PIX/ASA (版本7.x和以上)有网络地址转换配置示例的IPSec VPN通道

目录

简介
先决条件
要求
使用的组件
规则
相关产品
配置
网络图
配置
PIX 安全设备和访问列表配置
PIX 安全设备和 MPF（模块化策略框架）配置
验证
故障排除
路由器 IPSec 的故障排除命令
清除安全关联
PIX 的故障排除命令
相关信息

简介

此示例配置演示一个通过执行网络地址转换 (NAT) 的防火墙的 IPSec VPN 隧道。**如果所用 Cisco IOS® 软件版本早于且不包括 12.2(13)T，则此配置不适用于端口地址转换 (PAT)。**此类型的配置可以用于通过隧道传输 IP 流量。此配置不能用于对不通过防火墙的流量（如 IPX 或路由更新）进行加密。通用路由封装 (GRE) 隧道是更加合适的选择。在此示例中，Cisco 2621 和 3660 路由器是连接两个私有网络的 IPsec 隧道终点，并且在之间的 PIX 上具有管道或访问控制列表 (ACL) 以允许传输 IPsec 流量。

注意： NAT是一对一地址转换，与多对一（在防火墙内）地址转换的PAT不同。有关 NAT 操作和配置的详细信息，请参阅验证 NAT 操作和基本的 NAT 故障排除或 NAT 的工作原理。

注意： 因为外部隧道终点设备处理来自一个 IP 地址的多个隧道，所以使用 PAT 的 IPsec 可能无法正确工作。请与供应商联系以确定隧道终点设备是否适用于 PAT。此外，在 Cisco IOS 软件版本 12.2(13)T 及更高版本中，NAT 透明模式功能可以用于 PAT。有关详细信息，请参阅 IPSec NAT 透明模式。若要了解有关 Cisco IOS 软件版本 12.2(13)T 及更高版本中这些功能的详细信息，请参阅通过 NAT 支持 IPSec ESP。

注意： 在通过 Cisco 技术支持建立案例之前，请参阅 NAT 常见问题，其中有许多常见问题解答。

有关如何在 PIX 版本 6.x 及更低版本中，配置通过使用 NAT 的防火墙的 IPsec 隧道的详细信息，请参阅配置通过使用 NAT 的防火墙的 IPSec 隧道。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 软件版本 12.0.7.T（最高为 Cisco IOS 软件版本 12.2(13)T 但不包括该版本）对于更新版本，请参阅 IPSec NAT 透明模式。
- Cisco 2621 路由器
- Cisco 3660 路由器
- 运行 7.x 及更高版本的 Cisco PIX 500 系列安全设备。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

相关产品

本文可能也与Cisco ASA 5500系列自适应安全设备(ASA)一起使用与软件版本7.x和以后。

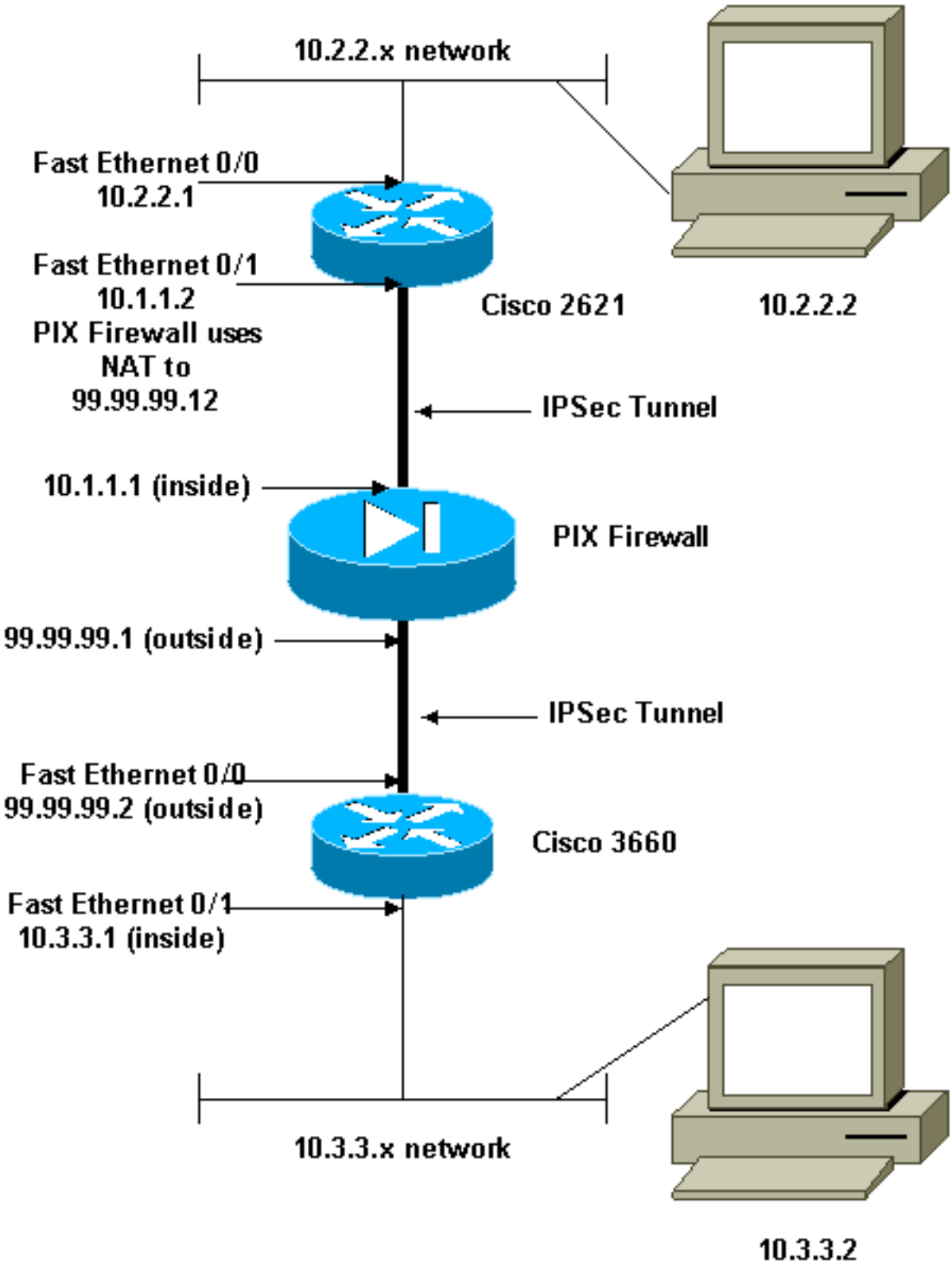
配置

此部分存在您与您能使用配置功能本文描述的信息。

注意： 要查找有关本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- Cisco 2621 配置
- Cisco 3660 配置
- PIX 安全设备和访问列表配置高级安全设备管理器 GUI (ASDM) 配置命令行界面 (CLI) 配置
- PIX 安全设备和 MPF（模块化策略框架）配置

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-
```

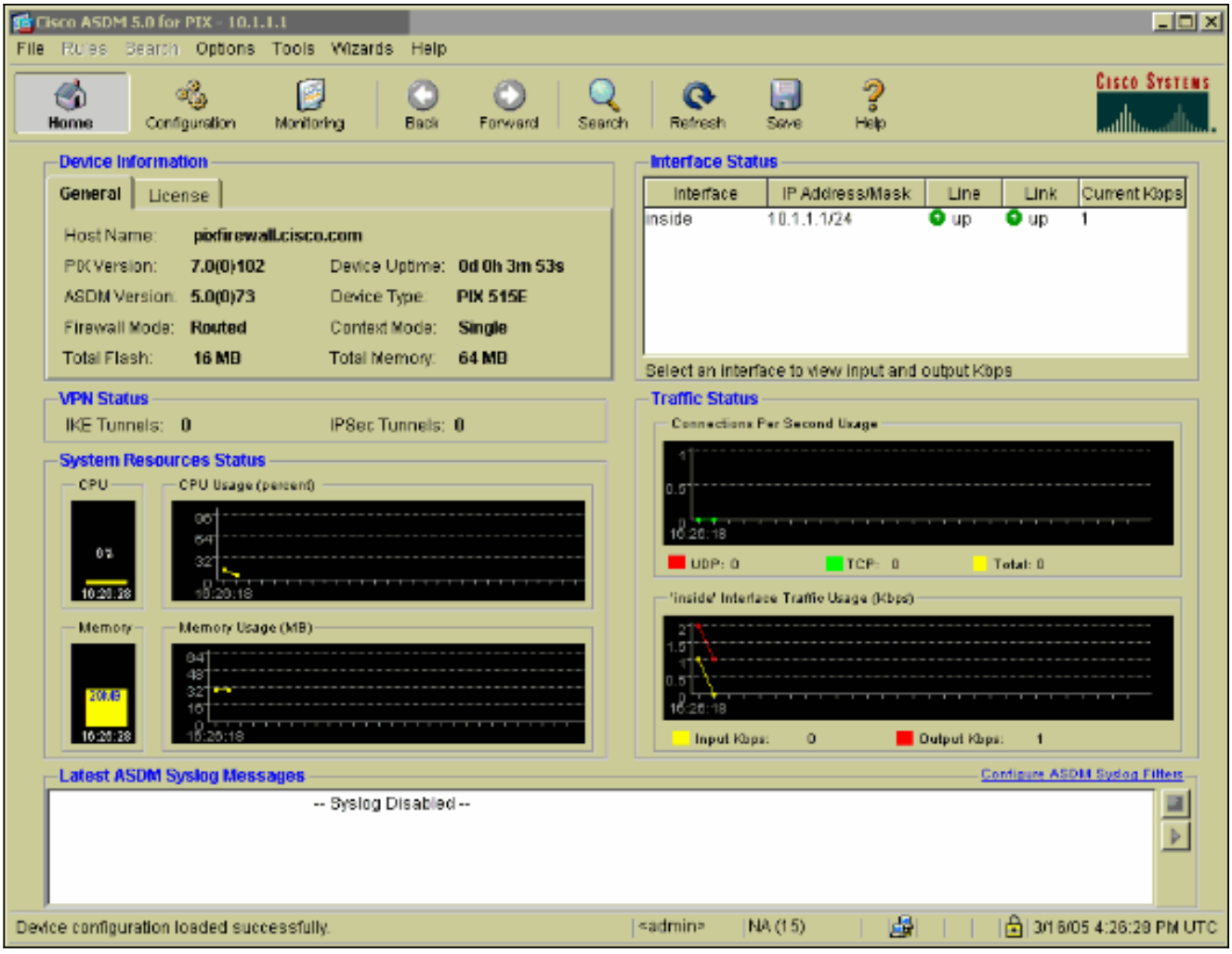
```
broadcast ip nat inside duplex auto speed auto !
interface Ethernet3/0 no ip address no ip directed-
broadcast shutdown ! interface Serial3/0 no ip address
no ip directed-broadcast no ip mroute-cache shutdown !
interface Ethernet3/1 no ip address no ip directed-
broadcast interface Ethernet4/0 no 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 安全设备和访问列表配置

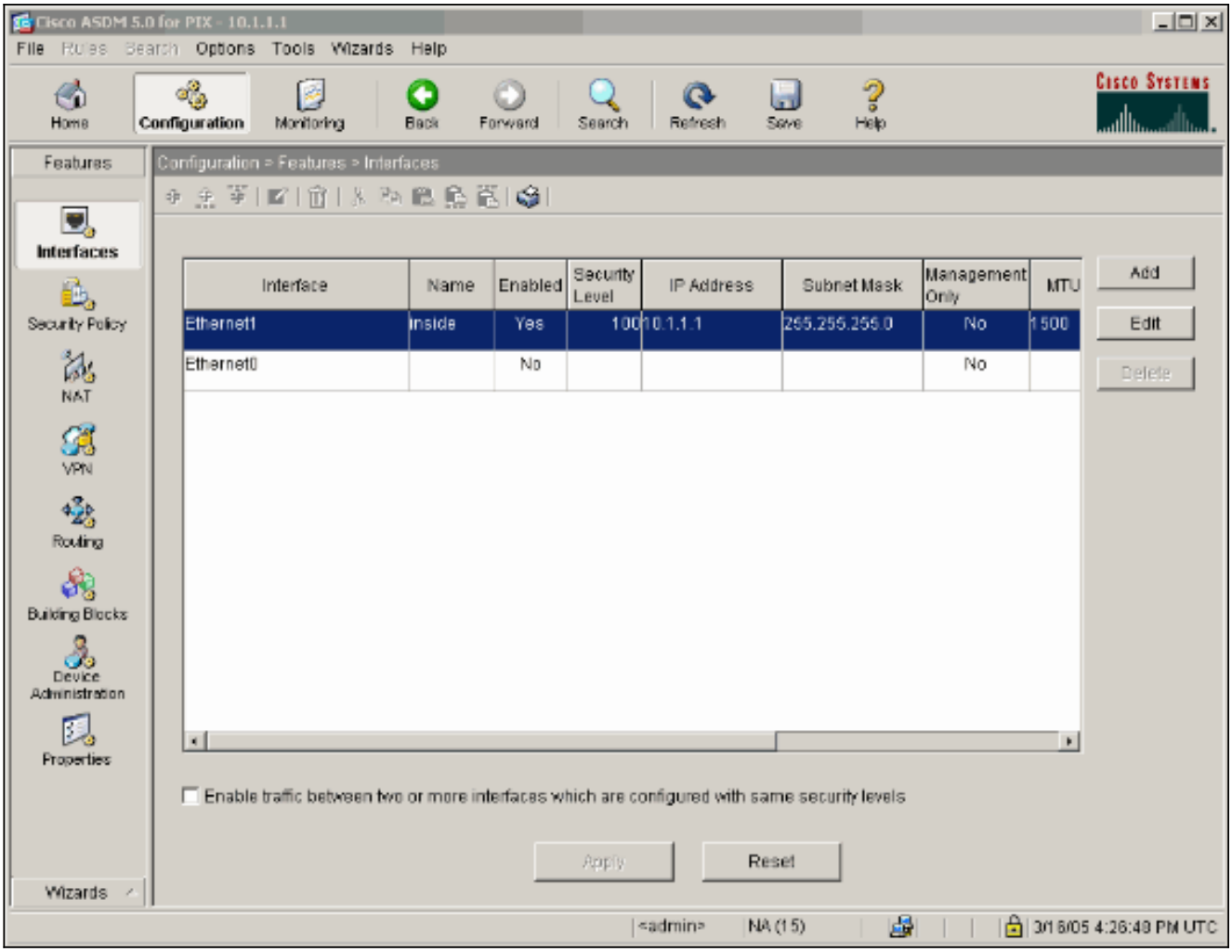
ASDM 5.0 配置

完成这些步骤可使用 ASDM 配置 PIX 防火墙版本 7.0。

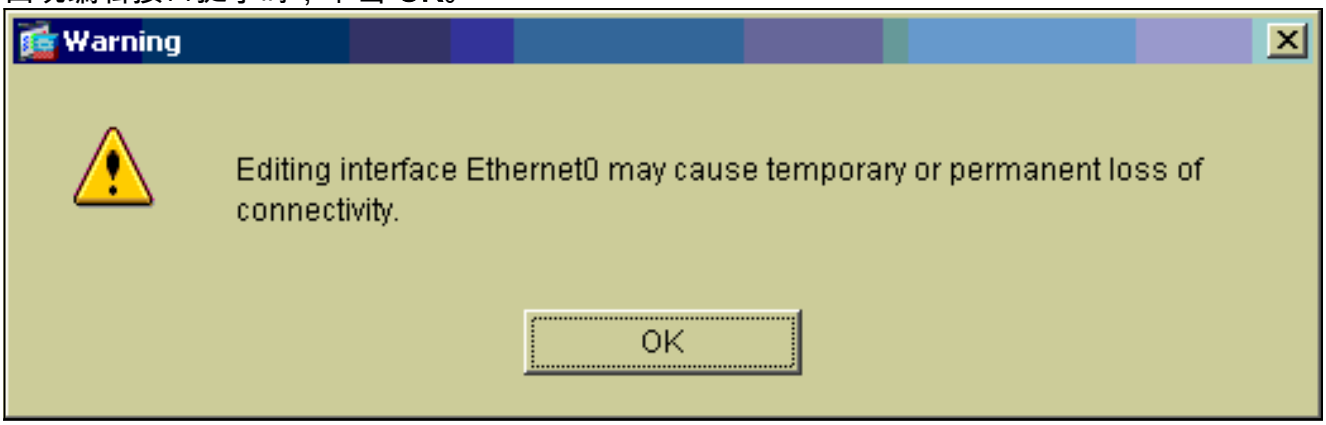
1. 通过控制台连接到 PIX。基于原始配置，使用交互式提示启用**高级安全设备管理器 GUI (ASDM)**，以便从工作站 10.1.1.3 管理 PIX。
2. 从工作站 10.1.1.3 打开 Web 浏览器并使用 ADSM（在此示例中为 https://10.1.1.1）。
3. 在出现证书提示时选择 **Yes**，并使用 PIX 防火墙 ASDM 引导配置中所配置的启用口令登录。
4. 如果这是在 PC 上首次运行 ASDM，则系统会提示您是使用 ASDM 启动程序还是使用 ASDM 作为 Java 应用程序。在此示例中会选择 ASDM 启动程序并安装这些提示。
5. 前进到 ASDM 主窗口并选择 Configuration 选项卡。



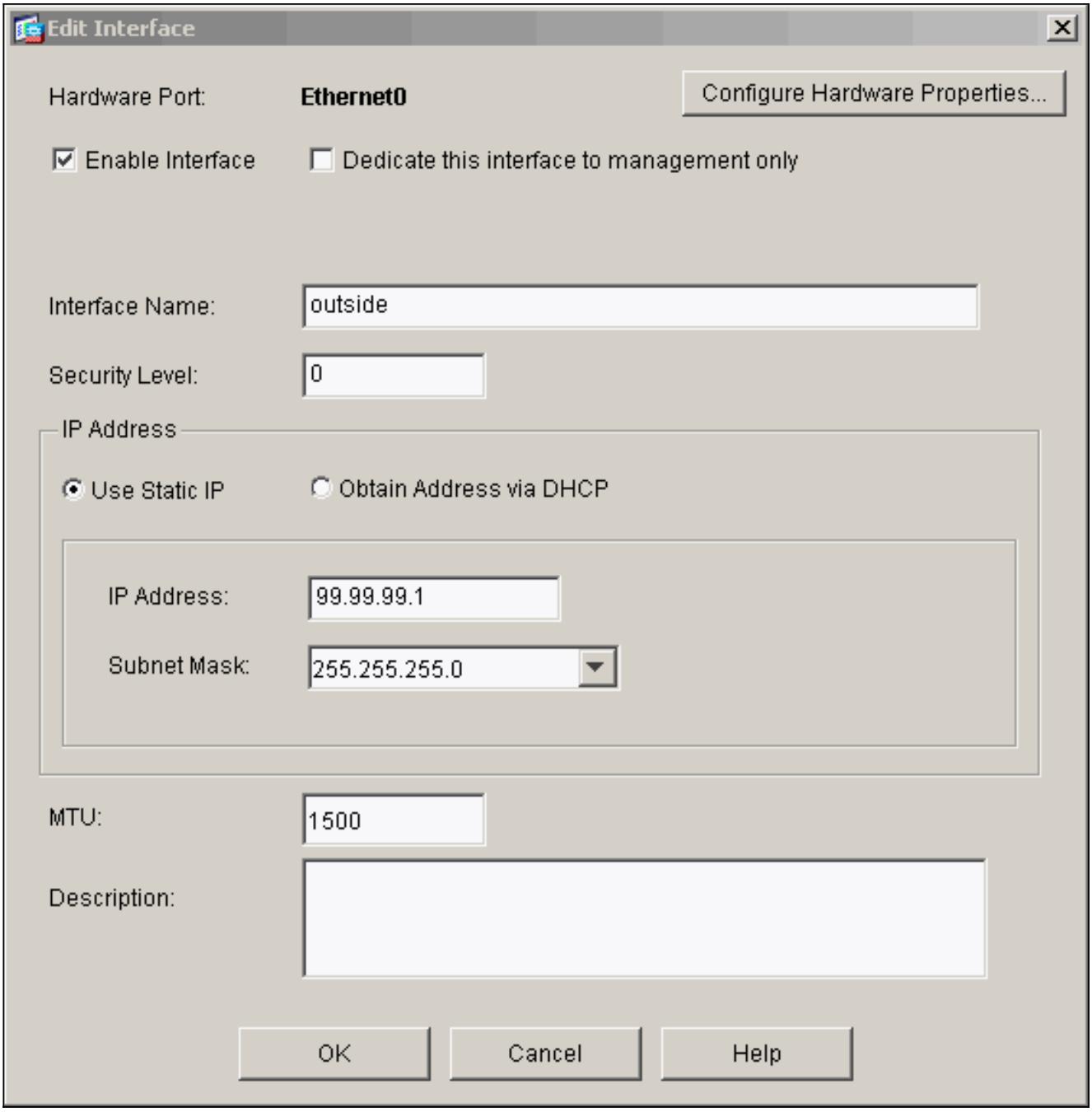
6. 突出显示 **Ethernet 0 Interface** 并单击 **Edit** 以配置外部接口。



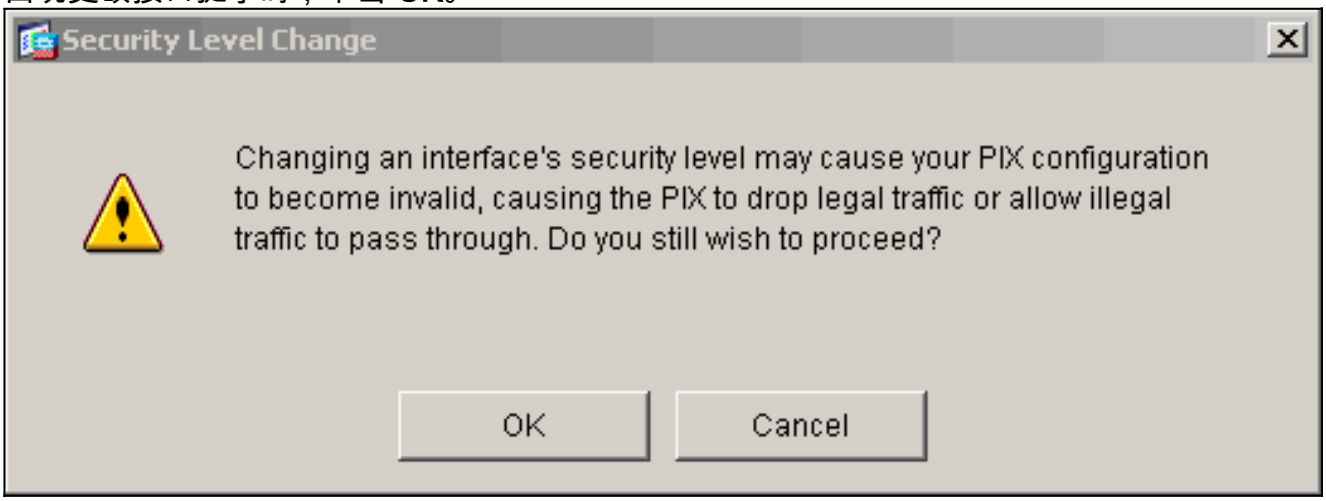
7. 出现编辑接口提示时，单击 **OK**。



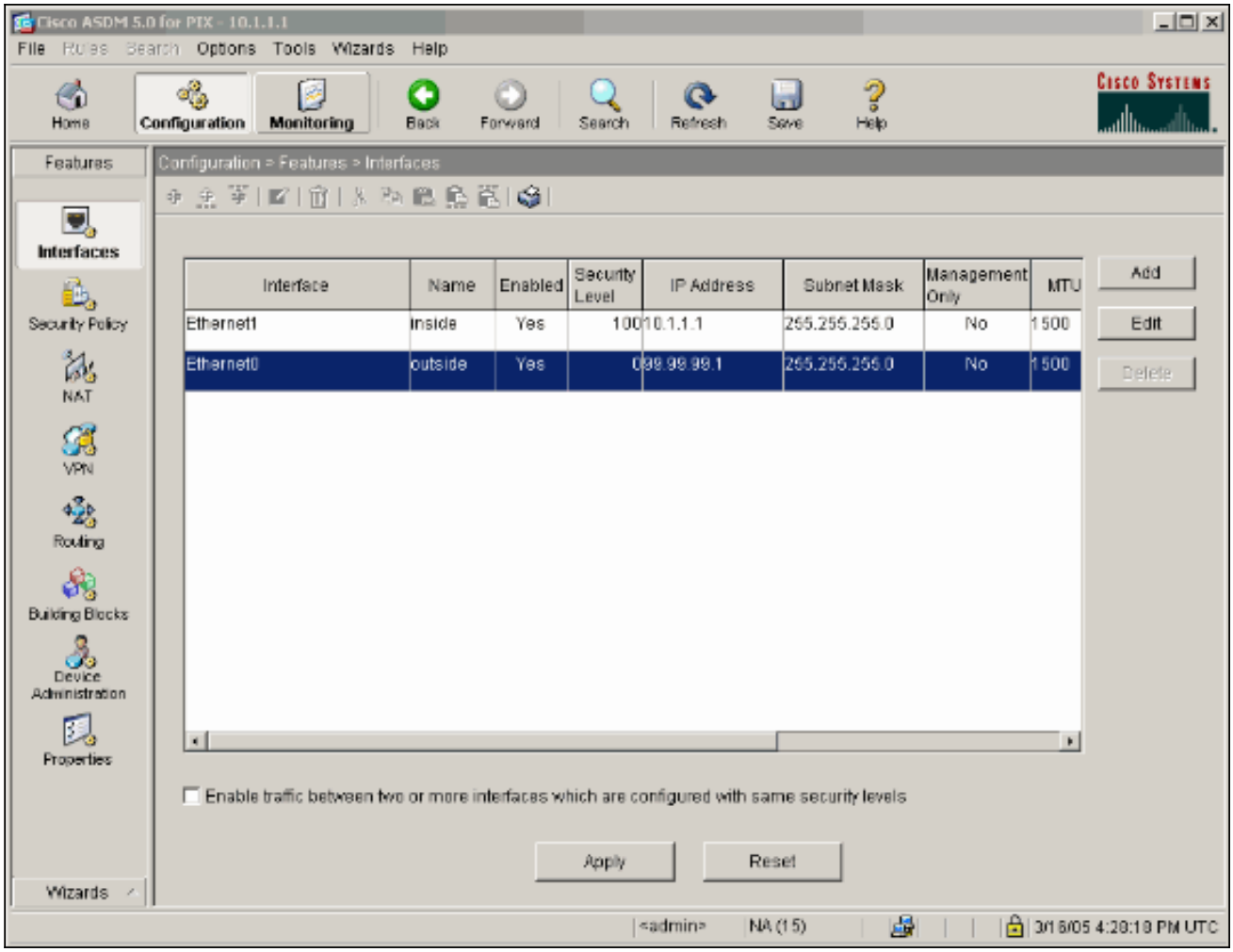
8. 输入接口详细资料，并在完成后单击 **OK**。



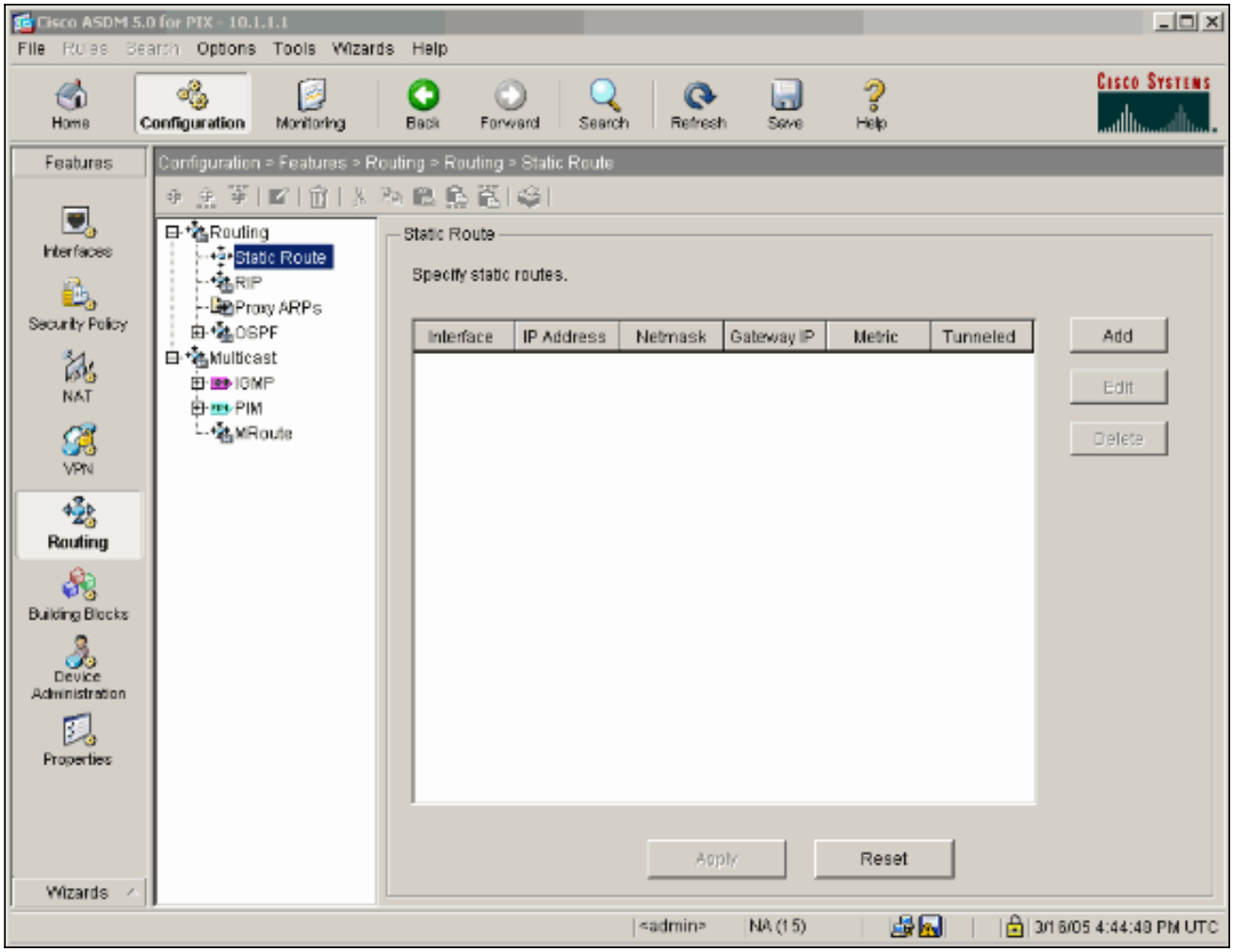
9. 出现更改接口提示时，单击 **OK**。



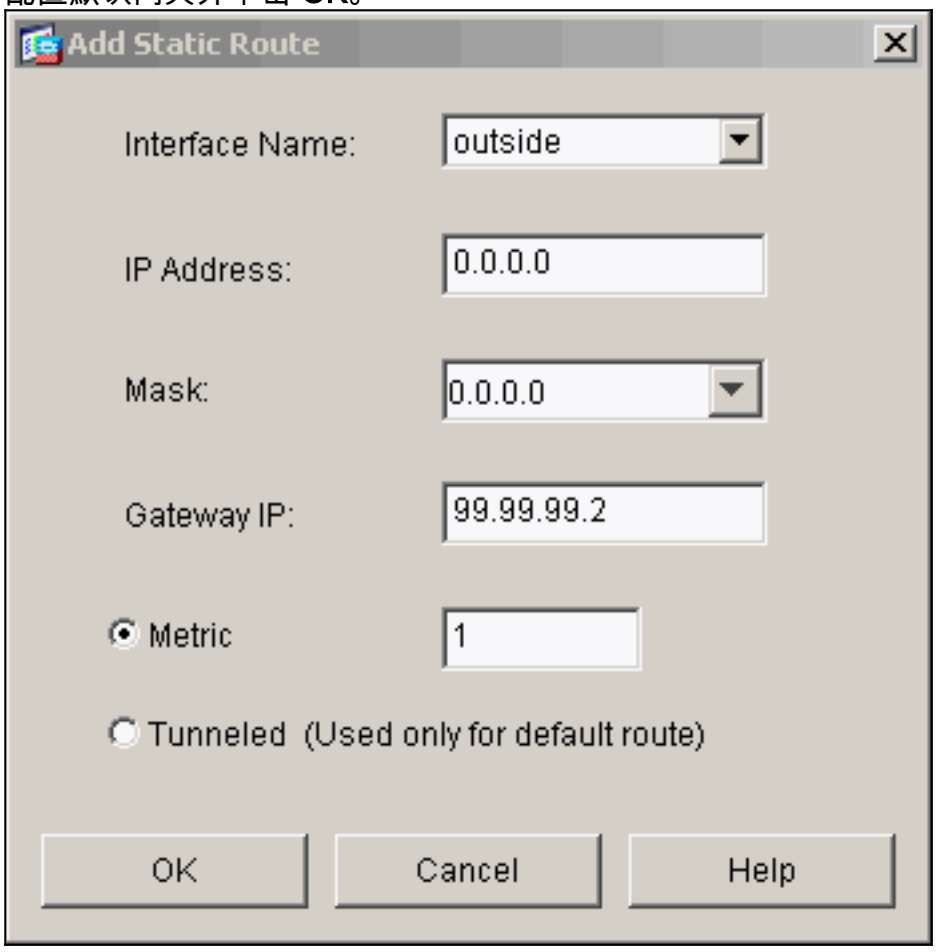
10. 单击 **Apply** 以接受接口配置。此配置也将被推送到 PIX 上。此示例使用静态路由。



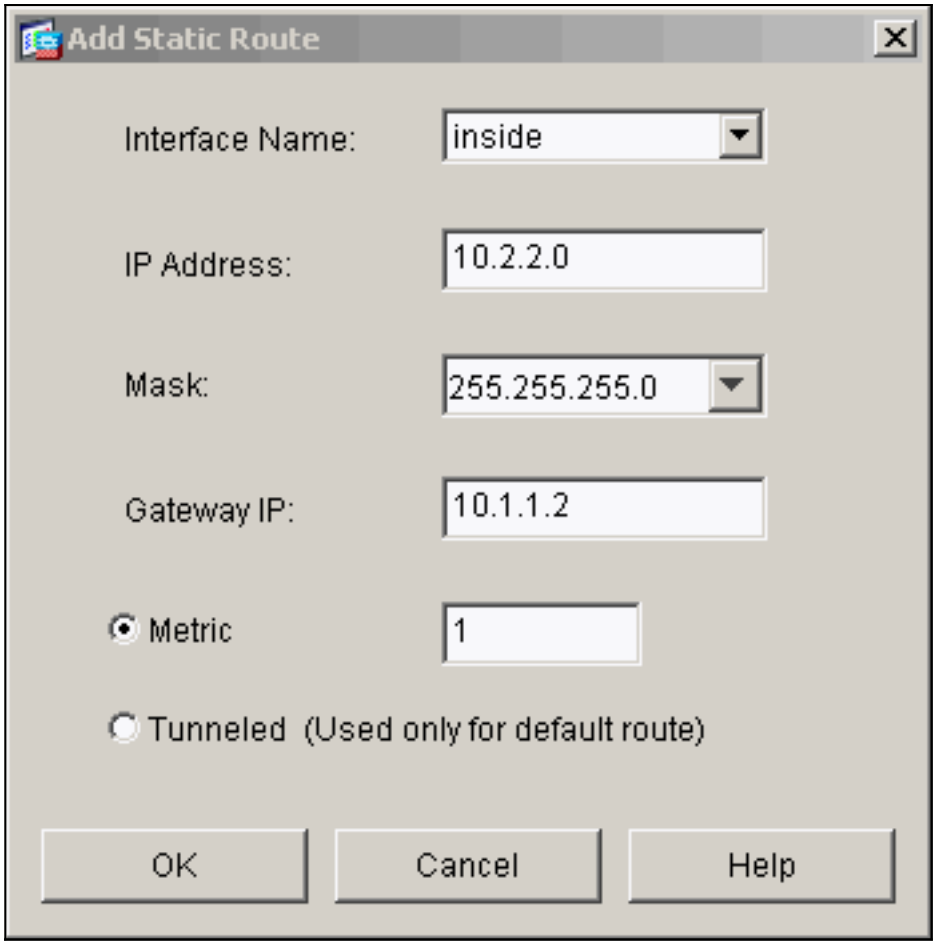
11. 在 Features 选项卡下单击 **Routing**，突出显示 **Static Route**，然后单击 **Add**。



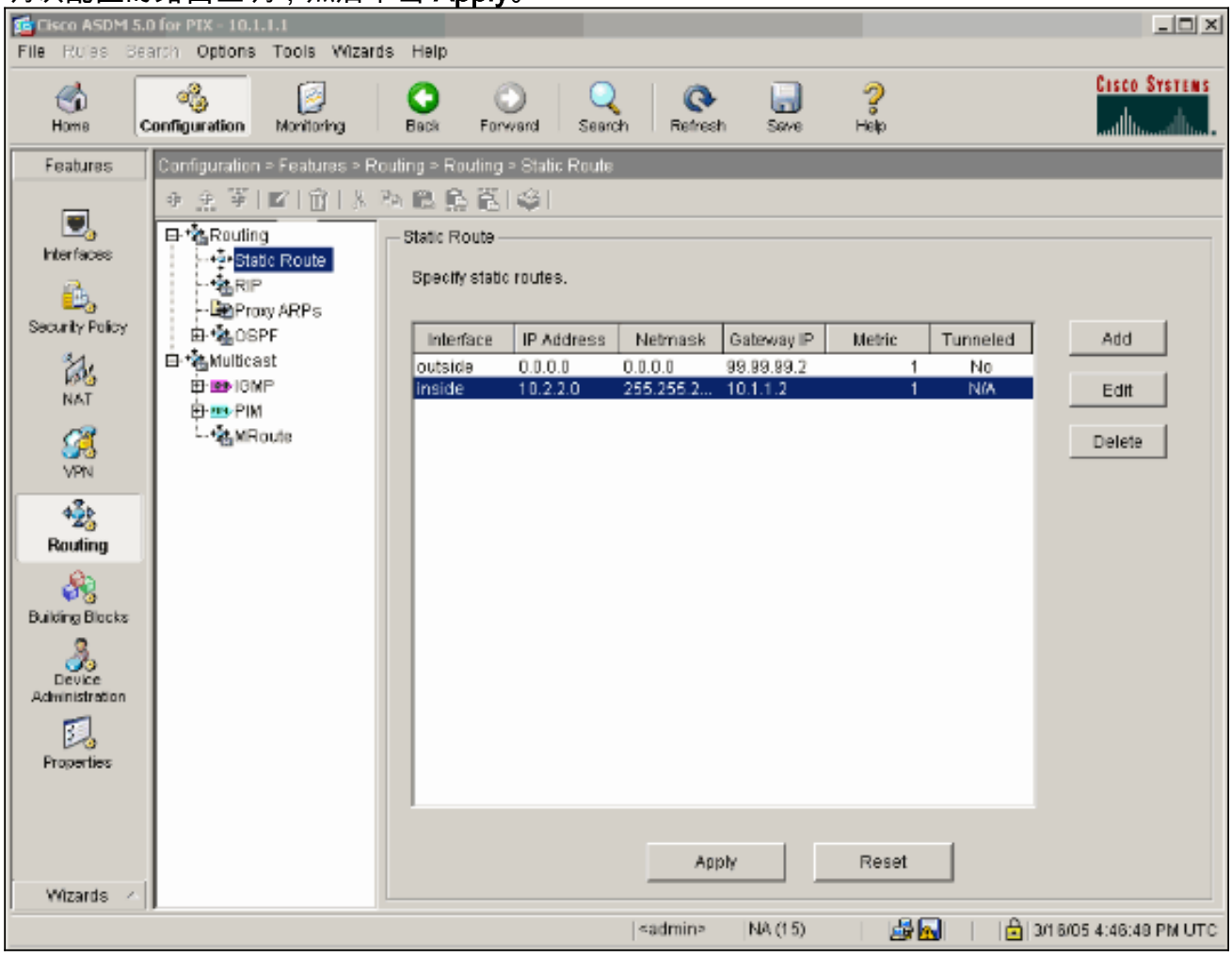
12. 配置默认网关并单击 **OK**。



13. 单击 **Add** 以将路由添加到网络内部。

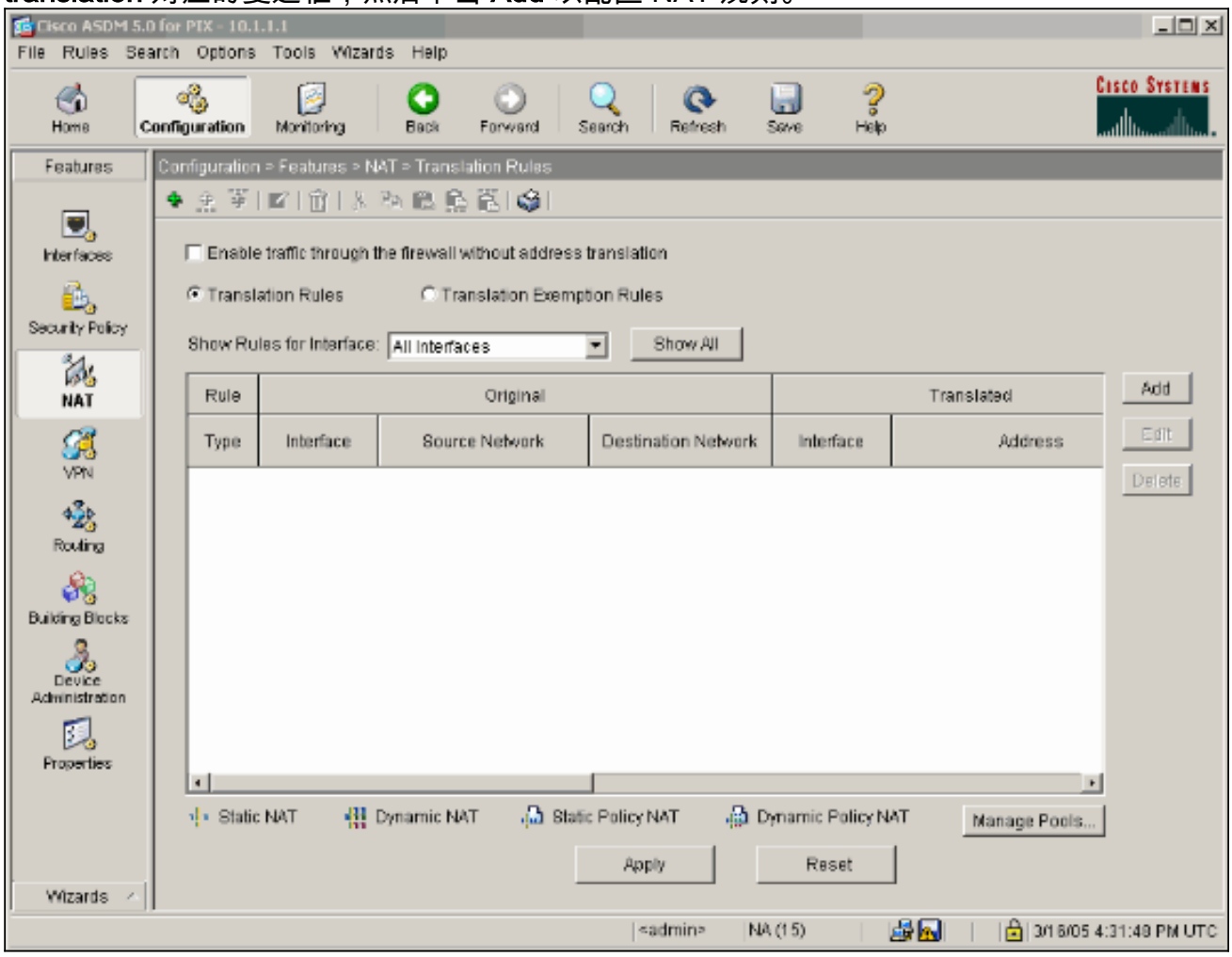


14. 确认配置的路由正确，然后单击 **Apply**。

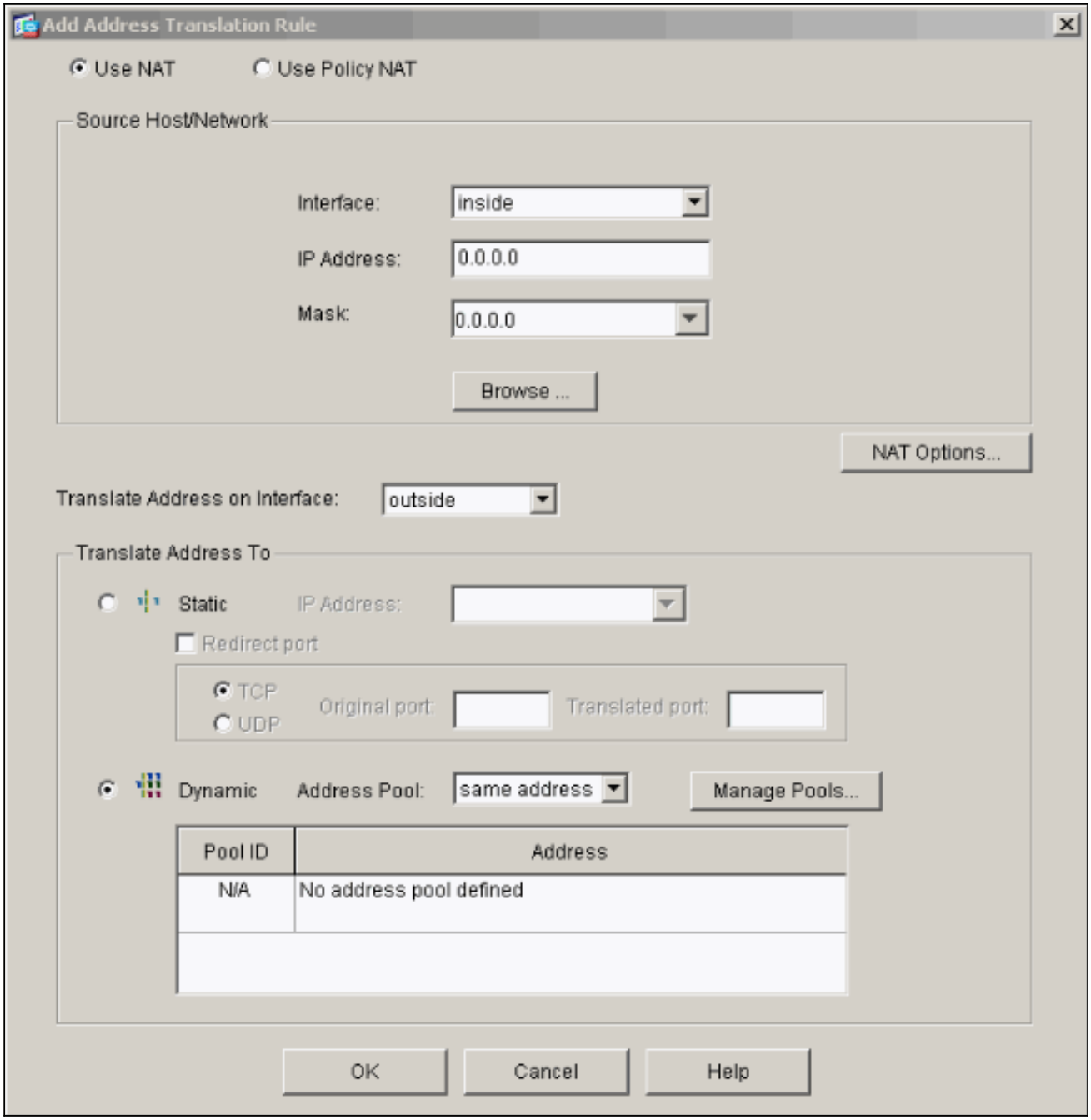


15. 在本示例中，使用 NAT。取消选中 **Enable traffic through the firewall without address**

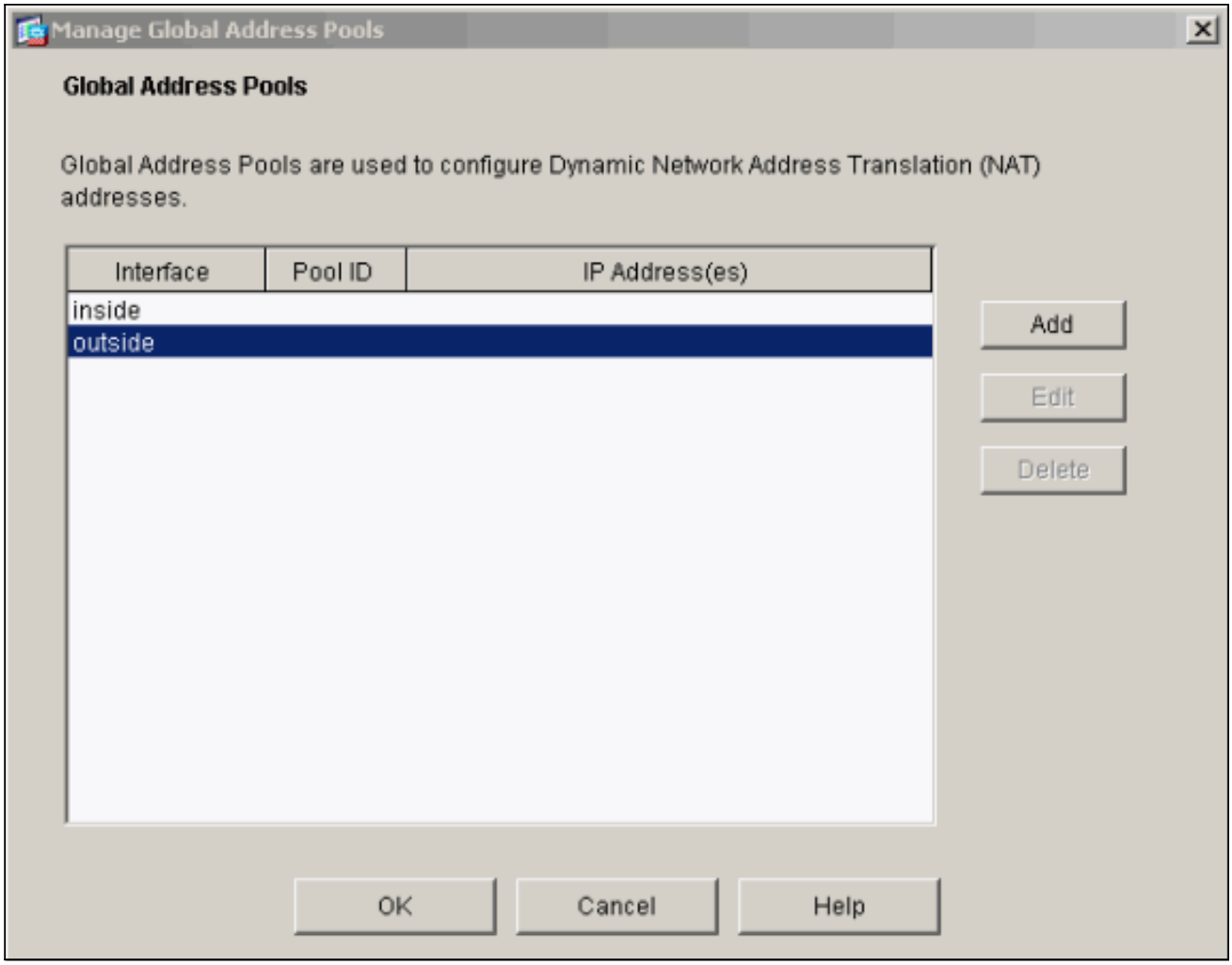
translation 对应的复选框，然后单击 **Add** 以配置 NAT 规则。



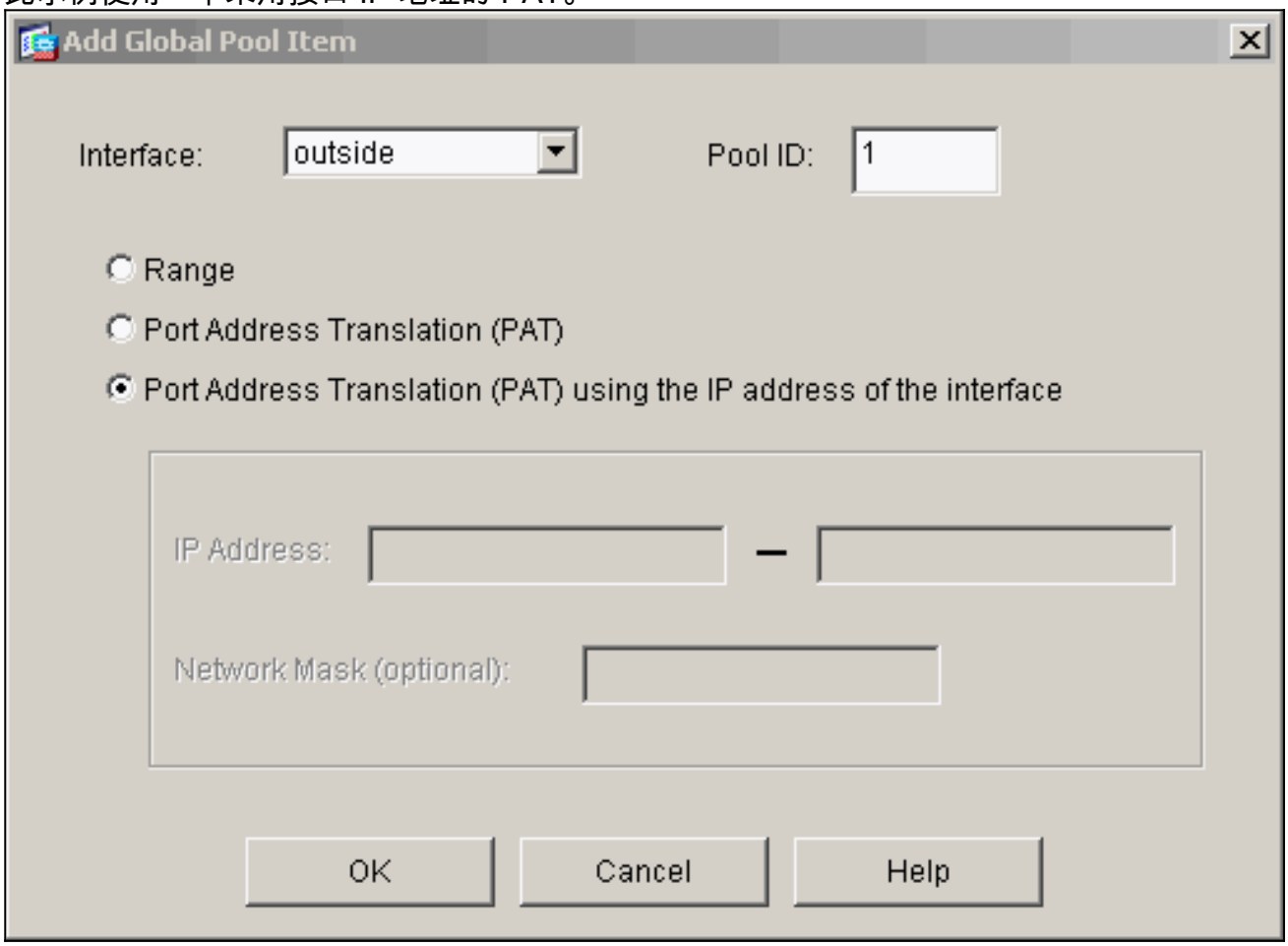
16. 配置源网络（此示例使用任意网络）。然后单击 **Manage Pools** 以定义 PAT。



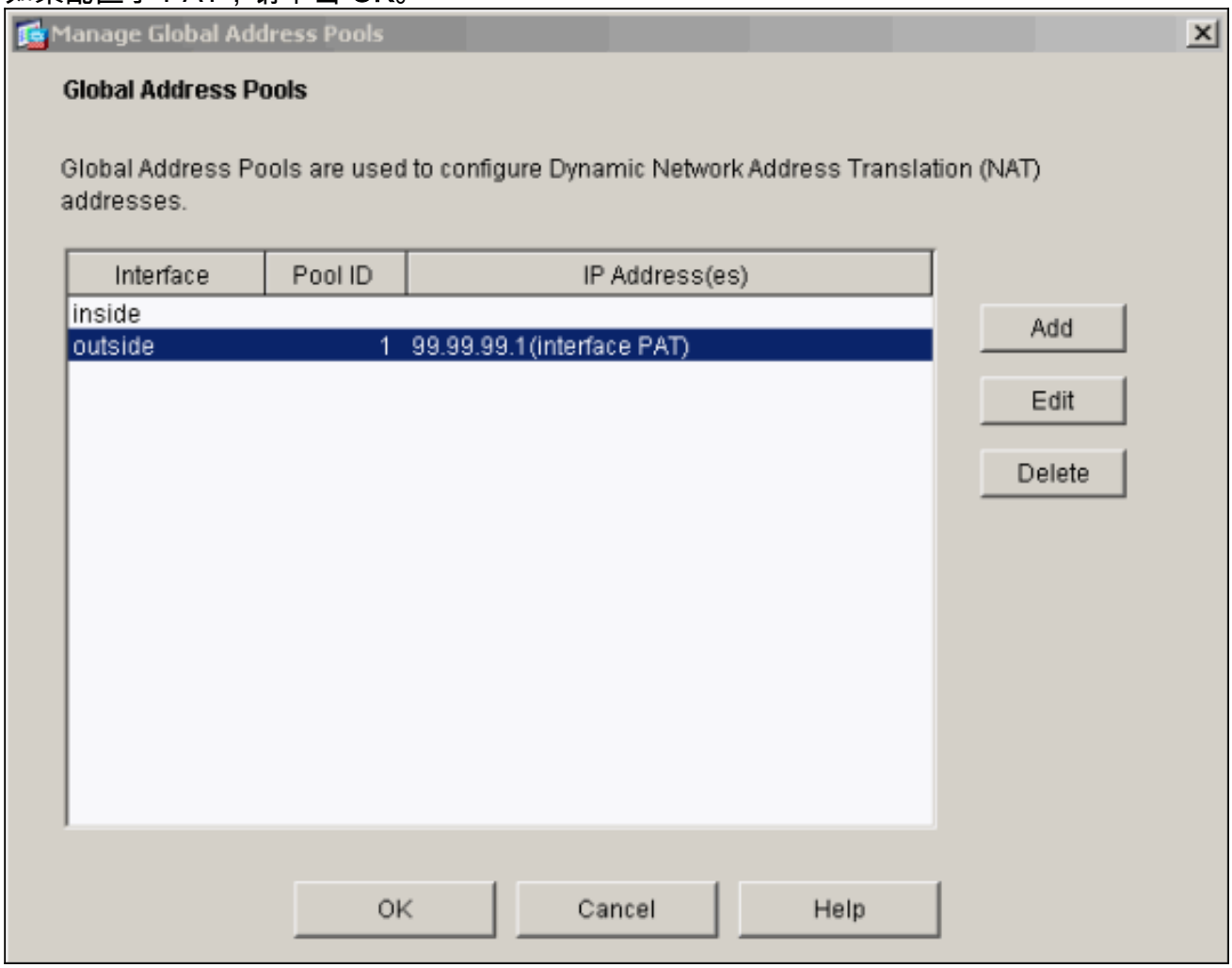
17. 选择外部接口并单击 **Add**。



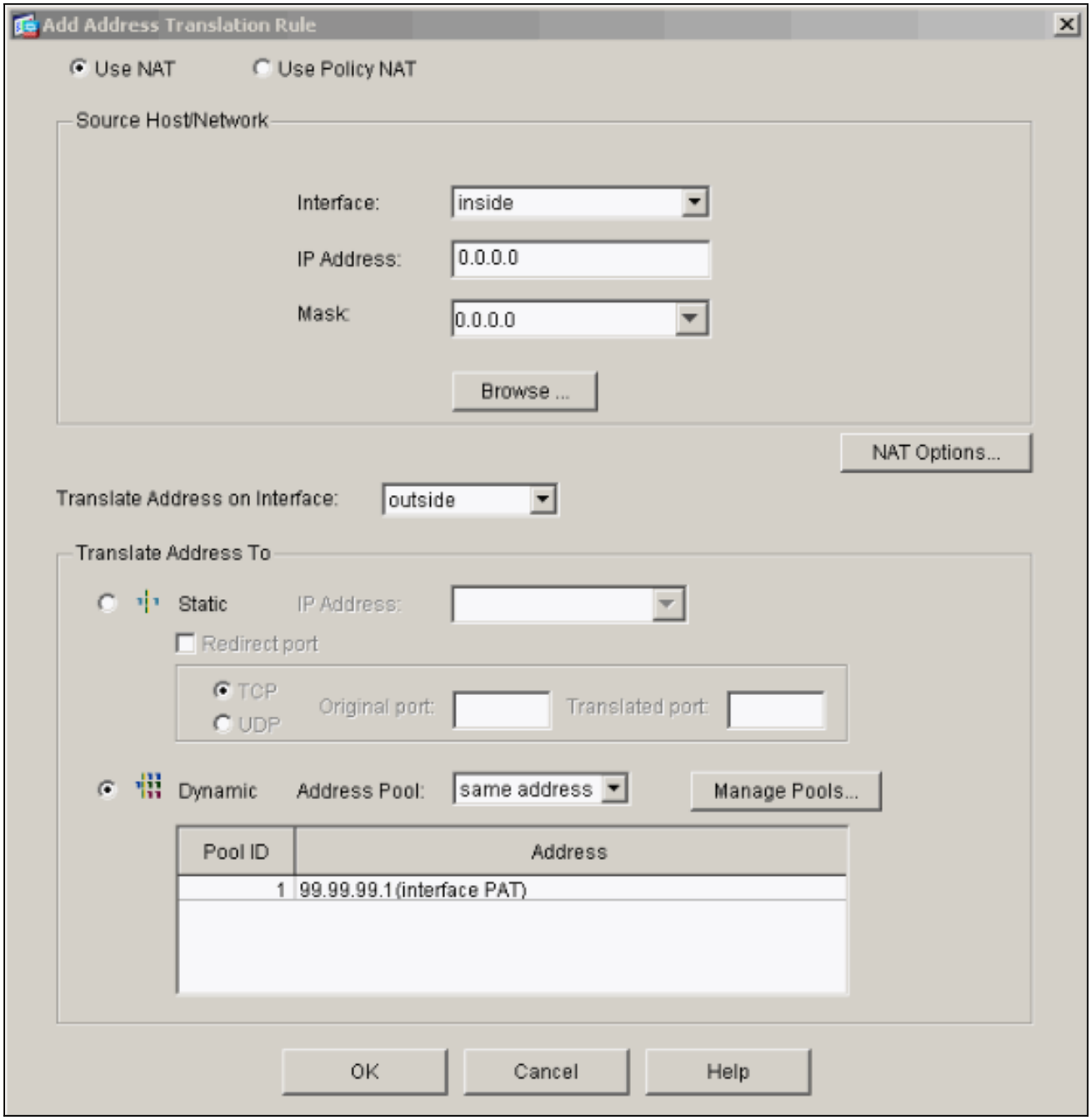
此示例使用一个采用接口 IP 地址的 PAT。



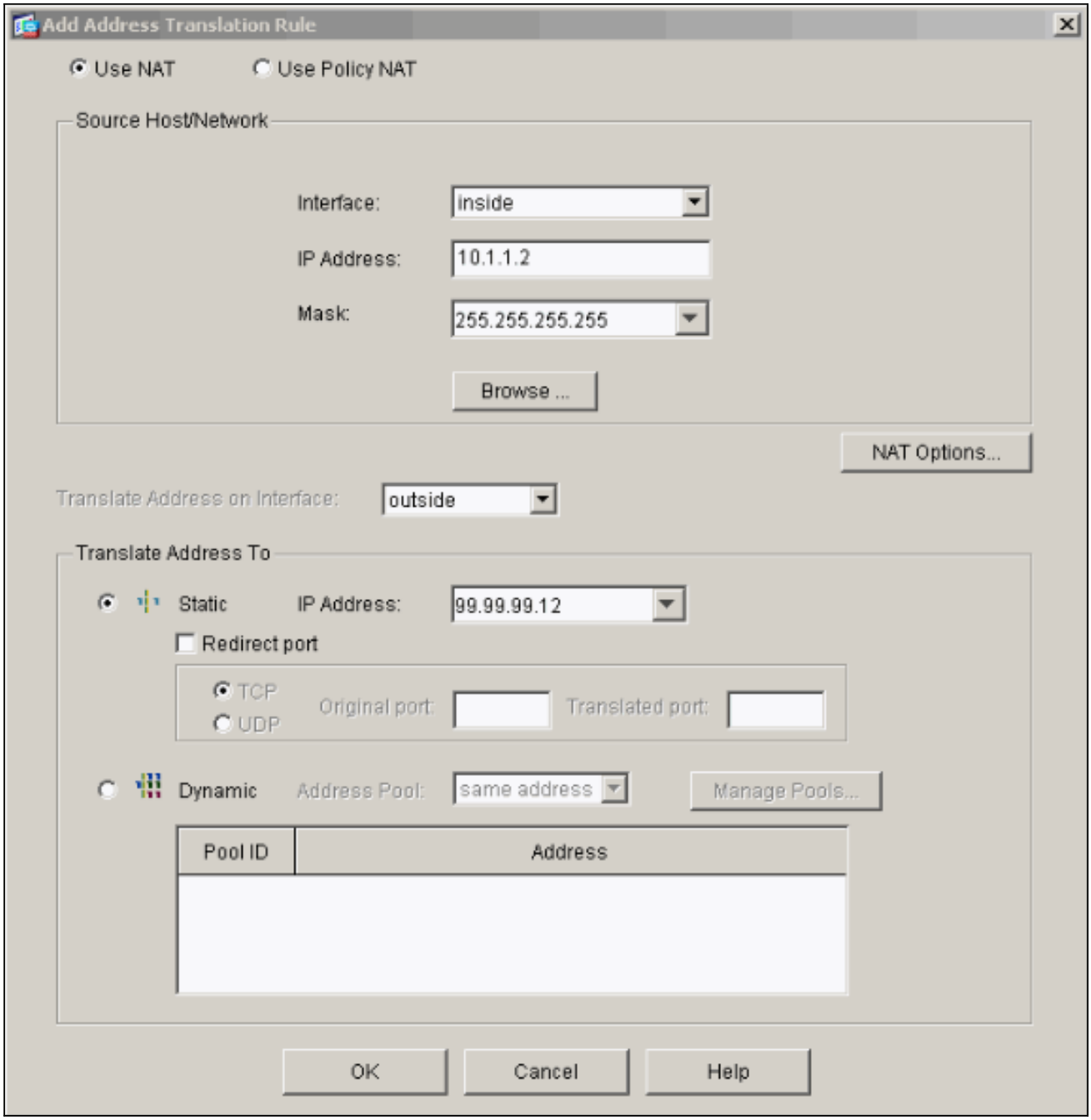
18. 如果配置了 PAT，请单击 **OK**。



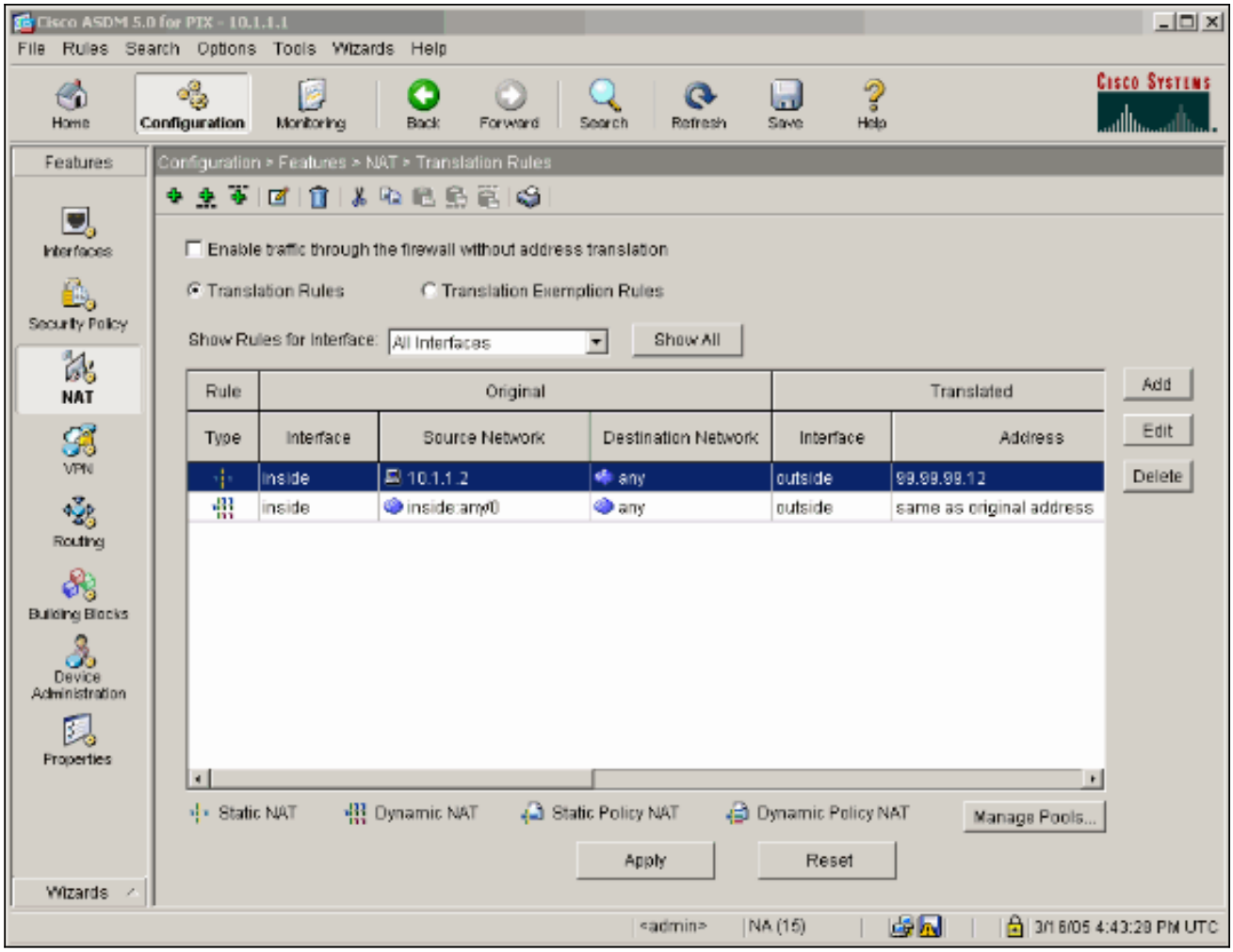
19. 单击 **Add** 以配置静态转换。



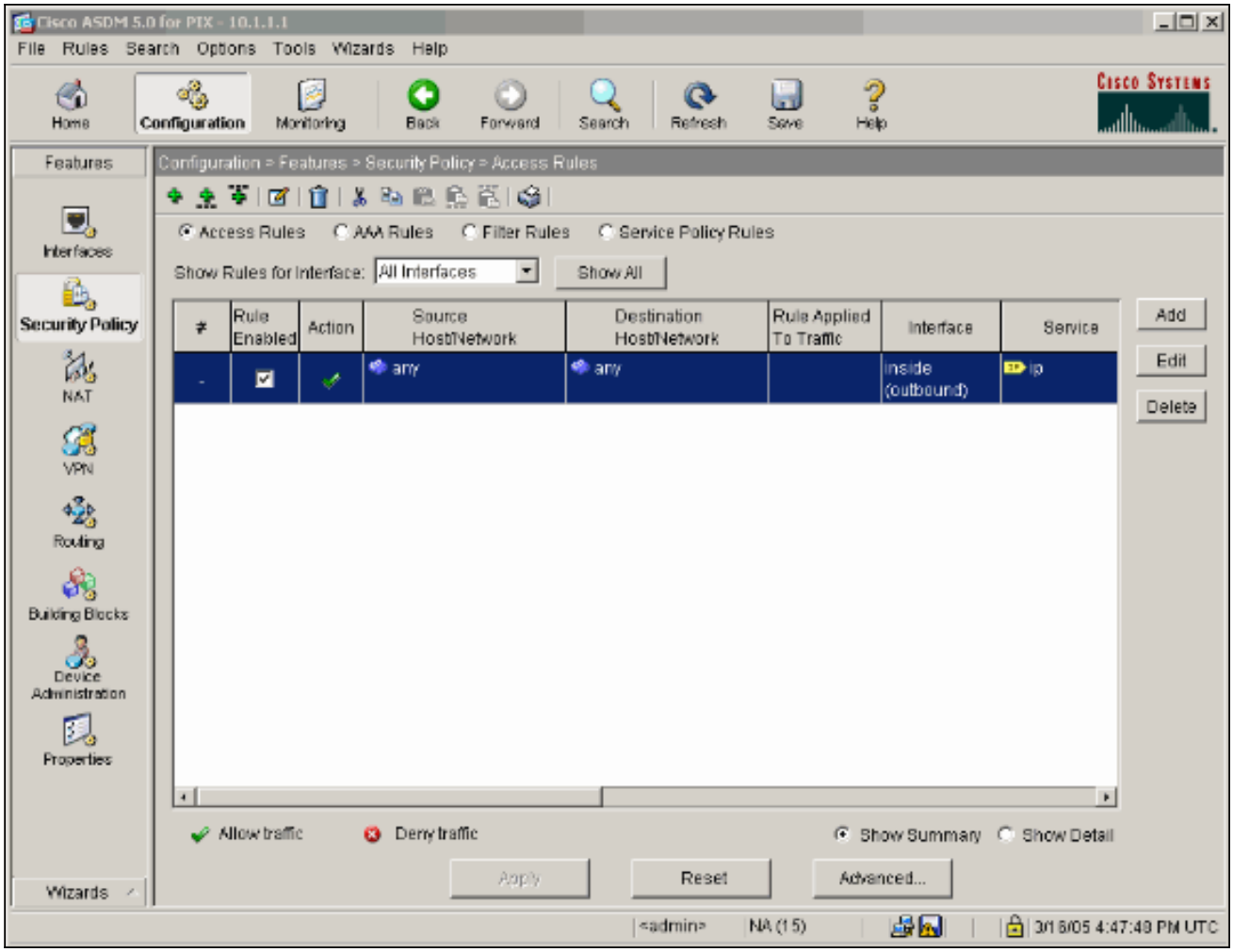
20. 在 Interface 下拉列表中选择 **inside**，然后输入 IP 地址 10.1.1.2 和子网掩码 **255.255.255.255**，选择 **Static**，并在 IP Address 字段中键入外部地址 **99.99.99.12**。完成后单击 **OK**。



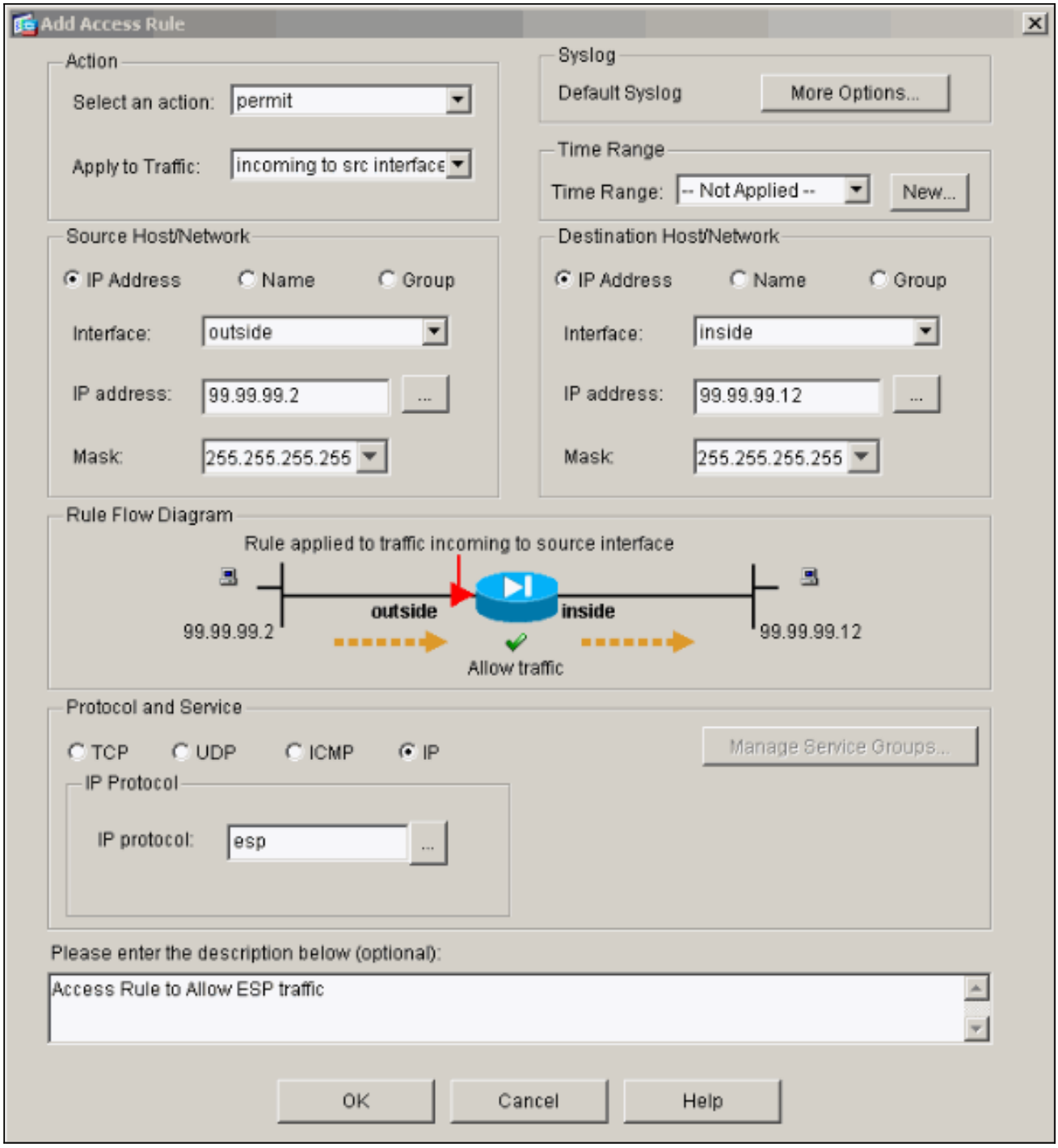
21. 点击 **Apply** 接受接口配置。此配置也将被推送到 PIX 上。



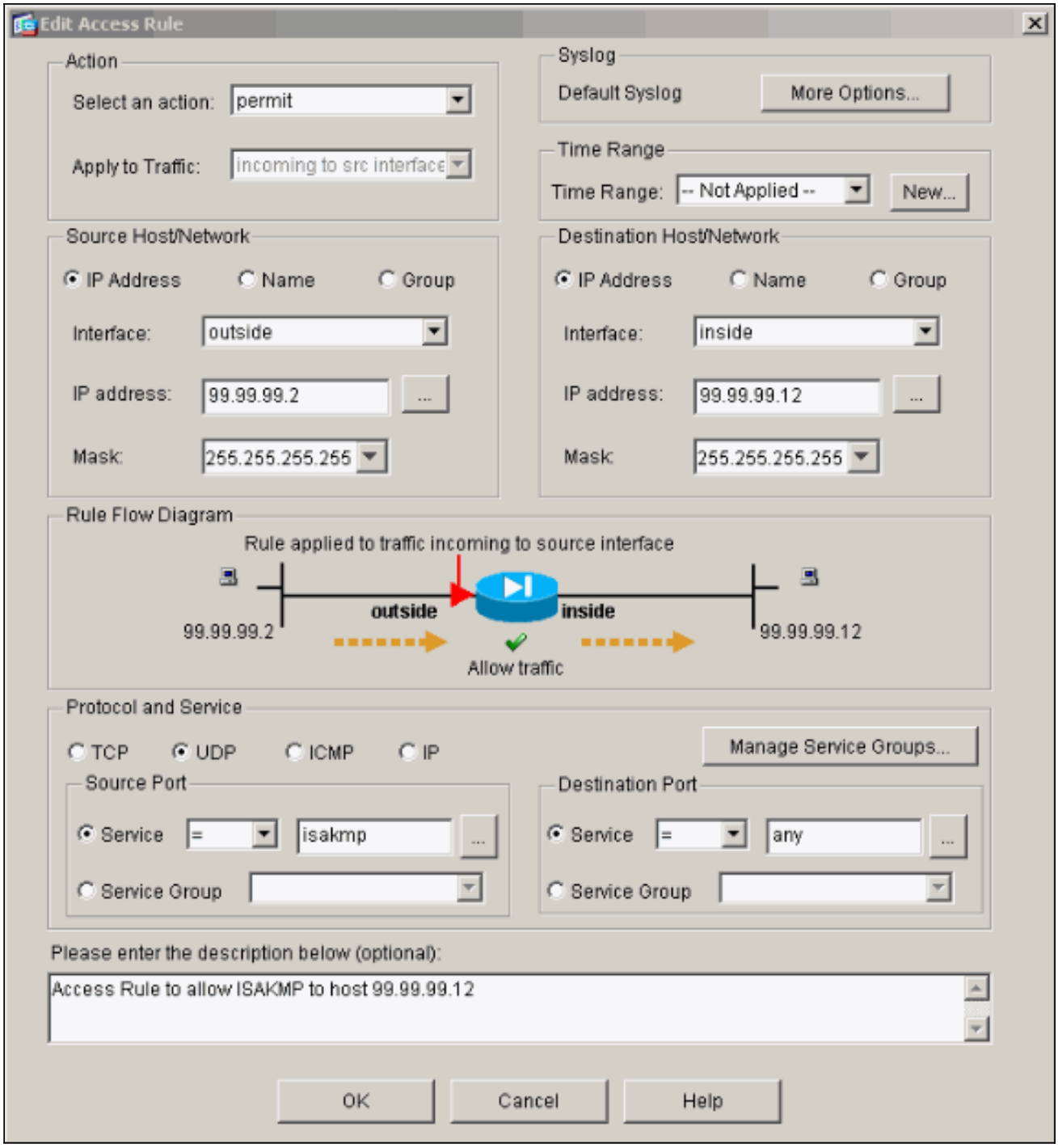
22. 在 Features 选项卡下选择 **Security Policy** 以配置安全策略规则。



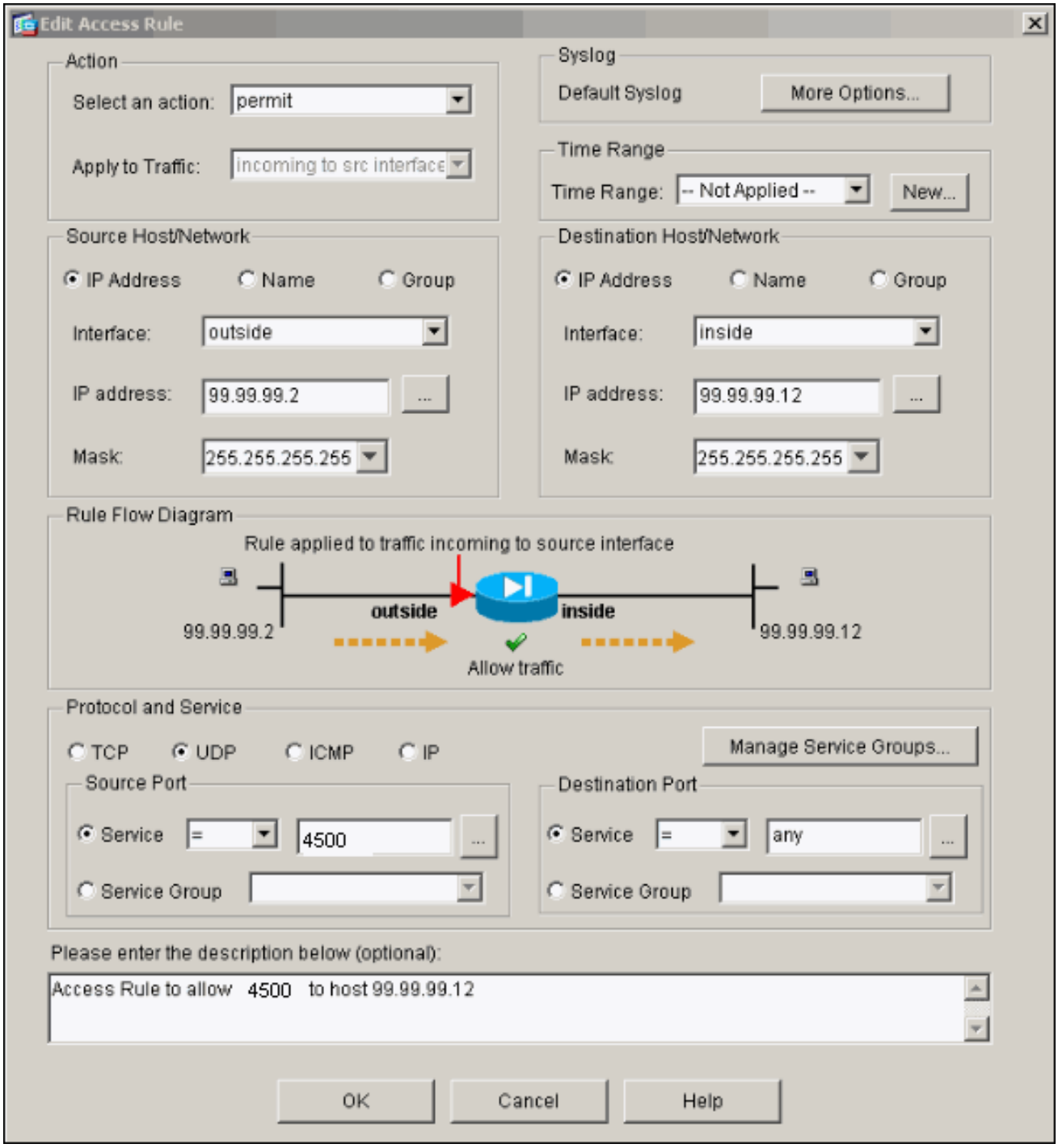
23. 单击 **Add** 以允许 esp 流量，然后单击 **OK** 以继续。



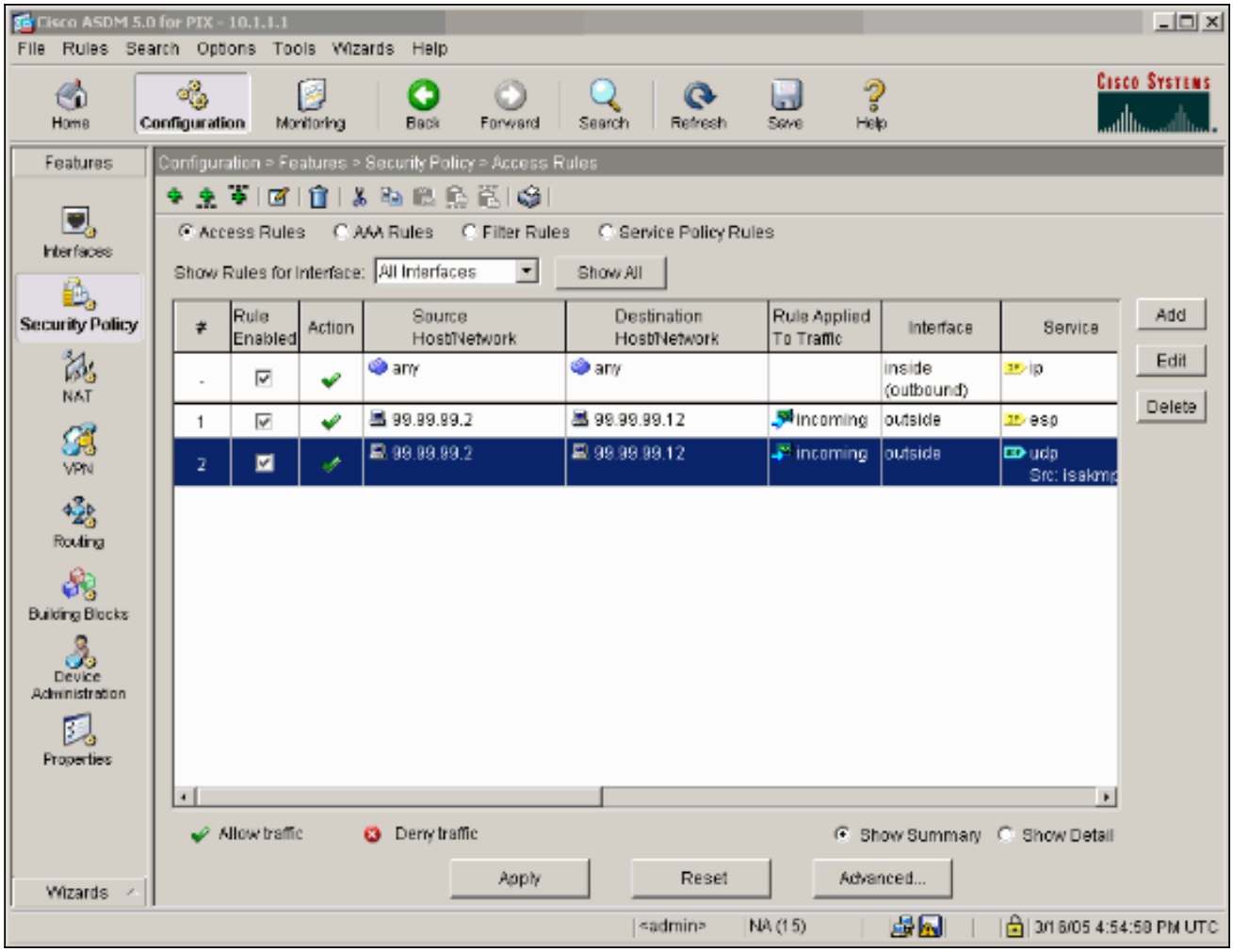
24. 单击 **Add** 以允许 ISAKMP 流量，然后单击 **OK** 以继续。



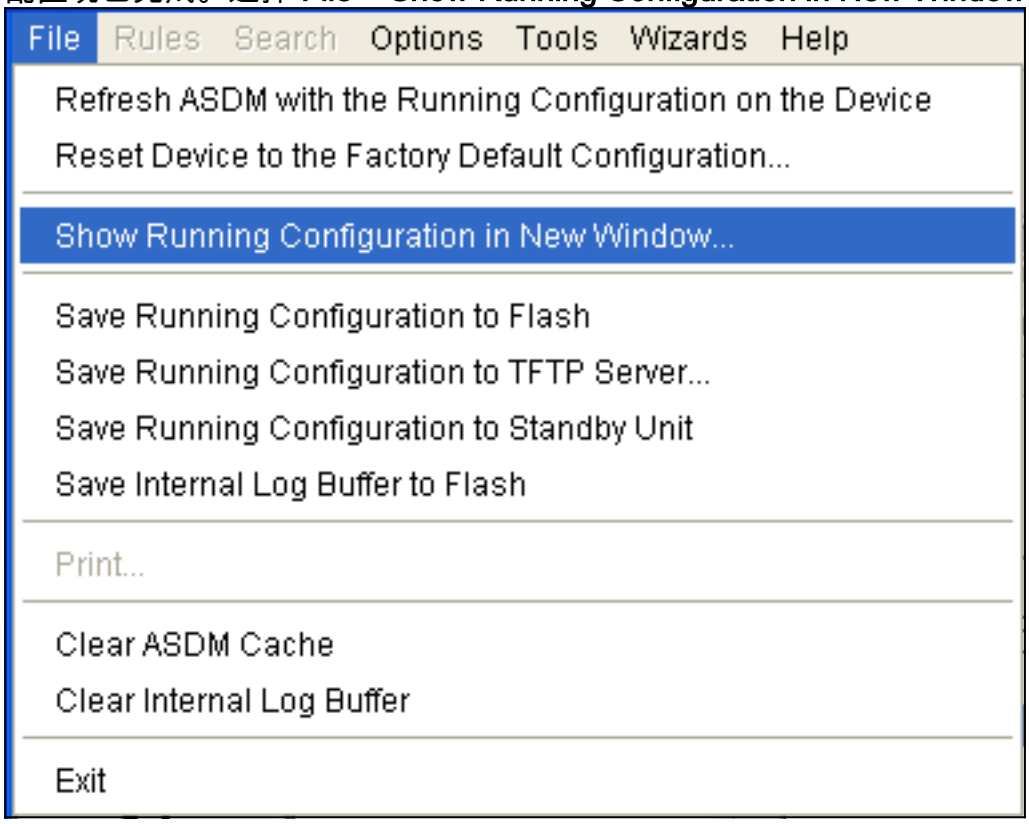
25. 单击 **Add** 以允许 NAT-T 的 UDP 端口 4500 流量，然后单击 **OK** 以继续。



26. 单击 **Apply** 以接受接口配置。此配置也将被推送到 PIX 上。



27. 配置现已完成。选择 **File > Show Running Configuration in New Window** 以查看 CLI 配置。



[PIX 防火墙配置]

PIX 防火墙

```
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 安全设备和 MPF（模块化策略框架）配置

应在 MPF（模块化策略框架）中使用 **inspect ipsec-pass-thru** 命令使 IPsec 流量通过 PIX/ASA 安全设备，而不是使用访问列表。

此检查会配置为 ESP 流量打开针孔。存在转发流时，会允许所有 ESP 数据流，对于可以允许的最大连接数没有限制。不允许 AH。ESP 数据流的默认空闲超时在默认情况下设置为 10 分钟。此检查可以应用于能应用其他检查的所有位置，包括类和 match 命令模式。IPSec Pass Through 应用程序检查提供对与 IKE UDP 端口 500 连接关联的 ESP（IP 协议 50）流量的方便遍历。它无需冗长的访问列表配置即可允许 ESP 流量，并且还通过超时和最大连接数来提供安全性。使用 **class-map**、**policy-map** 和 **service-policy** 命令可定义流量类，将检查命令应用于该类，以及将策略应用于一个或更多接口。在启用时，**inspect IPSec-pass-thru** 命令允许不受限制的 ESP 流量，并且超时为 10 分钟（不可配置）。允许 NAT 和非 NAT 流量。

```
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
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示第 2 阶段安全连接。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。
- **show crypto engine connections active** - 显示加密的数据包和解密的数据包。

故障排除

本部分提供的信息可用于对配置进行故障排除。

路由器 IPSec 的故障排除命令

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto engine** - 显示已加密的流量。
- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp**—显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。

清除安全关联

- **clear crypto isakmp** — 清除 Internet Key Exchange (IKE) 安全关联。
- **clear crypto ipsec sa** — 清除 IPsec 安全关联。

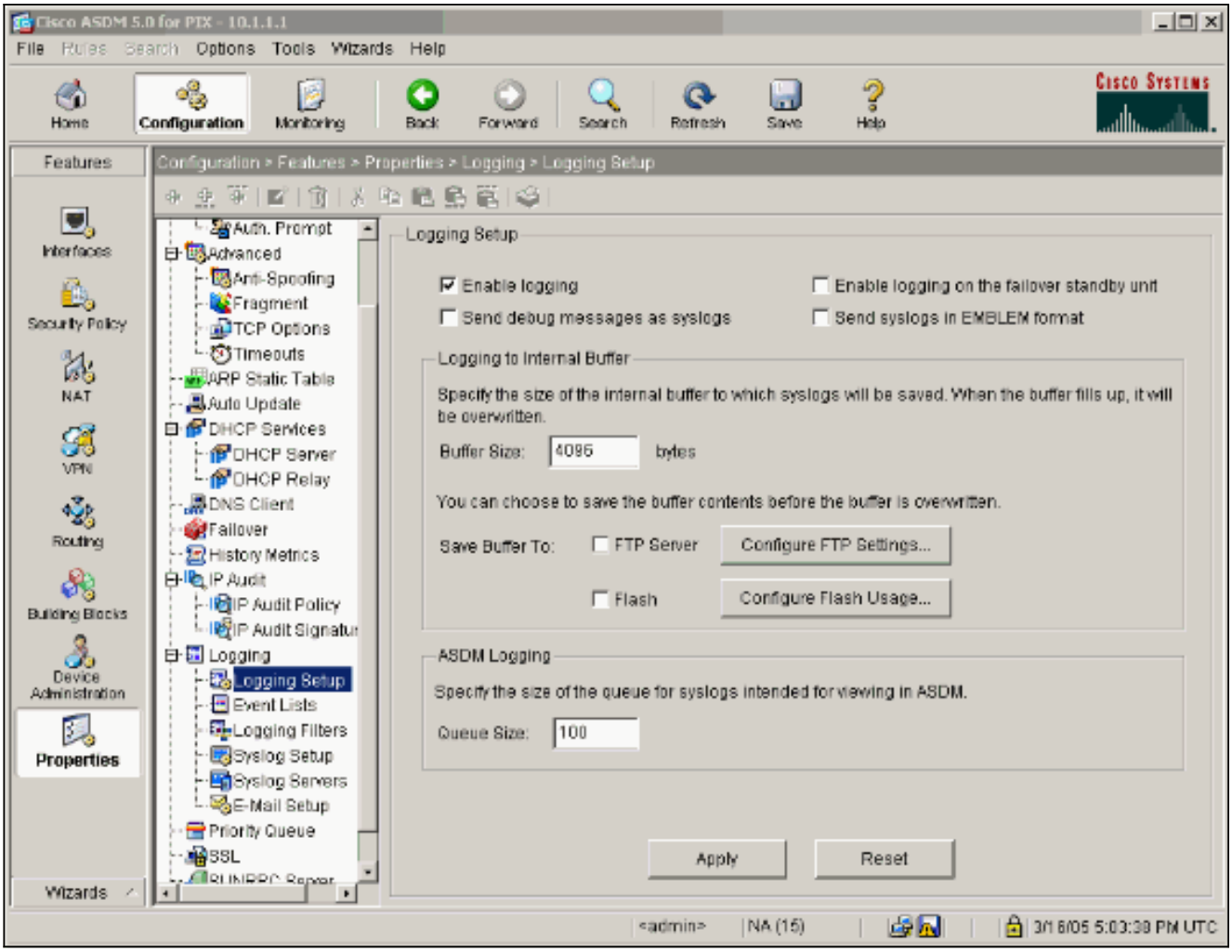
PIX 的故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

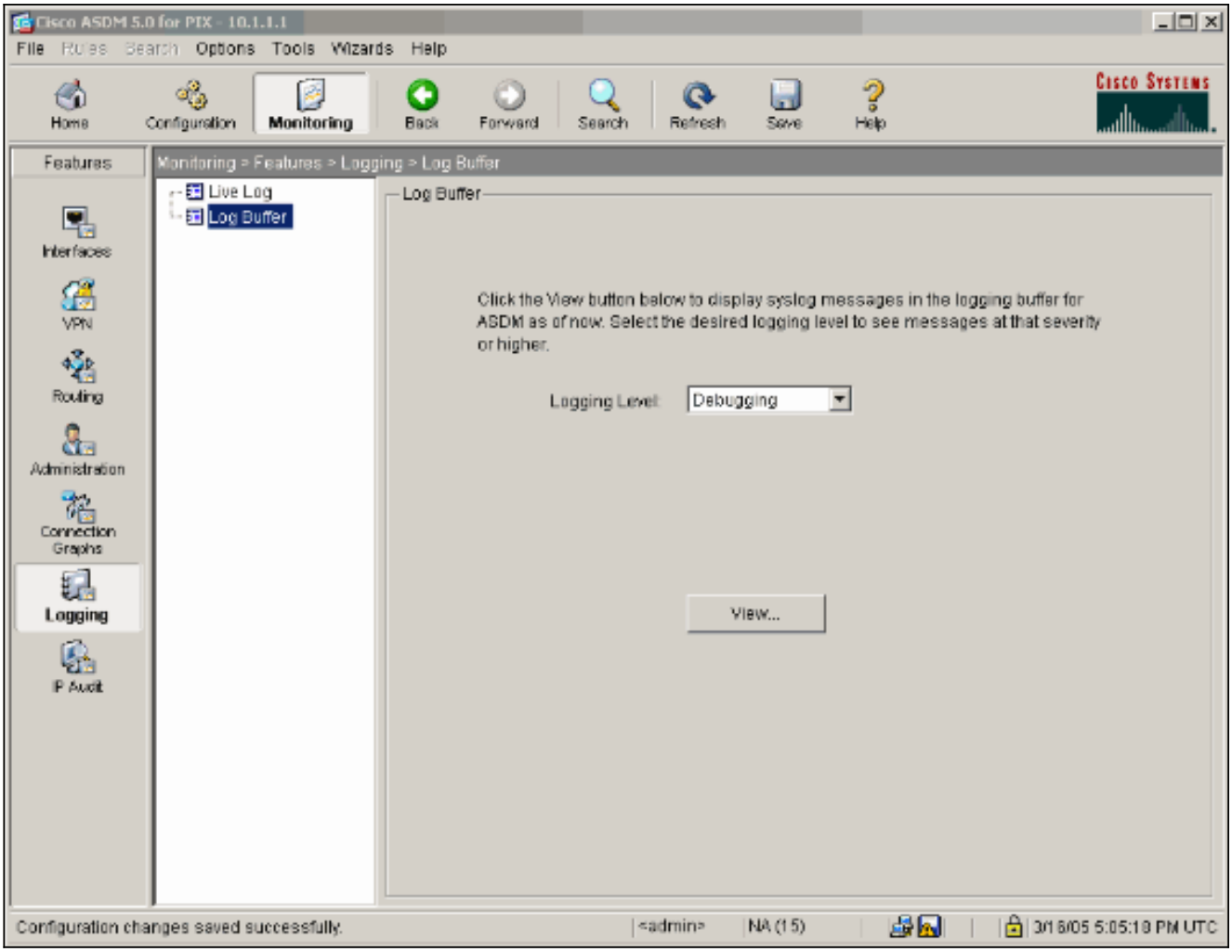
注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **logging buffer debugging** - 显示正在建立和已拒绝的连接，这些连接通过 PIX 指向主机。信息存储在 PIX 日志缓冲器中，使用 **show log** 命令可查看输出。
- 如这些步骤所示，ASDM 可用于启用日志记录以及查看日志。

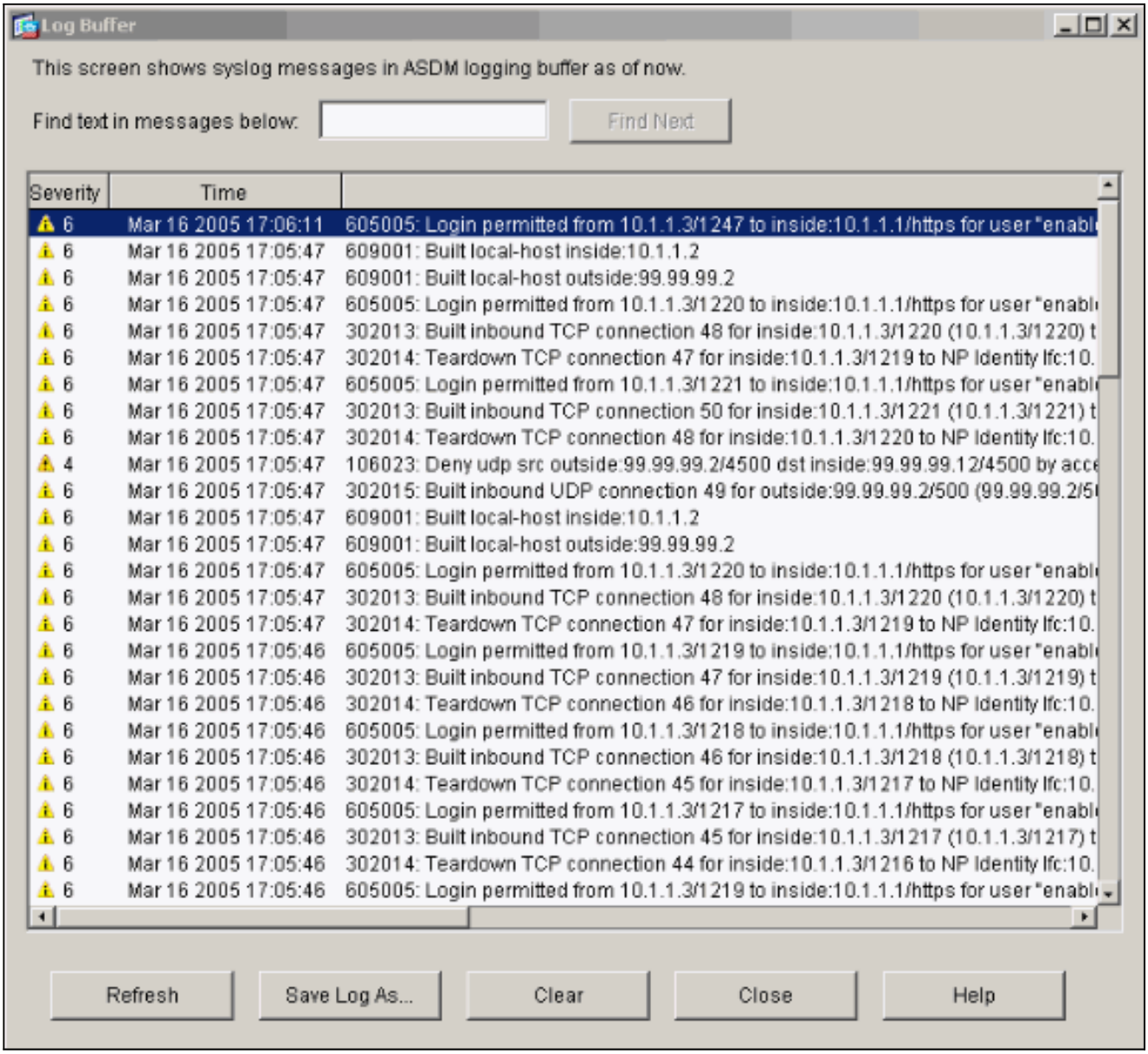
1. 选择 **Configuration > Properties > Logging > Logging Setup > Enable Logging**，然后单击 **Apply**。



2. 选择 **Monitoring > Logging > Log Buffer > On Logging Level > Logging Buffer**，然后单击 **View**。



下面是一个 Log Buffer 示例。



相关信息

- IPsec 协商/IKE 协议支持页
- PIX 支持页
- PIX 命令参考
- NAT 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems