



Using Application-Level Gateways with NAT

This module describes the basic tasks to configure an application-level gateway (ALG) with Network Address Translation (NAT). This module also provides information about the protocols that use ALGs for IP header translation.

NAT performs translation services on any TCP/UDP traffic that does not carry source and destination IP addresses in the application data stream. Protocols that do not carry the source and destination IP addresses include HTTP, TFTP, telnet, archie, finger, Network Time Protocol (NTP), Network File System (NFS), remote login (rlogin), remote shell (rsh) protocol, and remote copy (rcp).

Specific protocols that embed the IP address information within the payload require the support of an ALG. NAT requires a variety of ALGs to handle application data stream (Layer 7) protocol-specific services such as translating embedded IP addresses and port numbers in the packet payload and extracting new connection/session information from control channels.

NAT supports virtual routing and forwarding (VRF) for protocols that have a supported ALG.

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

- [Finding Feature Information, page 2](#)
- [Prerequisites for Using Application Level Gateways with NAT, page 2](#)
- [Restrictions for Using Application-Level Gateways with NAT, page 2](#)
- [Information About Using Application-Level Gateways with NAT, page 3](#)
- [How to Configure Application-Level Gateways with NAT, page 7](#)
- [Configuration Examples for Using Application-Level Gateways with NAT, page 13](#)
- [Where to Go Next, page 14](#)
- [Additional References for Using Application-Level Gateways with NAT, page 14](#)
- [Feature Information for Using Application-Level Gateways with NAT, page 15](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Using Application Level Gateways with NAT

- Before performing the tasks in this module, you should be familiar with the concepts described in the “Configuring NAT for IP Address Conservation” module.
- All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the “IP Access List Sequence Numbering” document.
- Before performing the tasks in this module, you should verify that the Session Initiation Protocol (SIP) and H.323 are not disabled. SIP and H.323 are enabled by default.

Restrictions for Using Application-Level Gateways with NAT

- Network Address Translation (NAT) translates only embedded IPv4 addresses.
- Protocols that require application-level gateway (ALG) processing are not compatible with load balancing. All process-switched packets use the per-packet load-balancing algorithm. Process switching uses the per-packet load-balancing algorithm across equal-cost paths. As a result, every odd or even process-switched packet may be dropped by ISPs in a dual-ISP scenario due to a failed Unicast Reverse Path Forwarding (uRPF) check because these packets have the same source IP address (which is allocated by NAT or Port Address Translation [PAT]), but are routed to different outside interfaces. The packet drop causes excessive delay and retransmission of packets.
- In Cisco IOS Release 12.4 Mainline, the NAT ALG for Session Initiation Protocol (SIP) does not support the following T.38 session attributes in the Session Description Protocol (SDP): sqn, cdsc, and cpar. These session attributes are removed from the SDP header by the NAT ALG, which causes the SIP-based T.38 calls to fail. This restriction is applicable only to the Cisco IOS Release 12.4 mainline. As a workaround, upgrade to Cisco IOS Release 12.4(1)T and later releases.

Information About Using Application-Level Gateways with NAT

Benefits of Configuring NAT IPsec

- NAT enables customers to deploy private IP addresses within their network and translate the private IP addresses to public IP addresses when connecting to the Internet or when interconnecting with another corporate network.
- NAT support for the Session Initiation Protocol (SIP) adds the ability to deploy NAT on VoIP solutions based on SIP.
- With NAT ALGs, customers can control their IP address scheme and include complete support for H.323 v2 gatekeeper designs.
- ESP entries in the translation table are normally delayed from being transmitted until a reply is received from the destination. With predictable security parameter indexes (SPIs) and SPI matching, the delay can be eliminated because SPI entries are matched. Some third-party concentrators require both source ports and incoming ports to use port 500. Use the **ip nat service preserve-port** command to preserve the ports rather than changing them, which is required with regular NAT.

IPsec

IPsec is a set of extensions to the IP protocol family in a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the IETF, IPsec ensures confidentiality, integrity, and authenticity of data communications across the public network and provides cryptographic security services.

Secure tunnels between two peers, such as two routers, are provided and decisions are made as to which packets are considered sensitive and should be sent through these secure tunnels, and which parameters should be used to protect these sensitive packets by specifying characteristics of these tunnels. When the IPsec peer receives a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

IPsec using Encapsulating Security Payload (ESP) can pass through a router running NAT without any specific support from it as long as Network Address Port Translation (NAPT) or address overloading is not configured.

There are a number of factors to consider when attempting an IPsec VPN connection that traverses a NAPT device that represents multiple private internal IP addresses as a single public external IP address. Such factors include the capabilities of the VPN server and client, the capabilities of the NAPT device, and whether more than one simultaneous connection is attempted across the NAPT device.

There are two possible methods for configuring IPsec on a router with NAPT:

- Encapsulate IPsec in a Layer 4 protocol such as TCP or UDP. In this case, IPsec is *sneaking* through NAT. The NAT device is unaware of the encapsulation.
- Add IPsec-specific support to NAPT. IPsec works with NAT in this case as opposed to *sneaking* through NAT. The NAT Support for IPsec ESP-- Phase II feature provides support for Internet Key Exchange (IKE) and ESP without encapsulation in tunnel mode through a Cisco IOS router configured with NAPT.

We recommend that TCP and UDP be used when conducting IPsec sessions that traverse a NAPT device. However, not all VPN servers or clients support TCP or UDP.

SPI Matching

SPI matching is used to establish VPN connections between multiple pairs of destinations. NAT entries will immediately be placed in the translation table for endpoints matching the configured access list..

Voice and Multimedia over IP Networks

SIP is a protocol developed by the IETF Multiparty Multimedia Session Control (MMUSIC) Working Group. The Cisco SIP functionality equips Cisco routers to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within the VoIP internetworking software.

Session Description Protocol (SDP) is a protocol that describes multimedia sessions. SDP may be used in SIP message bodies to describe multimedia sessions used for creating and controlling multimedia sessions with two or more participants.

The NAT Support for SIP feature allows SIP embedded messages passing through a router configured with NAT to be translated and encoded back to the packet. An ALG is used with NAT to translate the SIP or SDP messages.



Note

By default support for SIP is enabled on port 5060. Therefore, NAT-enabled devices interpret all packets on this port as SIP call messages. If other applications in the system use port 5060 to send packets, the NAT service may corrupt the packet as it attempts to interpret the packet as a SIP call message.

NAT Support of H.323 v2 RAS

Cisco IOS NAT supports all H.225 and H.245 message types, including those sent in the Registration, Admission, and Status (RAS) protocol. RAS provides a number of messages that are used by software clients and VoIP devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Some RAS messages include IP addressing information in the payload, typically meant to register a user with the gatekeeper or learn about another user already registered. If these messages are not known to NAT, they cannot be translated to an IP address that will be visible to the public.

In Cisco IOS Release 12.2(2)T and later releases, embedded IP addresses can be inspected for potential address translation. Prior to Cisco IOS Release 12.2(2)T, NAT did not support H.323 v2 RAS messages.

NAT Support for H.323 v3 and v4 in v2 Compatibility Mode

H.323 is an ITU-T specification for transmitting audio, video, and data across packet networks. NAT supports four versions of the H.323 protocols: Version 1, Version 2, Version 3, and Version 4. The NAT Support for H.323 v3 and v4 in v2 Compatibility Mode feature enables NAT routers to support messages coded in H.323 Version 3 and Version 4 when these messages contain fields that are compatible with H.323 Version 2. This feature does not support H.323 capabilities introduced in H.323 Version 3 and Version 4, such as new message types or new fields that require address translation.

NAT H.245 Tunneling Support

The NAT H.245 Tunneling Support feature supports H.245 tunneling in H.323 ALGs. The H.245 tunneling supports H.245 tunnel messages that are needed to create a media channel setup.

For an H.323 call to take place, an H.225 connection on TCP port 1720 must be opened. When the H.225 connection is opened, the H.245 session is initiated and established. The H.323 connection can take place on a separate channel other than the H.225 or it can be done by using H.245 tunneling on the same H.225 channel whereby the H.245 messages are embedded in H.225 messages and sent on the previously established H.225 channel.

If the H.245 tunneled message is not understood by NAT, the media address or the port number is left untranslated by NAT, resulting in media traffic failure. The H.245 FastConnect procedures will not help if the H.245 tunneled message is not understood by NAT because FastConnect is terminated as soon as an H.245 tunneled message is sent.

NAT Support of Skinny Client Control Protocol

Cisco IP phones use the SCCP to connect with and register to Cisco CallManager.

To be able to configure Cisco IOS NAT between the IP phone and Cisco CallManager in a scalable environment, NAT needs to be able to detect the SCCP and understand the information passed within the messages. Messages flow back and forth that include IP address and port information used to identify other IP phone users with which a call can be placed.

The SCCP client to Cisco CallManager communication typically flows from inside to outside. Domain Name System (DNS) should be used to resolve the Cisco CallManager IP address connection when the Cisco CallManager is on the inside (behind the NAT device), or static NAT should be configured to reach the Cisco CallManager in the inside.

When an IP phone attempts to connect to the Cisco CallManager and it matches the configured NAT rules, NAT will translate the original source IP address and replace it with one from the configured pool. This new address will be reflected in the Cisco CallManager and be visible to other IP phone users.

NAT Support of SCCP Fragmentation

Skinny Client Control Protocol (SCCP) messages, also called Skinny control messages, are exchanged over TCP. If either the IP phone or the Cisco Unified CallManager is configured to have a TCP maximum segment size (MSS) lower than the Skinny control message payload, the Skinny control message is segmented across multiple TCP segments. Prior to the introduction of this feature, Skinny control message exchanges used to fail during TCP segmentation because the NAT Skinny ALG was not able to reassemble Skinny control messages. The NAT SCCP Fragmentation Support feature adds support for TCP segments for the NAT Skinny ALG and fragmented payloads that requires an IP translation or a port translation is no longer dropped.

Skinny control messages can also be IP fragmented by using Virtual Fragmentation Reassembly (VFR).

In Cisco IOS Release 15.1(3)T and later releases, NAT works with SCCP phones Version 17 and higher.

NAT Segmentation with Layer 4 Forwarding

The NAT Segmentation with Layer 4 Forwarding feature is implemented for the H.323, Skinny Client Control Protocol (SCCP), and the TCP Domain Name System (DNS) protocol. NAT supports the processing of segmented H.323, SCCP, or TCP DNS messages that are split across multiple packets.

Layer 4 forwarding or TCP proxy is responsible for session handling that includes setting sequence numbers in order, acknowledging the numbers in a packet, resegmenting the translated packet if it is larger than the maximum segment size (MSS), and handling retransmissions in case of packet loss. Layer 4 forwarding also handles out-of-order packets and these packets are buffered and not dropped. Layer 4 forwarding buffers received packets and notifies the NAT ALG when an in-order packet is available, sends acknowledgments to end hosts for received packets, and sends translated packets that it receives from the NAT ALG back into the output packet path.

Restrictions

The NAT Segmentation with Layer 4 Forwarding feature does not work when:

- Firewalls are configured using the **ip inspect name** command. (Context-Based Access Control (CBAC) firewalls are not supported. Zone-based firewalls are supported.)
- H.323, SCCP, or TCP DNS messages are larger than 18 KB.
- Multiprotocol Label Switching (MPLS) is configured.
- NAT and the Cisco Unified CallManager are configured on the same device. In this case, a colocated solution in Call Manager Express is used.
- NAT Virtual Interface (NVI) is configured.
- Stateful Network Address Translation (SNAT) is enabled.



Note Effective January 31, 2014, Stateful NAT is not available in Cisco IOS software. For more information, see [End-of-Sale and End-of-Life Announcement for the Cisco IOS Stateful Failover of Network Address Translation \(SNAT\)](#).

- The **match-in-vrf** keyword is configured along with the **ip nat inside source** command for packet translation.
- The packets are IPv6 packets.

How to Configure Application-Level Gateways with NAT

Configuring IPsec Through NAT

Configuring IPsec ESP Through NAT

IPsec ESP Through NAT provides the ability to support multiple concurrent IPsec ESP tunnels or connections through a Cisco IOS NAT device configured in Overload or PAT mode.

Perform this task to configure IPsec ESP through NAT.


Note

IPsec can be configured for any NAT configuration, not just static NAT configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat [inside | outside] source static *local-ip global-ip* [vrf *vrf-name*]**
4. **exit**
5. **show ip nat translations**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nat [inside outside] source static <i>local-ip global-ip</i> [vrf <i>vrf-name</i>] Example: Router(config)# ip nat inside source static 10.10.10.10 192.168.30.30	Enables static NAT.

	Command or Action	Purpose
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.
Step 5	show ip nat translations Example: Router# show ip nat translations	(Optional) Displays active NATs.

Enabling the Preserve Port

This task is used for IPsec traffic using port 500 for the source port. Perform this task to enable port 500 to be preserved for the source port.



Note This task is required by certain VPN concentrators. Cisco VPN devices generally do not use this feature.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat service list** *access-list-number* **IKE preserve-port**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip nat service list <i>access-list-number</i> IKE preserve-port Example: <pre>Router(config)# ip nat service list 10 IKE preserve-port</pre>	Specifies IPsec traffic that matches the access list to preserve the port.

Enabling SPI Matching on the NAT Device



Note SPI matching is disabled by default.

Security parameter index (SPI) matching is used to establish VPN connections between multiple pairs of destinations. NAT entries are immediately placed in the translation table for endpoints matching the configured access list. SPI matching is available only for endpoints that choose SPIs according to the predictive algorithm implemented in Cisco IOS Release 12.2(15)T.

The generation of SPIs that are predictable and symmetric is enabled. SPI matching should be used in conjunction with NAT devices when multiple ESP connections across a NAT device are desired.

Before You Begin

Cisco IOS software must be running on both the source router and the remote gateway enabling parallel processing.



Note SPI matching must be configured on the NAT device and both endpoint devices.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat service list** *access-list-number* **ESP spi-match**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nat service list <i>access-list-number</i> ESP spi-match Example: Router(config)# ip nat service list 10 ESP spi-match	Specifies an access list to enable SPI matching. <ul style="list-style-type: none"> This example shows how to enter ESP traffic matching list 10 into the NAT table, making the assumption that both devices are Cisco devices and are configured to provide matchable SPIs.

Enabling SPI Matching on Endpoints

Before You Begin

Cisco software must be running on both the source device and the remote gateway, enabling parallel processing.



Note Security parameter index (SPI) matching must be configured on the Network Address Translation (NAT) device and on both endpoint devices.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto ipsec nat-transparency spi-matching
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	crypto ipsec nat-transparency spi-matching Example: Device(config)# crypto ipsec nat-transparency spi-matching	Enables SPI matching on both endpoints.
Step 4	end Example: Device(config)# end	Exits global configuration mode and enters privileged EXEC mode.

Enabling MultiPart SDP Support for NAT

The MultiPart SDP Support for NAT feature provides support for the multipart Session Description Protocol (SDP) in a SIP ALG. MultiPart SDP support for NAT is disabled by default.



Note NAT translates only embedded IPv4 addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat service allow-multipart**
4. **exit**
5. **show ip nat translations**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip nat service allow-multipart Example: Device(config)# ip nat service allow-multipart	Enables multipart SDP.
Step 4	exit Example: Device(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 5	show ip nat translations Example: Device# show ip nat translations	(Optional) Displays active NATs.

Configuring NAT Between an IP Phone and Cisco CallManager

This section describes configuring Cisco's Skinny Client Control Protocol (SCCP) for Cisco IP phone to Cisco CallManager communication. The task in this section configures NAT between an IP phone and Cisco CallManager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat service skinny tcp port *number***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>ip nat service skinny tcp port <i>number</i></pre> <p>Example:</p> <pre>Router(config)# ip nat service skinny tcp port 20002</pre>	Configures the skinny protocol on the specified TCP port.

Configuration Examples for Using Application-Level Gateways with NAT

Example: Specifying a Port for NAT Translation

```
ip nat service skinny tcp port 20002
```

Example: Enabling the Preserve Port

The following example shows how to configure TCP port 500 of the third-party concentrator. Access list 10 is configured.

```
ip nat service list 10 IKE preserve-port
access-list 10 permit 10.1.1.1
```

Example Enabling SPI Matching

The following example shows how to enable SPI matching. Access list 10 is configured:

```
ip nat service list 10 ESP spi-match
access-list 10 permit 10.1.1.1
```

Example: Enabling SPI Matching on Endpoints

```
crypto ipsec nat-transparency spi-matching
```

Example: Enabling MultiPart SDP Support for NAT

```
ip nat service allow-multipart
```

Example: Specifying a port for NAT Translation

```
ip nat service skinny tcp port 20002
```

Where to Go Next

- To learn about NAT and configure NAT for IP address conservation, see the “Configuring NAT for IP Address Conservation” module.
- To verify monitor, and maintain NAT, see the “Monitoring and Maintaining NAT” module.
- To integrate NAT with MPLS VPNs, see the “Integrating NAT with MPLS VPNs” module.
- To configure NAT for high availability, see the “Configuring NAT for High Availability” module.

Additional References for Using Application-Level Gateways with NAT

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
NAT commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Addressing Services Command Reference
IP access list sequence numbering	<i>IP Access List Sequence Numbering</i>
NAT IP address conservation	<i>Configuring NAT for IP Address Conservation</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Using Application-Level Gateways with NAT

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Using Application-Level Gateways with NAT

Feature Name	Releases	Feature Configuration Information
MultiPart SDP Support for NAT	15.0(1)M	The MultiPart SDP Support for NAT feature adds support for multipart SDP in a SIP ALG. This feature is disabled by default. The following commands were modified by this feature: debug ip nat and ip nat service .
NAT H.245 Tunneling Support	12.3(11)T	The NAT H.245 Tunneling Support feature allows H.245 tunneling in H.323 Application-Level Gateways (ALGs).
NAT Support for H.323 v2 RAS feature	12.2(2)T 15.0(1)S	NAT supports all H.225 and H.245 message types, including those sent in the RAS protocol.
NAT Support for H.323 v3 and v4 in v2 Compatibility Mode	12.3(2)T	The NAT Support for H.323 v3 and v4 in v2 Compatibility Mode feature enables NAT routers to support messages coded in H.323 Version 3 and Version 4 when these messages contain fields that are compatible with H.323 Version 2. This feature does not add support for H.323 capabilities introduced in H.323 Version 3 and Version 4, such as new message types or new fields that require address translation.
NAT Support for IPsec ESP—Phase II	12.2(15)T	The NAT Support for IPsec ESP—Phase II feature provides support for Internet Key Exchange (IKE) and ESP without encapsulation in tunnel mode through a router configured with NAPT.

Feature Name	Releases	Feature Configuration Information
NAT Support of SCCP Fragmentation	12.4(6)T 15.1(3)T	The NAT Support of SCCP Fragmentation feature adds support for TCP segments for the NAT Skinny ALG. A fragmented payload that requires an IP translation or a port translation is no longer be dropped. The following command was modified by this feature: debug ip nat .
NAT Support for SIP	12.2(8)T	NAT Support for SIP adds the ability to configure NAT on VoIP solutions based on SIP.
Support for applications that do not use H.323	12.2(33)XNC	NAT with an ALG will translate packets from applications that do not use H.323, as long as these applications use port 1720.
Support for IPsec ESP Through NAT	12.2(13)T	The IPsec ESP Through NAT feature provides the ability to support multiple concurrent IPsec Encapsulating Security Payload (ESP) tunnels or connections through a NAT device configured in Overload or Port Address Translation (PAT) mode.