Using Application-Level Gateways with NAT

Last Updated: November 29, 2012

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 ALG 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. The 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), and remote copy (rcp).

Specific protocols that embed IP address information within the payload require 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

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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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.
- You should have already configured all access lists required for use with the tasks in this module.
- You should verify that Session Initiation Protocol (SIP) and H.323 are not disabled. SIP and H.323 are enabled by default.

Information About Configuring Application-Level Gateways with NAT

Application-Level Gateways

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address information inside the payload of an application packet. An ALG is used to interpret the application-layer protocol and perform firewall and Network Address Translation (NAT) actions. These actions can be one or more of the following depending on your configuration of the firewall and NAT:

- Allow client applications to use dynamic TCP or UDP ports to communicate with the server application.
- Recognize application-specific commands and offer granular security control over them.
- Synchronize multiple streams or sessions of data between two hosts that are exchanging data.
- Translate the network-layer address information that is available in the application payload.

The firewall opens a pinhole, and NAT performs translation service on any TCP or UDP traffic that does not carry the source and destination IP addresses in the application-layer data stream. Specific protocols or applications that embed IP address information require the support of an ALG.

IPsec

IPsec is a set of extensions to the IP 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 the characteristics of these tunnels. When

the IPsec peer receives a sensitive packet, the peer 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. These factors include capabilities of the VPN server and client, 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 device 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 device 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.

- Benefits of Configuring NAT IPsec, page 3

Benefits of Configuring NAT IPsec

- NAT enables customers to deploy private IP addresses within their network and perform translation to public IP addresses when connecting to the Internet or interconnecting with another corporate network.
- 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 the SPI entries are matched. Some third-party concentrators require both the source and incoming ports to use port 500. Use of the **preserve-port** keyword with the **ip nat service** command preserves the ports rather than changing them, which is required with regular NAT.

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.

NAT Support for Application-Level Gateways

The following section provides information on NAT support for ALGs.

The features described in the following subsections are enabled by default unless otherwise noted; no configuration is necessary:

- NAT Support of Skinny Client Control Protocol, page 4
- NAT SCCP Video Support, page 4
- NAT vTCP ALG Support, page 4
- NAT NetBIOS ALG Support, page 5

NAT Support of Skinny Client Control Protocol

Cisco IP phones use the Skinny Client Control Protocol (SCCP) to connect with and register to Cisco Unified CallManager.

To deploy NAT between the IP phone and the Cisco Unified CallManager in a scalable environment, NAT must detect SCCP and understand the information that is passed within these messages. Messages that flow back and forth include the IP address and the port information to identify other IP phone users with whom calls can be placed.

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

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

NAT SCCP Video Support

NAT provides SCCP video message translation support.

NAT vTCP ALG Support

NAT provides virtual TCP (vTCP) support to handle TCP segmentation and reassembling for ALG. When a Layer 7 protocol uses TCP for transportation, the payload can be segmented due to various reasons, such as Maximum Segment Size (MSS), application design, and TCP window size. Proper recognition of these TCP segments is required to perform parsing. Therefore, a generic framework called vTCP is used by various ALGs to perform TCP segmentation.

Some applications such as SIP and NAT require the entire payload to rewrite embedded data. In addition, ALGs are not developed to consider data splitting between the packets, which is required for the firewall. Therefore, vTCP is also required for the firewall without any changes to current ALGs. NAT and the firewall ALG configuration activate the vTCP configuration.

vTCP does not support data channel traffic. To protect system resources, vTCP does not support reassembled messages larger than 8 KB.

- NAT ALG--vTCP for SIP, page 5

NAT ALG--vTCP for SIP

Cisco IOS XE Release 3.2S supports the NAT ALG—vTCP for SIP feature. With the introduction of vTCP support for SIP, individual TCP segments will be chained together to form a complete SIP message and passed to the SIP parser. vTCP also supports acknowledgement (ACK) and reliable transmission of buffered data. ACK is a SIP method that is used to acknowledge that the received message is valid and accepted.

The NAT ALG—vTCP for SIP feature does not support:

- Data channel traffic.
- Reassembled Layer 7 messages that are larger than 8 KB.
- TCP segments that are larger than 8 KB.
- vTCP SIP trunk calls.

NAT NetBIOS ALG Support

NAT application awareness includes support for Network Basic Input Output System (NetBIOS) applications. A NetBIOS ALG translates IP addresses and port numbers embedded in NetBIOS packets when a NAT mapping is processed. The NAT NetBIOS ALG Support feature introduced the **show platform hardware qfp** [**active** | **standby**] **feature alg statistics netbios** command to display NetBIOS-specific information for a device and the **match protocol netbios** command to configure network-based application recognition (NBAR) to match the NetBIOS traffic.

NAT RCMD ALG Support

NAT application awareness includes support for remote command (RCMD) execution service applications, remote login (rlogin), remote shell (rsh) protocol, and remote execution (rexec). An RCMD ALG translates IP addresses and port numbers embedded in RCMD application packets when a NAT mapping is processed. The NAT RCMD ALG Support feature introduced the **show platform software trace message** *process* **qfp active** command to display RCMD-specific information for a device.

NAT RTSP ALG Support

NAT application awareness includes support for Real-Time Streaming Protocol (RTSP) applications. An RTSP ALG translates IP addresses and port numbers embedded in RTSP packets when a NAT mapping is processed.

NAT Support for SIP—Voice and Multimedia over IP Networks

SIP is a protocol developed by the IETF Multiparty Multimedia Session Control (MMUSIC) Working Group. The Cisco Session Initiation Protocol (SIP) functionality equips Cisco devices to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within 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 device that is configured with NAT to be translated and encoded back to the packet. An ALG is used with NAT to translate SIP 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 ALG--SIP Multiple Media Line Support, page 6

NAT ALG--SIP Multiple Media Line Support

The NAT ALG—SIP Multiple Media Line Support feature supports a maximum of five media lines in SDP. These media lines can be a combination of audio, video, and data.

SDP describes multimedia sessions. The description includes the media type, the transport port to which the media stream is sent, the transport protocol, and the media format. All media descriptions start with the media line attribute “m=” and terminate at the end of the session description. There can be multiple media lines depending on the services supported by SIP peers.

The NAT ALG—SIP Multiple Media Line Support feature uses the transport port information in the media description to create a door for NAT. Doors are transient structures that allow incoming traffic that matches a specific criterion. A door is created when there is not enough information to create a complete NAT session entry. A door contains information about the source IP address and destination IP address and the destination port. However, it does not have information about the source port. When media data arrives, the source port information is known and the door is promoted to a real NAT session.

When a door receives information about the source IP address, destination IP address, source port, destination port, and protocol from the incoming packet, it will change itself from a door to a full NAT session. A door and a full NAT session are saved in different databases. When a door becomes a full NAT session, the door entry is removed from the door database and a new NAT entry is added to the NAT session database.

NAT ALG--SIP REFER Method

The NAT ALG—SIP REFER Method feature is used for call transfers. A REFER message is used to refer to a peer. The REFER method indicates that the recipient of a call, identified by a request Uniform Resource Identifier (URI), must contact a third party using the contact information provided in the request.

The NAT ALG—SIP REFER Method feature supports two types of call transfers, unattended (blind) transfer and attended (consultative) transfer.

NAT ALG--SIP Trunking Support

A SIP trunk is a direct connection of an IP PBX to a service provider over an IP network using SIP. There can be numerous concurrent calls in a SIP trunk. During the call setup process, all calls use the same control channel for call establishment. More than one call uses the same control channel for call setup. When the same control channel is used by more than one call, the stateful information stored in the control channel sessions becomes unreliable. SIP stateful information consists of media channel information such as the IP address and port number used by client/server endpoints to send media data. The media channel information is used to create a door for the data channel in NAT. Because multiple calls use the same control channel for call setup, there will be multiple sets of media data. The NAT ALG—SIP Trunking

Support feature uses a local database to store all media-related information within a SIP trunk. Call IDs of each call are used to index this local database.

TCP segmentation in a SIP trunk can cause unexpected behavior that includes packet drops, TCP reset, and slow response.

NAT SIP Extended Methods

NAT supports extended methods for SIP.

ALG--SCCP Version 17 Support

The ALG—SCCP Version 17 Support feature enables the SCCP ALG to parse SCCP Version 17 packets. Cisco Unified Communications Manager 7.0 and the IP phones that use Cisco Unified Communications Manager 7.0 support only SCCP Version 17 messages. The format of SCCP changed from Version 17 to support IPv6. The SCCP ALG checks for the SCCP version in the prefix of a message before parsing it according to the version. The SCCP message version is extracted from the message header and if it is greater than Version 17, the message is parsed by using the Version 17 format and the IPv4 address and port information is extracted. The SCCP ALG supports the inspection and translation of IPv4 address information in SCCP messages.

Note IPv6 address inspection and translation are not supported.

The IP address format of the following SCCP ALG-handled messages changed in Version 17:

- StationOpenMultiMediaReceiveChannelAck
- StationOpenReceiveChannelAckMessage
- StationRegisterMessage
- StationStartMediaTransmissionAckMessage
- StationStartMultiMediaTransmissionAckMessage
- StationStartMediaTransmissionMessage
- StationStartMultiMediaTransmissionMessage

Basic H.323 ALG Support

H.323 is a recommendation published by the ITU-T defining a series of network elements and protocols for multimedia transmission through packet-based networks. H.323 defines a number of network elements used in multimedia transmission.

Although most H.323 implementations today utilize TCP as the transport mechanism for signaling, H.323 Version 2 enables basic UDP transport.

- H.323 Terminal—This element is an endpoint in the network, providing two-way communication with another H.323 terminal or gateway.
- H.323 Gateway—This element provides protocol conversion between H.323 terminals and other terminals that do not support H.323.
- H.323 Gatekeeper—This element provides services like address translation, network access control, and bandwidth management and account for H.323 terminals and gateways.

The following core protocols are described by the H.323 specification:

- H.225—This protocol describes call signaling methods used between any two H.323 entities to establish communication.
- H.225 Registration, Admission, and Status (RAS)—This protocol is used by the H.323 endpoint and gateway for address resolution and admission control services.
- H.245—This protocol is used for exchanging the capabilities of multimedia communication and for the opening and closing of logical channels for audio, video, and data.

In addition to the protocols listed, the H.323 specification describes the use of various IETF protocols like the Real Time Transport (RTP) protocol and audio (G.711, G.729, and so on) and video (H.261, H.263, and H.264) codecs.

NAT requires a variety of ALGs to handle 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. The H.323 ALG performs these specific services for H.323 messages.

NAT Support of H.323 v2 RAS

NAT supports all H.225 and H.245 message types, including those sent in the Remote Access Service (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. 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 to learn about another user already registered. If these messages are not known to NAT, they cannot be translated to an IP address that is visible to the public.

Embedded IP addresses can be inspected for potential address translation.

ALG—H.323 v6 Support

ALG—H.323 v6 supports the parsing of H.323 v6 packets and the inspection and translation of IPv4 address information in H.323 messages. The basic H.323 ALG supports only the parsing of H.323 v4 messages. H.323 v6 extends the basic H.323 ALG support to recognize the new message format and to handle new fields that contain the IPv4 address information.

H.323 v6 consists of core protocols, H.225.0 v6, and H.245 v13 and uses an assigned gatekeeper for transmission.

ALG—H.323 v6 does not support:

- Stream Control Transmission Protocol (SCTP)—This protocol provides similar services like TCP or UDP.
- Configuring of the H225 port number.

NAT NetMeeting Directory (LDAP)

NAT provides ALG support for NetMeeting directory Lightweight Directory Access Protocol (LDAP) Version 2 and Version 3 messages.

Users can establish calls/connections among each other directly or through a NetMeeting directory. NetMeeting implements a series of LDAP messages for users to register themselves and perform lookups of other NetMeeting users against the directory. These messages include IP address information.

Before a NAT device can use a NetMeeting directory, NAT needs to understand the LDAP messages and perform standard NAT processing against the IP address information within these messages.

NAT DNS ALG Support

NAT application awareness includes support for the Domain Name System (DNS). An application-level gateway (ALG) translates IP addresses and port numbers embedded in the DNS payload when a NAT mapping is processed.

With CSCuc05660, for DNS payloads that are address-translated, the DNS time to live (TTL) value in CNAME entries is passed through. Before CSCuc05660 and before support for the **ip nat service dns-reset-ttl** command was added, the TTL value in the CNAME entries was reset by default.

NAT ICMP ALG Support

NAT application awareness includes translation support for the Internet Control Message Protocol (ICMP). An ALG translates data embedded in the ICMP payload when a NAT mapping is processed.

NAT TFTP ALG Support

NAT application awareness includes support for TFTP. A TFTP ALG creates a path for the TFTP data to traverse the NAT-enabled device.

NAT FTP ALG Support

NAT application awareness includes support for FTP. An FTP ALG performs translation for the IP addresses and TCP port information embedded in the payload of an FTP control session.

How to Configure Application-Level Gateways with NAT

Configuring IPsec ESP Through NAT

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat inside source static esp** *local-ip* **interface** *type number*
4. **exit**
5. **show ip nat translations**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat inside source static esp** *local-ip* **interface** *type number* **Example:** `Device(config)# ip nat inside source static esp 192.0.2.23 interface gigabitethernet 0/0/0`	Establishes the IPsec Encapsulating Security Payload (ESP) (tunnel mode) support.
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.

• Restrictions, page 10

Restrictions

- Network Address Translation (NAT) will translate only embedded IPv4 addresses.
- The multicast gatekeeper discovery mechanism is not supported.

Enabling the Preserve Port

This task is used for IPsec traffic using port 500 for the source port and incoming port. Some third-party concentrators require both the source and incoming ports to use port 500. Use of the **preserve-port** keyword with the **ip nat service** command preserves the ports rather than changing one, which is required with regular Network Address Translation (NAT).

Note This task is required by certain VPN concentrators, but will cause problems with other 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**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat service list** *access-list-number* **IKE preserve-port** **Example:** `Device(config)# ip nat service list 10 IKE preserve-port`	Preserves the UDP port in IKE packets.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Disabling SPI Matching on the NAT Device or Changing the Default Port

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

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

SPI matching is enabled by default for listening on port 2000. You can use this task to either change the default port or to disable SPI matching.

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. **ip nat service list** *access-list-number* **esp spi-match**
4. **no ip nat service list** *access-list-number* **esp spi-match**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat service list** *access-list-number* **esp spi-match** **Example:** `Device(config)# ip nat service list 10 esp spi-match`	Specifies a port other than the default port. • This example shows how to enter ESP traffic matching list 10 into the NAT table, based on the assumption that both devices are Cisco devices and are configured to provide matchable SPIs.
Step 4	**no ip nat service list** *access-list-number* **esp spi-match** **Example:** `Device(config)# no ip nat service list 10 esp spi-match`	Disables SPI matching.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Enabling SPI Matching on Endpoints

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec nat-transparency spi-matching** **Example:** `Device(config)# crypto ipsec nat-transparency spi-matching`	Enables SPI matching on both endpoints.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Specifying a Port for NAT Translation

The following task describes how to configure Skinny Client Control Protocol (SCCP) for a Cisco IP phone to Cisco Unified CallManager communication.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat service skinny tcp port** *number* **Example:** `Device(config)# ip nat service skinny tcp port 20002`	Configures the Skinny protocol on the specified TCP port.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuration Examples for Using Application-Level Gateways with NAT

Example: Configuring IPsec ESP Through NAT

The following example shows NAT configured on a device with a static route. NAT is configured as inside source static one-to-one translations.

```
ip nat pool outside 192.0.2.1 192.0.2.14 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 192.0.2.3 0.0.0.255
ip nat inside source static esp 192.0.2.23 interface gigabitethernet 0/0/0
ip nat inside source static esp 192.0.2.21 interface gigabitethernet 0/0/1
```

Example: Enabling the Preserve Port

The following example shows how to configure TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

Example: Disabling SPI Matching on the NAT Device or Changing the Default Port

```
ip nat service list 10 esp spi-match
no ip nat service list 10 esp spimatch
```

Example: Enabling SPI Matching on Endpoints

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

Example: Specifying a port for NAT Translation

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

Additional References for Using Application-Level Gateways with NAT

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
NAT commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
Configuring NAT for IP Address Conservation	"Configuring NAT for IP Address Conservation" module
IP Addressing Services configuration tasks	*Cisco IOS XE IP Addressing Services Configuration Guide*
NAT and Firewall ALG support	*NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers* matrix
SIP Call Flows	*"SIP Call Flows"* document

Standards and RFCs

Standard/RFC	Title
RFC 3515	*The Session Initiation Protocol (SIP) Refer Method*

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 Information
ALG--H.323 v6 Support	Cisco IOS XE Release 3.6S	The ALG-H.323 v6 supports the parsing of H.323 v6 packets and the inspection and translation of IPv4 address information in H.323 messages.
ALG--SCCP Version 17 Support	Cisco IOS XE Release 3.5S	The ALG-SCCP Version 17 Support feature enables the SCCP ALG to parse SCCP Version 17 packets. Cisco Unified Communications Manager 7.0 and IP phones that use Cisco Unified Communications Manager 7.0 support only SCCP Version 17 messages. The SCCP Version 17 packets support IPv6 packets. The SCCP ALG supports the inspection and translation of IPv4 address information in SCCP messages.
NAT ALG--SIP REFER Method	Cisco IOS XE Release 3.2S	The NAT ALG--SIP REFER method feature supports two types of call transfers, unattended (blind) transfer and attended (consultative) transfer.
NAT ALG--SIP Trunking Support	Cisco IOS XE Release 3.2S	The NAT ALG--SIP Trunking Support feature uses a local database to store all media-related information within a SIP trunk. Call IDs of each call are used to index this local database.
NAT Basic H.323 ALG Support	Cisco IOS XE Release 2.1	NAT requires a variety of ALGs to handle 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. The NAT Basic H.323 ALG support feature provides these specific services for H.323 messages.

Feature Name	Releases	Feature Information
NAT DNS ALG Support	Cisco IOS XE Release 2.1	The NAT DNS ALG Support feature supports translation of DNS packets.
NAT FTP ALG Support	Cisco IOS XE Release 2.1	The NAT FTP ALG Support feature supports translation of FTP packets.
NAT H.323 RAS	Cisco IOS XE Release 2.4	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.
NAT ICMP ALG Support	Cisco IOS XE Release 2.1	The NAT ICMP ALG Support feature supports translation of ICMP packets.
NAT NetBIOS ALG Support	Cisco IOS XE Release 3.1S	NAT provides Network Basic Input Output System (NetBIOS) message translation support. The NAT NetBIOS ALG Support feature introduced the following command to display NetBIOS-specific information for a device: **show platform hardware qfp** [**active** | **standby**] **feature alg statistics netbios**.
NAT NetMeeting Directory (LDAP)	Cisco IOS XE Release 2.4	The NAT NetMeeting Directory (LDAP) feature provides ALG support for NetMeeting directory LDAP messages.

Feature Name	Releases	Feature Information
NAT RCMD ALG Support	Cisco IOS XE Release 3.1S	NAT provides remote command execution service (RCMD) message translation support. The NAT RCMD ALG Support feature introduced the following command to display RCMD-specific information for a device: **show platform software trace message** *process* **qfp active**.
NAT RTSP ALG Support	Cisco IOS XE Release 3.1S	The NAT RTSP ALG Support feature provides RTSP message translation support.
NAT--SCCP for Video	Cisco IOS XE Release 2.4	The NAT--SCCP for Video feature provides SCCP video message translation support.
NAT--SIP ALG Enhancement for T.38 Fax Relay	Cisco IOS XE Release 2.4.1	The NAT--SIP ALG Enhancement for T.38 Fax Relay feature provides translation support for SIP ALG support of T.38 Fax Relay over IP.
NAT--SIP Extended Methods	Cisco IOS XE Release 2.4	The NAT--SIP Extended Methods feature supports extended methods for SIP.
NAT Support of IP Phone to Cisco CallManager	Cisco IOS XE Release 2.1	The NAT Support of IP Phone to Cisco CallManager feature adds NAT support for configuring Cisco SCCP for a Cisco IP phone-to-Cisco CallManager communication.
NAT Support for IPsec ESP--Phase II	Cisco IOS XE Release 2.1	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 device configured with NAPT.
NAT Support for SIP	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2S	The NAT Support for SIP feature adds the ability to deploy NAT between VoIP solutions based on SIP.
NAT TFTP ALG Support	Cisco IOS XE Release 2.1	The NAT TFTP ALG Support feature supports translation of TFTP packets.

Feature Name	Releases	Feature Information
NAT VRF-Aware ALG Support	Cisco IOS XE Release 2.5	The NAT VRF-Aware ALG Support feature supports VPN routing and forwarding (VRF) for protocols that have a supported ALG.
NAT vTCP ALG Support	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2S	The NAT vTCP ALG Support feature provides vTCP support to handle TCP segmentation and reassembling for ALG.
Support for IPsec ESP Through NAT	Cisco IOS XE Release 2.1	The Support for IPsec ESP Through NAT feature provides the ability to support multiple, concurrent IPsec ESP tunnels or connections through a NAT device configured in Overload or PAT mode.