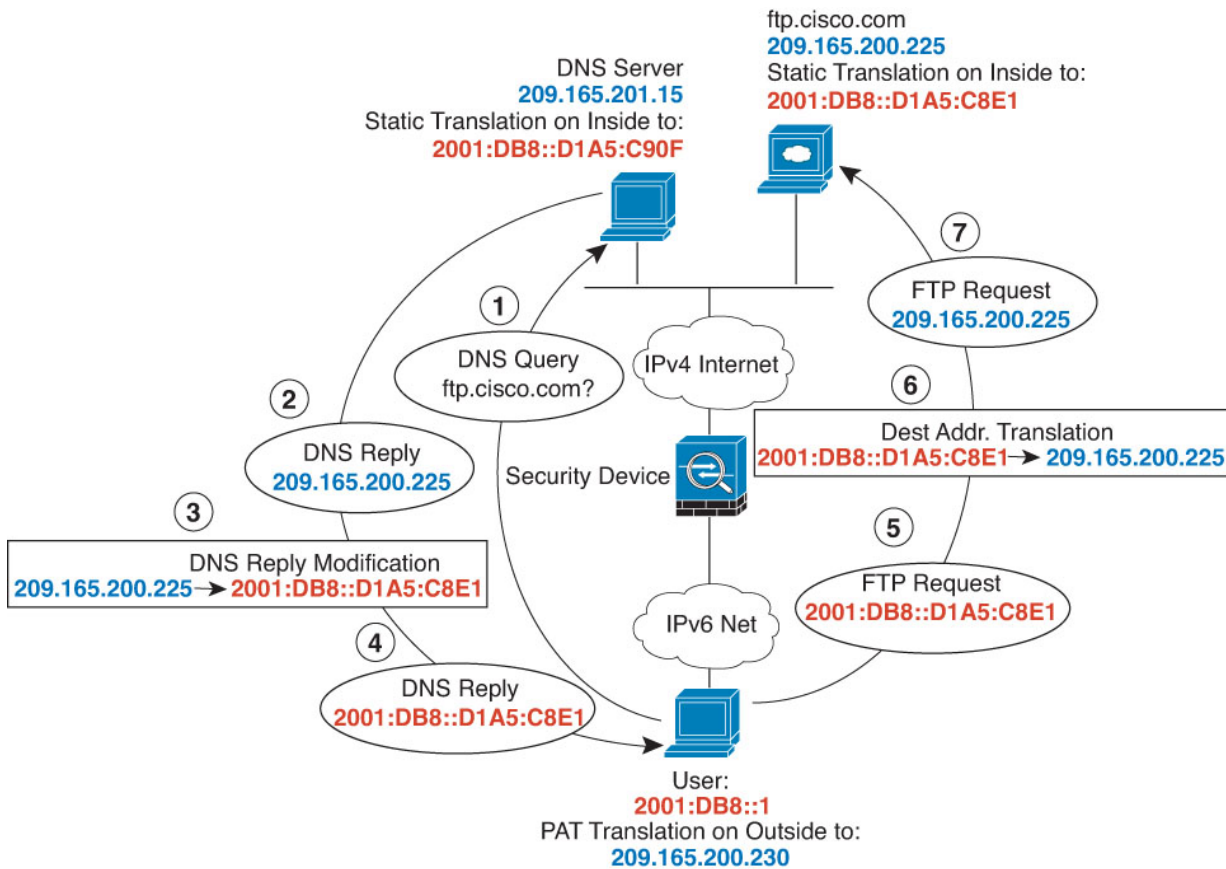
ftp.cisco.com
209.165.200.225
Static Translation on Inside to:
2001:DB8::D1A5:C8E1

DNS Server
209.165.201.15
Static Translation on Inside to:
2001:DB8::D1A5:C90F

① DNS Query ftp.cisco.com?

IPv4 Internet

⑦ FTP Request **209.165.200.225**

② DNS Reply **209.165.200.225**

Security Device

⑥ Dest Addr. Translation **2001:DB8::D1A5:C8E1** ➔ **209.165.200.225**

③ DNS Reply Modification **209.165.200.225** ➔ **2001:DB8::D1A5:C8E1**

⑤ FTP Request **2001:DB8::D1A5:C8E1**

IPv6 Net

④ DNS Reply **2001:DB8::D1A5:C8E1**

User:
2001:DB8::1
PAT Translation on Outside to:
209.165.200.230

（注） 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.

手順

ステップ **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.

Add Network Object

Name

ftp_server

Description

Type

○ Network   ● Host

Host

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.

Add Network Object

Name

dns_server

Description

Type

○ Network   ● Host

Host

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.

Add Network Object

Name

inside_v6

Description

Type

⊙ Network   ○ Host

Network

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.

Add Network Object

Name

ipv4_pat

Description

Type

○ Network   ⊙ Host

Host

209.165.200.230

j) Click **OK**.

ステップ **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**.

ステップ **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.

Add NAT Rule

Title	Create Rule for	Status
DNSServer	Auto NAT	(on)

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static

Packet Translation   Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface		Destination Interface	
outside		inside	

Original Address	Original Port	Translated Address	Translated Port
dns_server	Any	inside_v6	Any

d) Click **OK**.

ステップ **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.
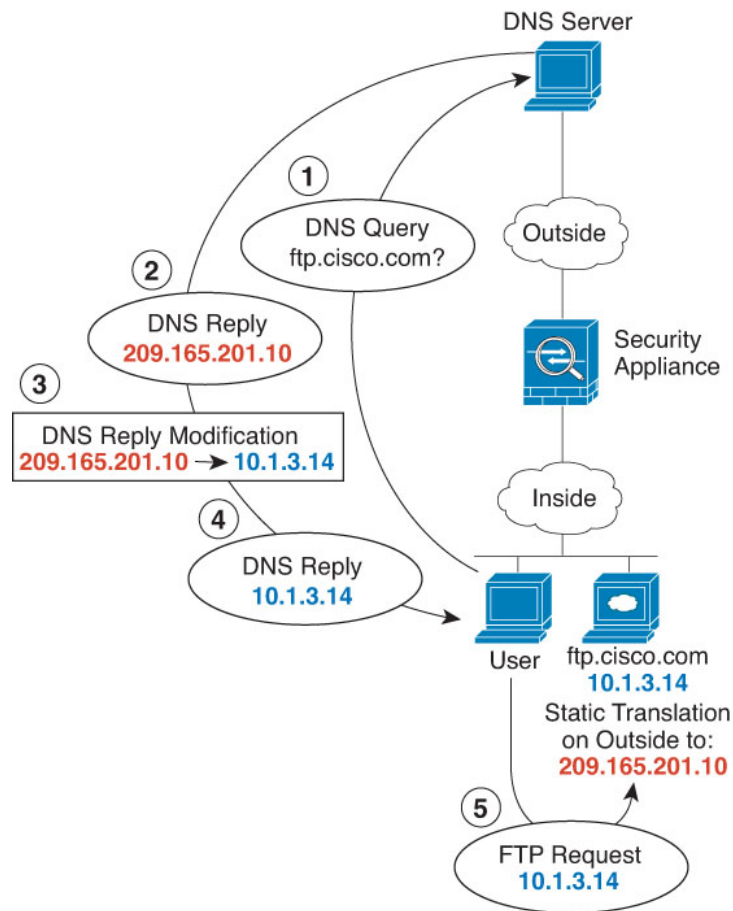
> ✎
>
> （注）   This example assumes that the inside interface is not a bridge group interface (BVI) but a standard routed interface. If the inside interface is a BVI, you need to duplicate the rules for each member interface.

手順

ステップ**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.

Add Network Object

Name

ftp_server

Description

Type

○ Network   ⦿ Host

Host

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.

Add Network Object

Name

ftp_server_outside

Description

Type

○ Network   ⦿ Host

Host

209.165.201.10

ステップ **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.

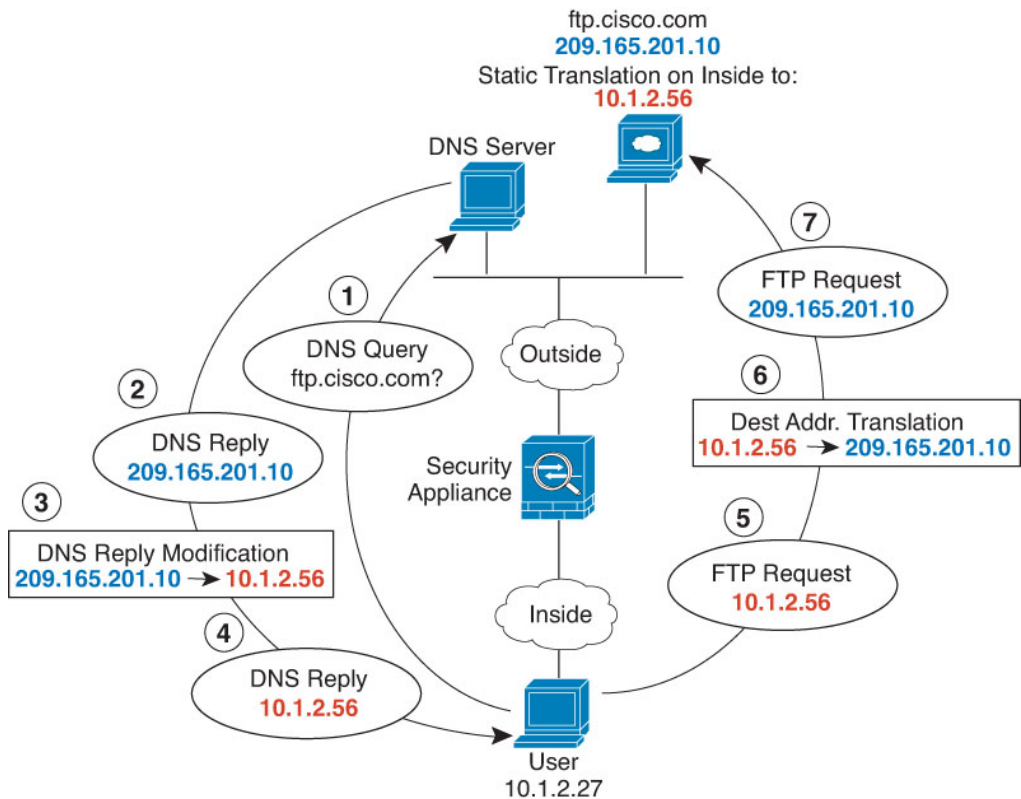- On the **Advanced Options** tab, select **Translate DNS replies that match this rule**.

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.

ftp.cisco.com
209.165.201.10
Static Translation on Inside to:
10.1.2.56

DNS Server

⑦ FTP Request
209.165.201.10

① DNS Query
ftp.cisco.com?

Outside

⑥ Dest Addr. Translation
10.1.2.56 → 209.165.201.10

② DNS Reply
209.165.201.10

Security
Appliance

③ DNS Reply Modification
209.165.201.10 → 10.1.2.56

⑤ FTP Request
10.1.2.56

④ DNS Reply
10.1.2.56

Inside

User
10.1.2.27

（注） 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.

手順

ステップ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.

Add Network Object

Name

ftp_server

Description

Type

○ Network　　◉ Host

Host

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.

Add Network Object

Name

ftp_server_translated

Description

Type

○ Network　　◉ Host

Host

10.1.2.56

ステップ **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**.