CHAPTER 27

Configuring NAT Control

This chapter describes NAT control, and it includes the following sections:

Information About NAT Control

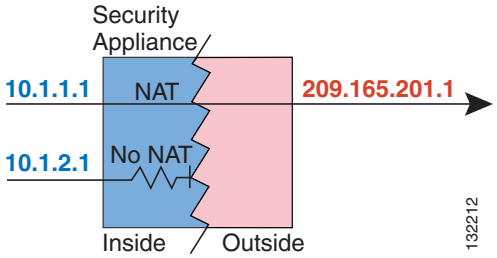
This section describes NAT control, and it includes the following topics:

NAT Control and Inside Interfaces

NAT control requires that packets traversing from an inside interface to an outside interface match a NAT rule; for any host on the inside network to access a host on the outside network, you must configure NAT to translate the inside host address, as shown in Figure 27-1.

Note NAT control is used for NAT configurations defined with earlier versions of the ASA. The best practice is to use access rules for access control instead of relying on the absence of a NAT rule to prevent traffic through the ASA.

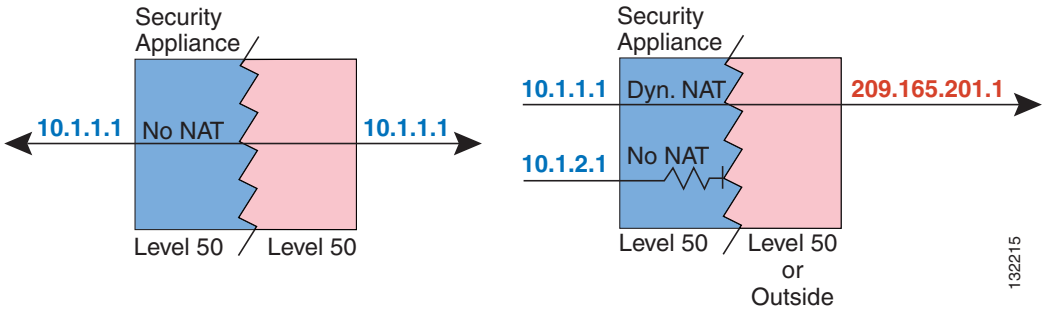
Figure 27-1 NAT Control and Outbound Traffic



NAT Control and Same Security Interfaces

Interfaces at the same security level are not required to use NAT to communicate. However, if you configure dynamic NAT or PAT on a same security interface, then all traffic from the interface to a same security interface or an outside interface must match a NAT rule, as shown in Figure 27-2.

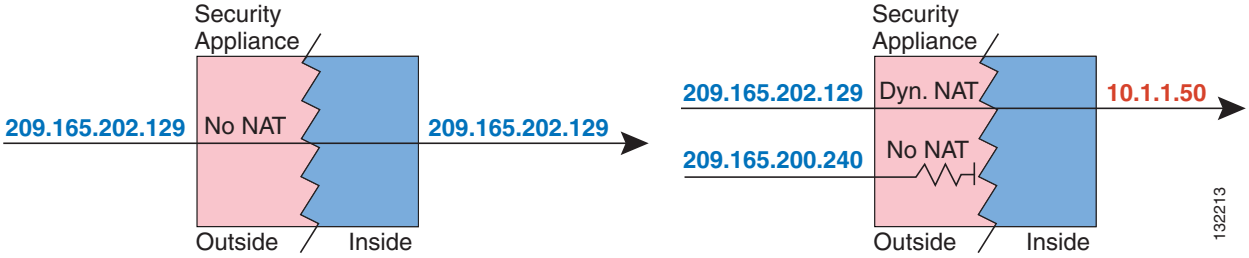
Figure 27-2 NAT Control and Same Security Traffic



NAT Control and Outside Dynamic NAT

Similarly, if you enable outside dynamic NAT or PAT, then all outside traffic must match a NAT rule when it accesses an inside interface. (See Figure 27-3.)

Figure 27-3 NAT Control and Inbound Traffic



NAT Control and Static NAT

NAT control does not affect static NAT and does not cause the restrictions seen with dynamic NAT.

Bypassing NAT When NAT Control is Enabled

If you want the added security of NAT control but do not want to translate inside addresses in some cases, you can apply a NAT exemption or identity NAT rule on those addresses.

If you enable NAT control, then inside hosts must match a NAT rule when accessing outside hosts. If you do not want to perform NAT for some hosts, then you can bypass NAT for those hosts or you can disable NAT control. You might want to bypass NAT, for example, if you are using an application that does not support NAT. See the "When to Use Application Protocol Inspection" section on page 40-2 for information about inspection engines that do not support NAT.

You can configure traffic to bypass NAT using one of the following three methods. All methods achieve compatibility with inspection engines. However, each method offers slightly different capabilities.

- Identity NAT (**nat 0** command)—When you configure identity NAT (which is similar to dynamic NAT), you do not limit translation for a host on specific interfaces; you must use identity NAT for connections through all interfaces. Therefore, you cannot choose to perform normal translation on real addresses when you access interface A, but you use identity NAT when accessing interface B. Regular dynamic NAT, on the other hand, enables you to specify a particular interface on which to translate the addresses. Make sure that the real addresses for which you use identity NAT are routable on all networks that are available according to your access lists.

  For identity NAT, even though the mapped address is the same as the real address, you cannot initiate a connection from the outside to the inside (even if the interface access list allows it). Use static identity NAT or NAT exemption for this functionality.

- Static identity NAT (**static** command)—Static identity NAT enables you to specify the interface on which you want to allow the real 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 enables you to use policy NAT, which identifies the real and destination addresses when determining the real addresses to translate. (See the "Policy NAT" section on page 26-5 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 0 access-list** command)—NAT exemption allows both translated and remote hosts to initiate connections. Like identity NAT, you do not limit translation for a host on specific interfaces; you must use NAT exemption for connections through all interfaces. However, NAT exemption does enable you to specify the real and destination addresses when determining the real addresses 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 access list. NAT exemption also does not support connection settings, such as maximum TCP connections.

Licensing Requirements

Model	License Requirement
All models	Base License.

Prerequisites for NAT Control

NAT control has the following prerequisites:

- NAT control requires that packets traversing from an inside interface to an outside interface match a NAT rule; for any host on the inside network to access a host on the outside network, you must configure NAT to translate the inside host address.
- Interfaces at the same security level are not required to use NAT to communicate. However, if you configure dynamic NAT or PAT on a same security interface with NAT control enabled, then all traffic from the interface to a same security interface or an outside interface must match a NAT rule.
- Similarly, if you enable outside dynamic NAT or PAT with NAT control, then all outside traffic must match a NAT rule when it accesses an inside interface.
- Static NAT with NAT control does not cause these restrictions.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- Supported in single and multiple context modes.
- In multiple context mode, the packet classifier might rely on the NAT configuration to assign packets to contexts if you do not enable unique MAC addresses for shared interfaces. See the "How the Security Appliance Classifies Packets" section on page 5-3 for more information about the relationship between the classifier and NAT.

Firewall Mode Guidelines

Supported in routed and transparent modes.

Additional Guidelines and Limitations

If you want the added security of NAT control but do not want to translate inside addresses in some cases, you can apply a NAT exemption (**nat 0 access-lis**t) or identity NAT (**nat 0** or **static**) rule on those addresses.

Default Settings

By default, NAT control is disabled; therefore, you do not need to perform NAT on any networks unless you want to do so. If you upgraded from an earlier version of software, however, NAT control might be enabled on your system. Even with NAT control disabled, you need to perform NAT on any addresses for which you configure dynamic NAT. See the Chapter 29, "Configuring Dynamic NAT and PAT," for more information about how dynamic NAT is applied.

Configuring NAT Control

To enable NAT control, enter the following command:

Command	Purpose
nat-control **Example:** hostname(config)# nat-control	Enables NAT control. To disable NAT control, enter the **no** form of the command.

Monitoring NAT Control

To monitor NAT control, perform one of the following tasks:

Command	Purpose
show running-config nat-control	Shows the NAT configuration requirement.

Configuration Examples for NAT Control

When NAT control is disabled with the **no-nat control** command, and a NAT and a global command pair are configured for an interface, the real IP addresses cannot go out on other interfaces unless you define those destinations with the **nat 0 access-list** command.

For example, the following NAT is the that one you want performed when going to the outside network:

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
```

The above configuration catches everything on the inside network, so if you do not want to translate inside addresses when they go to the DMZ, then you need to match that traffic for NAT exemption, as shown in the following example:

```
access-list EXEMPT extended permit ip any 192.168.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ1
access-list EXEMPT extended permit ip any 10.1.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ1
nat (inside) 0 access-list EXEMPT
```

Alternately, you can perform NAT translation on all interfaces:

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
global (dmz1) 1 192.168.1.230
global (dmz2) 1 10.1.1.230
```

Feature History for NAT Control

Table 27-1 lists the release history for this feature.

Table 27-1 Feature History for NAT Control

Feature Name	Releases	Feature Information
Ability to enable and disable NAT control	7.0(1)	The ability to enable and disable NAT control was introduced. The following command was introduced: **nat-control**.