CHAPTER 29

Configuring Dynamic NAT and PAT

This section describes dynamic network address translation. The configuration for dynamic NAT and PAT are almost identical; for NAT you specify a range of mapped addresses, and for PAT you specify a single address.

This chapter includes the following topics:

- Information About Dynamic NAT and PAT, page 29-1
- Licensing Requirements for Dynamic NAT and PAT, page 29-10
- Guidelines and Limitations, page 29-11
- Default Settings, page 29-11
- Configuring Dynamic NAT or Dynamic PAT, page 29-13
- Monitoring Dynamic NAT and PAT, page 29-18
- Configuration Examples for Dynamic NAT and PAT, page 29-18
- Feature History for Dynamic NAT and PAT, page 29-19

Information About Dynamic NAT and PAT

This section includes the following topics:

- Information About Dynamic NAT, page 29-1
- Information About PAT, page 29-4
- Information About Implementing Dynamic NAT and PAT, page 29-5

Information 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 may include fewer addresses than the real group. When a host you want to translate accesses the destination network, the ASA assigns the host an IP address from the mapped pool. The translation is added 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. For an example, see the **timeout xlate** command in the *Cisco ASA 5500 Series Command Reference*. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, although the connection is allowed by an access list, and

the ASA rejects any attempt to connect to a real host address directly. See Chapter 28, "Configuring Static NAT," or Chapter 30, "Configuring Static PAT," for information about how to obtain reliable access to hosts.

Note In some cases, a translation is added for a connection, although the session is denied by the ASA. This condition occurs with an outbound access list, a management-only interface, or a backup interface in which the translation times out normally. For an example, see the **show xlate** command in the *Cisco ASA 5500 Series Command Reference*.

Figure 29-1 shows a remote host attempting to connect to the real address. The connection is denied because the ASA only allows returning connections to the mapped address.

Figure 29-1 Remote Host Attempts to Connect to the Real Address

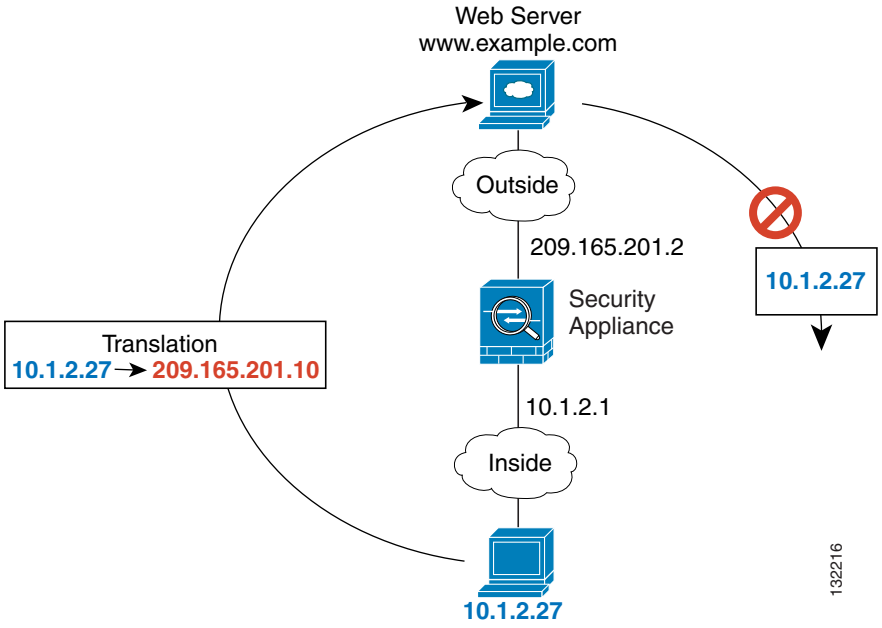
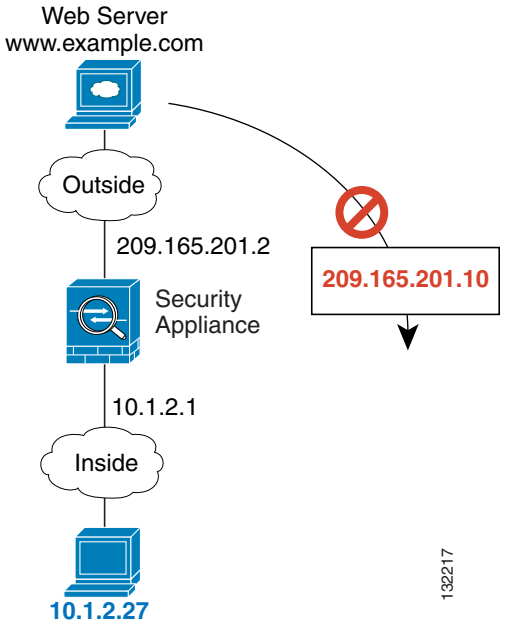


Figure 29-2 shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the ASA drops the packet.

Figure 29-2 Remote Host Attempts to Initiate a Connection to a Mapped Address



Note For the duration of the translation, a remote host can initiate a connection to the translated host if an access list 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 list.

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 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; 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 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.

See the "When to Use Application Protocol Inspection" section on page 40-2 for more information about NAT and PAT support.

Information About PAT

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. If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used.

Each connection requires a separate translation 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.

After the connection expires, the port translation also expires after 30 seconds of inactivity. The timeout is not configurable. Users on the destination network cannot reliably initiate a connection to a host that uses PAT (even if the connection is allowed by an access list). Not only can you not predict the real or mapped port number of the host, but the ASA does not create a translation at all unless the translated host is the initiator. See Chapter 28, "Configuring Static NAT," or Chapter 30, "Configuring Static PAT," for information about reliable access to hosts.

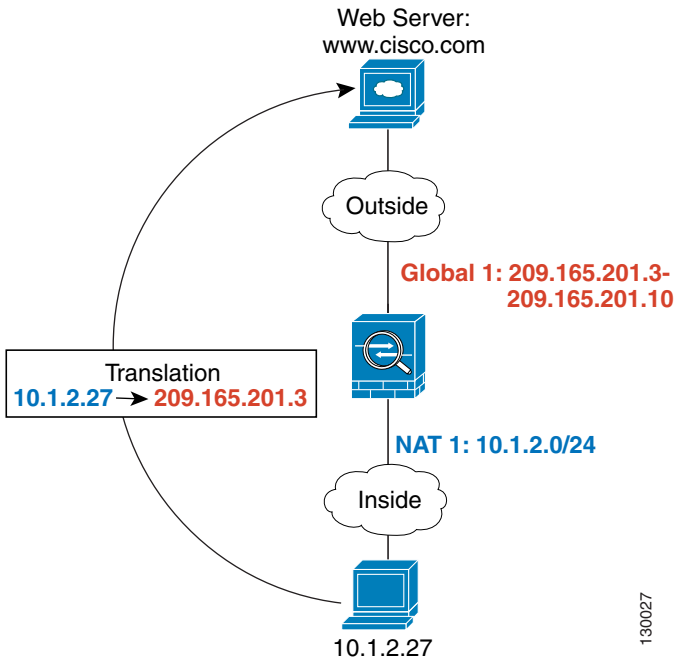
PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the ASA interface IP address as the PAT address. PAT does not work with some multimedia applications that have a data stream that is different from the control path. See the "When to Use Application Protocol Inspection" section on page 40-2 for more information about NAT and PAT support.

Note For the duration of the translation, a remote host can initiate a connection to the translated host if an access list 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 list. However, policy PAT does not support time-based ACLs.

Information About Implementing Dynamic NAT and PAT

For dynamic NAT and PAT, you first configure a **nat** command identifying the real addresses on a given interface that you want to translate. Then you configure a separate **global** command to specify the mapped addresses when exiting another interface (in the case of PAT, this is one address). Each **nat** command matches a **global** command by comparing the NAT ID, a number that you assign to each command. (See Figure 29-3.)

Figure 29-3 nat and global ID Matching

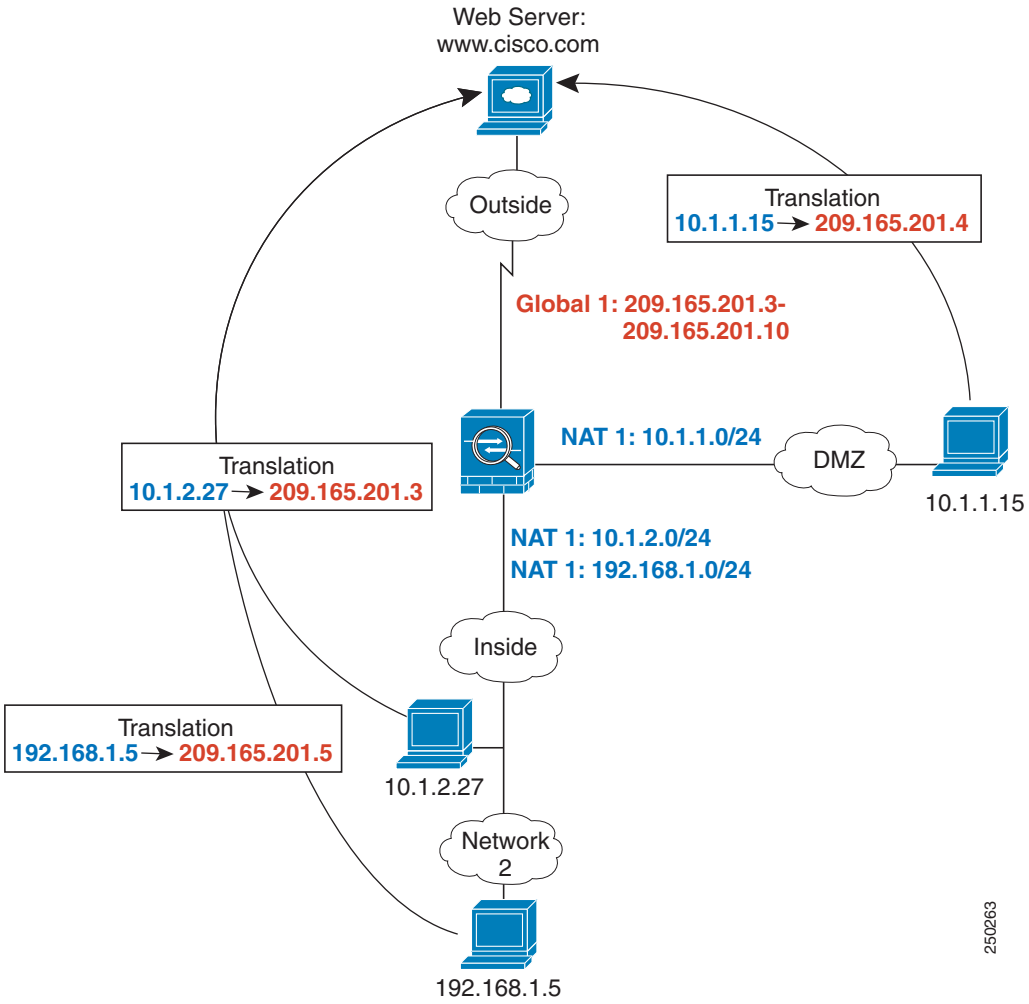


See the following commands for this example:

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

You can enter multiple **nat** commands using the same NAT ID on one or more interfaces; they all use the same **global** command when traffic exits a given interface. For example, you can configure **nat** commands for Inside and DMZ interfaces, both on NAT ID 1. Then you configure a **global** command on the Outside interface that is also on ID 1. Traffic from the Inside interface and the DMZ interface share a mapped pool or a PAT address when exiting the Outside interface. (See Figure 29-4.)

Figure 29-4 nat Commands on Multiple Interfaces

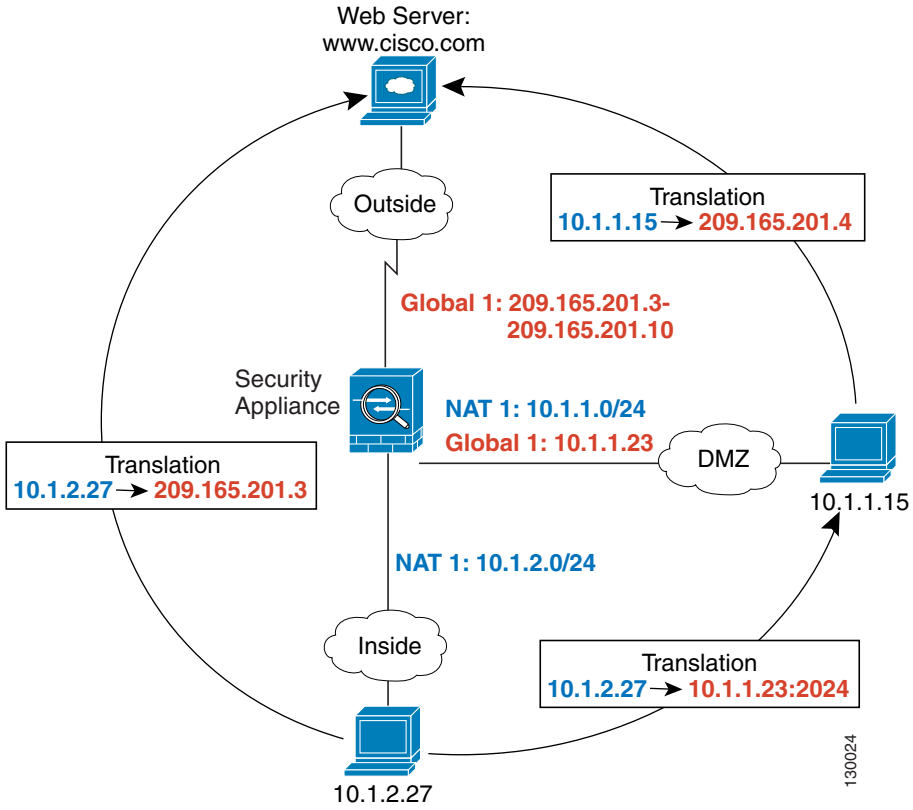


See the following commands for this example:

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (inside) 1 192.168.1.0 255.255.255.0
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

You can also enter a **global** command for each interface using the same NAT ID. If you enter a **global** command for the Outside and DMZ interfaces on ID 1, then the Inside **nat** command identifies traffic to be translated when going to both the Outside and the DMZ interfaces. Similarly, if you also enter a **nat** command for the DMZ interface on ID 1, then the **global** command on the Outside interface is also used for DMZ traffic. (See Figure 29-5.)

Figure 29-5 global and nat Commands on Multiple Interfaces

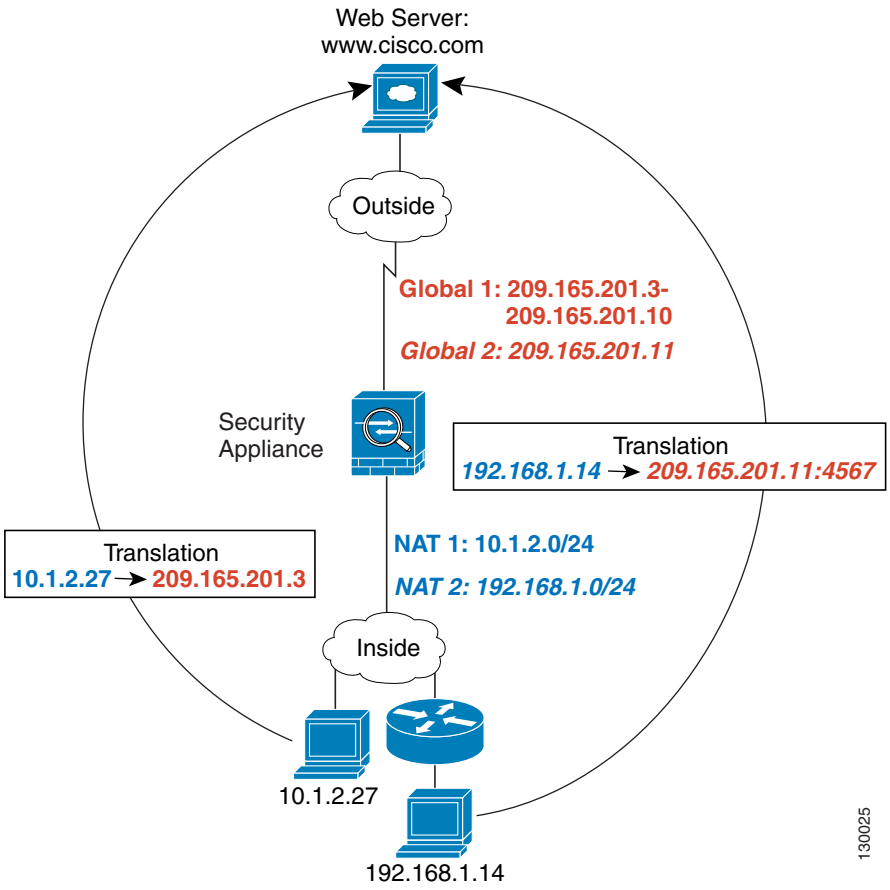


See the following commands for this example:

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

If you use different NAT IDs, you can identify different sets of real addresses to have different mapped addresses. For example, on the Inside interface, you can have two **nat** commands on two different NAT IDs. On the Outside interface, you configure two **global** commands 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 29-6.) If you use policy NAT, you can specify the same real addresses for multiple **nat** commands, as long as the destination addresses and ports are unique in each access list.

Figure 29-6 Different NAT IDs

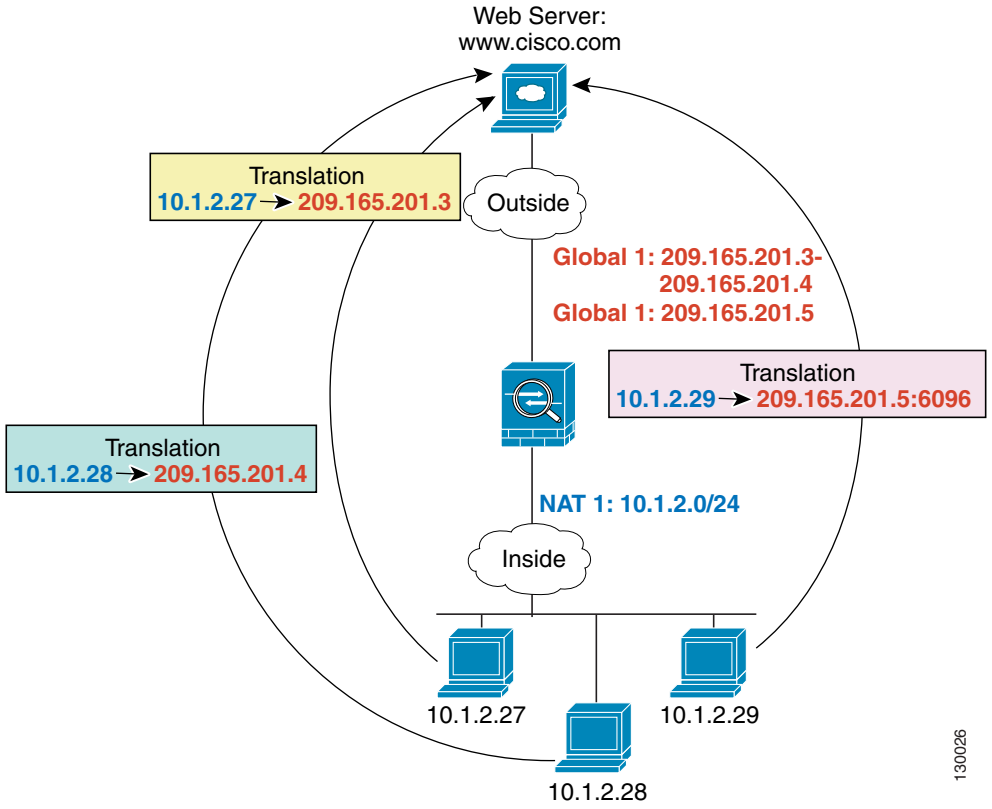


See the following commands for this example:

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

You can enter multiple **global** commands for one interface using the same NAT ID; the ASA uses the dynamic NAT **global** commands first, in the order they are in the configuration, and then it uses the PAT **global** commands in order. You might want to enter both a dynamic NAT **global** command and a PAT **global** command if you need to use dynamic NAT for a particular application, but you should have a backup PAT statement in case all the dynamic NAT addresses are depleted. Similarly, you might enter two PAT statements if you need more than the approximately 64,000 PAT sessions that a single PAT mapped statement supports. (See Figure 29-7.)

Figure 29-7 NAT and PAT Together

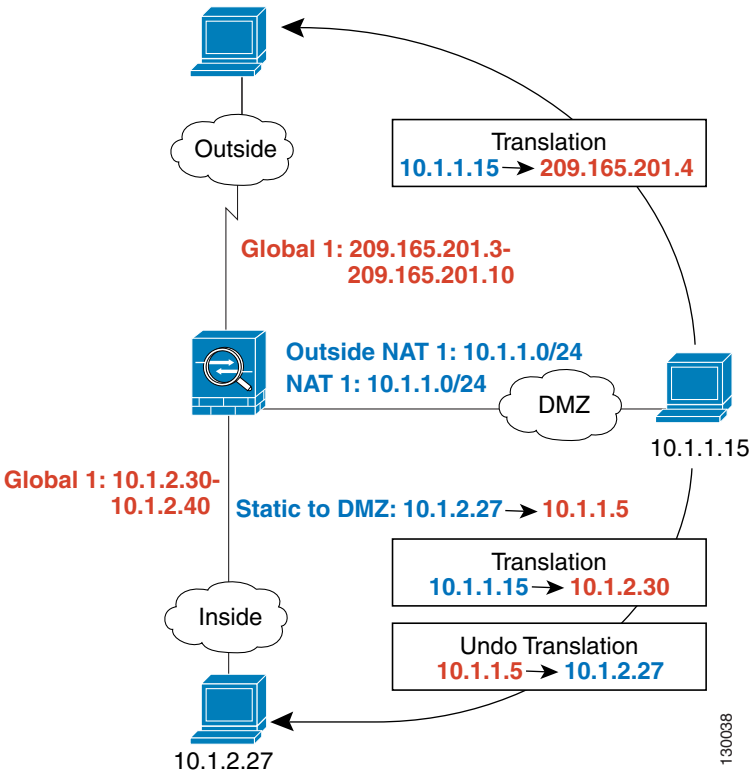


See the following commands for this example:

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

For outside NAT (from outside to inside), you need to use the **outside** keyword in the **nat** command. If you also want to translate the same traffic when it accesses an outside interface (for example, traffic on a DMZ is translated when accessing the Inside and the Outside interfaces), then you must configure a separate **nat** command without the **outside** option. In this case, you can identify the same addresses in both statements and use the same NAT ID. (See Figure 29-8.) Note that for outside NAT (DMZ interface to Inside interface), the inside host uses a **static** command to allow outside access, so both the source and destination addresses are translated.

Figure 29-8 Outside NAT and Inside NAT Combined



See the following commands for this example:

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

When you specify a group of IP address(es) in a **nat** command, then you must perform NAT on that group of addresses when they access any lower or same security level interface; you must apply a **global** command with the same NAT ID on each interface, or use a **static** command. NAT is not required for that group when it accesses a higher security interface because to perform NAT from outside to inside you must create a separate **nat** command using the **outside** keyword. If you do apply outside NAT, then the NAT requirements preceding come into effect for that group of addresses when they access all higher security interfaces. Traffic identified by a **static** command is not affected.

Licensing Requirements for Dynamic NAT and PAT

The following table shows the licensing requirements for these features:

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- Supported in single and multiple context mode.

Firewall Mode Guidelines

- Supported only in routed and transparent firewall mode.

Additional Guidelines and Limitations

The following features are not supported for dynamic NAT and PAT:

- 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 that use translations.

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

- You can identify overlapping addresses in other **nat** commands. For example, you can identify 10.1.1.0 in one command but 10.1.1.1 in another. The traffic is matched to a policy NAT command in order, until the first match, or for regular NAT, using the best match.
- All types of NAT support policy NAT except for NAT exemption. NAT exemption uses an access list to identify the real addresses, but it differs from policy NAT in that the ports are not considered. You can accomplish the same result as NAT exemption using static identity NAT, which does support policy NAT.
- When using dynamic PAT, for the duration of the translation a remote host can initiate a connection to the translated host if an access list allows it. Because the address (both real and mapped) is unpredictable, a connection to the host is unlikely. However, in this case you can rely on the security of the access list.
- If the mapped pool has fewer addresses than the real group, you might 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 mapped pool; if the destination network requires registered addresses, such as the Internet, you might encounter a shortage of usable addresses.

Default Settings

Table 29-1 lists the command options and default settings for policy NAT and regular NAT. Table 29-2 lists an additional command option for regular NAT.

See the **nat** command in the *Cisco Security Appliance Command Reference* for a complete description of command options.

Table 29-1 Configuring Command Options and Defaults for Policy NAT and Regular NAT

Command	Purpose
access-list *acl_name*	Identifies the real addresses and destination addresses using an extended access list. Create the extended access list using the **access-list extended** command. (See Chapter 11, "Adding an Extended Access List.") This access list should include only **permit** ACEs. You can optionally specify the real and destination ports in the access list using the **eq** operator. Policy NAT considers the **inactive** and **time-range** keywords, but it does not support ACL with all **inactive** and **time-range** ACEs.
nat_id	An integer between 1 and 65535. The NAT ID should match a **global** command NAT ID. See the "Information About Implementing Dynamic NAT and PAT" section on page 29-5 for more information about how NAT IDs are used. **0** is reserved for NAT exemption. (See the "Configuring Static Identity NAT" section on page 31-5 for more information about NAT exemption.)
dns	If your **nat** command 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 mapped address and one needs the real 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 26-9 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
norandomseq, **tcp** *tcp_max_conns*, **udp** *udp_max_conns*, and *emb_limit*	These keywords set connection limits. However, we recommend using a more versatile method for setting connection limits; for more information, see Chapter 53, "Configuring Connection Limits and Timeouts." The default value for *tcp_max_conns*, *emb_limit*, and *udp_max_conns* is 0 (unlimited), which is the maximum available.

Table 29-2 Command Options and Defaults for Regular NAT

nat_id	An integer between 1 and 2147483647. The NAT ID must match a **global** command NAT ID. See the "Information About Implementing Dynamic NAT and PAT" section on page 29-5 for more information about how NAT IDs are used. **0** is reserved for identity NAT. See the "Configuring Identity NAT" section on page 31-1 for more information about identity NAT.

Configuring Dynamic NAT or Dynamic PAT

This section describes how to configure dynamic NAT or dynamic PAT, and it includes the following topics:

- Task Flow for Configuring Dynamic NAT and PAT, page 29-13
- Configuring Policy Dynamic NAT, page 29-15
- Configuring Regular Dynamic NAT, page 29-17

Task Flow for Configuring Dynamic NAT and PAT

Use the following guidelines to configure either Dynamic NAT or PAT:

- First configure a **nat** command, identifying the real addresses on a given interface that you want to translate.
- Then configure a separate **global** command to specify the mapped addresses when exiting another interface. (In the case of PAT, this is one address.) Each nat command matches a global command by comparing the NAT ID, a number that you assign to each command.

Note The configuration for dynamic NAT and PAT are almost identical; for NAT you specify a range of mapped addresses, and for PAT you specify a single address.

Figure 29-9 shows a typical dynamic NAT scenario. Only translated hosts can create a NAT session, and responding traffic is allowed back. The mapped address is dynamically assigned from a pool defined by the **global** command.

Figure 29-9 Dynamic NAT

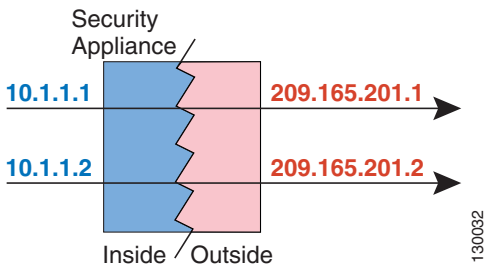
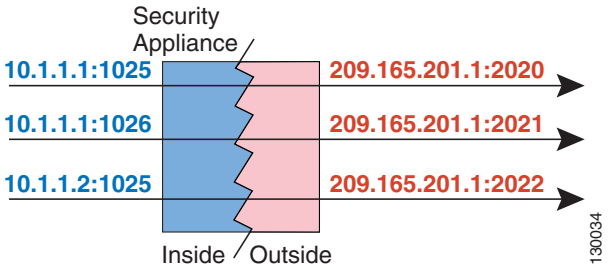


Figure 29-10 shows a typical dynamic PAT scenario. Only translated hosts can create a NAT session, and responding traffic is allowed back. The mapped address defined by the **global** command is the same for each translation, but the port is dynamically assigned.

Figure 29-10 Dynamic PAT



For more information about dynamic NAT, see the "Information About Dynamic NAT" section on page 29-1. For more information about PAT, see the "Information About PAT" section on page 29-4.

Configuring Policy Dynamic NAT

To configure dynamic NAT and PAT and identify the real addresses on one interface that are translated to mapped addressed on another interface, perform the following steps:

	Command	Purpose
Step 1	**nat** (*real_interface*) *nat_id* **access-list** *acl_name* [**dns**] [**outside**][[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*][**norandomseq**] **Example:** hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000	Configures dynamic policy NAT or PAT, identifying the real addresses on a given interface that you want to translate to one of a pool of mapped addresses. The *real_interface* specifies the name of the interface connected to the real IP address network. The *nat_id* should match a **nat** command NAT ID. The matching **nat** command 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 policy NAT, the *nat_id* argument is an integer between 1 and 65535. The **access-list** keyword identifies the real addresses and destination/source addresses using an extended access list. The *acl_name* argument identifies the name of the access list. The **dns** option rewrites the A record, or address record, in DNS replies that match this static. For DNS replies traversing from a mapped interface to any other interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the A record is rewritten from the real value to the mapped value. Enter the **outside** optional keyword if this interface is on a lower security level than the interface you identify by the matching global statement. This feature is called outside NAT or bidirectional NAT. The **tcp** option specifies the protocol at TCP. The *tcp_max_cons* argument specifies the maximum number of simultaneous TCP connections allowed to the local-host (see the local-host command). The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the timeout conn command.) The *emb_limit* option specifies the maximum number of embryonic connections per host. The default is **0,** which means unlimited embryonic connections. The **udp** *udp_max_conns* options specify the maximum number of simultaneous UDP connections allowed to the local host. The default is **0**, which means unlimited connections. The **norandomseq** option disables TCP ISN randomization protection.

	Command	Purpose
Step 2	**global** (*mapped_interface*) *nat_id* {*mapped_ip*[**-***mapped_ip*] | **interface**} **Example:** hostname(config)# global (outside) 1 209.165.202.129	Identifies the mapped address(es) to which you want to translate the real addresses when they exit a particular interface. (In the case of PAT, this is one address.) The *mapped_interface* option specifies the name of the interface connected to the mapped IP address network. The *nat_id* argument must match a **global** command NAT ID. See the "Information About Implementing Dynamic NAT and PAT" section on page 29-5 for more information about using NAT IDs. The *mapped_ip mapped_ip* specify the mapped address(es) to which you want to translate the real addresses when they exit the mapped interface. If you specify a single address, then you configure PAT. If you specify a range of addresses, then you configure dynamic NAT. If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC). The **interface** keyword uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP. See Table 29-1, "Command Options and Defaults for Policy NAT and Regular NAT," for information about other command options.

Configuring Regular Dynamic NAT

To configure regular dynamic NAT and identify the real addresses on one interface that are translated to mapped addressed on another interface, perform the following steps:

	Command	Purpose
Step 1	**nat** (*real_interface*) *nat_id real_ip* [*mask* [**dns**] [**outside**]] [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*]] [**norandomseq**] **Example:** hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0	Configures dynamic NAT or PAT, identifying the real addresses on a given interface that you want to translate to one of a pool of mapped addresses. The *nat_id* should match a **nat** command NAT ID. The matching **nat** command 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 regular NAT, the *nat_id* argument is an integer between 1 and 2147483647. The *real_ip* argument specifies the real address that you want to translate. You can use 0.0.0.0 (or the abbreviation 0) to specify all addresses. The *mask* argument specifies the subnet mask for the real addresses. If you do not enter a mask, then the default mask for the IP address class is used. The **dns** keyword rewrites the A record, or address record, in DNS replies that match this command. For DNS replies traversing from a mapped interface to any other interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the A record is rewritten from the real value to the mapped value. Enter the **outside** option if this interface is on a lower security level than the interface you identify by the matching global statement. This feature is called outside NAT or bidirectional NAT. The **tcp** *tcp_max_cons* argument specifies the maximum number of simultaneous TCP connections allowed to the local-host. (See the **local-host** command.) The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The **udp** *udp_max_conns* specify the maximum number of simultaneous UDP connections allowed to the local-host. (See the **local-host** command.) The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The **norandomseq** keyword disables TCP ISN randomization protection. Not supported for NAT exemption (nat 0 access-list). Although you can enter this argument at the CLI, it is not saved to the configuration. (For additional information about command options, see the *Cisco Security Appliance Command Reference*.)

	Command	Purpose
Step 2	**global** (*mapped_interface*) *nat_id* {*mapped_ip*[**-***mapped_ip*] | **interface**} **Example:** hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10	Identifies the mapped address(es) to which you want to translate the real addresses when they exit a particular interface. The *mapped_interface* option specifies the name of the interface connected to the mapped IP address network. The *nat_id* must match a **global** command NAT ID. For more information about how NAT IDs are used, see the "Information About Implementing Dynamic NAT and PAT" section on page 29-5. The *mapped_ip mapped_ip* specify the mapped address(es) to which you want to translate the real addresses when they exit the mapped interface. If you specify a single address, then you configure PAT. If you specify a range of addresses, then you configure dynamic NAT. If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC). The **interface** keyword uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP. See Table 29-1, "Command Options and Defaults for Policy NAT and Regular NAT," for information about other command options, and see and Table 29-2 for additional information specific to regular NAT only.

Monitoring Dynamic NAT and PAT

To monitor dynamic NAT and PAT, perform the following task:

Command	Purpose
show running-config nat	Displays a pool of global IP addresses that are associated with the network.

Configuration Examples for Dynamic NAT and PAT

For example, to translate the 10.1.1.0/24 network on the inside interface, enter the following command:

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(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:

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(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:

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

To identify a single real address with two different destination addresses using policy NAT, enter the following commands (see Figure 26-3 on page 26-5 for a related figure):

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

To identify a single real address/destination address pair that use different ports using policy NAT, enter the following commands (see Figure 26-4 on page 26-6 for a related figure):

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

Feature History for Dynamic NAT and PAT

Table 29-3 lists the release history for this feature.

Table 29-3 Feature History for Dynamic NAT and PAT

Feature Name	Releases	Feature Information
NAT in transparent firewall mode	8.0(2)	NAT is now supported in transparent firewall mode.