

# PIX/ASA (Version 7.x and Later) IPsec VPN Tunnel with Network Address Translation Configuration Example

Document ID: 63881

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions
- Related Products

#### Configure

- Network Diagram
- Configurations
  - PIX Security Appliance and Access List Configuration
  - PIX Security Appliance and MPF (Modular Policy Framework) Configuration

#### Verify

#### Troubleshoot

- Troubleshooting Commands for Router IPsec
- Clearing Security Associations
- Troubleshooting Commands for PIX

#### Related Information

## Introduction

This sample configuration demonstrates an IPsec VPN 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 earlier than 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 might 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.

Refer to [Configuring an IPSec Tunnel through a Firewall with NAT](#) for more information on how to configure IPsec tunnel through firewall with NAT on PIX version 6.x and earlier.

## 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 500 Series Security Appliance that runs 7.x and above.

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.

### Related Products

This document can also be used with the Cisco 5500 Series Adaptive Security Appliance (ASA) with software version 7.x and later.

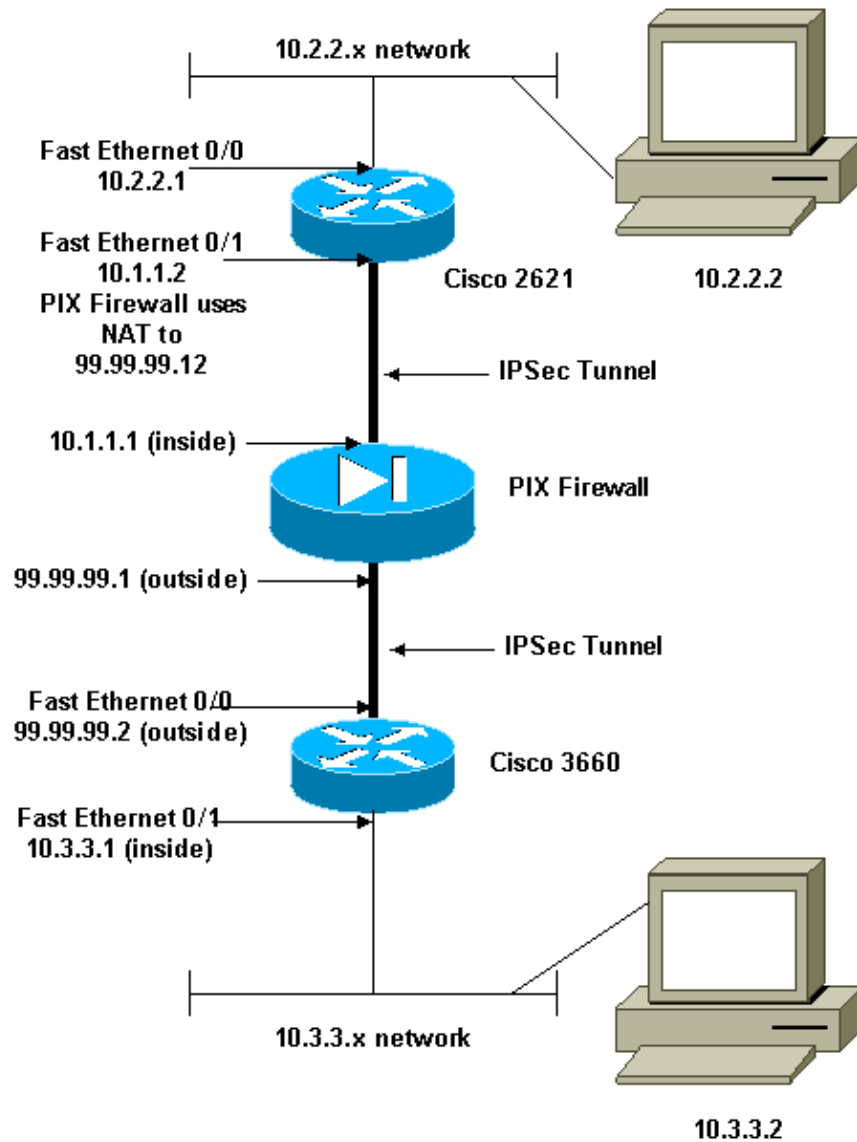
## Configure

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 Security Appliance and Access List Configuration
  - ◆ Advanced Security Device Manager GUI (ASDM) Configuration
  - ◆ Command Line Interface (CLI) Configuration
- PIX Security Appliance and MPF (Modular Policy Framework) Configuration

### 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 Security Appliance and Access List Configuration

### ASDM 5.0 Configuration

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

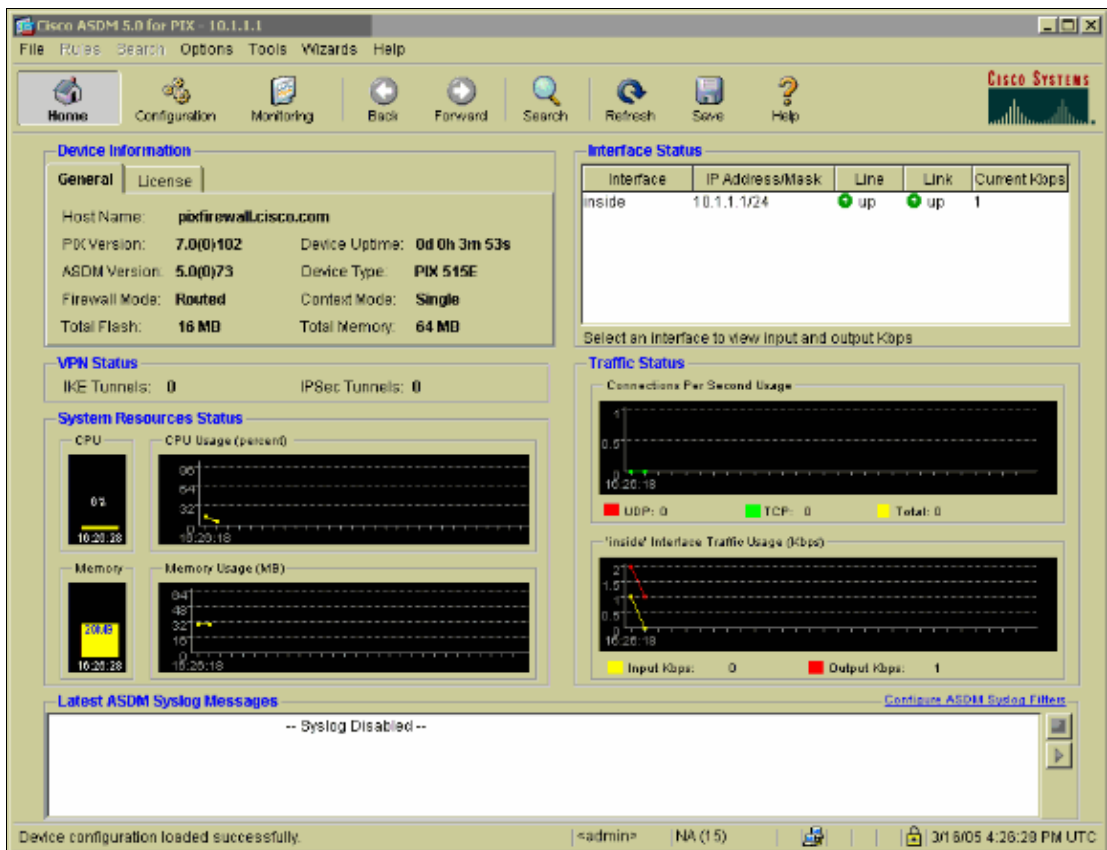
1. Console into the PIX. From a cleared configuration, use the interactive prompts to enable **Advanced Security Device Manager GUI (ASDM)** for the management of the PIX from the Workstation 10.1.1.3.

```
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
```

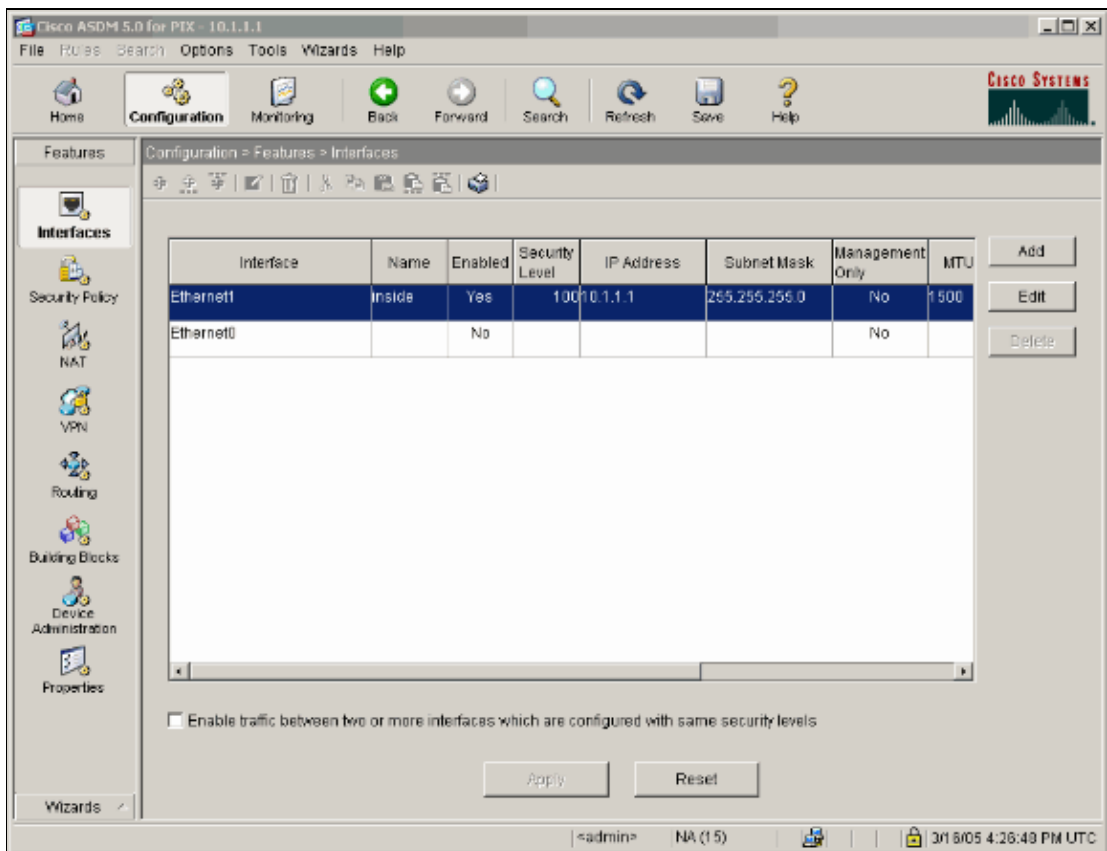
2. From Workstation 10.1.1.3, open up a Web Browser and use ADSM (in this example, <https://10.1.1.1>).
3. Choose **Yes** on the certificate prompts and login with the enable password as configured in the PIX Firewall ASDM Bootstrap configuration.
4. If this is the first time ASDM is run on the PC, it prompts you whether to use ASDM Launcher, or use ASDM as a Java App.

In this example, the ASDM Launcher is selected and installs these prompts.

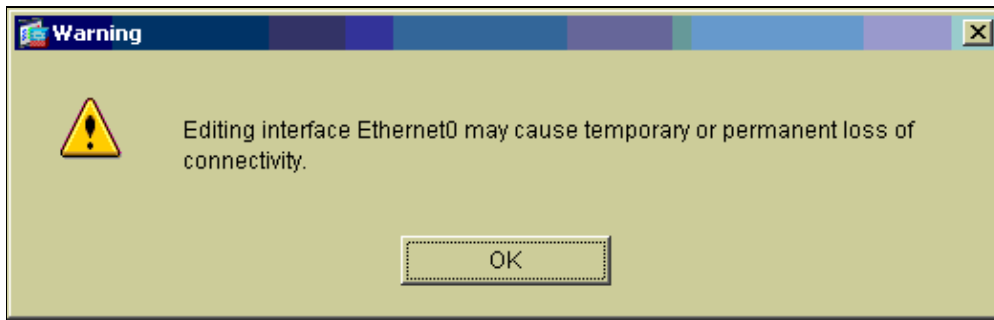
5. Proceed to the ASDM Home window and select the Configuration tab.



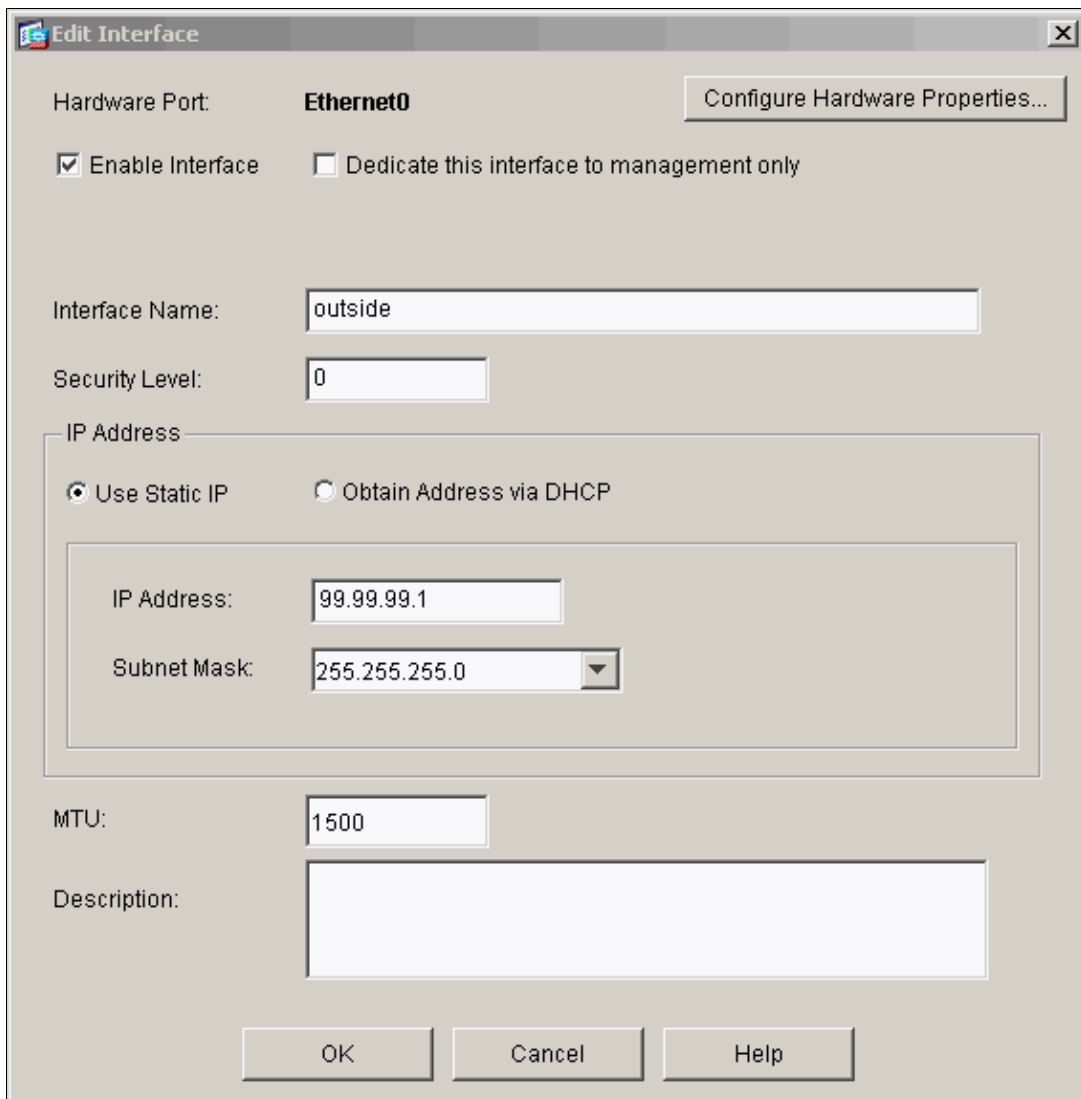
6. Highlight the **Ethernet 0 Interface** and click **Edit** in order to configure the Outside Interface.



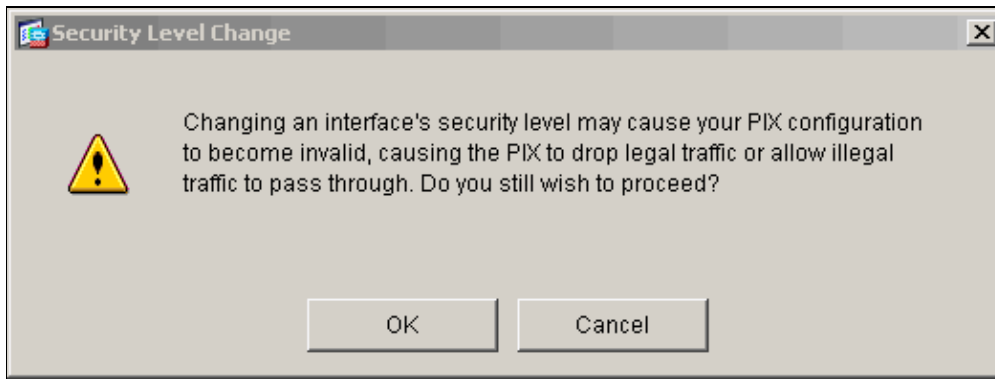
7. Click **OK** at the Editing interface prompt.



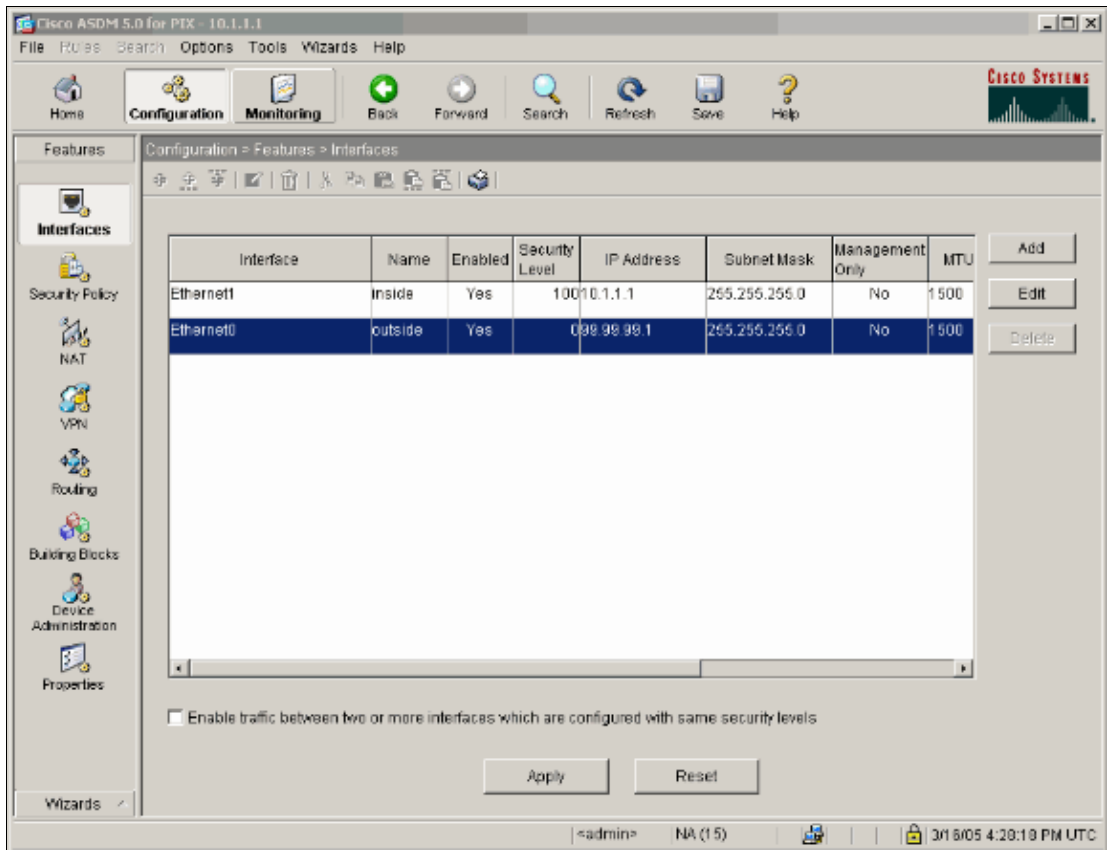
8. Enter the interface details and click **OK** when you are done.



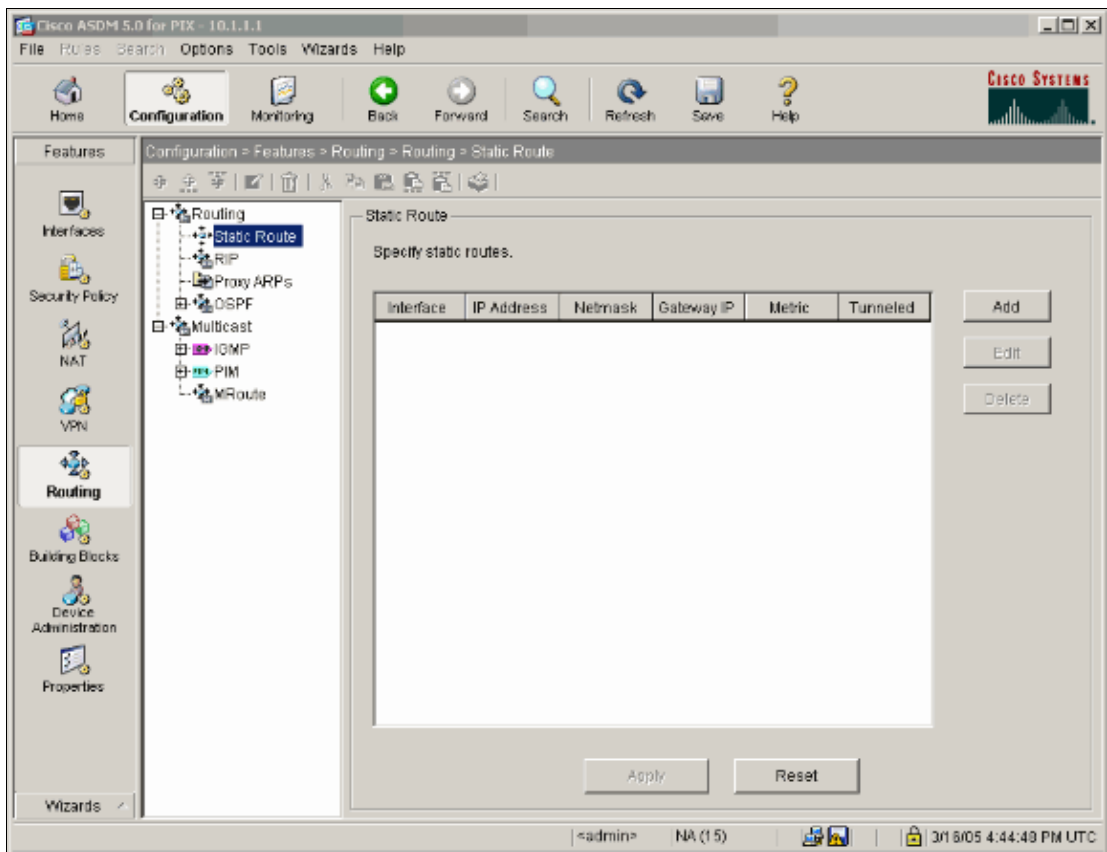
9. Click **OK** at the Changing an Interface prompt.



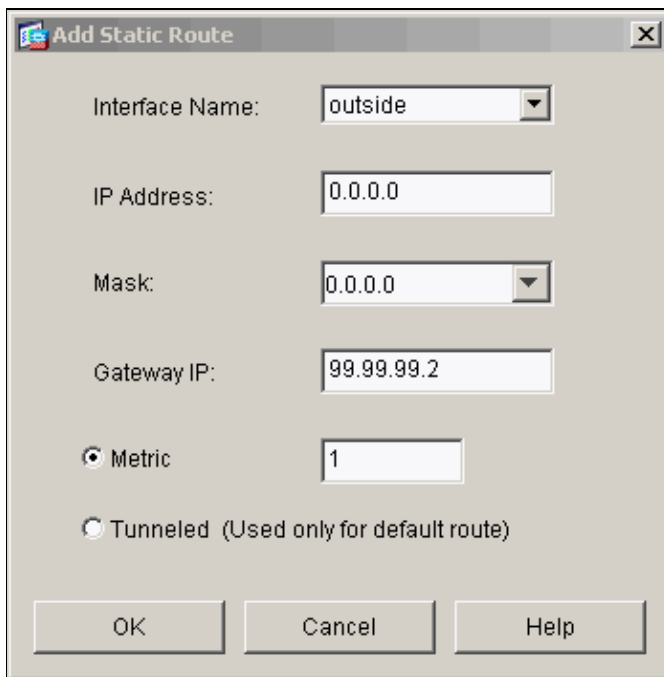
10. Click **Apply** in order to accept the interface configuration. The configuration also gets pushed onto the PIX. This example uses static routes.



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



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



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

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

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

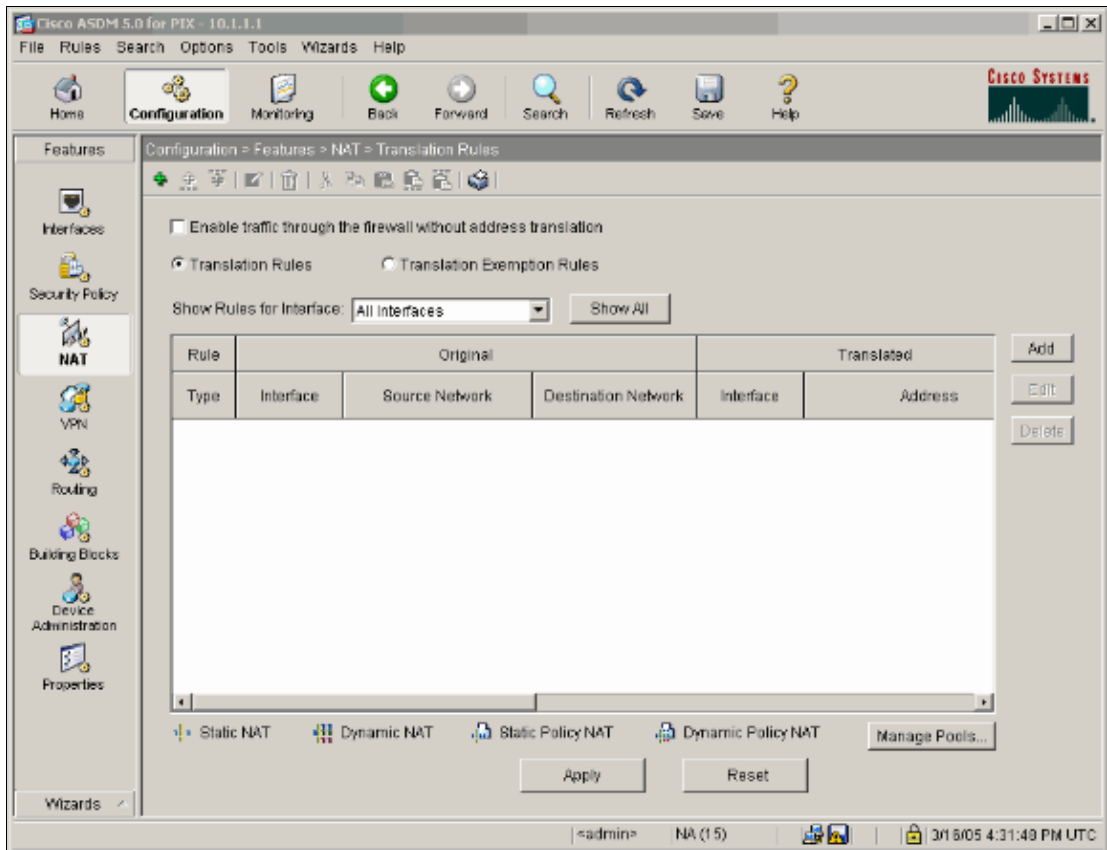
Configuration > Features > Routing > Routing > Static Route

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   | 255.255.255.0 | 10.1.1.2   | 1      | N/A      |

Apply Reset

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.



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

**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:

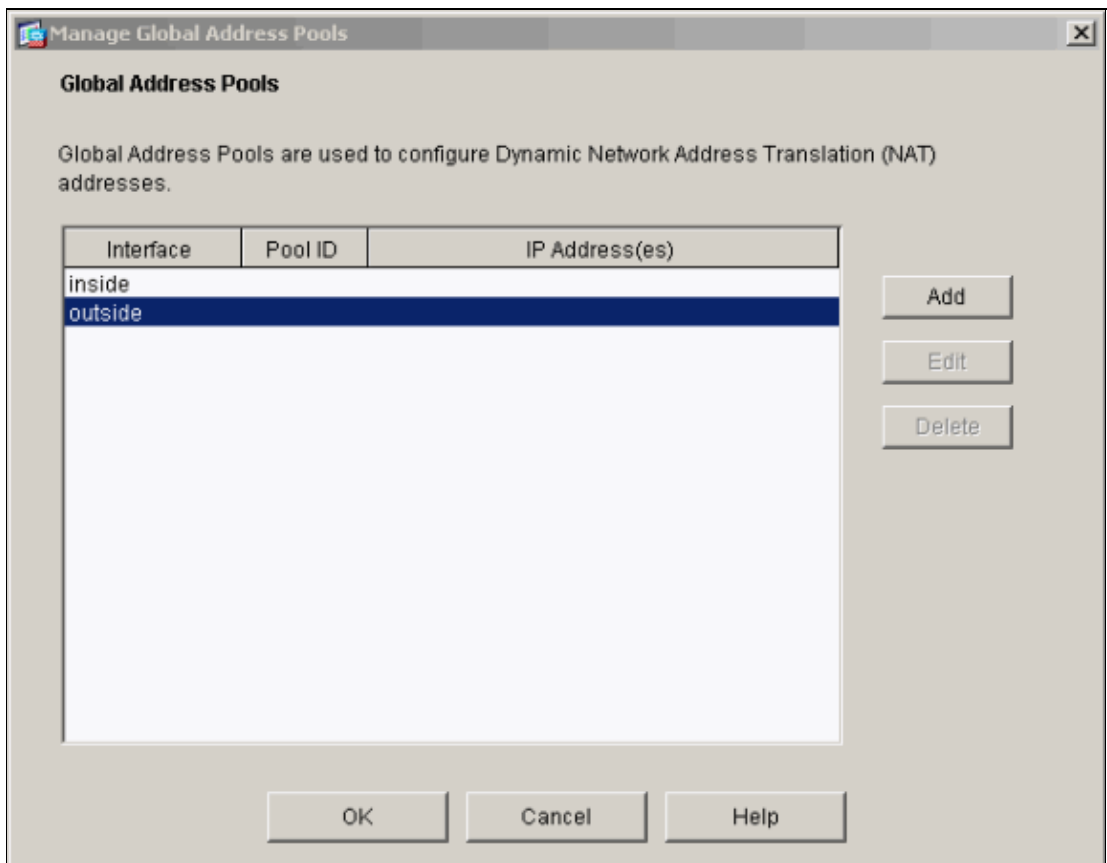
UDP

Dynamic    Address Pool:    

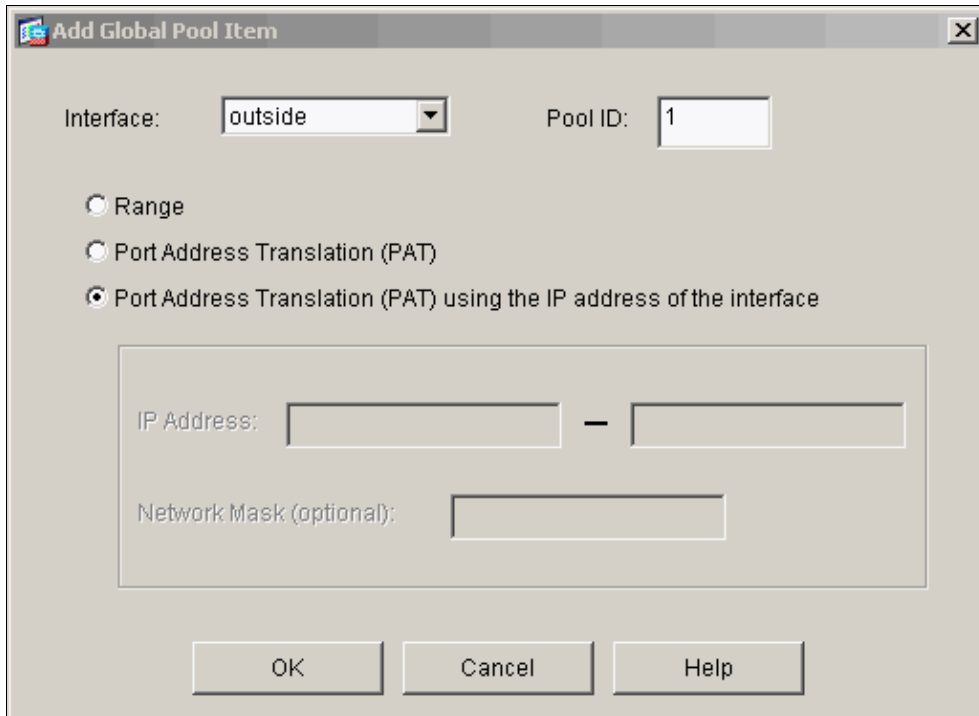
| Pool ID | Address                 |
|---------|-------------------------|
| N/A     | No address pool defined |
|         |                         |

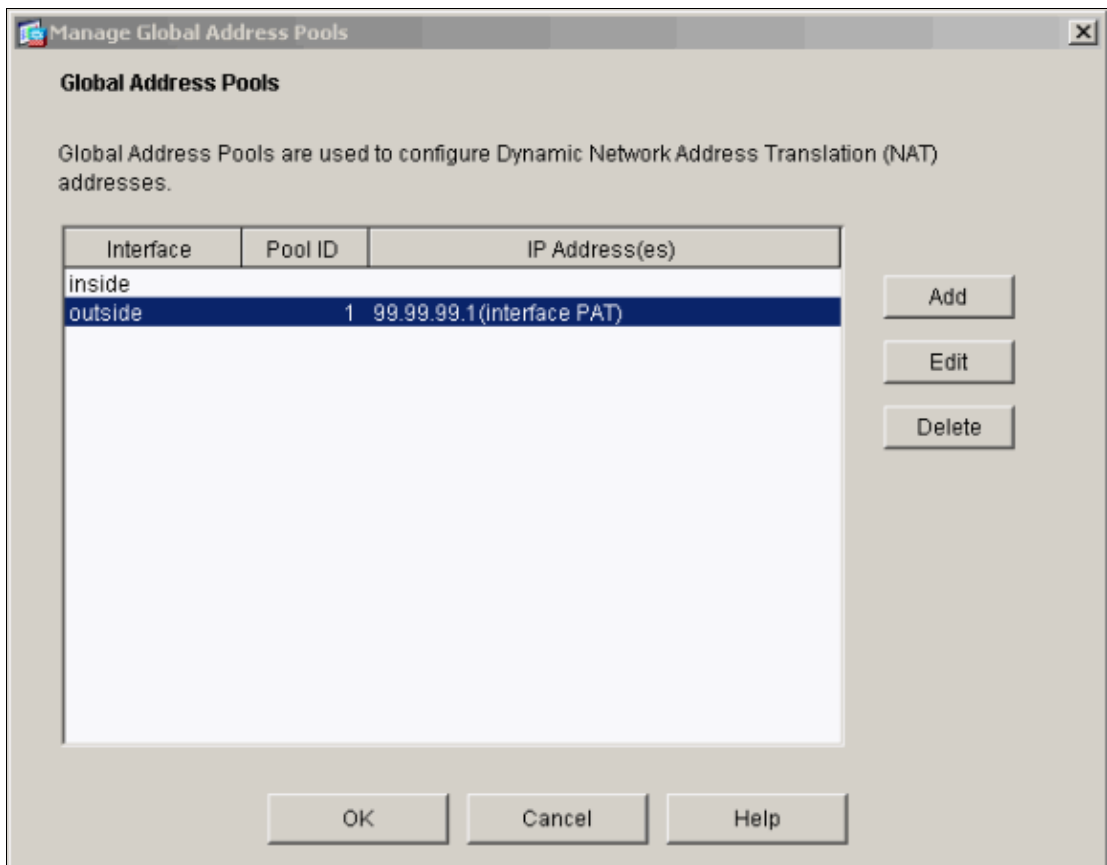
17. Select the **outside** interface and click **Add**.



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



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



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

**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                    |
|---------|----------------------------|
| 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**, choose **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:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static    IP Address:

Redirect port

TCP    Original port:     Translated port:

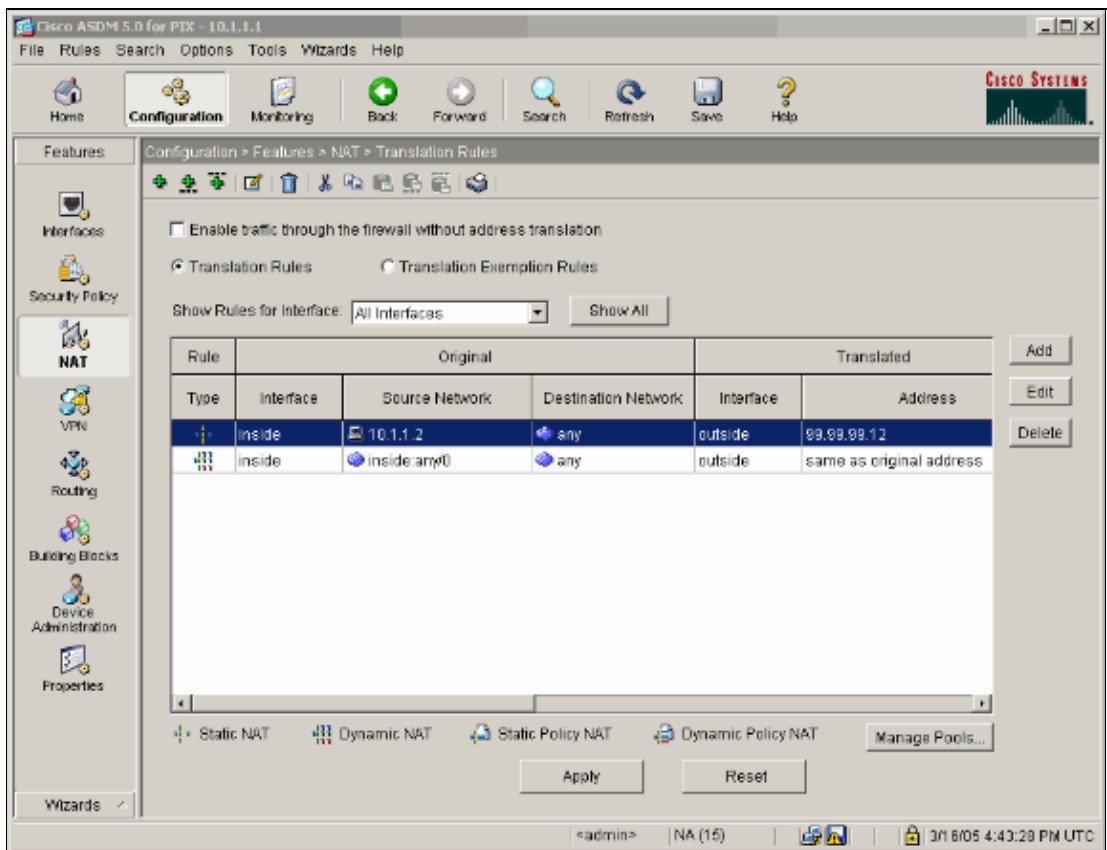
UDP

Dynamic    Address Pool:    

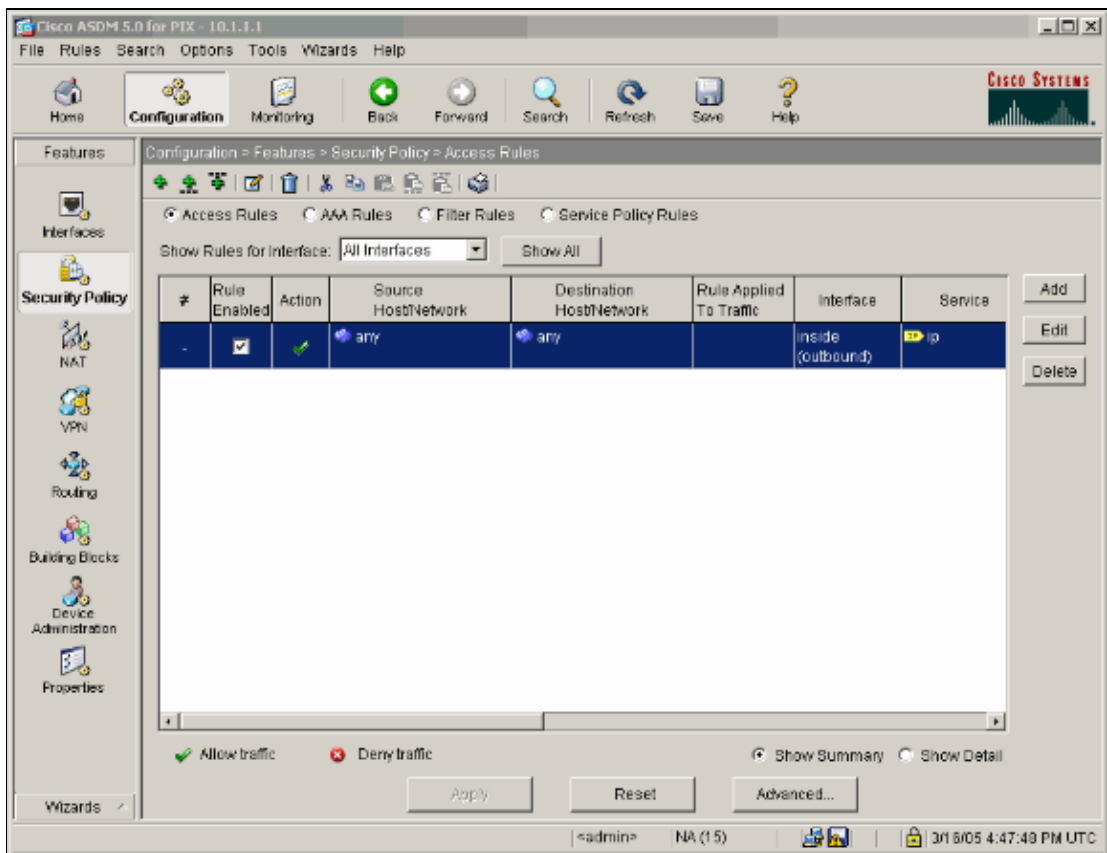
| Pool ID | Address |
|---------|---------|
|         |         |

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



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



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

**Add Access Rule**

**Action**  
 Select an action:   
 Apply to Traffic:

**Source Host/Network**  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

**Destination Host/Network**  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

**Rule Flow Diagram**  
 Rule applied to traffic incoming to source interface  
  
 The diagram shows a central router icon with two interfaces: 'outside' on the left and 'inside' on the right. A red arrow points from the 'outside' interface towards the router. A green arrow points from the router towards the 'inside' interface. Below the router, the text 'Allow traffic' is displayed with a green checkmark. On the far left, the IP address '99.99.99.2' is shown with a vertical line and a small computer icon. On the far right, the IP address '99.99.99.12' is shown with a vertical line and a small computer icon. Dashed orange arrows indicate the flow of traffic from the source IP to the router and then to the destination IP.

**Protocol and Service**  
 TCP  UDP  ICMP  IP   
 IP Protocol  
 IP protocol:  ...

Please enter the description below (optional):

24. Click **Add** in order to allow ISAKMP traffic and click **OK** in order to continue.

**Edit Access Rule**

**Action**  
 Select an action:   
 Apply to Traffic:

**Source Host/Network**  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

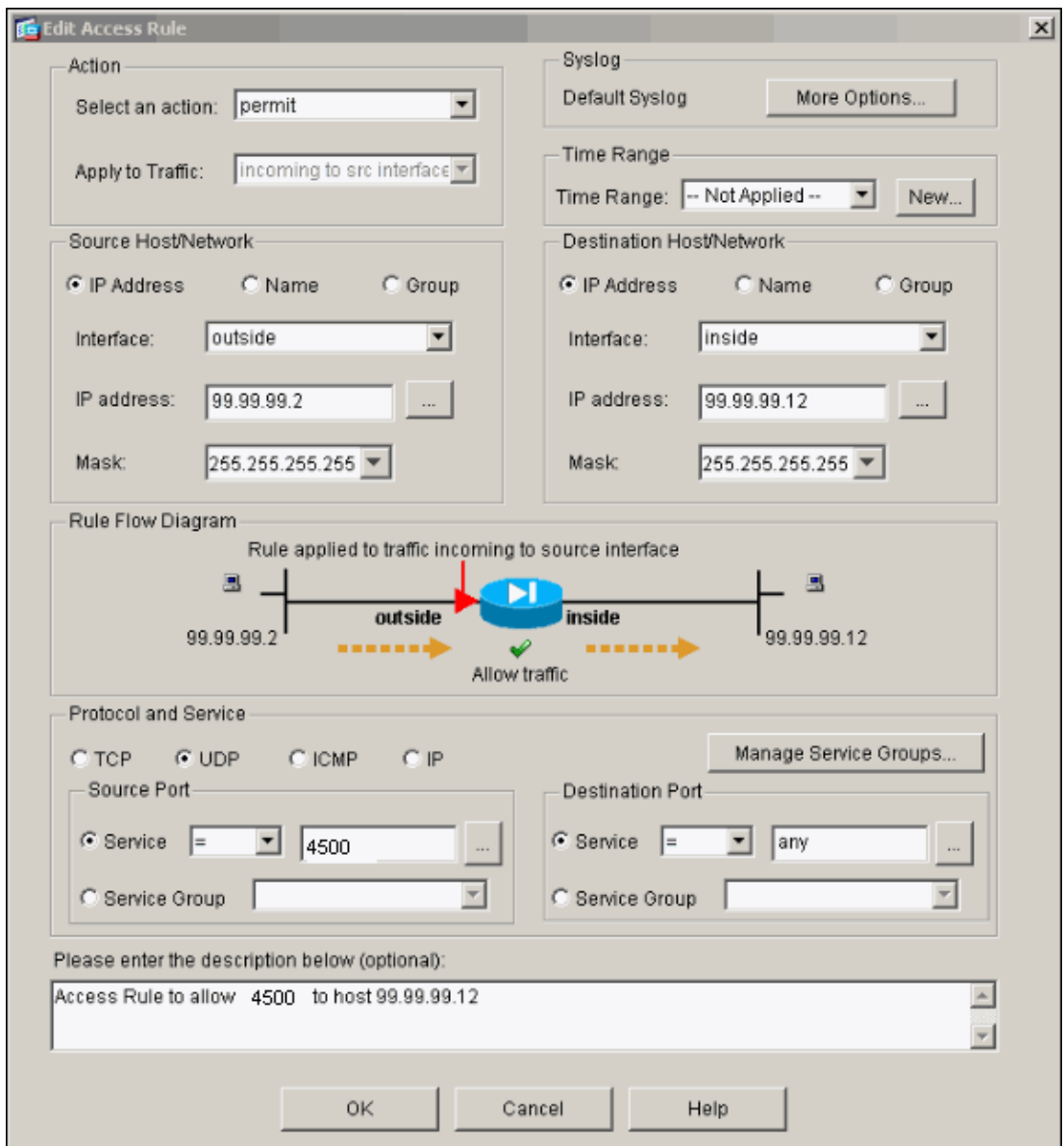
**Destination Host/Network**  
 IP Address  Name  Group  
 Interface:   
 IP address:  ...  
 Mask:

**Rule Flow Diagram**  
 Rule applied to traffic incoming to source interface  
  
 99.99.99.2 outside inside 99.99.99.12  
 Allow traffic

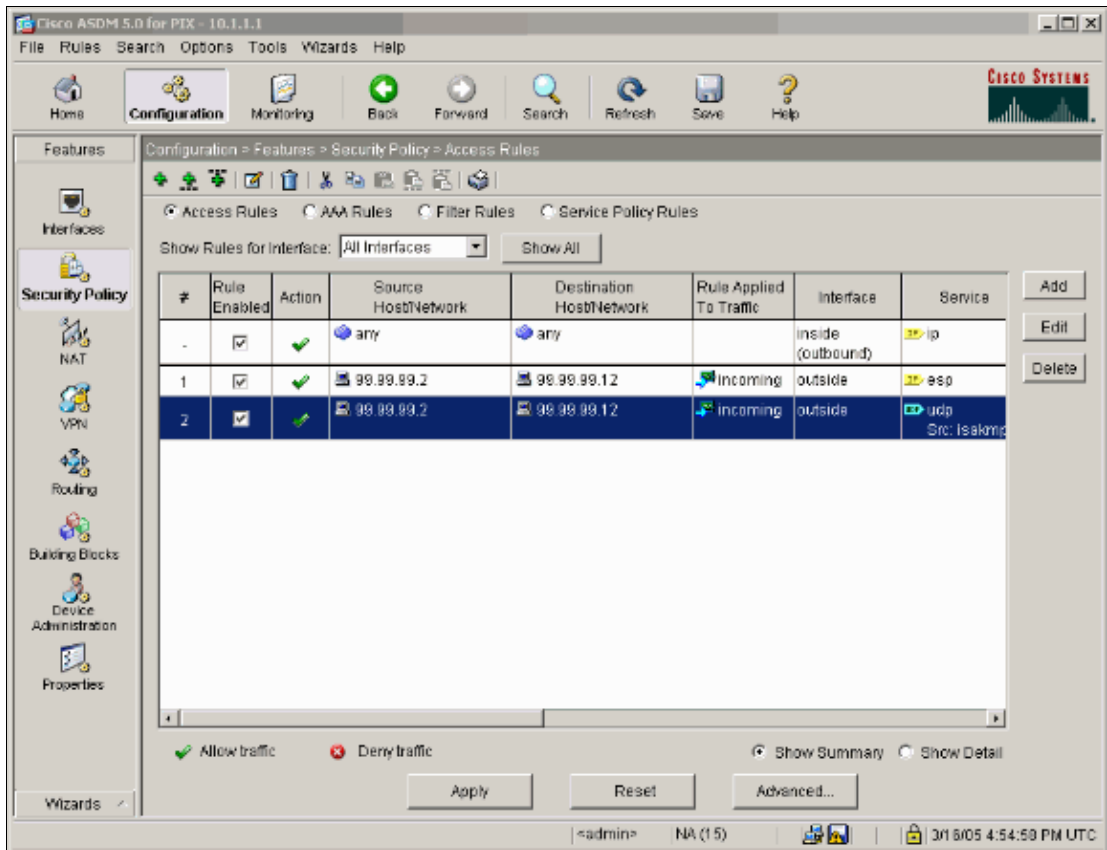
**Protocol and Service**  
 TCP  UDP  ICMP  IP Manage Service Groups...  
**Source Port**  
 Service =  ...  
 Service Group   
**Destination Port**  
 Service =  ...  
 Service Group

Please enter the description below (optional):

25. Click **Add** in order to allow UDP port 4500 traffic for NAT-T and click **OK** in order to continue.

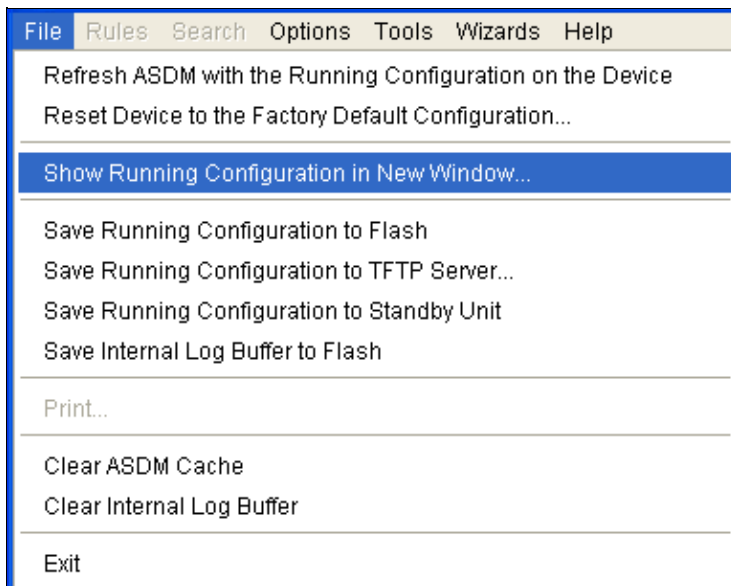


26. Click **Apply** in order to accept the interface configuration. The configuration also gets pushed onto the PIX.



27. The configuration is now complete.

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



## 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

access-list outside_access_in
  remark Access Rule to allow port 4500 (NAT-T) to host 99.99.99.12
access-list outside_access_in
  extended permit udp host 99.99.99.2 eq 4500 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

```

## PIX Security Appliance and MPF (Modular Policy Framework) Configuration

Instead of access list, use the command **inspect ipsec-pass-thru** in MPF (Modular Policy Framework) in order to pass the IPsec traffic through the PIX/ASA Security Appliances.

This inspection is configured to open pinholes for ESP traffic. All ESP data flows are permitted when a forward flow exists, and there is no limit on the maximum number of connections that can be allowed. AH is not permitted. The default idle timeout for ESP data flows is by default set to 10 minutes. This inspection can be applied in all locations that other inspections can be applied, which includes class and match command modes. IPsec Pass Through application inspection provides convenient traversal of ESP (IP protocol 50) traffic associated with an IKE UDP port 500 connection. It avoids lengthy access list configuration to permit ESP traffic and also provides security with timeout and max connections. Use **class-map**, **policy-map**, and **service-policy** commands in order to define a class of traffic, to apply the inspect command to the class, and to apply the policy to one or more interfaces. When enabled, the **inspect IPsec-pass-thru** command allows unlimited ESP traffic with a timeout of 10 minutes, which is not configurable. NAT and non-NAT traffic is permitted.

```

hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside

```

## 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:** Refer to Important Information on Debug Commands before you issue **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.

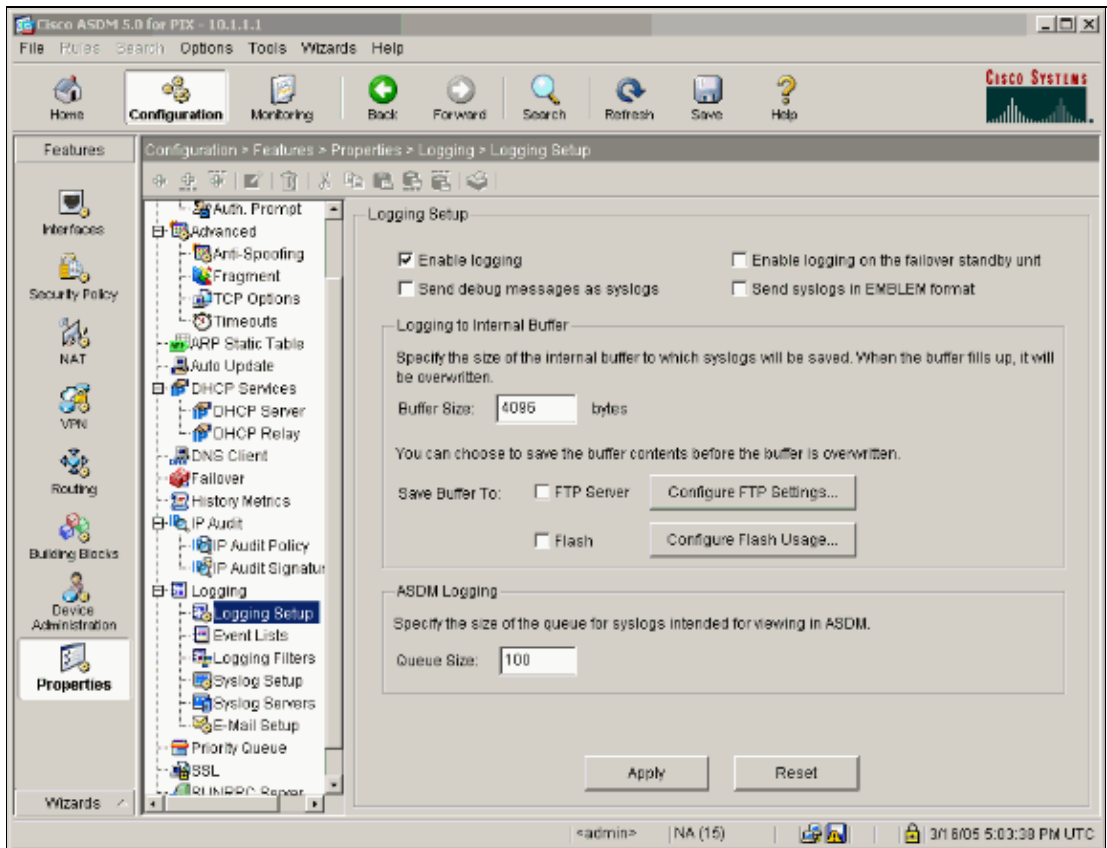
## Troubleshooting Commands for PIX

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

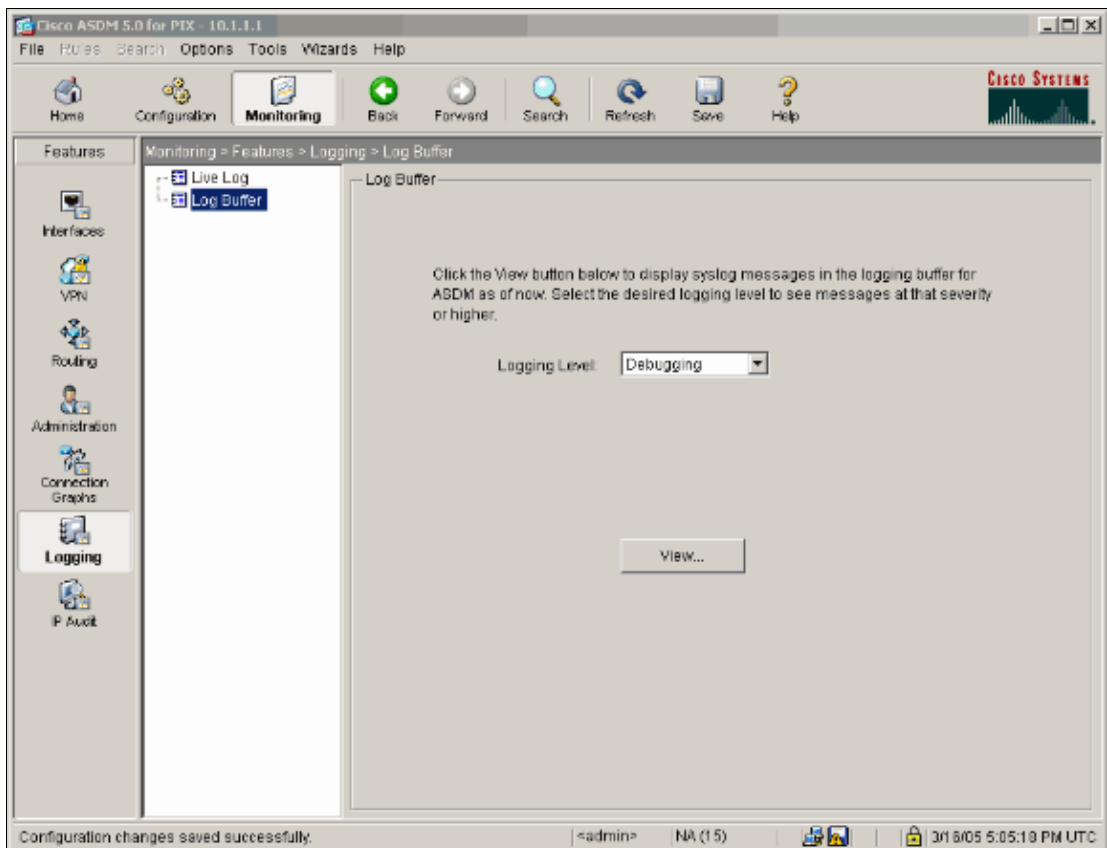
**Note:** Refer to Important Information on Debug Commands before you issue **debug** commands.

- **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.

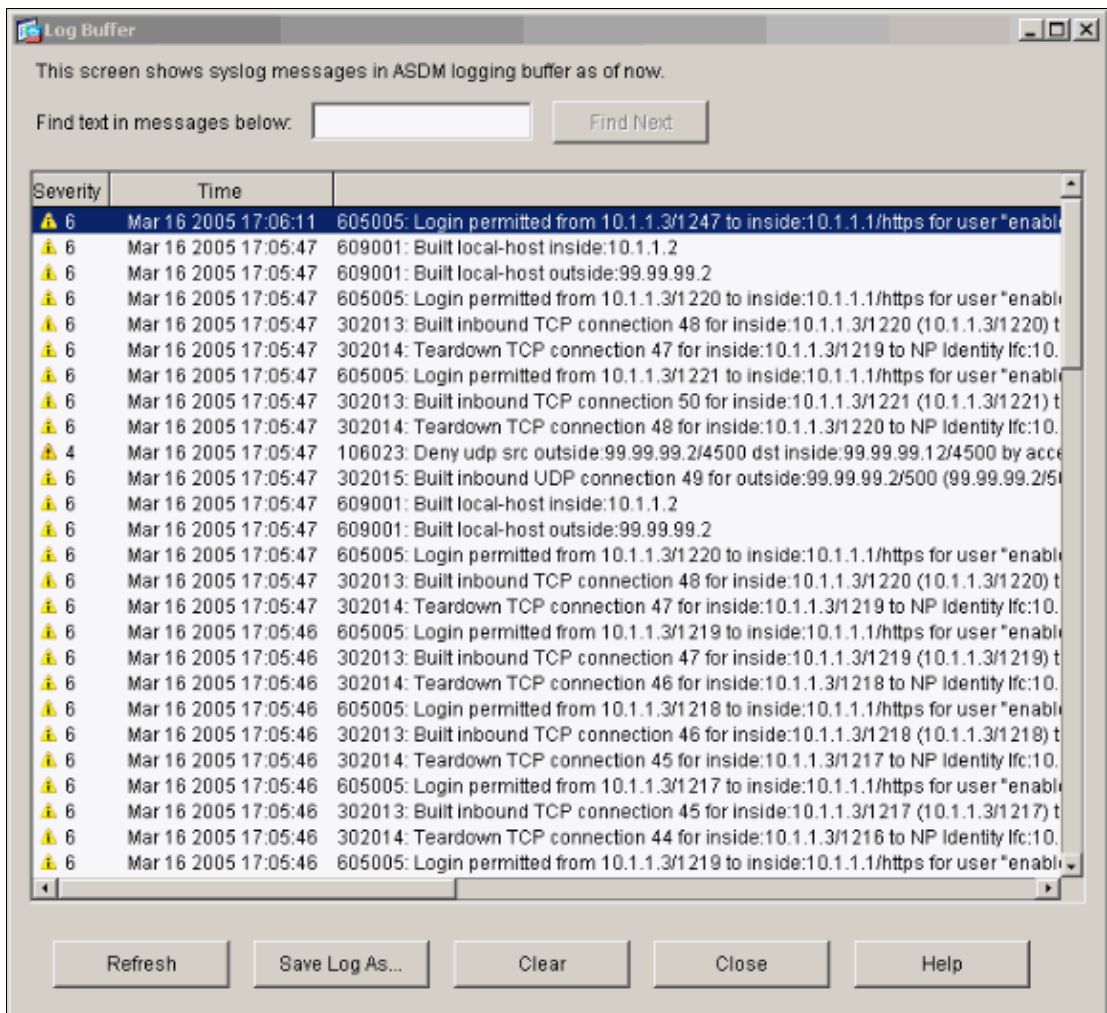
1. Choose **Configuration > Properties > Logging > Logging Setup > Enable Logging** and then click **Apply**.



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



This is an example of the Log Buffer.



## Related Information

- [IPsec Negotiation/IKE Protocols Support Page](#)
- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [NAT Support Page](#)
- [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: Sep 26, 2008

Document ID: 63881