



## Support for IPSec ESP Through NAT

The Support for IPSec ESP Through NAT feature provides the ability to support multiple concurrent IP Security (IPSec) Encapsulating Security Payload (ESP) tunnels or connections through a Cisco IOS Network Address Translation (NAT) device configured in Overload or Port Address Translation (PAT) mode.

### Feature Specifications for Support for IPSec ESP Through NAT Feature

---

#### Feature History

Release	Modification
12.2(13)T	This feature was introduced.

---

#### Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

---

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information about platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. In the release section, you can compare releases side by side to display both the features unique to each software release and the features that releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Contents

- [How to Configure IPsec ESP Through NAT, page 2](#)
- [Additional References, page 3](#)
- [Command Reference, page 5](#)

## How to Configure IPsec ESP Through NAT

This section contains the following procedures:

- [Configuring IPsec ESP Through NAT, page 2](#) (required)
- [Verifying IPsec ESP Through NAT, page 3](#) (optional)

## Configuring IPsec ESP Through NAT

To configure your NAT router for static translations to integrate with IPsec ESP, use the following commands:

### SUMMARY STEPS

1. **enable**
2. **configure { terminal | memory | network }**
3. **ip nat [inside | outside] source static *local-ip global-ip***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<code>configure {terminal   memory   network}</code>  <b>Example:</b> Router# configure terminal	<ul style="list-style-type: none"> <li>Enters global configuration mode.</li> </ul>
Step 3	<code>ip nat [inside   outside] source static local-ip global-ip</code>  <b>Example:</b> Router# ip nat inside source static 1.1.1.1 2.2.2.2	Enables static NAT translations.

## Verifying IPSec ESP Through NAT

To verify your configuration, perform the following optional step:

### SUMMARY STEPS

1. `enable`
2. `show ip nat translations`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>show ip nat translations</code>  <b>Example:</b> Router# show ip nat translations	(Optional) Displays active NAT translations.

## Additional References

For additional information related to Network Address Translation, refer to the following sections:

- [Related Documents, page 4](#)

- [Standards, page 4](#)
- [Standards, page 4](#)
- [RFCs, page 5](#)
- [Technical Assistance, page 5](#)

## Related Documents

Related Topic	Document Title
Additional NAT configuration tasks	The chapter “Configuring IP Addressing” in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2
Additional NAT commands	The chapter “IP Addressing Commands” in the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> , Release 12.2

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:  <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

RFCs <sup>1</sup>	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	

1. Not all supported RFCs are listed.

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents the modified **debug ip nat** command. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

# debug ip nat

To display information about IP packets translated by the IP Network Address Translation (NAT) feature, use the **debug ip nat** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip nat [access-list | detailed | h323 | ipsec | pptp | sip]
```

```
no debug ip nat [access-list | detailed | h323 | ipsec | pptp | sip]
```

## Syntax Description

<i>access-list</i>	(Optional) The standard IP access list number. If the datagram is not permitted by the specified access list, the related debugging output is suppressed.
<b>detailed</b>	(Optional) Displays debug information in a detailed format.
<b>h323</b>	(Optional) Displays H.225 and H.245 protocol information.
<b>ipsec</b>	(Optional) Displays IP Security (IPSec) packet information.
<b>pptp</b>	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) information.
<b>sip</b>	(Optional) Displays Session Initiation Protocol (SIP) information.

## Defaults

Disabled

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	This command was modified to include the <b>h323</b> keyword.
12.2(8)T	This command was modified to include the <b>sip</b> keyword.
12.2(13)T	This command was modified to include the <b>ipsec</b> keyword.

## Usage Guidelines

The NAT feature reduces the need for unique, registered IP addresses. It can also save private network administrators from needing to renumber hosts and routers that do not conform to global IP addressing.

Use the **debug ip nat** command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also outputs information about certain errors or exceptional conditions, such as the failure to allocate a global address. To display messages related to the processing of H.225 signaling and H.245 messages, use the **debug ip nat h323** command. To display messages related to the processing of SIP messages, use the **debug ip nat sip** command. To display messages related to the processing of IPSec messages, use the **debug ip nat ipsec** command.

**Caution**

Because the **debug ip nat** command generates a substantial amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

**Examples**

The following is sample output from the **debug ip nat** command. In this example, the first two lines show the debugging output produced by a Domain Name System (DNS) request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. All Telnet packets, except for the first packet, were translated in the fast path, as indicated by the asterisk (\*).

```
Router# debug ip nat
NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

Table 1 describes the significant fields shown in the display.

**Table 1** *debug ip nat Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature. An asterisk (*) indicates that the translation is occurring in the fast path. The first packet in a conversation always goes through the slow path (that is, it is process switched). The remaining packets go through the fast path if a cache entry exists.
s=192.168.1.95->172.31.233.209	Source address of the packet and how it is being translated.
d=172.31.2.132	Destination address of the packet.
[6825]	IP identification number of the packet. Might be useful in the debugging process to correlate with other packet traces from protocol analyzers.

The following is sample output from the **debug ip nat detailed** command. In this example, the first two lines show the debugging output produced by a DNS request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. In this example, the inside host 192.168.1.95 was assigned the global address 172.31.233.193.

```
Router# debug ip nat detailed
NAT: i: udp (192.168.1.95, 1493) -> (172.31.2.132, 53) [22399]
NAT: o: udp (172.31.2.132, 53) -> (172.31.233.193, 1493) [63671]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22400]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22002]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22401]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22402]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22060]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22071]
```

The following is sample output from the **debug ip nat h323** command. In this example, an H.323 call is established between two hosts, one host on the inside and the other one on the outside. The debug output displays the H.323 messages names that NAT recognizes and the embedded IP addresses contained in those messages.

```
Router# debug ip nat h323
NAT:H225:[0] processing a Setup message
NAT:H225:[0] found Setup sourceCallSignalling
NAT:H225:[0] fix TransportAddress addr=192.168.122.50 port=11140
NAT:H225:[0] found Setup fastStart
NAT:H225:[0] Setup fastStart PDU length:18
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC forward mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[0] Setup fastStart PDU length:29
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC reverse mediaChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16516
NAT:H245:[0] found OLC reverse mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[1] processing an Alerting message
NAT:H225:[1] found Alerting fastStart
NAT:H225:[1] Alerting fastStart PDU length:25
NAT:H245:[1] processing OpenLogicalChannel message, forward channe
```

Table 2 describes the significant fields shown in the display.

**Table 2** *debug ip nat h323 Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature.
H.225 and H.245:	Protocol of the packet.
[1]	Indicates that the packet is moving from a host inside the network to one outside the network.
[0]	Indicates that the packet is moving from a host outside the network to one inside the network.

The following is sample output from the **debug ip nat ipsec** command.

```
Router# debug ip nat ipsec
5d21h:NAT:new IKE going In->Out, source addr 192.168.122.35, destination addr
192.168.22.20, initiator cookie
0x9C42065D
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.35 SPI=0xAAE32A0A,
IG=192.168.22.40, OL=192.168.22.20,
OG=192.168.22.20
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0xA64B5BB6,
OL=192.168.22.20, IG=192.168.22.40,
IL=192.168.122.35
5d21h:NAT:new IKE going In->Out, source addr 192.168.122.20, destination addr
192.168.22.20, initiator cookie
0xC91738FF
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.20 SPI=0x3E2E1B92,
IG=192.168.22.40, OL=192.168.22.20,
```

```

OG=192.168.22.20
5d21h:NAT:IPSec:Inside host (IL=192.168.122.20) trying to open an ESP connection to
Outside host (OG=192.168.22.20),
wait for Out->In reply
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0x1B201366,
OL=192.168.22.20, IG=192.168.22.40,
IL=192.168.122.20

```

The following is sample output from the **debug ip nat sip** command. In this example, one IP phone registers with a Cisco SIP proxy and then calls another IP phone. The debug output displays the SIP messages that NAT recognizes and the embedded IP addresses contained in those messages.

```

Router# debug ip nat sip
NAT:SIP:[0] processing REGISTER message
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] message body found
NAT:SIP:[0] found address/port in SDP body:192.168.122.20
20332
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing SIP/2.0 200 OK reply message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing INVITE message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] message body found
NAT:SIP:[1] found address/port in SDP body:192.168.22.20

```

Table 3 describes the significant fields shown in the display.

**Table 3** *debug ip nat sip Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature.
SIP:	Protocol of the packet.
[1]	Indicates that the packet is moving from a host inside the network to one outside the network.
[0]	Indicates that the packet is moving from a host outside the network to one inside the network.

■ debug ip nat