Using Non–Standard FTP Port Numbers with NAT

Document ID: 13776

Contents

Introduction

Cisco IOS® Software Releases 11.2(13) and 11.3(3) introduced the functionality for Network Address Translation (NAT) to support non–standard File Transfer Protocol (FTP) port numbers. In earlier Cisco IOS software releases, when a NAT–enabled router receives a packet with IP addresses that need to be NAT–translated, and the standard TCP port number is for the FTP control connection (21), the router recognizes the packet as an FTP packet, and does any necessary translation in the payload (data portion) of the packet. However, if the FTP server is using a non–standard FTP port number, NAT ignores the payload of the packet. This can prevent FTP data connections from being established.

In order to support the use of non–standard FTP port numbers, you must use the **ip nat service** command. This table describes the options available on this command:

Option	Definition
list	Specify the access list describing global addresses.
name	Access list name for server local address.
number	Access list number for global addresses.
ftp	FTP protocol.
tcp	TCP protocol.
port	Special non–standard port.
port number	Number of special non–standard port.

This is a sample syntax:

```
router-6(config)#ip nat service list 10 ftp tcp port 2021
```

Some important things to note:

- The access list address in the above command must match the inside local IP address for the FTP server with the non–standard FTP control port.

- If a non−standard FTP control port is configured for an FTP server, NAT stops checking FTP control connections that are using port 21 for that FTP server. All other FTP servers continue to function normally.
- A host with an FTP server using a non−standard control port can also have an FTP client using the standard FTP control port (21).
- If an FTP server uses both port 21 and a non−standard port, then you need to configure both ports using the **ip nat service list** *<acl>* **ftp tcp** *<port>* command. For example:

```
ip nat service list 10 ftp tcp port 2021
ip nat service list 10 ftp tcp port 21
```

However, you cannot configure multiple access lists for the same port and the same service. For example:

```
router-6(config)#ip nat service list 17 ftp tcp port 2021
router-6(config)#ip nat service list 10 ftp tcp port 2021
% service "ftp tcp port 2021" is already configured for access-list 17
```

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Releases 11.2(13), 11.3(3), and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Sample Configurations

In each of the examples below, the flows that NAT processes as FTP control connections are described in a table following the configurations. In each table, "any local address" refers to any address that does not equal 10.1.1.1.

Sample Configuration 1

Assume that these FTP servers are running in your local network:

- An FTP server with IP address 10.1.1.1 running on TCP port number 2021.
- Additional FTP servers with IP address "any" (other than 10.1.1.1) at TCP port number 21.

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

Source Address	Source TCP Port	Destination Address	Destination TCP Port
any local address	any port	10.1.1.1	2021
any local address	any port	any local address (see note)	21
10.1.1.1	any port	any local address (see note)	21

Note: Any local address does not equal 10.1.1.1.

This list describes the NAT process that is detailed in the preceding table:

- **First line:** A packet with any source address and any port number destined to FTP server (10.1.1.1) with destination TCP port number 2021 needs to have the necessary NAT translation of the payload.
- **Second line:** A packet with any source address and any port number destined to any local address (other than 10.1.1.1) with destination TCP port number 21 (typical FTP control port) needs to have the necessary NAT translation of the payload. Therefore enabling all the FTP servers (other than 10.1.1.1) running on typical port 21 to have the necessary NAT translation of payload.
- **Third line:** A packet sourced from 10.1.1.1 with any port number destined to any local address (other than 10.1.1.1) with destination TCP port 21 needs to have the necessary NAT translation of payload.

Sample Configuration 2

Assume that these FTP servers are running in your local network:

- An FTP server with IP address 10.1.1.1 running on TCP port number 21 and 2021.
- Some FTP servers with IP address "any" (other than 10.1.1.1) at TCP port number 21.

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

Source Address	Source TCP Port	Destination Address	Destination TCP Port
any local address	any port	10.1.1.1	2021
any local address	any port	10.1.1.1	21
any local address	any port	any local address	21
any local address	any port	any local address	21

This list describes the NAT process that is detailed in the preceding table:

- **First line:** A packet with any source address and any port number destined to FTP server (10.1.1.1) with destination TCP port number 2021 needs to have the necessary NAT translation of the payload.
- **Second line:** A packet with any source address and any port number destined to FTP server (10.1.1.1) with destination TCP port number 21 needs to have the necessary NAT translation of the payload.

- **Third line:** A packet with any source address and any port number destined to any local address with destination TCP port number 21 (typical FTP control port) needs to have the necessary NAT translation of the payload. Therefore enabling all the FTP servers running on typical port 21 to have the necessary NAT translation of the payload.
- **Fourth line:** A packet sourced from 10.1.1.1 with any port number destined to any local address with destination TCP port 21 needs to have the necessary NAT translation of the payload.

Sample Configuration 3

Assume that these FTP servers are running in your local network:

- An FTP server with IP address 10.1.1.1 running on TCP port number 21.
- FTP servers with IP address 10.1.1.0/24 (other than 10.1.1.1) on TCP port number 2021.

```
ip nat service list 10 ftp tcp port 2021
access-list 10 deny 10.1.1.1
access-list 10 permit 10.1.1.0 0.0.0.255
```

Source Address	Source TCP Port	Destination Address	Destination TCP Port
any local address	any port	10.1.1.1	21
any local address	any port	10.1.1.x (see note)	2021
10.1.1.x (see note)	any port	Any address other than 10.1.1.x (see note)	21

Note: 10.1.1.x does not equal 10.1.1.1.

This list describes the NAT process that is detailed in the preceding table:

- **First line:** A packet with any source address and any port number destined to FTP server (10.1.1.1) with destination TCP port number 21 needs to have the necessary NAT translation of the payload.

  Note: Packets destined to 10.1.1.1 with port 2021 do not have NAT payload translation because of the deny 10.1.1.1 statement in the access−list.
- **Second line:** A packet with any source address and any port number destined to any local address (other than 10.1.1.1) with destination TCP port number 2021 needs to have the necessary NAT translation of the payload.
- **Third line:** A packet sourced from any 10.1.1.x (refer to the note below the table above) (other than 10.1.1.1) with any port number destined to any address (other than 10.1.1.x) with destination TCP port 21 needs to have the necessary NAT translation of the payload.

It is important to remember when a non−standard FTP control port is configured for an FTP server, NAT stops FTP control sessions that are using port 21 for that particular server. If an FTP server uses both standard and non−standard ports, then you need to configure both ports using the **ip nat service** command.

Sample Scenario and Configuration

The FTP server 10.1.1.1 at TCP port number 2021 is running on the inside network. The NAT router is configured to allow FTP traffic to be NAT'ed for control connections at port 2021.

Network Diagram
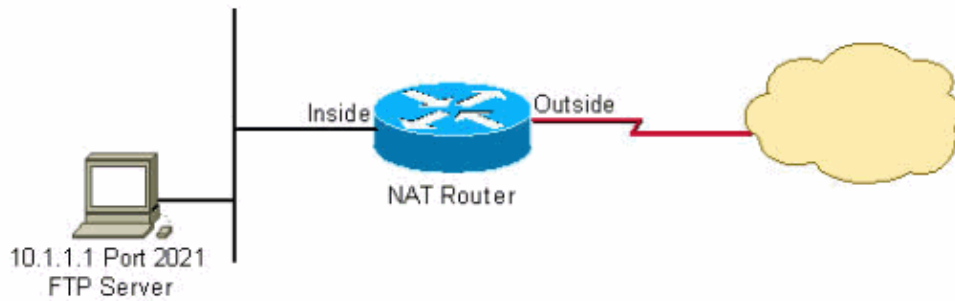
Configuration:

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 192.168.10.1 255.255.255.252
 ip nat outside
!
ip nat service list 10 ftp tcp port 2021
ip nat inside source static 10.1.1.1 20.20.20.1

!--- Static NAT translation for inside local address 10.1.1.1
!--- to inside global address 20.20.20.1.

!
access-list 10 permit 10.1.1.1
```

Related Information

- **How NAT Works**
- **NAT Frequently Asked Questions**
- **Sample Configuration Using the ip nat outside source static Command**
- **Verifying NAT Operation and Basic NAT Troubleshooting**
- **NAT Support Page**
- **Technical Support & Documentation – Cisco Systems**