

PIX/ASA 7.x: Reindirizzamento delle porte (inoltro) con comandi nat, globali, statici e access-list

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Esempio di rete](#)

[Configurazione iniziale](#)

[Consenti accesso in uscita](#)

[Consenti agli host interni l'accesso alle reti esterne con NAT](#)

[Consenti agli host interni l'accesso alle reti esterne con l'utilizzo di PAT](#)

[Limita l'accesso degli host interni alle reti esterne](#)

[Consenti agli host non attendibili l'accesso agli host della rete attendibile](#)

[Uso degli ACL in PIX versione 7.0 e successive](#)

[Disabilita NAT per host/reti specifiche](#)

[Reindirizzamento porte \(inoltro\) con statistiche](#)

[Esempio di rete - Reindirizzamento porte \(inoltro\)](#)

[Configurazione PIX parziale - Reindirizzamento porte](#)

[Limita sessione TCP/UDP tramite statico](#)

[Lista accessi temporizzati](#)

[Informazioni da raccogliere quando si apre una richiesta di assistenza tecnica](#)

[Informazioni correlate](#)

[Introduzione](#)

Per ottimizzare la sicurezza quando si implementa Cisco PIX Security Appliance versione 7.0, è importante capire come i pacchetti passano tra interfacce di sicurezza più alte e interfacce di sicurezza più basse quando si usano i comandi nat-control, nat, global, **static**, **access-list** e **access-group**. Questo documento spiega le differenze tra questi comandi e come configurare le funzionalità Port Redirection (Forwarding) e NAT (Network Address Translation) esterne nel software PIX versione 7.x, con l'uso dell'interfaccia della riga di comando o di Adaptive Security Device Manager (ASDM).

Nota: alcune opzioni di ASDM 5.2 e versioni successive possono essere diverse da quelle di ASDM 5.1. Per ulteriori informazioni, consultare la [documentazione di ASDM](#).

Prerequisiti

Requisiti

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:

- Cisco PIX serie 500 Security Appliance Software versione 7.0 e successive
- ASDM versione 5.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.

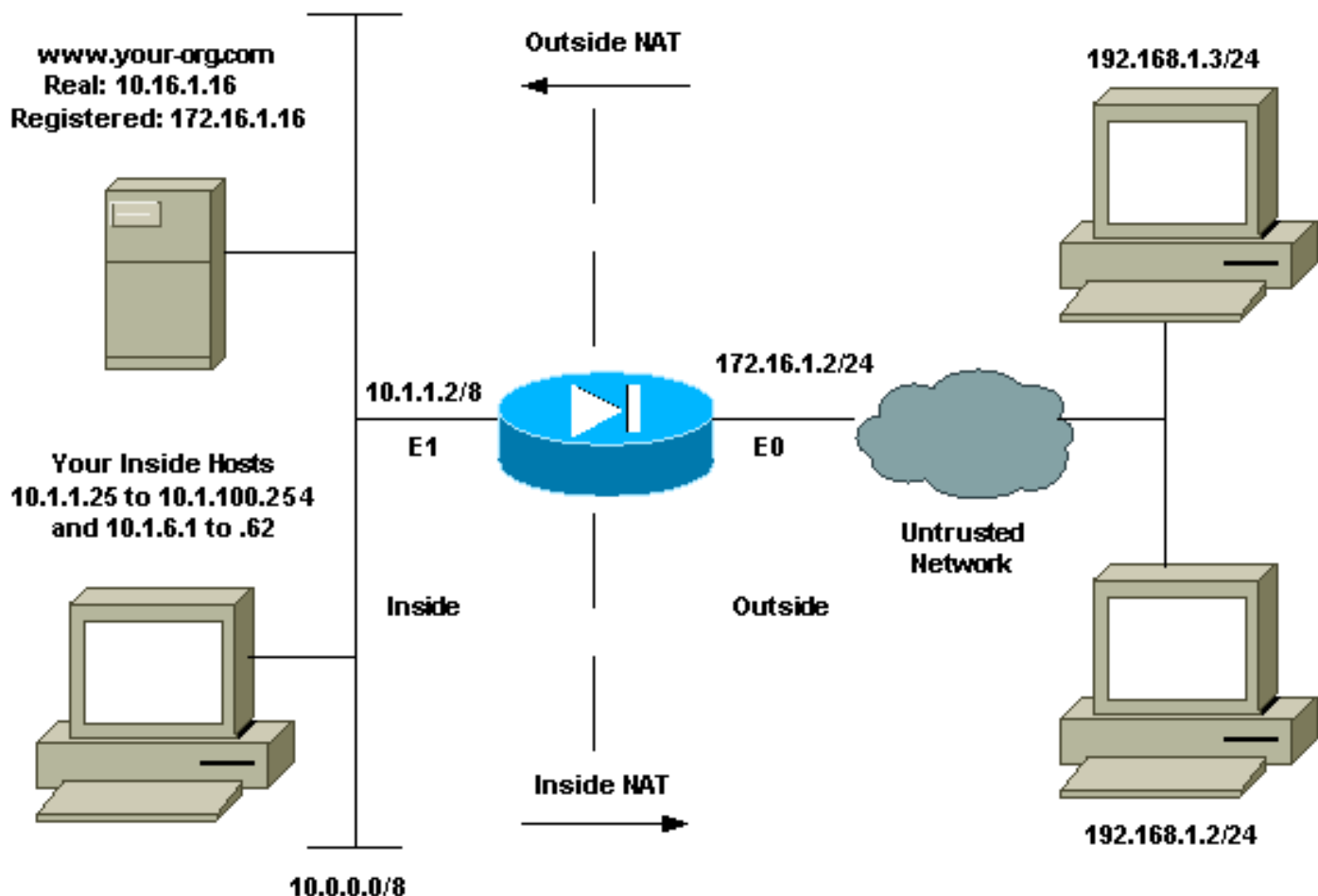
Prodotti correlati

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](#).

Esempio di rete



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.

Configurazione iniziale

I nomi delle interfacce sono:

- **interface ethernet 0** - nome se esterno
- **interface ethernet 1** - nome se all'interno

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

Consenti accesso in uscita

L'accesso in uscita descrive le connessioni da un'interfaccia con un livello di protezione più elevato a un'interfaccia con un livello di protezione più basso. Ciò include le connessioni dall'interno all'esterno, dall'interno alle zone demilitarizzate (DMZ) e le DMZ all'esterno. Questo può includere anche connessioni da una DMZ a un'altra, purché l'interfaccia dell'origine della connessione abbia un livello di protezione più alto rispetto alla destinazione. Per verificare questa condizione, esaminare la configurazione del "livello di sicurezza" sulle interfacce PIX.

L'esempio mostra il livello di protezione e la configurazione del nome dell'interfaccia:

```
pix(config)#interface ethernet 0
```

```
pix(config-if)#security-level 0
pix(config-if)#nameif outside
pix(config-if)#exit
```

PIX 7.0 introduce il comando **nat-control**. È possibile utilizzare il comando **nat-control** in modalità di configurazione per specificare se NAT è richiesto per le comunicazioni esterne. Con il controllo NAT abilitato, è necessaria la configurazione delle regole NAT per consentire il traffico in uscita, come avviene nelle versioni precedenti del software PIX. Se il controllo NAT è disabilitato (**nessun controllo NAT**), gli host interni possono comunicare con le reti esterne senza la configurazione di una regola NAT. Tuttavia, se gli host interni non dispongono di indirizzi pubblici, è necessario configurare NAT per tali host.

Per configurare il controllo NAT con l'uso di ASDM, selezionare la scheda Configurazione dalla finestra Home ASDM e scegliere **NAT** dal menu Funzioni.

Abilita il traffico attraverso il firewall senza conversione: Questa opzione è stata introdotta in PIX versione 7.0(1). Quando questa opzione è selezionata, non viene emesso alcun comando **nat-control** nella configurazione. Questo comando indica che non è necessaria alcuna traduzione per attraversare il firewall. Questa opzione viene in genere selezionata solo quando gli host interni dispongono di indirizzi IP pubblici o la topologia di rete non richiede la conversione degli host interni in indirizzi IP.

Se gli host interni dispongono di indirizzi IP privati, questa opzione deve essere deselezionata in modo che gli host interni possano essere convertiti in un indirizzo IP pubblico e accedere a Internet.

The screenshot displays the Cisco ASDM 5.1 for PIX - 10.1.1.1 interface. The main window is titled "Configuration > NAT > Translation Rules". The "Enable traffic through the firewall without address translation" checkbox is checked. Below this, there are radio buttons for "Translation Rules" (selected) and "Translation Exemption Rules". A dropdown menu shows "All Interfaces" and a "Show All" button. A table with the following structure is visible:

Rule	Original			Translated		
Type	Interface	Source Network	Destination Network	Interface	Address	

Buttons for "Add", "Edit", and "Delete" are on the right side of the table. At the bottom, there are tabs for "Static NAT", "Dynamic NAT", "Static Policy NAT", and "Dynamic Policy NAT", along with a "Manage Pools..." button. The "Apply" and "Reset" buttons are at the bottom center. The status bar at the bottom shows "<admin> NA (15) 7/11/06 6:02:29 PM UTC".

Per consentire l'accesso in uscita con il controllo NAT, sono necessari due criteri. Il primo è un metodo di traduzione. Può trattarsi di una traduzione statica con l'utilizzo del comando **static** o di una traduzione dinamica con l'utilizzo di una regola **nat/global**. Questa operazione non è necessaria se il controllo NAT è disabilitato e gli host interni dispongono di indirizzi pubblici.

L'altro requisito per l'accesso in uscita (che si applica indipendentemente dal fatto che il controllo NAT sia abilitato o disabilitato) è se è presente un elenco di controllo di accesso (ACL). Se è presente un ACL, deve consentire all'host di origine di accedere all'host di destinazione con il protocollo e la porta specifici. Per impostazione predefinita, non esistono restrizioni di accesso alle connessioni in uscita tramite PIX. Ciò significa che se non è configurato alcun ACL per l'interfaccia di origine, per impostazione predefinita la connessione in uscita è consentita se è stato configurato un metodo di conversione.

[Consenti agli host interni l'accesso alle reti esterne con NAT](#)

Questa configurazione fornisce a tutti gli host della subnet 10.1.6.0/24 l'accesso all'esterno. A tale scopo, utilizzare i comandi **nat** e **global**, come mostrato nella seguente procedura.

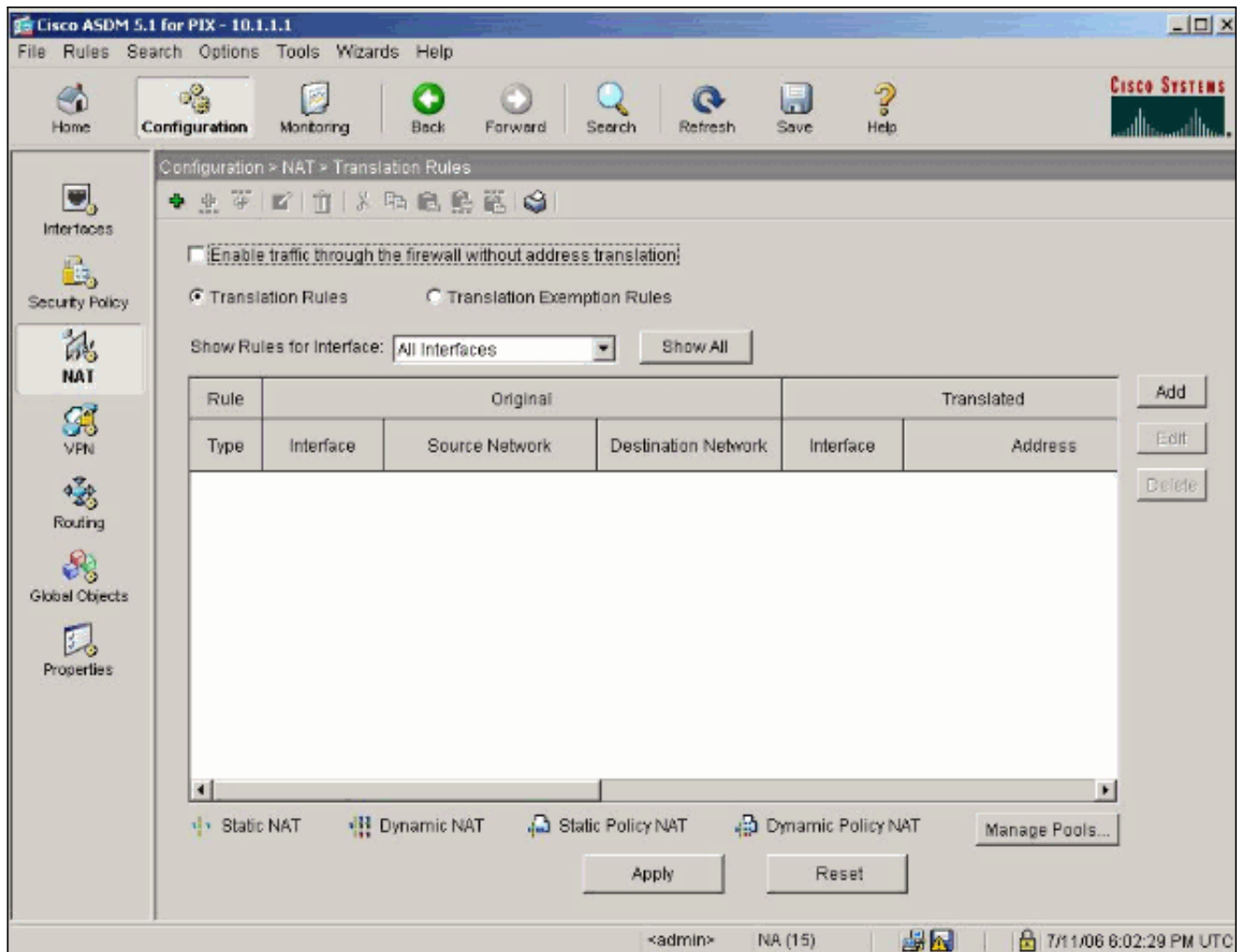
1. Definire il gruppo interno da includere per NAT.

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. Specificare un pool di indirizzi sull'interfaccia esterna a cui convertire gli host definiti nell'istruzione NAT.

```
global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
```

3. Per creare il pool di indirizzi globali, utilizzare ASDM. Scegliere **Configurazione > Funzionalità > NAT** e deselezionare **Attiva traffico attraverso il firewall senza conversione degli indirizzi**. Quindi fare clic su **Add** (Aggiungi) per configurare la regola NAT.



4. Per definire gli indirizzi del pool NAT, fare clic su **Manage Pools** (Gestisci pool).

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

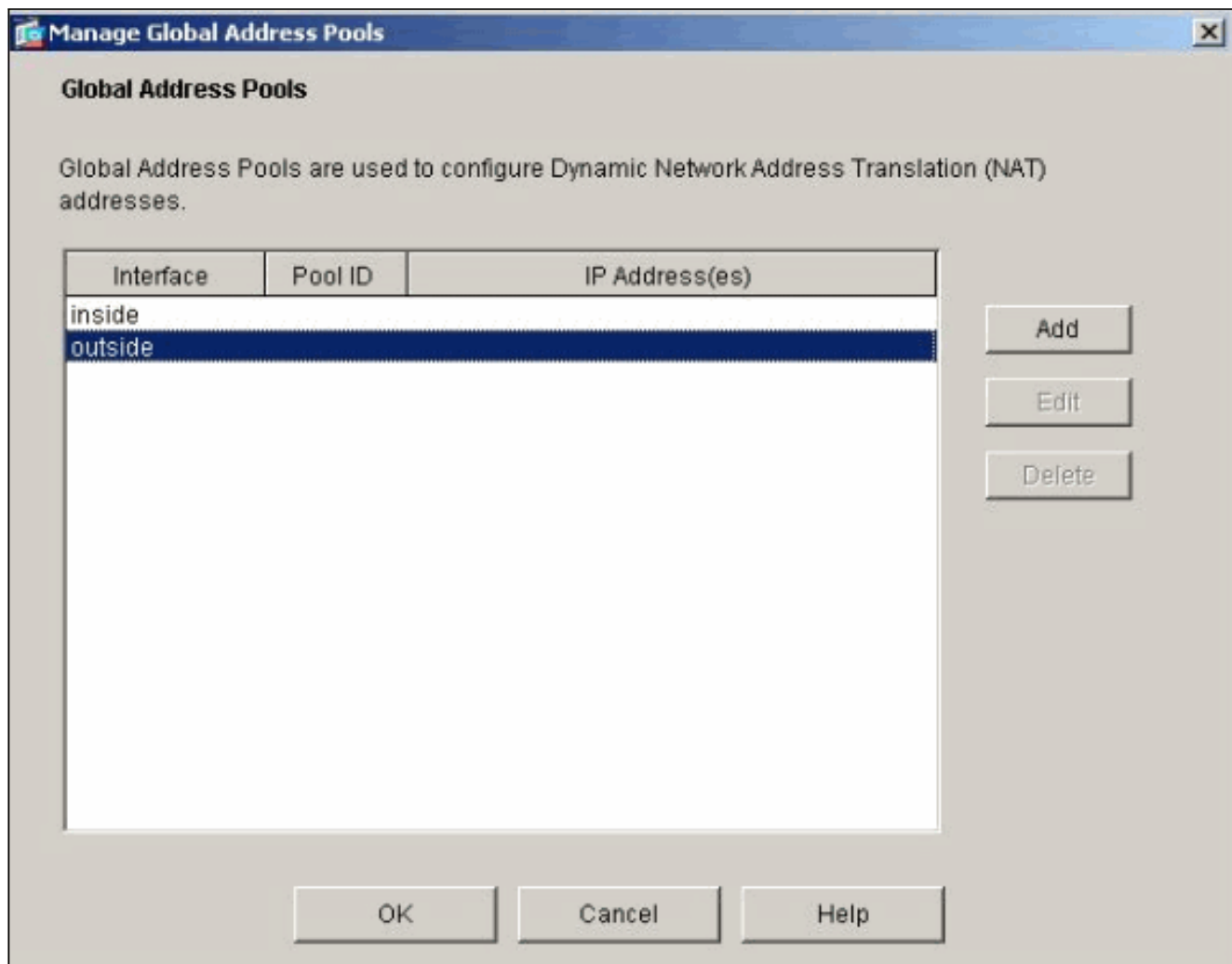
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

5. Scegliete **Esterno > Aggiungi**, quindi scegliete un intervallo per specificare un pool di indirizzi.



6. Immettere l'intervallo di indirizzi, immettere un ID pool 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):

7. Per creare la regola di conversione, scegliete **Configurazione > Caratteristiche > NAT > Regole** di conversione.
8. Selezionate **Interno (Inside)** come interfaccia di origine e immettete gli indirizzi che desiderate visualizzare nel campo NAT.
9. Per Traduci indirizzo su interfaccia, selezionare **Esterno**, scegliere **Dinamico**, quindi selezionare il pool di indirizzi appena configurato.
10. 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

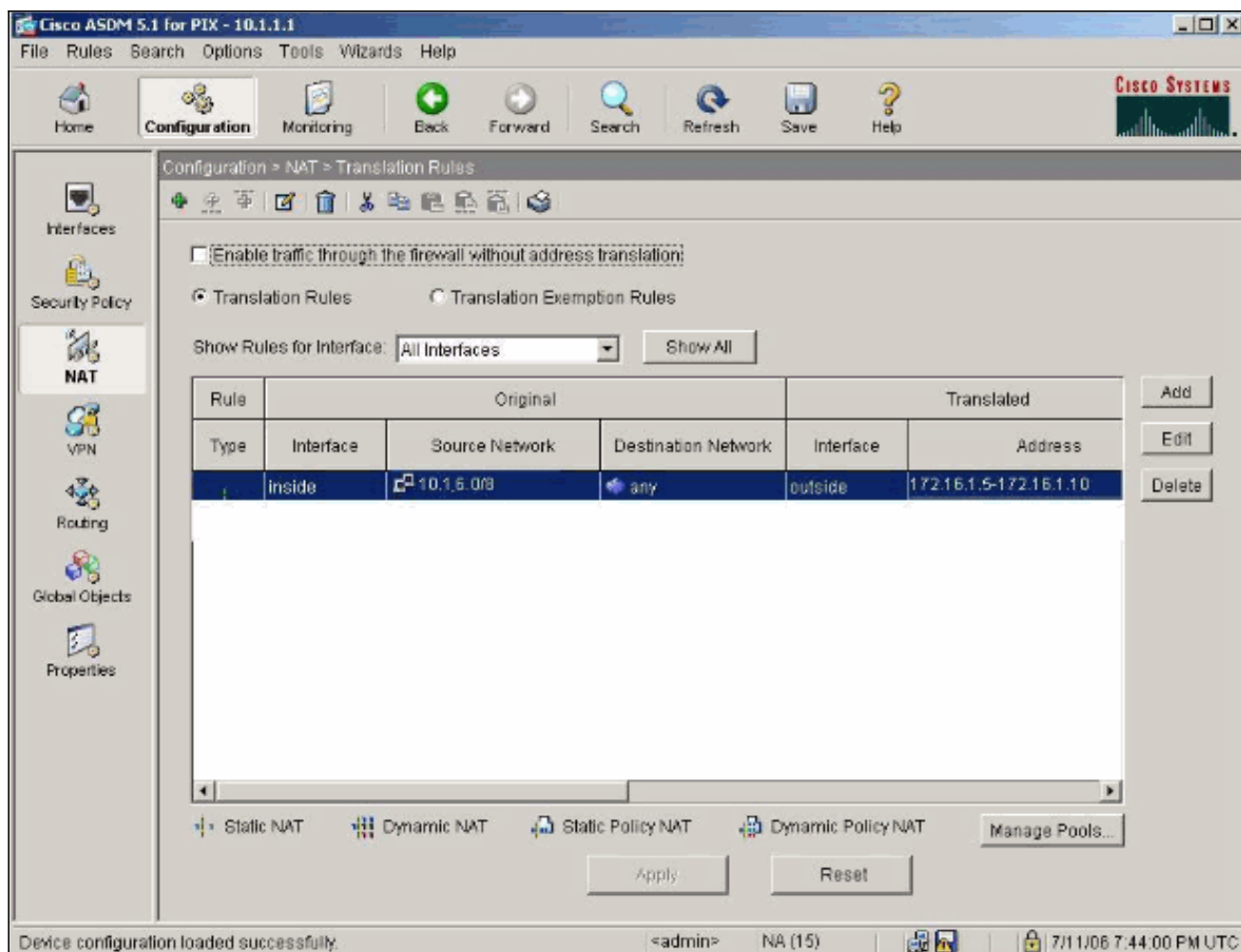
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
1	172.16.1.5-172.16.1.10

11. La traduzione viene visualizzata in Regole di conversione in **Configurazione > Caratteristiche > NAT > Regole di conversione**.



Ora gli host all'interno possono accedere alle reti esterne. Quando gli host dall'interno avviano una connessione all'esterno, vengono convertiti in un indirizzo dal pool globale. Gli indirizzi vengono assegnati dal pool globale in base all'ordine di arrivo, alla prima traduzione e iniziano con l'indirizzo più basso nel pool. Ad esempio, se l'host 10.1.6.25 è il primo ad avviare una connessione con l'esterno, riceve l'indirizzo 172.16.1.5. L'host successivo riceve l'indirizzo 172.16.1.6 e così via. Non si tratta di una traduzione statica e la traduzione scade dopo un periodo di inattività definito dal comando **timeout xlate hh:mm:ss**. Se gli host interni sono più numerosi degli indirizzi del pool, l'indirizzo finale del pool viene utilizzato per PAT (Port Address Translation).

[Consenti agli host interni l'accesso alle reti esterne con l'utilizzo di PAT](#)

Se si desidera che gli host interni condividano un singolo indirizzo pubblico per la traduzione, utilizzare PAT. Se l'istruzione **globale** specifica un indirizzo, tale indirizzo viene convertito in porta. Il PIX consente la traduzione di una porta per interfaccia e supporta fino a 65.535 oggetti xlate attivi per un singolo indirizzo globale. Completare questi passaggi per consentire agli host interni di accedere alle reti esterne con l'utilizzo di PAT.

1. Definire il gruppo interno da includere per PAT (quando si utilizza 0 0, vengono selezionati tutti gli host interni).

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. Specificare l'indirizzo globale da utilizzare per PAT. come indirizzo di interfaccia.

```
global (outside) 1 172.16.1.4 netmask 255.255.255.0
```

3. In ASDM, selezionare **Configurazione > Funzionalità > NAT** e deselezionare **Abilita il traffico attraverso il firewall senza traduzione degli indirizzi**.
4. Per configurare la regola NAT, fare clic su **Add** (Aggiungi).
5. Per configurare l'indirizzo PAT, scegliere **Gestisci pool**.
6. Scegliere **Esterno > Aggiungi** e fare clic su **Port Address Translation (PAT)** per configurare un singolo indirizzo per PAT.
7. Immettere un indirizzo, un ID pool 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):

8. Per creare la regola di conversione, scegliete **Configurazione > Caratteristiche > NAT > Regole** di conversione.
9. Selezionare **inside** come interfaccia di origine e immettere gli indirizzi che si desidera NAT.
10. Per Traduci indirizzo su interfaccia, selezionare **esterno**, scegliere **Dinamico** e selezionare il pool di indirizzi appena configurato. 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

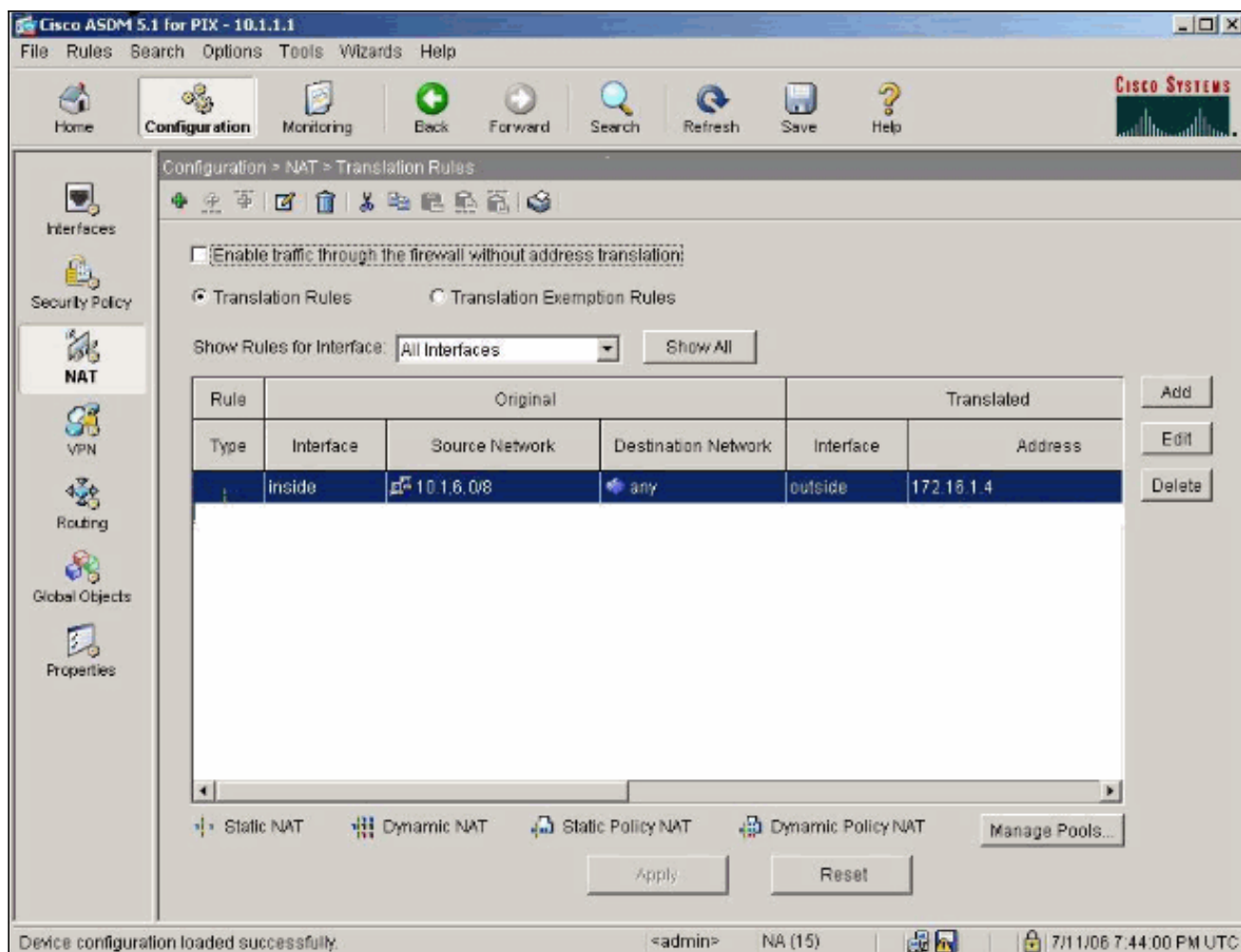
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
1	172.16.1.4

11. La traduzione viene visualizzata in Regole di conversione in **Configurazione > Caratteristiche > NAT > Regole di conversione**.



Quando si utilizza PAT è necessario tenere in considerazione alcuni aspetti.

- Gli indirizzi IP specificati per PAT non possono essere inclusi in un altro pool di indirizzi globale.
- PAT non funziona con le applicazioni H.323, i server dei nomi di cache e il protocollo PPTP (Point-to-Point Tunneling Protocol). PAT funziona con DNS (Domain Name Service), FTP e FTP passivo, HTTP, posta, RPC (Remote-Procedure Call), shell, Telnet, filtro URL e traceroute in uscita.
- Non utilizzare PAT quando è necessario eseguire applicazioni multimediali attraverso il firewall. Le applicazioni multimediali possono essere in conflitto con i mapping delle porte forniti da PAT.
- Nel software PIX versione 4.2(2), la funzione PAT non funziona con i pacchetti dati IP che arrivano in ordine inverso. Il software PIX versione 4.2(3) corregge questo problema.
- Gli indirizzi IP nel pool di indirizzi globali specificato con il comando **global** richiedono voci DNS inverse per garantire che tutti gli indirizzi di rete esterni siano accessibili tramite il PIX. Per creare mapping DNS inversi, utilizzare un record puntatore DNS (PTR) nel file di mapping indirizzo-nome per ogni indirizzo globale. Senza le voci PTR, la connettività Internet dei siti può essere lenta o intermittente e le richieste FTP hanno esito negativo in modo coerente. Ad esempio, se un indirizzo IP globale è 192.168.1.3 e il nome di dominio per PIX Security Appliance è pix.caguana.com, il record PTR è:


```
3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
4.1.1.175.in-addr.arpa. IN PTR
pix4.caguana.com & so on.
```

Limita l'accesso degli host interni alle reti esterne

Se per l'host di origine è stato definito un metodo di conversione valido e non è stato definito alcun ACL per l'interfaccia PIX di origine, la connessione in uscita è consentita per impostazione predefinita. Tuttavia, in alcuni casi è necessario limitare l'accesso in uscita in base all'origine, alla destinazione, al protocollo e/o alla porta. A tale scopo, configurare un ACL con il comando **access-list** e applicarlo all'interfaccia PIX dell'origine della connessione con il comando **access-group**. È possibile applicare gli ACL PIX 7.0 sia in entrata che in uscita. Questa procedura è un esempio che consente l'accesso HTTP in uscita per una subnet, ma nega a tutti gli altri host l'accesso HTTP all'esterno, consentendo tutto il resto del traffico IP per tutti gli altri host.

1. Definire l'ACL.

```
access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www
access-list acl_outbound deny tcp any any eq www
access-list acl_outbound permit ip any any
```

Nota: gli ACL PIX sono diversi dagli ACL sui router Cisco IOS® in quanto non usano una maschera con caratteri jolly come Cisco IOS. Nella definizione dell'ACL, viene usata una subnet mask regolare. Come per i router Cisco IOS, l'ACL PIX ha un "deny all" implicito alla fine dell'ACL. **Nota:** le nuove voci dell'elenco degli accessi verranno aggiunte alla fine delle voci ACE esistenti. Se è necessario elaborare prima una voce ACE specifica, è possibile utilizzare la parola chiave `line` nell'elenco degli accessi. Questo è un esempio di riepilogo dei comandi:

```
access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any
```

2. Applicare l'ACL all'interfaccia interna.

```
access-group acl_outbound in interface inside
```

3. Utilizzare ASDM per configurare la prima voce dell'elenco degli accessi al passaggio 1 in modo da consentire il traffico HTTP da 10.1.6.0/24. Scegliere **Configurazione > Funzionalità > Criteri di sicurezza > Regole di accesso**.
4. Fare clic su **Add**, immettere le informazioni visualizzate in questa finestra e fare clic su **OK**.

Add Access Rule

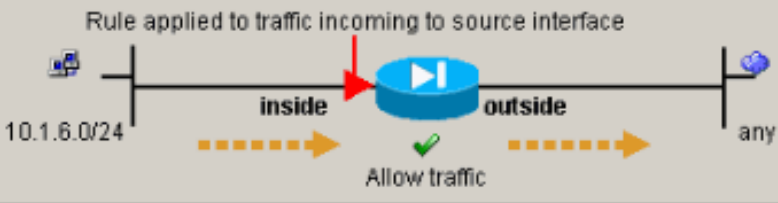
Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Time Range
 Time Range:

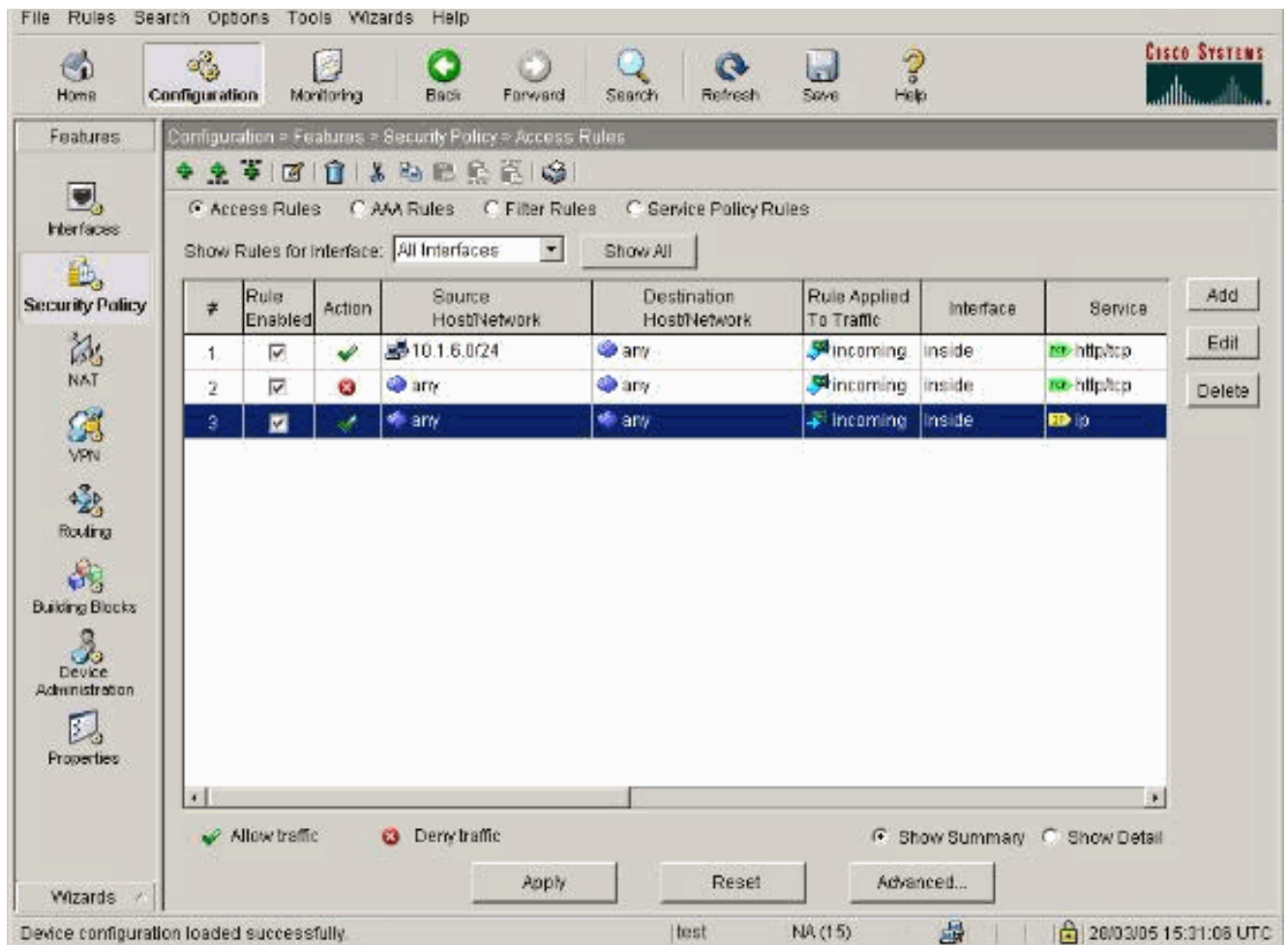
Syslog
 Default Syslog

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 The diagram shows a central router icon. On the left, a vertical line represents the 'inside' interface, with a computer icon and the IP range '10.1.6.0/24'. A red arrow points from this interface towards the router. On the right, a vertical line represents the 'outside' interface, with a cloud icon and the label 'any'. A green checkmark is placed below the router with the text 'Allow traffic'. Dashed orange arrows indicate the flow of traffic from the inside interface, through the router, and out to the outside interface.

Protocol and Service
 TCP UDP ICMP IP
Source Port
 Service = ...
 Service Group
Destination Port
 Service = ...
 Service Group

Please enter the description below (optional):

5. Una volta immesse le tre voci dell'elenco degli accessi, scegliere **Configurazione > Funzionalità > Criteri di sicurezza > Regole di accesso** per visualizzare queste regole.



Consenti agli host non attendibili l'accesso agli host della rete attendibile

La maggior parte delle organizzazioni deve consentire agli host non attendibili l'accesso alle risorse della propria rete attendibile. Un esempio comune è un server Web interno. Per impostazione predefinita, il PIX nega le connessioni dagli host esterni agli host interni. Per consentire questa connessione in modalità di controllo NAT, utilizzare il comando **static** con i comandi **access-list** e **access-group**. Se il controllo NAT è disabilitato, solo i comandi **access-list** e **access-group** sono richiesti, in assenza di traduzioni.

Applicare gli ACL alle interfacce con un comando **access-group**. Questo comando associa l'ACL all'interfaccia per esaminare il traffico che scorre in una particolare direzione.

A differenza dei comandi **nat** e **global** che permettono di usare gli host interni all'esterno, il comando **static** crea una conversione bidirezionale che permette di usare gli host interni esterni e esterni all'interno se si aggiungono gli ACL/gruppi corretti.

Negli esempi di configurazione PAT mostrati in questo documento, se un host esterno tenta di connettersi all'indirizzo globale, può essere utilizzato da migliaia di host interni. Il comando **static** crea un mapping uno-a-uno. Il comando **access-list** definisce il tipo di connessione consentita a un host interno ed è sempre richiesto quando un host di protezione inferiore si connette a un host di protezione superiore. Il comando **access-list** è basato sia sulla porta che sul protocollo e può essere molto permissivo o molto restrittivo, a seconda delle esigenze dell'amministratore di sistema.

Il [diagramma di rete](#) in questo documento illustra l'utilizzo di questi comandi per configurare il PIX in modo da consentire a tutti gli host non attendibili di connettersi al server Web interno e consentire all'host non attendibile 192.168.1.1 di accedere a un servizio FTP sullo stesso computer.

Uso degli ACL in PIX versione 7.0 e successive

Completare questi passaggi per il software PIX versione 7.0 e successive con l'uso di ACL.

1. Se il controllo NAT è abilitato, definire una conversione dell'indirizzo statico per il server Web interno in un indirizzo esterno/globale.

```
static (inside, outside) 172.16.1.16 10.16.1.16
```

2. Definire gli host che possono connettersi alle porte del server Web/FTP.

```
access-list 101 permit tcp any host 172.16.1.16 eq www
access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp
```

3. Applicare l'ACL all'interfaccia esterna.

```
access-group 101 in interface outside
```

4. Per creare la traduzione statica con ASDM, scegliere **Configurazione > Funzionalità > NAT** e fare clic su **Aggiungi**.
5. Selezionare **inside** come interfaccia di origine e immettere l'indirizzo interno per il quale si desidera creare una traduzione statica.
6. Scegliere **Static** (Statico) e immettere l'indirizzo esterno verso cui tradurre nel campo IP address (Indirizzo IP). Fare clic su **OK**.

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:

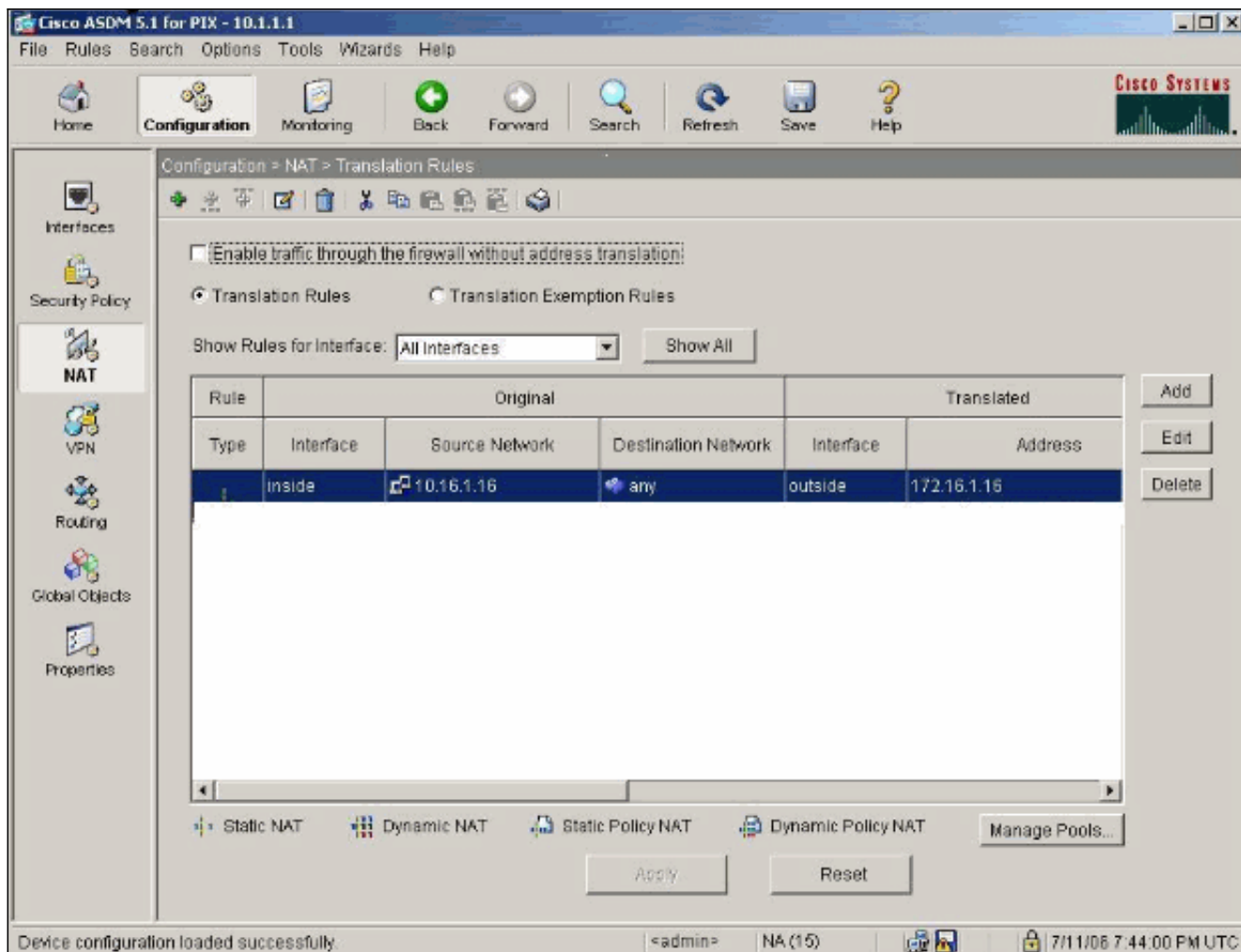
Redirect port

TCP Original port: Translated port:
 UDP

 Dynamic Address Pool:

Pool ID	Address

7. La traduzione viene visualizzata in Regole di conversione quando scegliete **Configurazione > Caratteristiche > NAT > Regole di conversione**.



8. Per accedere alle voci dell'**elenco degli accessi**, usare la procedura [Limita l'accesso degli host interni](#) alle [reti esterne](#). **Nota:** prestare attenzione quando si implementano questi comandi. Se si implementa il comando **access-list 101 allow ip any**, tutti gli host della rete non trusted possono accedere a qualsiasi host della rete trusted con l'utilizzo del protocollo IP, a condizione che sia in corso una traduzione attiva.

[Disabilita NAT per host/reti specifiche](#)

Se si utilizza il controllo NAT e si hanno alcuni indirizzi pubblici nella rete interna e si desidera che gli host interni specifici si estendano all'esterno senza conversione, è possibile disabilitare NAT per tali host, con comandi **nat 0** o **statici**.

Questo è un esempio di comando **nat**:

```
nat (inside) 0 10.1.6.0 255.255.255.0
```

Completare questa procedura per disabilitare NAT per host/reti specifiche con l'uso di ASDM.

1. Scegliete **Configurazione > Funzionalità > NAT** e fate clic su **Aggiungi**.
2. Scegliere **inside** come interfaccia di origine e immettere l'indirizzo interno/rete per cui si desidera creare una traduzione statica.
3. Scegliere **Dinamico** e selezionare lo stesso indirizzo per il pool di indirizzi. 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

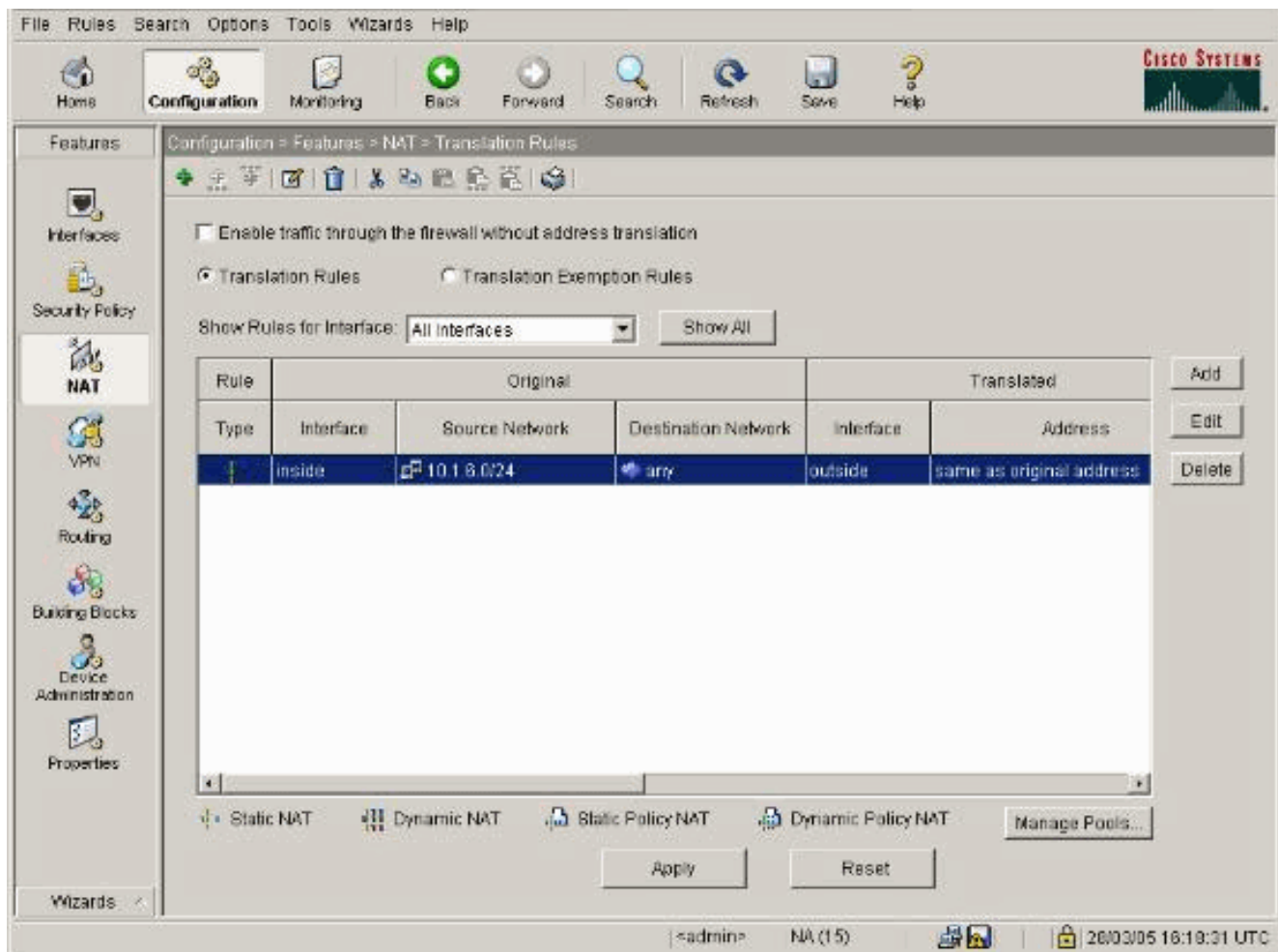
TCP Original port: Translated port:

 UDP

Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

4. La nuova regola viene visualizzata in Regole di conversione quando scegliete **Configurazione > Caratteristiche > NAT > Regole di conversione**.

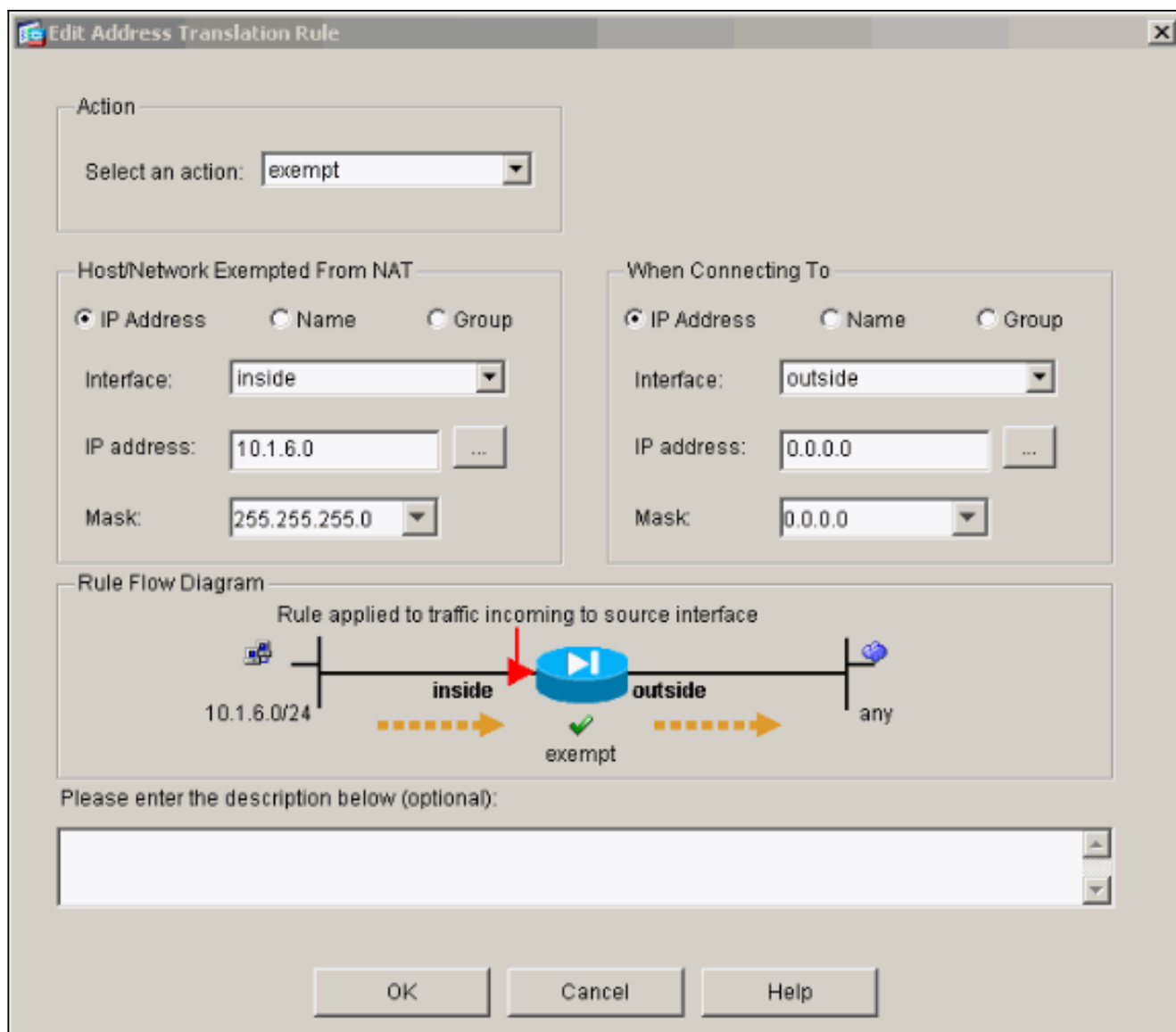


5. Se si usano gli ACL, che consentono un controllo più preciso del traffico che non si deve tradurre (in base all'origine o alla destinazione), usare questi comandi.

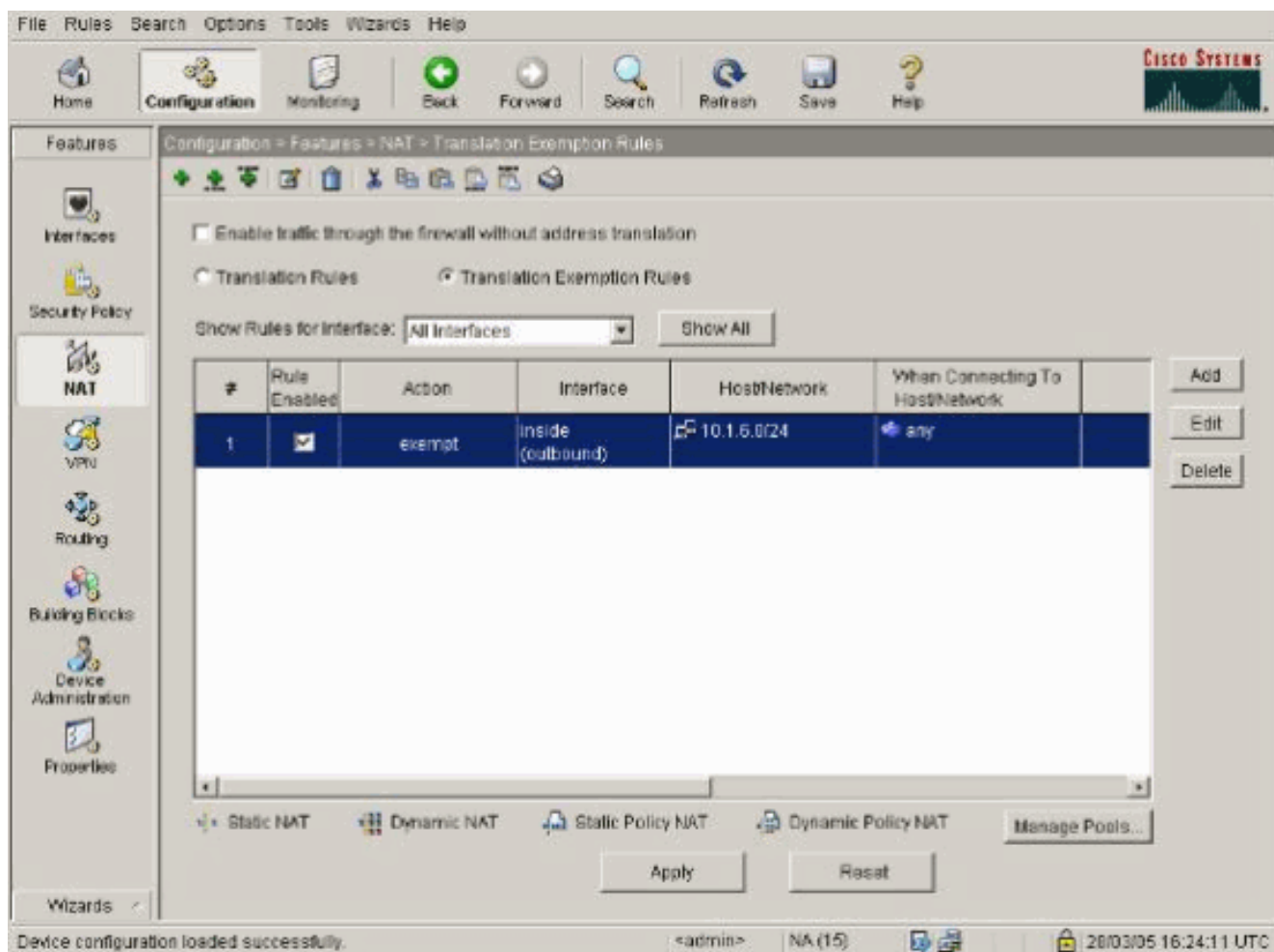
```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

6. Utilizzare ASDM e scegliere **Configurazione > Funzionalità > NAT > Regole di conversione**.

7. Scegliere **Regole di esenzione conversione** e fare clic su **Aggiungi**. Nell'esempio viene mostrato come esentare il traffico dalla rete 10.1.6.0/24 per portarlo ovunque dalla traduzione.



8. Scegliere **Configurazione > Funzionalità > NAT > Regole di esenzione dalla conversione** per visualizzare le nuove regole.



9. Il comando **static** per il server Web cambia come mostrato nell'esempio.

```
static (inside, outside) 10.16.1.16 10.16.1.16
```

10. Da ASDM, scegliere **Configurazione > Funzionalità > NAT > Regole di conversione**.

11. Selezionare **Regole di conversione** e fare clic su **Aggiungi**. Immettere le informazioni sull'indirizzo di origine e selezionare **Statico**. Immettere lo stesso indirizzo nel campo Indirizzo IP.

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

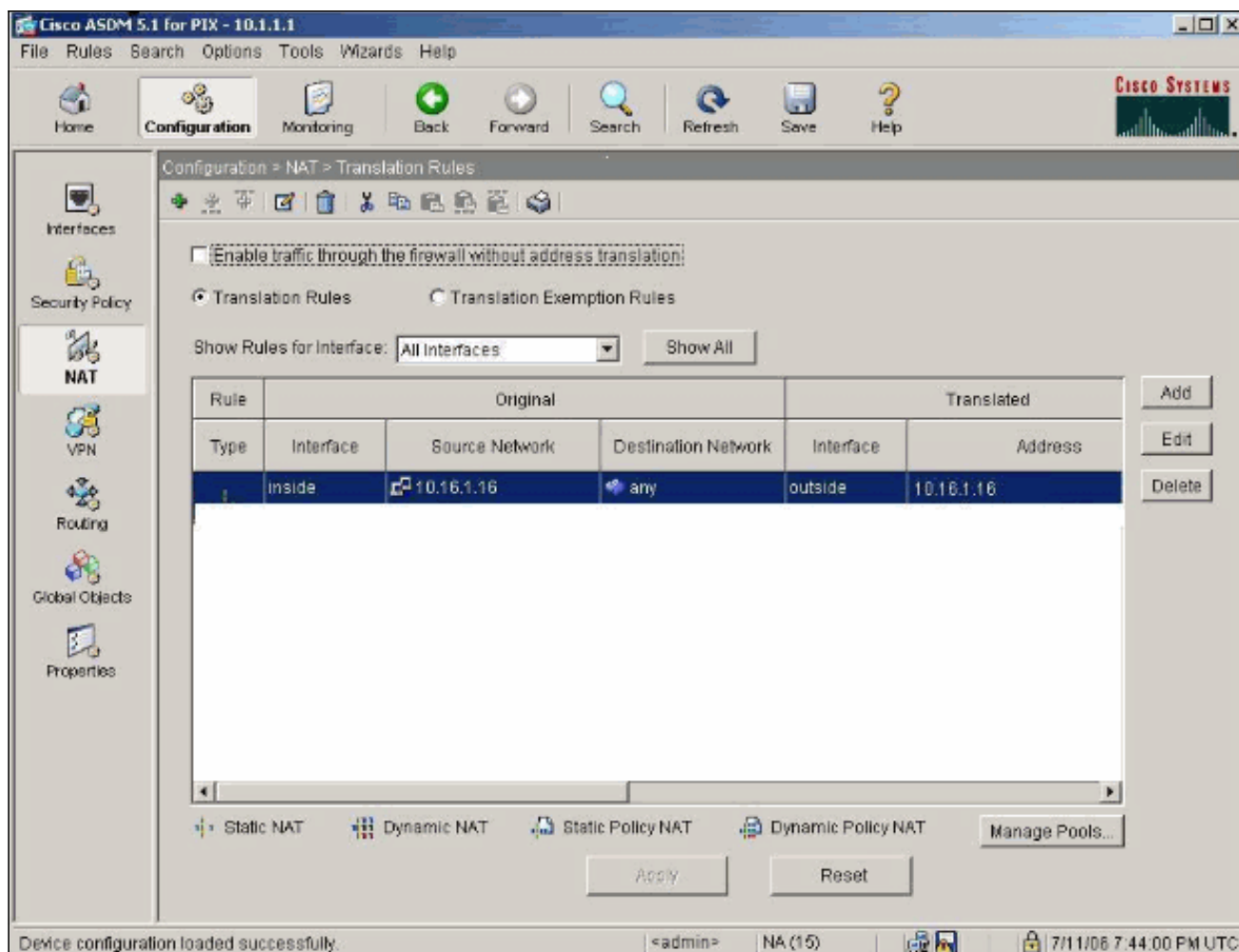
TCP Original port: Translated port:

UDP

 Dynamic Address Pool:

Pool ID	Address

12. La traduzione viene visualizzata in Regole di conversione quando scegliete **Configurazione > Caratteristiche > NAT > Regole di conversione**.



13. Se si usano gli ACL, usare questi comandi.

```
access-list 102 permit tcp any host 10.16.1.16 eq www
access-group 102 in interface outside
```

Per ulteriori informazioni sulla configurazione degli ACL in ASDM, vedere la sezione [Limitazione dell'accesso degli host interni alle reti esterne](#) di questo documento. Notare la differenza tra quando si usa **nat 0** e quando si specifica network/mask e quando si usa un ACL con una rete/mask che permette di avviare connessioni solo dall'interno. L'uso di ACL con **nat 0** permette di iniziare le connessioni dal traffico in entrata o in uscita. Le interfacce PIX devono trovarsi in subnet diverse per evitare problemi di raggiungibilità.

[Reindirizzamento porte \(inoltro\) con statistiche](#)

Nel PIX 6.0, è stata aggiunta la funzione Port Redirection(Forwarding) (Inoltro) per consentire agli utenti esterni di connettersi a un particolare indirizzo/porta IP e fare in modo che il PIX reindirizzi il traffico al server/porta interna appropriato. Il comando **statico** è stato modificato. L'indirizzo condiviso può essere un indirizzo univoco, un indirizzo PAT condiviso in uscita o condiviso con l'interfaccia esterna. Questa funzione è disponibile in PIX 7.0.

Nota: a causa dei limiti di spazio, i comandi vengono visualizzati su due righe.

```
static [(internal_if_name, external_if_name)] {global_ip/interface}local_ip [netmask mask]
[max_conns [emb_limit [norandomseq]]]
```

```
static [(internal_if_name, external_if_name)] {tcp|udp} {global_ip/interface} global_port
local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]
```

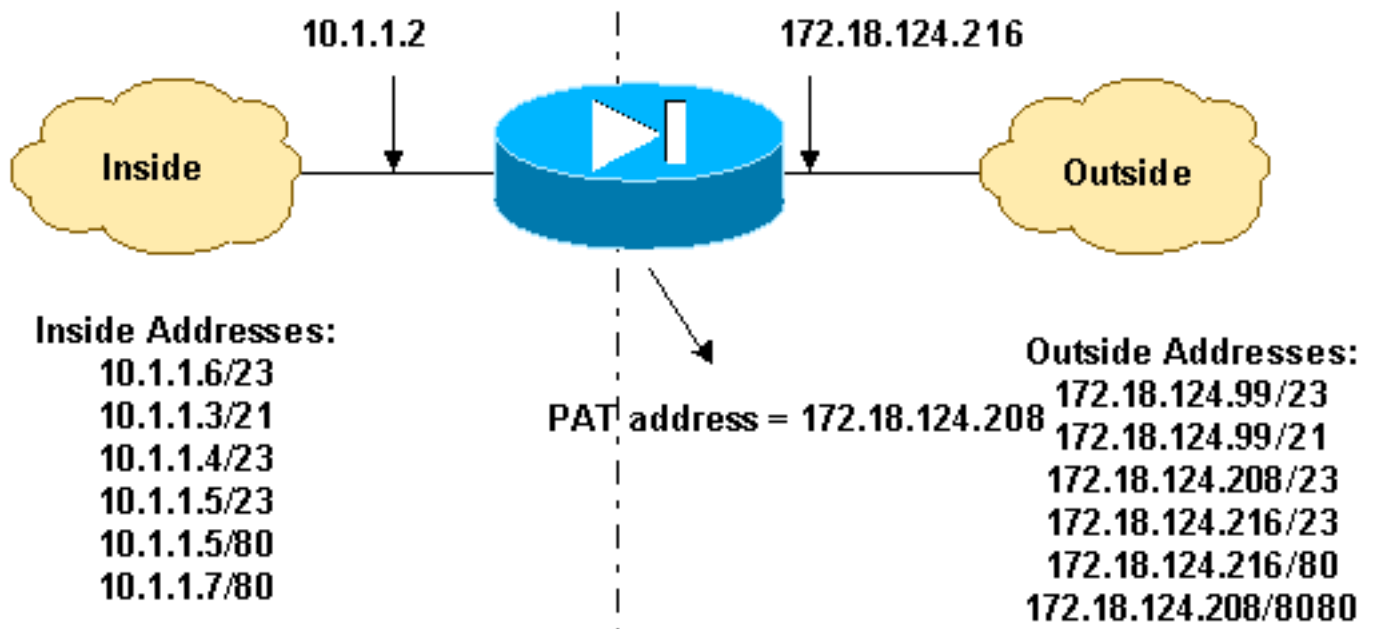
Nota: se il NAT statico utilizza l'indirizzo IP esterno (global_IP) per la conversione, potrebbe verificarsi una conversione. Pertanto, utilizzare la parola chiave **interface** anziché l'indirizzo IP nella traduzione statica.

Nell'esempio di rete seguente vengono illustrati i seguenti reindirizzamenti delle porte (inoltro):

- Gli utenti esterni indirizzano le richieste Telnet all'indirizzo IP univoco 172.18.124.99, che il PIX reindirizza a 10.1.1.6.
- Gli utenti esterni indirizzano le richieste FTP all'indirizzo IP univoco 172.18.124.99, che il PIX reindirizza a 10.1.1.3.
- Gli utenti esterni indirizzano le richieste Telnet all'indirizzo PAT 172.18.124.208, che il PIX reindirizza a 10.1.1.4.
- Gli utenti esterni indirizzano la richiesta Telnet a PIX all'indirizzo IP esterno 172.18.124.216, che il PIX reindirizza a 10.1.1.5.
- Gli utenti esterni indirizzano la richiesta HTTP a PIX all'indirizzo IP esterno 172.18.124.216, che il PIX reindirizza a 10.1.1.5.
- Gli utenti esterni indirizzano le richieste della porta HTTP 8080 all'indirizzo PAT 172.18.124.208, che il PIX reindirizza alla porta 80 10.1.1.7.

Questo esempio blocca anche l'accesso di alcuni utenti dall'interno all'esterno con ACL 100. Questo passaggio è facoltativo. Tutto il traffico è autorizzato in uscita senza l'ACL in posizione.

Esempio di rete - Reindirizzamento porte (inoltro)



Configurazione PIX parziale - Reindirizzamento porte

Questa configurazione parziale illustra l'utilizzo del reindirizzamento delle porte statiche (inoltro). Vedere il [diagramma](#) della [rete Reindirizzamento porte \(inoltro\)](#).

Configurazione PIX 7.x parziale - Reindirizzamento porte (inoltro)

```

fixup protocol ftp 21
!--- Use of an outbound ACL is optional. access-list 100
permit tcp 10.1.1.0 255.255.255.128 any eq www access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(inside,outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !!--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside

```

Nota: se il comando PIX/ASA è configurato con il comando **sysopt noproxyarp outside**, il firewall non è in grado di eseguire le traduzioni NAT statiche e proxy in PIX/ASA. Per risolvere questo problema, rimuovere il comando **sysopt noproxyarp outside** nella configurazione PIX/ASA e aggiornare le voci ARP utilizzando gratuitamente ARP. Ciò consente il corretto funzionamento delle voci NAT statiche.

Questa procedura è un esempio di come configurare il reindirizzamento della porta (inoltro) che consente agli utenti esterni di indirizzare le richieste Telnet all'indirizzo IP univoco 172.18.124.99, che il PIX reindirizza a 10.1.1.6.

1. Utilizzare ASDM e scegliere **Configurazione > Funzionalità > NAT > Regole di conversione**.
2. Selezionare **Regole di conversione** e fare clic su **Aggiungi**.
3. In Source Host/Network (Host/rete di origine), immettere le informazioni per l'indirizzo IP interno.
4. In Traduci indirizzo in, selezionare **Statico**, immettere l'indirizzo IP esterno e selezionare **Reindirizza porta**.
5. Immettere le informazioni sulla porta di pre-traduzione e post-traduzione (in questo esempio viene gestita la porta 23). Fare clic su **OK**.

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:

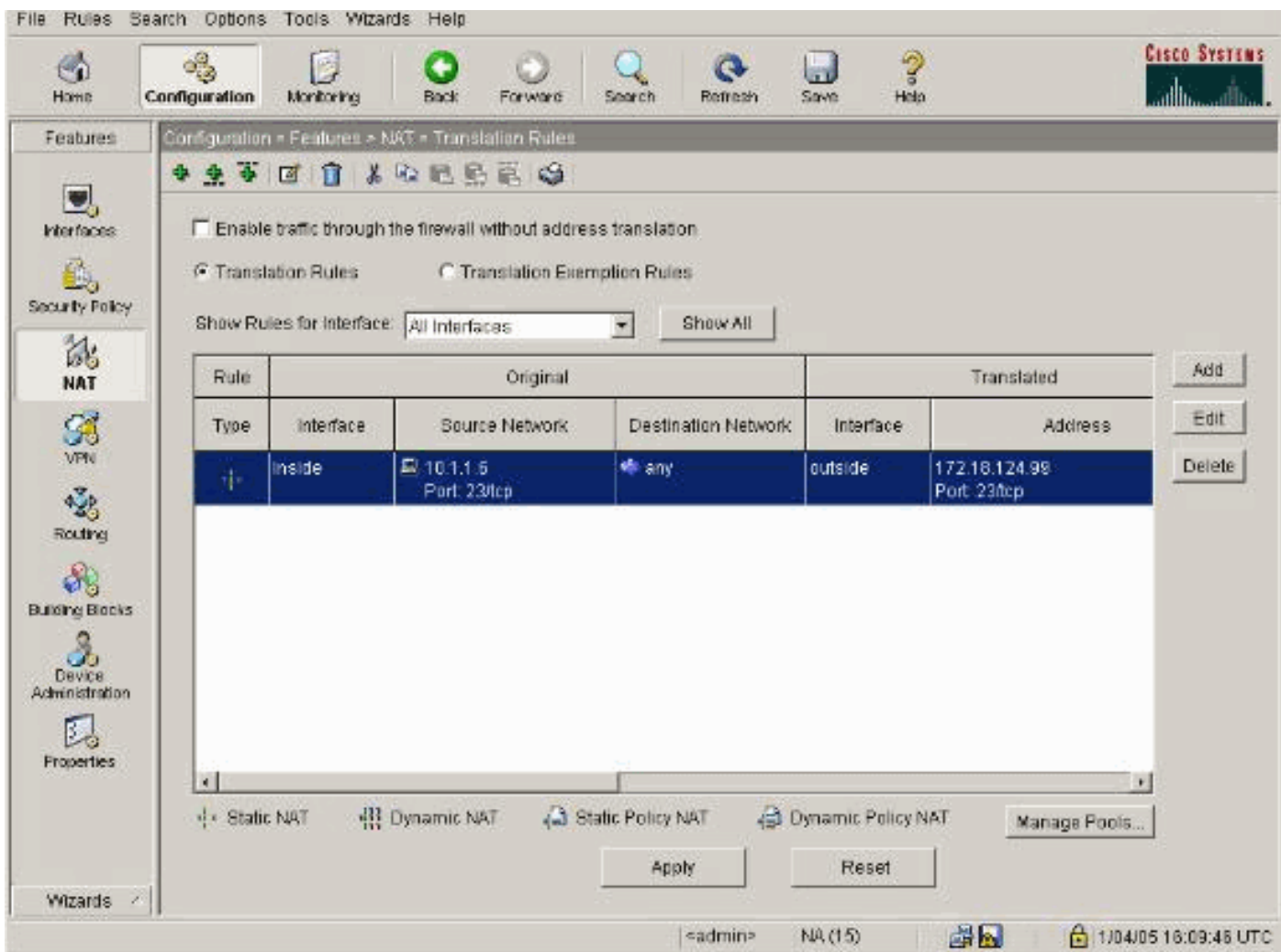
Redirect port

TCP
 UDP
Original port:
Translated port:

 Dynamic
Address Pool:

Pool ID	Address

La traduzione viene visualizzata in Regole di conversione quando scegliete **Configurazione > Caratteristiche > NAT > Regole di conversione**.



[Limita sessione TCP/UDP tramite statico](#)

Per limitare le sessioni TCP o UDP al server interno posizionato in PIX/ASA, usare il comando **static**.

Specifica il numero massimo di connessioni TCP e UDP simultanee per l'intera subnet. Il valore predefinito è 0, che significa connessioni illimitate (le connessioni inattive vengono chiuse dopo il timeout di inattività specificato dal comando **timeout conn**). Questa opzione non si applica al NAT esterno. L'accessorio di protezione tiene traccia delle connessioni solo da un'interfaccia di protezione superiore a un'interfaccia di protezione inferiore.

Limitare il numero di connessioni embrionali ti protegge da un attacco DoS. L'appliance di sicurezza usa il limite embrionale per attivare TCP Intercept, che protegge i sistemi interni da un attacco DoS perpetrato inondando un'interfaccia con i pacchetti TCP SYN. Una connessione embrionale è una richiesta di connessione che non ha completato il handshake necessario tra l'origine e la destinazione. Questa opzione non si applica al NAT esterno. La funzione TCP intercept si applica solo agli host o ai server con un livello di protezione più elevato. Se si imposta il limite embrionale per l'esterno di NAT, il limite embrionale viene ignorato.

Ad esempio:

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100
!--- The maximum number of simultaneous tcp connections the local IP !--- hosts are to allow is
500, default is 0 which means unlimited !--- connections. Idle connections are closed after the
```

time specified !--- by the **timeout conn** command !--- The maximum number of embryonic connections per host is **100**.

%PIX-3-20102: Troppe connessioni in {static|xlate} indirizzo_globale. econns ncon

Questo è un messaggio relativo alla connessione. Questo messaggio viene registrato quando è stato superato il numero massimo di connessioni all'indirizzo statico specificato. La variabile **econnns** è il numero massimo di connessioni embrionali e **ncon** è il numero massimo di connessioni consentite per l'elemento statico o xlate.

L'azione consigliata è quella di utilizzare il comando **show static** per controllare il limite imposto alle connessioni a un indirizzo statico. Il limite è configurabile.

%ASA-3-20101: Il limite di connessioni ha superato 1000/1000 per i pacchetti in entrata da 10.1.26.51/2393 a 10.0.86.155/135 sull'interfaccia esterna

Questo messaggio di errore è causato dall'ID bug Cisco [CSCsg52106](#) (solo utenti [registrati](#)). Per ulteriori informazioni, fare riferimento a questo bug.

Lista accessi temporizzati

La creazione di un intervallo di tempo non limita l'accesso al dispositivo. Il comando **time-range** definisce solo l'intervallo di tempo. Dopo aver definito un intervallo di tempo, è possibile allegarlo alle regole del traffico o a un'azione.

Per implementare un ACL con limiti di tempo, usare il comando **time-range** per definire gli orari del giorno e della settimana. Quindi, usare il comando **con access-list extended time-range** per associare l'intervallo di tempo a un ACL.

L'intervallo di tempo è sincronizzato con l'orologio di sistema dell'appliance di sicurezza. Tuttavia, la funzione offre risultati migliori con la sincronizzazione NTP.

Dopo aver creato un intervallo di tempo e aver immesso la modalità di configurazione dell'intervallo di tempo, è possibile definire i parametri dell'intervallo di tempo con i comandi **assoluto** e **periodico**. Per ripristinare le impostazioni predefinite delle parole chiave assolute e periodiche dei comandi dell'**intervallo di tempo**, usare il comando **default** in modalità di configurazione intervallo di tempo.

Per implementare un ACL con limiti di tempo, usare il comando **time-range** per definire gli orari del giorno e della settimana. Quindi, usare il comando **con access-list extended** per associare l'intervallo di tempo a un ACL. Nell'esempio seguente viene associato un ACL denominato "Sales" a un intervallo di tempo denominato "New York Minute":

In questo esempio viene creato un intervallo di tempo denominato "New York Minute" e viene attivata la modalità di configurazione dell'intervallo di tempo:

```
hostname(config)#time-range New_York_Minute
hostname(config-time-range)#periodic weekdays 07:00 to 19:00
hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute
hostname(config)#access-group Sales in interface inside
```

Informazioni da raccogliere quando si apre una richiesta di assistenza tecnica

Se si ha ancora bisogno di assistenza e si desidera aprire una richiesta di assistenza con il supporto tecnico Cisco, includere queste informazioni per la risoluzione dei problemi relativi all'appliance di sicurezza PIX.

- Descrizione del problema e dettagli relativi alla topologia.
- La procedura utilizzata per la risoluzione dei problemi prima dell'apertura della richiesta.
- Output del comando **show tech-support**.
- Output del comando **show log** dopo l'esecuzione del comando **logging buffered debugging** o acquisizioni della console che dimostrano il problema (se disponibile).

Allegare i dati raccolti alla richiesta in formato testo normale non compresso (txt). È possibile allegare informazioni alla richiesta nello [strumento TAC Service Request](#) (solo utenti [registrati](#)). Se non è possibile accedere allo [strumento TAC Service Request](#) (solo utenti [registrati](#)), è possibile inviare le informazioni in un allegato e-mail a attach@cisco.com con il numero della richiesta in oggetto.

Informazioni correlate

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