



# CHAPTER 31

## Bypassing NAT

---

If you enable NAT control, then inside hosts must match a NAT rule when accessing outside hosts. You might want to bypass NAT when you enable NAT control so that local IP addresses appear untranslated. You also might want to bypass NAT 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 bypass NAT using identity NAT, static identity NAT, or NAT exemption.

This chapter describes how to bypass NAT, and it includes the following topics:

- [Configuring Identity NAT, page 31-1](#)
- [Configuring Static Identity NAT, page 31-5](#)
- [Configuring NAT Exemption, page 31-11](#)

## Configuring Identity NAT

This section includes the following topics:

- [Information About Identity NAT, page 31-2](#)
- [Licensing Requirements for Identity NAT, page 31-2](#)
- [Guidelines and Limitations for Identity NAT, page 31-2](#)
- [Default Settings for Identity NAT, page 31-3](#)
- [Configuring Identity NAT, page 31-4](#)
- [Monitoring Identity NAT, page 31-4](#)
- [Feature History for Identity NAT, page 31-5](#)

## Information About Identity NAT

Identity NAT translates the real IP address to the same IP address. Only “translated” hosts can create NAT translations, and responding traffic is allowed back.

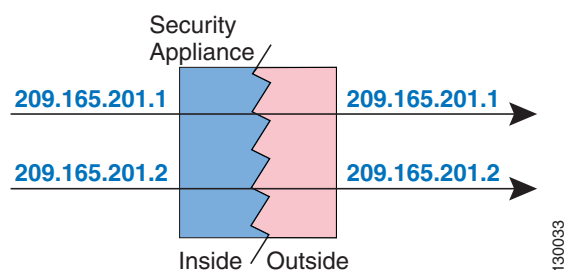
When you configure identity NAT (which is similar to dynamic NAT), you do not limit translation for a host on specific interfaces; you must use identity NAT for connections through all interfaces. For example, you cannot choose to perform normal translation on real addresses when you access interface A and then use identity NAT when accessing interface B. Because you use identity NAT for all connections through all interfaces, make sure that the real addresses for which you use identity NAT are routable on all networks that are available according to your access list.

**Note**

If you need to specify a particular interface on which to translate the addresses, use regular dynamic NAT.

Figure 31-1 shows a typical identity NAT scenario.

**Figure 31-1**      **Identity NAT**



## Licensing Requirements for Identity NAT

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

## Guidelines and Limitations for Identity NAT

This section includes the guidelines and limitations for this feature:

### Context Mode Guidelines

- Supported in single and multiple context mode.

### Firewall Mode Guidelines

- Supported in routed and transparent firewall modes.

**Additional Guidelines and Limitations**

- 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.
- The real addresses for which you use identity NAT must be 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.

## Default Settings for Identity NAT

Table 31-1 lists the default settings for identity NAT parameters.

**Table 31-1**      *Default Identity NAT Parameters*

Parameters	Default
<i>emb_limit</i>	The default is <b>0</b> , which means unlimited embryonic connections
<b>tcp</b> <i>tcp_max_conns</i>	The default is <b>0</b> , which means unlimited connections.
<b>udp</b> <i>udp_max_conns</i>	The default is <b>0</b> , which means unlimited connections.

# Configuring Identity NAT

To configure identity NAT, enter the following command:

Command	Purpose
<pre>nat (real_interface) 0 real_ip [mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]</pre> <p><b>Example:</b>  hostname(config)# nat (inside) 0 10.1.1.0 255.255.255.0</p>	<p>Configures identity NAT for the inside 10.1.1.0/24 network.</p> <p>The <i>real_interface</i> argument specifies the name of the interface connected to the real IP address network.</p> <p>For identity NAT, use the NAT ID of <b>0</b>. This ID is referenced by the global command to associate a global pool with the <i>real_ip</i>.</p> <p>The <i>real_ip</i> argument specifies the real address that you want to translate. You can use <b>0.0.0.0</b> (or the abbreviation <b>0</b>) to specify all addresses.</p> <p>The optional <i>mask</i> 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.</p> <p>The optional <b>dns</b> 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.</p> <p>You must enter <b>outside</b> if this interface is on a lower security level than the interface you identify by the matching global statement.</p> <p>The optional <b>norandomseq</b> keyword disables TCP ISN randomization protection.</p> <p>The optional <b>tcp</b> <i>tcp_max_conns</i> keyword and argument specify the maximum number of simultaneous TCP connections allowed to the local host. The default is <b>0</b>, which means unlimited connections.</p> <p>The optional <i>emb_limit</i> argument specifies the maximum number of embryonic connections per host. The default is <b>0</b>, which means unlimited embryonic connections.</p> <p>The optional <b>udp</b> <i>udp_max_conns</i> keyword and argument specify the maximum number of simultaneous UDP connections allowed to the local host. The default is <b>0</b>, which means unlimited connections.</p> <p>(For additional information about command options, see the <b>nat</b> command in the <i>Cisco Security Appliance Command Reference</i>.)</p>

# Monitoring Identity NAT

To monitor NAT bypass, enter the following command:

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

## Feature History for Identity NAT

Table 31-2 lists the release history for this feature.

**Table 31-2**      *Feature History for Identity NAT*

Feature Name	Releases	Feature Information
Identity NAT	7.0	Identity NAT translates the real IP address to the same IP address. You use identity NAT for connections through all interfaces.  The following command was introduced: <b>nat</b> .
NAT for transparent mode	8.0(2)	NAT began support in transparent firewall mode.

## Configuring Static Identity NAT

This section includes the following topics:

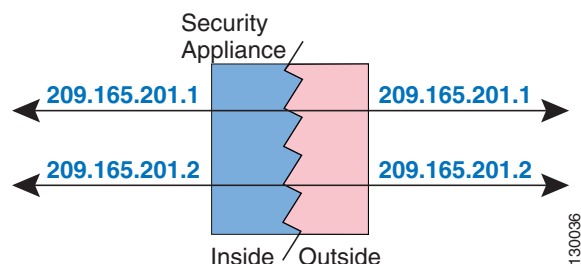
- [Information About Static Identity NAT, page 31-5](#)
- [Licensing Requirements for Static Identity NAT, page 31-6](#)
- [Guidelines and Limitations for Static Identity NAT, page 31-6](#)
- [Default Settings for Static Identity NAT, page 31-7](#)
- [Configuring Static Identity NAT, page 31-7](#)
- [Monitoring Static Identity NAT, page 31-10](#)
- [Feature History for Static Identity NAT, page 31-10](#)

## Information About Static Identity NAT

Static identity NAT translates the real IP address to the same IP address. 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 you can use a normal translation when accessing the outside server B. The translation is always active, and both “translated” and remote hosts can originate connections.

Figure 31-2 shows a typical static identity NAT scenario.

**Figure 31-2 Static Identity NAT**



## Licensing Requirements for Static Identity NAT

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

## Guidelines and Limitations for Static Identity NAT

This section includes the guidelines and limitations for this feature:

### Context Mode Guidelines

- Supported in single and multiple context mode.

### Firewall Mode Guidelines

- Supported in routed and transparent firewall modes.

### Additional Guidelines and Limitations

The following guidelines and limitations apply to static identity NAT:

- 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.
- If you remove a **static** command, existing connections that use the translation are not affected. To remove these connections, enter the **clear local-host** command.
- Policy static identity NAT does not consider the inactive or time-range keywords; all ACEs are considered to be active for policy NAT configurations. (See the “Policy NAT” section on page 26-5 for more information.)
- For static policy NAT, in undoing the translation, the ACL in the **static** command is not used. If the destination address in the packet matches the mapped address in the static rule, the static rule is used to untranslate the address.

## Default Settings for Static Identity NAT

Table 31-3 lists the default settings for static identity NAT parameters.

**Table 31-3**      *Default Static Identity NAT Parameters*

Parameters	Default
<i>emb_limit</i>	The default is <b>0</b> , which means unlimited embryonic connections.
<b>tcp</b> <i>tcp_max_conns</i>	The default is <b>0</b> , which means unlimited embryonic connections.
<b>udp</b> <i>udp_max_conns</i>	The default is <b>0</b> , which means unlimited embryonic connections.

## Configuring Static Identity NAT

This section describes how to configure policy static identity NAT and regular static identity NAT, and it includes the following topics:

- [Configuring Policy Static Identity NAT, page 31-8](#)
- [Configuring Regular Static Identity NAT, page 31-9](#)

## Configuring Policy Static Identity NAT

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

Command	Purpose
<pre><b>static</b> (real_interface,mapped_interface) real_ip <b>access-list</b> acl_id [<b>dns</b>] [<b>norandomseq</b>] [[<b>tcp</b>] tcp_max_conns [emb_limit]] [<b>udp</b> udp_max_conns]</pre> <p><b>Example:</b>  hostname(config)# static (inside,outside)  209.165.202.129 access-list NET1</p>	<p>Configures policy static NAT.</p> <p>The <i>real_interface,mapped_interface</i> arguments specify the name of the interface connected to the real IP address network and the name of the interface connected to the mapped IP address network.</p> <p>The <i>real_ip</i> argument specifies the real address that you want to translate.</p> <p>The <b>access-list</b> keyword and <i>acl_id</i> argument identify the real addresses and destination/source addresses using an extended access list. Create the extended access list using the <b>access-list extended</b> command. (See <a href="#">Chapter 11, “Adding an Extended Access List.”</a>) This access list should include only <b>permit</b> ACEs. Make sure that the source address in the access list matches the <i>real_ip</i> in this command.</p> <p>The optional <b>dns</b> keyword rewrites the A record, or address record, in DNS replies that match this <b>static</b> 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.</p> <p>The optional <b>norandomseq</b> keyword disables TCP ISN randomization protection.</p> <p>The optional <b>tcp</b> <i>tcp_max_conns</i> keyword and argument specify the maximum number of simultaneous TCP connections allowed to the local host. The default is <b>0</b>, which means unlimited connections.</p> <p>The optional <i>emb_limit</i> argument specifies the maximum number of embryonic connections per host. The default is <b>0</b>, which means unlimited embryonic connections.</p> <p>The optional <b>udp</b> <i>udp_max_conns</i> keyword and argument specify the maximum number of simultaneous UDP connections allowed to the local host. The default is <b>0</b>, which means unlimited connections.</p> <p>(For additional information about command options, see the <b>static</b> command in the <i>Cisco Security Appliance Command Reference</i>.)</p>

### Example of Policy Static Identity NAT


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

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



## Configuring Regular Static Identity NAT

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

Command	Purpose
<pre><b>static</b> (real_interface,mapped_interface) real_ip real_ip [<b>netmask</b> mask] [<b>dns</b>] [<b>norandomseq</b>] [[<b>tcp</b>] tcp_max_conns [emb_limit]] [<b>udp</b> udp_max_conns]</pre> <p><b>Example:</b>  hostname(config)# static (inside,outside)  10.1.1.3 10.1.1.3 netmask 255.255.255.255</p>	<p>Configures static identity NAT.</p> <p>The <i>real_interface,mapped_interface</i> arguments specify the name of the interface connected to the real IP address network and the name of the interface connected to the mapped IP address network.</p> <p>The <i>real_ip</i> argument specifies the real address that you want to translate. Specify the same IP address for both <i>real_ip</i> arguments.</p> <p>The <b>netmask mask</b> options specify the subnet mask for the real and mapped addresses.</p> <p>The <b>dns</b> 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.</p> <p></p> <p><b>Note</b> Note DNS inspection must be enabled to support this functionality.</p> <p>The <b>norandomseq</b> option disables TCP ISN randomization protection. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.</p> <p>For static PAT, the <b>tcp</b> option specifies the protocol as TCP.</p> <p>The <i>tcp_max_cons</i> 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.</p> <p>The optional <i>emb_limit</i> argument specifies the maximum number of embryonic connections per host. The default is 0, which means unlimited embryonic connections.</p> <p>The <b>udp udp_max_conns</b> option specifies 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.</p> <p>The example shown uses static identity NAT for an inside IP address (10.1.1.3) when accessed by the outside.</p>

### Examples of Regular Static Identity NAT

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

```
hostname(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:

```
hostname(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:

```
hostname(config)# static (inside,dmz) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
```

## Monitoring Static Identity NAT

To monitor static identity NAT, enter the following command:

Command	Purpose
<code>show running-config static</code>	Displays all static commands in the configuration.

## Feature History for Static Identity NAT

[Table 31-4](#) lists the release history for this feature.

**Table 31-4**      *Feature History for Static Identity NAT*

Feature Name	Releases	Feature Information
Static identity NAT	7.0	Static identity NAT translates the real IP address to the same IP address.  The following command was introduced: <b>static</b> .
NAT for transparent mode	8.0(2)	NAT began support in transparent firewall mode.

# Configuring NAT Exemption

This section includes the following topics:

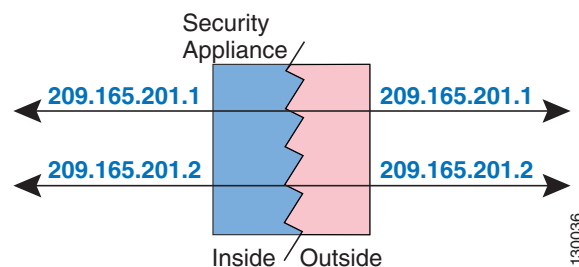
- [Information About NAT Exemption, page 31-11](#)
- [Licensing Requirements for NAT Exemption, page 31-11](#)
- [Guidelines and Limitations for NAT Exemption, page 31-12](#)
- [Configuring NAT Exemption, page 31-13](#)
- [Monitoring NAT Exemption, page 31-13](#)
- [Configuration Examples for NAT Exemption, page 31-13](#)
- [Feature History for NAT Exemption, page 31-14](#)

## Information About NAT Exemption

NAT exemption exempts addresses from translation and 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 than identity NAT. However, unlike policy NAT, NAT exemption does not consider the ports in the access list. Use static identity NAT to consider ports in the access list.

Figure 31-3 shows a typical NAT exemption scenario.

**Figure 31-3 NAT Exemption**



## Licensing Requirements for NAT Exemption

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

## Guidelines and Limitations for NAT Exemption

This section includes the guidelines and limitations for this feature:

### Context Mode Guidelines

- Supported in single and multiple context mode.

### Firewall Mode Guidelines

- Supported in routed and transparent firewall modes.

### Additional Guidelines and Limitations

- If you remove a NAT exemption configuration, existing connections that use NAT exemption are not affected. To remove these connections, enter the **clear local-host** command.
- NAT exemption does not support connection settings, such as maximum TCP connections.
- By default, the **nat** command exempts traffic from inside to outside. If you want traffic from outside to inside to bypass NAT, then add an additional **nat** command and enter **outside** to identify the NAT instance as outside NAT. You might want to use outside NAT exemption if you configure dynamic NAT for the outside interface and want to exempt other traffic.
- Access list hit counts, as shown by the **show access-list** command, do not increment for NAT exemption access lists.
- You can only apply one NAT exemption rule per interface. If you enter another rule for the same interface, the old rule is overwritten.

## Configuring NAT Exemption

To configure NAT exemption, enter the following command:

Command	Purpose
<pre>nat (real_interface) 0 access-list acl_name [outside]</pre> <p><b>Example:</b></p> <pre>hostname(config)# nat (inside) 0 access-list EXEMPT</pre>	<p>Configures NAT exemption.</p> <p>The <i>real_interface</i> argument specifies the name of the interface connected to the real IP address network.</p> <p>For NAT exemption, use the NAT ID of <b>0</b>.</p> <p>The <b>access-list</b> key word identifies local addresses and destination addresses using an extended access list. Create the extended access list using the <b>access-list extended</b> command. (See the <a href="#">Chapter 11, “Adding an Extended Access List.”</a>) This access list can include both <b>permit</b> ACEs and <b>deny</b> ACEs. Do not specify the real and destination ports in the access list; NAT exemption does not consider the ports. NAT exemption considers the <b>inactive</b> and <b>time-range</b> keywords, but it does not support ACL with all <b>inactive</b> and <b>time-range</b> ACEs.</p> <p>By default, this command exempts traffic from inside to outside. If you want traffic from outside to inside to bypass NAT, then add an additional <b>nat</b> command and enter <b>outside</b> to identify the NAT instance as outside NAT. You might want to use outside NAT exemption if you configure dynamic NAT for the outside interface and want to exempt other traffic.</p> <p>Enter <b>outside</b> if this interface is on a lower security level than the interface you identify by the matching global statement.</p> <p>(For additional information about command options, see the <b>nat</b> command in the Command Reference.)</p>

## Monitoring NAT Exemption

To monitor NAT bypass, enter the following command:

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

## Configuration Examples for NAT Exemption

The following examples show how to configure NAT exemption.

To exempt an inside network when accessing any destination address, enter the following command:

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

To use dynamic outside NAT for a DMZ network, and exempt another DMZ network, enter the following command:

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
hostname(config)# access-list EXEMPT permit ip 10.1.3.0 255.255.255.0 any
hostname(config)# nat (dmz) 0 access-list EXEMPT
```

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

```
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 NET1 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 0 access-list NET1
```

## Feature History for NAT Exemption

[Table 31-5](#) lists the release history for this feature.

**Table 31-5** Feature History for NAT Exemption

Feature Name	Releases	Feature Information
NAT exemption	7.0	NAT exemption exempts addresses from translation and allows both translated and remote hosts to initiate connections.  The following command was introduced: <b>nat</b> .
NAT for transparent mode	8.0(2)	NAT began support in transparent firewall mode.