

Using NAT and PAT Statements on the Cisco Secure PIX Firewall

Document ID: 15243

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

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Multiple NAT Statements with NAT 0

- Network Diagram

Multiple Global Pools

- Network Diagram

Mix NAT and PAT Global Statements

- Network Diagram

Multiple NAT Statements with NAT 0 Access-List

- Network Diagram

Use Policy NAT

- Network Diagram

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides examples of basic Network Address Translation (NAT) and Port Address Translation (PAT) configurations on the Cisco Secure PIX Firewall. This document also provides simplified network diagrams. Consult the PIX documentation for your PIX software version for detailed information.

Refer to PIX/ASA 7.x NAT and PAT Statements in order to learn more about the basic NAT and PAT configurations on the Cisco PIX 500 Series Security Appliances.

Refer to Using nat, global, static, conduit, and access-list Commands and Port Redirection(Forwarding) on PIX in order to learn more about the **nat**, **global**, **static**, **conduit**, and **access-list** Commands and Port Redirection(Forwarding) on PIX 5.x and later.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the Cisco Secure PIX Firewall.

Components Used

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

- Cisco Secure PIX Firewall Software version 5.3.1 and later.

Note: Policy NAT was introduced from 6.2.

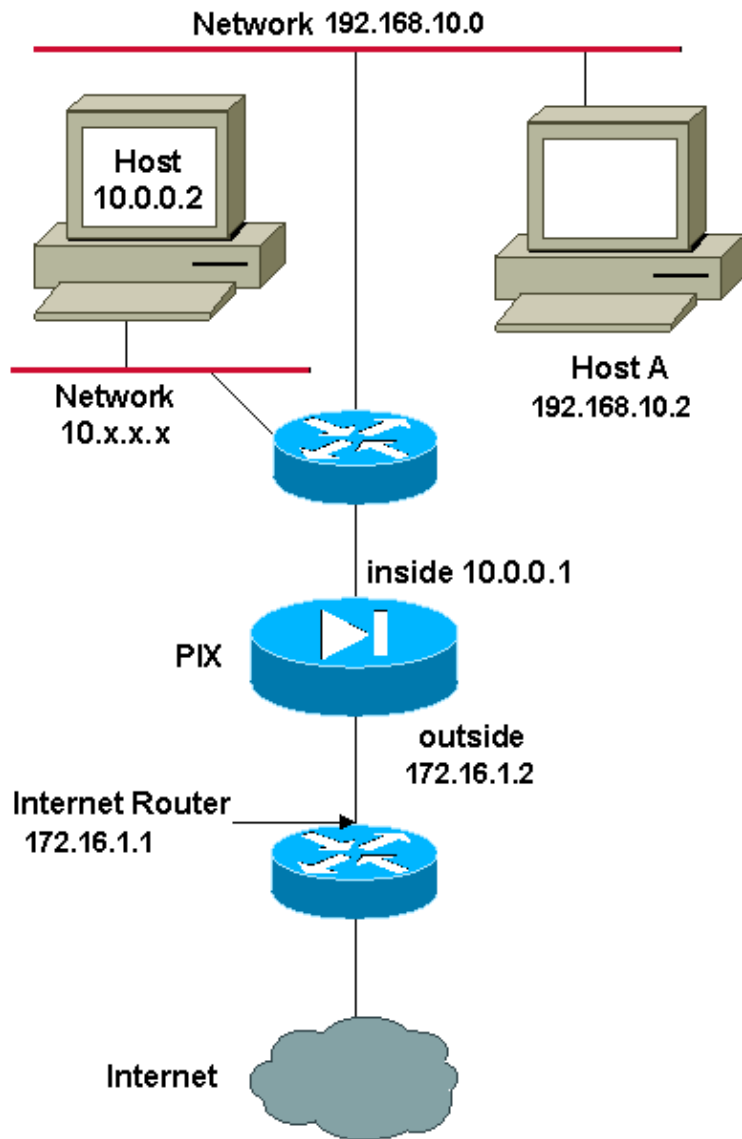
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Multiple NAT Statements with NAT 0

Network Diagram



In this example, the ISP provides the network manager with a range of addresses (for example, 172.16.1.1 to 172.16.1.63). (ISP issues the Public IP addresses. But for the sake of discussion, this document uses Private IP addresses.) The network manager decides to assign 172.16.1.1 to the inside interface on the Internet router, and 172.16.1.2 to the outside interface of the PIX.

The network administrator already has a Class C address assigned to the network, 192.168.10.0/24, 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:

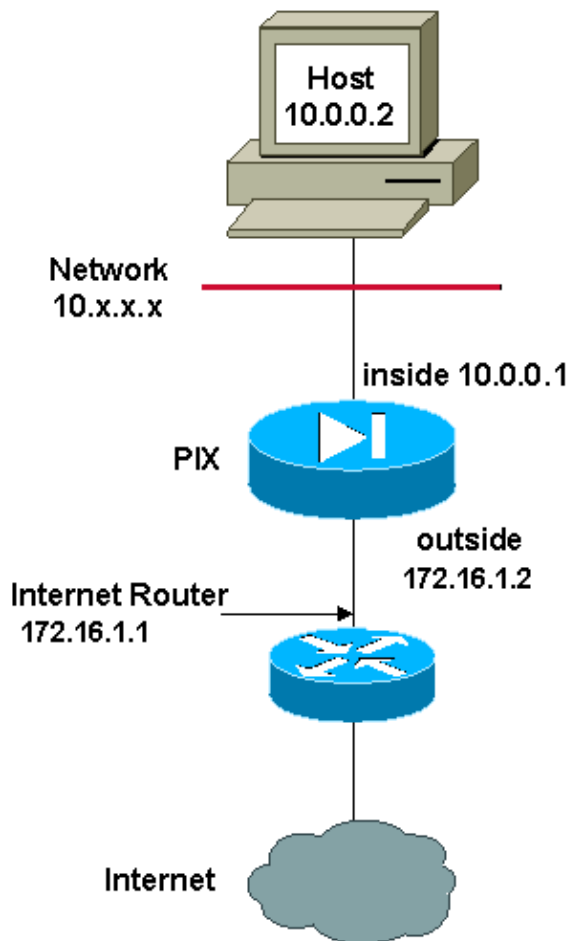
```
global (outside) 1 172.16.1.3-172.16.1.62 netmask 255.255.255.192
nat (inside) 0 192.168.10.0 255.255.255.0 0 0
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

This configuration does not translate the source address of any outbound traffic from the 192.168.10.0/24 network. It translates a source address in the 10.0.0.0/8 network into an address from the range 172.16.1.3 through 172.16.1.62.

Note: When you have an interface with a NAT policy and if there is no global pool to another interface, you need to use `nat 0` in order to set up NAT exception.

Multiple Global Pools

Network Diagram



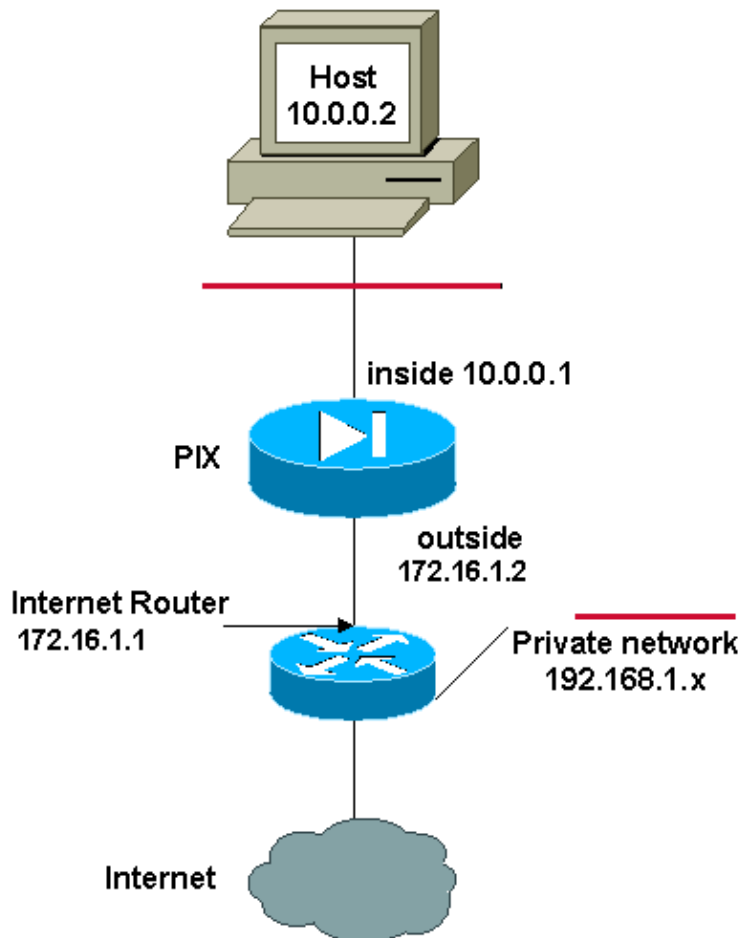
In this example, the network manager has two ranges of IP addresses that are registered on the Internet. The network manager must convert all of the internal addresses, which are in the 10.0.0.0/8 range, into registered addresses. The ranges of IP addresses that the network manager must use are 172.16.1.1 through 172.16.1.62 and 172.20.1.1 through 172.20.1.254 . The network manager can do this with:

```
global (outside) 1 172.16.1.3-172.16.1.62 netmask 255.255.255.192
global (outside) 1 172.20.1.1-172.20.1.254 netmask 255.255.255.0
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Note that 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 172.16.1.1 through 172.16.1.63 for the company to use. The network manager has decided to use 172.16.1.1 for the inside interface on the Internet router and 172.16.1.2 for the outside interface on the PIX. You are then left with 172.16.1.3 through 172.16.1.62 to use for the NAT pool. However, the network manager knows that, at any one time, there can be more than 60 people that try to go out of the PIX. The network manager has decided to take 172.16.1.62 and make it a PAT address so that multiple users can share one address at the same time.

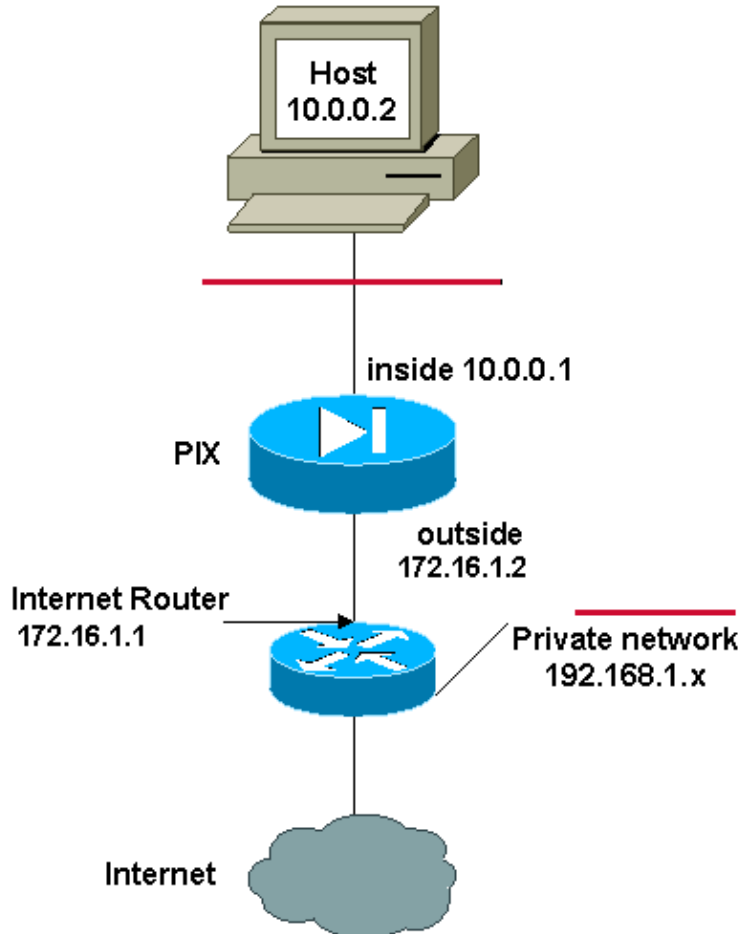
```
global (outside) 1 172.16.1.3-172.16.1.61 netmask 255.255.255.192
global (outside) 1 172.16.1.62 netmask 255.255.255.192
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

These commands instruct the PIX to translate the source address to 172.16.1.3 through 172.16.1.61 for the first 59 internal users to pass across the PIX. After these addresses are exhausted, the PIX then translates all subsequent source addresses to 172.16.1.62 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 desired.

Multiple NAT Statements with NAT 0 Access-List

Network Diagram



In this example, the ISP again provides the network manager with a range of addresses from 172.16.1.1 through 172.16.1.63. The network manager decides to assign 172.16.1.1 to the inside interface on the Internet router and 172.16.1.2 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 prefers not to 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 it goes out to the Internet.

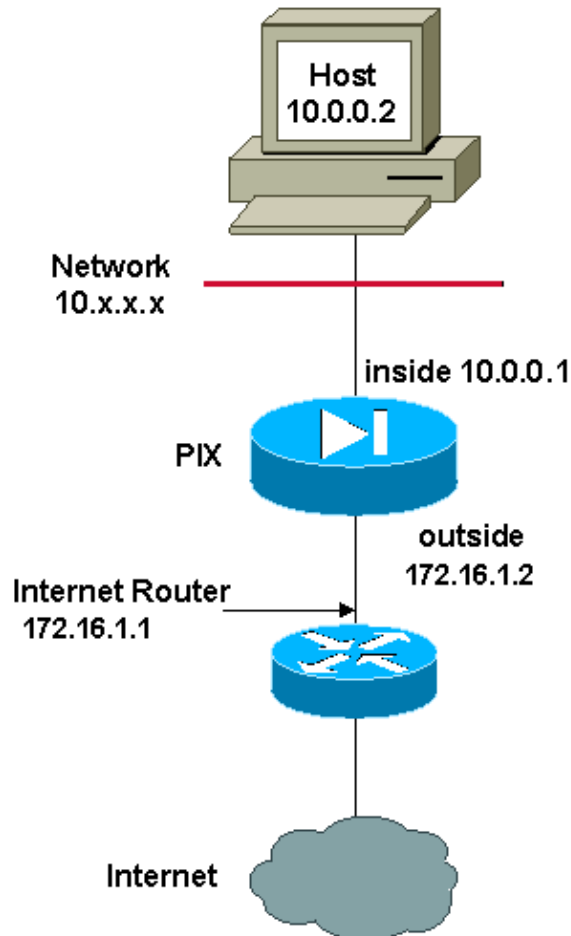
```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0
global (outside) 1 172.16.1.3-172.16.1.62 netmask 255.255.255.192
nat (inside) 0 access-list 101
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

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 172.16.1.3 through 172.16.1.62.

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, you enable policy NAT.

Policy NAT allows you to identify local traffic for address translation by the specification of the source and destination addresses (or ports) in an access list. Regular NAT uses source addresses/ports only. 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 has to provide access for destination IP address 172.30.1.11 for port 80 (web) and port 23 (Telnet), but must use two different IP addresses as a source address. 172.16.1.3 is used as a source address for web and 172.16.1.4 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
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 172.16.1.3 255.255.255.192
global (outside) 2 172.16.1.4 255.255.255.192
```

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 Reference](#)
- [Requests for Comments \(RFCs\)](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 11, 2007

Document ID: 15243
