Ejemplo de Configuración del Túnel VPN IPsec PIX/ASA (Versión 7.x y Posterior) con Traducción de Dirección de Red

Contenido

Introducción

Esta configuración de ejemplo demuestra un túnel VPN IPsec a través de un firewall que realiza la Conversión de Dirección de Red (NAT). Esta configuración no funciona con la traducción de direcciones de puerto (PAT) si utiliza versiones del software Cisco IOS® anteriores a la 12.2(13)T, sin incluirla. Este tipo de configuración se puede utilizar para tunelizar el tráfico IP. Esta configuración no se puede utilizar para cifrar el tráfico que no pasa a través de un firewall, como IPX o actualizaciones de ruteo. La tunelización de encapsulación de routing genérico (GRE) es una opción más apropiada. En este ejemplo, los routers Cisco 2621 y 3660 son los extremos del túnel IPsec que se unen a dos redes privadas, con conductos o listas de control de acceso (ACL) en el PIX en medio para permitir el tráfico IPsec.

Nota: NAT es una traducción de direcciones de uno a uno, no debe confundirse con PAT, que es una traducción de varios (dentro del firewall) a uno. Para obtener más información sobre el funcionamiento y la configuración de NAT, consulte Verificación del Funcionamiento de NAT y Troubleshooting de NAT Básico o Cómo Funciona NAT.

Nota: Es posible que IPsec con PAT no funcione correctamente porque el dispositivo de punto final del túnel exterior no puede gestionar varios túneles desde una dirección IP. Póngase en contacto con su proveedor para determinar si los dispositivos terminales de túnel funcionan con PAT. Además, en Cisco IOS Software Release 12.2(13)T y posteriores, la función NAT Transparency se puede utilizar para PAT. Para obtener más detalles, consulte Transparencia IPSec NAT. Consulte Soporte para IPSec ESP a través de NAT para obtener más información sobre estas funciones en Cisco IOS Software Release 12.2(13)T y posteriores.

Nota: Antes de abrir un caso con el Soporte Técnico de Cisco, consulte Preguntas Frecuentes sobre NAT, que tiene muchas respuestas a preguntas comunes.

Consulte Configuración de un Túnel IPSec a través de un Firewall con NAT para obtener más información sobre cómo configurar el túnel IPsec a través del firewall con NAT en la versión 6.x de PIX y anteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 12.0.7.T del software del IOS de Cisco (hasta la versión 12.2(13)T del software del IOS de Cisco, pero sin incluirla)

  Para ver las versiones más recientes, consulte IPSec NAT Transparency.

- Cisco 2621 router
- Router Cisco 3660
- Cisco PIX 500 Series Security Appliance que ejecuta 7.x y superior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Productos Relacionados

Este documento también se puede utilizar con Cisco 5500 Series Adaptive Security Appliance (ASA), con la versión de software 7.x o posteriores.

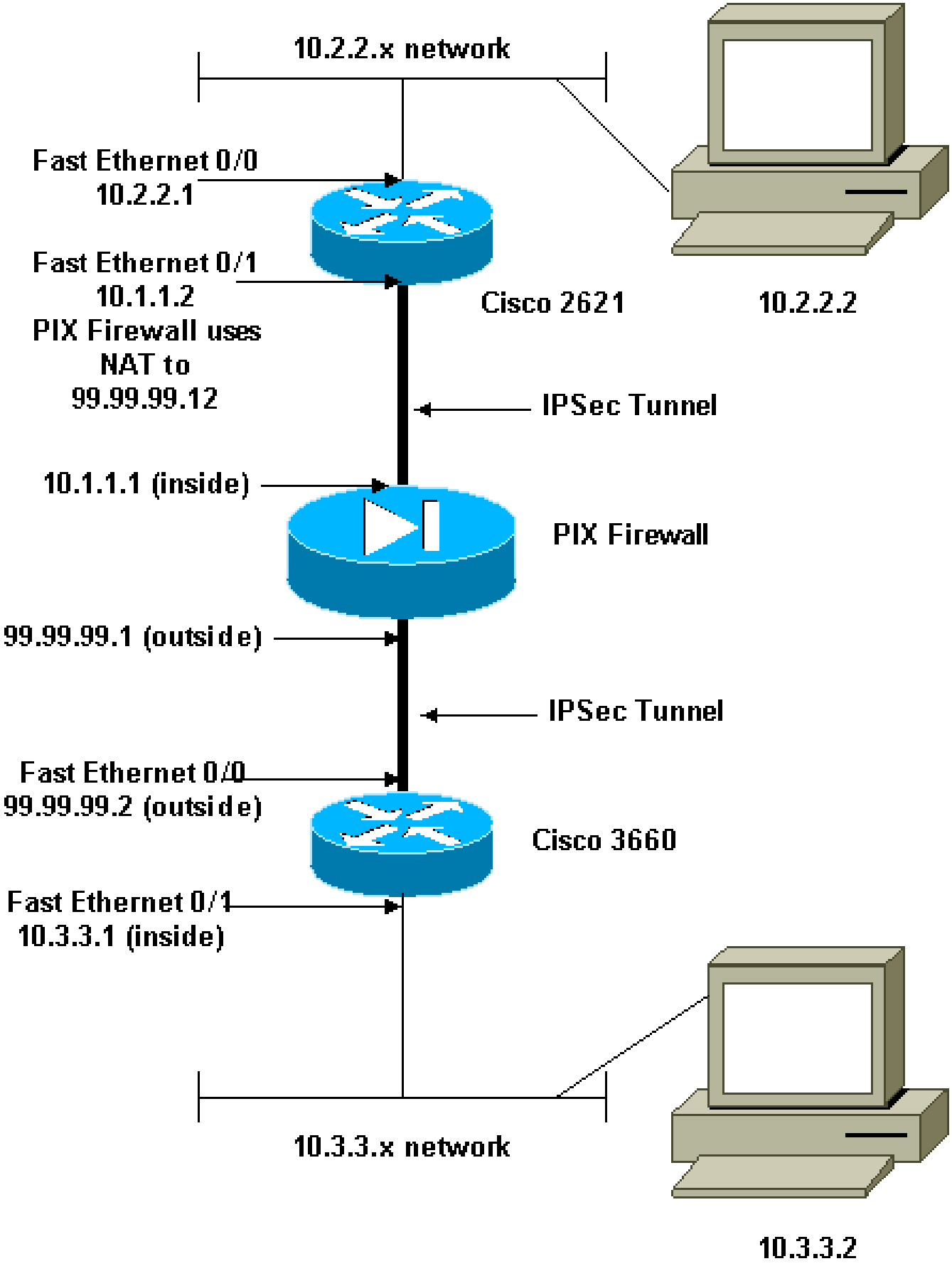
Configurar

En esta sección se presenta la información que puede utilizar para configurar las funciones que describe este documento.

Nota: Para encontrar información adicional sobre los comandos que este documento utiliza, utilice la Command Lookup Tool (sólo para clientes registrados) .

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de Cisco 2621
- Configuración del 3660 de Cisco
- Configuración del Dispositivo de Seguridad PIX y la Lista de Acceso
    - Configuración avanzada de la GUI del administrador de dispositivos de seguridad (ASDM)
    - Configuración de la interfaz de línea de comandos (CLI)
- Configuración de PIX Security Appliance y MPF (Modular Policy Framework)

Cisco 2621

<#root>

```
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

```
<#root>

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
```

Configuración del Dispositivo de Seguridad PIX y la Lista de Acceso

Configuración de ASDM 5.0

Complete estos pasos para configurar la versión 7.0 de Firewall PIX mediante ASDM.

1. Consola en el PIX. A partir de una configuración despejada, utilice los mensajes interactivos para habilitar la GUI del Administrador de dispositivos de seguridad avanzada (ASDM) para la administración del PIX desde la estación de trabajo 10.1.1.3.

Bootstrap de PIX Firewall ASDM

```
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
```

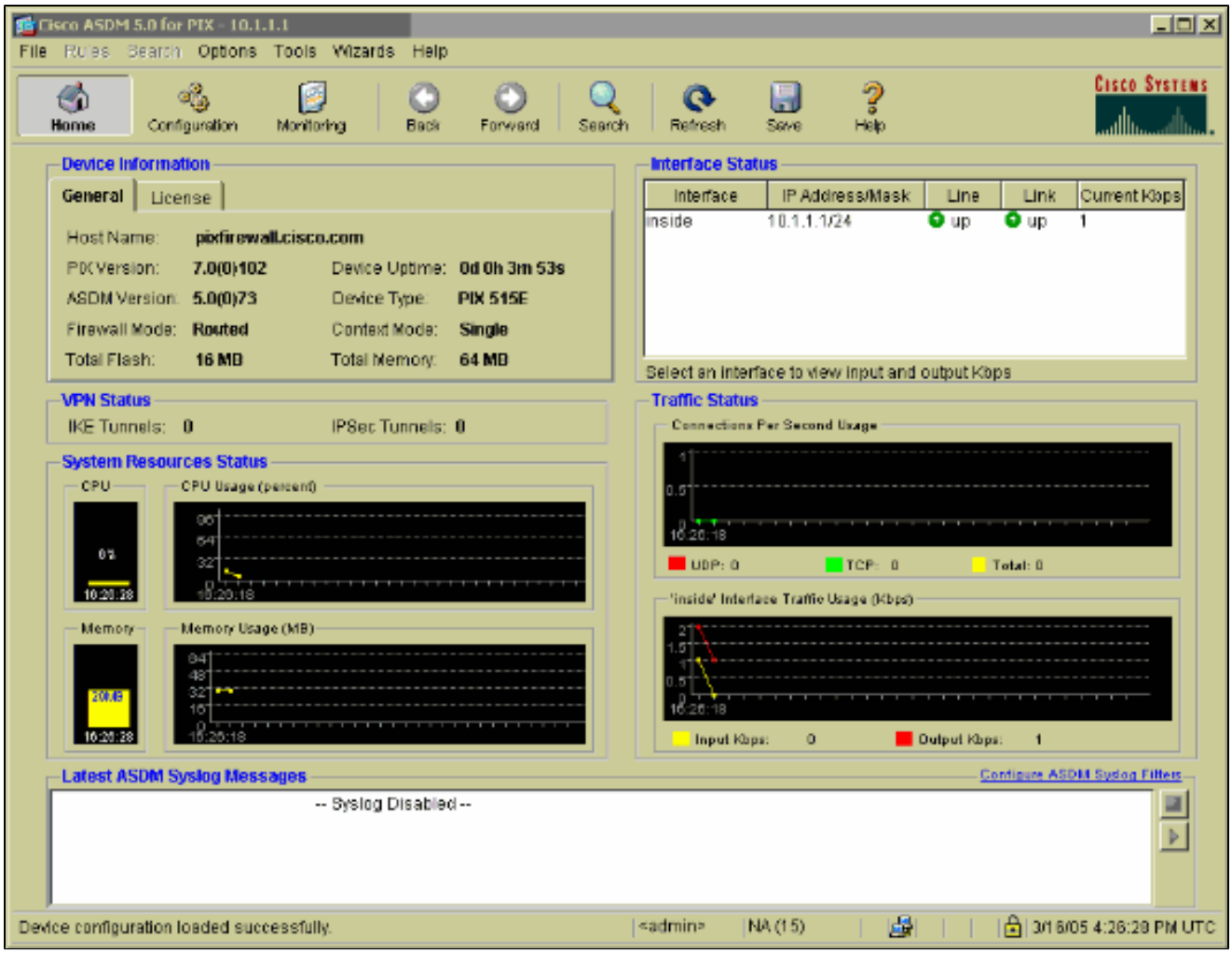
2. Desde Workstation 10.1.1.3, abra un explorador web y utilice ADSM (en este ejemplo, https://10.1.1.1).

3. Elija Yes en los mensajes de certificado e inicie sesión con la contraseña de habilitación según lo configurado en la configuración de Bootstrap de ASDM de Firewall PIX.

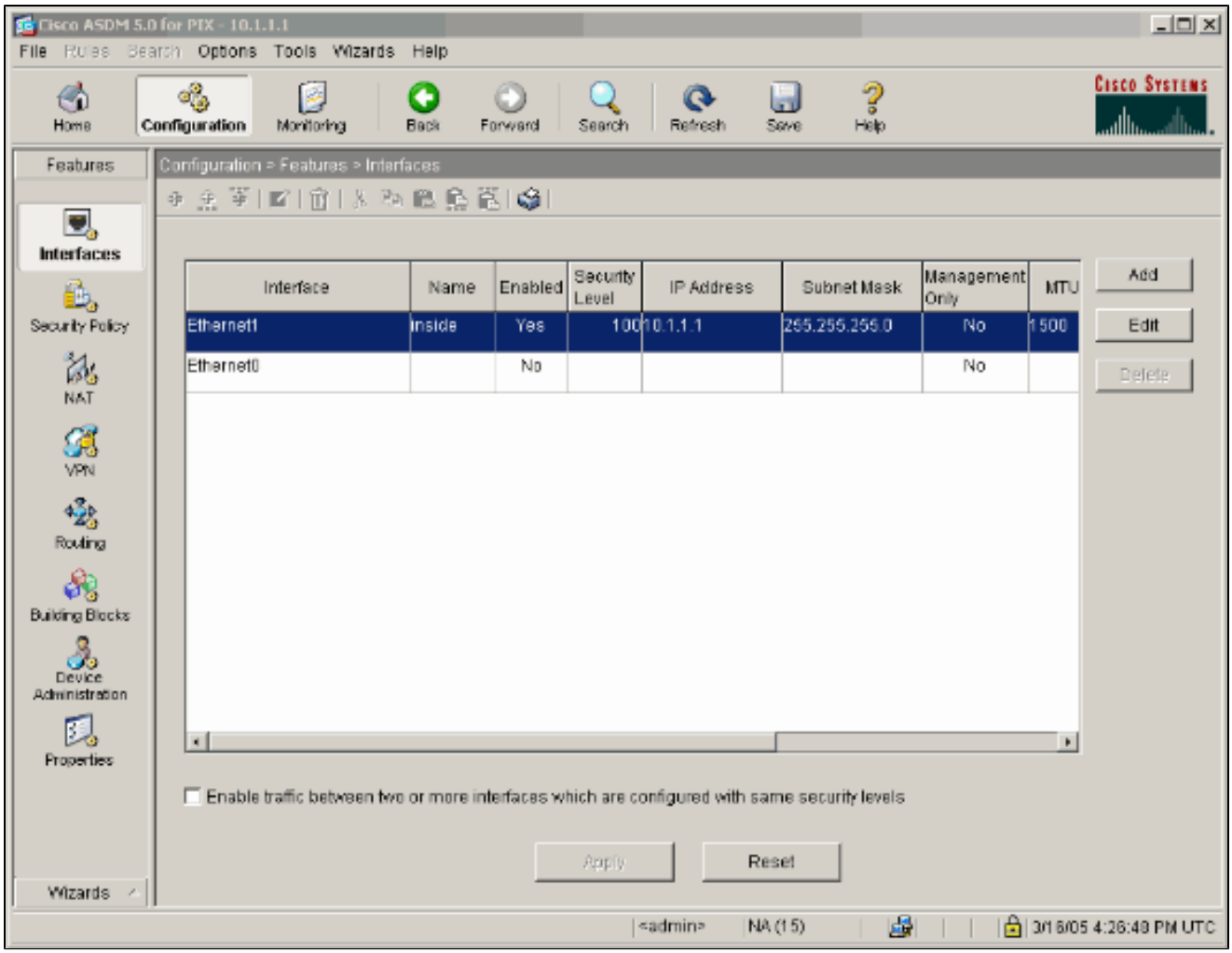
4. Si esta es la primera vez que se ejecuta ASDM en el PC, le preguntará si desea utilizar ASDM Launcher o ASDM como una aplicación Java.

   En este ejemplo, se selecciona el punto de ejecución de ASDM e instala estos mensajes.

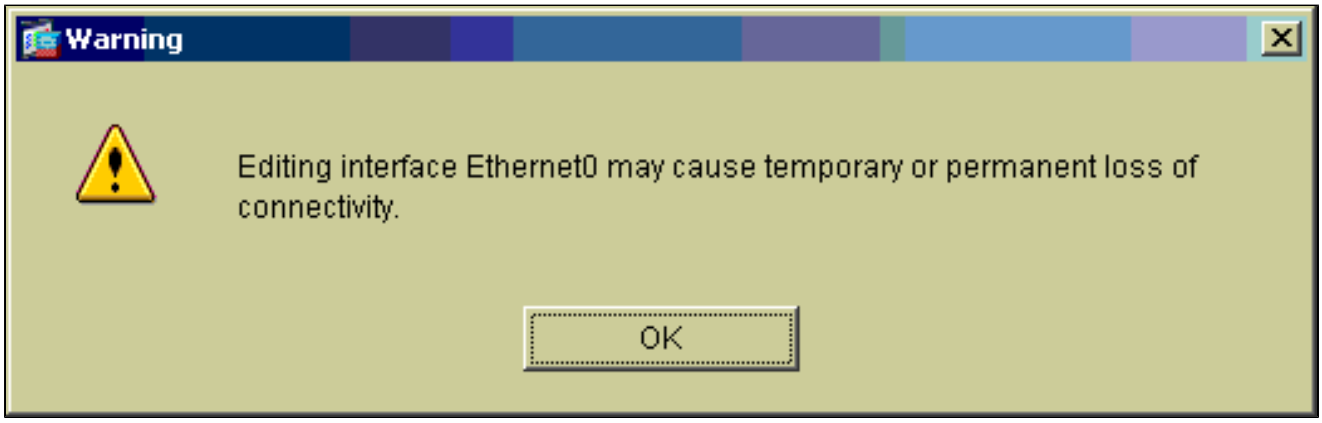
5. Vaya a la ventana de inicio de ASDM y seleccione la ficha Configuration.



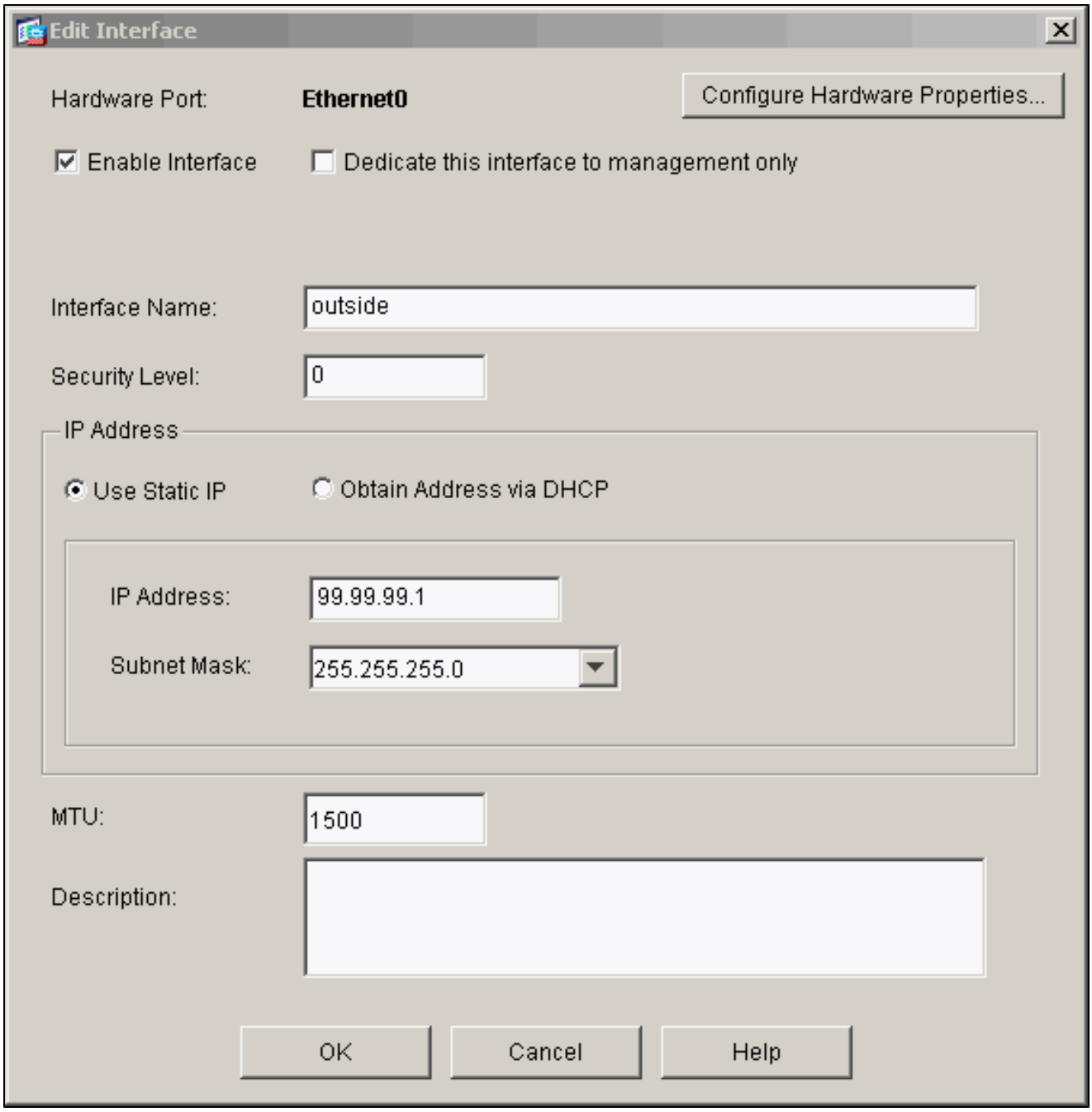
6. Resalte la Interfaz Ethernet 0 y haga clic en Editar para configurar la Interfaz Externa.



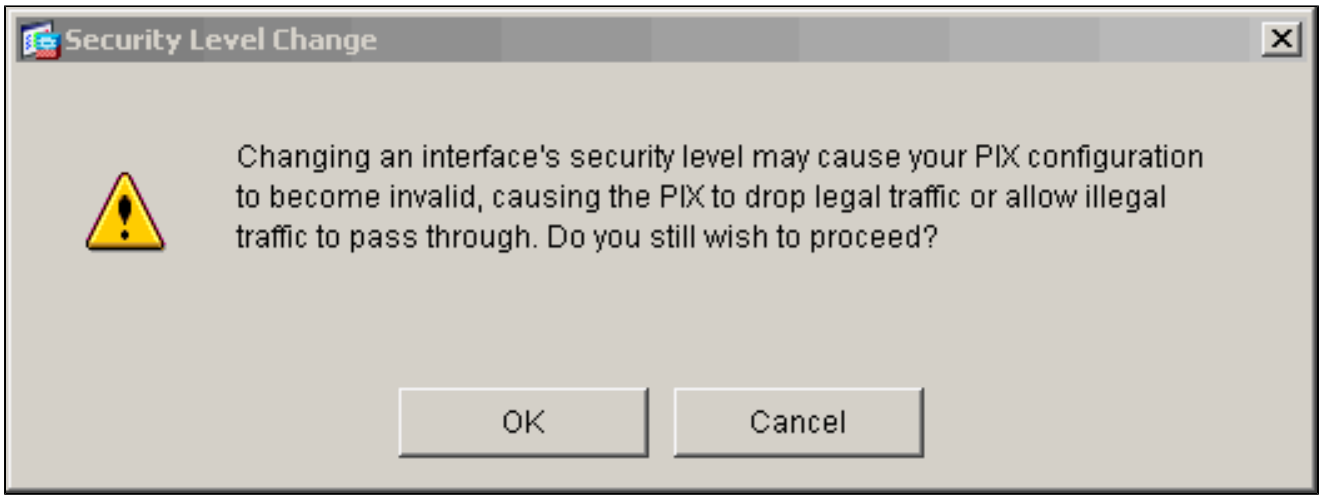
7. Haga clic en Aceptar en el indicador de la interfaz de edición.



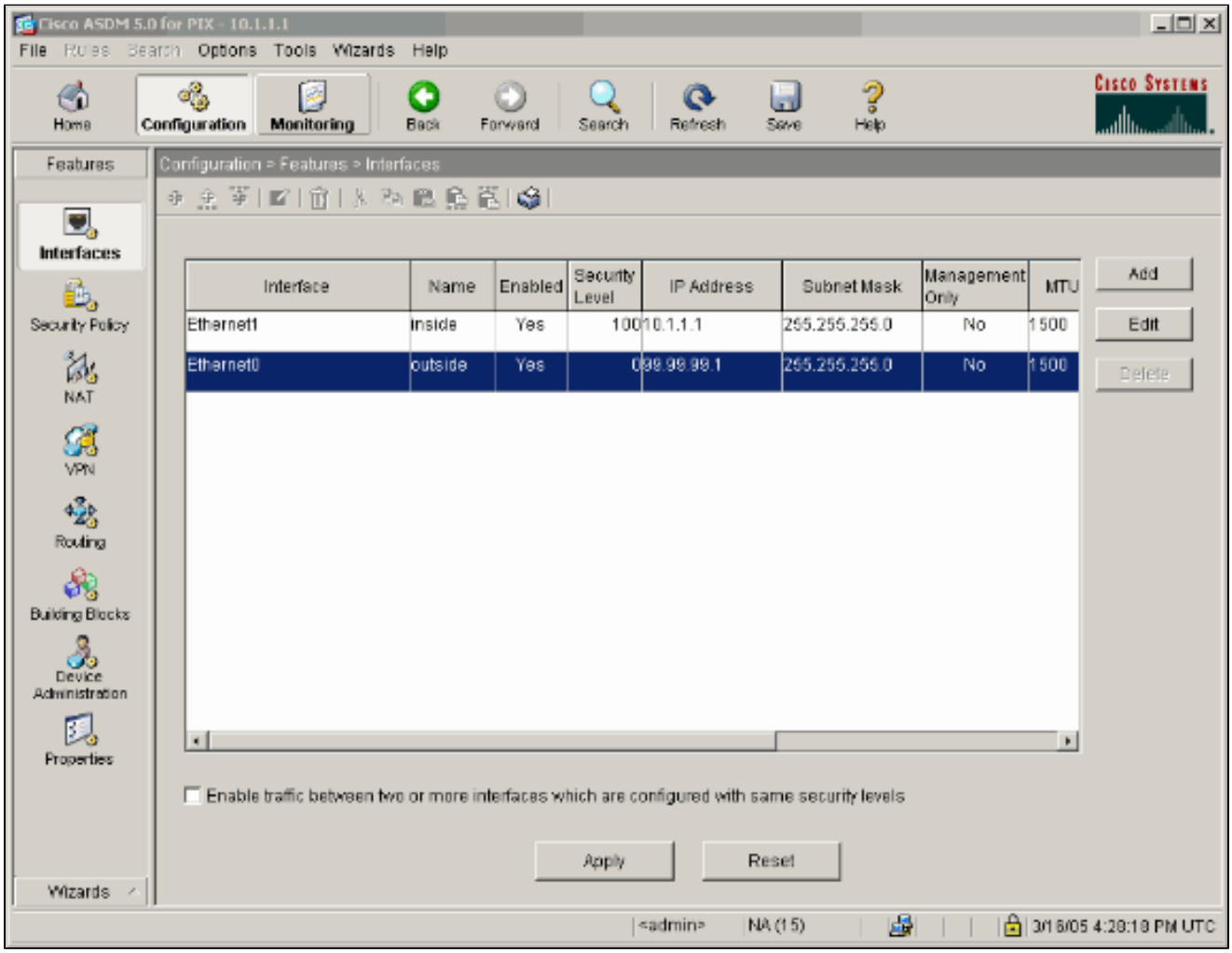
8. Ingrese los detalles de la interfaz y haga clic en Aceptar cuando haya terminado.



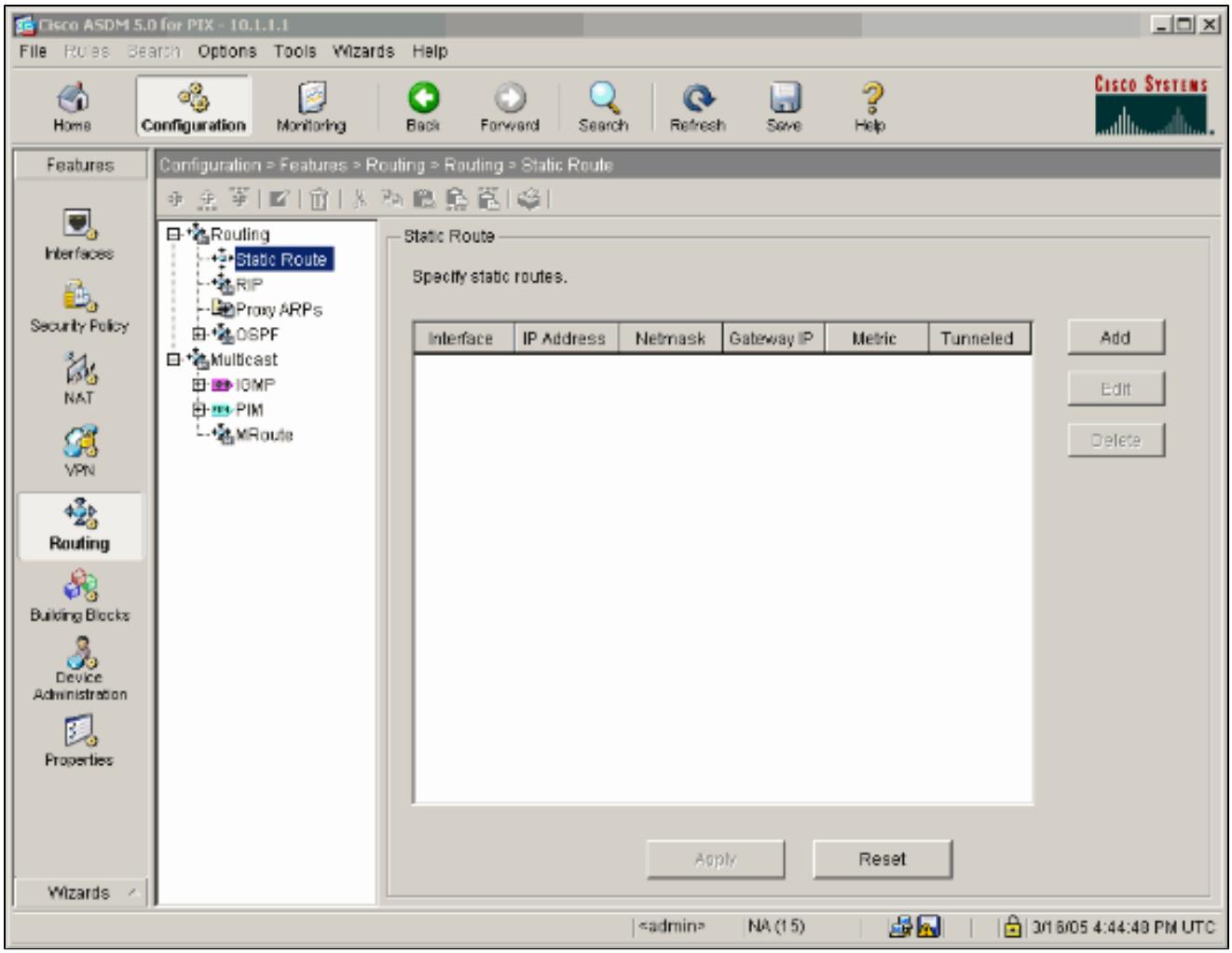
9. Haga clic en Aceptar en el prompt Cambio de una Interfaz.



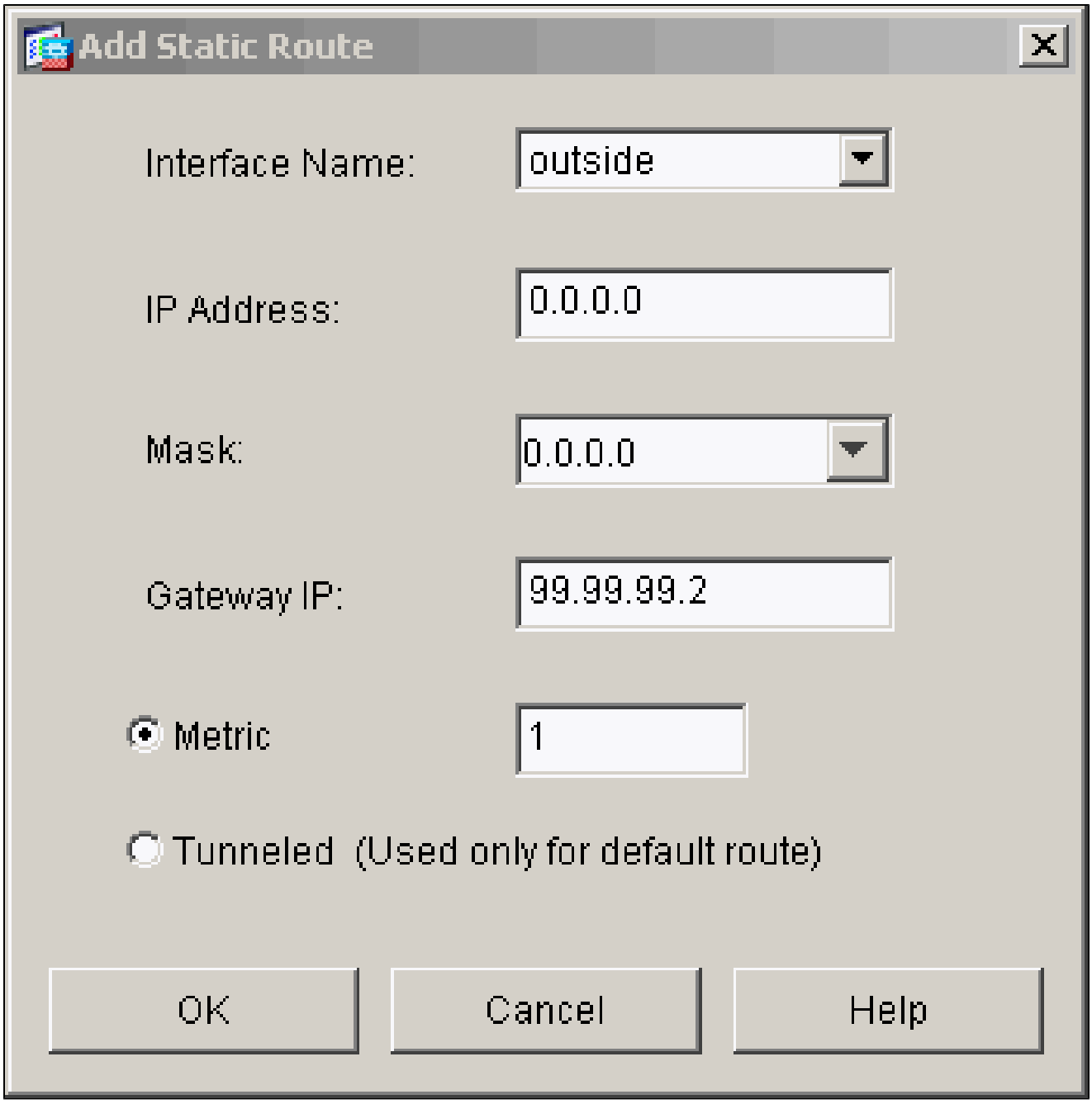
10. Haga clic en Apply para aceptar la configuración de la interfaz. La configuración también se envía al PIX. Este ejemplo utiliza rutas estáticas.



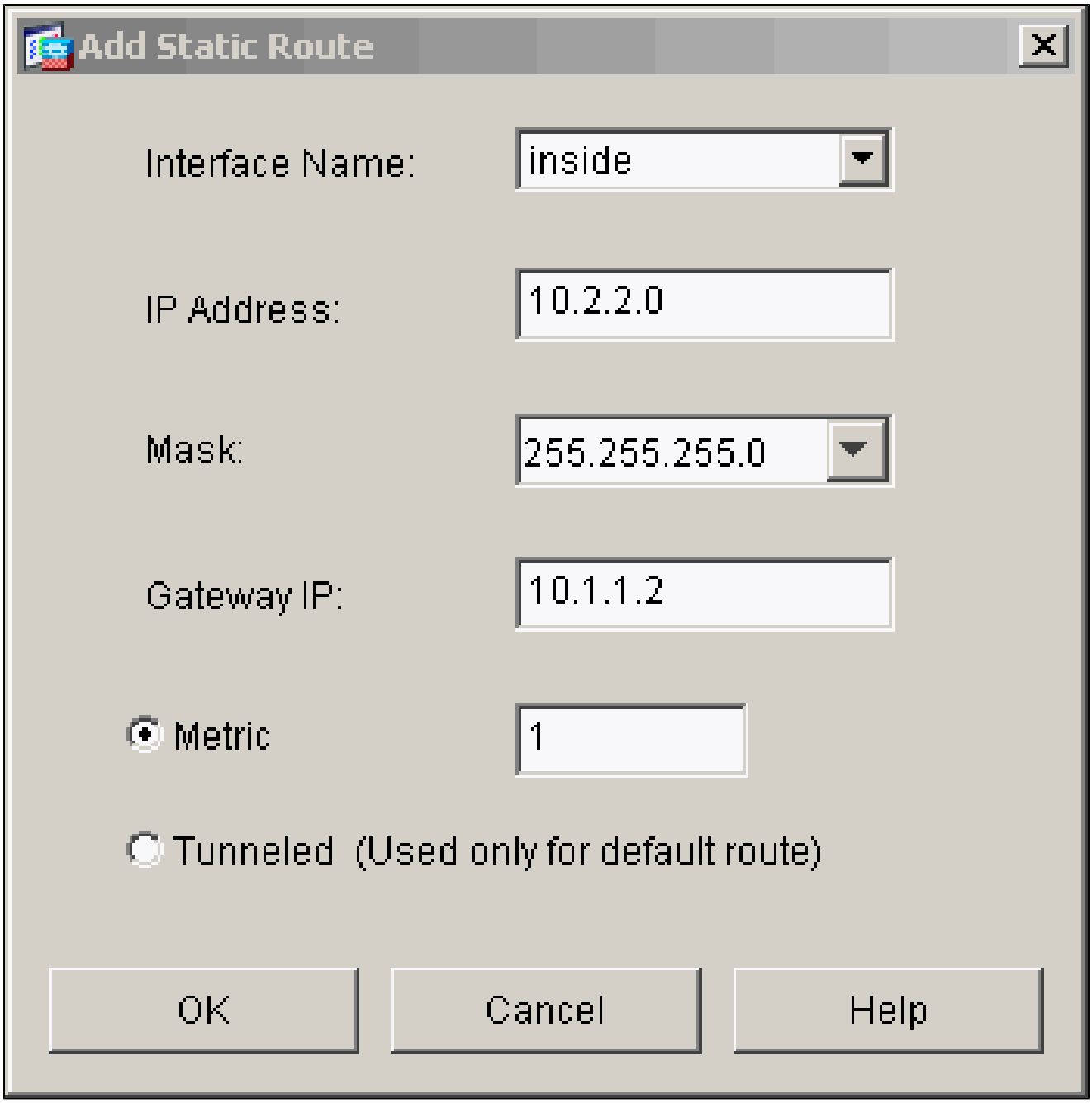
11. Haga clic en Routing en la pestaña Features , resalte Static Route y haga clic en Add.



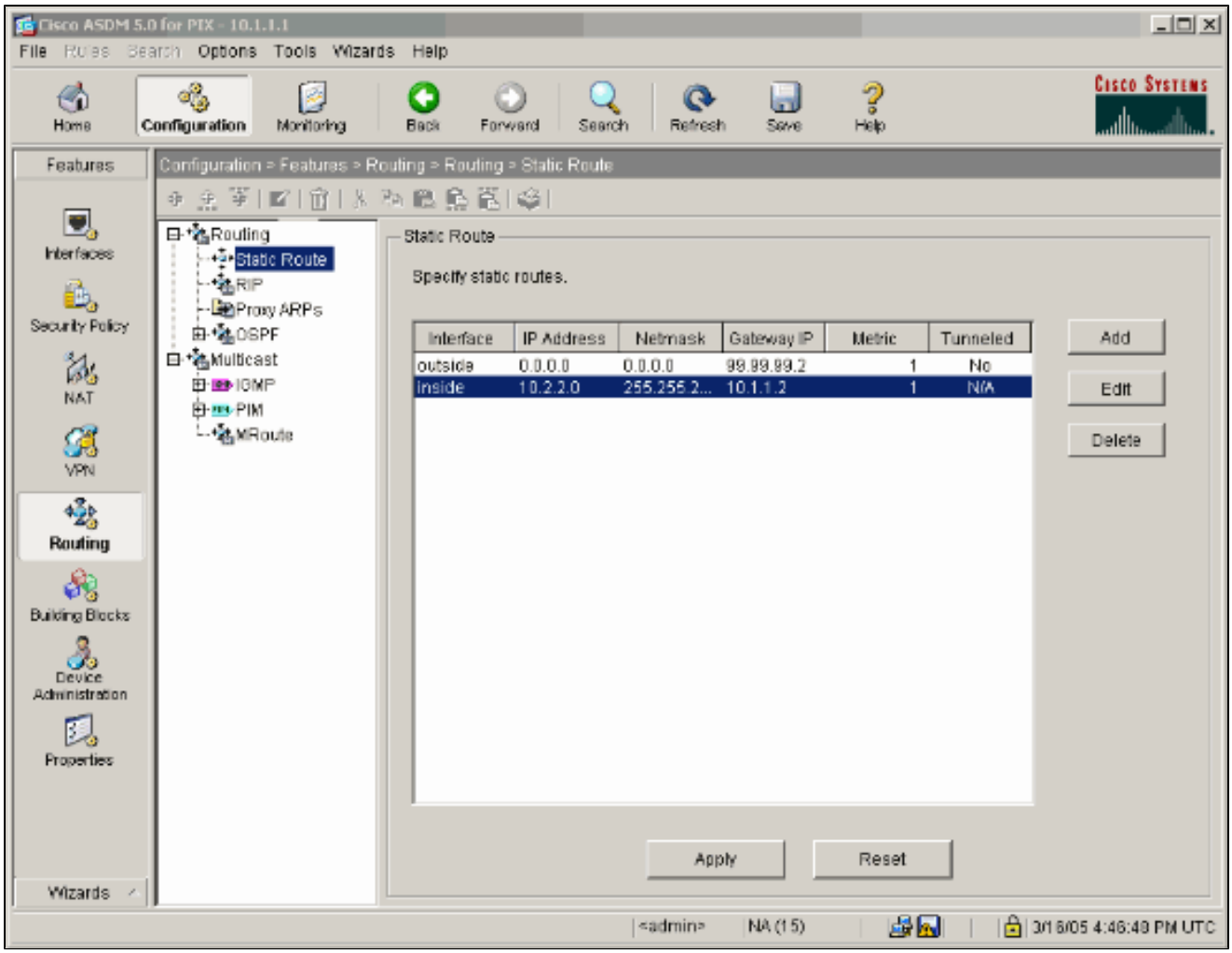
12. Configure la puerta de enlace predeterminada y haga clic en Aceptar.



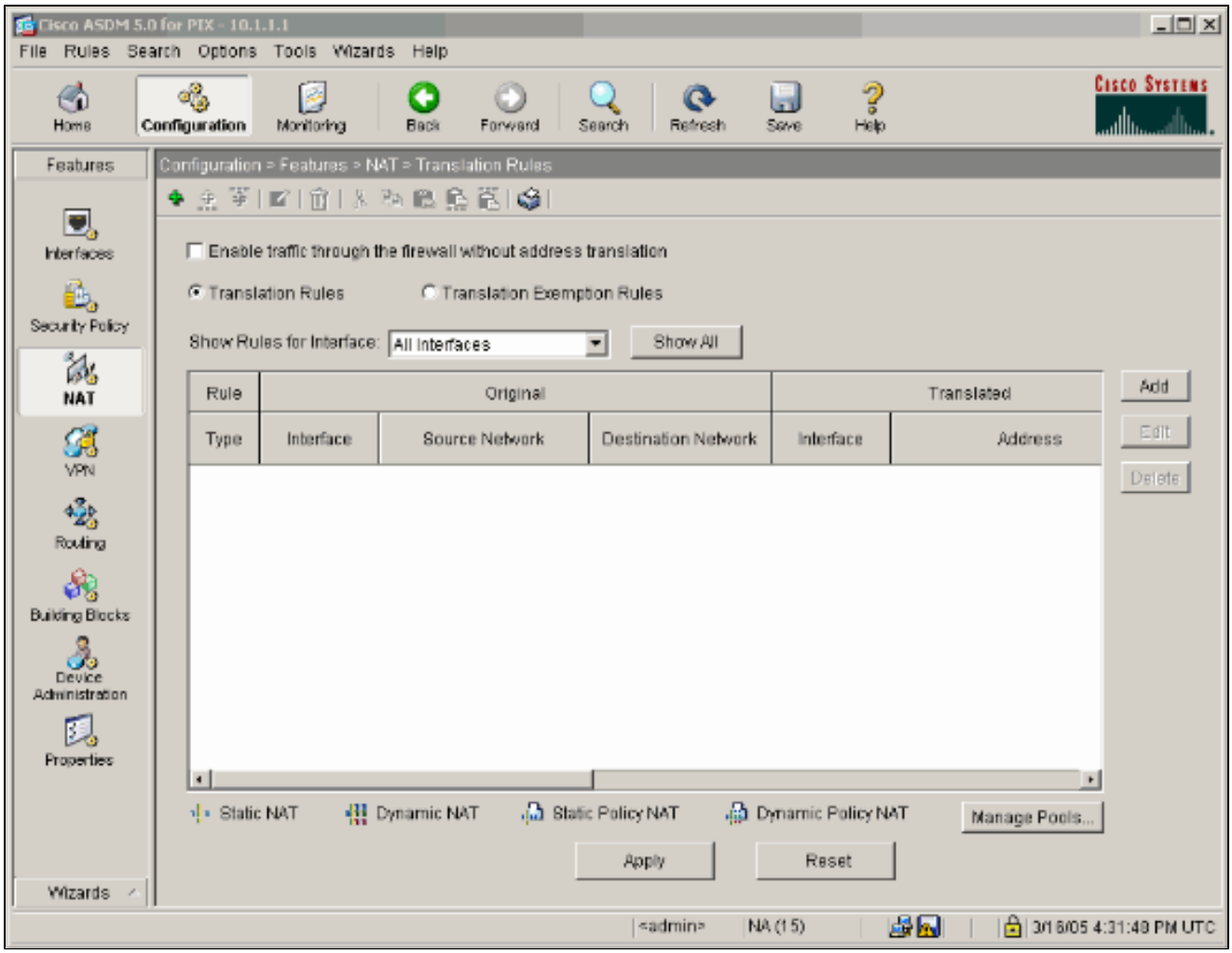
13. Haga clic en Agregar y agregue las rutas a las redes internas.



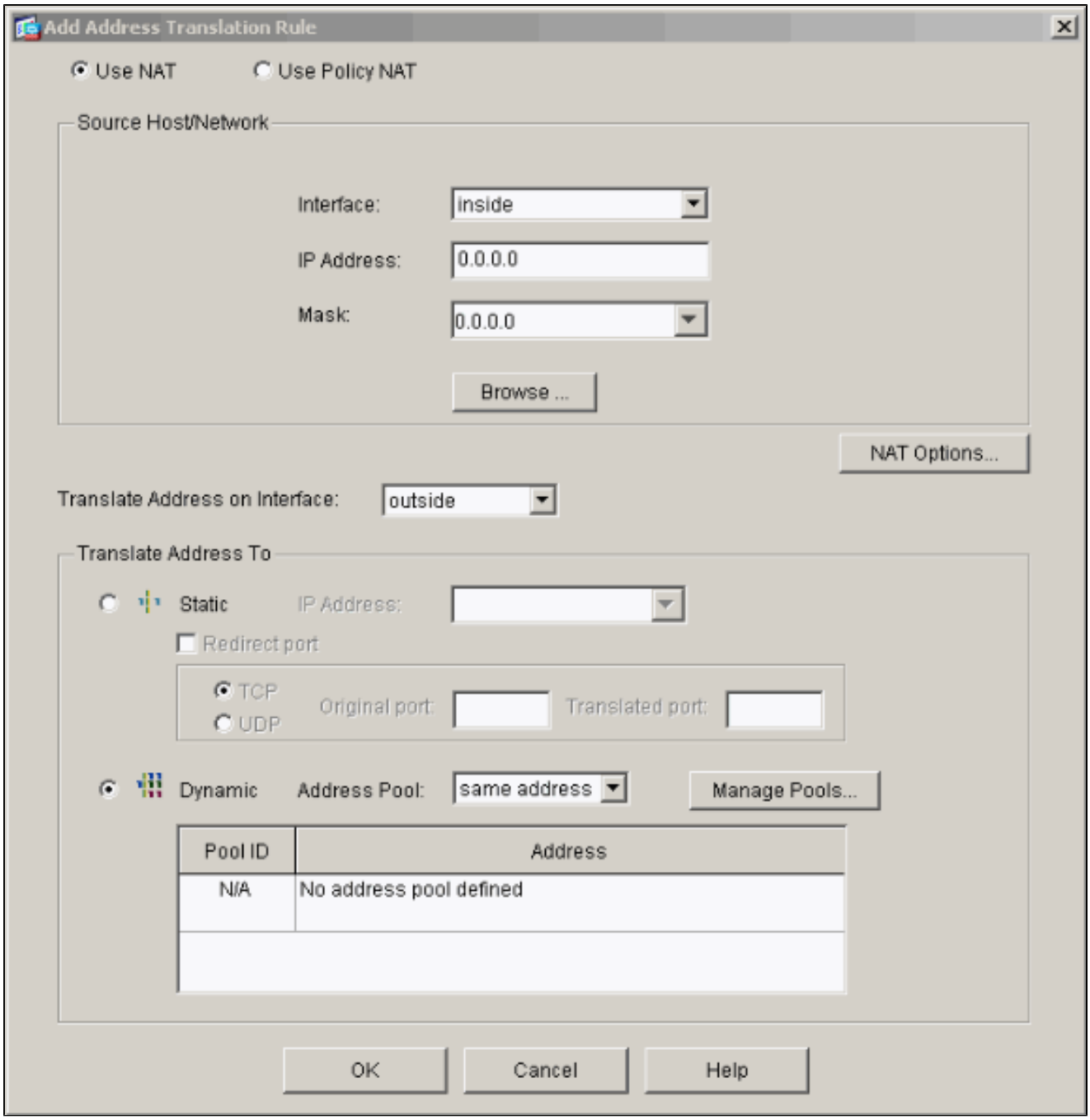
14. Confirme que las rutas correctas estén configuradas y haga clic en Apply.



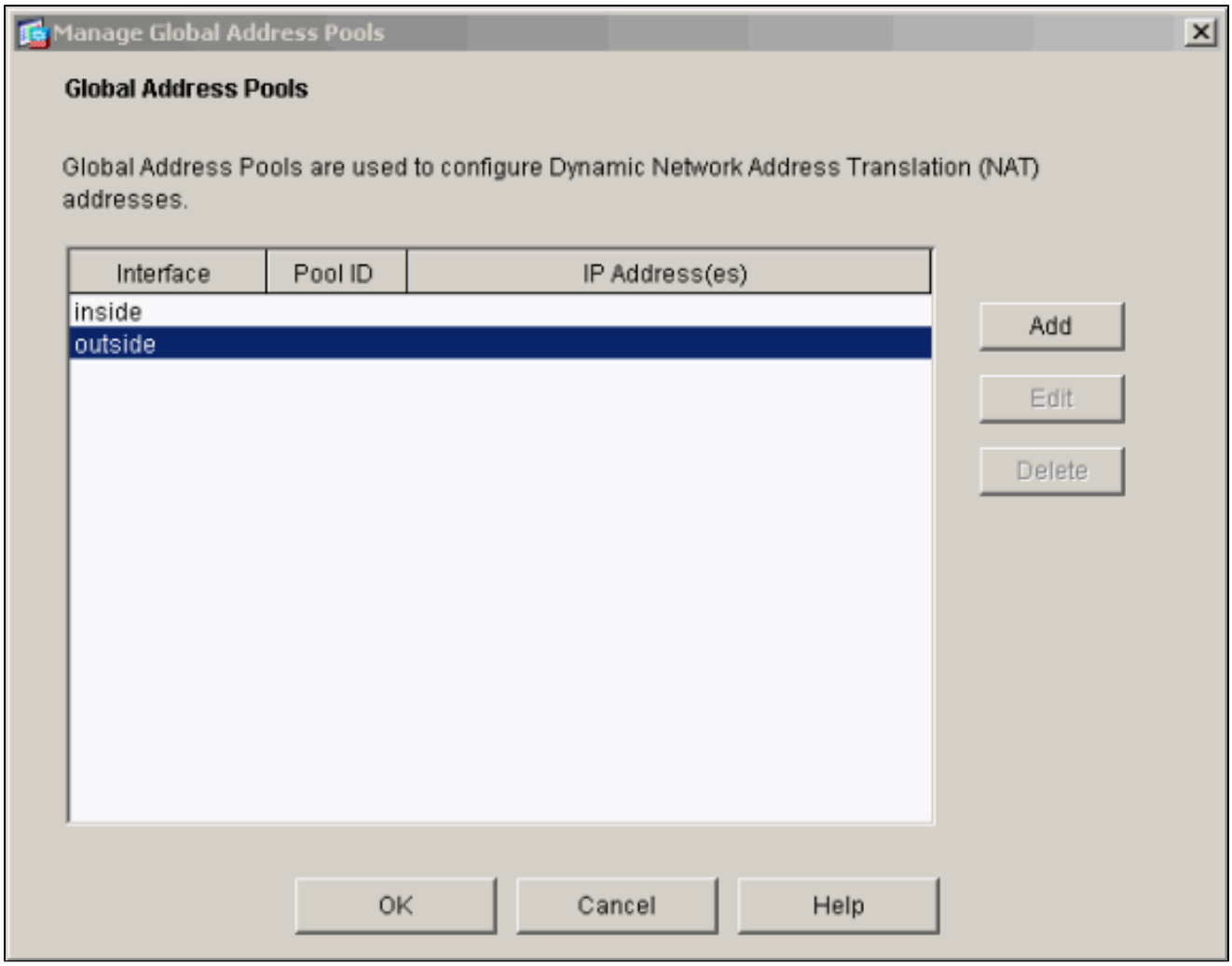
15. En este ejemplo, se utiliza NAT. Quite la marca en la casilla Enable traffic through the firewall without address translation y haga clic en Add para configurar la regla NAT.



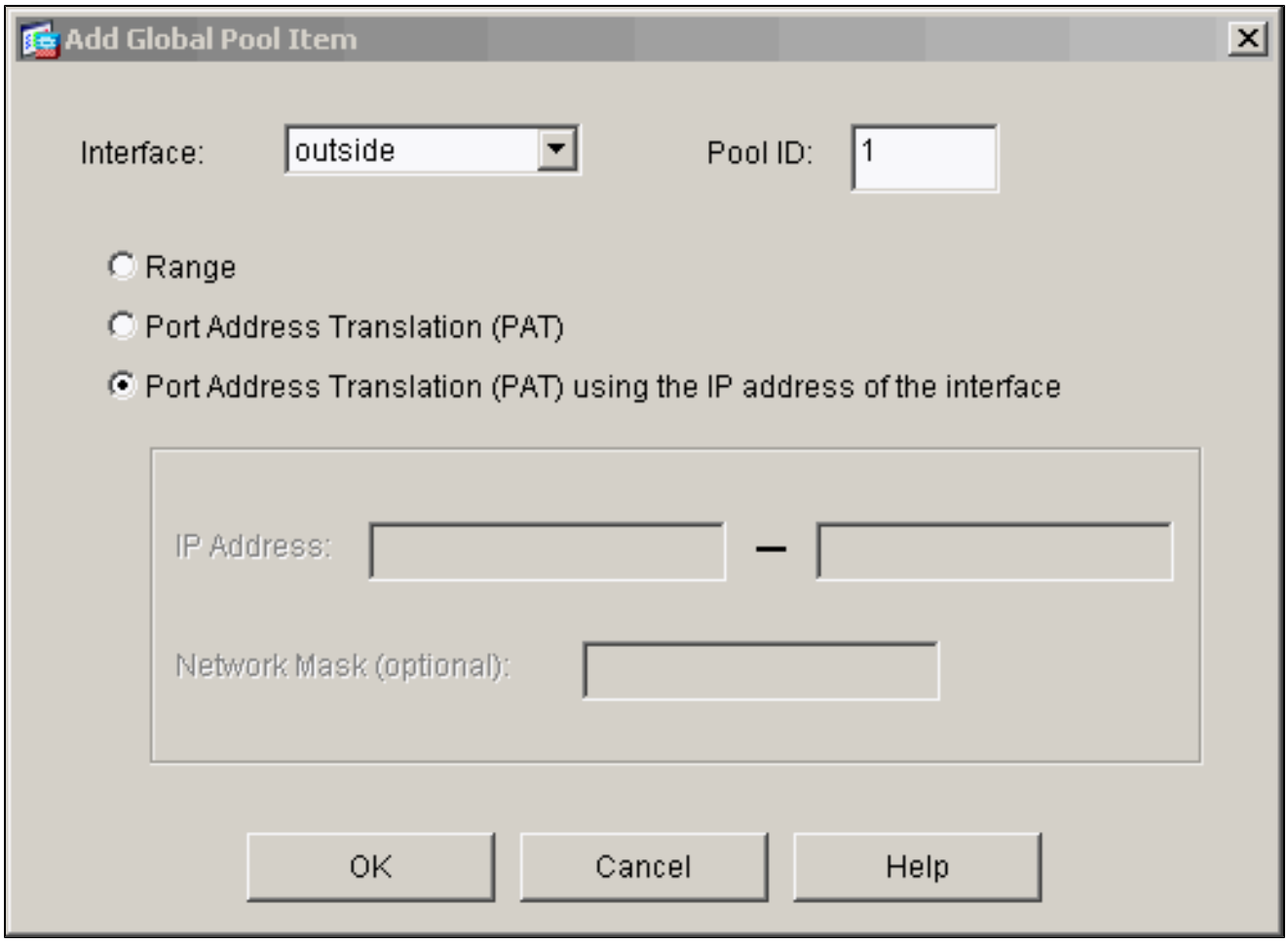
16. Configure la red de origen (en este ejemplo se utiliza any). Luego haga clic en Administrar Pools para definir el PAT.



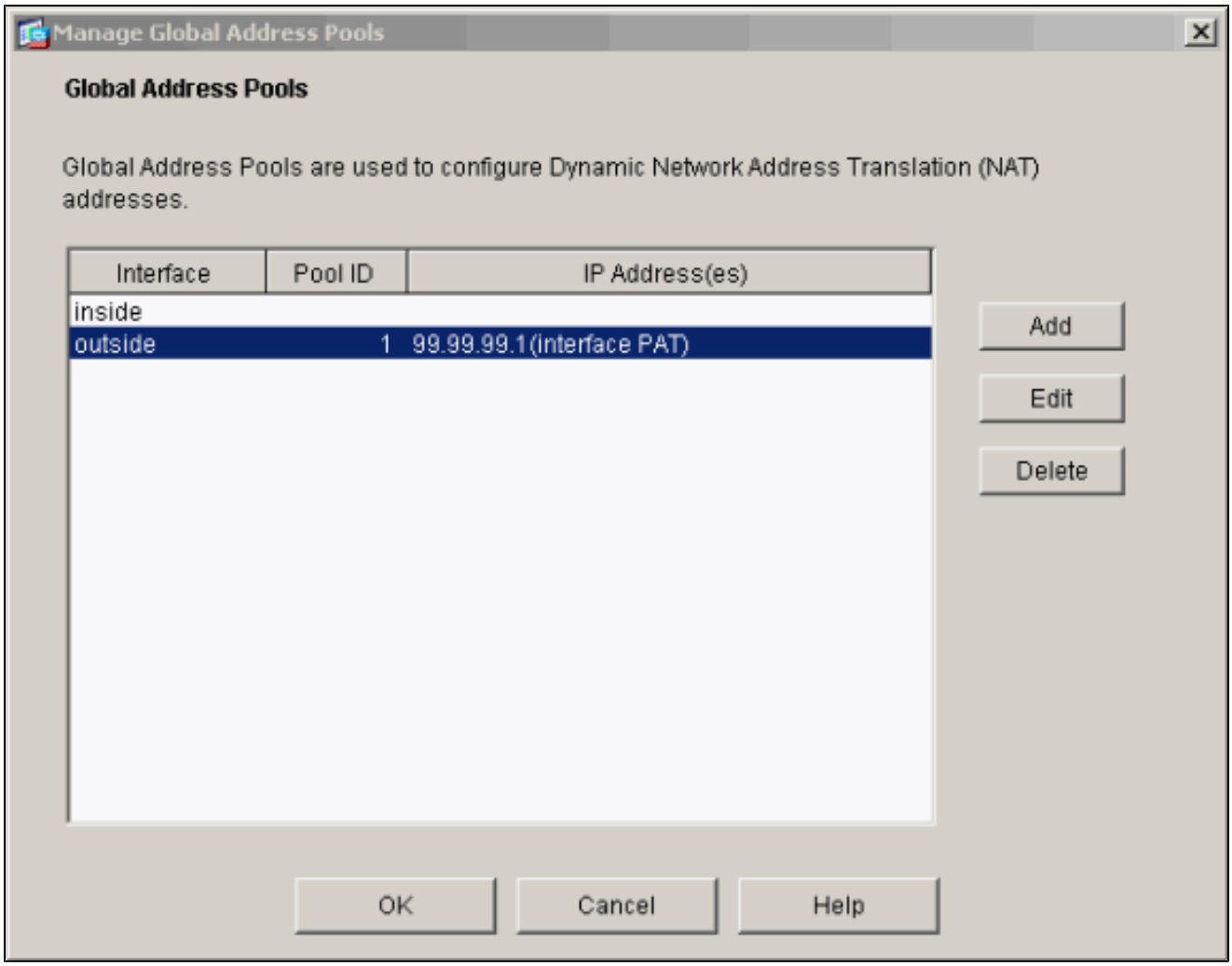
17. Seleccione la interfaz externa y haga clic en Agregar.



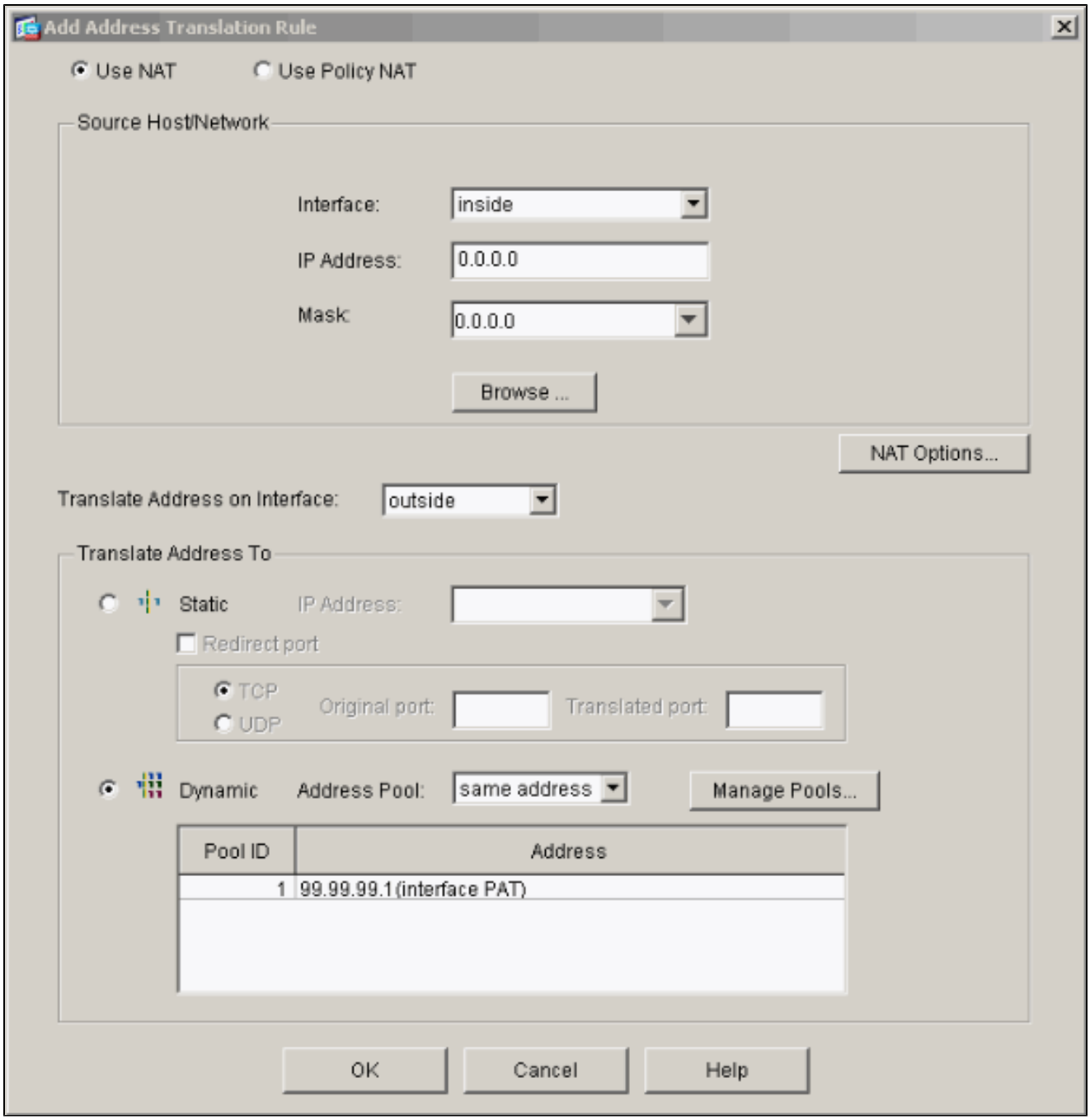
Este ejemplo utiliza una PAT que utiliza la dirección IP de la interfaz.



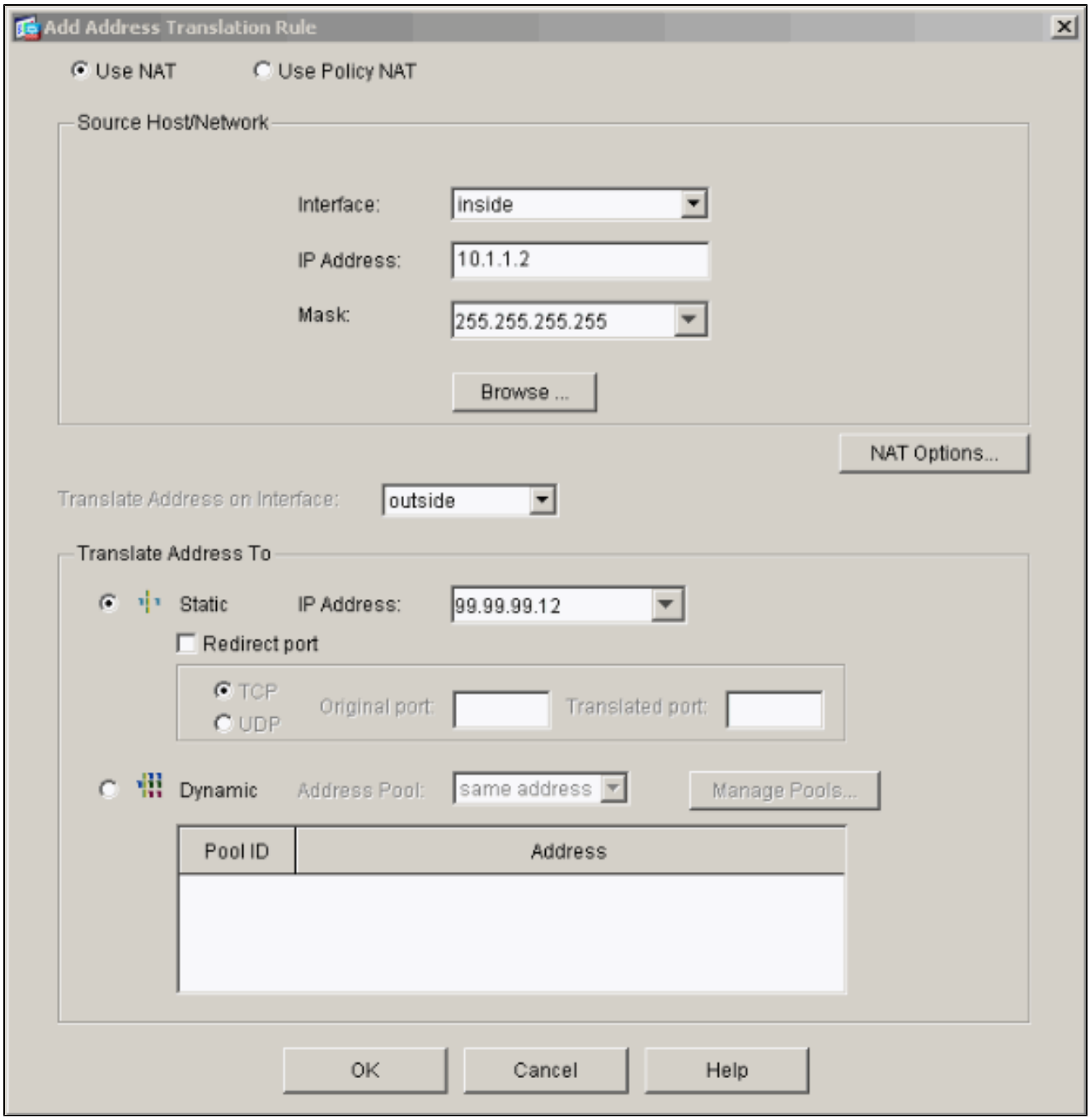
18. Haga clic en Aceptar cuando la PAT esté configurada.



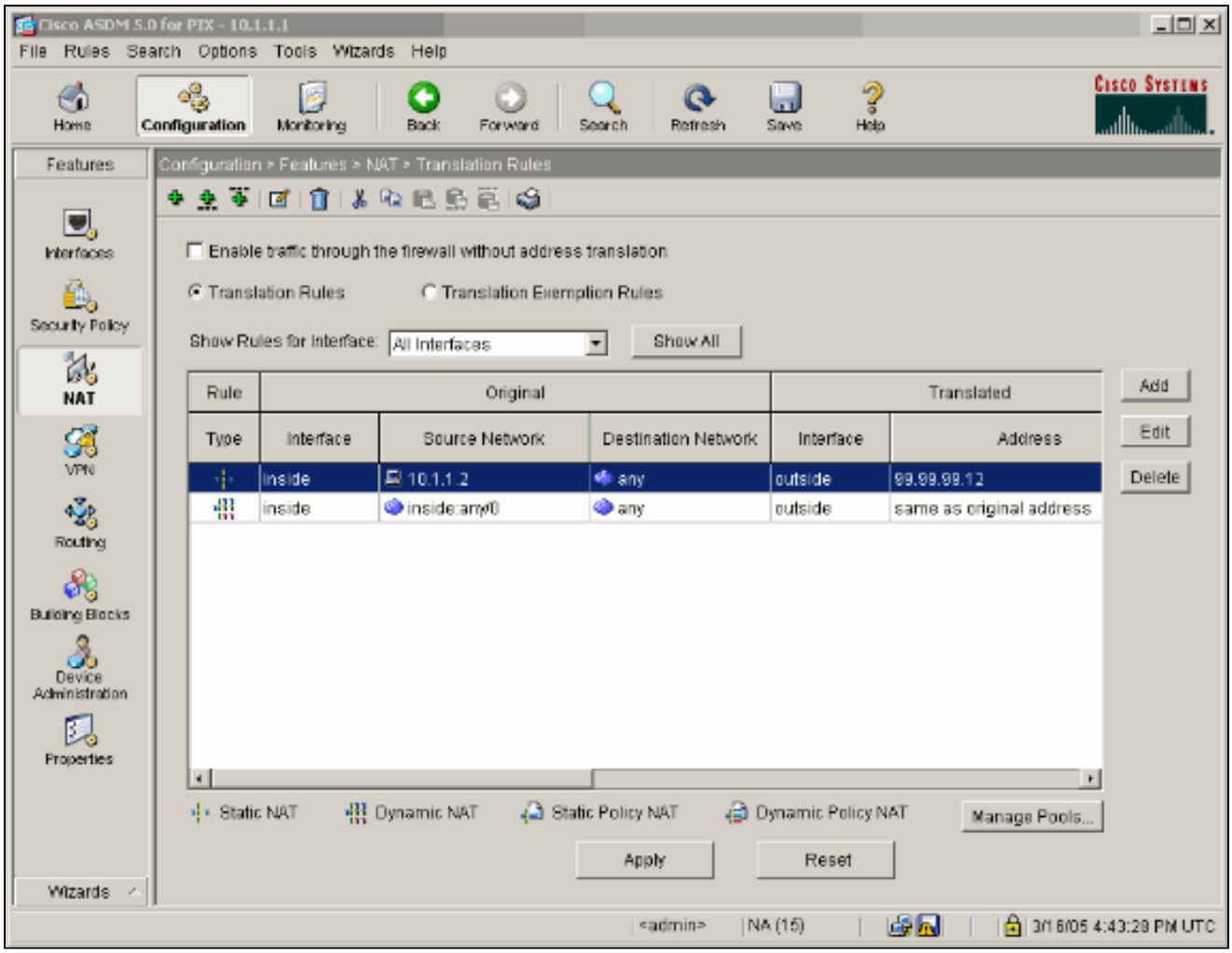
19. Haga clic en Agregar para configurar la traducción estática.



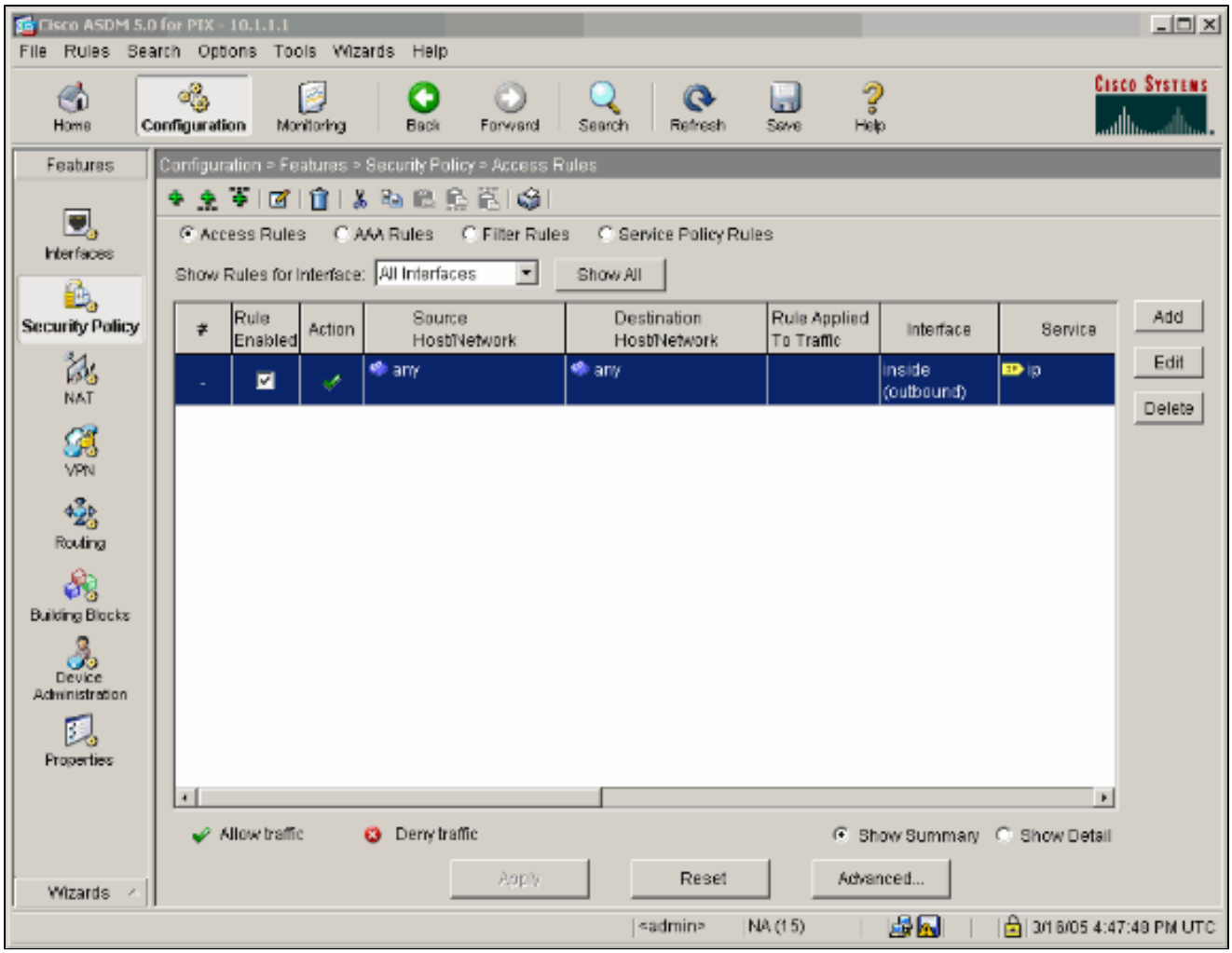
20. Seleccione inside en el menú desplegable Interface (Interfaz) y, a continuación, introduzca IP address 10.1.1.2, subnet mask 255.255.255.255, choose Static (Dirección IP) y, en el campo IP Address (Dirección IP), escriba outside address (Dirección externa) 99.99.99.12. Haga clic en Aceptar cuando haya terminado.



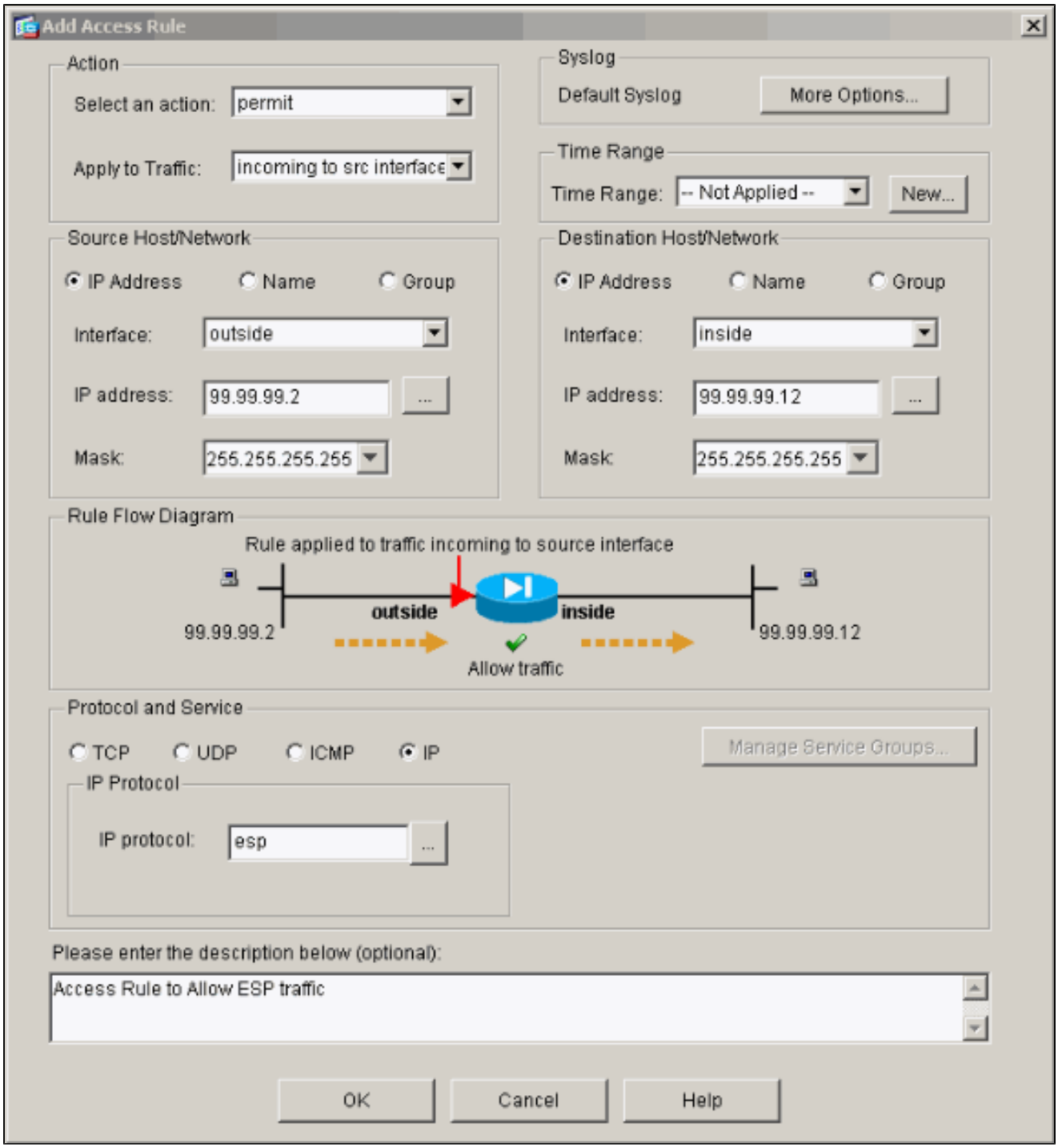
21. Haga clic en Apply para aceptar la configuración de la interfaz. La configuración también se envía al PIX.



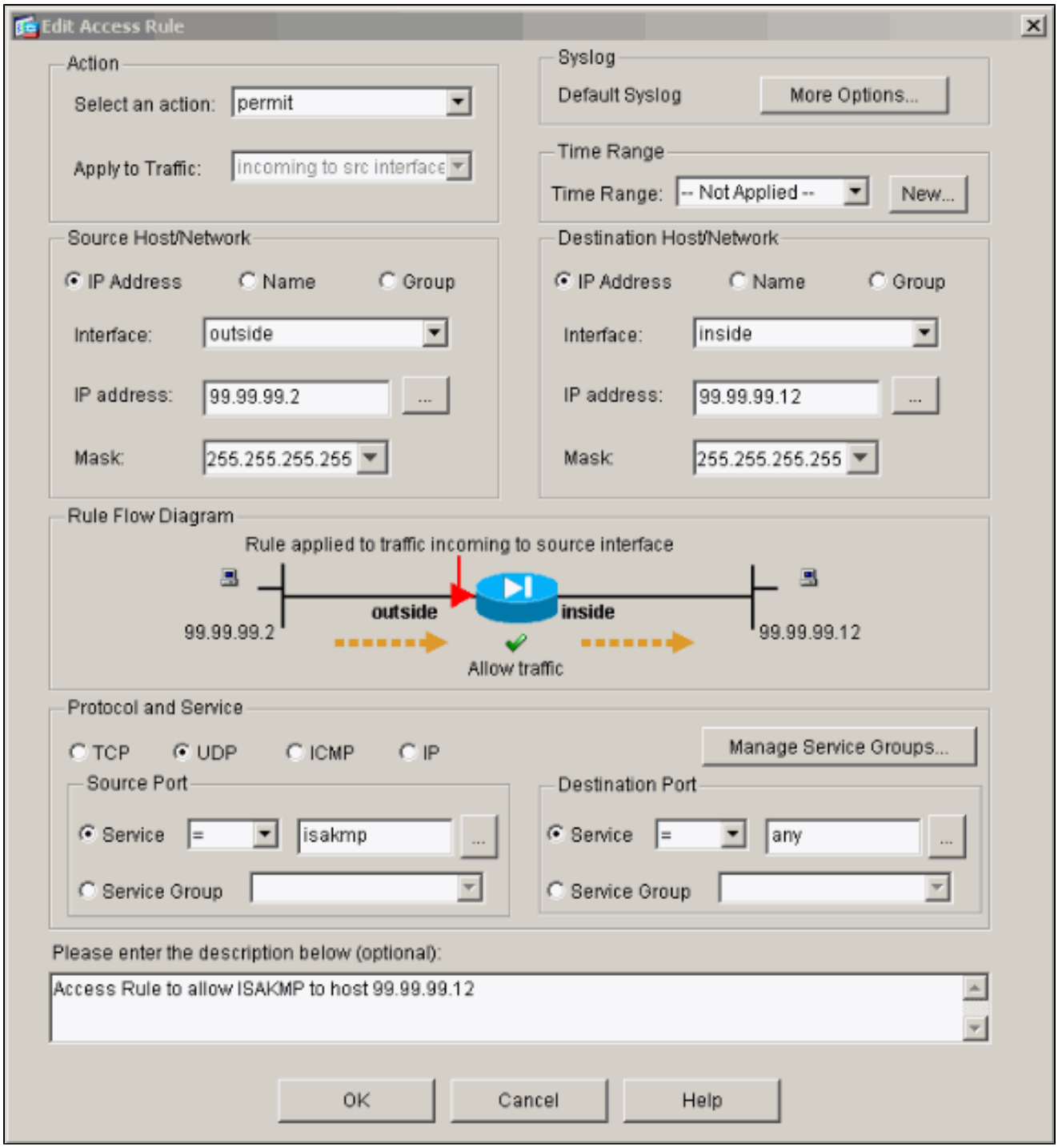
22. Seleccione Política de seguridad en la pestaña Funciones para configurar la regla de Política de seguridad.



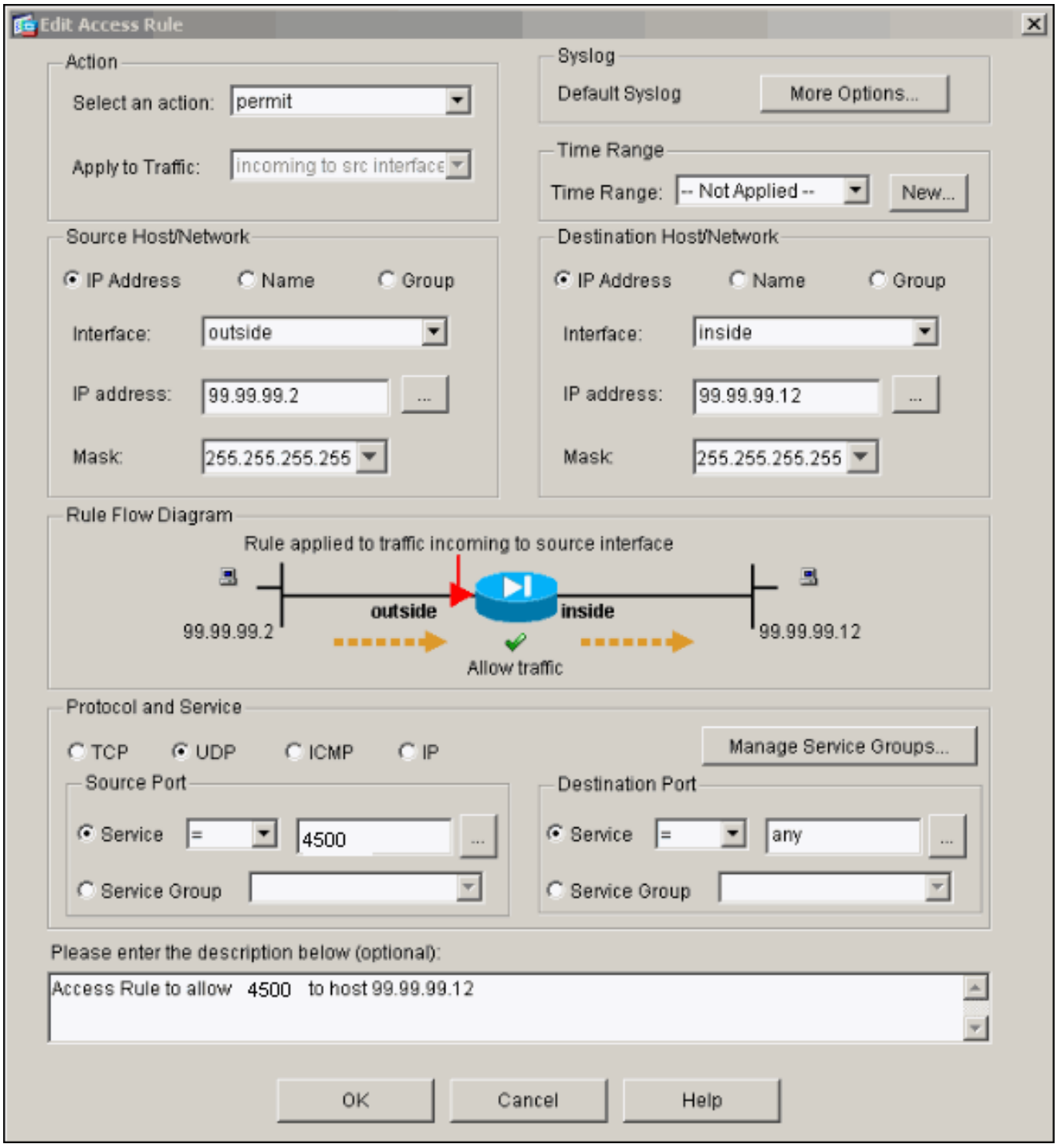
23. Haga clic en Agregar para permitir el tráfico esp y haga clic en Aceptar para continuar.



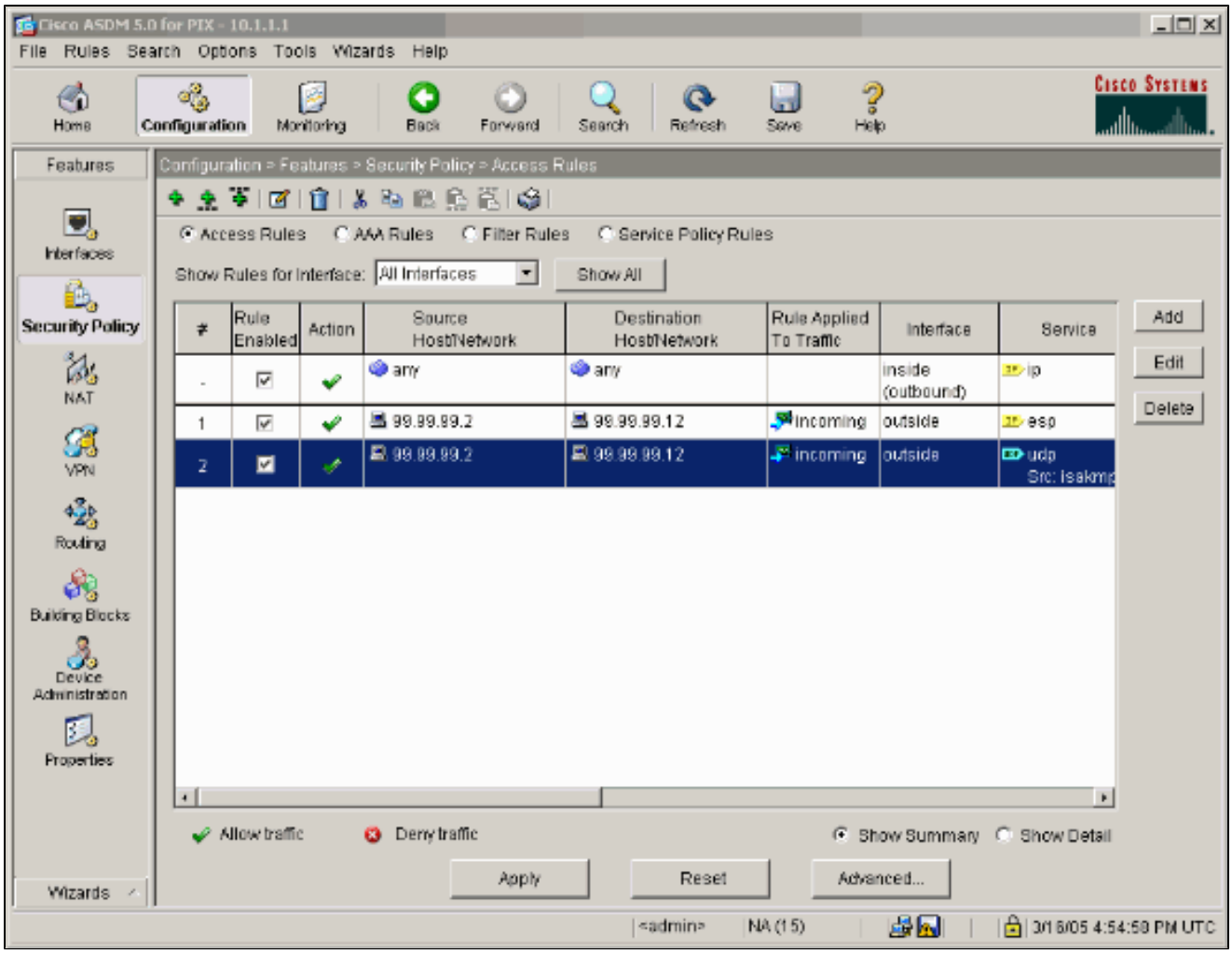
24. Haga clic en Agregar para permitir el tráfico ISAKMP y haga clic en Aceptar para continuar.



25. Haga clic en Add para permitir el tráfico del puerto UDP 4500 para NAT-T y haga clic en OK para continuar.

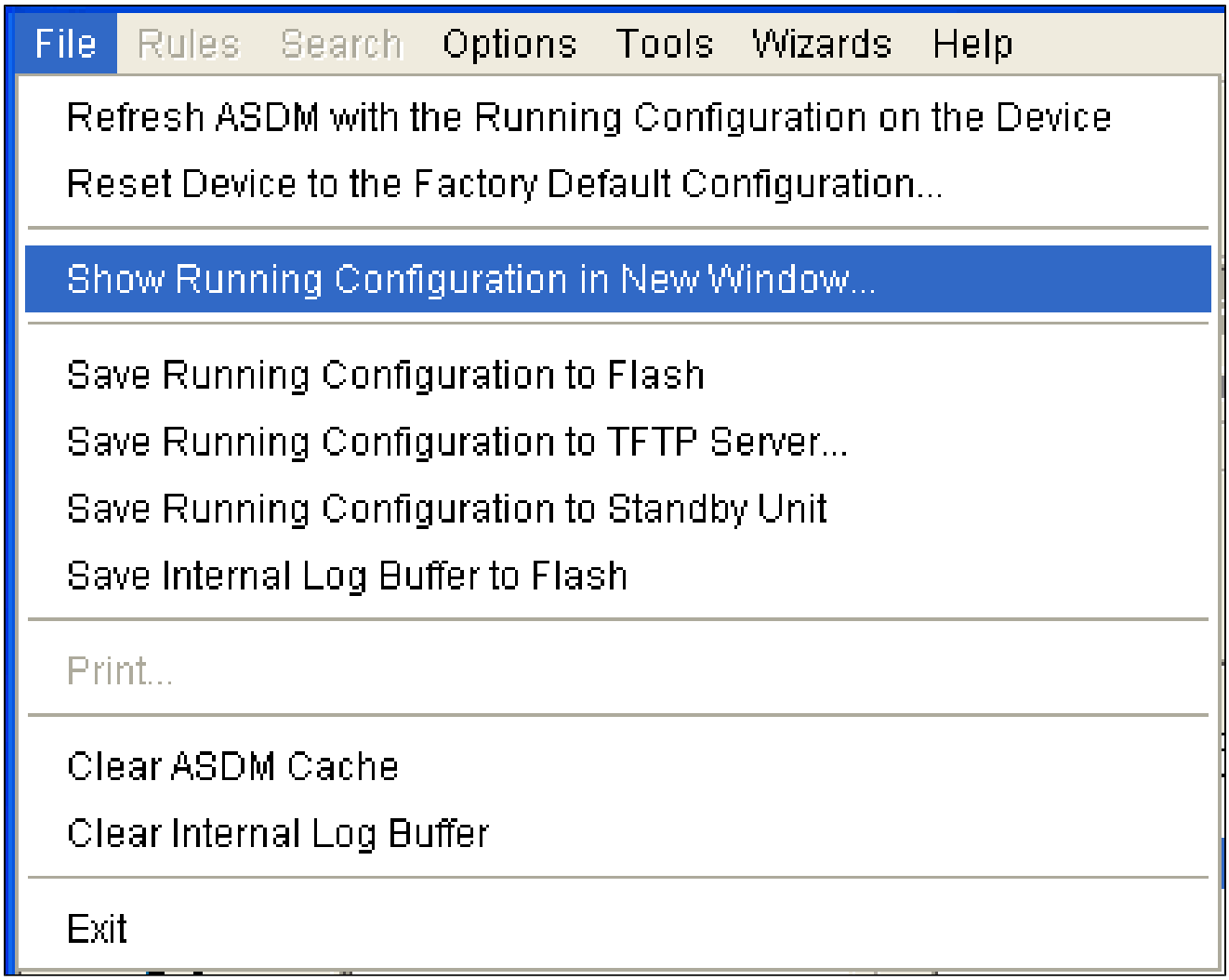


26. Haga clic en Apply para aceptar la configuración de la interfaz. La configuración también se envía al PIX.



27. La configuración ha finalizado.

    Elija File > Show Running Configuration in New Window para ver la configuración de CLI.



Configuración de Firewall de PIX

Firewall PIX

```
<#root>

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
```

Configuración de PIX Security Appliance y MPF (Modular Policy Framework)

En lugar de la lista de acceso, utilice el comando inspect ipsec-pass-thru en MPF(Modular Policy Framework) para pasar el tráfico IPsec a través de los dispositivos de seguridad PIX/ASA.

Esta inspección está configurada para abrir agujeros de conexión para el tráfico ESP. Se permiten todos los flujos de datos ESP cuando existe un flujo de reenvío y no hay límite en el número máximo de conexiones que se pueden permitir. AH no está permitido. El tiempo de espera inactivo predeterminado para flujos de datos ESP está establecido de forma predeterminada en 10 minutos. Esta inspección se puede aplicar en todas las ubicaciones en las que se pueden aplicar otras inspecciones, lo que incluye los modos de comando class y match. La inspección de aplicación de paso a través de IPSec proporciona una cómoda travesía del tráfico ESP (protocolo IP 50) asociado a una conexión IKE UDP puerto 500. Evita la larga configuración de la lista de acceso para permitir el tráfico ESP y también proporciona seguridad con tiempo de espera y conexiones máximas. Utilice los comandos class-map, policy-map y service-policy para definir una clase de tráfico, para aplicar el comando inspect a la clase y para aplicar la política a una o más interfaces. Cuando está habilitado, el comando inspect IPSec-pass-thru permite tráfico ESP ilimitado con un tiempo de espera de 10 minutos, que no es configurable. Se permite el tráfico NAT y no NAT.

<#root>

```
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
```

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- show crypto ipsec sa—Muestra las asociaciones de seguridad de fase 2.
- show crypto isakmp sa — Muestra las asociaciones de seguridad de la fase 1.
- show crypto engine connections active—Muestra los paquetes cifrados y descifrados.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos de Troubleshooting para Router IPsec

Nota: Consulte Información importante sobre los comandos de depuración antes de utilizar este tipo de comandos.

- debug crypto engine: muestra el tráfico que está cifrado.
- debug crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.

- debug crypto isakmp: muestra las negociaciones de la fase 1 del Protocolo ISAKMP (Internet Security Association and Key Management Protocol).

Verificación de las asociaciones de seguridad

- clear crypto isakmp: borra las asociaciones de seguridad de Intercambio de claves de Internet (IKE).
- clear crypto ipsec sa: borra las asociaciones de seguridad IPsec.

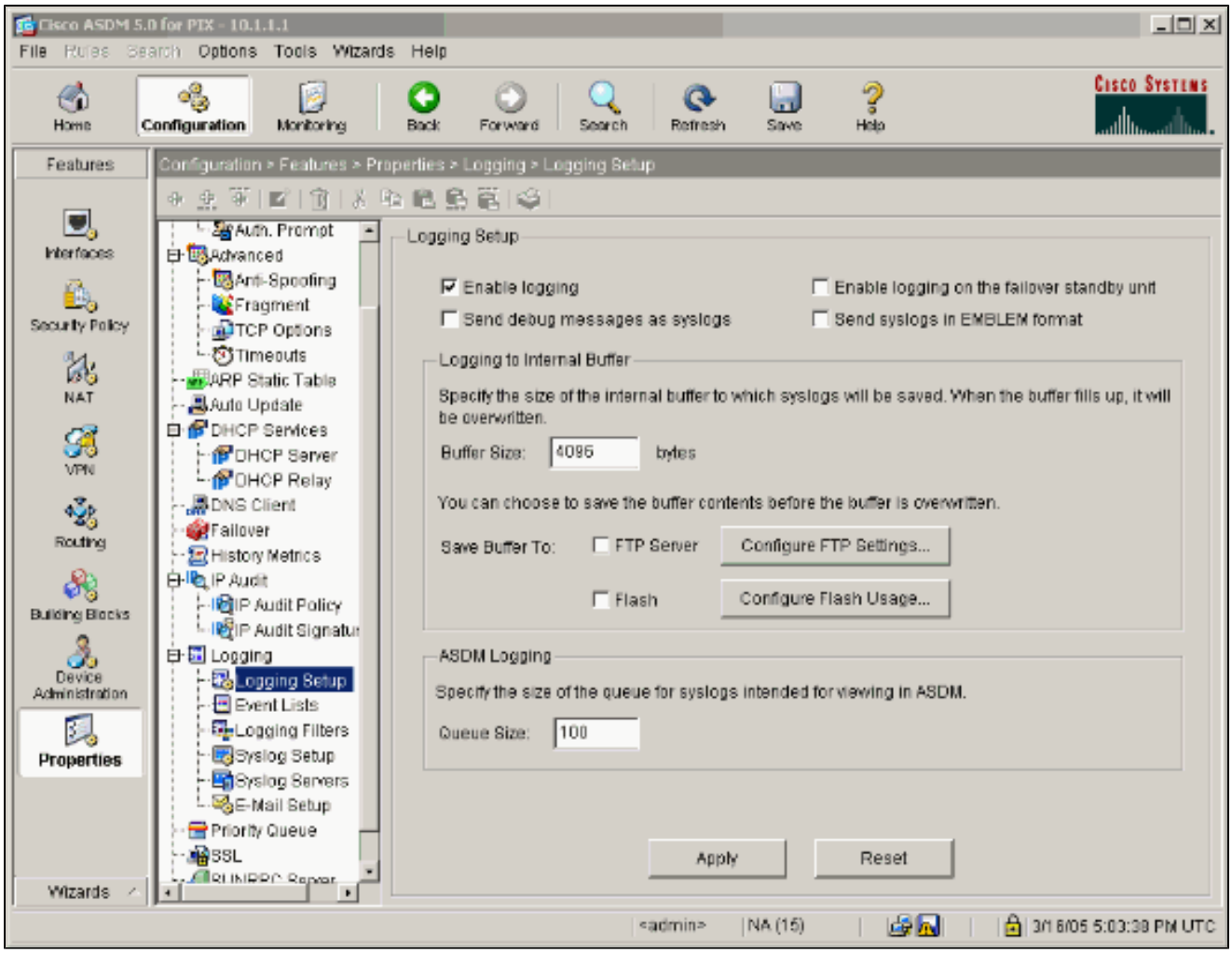
Comandos de Troubleshooting para PIX

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

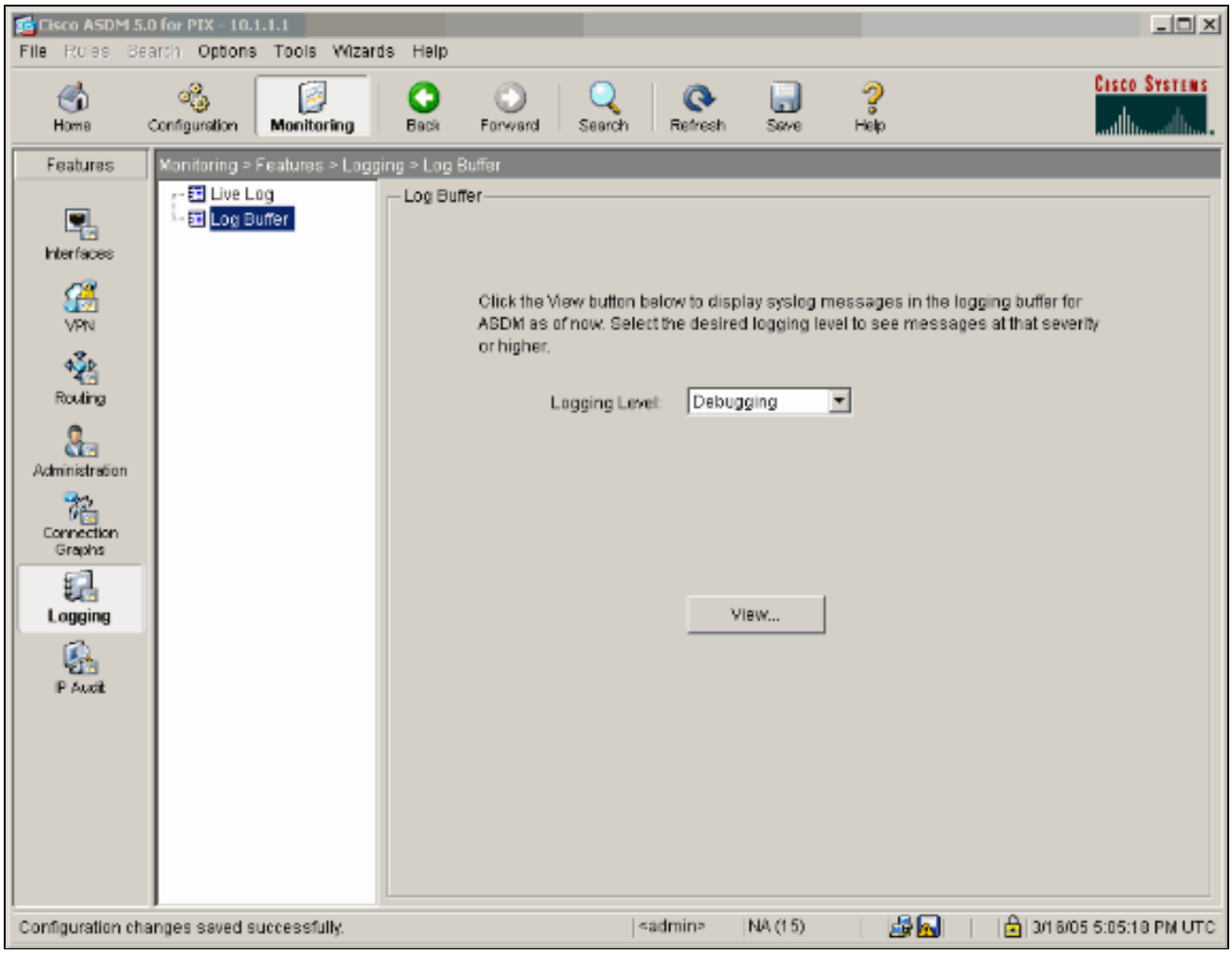
Nota: Consulte Información importante sobre los comandos de depuración antes de utilizar este tipo de comandos.

- logging buffer debugging—Muestra las conexiones que se establecen y las que se deniegan a los hosts que atraviesan el PIX. La información se almacena en el buffer de registro PIX y el resultado se puede ver usando el comando show log.
- ASDM se puede utilizar para habilitar el registro y también para ver los registros como se muestra en estos pasos.

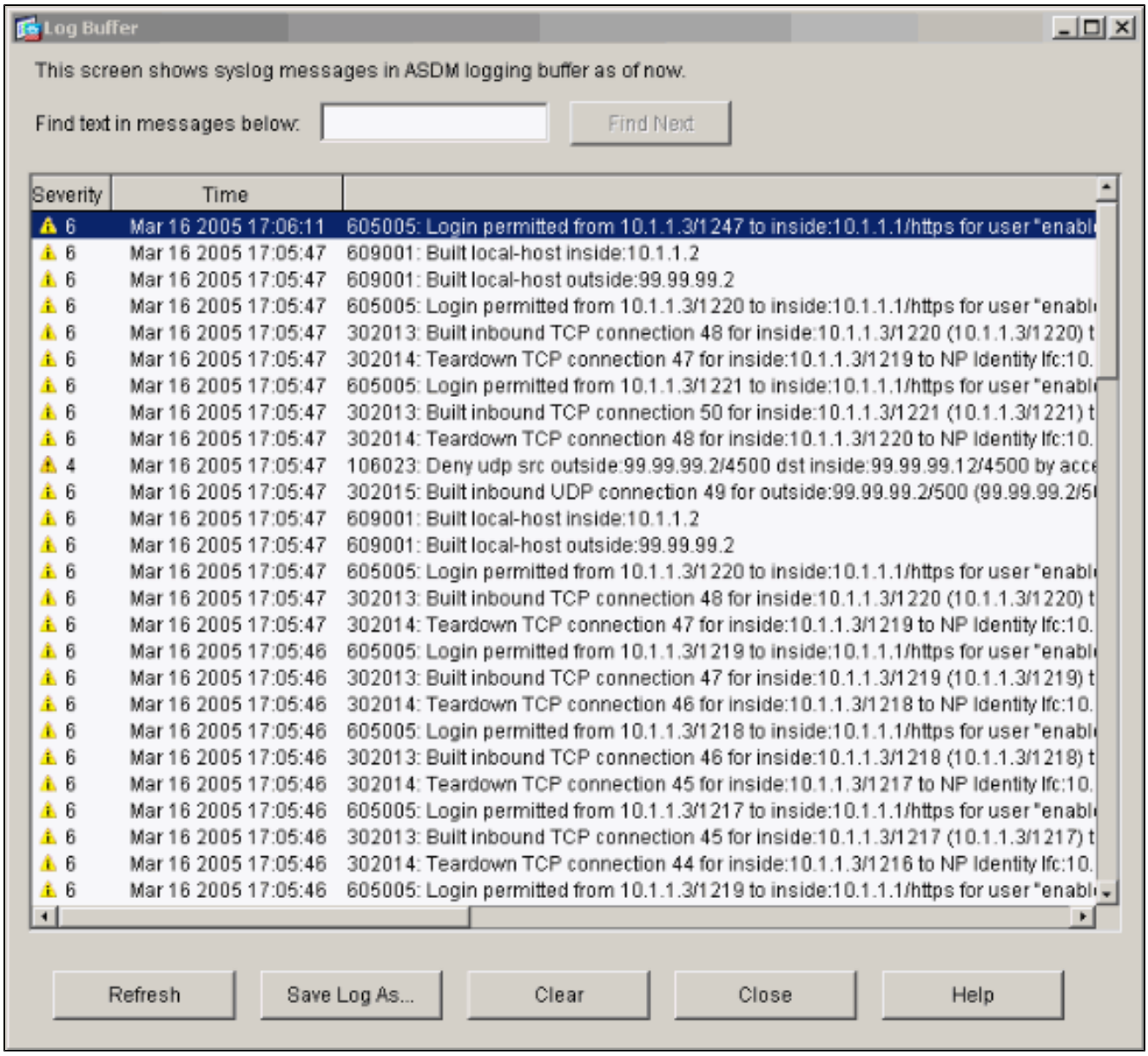
1. Elija Configuration > Properties > Logging > Logging Setup > Enable Logging y luego haga clic en Apply.



2. Elija Monitoring > Logging > Log Buffer > On Logging Level > Logging Buffer, a continuación, haga clic en View.



Este es un ejemplo de Log Buffer.



Información Relacionada

- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de Soporte de PIX
- Referencias de Comando PIX
- Página de Soporte de NAT
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).