



NAT Routemaps Outside-to-Inside Support

The NAT Routemaps Outside-to-Inside Support feature enables the deployment of a NAT routemap configuration that will allow IP sessions to be initiated from the outside to the inside.

History for the NAT Routemaps Outside-to-Inside Support Feature

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

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.

Contents

- [Restrictions for NAT Routemaps Outside-to-Inside Support, page 1](#)
- [Information About NAT Routemaps Outside-to-Inside Support, page 2](#)
- [How to Configure NAT Routemaps Outside-to-Inside Support, page 2](#)
- [Configuration Examples for NAT Routemaps Support, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)

Restrictions for NAT Routemaps Outside-to-Inside Support

- Only IP hosts that are part of the routemap configuration will allow outside sessions.
- Outside-to-inside support is not available with Port Address Translation (PAT).
- Outside sessions must use an access list.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- Access lists with reversible routemaps must be configured to match the inside-to-outside traffic.
- Match-interface or Match Next-hop is not supported for reversible routemaps.

Information About NAT Routemaps Outside-to-Inside Support

To configure the NAT Routemaps Outside-to-Inside Support feature, you should understand the following concept:

- [Routemaps Outside-to-Inside Support Feature Design, page 2](#)

Routemaps Outside-to-Inside Support Feature Design

An initial session from inside-to-outside is required to trigger a NAT translation. New translation sessions can then be initiated from outside-to-inside to the inside host that triggered the initial translation.

When routemaps are used to allocate global addresses, the global address can allow return traffic, and the return traffic is allowed only if the return traffic matches the defined routemap in the reverse direction. Current functionality remains unchanged by not creating additional entries to allow the return traffic for a routemap-based dynamic entry unless the **reversible** keyword is used with the **ip nat inside source** command.

How to Configure NAT Routemaps Outside-to-Inside Support

This section contains the following procedure:

- [Enabling NAT Routemaps Outside-to-Inside Support, page 2](#)

Enabling NAT Routemaps Outside-to-Inside Support

Perform this task to enable NAT Routemaps Outside-to-Inside Support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip netmask netmask*
4. **ip nat pool** *name start-ip end-ip netmask netmask*
5. **ip nat inside source route-map** *name pool name* [**reversible**]
6. **ip nat inside source route-map** *name pool name* [**reversible**]

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 pool name start-ip end-ip netmask netmask Example: Router# ip nat pool POOL-A 30.1.10.1 30.1.10.126 netmask 255.255.255.128	Defines a pool of network addresses for network address translation (NAT).
Step 4	ip nat pool name start-ip end-ip netmask netmask Example: Router# ip nat pool POOL-B 30.1.20.1 30.1.20.126 netmask 255.255.255.128	Defines a pool of network addresses for network address translation (NAT).
Step 5	ip nat inside source route-map name pool name reversible Example: Router# ip nat inside source route-map MAP-A pool POOL-A reversible	Enables outside-to-inside initiated sessions to use routemaps for destination-based NAT.
Step 6	ip nat inside source route-map name pool name reversible Example: Router# ip nat inside source route-map MAP-B pool POOL-B reversible	Enables outside-to-inside initiated sessions to use routemaps for destination-based NAT.

Configuration Examples for NAT Routemaps Support

This section provides the following configuration example:

- [Enabling NAT Routemaps Outside-to-Inside Support: Example, page 3](#)

Enabling NAT Routemaps Outside-to-Inside Support: Example

The following example shows how to configure routemap A and routemap B to allow outside-to-inside translation for a destination-based NAT translation:

```
ip nat pool POOL-A 30.1.10.1 30.1.10.126 netmask 255.255.255.128
ip nat pool POOL-B 30.1.20.1 30.1.20.126 netmask 255.255.255.128
```

```

ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
!
ip access-list extended ACL-A
 permit ip any 30.1.10.128 0.0.0.127
ip access-list extended ACL-B
 permit ip any 30.1.20.128 0.0.0.127
!
route-map MAP-A permit 10
 match ip address ACL-A
!
route-map MAP-B permit 10
 match ip address ACL-B

```

The following example shows how to configure routemap R1 to allow outside-to-inside translation for static NAT:

```

ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 30.1.10.128 0.0.0.127

route-map R1 permit 10
 match ip address ACL-A

```

Additional References

The following sections provide references related to the NAT Routemaps Outside-to-Inside Support feature.

Related Documents

Related Topic	Document Title
IP NAT commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services , Release 12.3T
IP NAT configuration tasks	“Configuring Network Address Translation” section of Part 1 of the Cisco IOS IP Configuration Guide , Release 12.3

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

This section documents one modified command only.

- **ip nat inside source**

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

Dynamic NAT

```
ip nat inside source {list {access-list-number | access-list-name} | route-map name} {interface
type number | pool name} [mapping-id map-id | overload | reversible | vrf name]
```

```
no ip nat inside source {list {access-list-number | access-list-name} | route-map name} {interface
type number | pool name} [mapping-id map-id | overload | reversible | vrf name]
```

Static NAT

```
ip nat inside source {static {esp local-ip interface type number | local-ip global-ip}} [extendable]
[mapping-id map-id] [no-alias] [no-payload] [redundancy group-name] [route-map name
[reversible]] [vrf name]
```

```
no ip nat inside source {static {esp local-ip interface type number | local-ip global-ip}}
[extendable] [mapping-id map-id] [no-alias] [no-payload] [redundancy group-name]
[route-map name [reversible]] [vrf name]
```

Port Static NAT

```
ip nat inside source {static {tcp | udp {local-ip local-port global-ip global-port | interface type
name global-port}}} [extendable] [mapping-id map-id] [no-alias] [no-payload] [redundancy
group-name] [route-map name [reversible]] [vrf name]
```

```
no ip nat inside source {static {tcp | udp {local-ip local-port global-ip global-port | interface type
name global-port}}} [extendable] [mapping-id map-id] [no-alias] [no-payload] [redundancy
group-name] [route-map name [reversible]] [vrf name]
```

Network Static NAT

```
ip nat inside source static network local-network global-network mask [extendable] [no-alias]
[no-payload] [mapping-id map-id] [redundancy group-name] [vrf name]
```

```
no ip nat inside source static network local-network global-network mask [extendable] [no-alias]
[no-payload] [mapping-id map-id] [redundancy group-name] [vrf name]
```

Syntax Description

list <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
route-map <i>name</i>	Specifies the named routemap.
interface <i>type</i>	Specifies the interface type for the global address.
interface <i>number</i>	Specifies the interface number for the global address.

pool <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
mapping-id <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
reversible	(Optional) Enables outside-to-inside initiated sessions to use routemaps for destination-based NAT.
vrf <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
static <i>local-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
<i>local-port</i>	Sets the local TCP/UDP port in a range from 1 to 65535.
static <i>global-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the globally unique IP address of an inside host as it appears to the outside network.
<i>global-port</i>	Sets the global TCP/UDP port in a range from 1 to 65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits an alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Establishes NAT redundancy.
esp <i>local-ip</i>	Establishes IPSec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	Specifies the global subnet translation.
<i>mask</i>	Established the IP Network mask to be used with subnet translations.

Defaults

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use ratemaps with static translations, and the route-map <i>name</i> keyword and argument combination was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the redundancy <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the no-payload keyword was added.
12.2(13)T	The interface keyword was added for static translations. The mapping-id <i>map-id</i> keyword and argument combination was added for dynamic translations. The vrf <i>name</i> keyword and argument combination was added.
12.3(7)T	The static mapping-id <i>map-id</i> keyword and argument combination was added.
12.3(14)T	The reversible keyword was added.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Examples

The following example shows how to translate between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example shows how to translate only traffic local to the providers edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface e 0 vrf shop overload
ip nat inside source list 1 interface e 0 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 192.1.1.1
ip route vrf bank 0.0.0.0 0.0.0.0 192.1.1.1
!
access-list 1 permit 10.1.1.1.0 0.0.0.255
!
```

```

ip nat inside source list 1 interface e 1 vrf shop overload
ip nat inside source list 1 interface e 1 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 172.1.1.1 global
ip route vrf bank 0.0.0.0 0.0.0.0 172.1.1.1 global
access-list 1 permit 10.1.1.0 0.0.0.255

```

The following example shows how to translate sessions from outside-to-inside.

```

ip nat pool POOL-A 30.1.10.1 30.1.10.126 255.255.255.128
ip nat pool POOL-B 30.1.20.1 30.1.20.126 255.255.255.128

ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
!
ip access-list extended ACL-A
 permit ip any 30.1.10.128 0.0.0.127
ip access-list extended ACL-B
 permit ip any 30.1.20.128 0.0.0.127
!
AP-A permit 10
 match ip address ACL-A
!
route-map MAP-B permit 10
 match ip address ACL-B
!

```

The following example shows how to configure routemap R1 to allow outside-to-inside translation for static NAT:

```

ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 30.1.10.128 0.0.0.127

route-map R1 permit 10
 match ip address ACL-A

```

Related Commands	Command	Description
	clear ip nat translation	Clears dynamic NAT translations from the translation table.
	ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
	ip nat inside destination	Enables NAT of the inside destination address.
	ip nat outside source	Enables NAT of the outside source address.
	ip nat pool	Defines a pool of IP addresses for NAT.
	ip nat service	Enables a port other than the default port.
	show ip nat statistics	Displays NAT statistics.
	show ip nat translations	Displays active NAT translations.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.