Configuring Network Address Translation: Getting Started

Contents

Introduction

This document explains configuring Network Address Translation (NAT) on a Cisco router for use in common network scenarios. The target audience of this document is first time NAT users.

Note: In this document, when we refer to the internet, or an internet device, we mean a device on any external network.

Quick Start Steps for Configuring and Deploying NAT

When configuring NAT it's sometimes difficult to know where to begin, especially if you're new to NAT. The following steps guide you through defining what you want NAT to do and how to configure it.

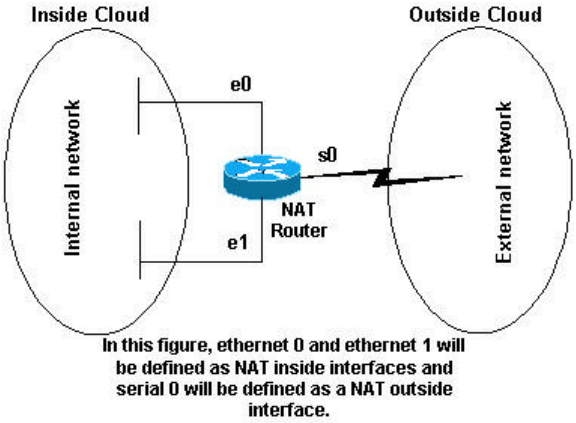
1. Define NAT inside and outside interfaces.
    - Do users exist off multiple interfaces?
    - Are there multiple interfaces going to the internet?
2. Define what you're trying to accomplish with NAT.
    - Are you trying to allow internal users to access the internet?
    - Are you trying to allow the internet to access internal devices (such as a mail server or w eb server)?
    - Are you trying to redirect TCP traffic to another TCP port or address?
    - Are you using NAT during a network transition (for example, you changed a server's IP address and until you can update all the clients you want the non-updated clients to be able to access the server using the original IP address as well as allow the updated clients to access the server using the new address)?
    - Are you using NAT to allow overlapping networks to communicate?
3. Configure NAT in order to accomplish what you defined above. Based on what you defined in Step 2, you need determine which of the following features to use:
    - Static NAT.
    - Dynamic NAT.
    - Overloading.
    - Any combination of the above.

4. Verify NAT operation.

Each of the following NAT examples guides you through steps 1 through 3 of the Quick Start Steps above. These examples describe some common scenarios in which we recommend you deploy NAT.

Defining NAT Inside and Outside Interfaces

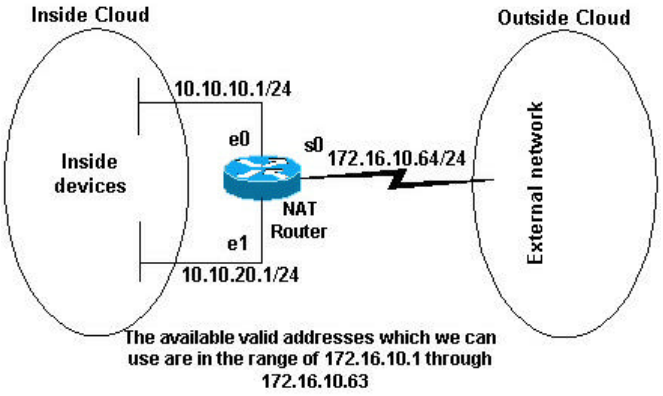
The first step in deploying NAT is to define NAT inside and outside interfaces. You may find it easiest to define your internal network as inside, and the external network as outside. However, the terms internal and external are subject to arbitration as well. The figure below shows an example of this.



Example: Allowing Internal Users to Access the Internet

You may want to allow internal users to access the internet, but you may not have enough valid addresses to accommodate everyone. If all communication with devices in the internet will originate from the internal devices, you need a single valid address or a pool of valid addresses.

The figure below shows a simple network diagram with the router interfaces defined as inside and outside.



In this example, we want NAT to allow certain devices (the first 31 from each subnet) on the inside to originate communication with devices on the outside by translating their invalid address to a valid address or pool of addresses. The pool has been defined as the range of addresses 172.16.10.1 through 172.16.10.63.

Now we're ready to configure NAT. In order to accomplish what we defined above, we need to use dynamic NAT. With dynamic NAT, the translation table in the router is initially empty and gets populated once traffic that needs to be translated passes through the router. (As opposed to static NAT, where a translation is statically configured and is placed in the translation table without the need for any traffic.)

In our example, we can configure NAT to translate each of the inside devices to a unique valid address, or to translate each of the inside devices to the same valid address. This second method is known as overloading. An example of how to configure each method is given below.

Configuring NAT to Allow Internal Users to Access the Internet

NAT Router

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!-- Defines Ethernet 0 with an IP address and as a NAT inside interface

interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside
!-- Defines Ethernet 1 with an IP address and as a NAT inside interface

interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside
!-- Defines serial 0 with an IP address and as a NAT outside interface

ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24
 !
!-- Defines a NAT pool named no-overload with a range of addresses
!-- 172.16.10.1 - 172.16.10.63

ip nat inside source list 7 pool no-overload
 !
 !
!-- Indicates that any packets received on the inside interface that
!-- are permitted by access-list 7
!-- will have the source address translated to an address out of the
!-- NAT pool "no-overload"

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31
!-- Access-list 7 permits packets with source addresses ranging from
!-- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

Note: We highly recommended that you do not configure access lists referenced by NAT commands with **permit any**. Using **permit any** can result in NAT consuming too many router resources which can cause network problems.

Notice in the above configuration that only the first 32 addresses from subnet 10.10.10.0 and the first 32 addresses from subnet 10.10.20.0 are permitted by **access-list 7**. Therefore, only these source addresses are translated. There may be other devices with other addresses on the inside network, but these won't be translated.

Configuring NAT to Allow Internal Users to Access the Internet Using Overloading

NAT Router

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!-- Defines Ethernet 0 with an IP address and as a NAT inside interface

interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside
!-- Defines Ethernet 1 with an IP address and as a NAT inside interface

interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside
!-- Defines serial 0 with an IP address and as a NAT outside interface

ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24
 !
!-- Defines a NAT pool named ovrld with a range of a single IP
!-- address, 172.16.10.1

ip nat inside source list 7 pool ovrld overload
 !
 !
 !
 !
!-- Indicates that any packets received on the inside interface that
!-- are permitted by access-list 7 will have the source address
!-- translated to an address out of the NAT pool named ovrld.
!-- Translations will be overloaded which will allow multiple inside
!-- devices to be translated to the same valid IP address.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31
!-- Access-list 7 permits packets with source addresses ranging from
!-- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

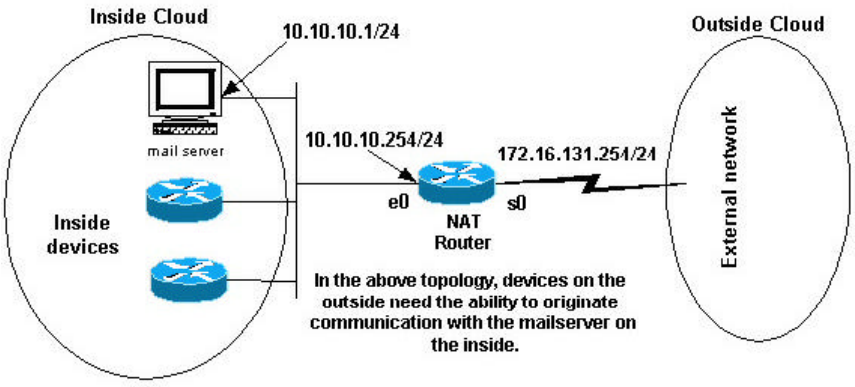
Note in the second configuration above, the NAT pool ovrld only has a range of one address. The keyword **overload** used in the **ip nat inside source list 7 pool ovrld overload** command allows NAT to translate multiple inside devices to the single address in the pool.

Another variation of this command is **ip nat inside source list 7 interface serial 0 overload**, which configures NAT to overload on the address that is assigned to the serial 0 interface. When this type of overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses. For definitions of global and local address, please refer to NAT: Global and Local Definitions.

The final step is to verify that NAT is operating as intended.

Example: Allowing the Internet to Access Internal Devices

You may need internal devices to exchange information with devices on the internet, where the communication is initiated from the internet devices, for example, email. It's typical for devices on the internet to send email to a mail server that resides on the internal network.



Configuring NAT to Allow the Internet to Access Internal Devices

In this example, we first defined the NAT inside and outside interfaces, as shown in the network diagram above.

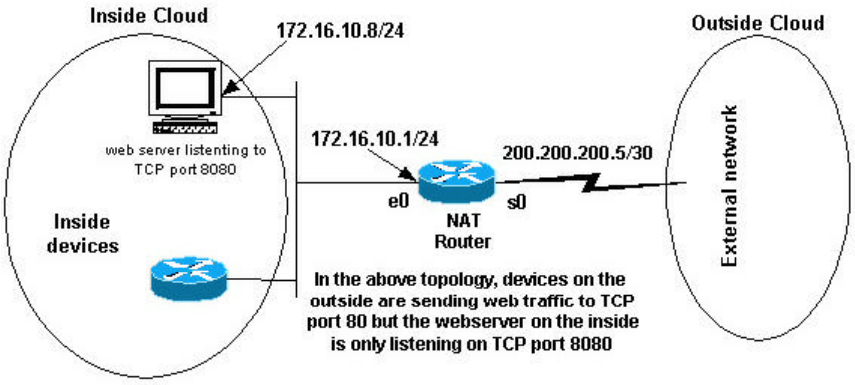
Second, we defined that we want users on the inside to be able to originate communication with the outside. Devices on the outside should be able to originate communication with only the mail server on the inside.

The third step is to configure NAT. To accomplish what we've defined, we can configure static and dynamic NAT together. For more information on how to configure this example, see Configuring Static and Dynamic NAT Simultaneously.

The final step is to verify that NAT is operating as intended.

Example: Redirecting TCP Traffic to Another TCP Port or Address

Having a web server on the internal network is another example of when it may be necessary for devices on the internet to initiate communication with internal devices. In some cases the internal web server may be configured to listen for web traffic on a TCP port other than port 80. For example, the internal web server may be configured to listen to TCP port 8080. In this case, you can use NAT to redirect traffic destined to TCP port 80 to TCP port 8080.



After defining the interfaces as shown in the network diagram above, we decide that we want NAT to redirect packets from the outside destined for 172.16.10.8:80 to 172.16.10.8:8080. We can achieve what we want using a **static nat** command to translate the TCP port number. An sample configuration is shown below.

Configuring NAT to Redirect TCP Traffic to Another TCP Port or Address

NAT Router

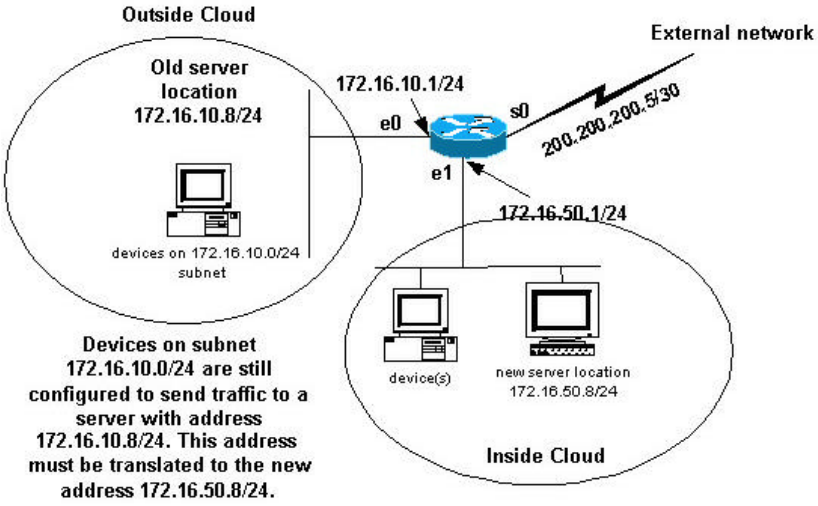
```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat inside
!-- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface serial 0
 ip address 200.200.200.5 255.255.255.252
 ip nat outside
!-- Defines serial 0 with an IP address and as a NAT outside interface.

ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80
!-- Static NAT command that states any packet received in the inside
!-- interface with a source address of 172.16.10.8:8080 will be
!-- translated to 172.16.10.8:80.
```

Note that the configuration description for the static NAT command indicates any packet received in the inside interface with a source address of 172.16.10.8:8080 will be translated to 172.16.10.8:80. This also implies that any packet received on the outside interface with a destination address of 172.16.10.8:80 will have the destination translated to 172.16.10.8:8080.

The final step is to verify that NAT is operating as intended.

Example: Using NAT During a Network Transition

Deploying NAT is useful when you need to readdress devices on the network or when you're replacing one device with another. For instance, if all devices in the network use a particular server and this server needs to be replaced with a new one that has a new IP address, reconfiguring all the network devices to use the new server address will take some time. In the meantime, you can use NAT to configure the devices using the old address to translate their packets to communicate with the new server.



Once we have defined the NAT interfaces as shown above, we decide that we want NAT to allow packets from the outside destined for the old server address (172.16.10.8) to be translated and sent to the new server address. Note that the new server is on another LAN, and devices on this LAN or any devices reachable through this LAN (devices on the inside part of the network), should be configured to use the new server's IP address if possible.

We can use static NAT to accomplish what we need. An sample configuration is shown below.

Configuring NAT for Use During a Network Transition

NAT Router

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat outside
!-- Defines Ethernet 0 with an IP address and as a NAT outside interface.

interface ethernet 1
 ip address 172.16.50.1 255.255.255.0
 ip nat inside
!-- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
 ip address 200.200.200.5 255.255.255.252
!-- Defines serial 0 with an IP address. This interface is not
!-- participating in NAT.

ip nat inside source static 172.16.50.8 172.16.10.8
!-- States that any packet received on the inside interface with a
!-- source address of 172.16.50.8 will be translated to 172.16.10.8.
```

Note that the inside source NAT command in this example also implies that packets received on the outside interface with a destination address of 172.16.10.8 will have the destination address translated to 172.16.50.8

The final step is to verify that NAT is operating as intended.

Example: Using NAT in Overlapping Networks

Overlapping networks result when you assign IP addresses to internal devices that are already being used by other devices within the internet.

Overlapping networks also result when two companies, both of whom use RFC 1918 IP addresses in their networks, merge. These two networks need to communicate, preferably without having to readdress all their devices. Refer to Using NAT in Overlapping Networks for more information about configuring NAT for this purpose.

Verifying NAT Operation

Once you've configured NAT, verify that it's operating as expected. You can do this in a number of ways: using a network analyzer, **show** commands, or **debug** commands. For a detailed example of NAT verification, please refer to Verifying NAT Operation and Basic NAT Troubleshooting.

Conclusion

The examples in this document demonstrate these quick start steps can help you configure and deploy NAT. These quick start steps include:

1. Define NAT inside and outside interfaces.
2. Define what you are trying to accomplish with NAT.
3. Configure NAT in order to accomplish what you defined in Step 2.
4. Verify NAT operation.

In each of the examples above, we used various forms of the **ip nat inside** command. You can also use the **ip nat outside** to accomplish the same objectives, keeping in mind the NAT order of operations. For configuration examples using the **ip nat outside** commands, refer to Sample Configuration Using ip nat outside source list Command and Sample Configuration Using ip nat outside source static Command.

The examples above also demonstrated the following:

Command	Action
ip nat inside source	• translates the source of IP packets that are traveling inside to outside • translates the destination of the IP packets that are traveling outside to inside
ip nat outside source	• translates the source of the IP packets that are traveling outside to inside • translates the destination of the IP packets that are traveling inside to outside

Related Information

- **NAT Support Page**
- **IP Routing Top Issues**
- **Frequently Asked Questions about Cisco IOS NAT**