CHAPTER 9

Configuring Network Address Translation

Routed firewall mode only

This chapter describes Network Address Translation (NAT). In routed firewall mode, the Firewall Services Module (FWSM) typically performs NAT between each network.

Note In transparent firewall mode, both the inside and outside network are the same network, and the FWSM does not perform NAT. See the "Configuring Connection Limits for Non-NAT Configurations" section on page 6-9 for connection limits for which you must configure a NAT statement in transparent firewall mode.

This chapter contains the following sections:

NAT Overview

This section describes how NAT works on the FWSM, and includes the following topics:

Introduction to NAT

Address translation substitutes the local address in a packet with a global address that is routable on the destination network. In this document, all types of translation are generally referred to as “NAT.”

On the FWSM, you must specifically configure some interfaces to either use or to bypass NAT. For example, when hosts on a higher security interface (inside) access hosts on a lower security interface (outside), you must configure NAT on the inside hosts *or* specifically configure the inside hosts to bypass NAT (See the “Configuring Interfaces” section on page 6-6 for more information about security levels).

Note When discussing NAT, the terms *inside* and *outside* are relative, and represent the security relationship between any two interfaces. The higher security level is inside and the lower security level is outside; for example, interface 1 is at 60 and interface 2 is at 50, so interface 1 is “inside” and interface 2 is “outside.”

An inside host can communicate with the untranslated local address of the outside host without any special configuration on the outside interface. However, you can also optionally configure NAT on the outside network.

Interfaces that are on the same security level that you have allowed to communicate do not have to perform NAT. You can, however, optionally configure NAT for these interfaces. (See the “Allowing Communication Between Interfaces on the Same Security Level” section on page 6-8 for more information.) In this case, there is no inside or outside when performing NAT between two interfaces.

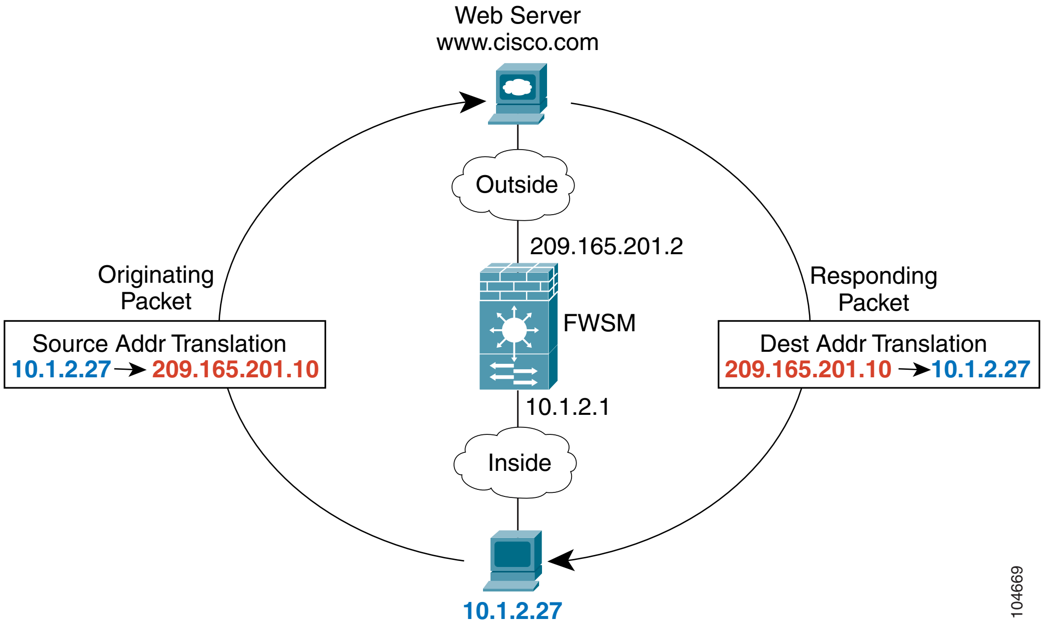
Some of benefits of NAT are as follows:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet. (See the “Private Networks” section on page D-2 for more information.)
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- You can resolve IP routing problems such as overlapping addresses.

Note See Table 13-1 on page 13-2 for information about protocols that are not supported by NAT.

Figure 9-1 shows a typical NAT scenario, with a private network on the inside. When the inside host sends a packet to a web server, the local source address of the packet is changed to a routable global address. When the server responds, it sends the response to the global address, and the FWSM receives the packet. The FWSM then translates the global address to the local address before sending it on to the host.

Figure 9-1 NAT Example



See the following commands for this example:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.0 255.255.255.0
FWSM/contexta(config)# global (outside) 1 209.165.201.1-209.165.201.15
```

NAT Types

You can implement address translation as dynamic NAT, Port Address Translation (PAT), static NAT, or static PAT or as a mix of these types. You can also bypass NAT. See the following sections for information about each type:

- Dynamic NAT, page 9-3
- PAT, page 9-4
- Static NAT, page 9-5
- Static PAT, page 9-5
- Bypassing NAT, page 9-7

Dynamic NAT

Dynamic NAT translates a group of local addresses to a pool of global addresses that are routable on the destination network. The global pool can include fewer addresses than the local group. When a local host accesses the destination network, the FWSM assigns it an IP address from the global pool. Because the translation is only in place for the duration of the connection, a given user does not keep the same IP address after the translation times out (see the **timeout xlate** command in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*). Users on the destination network, therefore, cannot reliably initiate a connection to a host that uses dynamic NAT (even if the connection is allowed by an access control list (ACL)). Not only can you not predict the global IP address of the host, but the FWSM does not create a translation at all unless the local host is the initiator. See "Static NAT" or "Static PAT" below for reliable access to hosts.

Note For the duration of the translation, a global host can initiate a connection to the local host if an ACL allows it. Because the address is unpredictable, a connection to the host is unlikely. However in this case, you can rely on the security of the ACL.

Dynamic NAT has these disadvantages:

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

  Use PAT 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 global pool; if the destination network requires registered addresses, such as the Internet, you might encounter a shortage of usable addresses.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with some applications that have a data stream on one port and the control path on another, such as some multimedia applications. See the "Inspection Engine Overview" section on page 13-1 for more information about NAT and PAT support.

PAT

PAT translates multiple local addresses to a single global IP address. Specifically, the FWSM translates the local address and local port for multiple connections and/or hosts to a single global address and a unique port (above 1024). When a local host connects to the destination network on a given source port, the FWSM assigns the global IP address to it and a unique port number. Each host receives the same IP address, but because the source port numbers are unique, the responding traffic, which includes the IP address and port number as the destination, can be sent to the correct host. Because there are over 64,000 ports available, you are unlikely to run out of addresses, which can happen with dynamic NAT. Because the translation is specific to the local address and local port, each connection, which generates a new source port, requires a separate translation. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The translation is only in place for the duration of the connection, so a given user does not keep the same global IP address port number after the translation times out (see the **timeout xlate** command in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*). Users on the destination network, therefore, cannot reliably initiate a connection to a host that uses PAT (even if the connection is allowed by an ACL). Not only can you not predict the local or global port number of the host, but the FWSM does not create a translation at all unless the local host is the initiator. See "Static NAT" or "Static PAT" below for reliable access to hosts.

PAT lets you use a single global address, thus conserving routable addresses. You can even use the FWSM interface IP address as the PAT address. PAT does not work with some multimedia applications that have a data stream that is different from the control path. See the "Inspection Engine Overview" section on page 13-1 for more information about NAT and PAT support.

Note For the duration of the translation, a global host can initiate a connection to the local host if an ACL allows it. Because the port address (both local and global) is unpredictable, a connection to the host is unlikely. However in this case, you can rely on the security of the ACL.

Static NAT

Static NAT translates each local address to a fixed global address. With dynamic NAT and PAT, each host uses a different address or port after the translation times out. Because the global address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the global network to initiate traffic to a local host (if there is an ACL that allows it).

The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a global host to initiate a connection to a local host (if there is an ACL that allows it), while dynamic NAT does not. You also need an equal number of global addresses as local addresses with static NAT.

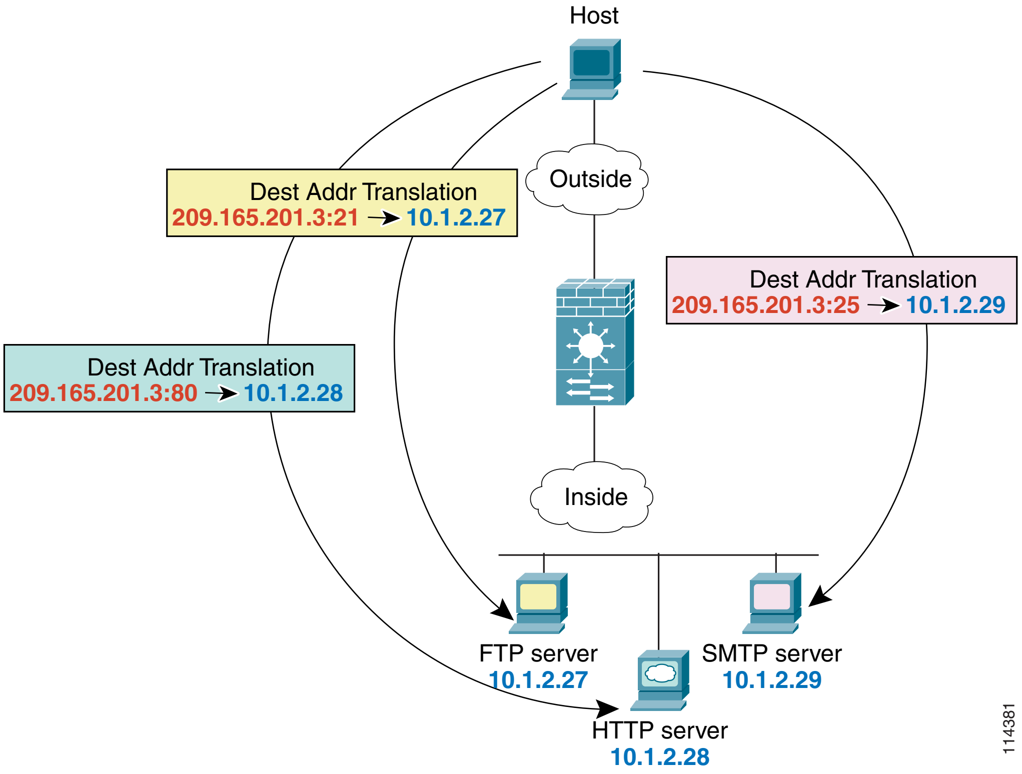
Static PAT

Static PAT is the same as static NAT, except it lets you specify the protocol (TCP or UDP) and port for the local and global addresses.

This feature lets you identify the same global address across many different static statements, so long as the port is different for each statement (you cannot use the same global address for multiple static *NAT* statements).

For example, if you want to provide a single address for global users to access FTP, HTTP, and SMTP, but these are all actually different servers on the local network, you can specify static PAT statements for each server that uses the same global IP address, but different ports (see Figure 9-2).

Figure 9-2 Static PAT



See the following commands for this example:

```
FWSM/contexta(config)# static (inside,outside) tcp 209.165.201.3 ftp 10.1.2.27 ftp netmask
255.255.255.255
FWSM/contexta(config)# static (inside,outside) tcp 209.165.201.3 http 10.1.2.28 http
netmask 255.255.255.255
FWSM/contexta(config)# static (inside,outside) tcp 209.165.201.3 smtp 10.1.2.29 smtp
netmask 255.255.255.255
```

If the application used by the server requires an inspection engine to allow data channels on other ports, such as FTP, then the server needs translation for other ports. Other protocols that require inspection engines for data channels include TFTP, RTSP, and Skinny. See Chapter 13, “Configuring Application Protocol Inspection,” for a complete list of protocols that require inspection engines. For example, add the following line to the above configuration to translate all other ports from the FTP server at 10.1.2.27:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.27 255.255.255.255
FWSM/contexta(config)# global (outside) 1 209.165.201.3
```

The above configuration also allows the FTP server to initiate connections, if desired.

You can also use static PAT to translate a well-known port to a non-standard port or vice versa. For example, if your inside web servers use port 8080, you can allow outside users to connect to port 80, and then translate them to the 8080 port. Similarly, if you want to provide extra security, you can tell your web users to connect to non-standard port 6785, and then translate them to port 80 on the local network.

Bypassing NAT

When hosts on a higher security interface (inside) access hosts on a lower security interface (outside), you must configure NAT on the inside hosts or specifically configure the inside interface to bypass NAT. You might want to bypass NAT in the following circumstances:

- You do not want the complication of NAT.
- You are using an application that does not support NAT (see the "Inspection Engine Overview" section on page 13-1 for information about inspection engines that do not support NAT).
- You are using a transparent firewall and want to set connection limits.
- You are using same security interfaces and want to set connection limits.

You can configure an interface to bypass NAT using three methods. All methods achieve compatibility with inspection engines and simplification of your addressing. However, each method offers slightly different capabilities, as follows:

- Identity NAT—When you configure identity NAT (which is similar to dynamic NAT), you do not specify global addresses, and therefore you do not specify a single global interface; you must use identity NAT for connections through all interfaces. Therefore, you cannot choose to perform normal translation on local addresses when you access interface A, but use identity NAT when accessing interface B. Regular dynamic NAT, on the other hand, lets you specify a particular global interface on which to translate the addresses. Make sure that the local addresses for which you use identity NAT are routable on all networks that are available according to your ACLs.

  For identity NAT, even though the translated address is the same as the local address, you cannot initiate a connection from the outside to the inside (even if the interface ACL allows it). Use static identity NAT or NAT exemption for this functionality. For same security interfaces, however, you can initiate connections both ways.
- Static identity NAT—Static identity NAT lets you specify the global interface on which you want to allow the local addresses to appear, so you can use identity NAT when you access interface A, and use regular translation when you access interface B. Static identity NAT also lets you use policy NAT, which identifies the local and destination addresses when determining the local traffic to translate (see the "Policy NAT" section on page 9-8 for more information about policy NAT). For example, you can use static identity NAT for an inside address when it accesses the outside interface and the destination is server A, but use a normal translation when accessing the outside server B.
- NAT exemption— NAT exemption allows both local and global hosts to initiate connections. Like identity NAT, you do not specify global addresses, and therefore you do not specify a single global interface; you must use NAT exemption for connections through all interfaces. However, NAT exemption does allow you to specify the local and destination addresses when determining the local traffic to translate (similar to policy NAT), so you have greater control using NAT exemption. However unlike policy NAT, NAT exemption does not consider the ports in the ACL.

Note In multiple context mode, you cannot initiate connections from an interface shared between contexts when you use NAT exemption for the destination address. The classifier can only assign packets from a shared interface to a context when you configure a static statement for the destination address. For example, if you share the outside interface, you cannot use NAT exemption on an inside interface if you want outside traffic to reach the inside addresses. The classifier only looks at static statements where the global interface matches the source interface of the packet. Because NAT exemption does not identify a global interface, the classifier does not consider those NAT statements for classification purposes.

Policy NAT

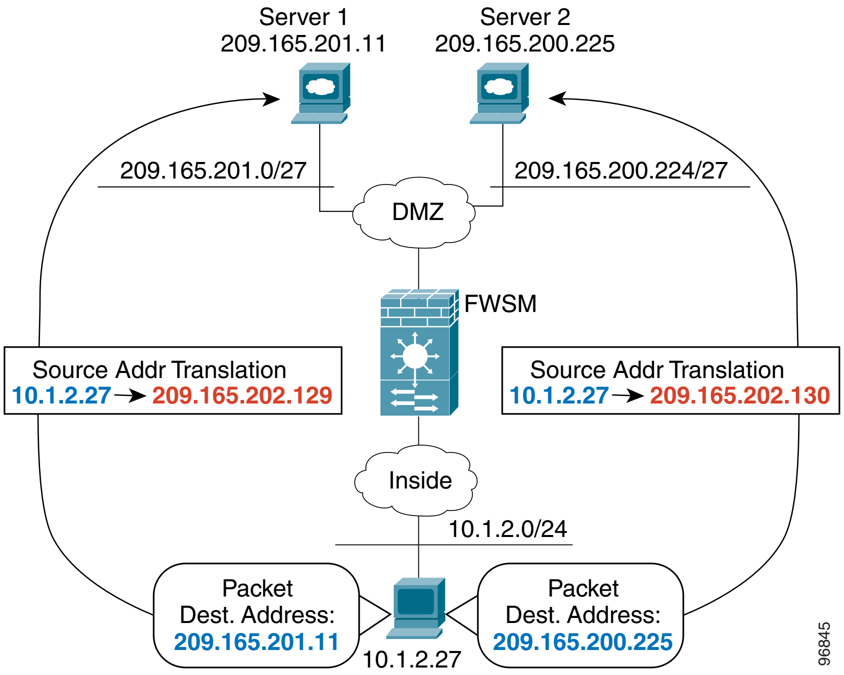
Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses in an extended ACL. You can also optionally specify the source and destination ports. Regular NAT can only consider the local addresses.

Note All types of NAT support policy NAT except for NAT exemption. NAT exemption uses an ACL to identify the local addresses, but differs from policy NAT in that the ports are not considered. See the "Bypassing NAT" section on page 9-29 for other differences.

With policy NAT, you can create multiple NAT or static statements that identify the same local address as long as the source/port and destination/port combination is unique for each statement. You can then match different global addresses to each source/port and destination/port pair.

Figure 9-3 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 local address is translated to 209.165.202.129. When the host accesses the server at 209.165.200.225, the local address is translated to 209.165.202.130 so that the host appears to be on the same network as the servers, which can help with routing.

Figure 9-3 Policy NAT with Different Destination Addresses

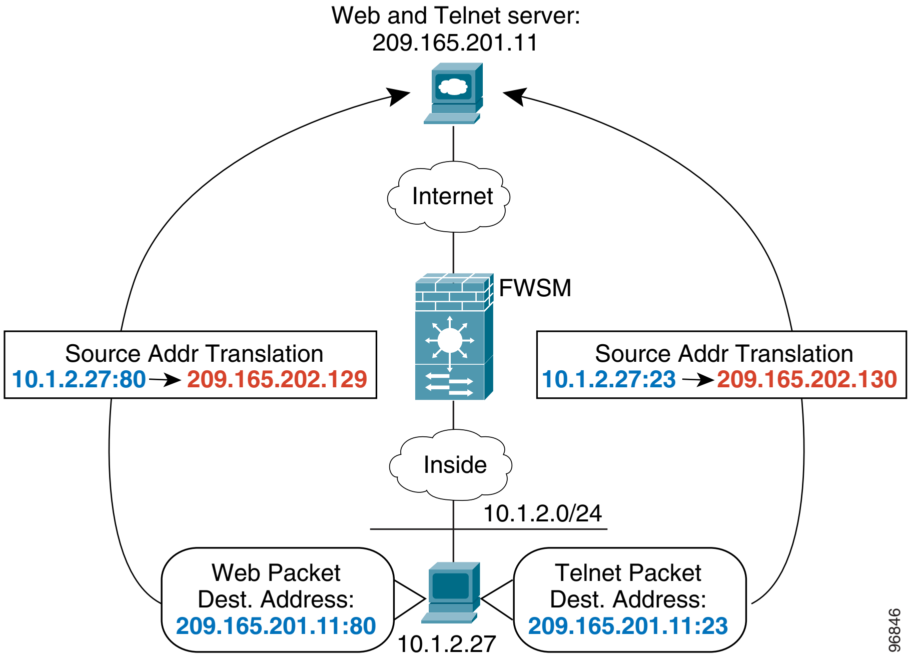


See the following commands for this example:

```
FWSM/contexta(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
FWSM/contexta(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
FWSM/contexta(config)# nat (inside) 1 access-list NET1
FWSM/contexta(config)# global (outside) 1 209.165.202.129
FWSM/contexta(config)# nat (inside) 2 access-list NET2
FWSM/contexta(config)# global (outside) 2 209.165.202.130
```

Figure 9-4 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 web services, the local address is translated to 209.165.202.129. When the host accesses the same server for Telnet services, the local address is translated to 209.165.202.130.

Figure 9-4 Policy NAT with Different Destination Ports

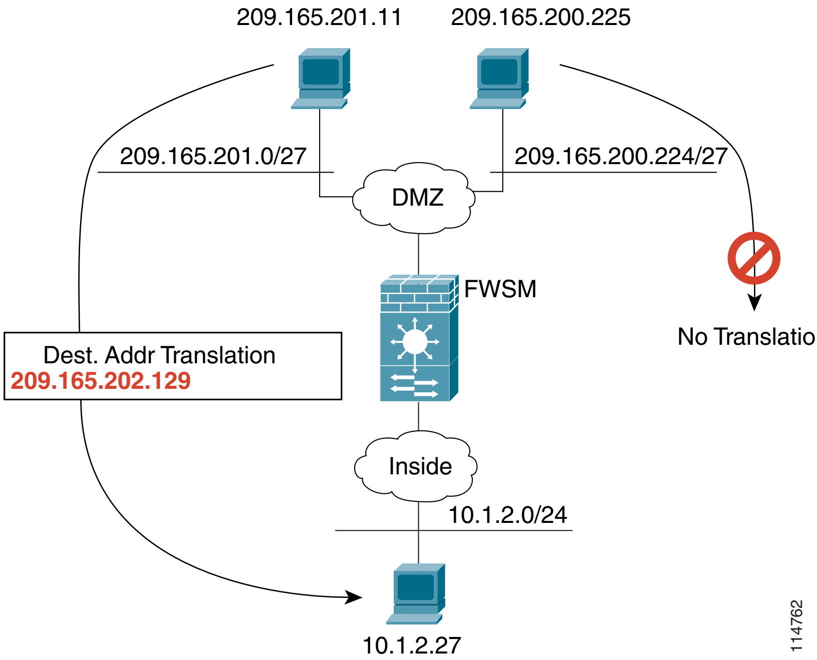


See the following commands for this example:

```
FWSM/contexta(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
FWSM/contexta(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
FWSM/contexta(config)# nat (inside) 1 access-list WEB
FWSM/contexta(config)# global (outside) 1 209.165.202.129
FWSM/contexta(config)# nat (inside) 2 access-list TELNET
FWSM/contexta(config)# global (outside) 2 209.165.202.130
```

For policy static NAT (and for NAT exemption, which also uses an ACL to identify traffic), both local and global hosts can originate traffic. For locally originated traffic, the NAT ACL specifies the local addresses and the *destination* addresses, but for globally originated traffic, the ACL identifies the local addresses and the *source* addresses of global hosts who are allowed to connect to the local host using this translation. Figure 9-5 shows a global host connecting to a local host. The local host has a policy static NAT translation that translates the local address only for traffic to and from the 209.165.201.0/27 network. A translation does not exist for the 209.165.200.224/27 network, so the local host cannot connect to that network, nor can a host on that network connect to the local host.

Figure 9-5 Policy Static NAT with Destination Address Translation



Note Policy NAT does not support SQL*Net, but it is supported by regular NAT. See the "Inspection Engine Overview" section on page 13-1 for information about NAT support for other protocols.

Note The number of access control entries (ACEs) used in policy NAT statements is limited. See the "Maximum Number of ACEs" section on page 10-7 for information about limits on certain types of rules.

Outside NAT

When hosts on a lower security interface (outside) access hosts on a higher security interface (inside), you do not have to perform NAT on the outside hosts. (See the "Configuring Interfaces" section on page 6-6 for more information about security levels.) You can, however, optionally configure NAT on outside interfaces so that the outside host address is translated. Because the inside host is also typically translated using a static NAT statement, both host addresses are translated.

If you configure dynamic NAT or PAT (**nat** and **global** commands) for any hosts on an outside interface when they access hosts on a given inside interface, then for any traffic between those two interfaces, the NAT requirements change for the outside interface. Namely, the outside interface takes on the NAT requirements of an inside interface, as follows:

- No traffic can originate on the outside interface without being translated (or being configured to bypass NAT).

  This requirement is true even if the dynamic NAT statement includes only a few addresses. Other addresses not included in the dynamic NAT statement require a NAT configuration to originate connections, even if the NAT configuration is to bypass NAT and use the original addresses.
- No traffic from the specified inside interface can access hosts behind the outside interface unless you configure a static NAT statement, static identity NAT statement, or a NAT exemption statement for the outside hosts.

If you only configure static NAT for the outside interface, these restrictions do not apply. Traffic between the outside interface and a different inside interface is not affected.

Connection limitations that are set using NAT commands are not applied for outside NAT. (See the "Setting Connection Limits in the NAT Configuration" section on page 9-16.)

You might want to use outside NAT, for example, to accommodate overlapping addresses. (See the "Overlapping Networks" section on page 9-33.)

NAT and Same Security Level Interfaces

NAT is not required between same security level interfaces (see the "Allowing Communication Between Interfaces on the Same Security Level" section on page 6-8 to enable same security communication). However, you can optionally configure NAT if desired. Because there is no "inside" and "outside" when configuring NAT between two interfaces at the same security, connection limits that you set in the NAT configuration apply in both directions.

If you configure dynamic NAT or PAT (**nat** and **global** commands) for any hosts on a local interface when they access hosts on a given same security interface, then for any traffic between those two interfaces, the NAT requirements change for the local interface. Namely, the local interface takes on the NAT requirements of an inside interface, as follows:

- No traffic can originate on the local interface without being translated (or being configured to bypass NAT).

  This requirement is true even if the dynamic NAT statement includes only a few addresses. Other addresses not included in the dynamic NAT statement require a NAT configuration to originate connections, even if the NAT configuration is to bypass NAT and use the original addresses.
- No traffic from the specified same security interface can access hosts behind the local interface unless you configure a static NAT statement, a NAT exemption statement, or an identity NAT statement for the local hosts.

If you only configure static NAT, identity NAT, or NAT exemption for the local interface, these restrictions do not apply. Traffic between the local interface and a different same security interface is not affected.

You might want to configure NAT exemption or identity NAT on same security interfaces to set connection limits. (See the "Setting Connection Limits in the NAT Configuration" section on page 9-16.)

Note The FWSM does not support VoIP inspection engines when you configure NAT on same security interfaces. These inspection engines include Skinny, SIP, and H.323. See the "Inspection Support" section on page 13-2 for supported inspection engines.

Order of NAT Commands Used to Match Local Addresses

The FWSM matches local traffic to NAT commands in the following order:

1. NAT exemption (**nat 0 access-list**)—In order, until the first match. Identity NAT is not included in this category; it is included in the regular static NAT or regular NAT category. We do not recommend overlapping addresses in NAT exemption statements because unexpected results can occur.
2. Static NAT and Static PAT (regular and policy) (**static**)—In order, until the first match. Static identity NAT is included in this category. We do not recommend overlapping addresses in static statements because unexpected results can occur.
3. Policy dynamic NAT (**nat access-list**)—In order, until the first match. Overlapping addresses are allowed.
4. Regular dynamic NAT (**nat**)—Best match. Regular identity NAT is included in this category. The order of the NAT commands does not matter; the NAT statement that best matches the local traffic is used. For example, you can create a general statement to translate all addresses (0.0.0.0) on an interface. If you want to translate a subset of your network (10.1.1.1) to a different address, then you can create a statement to translate only 10.1.1.1. When 10.1.1.1 makes a connection, the specific statement for 10.1.1.1 is used because it matches the local traffic best. We do not recommend using overlapping statements; they use more memory and can slow the performance of the FWSM.

Maximum Number of NAT Statements

The FWSM supports the following numbers of **nat**, **global**, and **static** commands divided between all contexts or in single mode:

- **nat** command—2 K
- **global** command—1,051
- **static** command—2 K

The FWSM also supports up to 3942 access control entries (ACEs) in ACLs used for policy NAT for single mode, and 7,272 ACEs for multiple mode.

Global Address Guidelines

When you translate the local address to a global address, you can use the following global addresses:

- Addresses on the same network as the global interface.

  If you use addresses on the same network as the global interface (through which traffic exits the FWSM), the FWSM uses proxy ARP to answer any requests for translated addresses, and thus intercepts traffic destined for a local address. This solution simplifies routing, because the FWSM does not have to be the gateway for any additional networks. However, this approach does put a limit on the number of available addresses used for translations.

  For PAT, you can even use the IP address of the global interface.
- Addresses on a unique network.

If you need more addresses than are available on the global interface network, you can identify addresses on a different subnet. The FWSM uses proxy ARP to answer any requests for translated addresses, and thus intercepts traffic destined for a local address. If you use OSPF, and you advertise routes on the global interface, then the FWSM advertises the translated addresses. If the global interface is passive (not advertising routes) or you are using static routing, then you need to add a static route on the upstream router that sends traffic destined for the translated addresses to the FWSM.

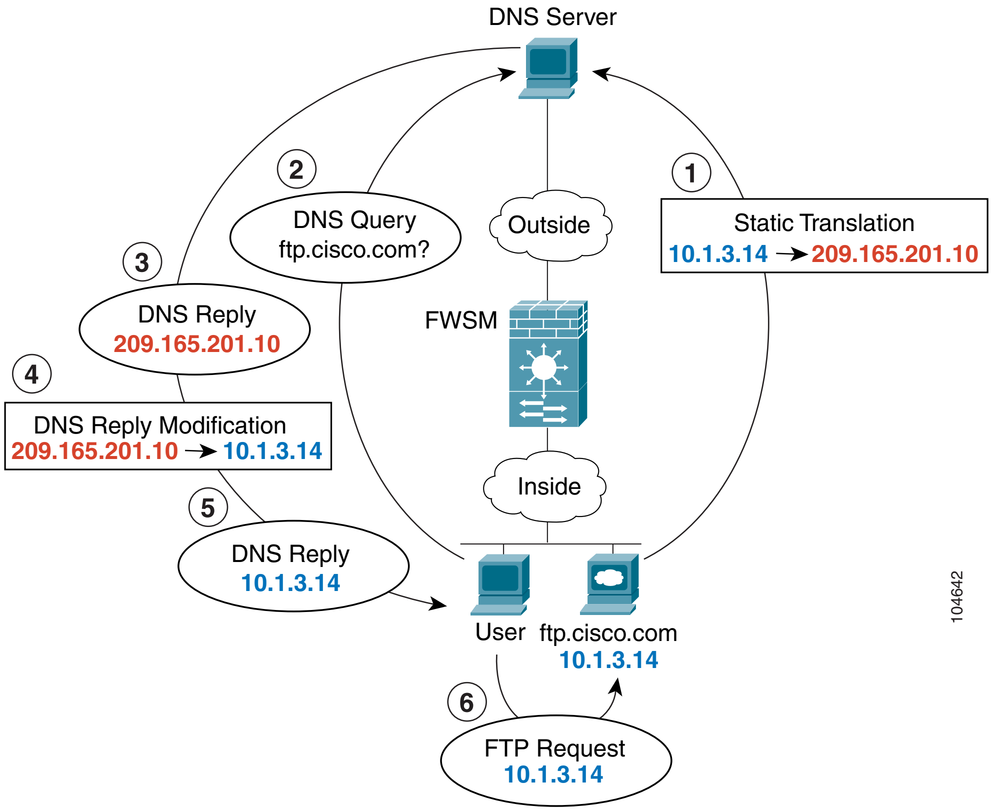
DNS and NAT

You might need to configure the FWSM to modify DNS replies by replacing the address in the reply with an address that matches the NAT configuration. You can configure DNS modification when you configure each NAT translation.

For example, a DNS server is accessible from the outside interface. A server, ftp.cisco.com, is on the inside interface. You configure the FWSM to statically translate the ftp.cisco.com local address (10.1.3.14) to a global address (209.165.201.10) that is visible on the outside network (See Figure 9-6). In this case, you want to enable DNS reply modification on this static statement so that inside users who have access to ftp.cisco.com using the local address receive the local address from the DNS server, and not the global address.

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

Figure 9-6 DNS Reply Modification

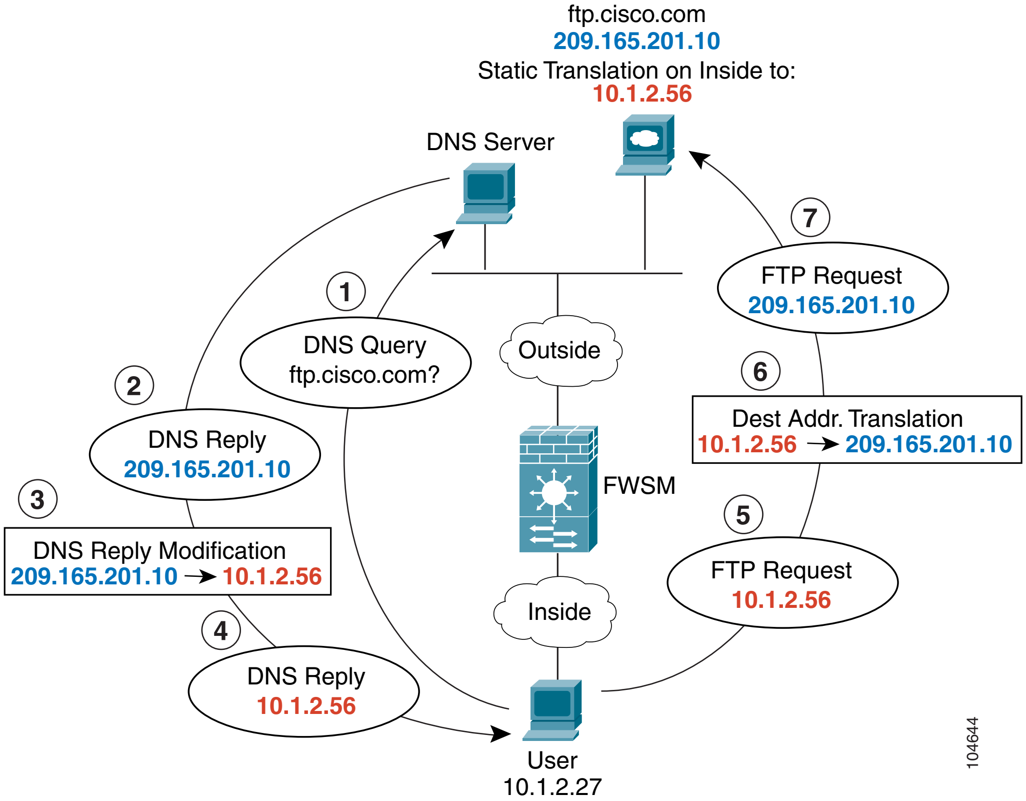


See the following command for this example:

```
FWSM/contexta(config)# static (inside,outside) 209.165.201.10 10.1.3.14 netmask
255.255.255.255 dns
```

Figure 9-7 shows a web server and DNS server on the outside. The FWSM 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 local address, 209.165.20.10. Because you want inside users to use the translated global address for ftp.cisco.com (10.1.2.56) you need to configure DNS reply modification for the static translation.

Figure 9-7 DNS Reply Modification Using Outside NAT



See the following command for this example:

```
FWSM/contexta(config)# static (outside,inside) 10.1.2.56 209.165.201.10 netmask
255.255.255.255 dns
```

Setting Connection Limits in the NAT Configuration

The NAT configuration lets you set some options for traffic that cannot be set anywhere else, including the following:

- Setting the maximum connections—The maximum number of simultaneous TCP and/or UDP connections for the entire subnet up to 65,536.
- Setting the maximum embryonic connections—The maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP intercept feature. (See the "Other Protection Features" section on page 1-6 for more information.)
- Disabling TCP sequence number randomization—Only use this option if another in-line firewall is also randomizing sequence numbers and the result is scrambling the data.

When you do not want to use NAT, such as for a transparent firewall or same security interfaces, you can set these options in an identity NAT statement or a NAT exemption statement.

Using Dynamic NAT and PAT

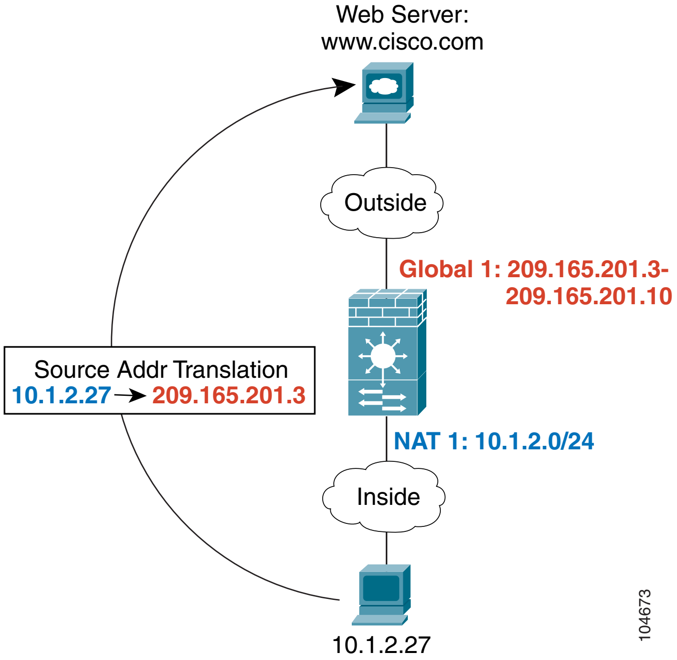
This section includes the following topics:

- Dynamic NAT and PAT Implementation, page 9-17
- Configuring NAT or PAT, page 9-23

Dynamic NAT and PAT Implementation

For dynamic NAT and PAT, you first configure a NAT statement (the **nat** command) identifying the addresses on a given interface that you want to translate. Then you configure a separate global statement (the **global** command) to specify the translated addresses when exiting another interface (in the case of PAT, this is one address). Each NAT statement matches a global statement by comparing the NAT ID, a number that you assign each statement (see Figure 9-8).

Figure 9-8 NAT and Global ID Matching

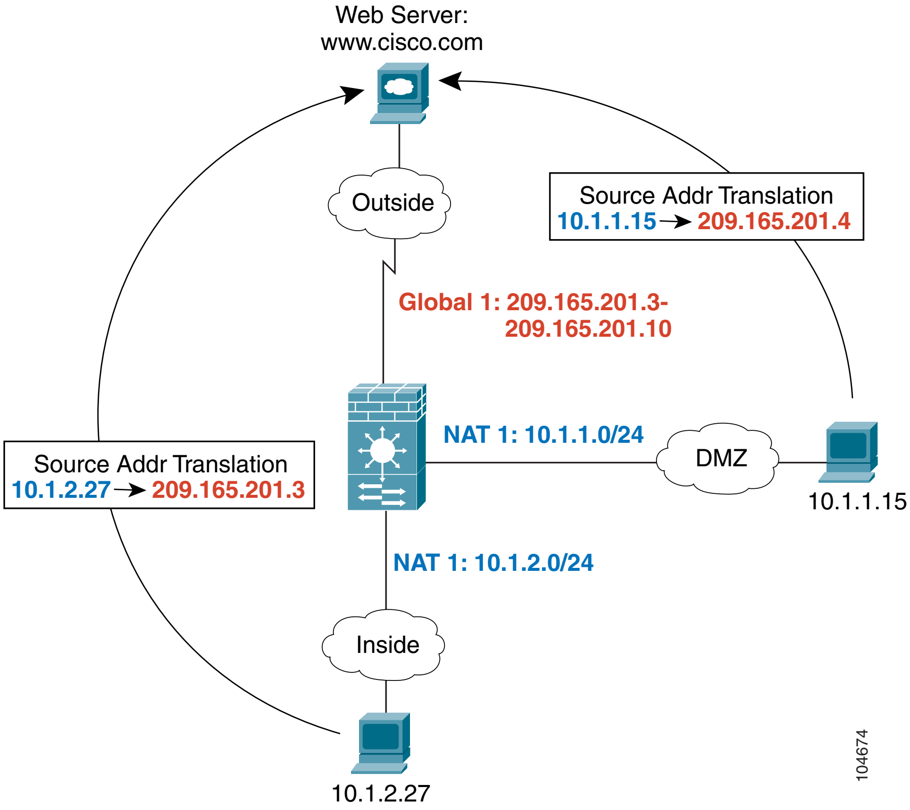


See the following commands for this example:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.0 255.255.255.0
FWSM/contexta(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

You can enter a NAT statement for each interface using the same NAT ID; they all use the same global statement when traffic exits a given interface. For example, you can configure NAT statements for Inside and DMZ interfaces, both on NAT ID 1. Then you configure a global statement on the Outside interface that is also on ID 1. Traffic from the Inside interface and the DMZ interface share a NAT pool or a PAT address when exiting the Outside interface (see Figure 9-9).

Figure 9-9 NAT Statements on Multiple Interfaces

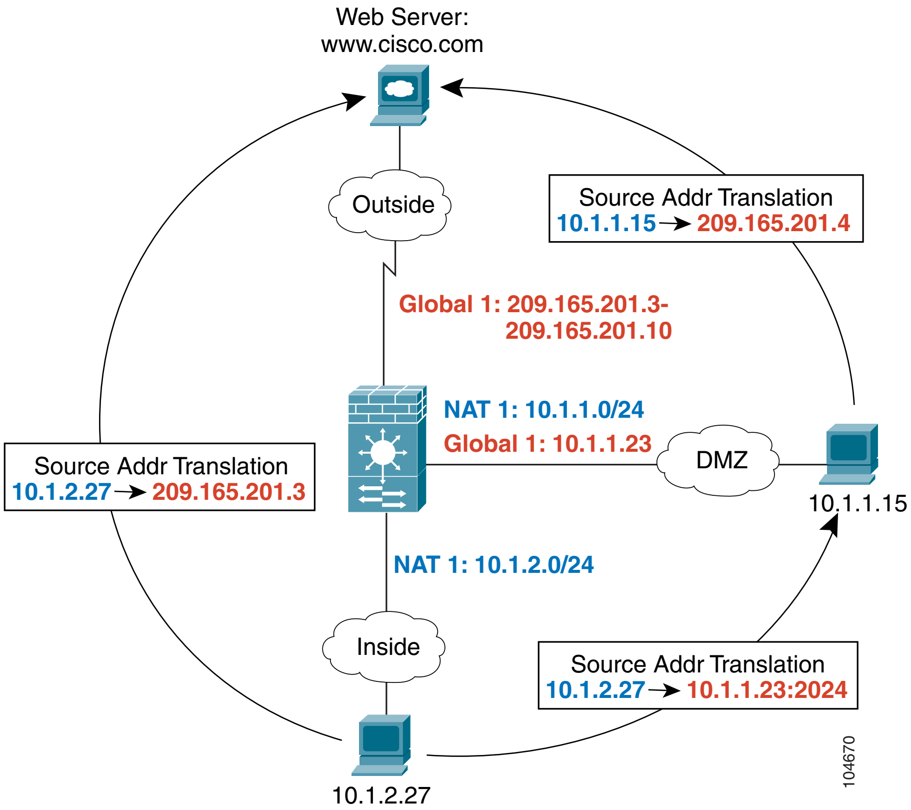


See the following commands for this example:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.0 255.255.255.0
FWSM/contexta(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
FWSM/contexta(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

You can also enter a global statement for each interface using the same NAT ID. If you enter a global statement for the Outside and DMZ interfaces on ID 1, then the Inside NAT statement identifies traffic to be translated when going to both the Outside and the DMZ interfaces. Similarly, if you also enter a NAT statement for the DMZ interface on ID 1, then the global statement on the Outside interface is also used for DMZ traffic. (See Figure 9-10).

Figure 9-10 Global and NAT Statements on Multiple Interfaces

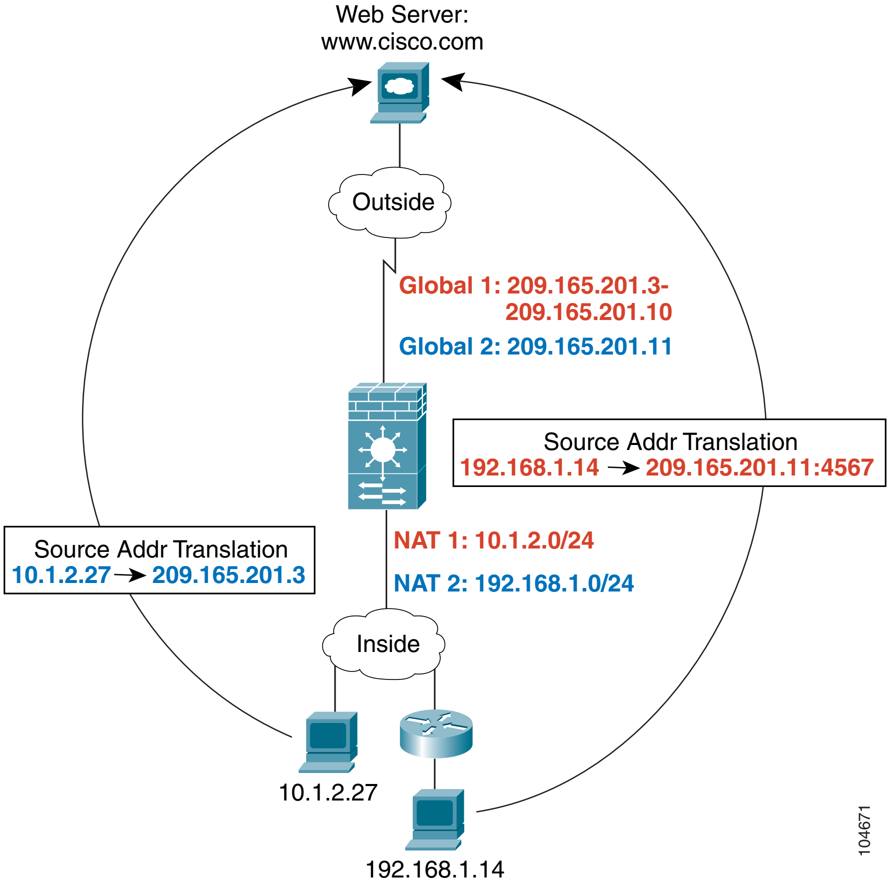


See the following commands for this example:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.0 255.255.255.0
FWSM/contexta(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
FWSM/contexta(config)# global (outside) 1 209.165.201.3-209.165.201.10
FWSM/contexta(config)# global (dmz) 1 10.1.1.23
```

If you use different NAT IDs, you can identify different sets of host addresses to have different global addresses. For example, on the Inside interface, you can have two NAT statements on two different NAT IDs. On the Outside interface, you configure two global statements for these two IDs. Then, when traffic from Inside network A exits the Outside interface, the IP addresses are translated to pool A addresses; while traffic from Inside network B are translated to pool B addresses (see Figure 9-11). If you use policy NAT, you can specify the same local addresses for multiple NAT statements, as long as the source address/port and destination address/port is unique for each statement. For regular NAT, you must identify different local addresses for each statement.

Figure 9-11 Different NAT IDs

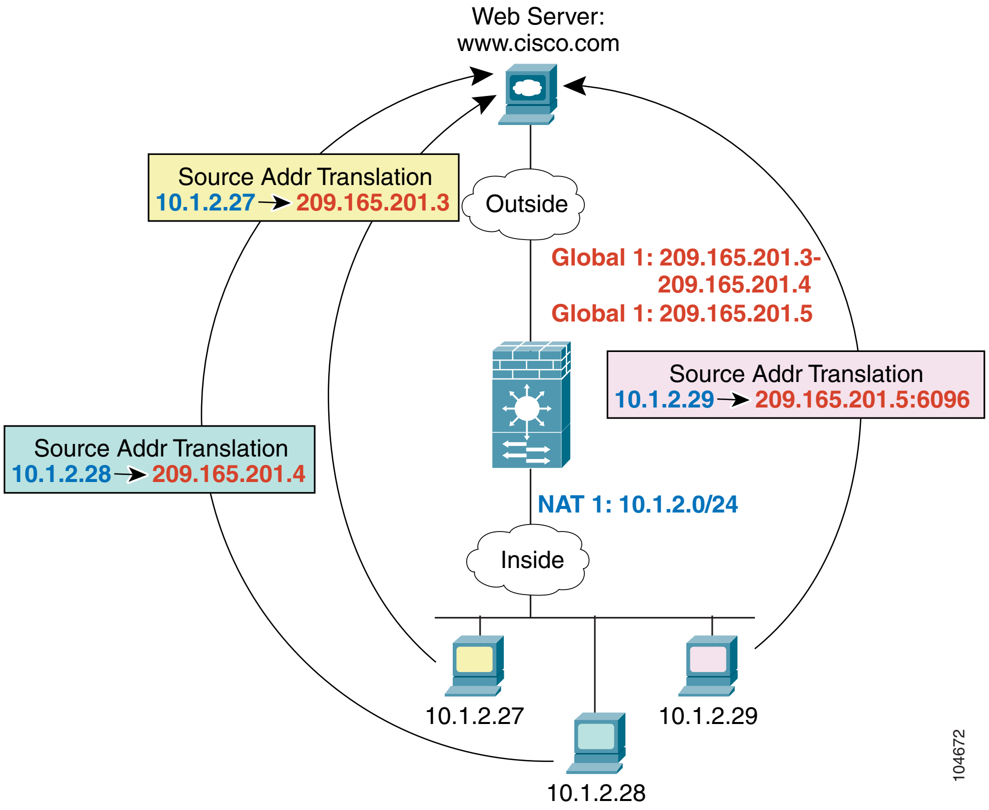


See the following commands for this example:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.0 255.255.255.0
FWSM/contexta(config)# nat (inside) 2 192.168.1.0 255.255.255.0
FWSM/contexta(config)# global (outside) 1 209.165.201.3-209.165.201.10
FWSM/contexta(config)# global (outside) 2 209.165.201.11
```

You can enter multiple global statements for one interface using the same NAT ID; the FWSM uses the dynamic NAT global statements first, in the order they are in the configuration, and then uses the PAT global statements in order. You might want to enter both a dynamic NAT global statement and a PAT global statement if you need to use dynamic NAT for a particular application, but want to have a backup PAT statement in case all the dynamic NAT addresses are used up. Similarly, you might enter two PAT statements if you need more than the approximately 64000 connections that a single PAT global statement supports (see Figure 9-12).

Figure 9-12 NAT and PAT Together



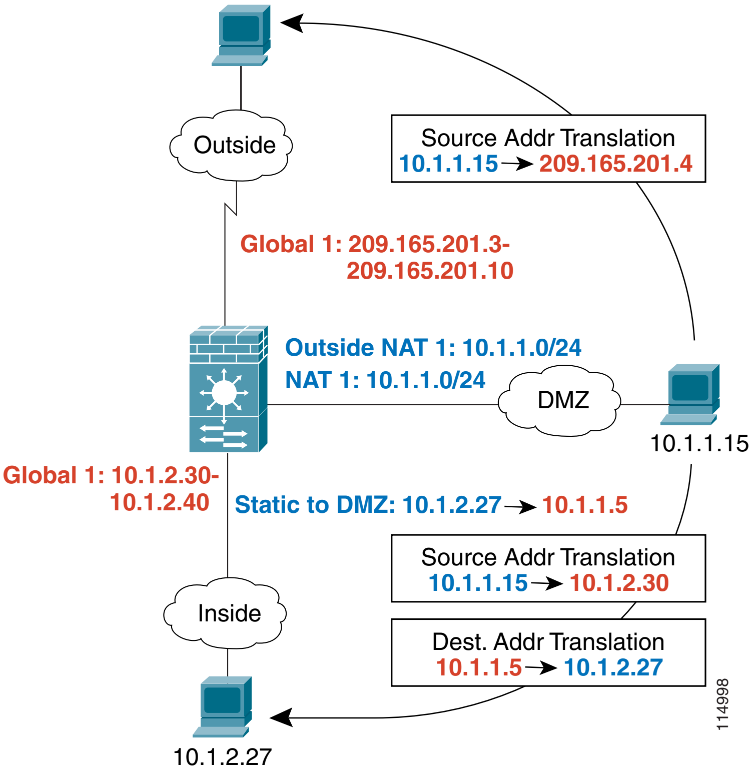
See the following commands for this example:

```
FWSM/contexta(config)# nat (inside) 1 10.1.2.0 255.255.255.0
FWSM/contexta(config)# global (outside) 1 209.165.201.3-209.165.201.4
FWSM/contexta(config)# global (outside) 1 209.165.201.5
```

For outside NAT (see the "Outside NAT" section on page 9-10 for more information), you need to identify the NAT statement for outside NAT (the **outside** keyword). If you also want to translate the same traffic when it accesses an inside interface (for example, traffic on a DMZ is translated when accessing the Inside and the Outside interfaces), then you must configure a separate NAT statement without the **outside** option. In this case, you can identify the same addresses in both statements and use the same

NAT ID (see Figure 9-13). Note that for outside NAT (DMZ interface to Inside interface), the inside host uses a static NAT statement to allow outside access, so both the source and destination addresses are translated.

Figure 9-13 Outside NAT and Inside NAT Combined



See the following commands for this example:

```
FWSM/contexta(config)# nat (dmz) 1 10.1.1.0 255.255.255.0 outside
FWSM/contexta(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
FWSM/contexta(config)# static (inside,dmz) 10.1.2.27 10.1.1.5 netmask 255.255.255.255
FWSM/contexta(config)# global (outside) 1 209.165.201.3-209.165.201.4
FWSM/contexta(config)# global (inside) 1 10.1.2.30-1-10.1.2.40
```

Configuring NAT or PAT

This section tells how to configure dynamic NAT or dynamic PAT. The configuration for dynamic NAT and PAT are almost identical; for NAT you specify a range of global addresses, and for PAT you specify a single address.

Figure 9-14 shows a typical dynamic NAT scenario. Only local traffic can originate connections, and the global address is dynamically assigned from a pool.

Figure 9-14 Dynamic NAT

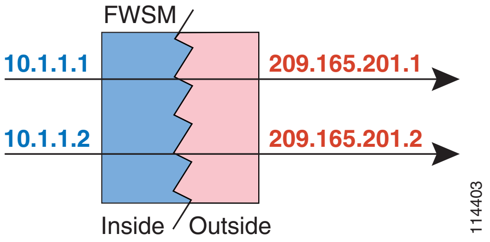
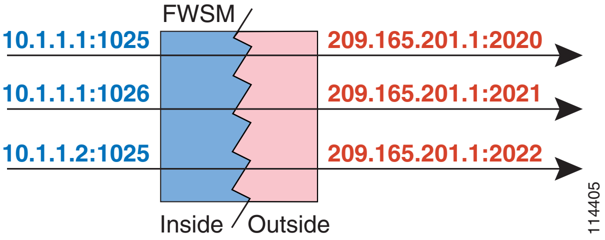


Figure 9-15 shows a typical dynamic PAT scenario. Only local traffic can originate connections, the global address is the same for each translation, but the port is dynamically assigned.

Figure 9-15 Dynamic PAT



For more information about dynamic NAT, see the "Dynamic NAT" section on page 9-3. For more information about PAT, see the "PAT" section on page 9-4.

Note If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To configure dynamic NAT or PAT, follow these steps:

Step 1 To identify the local addresses that you want to translate, enter one of the following commands:

- Policy NAT:

```
FWSM/contexta(config)# nat (local_interface) nat_id access-list acl_name [dns]
[outside | [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]]
```

  You can identify overlapping addresses in other **nat** statements. For example, you can identify 10.1.1.0 in one statement, but 10.1.1.1 in another. The traffic is matched to a policy NAT statement in order, until the first match, or for regular NAT, using the best match.

See the following description about options for this command:

- **access-list** *acl_name*—Identify the local addresses and destination addresses using an extended ACL. Create the ACL using the **access-list** command (see the "Adding an Extended Access Control List" section on page 10-13). This ACL should include only **permit** access control entries (ACEs). You can optionally specify the local and destination ports in the ACL using the **eq** operator.
- *nat_id*—An integer between 1 and 65535. The NAT ID must match a **global** statement NAT ID. See the "Dynamic NAT and PAT Implementation" section on page 9-17 for more information about how NAT IDs are used. **0** is reserved for NAT exemption. (See the "Configuring NAT Exemption" section on page 9-31 for more information about NAT exemption.)
- **dns**—If your NAT statement includes the address of a host that has an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host; one needs the global address and one needs the local address. This option rewrites the address in the DNS reply to the client. The translated host needs to be on the same interface as either the client or the DNS server. Typically, hosts that need to allow access from other interfaces use a static translation, so this option is more likely to be used with the **static** command. (See the "DNS and NAT" section on page 9-13 for more information.)
- **outside**—If this interface is on a lower security level than the interface you identify by the matching **global** statement, then you must enter **outside** to identify the NAT instance as outside NAT. (See the "Outside NAT" section on page 9-10 for more information.)
- **norandomseq—**No TCP Initial Sequence Number (ISN) randomization. Only use this option if another in-line firewall is also randomizing sequence numbers and the result is scrambling the data. See the "Security Level Overview" section on page 6-6 for information about TCP sequence numbers.
- **tcp** *tcp_max_conns,* **udp** *udp_max_conns*—The maximum number of simultaneous TCP and/or UDP connections for the entire subnet up to 65,536. The default is 0 for both protocols, which means the maximum connections.
- *emb_limit*—The maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. (See the "Other Protection Features" section on page 1-6 for more information.) The default is 0, which means the maximum embryonic connections. You must enter the **tcp** *tcp_max_conns* before you enter the *emb_limit*. If you want to use the default value for *tcp_max_conns*, but change the *emb_limit*, then enter **0** for *tcp_max_conns*. Not supported for outside NAT.

- Regular NAT:

```
FWSM/contexta(config)# nat (local_interface) nat_id local_ip [mask [dns] [outside |
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]]]
```

The *nat_id* is an integer between 1 and 2147483647. The NAT ID must match a **global** statement NAT ID. See the "Dynamic NAT and PAT Implementation" section on page 9-17 for more information about how NAT IDs are used. **0** is reserved for identity NAT. See the "Configuring Identity NAT" section on page 9-29 for more information about identity NAT.

See the policy NAT command above for information about other options.

Step 2 To identify the global address(es) to which you want to translate the local addresses when they exit a particular interface, enter the following command:

```
FWSM/contexta(config)# global (global_interface) nat_id {global_ip[-global_ip] |
interface}
```

This NAT ID must match a **nat** statement NAT ID. The matching **nat** statement identifies the addresses that you want to translate when they exit this interface.

You can specify a single address (for PAT) or a range of addresses (for NAT). The range can go across subnet boundaries if desired. For example, you can specify the following "supernet":

```
192.168.1.1-192.168.2.254
```

For example, to translate the 10.1.1.0/24 network on the inside interface, and to change the embryonic limit, enter the following command. You must specify the **tcp** *tcp_max_conns* before specifying *emb_limit*, so the command enters the default setting of **0** for *tcp_max_conns*.

```
FWSM/contexta(config)# nat (inside) 1 10.1.1.0 255.255.255.0 tcp 0 200
FWSM/contexta(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

To identify a pool of addresses for dynamic NAT as well as a PAT address for when the NAT pool is exhausted, enter the following commands:

```
FWSM/contexta(config)# nat (inside) 1 10.1.1.0 255.255.255.0 tcp 5000 1000 udp 5000
FWSM/contexta(config)# global (outside) 1 209.165.201.5
FWSM/contexta(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

To translate the lower security dmz network addresses so they appear to be on the same network as the inside network (10.1.1.0), for example, to simplify routing, enter the following commands:

```
FWSM/contexta(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
FWSM/contexta(config)# global (inside) 1 10.1.1.45
```

To identify a single local address with two different destination addresses using policy NAT, enter the following commands (see Figure 9-3 on page 9-8 for a related graphic):

```
FWSM/contexta(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
FWSM/contexta(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
FWSM/contexta(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
FWSM/contexta(config)# global (outside) 1 209.165.202.129
FWSM/contexta(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
FWSM/contexta(config)# global (outside) 2 209.165.202.130
```

To identify a single local address/destination address pair that use different ports using policy NAT, enter the following commands (see Figure 9-4 on page 9-9 for a related graphic):

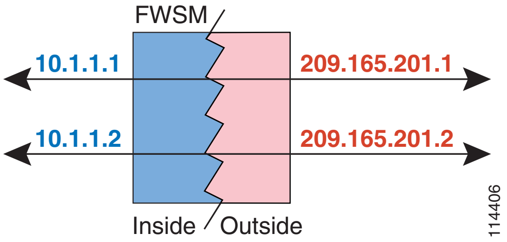
```
FWSM/contexta(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
FWSM/contexta(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
FWSM/contexta(config)# nat (inside) 1 access-list WEB
FWSM/contexta(config)# global (outside) 1 209.165.202.129
FWSM/contexta(config)# nat (inside) 2 access-list TELNET
FWSM/contexta(config)# global (outside) 2 209.165.202.130
```

Using Static NAT

This section tells how to configure a static translation.

Figure 9-16 shows a typical static NAT scenario. Both local and global traffic can originate connections, and the global address is statically assigned.

Figure 9-16 Static NAT



You cannot use the same local or global address in multiple **static** statements between the same two interfaces. Do not use an address that is also defined as a dynamic PAT address in a **global** statement.

For more information about static NAT, see the "Static NAT" section on page 9-5.

Note If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To configure static NAT, enter one of the following commands.

- For policy static NAT, enter the following command:

  ```
  FWSM/contexta(config)# static (local_interface,global_interface)
  {global_ip | interface} access-list acl_name [dns] [norandomseq] [[tcp] tcp_max_conns
  [emb_limit]] [udp udp_max_conns]
  ```

  Create the ACL using the **access-list** command (see the "Adding an Extended Access Control List" section on page 10-13). This ACL should include only **permit** access control entries (ACEs). The source subnet mask used in the ACL is also used for the global addresses. You can also specify the local and destination ports in the ACL using the **eq** operator. See the "Policy NAT" section on page 9-8 for more information.

  See the "Configuring NAT or PAT" section on page 9-23 for information about the other options.

- To configure regular static NAT, enter the following command:

  ```
  FWSM/contexta(config)# static (local_interface,global_interface)
  {global_ip | interface} local_ip [netmask mask] [dns] [norandomseq]
  [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
  ```

  See the "Configuring NAT or PAT" section on page 9-23 for information about the options.

For example, the following policy static NAT example shows a single local address that is translated to two global addresses depending on the destination address (see Figure 9-3 on page 9-8 for a related graphic):

```
FWSM/contexta(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
FWSM/contexta(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
FWSM/contexta(config)# static (inside,outside) 209.165.202.129 access-list NET1
FWSM/contexta(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

The following command maps an inside IP address (10.1.1.3) to an outside IP address (209.165.201.12):

```
FWSM/contexta(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255
```

The following command maps the outside address (209.165.201.15) to an inside address (10.1.1.6):

```
FWSM/contexta(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

The following command statically maps an entire subnet:

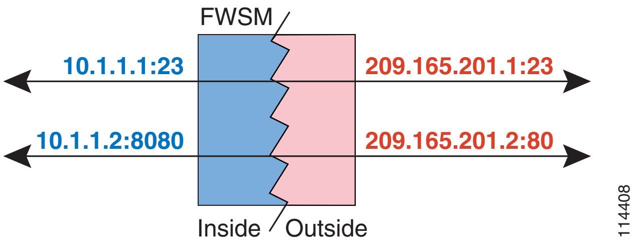
```
FWSM/contexta(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

Using Static PAT

This section tells how to configure a static port translation. Static PAT lets you translate the local IP address to a global IP address, as well as the local port to a global port. You can choose to translate the same port, which lets you translate specific types of traffic, or you can take it further by translating to a different port.

Figure 9-17 shows a typical static PAT scenario. Both local and global traffic can originate connections, and the global address and port is statically assigned.

Figure 9-17 Static PAT



You cannot use the same local or global address in multiple **static** statements between the same two interfaces. Do not use an address that is also defined as a dynamic PAT address in a **global** statement.

For more information about static PAT, see the "Static PAT" section on page 9-5.

Note If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To configure static PAT, enter one of the following commands.

- For policy static PAT, enter the following command:

  ```
  FWSM/contexta(config)# static (local_interface,global_interface) {tcp | udp}
  {global_ip | interface} global_port access-list acl_name [dns] [norandomseq]
  [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
  ```

  Create the ACL using the **access-list** command (see the "Adding an Extended Access Control List" section on page 10-13). The protocol in the ACL must match the protocol you set in this command. For example, if you specify **tcp** in the static command, then you must specify **tcp** in the ACL. Specify the port using the **eq** operator. This ACL should include only **permit** access control entries (ACEs). The source subnet mask used in the ACL is also used for the global addresses.

  See the "Configuring NAT or PAT" section on page 9-23 for information about the other options.

- To configure regular static PAT, enter the following command:

  ```
  FWSM/contexta(config)# static (local_interface,global_interface) {tcp | udp}
  {global_ip | interface} global_port local_ip local_port [netmask mask]
  [dns] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
  ```

  See the "Configuring NAT or PAT" section on page 9-23 for information about the options.

For example, for Telnet traffic initiated from hosts on the 10.1.3.0 network to the FWSM outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering the following commands:

```
FWSM/contexta(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
FWSM/contexta(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

For HTTP traffic initiated from hosts on the 10.1.3.0 network to the FWSM outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering:

```
FWSM/contexta(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
FWSM/contexta(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

To redirect Telnet traffic from the FWSM outside interface (10.1.2.14) to the inside host at 10.1.1.15, enter the following command:

```
FWSM/contexta(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
```

If you want to allow the local Telnet server above to initiate connections, though, then you need to provide additional translation. For example, to translate all other types of traffic, enter the following commands. The original **static** command provides translation for Telnet to the server, while the **nat** and **global** commands provide PAT for outbound connections from the server.

```
FWSM/contexta(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
FWSM/contexta(config)# nat (inside) 1 10.1.1.15 255.255.255.255
FWSM/contexta(config)# global (outside) 1 10.1.2.14
```

If you also have a separate translation for all inside traffic, and the inside hosts use a different global address from the Telnet server, you can still configure traffic initiated from the Telnet server to use the same global address as the **static** statement that allows Telnet traffic to the server. You need to create a more exclusive **nat** statement just for the Telnet server. Because **nat** statements are read for the best match, more exclusive **nat** statements are matched before general statements. The following example shows the Telnet **static** statement, the more exclusive **nat** statement for initiated traffic from the Telnet server, and the statement for other inside hosts, which uses a different global address.

```
FWSM/contexta(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
FWSM/contexta(config)# nat (inside) 1 10.1.1.15 255.255.255.255
FWSM/contexta(config)# global (outside) 1 10.1.2.14
FWSM/contexta(config)# nat (inside) 2 10.1.1.0 255.255.255.0
FWSM/contexta(config)# global (outside) 2 10.1.2.78
```

To translate a well-known port (80) to another port (8080), enter the following command:

```
FWSM/contexta(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

Bypassing NAT

You can bypass NAT using identity NAT, static identity NAT, or NAT exemption. See the "Bypassing NAT" section on page 9-7 for more information about these methods. This section includes the following topics:

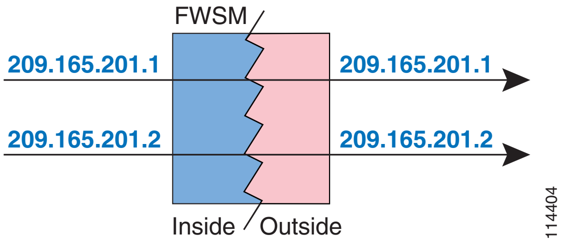
- Configuring Identity NAT, page 9-29
- Configuring Static Identity NAT, page 9-30
- Configuring NAT Exemption, page 9-31

Configuring Identity NAT

Identity NAT translates the local IP address to the same IP address, and only local traffic can originate connections. (For same security level interfaces, hosts connected to any interface on the same security level can initiate traffic.)

Figure 9-18 shows a typical identity NAT scenario.

Figure 9-18 Identity NAT



Note If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To configure identity NAT, enter the following command:

```
FWSM/contexta(config)# nat (local_interface) 0 local_ip [mask [dns] [outside |
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]]]
```

See the "Configuring NAT or PAT" section on page 9-23 for information about the options.

For example, to use identity NAT for the inside 10.1.1.0/24 network, enter the following command:

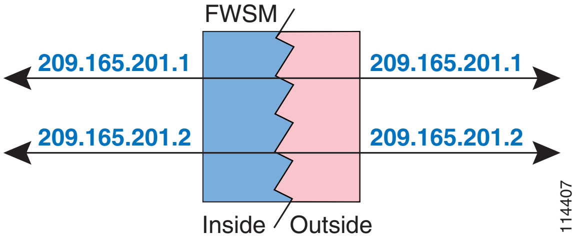
```
FWSM/contexta(config)# nat (inside) 0 10.1.1.0 255.255.255.0
```

Configuring Static Identity NAT

Static identity NAT translates the local IP address to the same IP address, and allows both local and global traffic to originate connections. Static identity NAT lets you use regular NAT or policy NAT. Policy NAT allow you to identify the local and destination addresses when determining the local traffic to translate (see the "Policy NAT" section on page 9-8 for more information about policy NAT). For example, you can use policy static identity NAT for an inside address when it accesses the outside interface and the destination is server A, but use a normal translation when accessing the outside server B.

Figure 9-19 shows a typical static identity NAT scenario.

Figure 9-19 Static Identity NAT



Note If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To configure static identity NAT, enter one of the following commands:

- To configure policy static identity NAT, enter the following command:

  ```
  FWSM/contexta(config)# static (local_interface,global_interface) local_ip access-list
  acl_id [dns] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
  ```

  Create the ACL using the **access-list** command (see the "Adding an Extended Access Control List" section on page 10-13). This ACL should include only **permit** access control entries (ACEs). Make sure the source address in the ACL matches the first *local_ip* in this command. See the "Policy NAT" section on page 9-8 for more information.

  See the "Configuring NAT or PAT" section on page 9-23 for information about the other options.

- To configure regular static identity NAT, enter the following command:

  ```
  FWSM/contexta(config)# static (local_interface,global_interface) local_ip local_ip
  [netmask mask] [dns] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
  udp_max_conns]
  ```

Specify the same IP address for both *local_ip* variables.

See the "Configuring NAT or PAT" section on page 9-23 for information about the other options.

For example, the following command uses static identity NAT for an inside IP address (10.1.1.3) when accessed by the outside:

```
FWSM/contexta(config)# static (inside,outside) 10.1.1.3 10.1.1.3 netmask 255.255.255.255
```

The following command uses static identity NAT for an outside address (209.165.201.15) when accessed by the inside:

```
FWSM/contexta(config)# static (outside,inside) 209.165.201.15 209.165.201.15 netmask
255.255.255.255
```

The following command statically maps an entire subnet:

```
FWSM/contexta(config)# static (inside,dmz) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
```

The following static identity policy NAT example shows a single local address that uses identity NAT when accessing one destination address, and a translation when accessing another:

```
FWSM/contexta(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
FWSM/contexta(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
FWSM/contexta(config)# static (inside,outside) 10.1.2.27 access-list NET1
FWSM/contexta(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

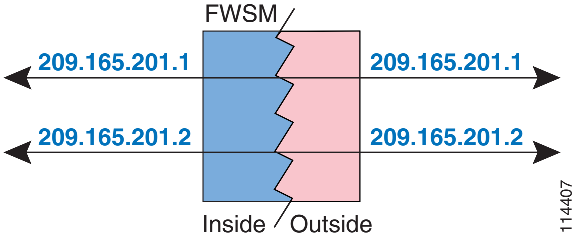
Configuring NAT Exemption

NAT exemption translates the local IP address to the same IP address, and allows both local and global traffic to originate connections. NAT exemption lets you specify the local and destination addresses when determining the local traffic to translate (similar to policy NAT), so you have greater control using NAT exemption than identity NAT. However unlike policy NAT, NAT exemption does not consider the ports in the ACL.

Note In multiple context mode, you cannot initiate connections from an interface shared between contexts when you use NAT exemption for the destination address. The classifier can only assign packets from a shared interface to a context when you configure a static statement for the destination address. For example, if you share the outside interface, you cannot use NAT exemption on an inside interface if you want outside traffic to reach the inside addresses. The classifier only looks at static statements where the global interface matches the source interface of the packet. Because NAT exemption does not identify a global interface, the classifier does not consider those NAT statements for classification purposes.

Figure 9-19 shows a typical NAT exemption scenario.

Figure 9-20 NAT Exemption



Note If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To configure NAT exemption, enter the following command:

```
FWSM/contexta(config)# FWSM/contexta(config)# nat (local_interface) 0 access-list acl_name
[outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

Create the ACL using the **access-list** command (see the "Adding an Extended Access Control List" section on page 10-13). This ACL should include only **permit** access control entries (ACEs). Do not specify the local and destination ports in the ACL; NAT exemption does not consider the ports.

See the "Configuring NAT or PAT" section on page 9-23 for information about the other options.

For example, to exempt an inside network when accessing any destination address, enter the following command:

```
FWSM/contexta(config)# access-list EXEMPT permit ip 10.1.2.0 255.255.255.0 any
FWSM/contexta(config)# nat (inside) 0 access-list EXEMPT
```

To exempt an inside address when accessing two different destination addresses, enter the following commands:

```
FWSM/contexta(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
FWSM/contexta(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
FWSM/contexta(config)# nat (inside) 0 access-list NET1
```

NAT Examples

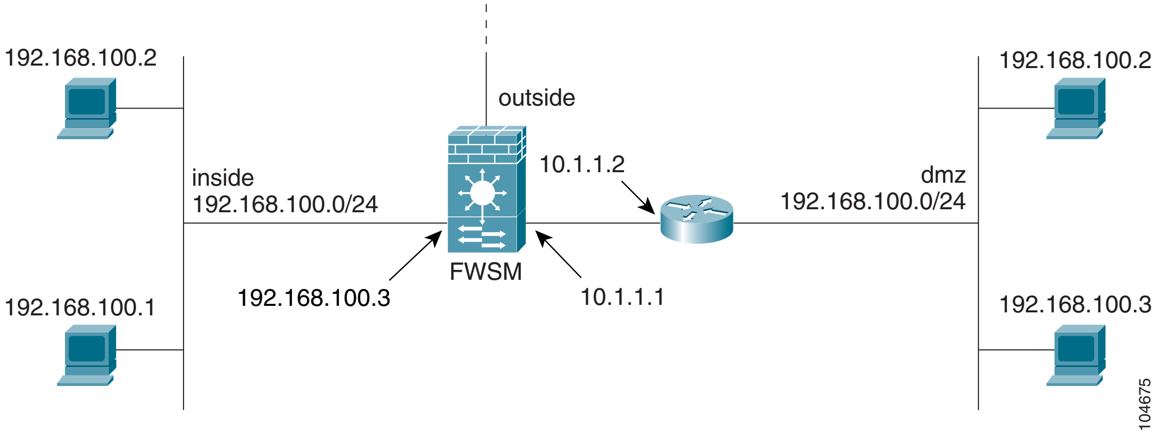
The following sections show typical scenarios that use NAT solutions:

- Overlapping Networks, page 9-33
- Redirecting Ports, page 9-34

Overlapping Networks

In Figure 9-21, the FWSM connects two private networks with overlapping address ranges.

Figure 9-21 Using Outside NAT with Overlapping Networks



Two networks use an overlapping address space (192.168.100.0/24), but hosts on each network must communicate (as allowed by ACLs). Without NAT, when a host on the inside network tries to access a host on the overlapping dmz network, the packet never makes it past the FWSM, which sees the packet as having a destination address on the inside network. Moreover, if the destination address is being used by another host on the inside network, that host receives the packet.

To solve this problem, use NAT to provide non-overlapping addresses. If you want to allow access in both directions, use static NAT for both networks. If you only want to allow the inside interface to access hosts on the dmz, then you can use dynamic NAT for the inside addresses, and static NAT for the dmz addresses you want to access. This example shows static NAT.

To configure static NAT for these two interfaces, follow these steps. The 10.1.1.0/24 network on the dmz is not translated.

Step 1 Translate 192.168.100.0/24 on the inside to 10.1.2.0 /24 when it accesses the dmz by entering the following command:

```
FWSM/contexta(config)# static (inside,dmz) 10.1.2.0 192.168.100.0 netmask 255.255.255.0
```

Step 2 Translate the 192.168.100.0/24 network on the dmz to 10.1.3.0/24 when it accesses the inside by entering the following command:

```
FWSM/contexta(config)# static (dmz,inside) 10.1.3.0 192.168.100.0 netmask 255.255.255.0
```

Step 3 Configure the following static routes so that traffic to the dmz network can be routed correctly by the FWSM:

```
FWSM/contexta(config)# route dmz 192.168.100.128 255.255.255.128 10.1.1.2 1
FWSM/contexta(config)# route dmz 192.168.100.0 255.255.255.128 10.1.1.2 1
```

The FWSM already has a connected route for the inside network. These static routes allow the FWSM to send traffic for the 192.168.100.0/24 network out the dmz interface to the gateway router at 10.1.1.2. (You need to split the network into two because you cannot create a static route with the exact same network as a connected route.) Alternatively, you could use a more broad route for the dmz traffic, such as a default route.

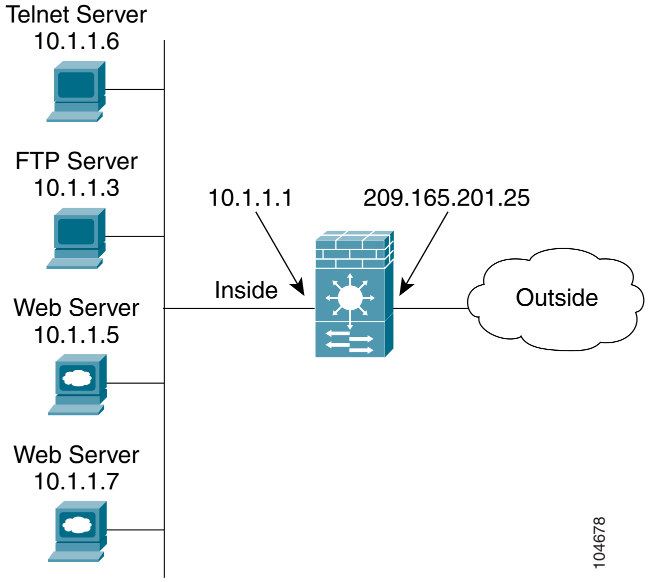
If host 192.168.100.2 on the dmz network wants to initiate a connection to host 192.168.100.2 on the inside network, the following events occur:

1. The dmz host 192.168.100.2 sends the packet to IP address 10.1.2.2.
2. When the FWSM receives this packet, the FWSM translates the source address from 192.168.100.2 to 10.1.3.2.
3. Then the FWSM translates the destination address from 10.1.2.2 to 192.168.100.2, and the packet is forwarded.

Redirecting Ports

Figure 9-22 illustrates a typical network scenario in which the port redirection feature might be useful.

Figure 9-22 Port Redirection Using Static PAT



In the configuration described in this section, port redirection occurs for hosts on external networks as follows:

- Telnet requests to IP address 209.165.201.5 are redirected to 10.1.1.6
- FTP requests to IP address 209.165.201.5 are redirected to 10.1.1.3
- HTTP request to FWSM outside IP address 209.165.201.25 are redirected to 10.1.1.5
- HTTP port 8080 requests to PAT address 209.165.201.15 are redirected to 10.1.1.7 port 80

To implement this scenario, complete the following steps:

Step 1 Configure PAT for the inside network by entering the following commands:

```
FWSM/contexta(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
FWSM/contexta(config)# global (outside) 1 209.165.201.15
```

Step 2 Redirect Telnet requests for 209.165.201.5 to 10.1.1.6 by entering the following command:

```
FWSM/contexta(config)# static (inside,outside) tcp 209.165.201.5 telnet 10.1.1.6 telnet
netmask 255.255.255.255
```

Step 3 Redirect FTP requests for IP address 209.165.201.5 to 10.1.1.3 by entering the following command:

```
FWSM/contexta(config)# static (inside,outside) tcp 209.165.201.5 ftp 10.1.1.3 ftp netmask
255.255.255.255
```

Step 4 Redirect HTTP requests for the FWSM outside interface address to 10.1.1.5 by entering the following command:

```
FWSM/contexta(config)# static (inside,outside) tcp interface www 10.1.1.5 www netmask
255.255.255.255
```

Step 5 Redirect HTTP requests on port 8080 for PAT address 209.165.201.15 to 10.1.1.7 port 80 by entering the following command:

```
FWSM/contexta(config)# static (inside,outside) tcp 209.165.201.15 8080 10.1.1.7 www
netmask 255.255.255.255
```