Túnel del IPSec VPN del PIX/ASA (versión 7.x y posterior) con el ejemplo de configuración de la 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 trabaja con el Port Address Translation (PAT) si usted utiliza las versiones de software de Cisco IOS® anterior que y no incluyendo 12.2(13)T.** Los este tipos de configuración se pueden utilizar para hacer un túnel el tráfico IP. Esta configuración no se puede utilizar para cifrar el tráfico que no pasa con un Firewall, tal como IPX o actualizaciones de ruteo. El hacer un túnel del Generic Routing Encapsulation (GRE) es una opción más apropiada. En este ejemplo, los Cisco 2621 y 3660 Router son los puntos finales de la tunelización de IPSec que se unen a dos redes privadas, con los conductos o Listas de control de acceso (ACL) en el PIX mientras tanto para permitir el tráfico IPSec.

Nota: El NAT es una traducción de direcciones de uno a uno, no ser confundido con la PALMADITA, que es muchas (dentro del Firewall) - -uno a la traducción. Para más información sobre el Funcionamiento de NAT y la configuración, refiera a verificar el Funcionamiento de NAT y el Troubleshooting de NAT básico o cómo el NAT trabaja.

Nota: El IPSec con la PALMADITA no pudo trabajar correctamente porque el dispositivo del punto

final del túnel exterior no puede manejar los túneles múltiples a partir de una dirección IP. Entre en contacto a su vendedor para determinar si los dispositivos del punto finales del túnel funcionan con el patente. Además, en el Cisco IOS Software Release 12.2(13)T y Posterior, la característica de la Transparencia NAT se puede utilizar para el patente. Para más detalles, refiera a la Transparencia IPSec NAT. Refiera al soporte para el IPSec ESP con el NAT para aprender más sobre estas características en el Cisco IOS Software Release 12.2(13)T y Posterior.

Nota: Antes de que usted abra un caso con el Soporte técnico de Cisco, refiera a las Preguntas frecuentes sobre NAT, que tiene muchas respuestas a las preguntas comunes.

Refiera a configurar un túnel IPsec con un Firewall con el NAT para más información sobre cómo configurar el túnel IPsec con el Firewall con el NAT en la versión de PIX 6.x y anterior.

prerrequisitos

Requisitos

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.

- Cisco IOS Software Release 12.0.7.T (hasta pero no incluyendo el Cisco IOS Software Release 12.2(13)T)Para más versiones recientes, refiera a la Transparencia IPSec NAT.
- Cisco 2621 Router
- Router Cisco 3660
- Dispositivo de seguridad de la serie del Cisco PIX 500 que ejecuta 7.x y arriba.

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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.

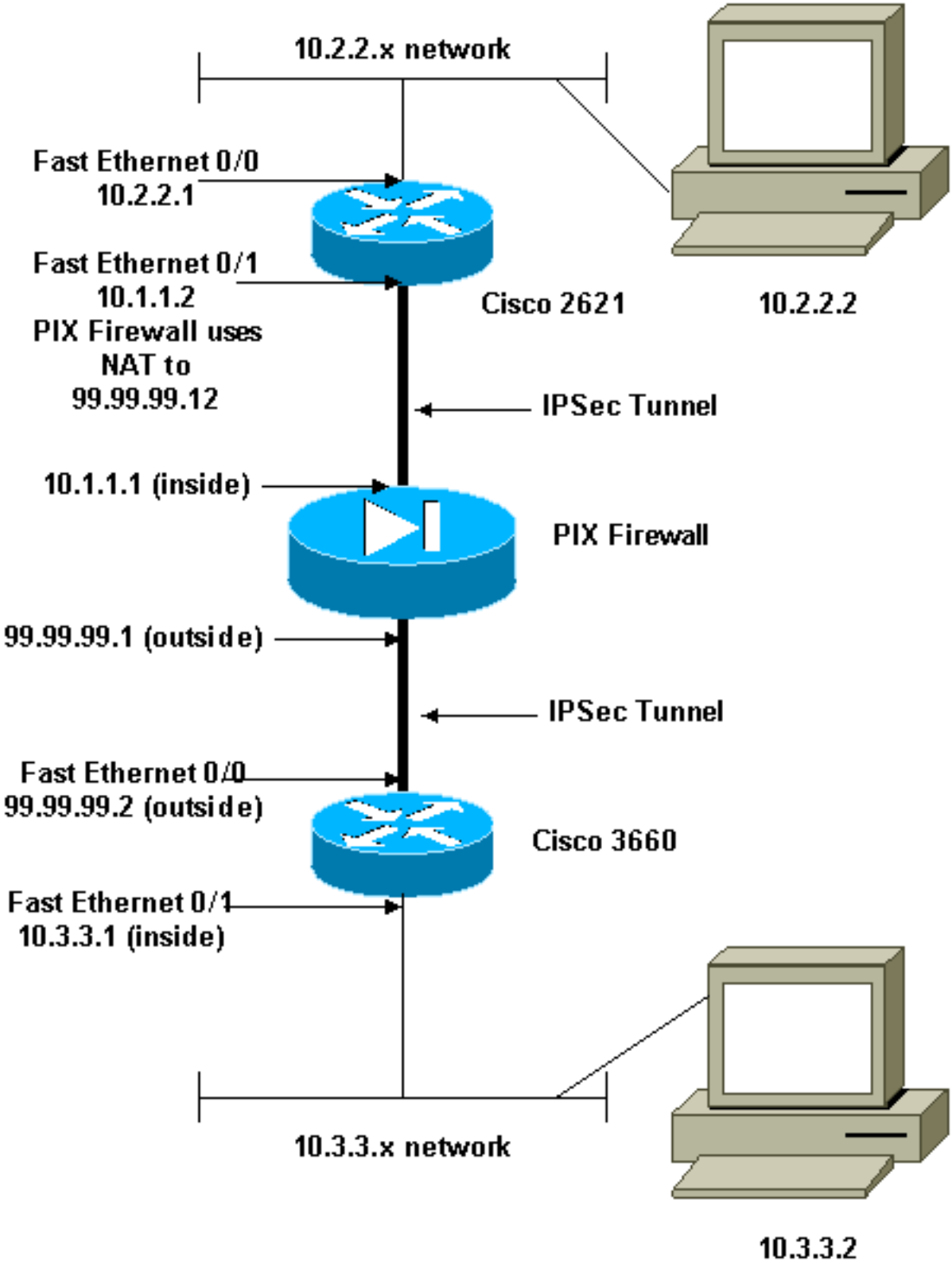
Configurar

Esta sección le presenta con la información que usted puede utilizar para configurar las características este documento describe.

Nota: Para encontrar la información adicional en los comandos que este documento utiliza, que utilice la herramienta de búsqueda de comandos (clientes registrados solamente).

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
- Dispositivo de seguridad y configuración de la lista de acceso PIXConfiguración del administrador de dispositivo GUI (ASDM) de la Seguridad avanzadaConfiguración del comando line interface(cli)
- Dispositivo de seguridad PIX y configuración del MPF (Marco de políticas modular)

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
```

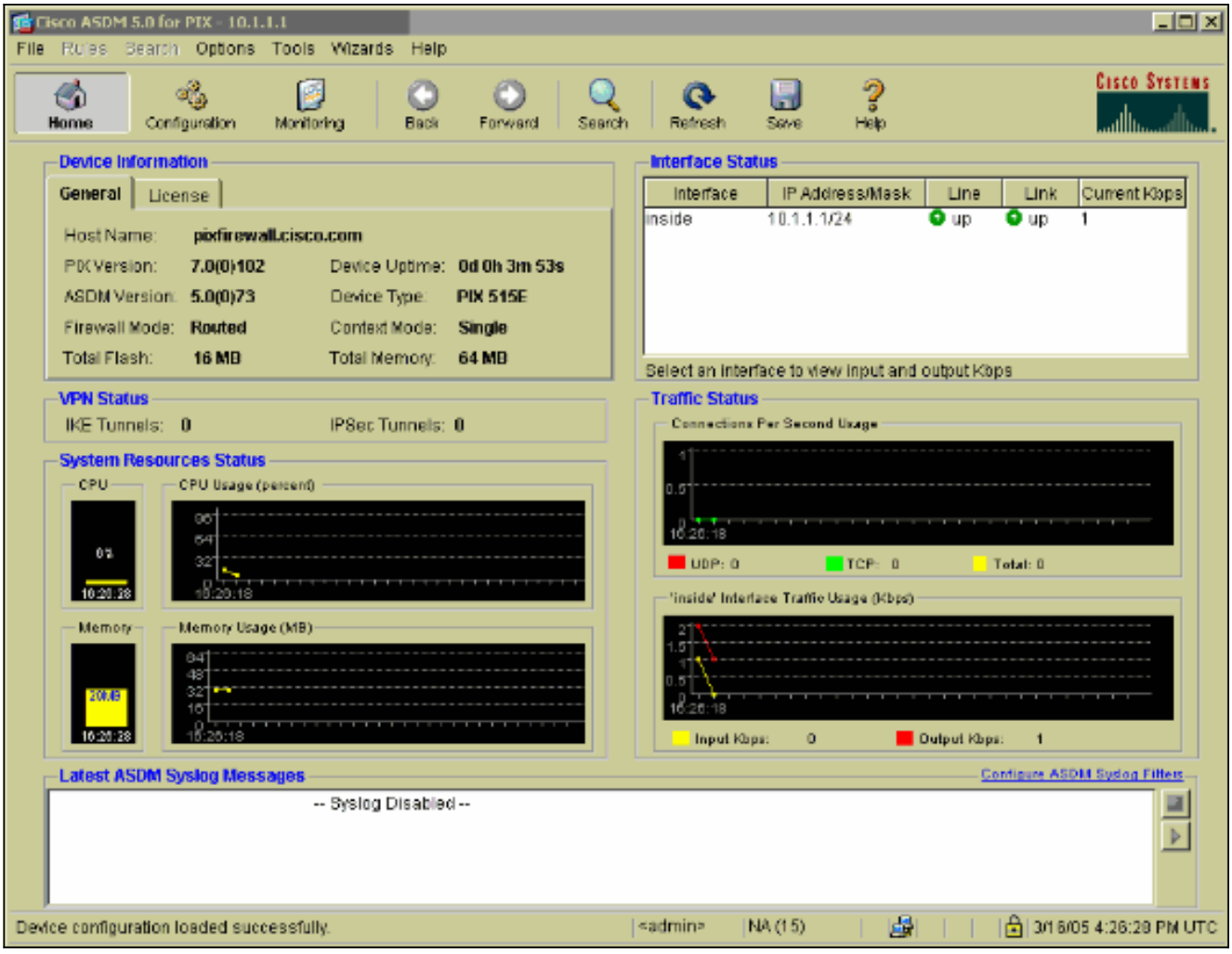
```
authentication pre-share crypto isakmp key cisco123
address 99.99.99.12 ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map mymap local-address
FastEthernet0/0 !--- The IPsec policy. crypto map mymap
10 ipsec-isakmp set peer 99.99.99.12 set transform-set
myset !--- Include the private-network-to-private-
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
```

Dispositivo de seguridad y configuración de la lista de acceso PIX

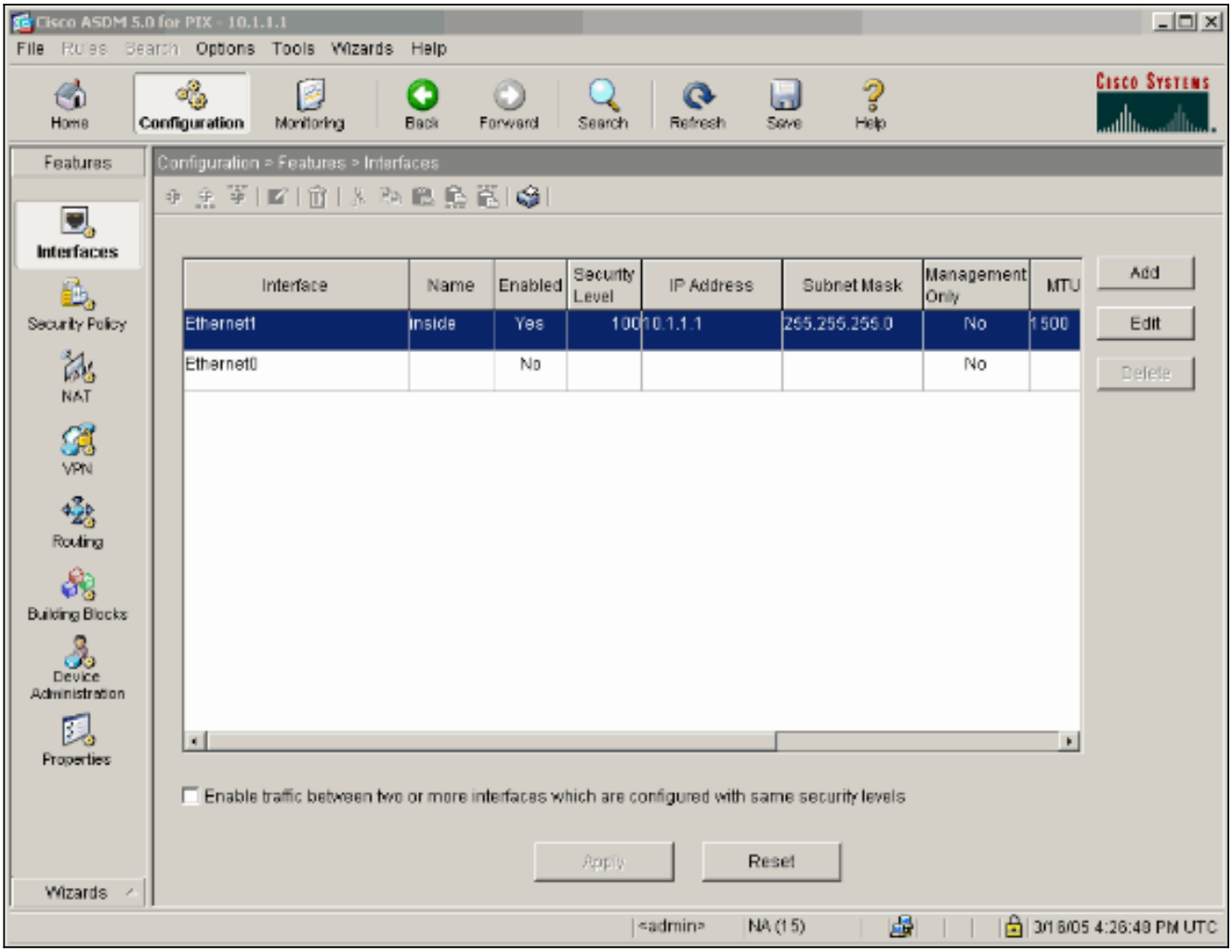
Configuración del ASDM 5.0

Complete estos pasos para configurar la versión 7.0 del firewall PIX usando el ASDM.

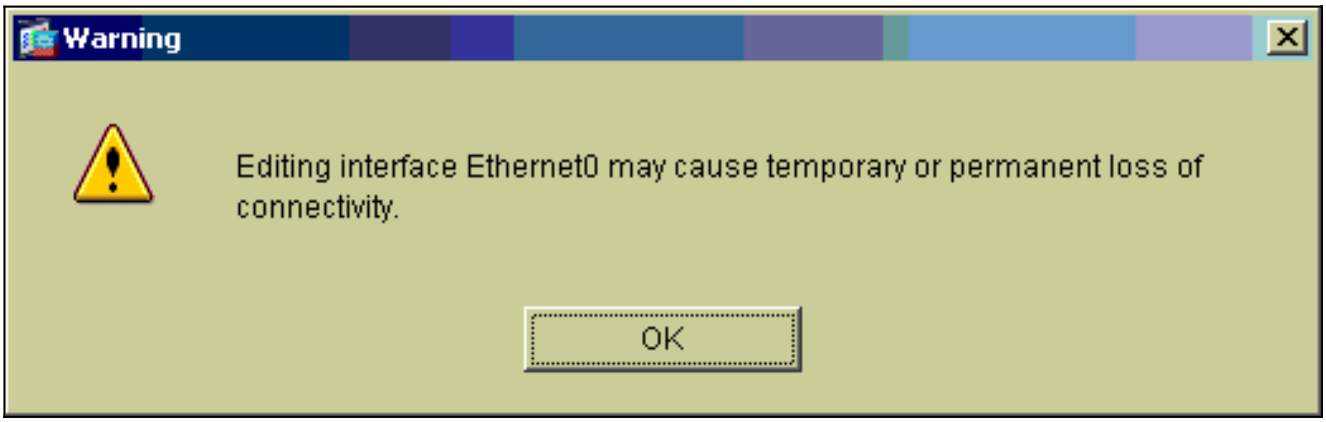
1. Consola en el PIX. De una configuración despejada, utilice los prompts interactivos para habilitar al **administrador de dispositivo GUI (ASDM) de la Seguridad avanzada** para la Administración del PIX del puesto de trabajo 10.1.1.3.
2. Del puesto de trabajo 10.1.1.3, abra a un buscador Web y utilice el ADSM (en este ejemplo, https://10.1.1.1).
3. Elija **sí** en los prompts del certificado y inicie sesión con la contraseña habilitada como está configurado en la configuración de arranque de ASDM del firewall PIX.
4. Si esto está la primera vez el ASDM se ejecuta en el PC, le indica si utilizar el activador de ASDM, o utilizar el ASDM como subprograma Java.En este ejemplo, el activador de ASDM se selecciona y instala estos prompts.
5. Proceda a la ventana de inicio de ASDM y seleccione la ficha de configuración.



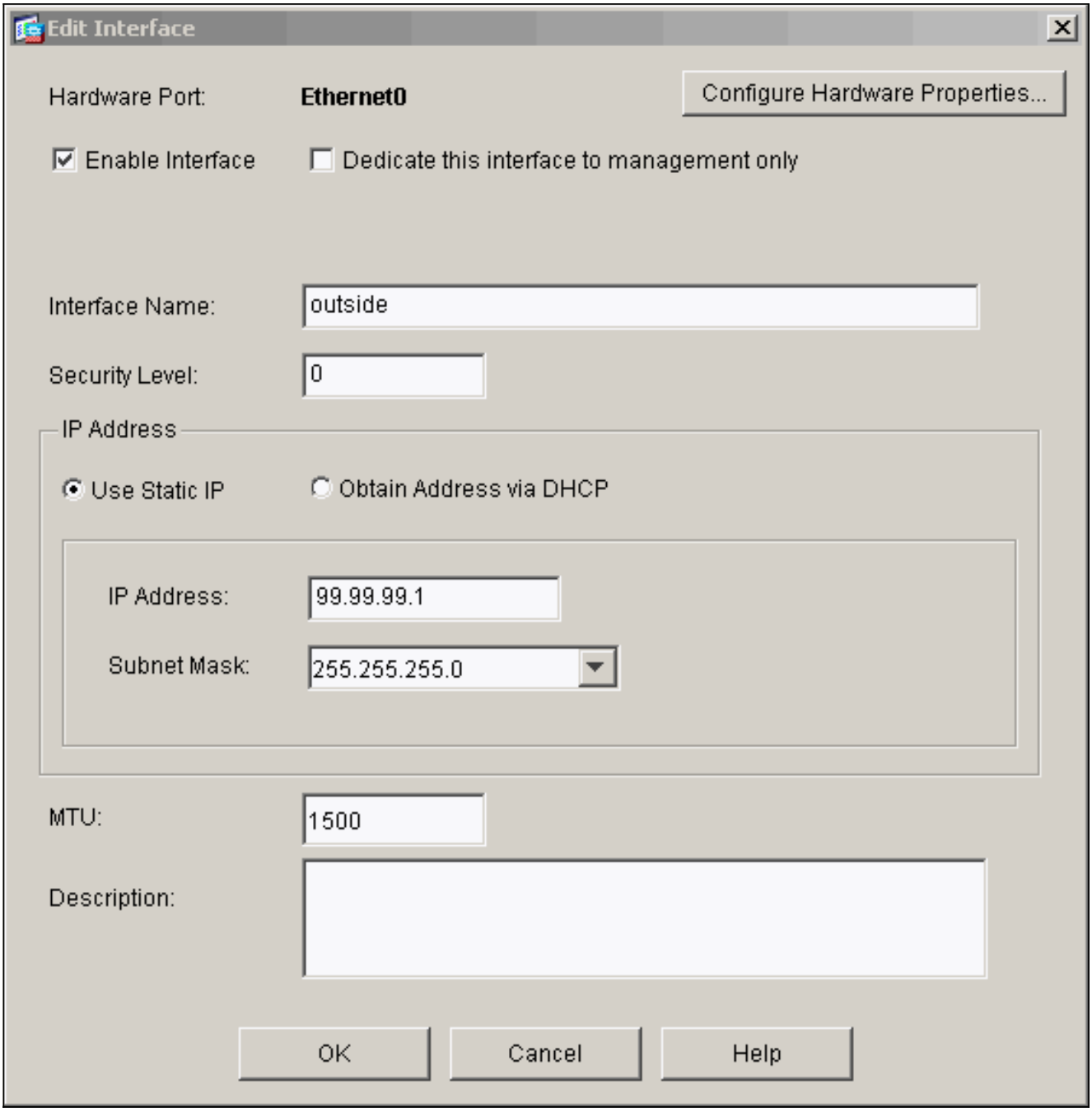
6. Resalte la **interfaz del ethernet0** y el tecleo **edita** para configurar la interfaz exterior.



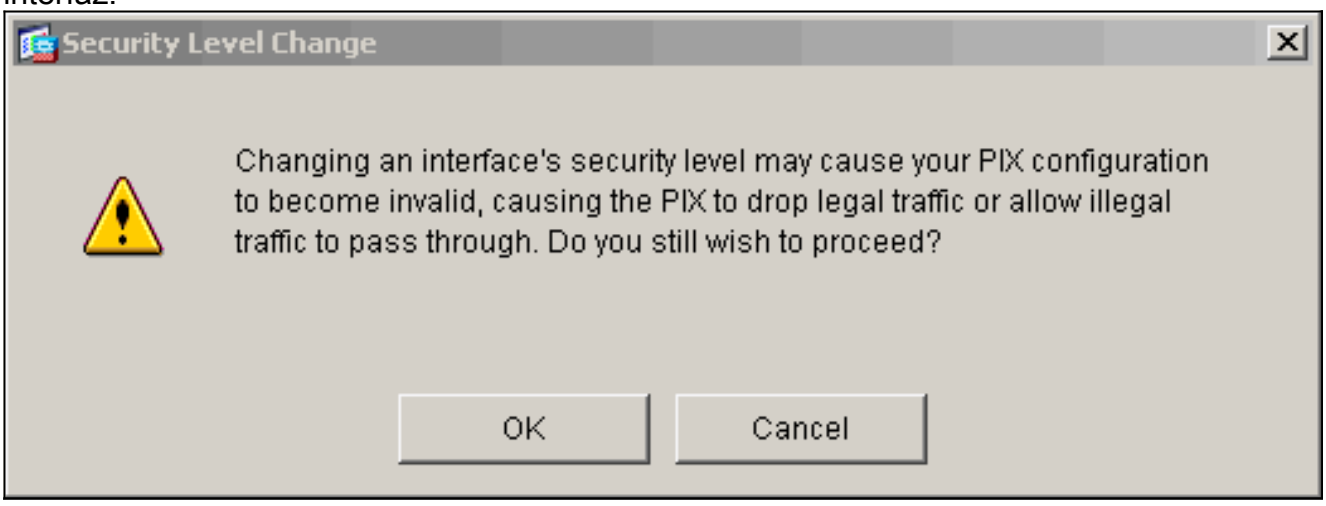
7. Haga Click en OK en el prompt de la interfaz que edita.



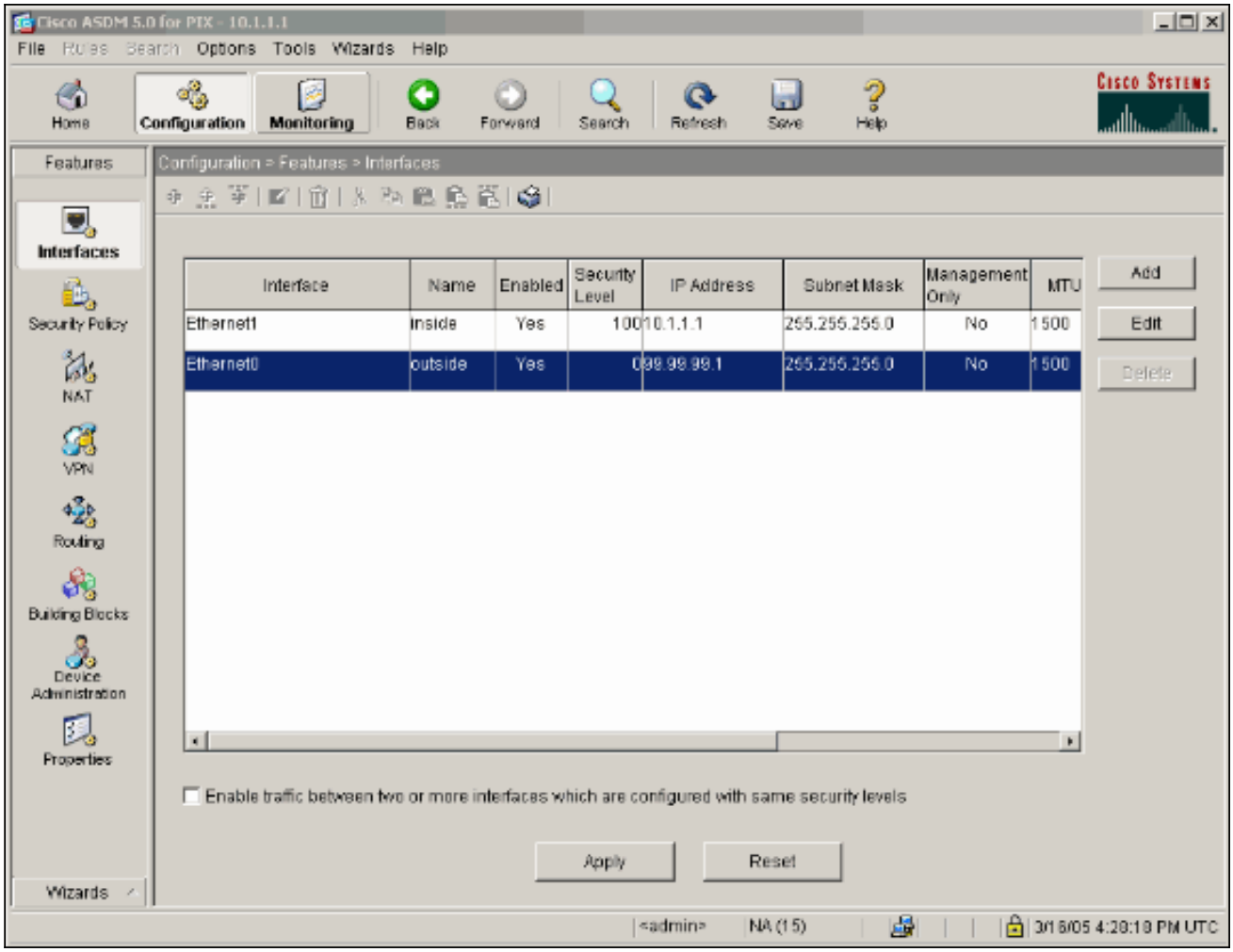
8. Ingrese los detalles de la interfaz y haga clic la **AUTORIZACIÓN** cuando le hacen.



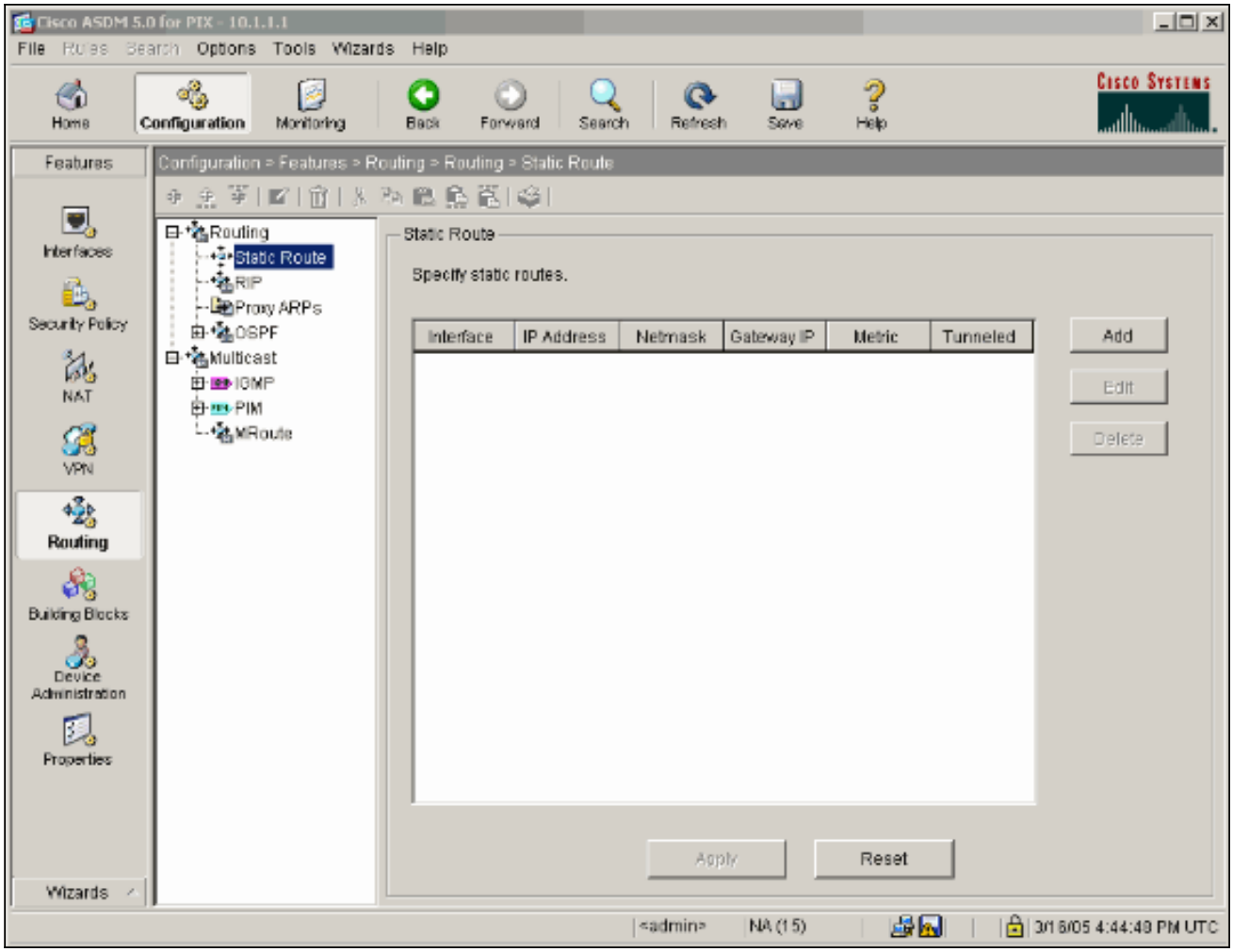
9. Haga Click en OK en el cambio de un prompt de la interfaz.



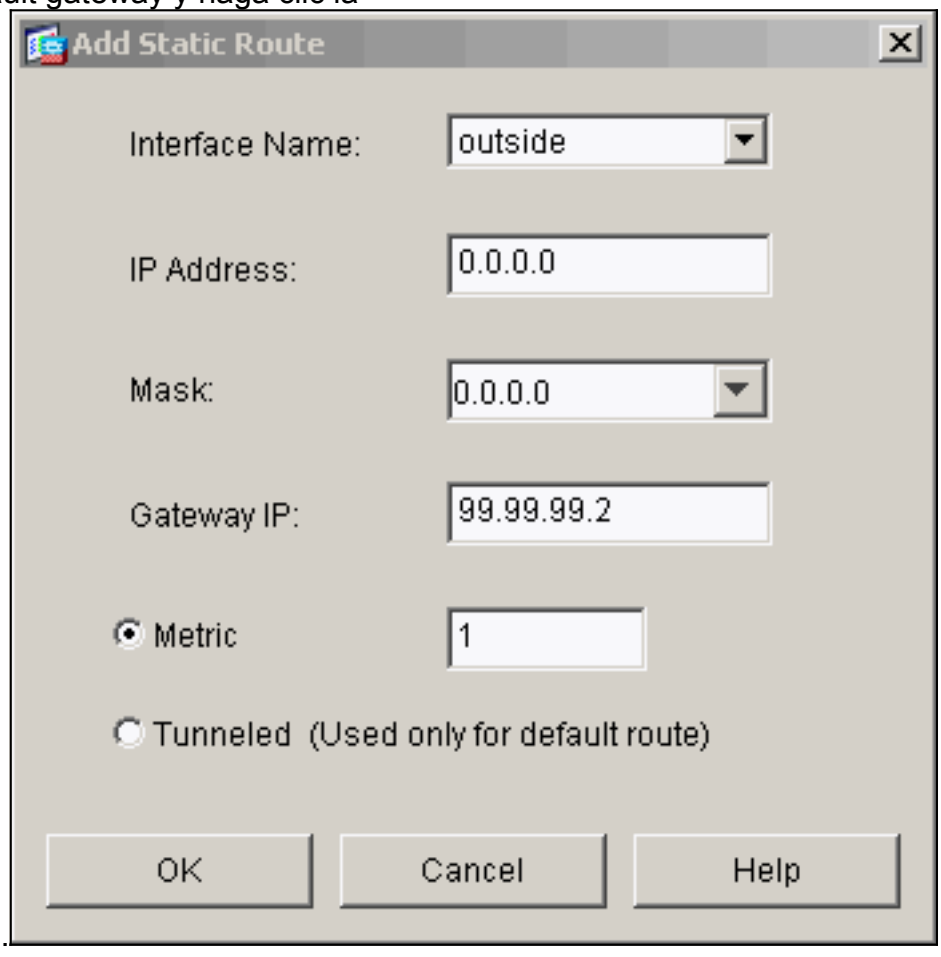
10. El tecleo **se aplica** para validar la configuración de la interfaz. La configuración también consigue avanzada sobre el PIX. Este ejemplo utiliza las Static rutas.



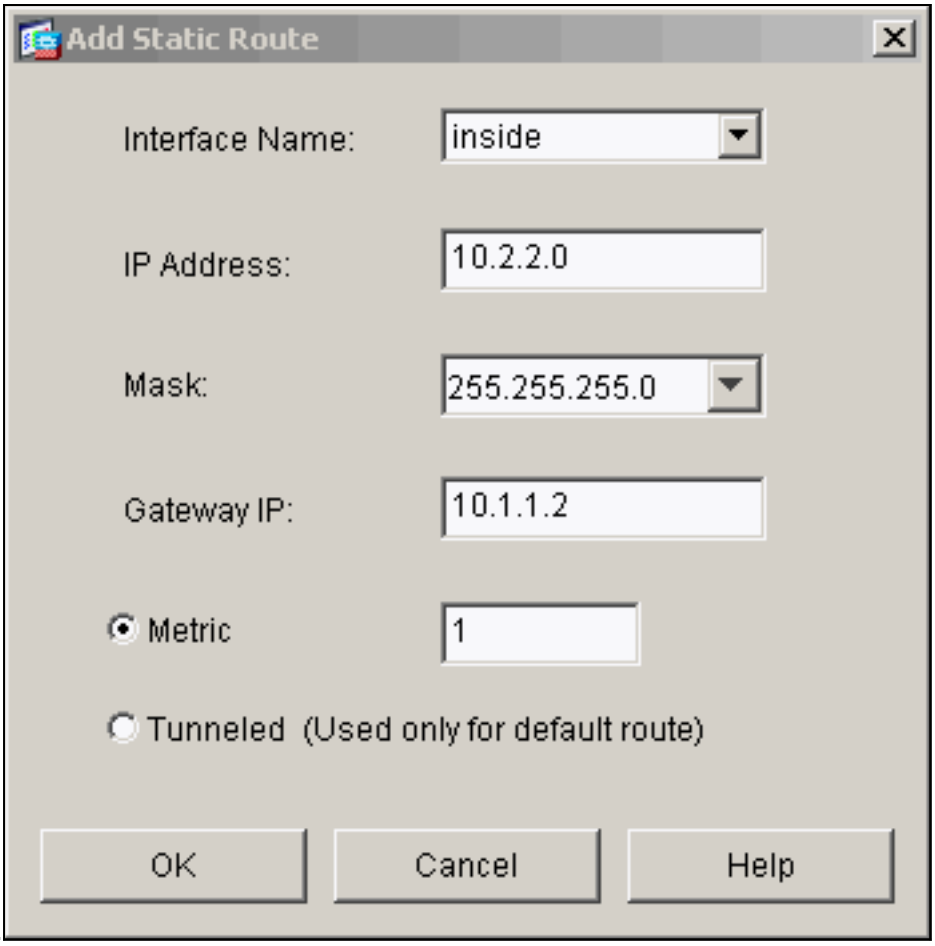
11. **La encaminamiento del** tecleo bajo características tabula, **Static ruta del** resaltado, y haga click en
    Add



12. Configure el default gateway y haga clic la AUTORIZACIÓN.

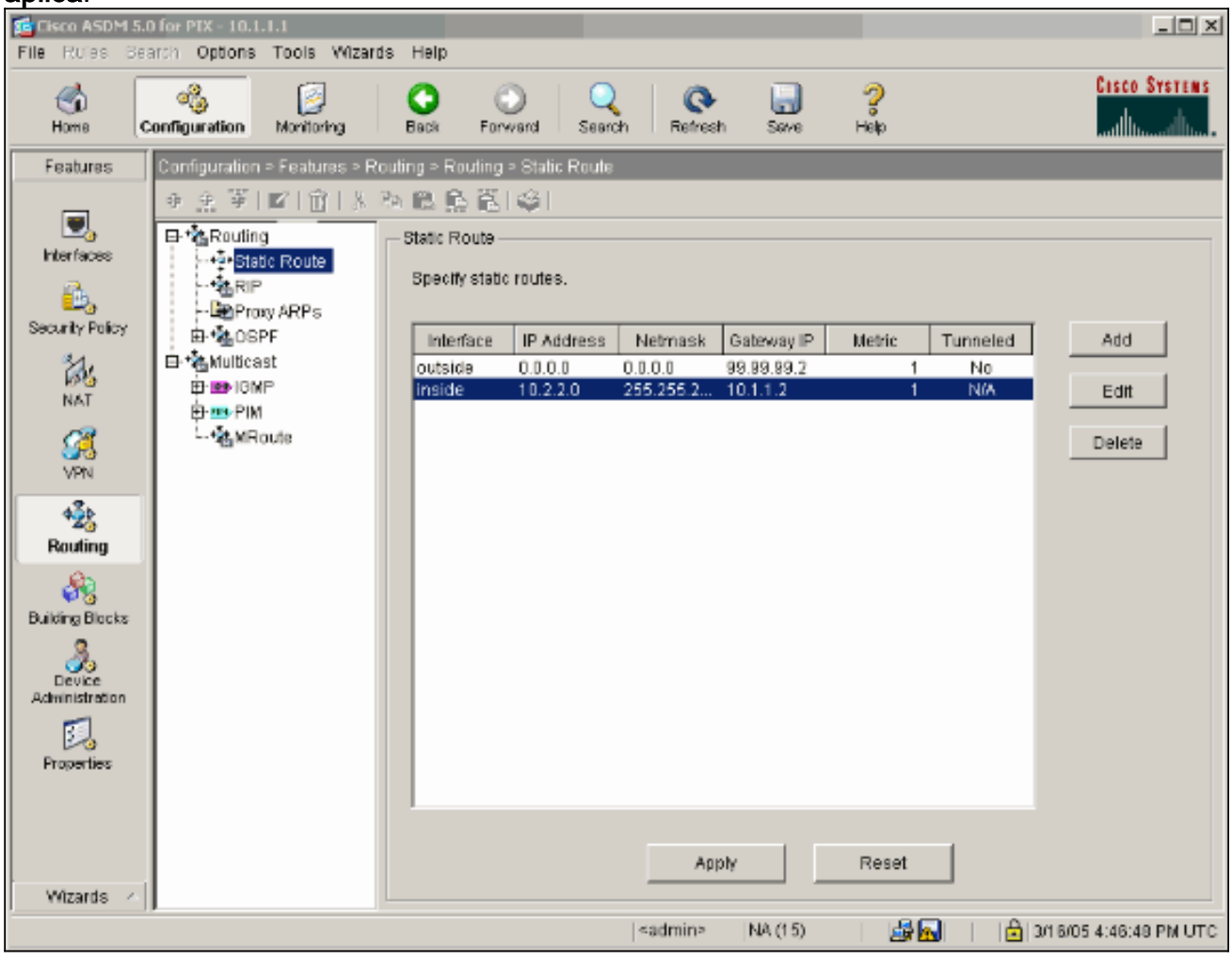


13. El tecleo **agrega** y agrega las rutas a las redes

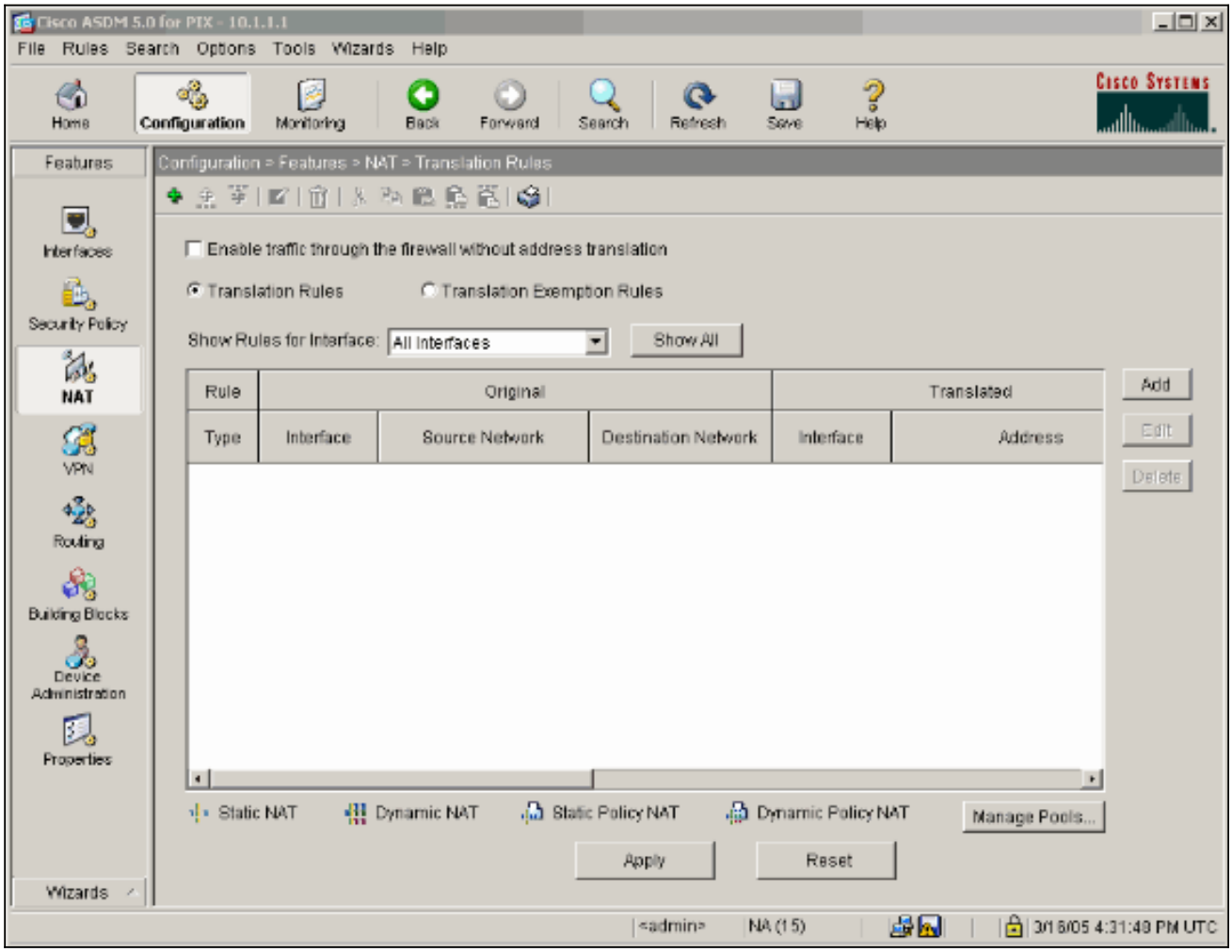


internas.

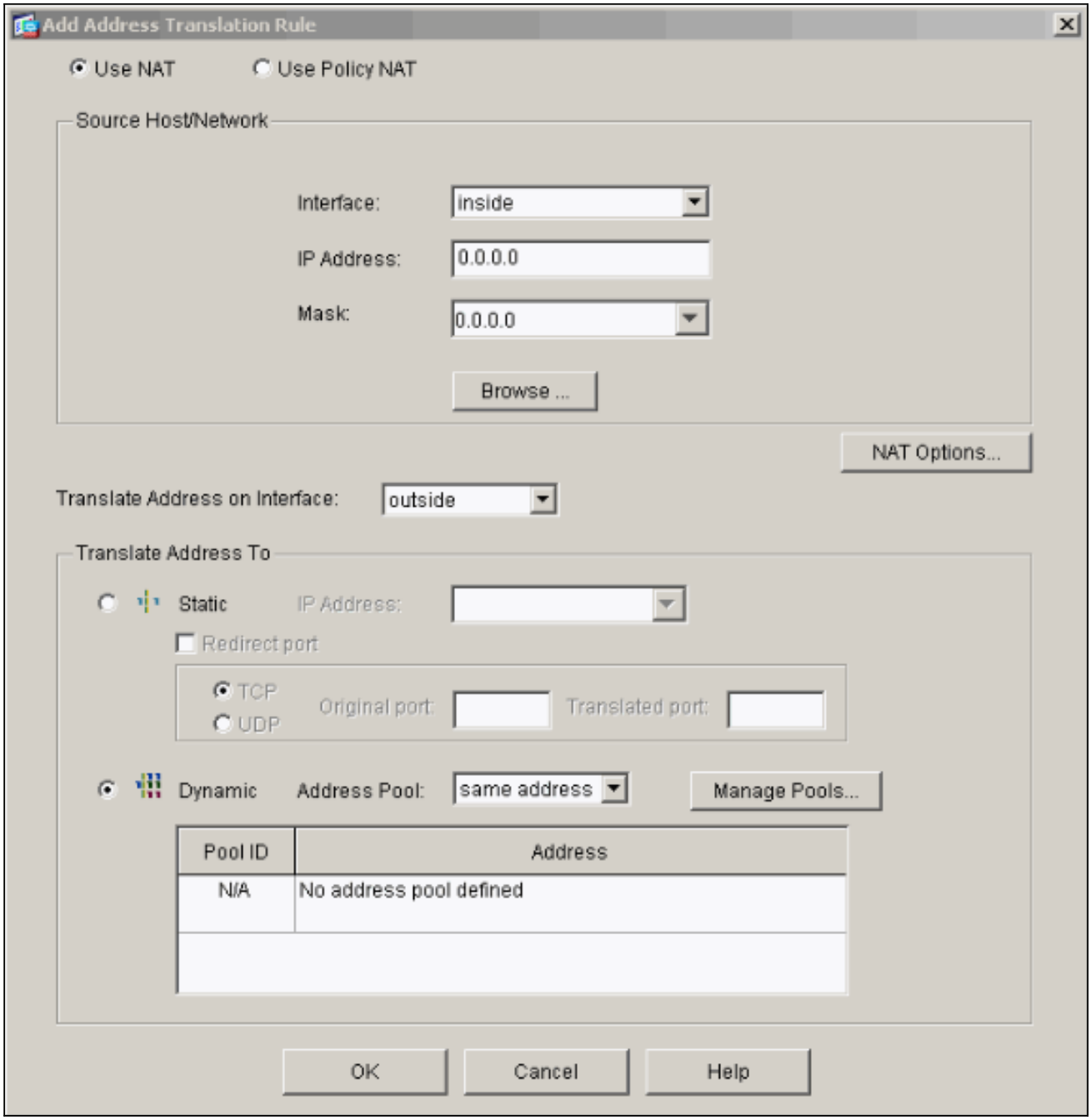
14. Confirme que las rutas correctas están configuradas y el tecleo **se aplica**.



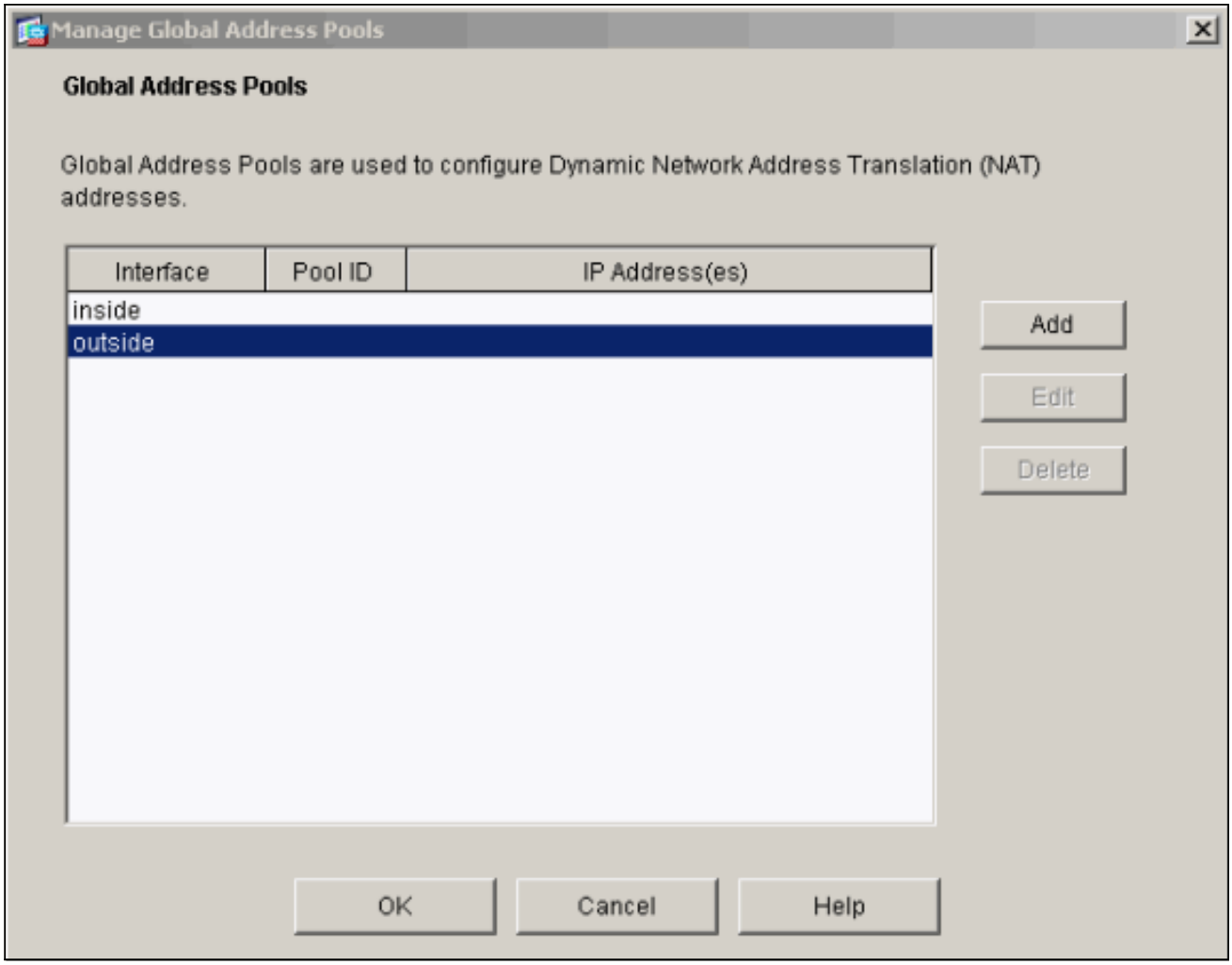
15. En este ejemplo, se utiliza el NAT. Quite el control en el cuadro para el **tráfico del permiso con el Firewall sin la traducción de la dirección** y el tecleo **agrega** para configurar la regla NAT.



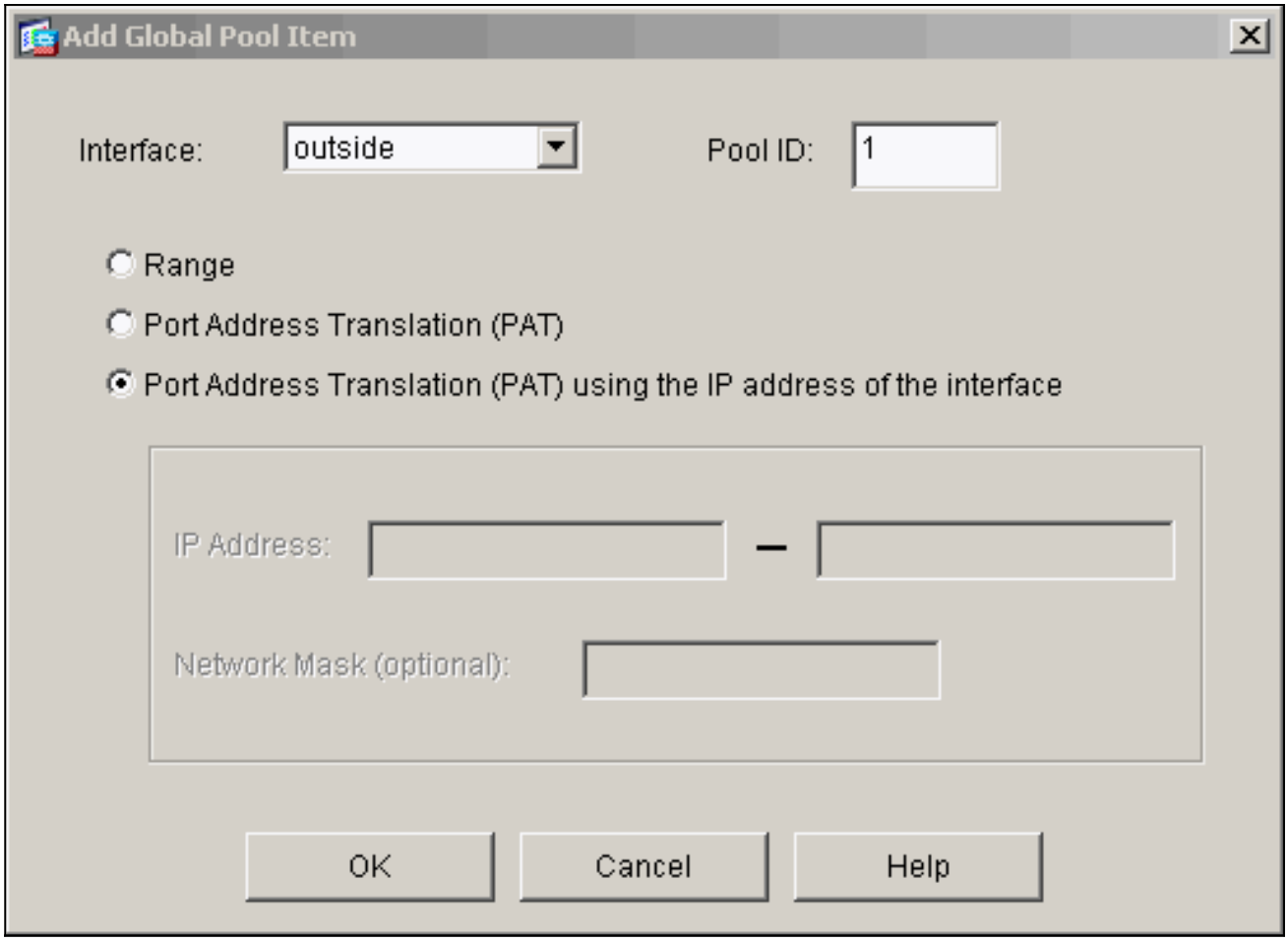
16. Configure la red de origen (este ejemplo utiliza). Entonces haga clic **manejan a los pools** para definir el
patente.



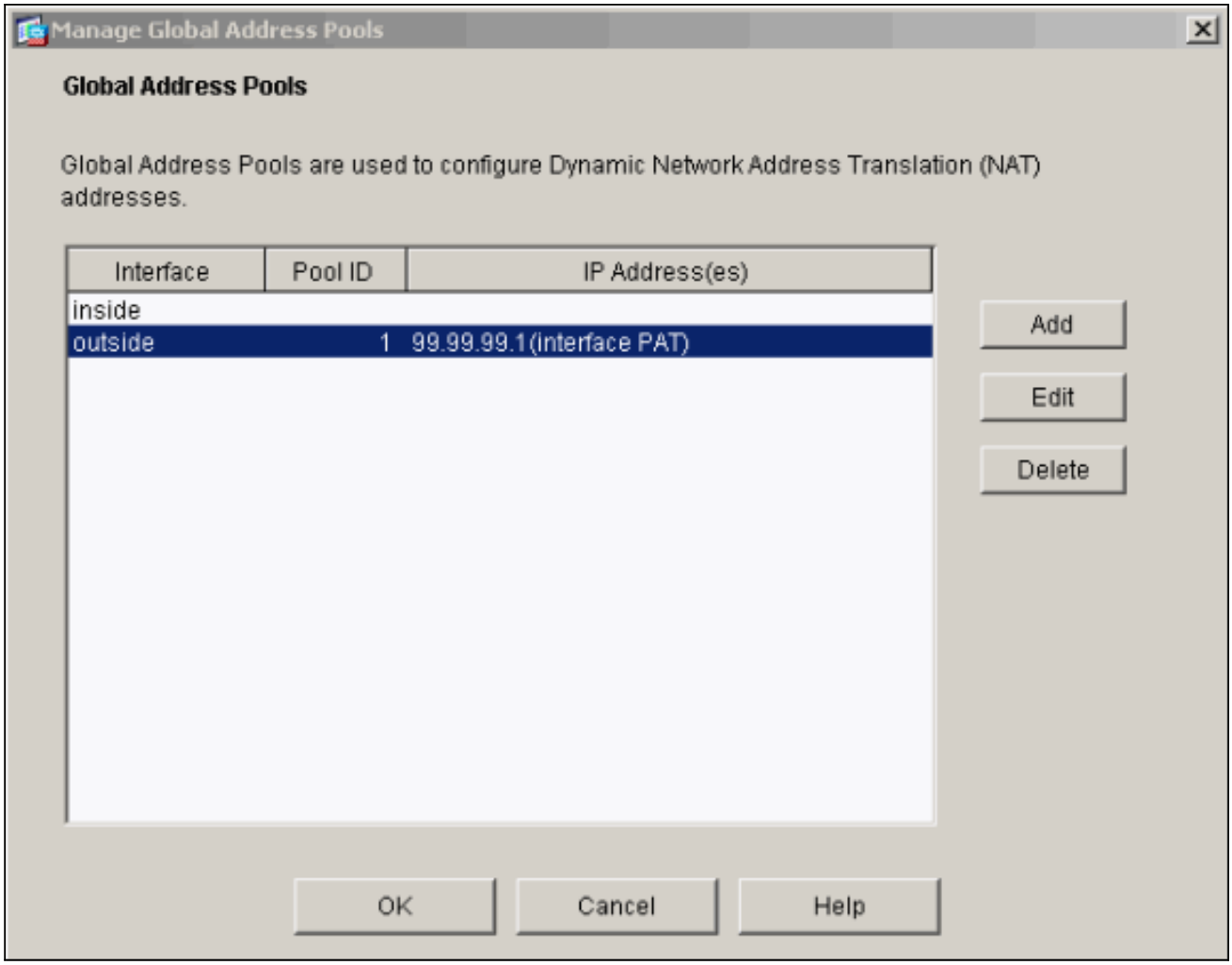
17. Seleccione la **interfaz exterior** y el haga click en Add



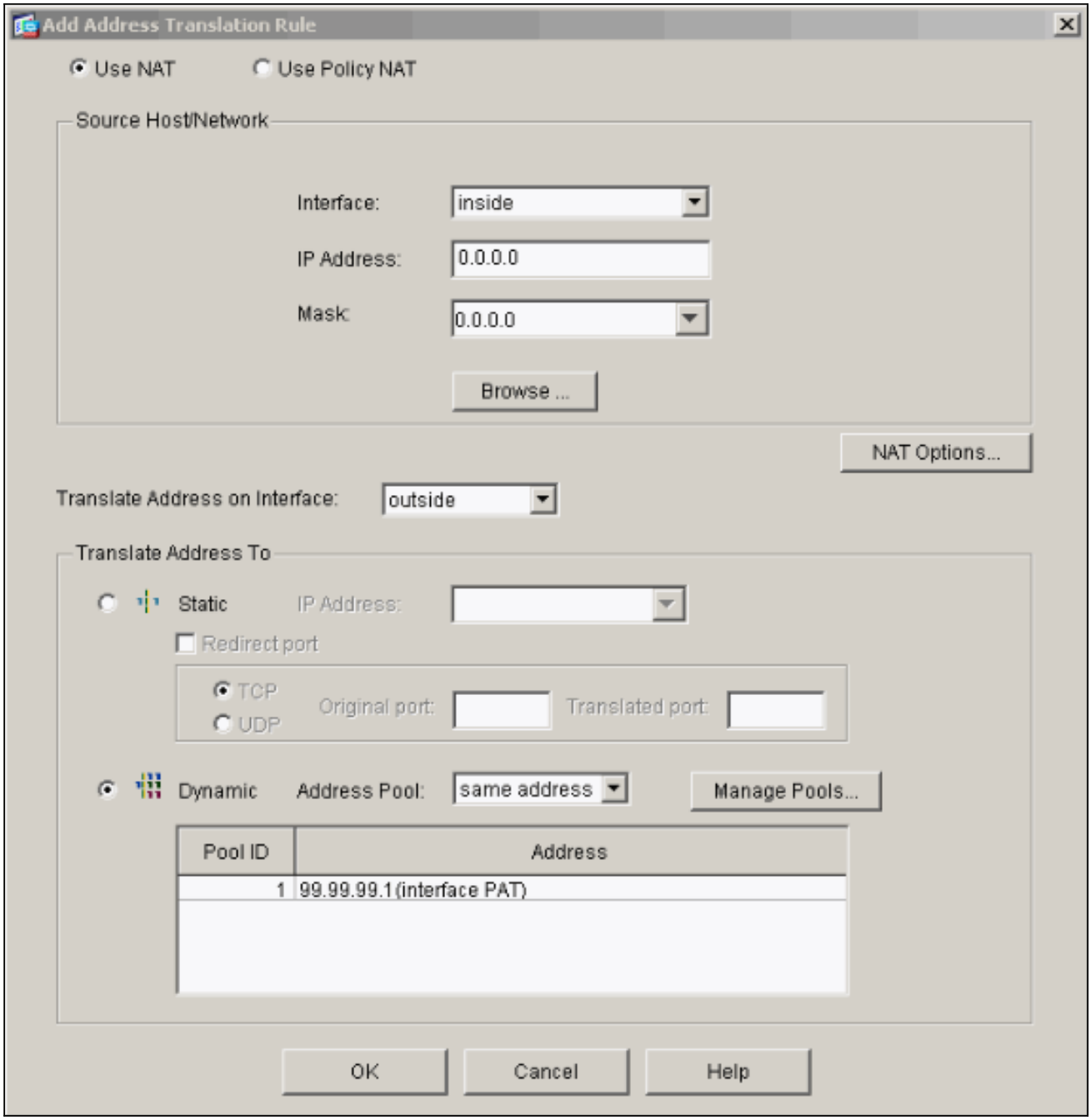
Este ejemplo utiliza una PALMADITA usando la dirección IP de la interfaz.



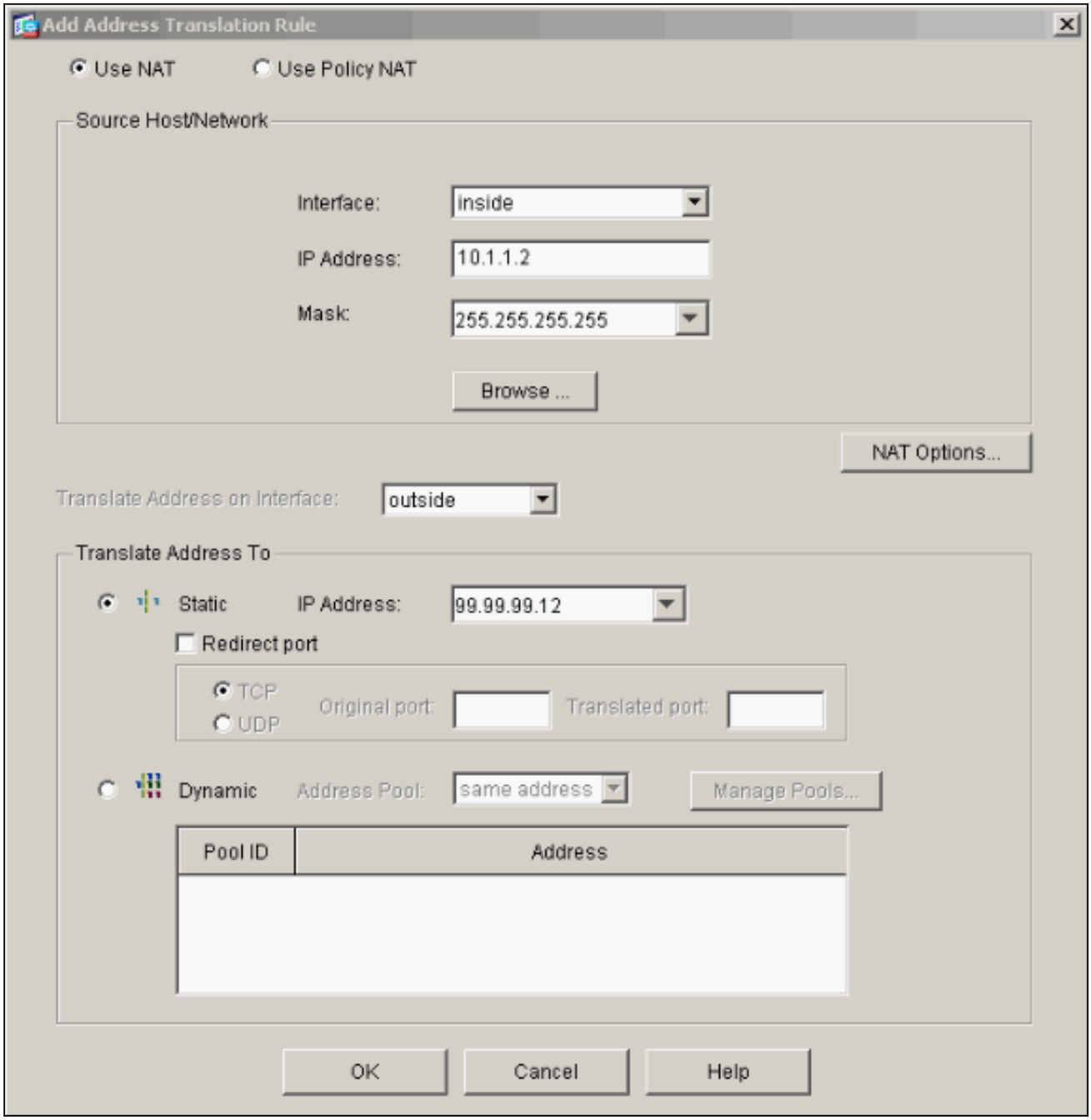
18. Haga Click en OK cuando se configura la PALMADITA.



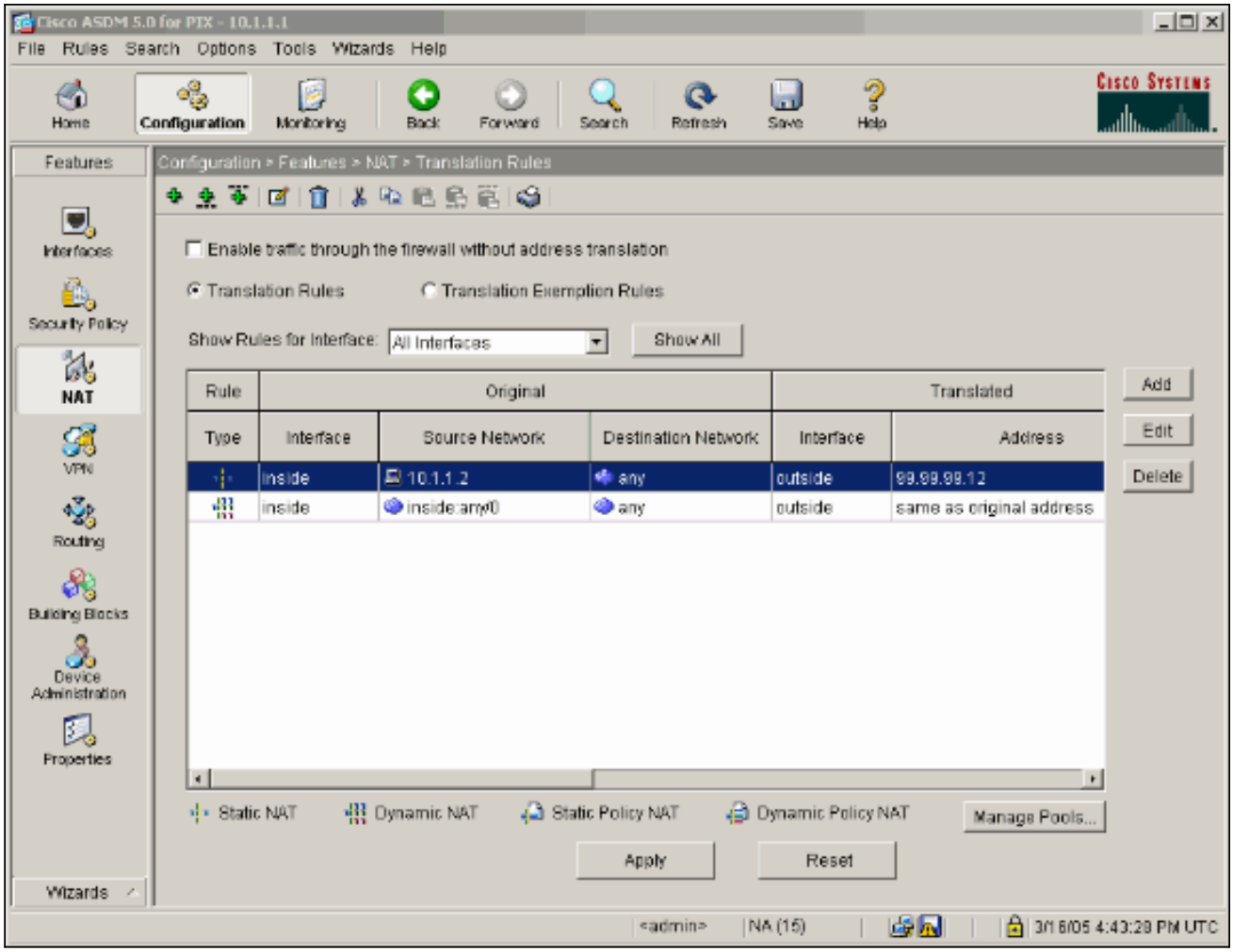
19. El tecleo **agrega** para configurar la traducción estática.



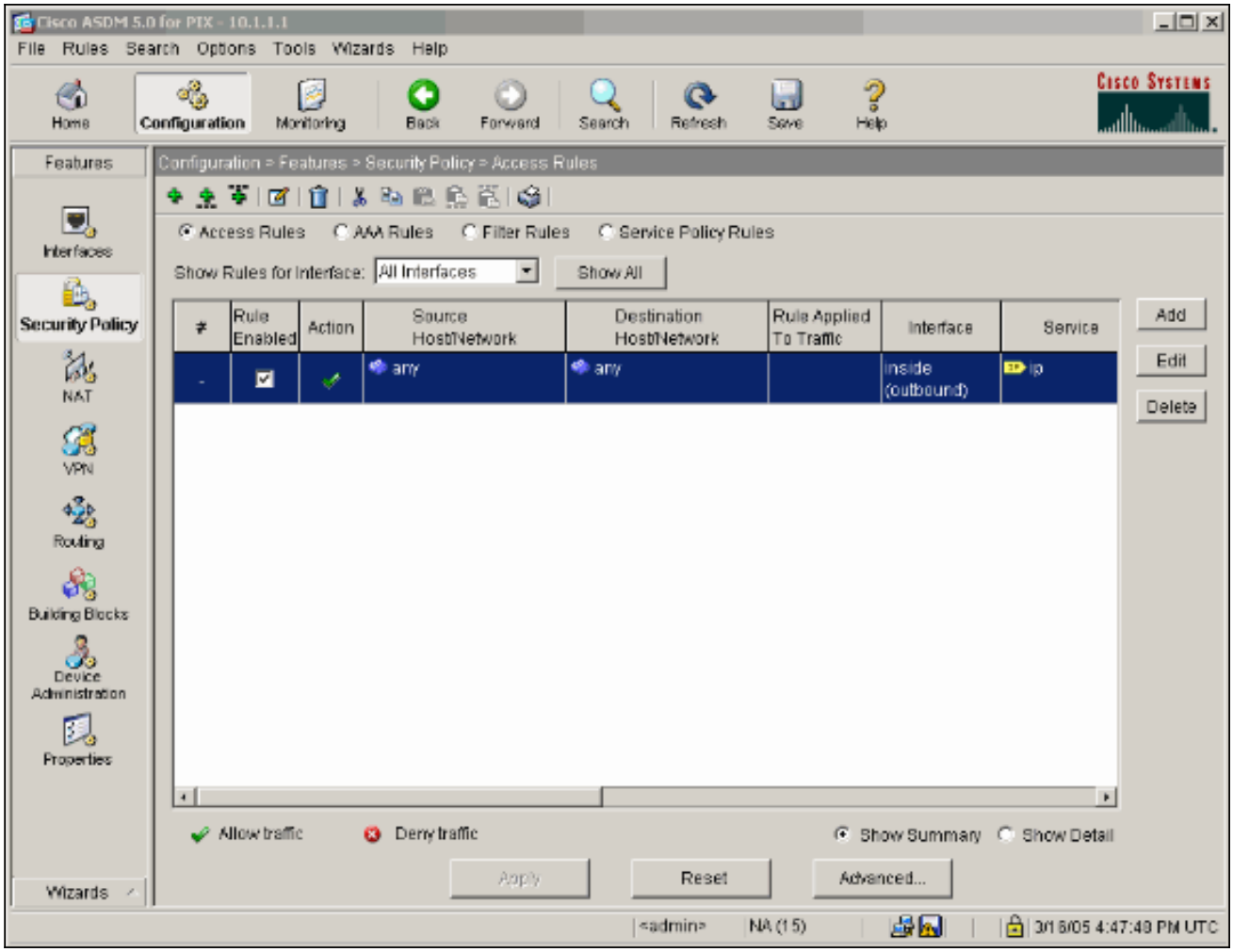
20. Seleccione el **interior** en el descenso-abajo de la interfaz, después ingrese a la dirección IP 10.1.1.2, máscara de subred **255.255.255.255**, elija los **parásitos atmosféricos** y en la dirección externa **99.99.99.12 del** tipo de campo del IP Address. Haga Click en OK cuando le
hacen.



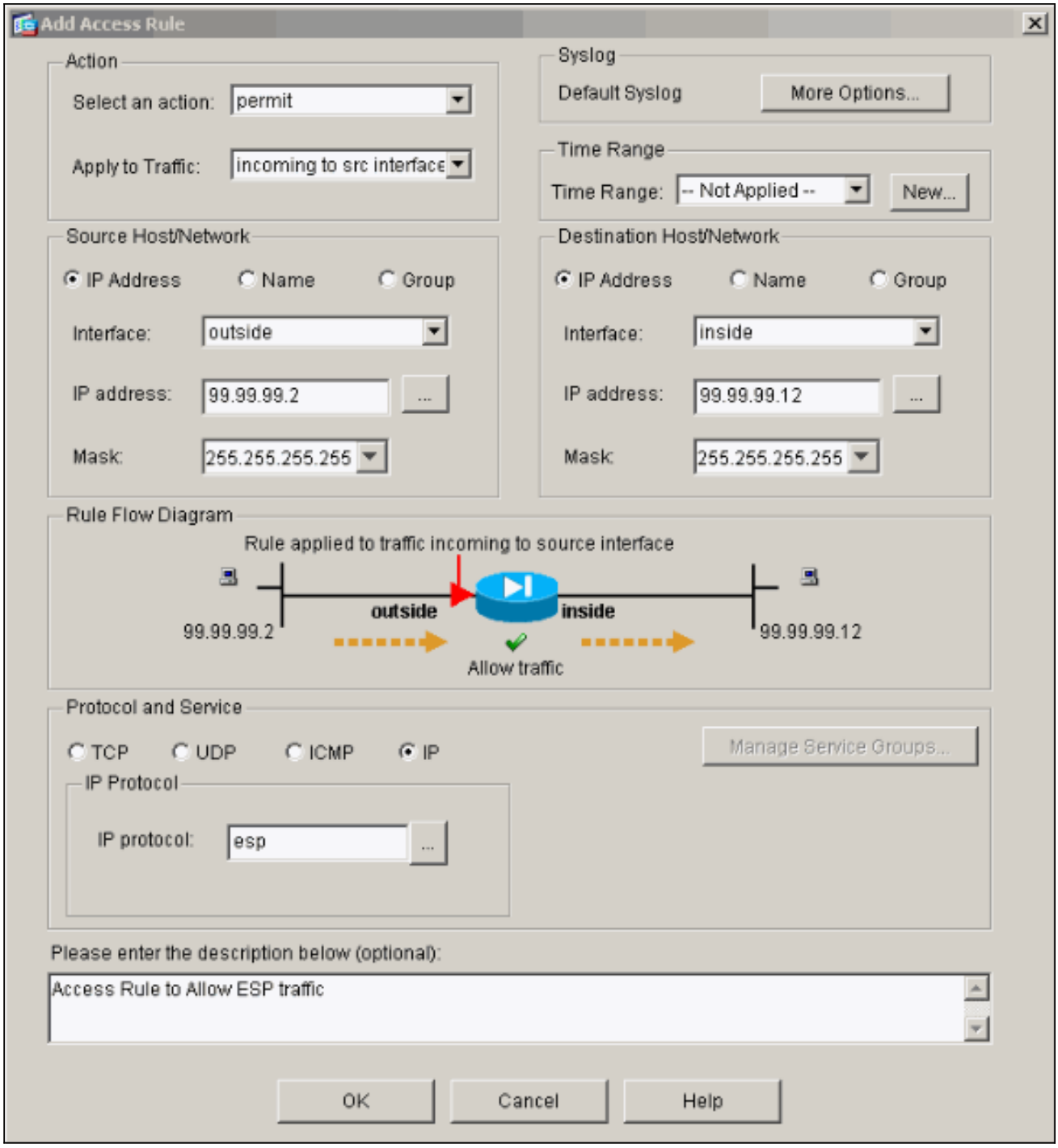
21. El tecleo **se aplica** para validar la configuración de la interfaz. La configuración también consigue avanzada sobre el
PIX.



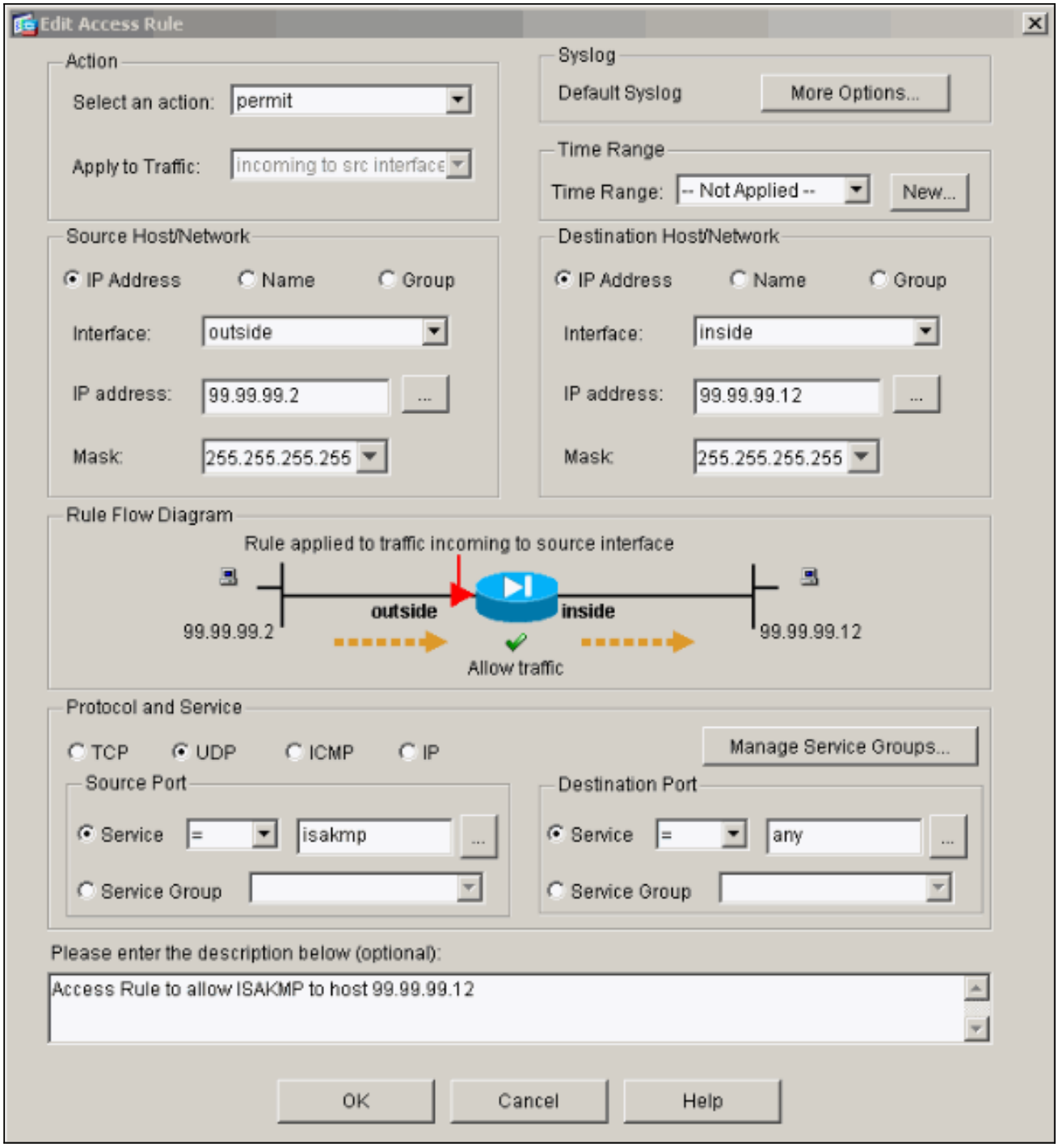
22. **La política de seguridad** selecta bajo características tabula para configurar la regla de la política de
seguridad.



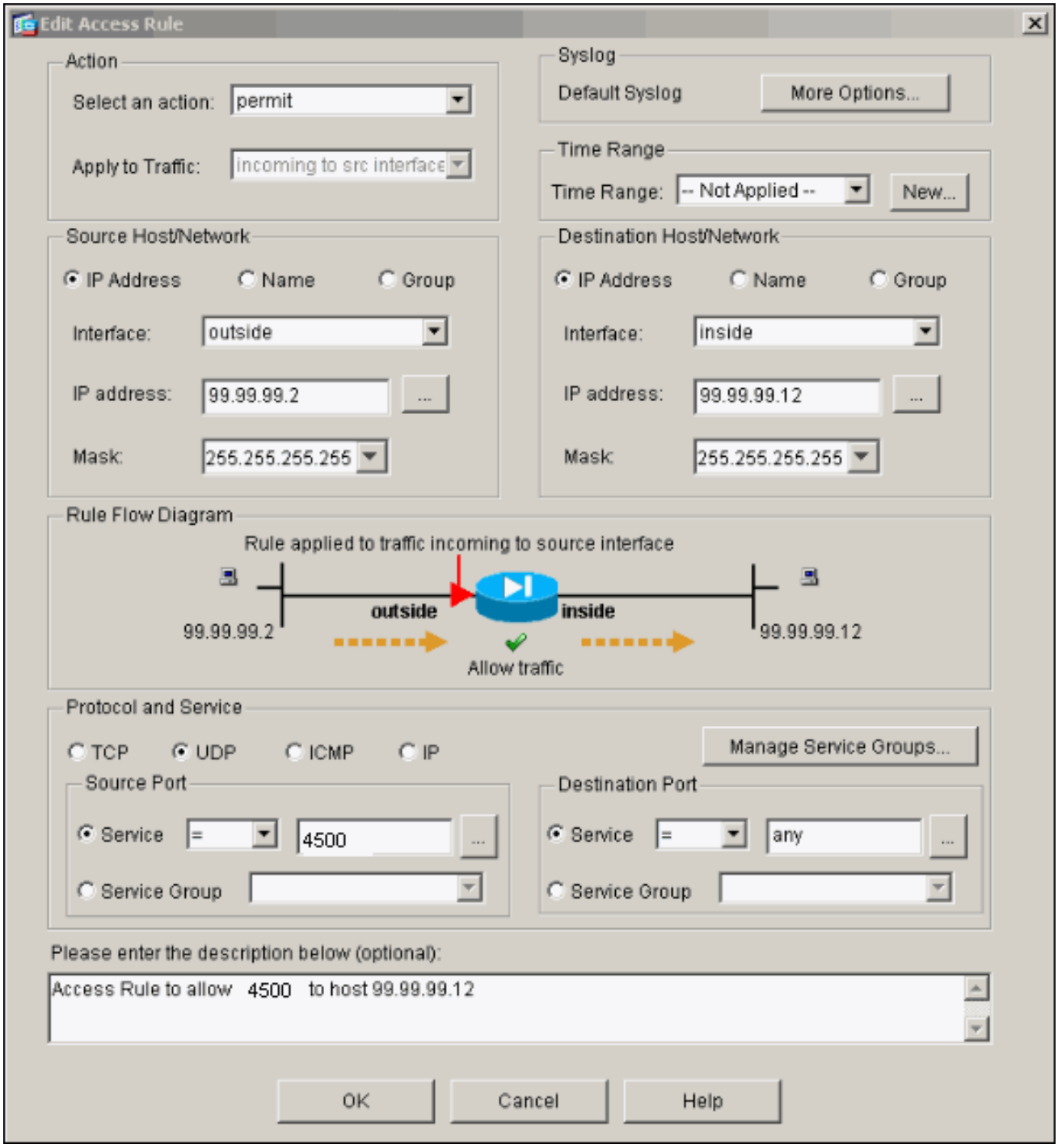
23. El tecleo **agrega** para permitir que la **AUTORIZACIÓN** especialmente del tráfico y del tecleo para
continuar.



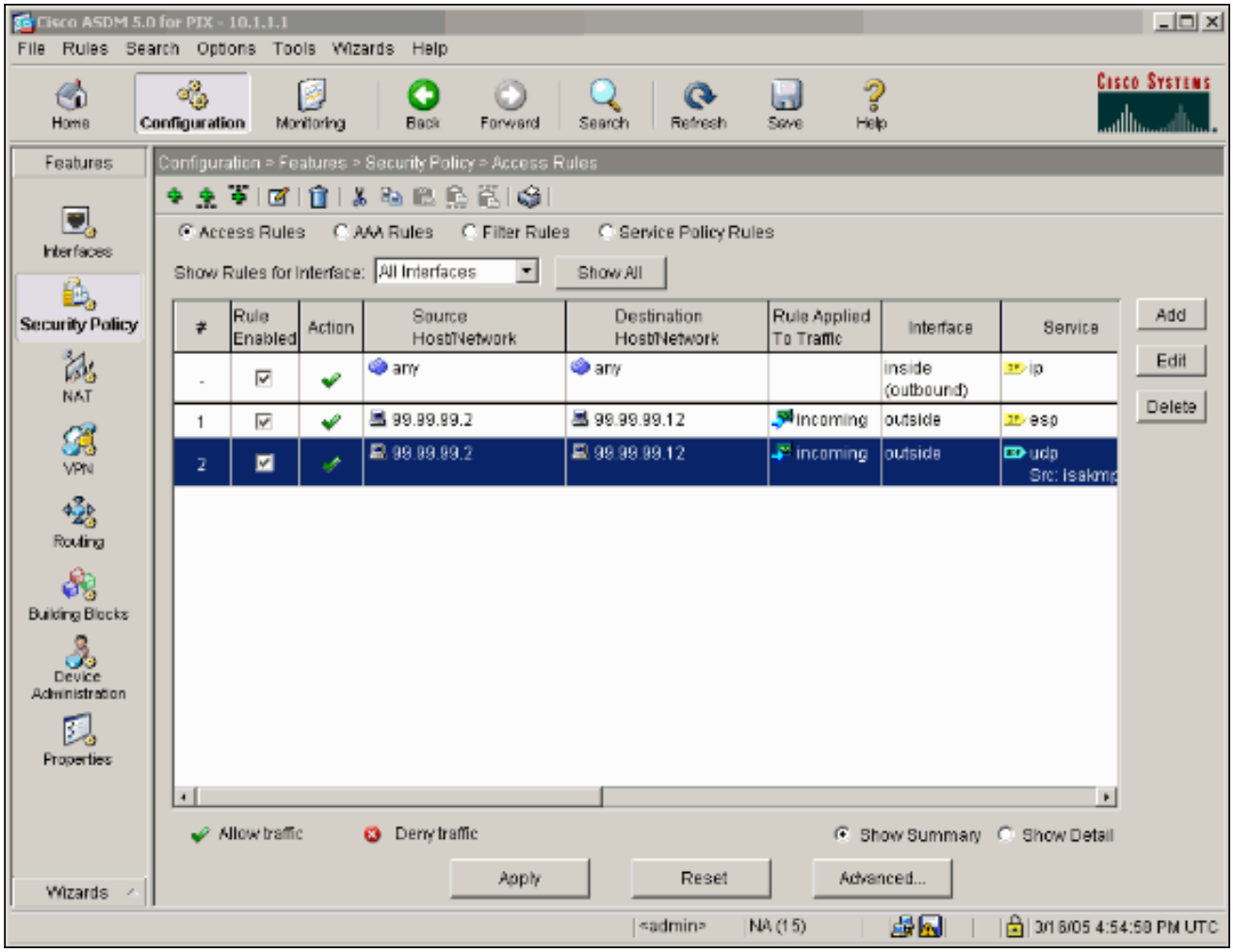
24. El tecleo **agrega** para permitir que el tráfico ISAKMP y la **AUTORIZACIÓN del** tecleo para continuar.



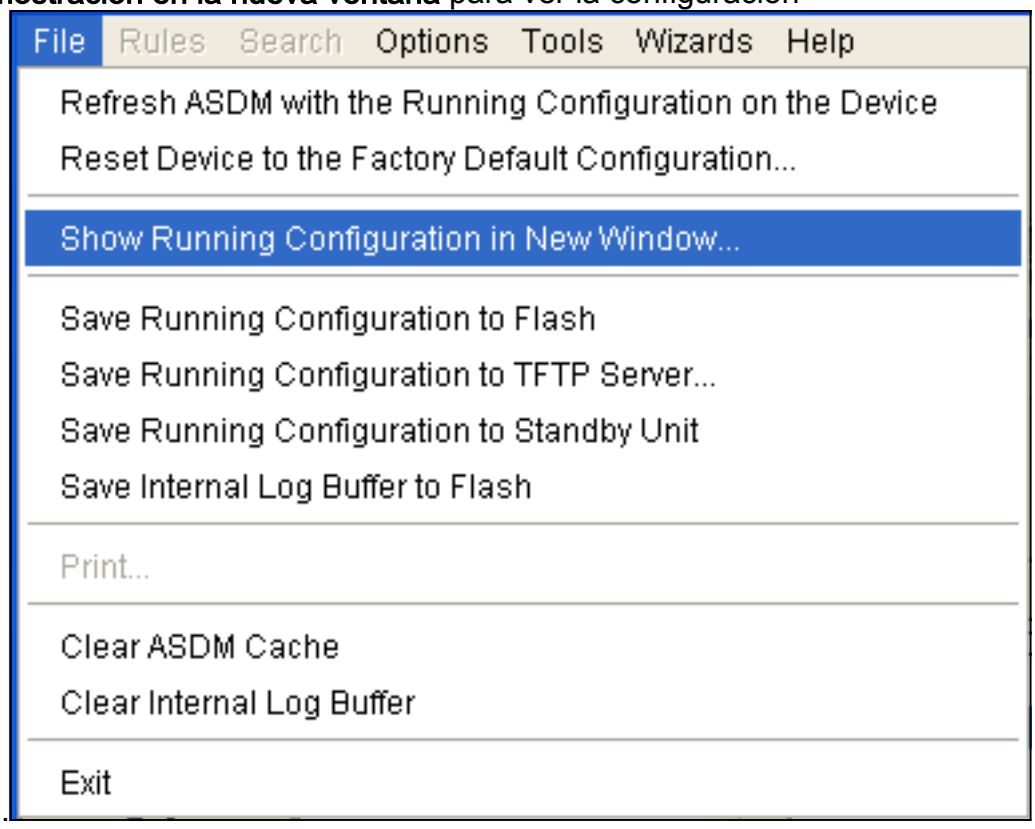
25. El tecleo **agrega** para permitir que el tráfico del puerto 4500 UDP para el NAT-T y la **AUTORIZACIÓN del** tecleo para continuar.



26. El tecleo **se aplica** para validar la configuración de la interfaz. La configuración también consigue avanzada sobre el
PIX.



27. La configuración es completa ahora.Elija la **configuración corriente del archivo > de la demostración en la nueva ventana** para ver la configuración CLI.



[Configuración de Firewall de PIX]

Firewall PIX

```
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
```

Dispositivo de seguridad PIX y configuración del MPF (Marco de políticas modular)

En vez de la lista de acceso, utilice el comando inspect IPSec-paso-por en el MPF (Marco de políticas modular) para pasar el tráfico IPSec a través de los dispositivos de seguridad del PIX/ASA.

Este examen se configura para abrir los agujeritos para el tráfico ESP. Se permiten todos los flujos de datos ESP cuando existe un flujo delantero, y no hay límite en la cantidad máxima de conexiones que puede ser permitida. AH no se permite. El tiempo de espera ocioso predeterminado para los flujos de datos ESP por abandono se fija a 10 minutos. Este examen se puede aplicar en todas las ubicaciones que otros exámenes pueden ser aplicados, que incluye los modos de la clase y de comando match. El paso del IPSec con la Inspección de la aplicación proporciona el traversal conveniente del tráfico ESP (protocolo IP 50) asociado a una conexión del puerto 500 IKE UDP. Evita la configuración de la lista de acceso muy larga para permitir el tráfico ESP y también proporciona la Seguridad con el descanso y las conexiones máximas.

Utilice el clase-**mapa**, el directiva-**mapa**, y los **comandos service-policy** para definir una clase de tráfico, aplicar el comando inspect a la clase, y aplicar la directiva a una o más interfaces. Cuando está habilitada, la **inspección IPSec-paso-por el** comando permite el tráfico ilimitado ESP con un descanso de 10 minutos, que no es configurable. Se permite el tráfico NAT y NON-NAT.

```
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 la fase 2.
- show crypto isakmp sa — Muestra las asociaciones de seguridad de la fase 1.
- **active del show crypto engine connections** — Muestra los paquetes encriptados y desencriptados.

Troubleshooting

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

Comandos de Troubleshooting para router IPSec

Nota: Consulte información importante en los comandos debug antes de ejecutar los comandos debug.

- debug crypto engine - Muestra el tráfico cifrado.
- **IPSec del debug crypto** — Visualiza los IPSec Negotiations de la fase 2.
- **isakmp del debug crypto** — Visualiza las negociaciones del Internet Security Association and Key Management Protocol (ISAKMP) de la fase 1.

Verificación de las asociaciones de seguridad

- clear crypto isakmp - Elimina las asociaciones de seguridad de Intercambio de claves de Internet (IKE).
- **clear crypto ipsec sa** — Asociaciones de seguridad IPSec de los claros.

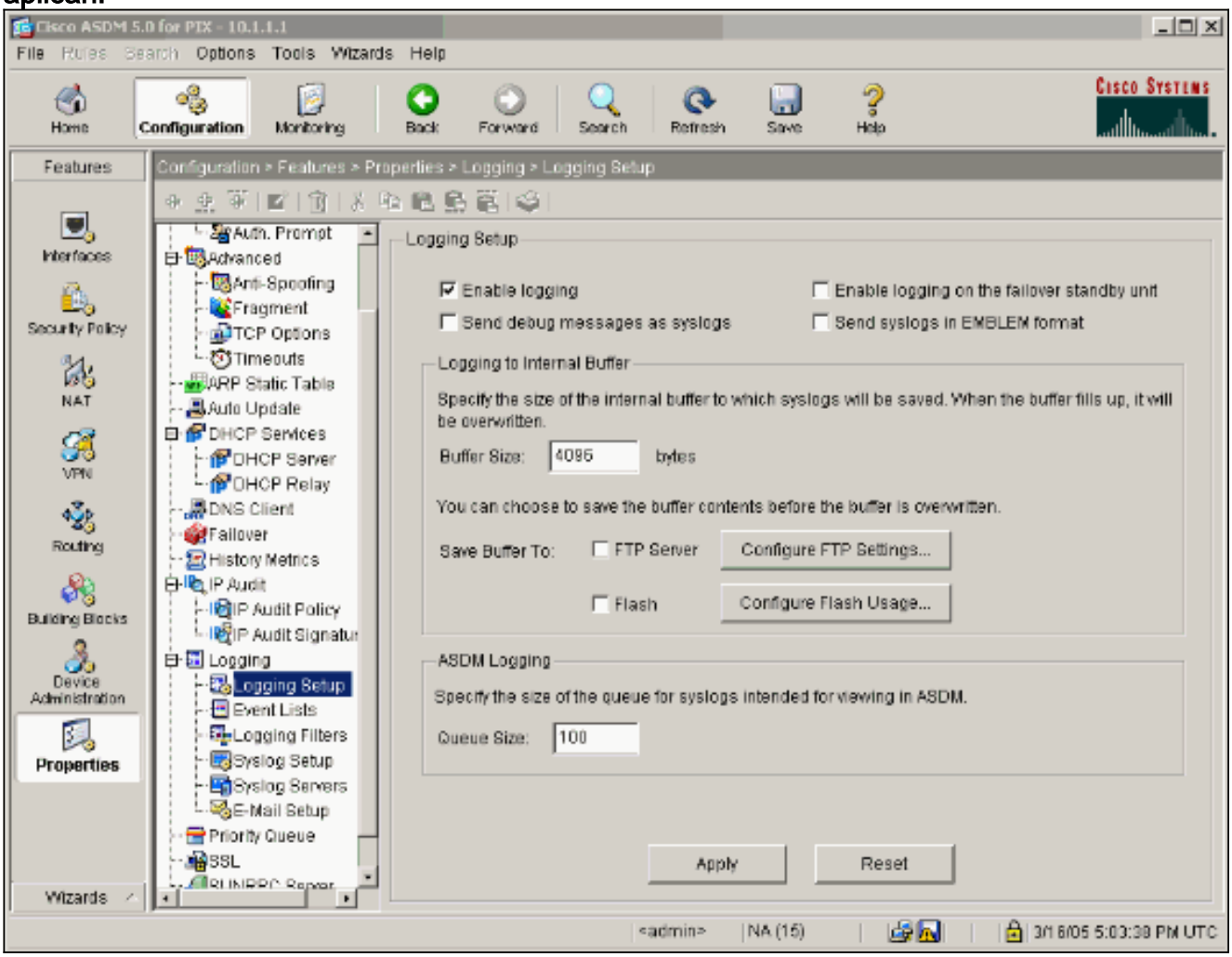
Comandos de Troubleshooting para el PIX

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

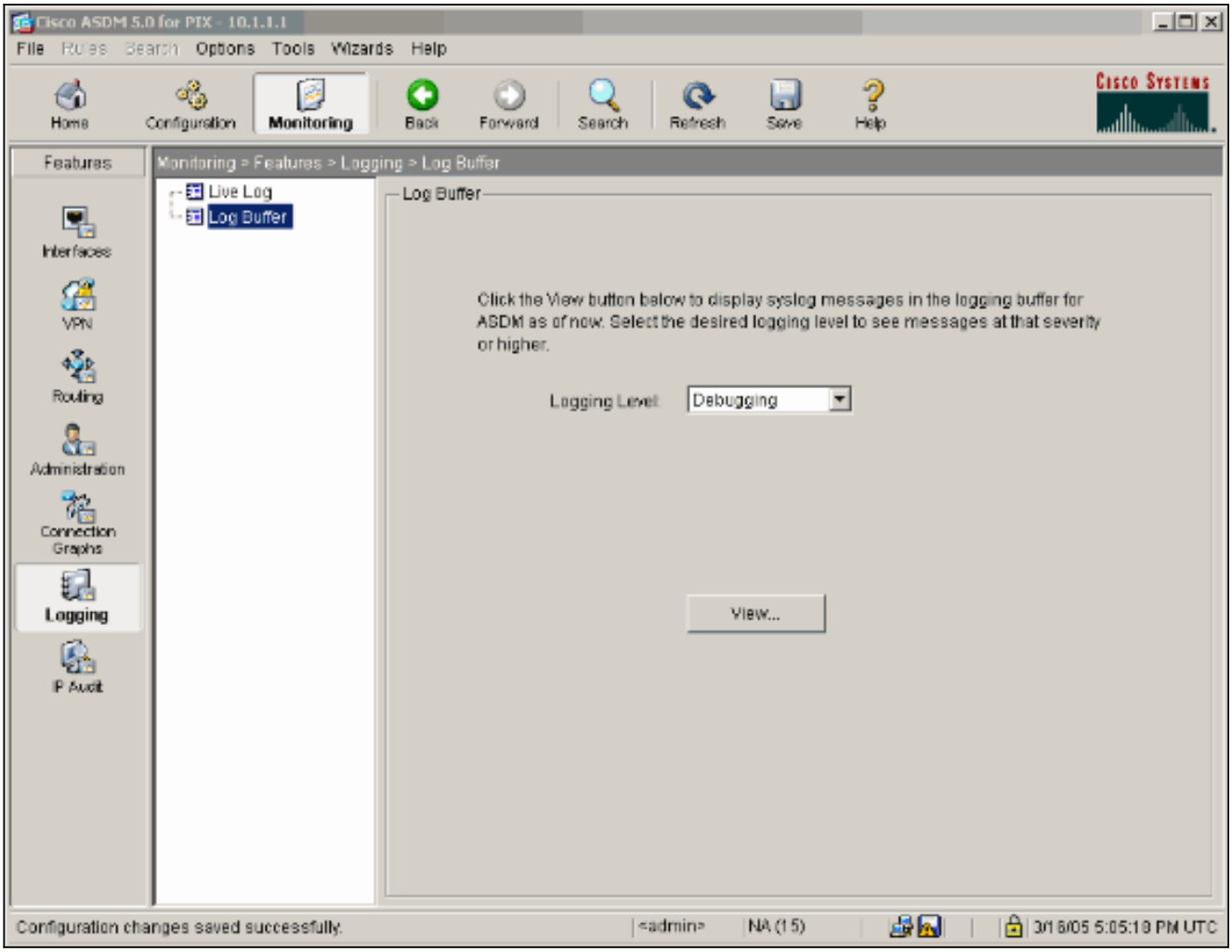
Nota: Consulte información importante en los comandos debug antes de ejecutar los comandos debug.

- logging buffer debugging—Muestra las conexiones que se establecen y las que se deniegan a los hosts que atraviesan el PIX. La información se salva en el búfer del registro PIX y la salida se puede considerar usando el **comando show log**.
- El ASDM se puede utilizar para habilitar el registro y también para ver los registros tal y como se muestra en de estos pasos.

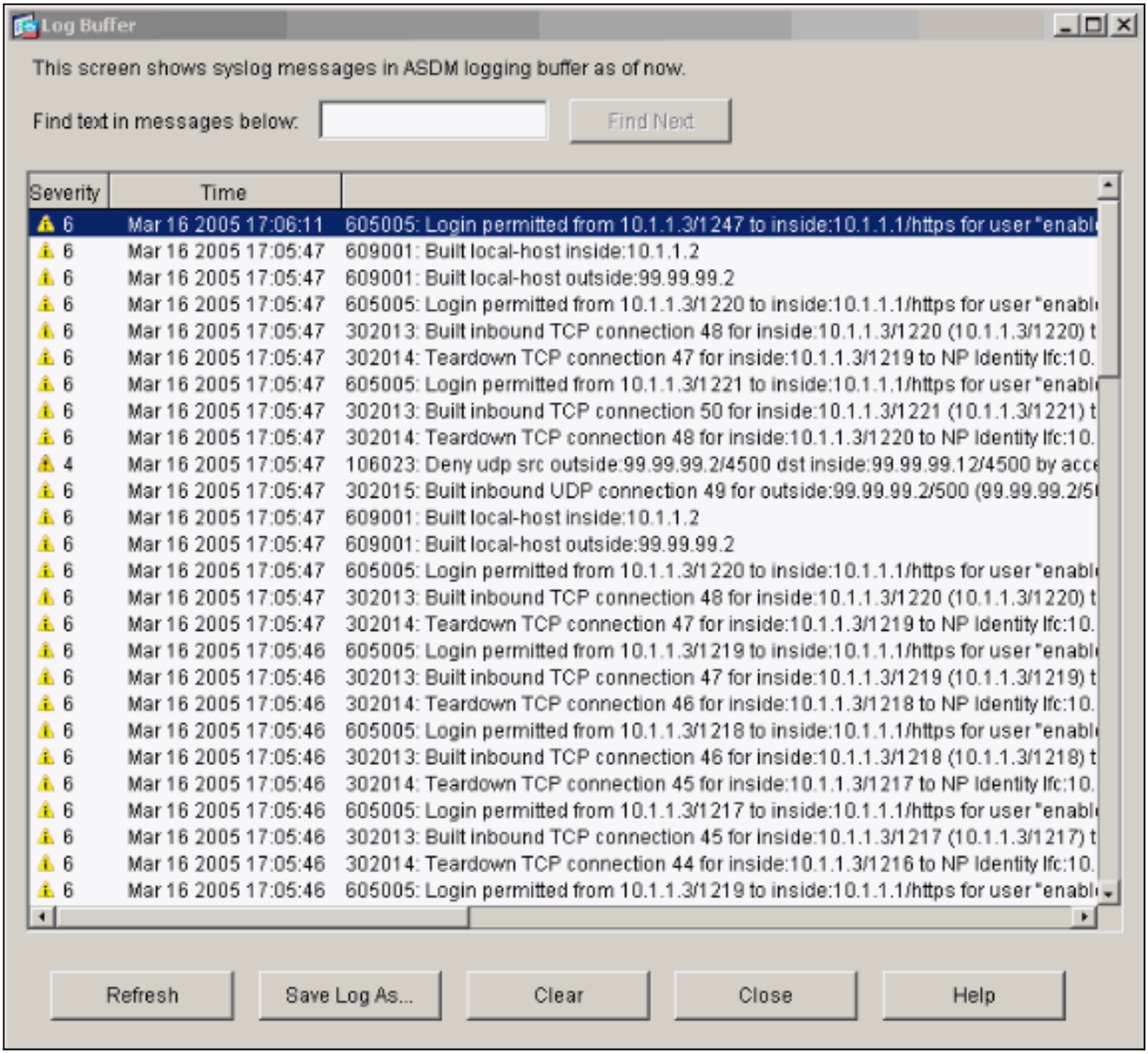
1. Elija la **configuración > las propiedades > el registro > el registro puesto > registro del permiso** y después haga clic **se aplican.**



2. Elija la **supervisión > el registro > el búfer del registro > en el nivel de registro > memoria intermedia de registro**, después haga clic la **visión**.



Éste es un ejemplo del búfer del registro.



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