VPN/IPsec with OSPF (PIX Version 7.0 or ASA) Configuration Example

Document ID: 63882

Introduction

This document provides a sample configuration for a VPN/IPsec with Open Shortest Path First (OSPF) on Cisco PIX Security Appliance Software Version 7.0 or Cisco Adaptive Security Appliance (ASA).

PIX 7.0 allows OSPF unicast to run over an existing VPN connection. You no longer need to configure a Generic Routing Encapsulation (GRE) tunnel.

Prerequisites

Requirements

Before you attempt this configuration, ensure that you meet this requirement:

- You can establish the VPN connection.

Components Used

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

- Cisco 3600 that runs Cisco IOS® Software Release 12.3
- Cisco 2600 that runs Cisco IOS Software Release 12.3
- PIX Security Appliance Software Version 7.0

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.

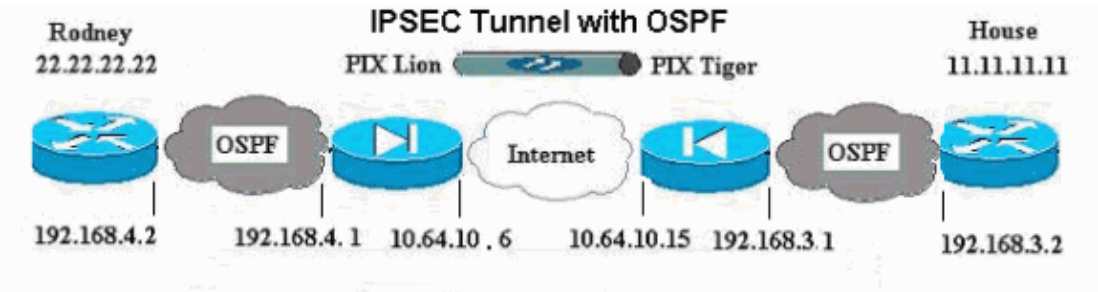
Configure

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:



Configurations

This document uses these configurations:

- Router Rodney
- Router House

Router Rodney

```
version 12.3

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rodney
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!
interface Loopback1
ip address 22.22.22.22 255.255.255.0
!
interface Ethernet0/1
ip address 192.168.4.2 255.255.255.0
!
router ospf 22
log-adjacency-changes
```

```
network 22.22.22.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.4.1
no ip http server
!
line con 0
line aux 0
line vty 0 4
login
!
end!
End
```

Router House

```
version 12.3


service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback1
ip address 11.11.11.11 255.255.255.0
!
interface FastEthernet0/1
ip address 192.168.3.2 255.255.255.0
!
router ospf 11
log-adjacency-changes
network 11.11.11.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
ip http server
!
line con 0
line aux 0
line vty 0 4
```

Configure the PIX Security Appliance Version 7.0

You can configure the PIX Security Appliance by either command−line interface (CLI) or GUI, with use of the Advanced Security Device Manager (ASDM). The configuration in this section is for the PIX "Lion". You configure the PIX "Tiger" in the same way. This document does not demonstrate the PIX Tiger configuration with the ASDM example. However, you can find CLI configurations for both in the Use ASDM section.

In order to configure the PIX Security Appliance version 7.0, console into the PIX. From a cleared configuration, use the interactive prompts in order to enable the ASDM GUI for the management of the PIX from workstation 10.1.1.5.

PIX/ASDM Bootstrap

```
Pre-configure Firewall now through interactive prompts [yes]?
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Aug]:
  Day [6]:
  Time [06:00:44]:
Inside IP address: 192.168.4.1
Inside network mask: 255.255.255.0
Host name: lion
Domain name: cisco.com
IP address of host running Device Manager: 192.168.4.50

The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 06:00:44 Aug 6 2005
Firewall Mode: Routed
Inside IP address: 192.168.4.1
Inside network mask: 255.255.255.0
Host name: lion
Domain name: cisco.com
IP address of host running Device Manager: 192.168.4.50

Use this configuration and write to flash? yes
INFO: Security level for "inside" set to 100 by default.
Cryptochecksum: 34f55366 a32e232d ebc32ac1 3bfa201a

969 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
```

Use ASDM

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

1. From workstation 192.168.4.50, open a browser and use ADSM.

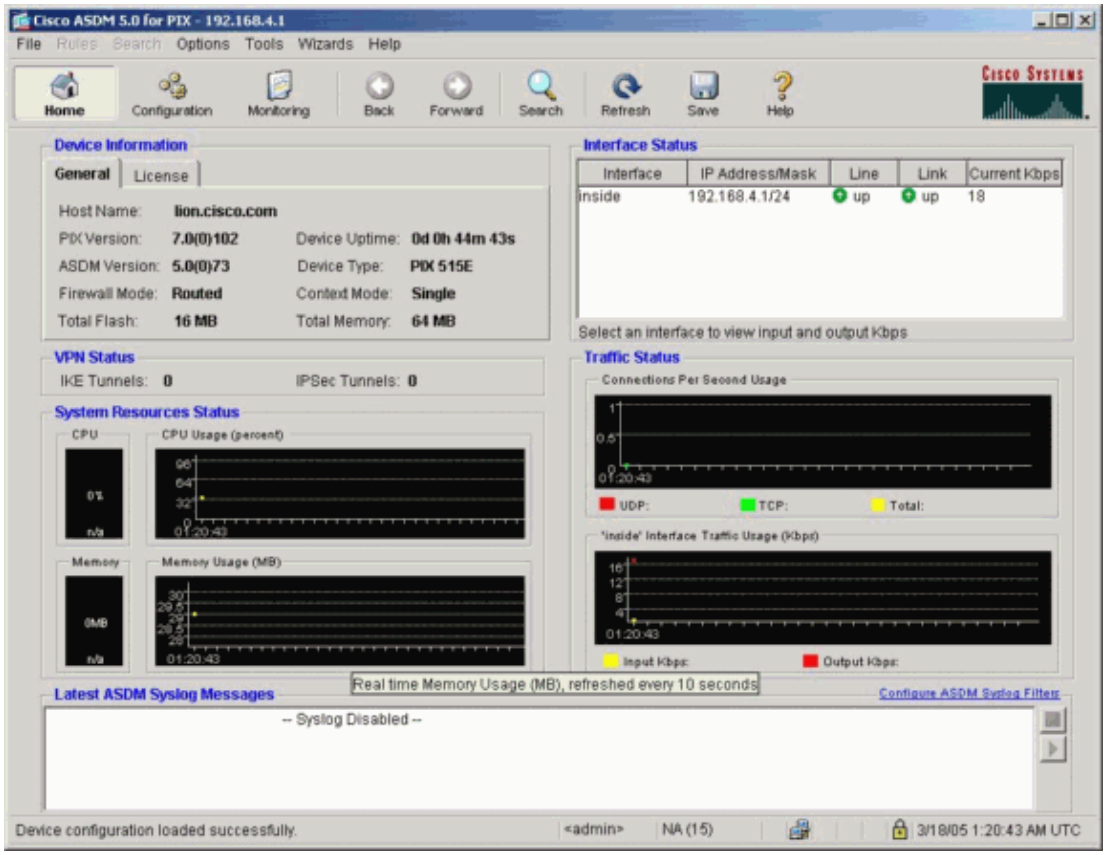
   In this example, you use https://192.168.4.1.
2. Click **Yes** on the certificate prompts.
3. Log in with the enable password.

   This login appears in the PIX/ASDM Bootstrap configuration.
4. At the prompt to use ASDM Launcher or ASDM as a Java App, make a selection.

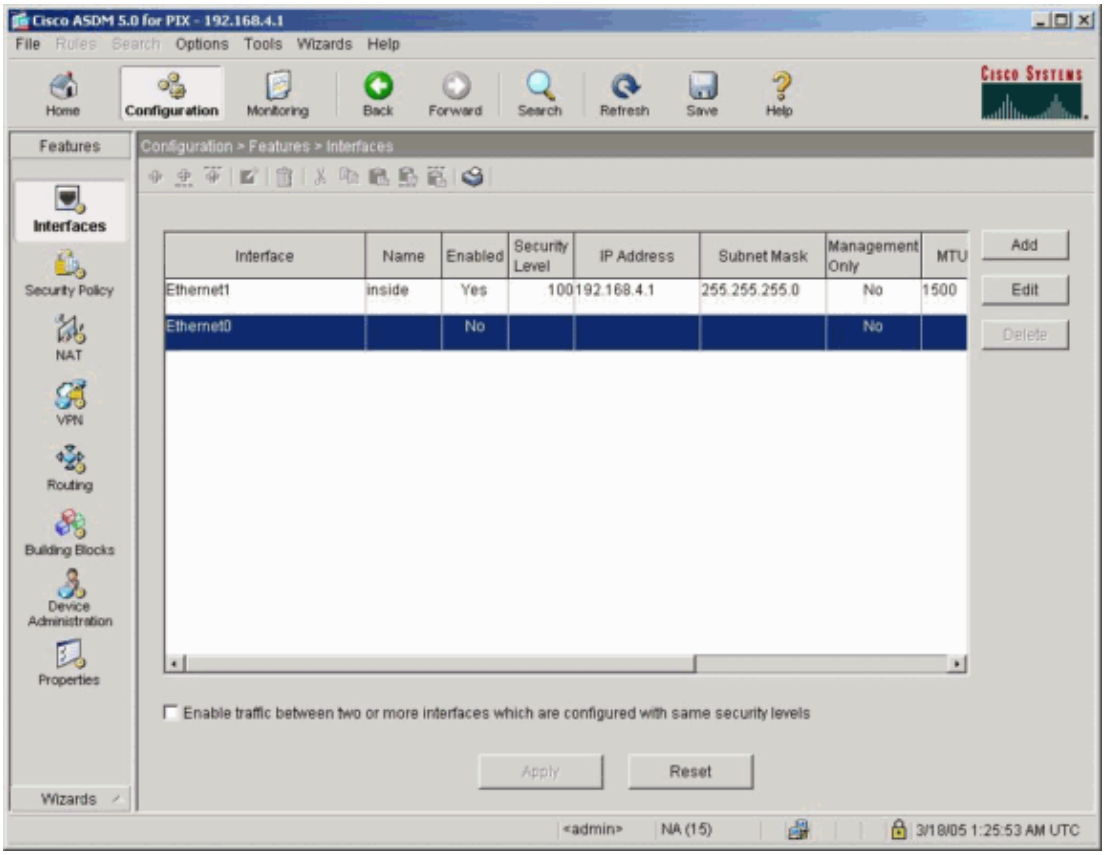
This prompt appears only if this is the first time that you have run ASDM on the PC.

This example has selected and installed the ASDM Launcher.

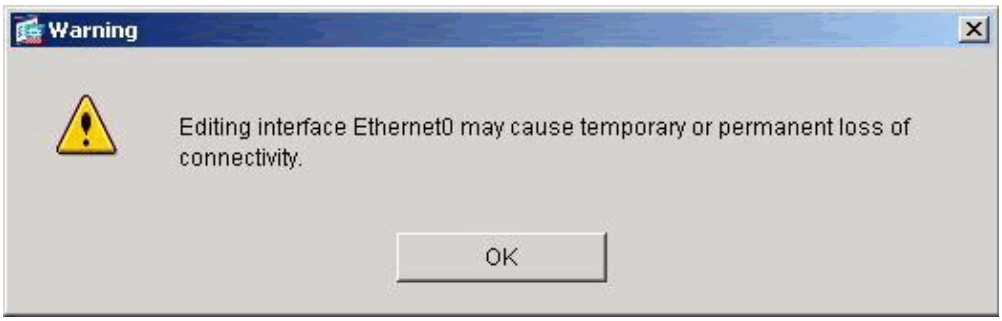
5. Go to the ASDM Home screen and click the **Configuration** tab.



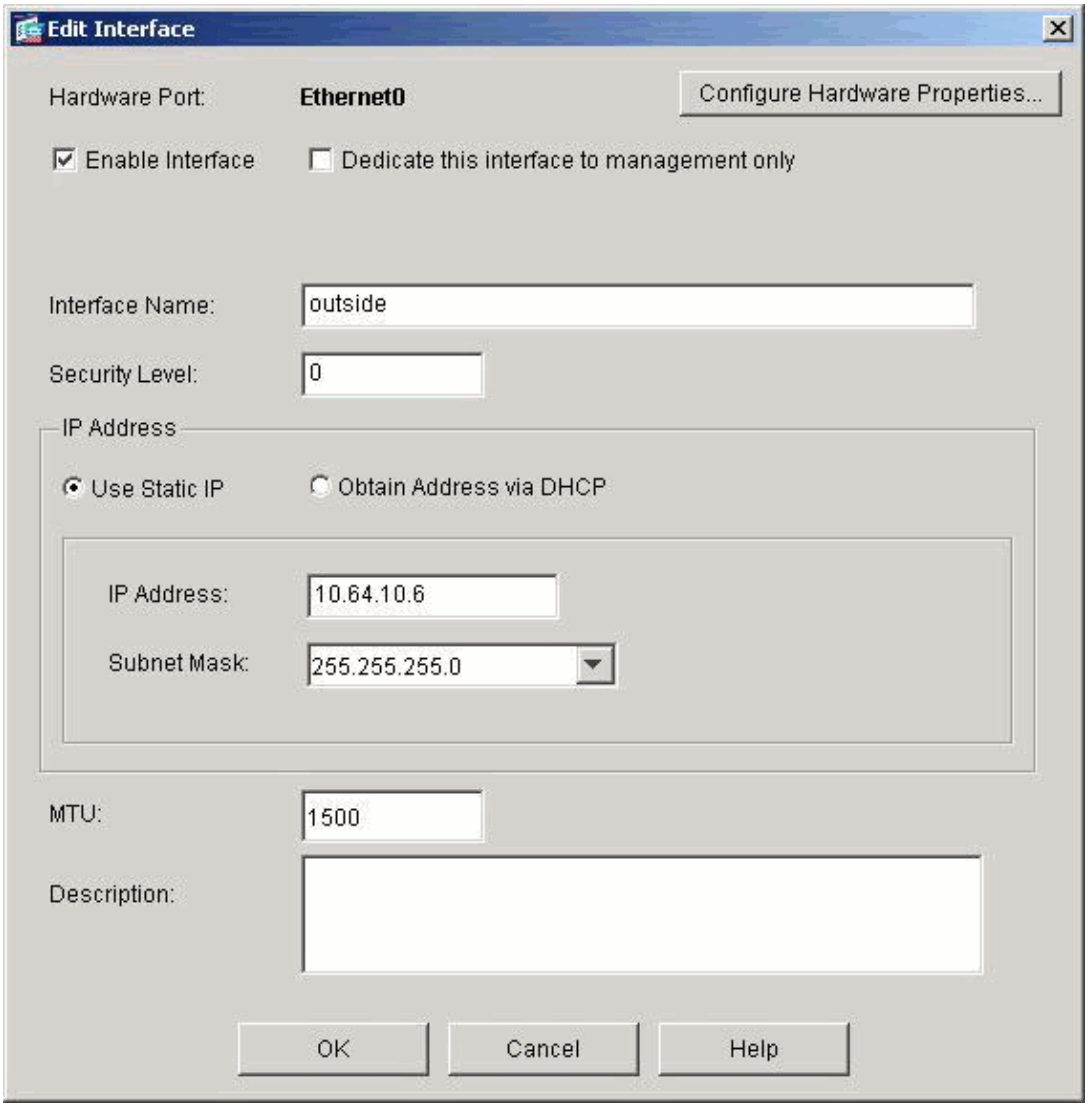
6. In order to configure the outside interface, choose **Interface** > **Edit**.



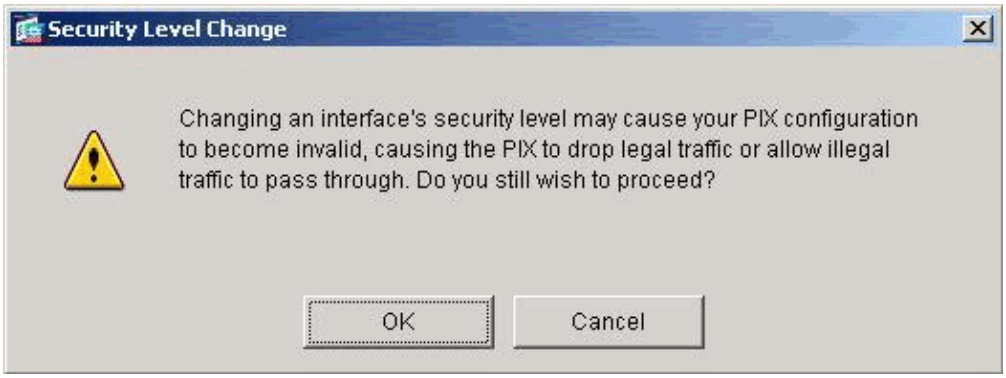
7. Click **OK** in the editing interface dialog box.



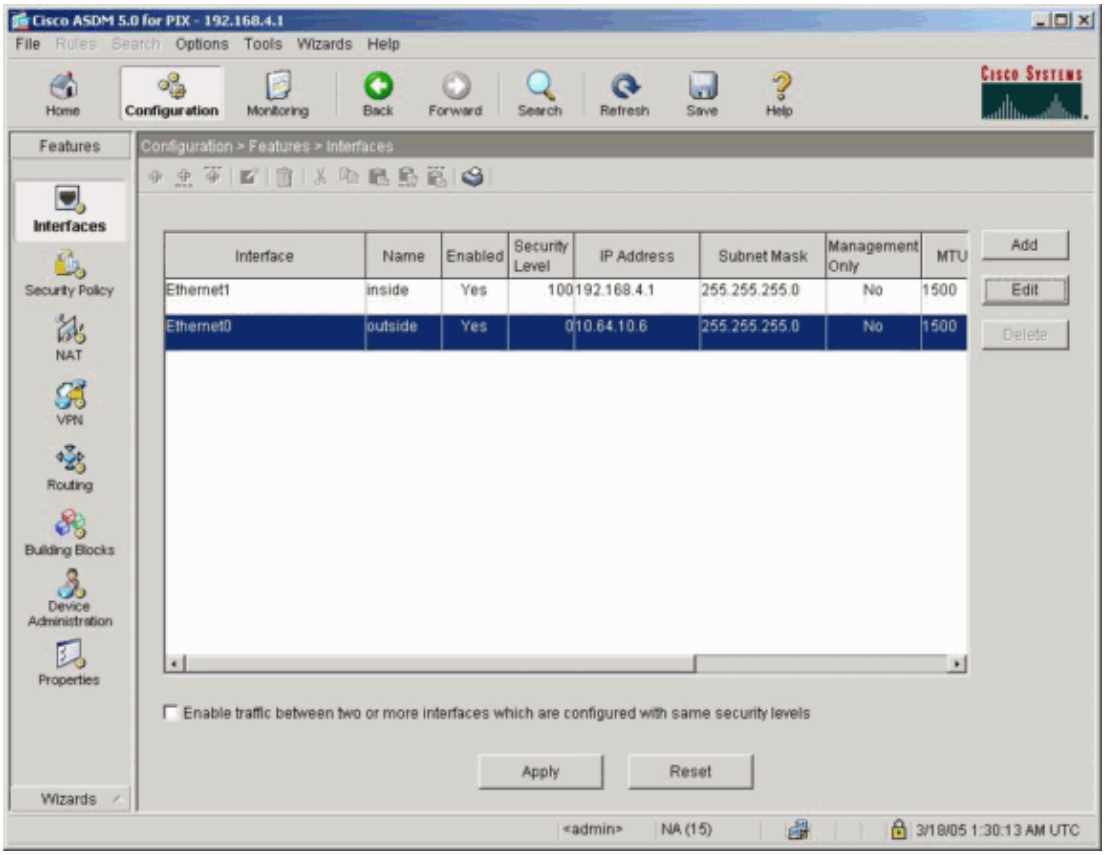
8. Enter the interface details and click **OK** when complete.



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



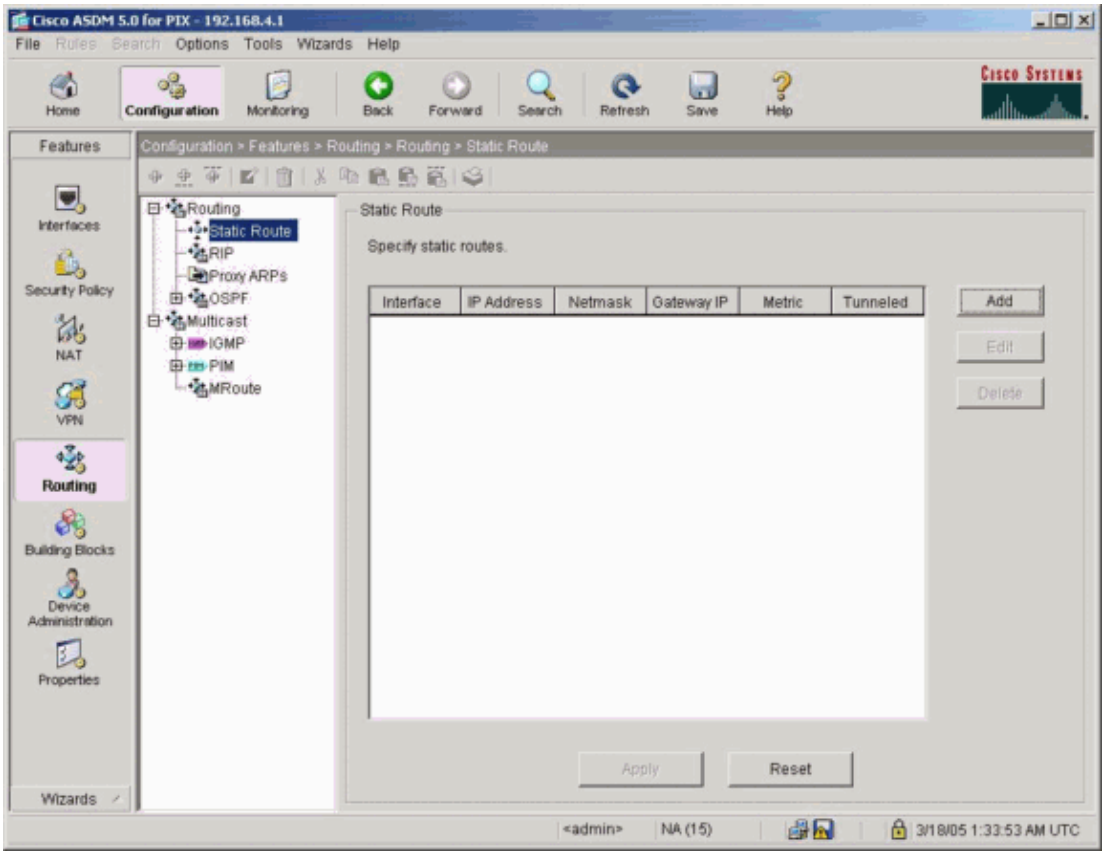
10. In order to accept the interface configuration, click **Apply**.



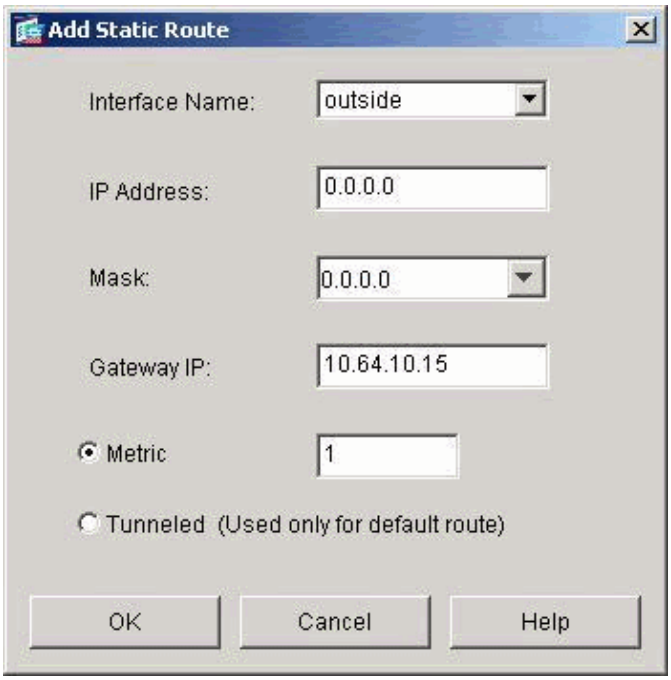
The configuration also gets pushed onto the PIX.

Note: This example uses static routes.

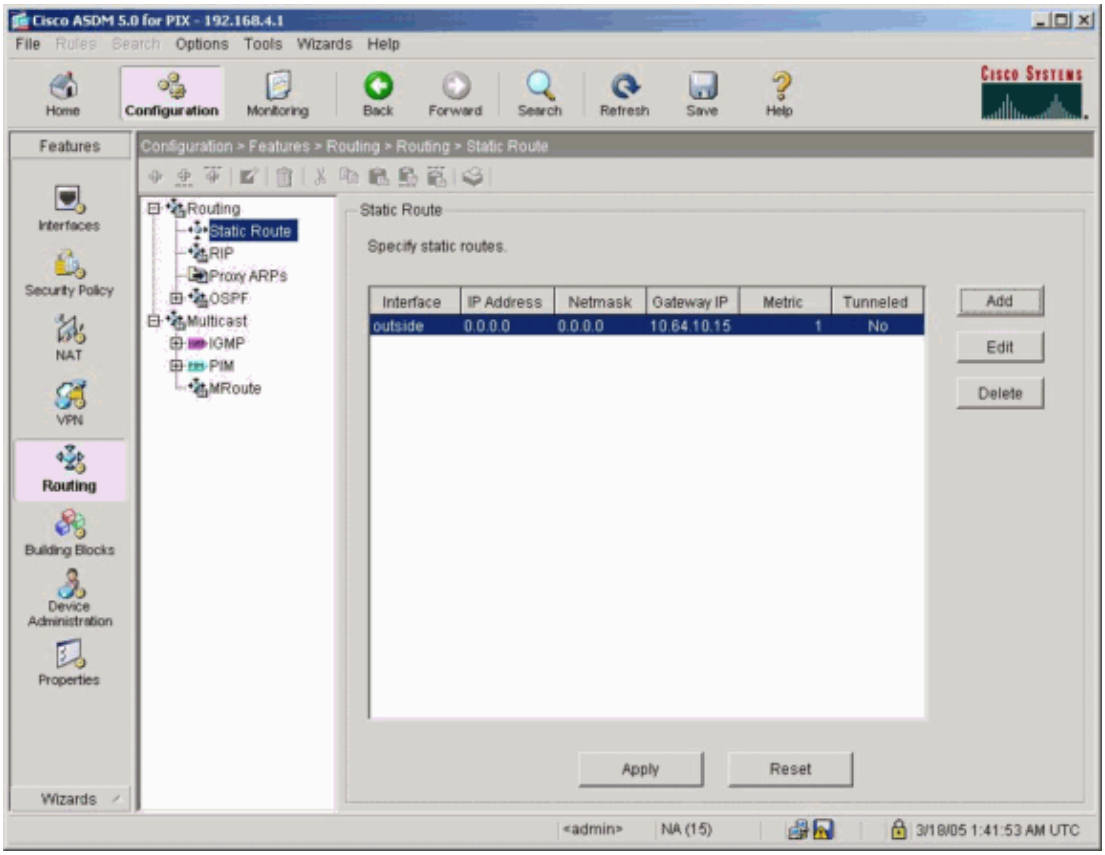
11. Choose **Features > Routing**, then choose **Static Route > Add**.



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

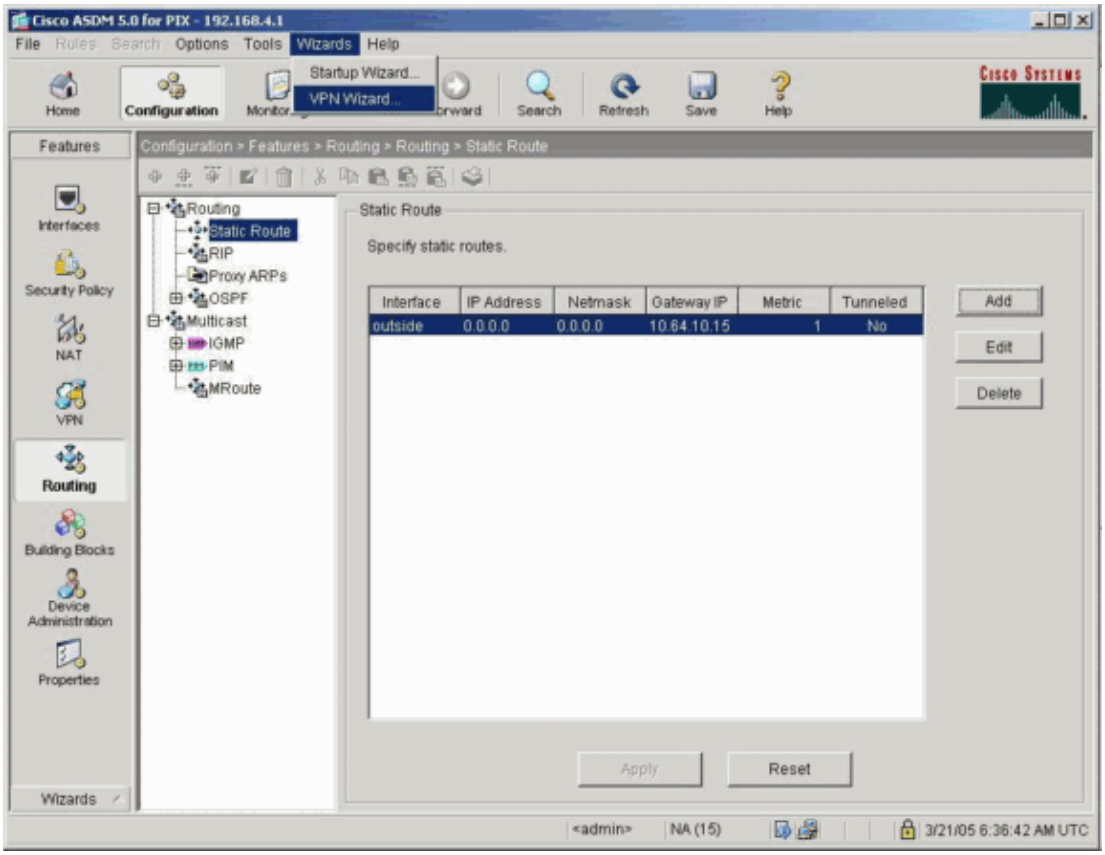


13. In order to accept the interface configuration, click **Apply** .

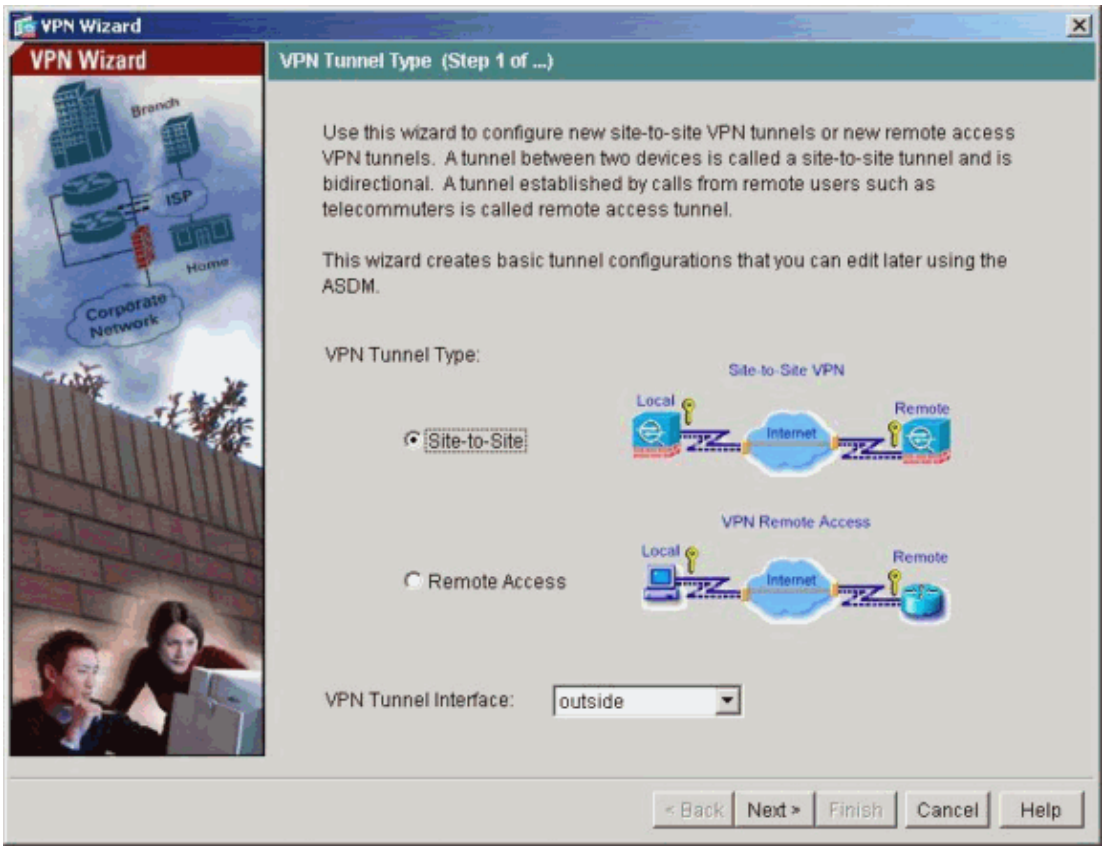


The configuration also gets pushed onto the PIX.

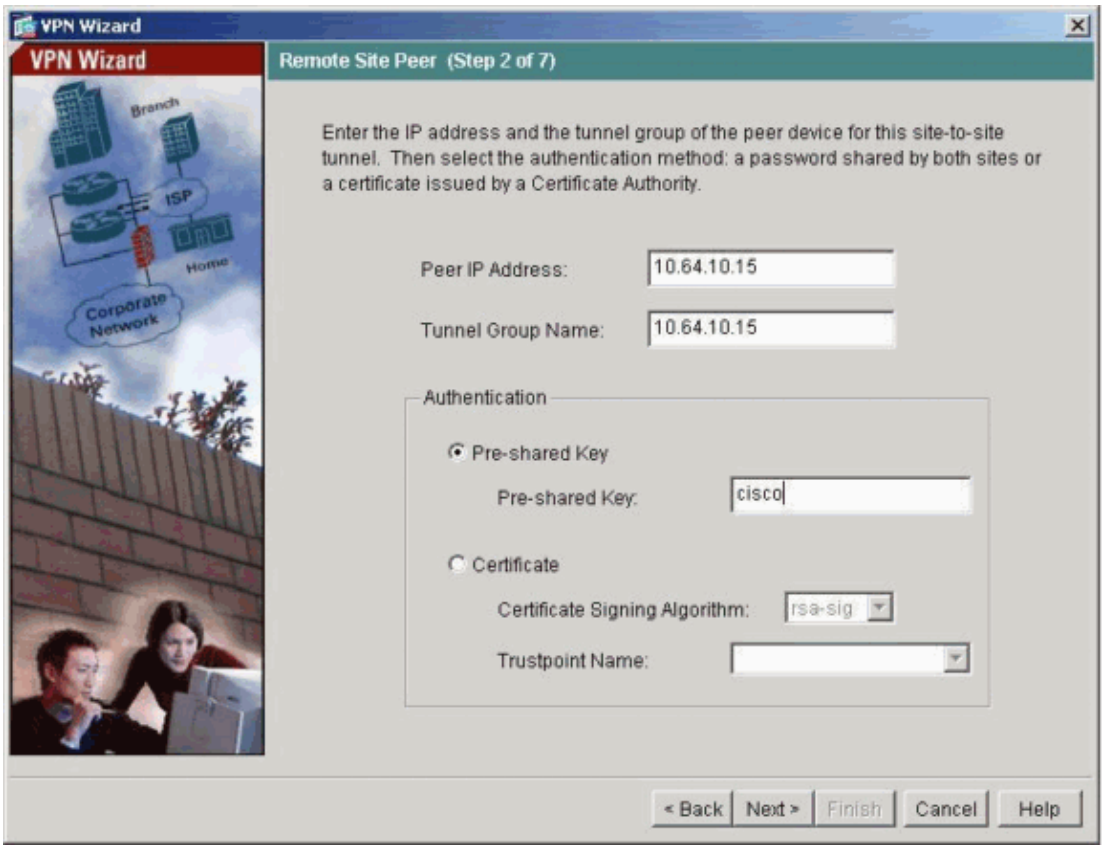
14. In order to use the VPN Wizard and create the LAN−to−LAN connection, choose **Wizards > VPN Wizard...**.



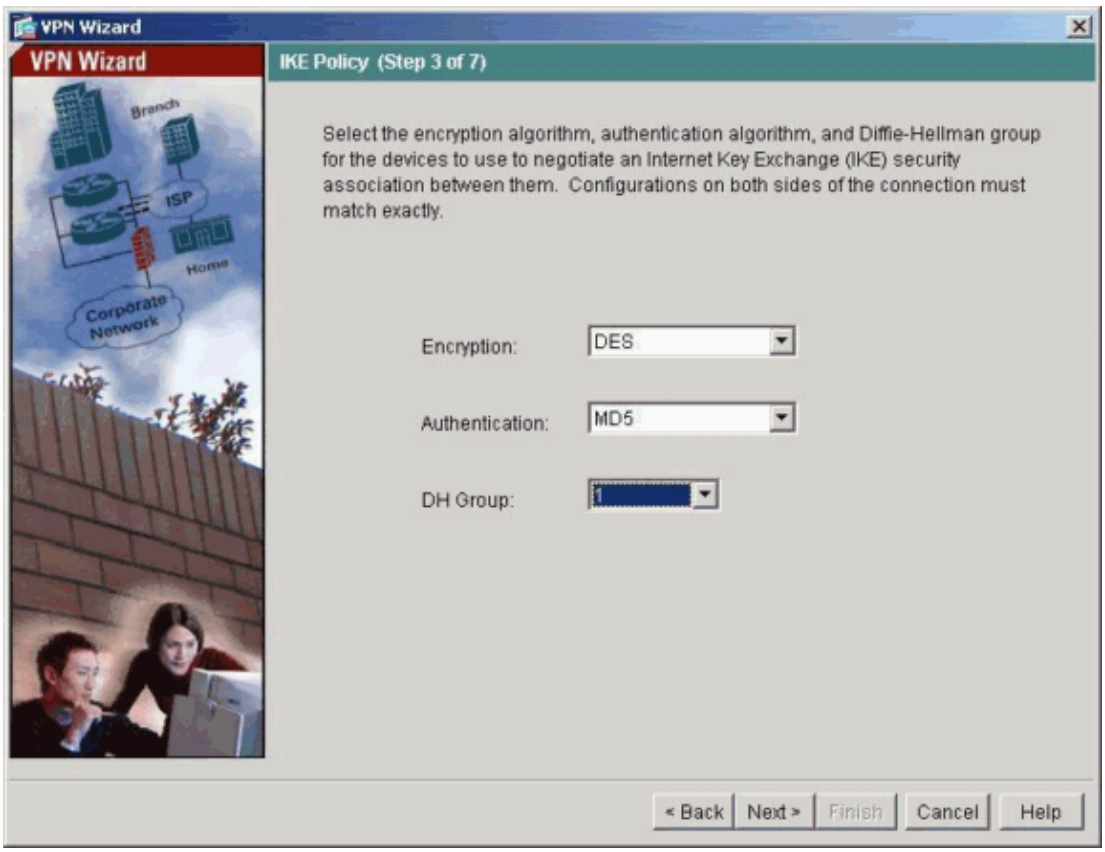
15. In the VPN Wizard window, where Site−to−Site is the default selection, click **Next**.



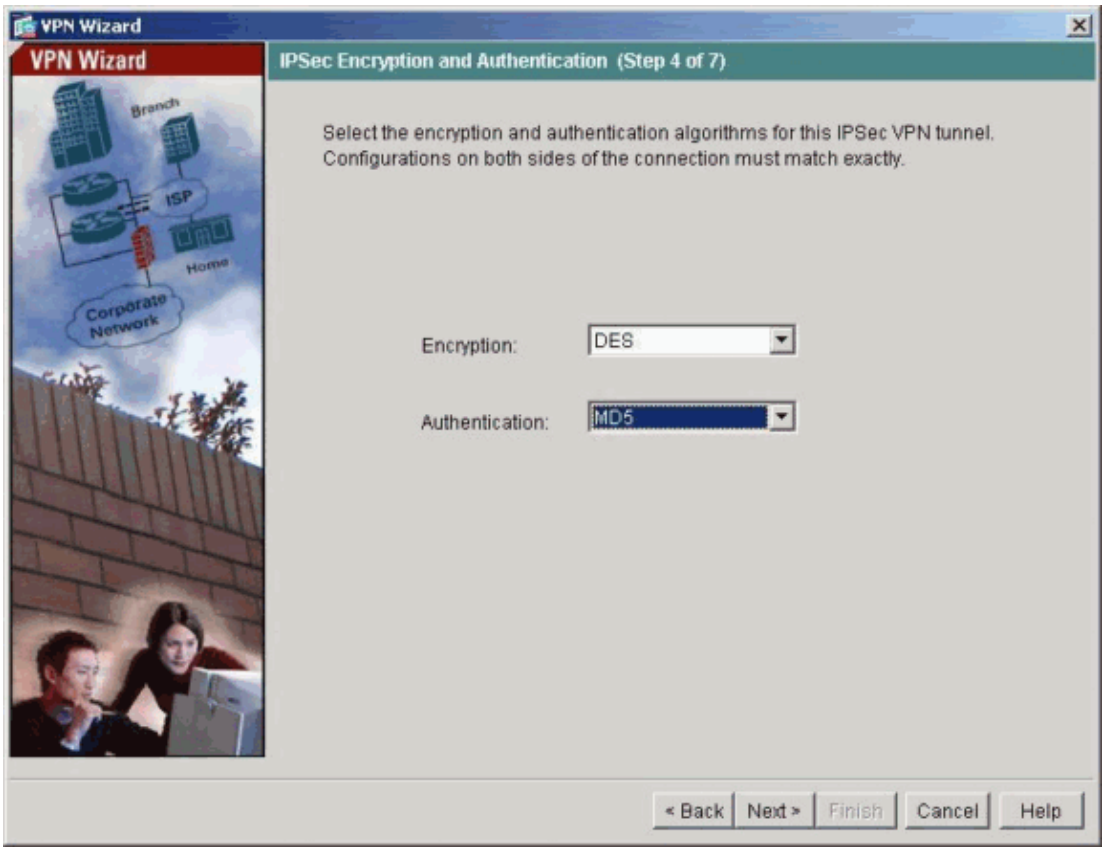
16. Add the Peer IP Address, Tunnel Group Name (which is the IP address), and Pre−Shared Key information, and click **Next**.



17. Add the Encryption type, Authentication type, and DH Group information, and click **Next**.

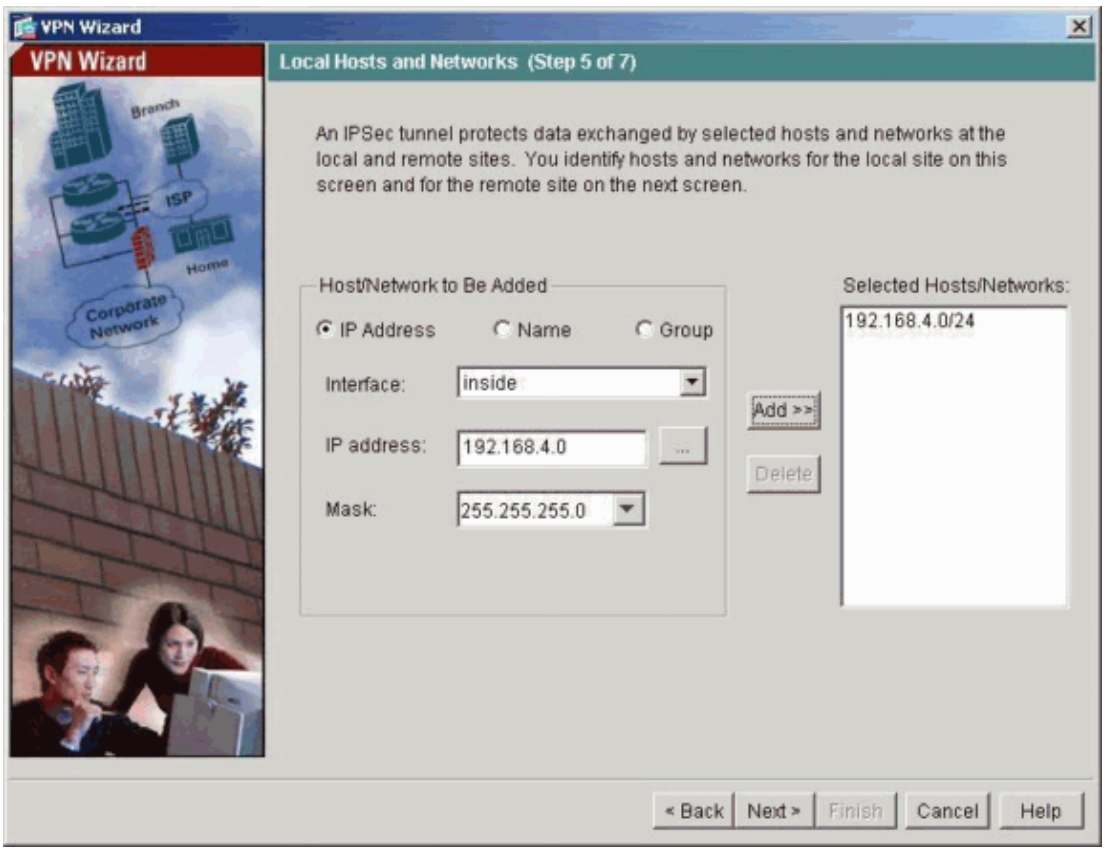


18. Add the IPsec parameters, Encryption type, and Authentication type information, and click **Next**.



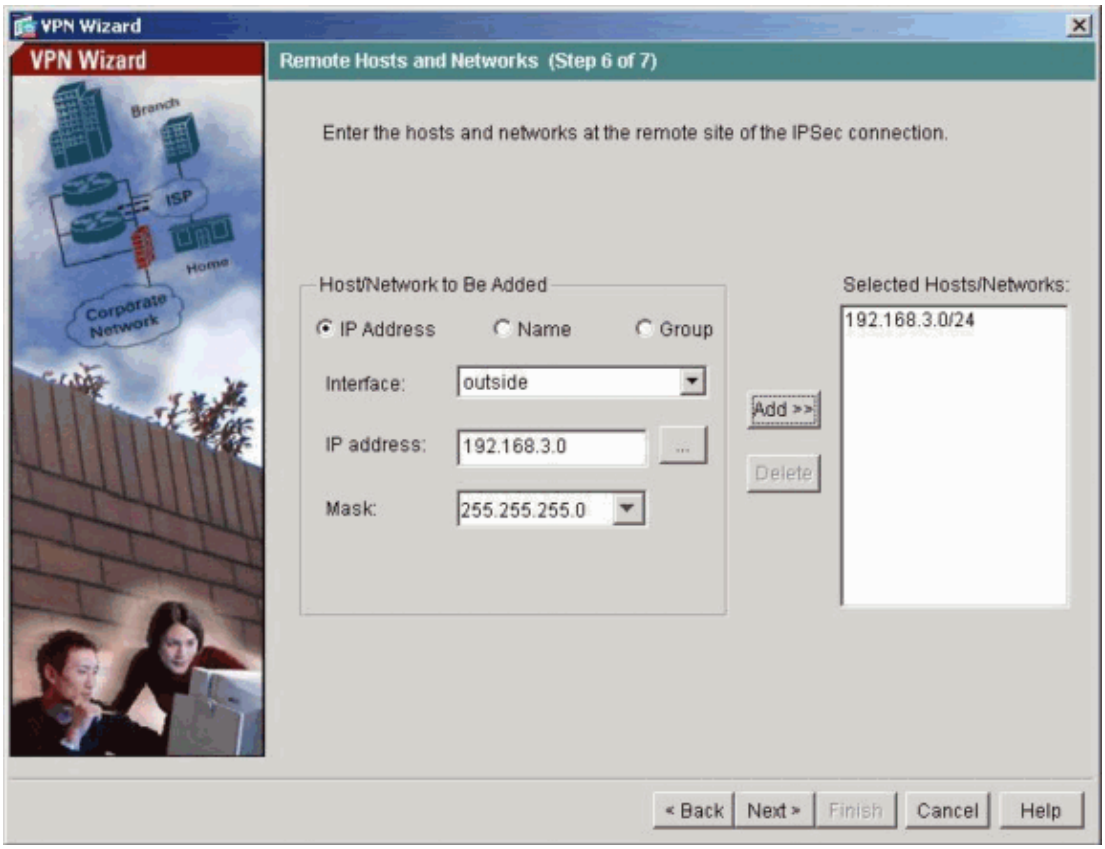
19. Configure the inside host network.

    In order to move the address to the Selected Host/Networks field within this window, click **Add**. When complete, click **Next**

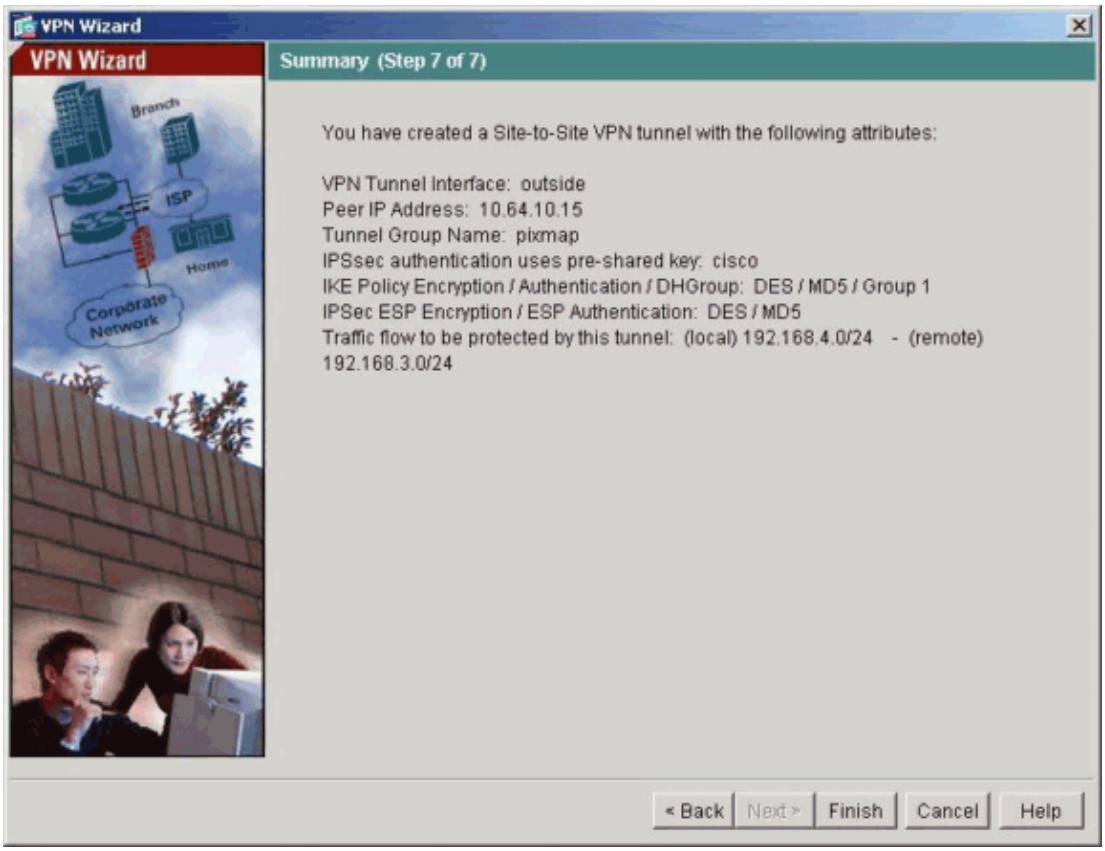


20. Configure the outside host network.

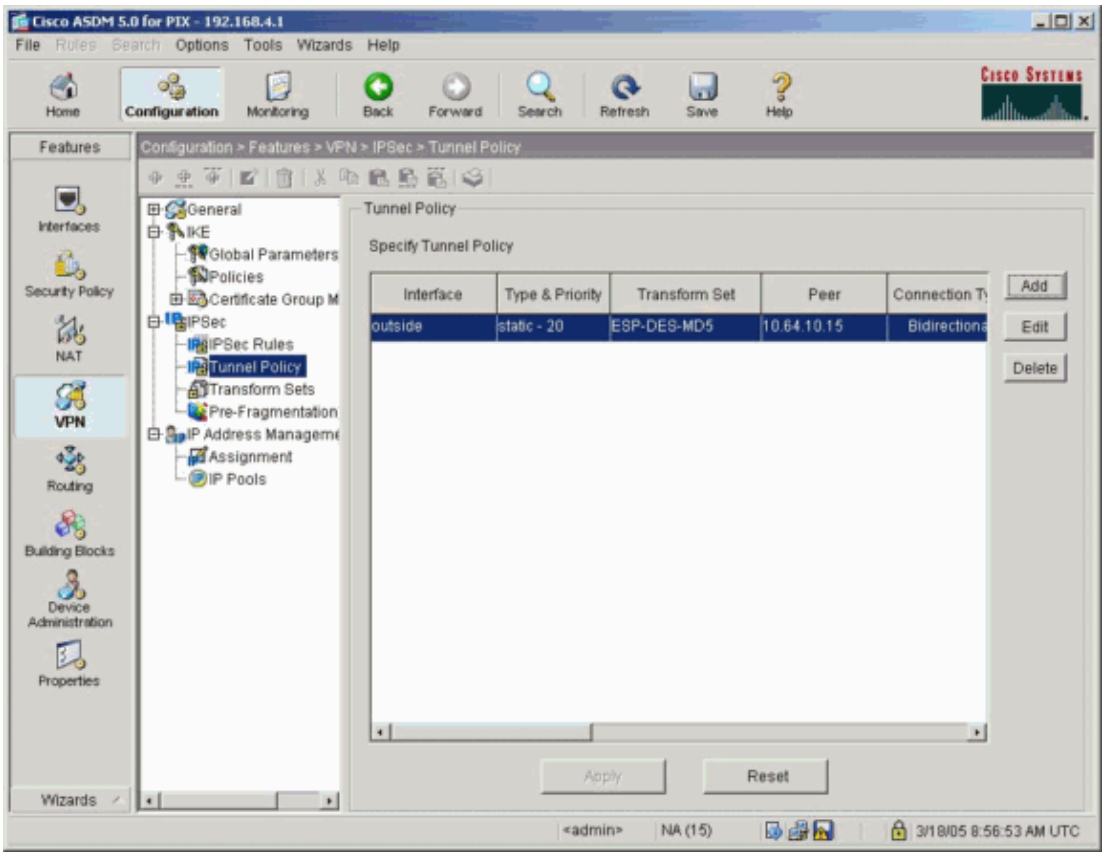
    In order to move the address to the Selected Host/Networks field within this window, click **Add**. When complete, click **Next**.



21. Review the Summary for accuracy, then click **Next**.

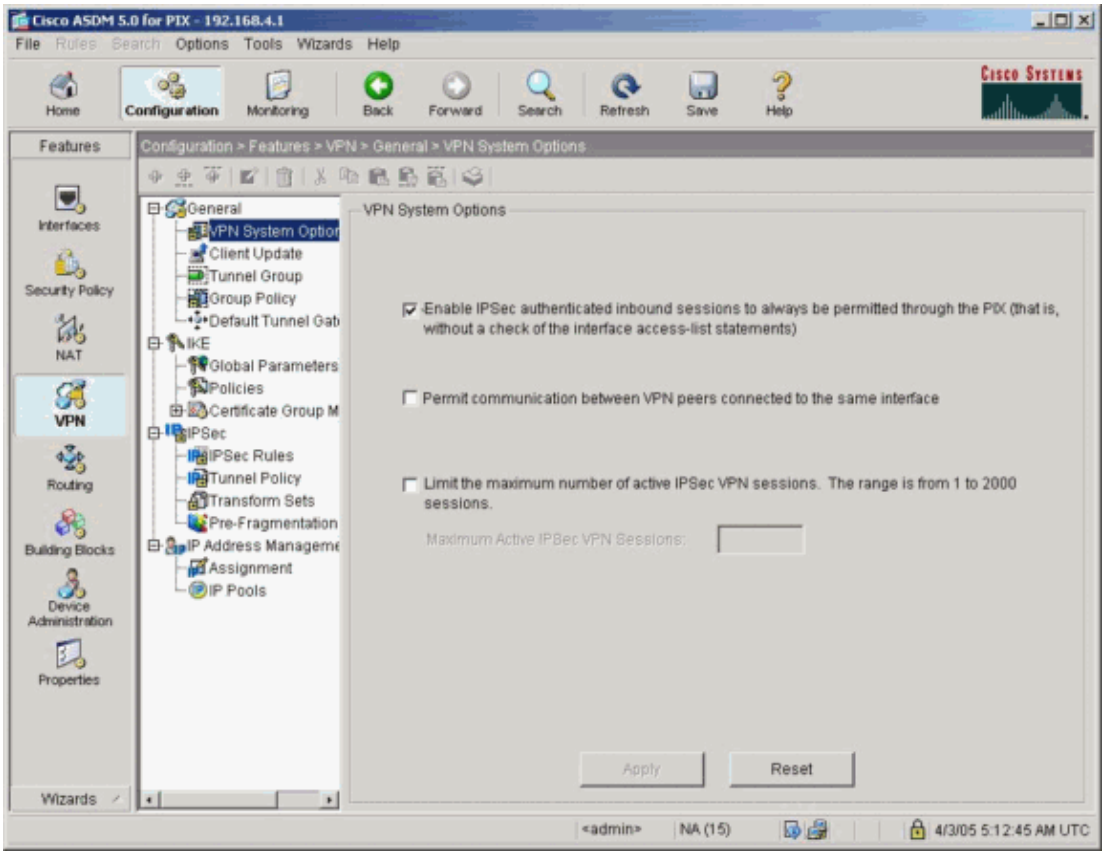


22. In order to verify the LAN−to−LAN tunnel configurations that the VPN Wizard created, choose **Configuration > VPN**.

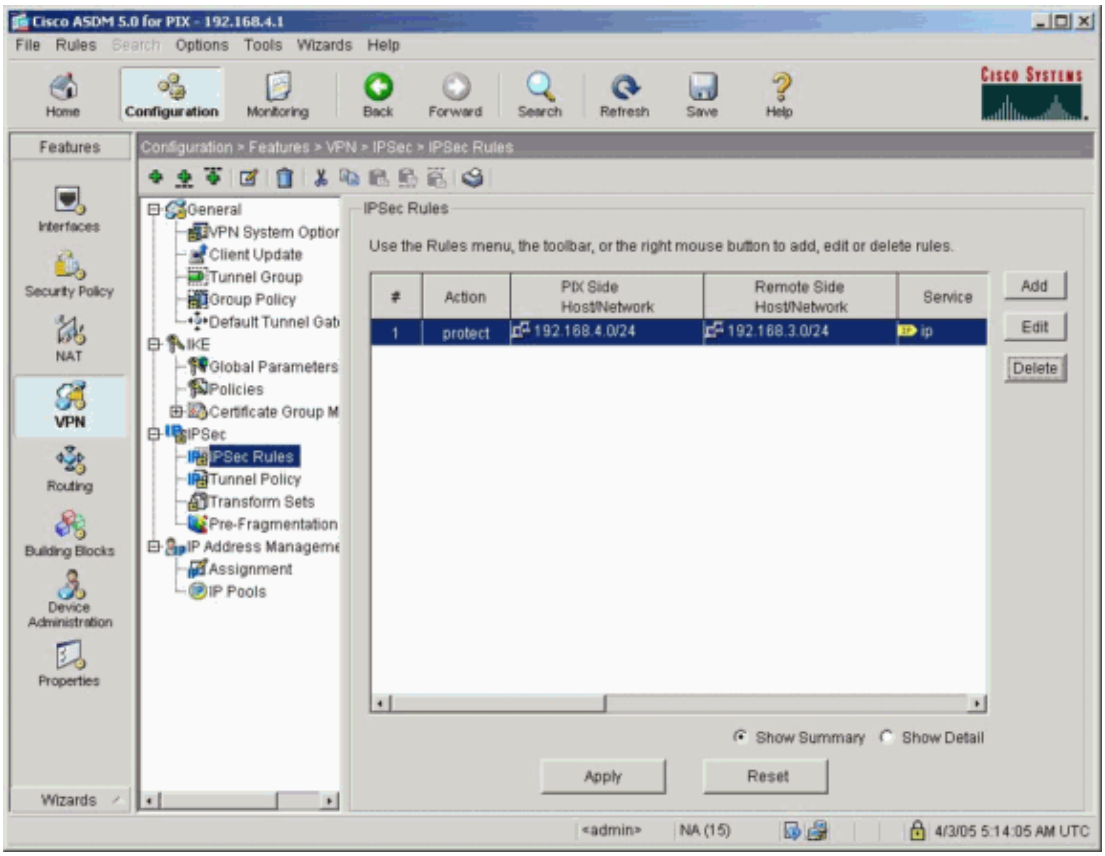


23. Create an access list in order to allow OSPF traffic to go across the VPN.

This VPN access list is for the OSPF routes that are learned. Choose **Configuration > VPN**.

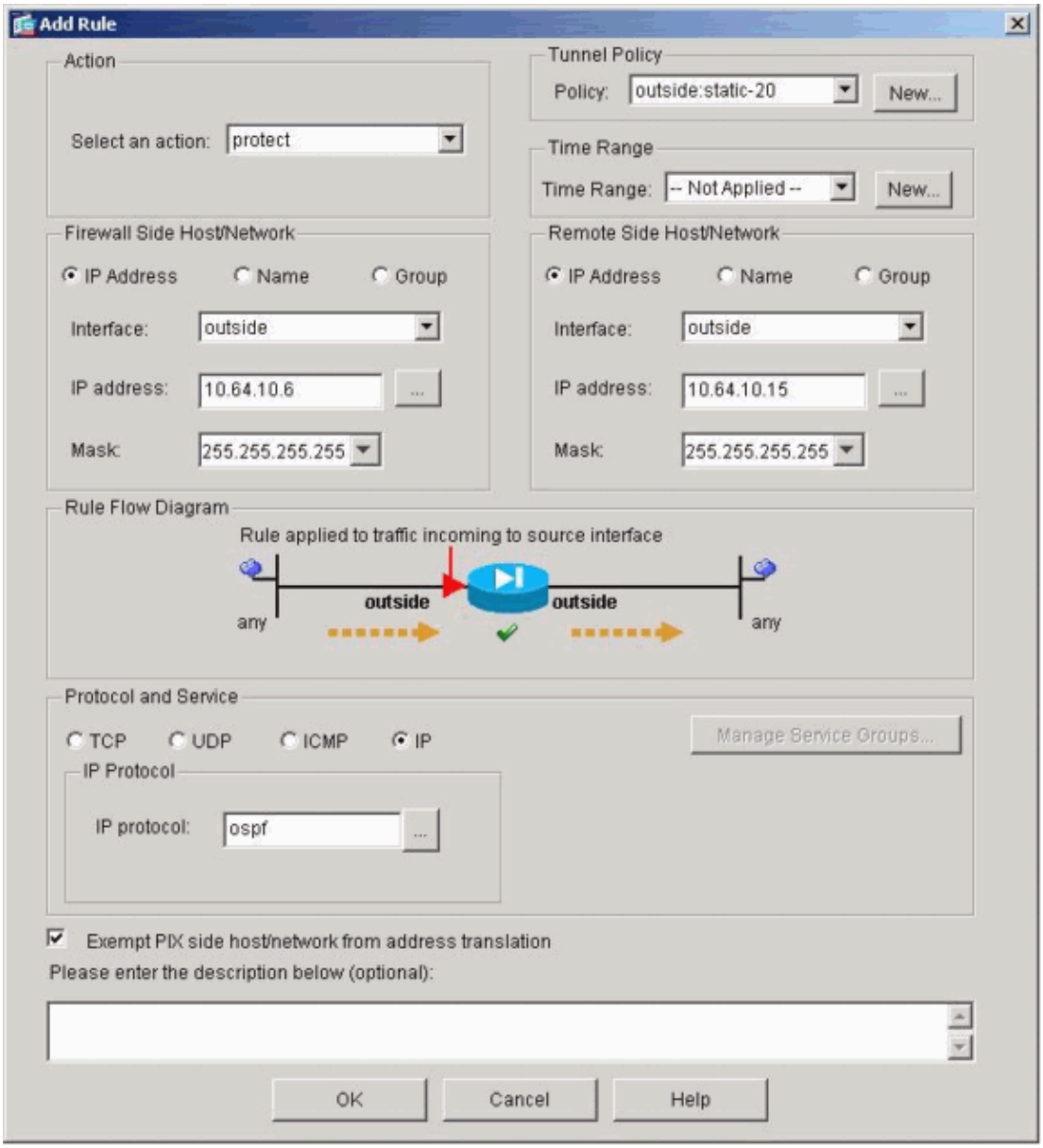


24. Choose **IPSec > IPSec Rules > Add**.

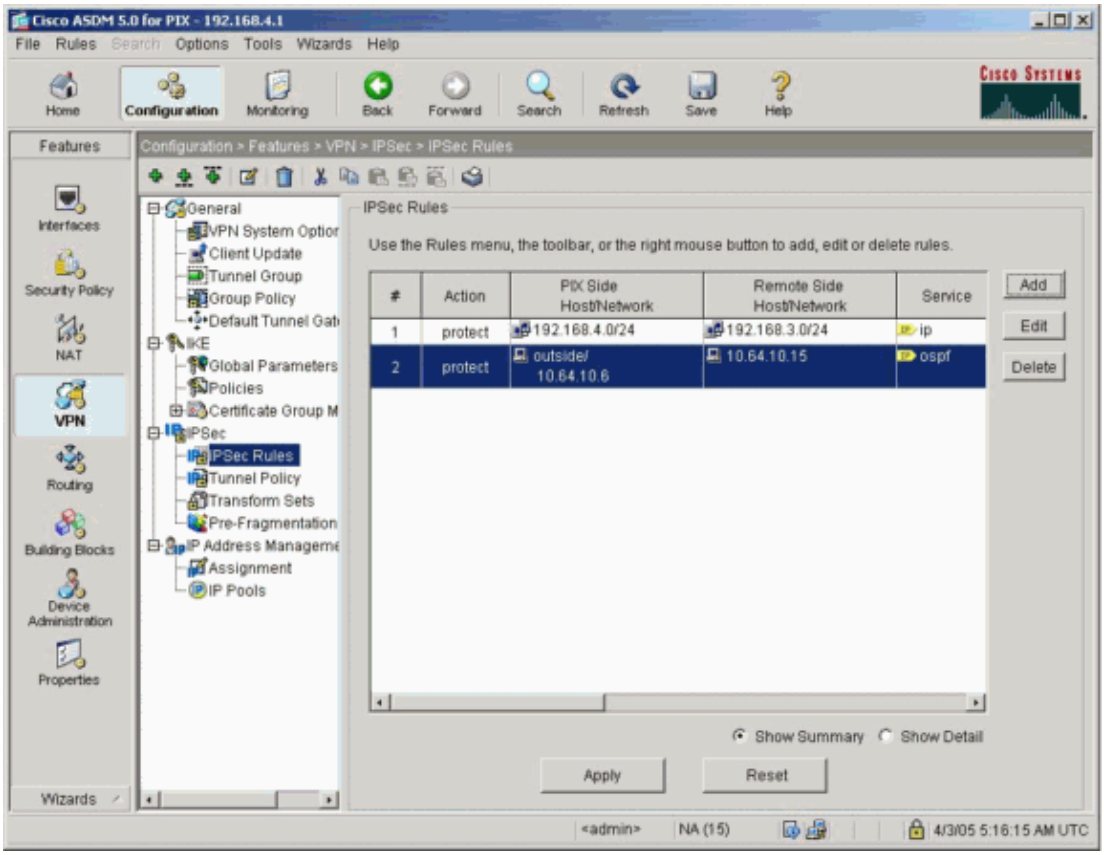


25. Add the OSPF neighbor (IP Address) data in this window and click **OK**.

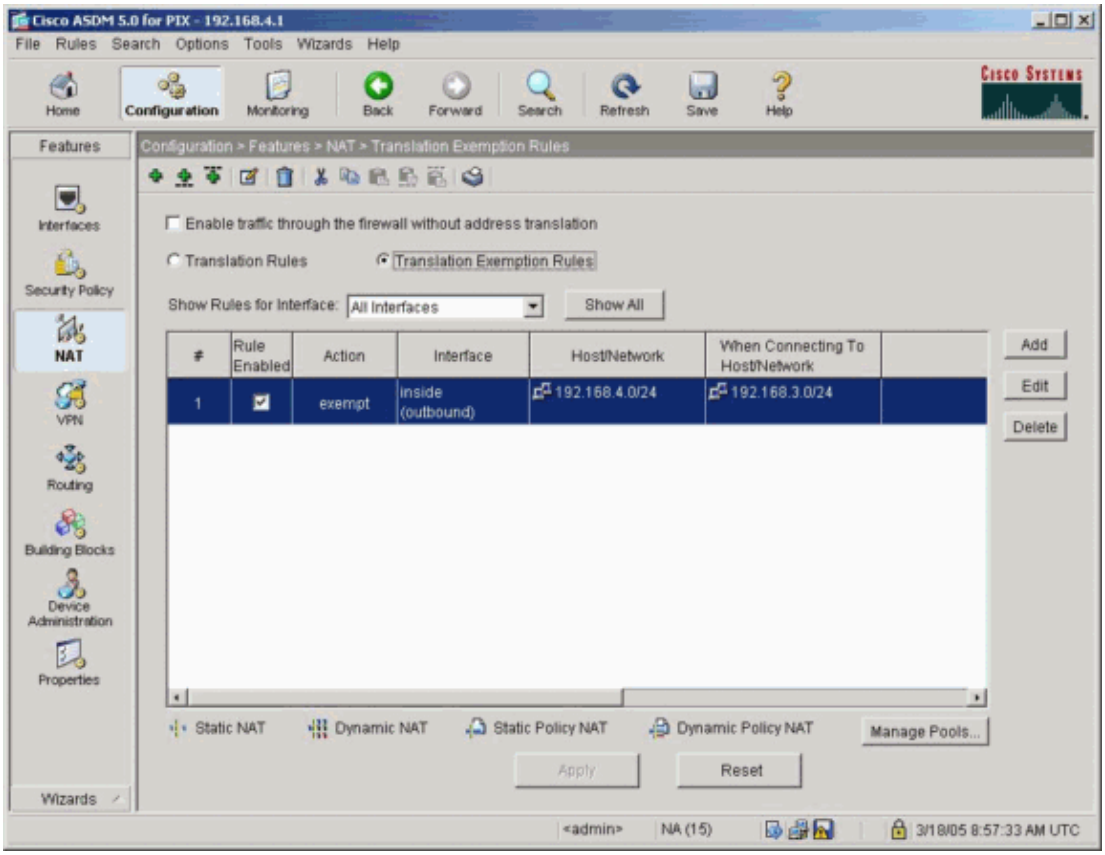
Note: Be sure that you work on the outside interface.



26. Verify that the information is correct and click **Apply**.



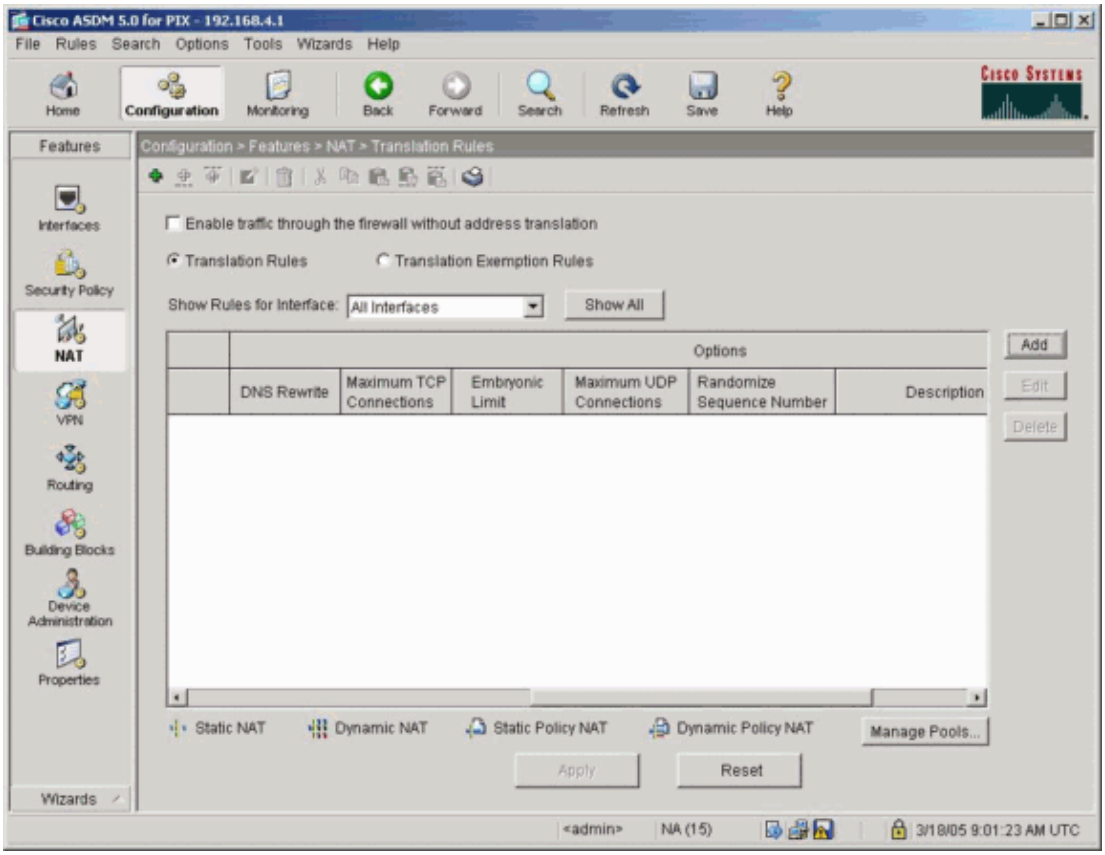
27. In order to verify the Network Address Translation (NAT) configurations that the VPN Wizard created, choose **Configuration > NAT > Translation Exemption Rules**.



28. Because this example uses NAT, uncheck the check box for **Enable traffic through the firewall**

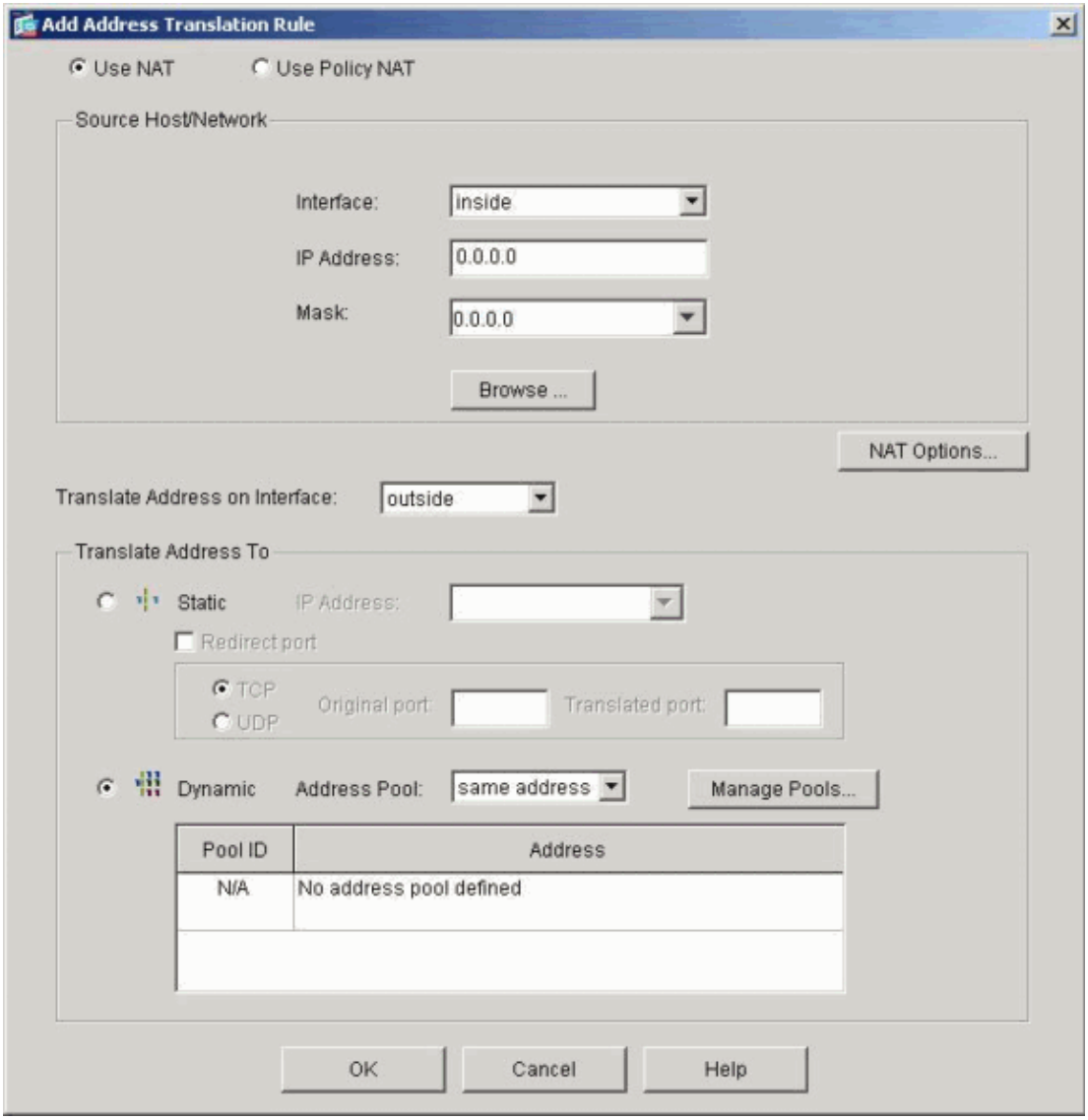
without address translation, then click **Add**.

This step configures the NAT Rule.

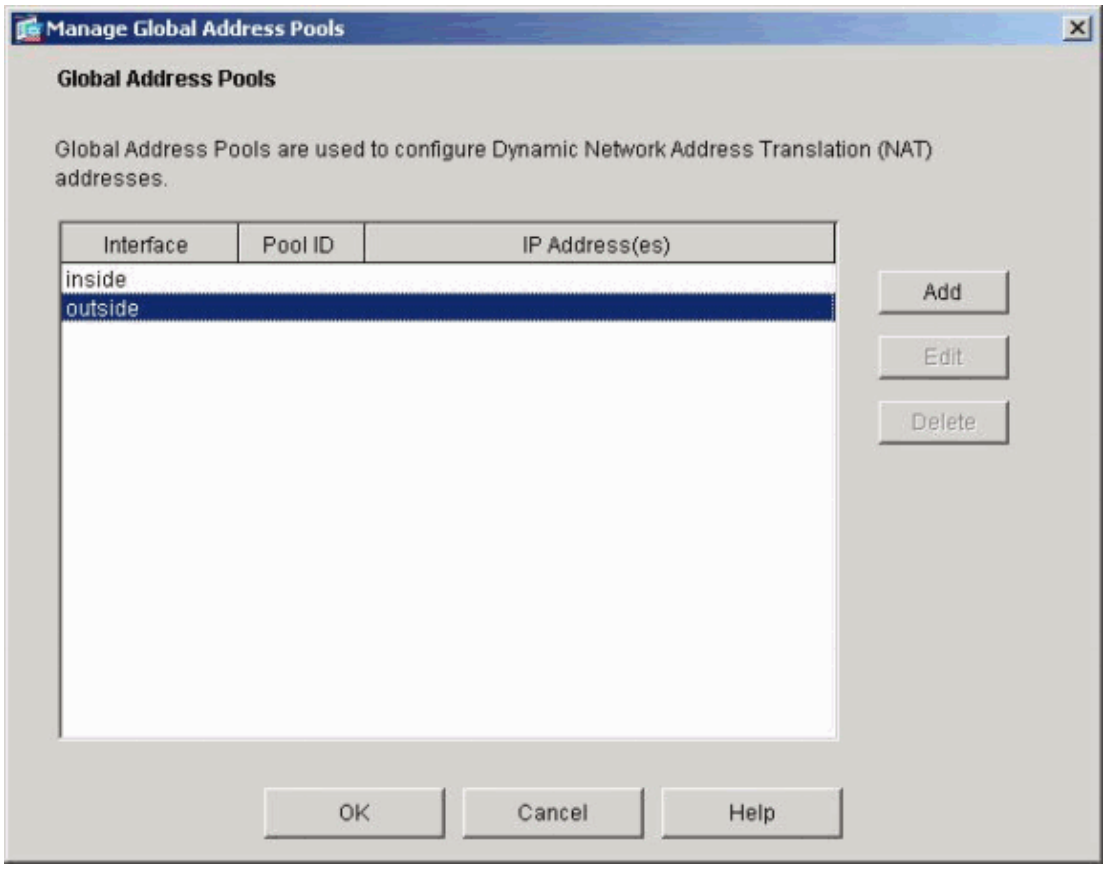


29. Configure the Source Network.

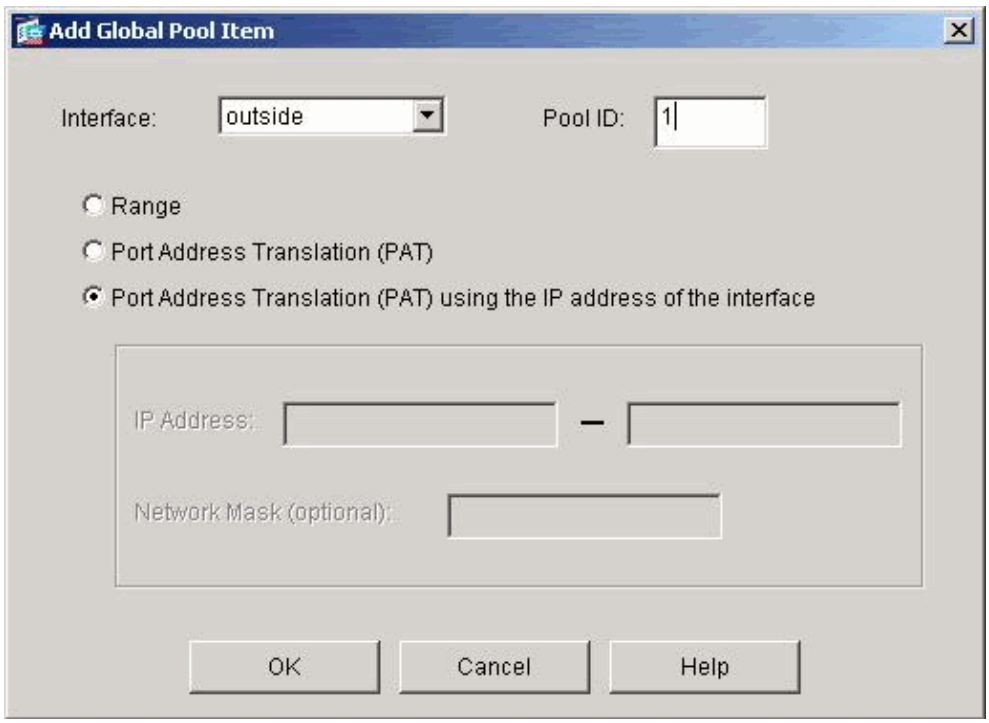
    Choose **any > Manage Pools** to define the NAT pool addresses.



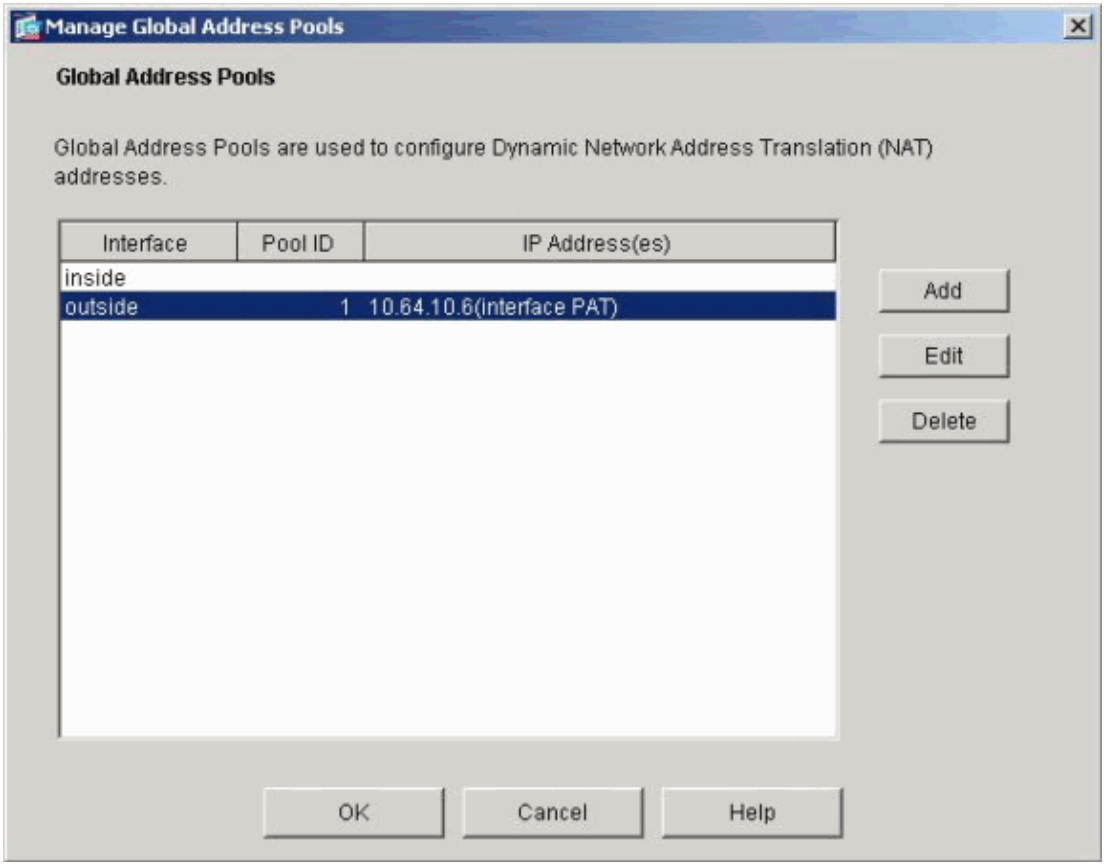
30. Select the **outside** interface and click **Add**.



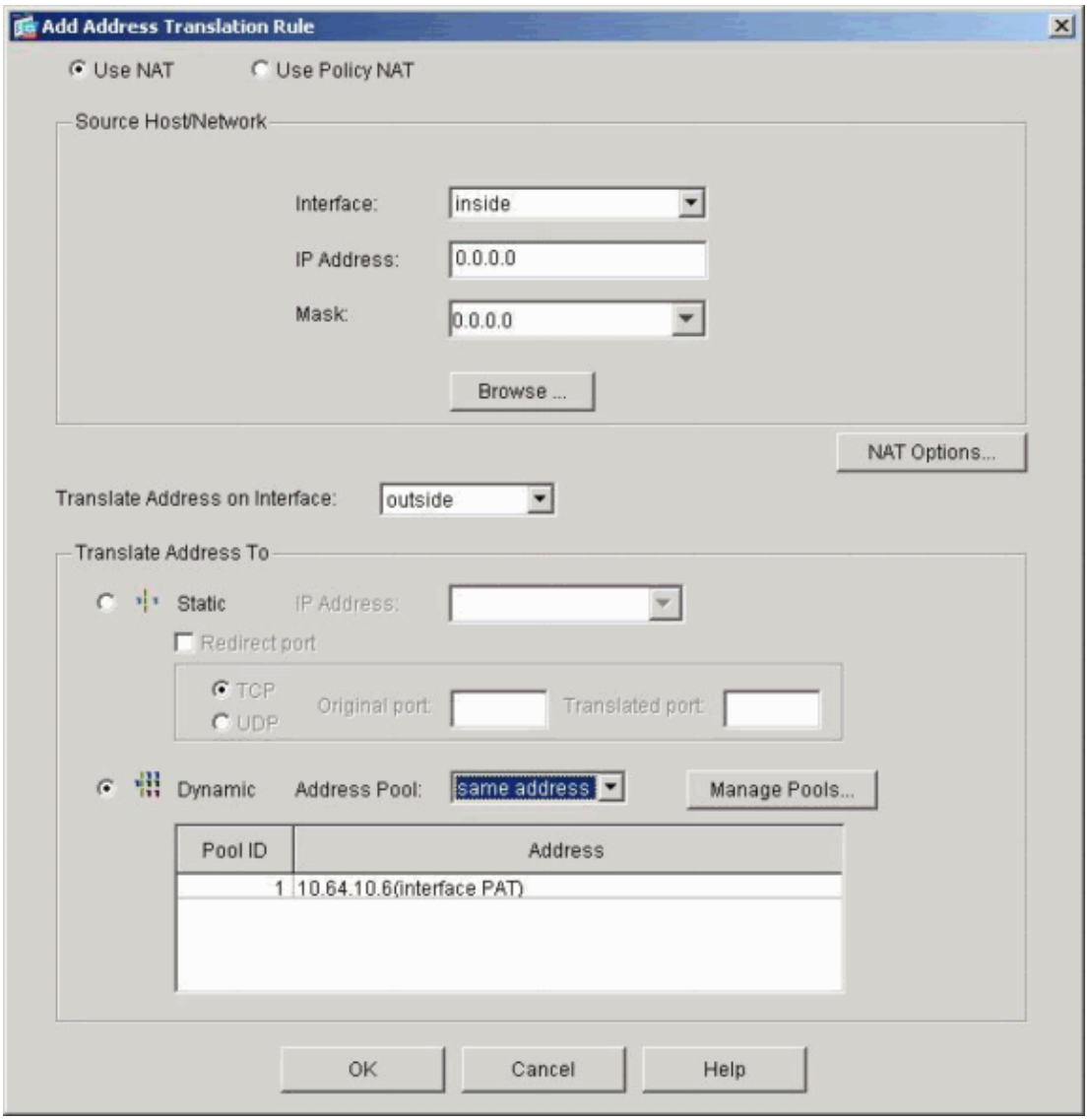
31. Because Port Address Translation (PAT) uses the IP address of the interface in this example, click the **Port Address Translation (PAT) using the IP address of the interface** radio button.



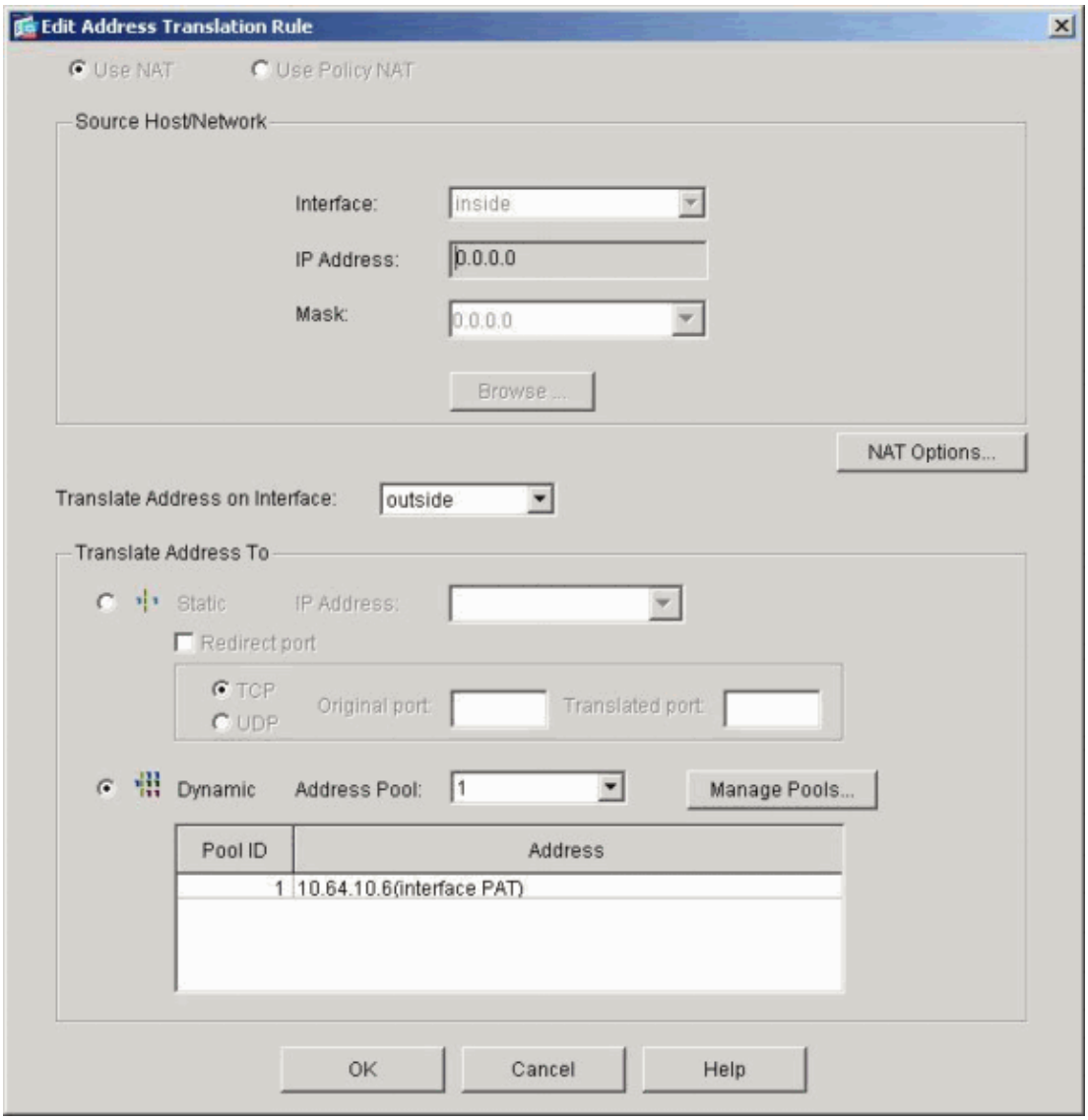
32. Click **OK** after configuration of the PAT pools.



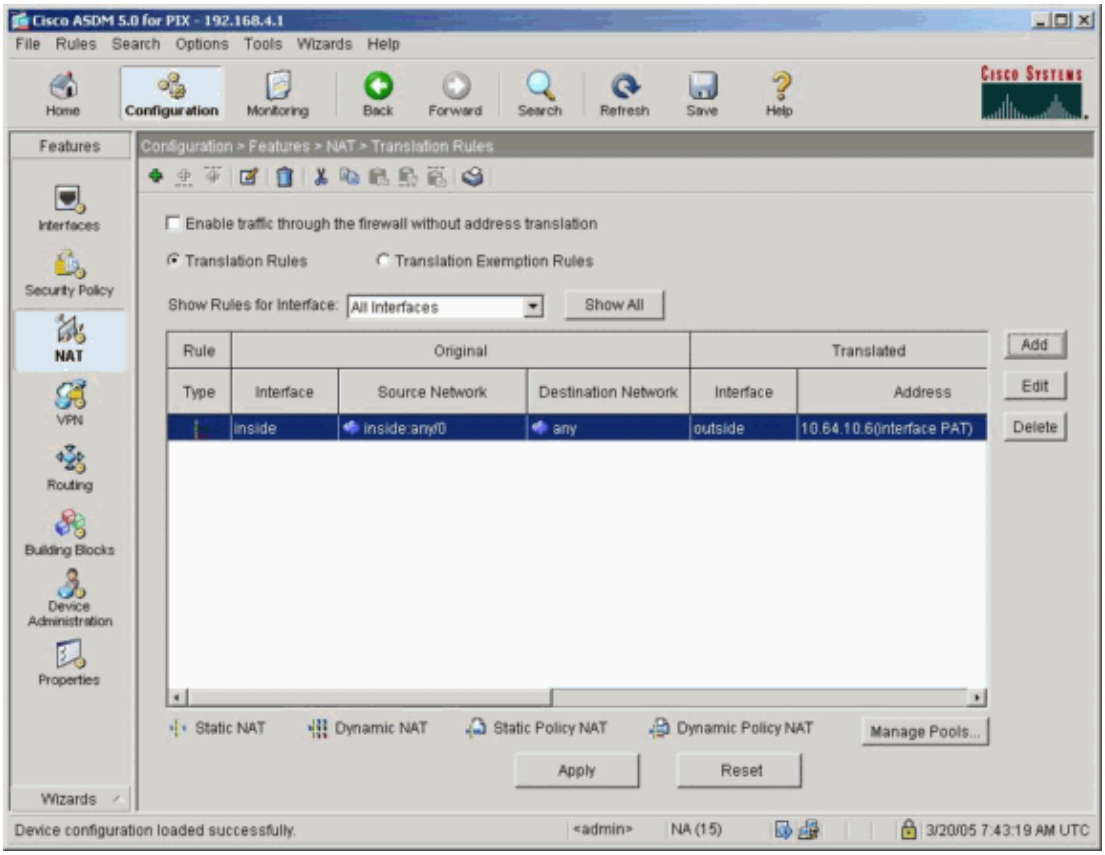
33. In the Add Address Translation Rule window, select the Address Pool that the configured Source Network will use.



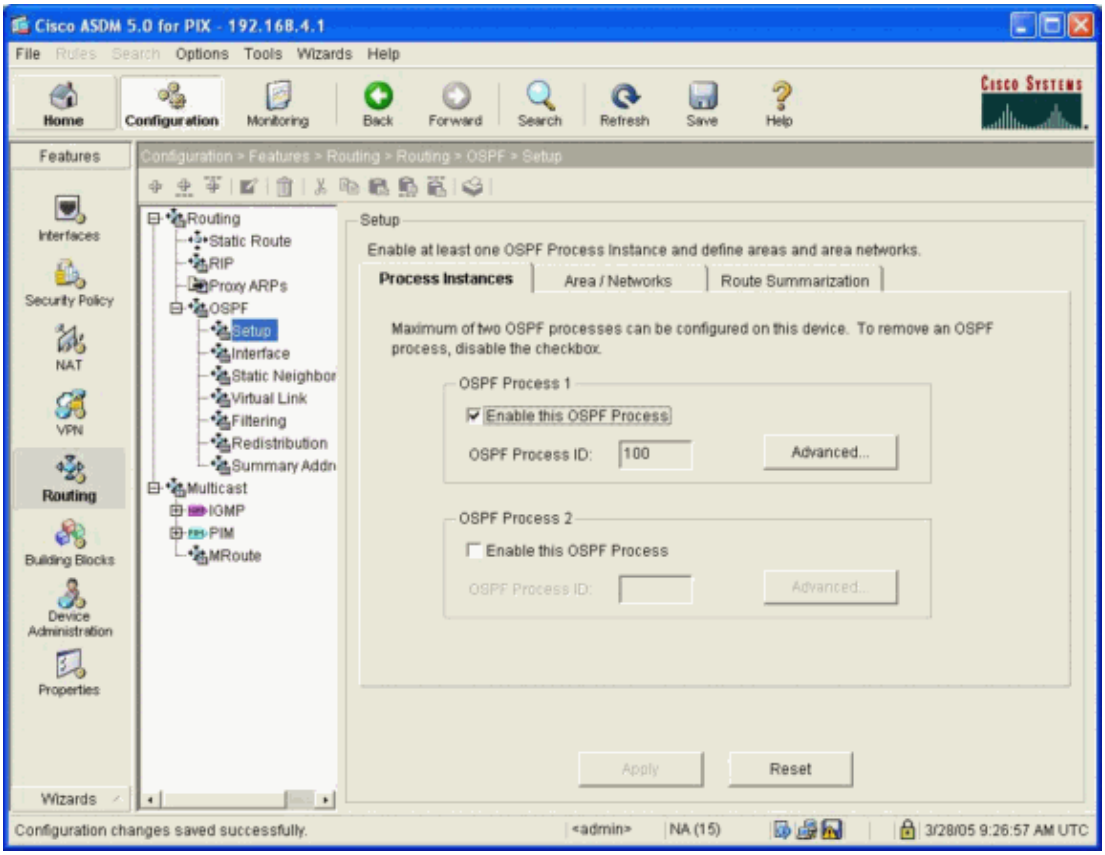
34. In this window, which shows the output from the NAT configuration, click **OK**:



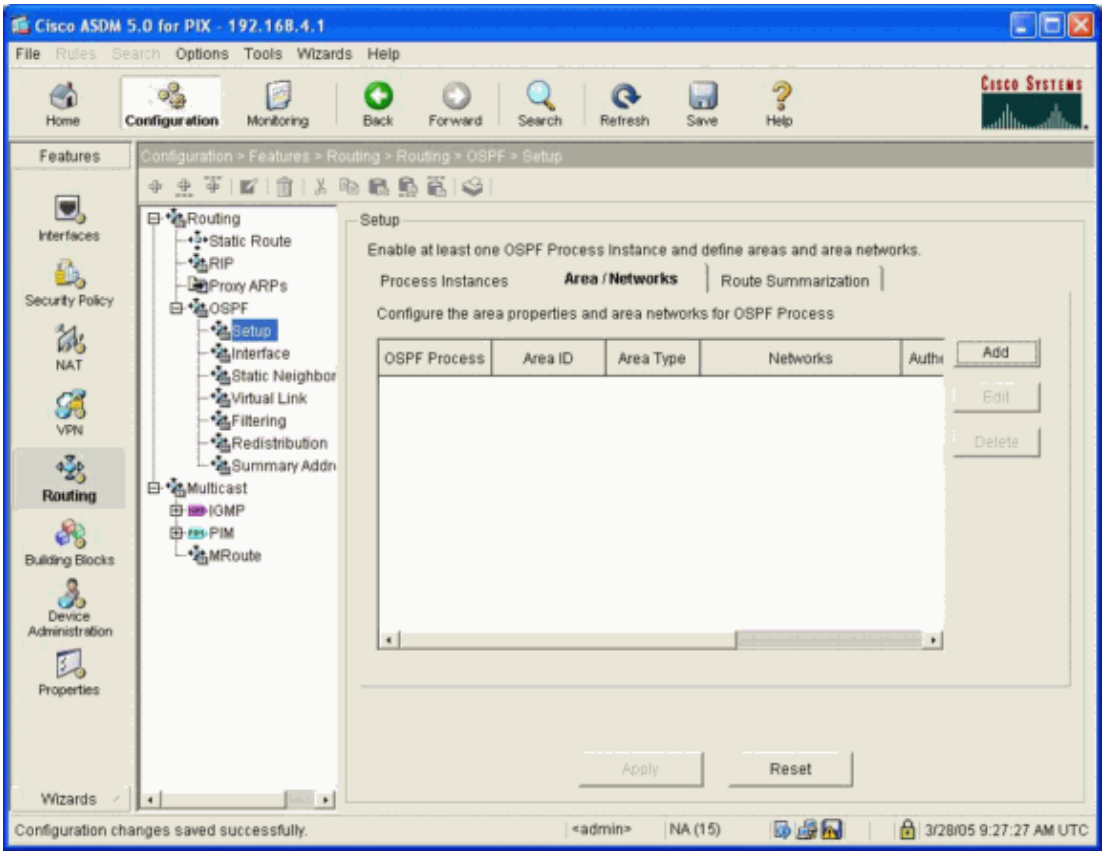
35. Click **Apply** in order to save the configuration.



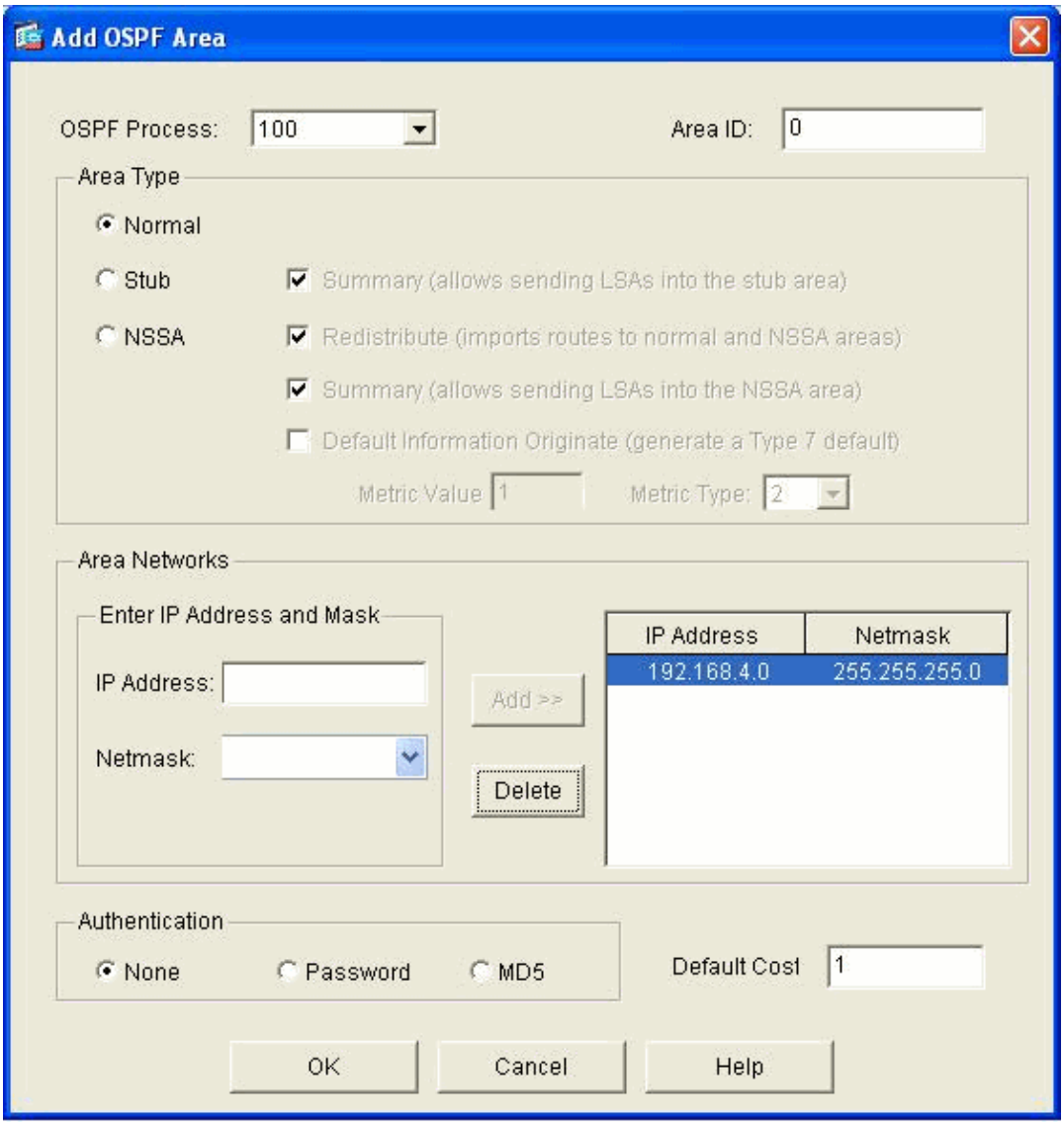
36. In order to set up OSPF on the PIX, choose **Configuration > Routing > OSPF > Setup > Process Instances**, then check **Enable this OSPF Process**.



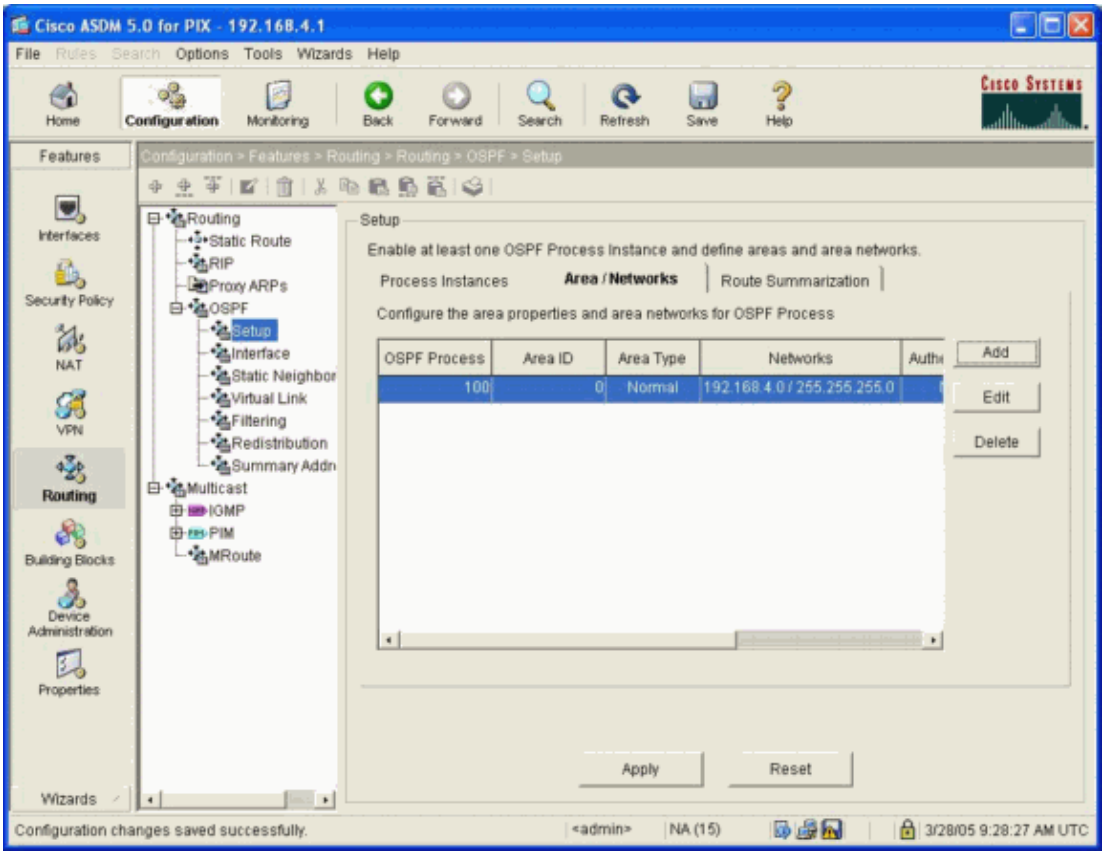
37. Choose **Area/Networks** and click **Add**.



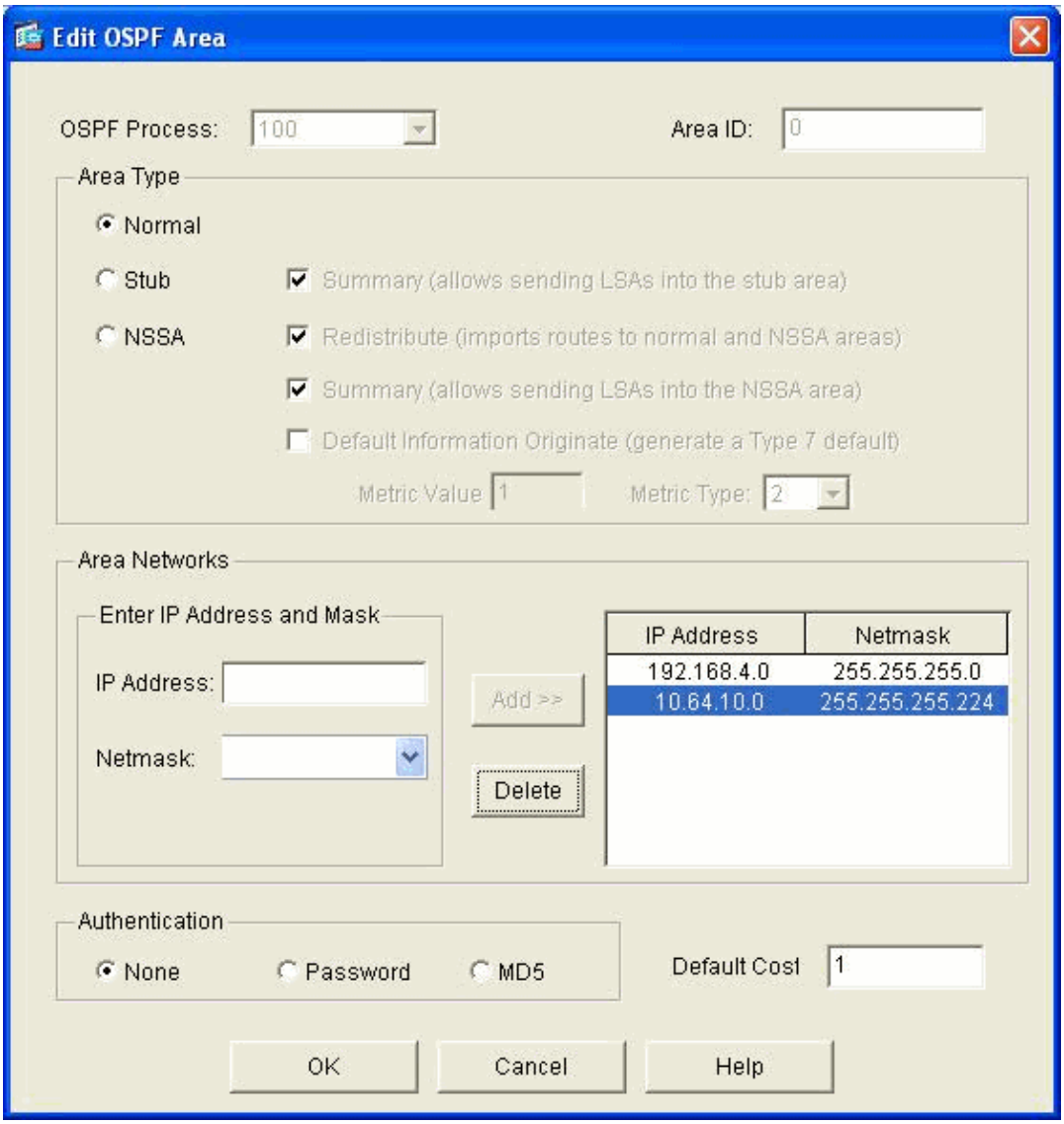
38. Enter the IP Address and Netmask of one network in the OSPF process field and click **OK**.



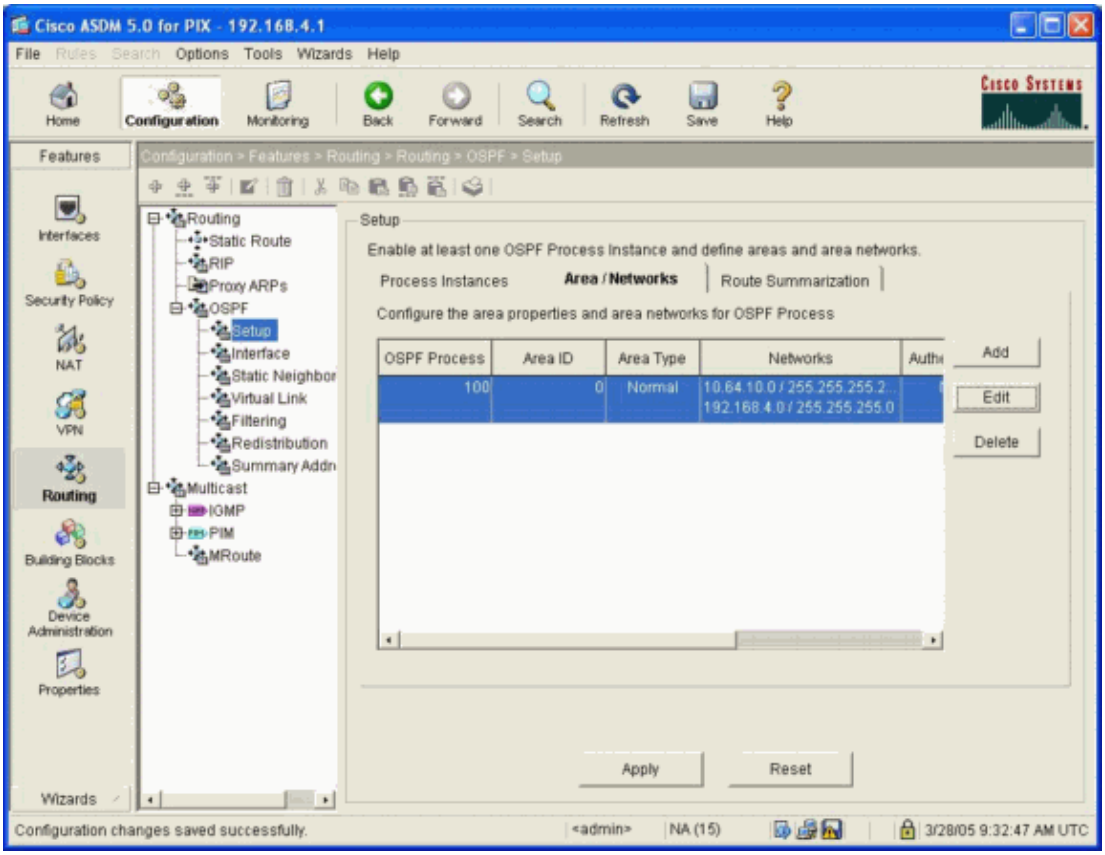
39. Verify that the information is correct and click **Edit**.



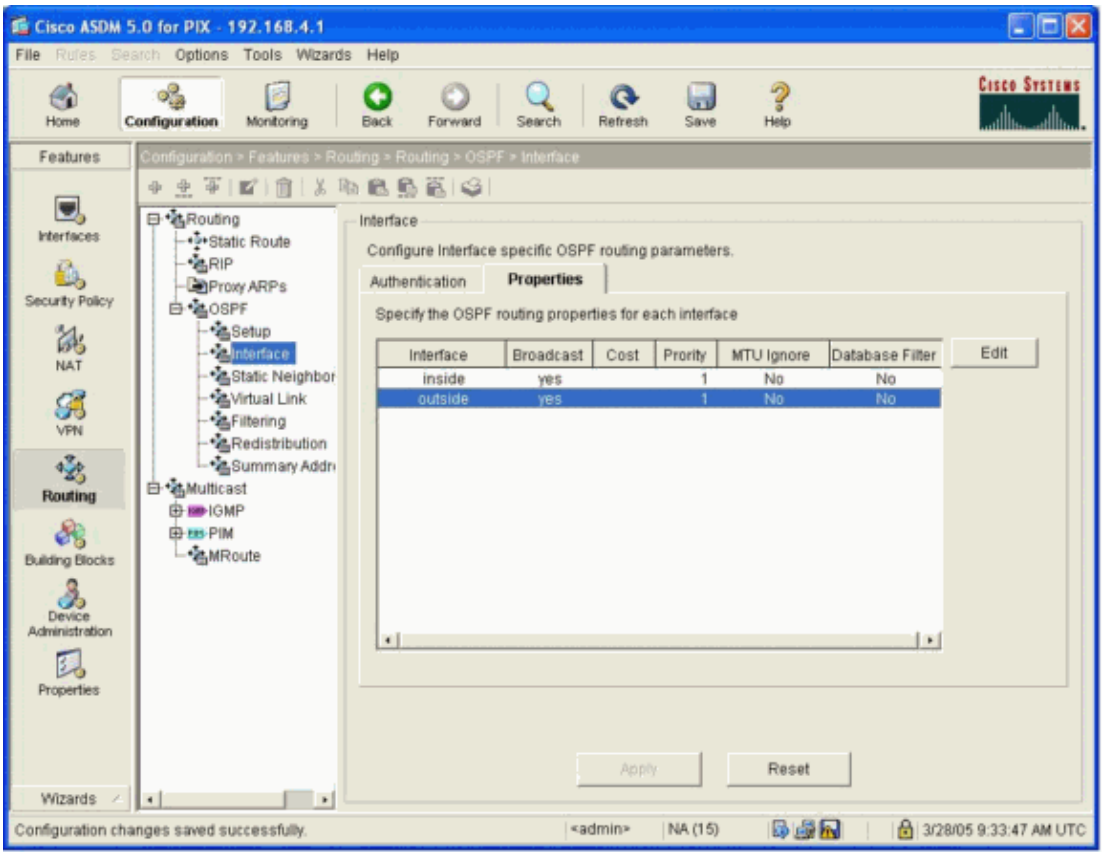
40. Enter the IP Address and Netmask of the second network in the OSPF process field and click **OK**.



41. Verify that the information is correct and click **Apply**.

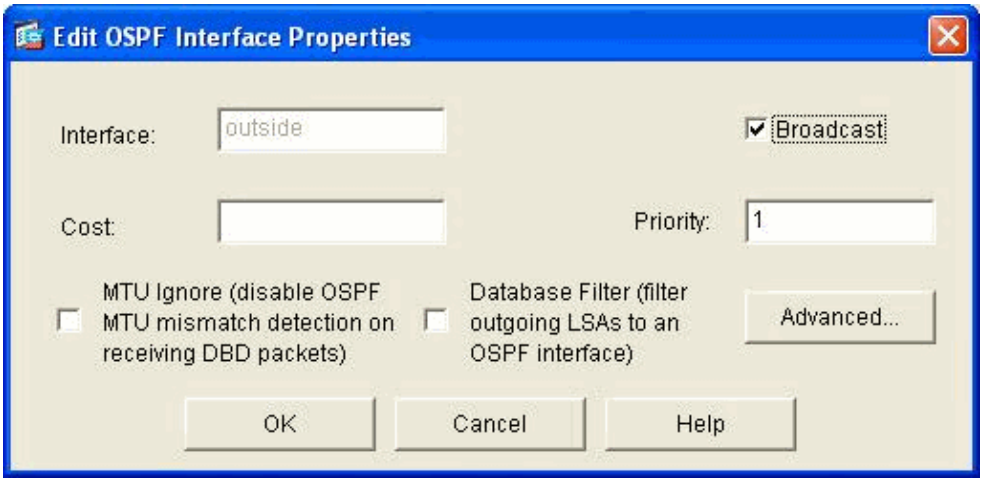


42. Choose **OSPF > Interface > Properties > Outside** and click **Edit**.

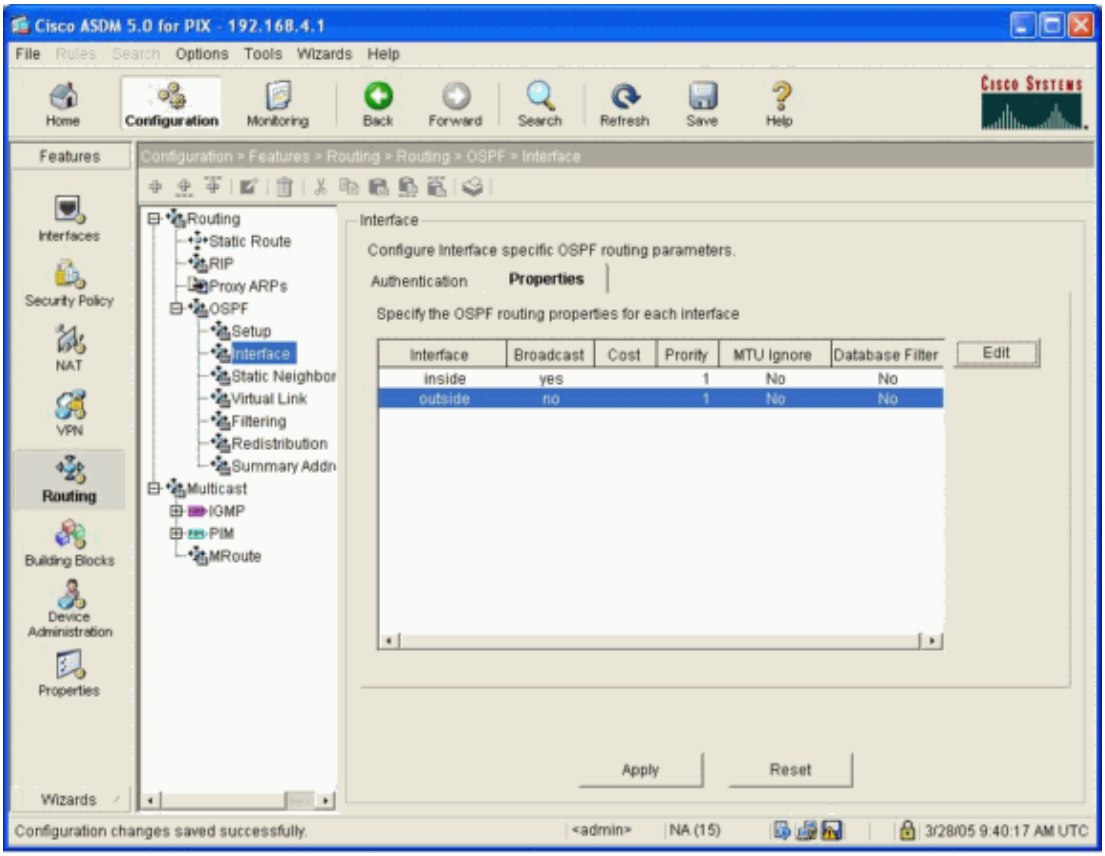


43. Uncheck the **Broadcast** check box on the outside interface.

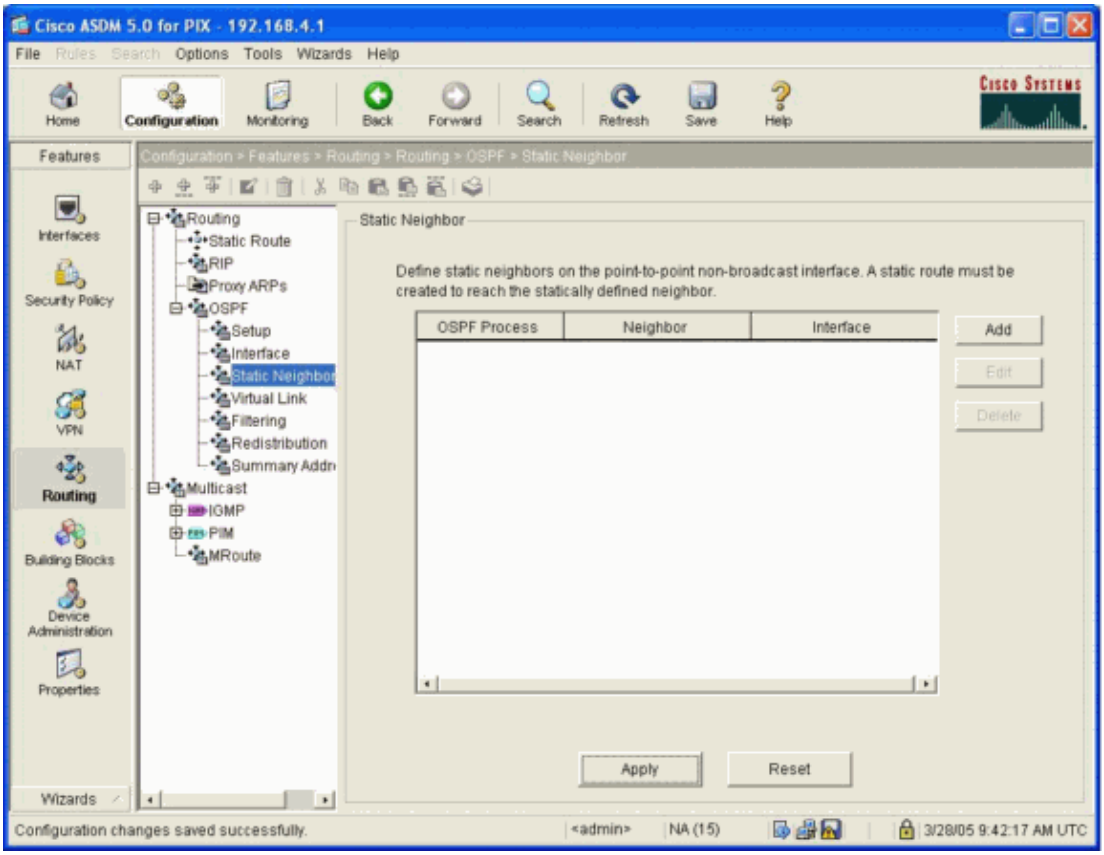
Note: This *must* be unicast.



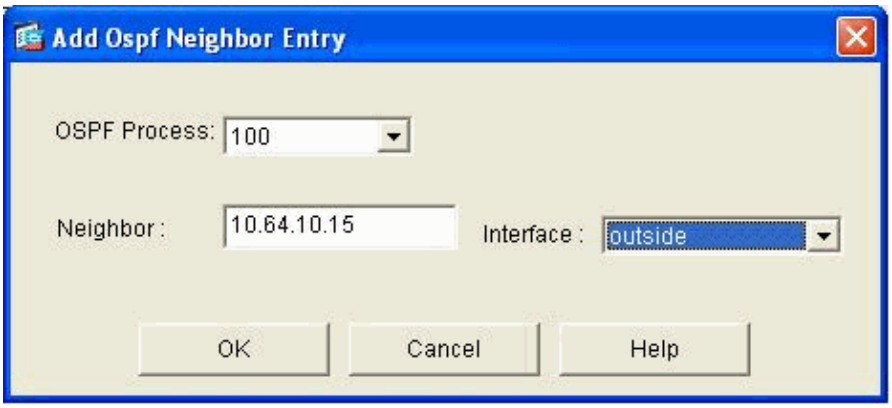
44. Check the Broadcast column for the outside interface in order to verify that the selection is **no**, then click **Apply**.



45. Choose **OSPF > Static Neighbor** and click **Add**.

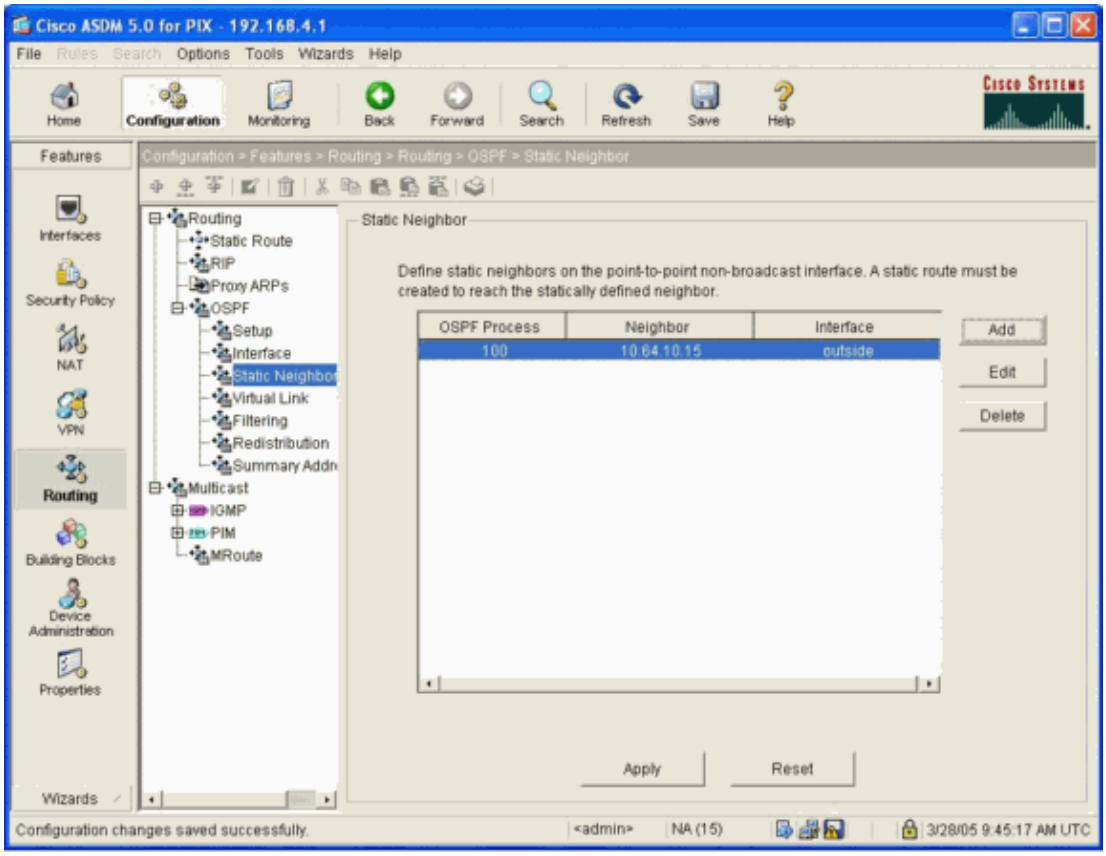


46. Enter the Neighbor IP address in the field for the outside interface and click **OK**.

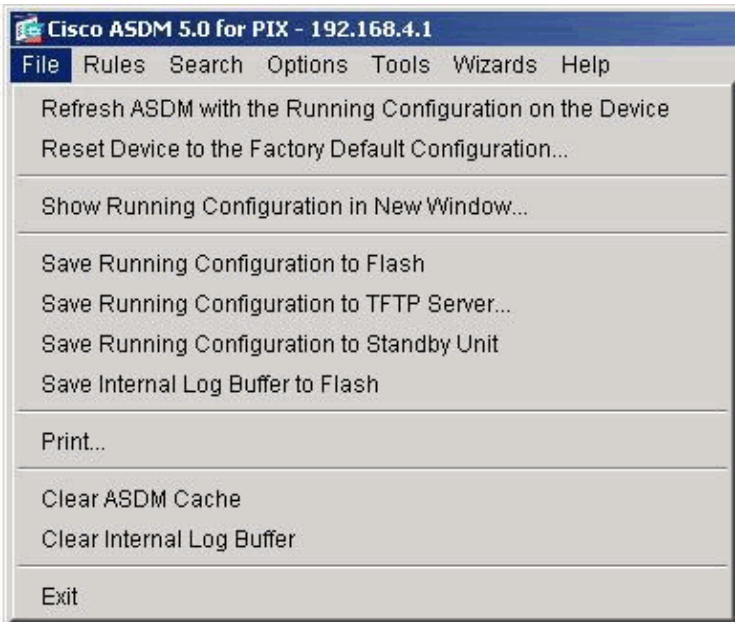


47. Verify that the information is correct and click **Apply**.

    This action completes the configuration.



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



PIX Lion
PIX Version 7.0 interface Ethernet0 nameif outside security-level 0 **ip address 10.64.10.6 255.255.255.0**

```
ospf network point-to-point non-broadcast

interface Ethernet1
nameif inside
security-level 100
ip address 192.168.4.1 255.255.255.0

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

hostname Lion
domain-name cisco.com
ftp mode passive

!--- This traffic is from networks.

access-list inside_nat0_outbound extended permit ip 192.168.4.0 255.255.255.0
   192.168.3.0 255.255.255.0
access-list outside_cryptomap_20 extended permit ip 192.168.4.0 255.255.255.0
   192.168.3.0 255.255.255.0
access-list outside_cryptomap_20 extended permit ospf interface outside host 10.64.10.15
pager lines 24
logging enable
logging buffered informational
no logging message 713906
no logging message 715075
no logging message 715036
no logging message 715005
mtu outside 1500
mtu inside 1500
no failover
monitor-interface outside
monitor-interface inside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface

!--- Do not translate traffic with NAT.

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0

!--- This is OSPF.

router ospf 100
network 10.64.10.0 255.255.255.224 area 0
network 192.168.4.0 255.255.255.0 area 0
area 0
neighbor 10.64.10.15 interface outside
log-adj-changes

route outside 0.0.0.0 0.0.0.0 10.64.10.15 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 192.168.4.50 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
```

```
!--- This is the IPsec configuration.

crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 10.64.10.15
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 10.64.10.15 type ipsec-l2l
tunnel-group 10.64.10.15 ipsec-attributes
pre-shared-key *

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:3d5f16a67ec0fa20aa3882acaa348e28
: end
```

PIX Tiger

```
PIX Version 7.0

interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.64.10.15 255.255.255.0

interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.3.1 255.255.255.0
```

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

hostname tiger
domain-name cisco.com
ftp mode passive

access-list inside_nat0_outbound extended permit ip 192.168.3.0 255.255.255.0
   192.168.4.0 255.255.255.0
access-list outside_cryptomap_20 extended permit ip 192.168.3.0 255.255.255.0
   192.168.4.0 255.255.255.0
pager lines 24
logging enable
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
global (outside) 1 interface

!--- Do not translate traffic with NAT.

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 10.64.10.6 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 192.168.3.50 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

!--- This is the IPsec configuration.

crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 10.64.10.6
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 10.64.10.6 type ipsec-l2l
```

```
tunnel-group 10.64.10.6 ipsec-attributes
 pre-shared-key *

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:5e99bf942a67f20dad116c7d99011315
: end
```

Verify

This section provides information you can use to confirm that 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.

- **logging buffer debugging** Shows the establishment of connections and denial of connections to hosts that go through the PIX. The PIX log buffer stores the information. You can see the output if you use the **show log** command.
- You can use ASDM in order to enable logging and to view the logs:

    - **show crypto isakmp sa** Shows the Internet Security Association and Key Management Protocol (ISAKMP) security association (SA) that is built between peers.

```
lion# show crypto isakmp sa
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.64.10.15
Type : L2L Role : responder
Rekey : no State : MM_ACTIVE

tiger# show crypto isa sa
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.64.10.6
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

show crypto ipsec sa Shows each Phase 2 SA that is built and the amount of traffic that is sent.

```
lion# show crypto ipsec sa
interface: outside
Crypto map tag: outside_map, local addr: 10.64.10.6

local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 10.64.10.15

#pkts encaps: 81, #pkts encrypt: 81, #pkts digest: 81
#pkts decaps: 81, #pkts decrypt: 81, #pkts verify: 81
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 81, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.64.10.6, remote crypto endpt.: 10.64.10.15

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 07DB50AF

inbound esp sas:
spi: 0x75E2D691 (1977800337)
transform: esp-des esp-md5-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3824991/28084)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x07DB50AF (131813551)
transform: esp-des esp-md5-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3824992/28082)
IV size: 8 bytes
replay detection support: Y

tiger# show crypto ipsec sa
interface: outside
Crypto map tag: outside_map, local addr: 10.64.10.15

local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer: 10.64.10.6

#pkts encaps: 83, #pkts encrypt: 83, #pkts digest: 83
#pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 83, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.64.10.15, remote crypto endpt.: 10.64.10.6

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 75E2D691

inbound esp sas:
spi: 0x07DB50AF (131813551)
transform: esp-des esp-md5-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274992/28062)
```

```
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x75E2D691 (1977800337)
transform: esp-des esp-md5-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274991/28062)
IV size: 8 bytes
replay detection support: Y
```

- **show debug** Displays the debug output.

```
lion(config)# show debug
debug crypto ipsec enabled at level 1
debug crypto engine enabled at level 1
debug crypto isakmp enabled at level 1

%PIX-6-609001: Built local-host outside:10.64.10.15
%PIX-6-609001: Built local-host NPMar 20 09:26:11 [IKEv1] Id:
   QM IsRekeyed old sa not found by addr
entity Ifc:10.64.10.6
%PIX-6-302015: Built inbound UDP connection 133 for outside:10.64.10.15/500
   (10.64.10.15/500) to NP Identity Ifc:10.64.10.6/500 (10.64.10.6/500)
%PIX-7-715005: Group = , IP = 10.64.10.15 , processing SA payload
%PIX-7-715005: Group = , IP = 10.64.10.15 , Oakley proposal is acceptable
%PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
%PIX-7-715049: Group = , IP = 10.64.10.15 Received Fragmentation VID,
%PIX-7-715064: Group = , IP = 10.64.10.15 IKE Peer included IKE
   fragmentation capability flags: Main Mode: True Aggressive Mode: True,
%PIX-7-715005: Group = , IP = 10.64.10.15 , processing IKE SA
%PIX-7-715028: Group = , IP = 10.64.10.15 IKE SA Proposal # 1,
   Transform # 1 acceptable Matches global IKE entry # 3,
%PIX-7-715005: Group = , IP = 10.64.10.15 , constructing ISA_SA for isakmp
%PIX-7-715046: Group = , IP = 10.64.10.15 constructing Fragmentation
   VID + extended capabilities payload,
%PIX-7-713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=0)
   with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 108
%PIX-7-713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=0)
   with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
   + VENDOR (13) + VENDOR (13) + NONE (0) total length : 224
%PIX-7-715005: Group = , IP = 10.64.10.15 , processing ke payload
%PIX-7-715005: Group = , IP = 10.64.10.15 , processing ISA_KE
%PIX-7-715001: Group = , IP = 10.64.10.15 processing nonce payload,
%PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
%PIX-7-715049: Group = , IP = 10.64.10.15 Received Cisco Unity client VID,
%PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
%PIX-7-715049: Group = , IP = 10.64.10.15 Received xauth V6 VID,
%PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
%PIX-7-715038: Group = , IP = 10.64.10.15 Processing VPN3000/ASA
   spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001),
%PIX-7-715047: Group = , IP = 10.64.10.15 processing VID payload,
%PIX-7-715049: Group = , IP = 10.64.10.15 Received Altiga/Cisco VPN3000/
   Cisco ASA GW VID,
%PIX-7-715005: Group = , IP = 10.64.10.15 , constructing ke payload
%PIX-7-715001: Group = , IP = 10.64.10.15 constructing nonce payload,
%PIX-7-715046: Group = , IP = 10.64.10.15 constructing Cisco Unity VID
   payload,
%PIX-7-715046: Group = , IP = 10.64.10.15 constructing xauth V6 VID
   payload,
%PIX-7-715048: Group = , IP = 10.64.10.15 Send IOS VID,
%PIX-7-715038: Group = , IP = 10.64.10.15 Constructing ASA spoofing IOS
   Vendor ID payload (version: 1.0.0, capabilities: 20000001),
%PIX-7-715046: Group = , IP = 10.64.10.15 constructing VID payload,
%PIX-7-715048: Group = , IP = 10.64.10.15 Send Altiga/Cisco VPN3000/Cisco
```

```
   ASA GW VID,
%PIX−7−713906: IP = 10.64.10.15 , Connection landed on tunnel_group
   10.64.10.15
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , Generating keys
   for Responder...
%PIX−7−713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=0)
   with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
   + VENDOR (13) + VENDOR (13) + NONE (0) total length : 224
%PIX−7−713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=0)
   with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) +
   VENDOR (13) + NONE (0) total length : 103
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing hash
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , computing hash
%PIX−7−715034: IP = 10.64.10.15 Processing IOS keep alive payload:
   proposal=32767/32767 sec.,
%PIX−7−715047: Group = 10.64.10.15, IP = 10.64.10.15 processing VID
   payload,
%PIX−7−715049: Group = 10.64.10.15, IP = 10.64.10.15 Received DPD VID,
%PIX−7−713906: IP = 10.64.10.15 , Connection landed on tunnel_group
   10.64.10.15
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing ID,
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , construct hash
   payload
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , computing hash
%PIX−7−715034: IP = 10.64.10.15 Constructing IOS keep alive payload:
   proposal=32767/32767 sec.,
%PIX−7−715046: Group = 10.64.10.15, IP = 10.64.10.15 constructing dpd
   vid payload,
%PIX−7−713906: IP = 10.64.10.15 , IKE DECODE SENDING Message (msgid=0)
   with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14)
   + VENDOR (13) + NONE (0) total length : 102
%PIX−6−113009: AAA retrieved default group policy (DfltGrpPolicy) for
   user = 10.64.10.15
%PIX−3−713119: Group = 10.64.10.15, IP = 10.64.10.15 PHASE 1 COMPLETED,
%PIX−7−713121: IP = 10.64.10.15 Keep−alive type for this connection: DPD,
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , Starting phase 1
   rekey timer:
   73440000 (ms)
%PIX−7−714003: IP = 10.64.10.15 IKE Responder starting QM: msg id =
   6a9f3592,
%PIX−7−713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message (msgid=
   6a9f3592) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
   + ID (5) + NOTIFY (11) + NONE (0) total length : 192
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing hash
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing SA
   payload
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 processing nonce
   payload,
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,
%PIX−7−714011ID_IPV4_ADDR_SUBNET ID received−−192.168.3.0−−255.255.255.0,
%PIX−7−713035: Group = 10.64.10.15, IP = 10.64.10.15 Received remote IP
   Proxy Subnet data in ID Payload: Address 192.168.3.0, Mask
   255.255.255.0, Protocol 0, Port 0,
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 Processing ID,
%PIX−7−714011ID_IPV4_ADDR_SUBNET ID received−−192.168.4.0−−255.255.255.0,
%PIX−7−713034: Group = 10.64.10.15, IP = 10.64.10.15 Received local IP
   Proxy Subnet data in ID Payload: Address 192.168.4.0, Mask s,
   Protocol 25585052, Port 0,
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , Processing Notify
   payload
%PIX−5−713904: QM IsRekeyed old sa not found by addr
%PIX−7−713221: Group = 10.64.10.15, IP = 10.64.10.15 Static Crypto Map
   check, checking map = outside_map, seq = 20...,
```

```
%PIX−7−713225: Group = 10.64.10.15, IP = 10.64.10.15 Static Crypto Map
   check, map outside_map, seq = 20 is a successful match,
%PIX−7−713066: Group = 10.64.10.15, IP = 10.64.10.15 IKE Remote Peer
   configured for SA: outside_map,
%PIX−7−713906: Group = 10.64.10.15, IP = 10.64.10.15 , processing IPSEC SA
%PIX−7−715027: Group = 10.64.10.15, IP = 10.64.10.15 IPSec SA Proposal # 1,
   Transform # 1 acceptable Matches global IPSec SA entry # 20,
%PIX−7−713906: Group = 10.64.10.15, IP = 10.64.10.15 , IKE: requesting SPI!
%PIX−7−713906: Received unexpected event EV_ACTIVATE_NEW_SA in state
   MM_ACTIVE
%PIX−7−715006IKE got SPI from key engine: SPI = 0xcb804517,
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , oakley constucting
   quick mode
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , constructing blank
   hash
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , constructing ISA_SA
   for ipsec
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing ipsec
   nonce payload,
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 constructing proxy ID,
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , Transmitting Proxy
   Id:
Remote subnet: 192.168.3.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 192.168.4.0 mask 255.255.255.0 Protocol 0 Port 0
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , constructing qm
   hash
%PIX−7−714005IKE Responder sending 2nd QM pkt: msg id = 6a9f3592,
%PIX−7−713906: IP = 10.64.10.15 , IKE DECODE SENDING Message
   (msgid=6a9f3592) with payloads : HDR + HASH (8) + SA (1) + NONCE (10)
   + ID (5) + ID (5) + NONE (0) total length : 164
%PIX−7−713906: IP = 10.64.10.15 , IKE DECODE RECEIVED Message
   (msgid=6a9f3592) with payloads : HDR + HASH (8) + NONE (0) total
   length : 48
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , processing hash
%PIX−7−715005: Group = 10.64.10.15, IP = 10.64.10.15 , loading all IPSEC
   SAs
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 Generating Quick
   Mode Key!,
%PIX−7−715001: Group = 10.64.10.15, IP = 10.64.10.15 Generating Quick
   Mode Key!,
%PIX−5−713049: Group = 10.64.10.15, IP = 10.64.10.15 Security negotiation
   complete for LAN−to−LAN Group (10.64.10.15) Responder, Inbound SPI =
   0xcb804517, Outbound SPI = 0x6935f1ee,
%PIX−7−715007IKE got a KEY_ADD msg for SA: SPI = 0x6935f1ee,
%PIX−7−715005: pitcher: rcv KEY_UPDATE, spi 0xcb804517
%PIX−6−713905: Group = 10.64.10.15, IP = 10.64.10.15 , PHASE 2 COMPLETED
   (msgid=6a9f3592)
%PIX−6−609001: Built local−host inside:192.168.4.2
%PIX−6−609001: Built local−host outside:192.168.3.2
```

- Verify that the LAN−to−LAN connection passes routing traffic:

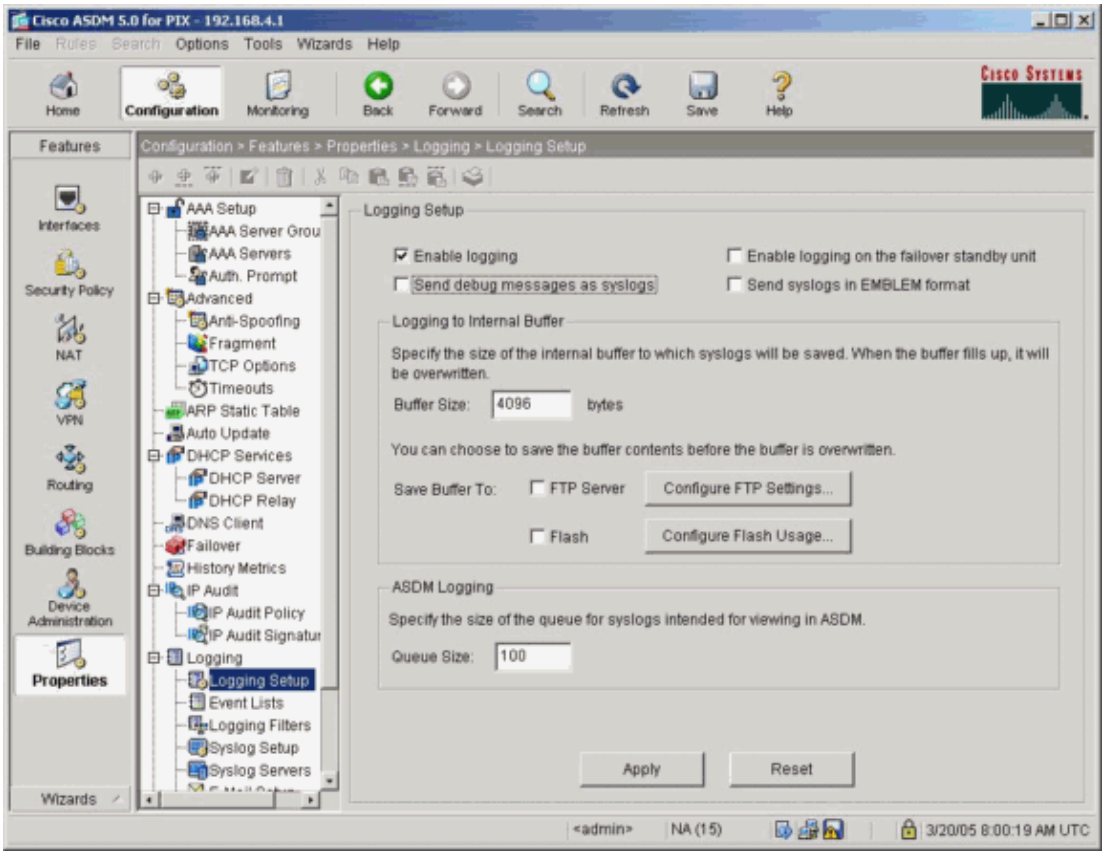
  - **show ip route** Displays IP routing table entries.

```
rodney# show ip route
Codes: C − connected, S − static, I − IGRP, R − RIP, M − mobile, B − BGP
D − EIGRP, EX − EIGRP external, O − OSPF, IA − OSPF inter area
N1 − OSPF NSSA external type 1, N2 − OSPF NSSA external type 2
E1 − OSPF external type 1, E2 − OSPF external type 2, E − EGP
i − IS−IS, su − IS−IS summary, L1 − IS−IS level−1, L2 − IS−IS level−2
ia − IS−IS inter area, * − candidate default, U − per−user static route
o − ODR, P − periodic downloaded static route

Gateway of last resort is 192.168.4.1 to network 0.0.0.0
```

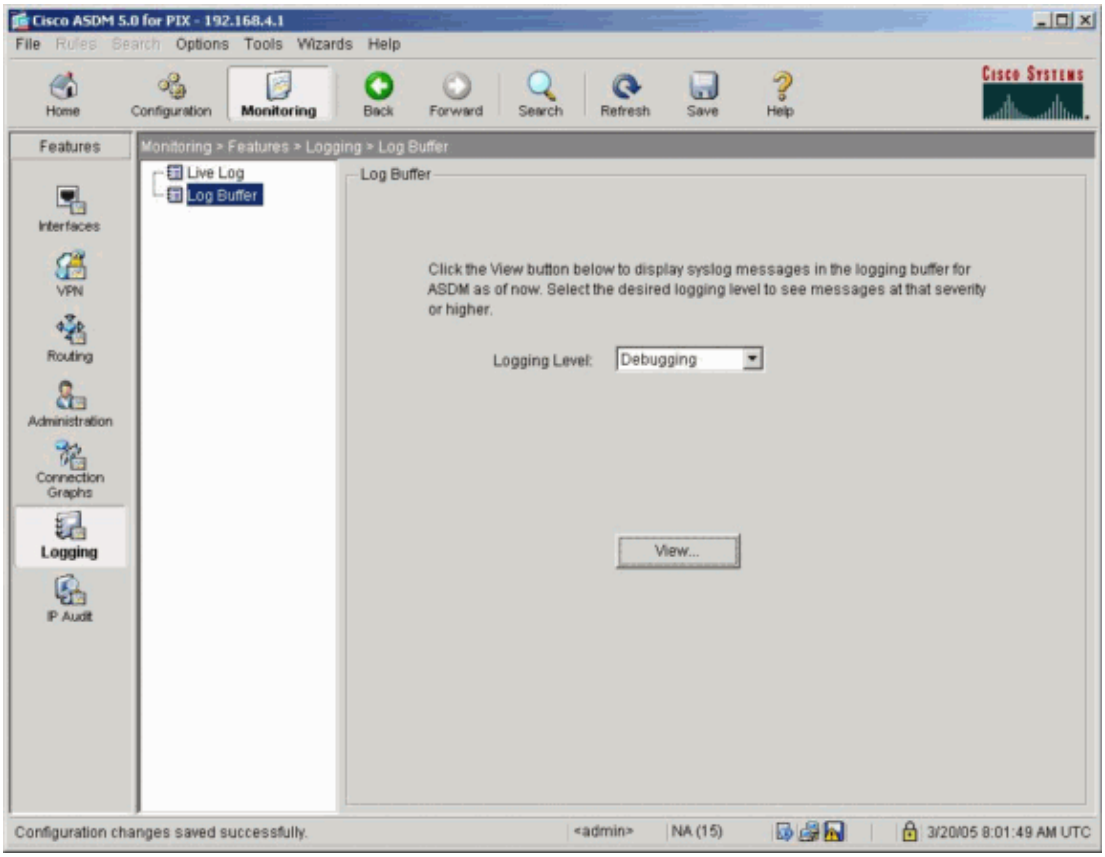
```
1.0.0.0/24 is subnetted, 1 subnets
C 1.1.1.0 is directly connected, Tunnel0
20.0.0.0/24 is subnetted, 1 subnets
C 20.20.20.0 is directly connected, Loopback0
22.0.0.0/24 is subnetted, 1 subnets
C 22.22.22.0 is directly connected, Loopback1
C 192.168.4.0/24 is directly connected, Ethernet0/1
10.0.0.0/24 is subnetted, 1 subnets
S 10.10.10.0 is directly connected, Tunnel0
11.0.0.0/32 is subnetted, 1 subnets
O 11.11.11.11 [110/11112] via 1.1.1.1, 00:13:34, Tunnel0
S* 0.0.0.0/0 [1/0] via 192.168.4.1

rodney# ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100−byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round−trip min/avg/max = 1/2/4 ms

house# show ip route
Codes: C − connected, S − static, R − RIP, M − mobile, B − BGP
D − EIGRP, EX − EIGRP external, O − OSPF, IA − OSPF inter area
N1 − OSPF NSSA external type 1, N2 − OSPF NSSA external type 2
E1 − OSPF external type 1, E2 − OSPF external type 2
i − IS−IS, L1 − IS−IS level−1, L2 − IS−IS level−2, ia − IS−IS inter area
* − candidate default, U − per−user static route, o − ODR
P − periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets
C 1.1.1.0 is directly connected, Tunnel0
20.0.0.0/24 is subnetted, 1 subnets
S 20.20.20.0 is directly connected, Tunnel0
22.0.0.0/32 is subnetted, 1 subnets
O 22.22.22.22 [110/11112] via 1.1.1.2, 00:14:29, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Loopback0
11.0.0.0/24 is subnetted, 1 subnets
C 11.11.11.0 is directly connected, Loopback1
C 192.168.253.0/24 is directly connected, FastEthernet0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.3.1

house# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100−byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round−trip min/avg/max = 4/4/4 ms
```

Complete these steps in order to view the logs:

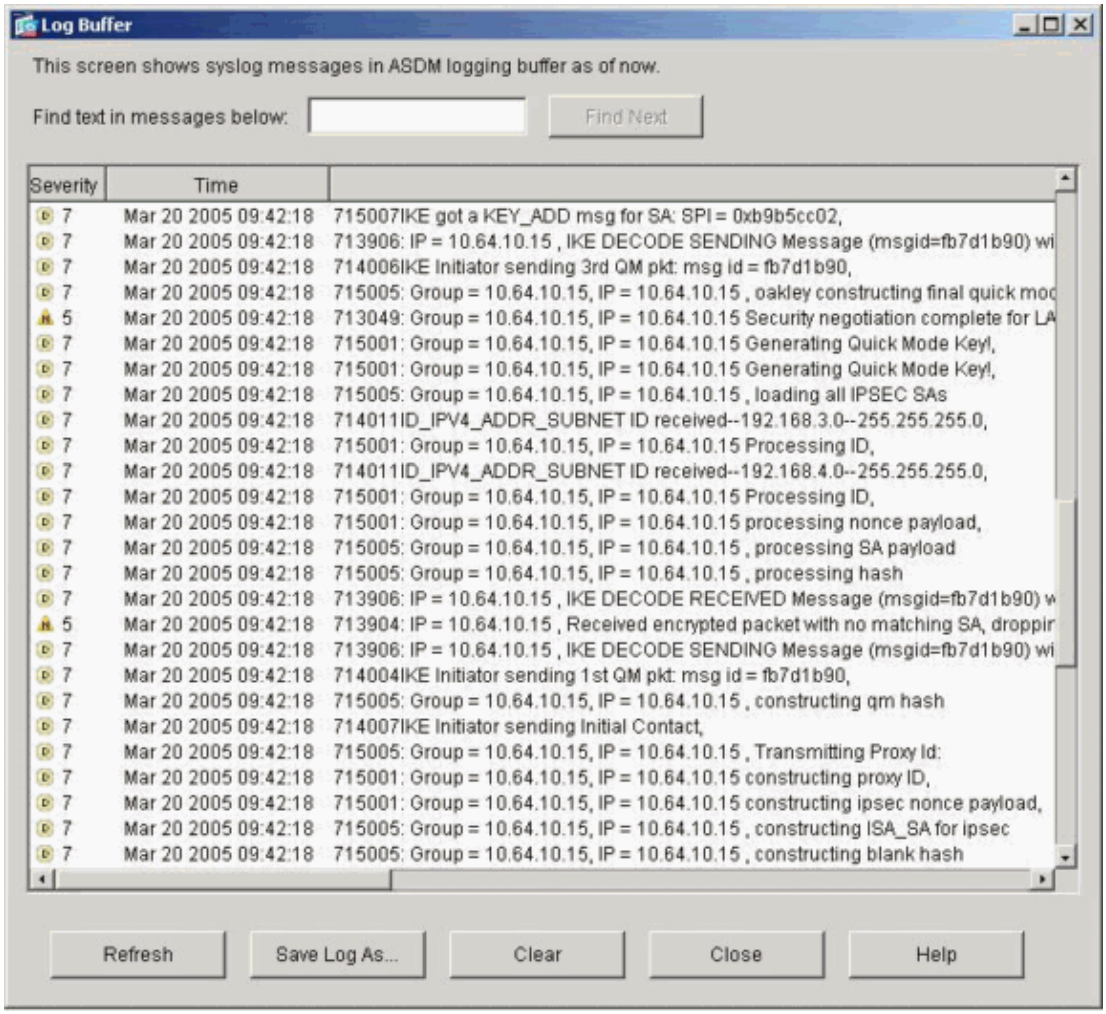
1. Choose **Configuration > Properties > Logging > Logging Setup**, check **Enable logging**, and click **Apply**.



2. Choose **Monitoring > Logging > Log Buffer > Logging Level**, select **Logging Buffer** from the drop−down menu, and click **View**.



Here is an example of the Log Buffer:



In order to view related graphs, choose **Monitoring > VPN > IPSEC Tunnels**. Then, move **IPSec Active Tunnels** and **IKE Active Tunnels** to Selected Graphs, and choose **Show Graphs**.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

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

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco PIX 500 Series Security Appliances**
- **Cisco Secure PIX Firewall Command References**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 28, 2005 Document ID: 63882