CHAPTER 30

Configuring Static PAT

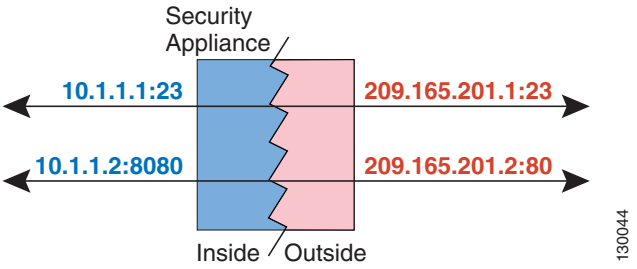
Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. That is, both the address and the port numbers are translated. This chapter describes how to configure static PAT and includes the following topics:

Information About Static PAT

Static PAT is the same as static NAT, except that it enables you to specify the protocol (TCP or UDP) and port for the real and mapped addresses. Static PAT enables you to identify the same mapped address across many different static statements, provided that the port is different for each statement. You cannot use the same mapped address for multiple static NAT statements.

Figure 30-1 shows a typical static PAT scenario. The translation is always active so both translated and remote hosts can originate connections, and the mapped address and port are statically assigned by the **static** command.

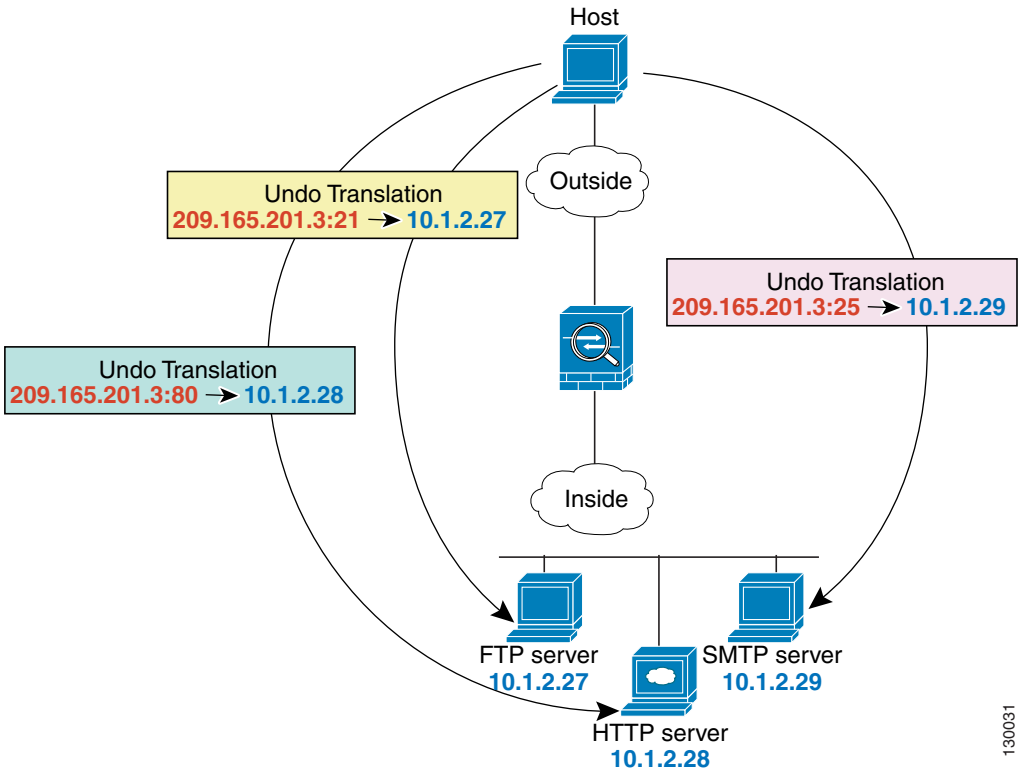
Figure 30-1 Typical Static PAT Scenario



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

For example, if you want to provide a single address for remote users to access FTP, HTTP, and SMTP, but these are all actually different servers on the real network, you can specify static PAT statements for each server that uses the same mapped IP address, but different ports. (See Figure 30-2.)

Figure 30-2 Static PAT



See the following commands for this example:

```
hostname(config)# static (inside,outside) tcp 209.165.201.3 ftp 10.1.2.27 ftp netmask
255.255.255.255
```

```
hostname(config)# static (inside,outside) tcp 209.165.201.3 http 10.1.2.28 http netmask
255.255.255.255
hostname(config)# static (inside,outside) tcp 209.165.201.3 smtp 10.1.2.29 smtp netmask
255.255.255.255
```

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

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

Licensing Requirements for Static PAT

Model	License Requirement
All models	Base License.

Prerequisites for Static PAT

Static PAT has the following prerequisites:

An extended access list must be configured. Create the extended access list using the access-list extended command. (See the Chapter 11, “Adding an Extended Access List,” for more information.)

Identify the real addresses and destination/source 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.”). The first address in the access list is the real address; the second address is either the source or destination address, depending on where the traffic originates. For example, to translate the real address 10.1.1.1 to the mapped address 192.168.1.1 when 10.1.1.1 sends traffic to the 209.165.200.224 network, the **access-list** and **static** commands are:

```
hostname(config)# access-list TEST extended ip host 10.1.1.1 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 192.168.1.1 access-list TEST
```

In this case, the second address is the destination address. However, the same configuration is used for hosts to originate a connection to the mapped address. For example, when a host on the 209.165.200.224/27 network initiates a connection to 192.168.1.1, then the second address in the access list is the source address.

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 does not consider the **inactive** or **time-range** keywords; all ACEs are considered to be active for policy NAT configuration. See the “Policy NAT” section on page 26-5 for more information.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the ASA translates the .0 and .255 addresses. If you want to prevent access to these addresses, be sure to configure an access list to deny access. See the Chapter 29, “Configuring Dynamic NAT and PAT,” for information about the other options.

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 guidelines and limitations apply to the static PAT feature:

- Static translations can be defined for a single host or for all addresses contained in an IP subnet.
- Do not use a mapped address in the **static** command that is also defined in a **global** command for the same mapped interface.
- If you remove a **static** command, existing connections that use the translation are not affected. To removed these connections, enter the **clear local-host** command.
- You cannot clear static translations from the translation table with the **clear xlate** command; you must remove the **static** command instead. Only dynamic translations created by the **nat** and **global** commands can be removed with the **clear xlate** command.
- When configuring static PAT with FTP, you need to add entries for both TCP ports 20 and 21. You must specify port 20 so that the source port for the active transfer is not modified to another port, which may interfere with other devices that perform NAT on FTP traffic.

Default Settings

Table 30-1 lists the default settings for static PAT parameters.

Table 30-1 Default static PAT Parameters

Parameters	Default
emb_limit	The default value is **0** (unlimited), which is the maximum available.
tcp_max_cons	The default value is **0** (unlimited), which is the maximum available.
udp_max_cons	The default value is **0** (unlimited), which is the maximum available.

Configuring Static PAT

This section describes how to configure a static port translation and includes the following topics:

Configuring Policy Static PAT

Policy static PAT enables you to reference a route map to identify specific conditions or policies that trigger a static translation.

To configure policy static PAT, enter the following command:

Command	Purpose
static (*real_interface*,*mapped_interface*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* **access-list** *acl_name* [**dns**] [**norandomseq**] [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] **Example:** hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET	Configures a route map to identify policies that trigger a static translation. The real *real_interface*argument specifies the name of the interface connected to the real IP address network, and the *mapped_interface* argument specifies the name of the interface connected to the mapped IP address network. Either **tcp** or **udp** specifies the protocol. The *mapped_ip* argument specifies the address to which the real address is translated (the interface connected to the mapped IP address network). 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. You must use the interface keyword instead of specifying the actual IP address when you want to include the IP address of an interface in a static PAT entry. The *mapped_port* argument specifies the mapped TCP or UDP port. You can specify the ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers The **access-list** keyword and *acl_id* argument identify the real addresses and destination/source 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," for more information.) This access list should include only **permit** ACEs. Make sure that the source address in the access list matches the *real_ip* in this command. The optional **dns** keyword rewrites the A record, or address record, in DNS replies that match this **static** 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. DNS inspection must be enabled to support this functionality. The optional **norandomseq** keyword disables TCP ISN randomization protection The optional **tcp** *tcp_max_conns* keyword specifies the maximum number of simultaneous TCP connections allowed to the local host. The optional *emb_limit* argument specifies the maximum number of embryonic connections per host. **Note** An embryonic limit applied using static NAT is applied to all connections to or from the real IP address, and not just connections between the specified interfaces. To apply limits to specific flows, see the "Configuring Connection Limits and Timeouts" section on page 53-3. The optional **udp** *udp_max_conns* keyword and argument specify the maximum number of simultaneous UDP connections allowed to the local host. (For additional information about command options, see the *Cisco Security Appliance Command Reference*.)

Configuring Regular Static PAT

Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address.

To configure regular static PAT, enter the following command:

Command	Purpose
static (*real_interface*,*mapped_interface*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port real_ip real_port* [**netmask** *mask*] [**dns**] [**norandomseq**] [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] **Example:** hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask 255.255.255.255	Configures static PAT. The real *real_interface*argument specifies the name of the interface connected to the real IP address network, and the *mapped_interface* argument specifies the name of the interface connected to the mapped IP address network. Either **tcp** or **udp** specifies the protocol. The *mapped_ip* argument specifies the address to which the real address is translated (the interface connected to the mapped IP address network). 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. You must use the interface keyword instead of specifying the actual IP address when you want to include the IP address of an interface in a static PAT entry. The *mapped_port* and *real_port* arguments specify the mapped and real TCP or UDP ports. You can specify the ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers The **netmask** *mask* option specifies the subnet mask for the real and mapped addresses. For single hosts, use 255.255.255.255. If you do not enter a mask, then the default mask for the IP address class is used, with one exception. If a host-bit is non-zero after masking, a host mask of 255.255.255.255 is used. If you use the access-list keyword instead of the real_ip, then the subnet mask used in the access list is also used for the mapped_ip. The **dns** option rewrites the A record, or address record, in DNS replies that match this **static** 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. DNS inspection must be enabled to support this functionality. The **norandomseq** option disables TCP ISN randomization protection The **tcp** *tcp_max_conns* options specify the maximum number of simultaneous TCP connections allowed to the local host. The *emb_limit* option specifies the maximum number of embryonic connections per host. **Note** An embryonic limit applied using static NAT is applied to all connections to or from the real IP address, and not just connections between the specified interfaces. To apply limits to specific flows, see the "Configuring Connection Limits and Timeouts" section on page 53-3. The **udp** *udp_max_conns* options specify the maximum number of simultaneous UDP connections allowed to the local host. (For additional information about command options, see the *Cisco Security Appliance Command Reference*.)

Monitoring Static PAT

To monitor static PAT, enter the following command:

Command	Purpose
`show running-config static`	Displays all static commands in the configuration.

Configuration Examples for Static PAT

This section includes configuration examples for policy static PAT and regular static PAT, and it contains these topics:

Examples of Policy Static PAT

For Telnet traffic initiated from hosts on the 10.1.3.0 network to the ASA 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:

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0
hostname(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 ASA outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering:

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

Examples of Regular Static PAT

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

```
hostname(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 preceding real Telnet server 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.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(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 mapped address from the Telnet server, you can still configure traffic initiated from the Telnet server to use the same mapped 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 mapped address.

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

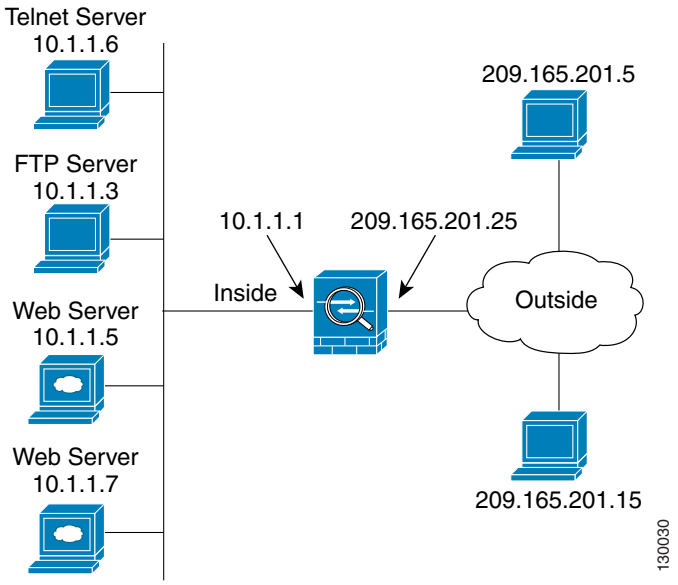
To translate a well-known port (80) to another port (8080), enter the following command:

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

Example of Redirecting Ports

Figure 30-3 shows an example of a network configuration in which the port redirection feature might be useful.

Figure 30-3 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 an ASA 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 configuration, perform the following steps:

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

```
hostname(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
hostname(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:

```
hostname(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:

```
hostname(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 ASA outside interface address to 10.1.1.5 by entering the following command:

```
hostname(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:

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

Feature History for Static PAT

Table 30-2 lists the release history for this feature.

Table 30-2 Feature History for Static PAT

Feature Name	Releases	Feature Information
Static PAT	7.0	Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. This feature was introduced.
NAT and static PAT	7.3.(1)	NAT are supported in transparent firewall mode.