# PIX/ASA (versie 7.x en later) IPsec VPN-tunnelheid met configuratievoorbeeld voor netwerkadresomzetting

## Inhoud



## Inleiding

Deze voorbeeldconfiguratie demonstreert een IPsec VPN-tunnel door een firewall die netwerkadresomzetting (NAT) uitvoert. **Deze configuratie werkt niet met poortadresomzetting (PAT) als u Cisco IOS®-softwarereleases eerder dan en zonder 12.2(13)T gebruikt.** Dit type configuratie kan worden gebruikt voor tunnelIP-verkeer. Deze configuratie kan niet worden gebruikt om verkeer te versleutelen dat niet door een firewall gaat, zoals IPX of routingupdates. Generic Routing Encapsulation (GRE)-tunneling is een passender keuze. In dit voorbeeld zijn de routers van Cisco 2621 en 3660 de IPsec-tunnelendpoints die zich bij twee particuliere netwerken aansluiten, met circuits of toegangscontrolelijsten (ACL's) op de PIX-tussenin om het IPsec-verkeer toe te staan.

**Opmerking:** NAT is een één-op-één adresvertaling, niet om te worden verward met PAT, wat een groot aantal (binnen de firewall) is-op-één vertaling. Raadpleeg voor meer informatie over de werking en configuratie van NAT het controleren van NAT-werking en fundamentele NAT-probleemoplossing of de manier waarop NAT werkt.

**Opmerking:** IPsec met PAT werkt mogelijk niet goed omdat het externe tunneleindapparaat geen

meerdere tunnels vanaf één IP-adres kan verwerken. Neem contact op met uw verkoper om te bepalen of de tunneleindapparatuur met PAT werkt. Daarnaast kan in Cisco IOS-softwarerelease 12.2(13)T en later de NAT Transparency-functie worden gebruikt voor PAT. Raadpleeg voor meer informatie IPSec NAT Transparency. Raadpleeg Ondersteuning voor IPSec ESP via NAT om meer te weten te komen over deze functies in Cisco IOS-softwarerelease 12.2(13)T en hoger.

**N.B.:** Voordat u een case opent met Cisco Technical Support, raadpleegt u NAT vaak gestelde vragen, die veel antwoorden bevat op gebruikelijke vragen.

Raadpleeg de modus Een IPSec-tunneldoor een firewall met NAT voor meer informatie over de manier waarop u IPsec-tunnels kunt configureren met NAT in PIX versie 6.x en eerder.

# Voorwaarden

## Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 12.0.7.T (tot maar niet met Cisco IOS-softwarerelease 12.2(13)T)Raadpleeg voor meer recente versies IPSec NAT Transparency.
- Cisco 2621 router
- Cisco 3660 router
- Cisco PIX 500 Series security applicatie die 7.x en hoger werkt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

## Verwante producten

Dit document kan ook worden gebruikt met Cisco 5500 Series adaptieve security applicatie (ASA) met softwareversie 7.x en hoger.

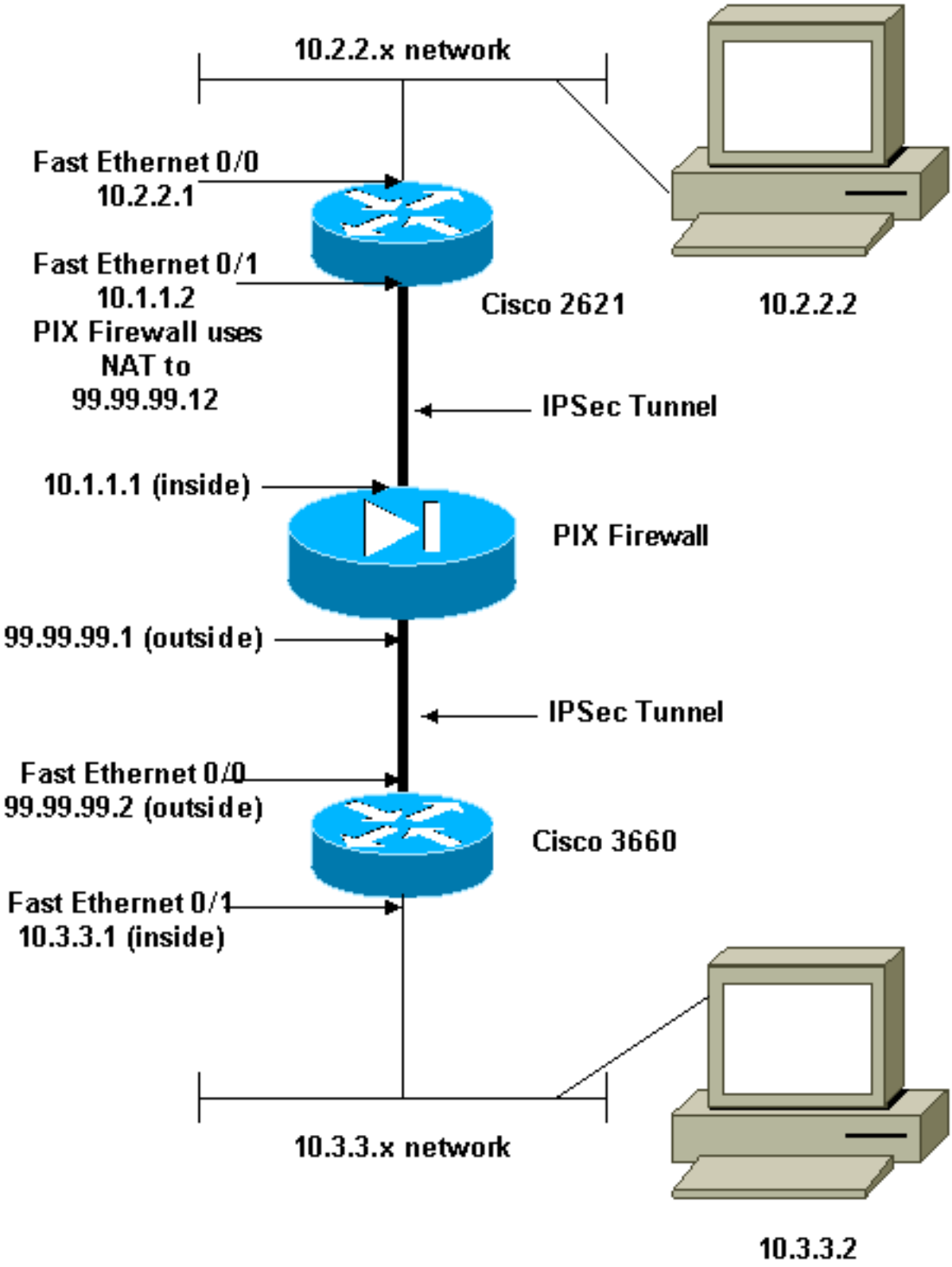
# Configureren

In dit gedeelte wordt de informatie gegeven die u kunt gebruiken om de functies te configureren die in dit document worden beschreven.

**N.B.:** Om extra informatie over de opdrachten te vinden die in dit document worden gebruikt, gebruikt u het Opdrachtprotocol (alleen geregistreerde klanten).

## Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:




## Configuraties

Dit document gebruikt deze configuraties:

- Cisco 2621-configuratie

- Cisco 3660-configuratie
- Configuratie van PIX-security applicatie en toegangslijstConfiguratie van geavanceerde Security Devices Manager GUI (ASDM)CLI-configuratie (Opdracht Line Interface)
- Configuratie van PIX security applicatie en MPF (modulair beleidskader)

**Cisco 2621 router**

```
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 router

```
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
```

## Configuratie van PIX-security applicatie en toegangslijst

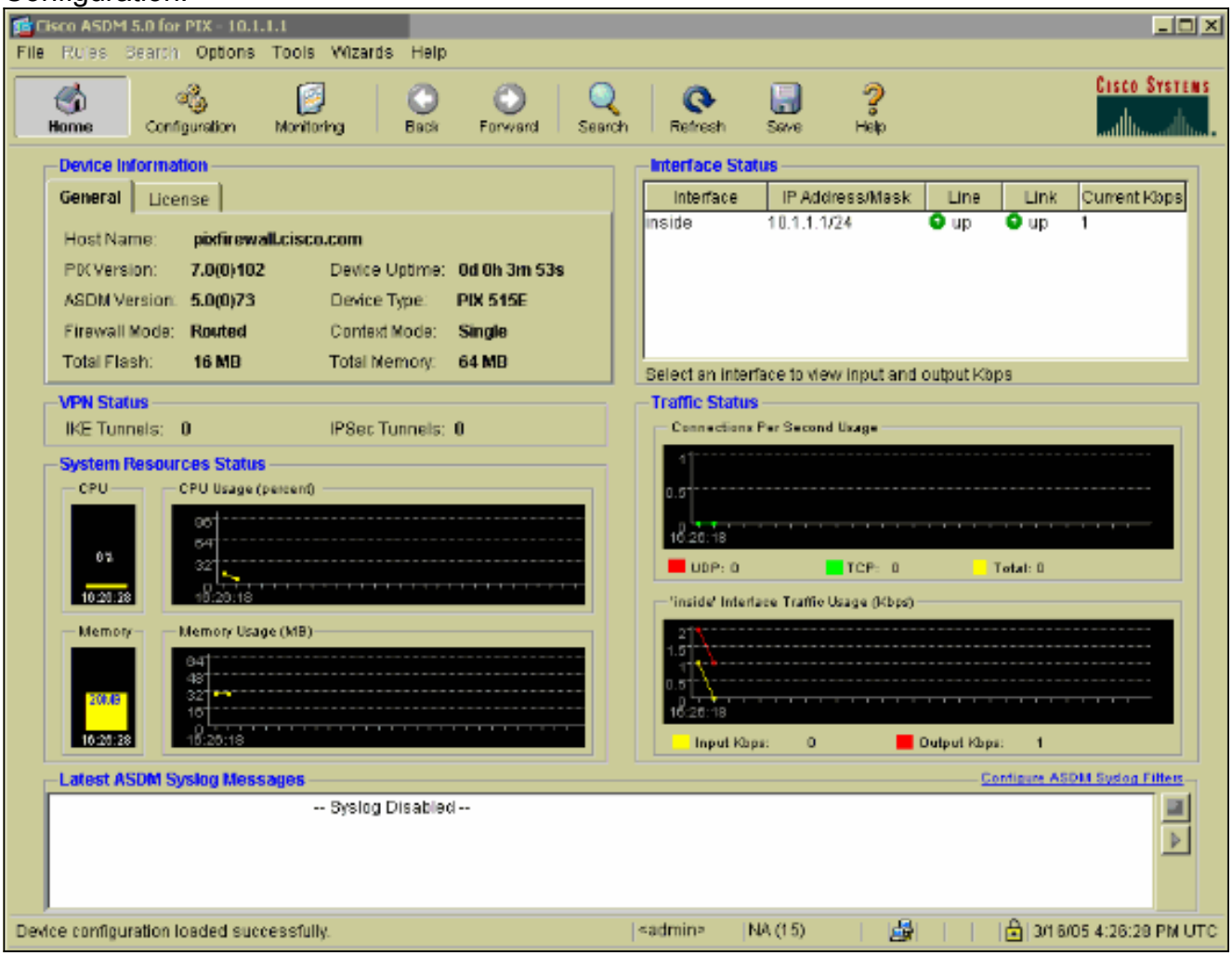
### ASDM 5.0-configuratie

Voltooi deze stappen om PIX-firewall, versie 7.0, te configureren met ASDM.

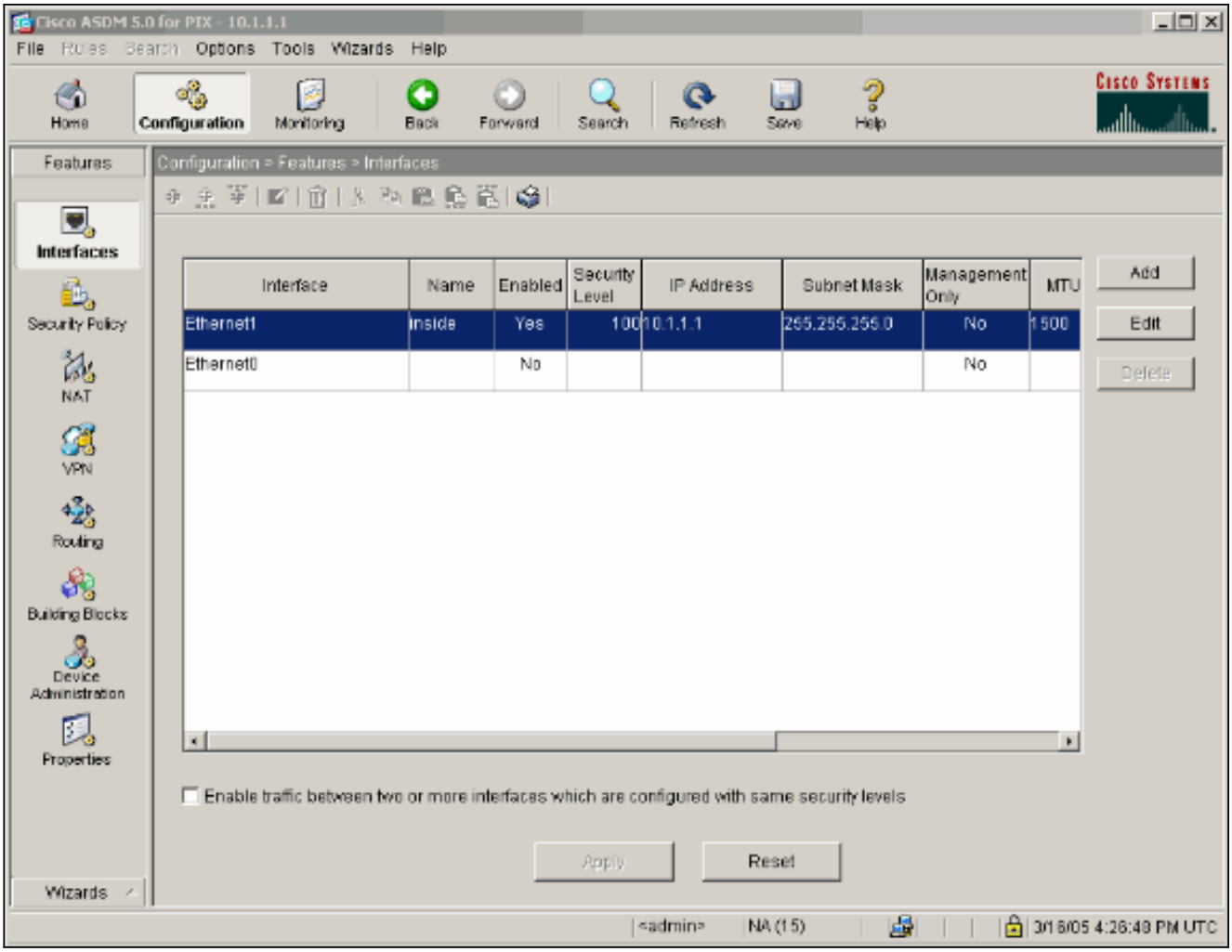
1. console in de PIX. Gebruik vanuit een geautoriseerde configuratie de interactieve aanwijzingen om **Advanced Security Apparaat Manager GUI (ASDM)** mogelijk te maken voor het beheer van de PIX vanaf het werkstation 10.1.1.3.
2. Open vanuit Workstation 10.1.1.3 een webbrowser en gebruik ADSM (in dit voorbeeld

https://10.1.1.1).

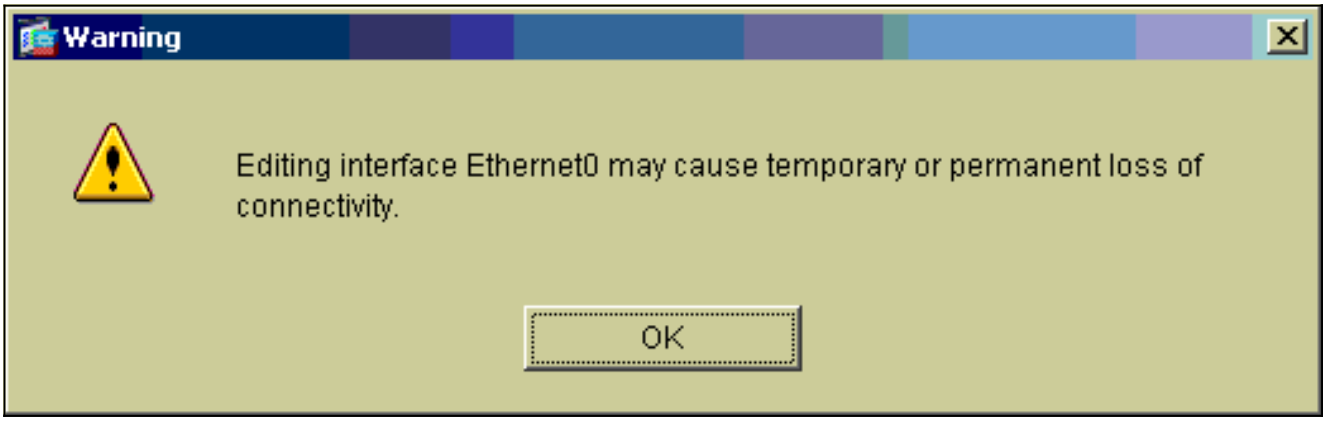
3. Kies **ja** op de certificaatvragen en inloggen met het wachtwoord voor het inschakelen zoals ingesteld in de PIX-firewall ASDM Bootstrap-configuratie.
4. Als dit de eerste keer is dat ASDM op de PC wordt uitgevoerd, wordt u gevraagd of u ASDM Launcher wilt gebruiken of ASDM als Java-app gebruikt.In dit voorbeeld wordt ASDM Launcher geselecteerd en installeert deze aanwijzingen.
5. Ga verder naar het ASDM Home-venster en selecteer het tabblad Configuration.



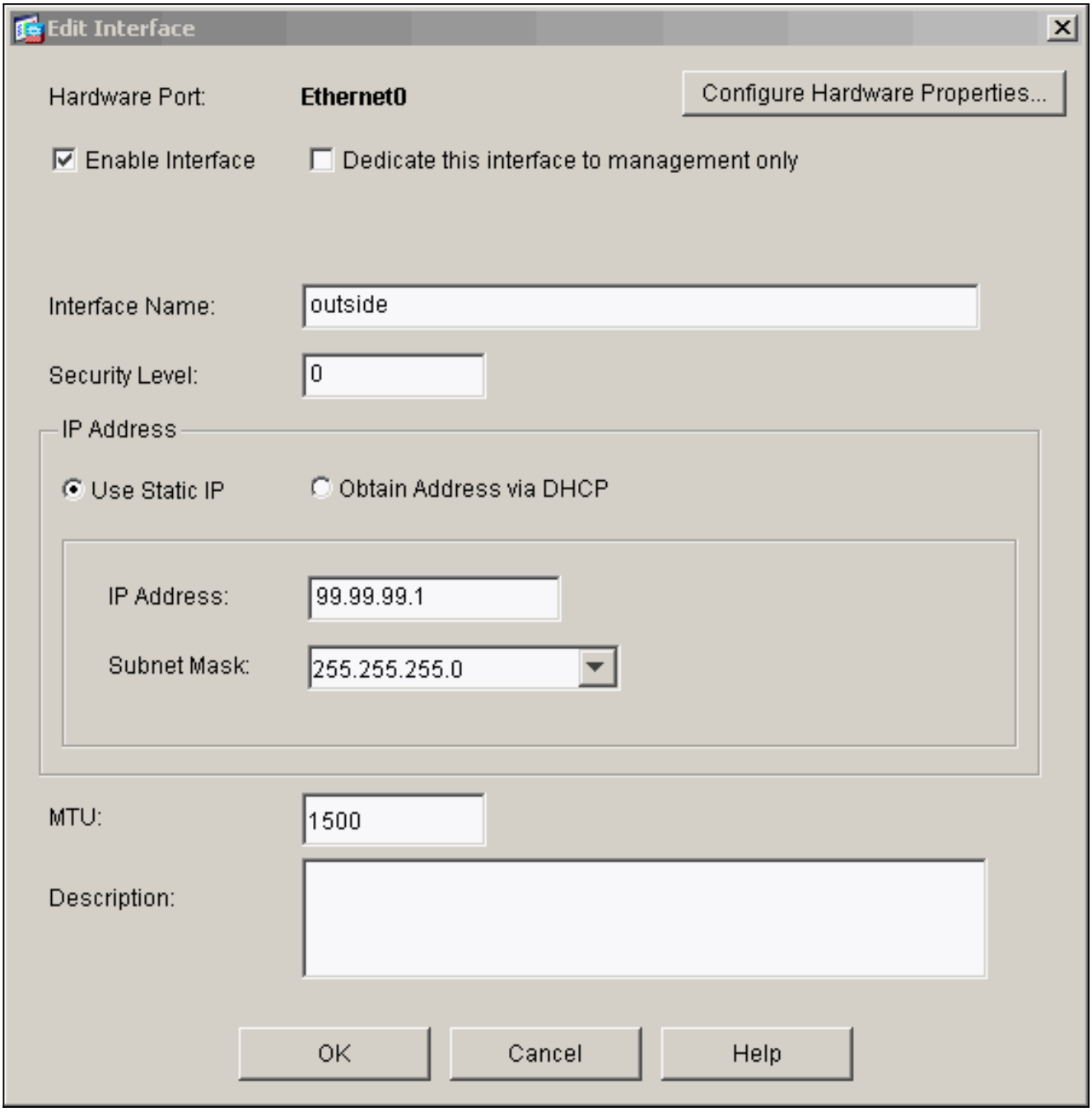

6. Markeer de **Ethernet 0-interface** en klik op **Bewerken** om de externe interface te configureren.



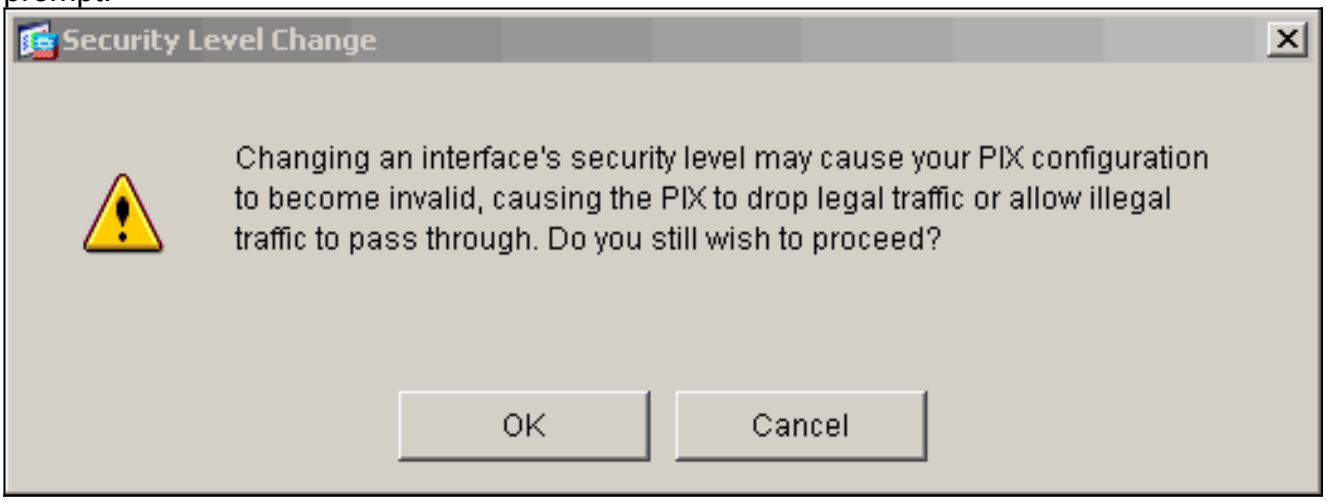

7. Klik op **OK** in de Password-interface.



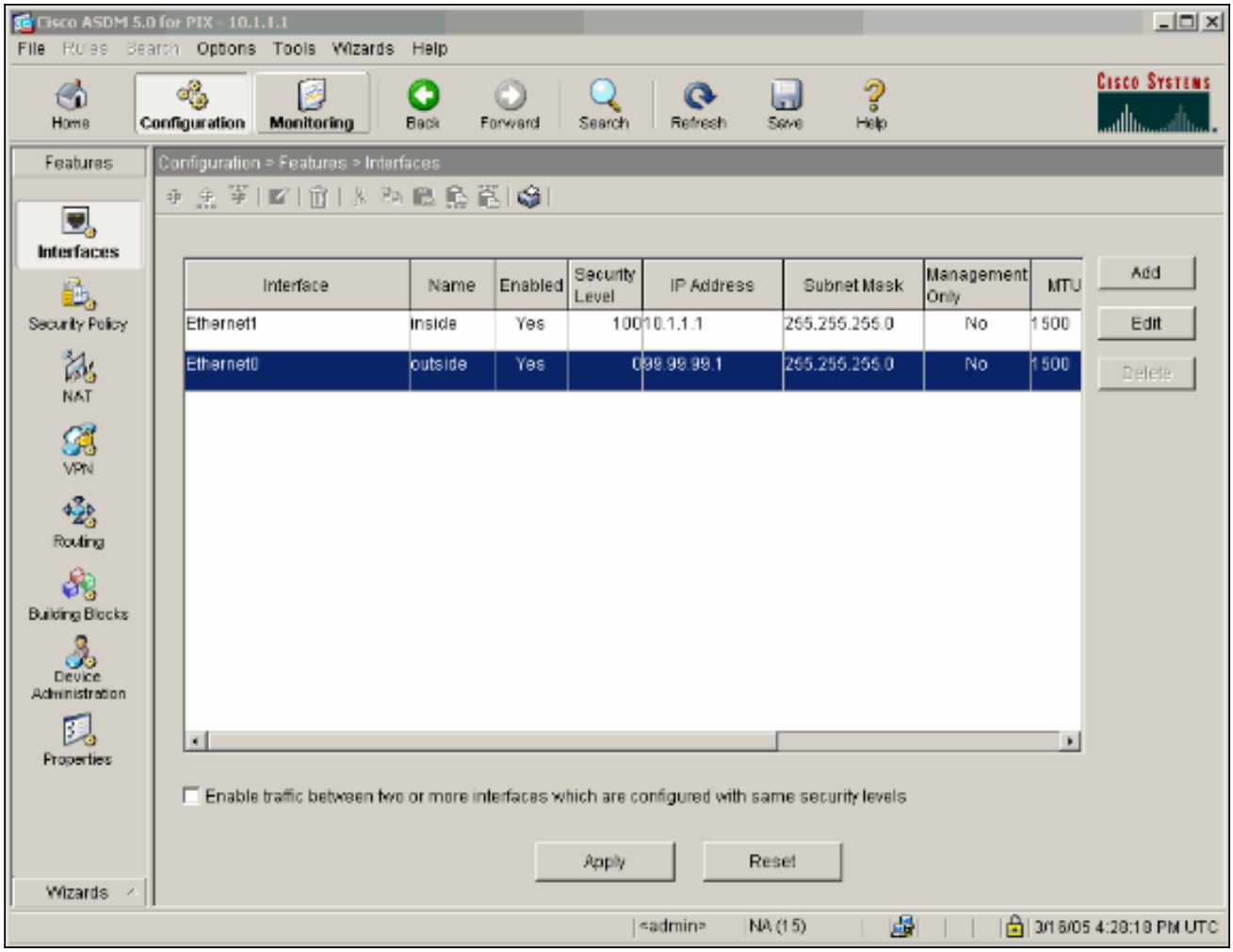

8. Voer de interfacedetails in en klik op **OK** wanneer u klaar bent.



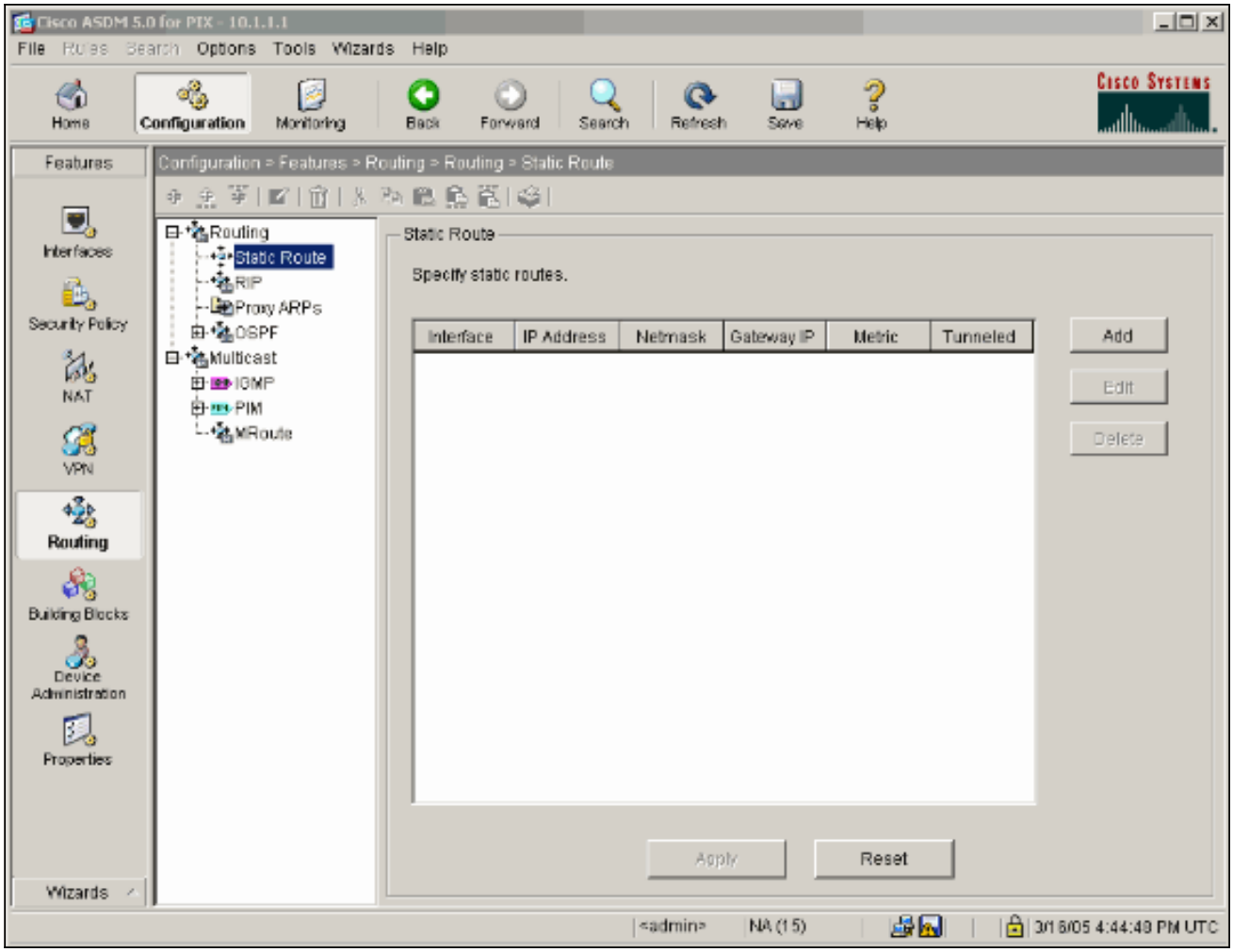

9. Klik op **OK** in de Password-prompt.



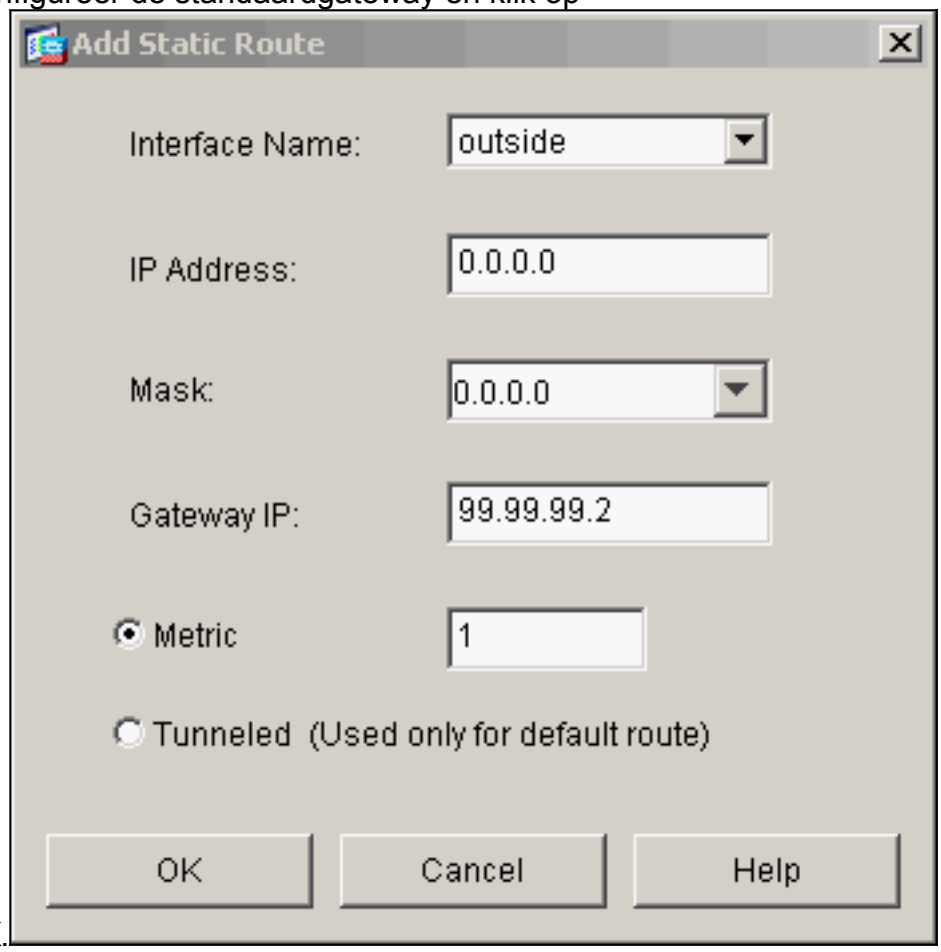

10. Klik op **Toepassen** om de interfaceconfiguratie te aanvaarden. De configuratie wordt ook op de PIX geduwd. Dit voorbeeld gebruikt statische routes.




11. Klik op **Routing** onder het tabblad Functies, markeer **statische route** en klik op **Toevoegen**.

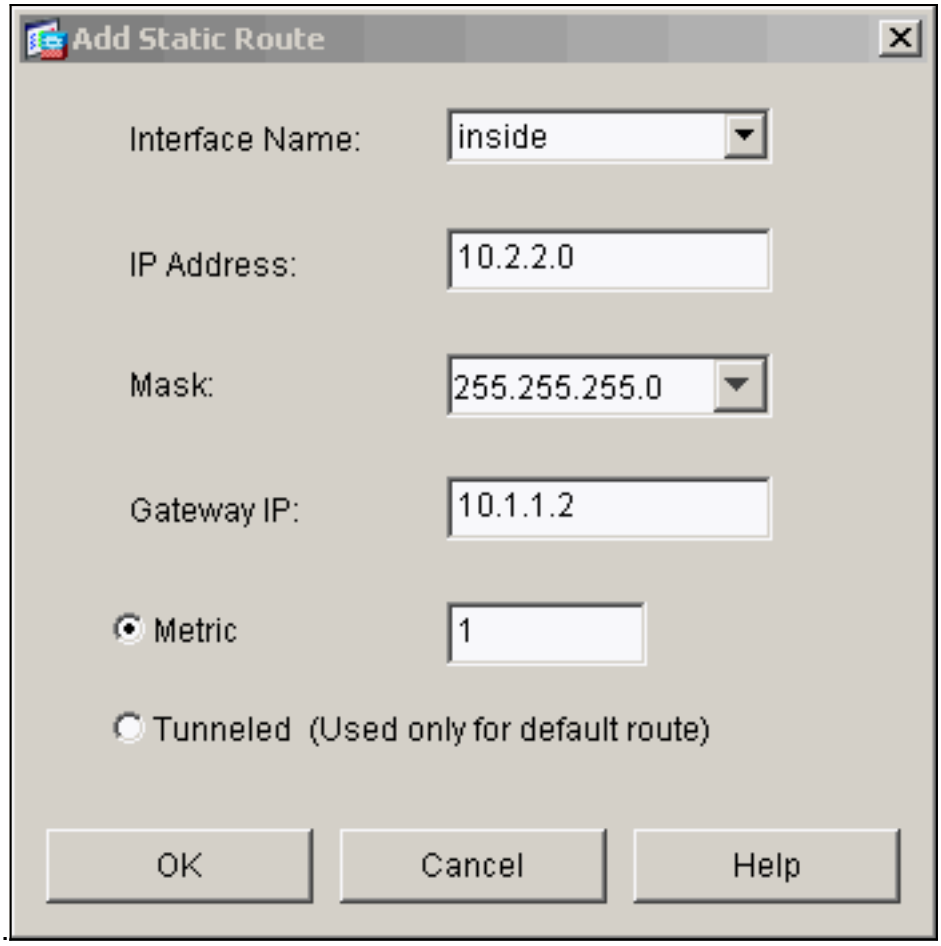



12. Configureer de standaardgateway en klik op



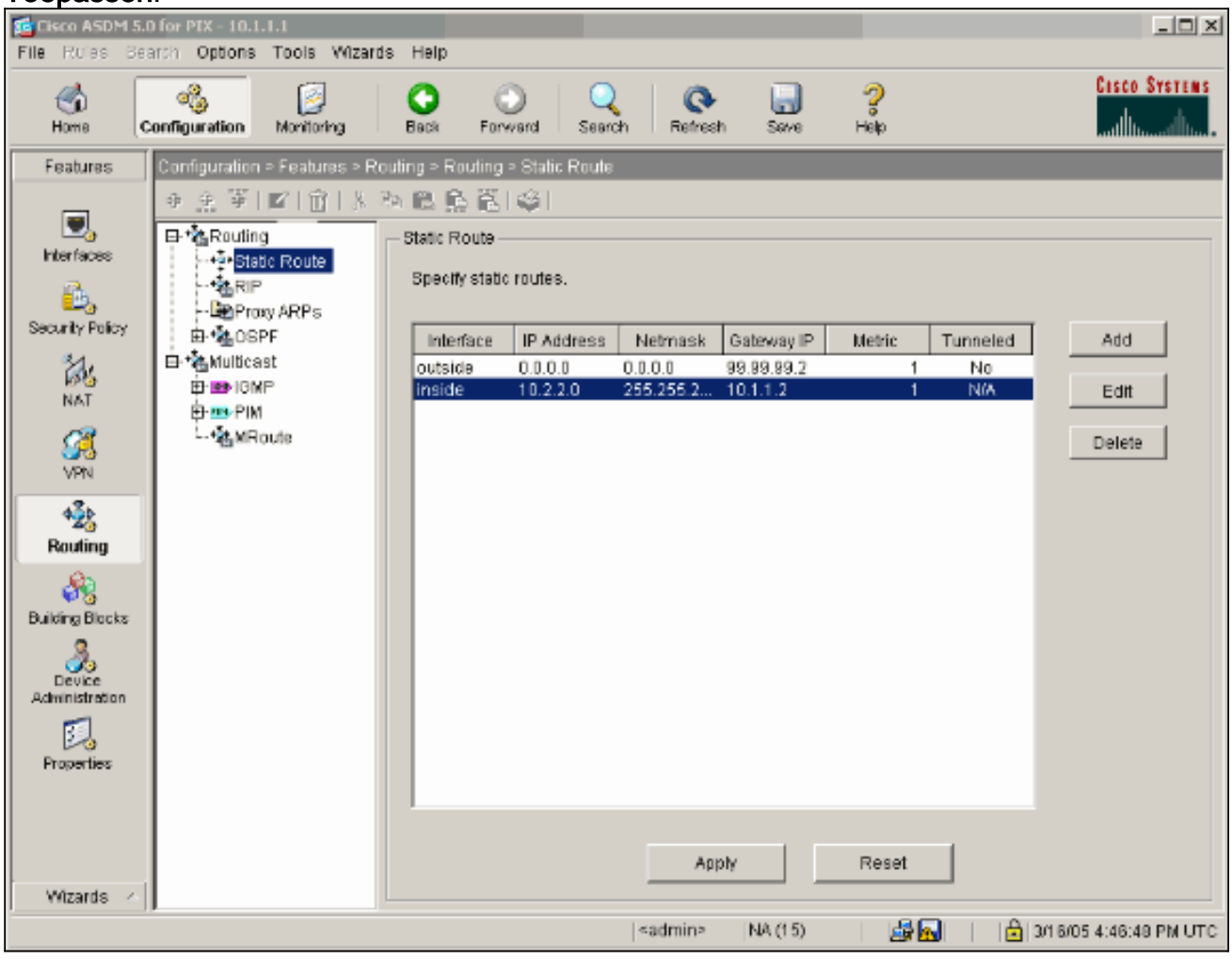

OK.

13. Klik op **Add** en voeg de routes aan de binnennetwerken

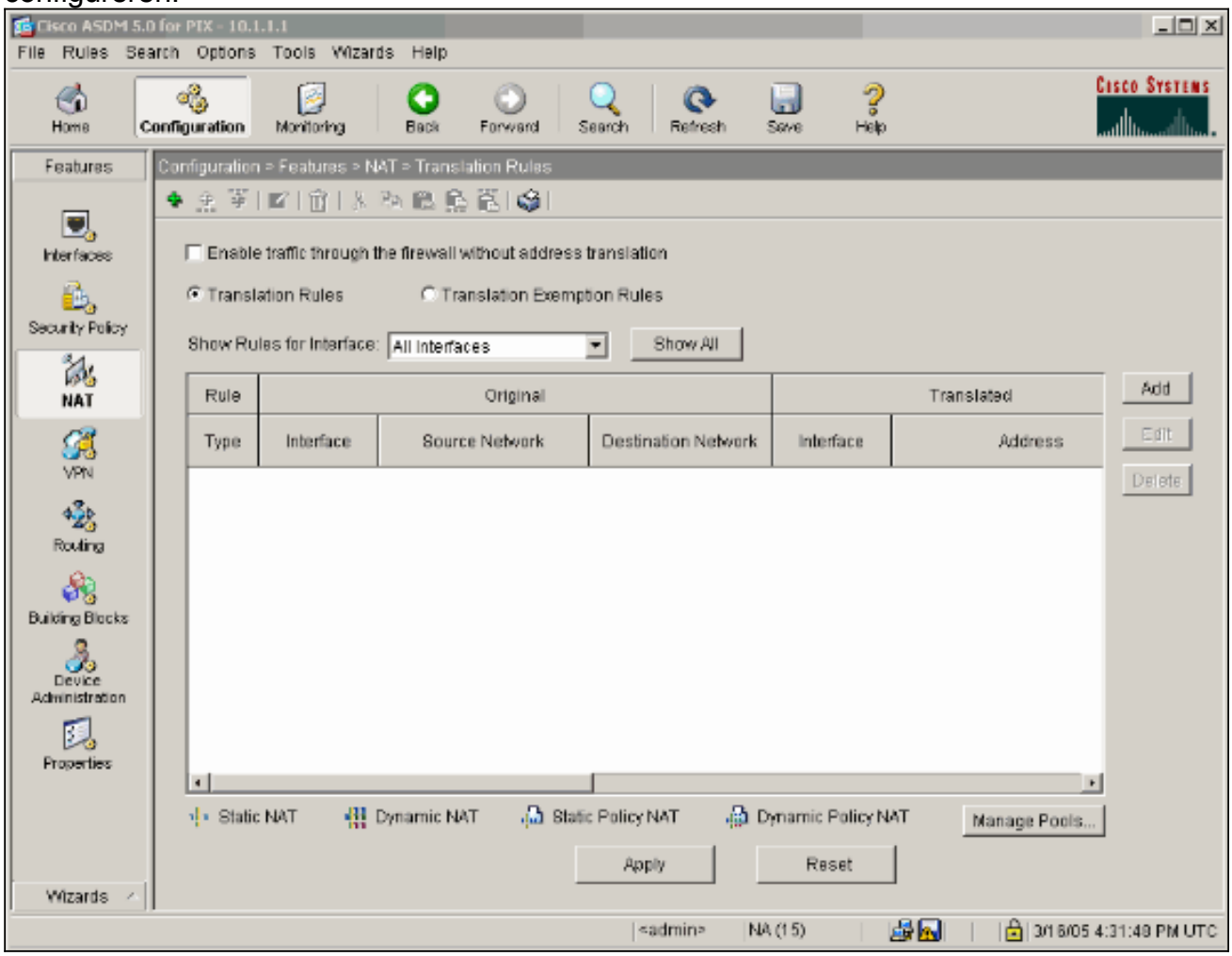



toe.

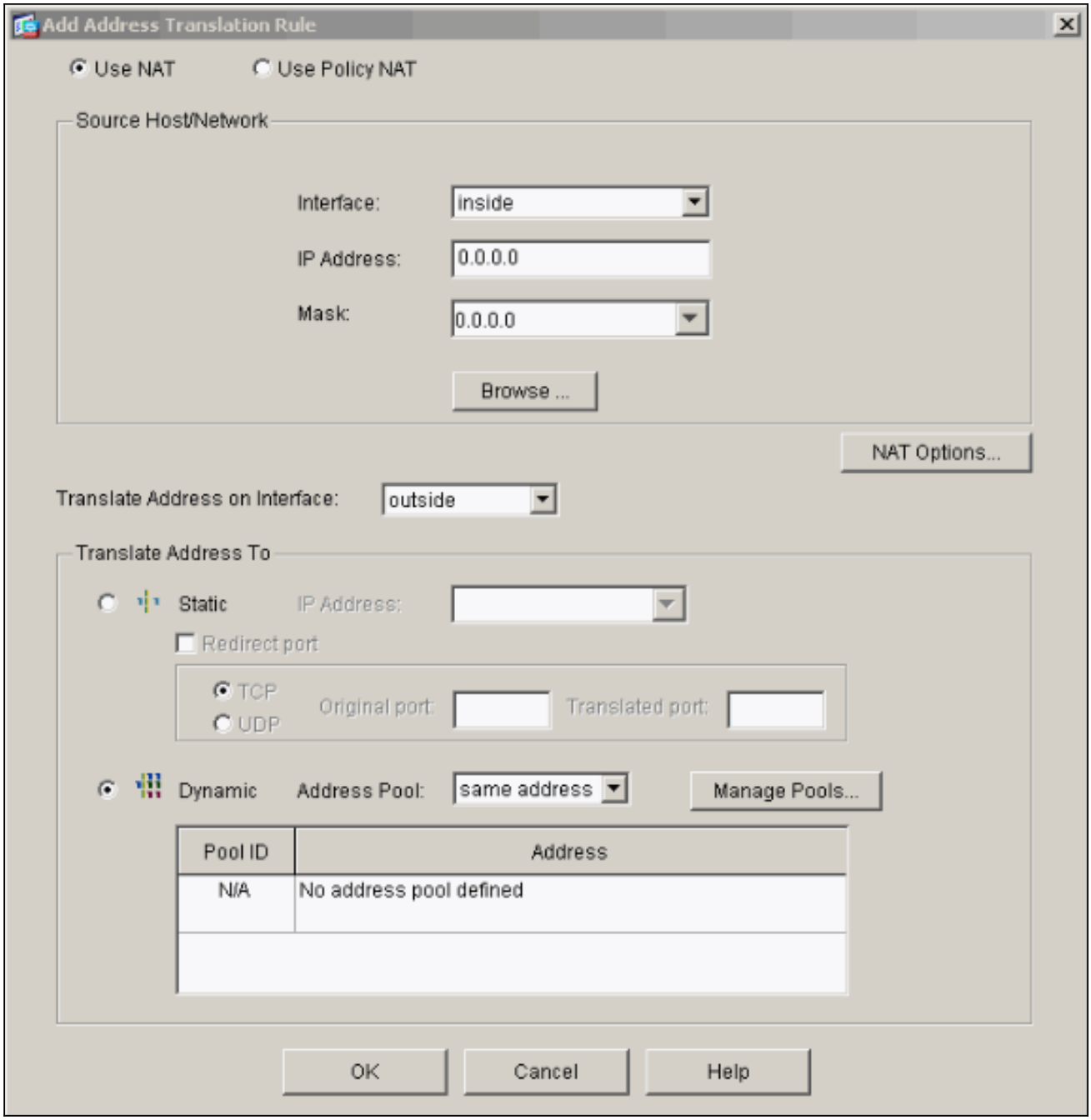
14. Bevestig dat de juiste routes zijn geconfigureerd en klik op **Toepassen**.



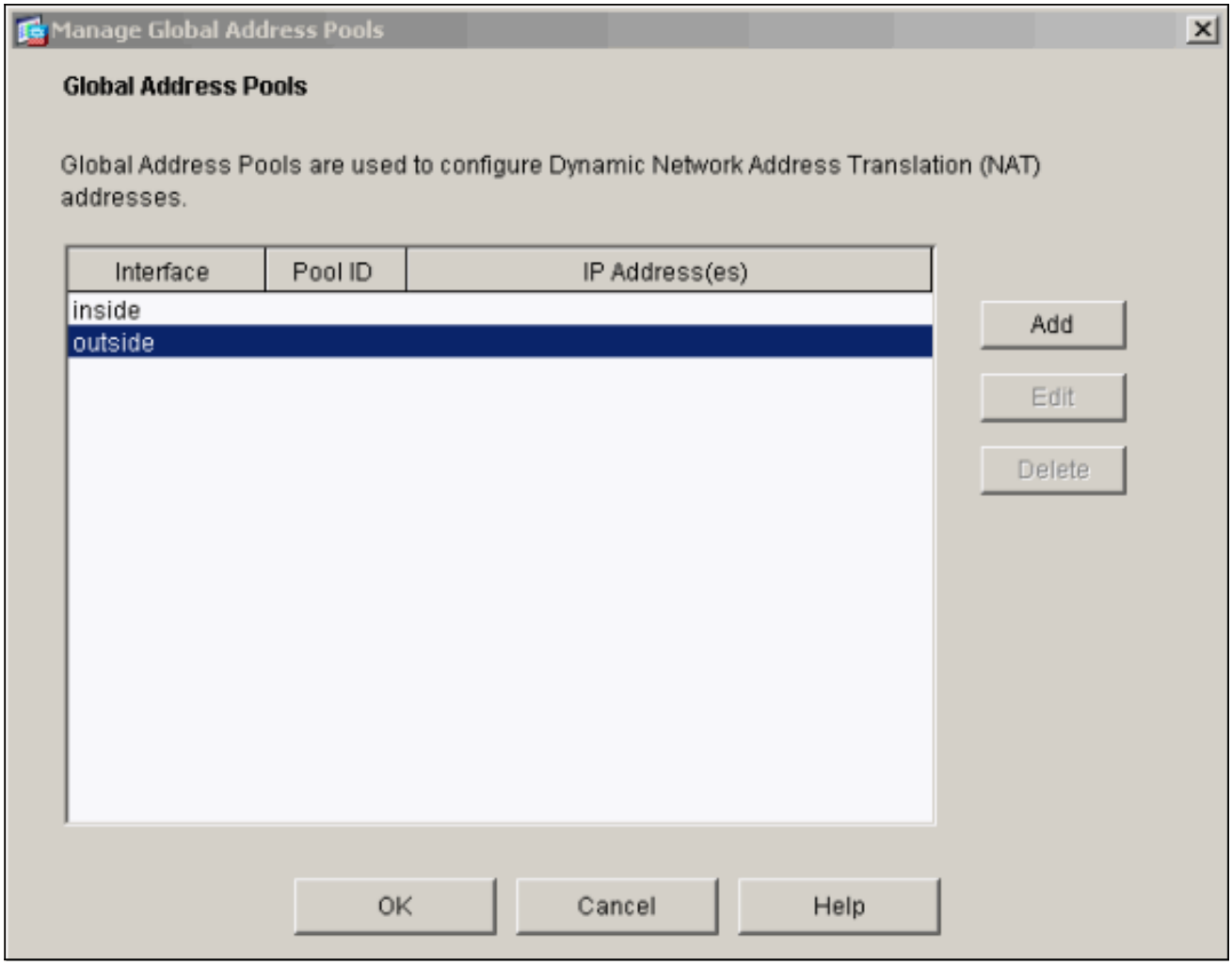
15. In dit voorbeeld wordt NAT gebruikt. Verwijder de controle in het vakje voor **Schakel verkeer door de firewall in zonder adresomzetting** en klik op **Add** om de NAT-regel te configureren.



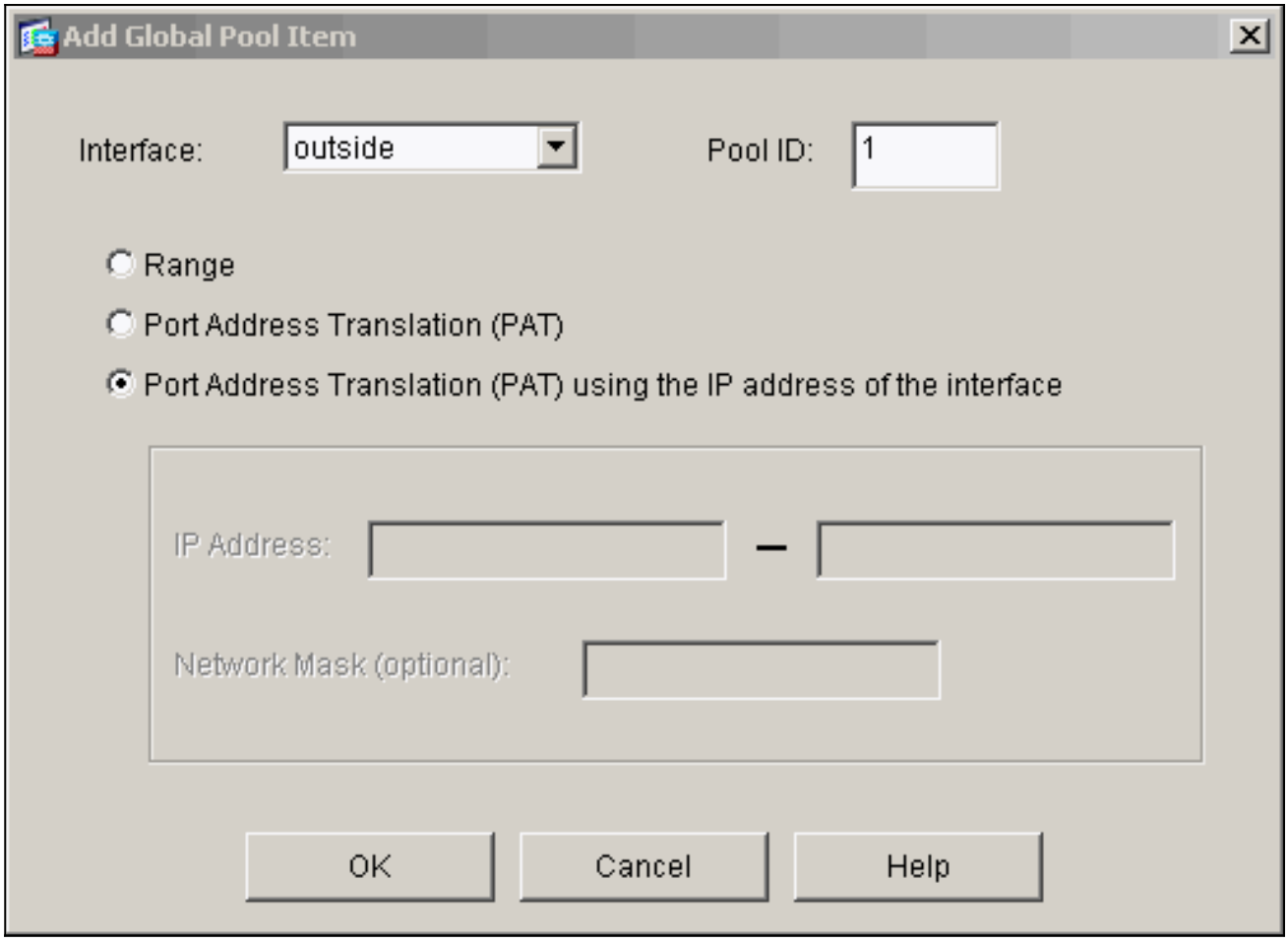

16. Configureer het bronnetwerk (dit voorbeeld wordt gebruikt). Klik vervolgens op **Pools beheren** om het PAT te definiëren.



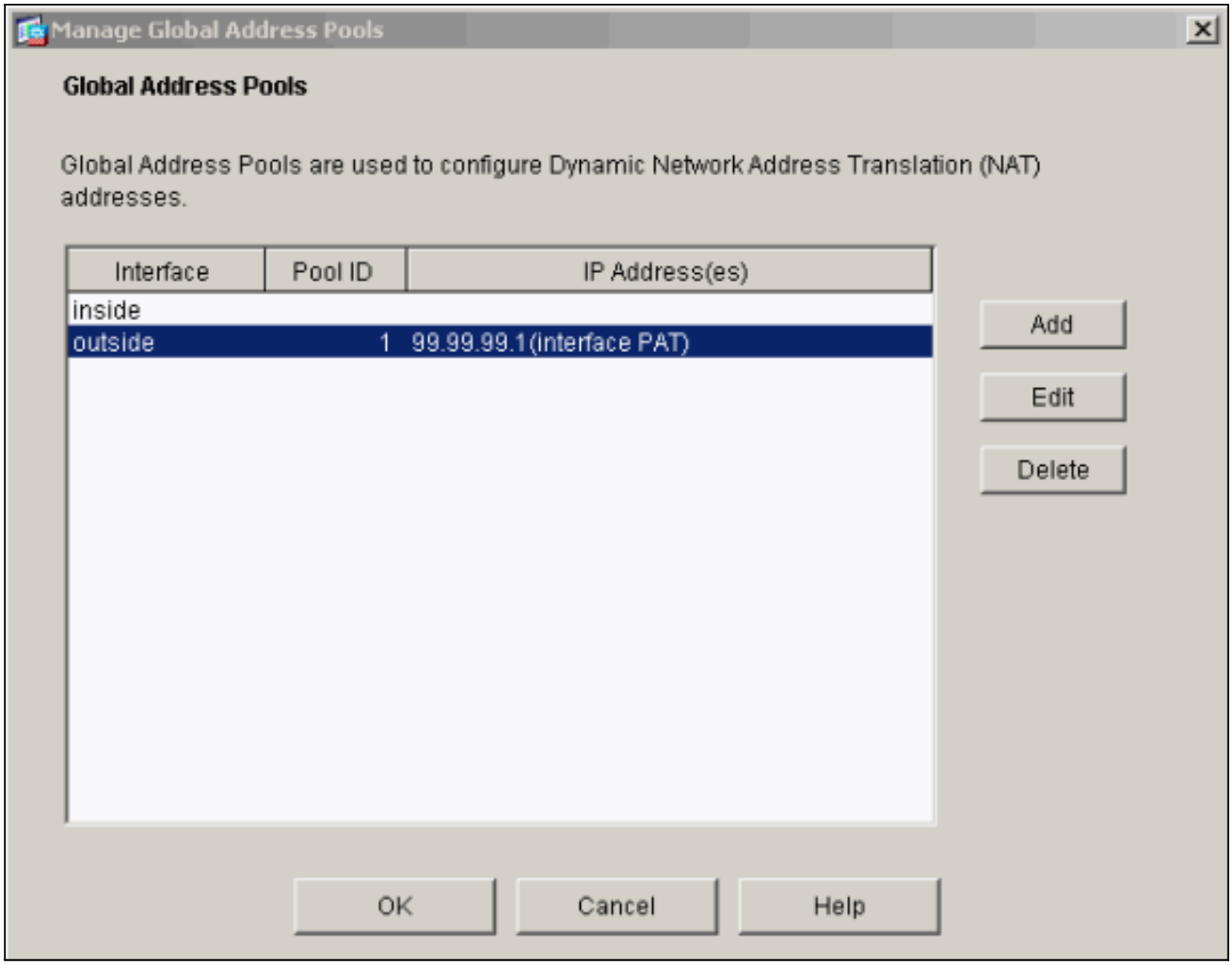

17. Selecteer de **externe** interface en klik op **Add**.



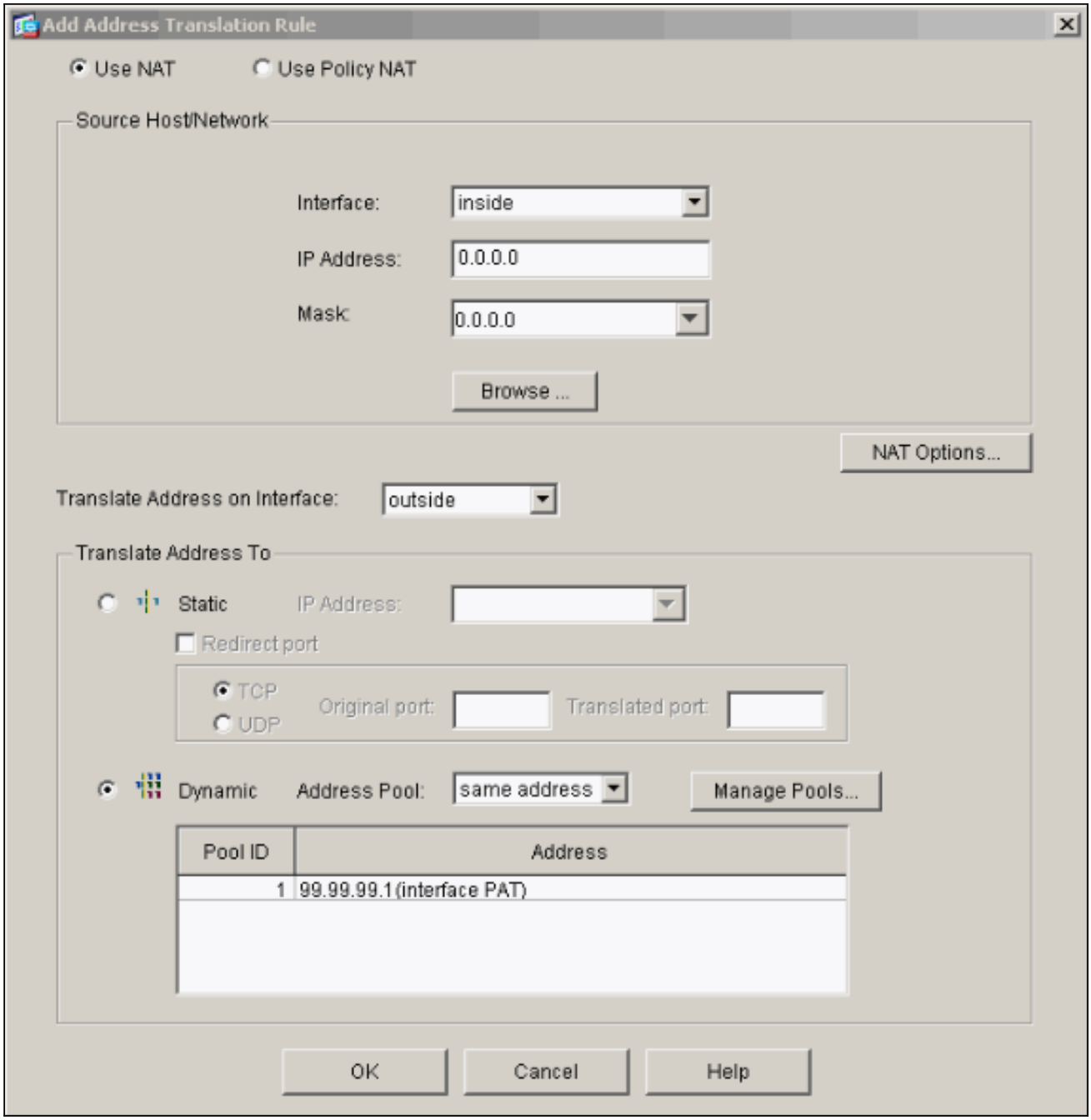

Dit voorbeeld gebruikt een PAT die het IP adres van de interface gebruikt.



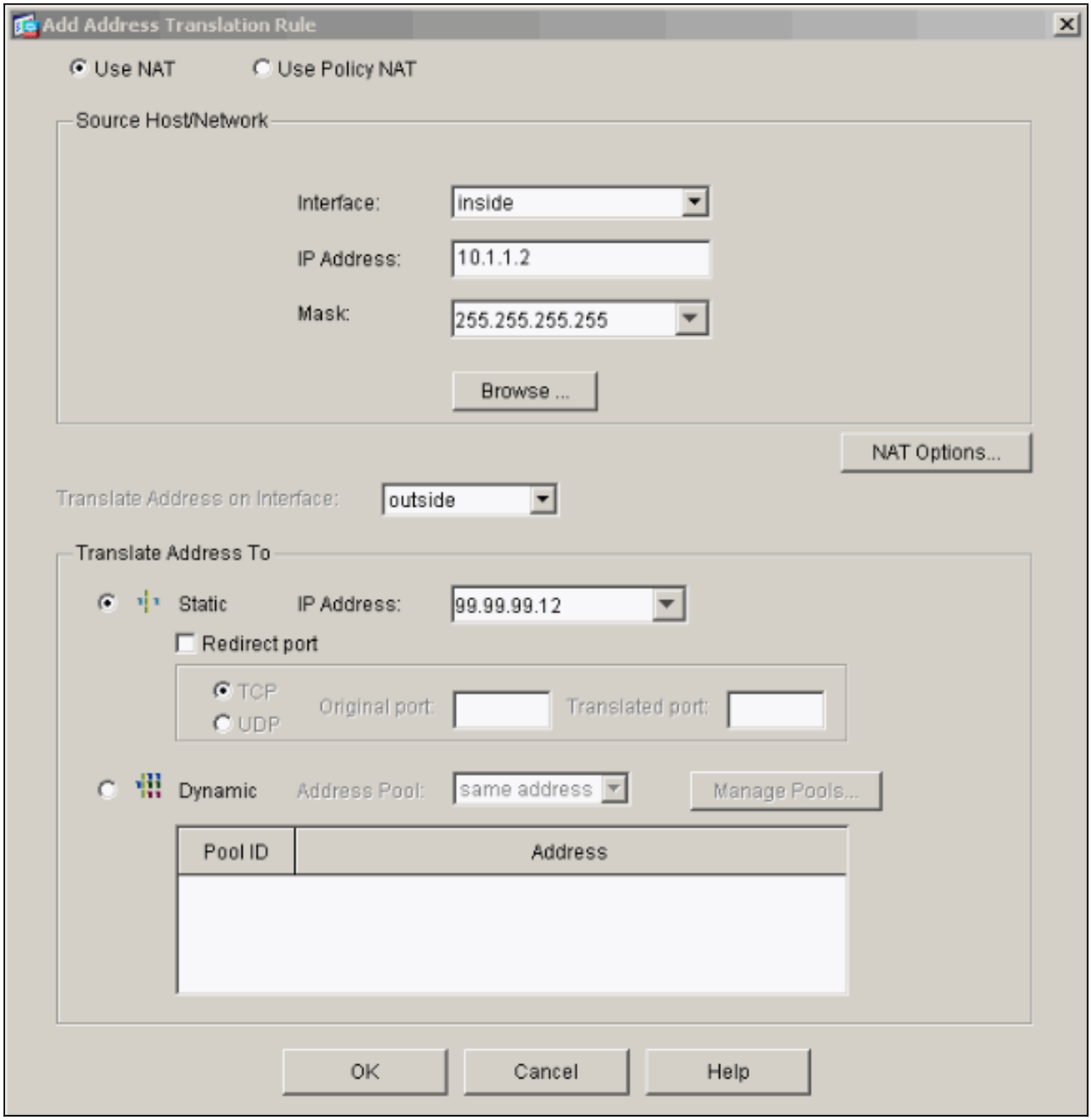

18. Klik op **OK** wanneer de PAT is ingesteld.



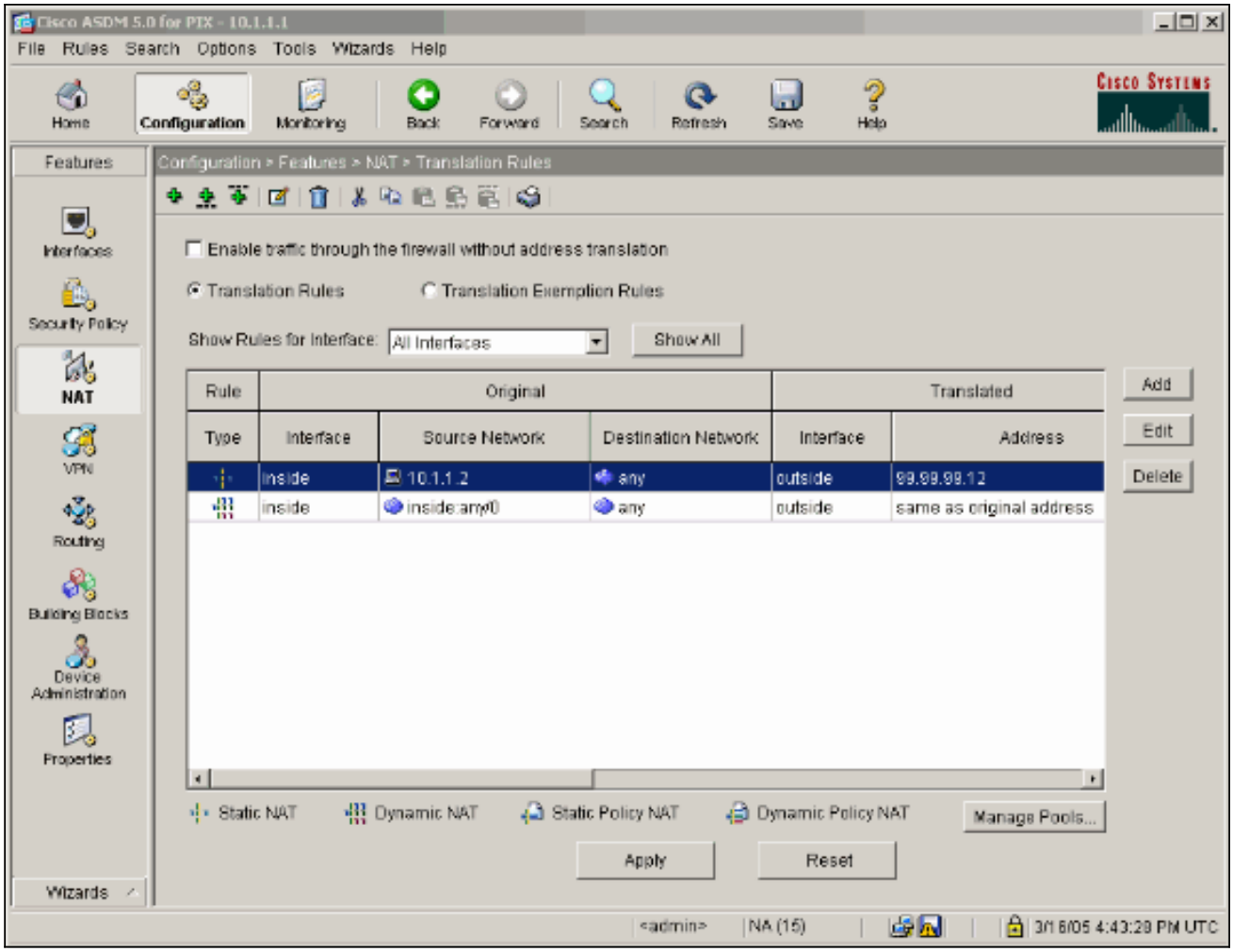

19. Klik op **Add** om de statische vertaling te configureren.



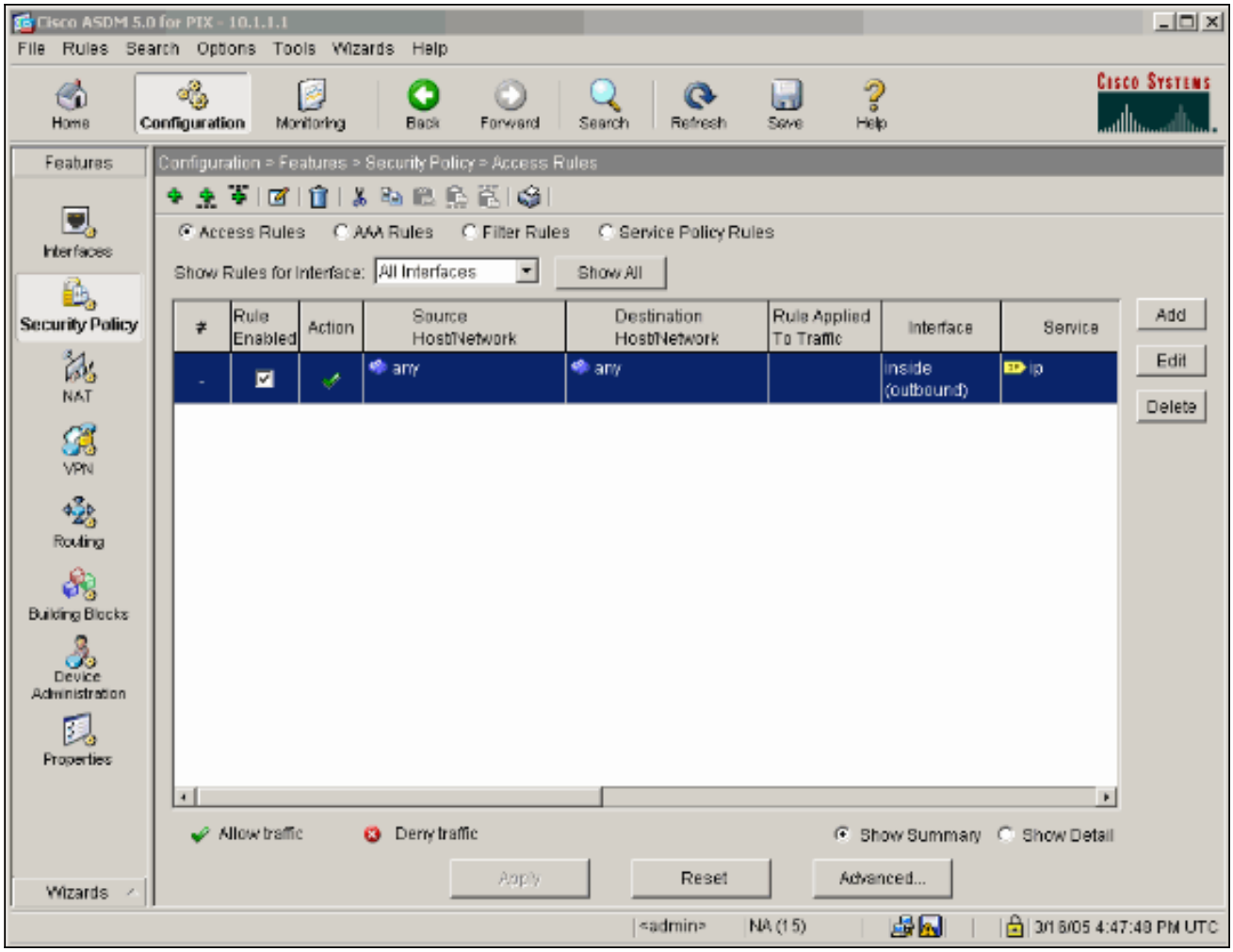

20. Selecteer **binnen** op de vervolgkeuzelijst Interface en voer vervolgens IP-adres **10.1.1.2**, subnetmasker **255.255.255.255 in**, kies **Statisch** en kies in het IP-adresveldtype buiten adres **99.99.12. klaar**
**zijn.**



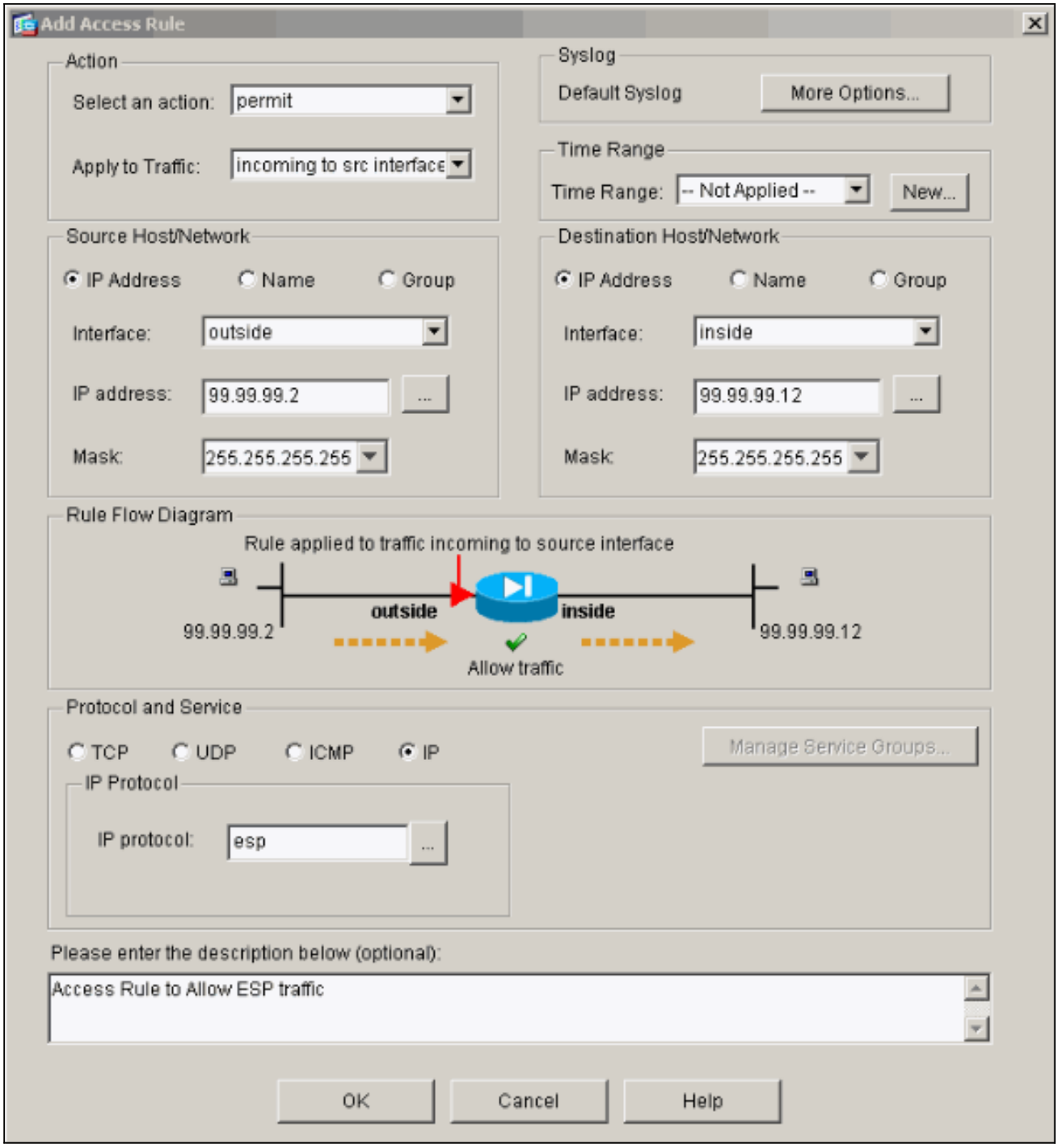

21. Klik op **Toepassen** om de interfaceconfiguratie te aanvaarden. De configuratie wordt ook op de PIX
geduwd.



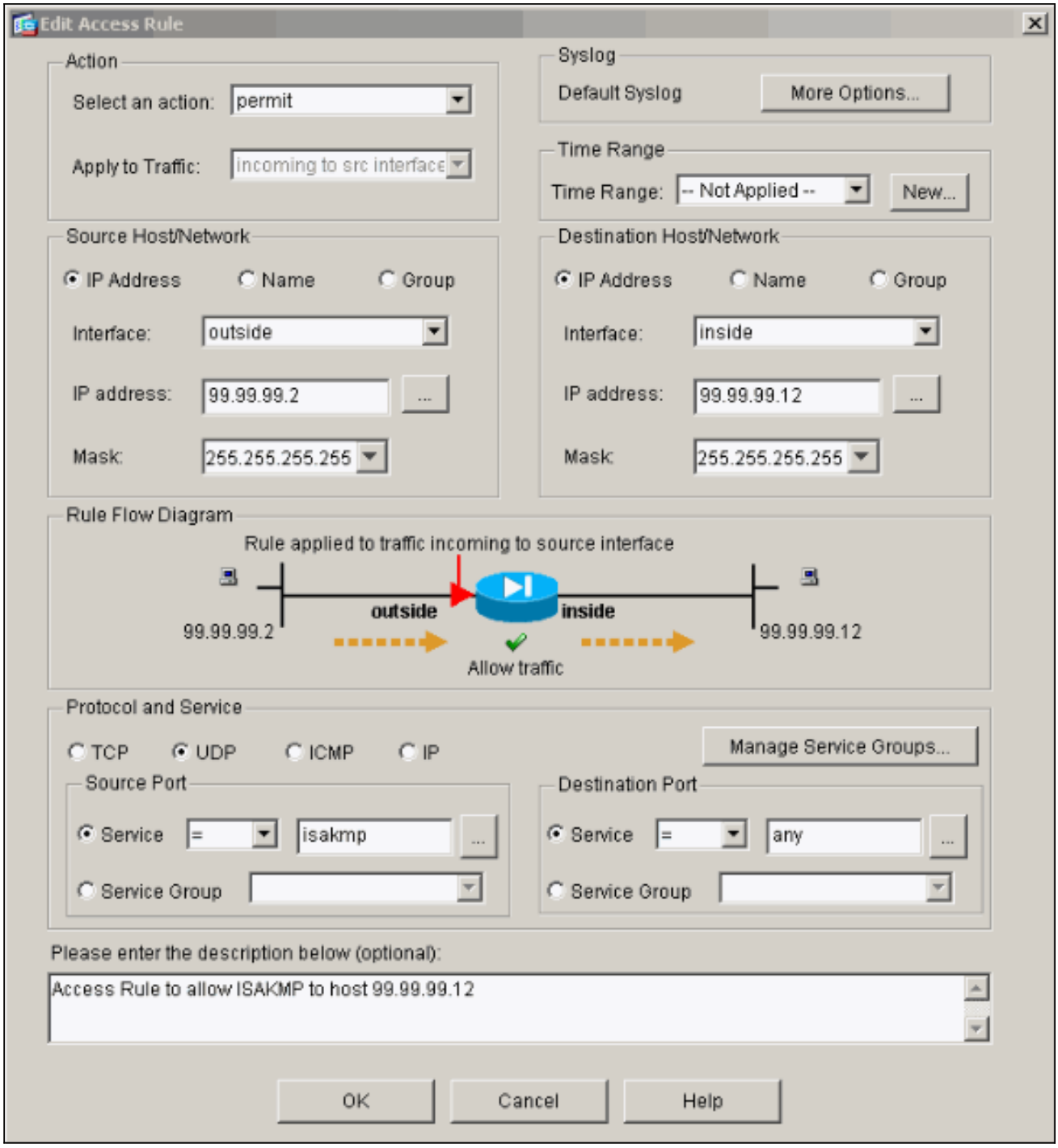

22. Selecteer **Veiligheidsbeleid** onder het tabblad Opties om de regel Beveiligingsbeleid te configureren.



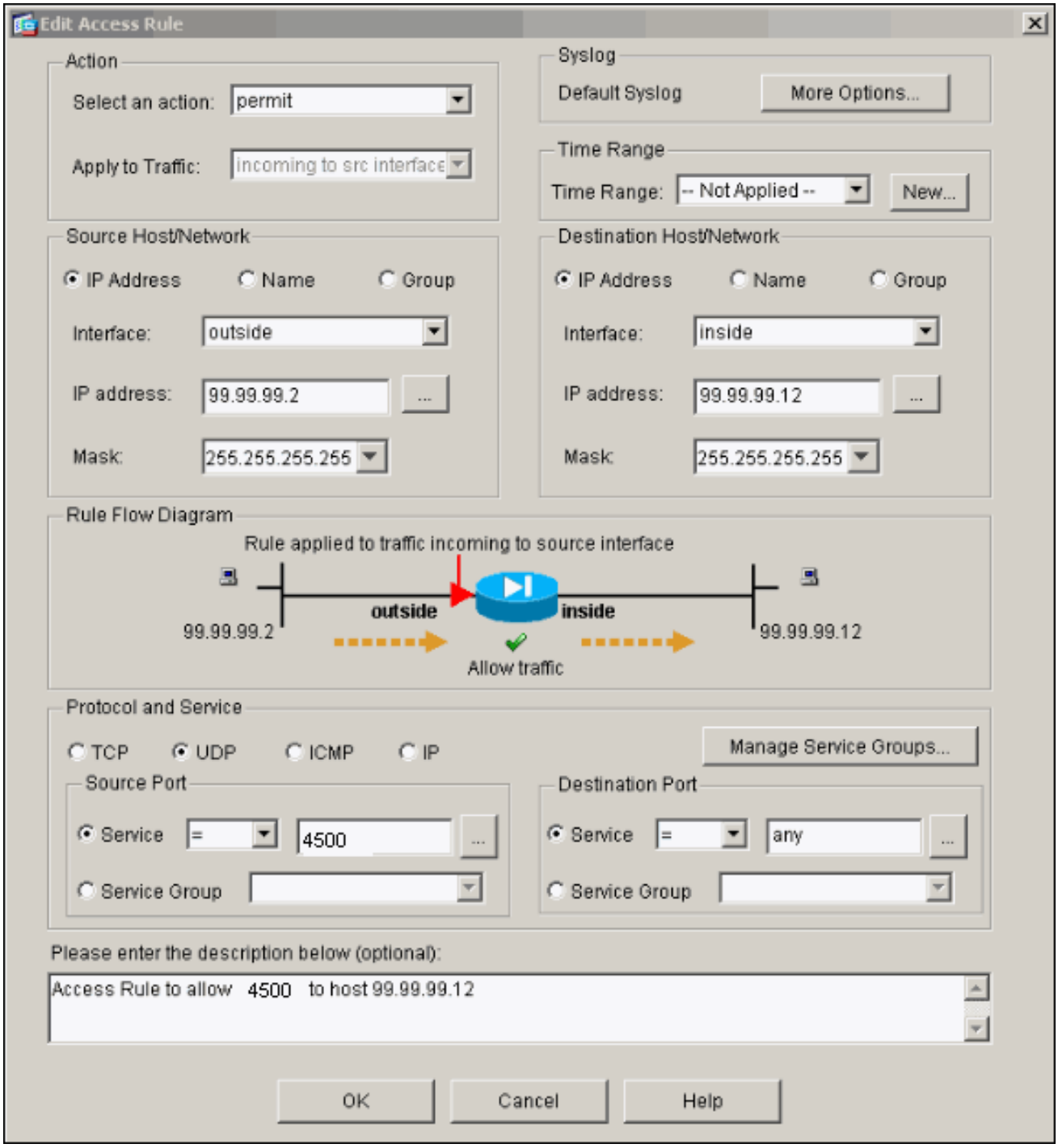

23. Klik op **Add** om esp-verkeer toe te staan en klik op **OK** om verder te gaan.



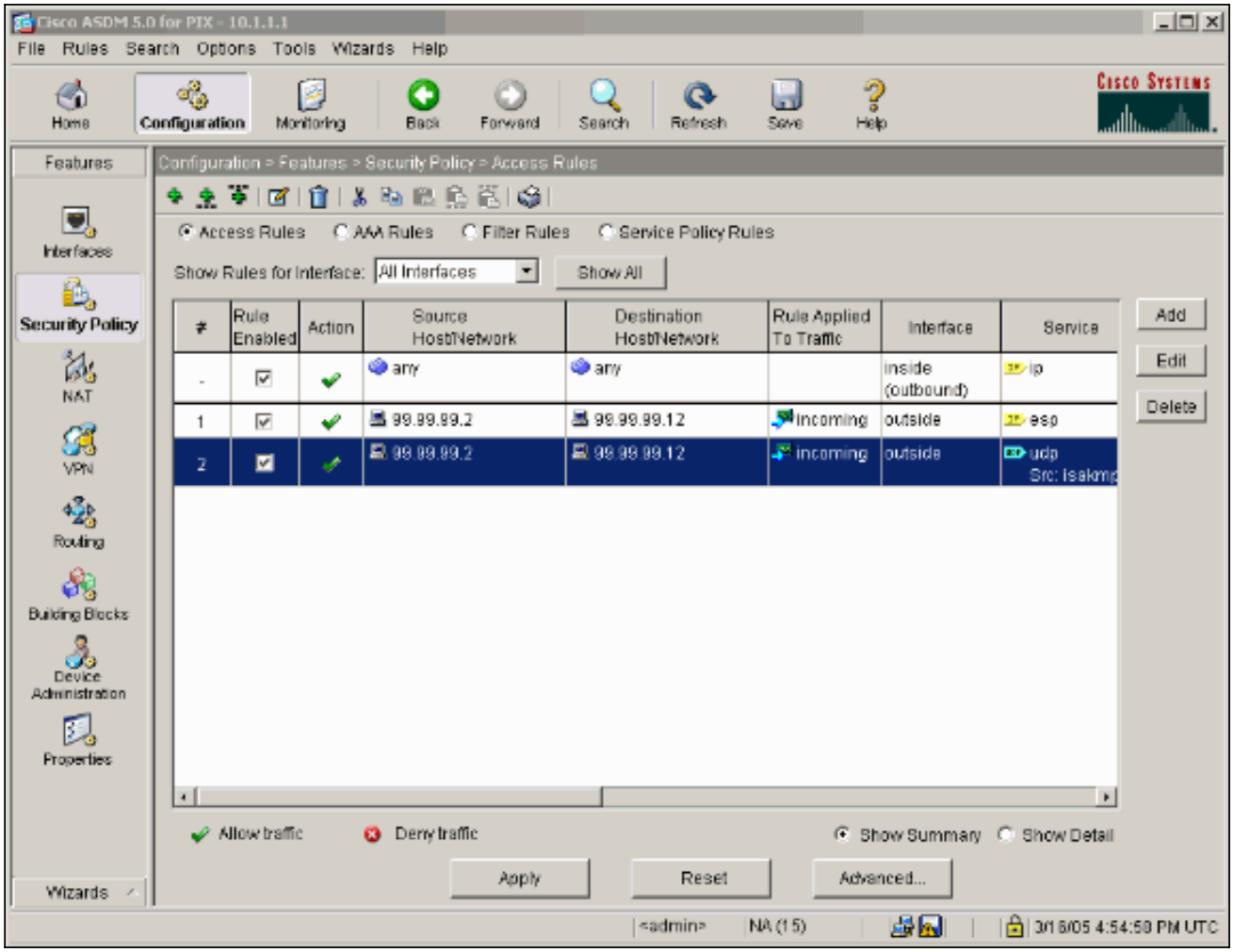

24. Klik op **Add** om ISAKMP-verkeer toe te staan en klik vervolgens op **OK** om door te gaan.



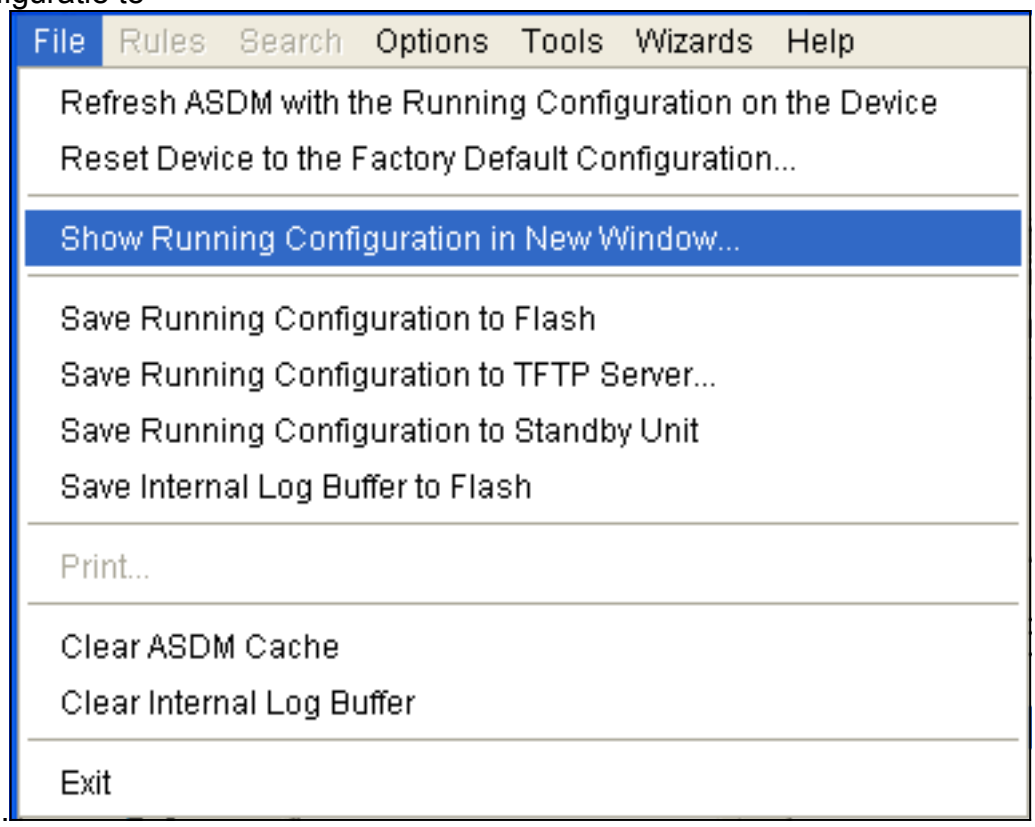

25. Klik op **Add** om UDP poort 4500 voor NAT-T mogelijk te maken en klik vervolgens op **OK** om verder te
gaan.




26. Klik op **Toepassen** om de interfaceconfiguratie te aanvaarden. De configuratie wordt ook op de PIX
geduwd.




27. De configuratie is nu voltooid.Kies **Bestand > Configuratie in nieuw venster tonen** om de CLI-configuratie te bekijken.




[Configuratie PIX-firewall]

## PIX-firewall

```
pixfirewall# show run
: Saved
:
PIX Version 7.0(0)102
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 99.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive

access-list outside_access_in remark Access Rule to
Allow ESP traffic
access-list outside_access_in
            extended permit esp host 99.99.99.2 host
99.99.99.12

access-list outside_access_in
            remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside_access_in
            extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12



access-list outside_access_in
            remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside_access_in
                    extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
```

```
icmp 0:00:02
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map asa_global_fw_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
: end
```

## Configuratie van PIX security applicatie en MPF (modulair beleidskader)

In plaats van toegangslijst, gebruik de opdracht **om ipsec-pass-thru** in MPF (modulair beleidskader) te **inspecteren** om het IPsec-verkeer door de PIX/ASA security applicaties te laten passeren.

Deze inspectie is ingesteld om pingaten te openen voor ESP-verkeer. Alle ESP - gegevensstromen zijn toegestaan wanneer een termijnstroom bestaat, en er is geen limiet aan het maximum aantal verbindingen dat kan worden toegestaan. AH is niet toegestaan. De standaard uitwijktijd voor ESP-gegevensstromen wordt standaard ingesteld op 10 minuten. Deze inspectie kan worden toegepast op alle locaties waar andere inspecties kunnen worden uitgevoerd, waaronder klasse- en matchcommandomodi. IPsec Pass Through Application inspection biedt een handig verkeer van ESP (IP protocol 50) dat gekoppeld is aan een IKE UDP-poort 500 verbinding. Het vermijdt langdurige configuratie van de toegangslijst om ESP verkeer toe te staan en voorziet ook veiligheid van tijd en maximum verbindingen. Gebruik **class-map**, **policy-map** en **service-beleid** opdrachten om een klasse van verkeer te definiëren, de opdracht Inspecteren op de class toe te passen en het beleid op een of meer interfaces toe te passen. Indien ingeschakeld, staat de opdracht **IPSec-pass-thru** onbeperkt ESP-verkeer toe met een time-out van 10 minuten, wat niet aanpasbaar is. NAT- en niet-NAT-verkeer zijn toegestaan.

```
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
```

# Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **toon crypto ipsec sa**-shows the fase 2 security associaties.
- **toon crypto isakmp sa** - toont de fase 1 veiligheidsassociaties.
- **Laat actieve crypto motorverbindingen zien** - toont de gecodeerde en gedecrypteerde pakketten.

# Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

## Opdrachten voor probleemoplossing voor IPsec-router

**Opmerking:** Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten afgeeft.

- **debug van crypto motor**-displays het verkeer dat versleuteld wordt.
- **debug crypto ipsec**-displays de IPsec onderhandelingen van fase 2.
- **debug van crypto isakmp** — Hiermee geeft u de onderhandelingen over fase 1 weer van de Internet Security Association en Key Management Protocol (ISAKMP).

## Security associaties reinigen

- **duidelijke crypto isakmp**-Clears Internet Key Exchange (IKE) - beveiligingsassociaties.
- **duidelijke crypto ipsec sa**-cleert IPsec security associaties.

## Opdrachten voor probleemoplossing voor PIX

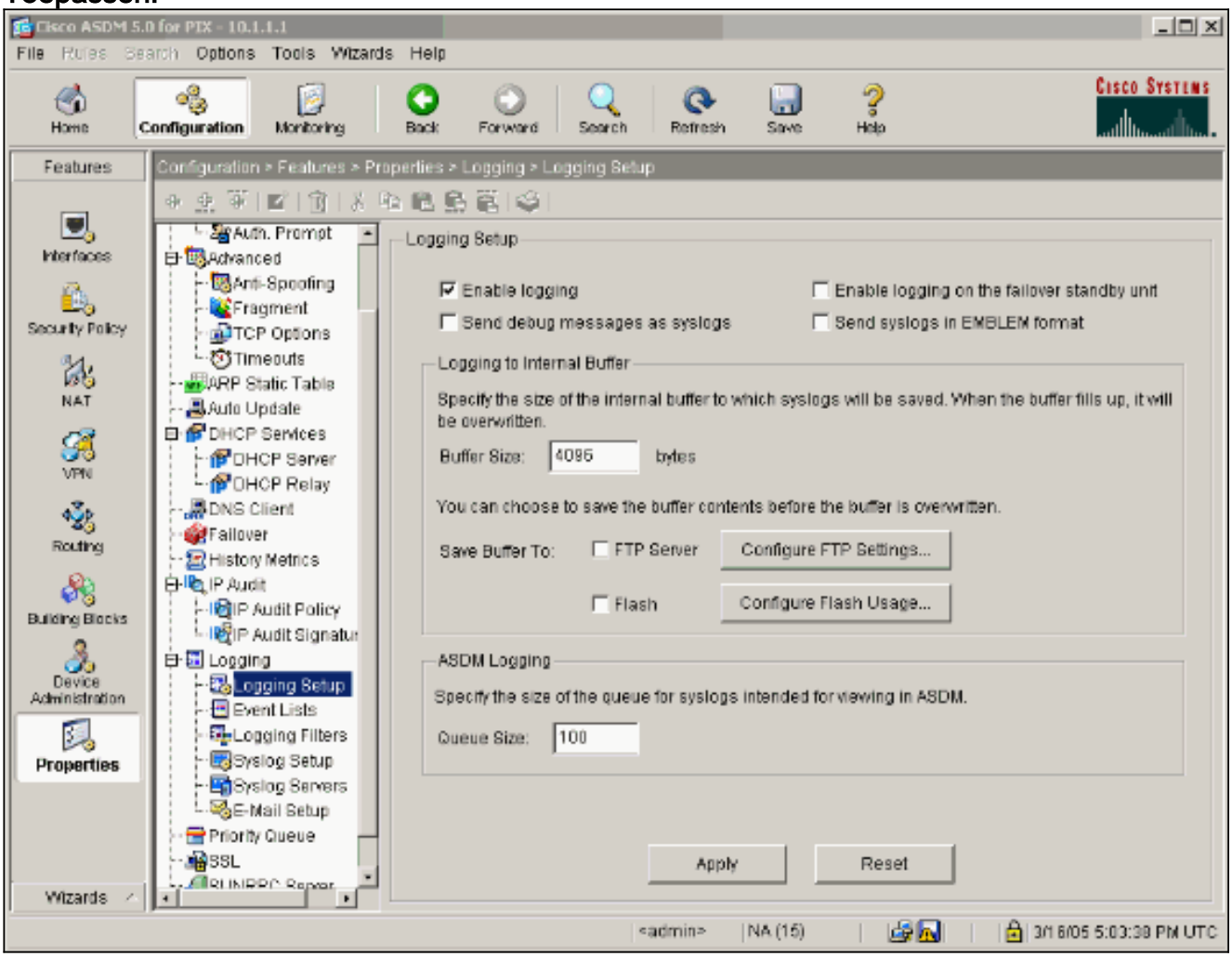
Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

**Opmerking:** Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**

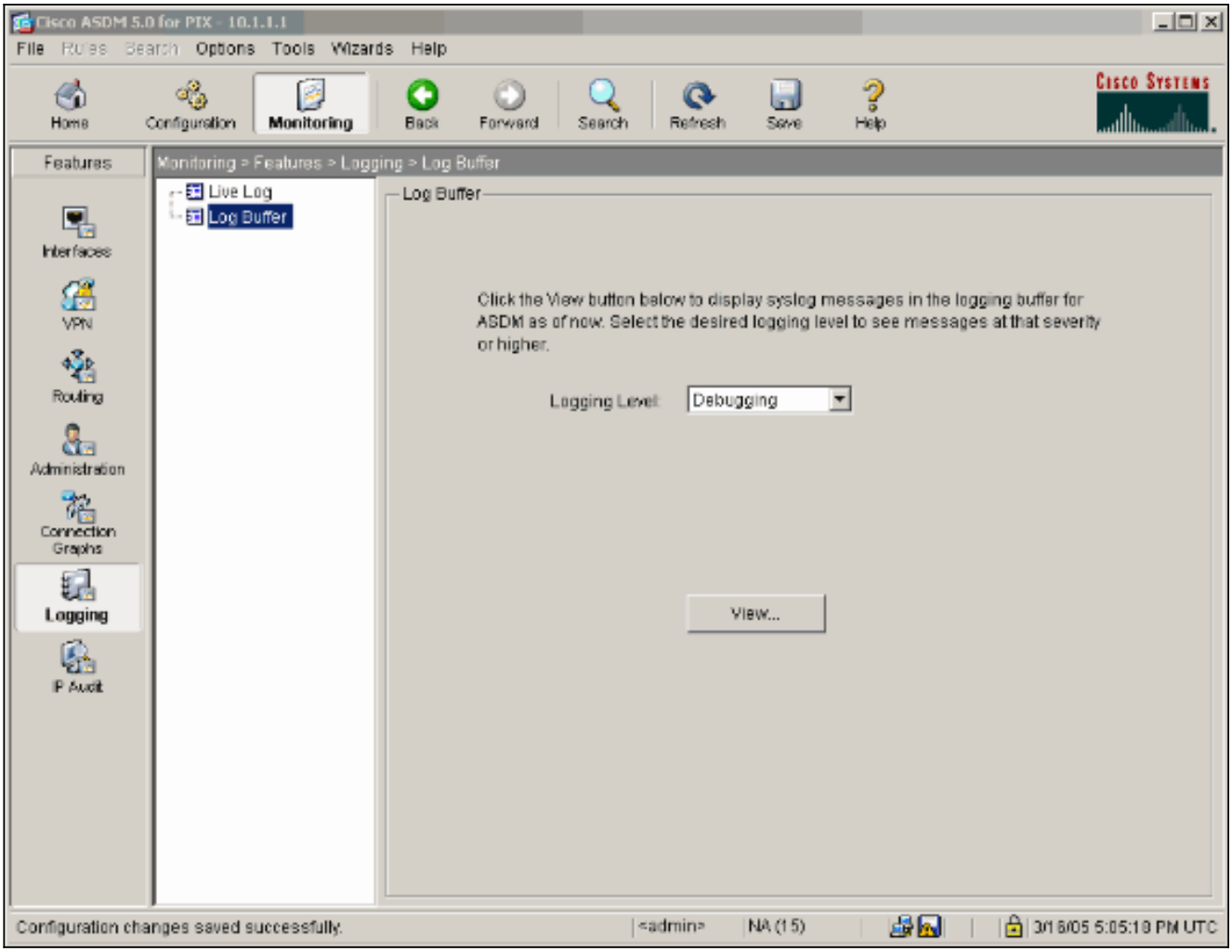
opdrachten afgeeft.

- **het foutoptreden van de houtbuffer** - toont verbindingen die worden gevestigd en ontkend aan hosts die door de PIX gaan. De informatie wordt opgeslagen in de PIX-logbuffer en de uitvoer kan worden gezien met behulp van de opdracht **Show log**.
- ASDM kan worden gebruikt om houtkap mogelijk te maken en ook om de logbestanden te bekijken zoals in deze stappen.

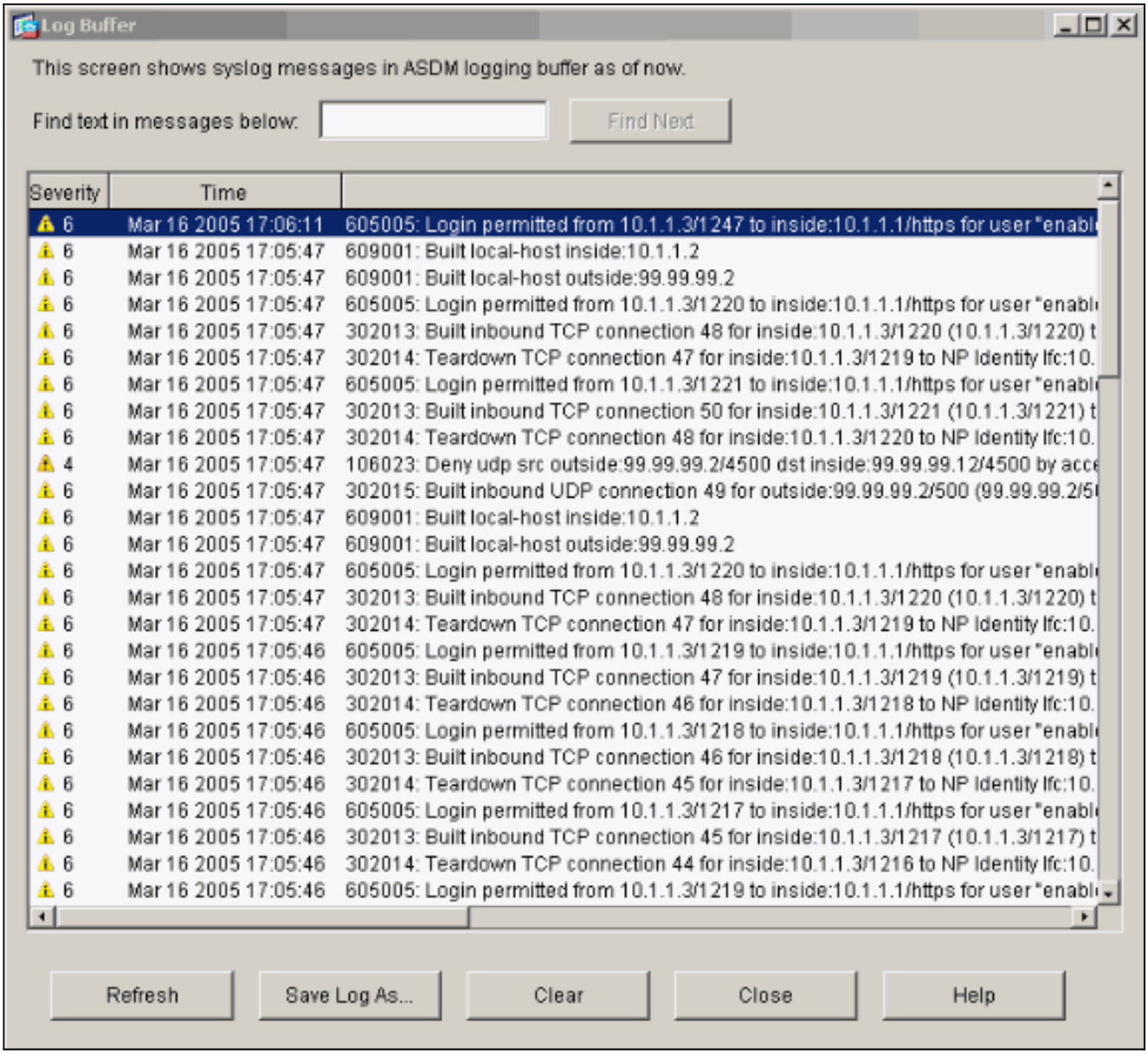
1. Kies **Configuratie > Eigenschappen > Vastlegging > Instellen vastlegging > Vastlegging inschakelen** en klik vervolgens op **Toepassen.**




2. Kies **Controle > Vastlegging > Logboek Buffer > Op vastlegging niveau > Logging Buffer**, en klik op **Weergeven**.




Dit is een voorbeeld van de Log Buffer.




## Gerelateerde informatie

- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- PIX-ondersteuningspagina
- PIX-opdrachtreferenties
- NAT-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems