

# PIX/ASA 7.x e versioni successive: Esempio di connessione di più reti interne con la configurazione di Internet

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Configurazione](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione PIX con ASDM](#)

[Configurazione PIX con CLI](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Procedura di risoluzione dei problemi](#)

[Impossibile accedere ai siti Web per nome](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene fornita una configurazione di esempio per PIX/ASA Security Appliance versione 7.x e successive con più reti interne che si connettono a Internet (o a una rete esterna) tramite l'interfaccia della riga di comando (CLI) o Adaptive Security Device Manager (ASDM) versione 5.x e successive.

Per informazioni su come stabilire e risolvere i problemi di connettività tramite PIX/ASA, consultare il documento sulla [definizione e risoluzione dei problemi di connettività tramite Cisco Security Appliance](#).

Per informazioni sui comandi PIX comuni, fare riferimento a [Uso dei comandi nat, global, static, conduit e access-list](#) e a [Reindirizzamento porte \(inoltro\) su PIX](#).

**Nota:** alcune opzioni di altre versioni di ASDM possono essere diverse da quelle di ASDM 5.1. Per ulteriori informazioni, consultare la [documentazione di ASDM](#).

# Prerequisiti

## Requisiti

Quando si aggiungono più reti interne dietro un firewall PIX, tenere presente quanto segue:

- Il PIX non supporta l'indirizzamento secondario.
- È necessario usare un router dietro il PIX per ottenere il routing tra la rete esistente e la rete appena aggiunta.
- Il gateway predefinito di tutti gli host deve puntare al router interno.
- Aggiungere un percorso predefinito sul router interno che punti al PIX.
- Cancellare la cache ARP (Address Resolution Protocol) sul router interno.

Per consentire la configurazione del dispositivo da parte di ASDM, consultare il documento sulla [concessione dell'accesso HTTPS per ASDM](#).

## Componenti usati

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

- PIX Security Appliance 515E con versione software 7.1
- ASDM 5.1
- Router Cisco con software Cisco IOS® versione 12.3(7)T

**Nota:** questo documento è stato ricertificato con il software PIX/ASA versione 8.x e con il software Cisco IOS versione 12.4.

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.

## Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA Security Appliance versione 7.x e successive.

## Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

## Premesse

In questo scenario, sono disponibili tre reti interne (10.1.1.0/24, 10.2.1.0/24 e 10.3.1.0/24) da connettere a Internet (o a una rete esterna) tramite PIX. Le reti interne sono collegate all'interfaccia interna di PIX. La connettività Internet avviene tramite un router collegato all'interfaccia esterna del PIX. Il PIX ha l'indirizzo IP 172.16.1.1/24.

Le route statiche vengono utilizzate per indirizzare i pacchetti dalle reti interne a Internet e viceversa. Anziché utilizzare le route statiche, è inoltre possibile utilizzare un protocollo di routing dinamico, ad esempio RIP (Routing Information Protocol) o OSPF (Open Shortest Path First).

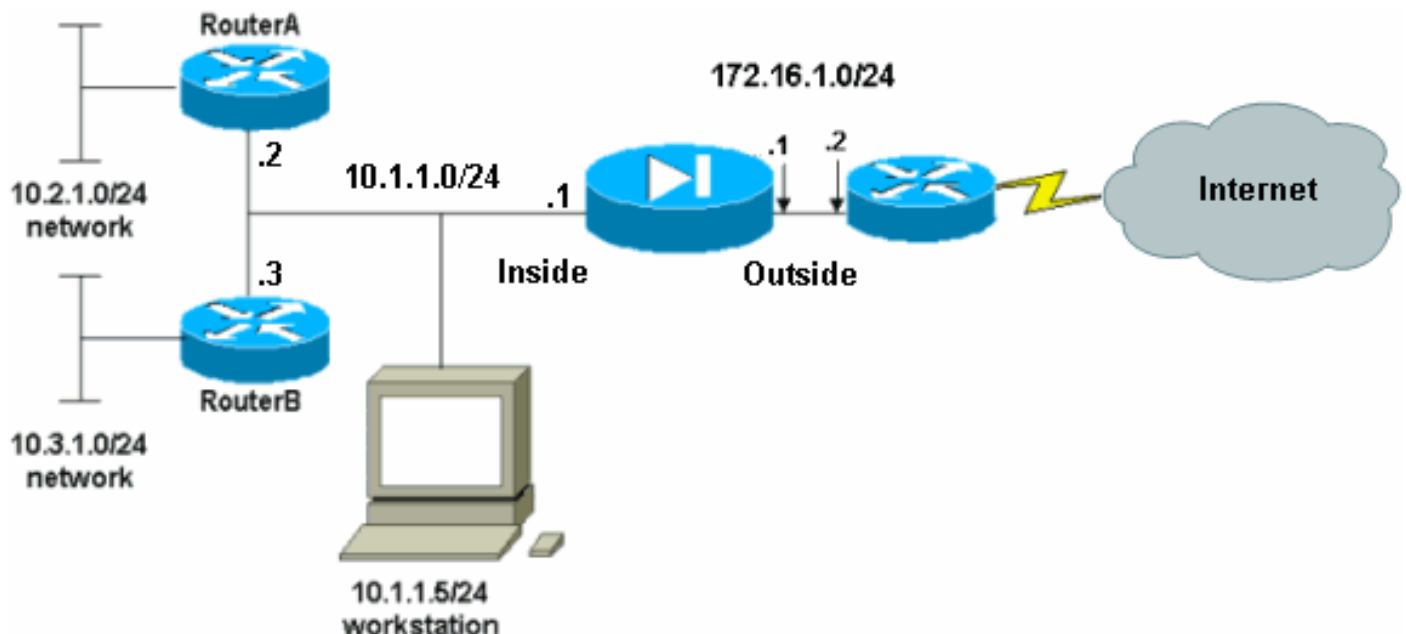
Gli host interni comunicano con Internet convertendo le reti interne in PIX utilizzando NAT dinamico (pool di indirizzi IP - da 172.16.1.5 a 172.16.1.10 ). Se il pool di indirizzi IP è esaurito, il PIX invierà (utilizzando l'indirizzo IP 172.16.1.4) gli host interni per raggiungere Internet.

Per ulteriori informazioni su NAT/PAT, fare riferimento alle [istruzioni PIX/ASA 7.x NAT e PAT](#).

**Nota:** se il NAT statico utilizza l'indirizzo IP esterno (global\_IP) per la conversione, potrebbe verificarsi una conversione. Pertanto, nella traduzione statica utilizzare la parola chiave interface anziché l'indirizzo IP.

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



Il gateway predefinito degli host sulla rete 10.1.1.0 punta al router A. Viene aggiunto un percorso predefinito sul router B che punta al router A. Il router A ha una route predefinita che punta al PIX all'interno dell'interfaccia.

## Configurazioni

Nel documento vengono usate queste configurazioni:

- [Configurazione routerA](#)
- [Configurazione routerB](#)
- [Configurazione di PIX Security Appliance 7.1](#)[Configurazione PIX con ASDM](#)[Configurazione CLI di PIX Security Appliance](#)

### Configurazione routerA

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!

interface Ethernet2/0
  ip address 10.2.1.1 255.255.255.0
  half-duplex
!

interface Ethernet2/1
  ip address 10.1.1.2 255.255.255.0
  half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterA#
```

### Configurazione routerB

```
RouterB#show running-config
Building configuration...
Current configuration : 1132 bytes
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!

interface FastEthernet0/0
```

```

ip address 10.1.1.3 255.255.255.0
speed auto
!
interface Ethernet1/0
ip address 10.3.1.1 255.255.255.0
half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterB#

```

Se si desidera utilizzare ASDM per la configurazione dell'appliance di sicurezza PIX, ma il dispositivo non è stato avviato, attenersi alla seguente procedura:

1. Collegare la console al PIX.
2. Da una configurazione cancellata, usare i prompt interattivi per abilitare ASDM per la gestione del PIX dalla workstation 10.1.1.5.

### Configurazione di PIX Security Appliance 7.1

```

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: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

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:
10.1.1.5

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  
    INFO: converting 'fixup protocol dns maximum-  
length 512' to MPF commands  
    INFO: converting 'fixup protocol ftp 21' to MPF  
commands  
    INFO: converting 'fixup protocol h323_h225  
1720' to MPF commands  
    INFO: converting 'fixup protocol h323_ras 1718-  
1719' to MPF commands  
    INFO: converting 'fixup protocol netbios 137-  
138' to MPF commands  
    INFO: converting 'fixup protocol rsh 514' to  
MPF commands  
    INFO: converting 'fixup protocol rtsp 554' to  
MPF commands  
    INFO: converting 'fixup protocol sip 5060' to  
MPF commands  
    INFO: converting 'fixup protocol skinny 2000'  
to MPF commands  
    INFO: converting 'fixup protocol smtp 25' to  
MPF commands  
    INFO: converting 'fixup protocol sqlnet 1521'  
to MPF commands  
    INFO: converting 'fixup protocol sunrpc_udp  
111' to MPF commands  
    INFO: converting 'fixup protocol tftp 69' to  
MPF commands  
    INFO: converting 'fixup protocol sip udp 5060'  
to MPF commands  
    INFO: converting 'fixup protocol xdmcp 177' to  
MPF commands  
  
Type help or '?' for a list of available commands.  
OZ-PIX>
```

## [Configurazione PIX con ASDM](#)

Per eseguire la configurazione tramite l'interfaccia utente grafica ASDM, completare i seguenti passaggi:

1. Dalla workstation 10.1.1.5, aprire un browser Web per utilizzare ASDM (in questo esempio, <https://10.1.1.1>).
2. Fare clic su **sì** nelle richieste di certificato.
3. Accedere con la password enable, come configurato in precedenza.
4. Se è la prima volta che ASDM viene eseguito sul PC, viene richiesto di utilizzare ASDM Launcher o ASDM come app Java. Nell'esempio, l'utilità di avvio ASDM è selezionata e installata.
5. Andare alla finestra Home ASDM e fare clic su **Configuration** (Configurazione).

Cisco ASDM 5.1 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

**Device Information**

General License

Host Name: **pixfirewall.default.domain.invalid**

PIX Version: **7.1(1)** Device Uptime: **14d 6h 4m 4s**

ASDM Version: **5.1(1)** Device Type: **PIX 515E**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **16 MB** Total Memory: **64 MB**

**VPN Status**

IKE Tunnels: **0** IPsec Tunnels: **0**

**System Resources Status**

CPU

CPU Usage (percent)

1% 17:58:19

Memory

Memory Usage (MB)

38MB 17:58:19

**Interface Status**

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1

Select an interface to view input and output Kbps

**Traffic Status**

Connections Per Second Usage

17:58:19

UDP: 0 TCP: 0 Total: 0

'inside' Interface Traffic Usage (Kbps)

17:58:19

Input Kbps: 0 Output Kbps: 1

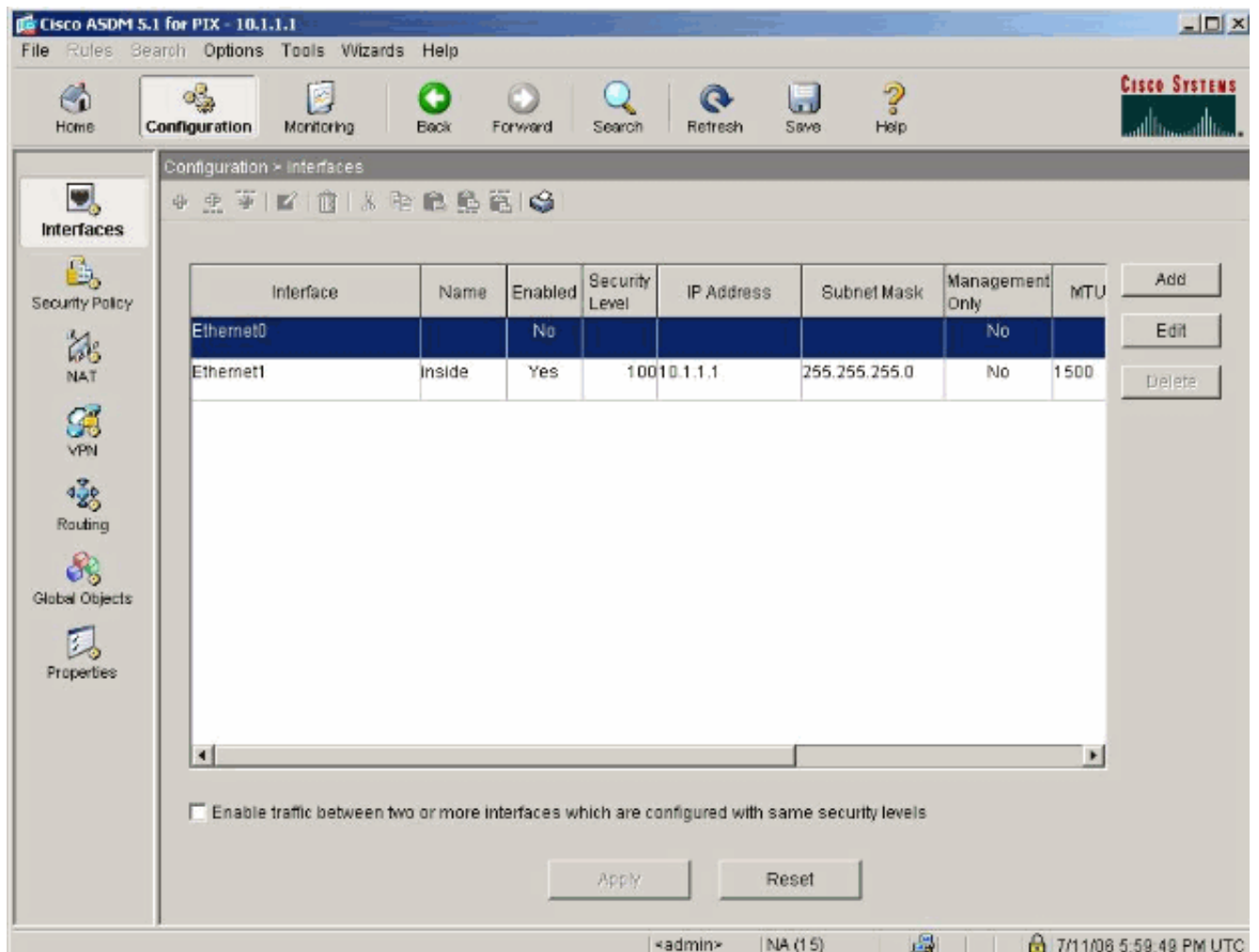
**Latest ASDM Syslog Messages**

-- Syslog Disabled --

Configure ASDM Syslog Filter

<admin> NA (15) 7/11/06 5:58:59 PM UTC

6. Per configurare l'interfaccia esterna, scegliere **Interfaccia > Modifica**.



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



Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface  Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP  Obtain Address via DHCP

IP Address:


Subnet Mask:

MTU:

Description:

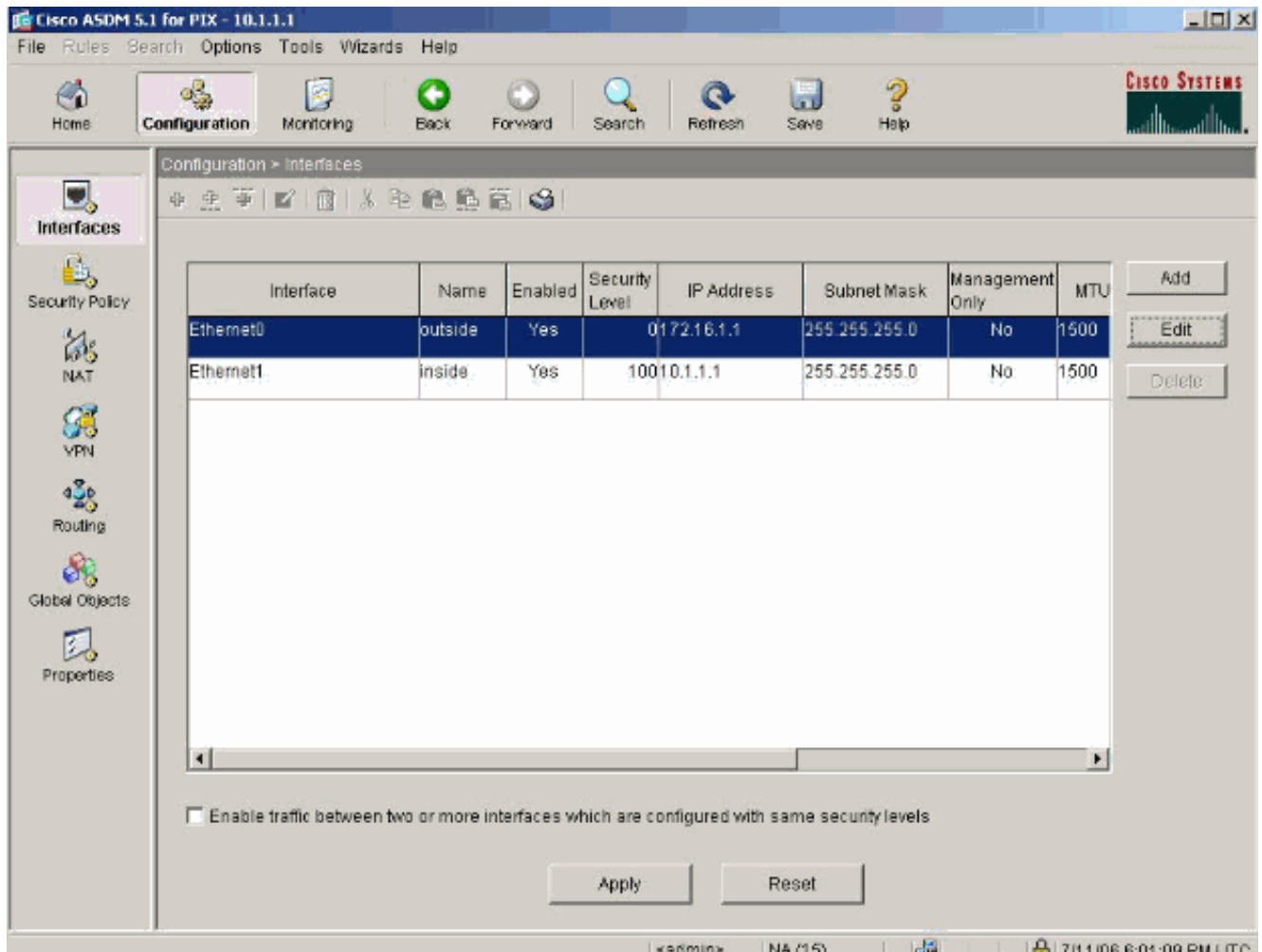
OK Cancel Help

8. Fare clic su **OK** nella finestra di dialogo Modifica del livello di protezione.

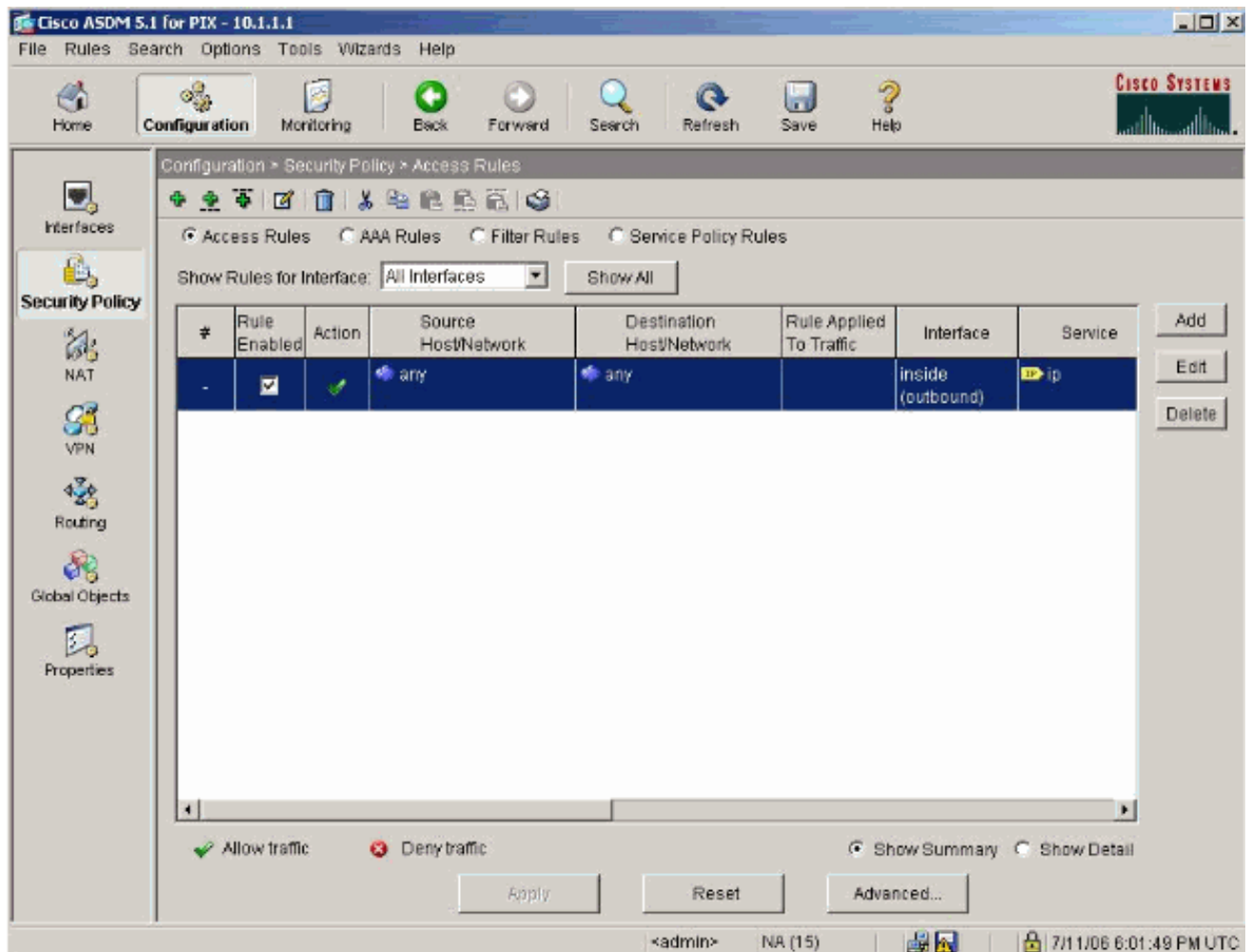
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

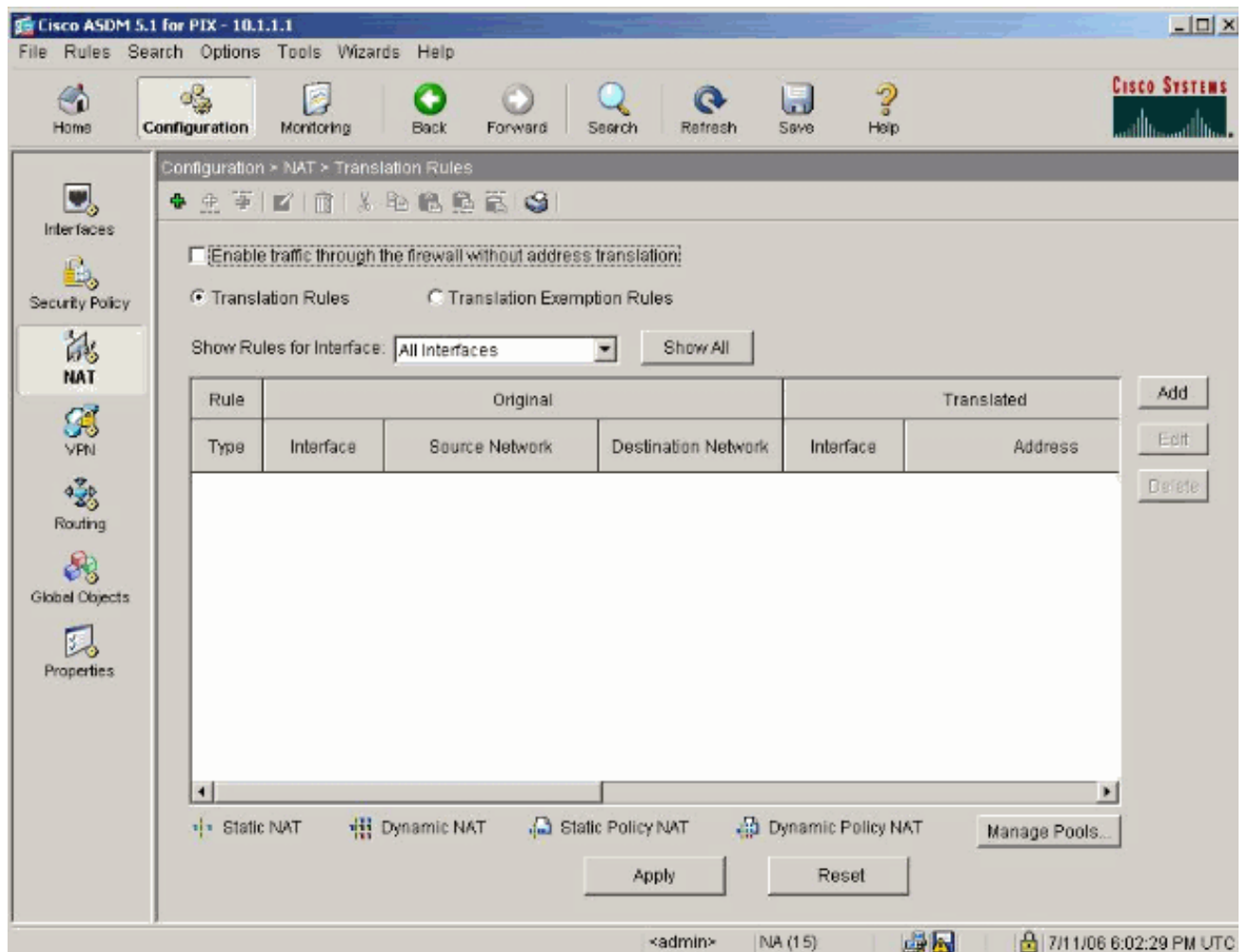
9. Fare clic su **Apply** (Applica) per accettare la configurazione dell'interfaccia. La configurazione viene inoltre inserita nel PIX.



10. Per esaminare la regola del criterio di protezione utilizzata, scegliere **Criterio di protezione** nella scheda Funzionalità. Nell'esempio viene utilizzata la regola interna predefinita.



11. Nell'esempio viene utilizzato NAT. Deselezionare la casella di controllo **Abilita traffico attraverso il firewall senza conversione indirizzi** e fare clic su **Aggiungi** per configurare la regola NAT.



12. Configurare la rete di origine. Nell'esempio, viene usato 10.0.0.0 per l'indirizzo IP e 255.0.0.0 per la maschera. Per definire gli indirizzi del pool NAT, fare clic su **Manage Pools** (Gestisci pool).

**Add Address Translation Rule**

Use NAT      Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static     IP Address:

Redirect port

TCP     Original port:      Translated port:

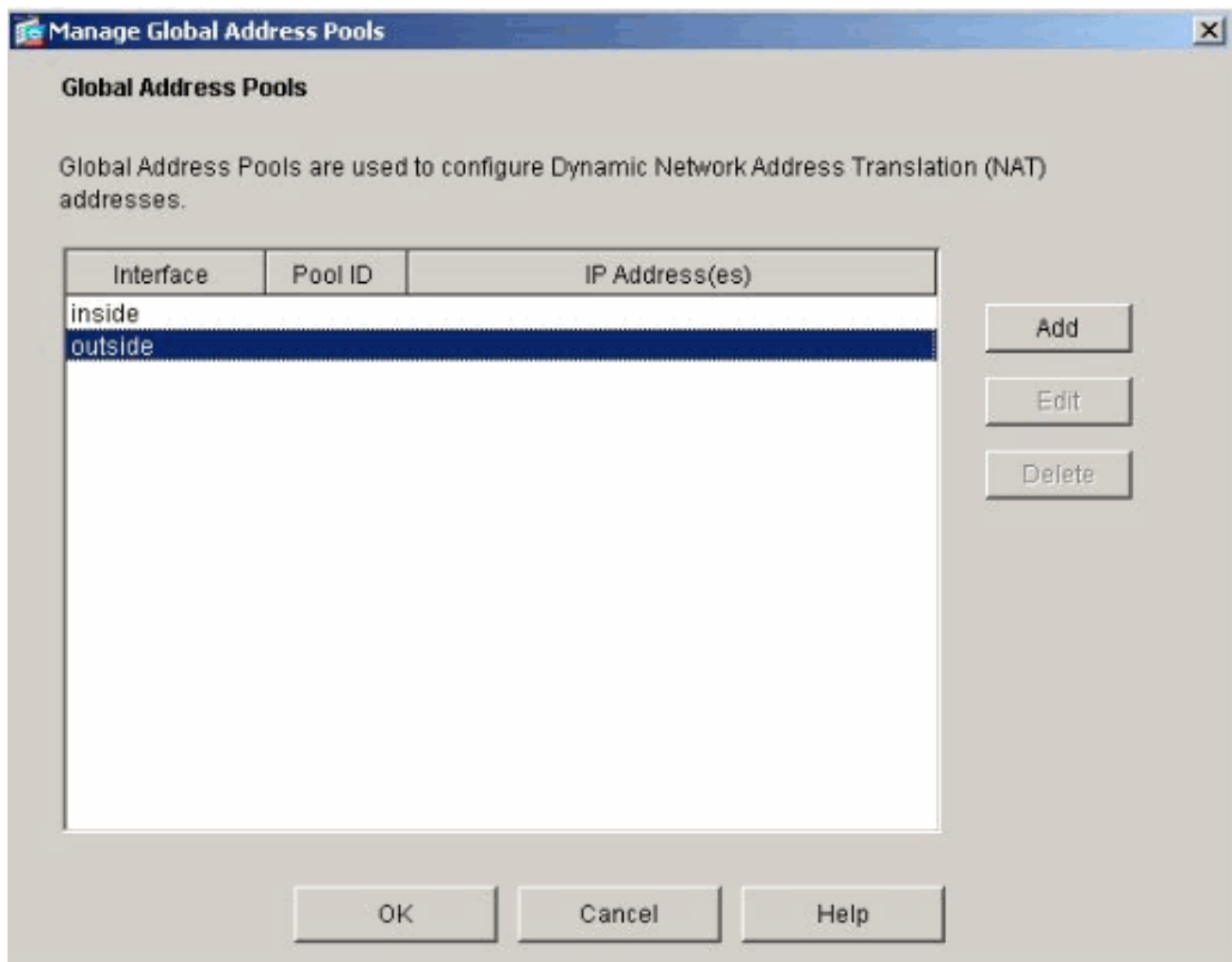
UDP

Dynamic     Address Pool:     

Pool ID	Address
N/A	No address pool defined

13. Selezionare l'interfaccia esterna e fare clic su **Add** (Aggiungi).



14. In questo esempio vengono configurati un pool di indirizzi Range e PAT. Configurare l'intervallo dell'indirizzo del pool NAT e fare clic su **OK**.

**Add Global Pool Item**

Interface:  Pool ID:

Range  
 Port Address Translation (PAT)  
 Port Address Translation (PAT) using the IP address of the interface

IP Address:  —

Network Mask (optional):

15. Per configurare l'indirizzo PAT, selezionare l'interfaccia esterna al passaggio 13. Fare clic su OK.

**Add Global Pool Item**

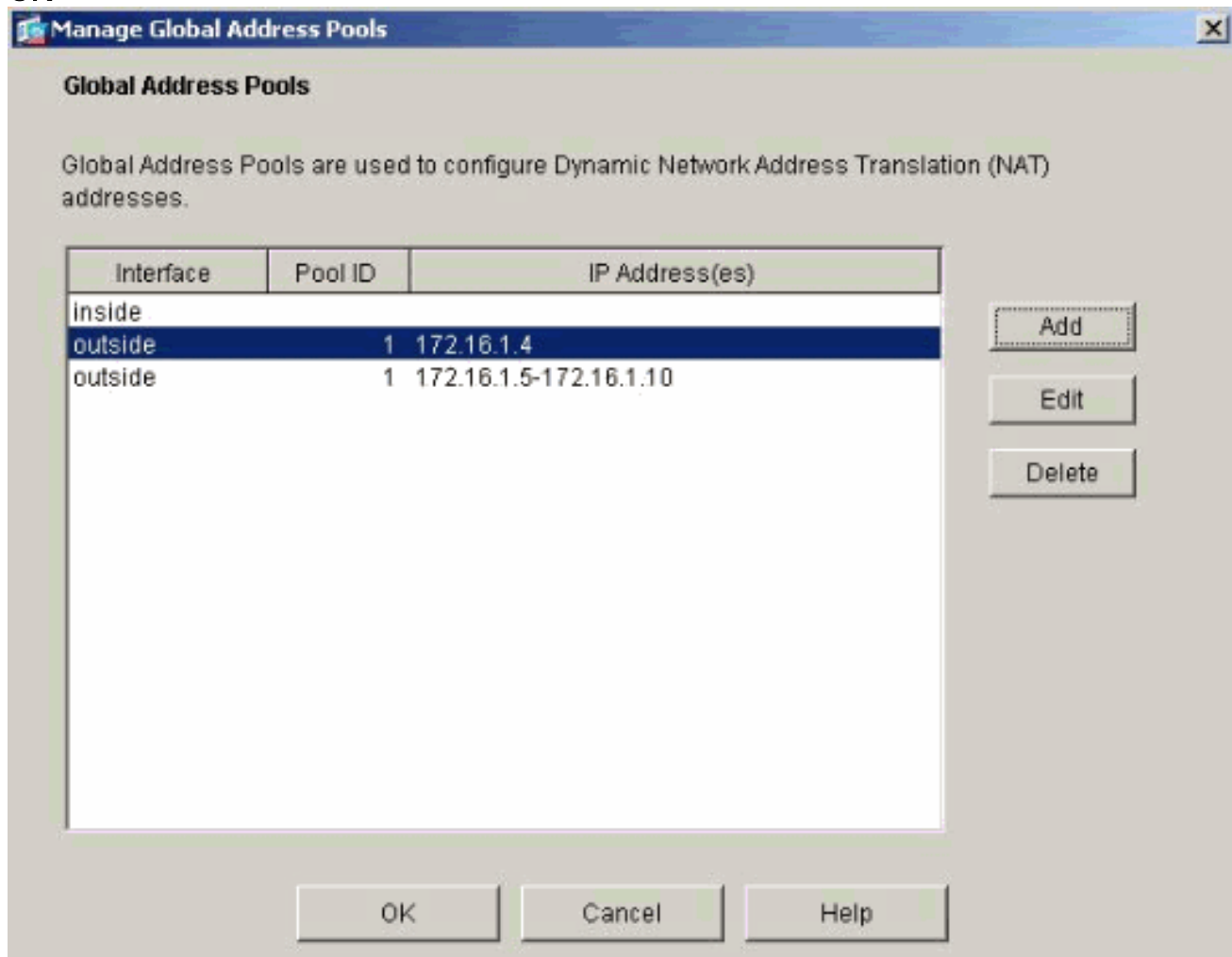
Interface:  Pool ID:

Range  
 Port Address Translation (PAT)  
 Port Address Translation (PAT) using the IP address of the interface

IP Address:  —

Network Mask (optional):

Per continuare, fare clic su  
**OK.**



16. Nella finestra Modifica regola di conversione indirizzi selezionare l'ID pool che deve essere utilizzato dalla rete di origine configurata. Fare clic su **OK.**



**Edit Address Translation Rule**

Use NAT    
 Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static     IP Address:

Redirect port

TCP     Original port:      Translated port:

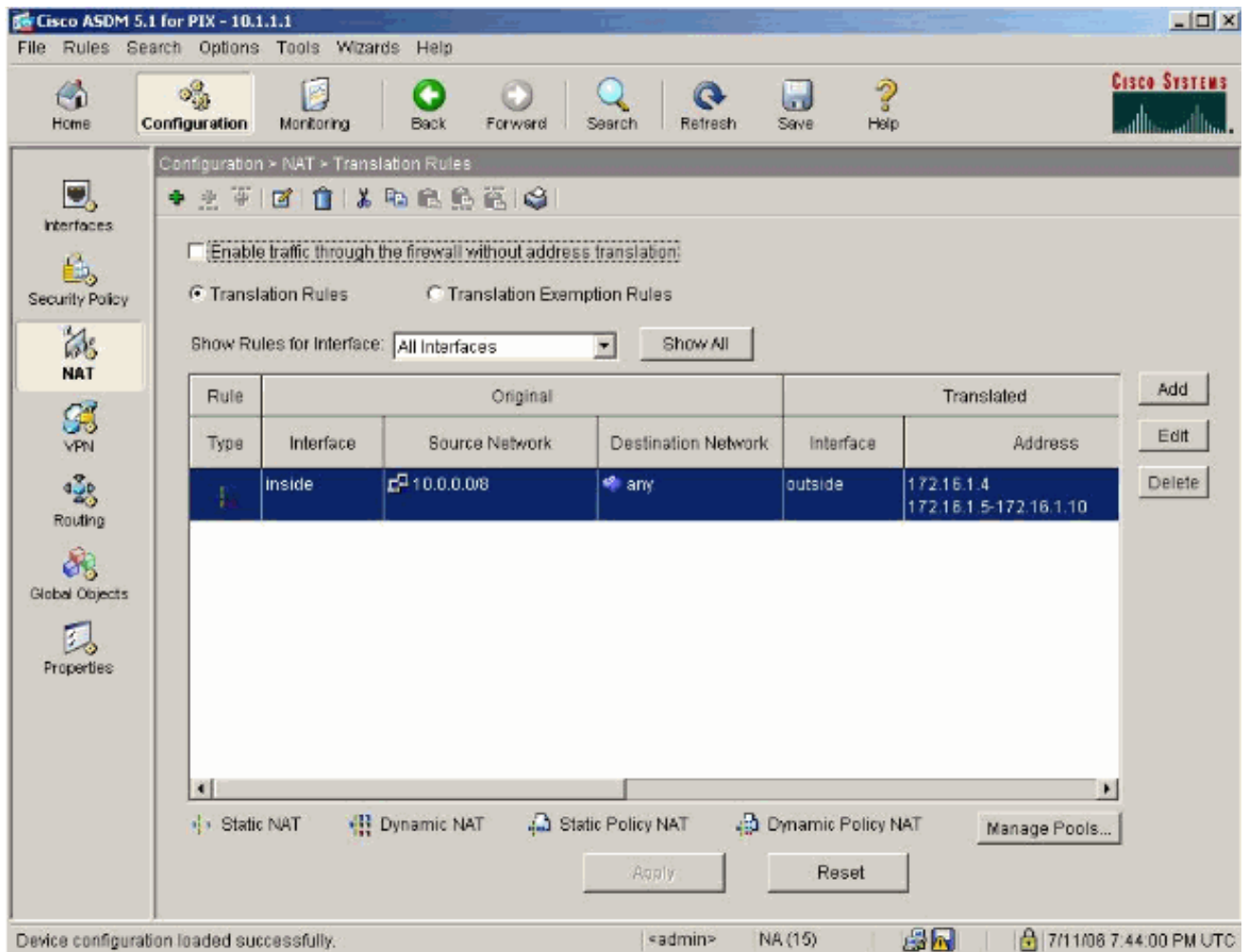
UDP

Dynamic     Address Pool:     

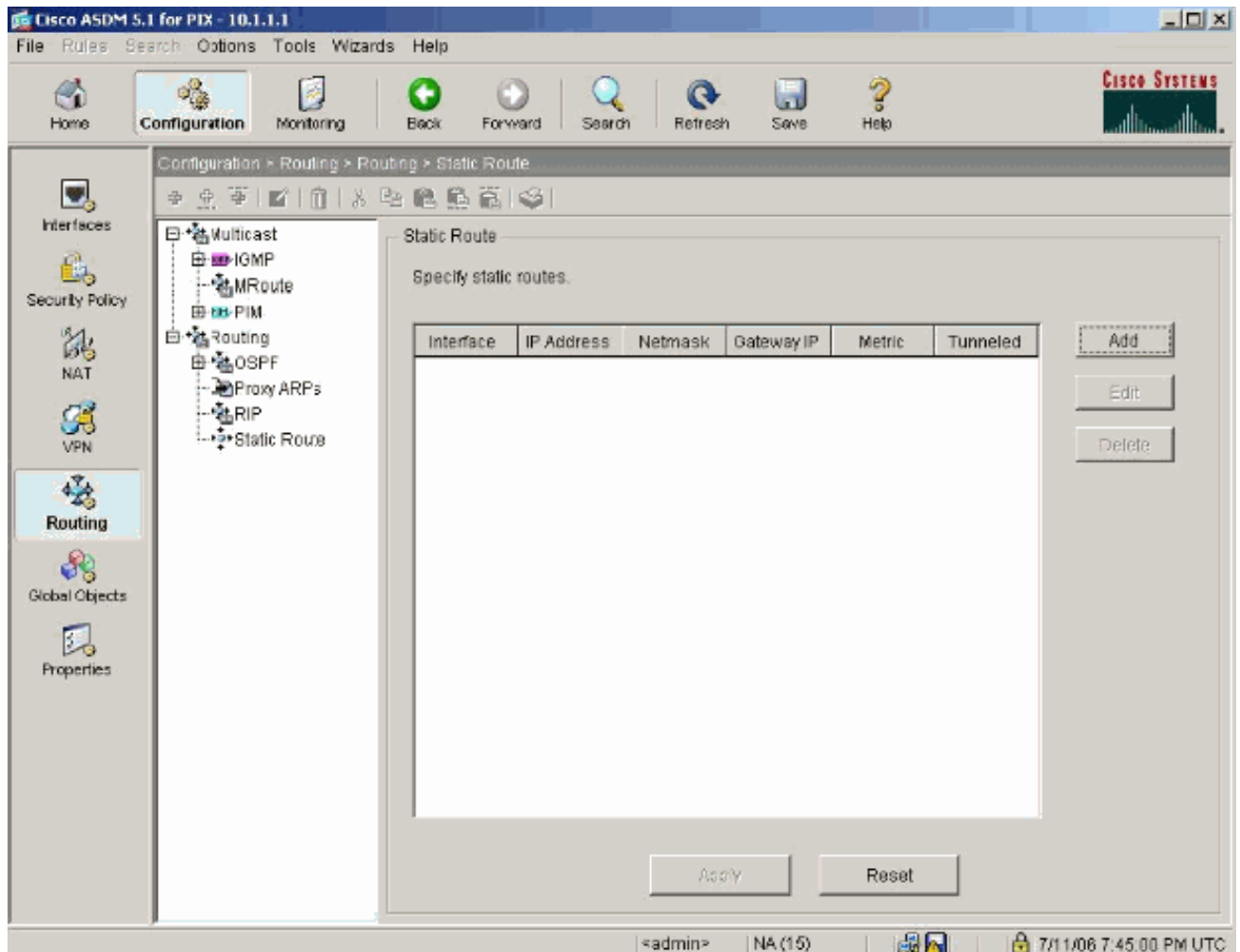
Pool ID	Address
1	172.16.1.4 172.16.1.5-172.16.1.10

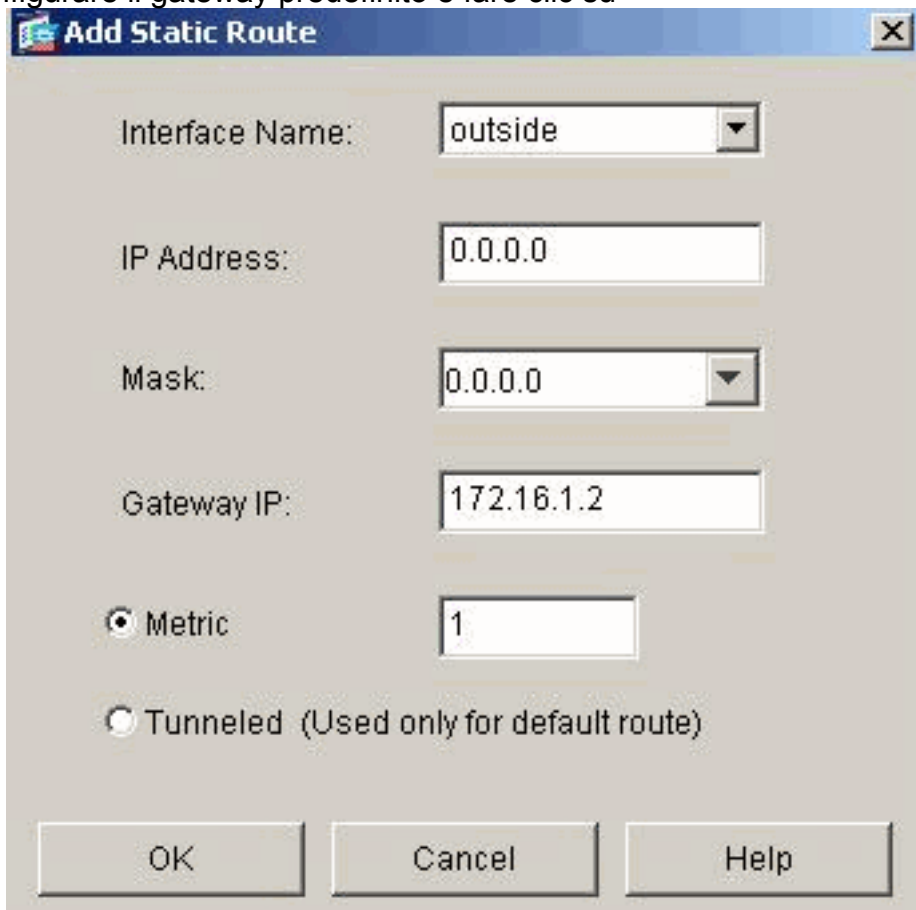
17. Fare clic su **Apply** (Applica) per eseguire il push della regola NAT configurata nel PIX.



18. Nell'esempio vengono utilizzate route statiche. Fare clic su **Routing**, selezionare **Static Route**, quindi fare clic su **Add**.



19. Configurare il gateway predefinito e fare clic su



OK.

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

**Add Static Route** [X]

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

interne.

**Add Static Route** [X]

Interface Name:

IP Address:

Mask:

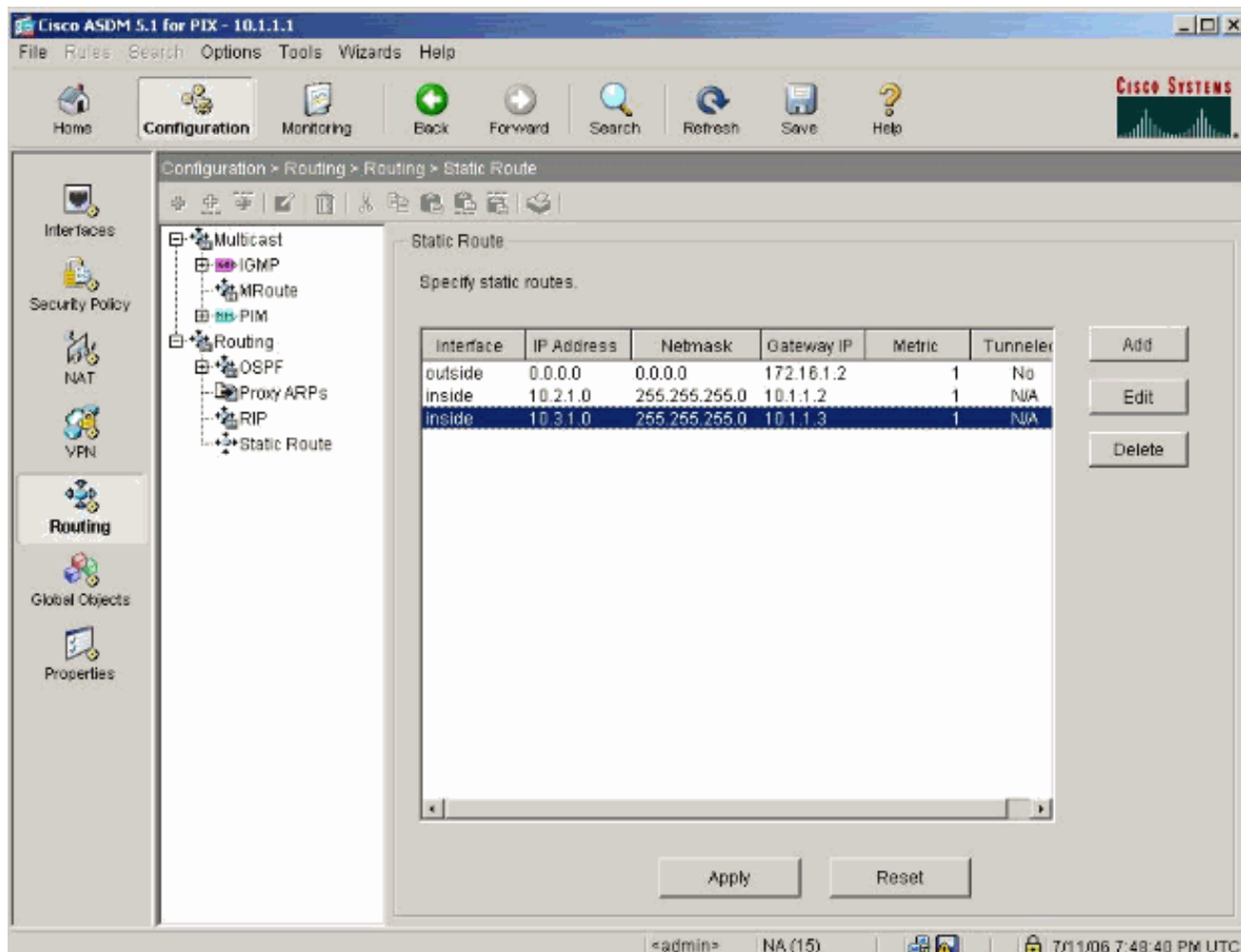
Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

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



## Configurazione PIX con CLI

La configurazione tramite l'interfaccia grafica ASDM è ora completata.

È possibile visualizzare questa configurazione dalla CLI:

```

PIX Security Appliance CLI

pixfirewall(config)#write terminal
PIX Version 7.0(0)102
names
!
interface Ethernet0
  nameif outside
  security-level 0
  ip address 172.16.1.1 255.255.255.0
!

interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!---- Assign name and IP address to the interfaces enable
password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control
!---- Enforce a strict NAT for all the traffic through
the Security appliance global (outside) 1 172.16.1.5-

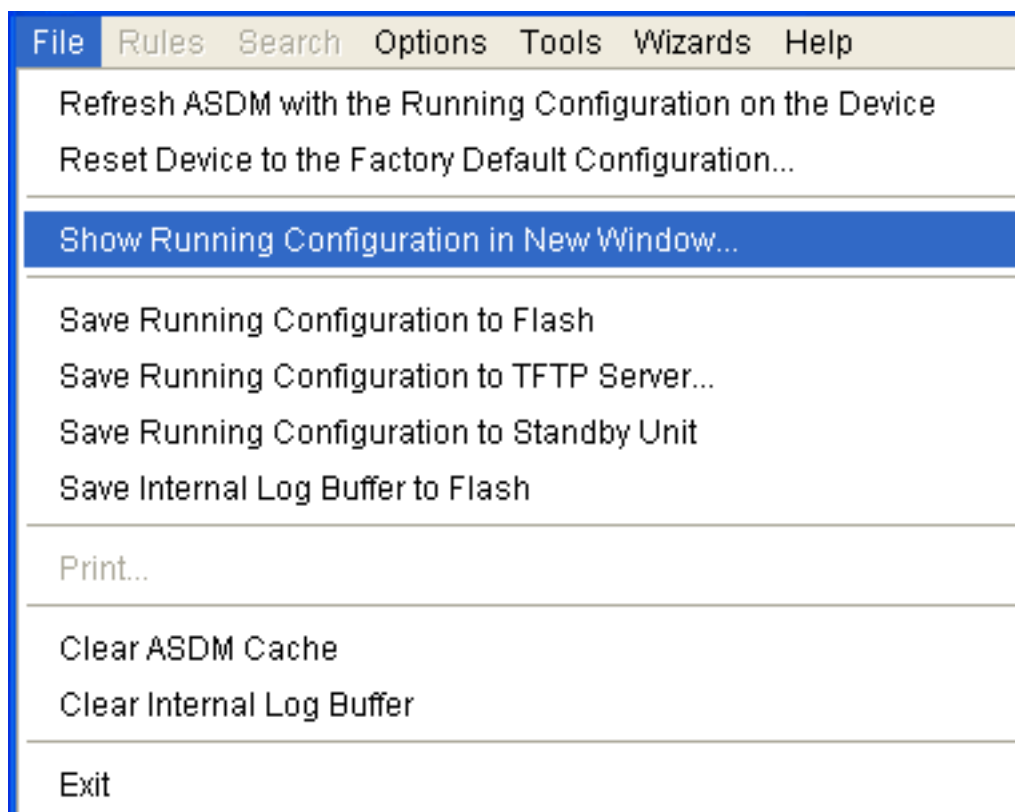
```

```

172.16.1.10 netmask 255.255.255.0
!--- Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0
!--- Define a single IP address 172.16.1.4 with NAT ID 1
to be used for PAT nat (inside) 1 10.0.0.0 255.0.0.0
!--- Define the inside networks with same NAT ID 1 used
in the global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1
!--- Configure static routes for routing the packets
towards the internal network route outside 0.0.0.0
0.0.0.0 172.16.1.2 1
!--- Configure static route for routing the packets
towards the Internet (or External network) 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
!--- Enable the HTTP server on PIX for ASDM access http
10.1.1.5 255.255.255.255 inside
!--- Enable HTTP access from host 10.1.1.5 to configure
PIX using ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bfff9bbaa3d815fc9fd269a3f67fef5 : end

```

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



## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

# Risoluzione dei problemi

## Comandi per la risoluzione dei problemi

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

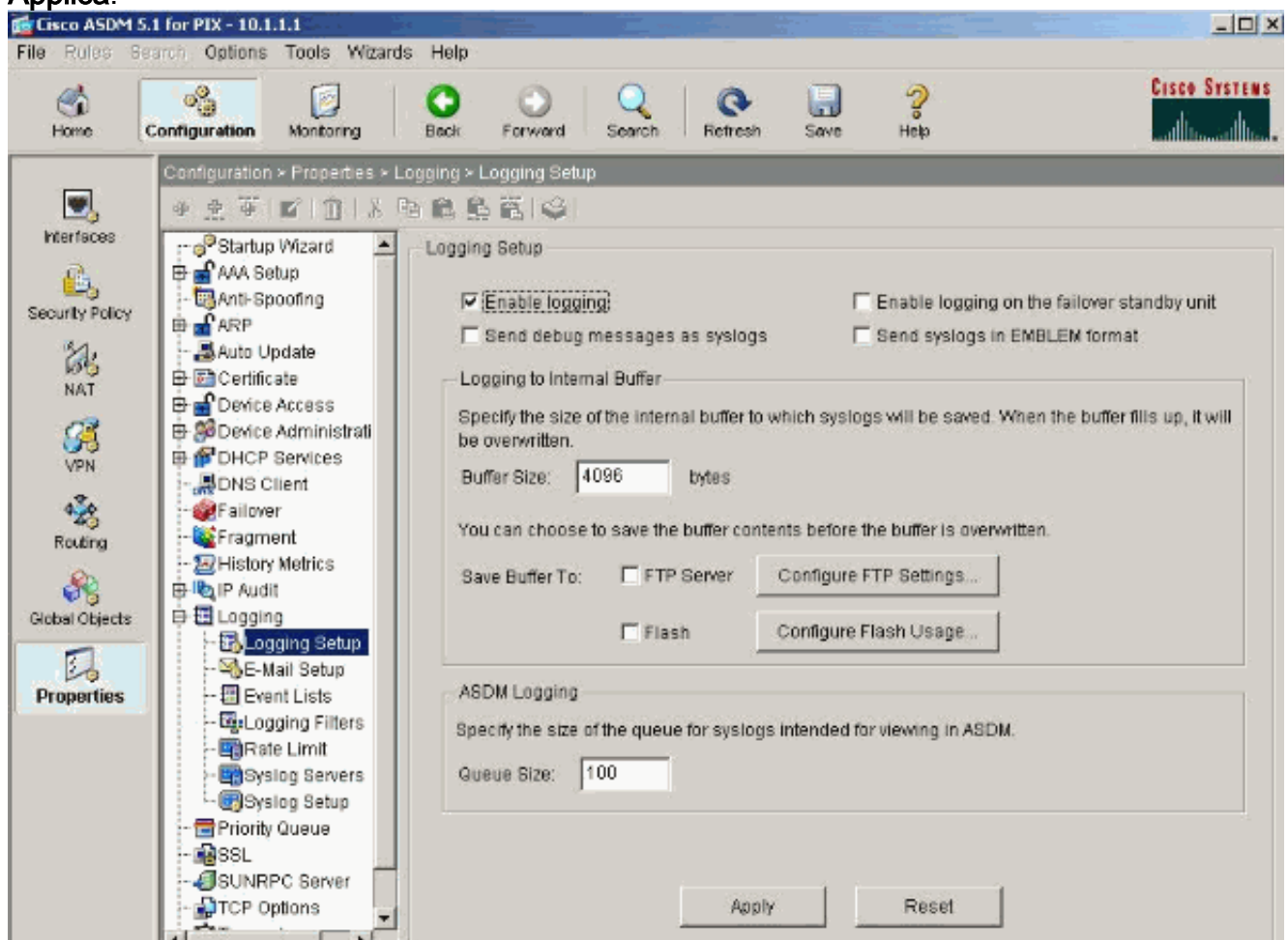
**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

- **debug icmp trace:** visualizza se le richieste ICMP dagli host raggiungono il PIX. Per eseguire il debug, aggiungere il comando **access-list** per autorizzare l'uso di ICMP nella configurazione.
- **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**.

## Procedura di risoluzione dei problemi

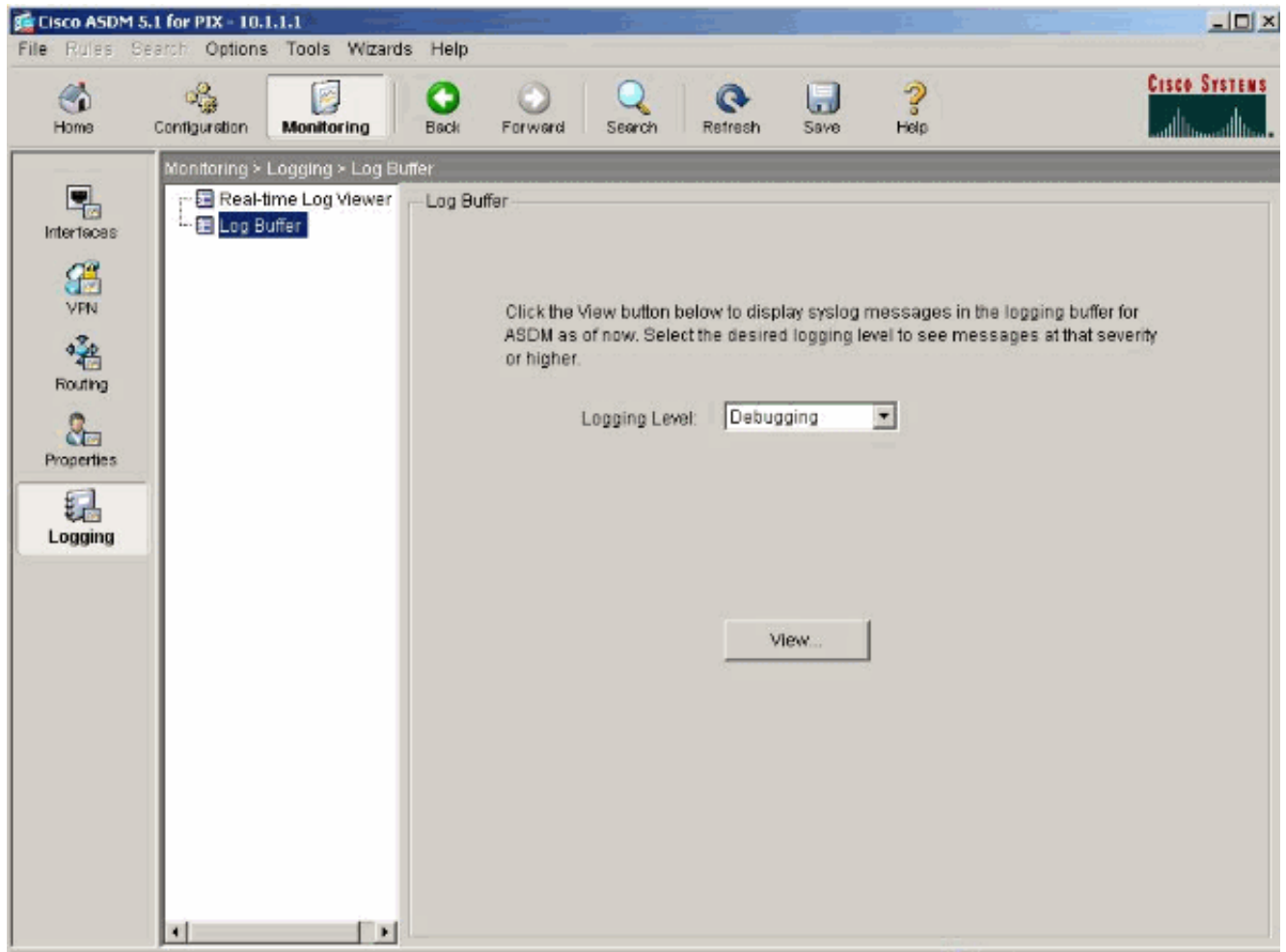
ASDM può essere utilizzato per abilitare il logging e anche per visualizzare i log:

1. Scegliete **Configurazione > Proprietà > Registrazione > Impostazione registrazione**, selezionate **Abilita registrazione** e fate clic su **Applica**.



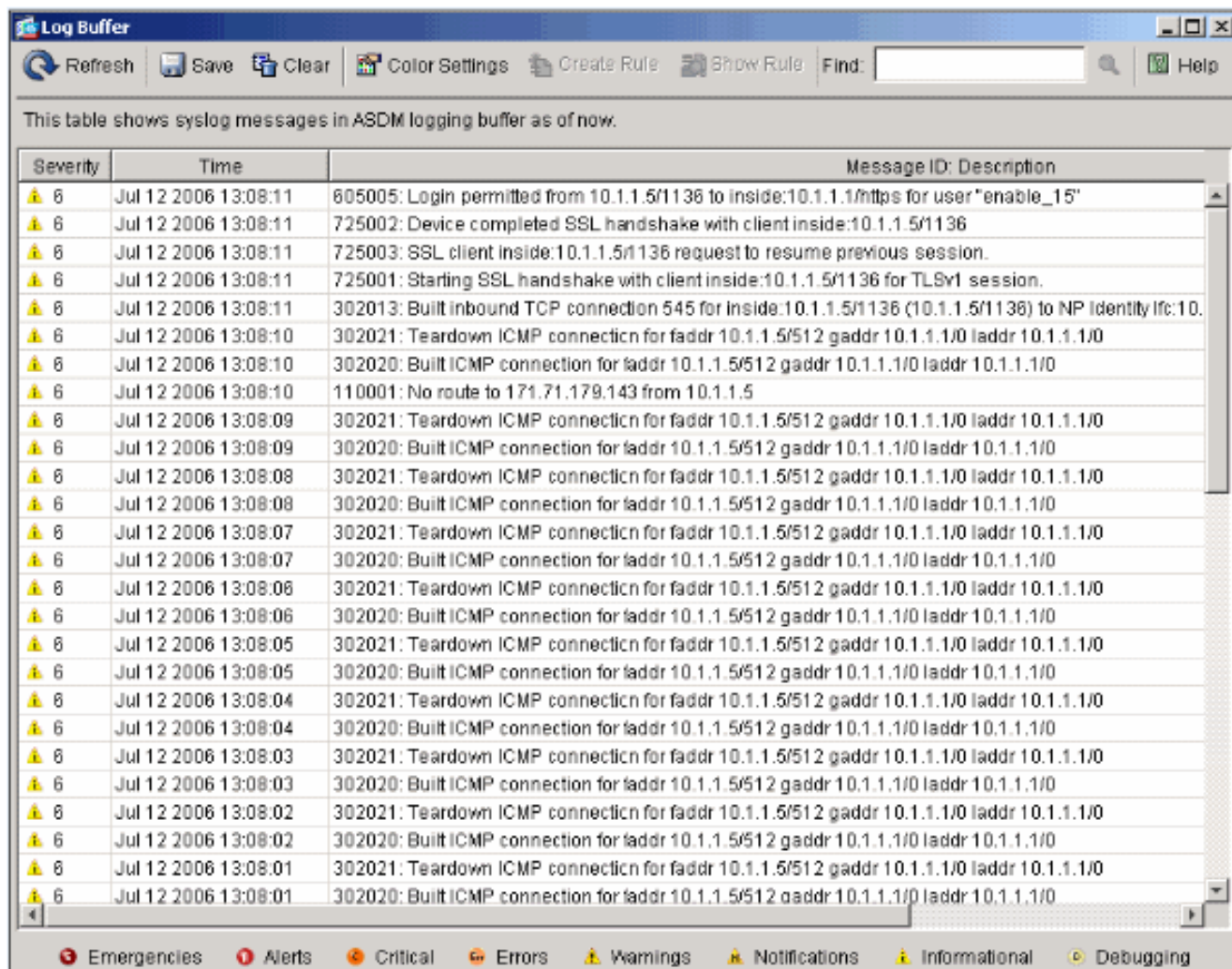
2. Scegliere **Monitoraggio > Log buffer > Livello di log** e scegliere **Log buffer** dall'elenco a discesa. Fare clic su

## Visualizza.



3. Di seguito è riportato un esempio di buffer del log:





Severity	Time	Message ID: Description
6	Jul 12 2006 13:08:11	805005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user "enable_15"
6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
6	Jul 12 2006 13:08:10	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
6	Jul 12 2006 13:08:09	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0

## [Impossibile accedere ai siti Web per nome](#)

In alcuni casi, le reti interne non possono accedere ai siti Web utilizzando il nome (funziona con l'indirizzo IP) nel browser. Questo problema è comune e si verifica in genere se il server DNS non è definito, in particolare nei casi in cui PIX/ASA è il server DHCP. Inoltre, ciò può verificarsi se il PIX/ASA non è in grado di eseguire il push del server DNS o se il server DNS non è raggiungibile.

## [Informazioni correlate](#)

- [Cisco PIX serie 500 Security Appliance](#)
- [Cisco ASA serie 5500 Adaptive Security Appliance](#)
- [Riferimenti per i comandi di Cisco Secure PIX Firewall](#)
- [Cisco Adaptive Security Device Manager](#)
- [Risoluzione dei problemi e avvisi di Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)