

# PIX/ASA 7.x and later: Connecting Multiple Internal Networks with Internet Configuration Example

Document ID: 63880

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

#### Configure

- Background Information
- Network Diagram
- Configurations
- PIX Configuration using ASDM
- PIX Configuration using CLI

#### Verify

#### Troubleshoot

- Troubleshooting Commands
- Troubleshooting Procedure
- Unable to Access Websites by Name

#### Related Information

## Introduction

This document provides a sample configuration for PIX/ASA Security Appliance version 7.x and later with multiple internal networks that connect to the Internet (or an external network) using the command line interface (CLI) or Adaptive Security Device Manager (ASDM) 5.x and later.

Refer to Establish and Troubleshoot Connectivity through the Cisco Security Appliance for information on how to establish and troubleshoot connectivity through PIX/ASA.

Refer to Using nat, global, static, conduit, and access-list Commands and Port Redirection(Forwarding) on PIX for information about common PIX commands.

**Note:** Some options in other ASDM versions can appear different from the options in ASDM 5.1. Refer to the ASDM documentation for more information.

## Prerequisites

### Requirements

When you add more than one internal network behind a PIX Firewall, keep these points in mind:

- The PIX does not support secondary addressing.
- A router has to be used behind the PIX in order to achieve routing between the existing network and the newly added network.
- The default gateway of all the hosts needs to point to the inside router.

- Add a default route on the inside router that points to the PIX.
- Clear the Address Resolution Protocol (ARP) cache on the inside router.

Refer to Allowing HTTPS Access for ASDM in order to allow the device to be configured by the ASDM.

## Components Used

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

- PIX Security Appliance 515E with software version 7.1
- ASDM 5.1
- Cisco routers with Cisco IOS® Software Release 12.3(7)T

**Note:** This document has been recertified with PIX/ASA software version 8.x and Cisco IOS Software Release 12.4.

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.

## Related Products

This configuration can also be used with Cisco ASA Security Appliance version 7.x and later.

## Conventions

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

## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

## Background Information

In this scenario, there are three internal networks (10.1.1.0/24, 10.2.1.0/24 and 10.3.1.0/24) to be connected to the Internet (or an External network) through PIX. The internal networks are connected to the inside interface of PIX. The Internet connectivity is through a router which is connected to the outside interface of the PIX. The PIX has the IP address 172.16.1.1/24.

The static routes are used to route the packets from the internal networks to the Internet and vice versa. Instead of using the static routes, you can also use a dynamic routing protocol such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).

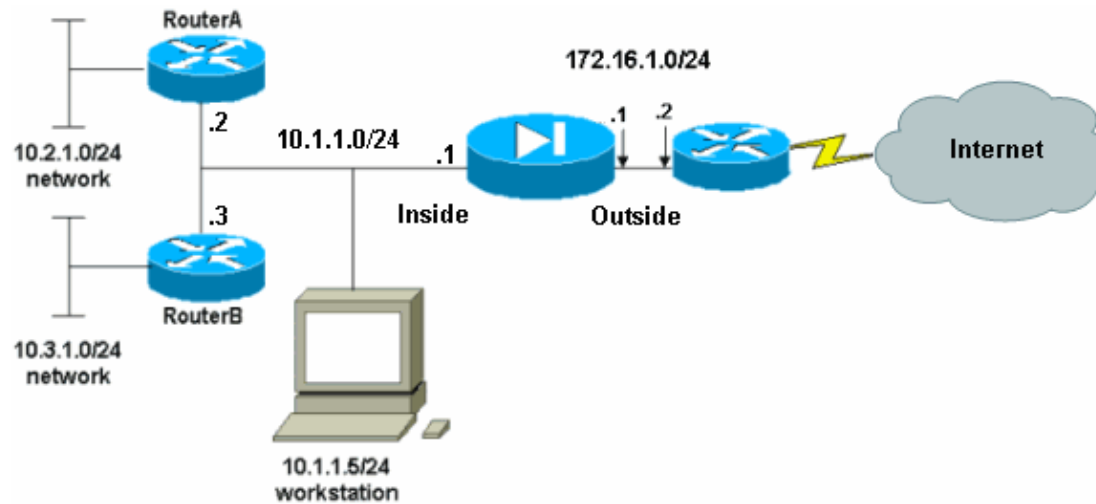
The internal hosts communicate with the Internet by translating the internal networks on PIX using dynamic NAT (pool of IP addresses – 172.16.1.5 to 172.16.1.10 ). If the pool of IP addresses is exhausted, the PIX will PAT (using IP address 172.16.1.4) the internal hosts to reach the Internet.

Refer to PIX/ASA 7.x NAT and PAT Statements for more information on NAT/PAT.

**Note:** If the static NAT uses the outside IP (global\_IP) address to translate, then this might cause a translation. Therefore, use the keyword interface instead of the IP address in the static translation.

## Network Diagram

This document uses this network setup:



The default gateway of the hosts on the 10.1.1.0 network points to RouterA. A default route on RouterB is added that points to RouterA. RouterA has a default route that points to the PIX inside interface.

## Configurations

This document uses these configurations:

- RouterA Configuration
- RouterB Configuration
- PIX Security Appliance 7.1 Configuration
  - ◆ PIX Configuration using ASDM
  - ◆ PIX Security Appliance CLI Configuration

### RouterA Configuration

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!

interface Ethernet2/0
 ip address 10.2.1.1 255.255.255.0
 half-duplex
```

```

!
interface Ethernet2/1
 ip address 10.1.1.2 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterA#

```

### RouterB Configuration

```

RouterB#show running-config
Building configuration...
Current configuration : 1132 bytes
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!

interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 speed auto
!

interface Ethernet1/0
 ip address 10.3.1.1 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterB#

```

If you want to use the ASDM for the configuration of the PIX Security Appliance, but have not bootstrapped the device, complete these steps:

1. Console into the PIX.
2. From a cleared configuration, use the interactive prompts in order to enable ASDM for the management of the PIX from workstation 10.1.1.5.

## PIX Security Appliance 7.1 Configuration

```
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5
```

The following configuration will be used:

```
  Enable password: cisco
  Allow password recovery: yes
  Clock (UTC): 14:45:00 Mar 15 2005
  Firewall Mode: Routed
  Inside IP address: 10.1.1.1
  Inside network mask: 255.255.255.0
  Host name: OZ-PIX
  Domain name: cisco.com
  IP address of host running Device Manager: 10.1.1.5
```

Use this configuration and write to flash? yes

```
INFO: Security level for "inside" set to 100 by default.
Cryptochecksum: a0bff9bb aa3d815f c9fd269a 3f67fef5
```

965 bytes copied in 0.880 secs

```
INFO: converting 'fixup protocol dns maximum-length 512' to MPF commands
INFO: converting 'fixup protocol ftp 21' to MPF commands
INFO: converting 'fixup protocol h323_h225 1720' to MPF commands
INFO: converting 'fixup protocol h323_ras 1718-1719' to MPF commands
INFO: converting 'fixup protocol netbios 137-138' to MPF commands
INFO: converting 'fixup protocol rsh 514' to MPF commands
INFO: converting 'fixup protocol rtsp 554' to MPF commands
INFO: converting 'fixup protocol sip 5060' to MPF commands
INFO: converting 'fixup protocol skinny 2000' to MPF commands
INFO: converting 'fixup protocol smtp 25' to MPF commands
INFO: converting 'fixup protocol sqlnet 1521' to MPF commands
INFO: converting 'fixup protocol sunrpc_udp 111' to MPF commands
INFO: converting 'fixup protocol tftp 69' to MPF commands
INFO: converting 'fixup protocol sip udp 5060' to MPF commands
INFO: converting 'fixup protocol xdmcp 177' to MPF commands
```

```
Type help or '?' for a list of available commands.
OZ-PIX>
```

## PIX Configuration using ASDM

Complete these steps in order to configure via the ASDM GUI:

1. From workstation 10.1.1.5, open a web browser to use ASDM (in this example, <https://10.1.1.1>).
2. Click **yes** on the certificate prompts.
3. Log in with the enable password, as previously configured.
4. If this is the first time ASDM is run on the PC, you are prompted to use ASDM Launcher or ASDM as a Java App. In this example, the ASDM Launcher is selected and installed.
5. Go to the ASDM Home window and click **Configuration**.

The screenshot shows the Cisco ASDM 5.1 for PIX - 10.1.1.1 interface. The top navigation bar includes Home, Configuration, Monitoring, Back, Forward, Search, Refresh, Save, and Help. The main content area is divided into several sections:

- Device Information:**
  - General tab: Host Name: `pixfirewall.default.domain.invalid`, PIX Version: `7.1(1)`, Device Uptime: `14d 6h 4m 4s`, ASDM Version: `5.1(1)`, Device Type: `PIX 515E`, Firewall Mode: `Routed`, Context Mode: `Single`, Total Flash: `16 MB`, Total Memory: `64 MB`.
  - License tab: (Empty)
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1
- VPN Status:** IKE Tunnels: `0`, IPSec Tunnels: `0`
- System Resources Status:**
  - CPU: `1%` (at 17:58:29)
  - Memory: `3840` (at 17:58:29)
  - CPU Usage (percent) graph: Shows usage over time, peaking at approximately 32%.
  - Memory Usage (MB) graph: Shows usage over time, peaking at approximately 3840 MB.
- Traffic Status:**
  - Connections Per Second Usage graph: Shows usage over time, peaking at approximately 1.
  - 'inside' Interface Traffic Usage (Kbps) graph: Shows Input Kbps (0) and Output Kbps (1) over time.
- Latest ASDM Syslog Messages:** -- Syslog Disabled --

The bottom status bar shows: `<admin>`, `NA (15)`, and `7/11/06 5:58:59 PM UTC`.

6. Choose **Interface > Edit** in order to configure the outside interface.

The screenshot shows the Cisco ASDM 5.1 for PIX - 10.1.1.1 interface in the Configuration > Interfaces section. The left sidebar shows navigation options: Interfaces, Security Policy, NAT, VPN, Routing, Global Objects, and Properties. The main content area displays a table of interfaces:

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU	
Ethernet0		No				No		Add
Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No	1500	Edit Delete

Below the table, there is a checkbox labeled "Enable traffic between two or more interfaces which are configured with same security levels" which is currently unchecked. At the bottom, there are "Apply" and "Reset" buttons.

The bottom status bar shows: `<admin>`, `NA (15)`, and `7/11/06 5:59:49 PM UTC`.

7. Enter the interface details and click **OK** when you are done.

**Edit Interface**

Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface  Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP  Obtain Address via DHCP

IP Address:

Subnet Mask:


MTU:

Description:

OK Cancel Help

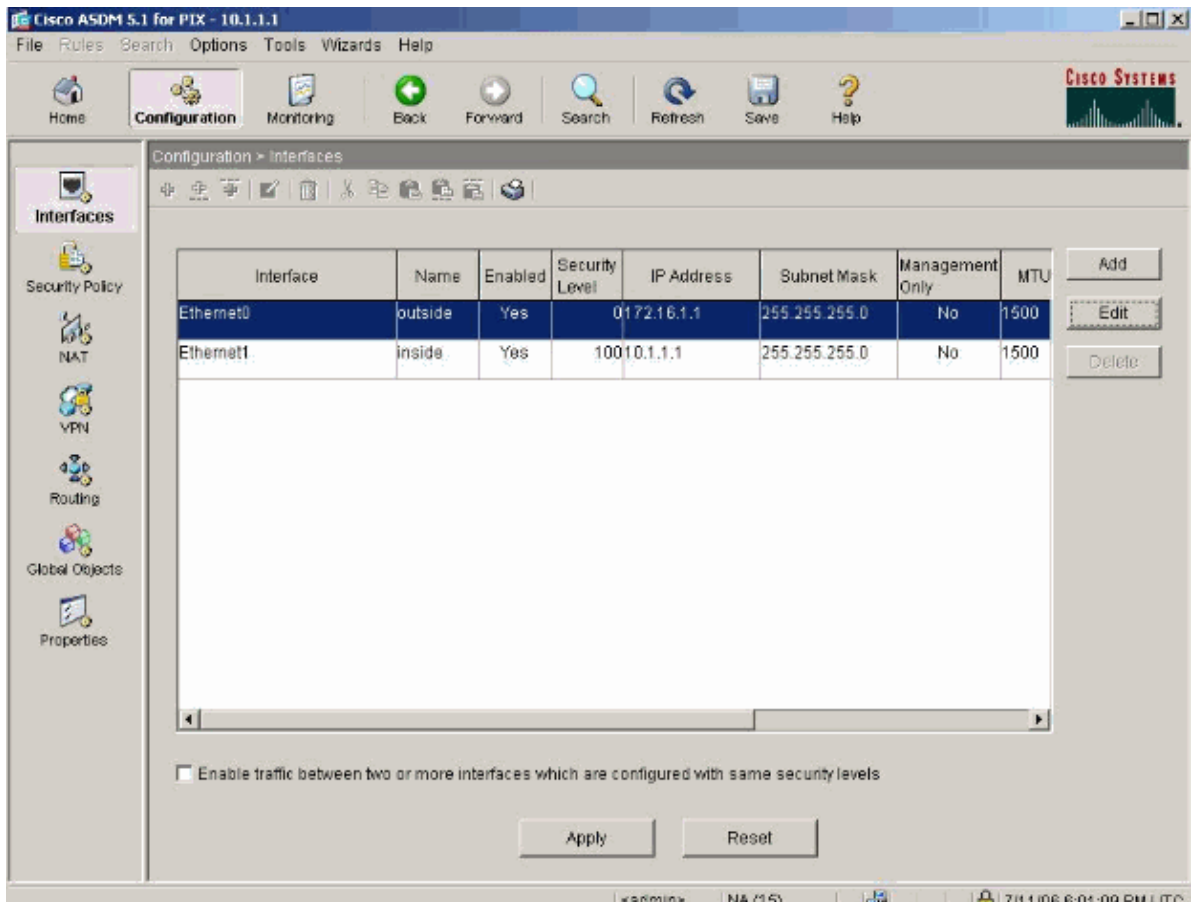
8. Click **OK** on the Security Level Change dialog box.

**Security Level Change**

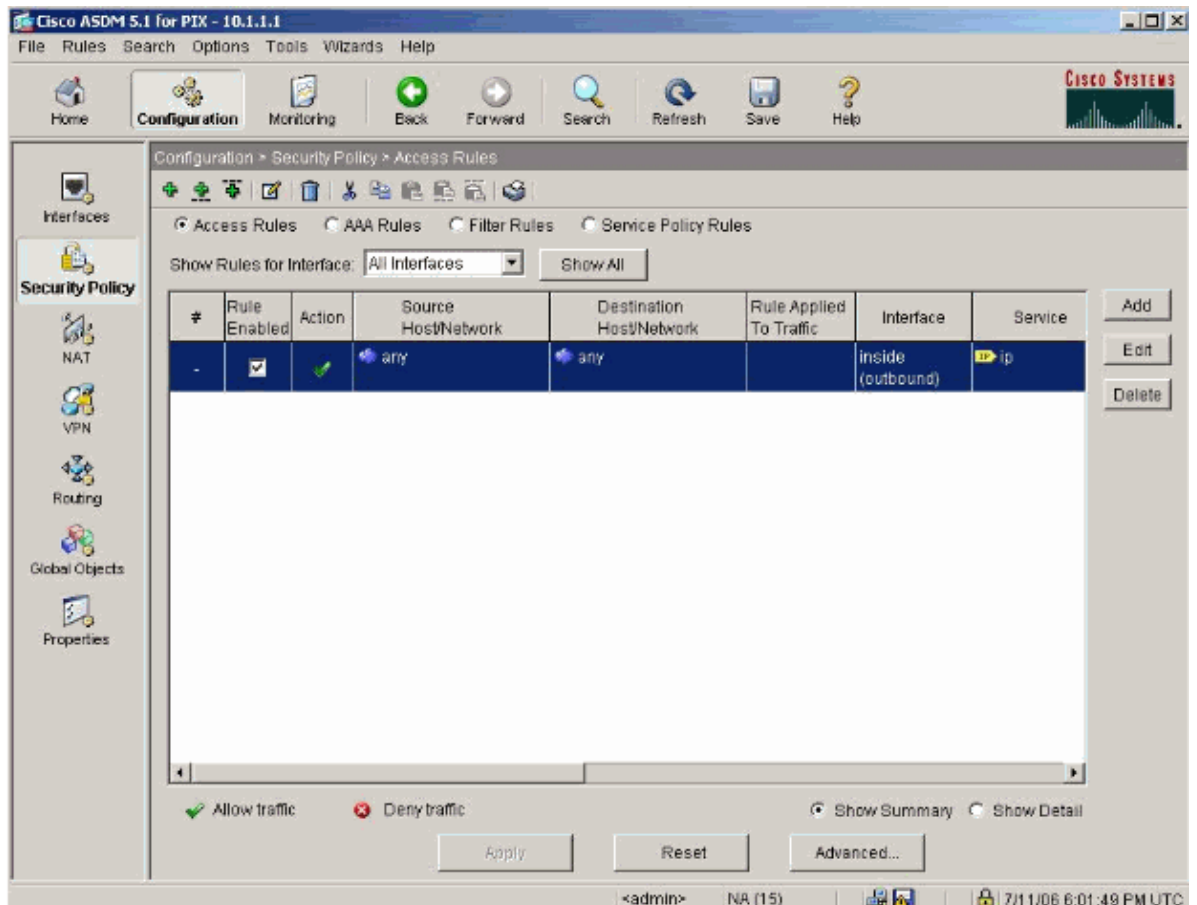
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

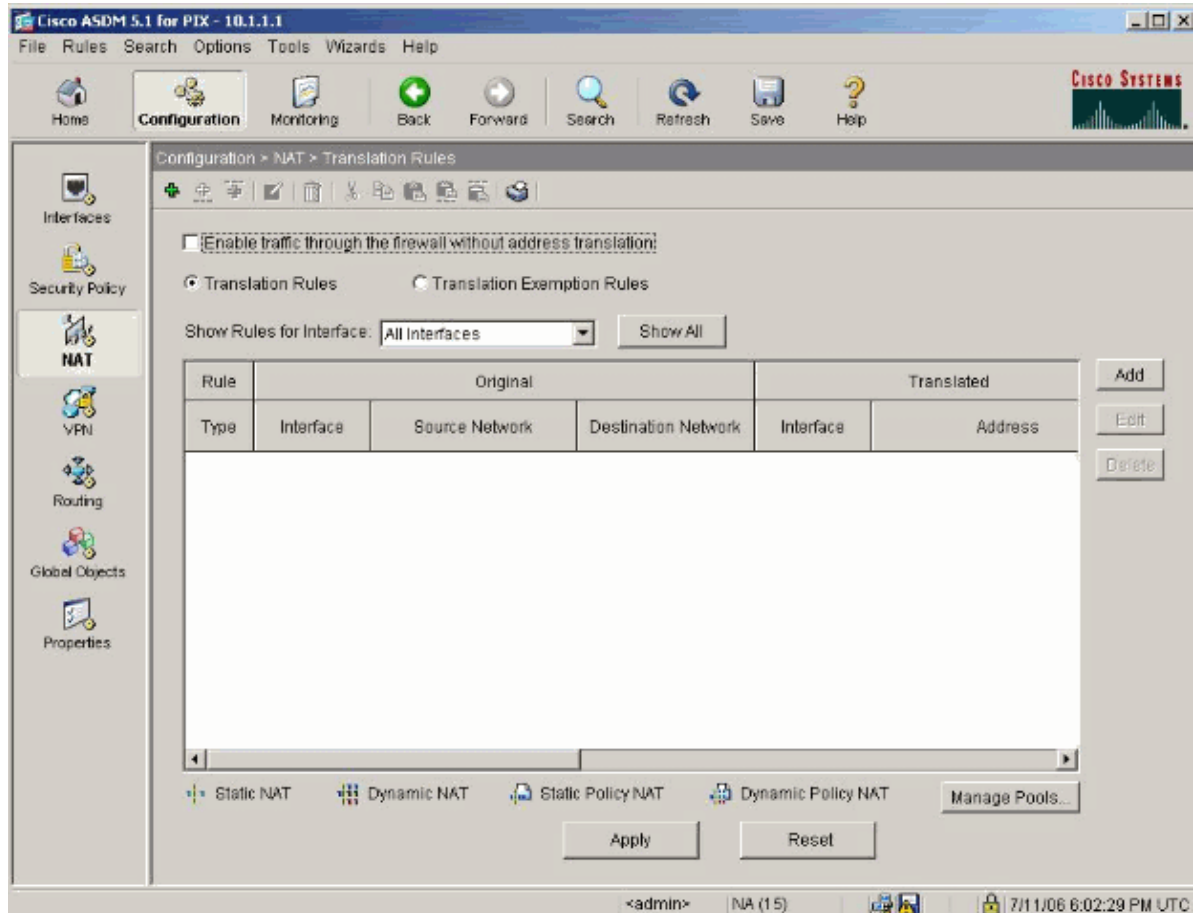
9. Click **Apply** to accept the interface configuration. The configuration also gets pushed onto the PIX.



10. Choose **Security Policy** on the Features tab in order to review the security policy rule used. In this example, the default inside rule is used.



11. In this example, NAT is used. Uncheck the **Enable traffic through the firewall without address translation** check box and click **Add** in order to configure the NAT rule.



12. Configure the Source Network. In this example, 10.0.0.0 is used for the IP address, and 255.0.0.0 is used for the mask.

Click **Manage Pools** in order to define the NAT pool addresses.

**Add Address Translation Rule**

Use NAT     Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static    IP Address:

Redirect port

TCP    Original port:     Translated port:

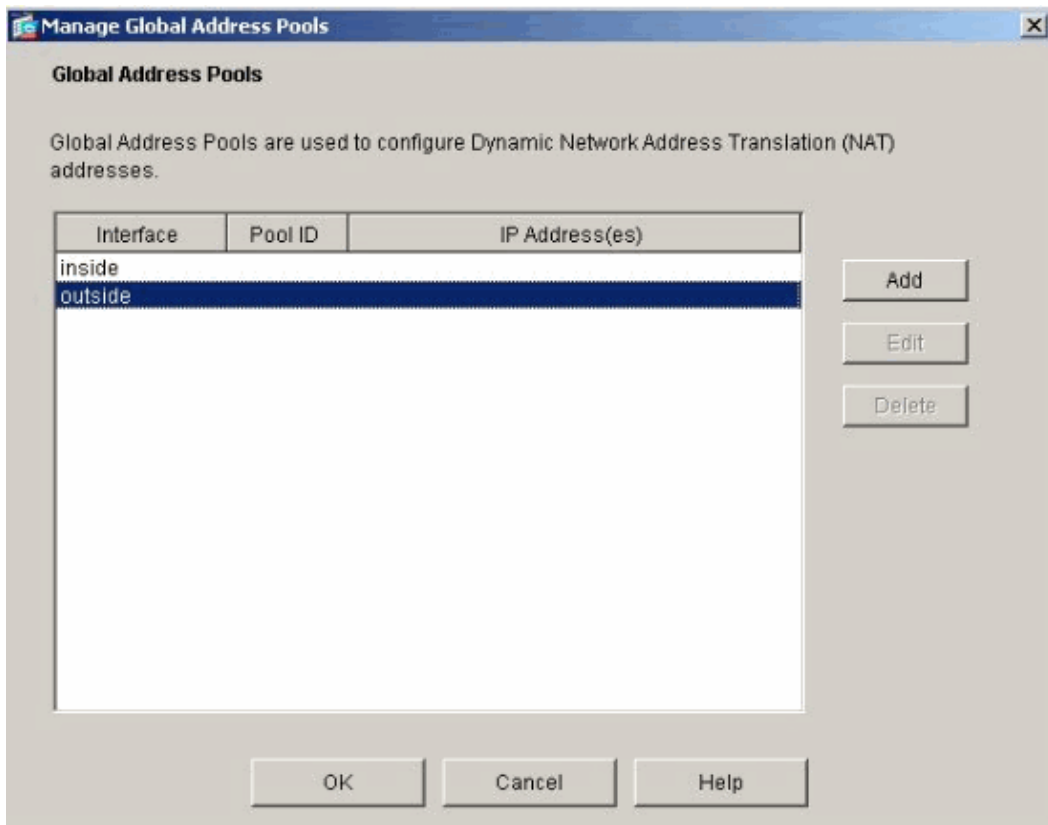
UDP

Dynamic    Address Pool:    

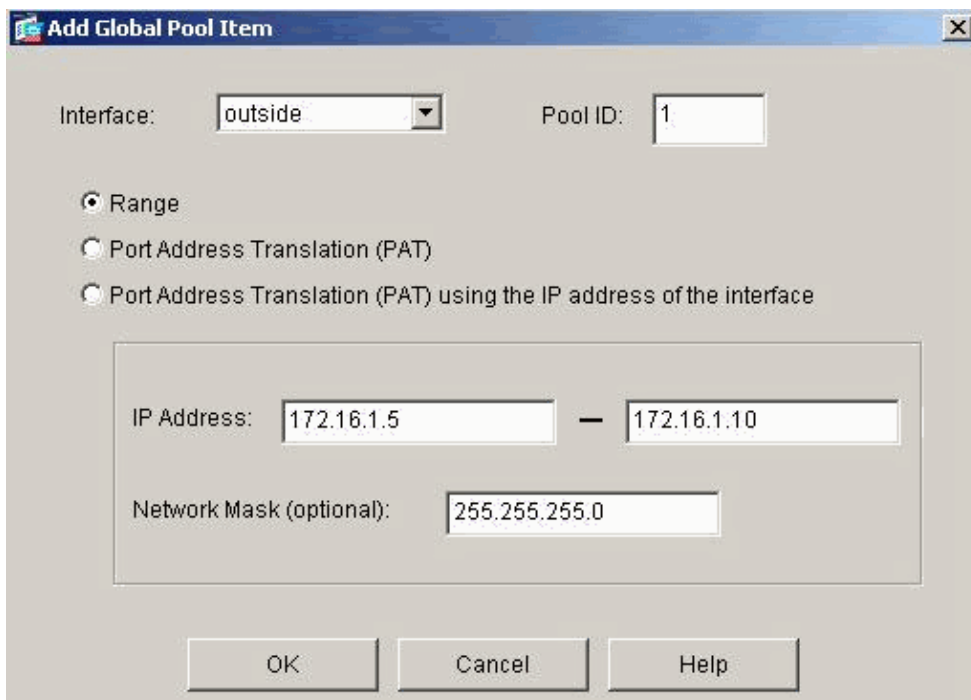
Pool ID	Address
N/A	No address pool defined

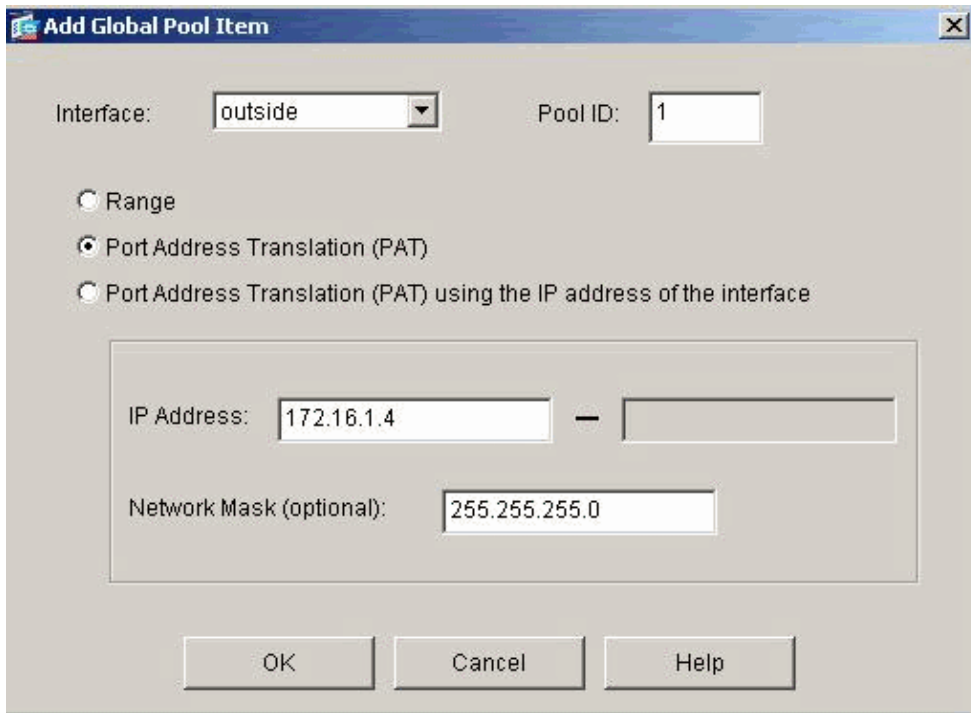
13. Select the outside interface and click **Add**.



14. In this example, a Range and PAT address pool are configured. Configure the range NAT pool address and click **OK**.



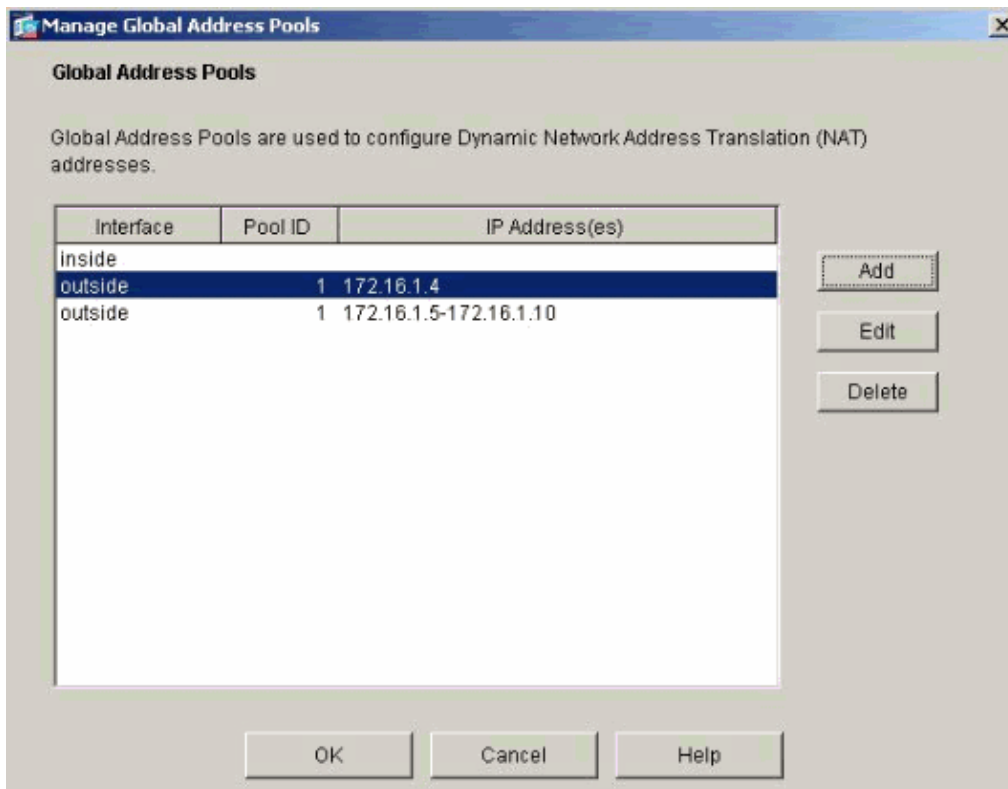
15. Select the outside interface in step 13 in order to configure the PAT address. Click **OK**



The dialog box titled "Add Global Pool Item" contains the following fields and options:

- Interface:
- Pool ID:
- Radio buttons:
  - Range
  - Port Address Translation (PAT)
  - Port Address Translation (PAT) using the IP address of the interface
- IP Address:  —
- Network Mask (optional):
- Buttons: OK, Cancel, Help

Click **OK** in order to continue.



The dialog box titled "Manage Global Address Pools" displays a table of existing pools and control buttons:

Global Address Pools are used to configure Dynamic Network Address Translation (NAT) addresses.

Interface	Pool ID	IP Address(es)
inside		
outside	1	172.16.1.4
outside	1	172.16.1.5-172.16.1.10

Buttons: Add, Edit, Delete, OK, Cancel, Help

- On the Edit Address Translation Rule window, select the Pool ID to be used by the source network configured. Click **OK**.

**Edit Address Translation Rule**

Use NAT   
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static    IP Address:

Redirect port:

TCP    Original port:     Translated port:

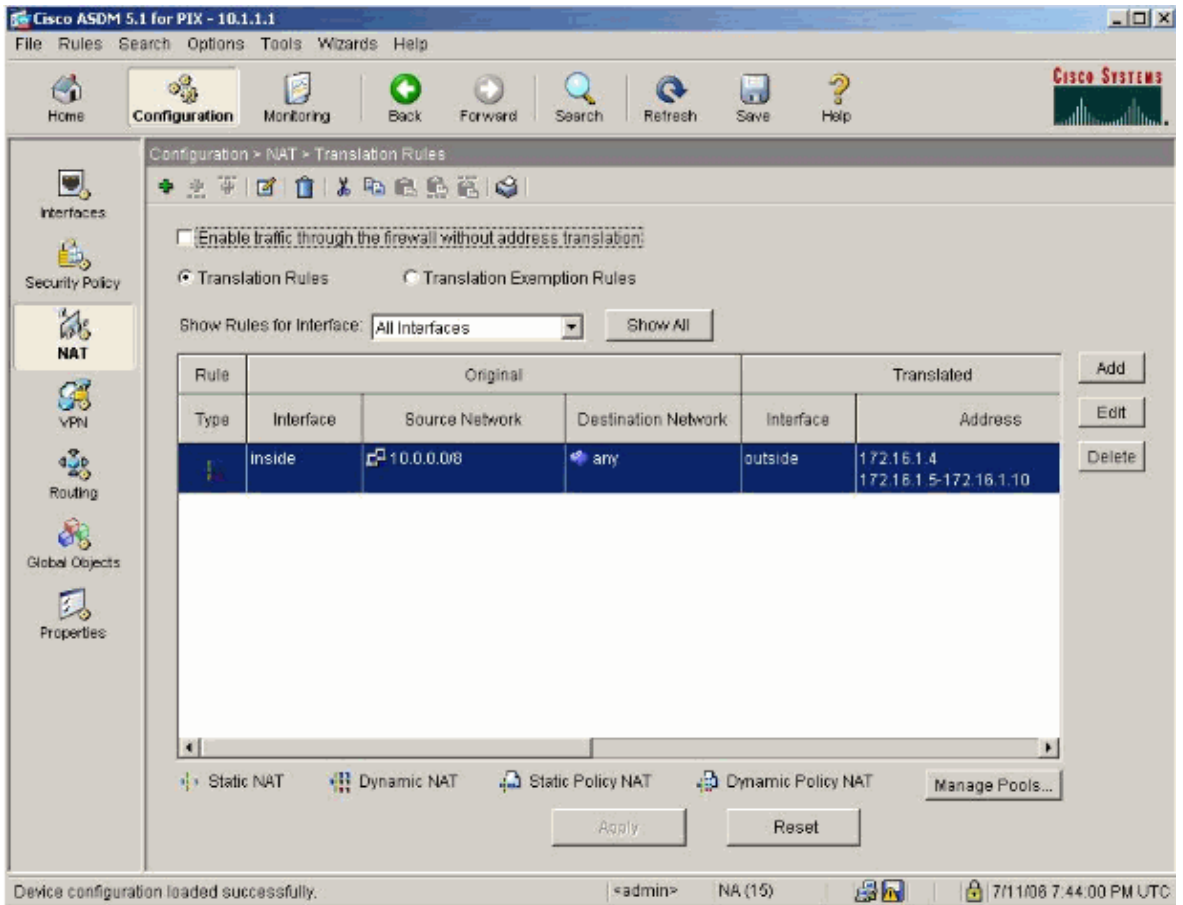
UDP

Dynamic    Address Pool:    

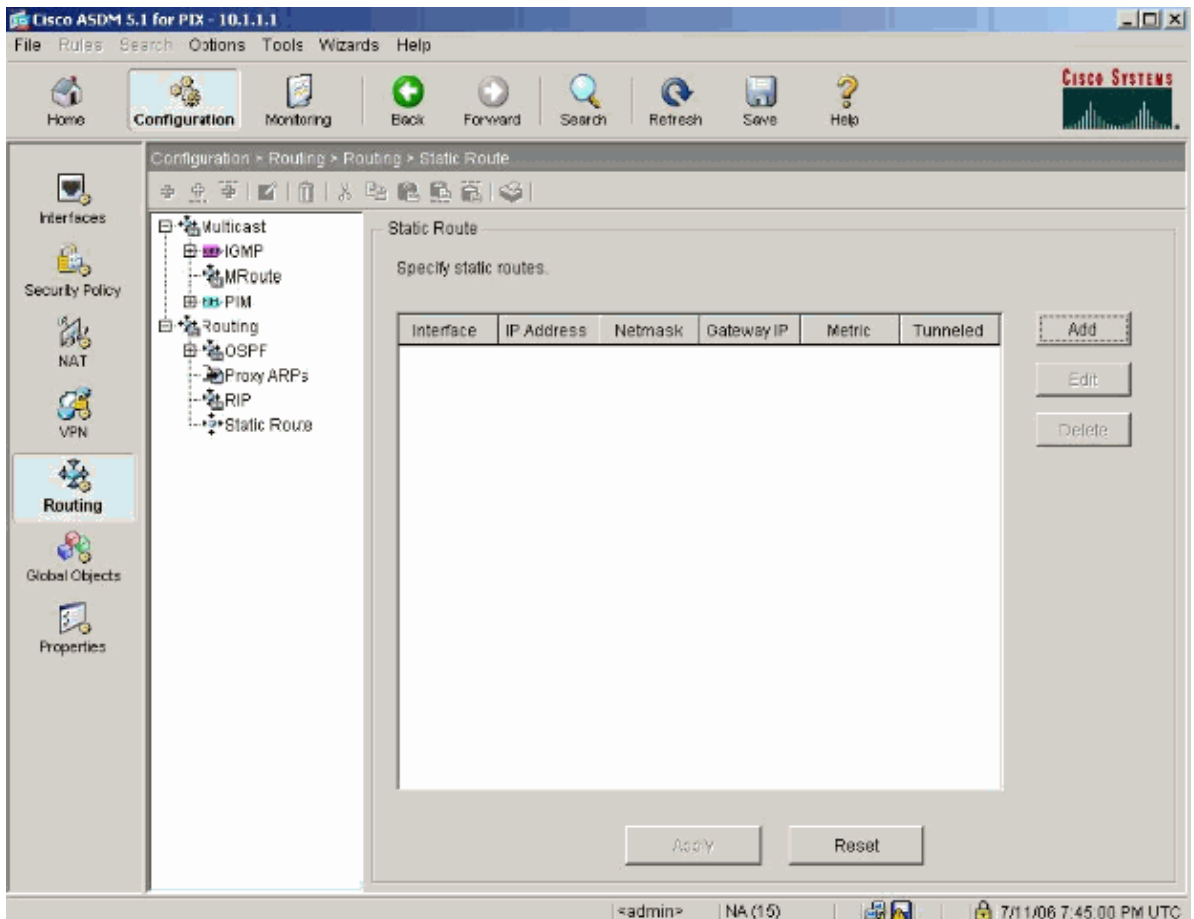
Pool ID	Address
1	172.16.1.4 172.16.1.5-172.16.1.10

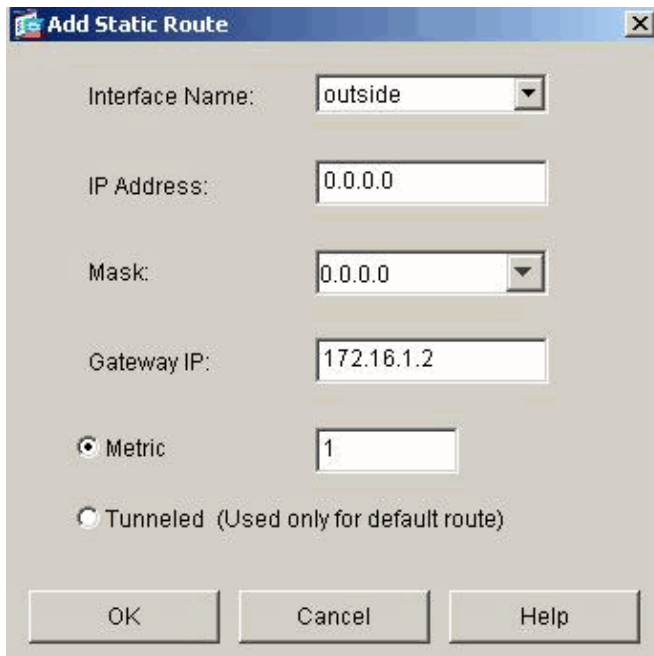
17. Click **Apply** in order to push the configured NAT rule to the PIX.



18. In this example, static routes are used. Click **Routing**, choose **Static Route** and click **Add**.



19. Configure the default gateway and click **OK**.



Interface Name: outside

IP Address: 0.0.0.0

Mask: 0.0.0.0

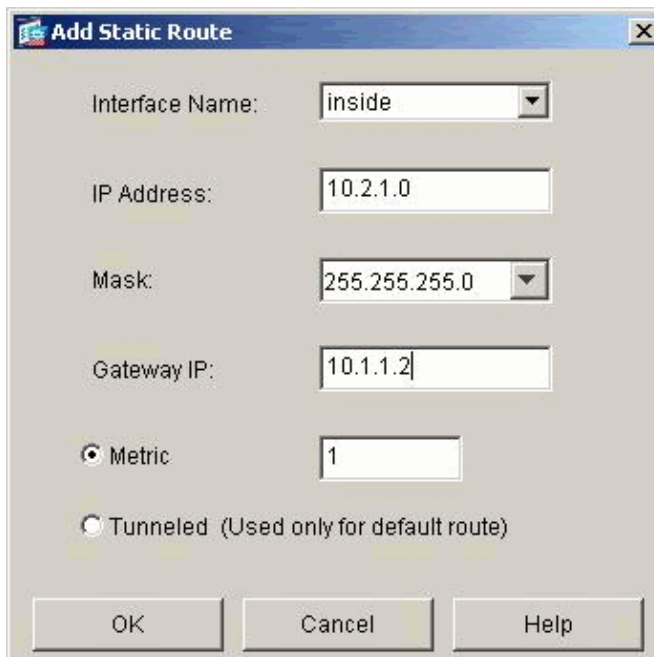
Gateway IP: 172.16.1.2

Metric 1

Tunneled (Used only for default route)

OK Cancel Help

20. Click **Add** and add the routes to the inside networks.



Interface Name: inside

IP Address: 10.2.1.0

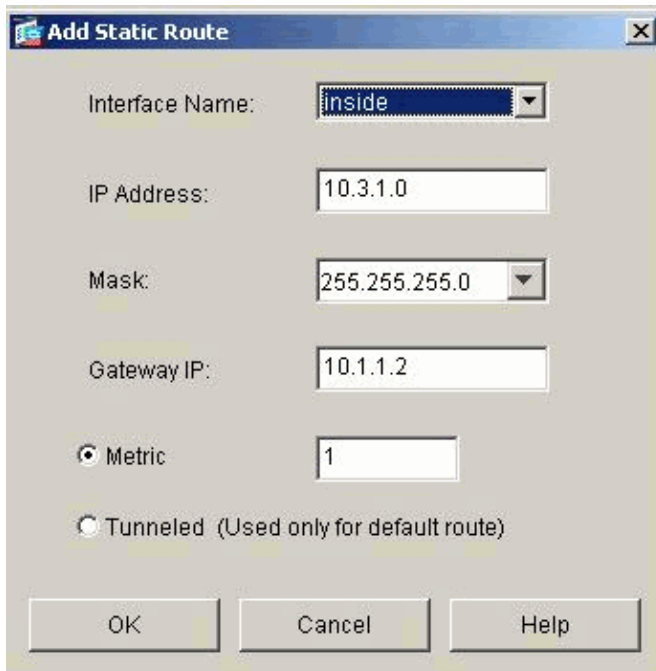
Mask: 255.255.255.0

Gateway IP: 10.1.1.2

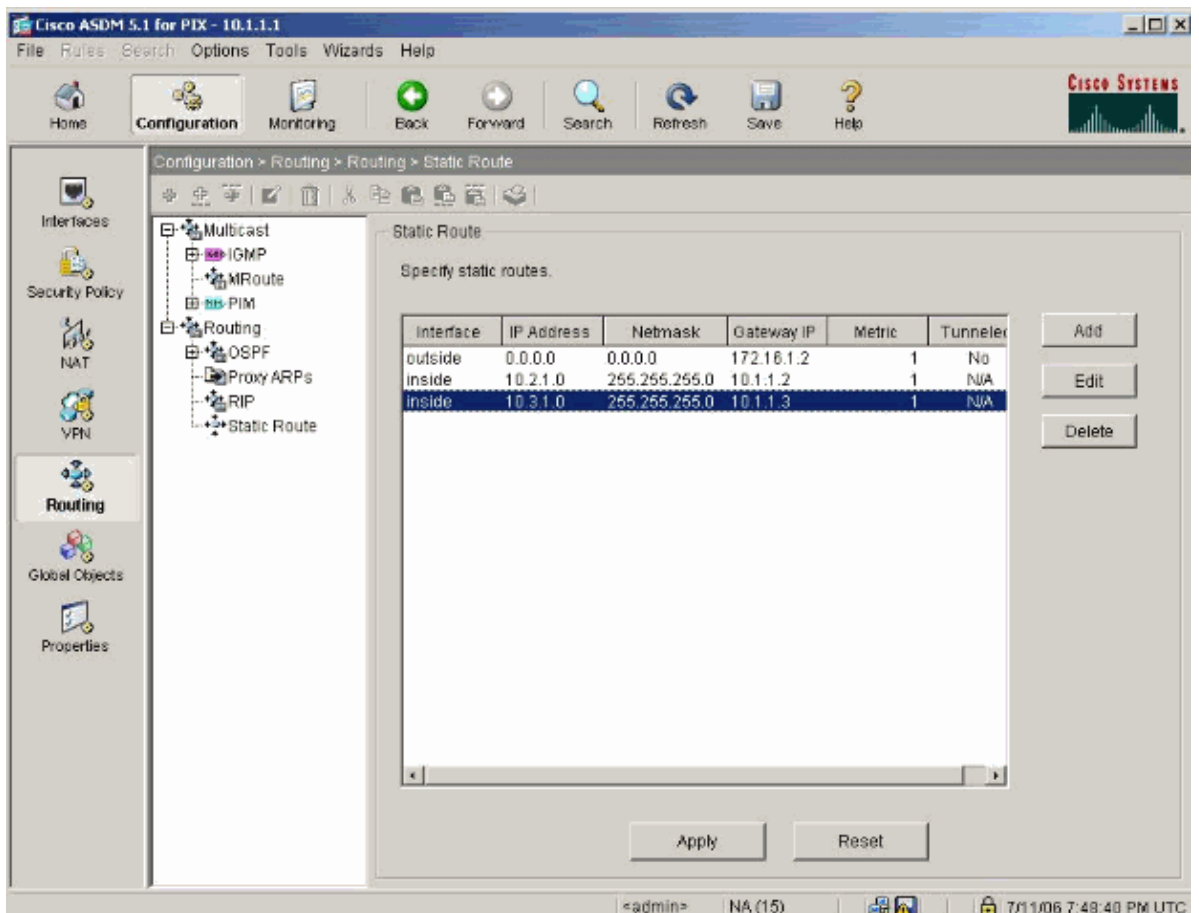
Metric 1

Tunneled (Used only for default route)

OK Cancel Help



21. Confirm that the correct routes are configured and click **Apply**.



## PIX Configuration using CLI

Configuration via the ASDM GUI is now complete.

You can see this configuration via the CLI:

## PIX Security Appliance CLI

```
pixfirewall(config)#write terminal
PIX Version 7.0(0)102
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!

interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0

!--- Assign name and IP address to the interfaces

enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted

asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400

nat-control

!--- Enforce a strict NAT for all the traffic through the Security appliance

global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0

!--- Define a pool of global addresses 172.16.1.5 to 172.16.1.10 with
!--- NAT ID 1 to be used for NAT

global (outside) 1 172.16.1.4 netmask 255.255.255.0

!--- Define a single IP address 172.16.1.4 with NAT ID 1 to be used for NAT

nat (inside) 1 10.0.0.0 255.0.0.0

!--- Define the inside networks with same NAT ID 1 used in the global command for NAT

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Configure static routes for routing the packets towards the internal network

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1

!--- Configure static route for routing the packets towards the Internet (or External network)

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
 sip_media 0:02:00
timeout uauth 0:05:00 absolute

http server enable

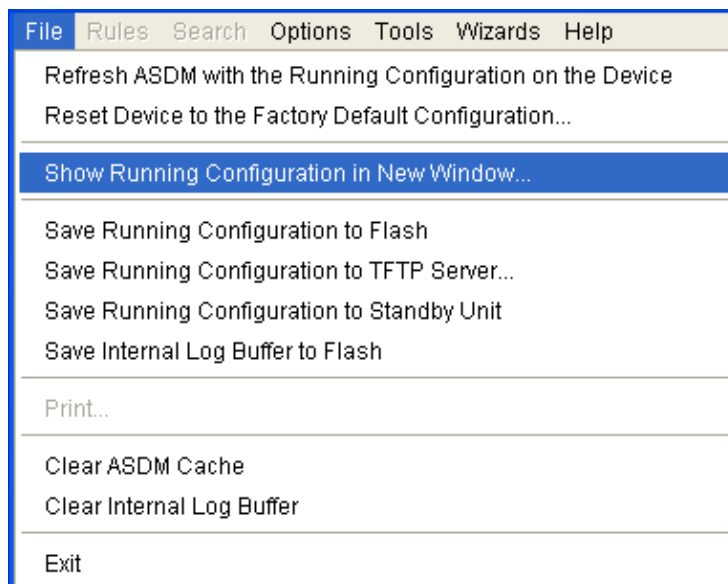
!--- Enable the HTTP server on PIX for ASDM access

http 10.1.1.5 255.255.255.255 inside

!--- Enable HTTP access from host 10.1.1.5 to configure PIX using ASDM (GUI)
```

```
!  
  
!--- Output suppressed  
  
!  
!  
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5  
: end
```

Choose **File > Show Running Configuration in New Window** in order to view the CLI configuration in ASDM.



## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

### Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

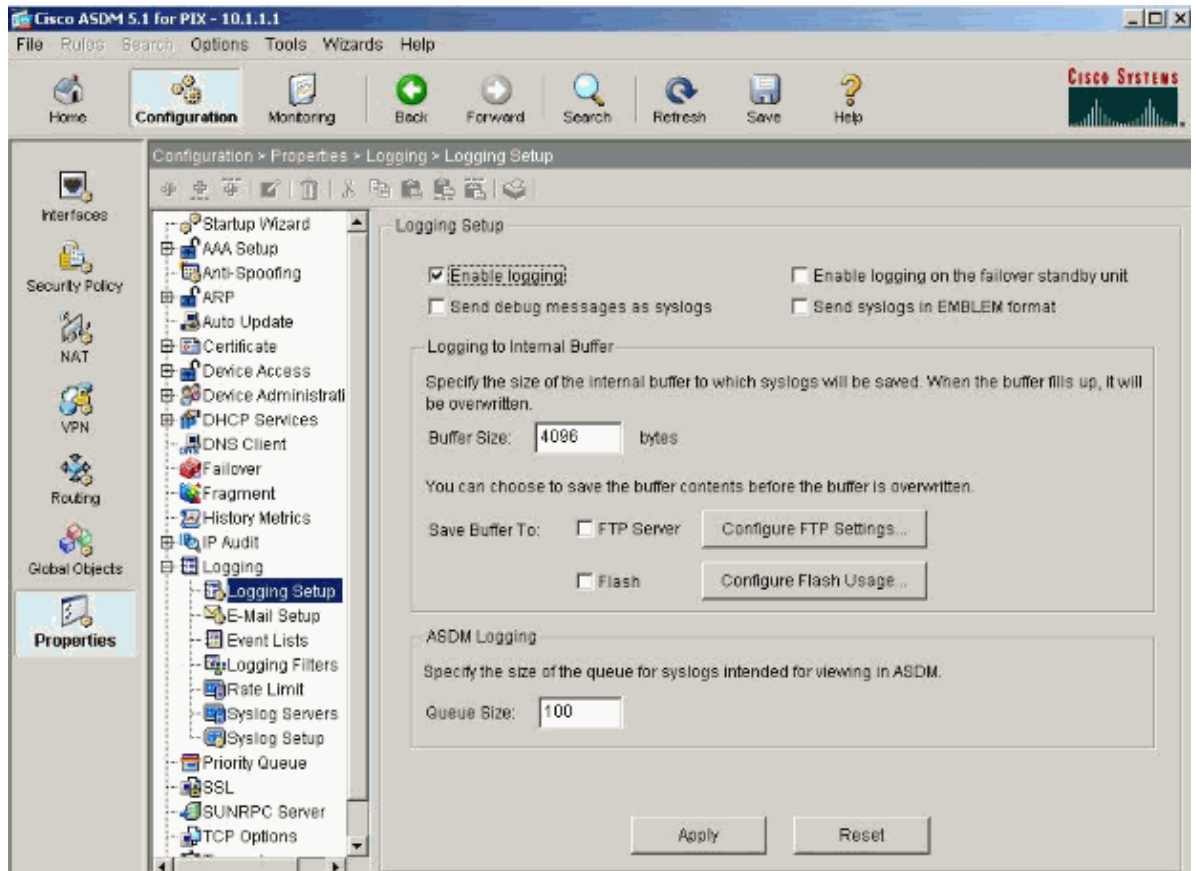
**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug icmp trace** Shows whether ICMP requests from the hosts reach the PIX. In order to run this debug, you need to add the **access-list** command to permit ICMP in your configuration.
- **logging buffer debugging** Shows connections that are established and denied to hosts that go through the PIX. The information is stored in the PIX log buffer and you can see the output with the **show log** command.

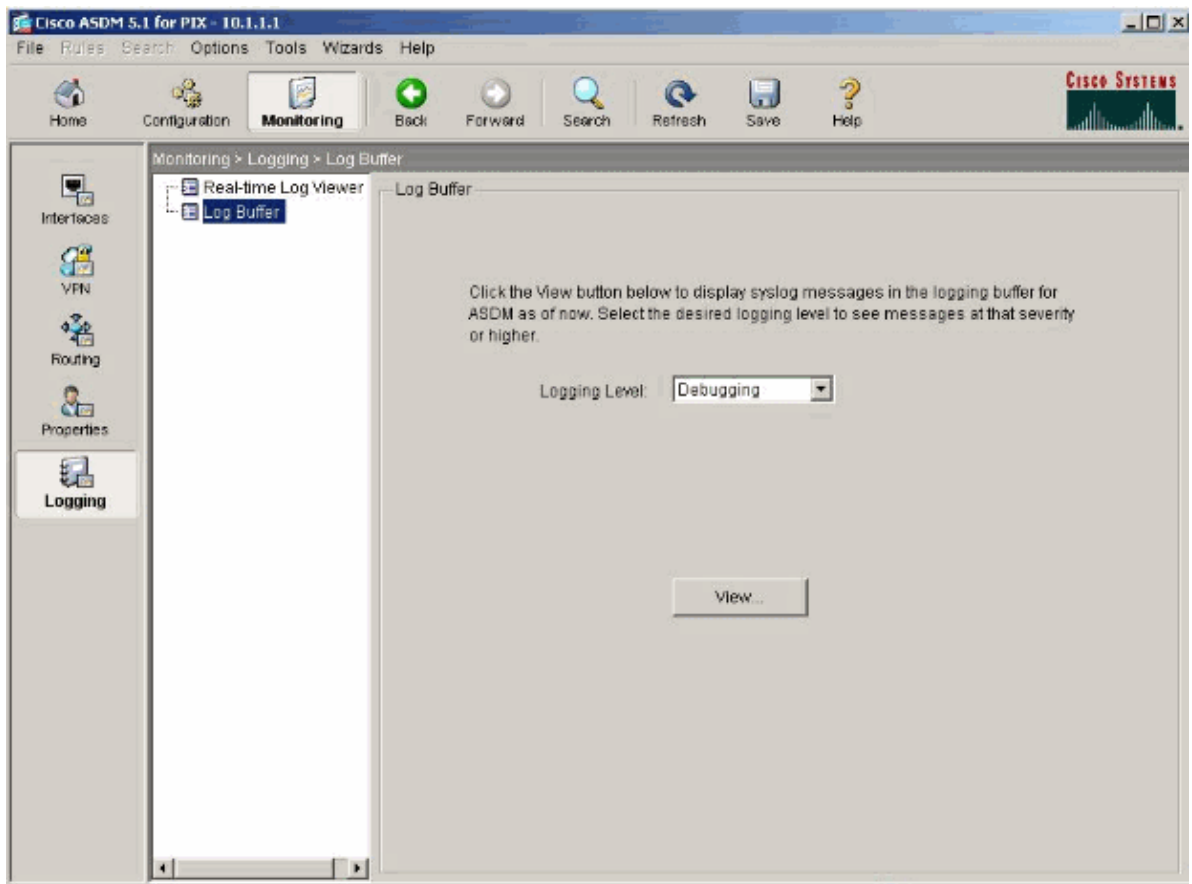
# Troubleshooting Procedure

ASDM can be used to enable logging, and also to view the logs:

1. Choose **Configuration > Properties > Logging > Logging Setup**, check **Enable Logging**, and click **Apply**.



2. Choose **Monitoring > Logging > Log Buffer > Logging Level** and choose **Logging Buffer** from the drop-down list. Click **View**.



3. Here is an example of the Log Buffer:

The screenshot shows the 'Log Buffer' window with a table of syslog messages. The table has three columns: 'Severity', 'Time', and 'Message ID: Description'. The messages are as follows:

Severity	Time	Message ID: Description
6	Jul 12 2006 13:08:11	605005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user 'enable_15'
6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
6	Jul 12 2006 13:08:10	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
6	Jul 12 2006 13:08:09	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302021: Teardown ICMP connectio for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0

At the bottom of the window, there is a legend for severity levels: Emergencies (red circle), Alerts (red circle), Critical (orange circle), Errors (orange circle), Warnings (yellow triangle), Notifications (yellow triangle), Informational (yellow triangle), and Debugging (yellow circle).

## Unable to Access Websites by Name

In certain scenarios, the internal networks cannot access the internet websites by using name (works with IP address) in the web browser. This issue is common and usually occurs if the DNS server is not defined, especially in cases where PIX/ASA is the DHCP server. Also, this can occur in cases if the PIX/ASA is unable to push the DNS server or if the DNS server is not reachable.

## Related Information

- [Cisco PIX 500 Series Security Appliances](#)
  - [Cisco ASA 5500 Series Adaptive Security Appliances](#)
  - [Documentation for PIX Firewall](#)
  - [Cisco Secure PIX Firewall Command References](#)
  - [Cisco Adaptive Security Device Manager](#)
  - [Cisco Adaptive Security Device Manager \(ASDM\) Troubleshoot and Alerts](#)
  - [Requests for Comments \(RFCs\)](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 24, 2008

Document ID: 63880

---