Esempio di configurazione del tunnel VPN IPsec PIX/ASA (versione 7.x e successive) con Network Address Translation

Sommario

Introduzione

In questa configurazione di esempio viene mostrato un tunnel VPN IPsec attraverso un firewall che esegue NAT (Network Address Translation). **Questa configurazione non funziona con Port Address Translation (PAT) se si usa il software Cisco IOS® versioni precedenti a 12.2(13)T esclusa.** Questo tipo di configurazione può essere utilizzata per eseguire il tunnel del traffico IP. Questa configurazione non può essere utilizzata per crittografare il traffico che non attraversa un firewall, ad esempio gli aggiornamenti di routing o IPX. Il tunneling GRE (Generic routing Encapsulation) è una scelta più appropriata. Nell'esempio, i router Cisco 2621 e 3660 sono gli endpoint del tunnel IPsec che si uniscono a due reti private, con condotti o elenchi di controllo di accesso (ACL) sul PIX nel mezzo per consentire il traffico IPsec.

Nota: NAT è una traduzione di indirizzi uno a uno, da non confondere con PAT, che è una traduzione molti (all'interno del firewall)-a-uno. Per ulteriori informazioni sul funzionamento e la configurazione NAT, fare riferimento a Verifica del funzionamento NAT e risoluzione dei problemi NAT di base o a Come funziona NAT.

Nota: IPsec con PAT potrebbe non funzionare correttamente perché il dispositivo endpoint del

tunnel esterno non è in grado di gestire più tunnel da un indirizzo IP. Contattare il fornitore per determinare se i dispositivi di endpoint del tunnel funzionano con PAT. Inoltre, nel software Cisco IOS versione 12.2(13)T e successive, la funzione di trasparenza NAT può essere utilizzata per PAT. Per ulteriori informazioni, vedere Trasparenza NAT IPSec. per ulteriori informazioni su queste funzionalità nel software Cisco IOS versione 12.2(13)T e successive, fare riferimento al supporto di IPSec ESP tramite NAT.

Nota: prima di aprire una richiesta di assistenza con il supporto tecnico Cisco, fare riferimento alle domande frequenti NAT, che contengono molte risposte alle domande frequenti.

Per ulteriori informazioni su come configurare il tunnel IPSec attraverso il firewall con NAT sulla versione 6.x e precedenti, fare riferimento a Configurazione di un tunnel IPSec attraverso il firewall con NAT su PIX.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 12.0.7.T (fino al software Cisco IOS release 12.2(13)T escluso)Per le versioni più recenti, fare riferimento a Trasparenza NAT IPSec.
- Cisco 2621 router
- Cisco 3660 router
- Cisco PIX serie 500 Security Appliance con versione 7.x e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Prodotti correlati

Questo documento può essere usato anche con Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 7.x e successive.

Configurazione

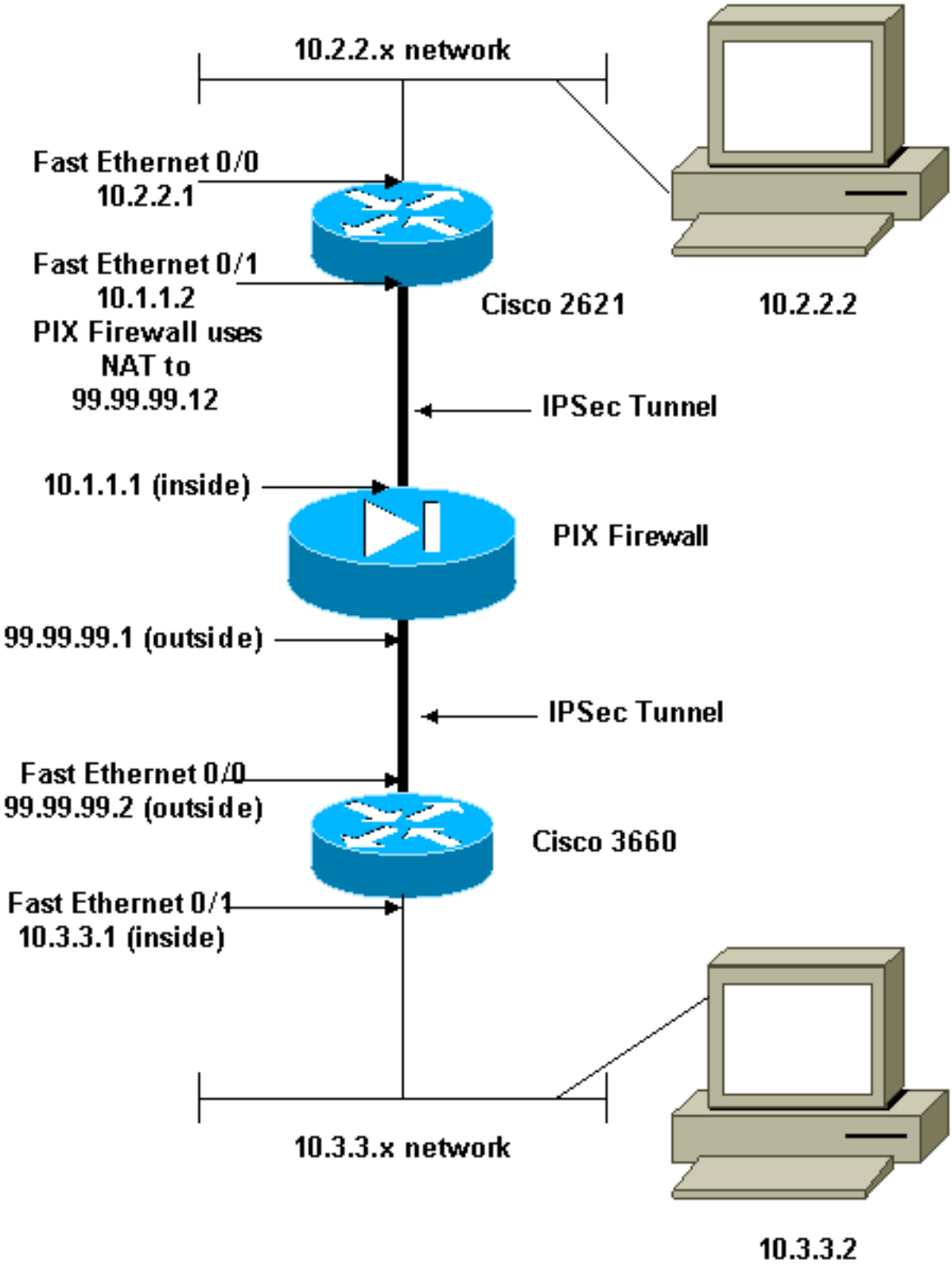
In questa sezione vengono presentate le informazioni che è possibile utilizzare per configurare le

funzionalità descritte nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione di Cisco 2621
- Configurazione di Cisco 3660
- Configurazione di PIX Security Appliance e elenco accessiConfigurazione ASDM (Advanced Security Device Manager GUI)Configurazione CLI (Command Line Interface)
- Configurazione di PIX Security Appliance e MPF (Modular Policy Framework)

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
```

Configurazione di PIX Security Appliance e elenco accessi

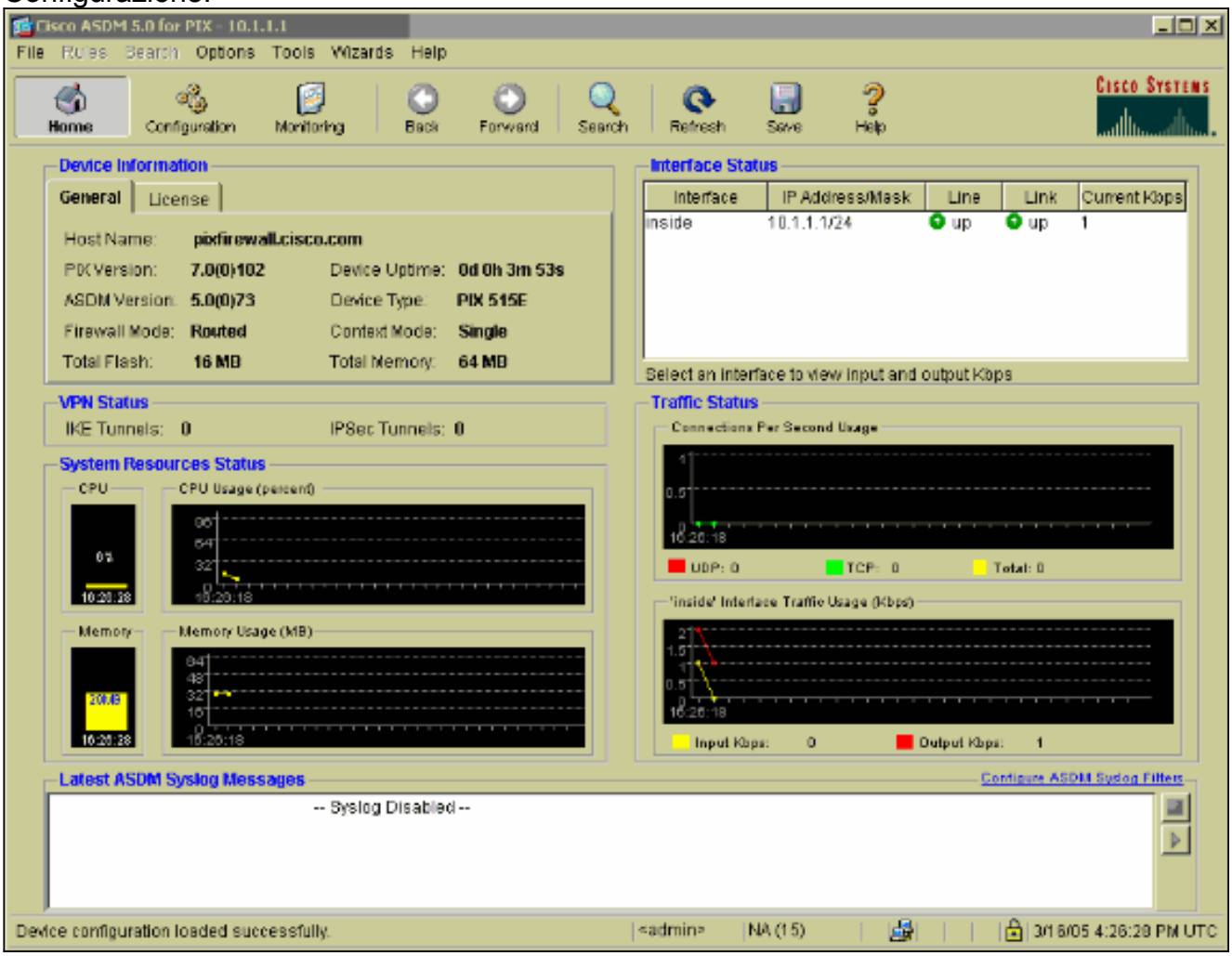
Configurazione di ASDM 5.0

Completare questa procedura per configurare PIX Firewall versione 7.0 con ASDM.

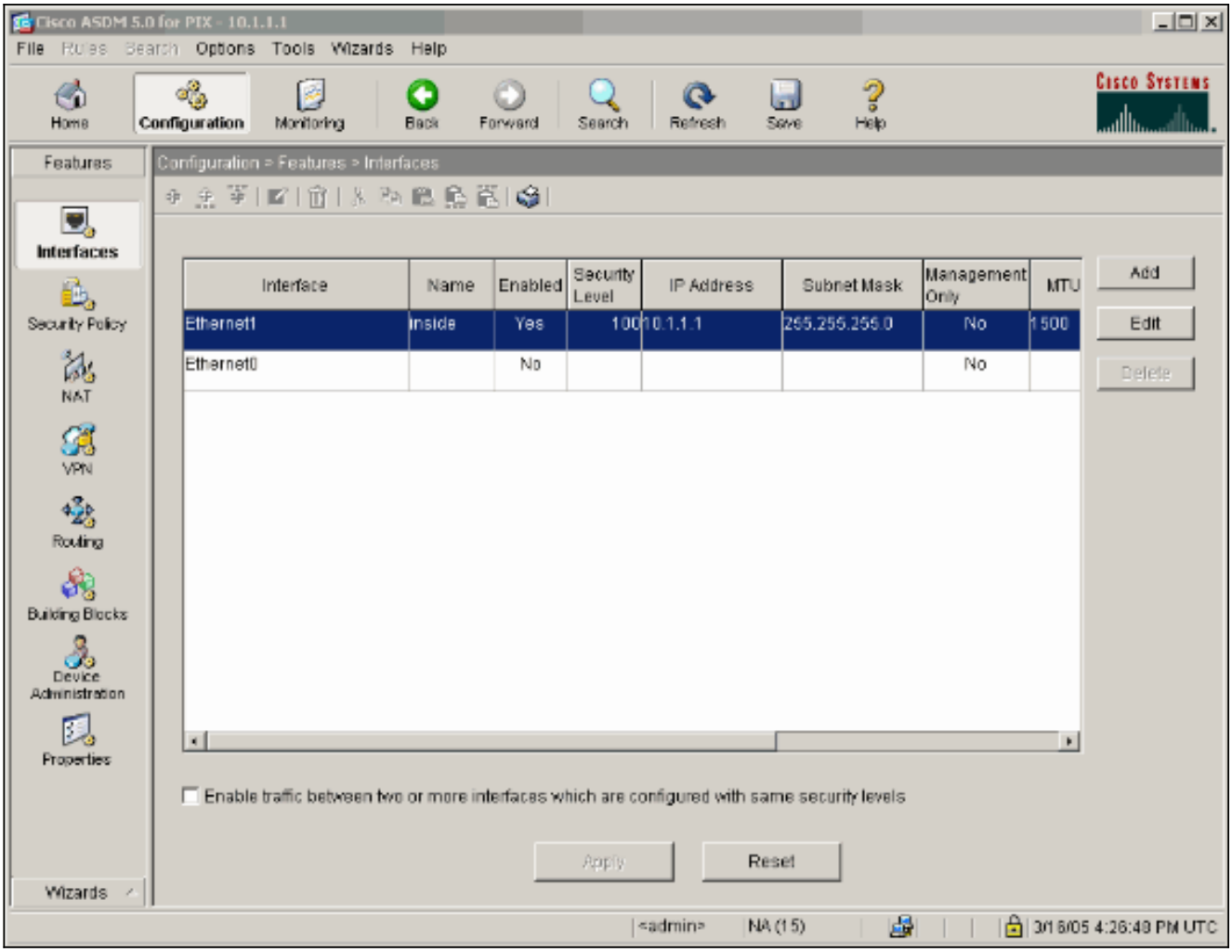
1. Collegare la console al PIX. Da una configurazione ripristinata ai valori predefiniti, usare le

istruzioni interattive per abilitare l'**interfaccia grafica di Advanced Security Device Manager (ASDM)** per la gestione dei PIX dalla workstation 10.1.1.3.

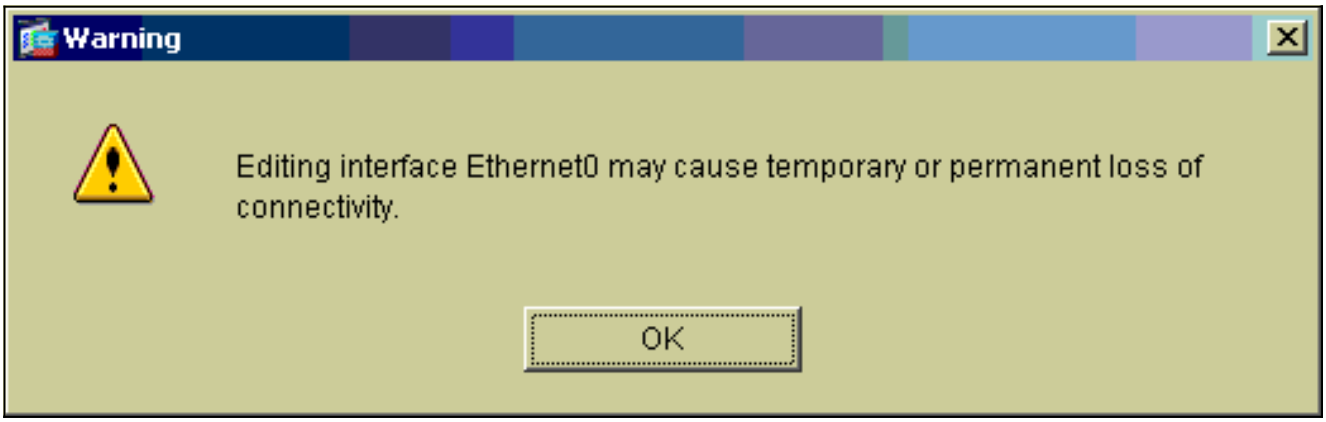
2. Da Workstation 10.1.1.3, aprire un browser Web e utilizzare ADSM (in questo esempio, https://10.1.1.1).
3. Selezionare **Yes** (Sì) nelle richieste del certificato e accedere con la password enable configurata nella configurazione di bootstrap ASDM di PIX Firewall.
4. Se è la prima volta che ASDM viene eseguito sul PC, viene richiesto se utilizzare ASDM Launcher o se utilizzare ASDM come app Java.Nell'esempio, l'Utilità di avvio ASDM è selezionata e installa questi prompt.
5. Passare alla finestra Home ASDM e selezionare la scheda Configurazione.



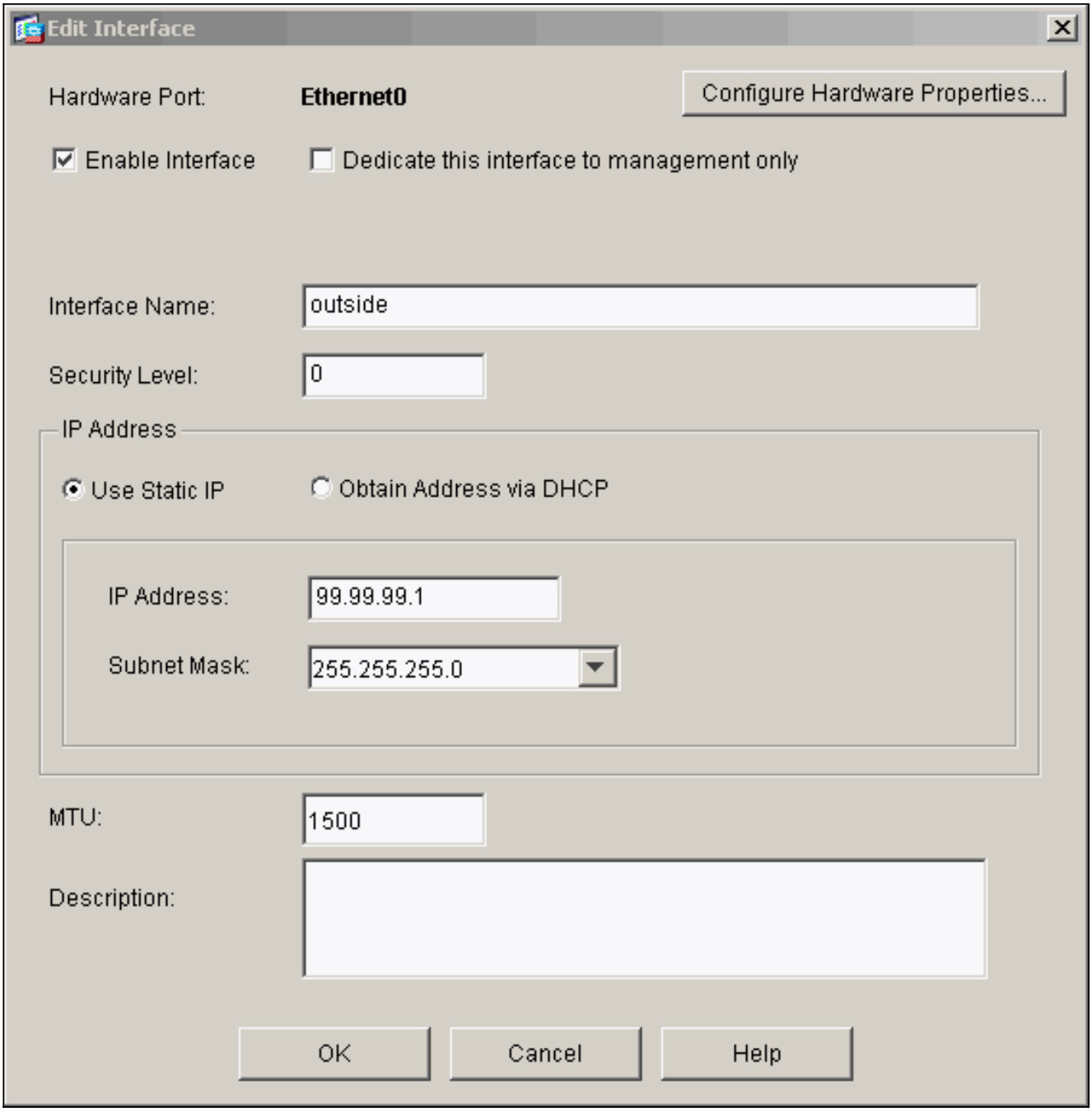
6. Per configurare l'interfaccia esterna, evidenziare **Ethernet 0 Interface** e fare clic su **Edit** (Modifica).



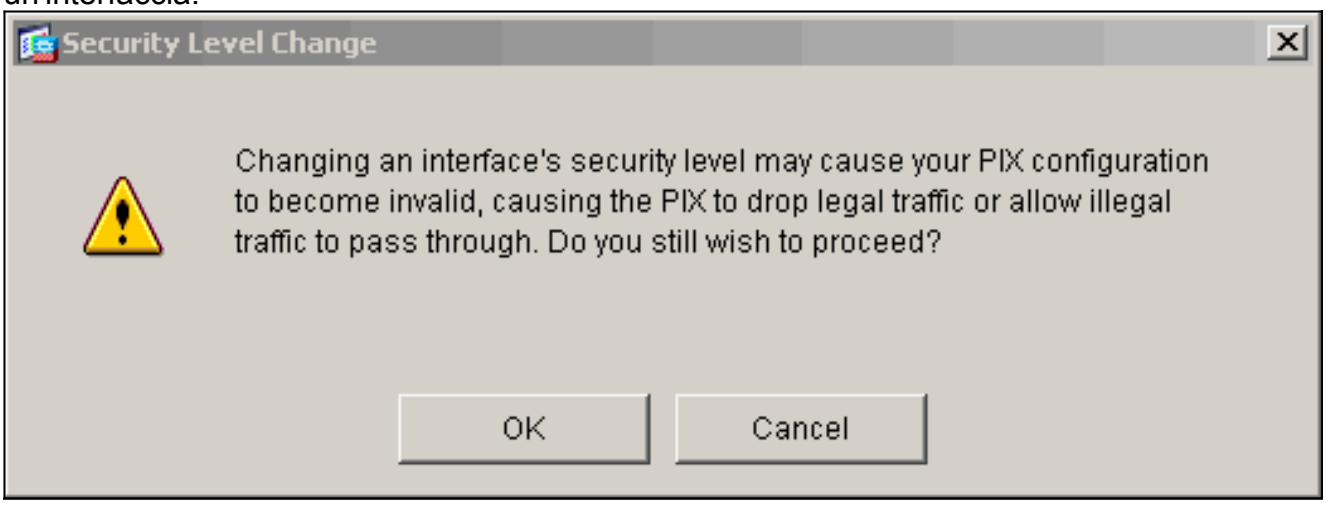
7. Fare clic su **OK** al prompt dell'interfaccia di modifica.



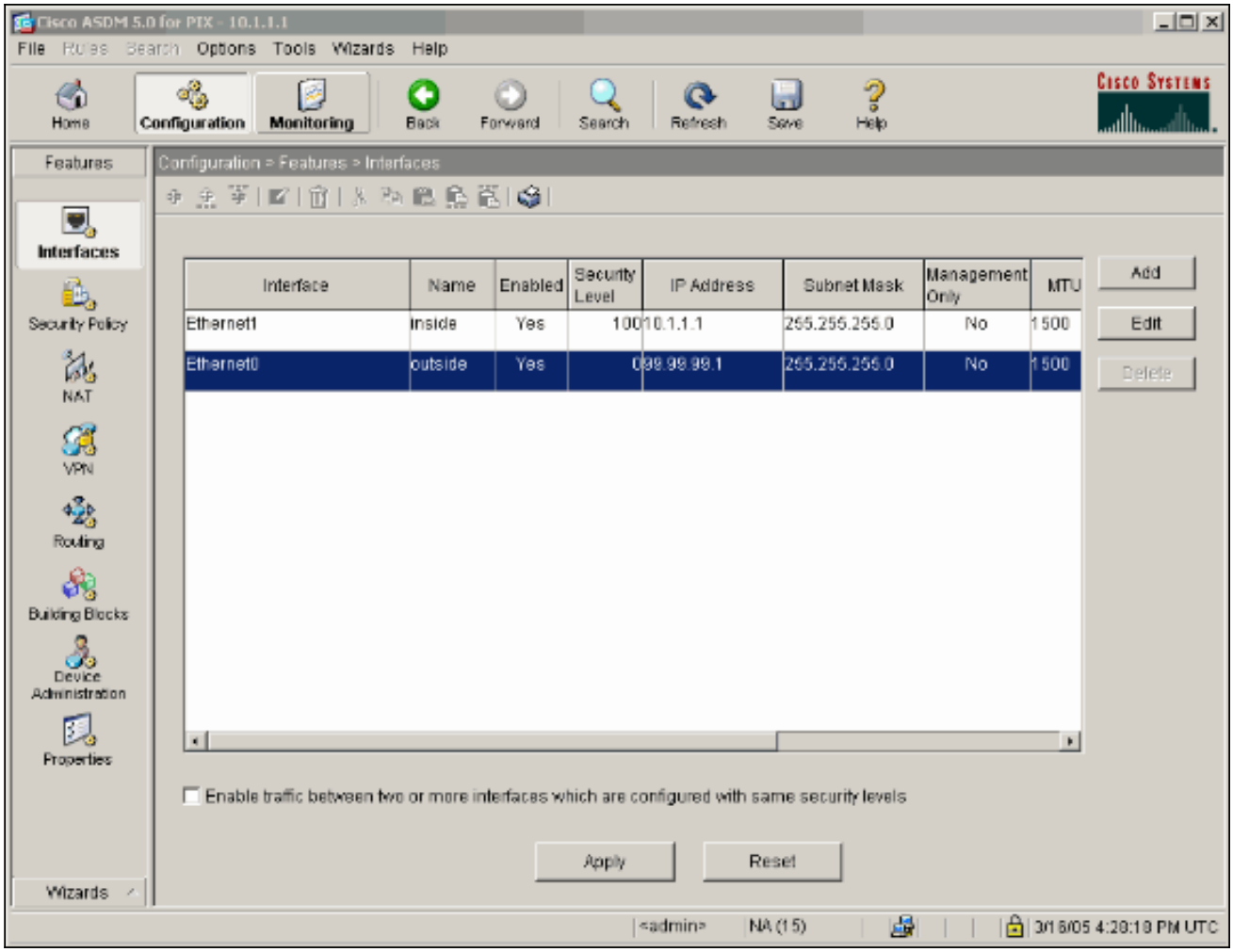
8. Immettere i dettagli dell'interfaccia e al termine fare clic su **OK**.



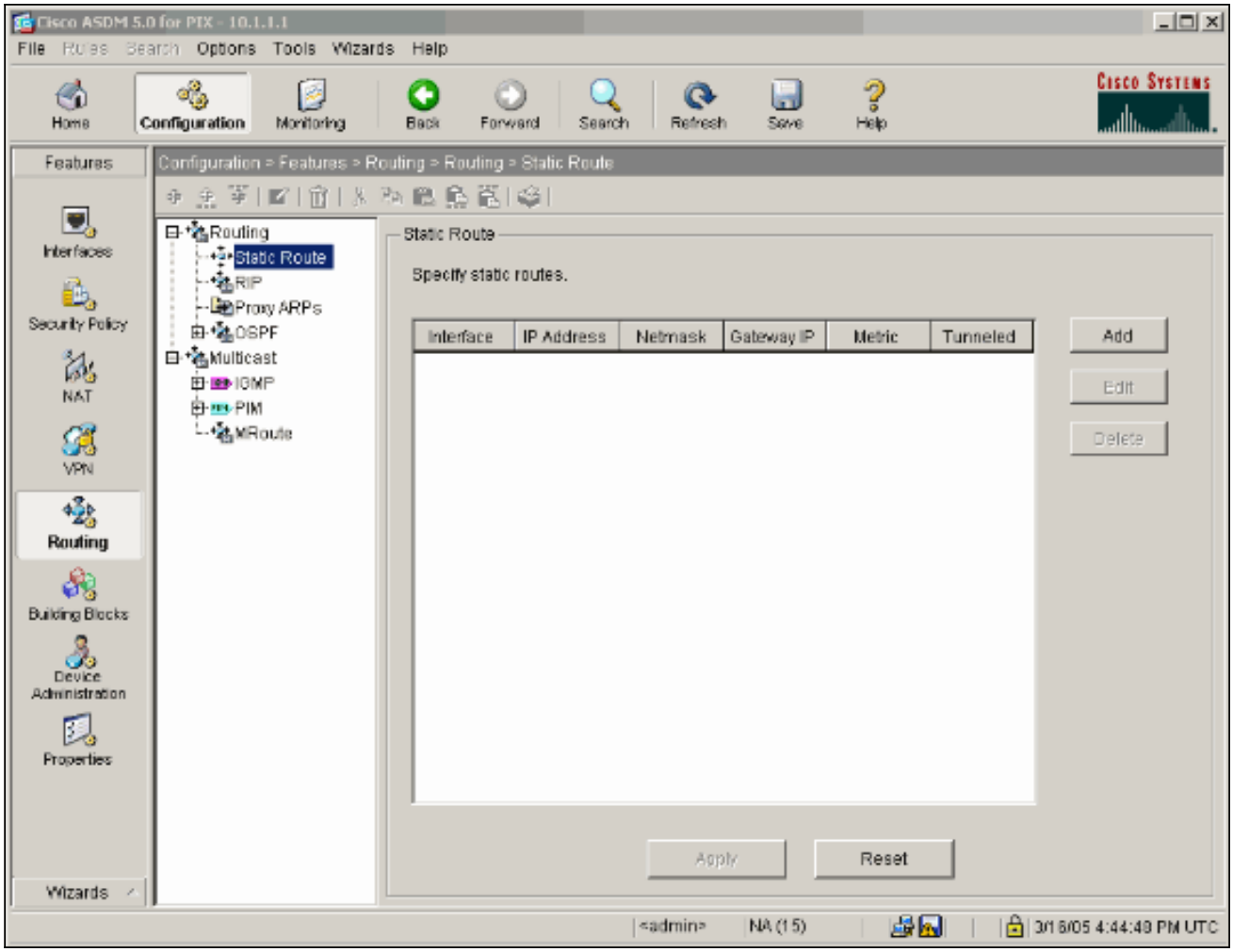
9. Fare clic su **OK** al prompt Modifica di un'interfaccia.



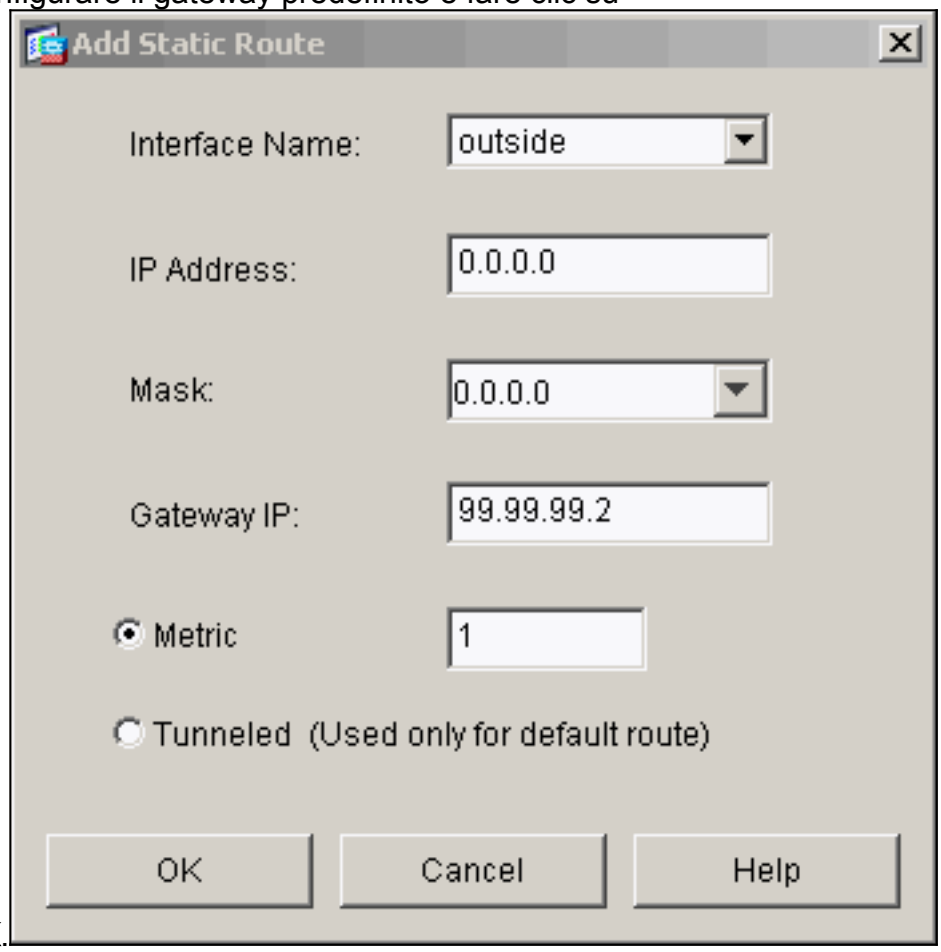
10. Per accettare la configurazione dell'interfaccia, fare clic su **Apply** (Applica). La configurazione viene inoltre inserita nel PIX. In questo esempio vengono utilizzate route statiche.



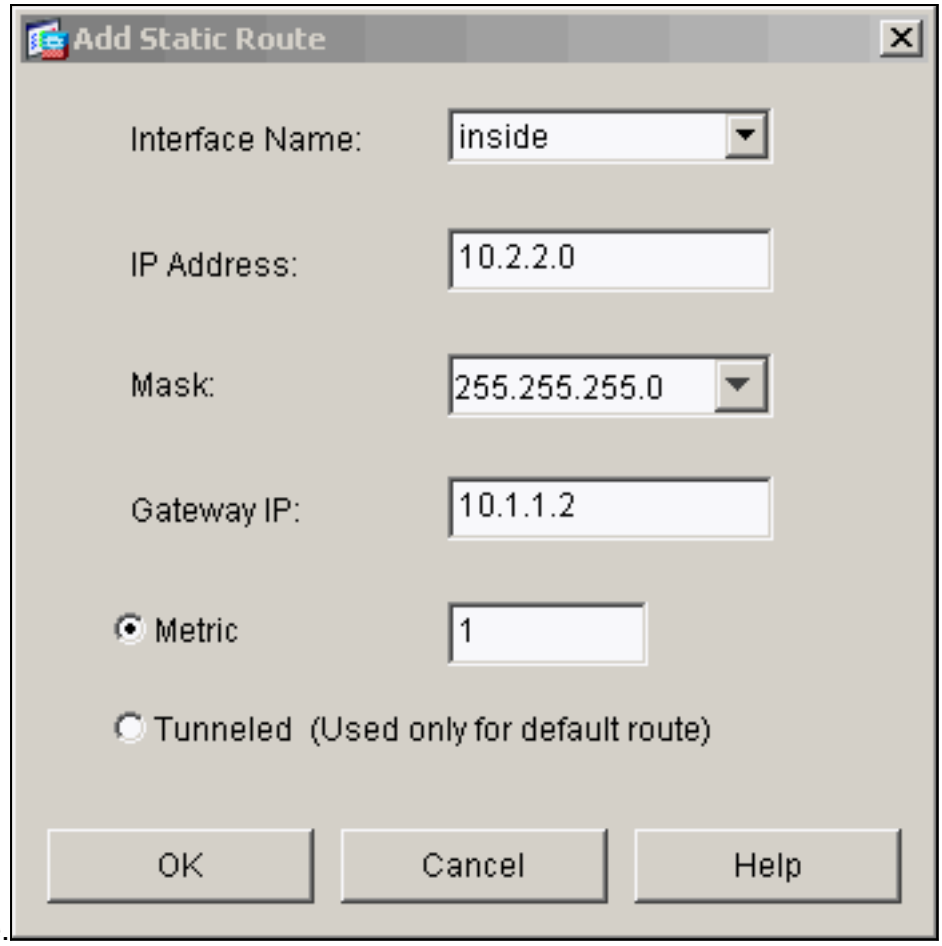
11. Fare clic su **Routing** nella scheda Features, evidenziare **Static Route**, quindi fare clic su **Add**.



12. Configurare il gateway predefinito e fare clic su OK.

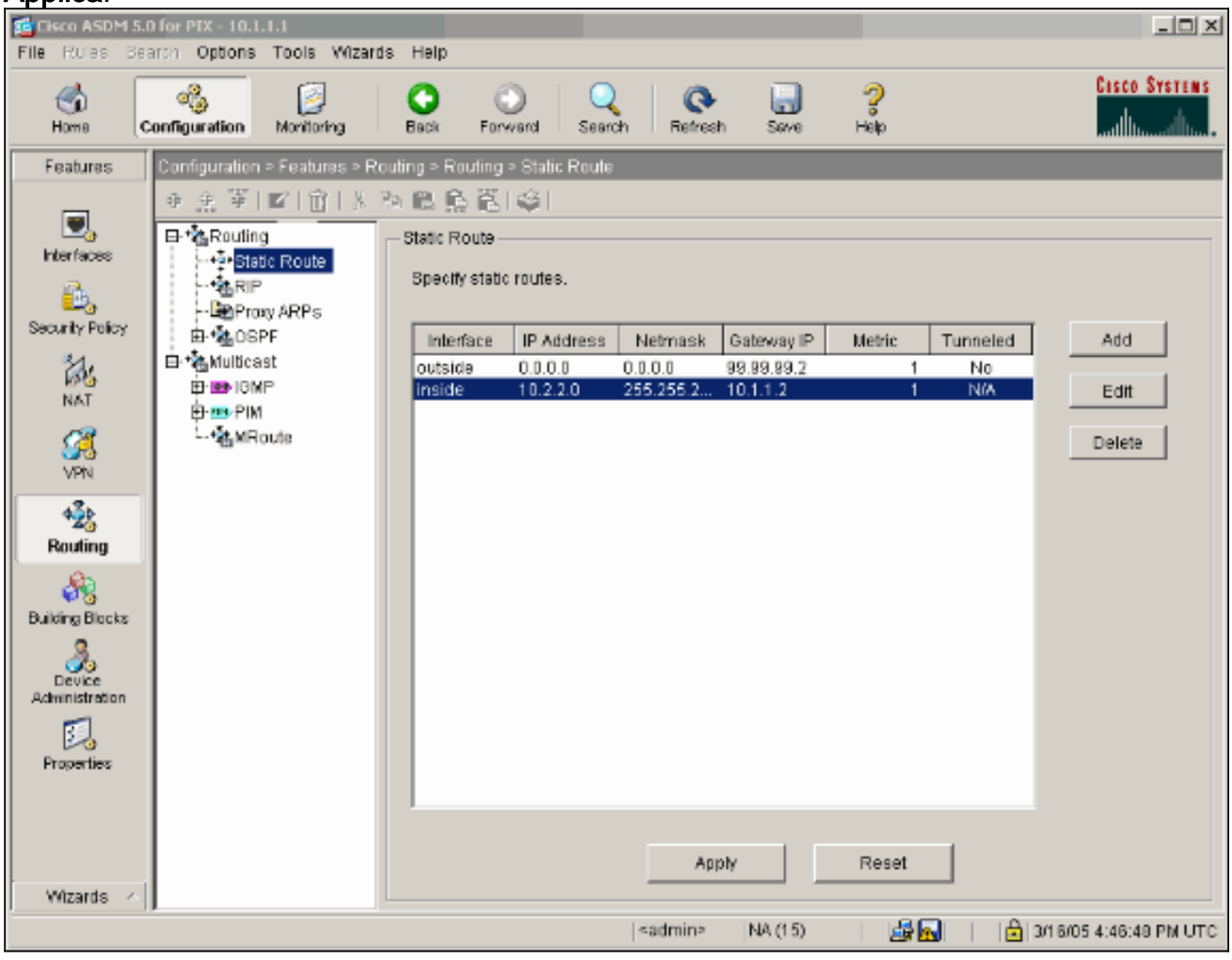


13. Fare clic su **Add** (Aggiungi) e aggiungere le route alle reti

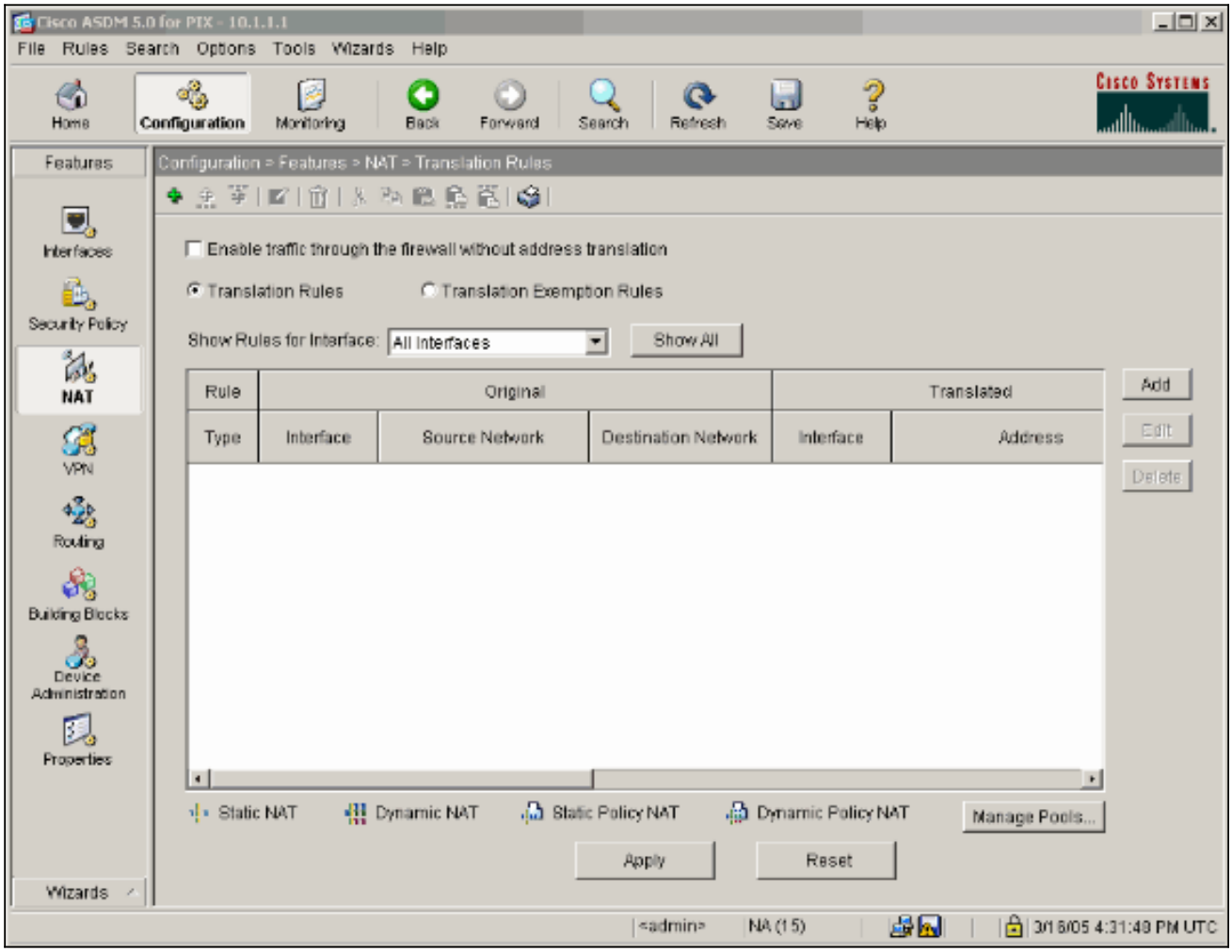


interne.

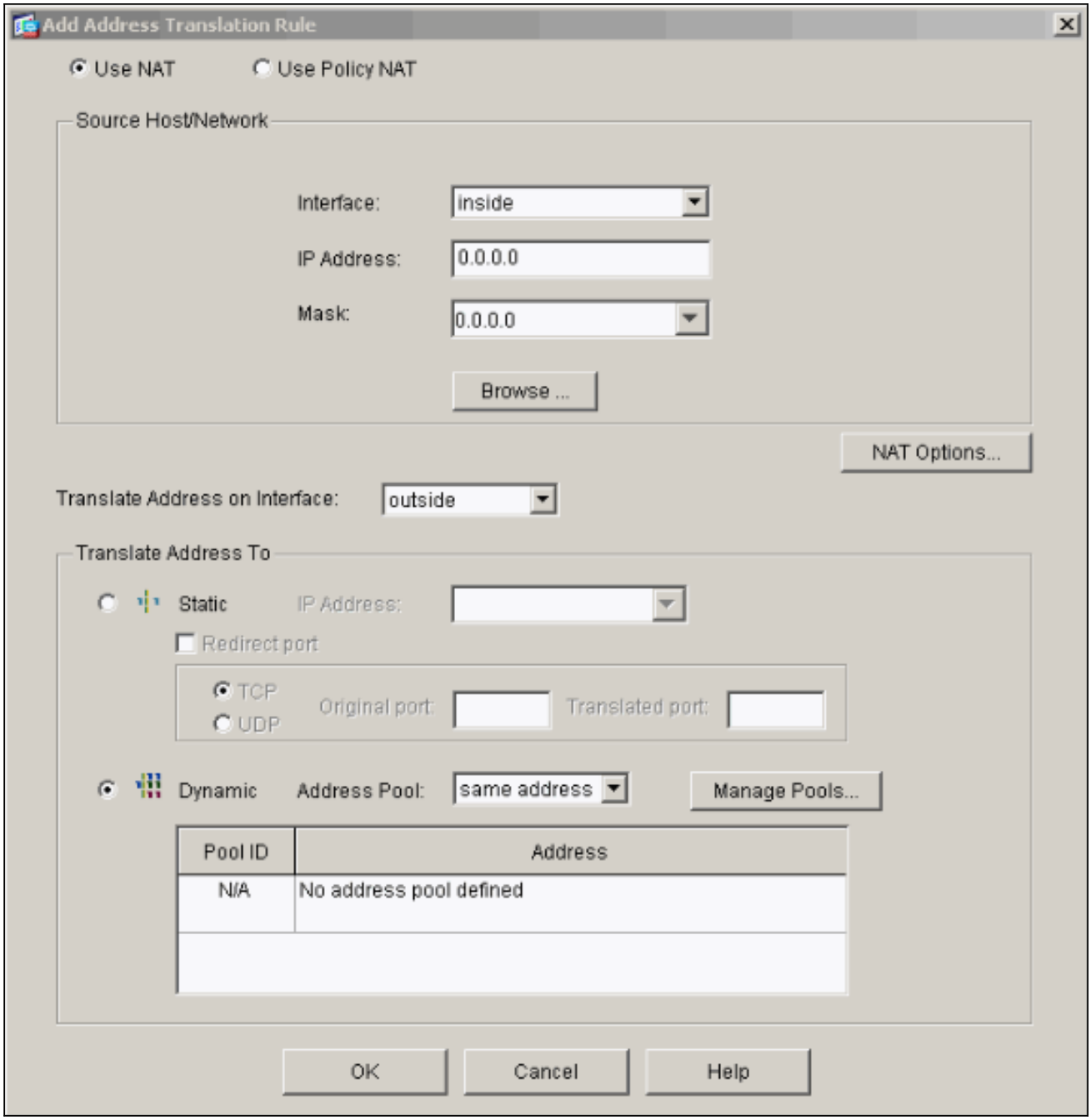
14. Verificare che siano configurate le route corrette e fare clic su **Applica**.



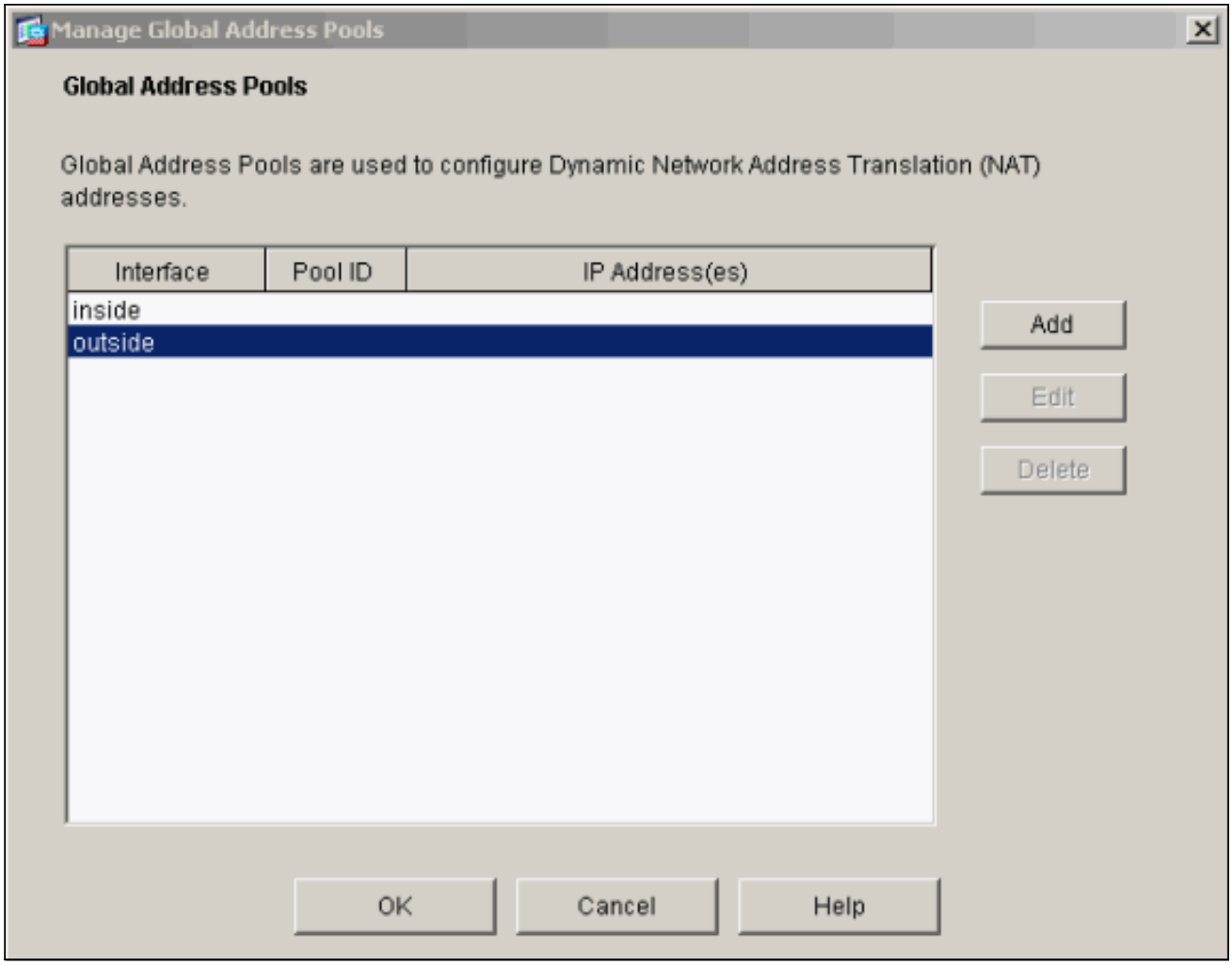
15. Nell'esempio viene utilizzato NAT. Rimuovere la casella di controllo **Abilita traffico attraverso il firewall senza conversione degli indirizzi** e fare clic su **Add** per configurare la regola
NAT.



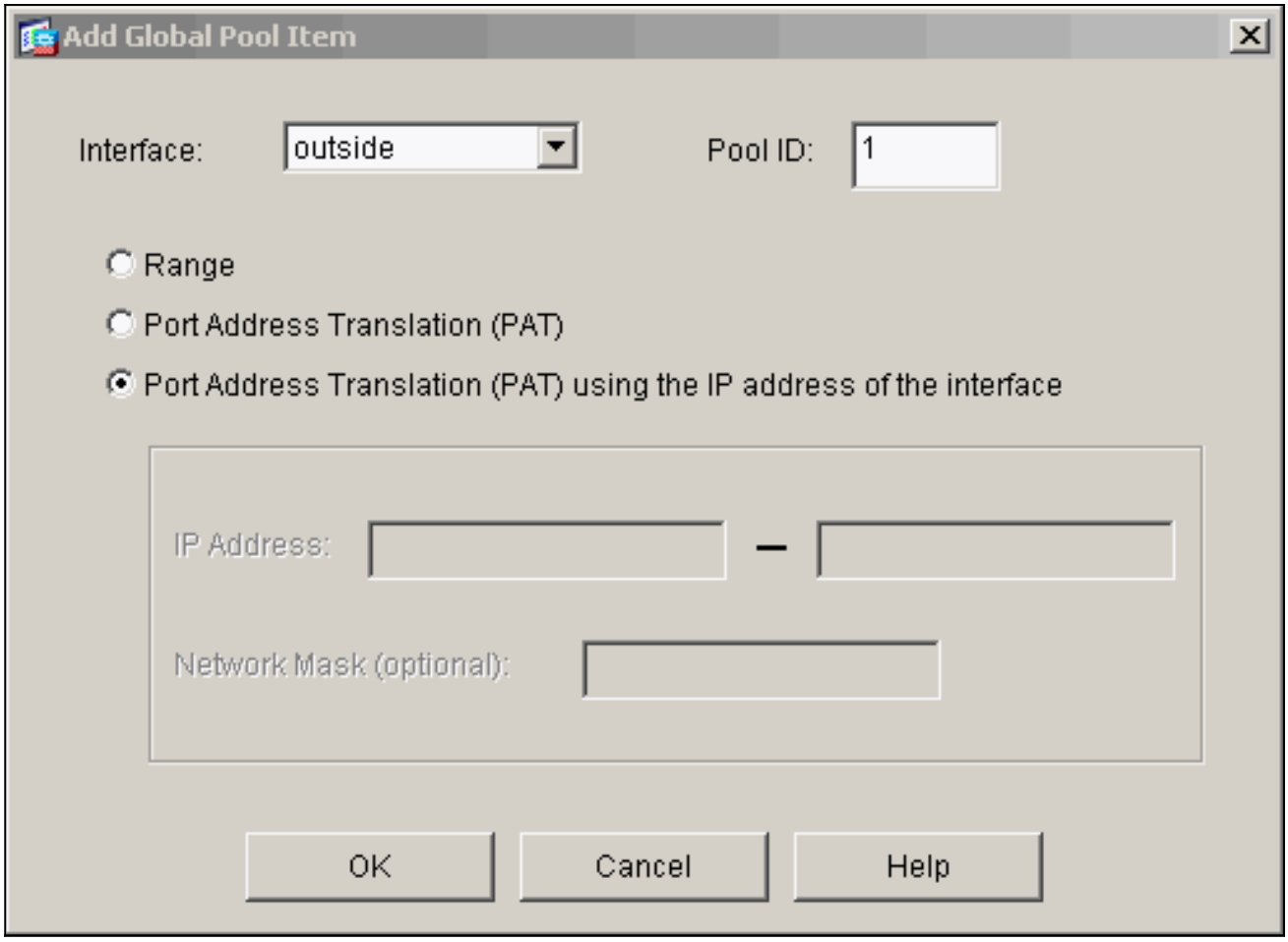
16. Configurare la rete di origine (nell'esempio riportato viene utilizzato any). Quindi, fare clic su **Gestisci pool** per definire il
percorso.



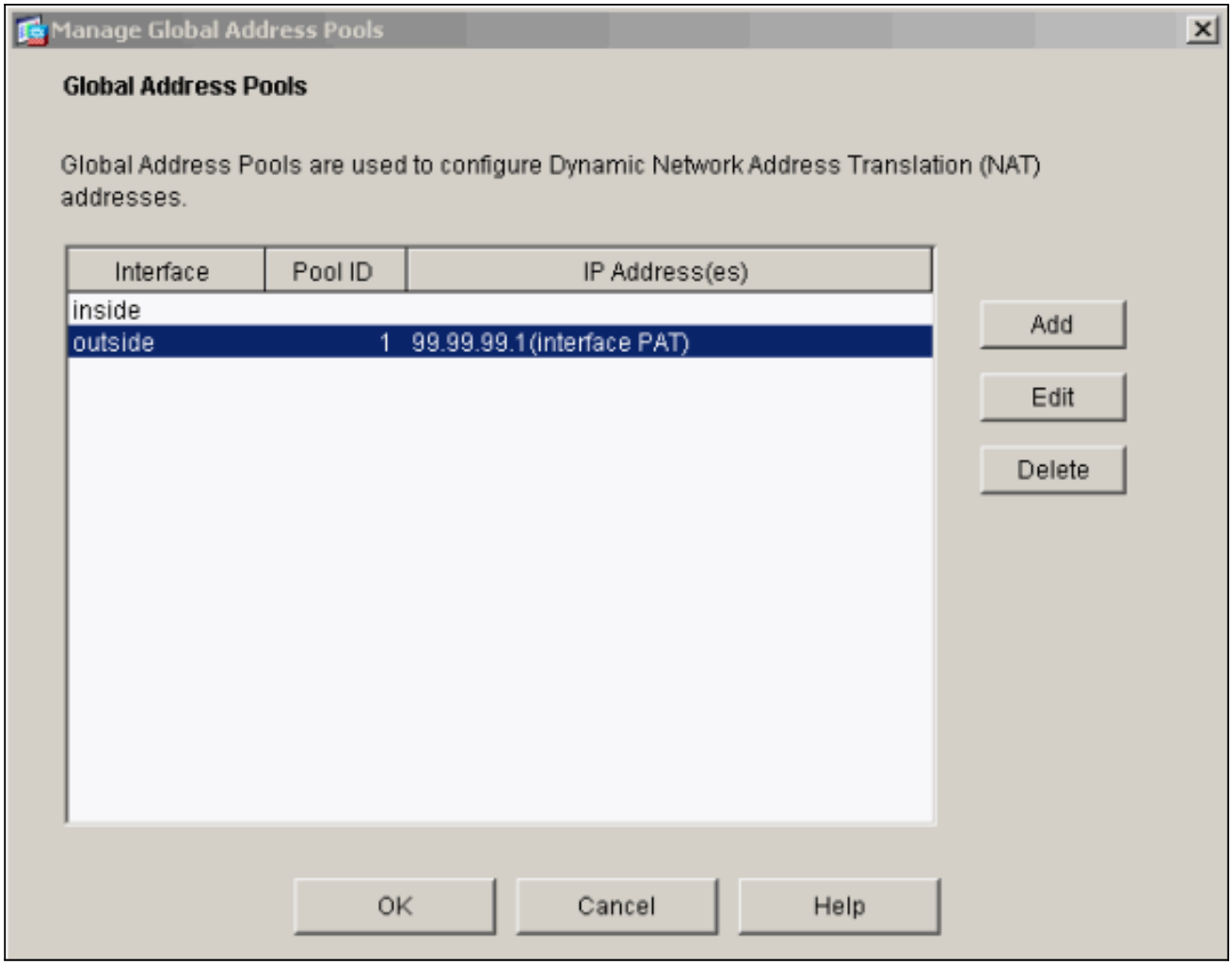
17. Selezionare l'interfaccia **esterna** e fare clic su **Aggiungi**.



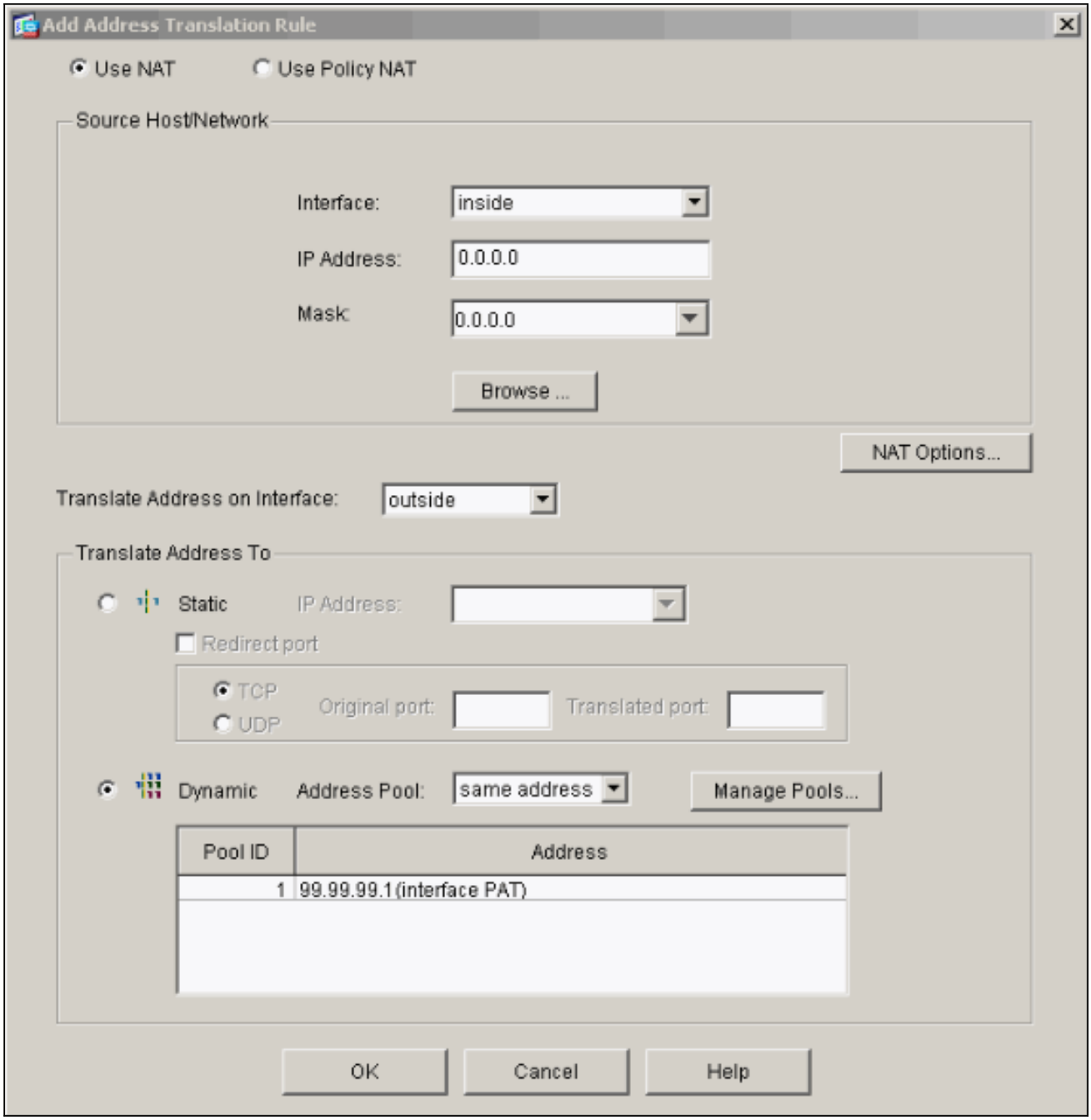
In questo esempio viene utilizzato un PAT con l'indirizzo IP dell'interfaccia.



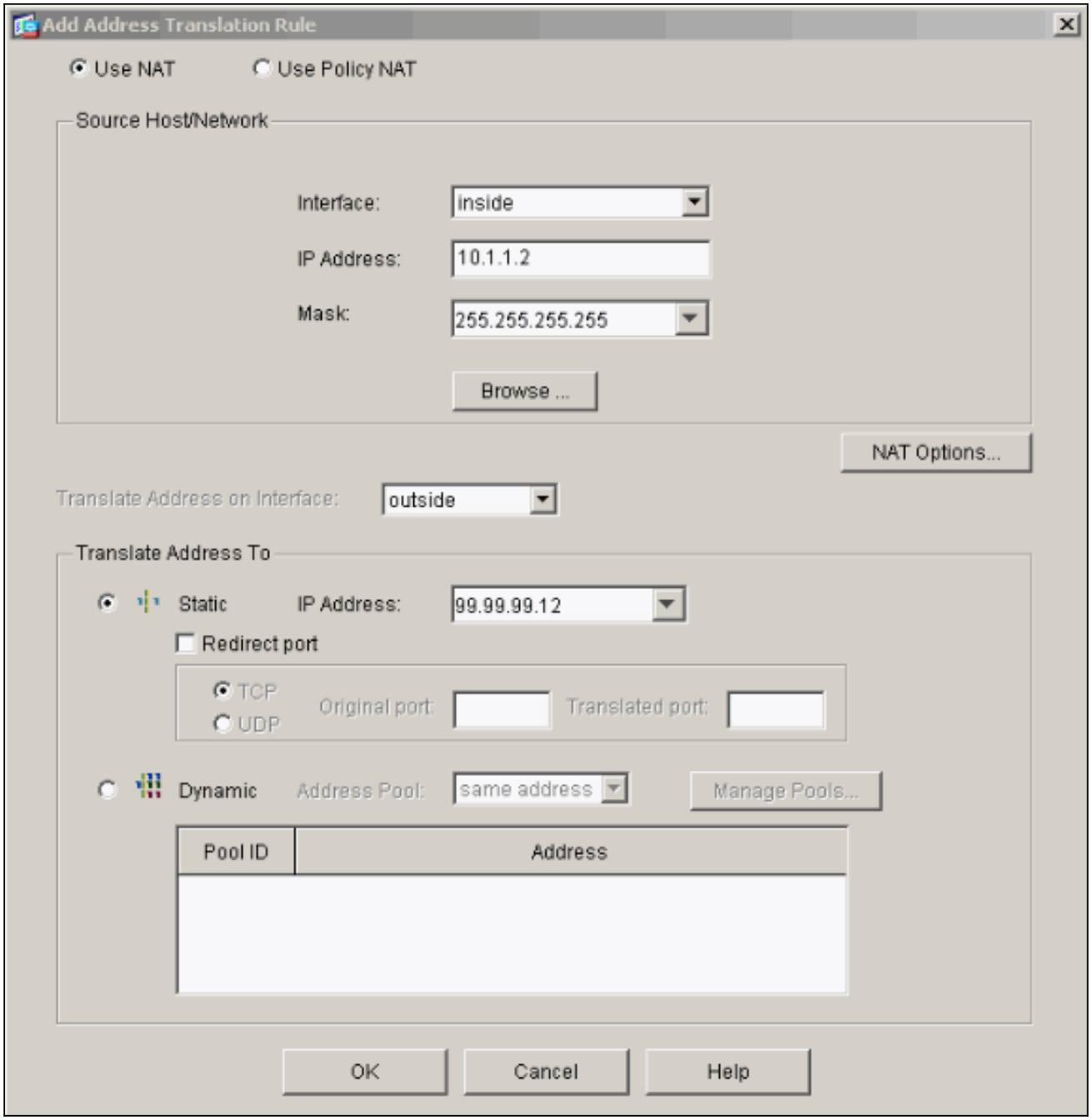
18. Fare clic su **OK** quando la parte è configurata.



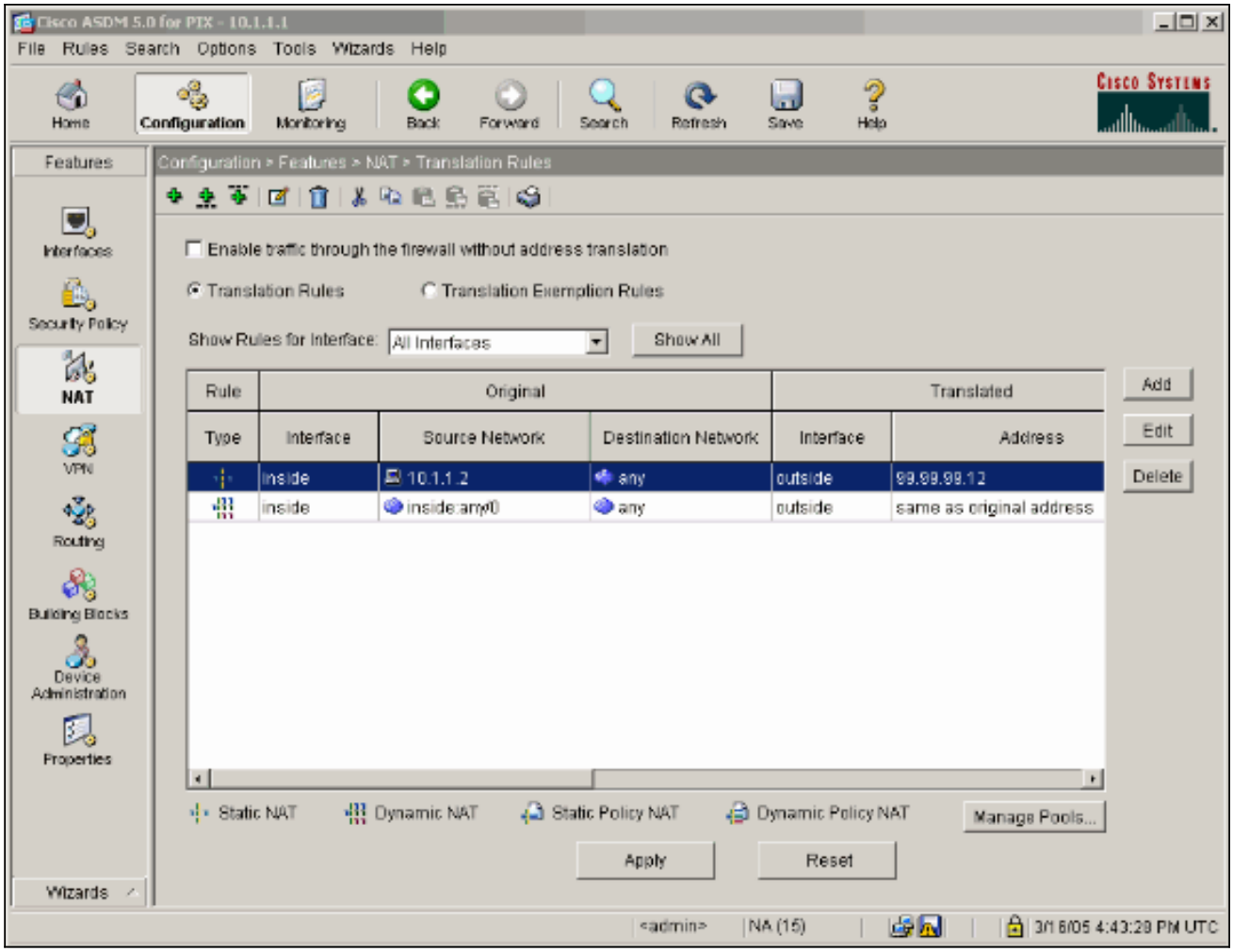
19. Per configurare la traduzione statica, fare clic su **Add** (Aggiungi).



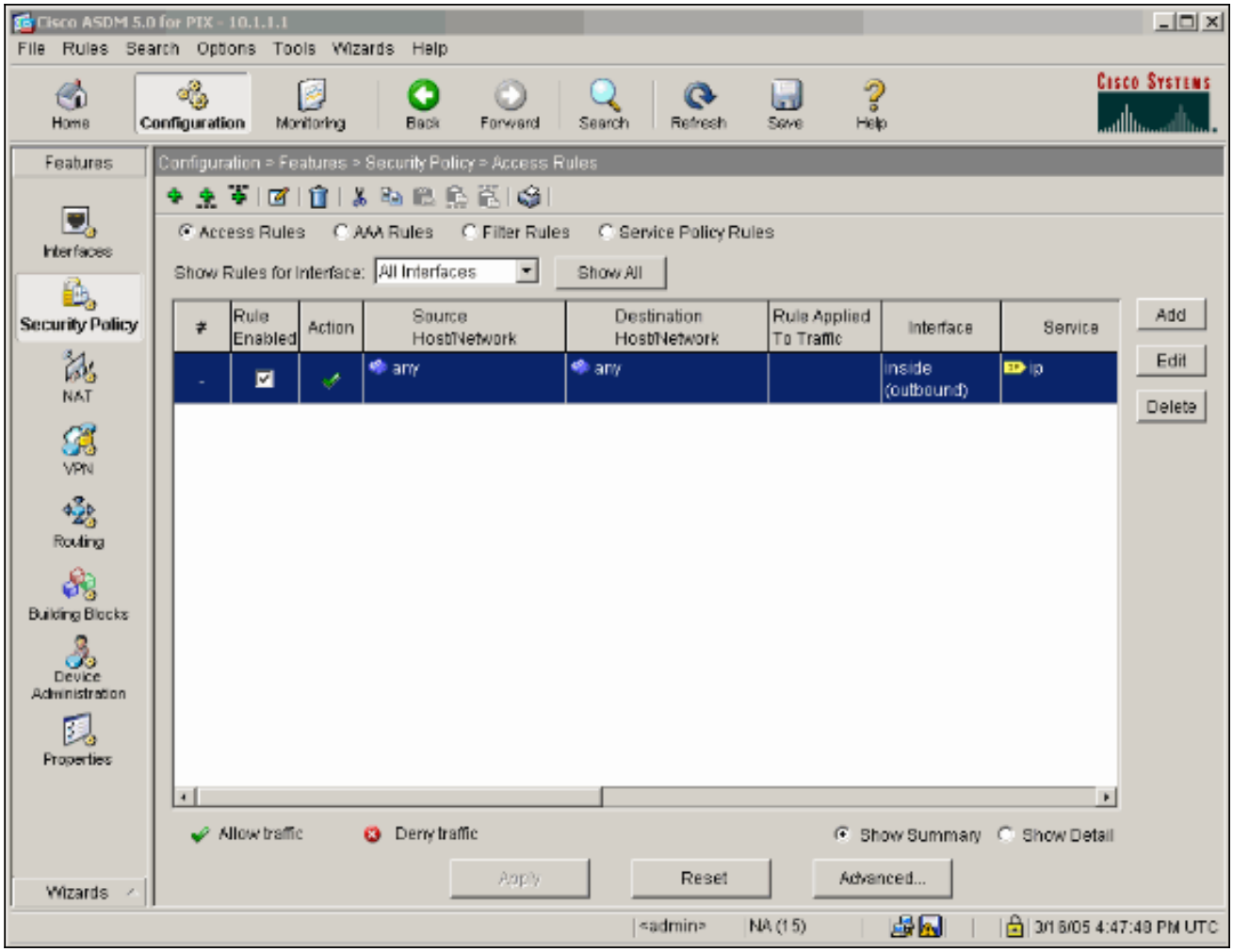
20. Selezionare dall'interno dell'elenco a discesa Interfaccia, quindi immettere l'indirizzo IP 10.1.1.2, la subnet mask 255.255.255.255, scegliere **Statico** e nel campo Indirizzo IP digitare l'indirizzo esterno **99.99.12**. Al termine, fare clic su **OK**.



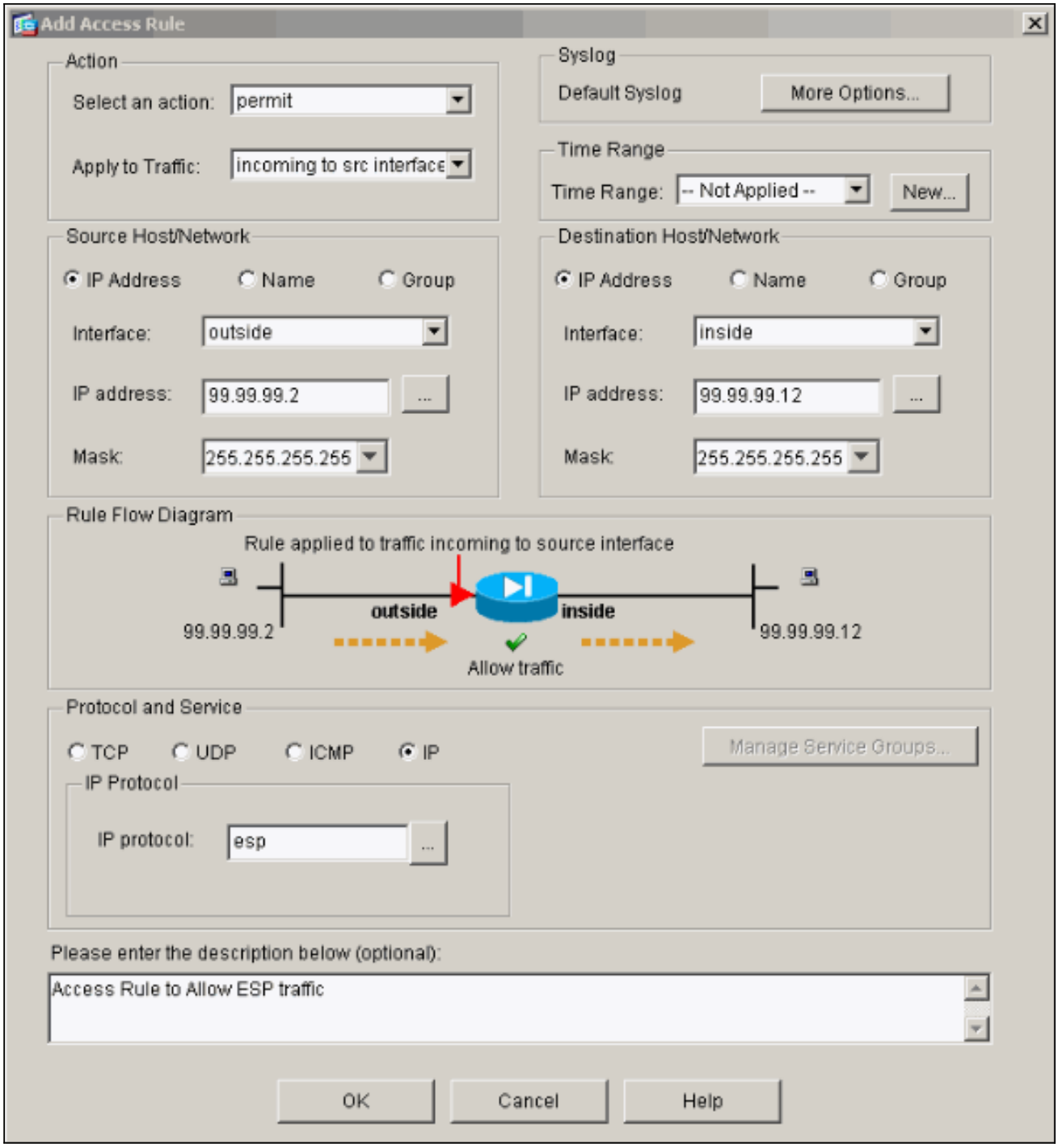
21. Fare clic su **Apply** (Applica) per accettare la configurazione dell'interfaccia. La configurazione viene inoltre inserita nel PIX.



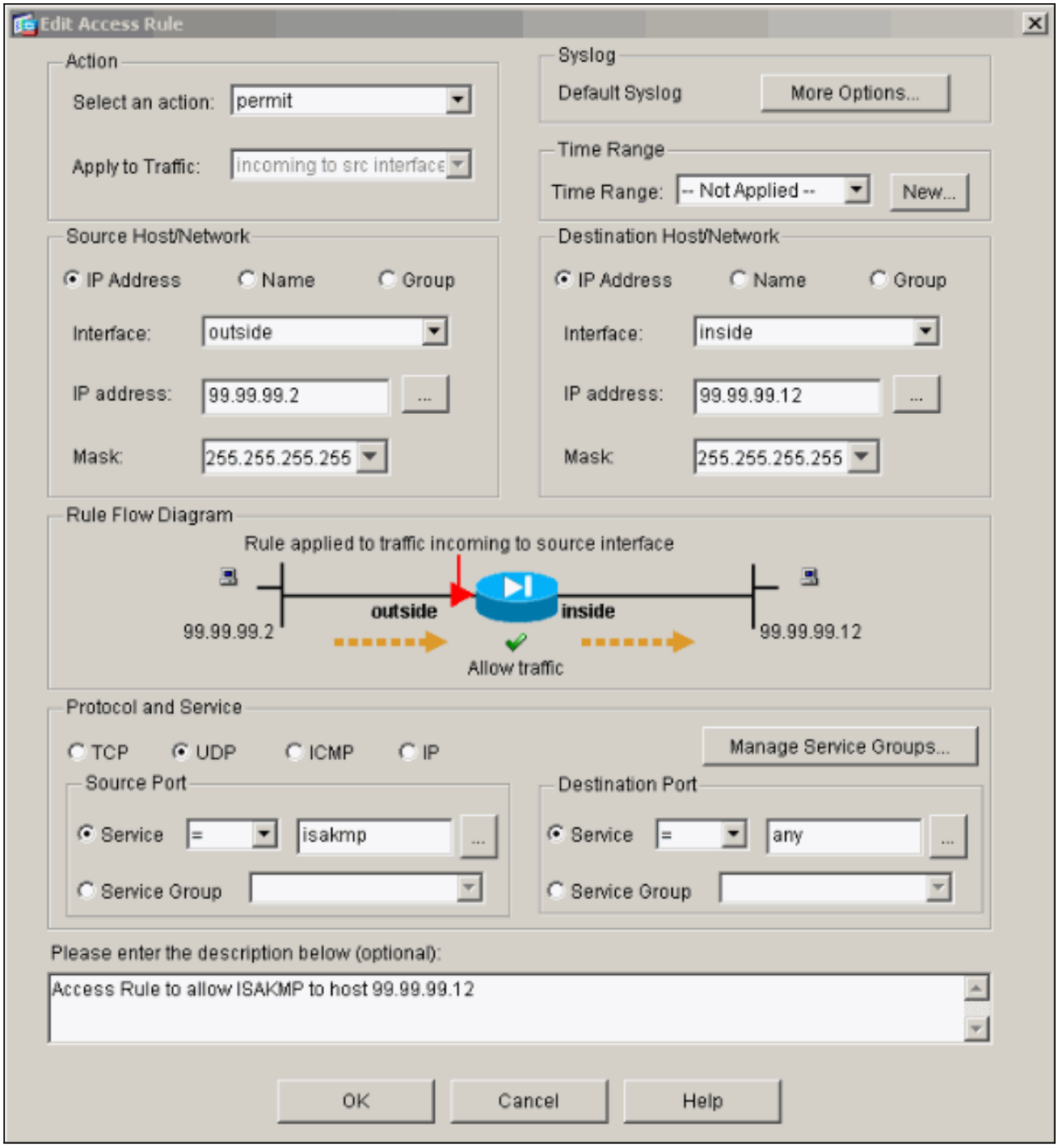
22. Per configurare la regola dei criteri di sicurezza, selezionare **Criteri di sicurezza** nella scheda
Funzionalità.



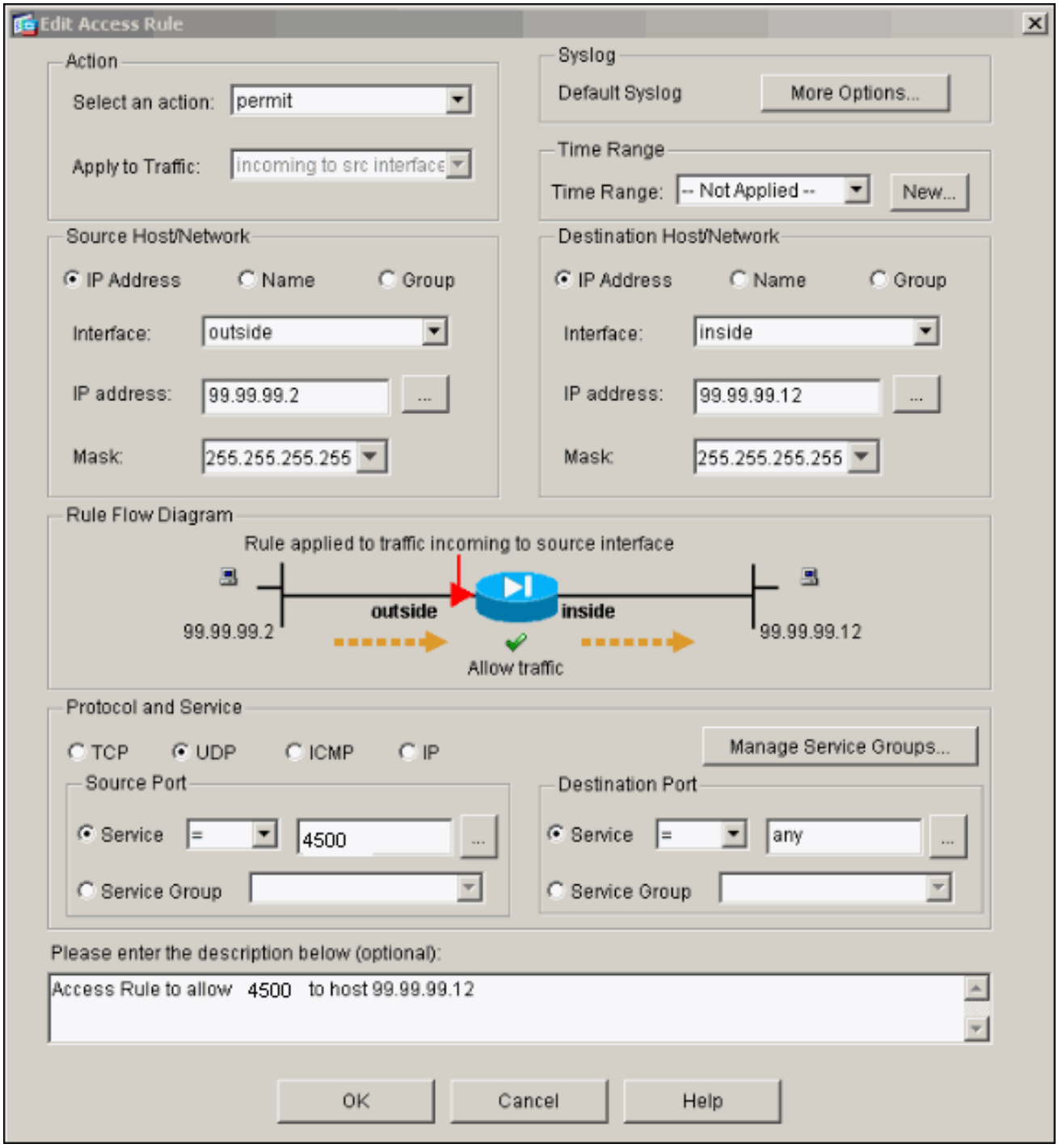
23. Per continuare, fare clic su **Add** (Aggiungi) per consentire il traffico esp e fare clic su **OK**.



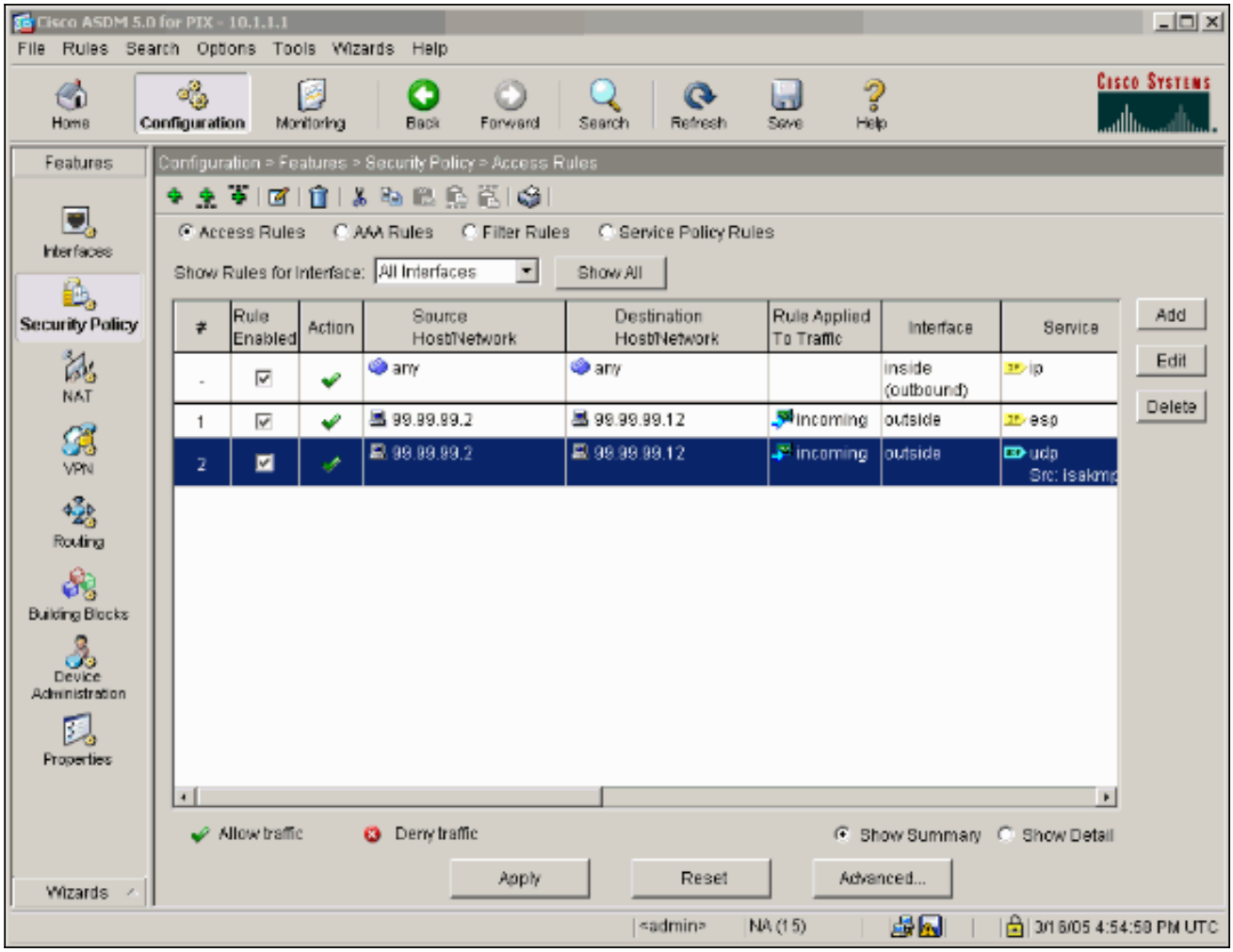
24. Per autorizzare il traffico ISAKMP, fare clic su **Add** (Aggiungi), quindi su **OK**.



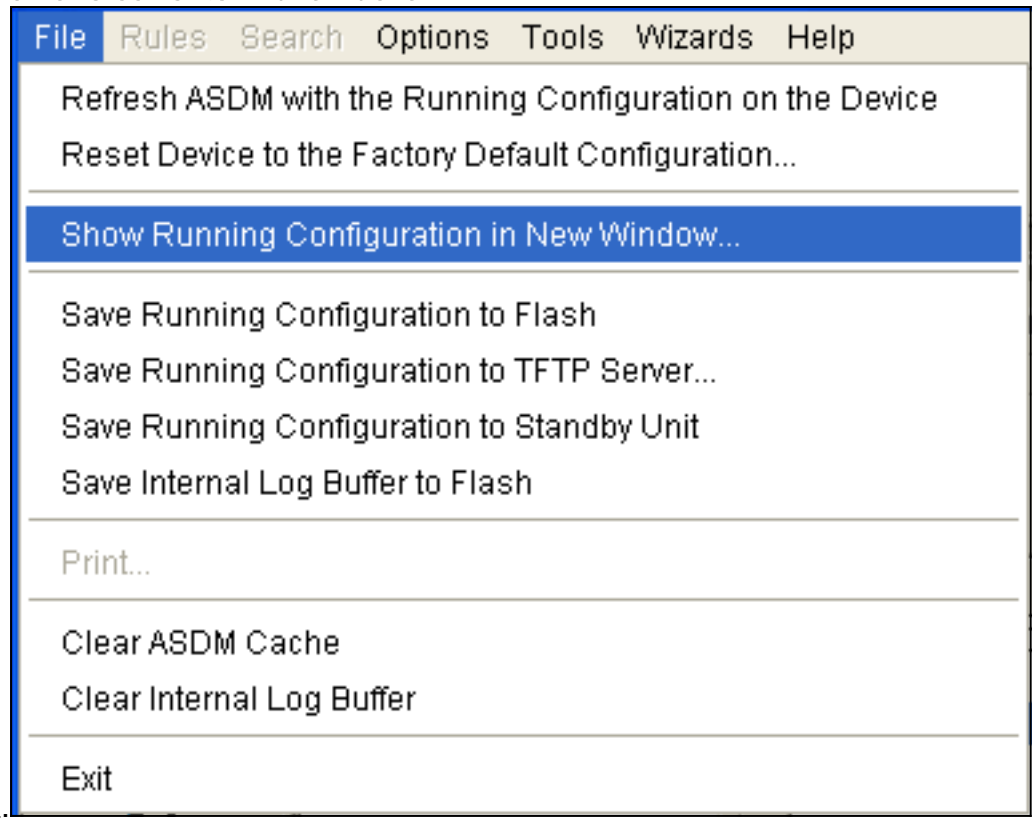
25. Fare clic su **Add** (Aggiungi) per consentire il traffico UDP porta 4500 per NAT-T e fare clic su **OK** per
continuare.



26. Per accettare la configurazione dell'interfaccia, fare clic su **Apply** (Applica). La configurazione viene inoltre inserita nel PIX.



27. Configurazione completata.Per visualizzare la configurazione CLI, scegliere **File > Mostra configurazione corrente** in **una nuova** finestra.



[Configurazione firewall PIX]

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
```

Configurazione di PIX Security Appliance e MPF (Modular Policy Framework)

Anziché utilizzare l'elenco degli accessi, usare il comando **inspect ipsec-pass-thru** in MPF(Modular Policy Framework) per passare il traffico IPsec attraverso le appliance di sicurezza PIX/ASA.

Questa ispezione è configurata per aprire i fori per il traffico ESP. Tutti i flussi di dati ESP sono consentiti quando esiste un flusso in avanti e non esiste alcun limite al numero massimo di connessioni consentite. AH non è permesso. Il timeout di inattività predefinito per i flussi di dati ESP è impostato per impostazione predefinita su 10 minuti. Questa ispezione può essere applicata in tutti i punti in cui è possibile eseguire altre ispezioni, incluse le modalità di comando class e match. L'ispezione delle applicazioni pass-through IPSec consente di attraversare agevolmente il traffico ESP (protocollo IP 50) associato a una connessione con porta UDP IKE 500. Evita la configurazione di lunghi elenchi degli accessi per consentire il traffico ESP e fornisce anche la sicurezza con timeout e connessioni massime. Utilizzare i comandi **class-map**, **policy-map** e **service-policy** per definire una classe di traffico, applicare il comando inspect alla classe e applicare il criterio a una o più interfacce. Se abilitato, il comando **inspect IPSec-pass-thru** consente un traffico ESP illimitato con un timeout di 10 minuti, che non è configurabile. È consentito il traffico NAT e 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.
- **show crypto engine connections active**: visualizza i pacchetti crittografati e decrittografati.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi di IPSec del router

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto engine**: visualizza il traffico crittografato.
- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.

Cancellazione delle associazioni di protezione

- **clear crypto isakmp**: cancella le associazioni di protezione IKE (Internet Key Exchange).
- **clear crypto ipsec sa**: cancella le associazioni di sicurezza IPsec.

Comandi per la risoluzione dei problemi per PIX

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

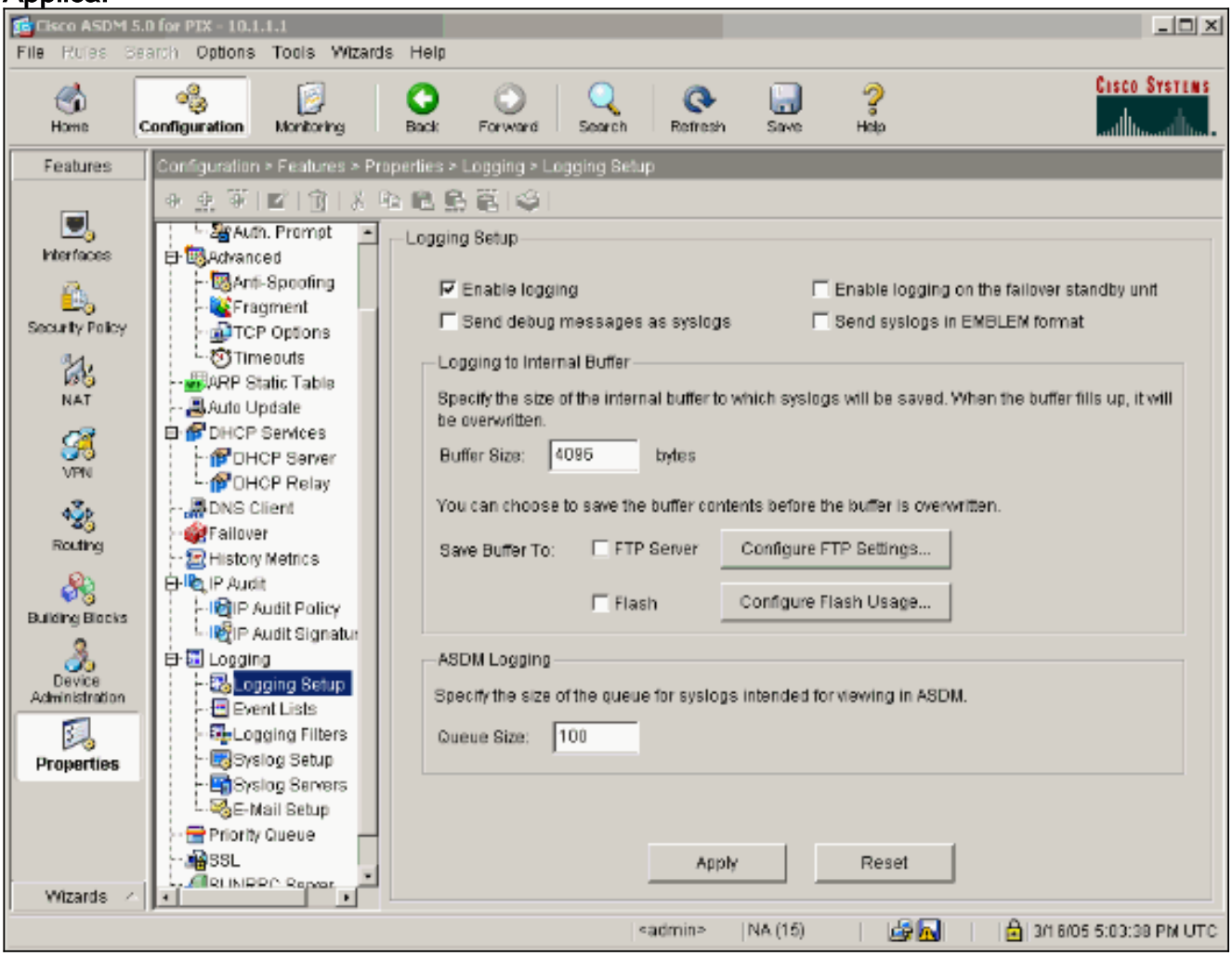
Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **logging buffer debugging**: visualizza le connessioni stabilite e negate agli host che passano

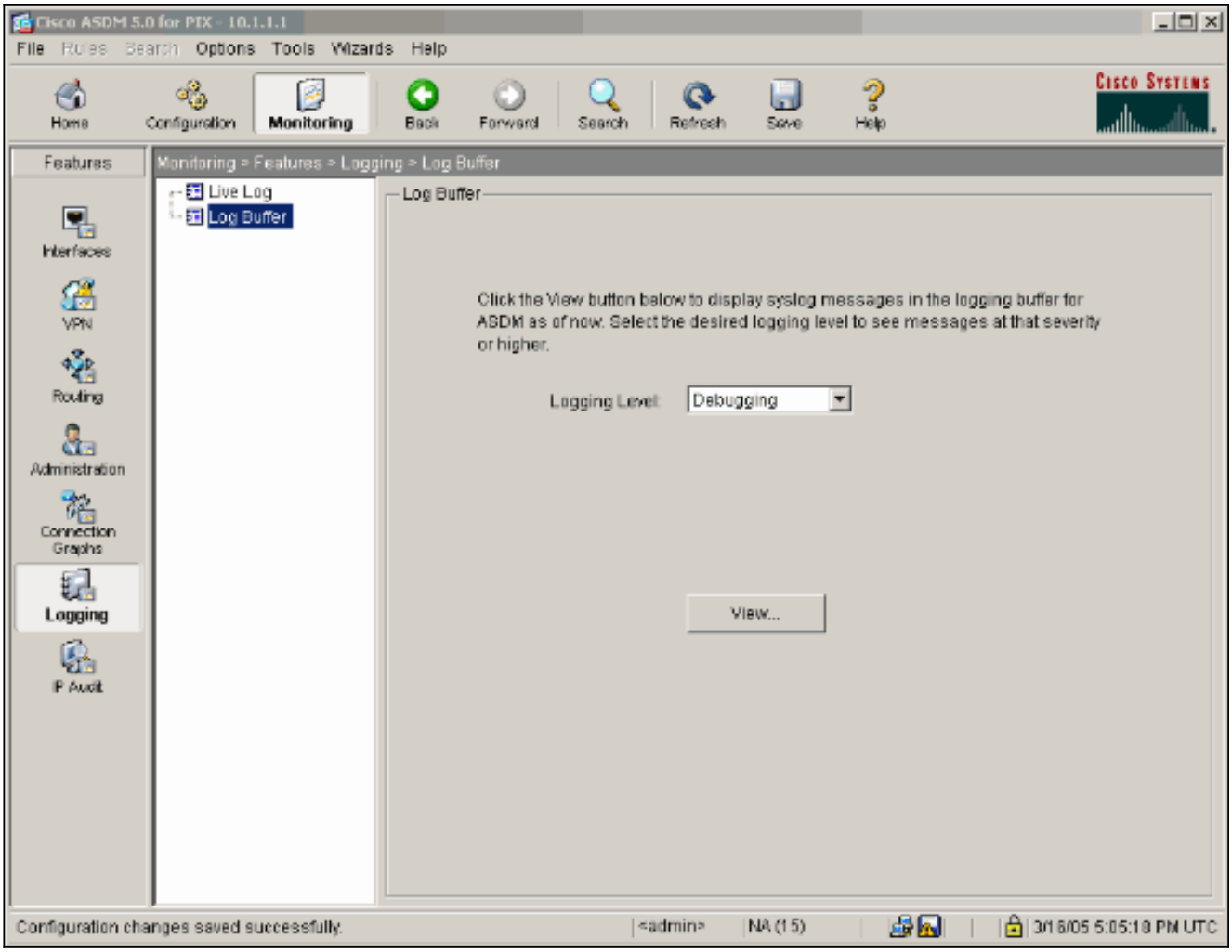
attraverso il PIX. Le informazioni vengono memorizzate nel buffer di registro PIX e l'output può essere visualizzato con il comando **show log**.

- ASDM può essere utilizzato per abilitare il log e anche per visualizzare i log, come mostrato in questa procedura.

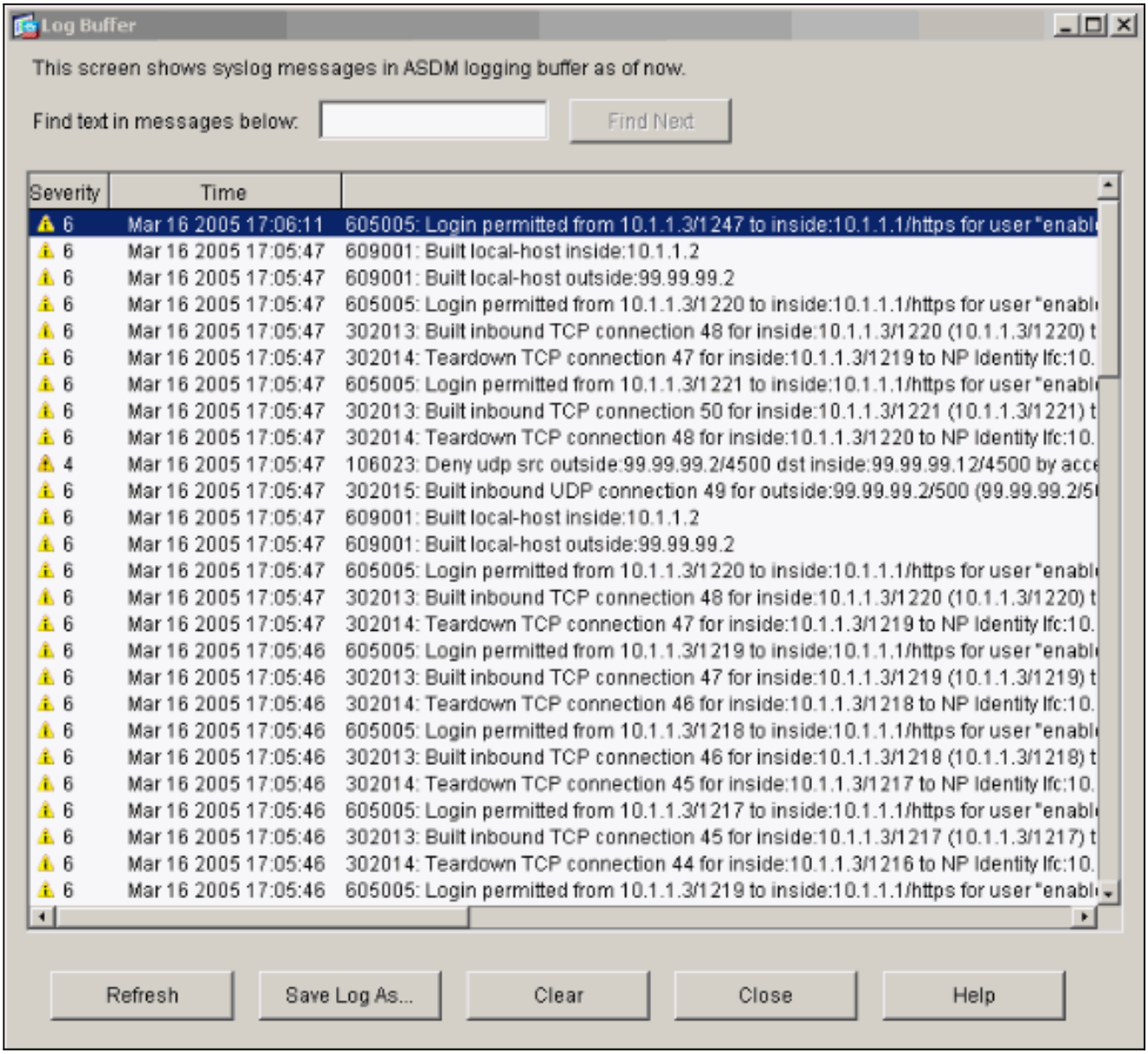
1. Scegliete **Configurazione > Proprietà > Log > Impostazione log > Abilita log** e fate clic su **Applica.**



2. Scegliere **Controllo > Log > Buffer di log > Al livello di log > Buffer di log**, quindi fare clic su **Visualizza**.



Questo è un esempio di buffer di registro.



Informazioni correlate

- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Pagina di supporto PIX
- Riferimenti per i comandi PIX
- Pagina di supporto NAT
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems