Table of Contents

IPSec Tunnel through a PIX Firewall (Version 7.0) with NAT Configuration Example

Document ID: 63881

Introduction

This sample configuration demonstrates an IPSec tunnel through a firewall that performs network address translation (NAT). **This configuration does not work with port address translation (PAT) if you use Cisco IOS® Software Releases prior to and not including 12.2(13)T.** This type of configuration can be used to tunnel IP traffic. This configuration cannot be used to encrypt traffic that does not go through a firewall, such as IPX or routing updates. Generic routing encapsulation (GRE) tunneling is a more appropriate choice. In this example, the Cisco 2621 and 3660 routers are the IPSec tunnel endpoints that join two private networks, with conduits or access control lists (ACLs) on the PIX in between in order to allow the IPSec traffic.

Note: NAT is a one−to−one address translation, not to be confused with PAT, which is a many (inside the firewall)−to−one translation. For more information on NAT operation and configuration, refer to Verifying NAT Operation and Basic NAT Troubleshooting or How NAT Works.

Note: IPSec with PAT may not work properly because the outside tunnel endpoint device cannot handle multiple tunnels from one IP address. Contact your vendor in order to determine if the tunnel endpoint devices work with PAT. Additionally, in Cisco IOS Software Release 12.2(13)T and later, the NAT Transparency feature can be used for PAT. For more details, refer to IPSec NAT Transparency. Refer to Support for IPSec ESP Through NAT in order to learn more about these features in Cisco IOS Software Release 12.2(13)T and later.

Note: Before you open a case with Cisco Technical Support, refer to NAT Frequently Asked Questions, which has many answers to common questions.

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:

- Cisco IOS Software Release 12.0.7.T (up to but not including Cisco IOS Software Release 12.2(13)T)

  For more recent versions, refer to IPSec NAT Transparency.
- Cisco 2621 router
- Cisco 3660 router
- Cisco PIX Firewall

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.

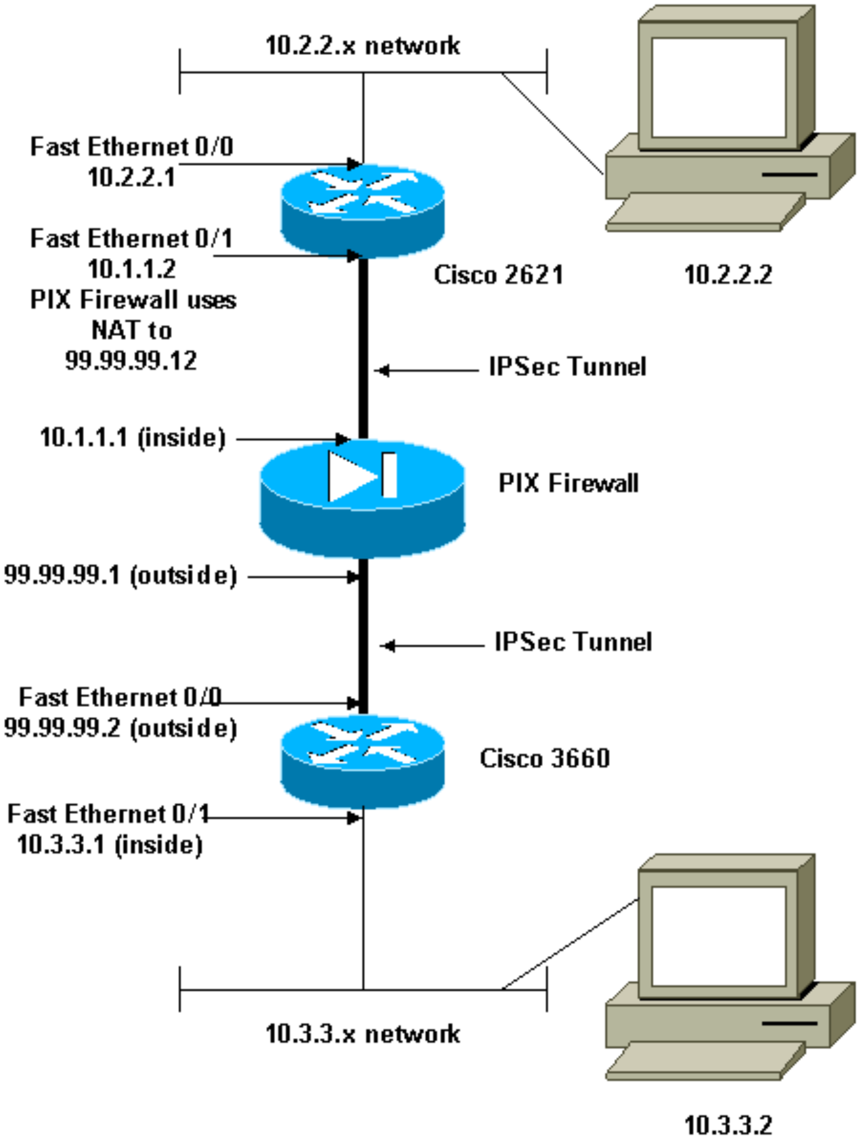
Configure

This section presents you with the information you can use to configure the features this document describes.

Note: In order to find additional information on the commands this document uses, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- Cisco 2621 Configuration
- Cisco 3660 Configuration
- PIX Firewall (Version 7.0) Configuration
    - Advanced Security Device Manager GUI (ASDM)
    - Command Line Interface (CLI)

Cisco 2621

```
Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !

!--- The IKE policy.

 crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 99.99.99.2
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/1


!--- IPSec policy.


 crypto map mymap 10 ipsec-isakmp
  set peer 99.99.99.2
  set transform-set myset


!--- Include the private-network-to-private-network traffic
 !--- in the encryption process.


  match address 101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto


!--- Apply to the interface.


  crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server


!--- Include the private-network-to-private-network traffic
 !--- in the encryption process.
 access-list 101 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
 end
```

Cisco 3660

```
version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !


!--- The IKE policy.


 crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 99.99.99.12
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/0


!--- The IPSec policy.


 crypto map mymap 10 ipsec-isakmp
  set peer 99.99.99.12
  set transform-set myset


!--- Include the private-network-to-private-network traffic
 !--- in the encryption process.


  match address 101
 !
 interface FastEthernet0/0
  ip address 99.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto


!--- Apply to the interface.
```

```
  crypto map mymap
 !
 interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
 !
 interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
 !
 interface Ethernet3/1
  no ip address
  no ip directed-broadcast
 interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
 !


!--- The pool from which inside hosts translate to
 !--- the globally unique 99.99.99.0/24 network.


 ip nat pool OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0


!--- Except the private network from the NAT process.


 ip nat inside source route-map nonat pool OUTSIDE
 ip classless
 ip route 0.0.0.0 0.0.0.0 99.99.99.1
 no ip http server
 !


!--- Include the private-network-to-private-network traffic
 !--- in the encryption process.


 access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any


!--- Except the private network from the NAT process.
```

```
access−list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access−list 110 permit ip 10.3.3.0 0.0.0.255 any
route−map nonat permit 10
 match ip address 110
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
end
```

PIX Firewall (Version 7.0) Configuration

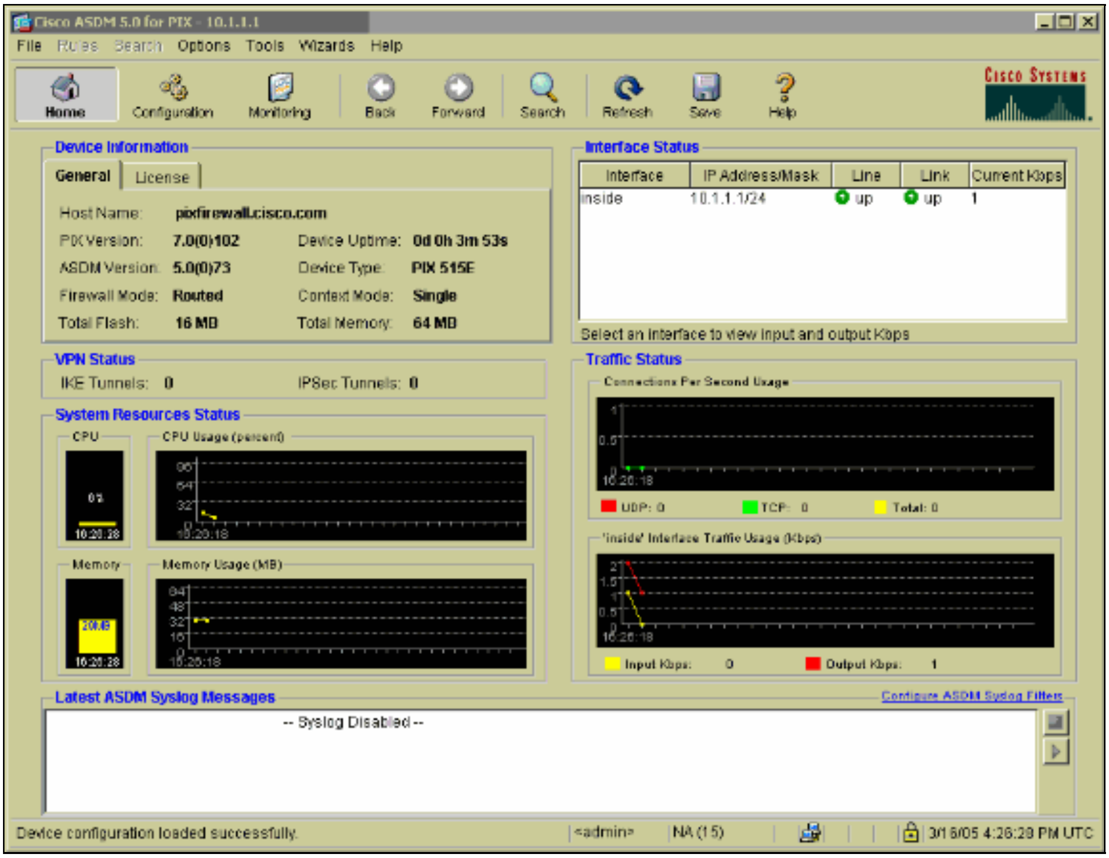
Complete these steps in order to configure PIX Firewall Version 7.0.

1. Console into the PIX. From a cleared configuration, use the interactive prompts to enable **Advanced Security Device Manager GUI (ASDM)** for the management of the PIX from the Workstation 10.1.1.3.

   PIX Firewall ASDM Bootstrap

   ```
   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: pix−firewall
   Domain name: cisco.com
   IP address of host running Device Manager: 10.1.1.3
   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: 10.1.1.3
   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
   ```
2. From Workstation 10.1.1.3, open up a Web Browser and use ADSM (in this example, https://10.1.1.1).
3. Select **Yes** on the certificate prompts and login with the enable password as configured in the PIX Firewall ASDM Bootstrap configuration.
4. If this is the first time ASDM is run on the PC, it prompts you whether to use ASDM Launcher, or use ASDM as a Java App.

   In this example, the ASDM Launcher is selected and installed following the prompts.
5. Proceed to the ASDM Home screen and select the Configuration tab.


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
Cisco Systems
Device Information
General License
Interface Status
VPN Status
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Traffic Status
Connections Per Second Usage
'inside' Interface Traffic Usage (Kbps)
Latest ASDM Syslog Messages
Configure ASDM Syslog Filters

Host Name: pixfirewall.cisco.com

PIX Version: 7.0(0)102 Device Uptime: 0d 0h 3m 53s

ASDM Version: 5.0(0)73 Device Type: PIX 515E

Firewall Mode: Routed Context Mode: Single

Total Flash: 16 MB Total Memory: 64 MB

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	● up	● up	1

Select an interface to view input and output Kbps

IKE Tunnels: 0 IPSec Tunnels: 0

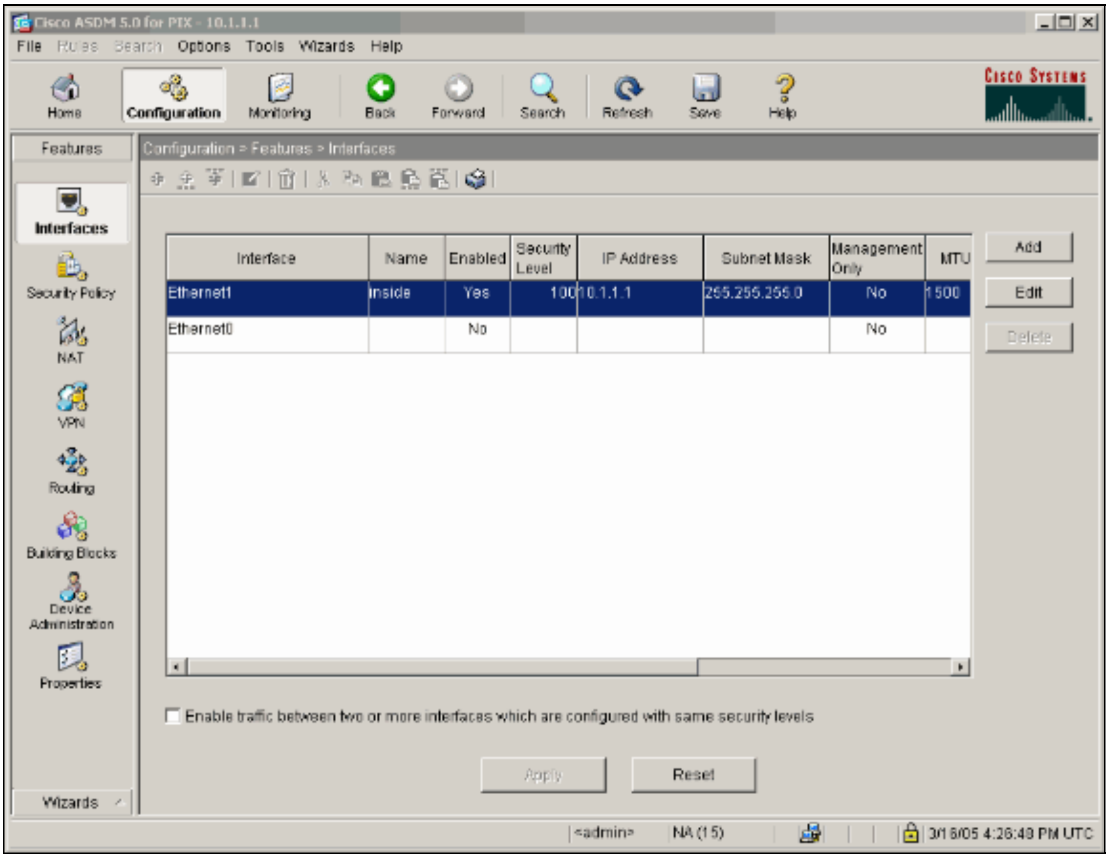
🟥 UDP: 0 🟩 TCP: 0 🟨 Total: 0

🟨 Input Kbps: 0 🟥 Output Kbps: 1

-- Syslog Disabled --

Device configuration loaded successfully. <admin> NA (15) 3/16/05 4:26:28 PM UTC

6. Highlight the **Ethernet 0 Interface** and select **Edit** in order to configure the Outside Interface.


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
Cisco Systems
Features
Interfaces
Security Policy
NAT
VPN
Routing
Building Blocks
Device Administration
Properties
Wizards
Add
Edit
Delete
Apply
Reset

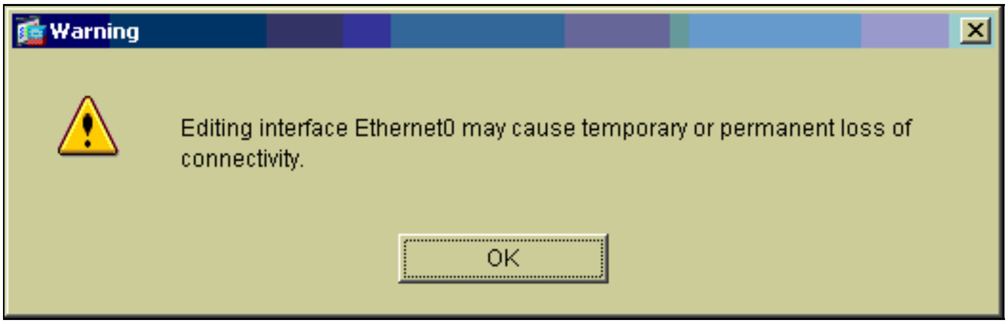
Configuration > Features > Interfaces

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

☐ Enable traffic between two or more interfaces which are configured with same security levels

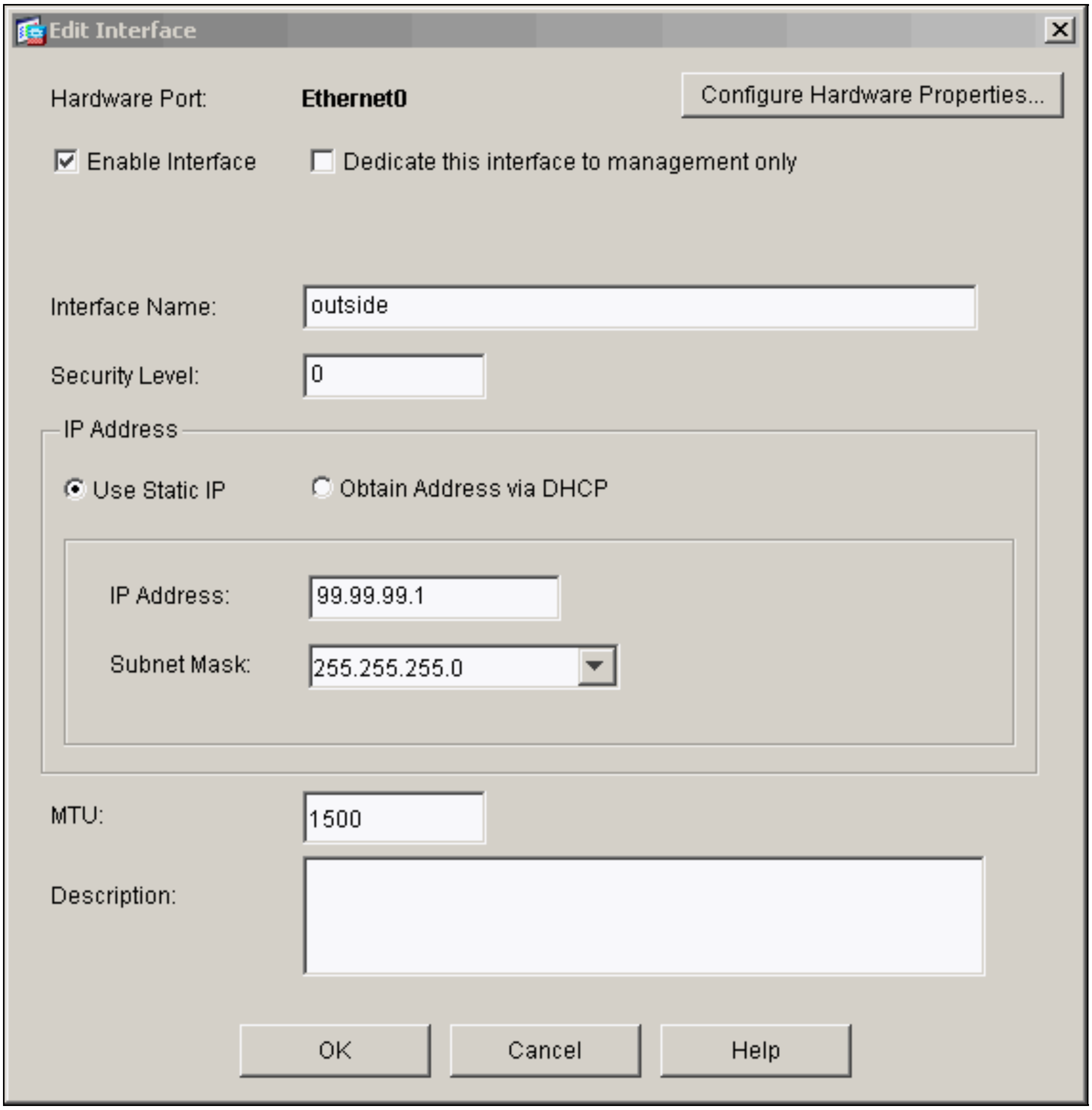
<admin> NA (15) 3/16/05 4:26:48 PM UTC

7. Click **OK** at the Editing interface prompt.



Editing interface Ethernet0 may cause temporary or permanent loss of connectivity.

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



Hardware Port: Ethernet0

☑ Enable Interface ☐ Dedicate this interface to management only

Interface Name: outside

Security Level: 0

IP Address

● Use Static IP ○ Obtain Address via DHCP

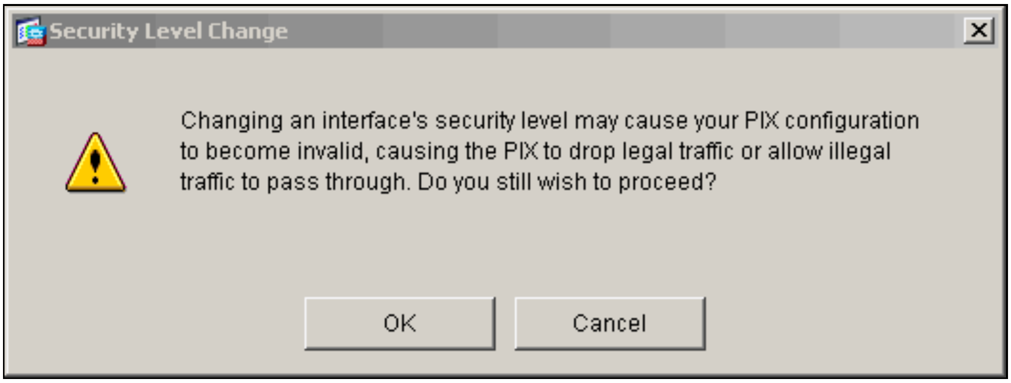
IP Address: 99.99.99.1

Subnet Mask: 255.255.255.0

MTU: 1500

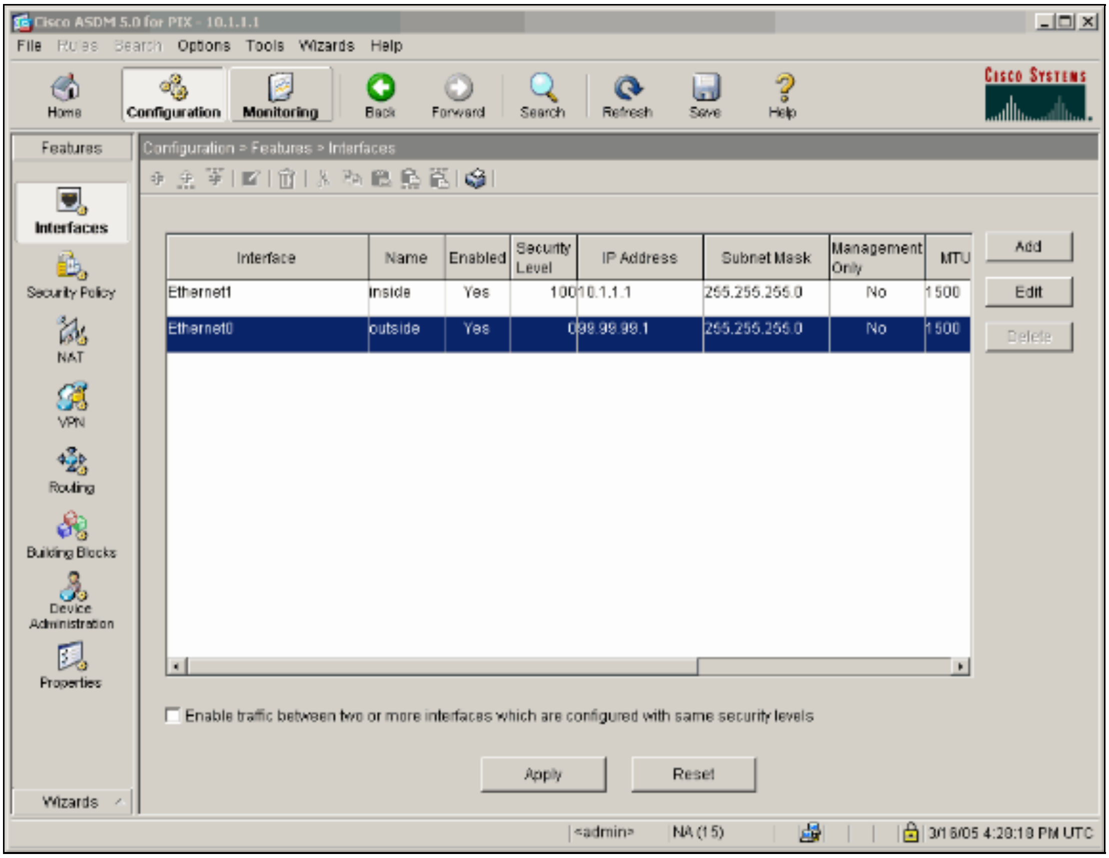
Description:

9. Click **OK** at the Changing an Interface Prompt.



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?

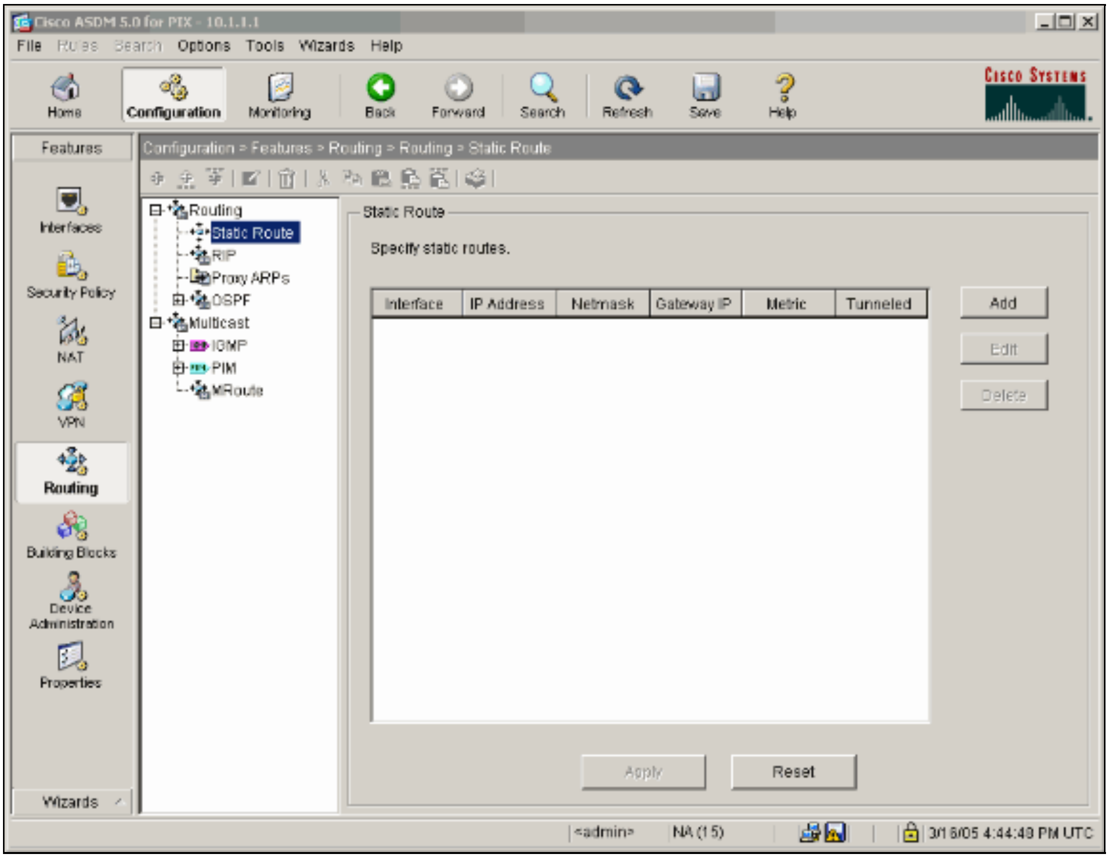
10. Click **Apply** in order to accept the interface configuration. The configuration also gets pushed onto the PIX. This example uses static routes.



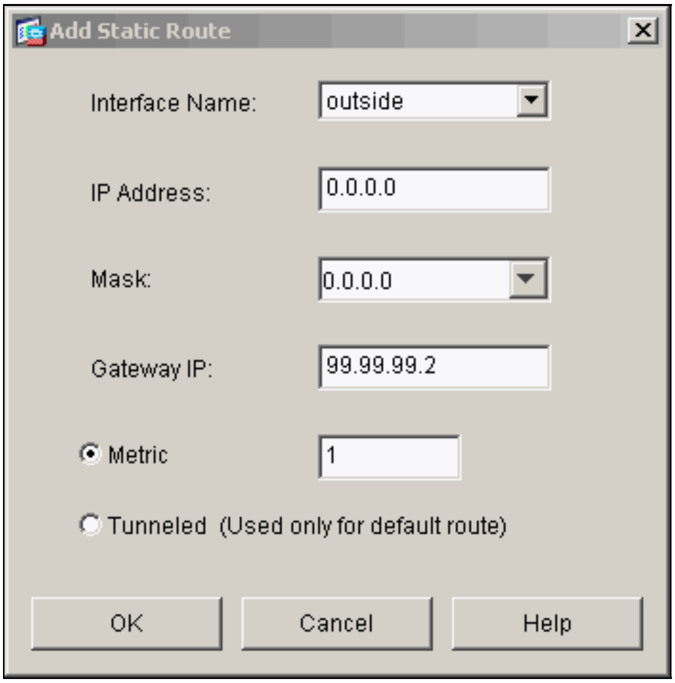
Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No	1500
Ethernet0	outside	Yes	0	99.99.99.1	255.255.255.0	No	1500

□ Enable traffic between two or more interfaces which are configured with same security levels

11. Select **Routing** under the Features tab, highlight **Static Route**, and click **Add**.



12. Configure the default Gateway and click **OK**.



Add Static Route

Interface Name: outside

IP Address: 0.0.0.0

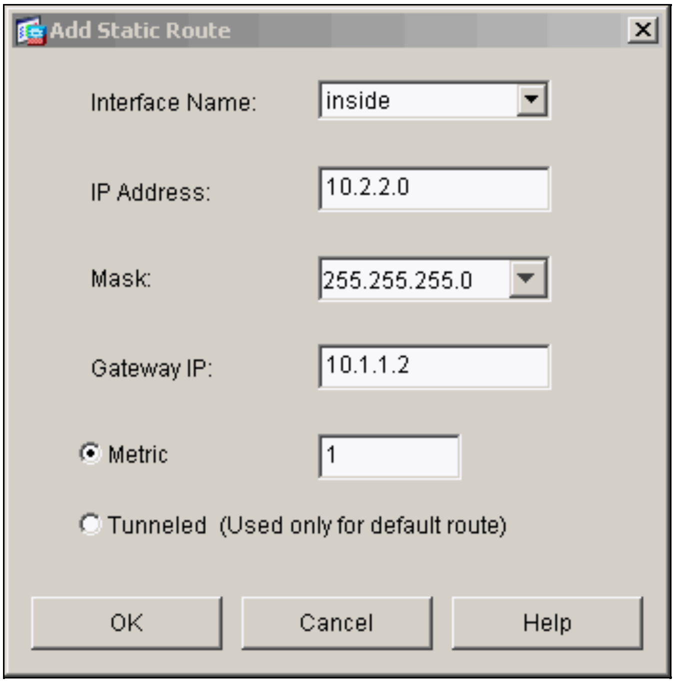
Mask: 0.0.0.0

Gateway IP: 99.99.99.2

● Metric 1

○ Tunneled (Used only for default route)

13. Click **Add** and add the routes to the Inside networks.



Add Static Route

Interface Name: inside

IP Address: 10.2.2.0

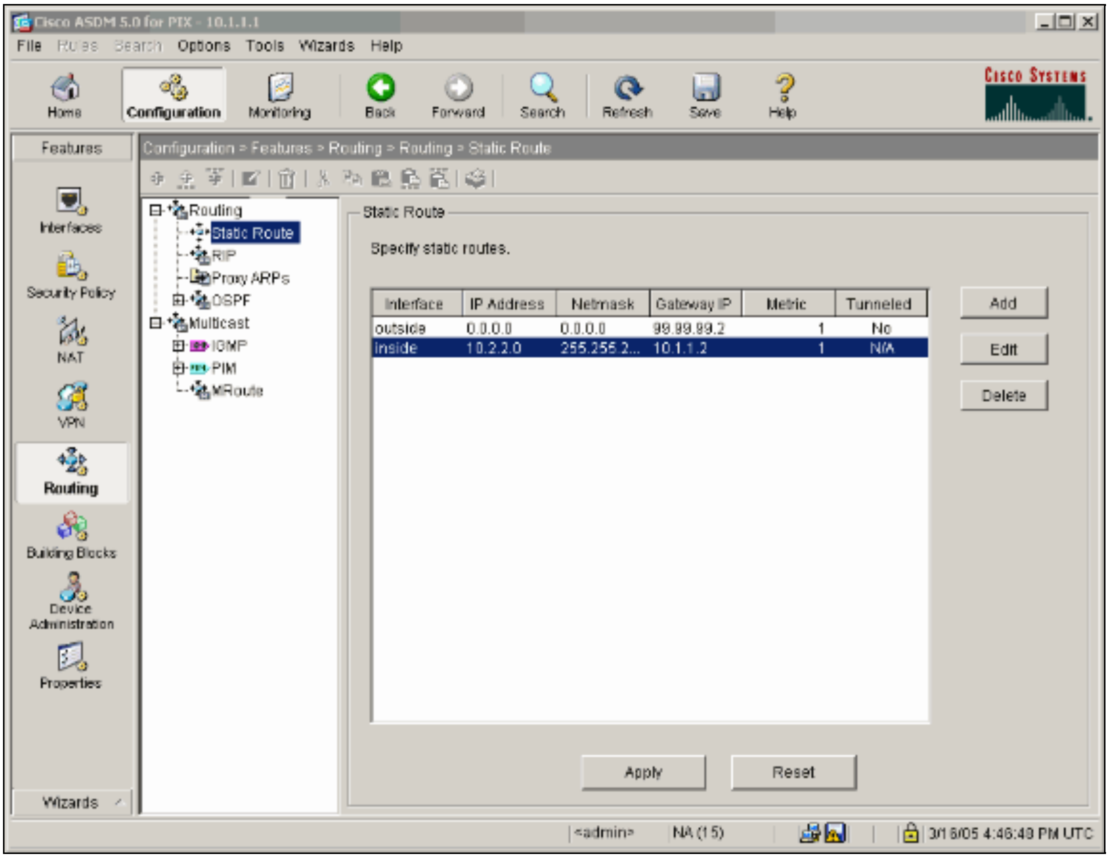
Mask: 255.255.255.0

Gateway IP: 10.1.1.2

● Metric 1

○ Tunneled (Used only for default route)

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



Cisco ASDM 5.0 for PIX - 10.1.1.1

Configuration > Features > Routing > Routing > Static Route

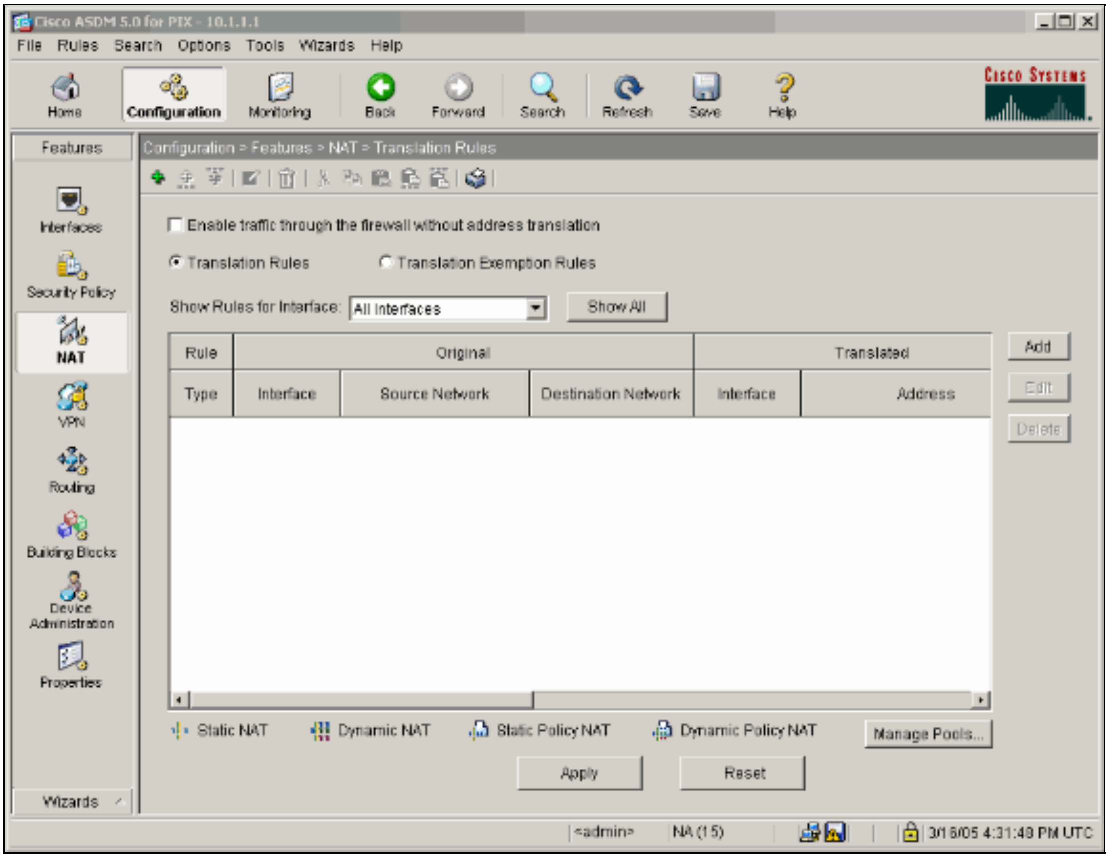
Static Route

Specify static routes.

Interface	IP Address	Netmask	Gateway IP	Metric	Tunneled
outside	0.0.0.0	0.0.0.0	99.99.99.2	1	No
inside	10.2.2.0	255.255.2...	10.1.1.2	1	N/A

<admin> NA (15) 3/16/05 4:46:49 PM UTC

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



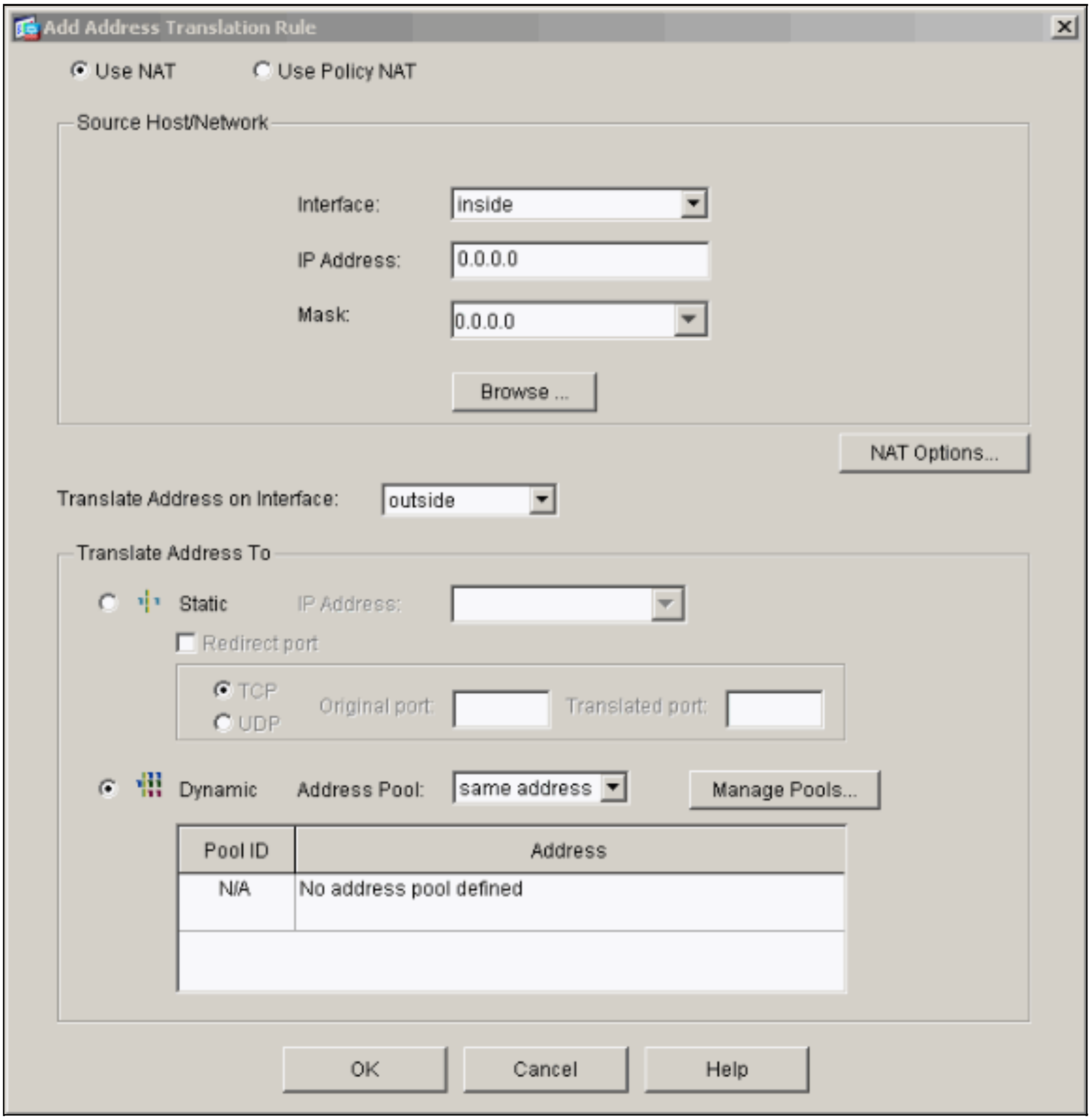
□ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address

16. Configure the Source Network (this example uese any). Then click **Manage Pools** in order to define the PAT.



● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 0.0.0.0

Mask: 0.0.0.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

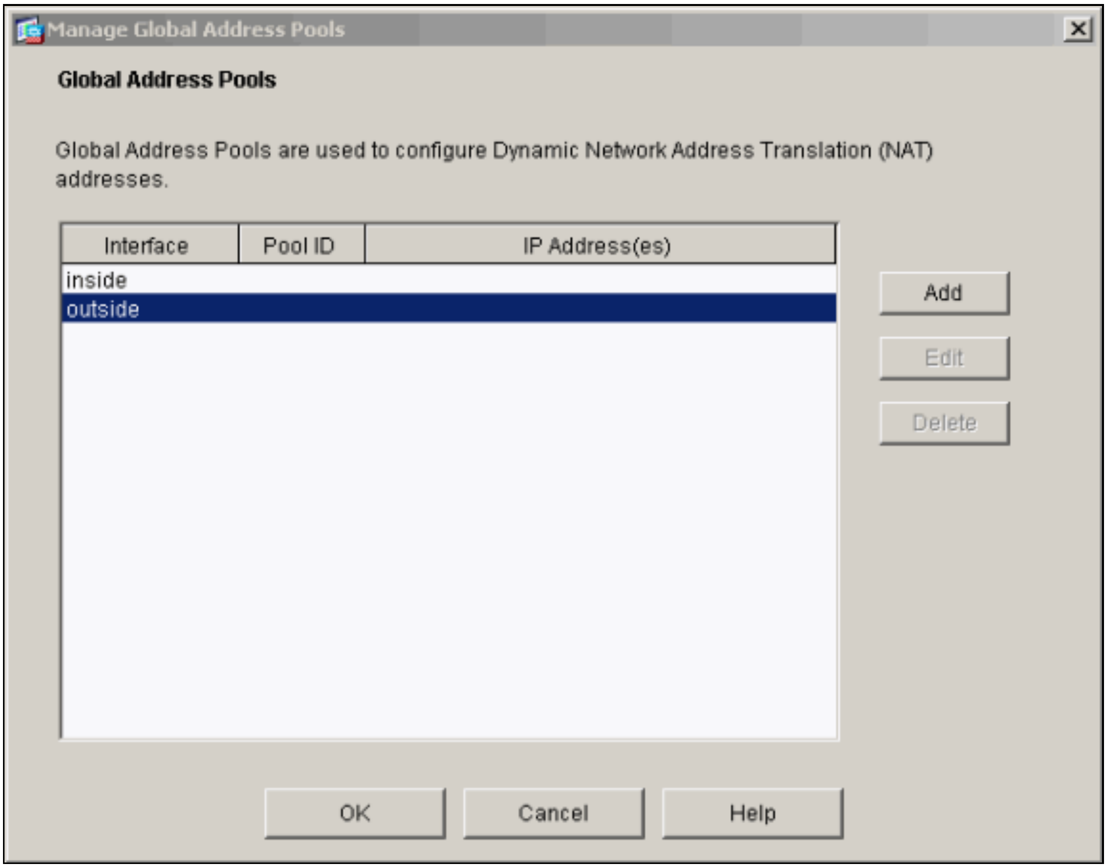
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: same address

Pool ID	Address
N/A	No address pool defined

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



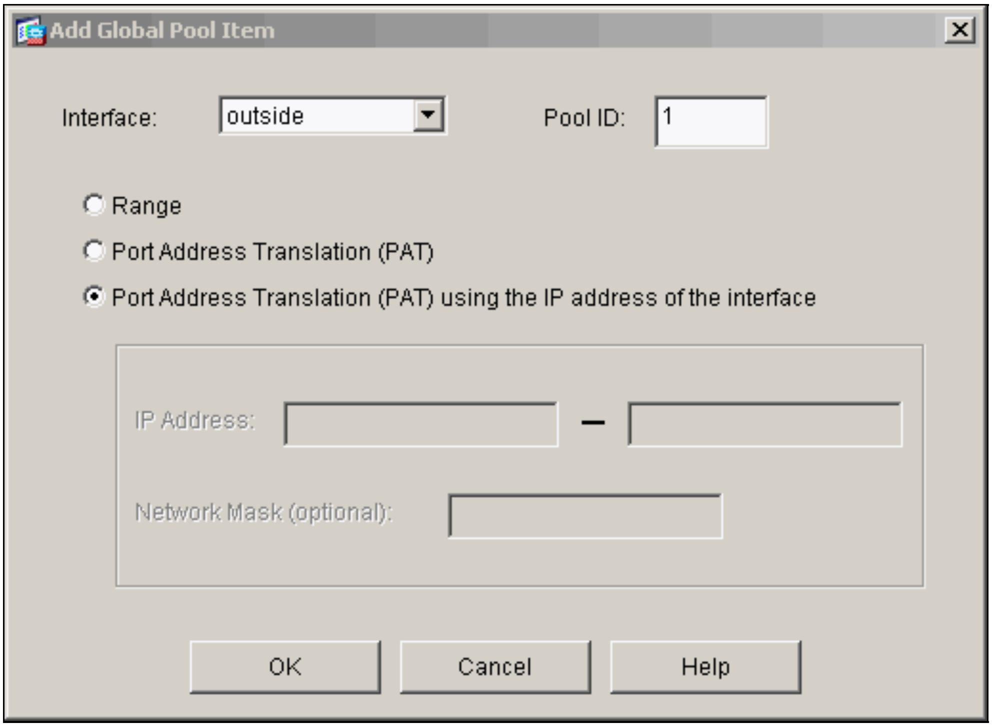
Manage Global Address Pools

Global Address Pools

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

Interface	Pool ID	IP Address(es)
inside		
outside		

This example uses a PAT using the IP address of the interface.



Add Global Pool Item

Interface: outside

Pool ID: 1

○ Range

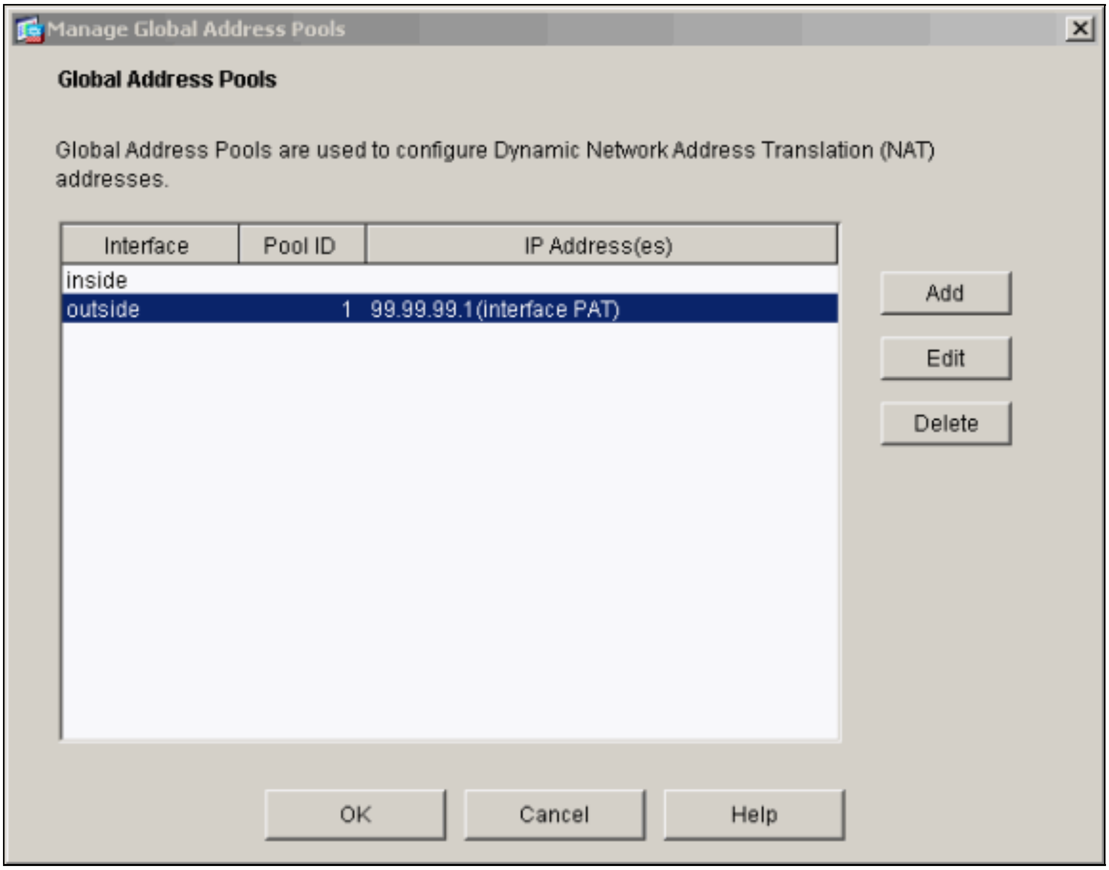
○ Port Address Translation (PAT)

● Port Address Translation (PAT) using the IP address of the interface

IP Address: –

Network Mask (optional):

18. Click **OK** when the PAT is configured.

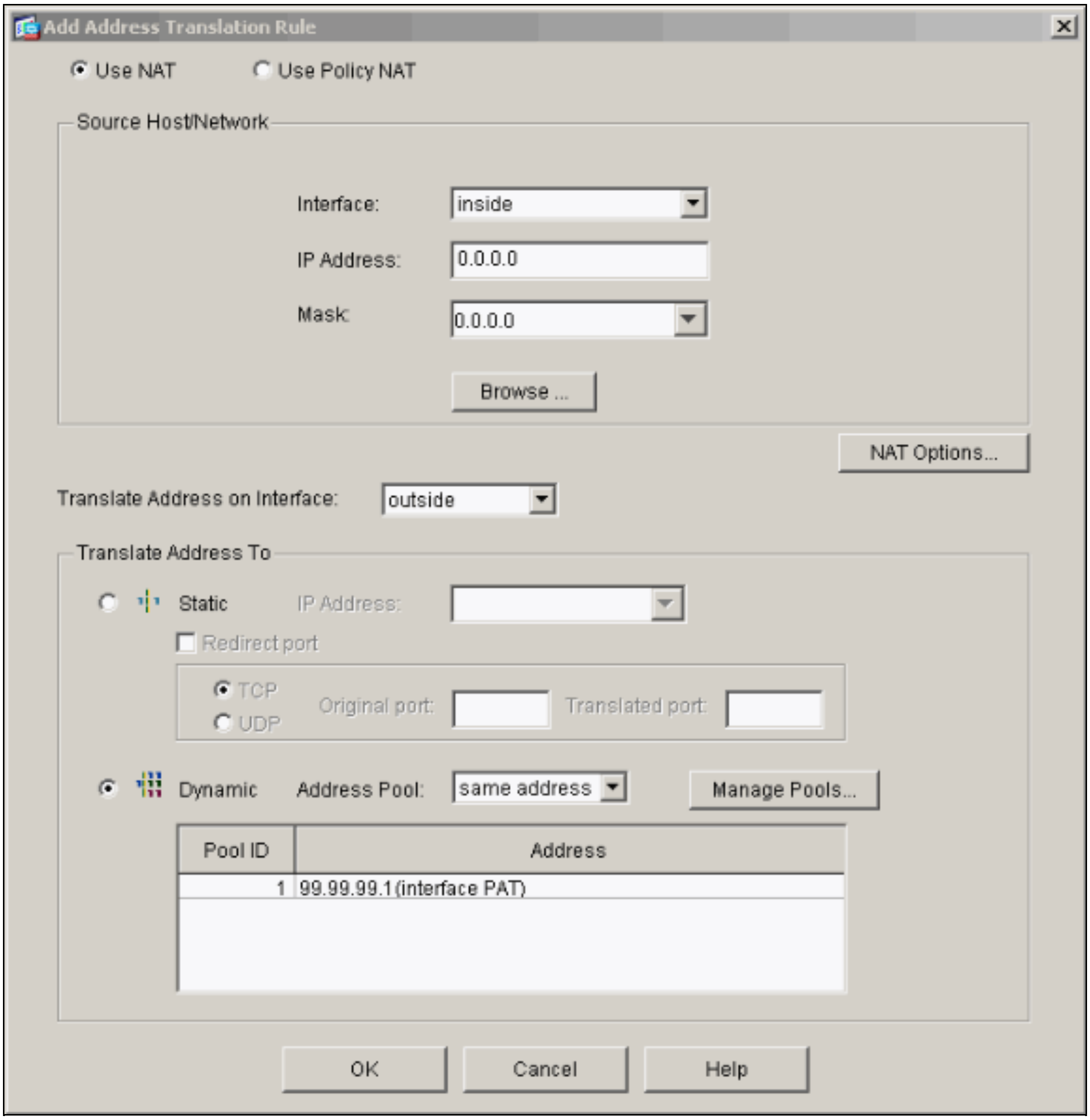


Global Address Pools

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

Interface	Pool ID	IP Address(es)
inside		
outside	1	99.99.99.1(interface PAT)

19. Click **Add** in order to configure the static translation.



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 0.0.0.0

Mask: 0.0.0.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

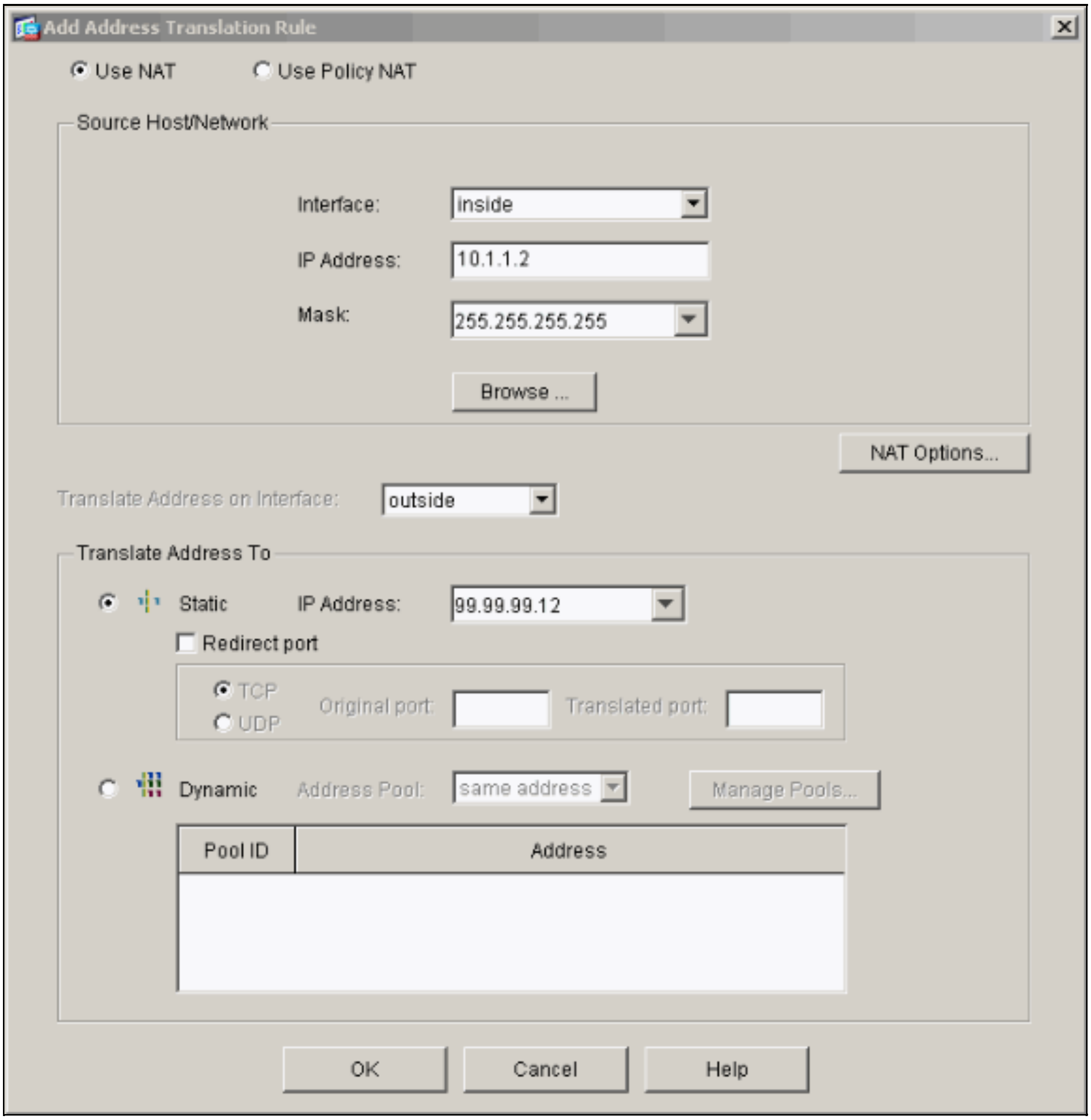
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: same address

Pool ID	Address
1	99.99.99.1(interface PAT)

20. Select **inside** on the Interface drop down, then enter IP address **10.1.1.2**, subnet mask **255.255.255.255**, select **Static** and in the IP Address field type outside address **99.99.99.12**. Click **OK** when you are done.



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.1.1.2

Mask: 255.255.255.255

Translate Address on Interface: outside

Translate Address To

● Static IP Address: 99.99.99.12

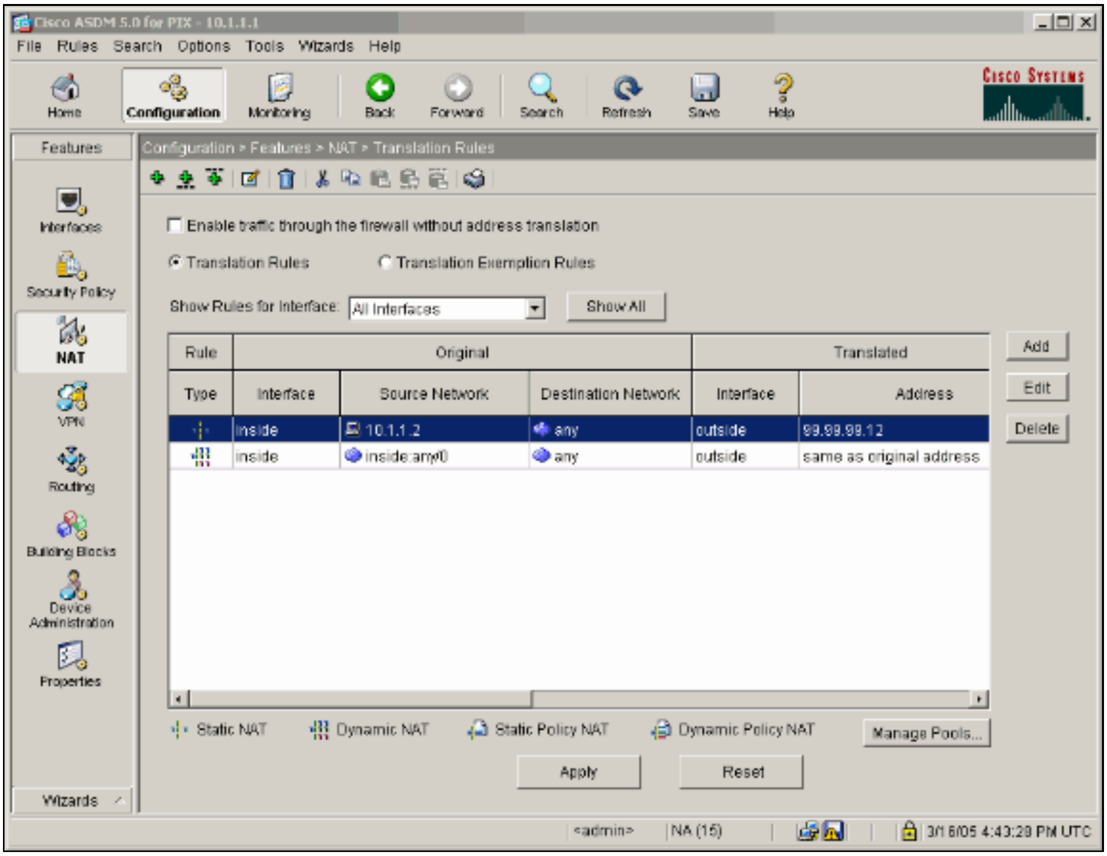
□ Redirect port

● TCP ○ UDP Original port: Translated port:

○ Dynamic Address Pool: same address

Pool ID	Address

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



Configuration > Features > NAT > Translation Rules

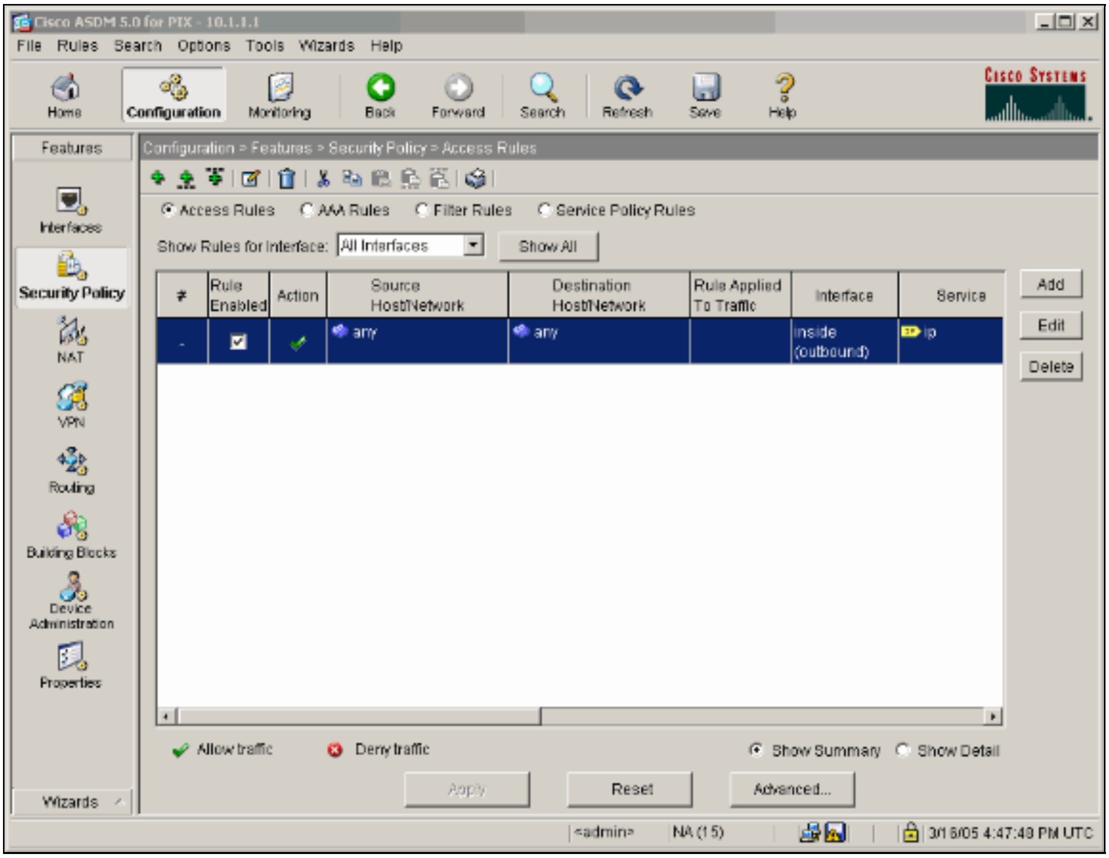
□ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.1.1.2	any	outside	99.99.99.12
	inside	inside:any/0	any	outside	same as original address

22. Select **Security Policy** under the Features tab in order to configure the Security Policy rule.


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
Cisco Systems
Features
Interfaces
Security Policy
NAT
VPN
Routing
Building Blocks
Device Administration
Properties
Wizards
Add
Edit
Delete
Allow traffic
Deny traffic
Apply
Reset
Advanced...
<admin> NA (15) 3/16/05 4:47:48 PM UTC

Configuration > Features > Security Policy > Access Rules

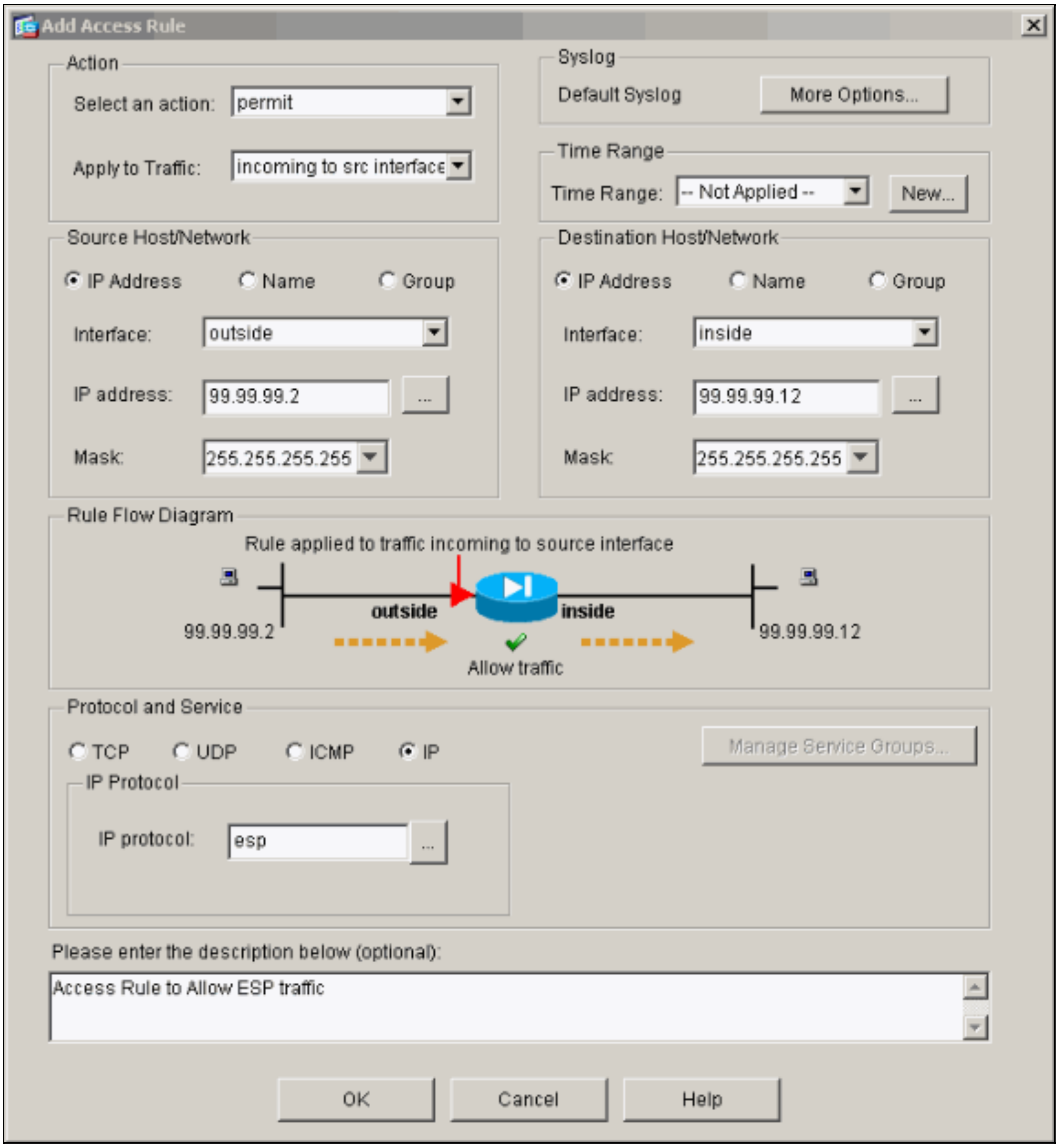
● Access Rules ○ AAA Rules ○ Filter Rules ○ Service Policy Rules

Show Rules for Interface: All Interfaces

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	☑	✓	any	any		inside (outbound)	ip

● Show Summary ○ Show Detail

23. Select **Add** to allow esp traffic and click **OK** in order to continue.



Action

Select an action: permit

Apply to Traffic: incoming to src interface

Syslog

Default Syslog

Time Range

Time Range: -- Not Applied --

Source Host/Network

● IP Address ○ Name ○ Group

Interface: outside

IP address: 99.99.99.2

Mask: 255.255.255.255

Destination Host/Network

● IP Address ○ Name ○ Group

Interface: inside

IP address: 99.99.99.12

Mask: 255.255.255.255

Rule Flow Diagram

Protocol and Service

○ TCP ○ UDP ○ ICMP ● IP

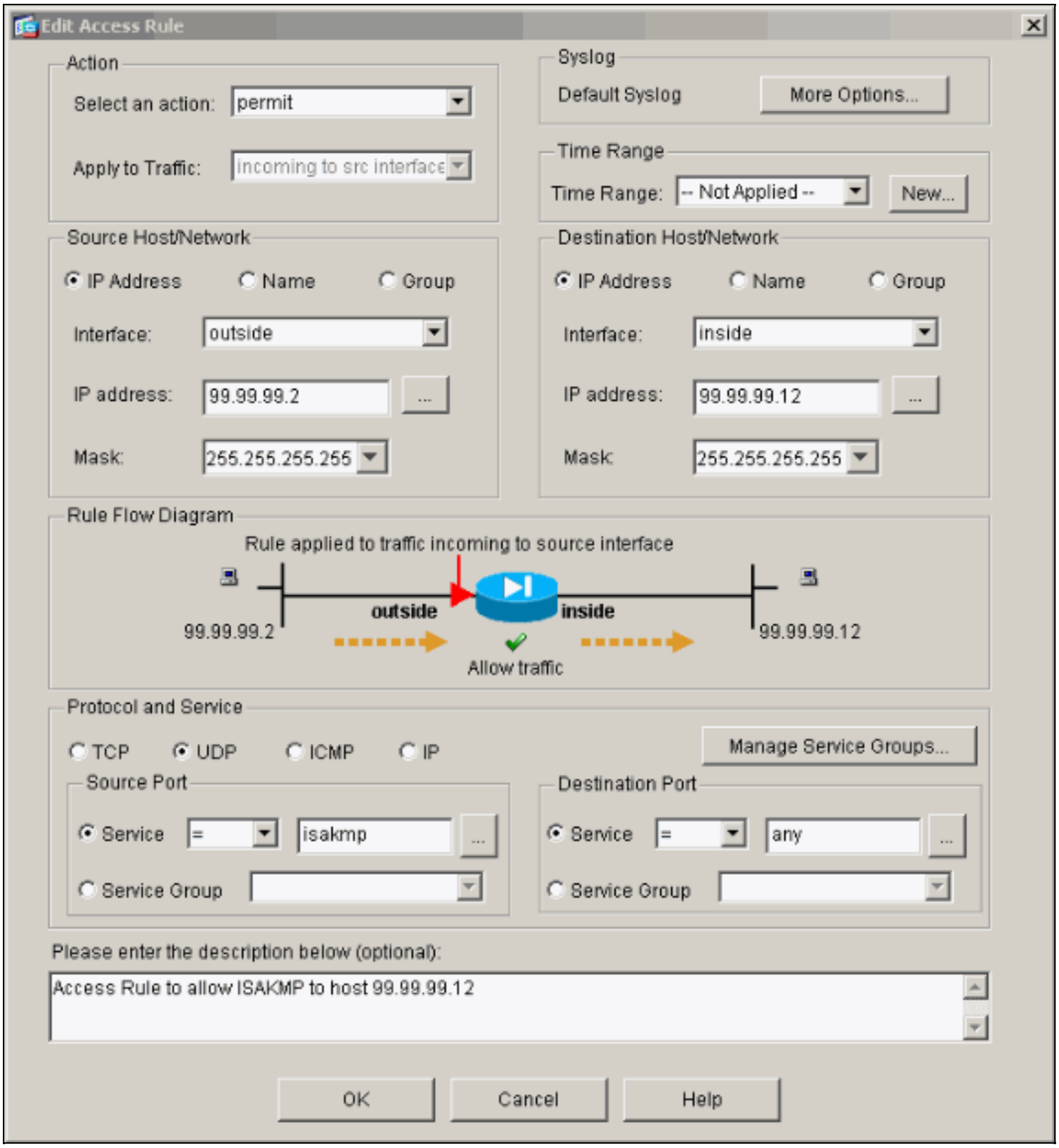
IP Protocol

IP protocol: esp

Please enter the description below (optional):

Access Rule to Allow ESP traffic

24. Select **Add** to allow isakmp traffic and click **OK** in order to continue.



Edit Access Rule

Action

Select an action: permit

Apply to Traffic: incoming to src interface

Syslog

Default Syslog   More Options...

Time Range

Time Range: -- Not Applied --   New...

Source Host/Network

● IP Address   ○ Name   ○ Group

Interface: outside

IP address: 99.99.99.2   ...

Mask: 255.255.255.255

Destination Host/Network

● IP Address   ○ Name   ○ Group

Interface: inside

IP address: 99.99.99.12   ...

Mask: 255.255.255.255

Rule Flow Diagram

Rule applied to traffic incoming to source interface

Protocol and Service

○ TCP   ● UDP   ○ ICMP   ○ IP   Manage Service Groups...

Source Port

● Service = isakmp ...

○ Service Group

Destination Port

● Service = any ...

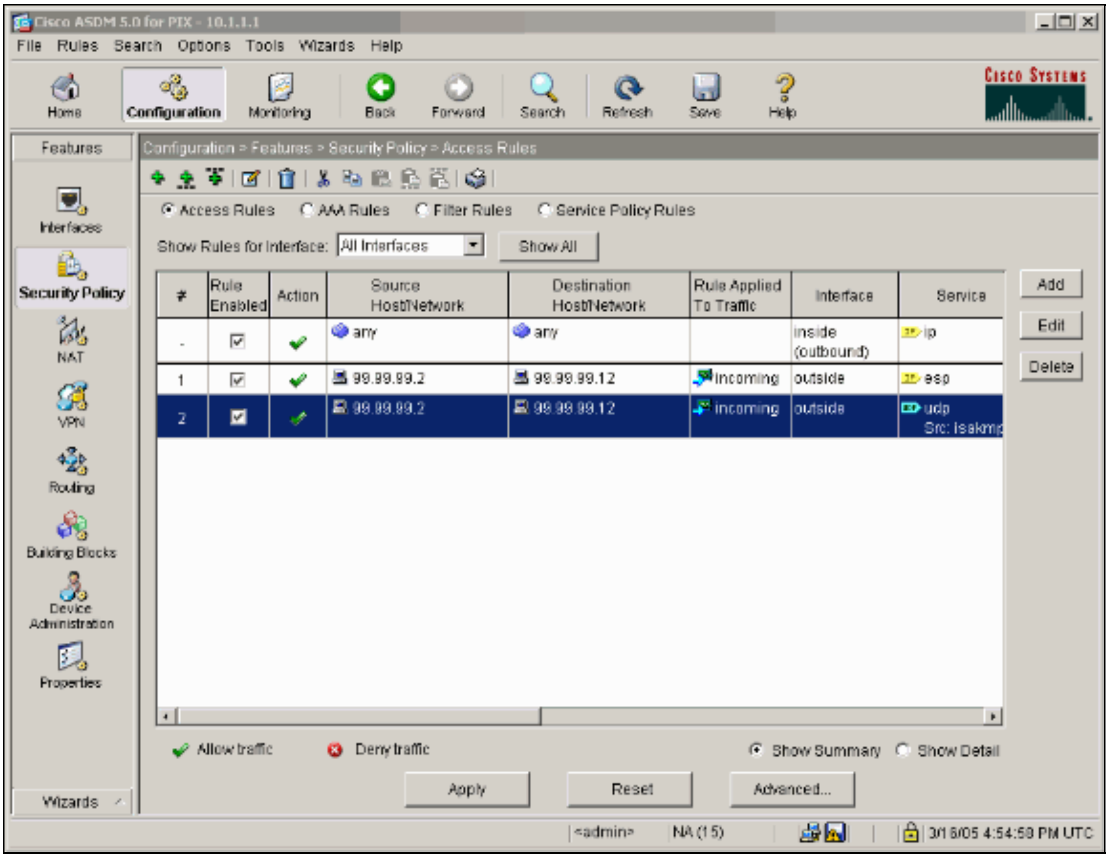
○ Service Group

Please enter the description below (optional):

Access Rule to allow ISAKMP to host 99.99.99.12

OK   Cancel   Help

25. Click **Apply** in order to accept the interface configuration. The configuration also gets pushed onto the PIX.



● Access Rules ○ AAA Rules ○ Filter Rules ○ Service Policy Rules

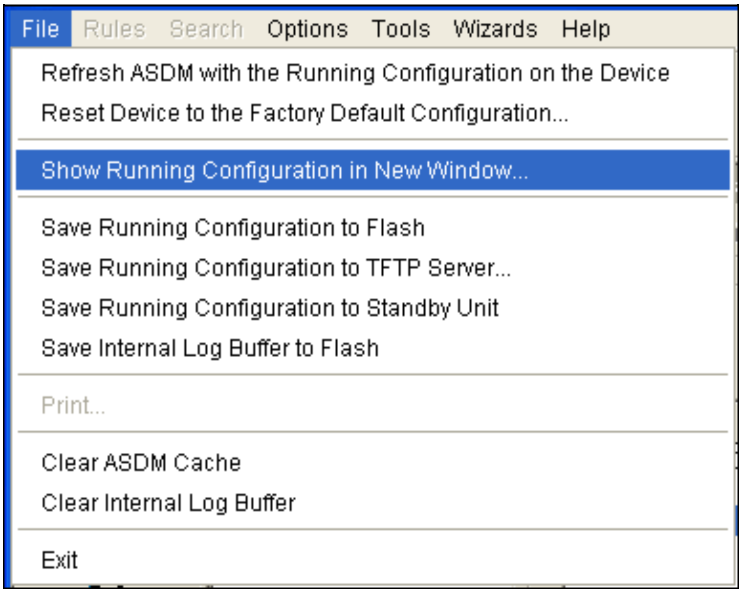
Show Rules for Interface: All Interfaces   Show All

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	☑	✓	any	any		inside (outbound)	ip
1	☑	✓	99.99.99.2	99.99.99.12	incoming	outside	esp
2	☑	✓	99.99.99.2	99.99.99.12	incoming	outside	udp Src: isakmp

● Show Summary ○ Show Detail

26. The configuration is now complete.

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


File
Rules
Search
Options
Tools
Wizards
Help
Refresh ASDM with the Running Configuration on the Device
Reset Device to the Factory Default Configuration...
Show Running Configuration in New Window...
Save Running Configuration to Flash
Save Running Configuration to TFTP Server...
Save Running Configuration to Standby Unit
Save Internal Log Buffer to Flash
Print...
Clear ASDM Cache
Clear Internal Log Buffer
Exit

PIX Firewall Configuration

PIX Firewall

```
pixfirewall# show run
: Saved
:
PIX Version 7.0(0)102
```

```
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 99.99.99.1 255.255.255.0
!
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 pixfirewall
domain-name cisco.com
ftp mode passive
access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in extended permit esp host 99.99.99.2 host 99.99.99.12
access-list outside_access_in remark Access Rule to allow ISAKMP to host 99.99.99.12
access-list outside_access_in extended permit
 udp host 99.99.99.2 eq isakmp host 99.99.99.12
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 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask 255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 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 10.1.1.3 255.255.255.255 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:0a12956036ce4e7a97f351cde61fba7e
: end
```

Verify

This section provides information you can use to confirm your configuration works properly.

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

- **show crypto ipsec sa** Shows the phase 2 security associations.
- **show crypto isakmp sa** Shows the phase 1 security associations.
- **show crypto engine connections active** Shows the encrypted and decrypted packets.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands for Router IPSec

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

- **debug crypto engine** Displays the traffic that is encrypted.
- **debug crypto ipsec** Displays the IPSec negotiations of phase 2.
- **debug crypto isakmp** Displays the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.

Clearing Security Associations

- **clear crypto isakmp** Clears Internet Key Exchange (IKE) security associations.
- **clear crypto ipsec sa** Clears IPSec security associations.

Troubleshooting Commands for PIX

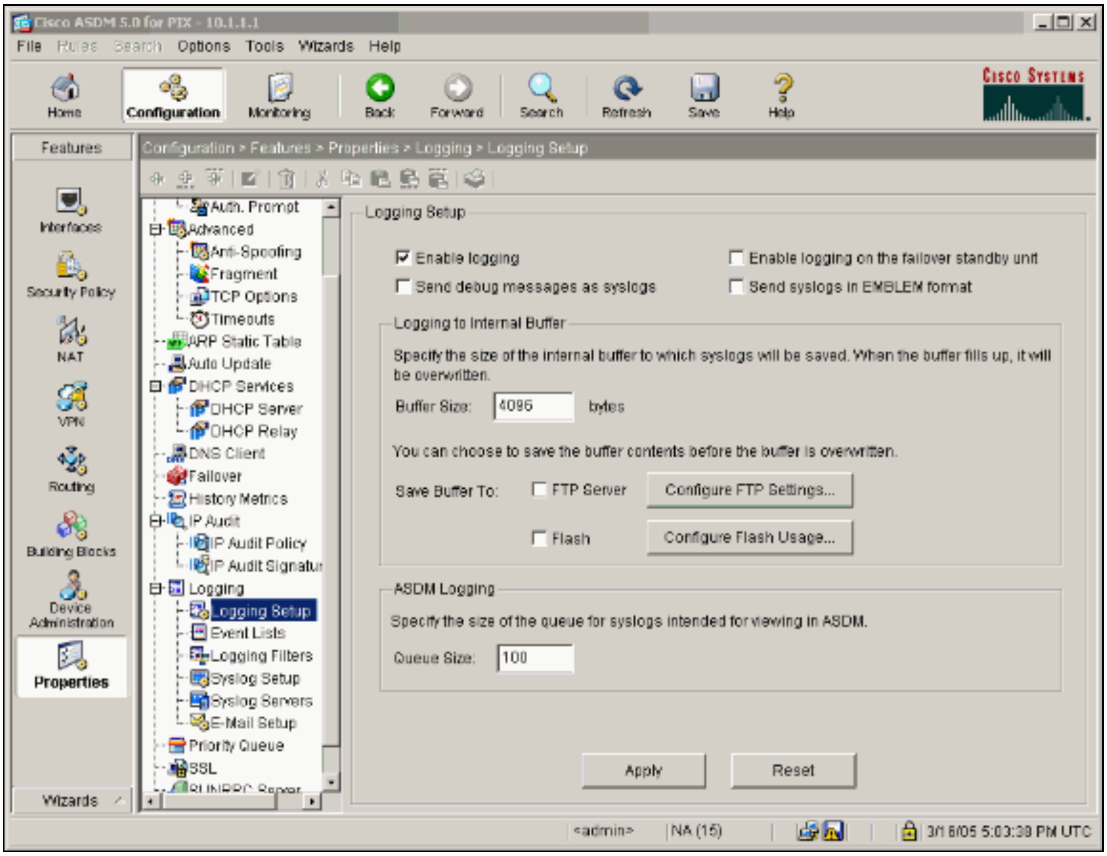
Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

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

- **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 as shown in these steps.

1. Select **Configuration > Properties > Logging > Logging Setup > Enable Logging** and then click **Apply.**



Logging Setup

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send debug messages as syslogs

□ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 4096 bytes

You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: □ FTP Server

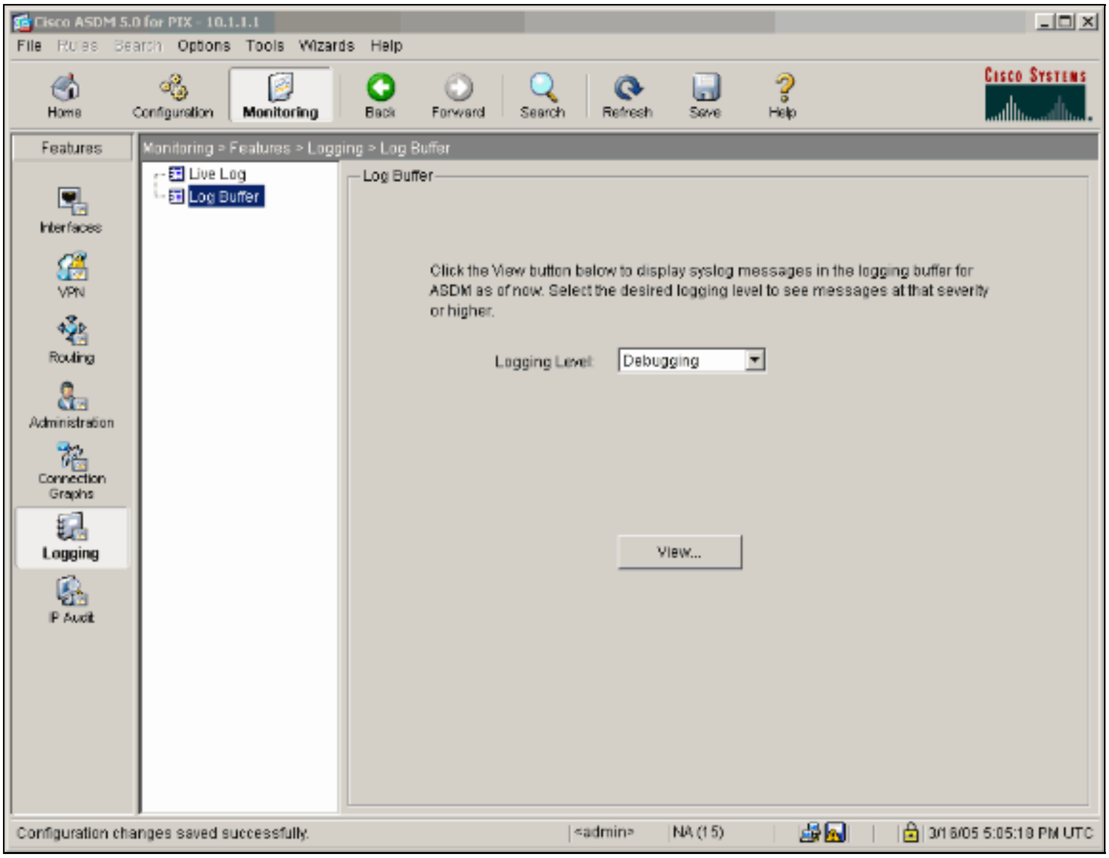
□ Flash

ASDM Logging

Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100

2. Select **Monitoring** > **Logging** > **Log Buffer** > **On Logging Level** > **Logging Buffer**, then click **View**.

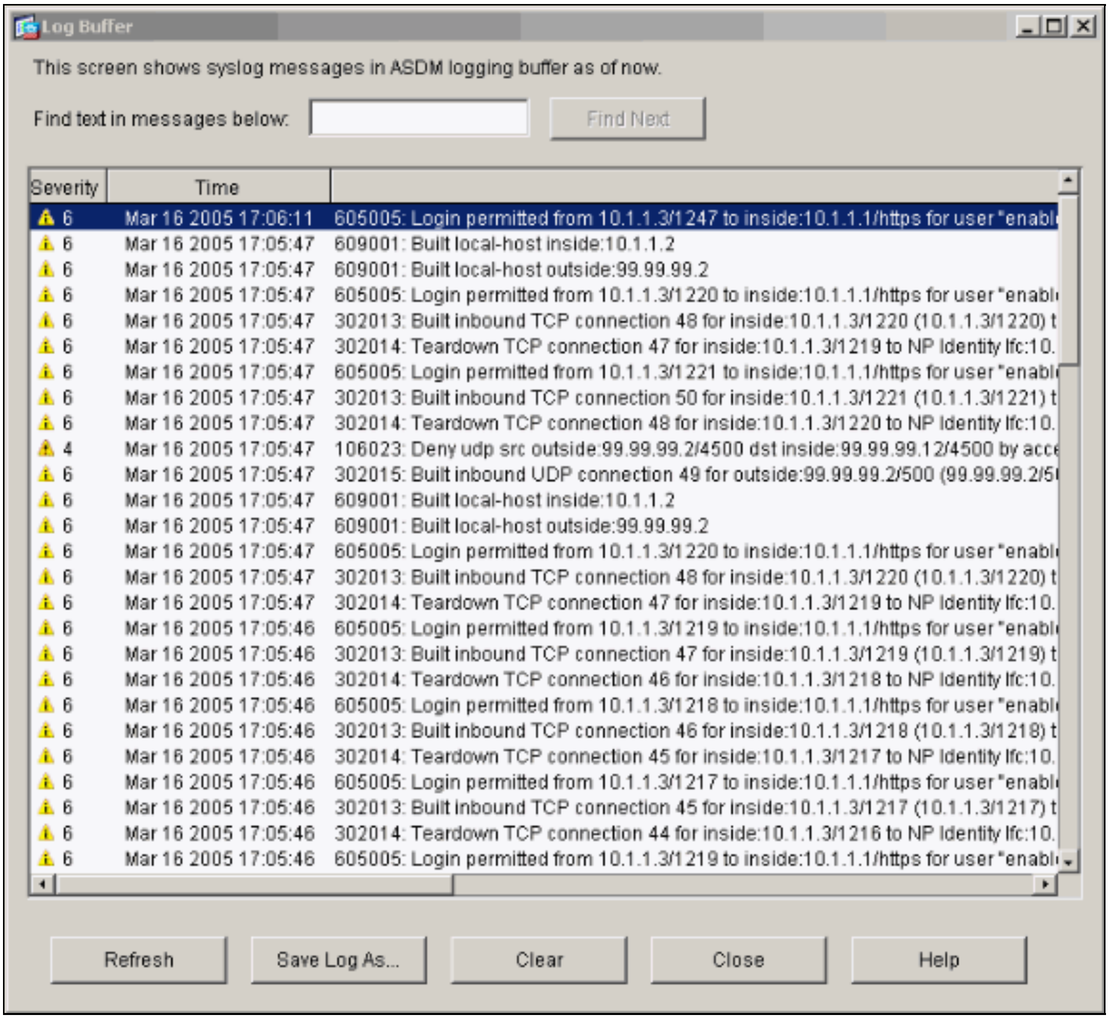


Click the View button below to display syslog messages in the logging buffer for ASDM as of now. Select the desired logging level to see messages at that severity or higher.

Logging Level: Debugging

Configuration changes saved successfully. <admin> NA (15) 3/16/05 5:05:18 PM UTC

This is an example of the Log Buffer.



This screen shows syslog messages in ASDM logging buffer as of now.

Find text in messages below:

```
Severity  Time
6   Mar 16 2005 17:06:11   605005: Login permitted from 10.1.1.3/1247 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:47   609001: Built local-host inside:10.1.1.2
6   Mar 16 2005 17:05:47   609001: Built local-host outside:99.99.99.2
6   Mar 16 2005 17:05:47   605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:47   302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t
6   Mar 16 2005 17:05:47   302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.
6   Mar 16 2005 17:05:47   605005: Login permitted from 10.1.1.3/1221 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:47   302013: Built inbound TCP connection 50 for inside:10.1.1.3/1221 (10.1.1.3/1221) t
6   Mar 16 2005 17:05:47   302014: Teardown TCP connection 48 for inside:10.1.1.3/1220 to NP Identity Ifc:10.
4   Mar 16 2005 17:05:47   106023: Deny udp src outside:99.99.99.2/4500 dst inside:99.99.99.12/4500 by acce
6   Mar 16 2005 17:05:47   302015: Built inbound UDP connection 49 for outside:99.99.99.2/500 (99.99.99.2/5
6   Mar 16 2005 17:05:47   609001: Built local-host inside:10.1.1.2
6   Mar 16 2005 17:05:47   609001: Built local-host outside:99.99.99.2
6   Mar 16 2005 17:05:47   605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:47   302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t
6   Mar 16 2005 17:05:47   302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.
6   Mar 16 2005 17:05:46   605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:46   302013: Built inbound TCP connection 47 for inside:10.1.1.3/1219 (10.1.1.3/1219) t
6   Mar 16 2005 17:05:46   302014: Teardown TCP connection 46 for inside:10.1.1.3/1218 to NP Identity Ifc:10.
6   Mar 16 2005 17:05:46   605005: Login permitted from 10.1.1.3/1218 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:46   302013: Built inbound TCP connection 46 for inside:10.1.1.3/1218 (10.1.1.3/1218) t
6   Mar 16 2005 17:05:46   302014: Teardown TCP connection 45 for inside:10.1.1.3/1217 to NP Identity Ifc:10.
6   Mar 16 2005 17:05:46   605005: Login permitted from 10.1.1.3/1217 to inside:10.1.1.1/https for user "enabl
6   Mar 16 2005 17:05:46   302013: Built inbound TCP connection 45 for inside:10.1.1.3/1217 (10.1.1.3/1217) t
6   Mar 16 2005 17:05:46   302014: Teardown TCP connection 44 for inside:10.1.1.3/1216 to NP Identity Ifc:10.
6   Mar 16 2005 17:05:46   605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enabl
```

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 VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- **IPSec Support Page**
- **PIX Support Page**
- **Documentation for PIX Firewall**
- **PIX Command References**
- **NAT Support Page**
- **Requests for Comments (RFCs)**

- **Technical Support − Cisco Systems**

Updated: Nov 16, 2005 Document ID: 63881