Table of Contents

PIX Security Appliance (Version 7.x) or ASA 5500 with Three Internal Networks Configuration Example

Document ID: 63880

Introduction

This document provides a sample configuration for PIX Security Appliance (Version 7.x) or Adaptive Security Appliance (ASA) 5500, with three internal networks. For simplicity, static routes are used.

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:

- PIX Security Appliance 515E with Software version 7.0
- Cisco routers with Cisco IOS® Software Release 12.3(7)T

Note: While the configuration in this document was tested on a PIX Security Appliance, it is also compatible with the ASA 5500.

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

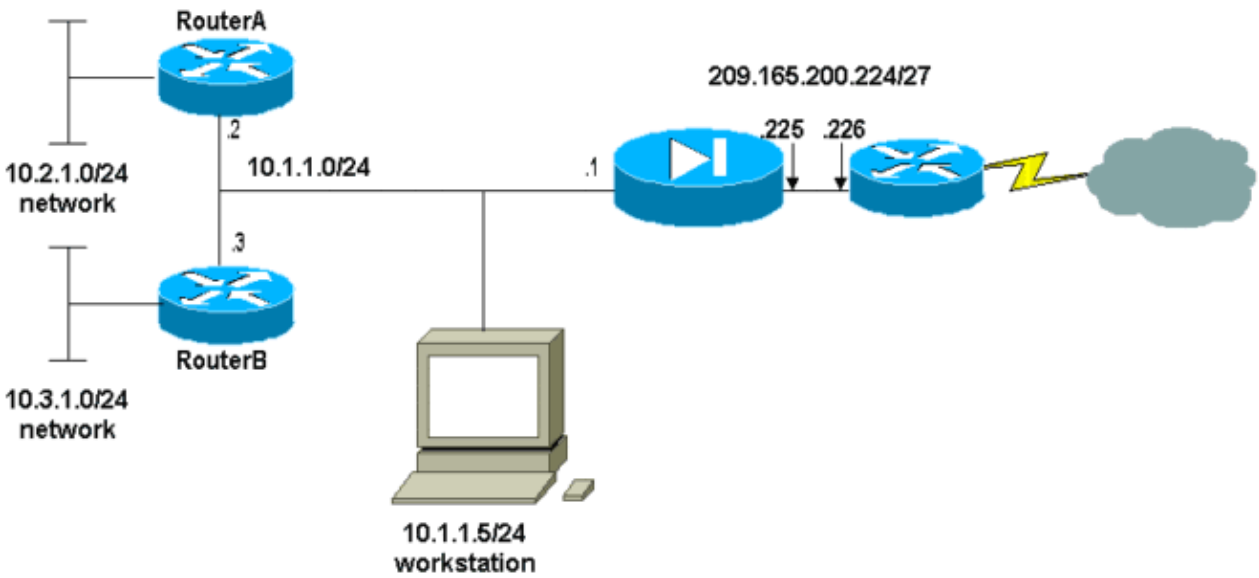
Configure

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

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

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 (Version 7.0) Configuration, including both:
    - PIX Security Appliance Advanced Security Device Manager (ASDM) Bootstrap and GUI
    - PIX Security Appliance Command Line Interface (CLI)

RouterA Configuration

`RouterA#show running-config`
`Building configuration...`
 	
`Current configuration : 1151 bytes`

```
!
version 12.3
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 12.3
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 would like to use the ASDM for configuration of the PIX Security Appliance, but have not yet bootstrapped the device, see these instructions:

- Console into the PIX.
- From a cleared configuration, use the interactive prompts to enable ASDM for the management of the PIX from the Workstation 10.1.1.

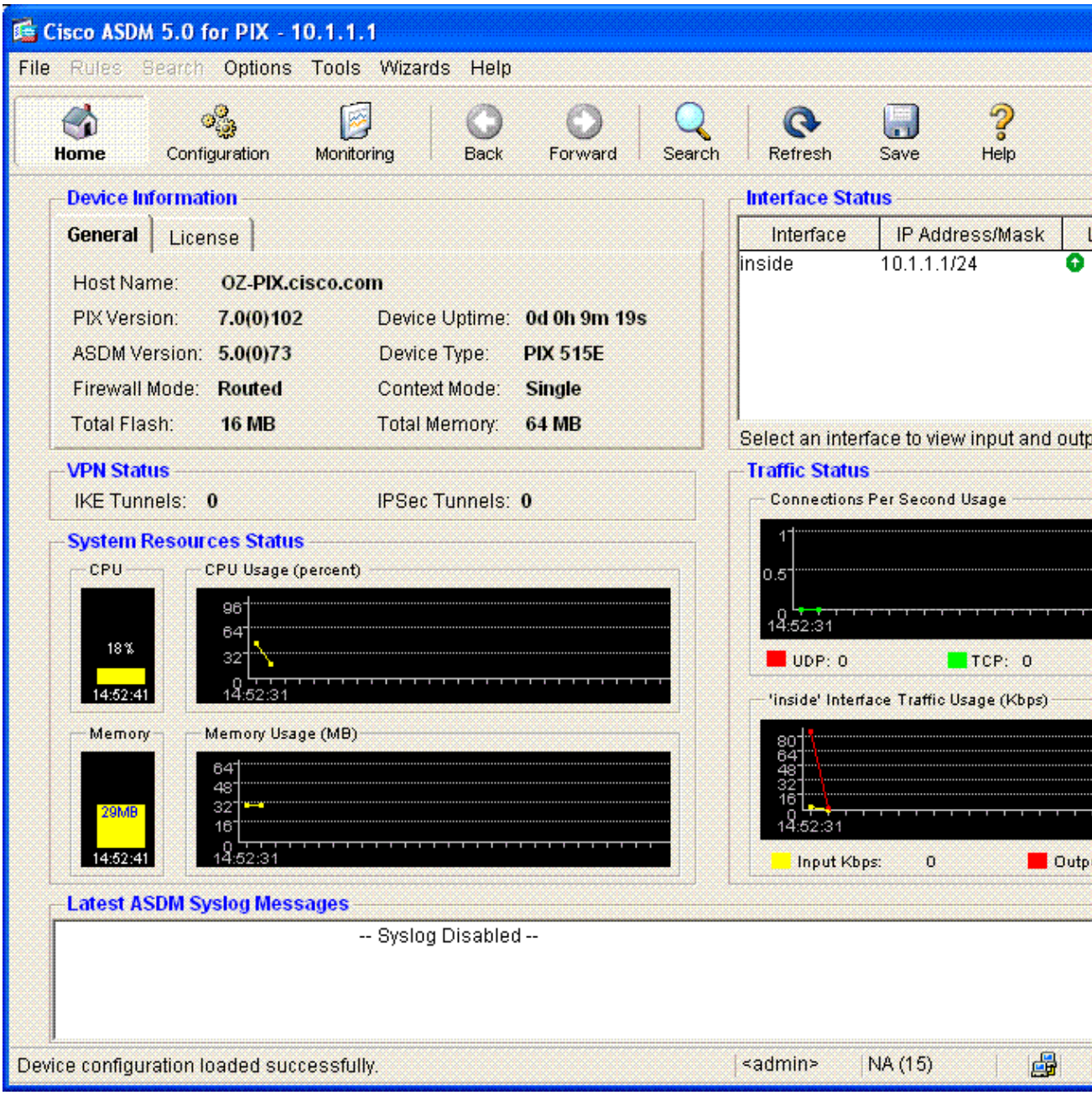
PIX Security Appliance (Version 7.0) Configuration

```
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
```

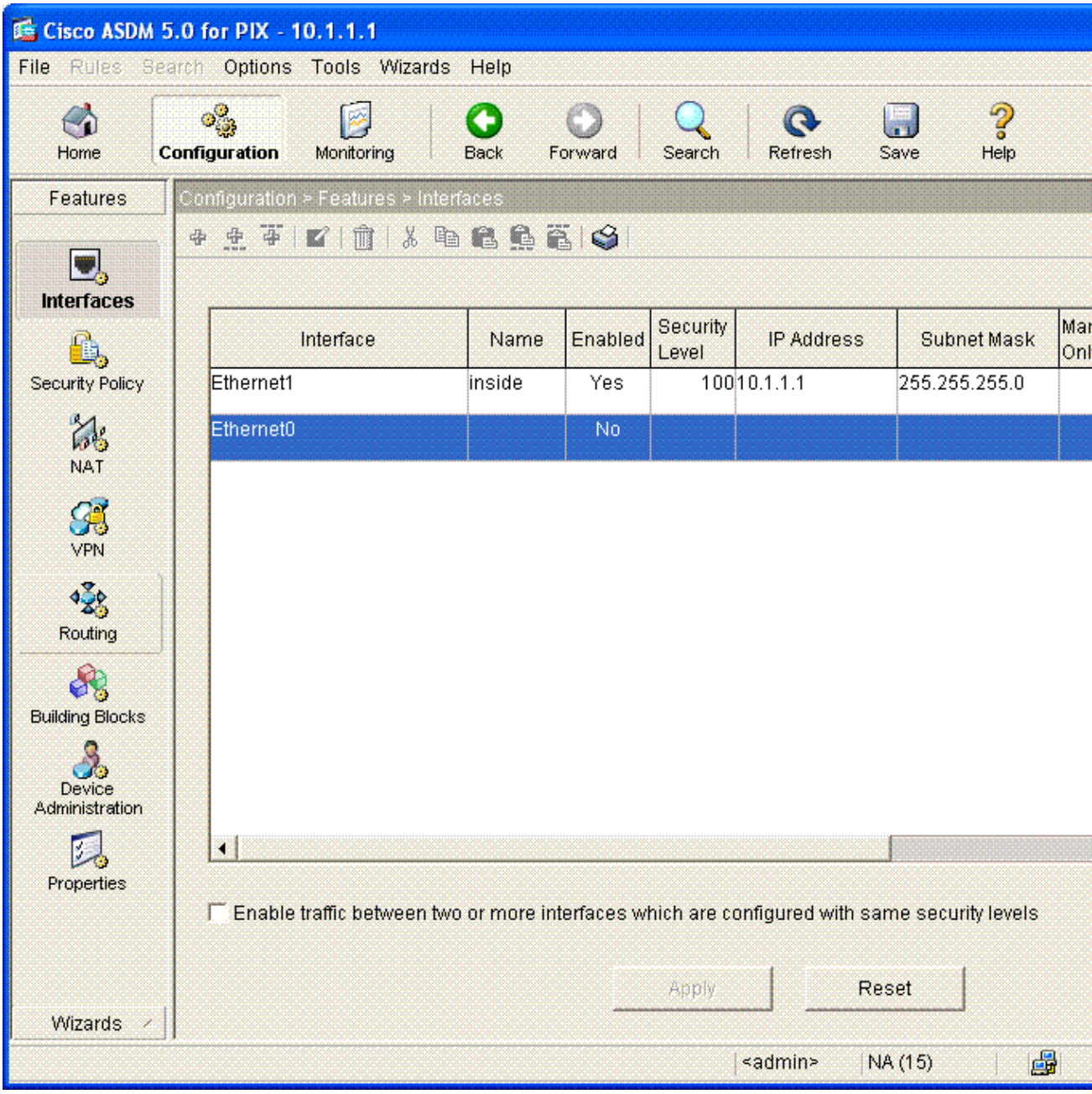
```
Type help or '?' for a list of available commands.
        OZ-PIX>
```

Complete these steps to configure via the ASDM GUI:

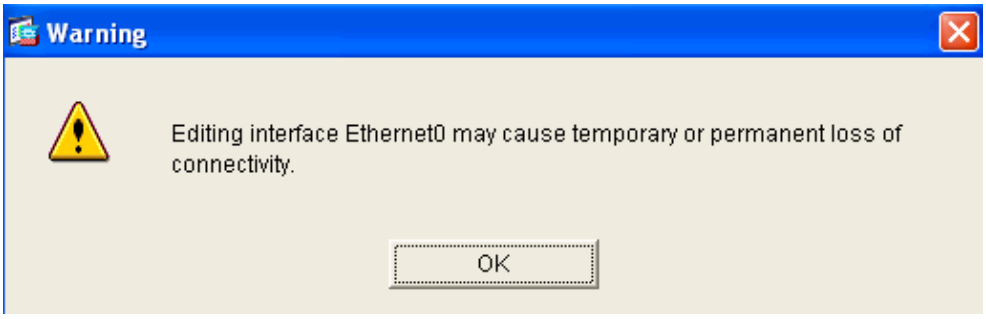
1. From Workstation 10.1.1.5, open a Web browser to use ADSM (in this example, https://10.1.1.1).
2. Click **yes** on the certificate prompts.
3. Log in with the enable password, as configured above.
4. If this is the first time ASDM is run on the PC, you are prompted to use ASDM Launcher or ASDM as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



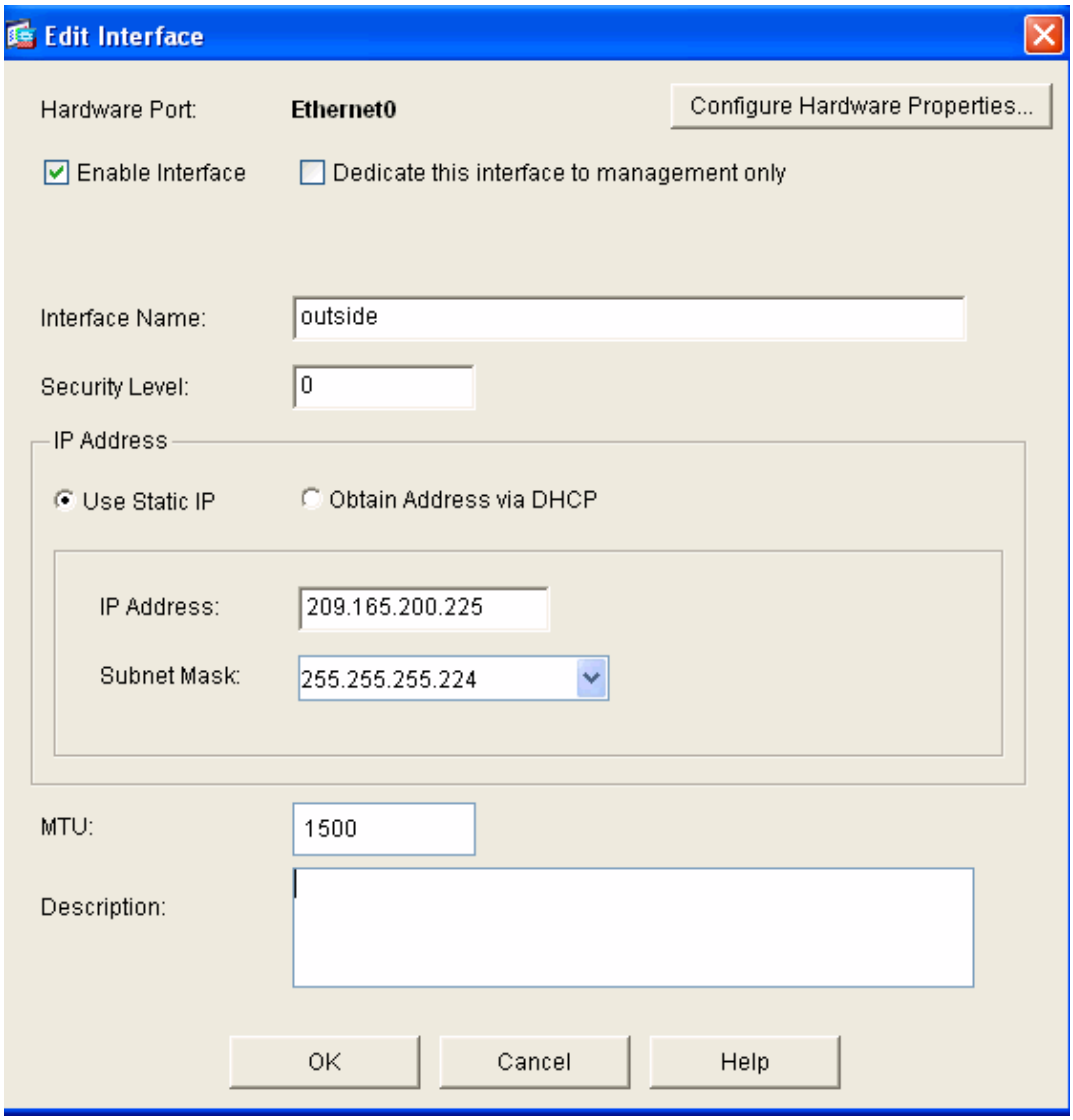
6. Configure the Outside Interface by selecting **Interface** > **Edit**.



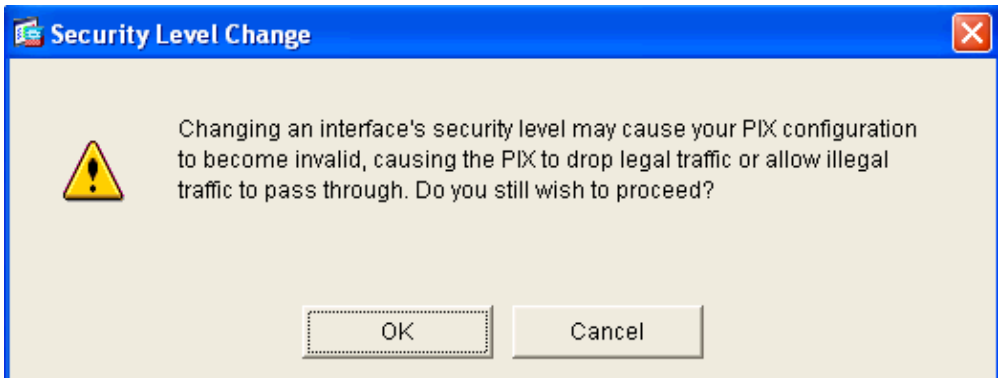
7. Click **OK** on the Warning dialog box.



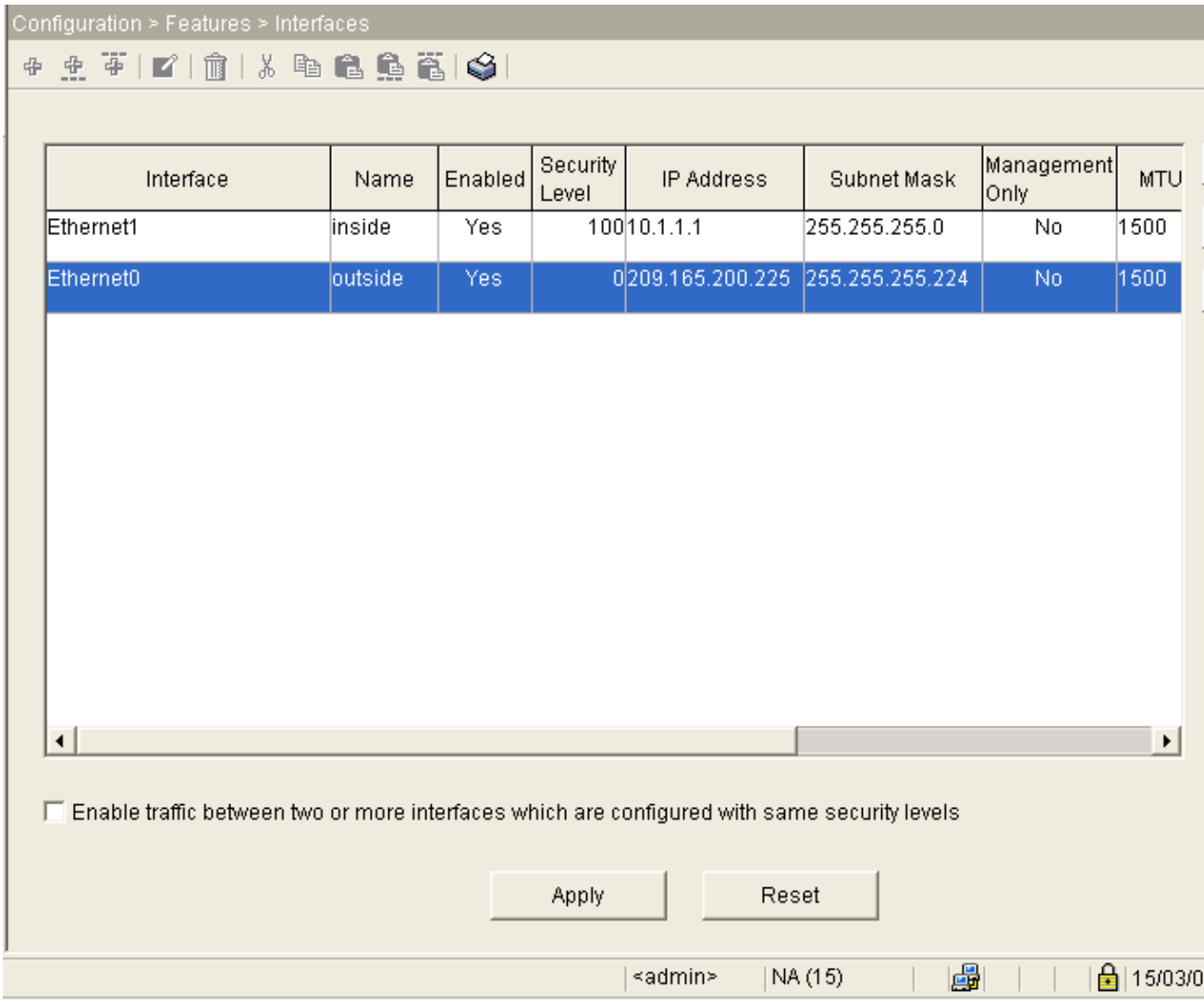
8. Enter the Interface details. Click **OK** when finished.



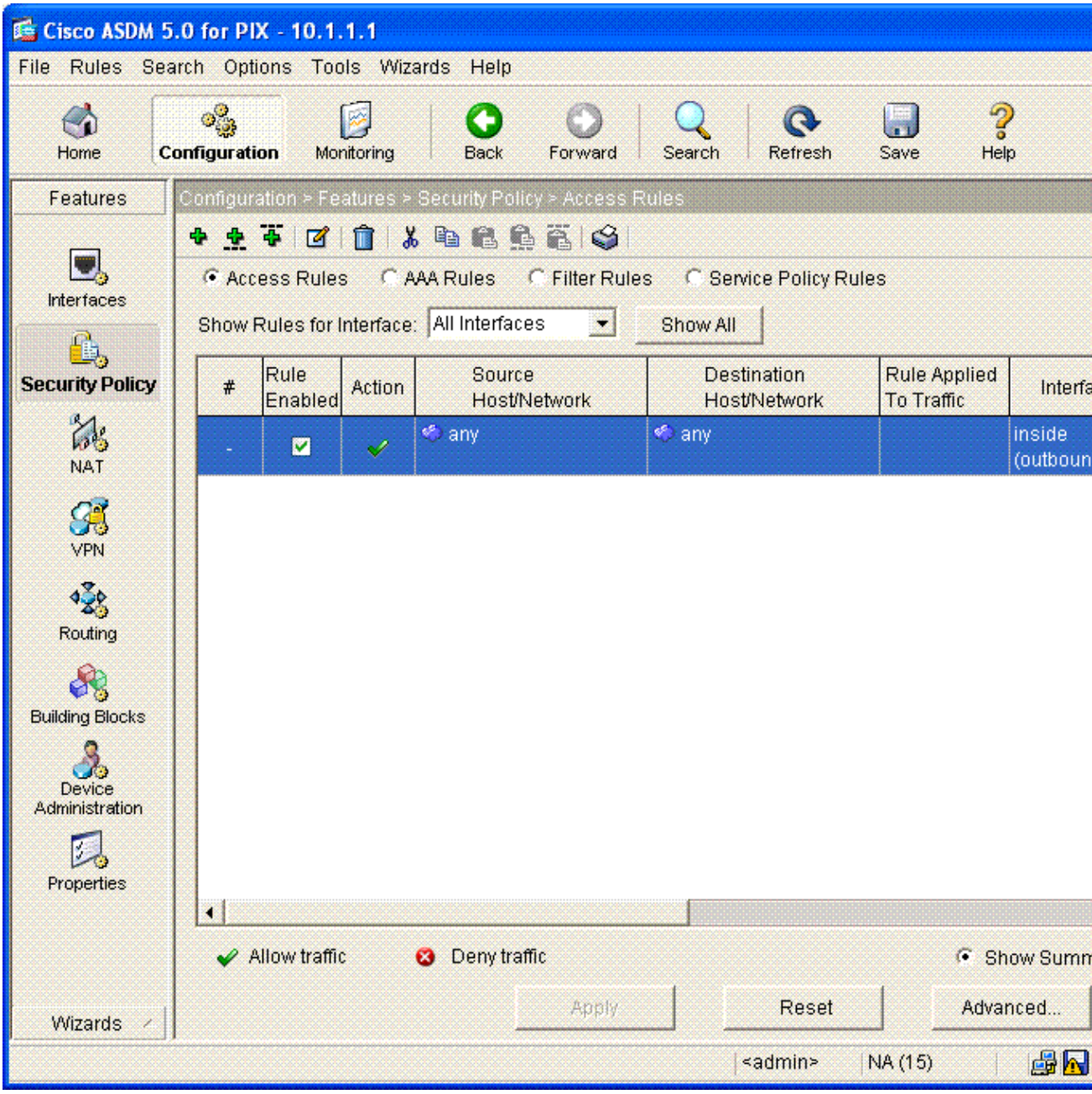
9. Click **OK** on the Security Level Change dialog box.



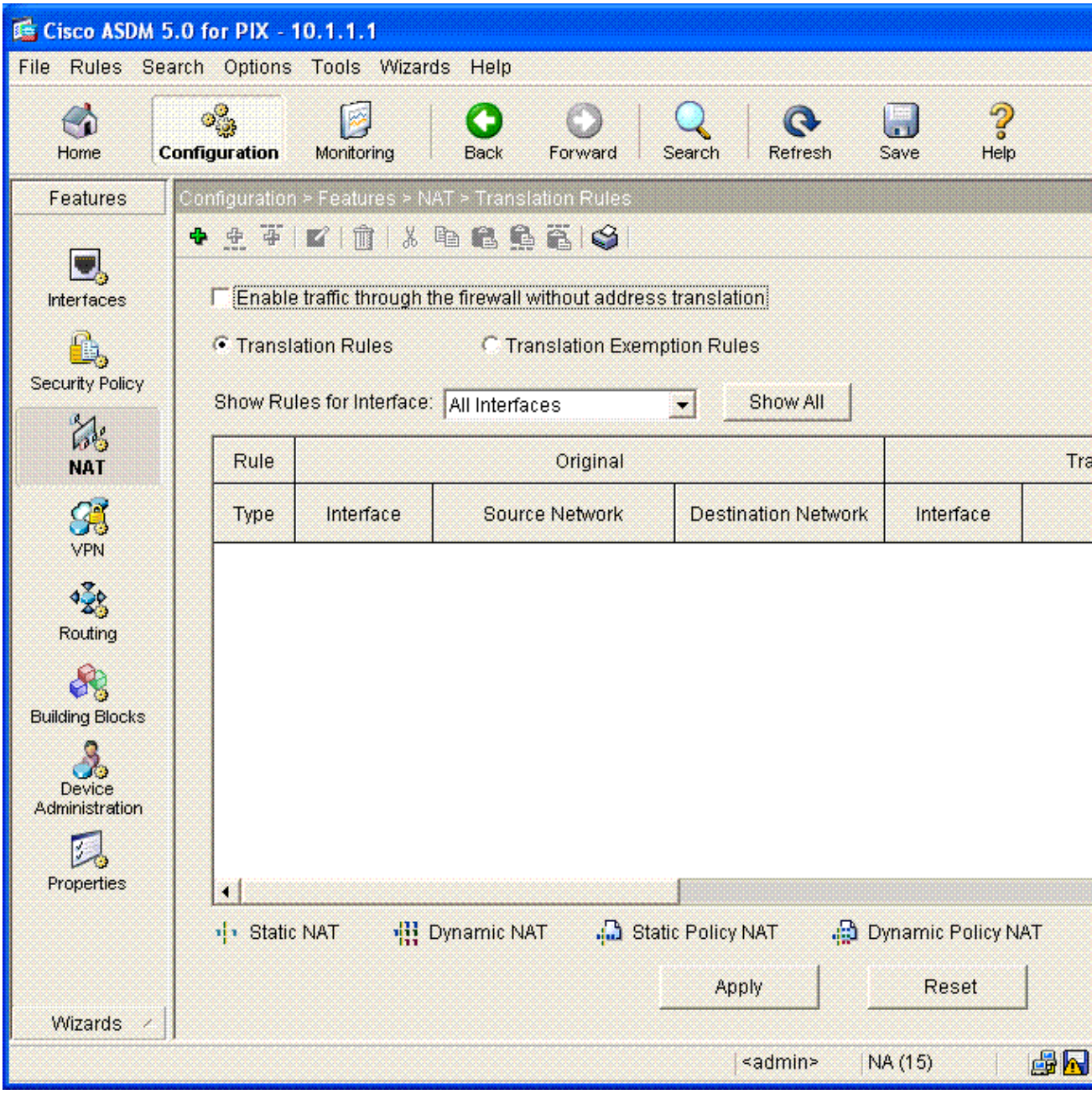
10. Click **Apply** to accept the interface configuration. The configuration also gets pushed onto the PIX.



11. Review the Security Policy Rule used by choosing **Security Policy** on the **Features** Tab. In this example, the Default Inside Rule is used.

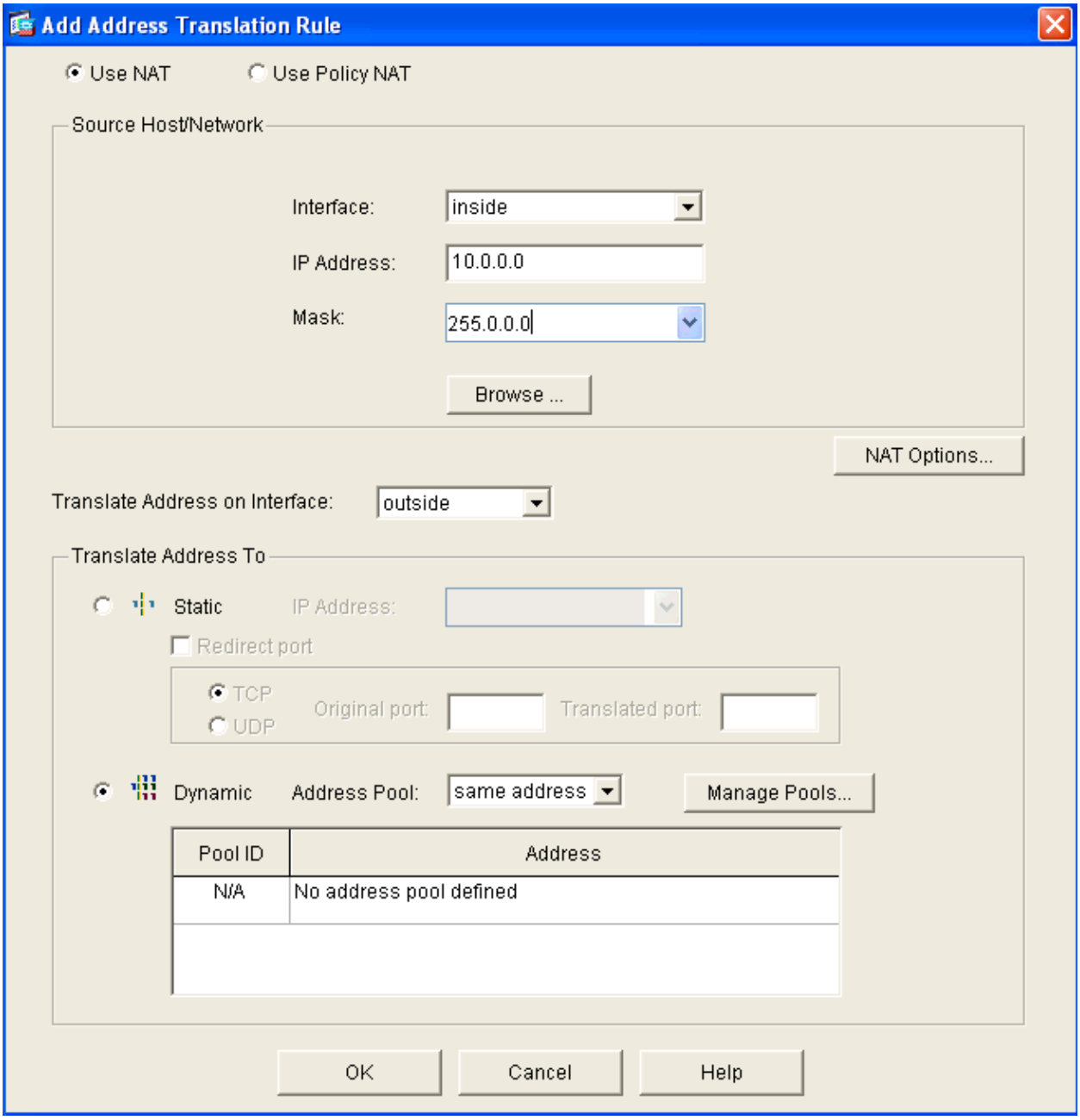


12. In this example, NAT is used. Uncheck the box for **Enable traffic through the firewall without address translation**. Click **Add** to configure the NAT Rule.

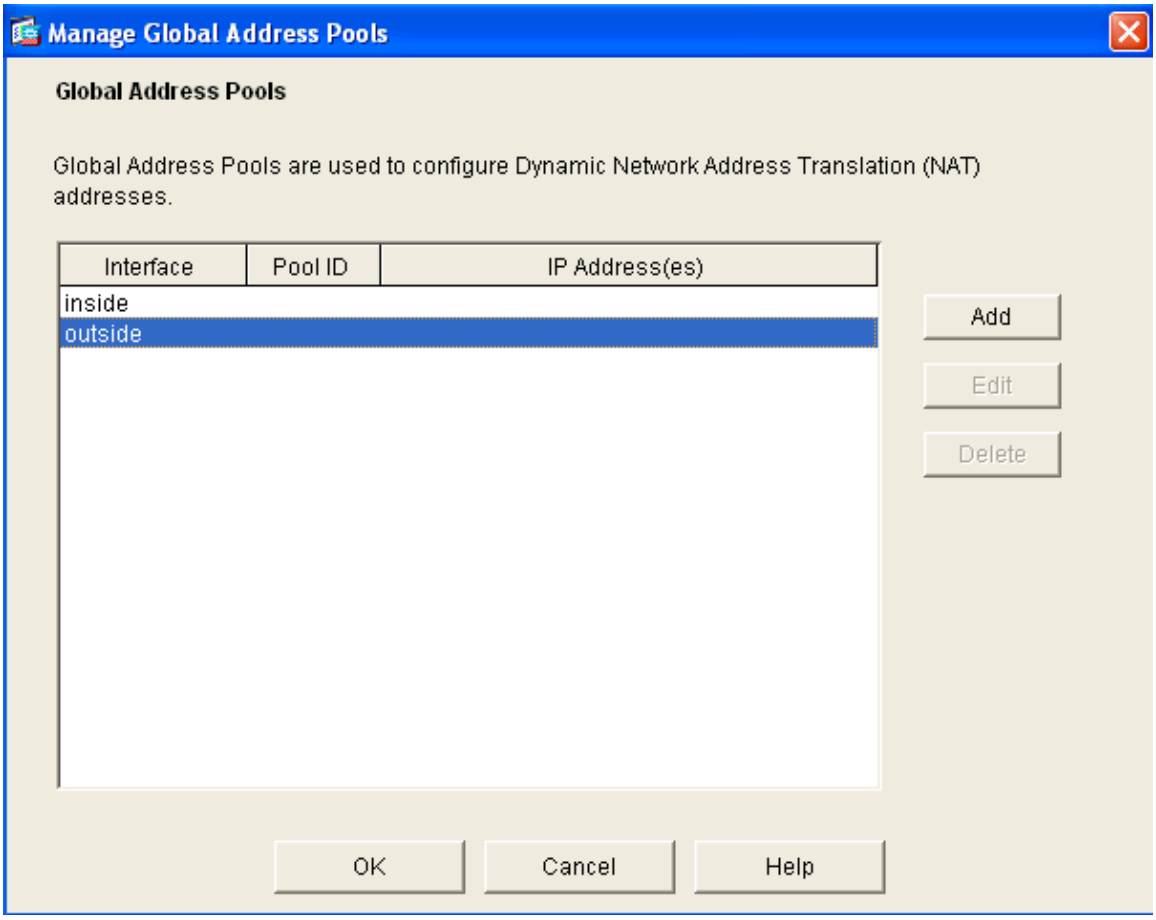


13. Configure the Source Network. In this example, 10.0.0.0 is used for the IP address, and 255.0.0.0 is used for the mask.

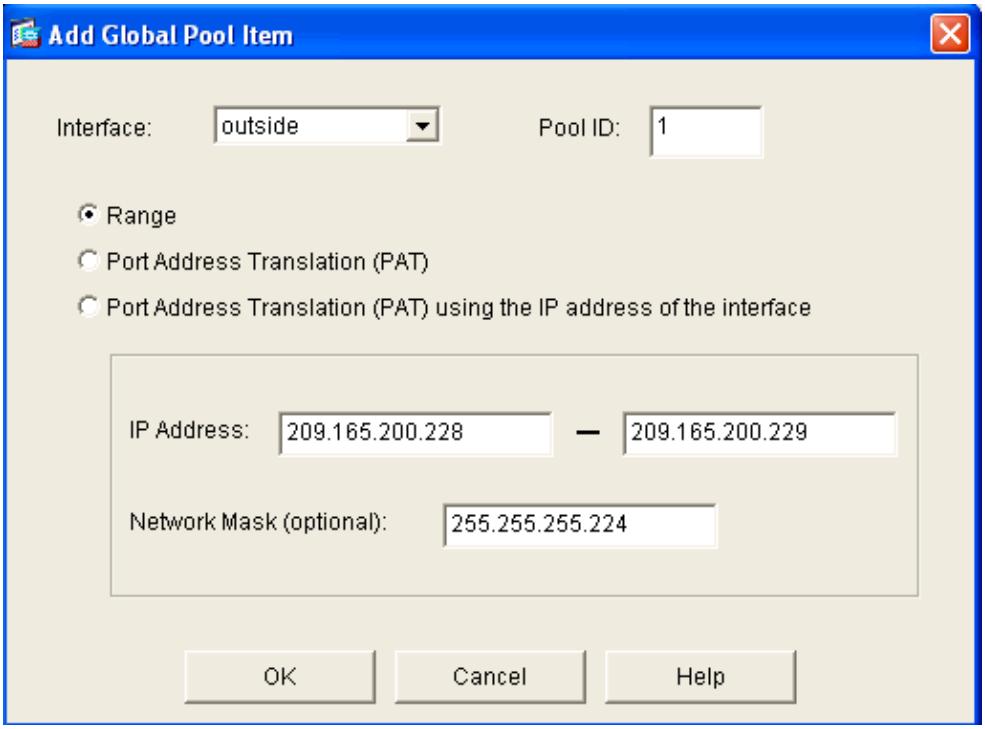
    Click **Manage Pools** to define the NAT Pool Addresses.



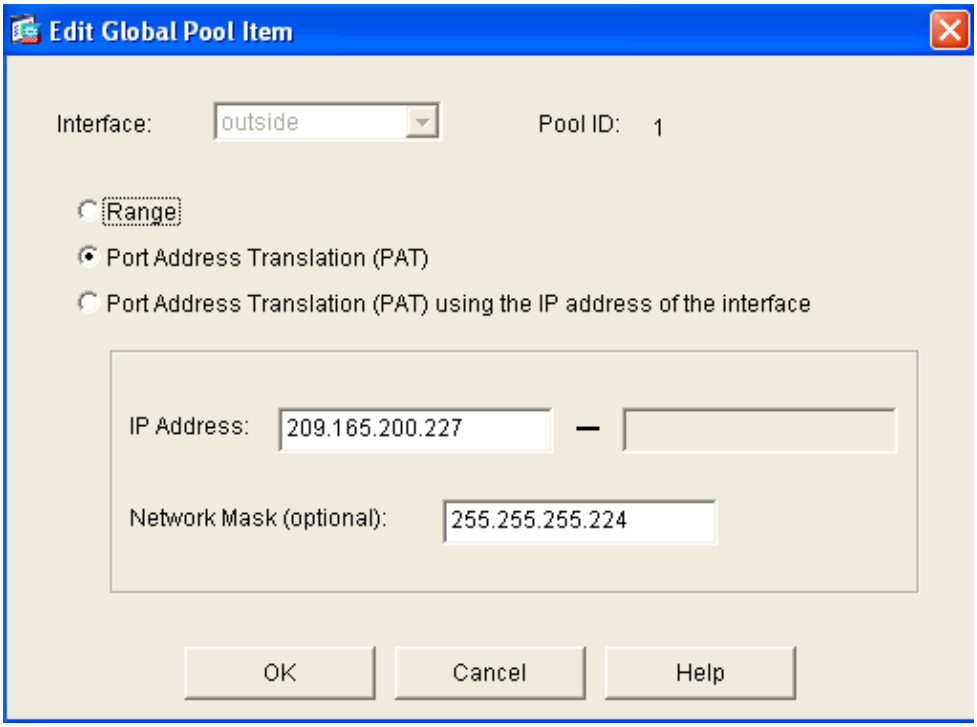
14. Select the outside Interface. Click **Add**.

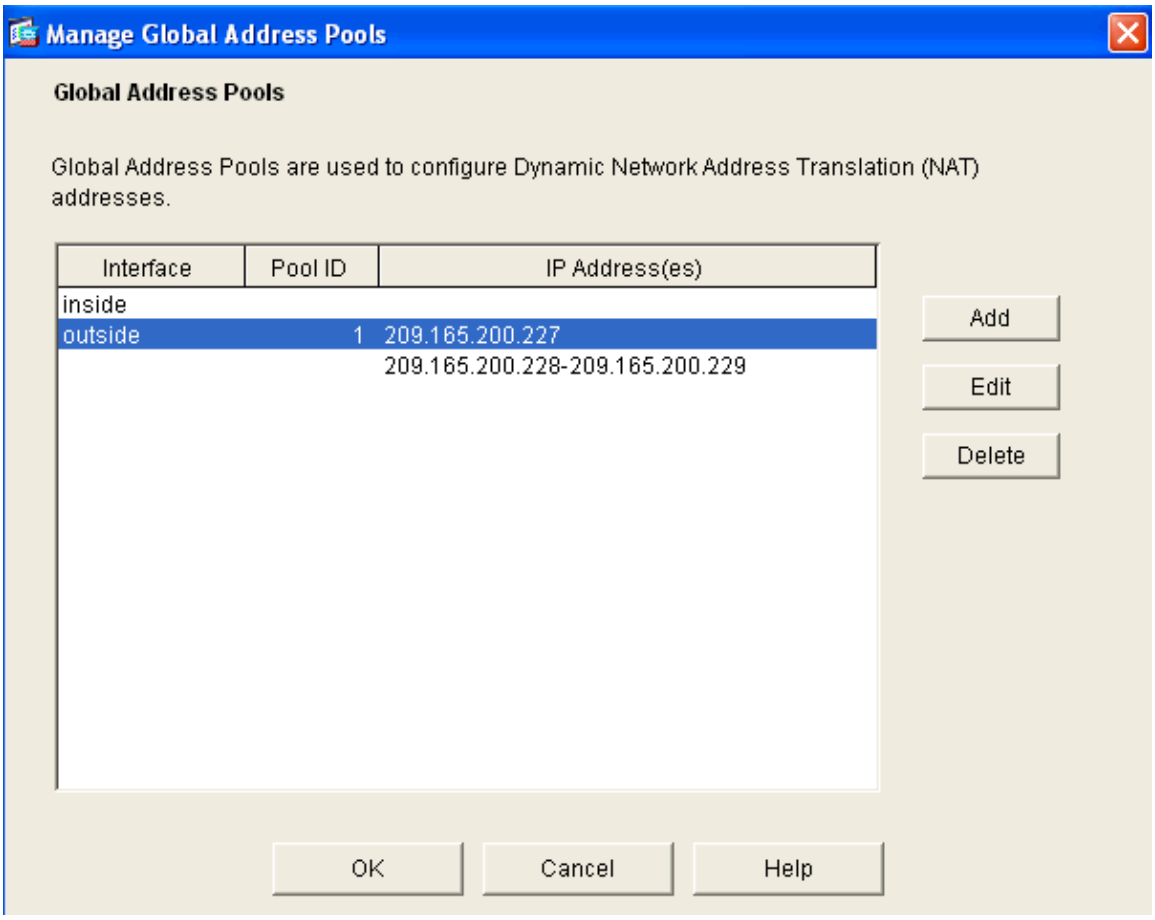


15. In this example, a Range and PAT Address Pool are configured. Configure the Range NAT Pool Address. Click **OK**.

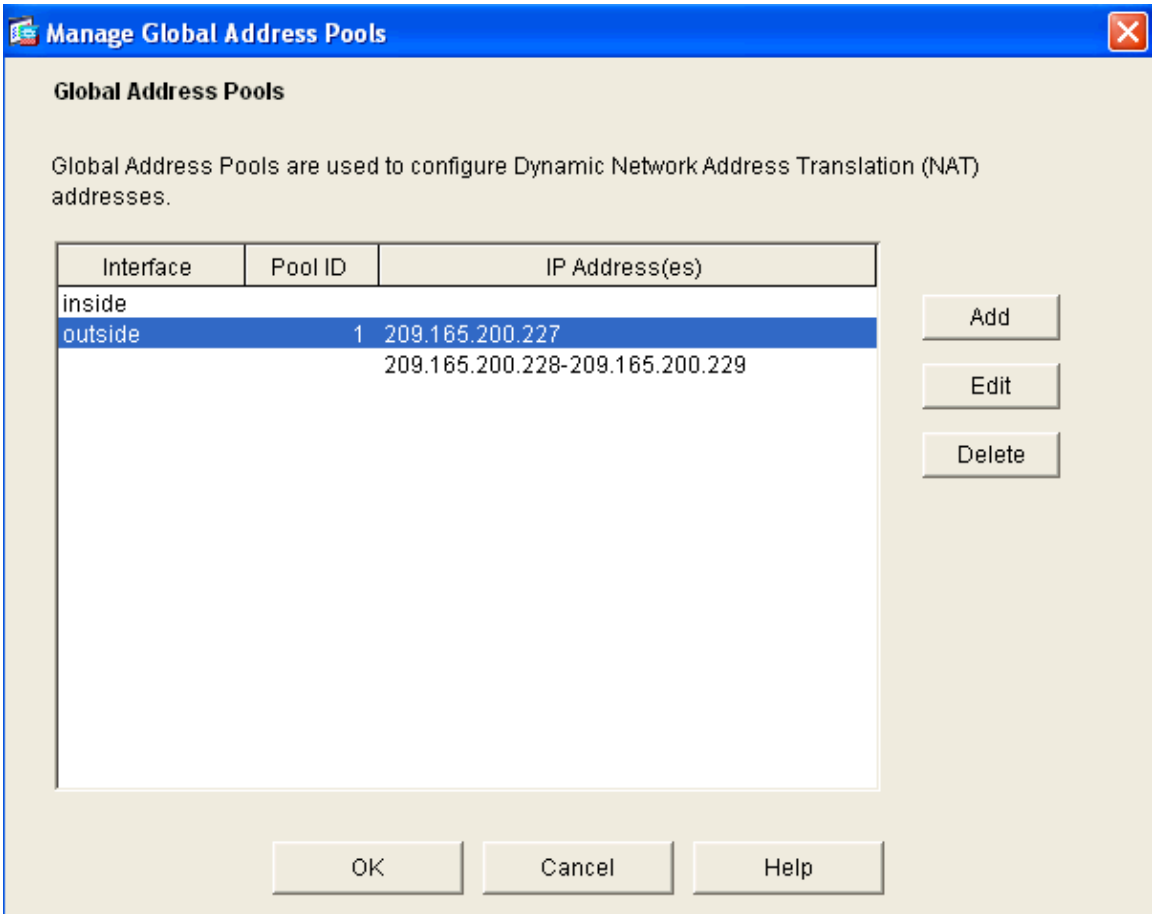


16. Configure the PAT Address Pool.

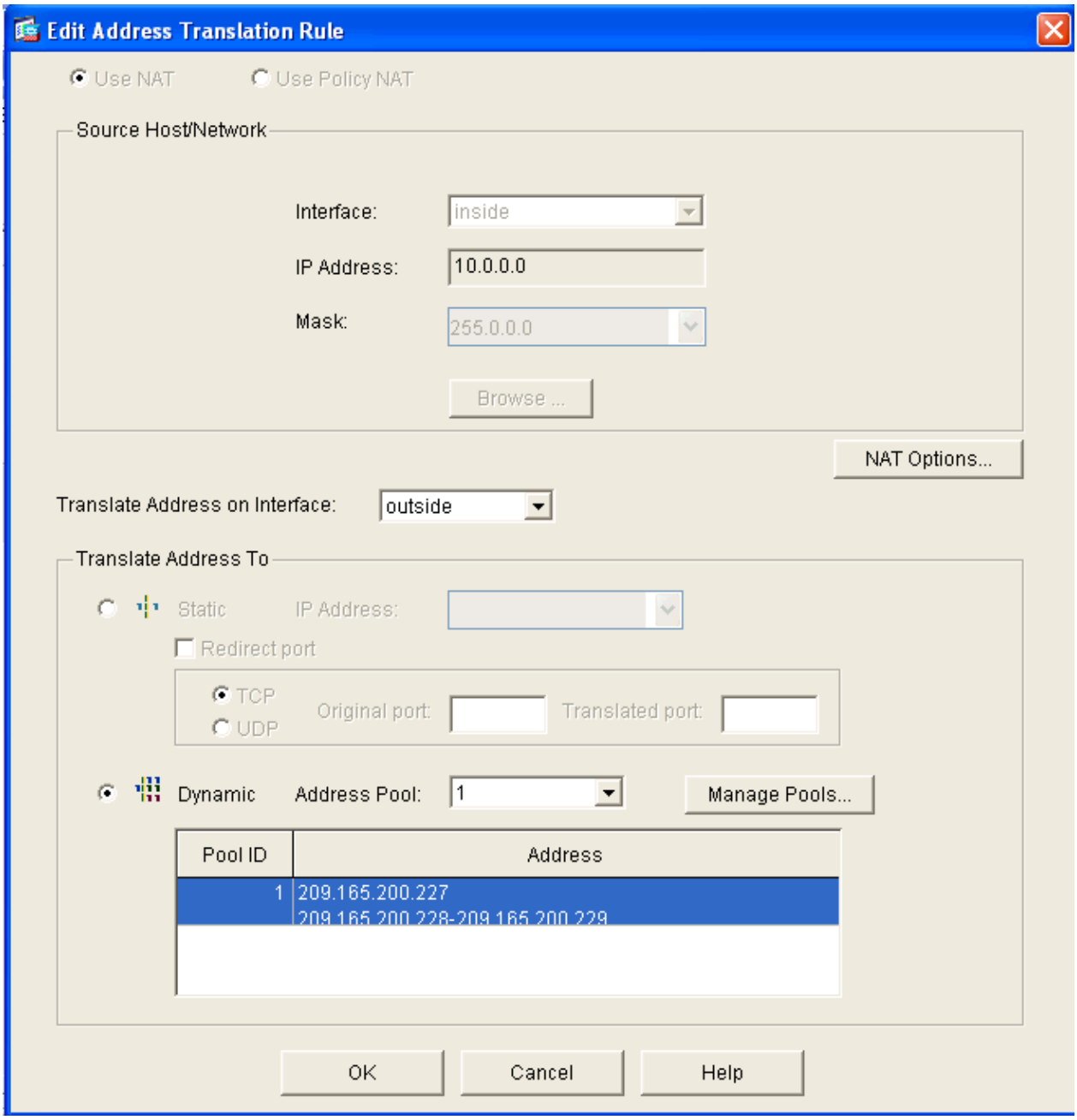

Edit Global Pool Item
Interface:
outside
Pool ID:
1
Range
Port Address Translation (PAT)
Port Address Translation (PAT) using the IP address of the interface
IP Address:
209.165.200.227
Network Mask (optional):
255.255.255.224
OK
Cancel
Help


Manage Global Address Pools
Global Address Pools
Global Address Pools are used to configure Dynamic Network Address Translation (NAT) addresses.
Interface
Pool ID
IP Address(es)
inside
outside
1
209.165.200.227
209.165.200.228-209.165.200.229
Add
Edit
Delete
OK
Cancel
Help

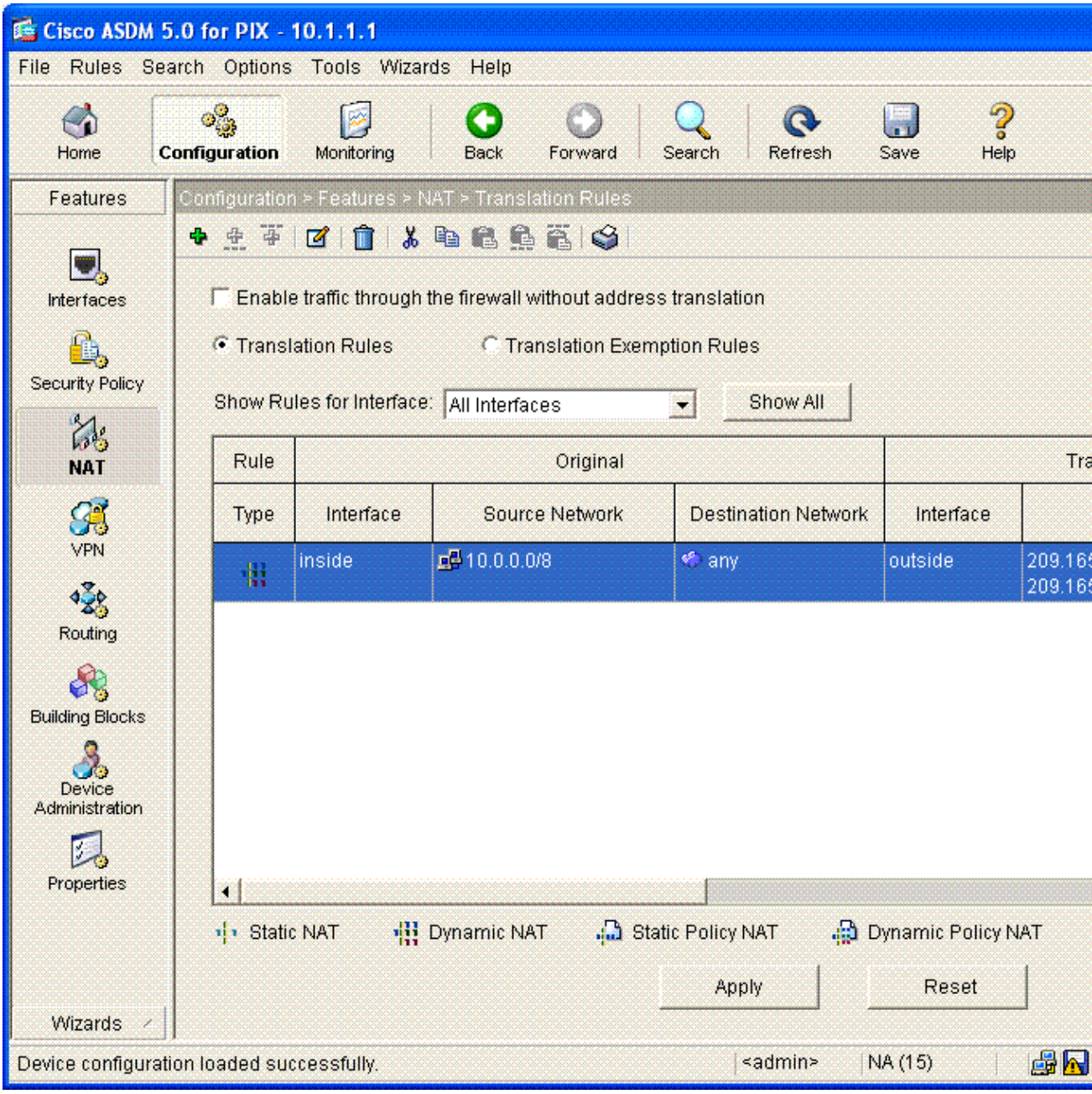
Click **OK**.



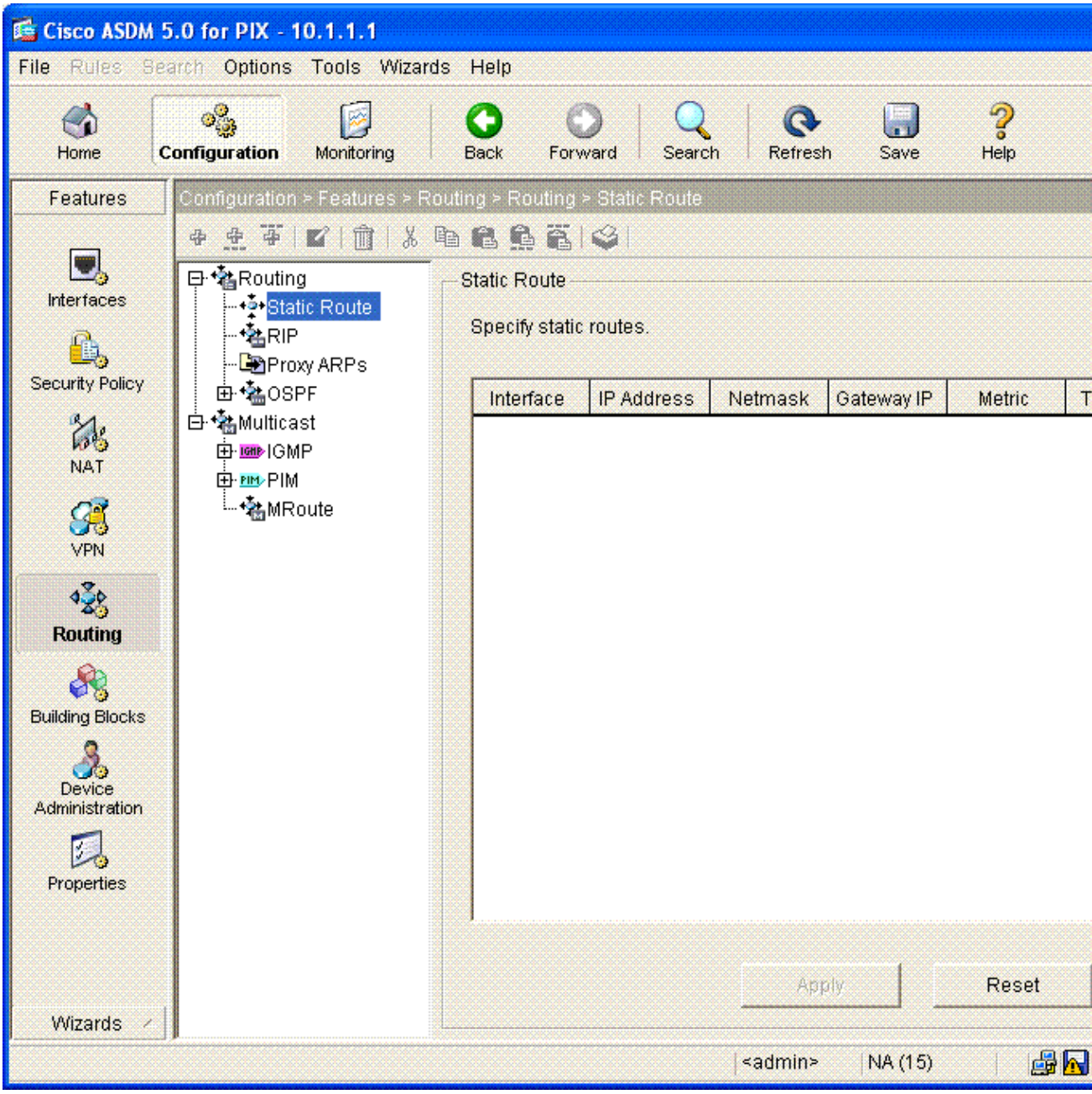
17. On the Edit Address Translation Rule, select the Pool Id to be used by the Source Network configured. Click **OK**.



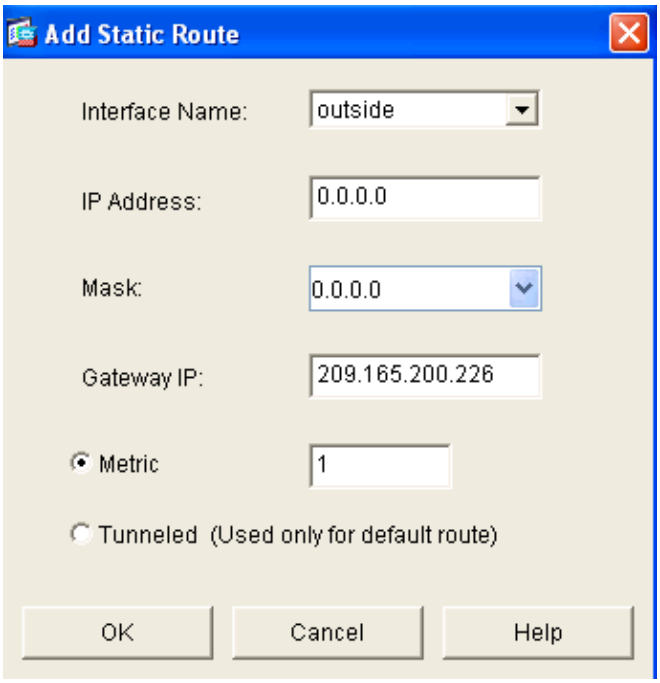
18. Click **Apply** to push the configured NAT Rule to the PIX.



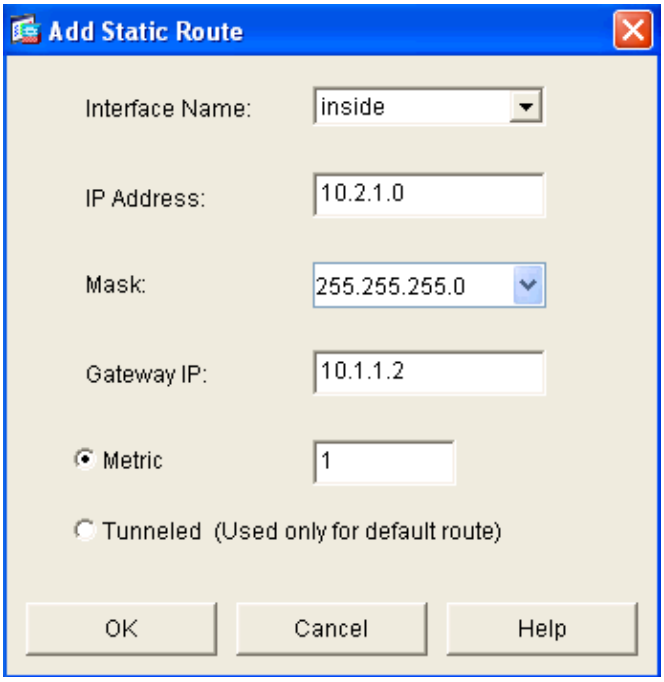
19. In this example, static routes are used. Choose Routing under the **Features** Tab. Choose **Static Route > Add**

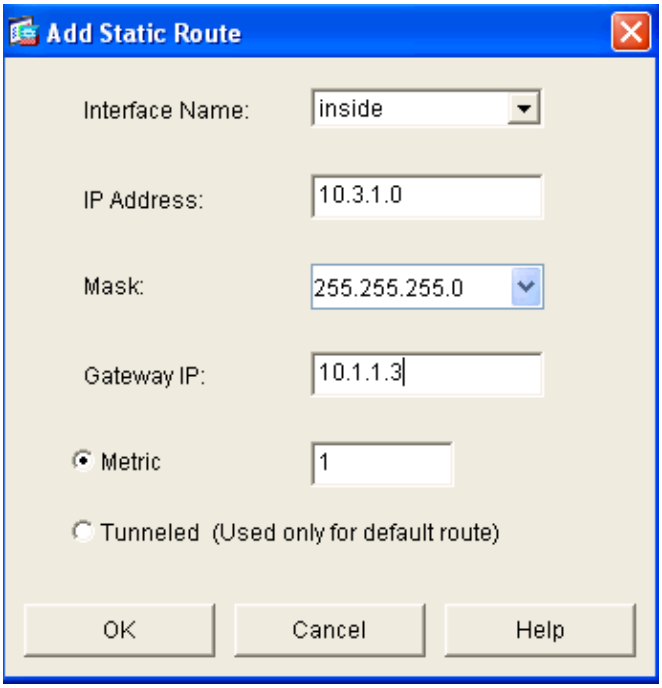


20. Configure the Default Gateway. Click **OK**.

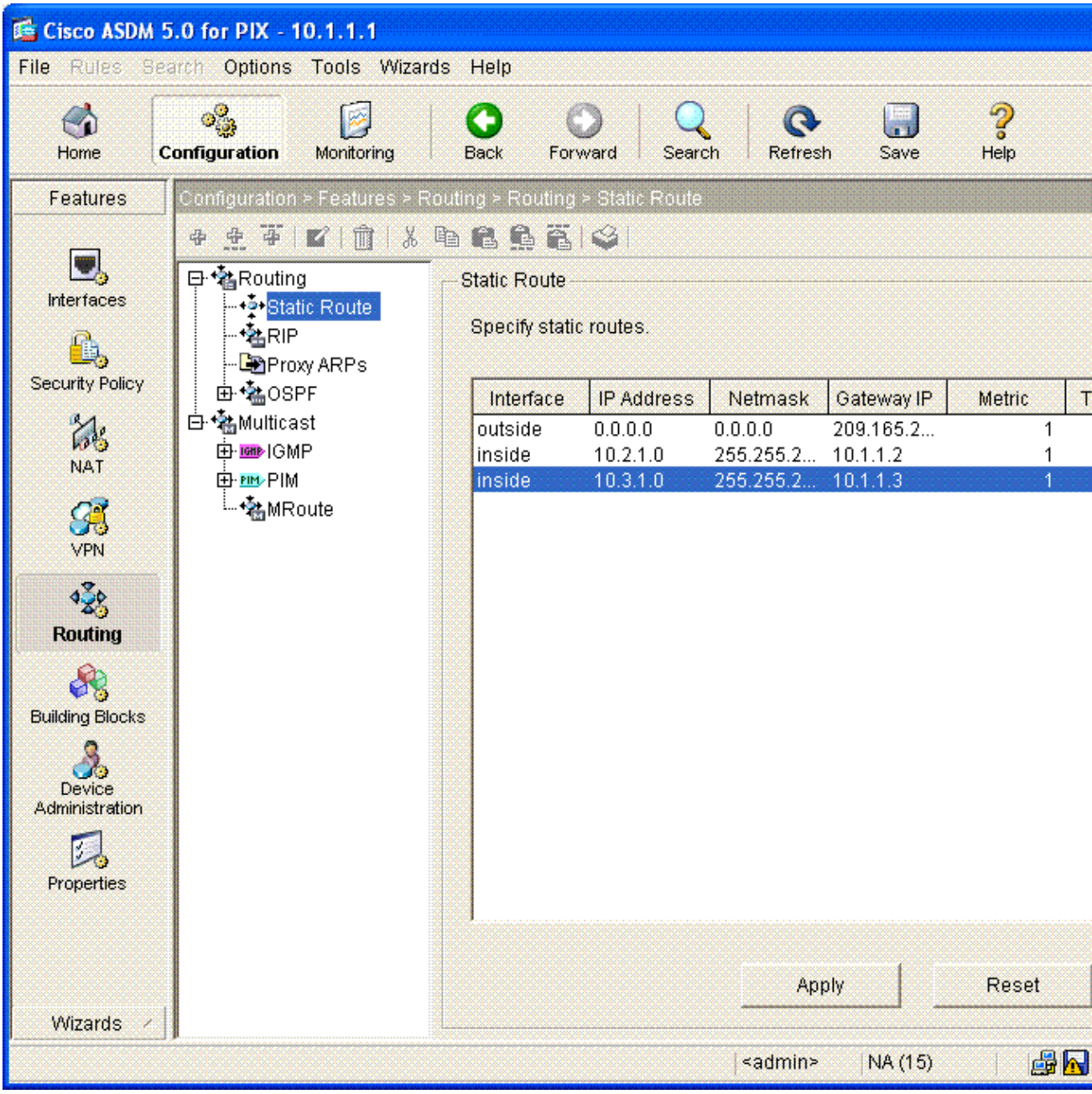


21. Click **Add**. Add the routes to the Inside Networks.





22. Confirm that the Correct Routes are configured. Click **Apply**.



Configuration via the ASDM GUI is now complete.

The following configuration is what you should see via the command line interface:

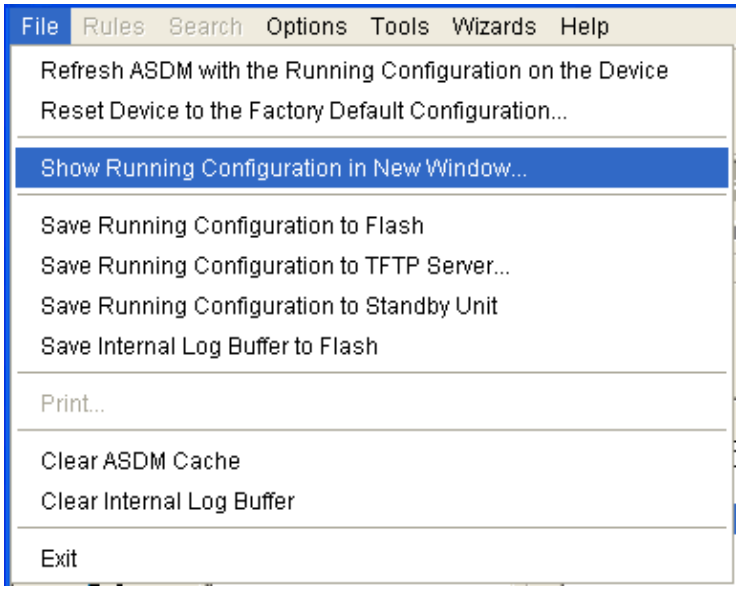
PIX Security Appliance Command Line Interface (CLI)

```
pixfirewall(config)# write terminal
PIX Version 7.0(0)102
names
!

interface Ethernet0
 nameif outside
 security-level 0
 ip address 209.165.200.225 255.255.255.224
!
```

```
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname OZ-PIX
domain-name cisco.com
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400

nat-control
global (outside) 1 209.165.200.228-209.165.200.229 netmask 255.255.255.224
global (outside) 1 209.165.200.227 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0
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
route outside 0.0.0.0 0.0.0.0 209.165.200.226 1
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
http 10.1.1.5 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!

class-map inspection_default
 match default-inspection-traffic
!
!
policy-map asa_global_fw_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy asa_global_fw_policy global
```

```
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5
: end
```

The resulting CLI configuration can be viewed in ASDM by choosing **File** > **Show Running Configuration in New Window**.



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Troubleshooting Commands

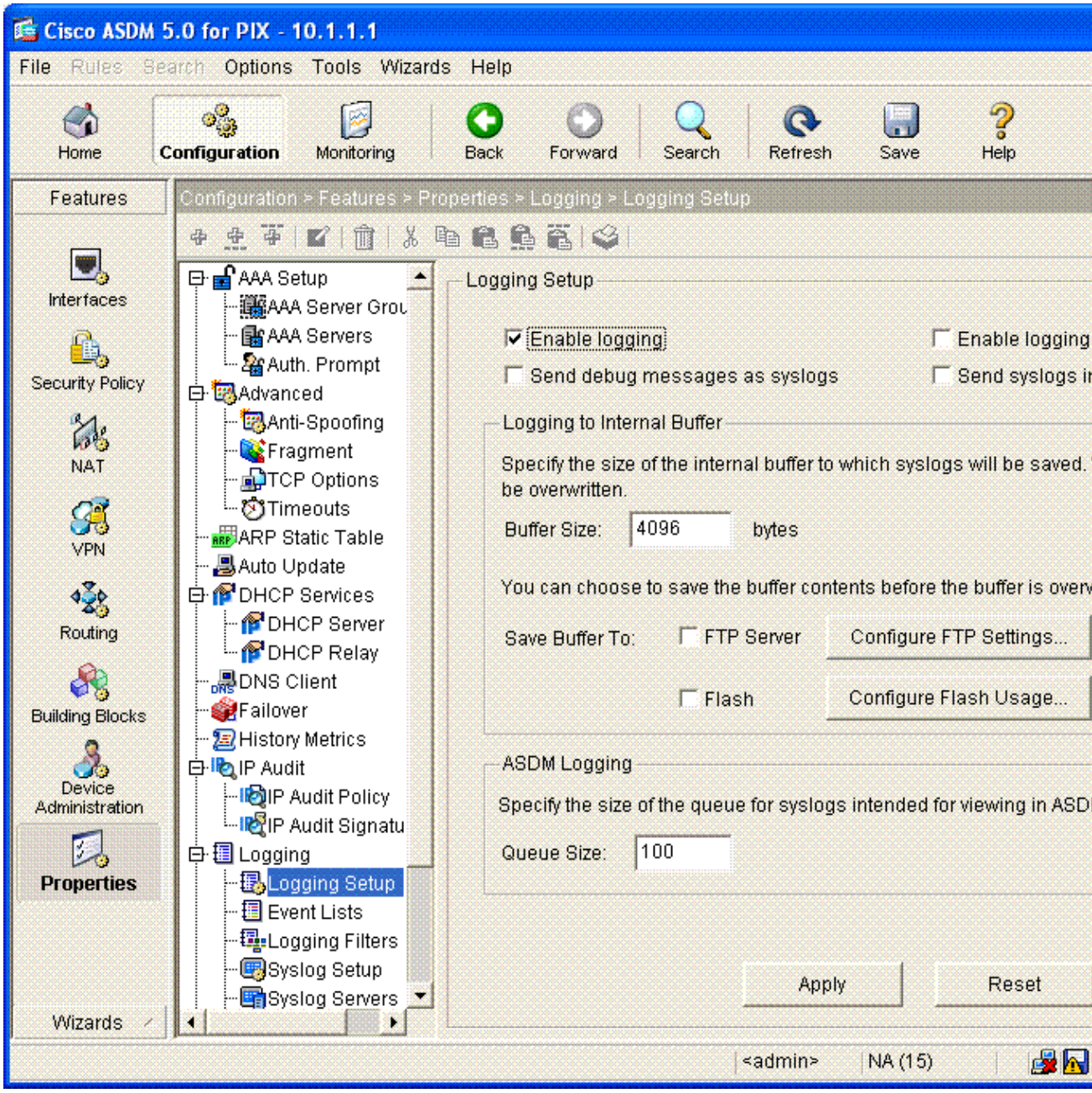
Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

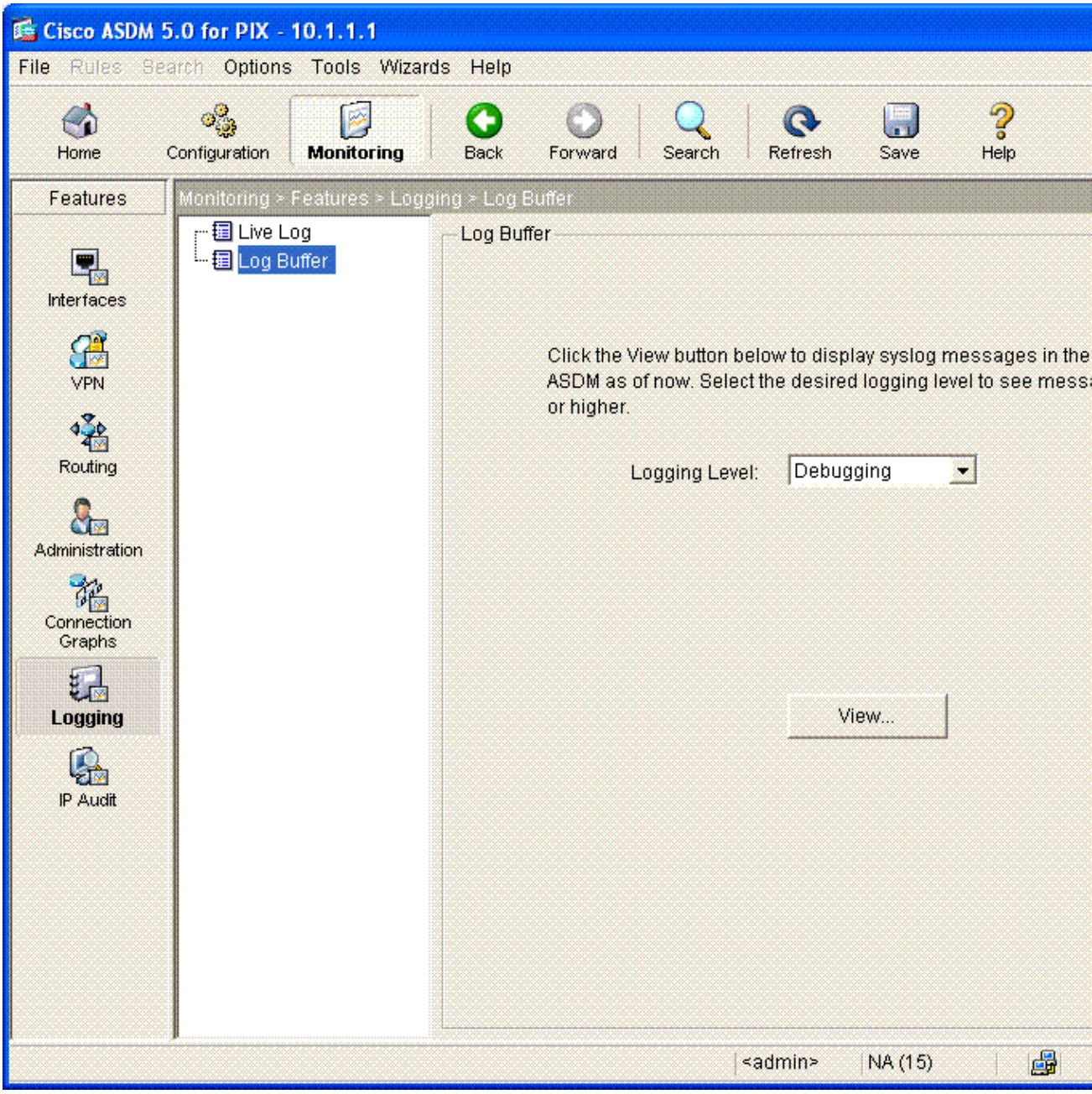
Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

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

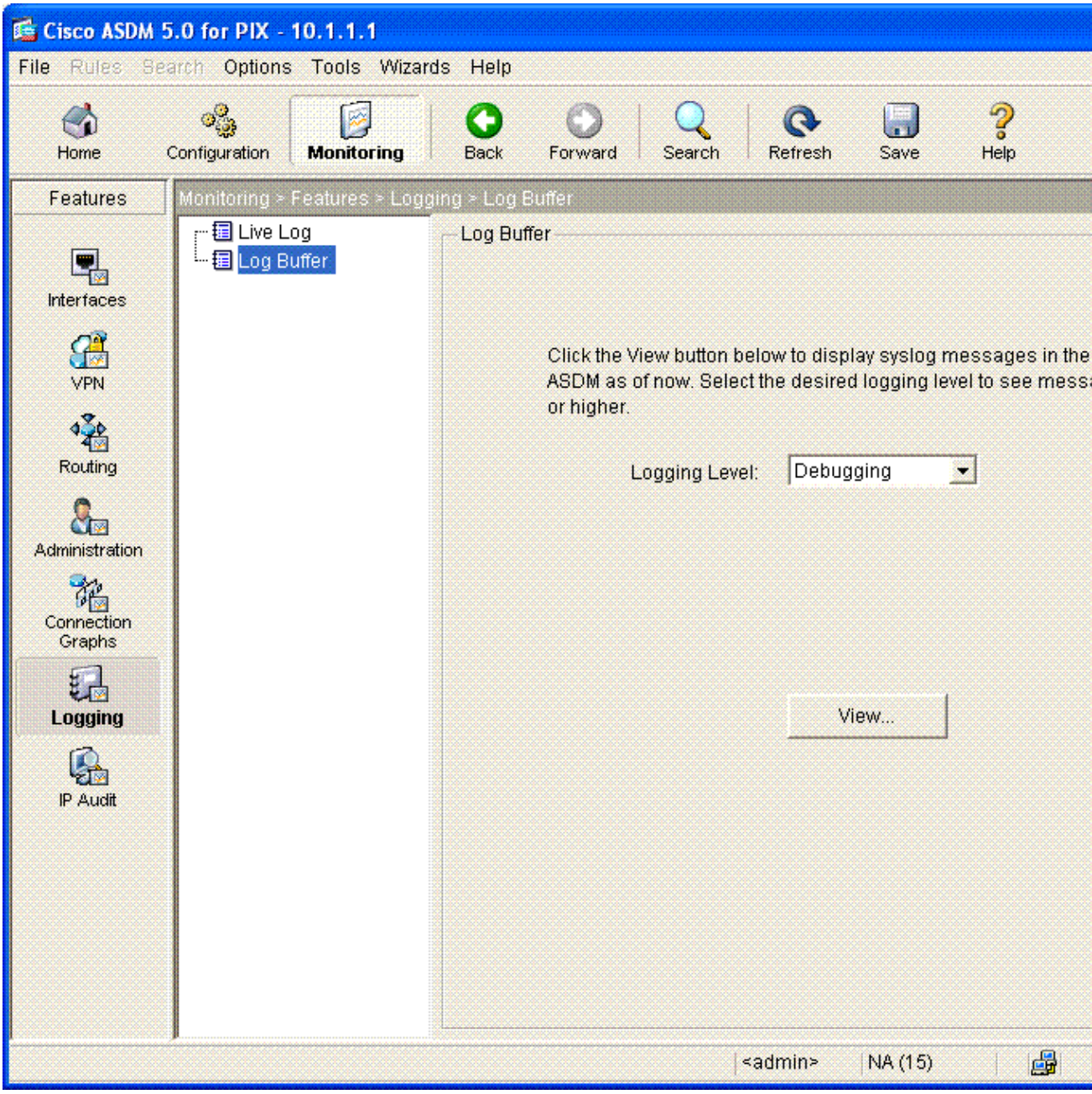
ASDM can be used to enable logging, and also to view the logs:

1. Choose **Configuration** > **Properties** > **Logging** > **Logging Setup**. Choose **Enable Logging**. Click **Apply**.

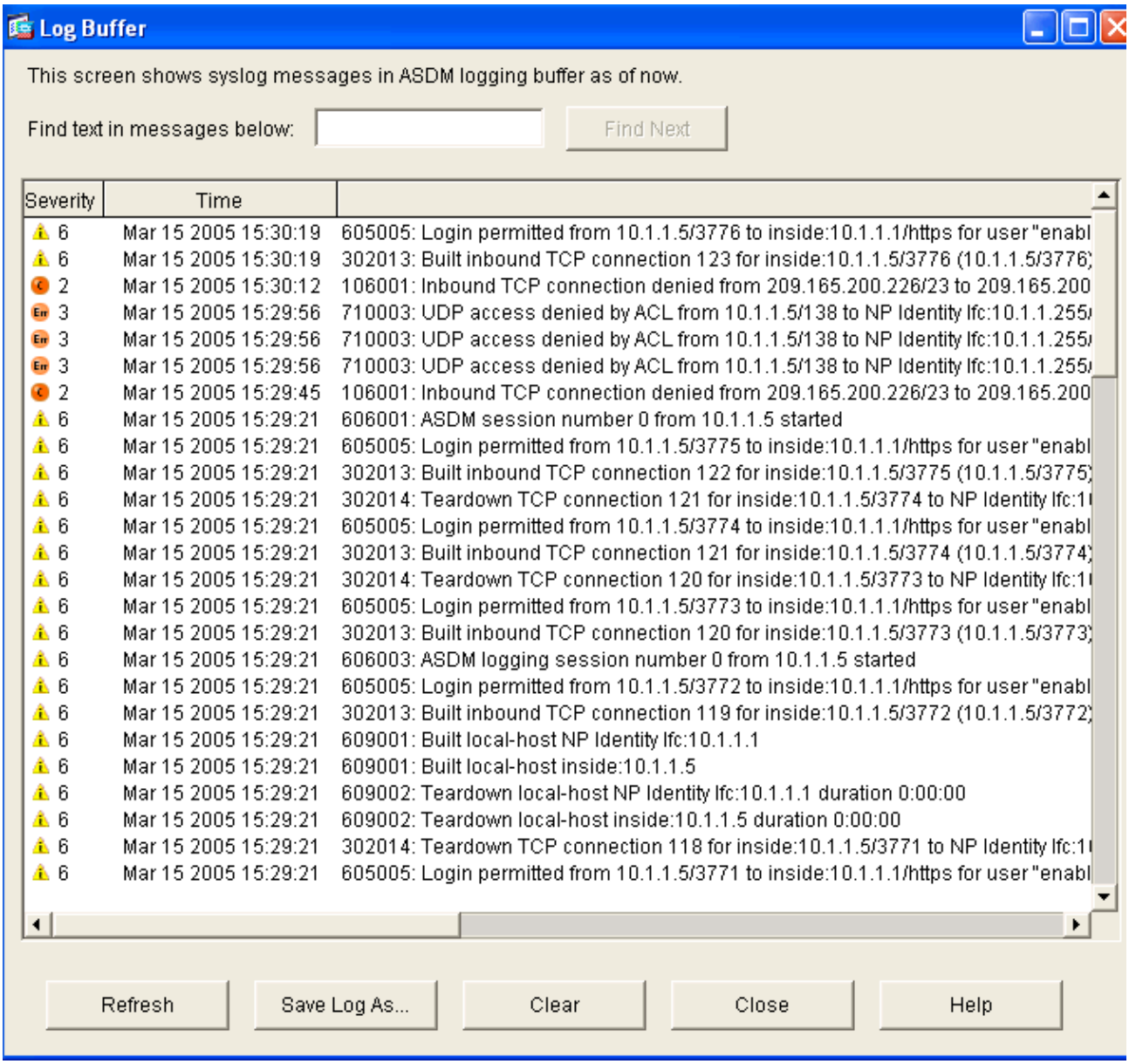

Cisco ASDM 5.0 for PIX - 10.1.1.1
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Features
Interfaces
Security Policy
NAT
VPN
Routing
Building Blocks
Device Administration
Properties
Wizards
Configuration > Features > Properties > Logging > Logging Setup
AAA Setup
AAA Server Grou
AAA Servers
Auth. Prompt
Advanced
Anti-Spoofing
Fragment
TCP Options
Timeouts
ARP Static Table
Auto Update
DHCP Services
DHCP Server
DHCP Relay
DNS Client
Failover
History Metrics
IP Audit
IP Audit Policy
IP Audit Signatu
Logging
Logging Setup
Event Lists
Logging Filters
Syslog Setup
Syslog Servers
Logging Setup
Enable logging
Enable logging
Send debug messages as syslogs
Send syslogs i
Logging to Internal Buffer
Specify the size of the internal buffer to which syslogs will be saved.
be overwritten.
Buffer Size: 4096 bytes
You can choose to save the buffer contents before the buffer is overw
Save Buffer To: FTP Server
Configure FTP Settings...
Flash
Configure Flash Usage...
ASDM Logging
Specify the size of the queue for syslogs intended for viewing in ASD
Queue Size: 100
Apply
Reset
<admin>
NA (15)



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



3. Here is an exampe of the Log Buffer.



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 Security Appliance Technical Support and Documentation**
- **Cisco Adaptive Security Device Manager (ASDM) Troubleshoot and Alerts**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**

Updated: May 09, 2005 Document ID: 63880