Table of Contents

PIX Security Appliance 7.0 and Adaptive Security Appliance NAT and PAT Statements

Document ID: 64758

Interactive: This document offers customized analysis of your Cisco device.

Introduction

This document provides examples of basic Network Address Translation (NAT) and Port Address Translation (PAT) configurations on the Cisco PIX 500 Series Security Appliances. Simplified network diagrams are provided. Consult the PIX documentation for your PIX software version for detailed information.

Prerequisites

Requirements

Readers of this document should be knowledgeable about the Cisco PIX 500 Series Security Appliances.

Components Used

The information in this document is based on this software version:

- Cisco PIX 500 Series Security Appliance Software version 7.0 and later.

Note: Policy NAT was introduced in version 6.2.

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 the Cisco Technical Tips Conventions for more information on document conventions.

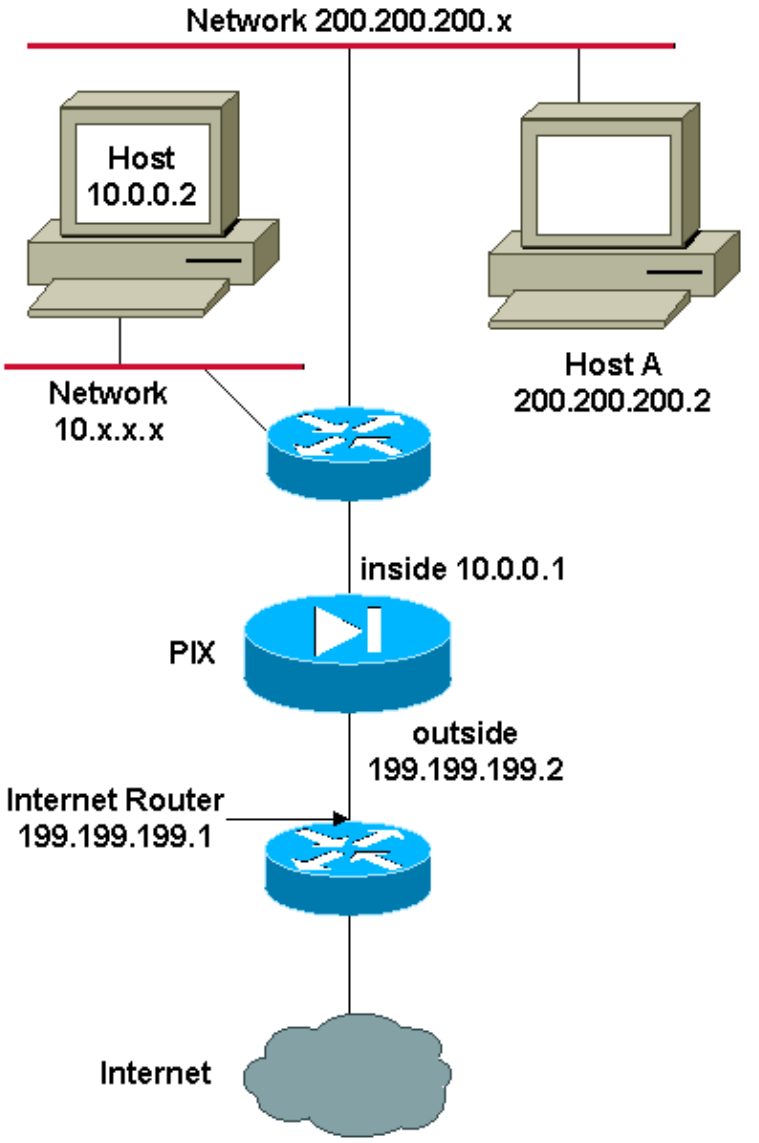
The nat−control Command

The **nat−control** command on the PIX specifies that all traffic through the firewall must have a specific translation entry (**nat** statement with a matching **global**, or a **static** statement) for that traffic to pass through the firewall. The **nat−control** command ensures that the translation behavior is the same as PIX Firewall versions earlier than 7.0. The default configuration of PIX 7.0 is the specification of the **no nat−control** command. With PIX Firewall version 7.0, you can change this behavior when you issue the **nat−control** command.

With **nat−control** disabled, the PIX forwards packets from a higher−security interface to a lower one without a specific translation entry in the configuration. In order to pass traffic from a lower security interface to a higher one, use access−lists to permit the traffic. The PIX then forwards the traffic. This document focuses on the PIX firewall behavior with **nat−control** enabled.

Multiple NAT Statements with NAT 0

Network Diagram



In this example, the ISP provides the network manager with a range of addresses from 199.199.199.1 to 199.199.199.63. The network manager decides to assign 199.199.199.1 to the the inside interface on the Internet router, and 199.199.199.2 to the outside interface of the PIX.

The network administrator already had a Class C address assigned to the network, 200.200.200.0/24, and has some workstations that use these addresses in order to access the Internet. These workstations do not require any address translation as they already have valid addresses. However, new workstations are assigned addresses in the 10.0.0.0/8 network and they need to be translated (because 10.x.x.x is one of the unroutable address spaces per RFC 1918 .

In order to accommodate this network design, the network administrator must use two NAT statements and one global pool in the PIX configuration, as this output shows:

```
global (outside) 1 199.199.199.3-199.199.199.62 netmask 255.255.255.192

nat (inside) 0 200.200.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

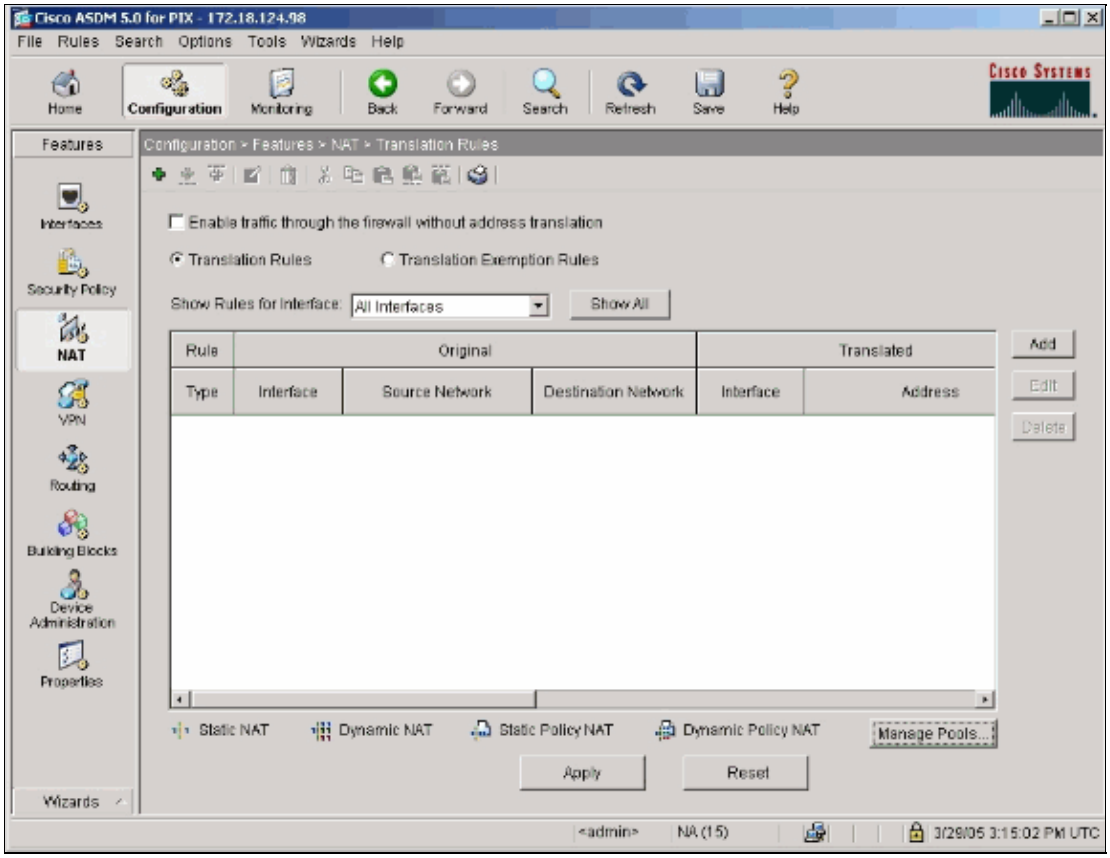
This configuration does not translate the source address of any outbound traffic from the 200.200.200.0/24 network. It translates a source address in the 10.0.0.0/8 network into an address from the range 199.199.199.3 to 199.199.199.62.

These steps provide an explanation of how to apply this same configuration with the use of Adaptive Security Device Manager (ASDM).

Note: Perform all configuration changes through either the CLI or ASDM. The use of both CLI and ASDM for configuration changes causes very erratic behavior in terms of what gets applied by ASDM. This is not a bug, but occurs due to how ASDM works.

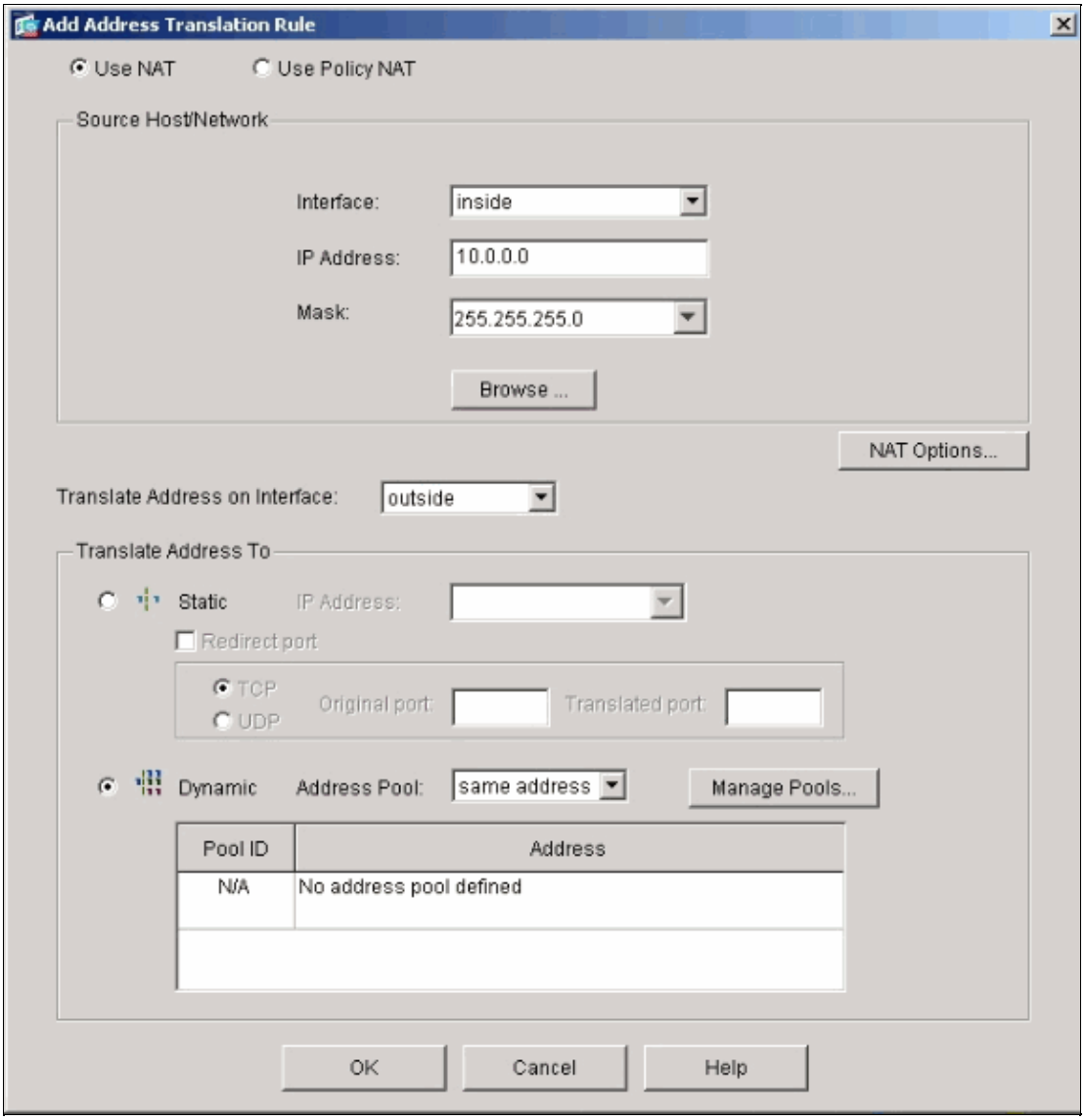
Note: When you open ASDM, it imports the current configuration from the PIX and works from that configuration when you make and apply changes. If a change gets made on the PIX while the ASDM session is open, then ASDM no longer works with what it "thinks" is the current configuration of the PIX. Be sure to close out any ASDM sessions if you make configuration changes via CLI. Then re−open ASDM when you want to work via GUI again.

1. Launch ASDM, browse to the Configuration tab, and click **NAT**.
2. Click **Add** in order to create a new rule.

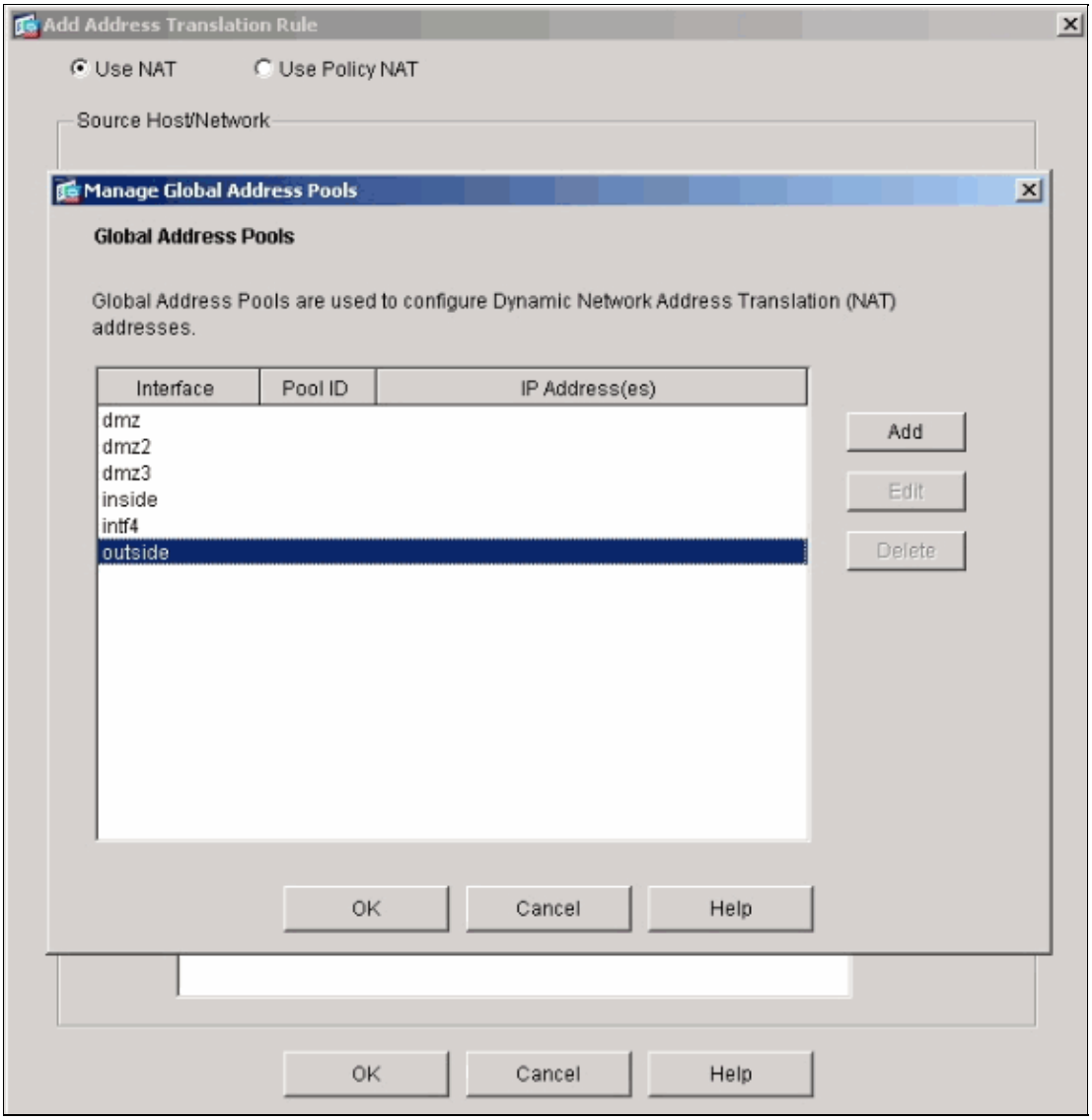


3. A new window appears that allows for the user to change NAT options for this NAT entry. For this example, perform NAT on packets that arrive on the inside interface that are sourced from the specific 10.0.0.0/24 network.

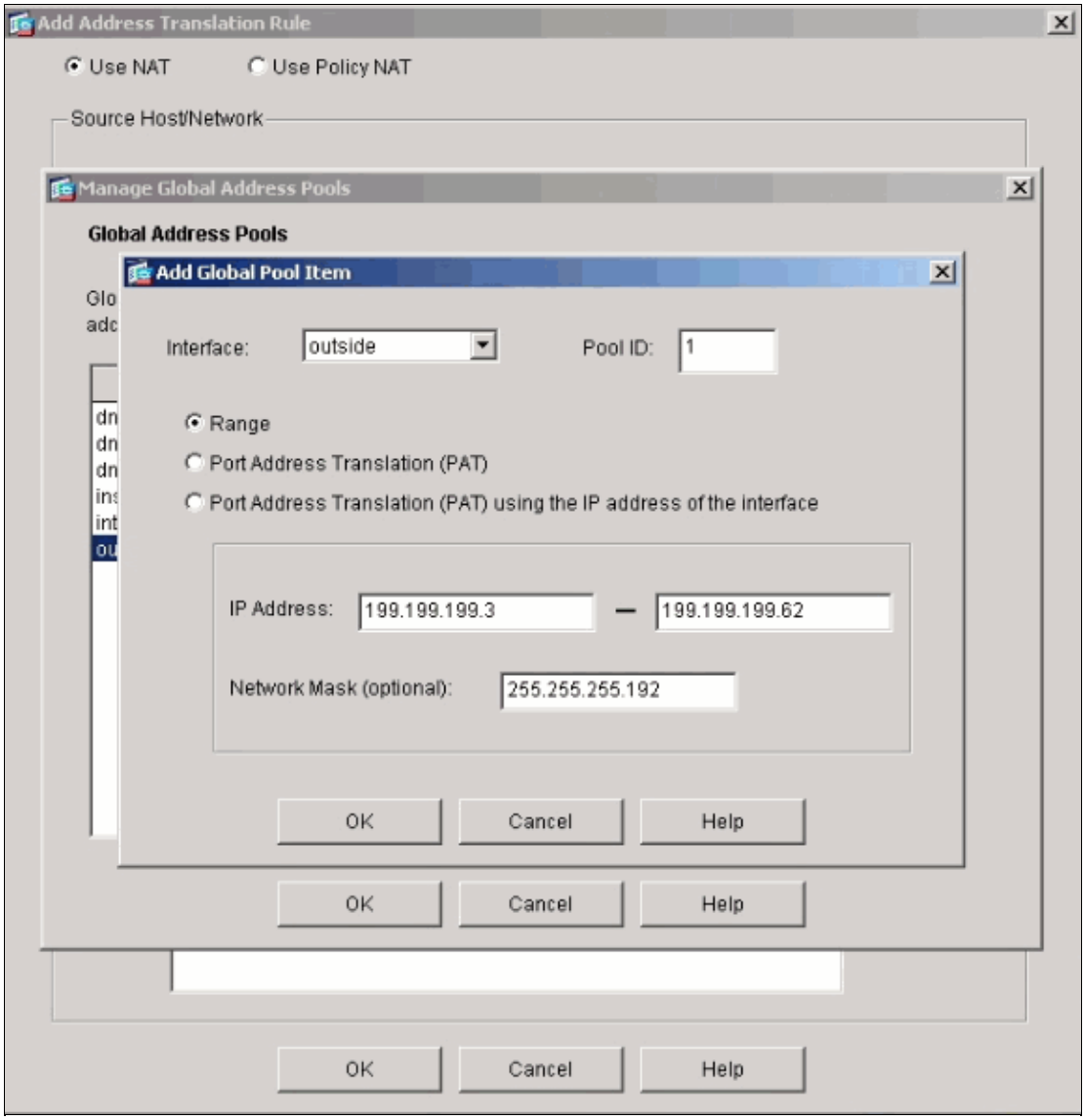
   The PIX translates these packets to a Dynamic IP pool on the outside interface. After you enter the information that describes what traffic to NAT, define a pool of IP addresses for the translated traffic. Click **Manage Pools** in order to add a new IP pool.



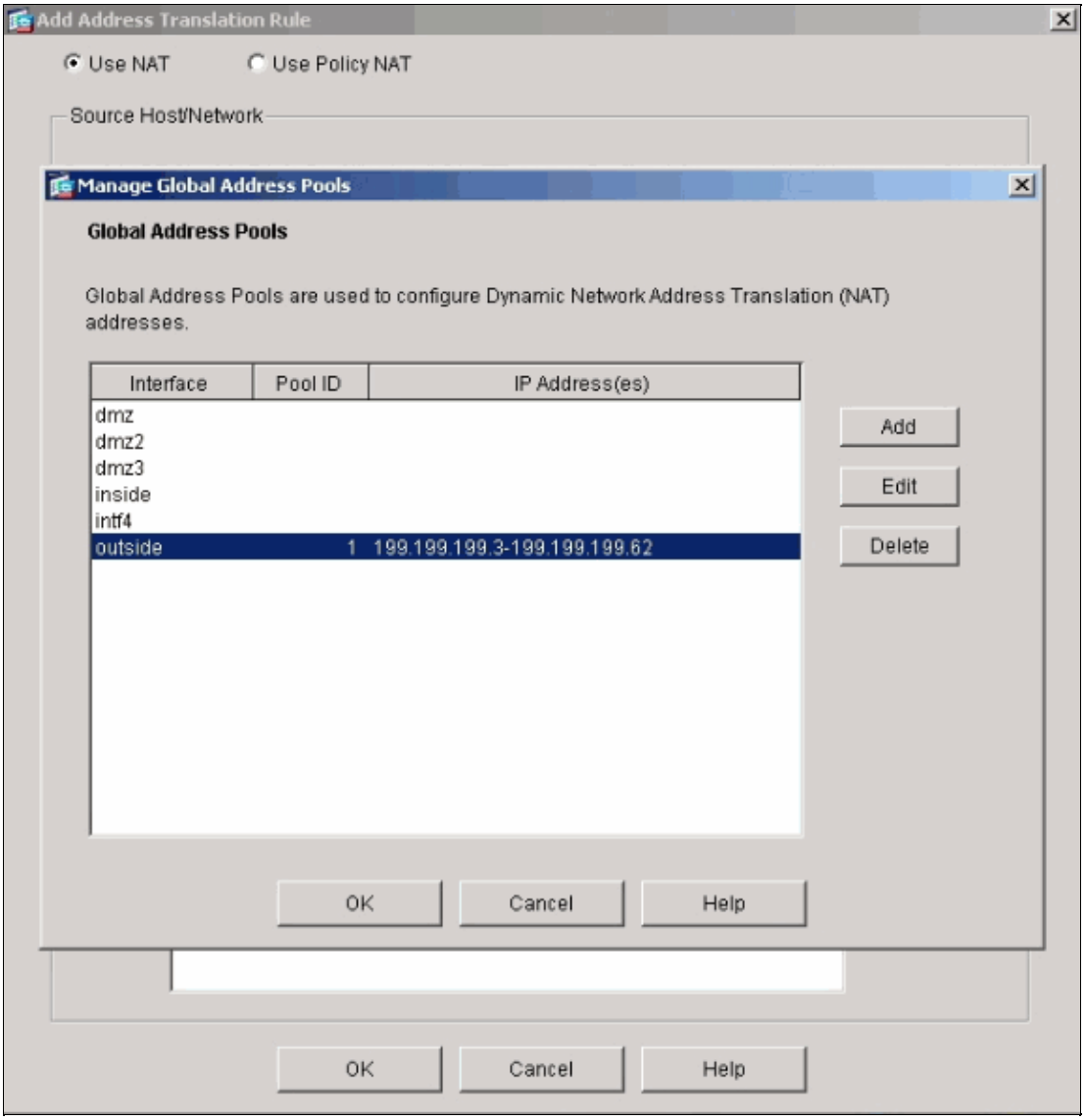
4. Choose **outside** and click **Add**.



5. Specify the IP range for the pool, and give the pool a unique integer id number.

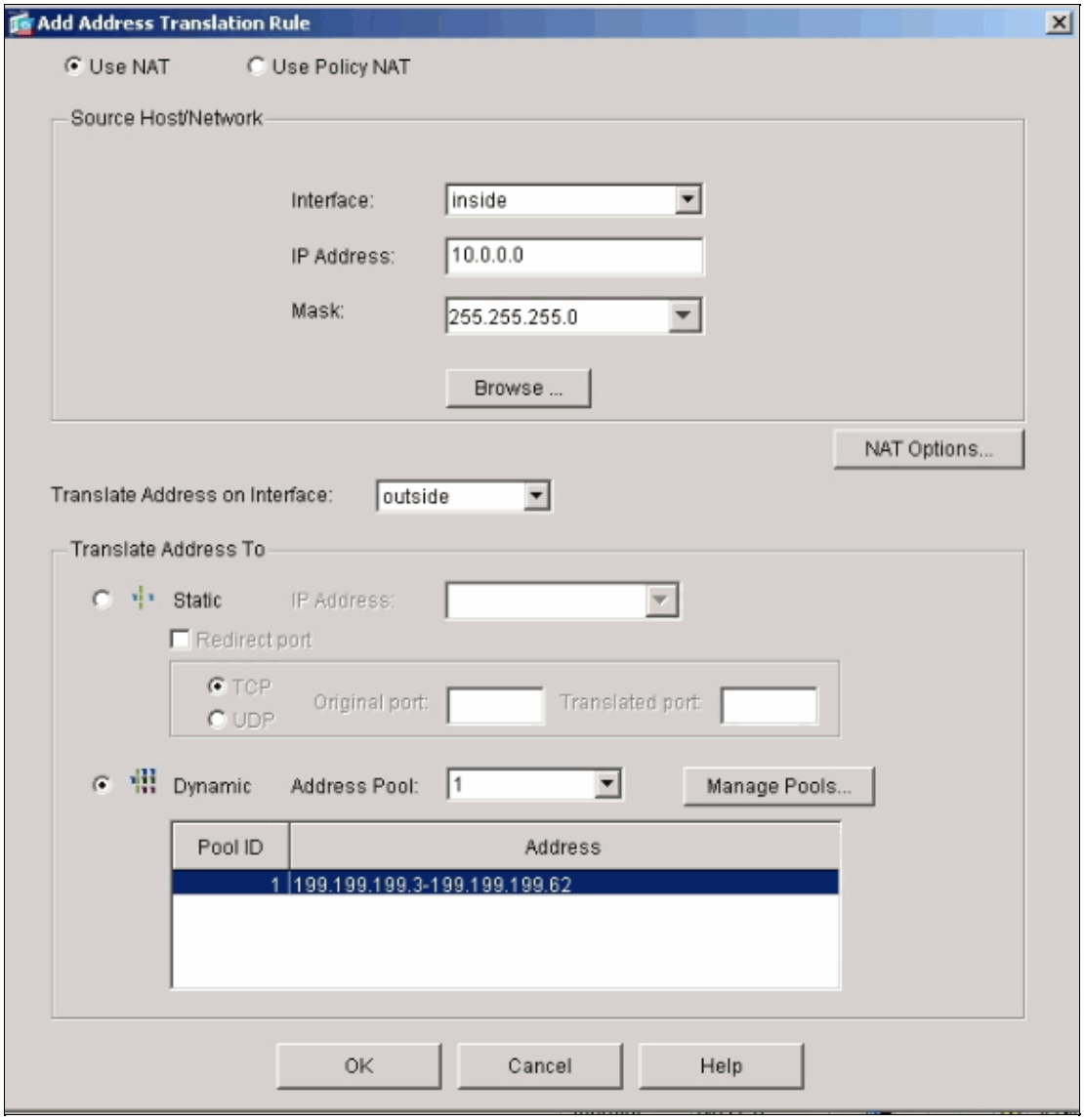


6. After you enter the appropriate values and click **OK**, you see the new pool defined for the outside interface.

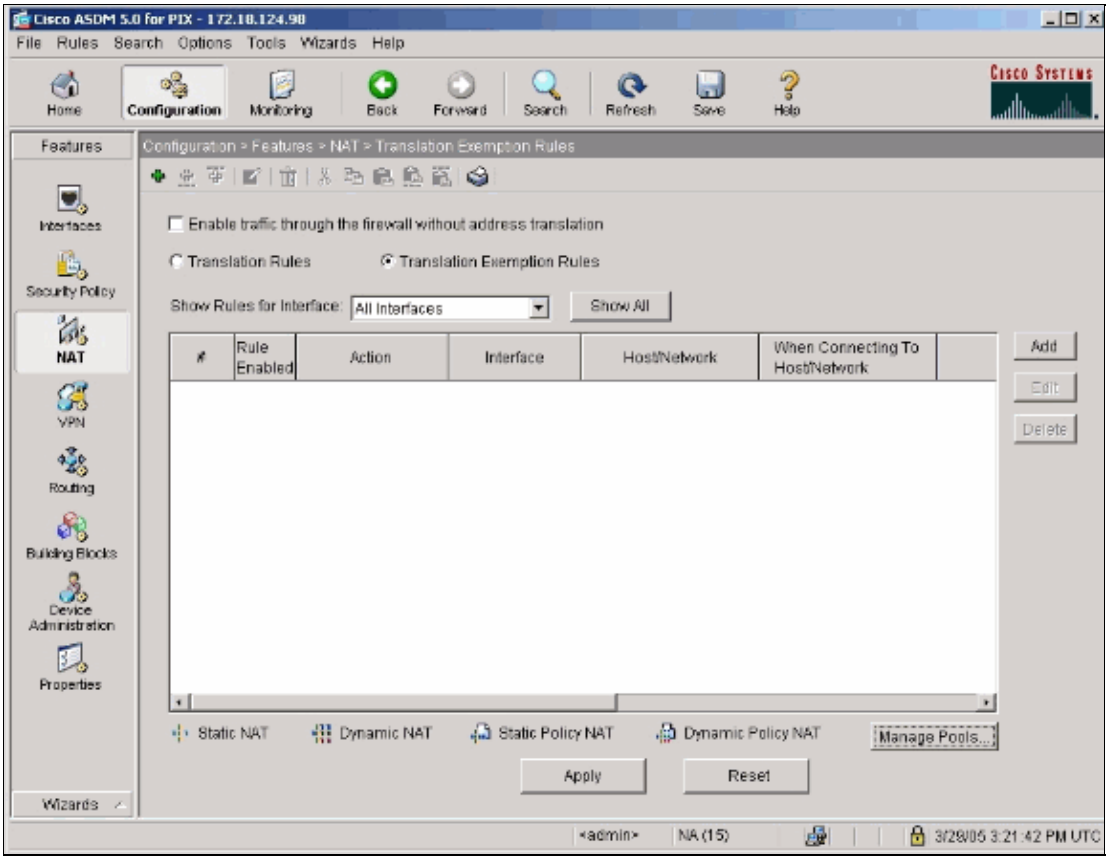


7. After you define the pool, click **OK** in order to return to the NAT Rule configuration window.

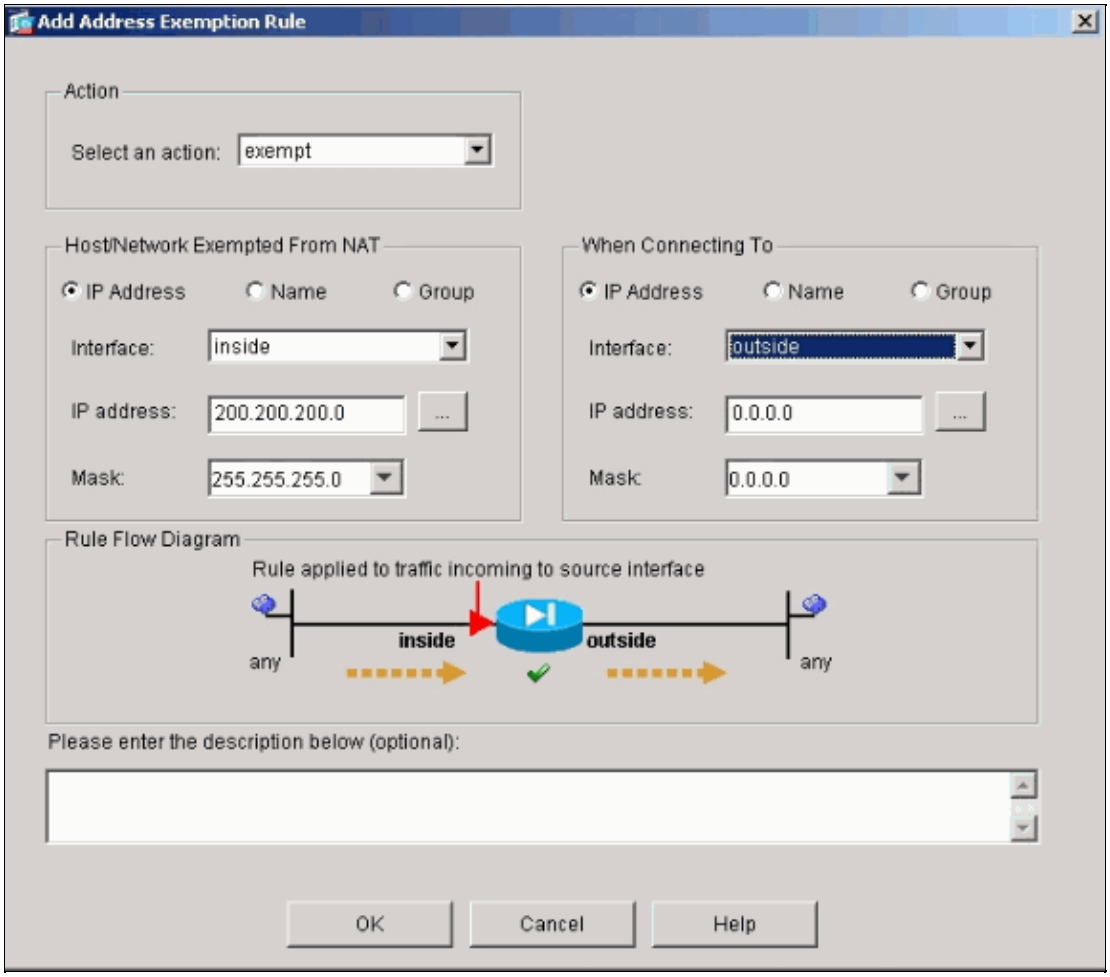
   Make sure to choose the correct pool that you just created under the Address Pool drop−down menu.



8. You have now created a NAT translation through the firewall. However, you still need to create the NAT entry that specifies what traffic not to NAT. Click **Translation Exemption Rules** located at the top of the window. Then click **Add** in order to create a new rule.



9. Choose the **inside** interface as the source and specify the **200.200.200.0/24** subnet. Leave the "When connecting" values as the defaults.



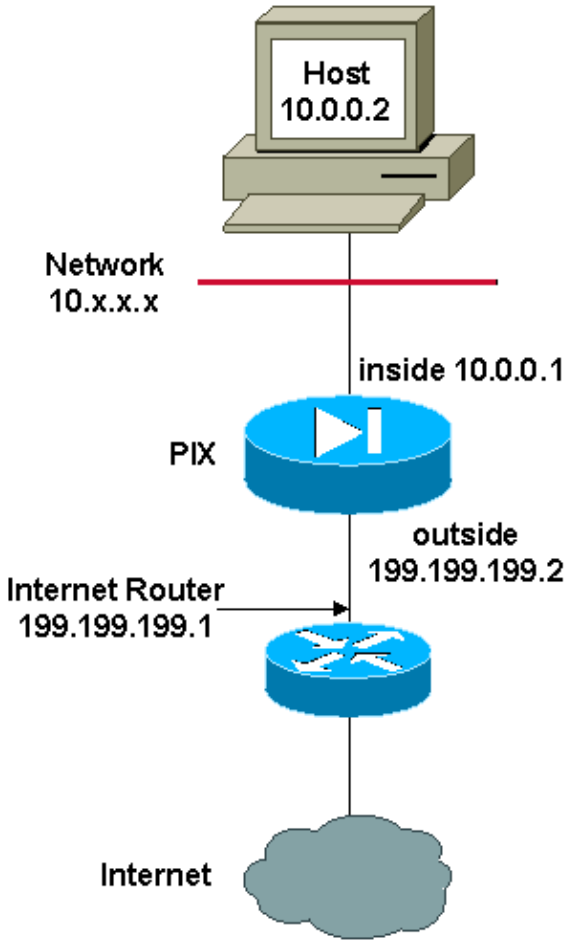
10. The NAT rules are now defined. Click **Apply** in order to apply the changes to the current running configuration of the firewall.

    This output shows the actual additions that are applied to the PIX configuration. They are slightly different from the commands entered from the manual method, but they are equal.

```
access-list inside_nat0_outbound extended permit
ip 200.200.200.0 255.255.255.0 any

global (outside) 1 199.199.199.3-199.199.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

Multiple Global Pools

Network Diagram



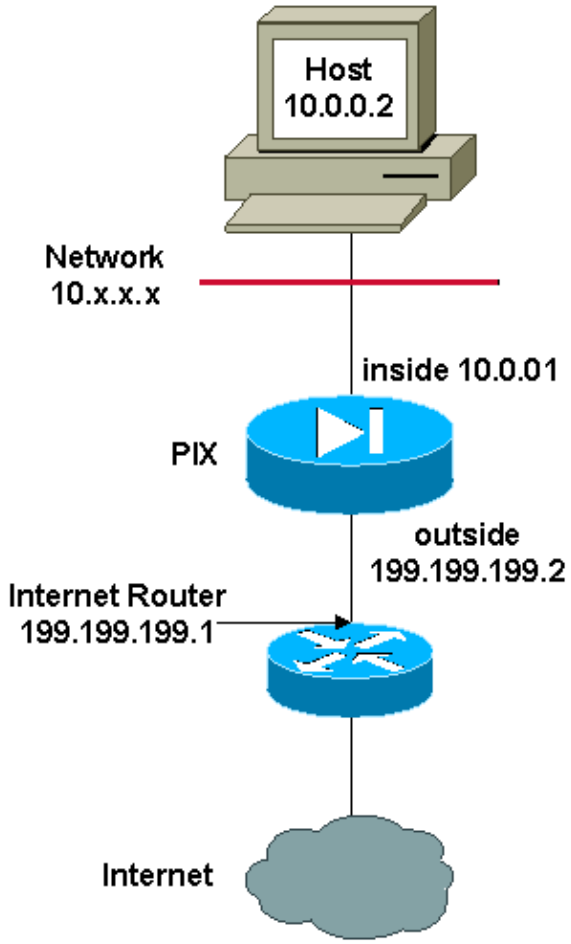
In this example, the network manager has two ranges of IP addresses that register on the Internet. The network manager must convert all of the internal addresses, which are in the 10.0.0.0/8 range, into registered addresses. The ranges of IP addresses that the network manager must use are 199.199.199.1 through 199.199.199.62 and 150.150.150.1 through 150.150.150.254. The network manager can do this with:

```
global (outside) 1 199.199.199.3−199.199.199.62 netmask 255.255.255.192

global (outside) 1 150.150.150.1−150.150.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Note: A wildcard addressing scheme is used in the NAT statement. This statement tells the PIX to translate any internal source address when it goes out to the Internet. The address in this command can be more specific if desired.

Mix NAT and PAT Global Statements

Network Diagram



In this example, the ISP provides the network manager with a range of addresses from 199.199.199.1 through 199.199.199.63 for the use of the company. The network manager decides to use 199.199.199.1 for the inside interface on the Internet router and 199.199.199.2 for the outside interface on the PIX. You are left with 199.199.199.3 through 199.199.199.62 to use for the NAT pool. However, the network manager knows that, at any one time, there can be more than sixty people who attempt to go out of the PIX. Therefore, the network manager decides to take 199.199.199.62 and make it a PAT address so that multiple users can share one address at the same time.

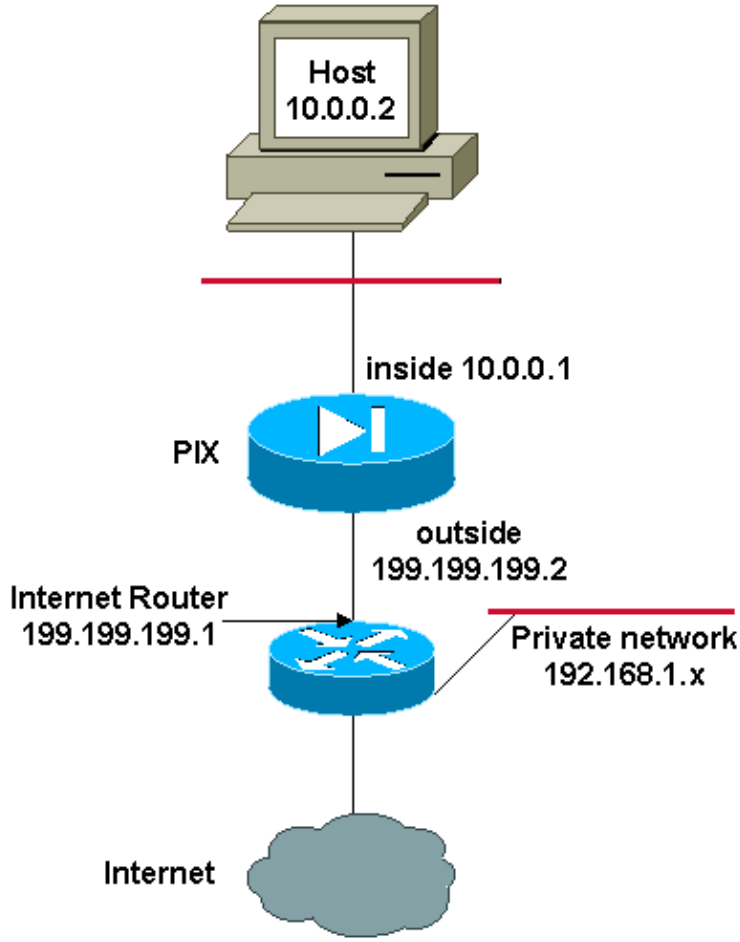
```
global (outside) 1 199.199.199.3−199.199.199.61 netmask 255.255.255.192

global (outside) 1 199.199.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

These commands instruct the PIX to translate the source address to 199.199.199.3 through 199.199.199.61 for the first fifty−nine internal users to pass across the PIX. After these addresses are exhausted, the PIX then translates all subsequent source addresses to 199.199.199.62 until one of the addresses in the NAT pool becomes free.

Note: A wildcard addressing scheme is used in the NAT statement. This statement tells the PIX to translate any internal source address when it goes out to the Internet. The address in this command can be more specific if you desire.

Multiple NAT Statements with NAT 0 Access−List

Network Diagram



In this example, the ISP provides the network manager with a range of addresses from 199.199.199.1 through 199.199.199.63. The network manager decides to assign 199.199.199.1 to the inside interface on the Internet router and 199.199.199.2 to the outside interface of the PIX.

However, in this scenario another private LAN segment is placed off of the Internet router. The network manager would rather not waste addresses from the global pool when hosts in these two networks talk to each other. The network manager still needs to translate the source address for all of the internal users (10.0.0.0/8) when they go out to the Internet.

```
access−list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 199.199.199.3−199.199.199.62 netmask 255.255.255.192

nat (inside) 0 access−list 101

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

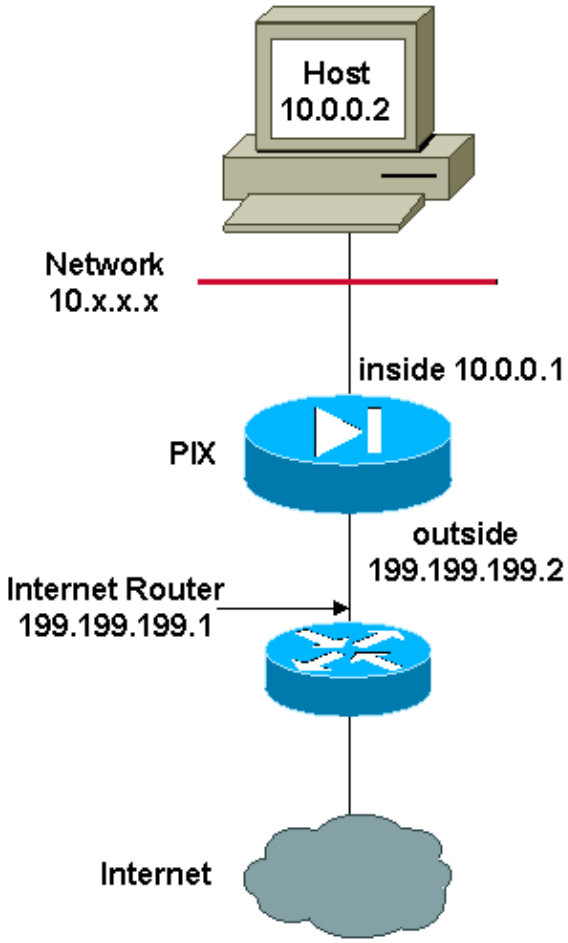
This configuration does not translate those addresses with a source address of 10.0.0.0/8 and a destination address of 192.168.1.0/24. It translates the source address from any traffic initiated from within the 10.0.0.0/8 network and destined for anywhere other than 192.168.1.0/24 into an address from the range 199.199.199.3

through 199.199.199.62.

If you have the output of a **write terminal** command from your Cisco device, you can use the Output Interpreter Tool (registered customers only) .

Use Policy NAT

Network Diagram



When you use an access list with the **nat** command for any NAT ID other than 0, then you enable policy NAT.

Policy NAT allows you to identify local traffic for address translation when you specify the source and destination addresses (or ports) in an access list. Regular NAT uses source addresses/ports only, whereas policy NAT uses both source and destination addresses/ports.

Note: All types of NAT support policy NAT except for NAT exemption (**nat 0 access−list**). NAT exemption uses an access control list in order to identify the local addresses, but differs from policy NAT in that the ports are not considered.

With policy NAT, you can create multiple NAT or static statements that identify the same local address as long as the source/port and destination/port combination is unique for each statement. You can then match different global addresses to each source/port and destination/port pair.

In this example, the network manager provides access for destination IP address 209.165.201.11 for port 80 (web) and port 23 (Telnet), but must use two different IP addresses as a source address. IP address 199.199.199.3 is used as the source address for web. IP address 199.199.199.4 is used for Telnet, and must convert all of the internal addresses, which are in the 10.0.0.0/8 range. The network manager can do this with:

```
access−list WEB permit tcp 10.0.0.0 255.0.0.0 209.165.201.11
255.255.255.255 eq 80

access−list TELNET permit tcp 10.0.0.0 255.0.0.0 209.165.201.11
255.255.255.255 eq 23

nat (inside) 1 access−list WEB

nat (inside) 2 access−list TELNET

global (outside) 1 199.199.199.3 255.255.255.192

global (outside) 2 199.199.199.4 255.255.255.192
```

You can use Output Interpreter Tool (registered customers only) in order to display potential issues and fixes.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **PIX Support Page**
- **Documentation for PIX Firewall**
- **PIX Command References**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**

Updated: Feb 16, 2006 Document ID: 64758