Using Application Level Gateways with NAT

Network Address Translation (NAT) performs translation service on any Transmission Control Protocol/User Datagram Protocol (TCP/UDP) traffic that does not carry source and/or destination IP addresses in the application data stream. These protocols include HTTP, Trivial File Transfer Protocol (TFTP), telnet, archie, finger, Network TimeProtocol (NTP), Network File System (NFS), remote login (rlogin), remote shell protocol (rsh), and remote copy protocol (rcp). Specific protocols that do imbed IP address information within the payload require support of an Application Level Gateway (ALG).

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 NAT device configured in Overload or Port Address Translation (PAT) mode.

Module History

This module was first published on May 2, 2005, and last updated on February 27, 2006.

Finding Feature Information in This Module

To find information about feature support and configuration, use the "Feature Information for Using Application Level Gateways with NAT" section on page 11.

Contents

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.

Cisco Systems

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

- 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 at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm
- Before performing the tasks in this module, you should verify that Session Initiation Protocol (SIP) and H.323 have not been disabled. SIP and H.323 are enabled by default.

Information About Configuring Application Level Gateways with NAT

To configure ALGs with NAT, you should understand the following concept:

- Application Level Gateway, page 2

Application Level Gateway

An application level gateway is an application that translates IP address information inside the payload of an applications packet.

How to Configure Application Level Gateways with NAT

This section contains the following procedures:

- Configuring IPSec Through NAT, page 2
- Deploying NAT Between an IP Phone and Cisco CallManager, page 8

Configuring IPSec Through NAT

This section contains the following tasks related to configuring IPSec through NAT:

- Configuring IPSec ESP Through NAT, page 4 (required)
- Enabling Preserve Port, page 6 (optional)
- Disabling SPI Matching on the NAT Device or Changing the Default Port, page 6 (required)
- Enabling SPI Matching on the Endpoints, page 7 (required)

Benefits of Configuring NAT IPSec

- NAT support for SIP adds the ability to deploy Cisco IOS NAT between VoIP solutions based on SIP.
- Customers can control their IP address scheme and include complete support for H.323 v2 gatekeeper designs.

- 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.
- Normally ESP entries in the translation table are 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 since 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 one, which is required with regular NAT.

IP Security

IP Security (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 Internet Engineering Task Force (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 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 are not configured.

There are a number of factors to consider when attempting an IPSec Virtual Private Network (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.

The recommended protocols to use when conducting IPSec sessions that traverse a NAPT device are TCP and UDP but not all VPN servers or clients support TCP or UDP.

SPI Matching

Security Parameter Index (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. SPI matching is available only for endpoints that choose SPIs according to the predictive algorithm implemented in Cisco IOS Release 12.2(15)T.

Voice and Multimedia over IP Networks

SIP is a protocol developed by the Internet Engineering Task Force (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 Voice over IP (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.

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 Voice over IP (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.

Previously, NAT did not support H.323 v2 RAS messages. With this enhancement, embedded IP addresses can be inspected for potential address translation.

NAT H.245 Tunneling Support

NAT H.245 tunneling allows H.245 tunneling in H.323 ALGs. NAT H.245 tunneling provides a mechanism for supporting H.245 tunnel message which are needed to create a media channel setup.

In order for an H.323 call to take place, an H.225 connection on TCP port 1720 needs to be opened. When the H.225 connection is opened, the H.245 session is initiated and established. This connection can take place on a separate channel from the H.225 or it can be done using H.245 tunneling on the same H.225 channel whereby the H.245 messages are embedded in the H.225 messages and sent on the previously established H.225 channel.

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

Restrictions

- NAT will translate only embedded IP version 4 addresses.

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.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• 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`** *`local-ip global-ip`*
	Example:
	`Router(config)# ip nat inside source static 10.10.10.10 172.16.30.30`
		Enables static NAT.

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 Preserve Port

This task is used for IPSec traffic using port 500 for the source and incoming ports. Perform this task to enable port 500 to be preserved for both source and incoming ports.

Restrictions

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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ip nat service list`** *`access-list-number`* **`ike preserve-port`**
	Example:
	`Router(config)# ip nat service list 10 ike preserve-port`
		Specifies a port other than the default port.

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

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.

SPI Matching is enabled by default for listening on port 2000. This task may be used to either change the default port or disable SPI matching.

Prerequisites

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

Restrictions

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ip nat service list`** *`access-list-number`* **`esp spi-match`**
	Example:
	`Router(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, making 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:
	`Router(config)# no ip nat service list 10 esp spi-match`
		Disables SPI matching.

Enabling SPI Matching on the Endpoints

Perform this task to enable SPI matching on both endpoints.

Prerequisites

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

Restrictions

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec spi-matching**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec spi-matching** **Example:** `Router(config)# crypto ipsec spi-matching`	Enables SPI matching on both endpoints.

Deploying NAT Between an IP Phone and Cisco CallManager

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

NAT Support of Skinny Client Control Protocol

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

To be able to deploy Cisco IOS NAT between the IP phone and CCM 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 CCM communication typically flows from inside to outside. DNS should be used to resolve the CCM IP address connection when the CCM is on the inside (behind the NAT device), or static NAT should be configured to reach the CCM in the inside.

When an IP phone attempts to connect to the CCM 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 CCM and be visible to other IP phone users.

NAT Support of SCCP Fragmentation

Skinny control messages are exchanged over TCP. If either the IP phone or CCM has been configured to have TCP maximum segment size (MSS) lower than the skinny control message payload, the skinny control message will be segmented across multiple TCP segments. Prior to this feature skinny control message exchanges would fail in a TCP segmentation scenario because NAT skinny ALG was not able to reassemble the skinny control messages. The NAT SCCP Fragmentation Support feature adds support for TCP segments for NAT skinny ALG. A fragmented payload that requires an IP or port translation will no longer be dropped.

Skinny control messages can also be IP fragmented but they are supported using Virtual Fragmentation Reassembly (VFR).

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.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ip nat service skinny tcp port`** *`number`*
	Example:
	`Router(config)# ip nat service skinny tcp port 20002`
		Configures the skinny protocol on the specified TCP port.

Configuration Examples for Using Application Level Gateways with NAT

This section provides the following configuration examples:

- Configuring IPSec ESP Through NAT: Example, page 10
- Enabling the Preserve Port: Example, page 10
- Enabling SPI Matching: Example, page 10
- Configuring SPI Matching on the Endpoint Routers: Example, page 10
- Deploying NAT Between an IP Phone and Cisco CallManager: Example, page 10

Configuring IPSec ESP Through NAT: Example

The following example shows NAT configured on the Provider Edge (PE) router with a static route to the shared service for the gold and silver Virtual Private Networks (VPNs). NAT is configured as inside source static 1- to-1 translations.

```
ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 168.58.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 2.2.2.1 vrf gold
ip nat inside source static 192.169.121.33.2.2.2.2 vrf silver
```

Enabling the Preserve Port: Example

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

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

Enabling SPI Matching: Example

The following example shows how to enable SPI matching:

```
ip nat service list 10 esp spi-match
```

Configuring SPI Matching on the Endpoint Routers: Example

The following example show how to enable SPI matching on the endpoint routers:

```
crypto ipsec spi-matching
```

Deploying NAT Between an IP Phone and Cisco CallManager: Example

The following example shows how to configure the 20002 port of the CallManager:

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

Where to Go Next

- To learn about Network Address Translation 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

The following sections provide references related to using application level gateways with NAT.

Related Documents

Related Topic	Document Title
NAT commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"IP Addressing Commands" chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*, Release 12.4T

Standards

Standards	Title
None	

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Using Application Level Gateways with NAT

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the "Configuring Network Address Translation Features Roadmap."

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Using Application Level Gateways with NAT

Feature Name	Releases	Feature Configuration Information
The NAT Support for IPSec ESP— Phase II feature	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 Cisco IOS router configured with NAPT. The following sections provide information about this feature: • "Configuring IPSec Through NAT" section on page 2 • "Configuring IPSec ESP Through NAT: Example" section on page 10
NAT Support for SIP feature	12.2(8)T	NAT Support for SIP adds the ability to deploy Cisco IOS NAT between VoIP solutions based on SIP. The following section provides information about this feature: • "Configuring IPSec Through NAT" section on page 2
NAT Support for H.323 v2 RAS feature	12.2(2)T	Cisco IOS NAT supports all H.225 and H.245 message types, including those sent in the RAS protocol. The following section provides information about this feature: • "NAT Support of H.323 v2 RAS" section on page 4
Support for IPSec ESP Through NAT	12.2(13)T	IPSec ESP Through NAT 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. The following section provides information about this feature: • "Configuring IPSec ESP Through NAT" section on page 4

Table 1 Feature Information for Using Application Level Gateways with NAT

Feature Name	Releases	Feature Configuration Information
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). The following section provides information about this feature: • "NAT H.245 Tunneling Support" section on page 4
NAT SCCP Fragmentation Support	12.4(6)T	The NAT SCCP Fragmentation Support feature adds support for TCP segments for NAT skinny ALG. A fragmented payload that requires an IP or port translation will no longer be dropped. The following section provides information about this feature: • "NAT Support of SCCP Fragmentation" section on page 9

This module first published May 2, 2005. Last updated May 2, 2005