

# PIX/ASA 7.x: Port Redirection(Forwarding) mit NAT-, Global-, statischen und Zugriffslistenbefehlen

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Netzwerkdiagramm](#)

[Erstkonfiguration](#)

[Ausgehenden Zugriff zulassen](#)

[Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen](#)

[Zulassen des Zugriffs von internen Hosts auf externe Netzwerke mithilfe von PAT](#)

[Einschränken des Zugriffs von internen Hosts auf externe Netzwerke](#)

[Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen](#)

[Verwenden von ACLs auf PIX 7.0 und höher](#)

[Deaktivieren von NAT für bestimmte Hosts/Netzwerke](#)

[Port Redirection \(Forwarding\) mit Statistiken](#)

[Netzwerkdiagramm - Port Redirection \(Forwarding\)](#)

[Partielle PIX-Konfiguration - Port-Umleitung](#)

[Einschränkung der TCP/UDP-Sitzung mithilfe von Static](#)

[Zeitbasierte Zugriffsliste](#)

[Informationen zum Sammeln, wenn Sie ein technisches Support-Ticket öffnen](#)

[Zugehörige Informationen](#)

## Einführung

Um die Sicherheit bei der Implementierung der Cisco PIX Security Appliance Version 7.0 zu maximieren, müssen Sie wissen, wie Pakete zwischen höheren Sicherheitsschnittstellen und niedrigeren Sicherheitsschnittstellen weitergeleitet werden, wenn Sie die Befehle **nat-control**, **nat**, **global**, **static**, **access-list** und **access-group** verwenden. In diesem Dokument werden die Unterschiede zwischen diesen Befehlen und die Konfiguration der Port Redirection (Forwarding) und der externen Network Address Translation (NAT)-Funktionen in der PIX-Software Version 7.x unter Verwendung der Befehlszeilenschnittstelle oder des Adaptive Security Device Manager (ASDM) erläutert.

**Hinweis:** Einige Optionen in ASDM 5.2 und höher können sich von den Optionen in ASDM 5.1 unterscheiden. Weitere Informationen finden Sie in der [ASDM-Dokumentation](#).

## [Voraussetzungen](#)

### [Anforderungen](#)

Informationen zur Konfiguration des Geräts durch den ASDM finden Sie unter [Zulassen von HTTPS-Zugriff für ASDM](#).

### [Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco PIX Security Appliance Software der Serie 500, Version 7.0 und höher
- ASDM Version 5.x oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

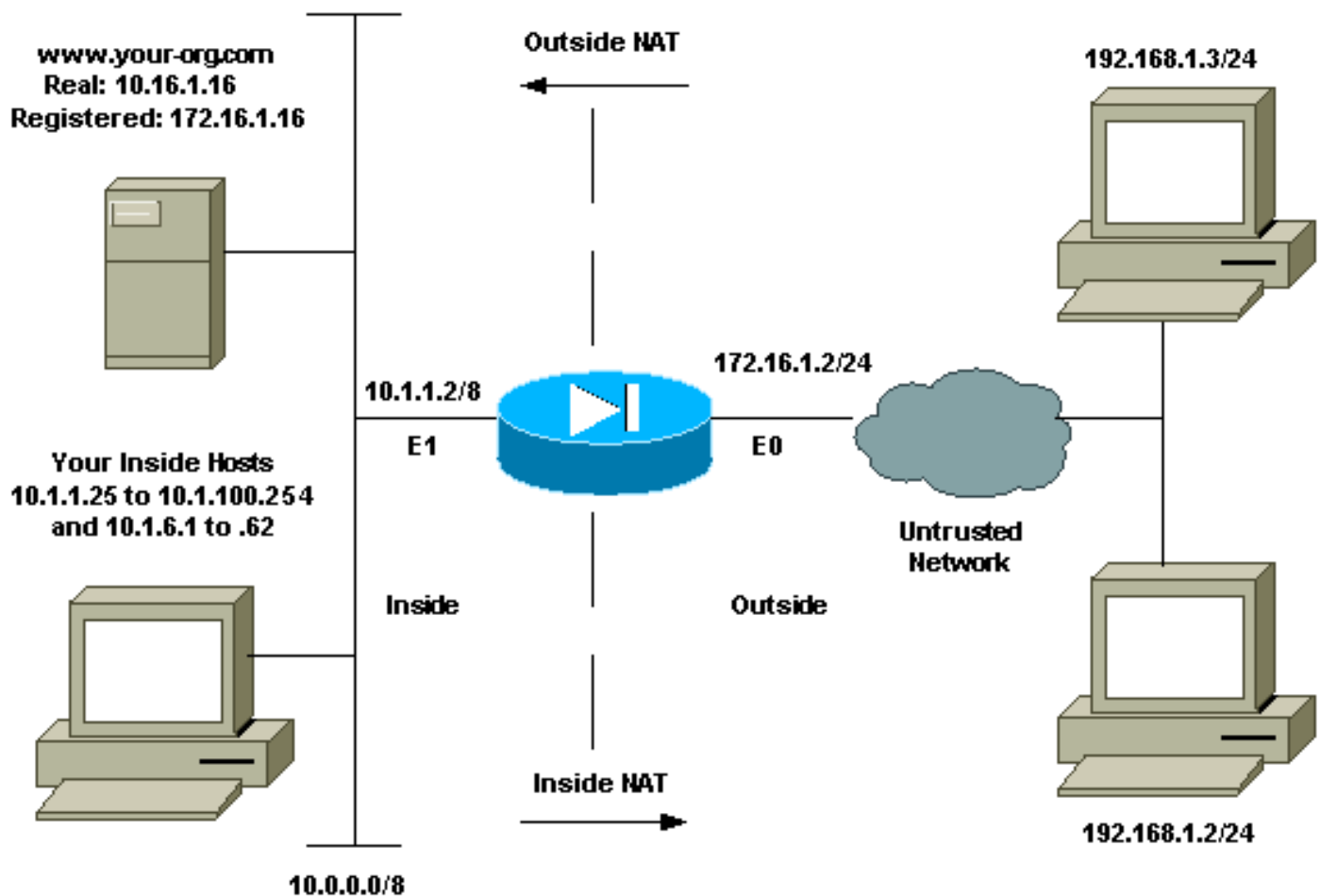
### [Zugehörige Produkte](#)

Sie können diese Konfiguration auch mit Cisco ASA Security Appliance Version 7.x oder höher verwenden.

### [Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## [Netzwerkdiagramm](#)



Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

## Erstkonfiguration

Die Schnittstellennamen lauten:

- **interface ethernet 0** - Name außerhalb
- **interface ethernet 1** - Name innen

**Hinweis:** Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

## Ausgehenden Zugriff zulassen

Der ausgehende Zugriff beschreibt Verbindungen von einer Schnittstelle mit höherer Sicherheitsstufe zu einer Schnittstelle mit niedrigerer Sicherheitsstufe. Dazu gehören Verbindungen von innen nach außen, von innen nach Demilitarized Zones (DMZs) und von DMZs nach außen. Dies kann auch Verbindungen von einer DMZ zu einer anderen umfassen, sofern die Schnittstelle der Verbindungsquelle eine höhere Sicherheitsstufe als das Ziel hat. Überprüfen Sie die Konfiguration der "Sicherheitsstufe" an den PIX-Schnittstellen, um dies zu bestätigen.

Dieses Beispiel zeigt die Sicherheitsstufe und die Konfiguration des Schnittstellennamen:

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

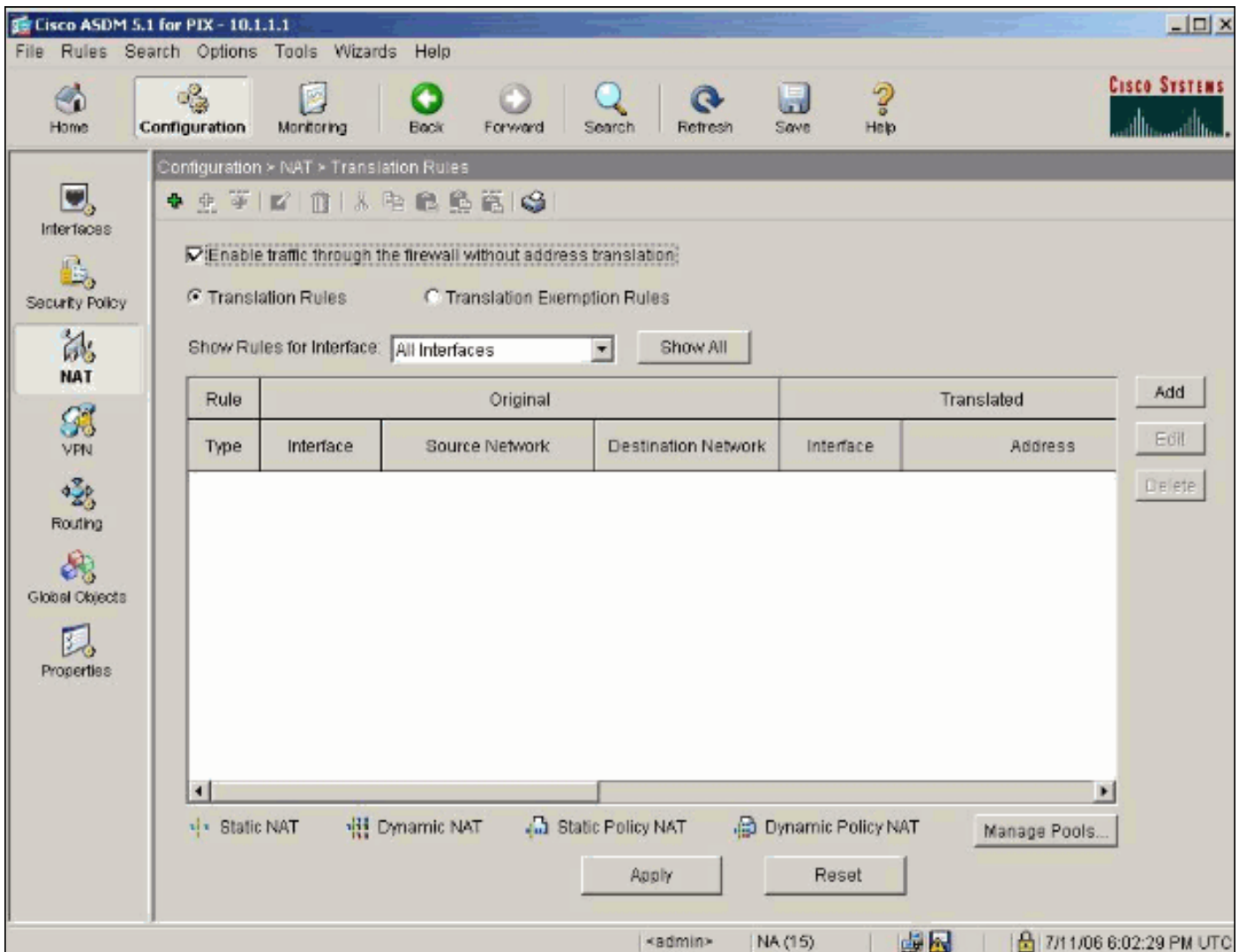
```
pix(config-if)#security-level 0  
pix(config-if)#nameif outside  
pix(config-if)#exit
```

PIX 7.0 führt den Befehl **nat-control ein**. Sie können den Befehl **nat-control** im Konfigurationsmodus verwenden, um anzugeben, ob NAT für externe Kommunikation erforderlich ist. Bei aktivierter NAT-Kontrolle ist eine Konfiguration von NAT-Regeln erforderlich, um ausgehenden Datenverkehr zuzulassen, wie dies bei früheren Versionen der PIX-Software der Fall ist. Wenn die NAT-Steuerung deaktiviert ist (**keine NAT-Kontrolle**), können interne Hosts ohne Konfiguration einer NAT-Regel mit externen Netzwerken kommunizieren. Wenn Sie jedoch interne Hosts haben, die keine öffentlichen Adressen haben, müssen Sie NAT für diese Hosts konfigurieren.

Um die NAT-Steuerung mithilfe von ASDM zu konfigurieren, wählen Sie im ASDM Home-Fenster die Registerkarte Configuration (Konfiguration) aus, und wählen Sie **NAT** im Funktionsmenü aus.

**Ermöglichen Sie ohne Übersetzung Datenverkehr durch die Firewall:** Diese Option wurde in PIX Version 7.0(1) eingeführt. Wenn diese Option aktiviert ist, wird in der Konfiguration kein Befehl zur **Nichtkontrolle** ausgegeben. Dieser Befehl bedeutet, dass keine Übersetzung erforderlich ist, um die Firewall zu passieren. Diese Option wird in der Regel nur aktiviert, wenn interne Hosts öffentliche IP-Adressen haben oder die Netzwerktopologie keine Übersetzung interner Hosts in eine beliebige IP-Adresse erfordert.

Wenn interne Hosts über private IP-Adressen verfügen, muss diese Option deaktiviert werden, damit interne Hosts in eine öffentliche IP-Adresse übersetzt werden und auf das Internet zugreifen können.



Es gibt zwei Richtlinien, die erforderlich sind, um den ausgehenden Zugriff mit NAT-Kontrolle zu ermöglichen. Die erste Methode ist eine Übersetzungsmethode. Dabei kann es sich um eine statische Übersetzung mit dem **statischen** Befehl oder um eine dynamische Übersetzung mit einer **nat/global**-Regel handeln. Dies ist nicht erforderlich, wenn die NAT-Kontrolle deaktiviert ist und Ihre internen Hosts öffentliche Adressen haben.

Die andere Anforderung für den ausgehenden Zugriff (gilt für die Aktivierung oder Deaktivierung der NAT-Steuerung) besteht darin, dass eine Zugriffskontrollliste (ACL) vorhanden ist. Wenn eine ACL vorhanden ist, muss sie dem Quell-Host mithilfe des spezifischen Protokolls und Ports Zugriff auf den Zielhost gewähren. Standardmäßig gibt es keine Zugriffsbeschränkungen für ausgehende Verbindungen über den PIX. Wenn für die Ausgangsschnittstelle keine ACL konfiguriert ist, ist die ausgehende Verbindung standardmäßig zulässig, wenn eine Übersetzungsmethode konfiguriert wurde.

### [Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen](#)

Diese Konfiguration gewährt allen Hosts im Subnetz 10.1.6.0/24 Zugriff auf die Außenseite. Verwenden Sie dazu die **nat**- und die **globalen** Befehle, wie in diesem Verfahren veranschaulicht wird.

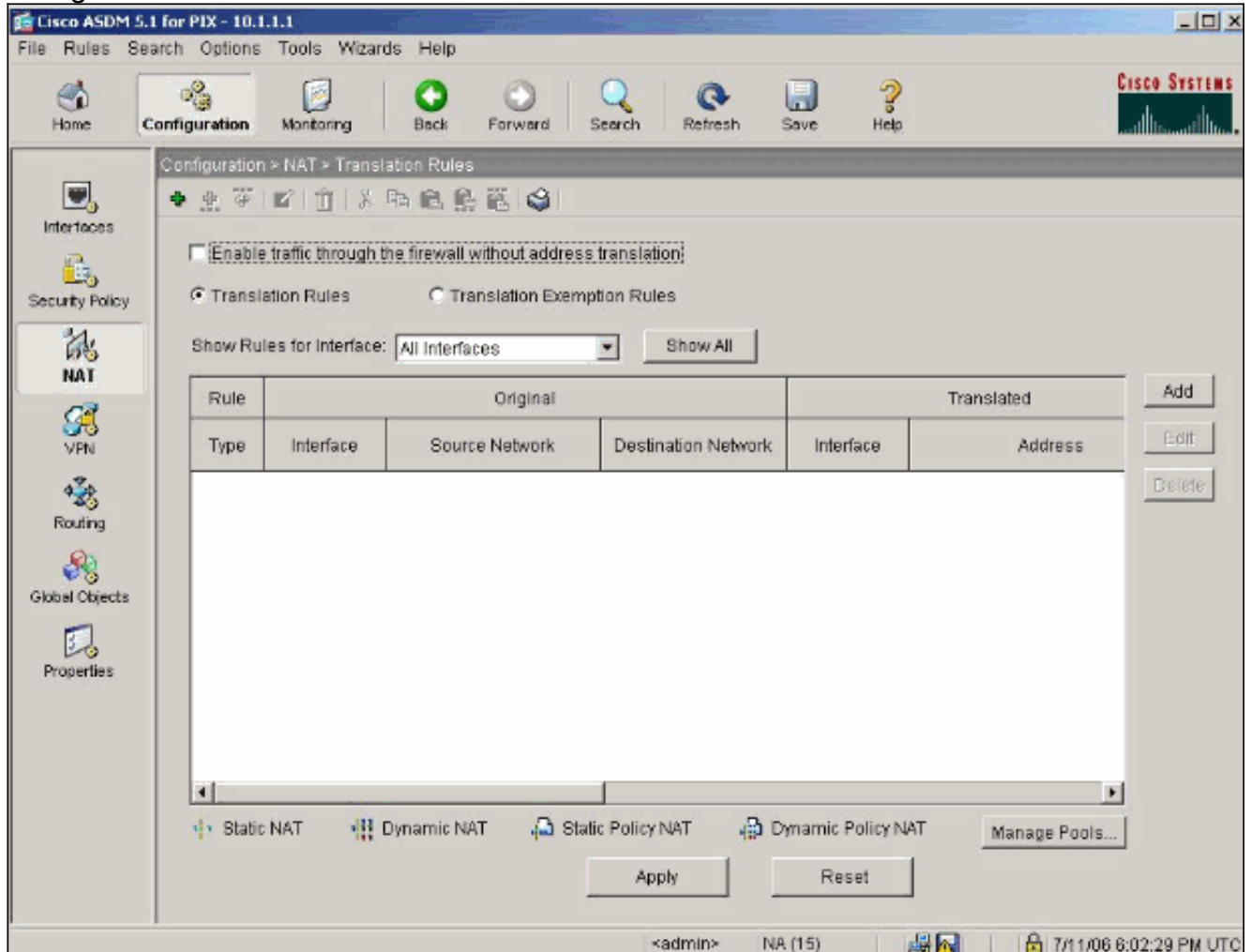
1. Definieren Sie die interne Gruppe, die Sie für NAT einschließen möchten.

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

2. Geben Sie einen Adresspool auf der externen Schnittstelle an, in die die in der NAT-Anweisung definierten Hosts übersetzt werden.

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

3. Verwenden Sie ASDM, um Ihren globalen Adresspool zu erstellen. Wählen Sie **Configuration > Features > NAT** aus, und deaktivieren Sie **Enable traffic through the firewall without address translation**. Klicken Sie anschließend auf **Hinzufügen**, um die NAT-Regel zu konfigurieren.



4. Klicken Sie auf **Pools verwalten**, um die NAT-Pooladressen zu definieren.

**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:

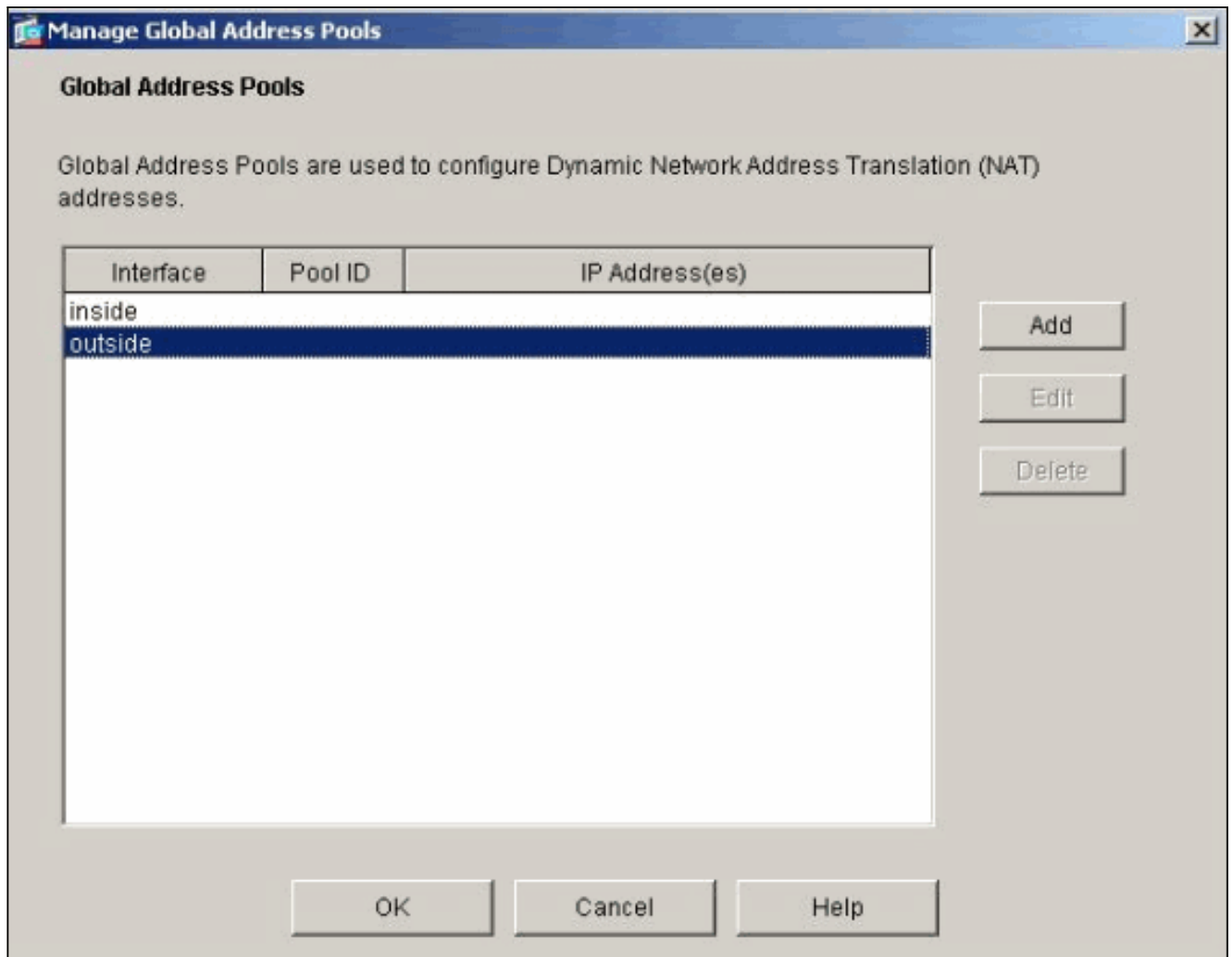
UDP

Dynamic    Address Pool:    

Pool ID	Address
N/A	No address pool defined

5. Wählen Sie **Außen > Hinzufügen**, und wählen Sie einen Bereich aus, um einen Adresspool anzugeben.



6. Geben Sie Ihren Adressbereich ein, geben Sie eine Pool-ID ein, und klicken Sie auf **OK**.



**Add Global Pool Item**

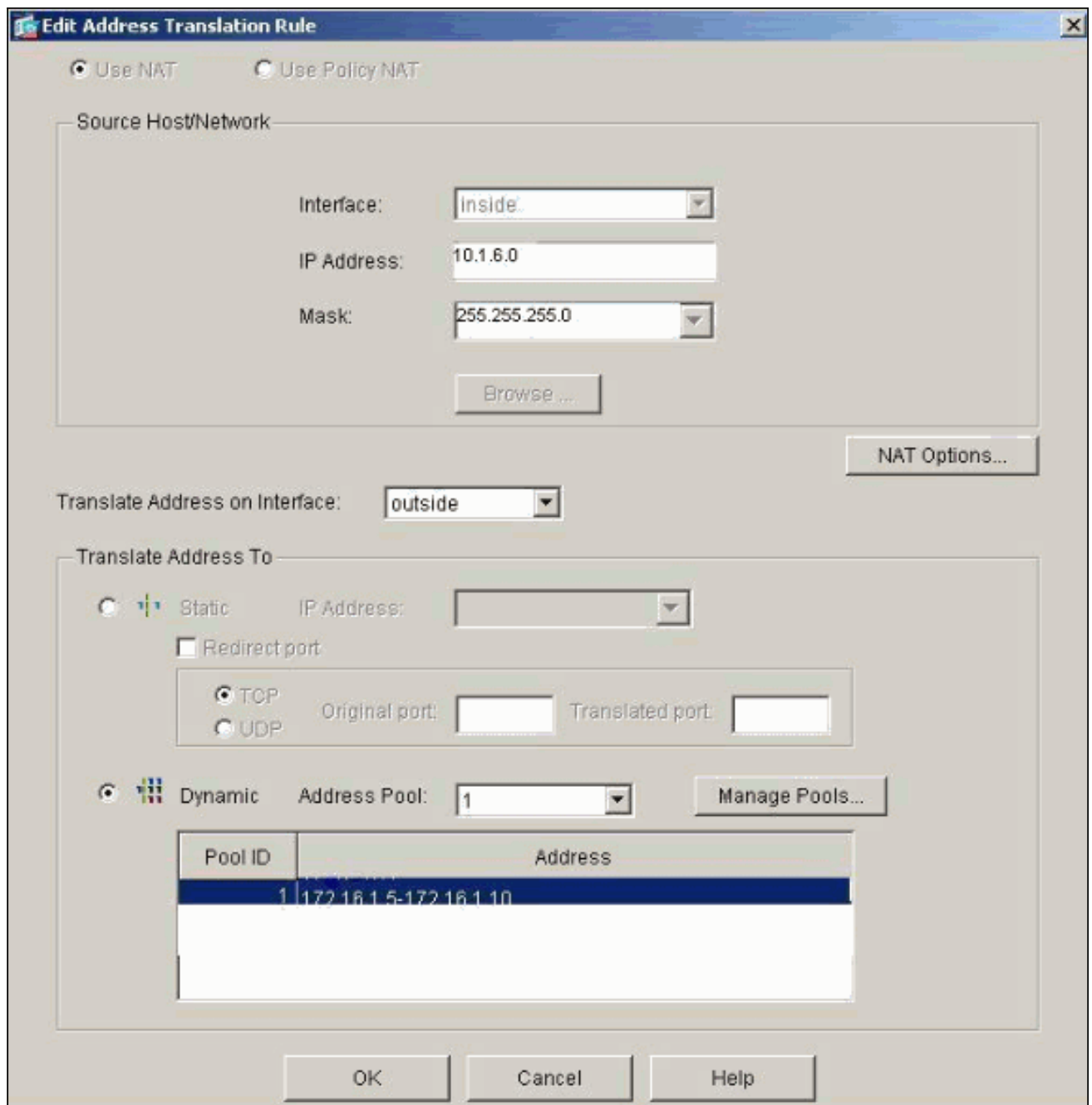
Interface:  Pool ID:

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

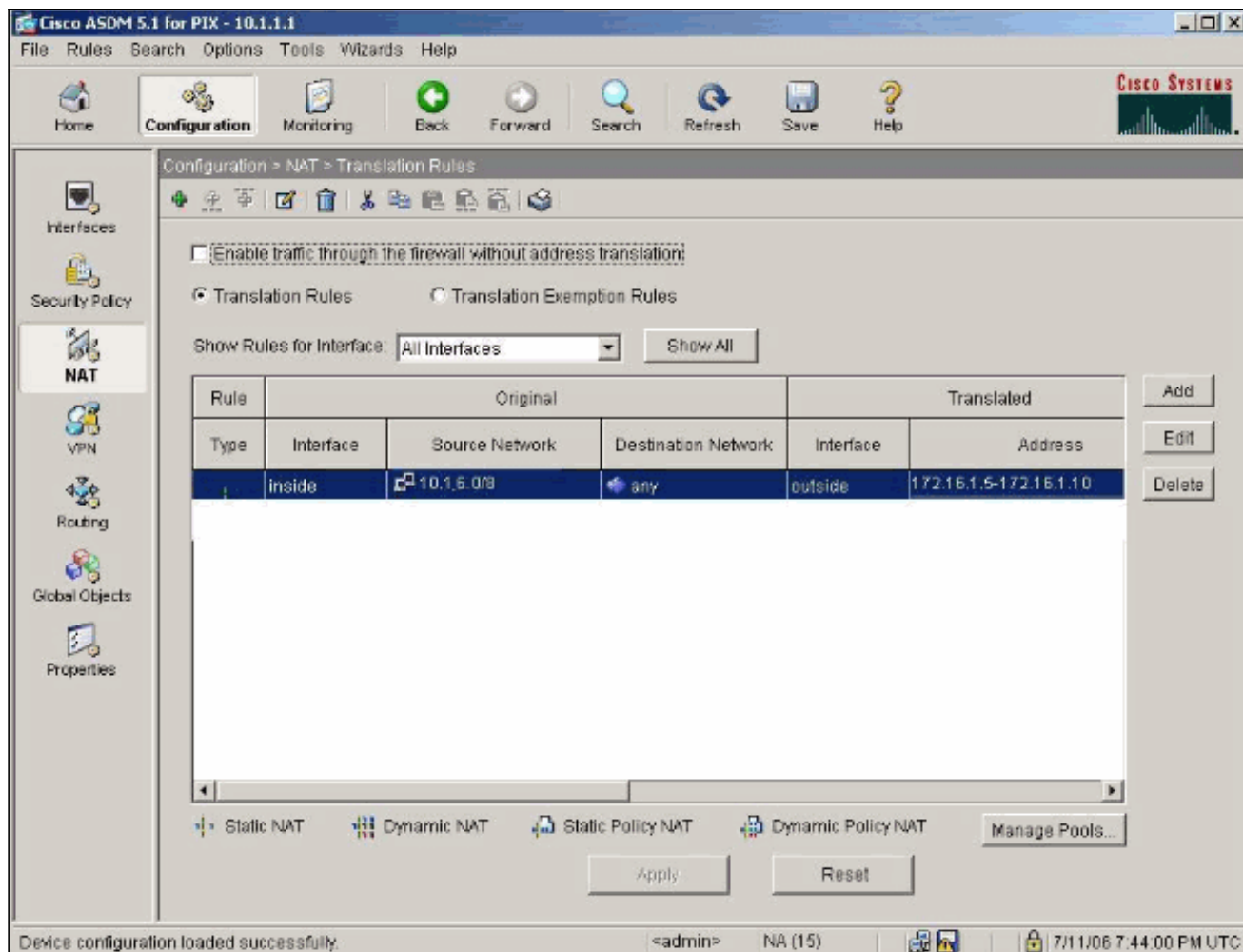
IP Address:  —

Network Mask (optional):

7. Wählen Sie **Konfiguration > Funktionen > NAT > Übersetzungsregeln**, um die Übersetzungsregel zu erstellen.
8. Wählen Sie **Inside** als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT hinzufügen möchten.
9. Wählen Sie zum Übersetzen der Adresse auf der Schnittstelle die Option **Außen aus**, wählen Sie **Dynamisch**, und wählen Sie den soeben konfigurierten Adresspool aus.
10. Klicken Sie auf **OK**.



11. Die Übersetzung wird unter Übersetzungsregeln unter **Konfiguration > Funktionen > NAT > Übersetzungsregeln** angezeigt.



Die Hosts im Inneren können nun auf externe Netzwerke zugreifen. Wenn Hosts von innen eine Verbindung nach außen initiieren, werden sie in eine Adresse aus dem globalen Pool übersetzt. Die Adressen werden aus dem globalen Pool auf Basis des "first-come", "first-translated" zugewiesen und beginnen mit der "low address" im Pool. Wenn beispielsweise Host 10.1.6.25 als erster eine Verbindung mit der Außenseite initiiert, erhält er die Adresse 172.16.1.5. Der nächste Host erhält 172.16.1.6 usw. Dabei handelt es sich nicht um eine statische Übersetzung, und die Übersetzung wird nach einer Inaktivität gemäß dem Befehl **timeout xlate hh:mm:ss** abgebrochen. Wenn mehr interne Hosts vorhanden sind, als Adressen im Pool vorhanden sind, wird die letzte Adresse im Pool für die Port Address Translation (PAT) verwendet.

## [Zulassen des Zugriffs von internen Hosts auf externe Netzwerke mithilfe von PAT](#)

Wenn interne Hosts eine einzige öffentliche Adresse für die Übersetzung freigeben möchten, verwenden Sie PAT. Wenn die **globale** Anweisung eine Adresse angibt, wird diese Adresse vom Port übersetzt. Das PIX ermöglicht die Übersetzung eines Ports pro Schnittstelle und unterstützt bis zu 65.535 aktive Xlate-Objekte in eine globale Adresse. Führen Sie diese Schritte aus, um internen Hosts den Zugriff auf externe Netzwerke mithilfe von PAT zu ermöglichen.

1. Definieren Sie die interne Gruppe, die Sie für PAT einschließen möchten (wenn Sie 0 0 verwenden, wählen Sie alle internen Hosts aus.)

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

2. Geben Sie die globale Adresse an, die Sie für PAT verwenden möchten. Dies kann die

Schnittstellenadresse sein.

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

3. Wählen Sie im ASDM **Configuration > Features > NAT aus**, und deaktivieren Sie **Enable traffic through the firewall Without address translation**.
4. Klicken Sie auf **Hinzufügen**, um die NAT-Regel zu konfigurieren.
5. Wählen Sie **Pools verwalten**, um Ihre PAT-Adresse zu konfigurieren.
6. Wählen Sie **Outside > Add** und klicken Sie auf **Port Address Translation (PAT)**, um eine einzelne Adresse für PAT zu konfigurieren.
7. Geben Sie eine Adresse und eine Pool-ID ein, und klicken Sie auf **OK**.

The screenshot shows a dialog box titled "Add Global Pool Item". It has a blue title bar with a close button. The main area is light gray. At the top, there are two fields: "Interface:" with a dropdown menu showing "outside" and "Pool ID:" with a text box containing "1". Below these are three radio buttons: "Range" (unselected), "Port Address Translation (PAT)" (selected), and "Port Address Translation (PAT) using the IP address of the interface" (unselected). In the center, there is a larger gray box containing two input fields: "IP Address:" with "172.16.1.4" and "Network Mask (optional):" with "255.255.255.0". At the bottom, there are three buttons: "OK", "Cancel", and "Help".

8. Wählen Sie **Konfiguration > Funktionen > NAT > Übersetzungsregeln**, um die Übersetzungsregel zu erstellen.
9. Wählen Sie als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT hinzufügen möchten.
10. Wählen Sie zum Übersetzen der Adresse auf der Schnittstelle **außerhalb aus**, wählen Sie **Dynamic (Dynamisch)**, und wählen Sie den soeben konfigurierten Adresspool aus. Klicken Sie auf **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:

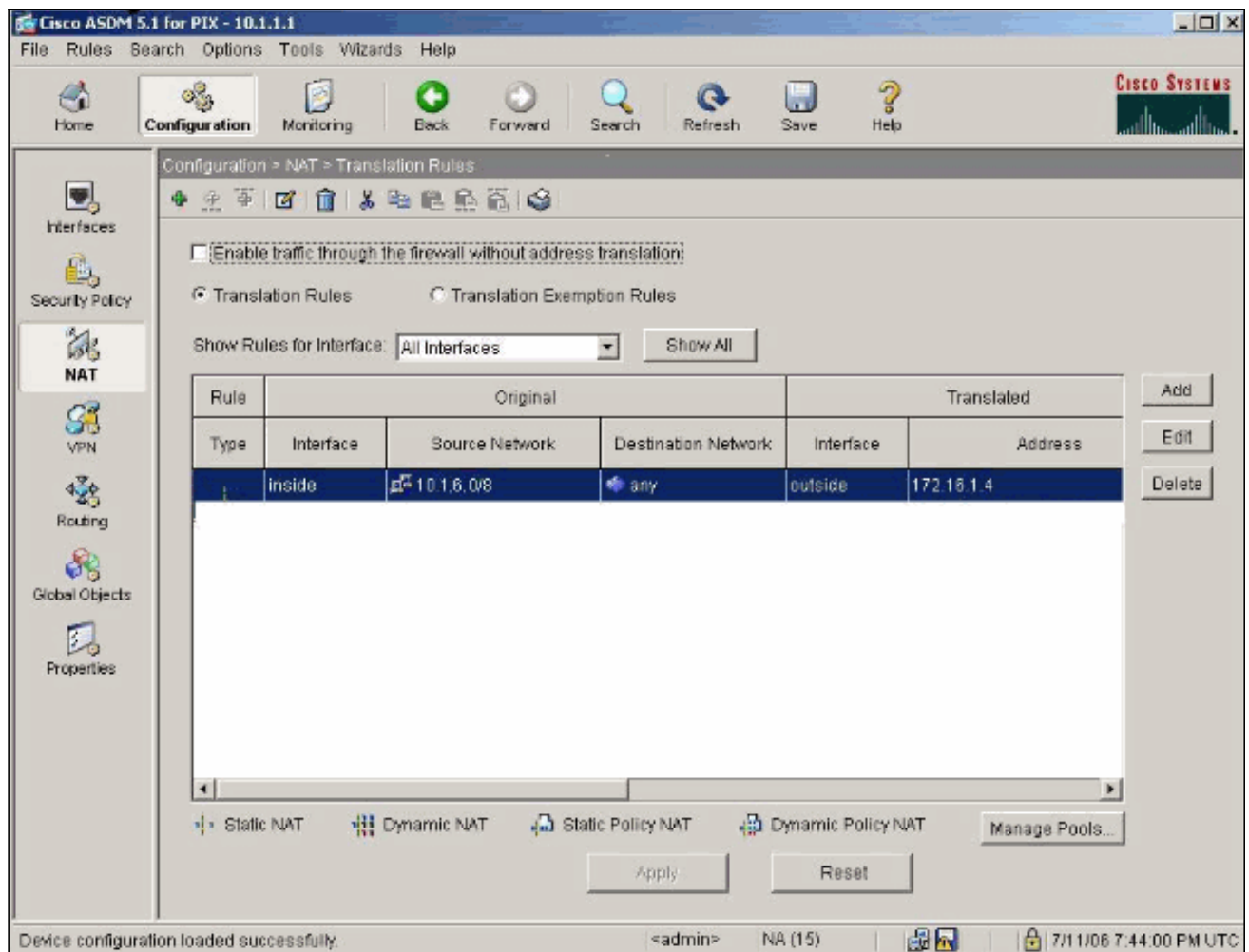
UDP

Dynamic    Address Pool:    

Pool ID	Address
1	172.16.1.4

11. Die Übersetzung wird unter Übersetzungsregeln unter **Konfiguration > Funktionen > NAT > Übersetzungsregeln** angezeigt.



Bei der Verwendung von PAT müssen einige Punkte beachtet werden.

- Die von Ihnen für PAT angegebenen IP-Adressen dürfen sich nicht in einem anderen globalen Adresspool befinden.
- PAT funktioniert nicht mit H.323-Anwendungen, Caching-Nameservern und Point-to-Point Tunneling Protocol (PPTP). PAT arbeitet mit Domain Name Service (DNS), FTP und passivem FTP, HTTP, E-Mail, RPC (Remote Procedure Call), Rshell, Telnet, URL-Filterung und Outbound Traceroute zusammen.
- Verwenden Sie PAT nicht, wenn Sie Multimedia-Anwendungen über die Firewall ausführen müssen. Multimedia-Anwendungen können mit Port-Zuordnungen kollidieren, die PAT bereitstellt.
- In der PIX-Softwareversion 4.2(2) funktioniert die PAT-Funktion nicht mit IP-Datenpaketen, die in umgekehrter Reihenfolge eintreffen. PIX Software Version 4.2(3) behebt dieses Problem.
- IP-Adressen im Pool globaler Adressen, die mit dem **globalen** Befehl angegeben werden, erfordern umgekehrte DNS-Einträge, um sicherzustellen, dass alle externen Netzwerkadressen über den PIX zugänglich sind. Um umgekehrte DNS-Zuordnungen zu erstellen, verwenden Sie einen DNS-Zeiger-Datensatz (PTR) in der Datei für die Zuordnung von Adressen zu Namen für jede globale Adresse. Ohne die PTR-Einträge können an Standorten langsame oder zeitweilige Internetverbindungen auftreten, und FTP-Anfragen fallen konsistent aus. Wenn eine globale IP-Adresse beispielsweise 192.168.1.3 lautet und der Domänenname für die PIX Security Appliance pix.caguana.com lautet, lautet der PTR-Datensatz:

```
3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
4.1.1.175.in-addr.arpa. IN PTR
```

## Einschränken des Zugriffs von internen Hosts auf externe Netzwerke

Wenn für den Quellhost eine gültige Übersetzungsmethode definiert ist und für die Quell-PIX-Schnittstelle keine ACL definiert ist, ist die ausgehende Verbindung standardmäßig zulässig. In einigen Fällen ist es jedoch erforderlich, den ausgehenden Zugriff basierend auf Quelle, Ziel, Protokoll und/oder Port einzuschränken. Konfigurieren Sie dazu eine ACL mit dem Befehl **access-list**, und wenden Sie sie mit dem Befehl **access-group** auf die PIX-Schnittstelle der Verbindungsquelle an. Sie können PIX 7.0-ACLs sowohl in ein- als auch in ausgehende Richtungen anwenden. Dieses Verfahren ist ein Beispiel, das den ausgehenden HTTP-Zugriff für ein Subnetz zulässt, aber allen anderen Hosts den HTTP-Zugriff auf die Außenseite verweigert, während der gesamte andere IP-Datenverkehr für alle zugelassen wird.

### 1. Definieren Sie die 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
```

**Hinweis:** PIX-ACLs unterscheiden sich von ACLs auf Cisco IOS®-Routern, da PIX keine Platzhaltermaske wie Cisco IOS verwendet. In der ACL-Definition wird eine reguläre Subnetzmaske verwendet. Wie auch bei Cisco IOS-Routern verfügt die PIX-ACL am Ende der ACL über eine implizite "Deny all" (Alle verweigern). **Hinweis:** Neue Zugriffslisteneinträge werden am Ende der bestehenden ACEs angefügt. Wenn Sie zuerst einen bestimmten ACE benötigen, können Sie das `line`-Schlüsselwort in der Zugriffsliste verwenden. Dies ist eine Beispielbefehlsübersicht:

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

### 2. Wenden Sie die ACL auf die interne Schnittstelle an.

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

### 3. Verwenden Sie ASDM, um den ersten Zugriffslisteneintrag in Schritt 1 so zu konfigurieren, dass HTTP-Datenverkehr von 10.1.6.0/24 zugelassen wird. Wählen Sie **Konfiguration > Funktionen > Sicherheitsrichtlinie > Zugriffsregeln** aus.

### 4. Klicken Sie auf **Hinzufügen**, geben Sie die Informationen wie in diesem Fenster angezeigt ein, und klicken Sie auf **OK**.



**Add Access Rule**

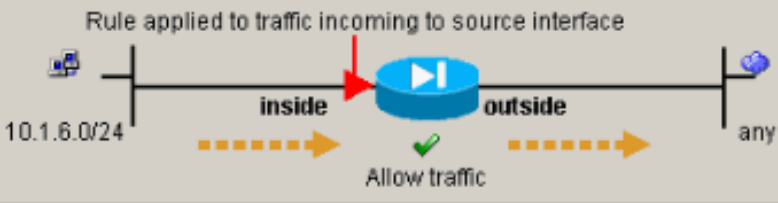
**Action**  
 Select an action:   
 Apply to Traffic:

**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 red arrow pointing towards the router. To the left of this line is a computer icon and the text '10.1.6.0/24'. On the right, a vertical line represents the 'outside' interface, with a red arrow pointing away from the router. To the right of this line is a server icon and the text 'any'. A green checkmark is positioned below the router with the text 'Allow traffic'. Dashed orange arrows indicate the flow of traffic from the inside interface through the router to the outside interface.

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

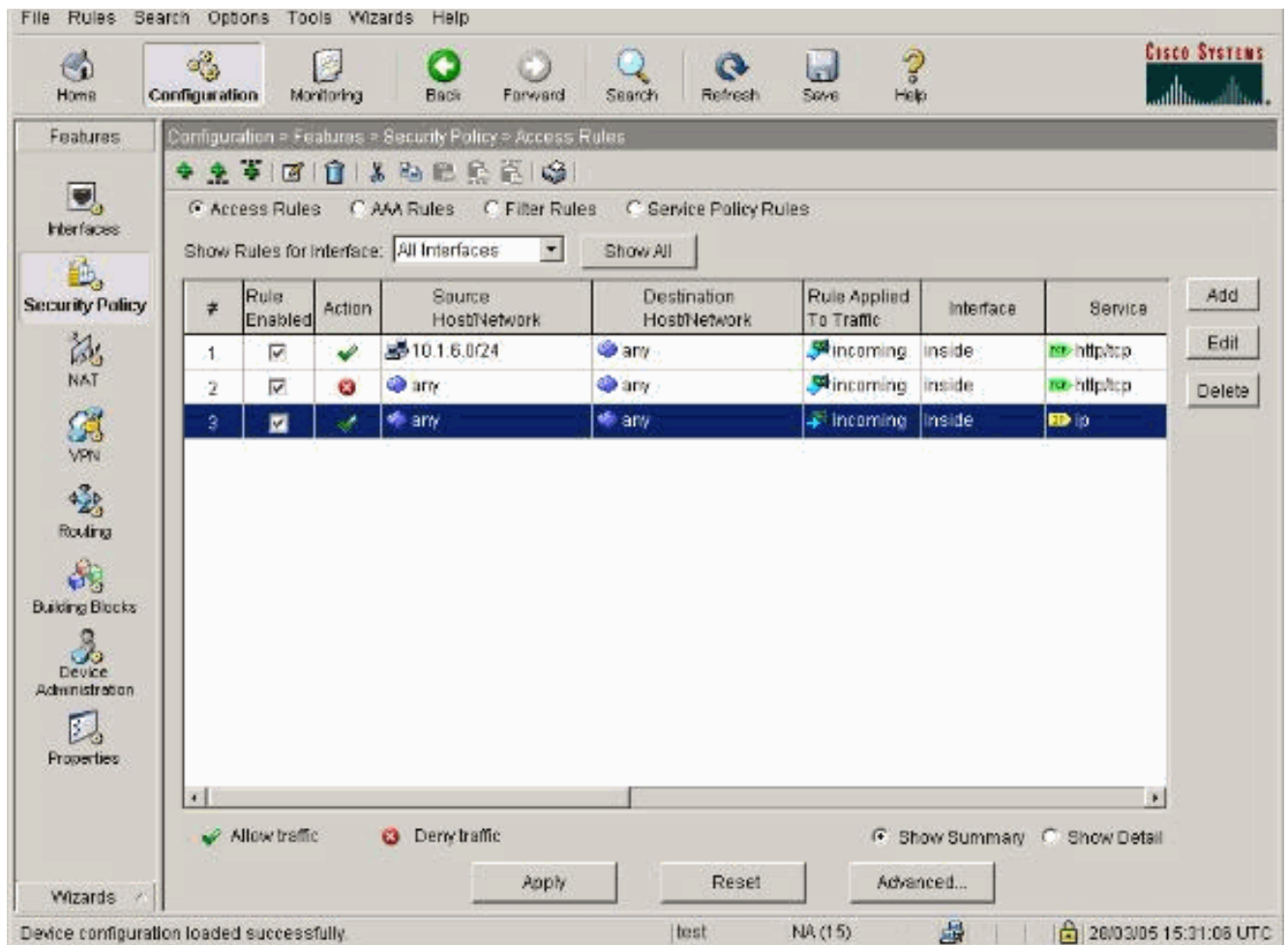
**Destination Port**  
 Service =  ...  
 Service Group

Please enter the description below (optional):

5. Wenn Sie die drei Zugriffslisteneinträge eingegeben haben, wählen Sie **Konfiguration > Funktion > Sicherheitsrichtlinie > Zugriffsregeln**, um diese Regeln anzuzeigen.





## Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen

Die meisten Unternehmen müssen nicht vertrauenswürdigen Hosts den Zugriff auf Ressourcen in ihrem vertrauenswürdigen Netzwerk ermöglichen. Ein gängiges Beispiel ist ein interner Webserver. Standardmäßig verweigert der PIX Verbindungen von externen Hosts zu internen Hosts. Um diese Verbindung im NAT-Steuerungsmodus zuzulassen, verwenden Sie den **statischen** Befehl mit **Zugriffslisten-** und **Zugriffsgruppen-**Befehlen. Wenn die NAT-Kontrolle deaktiviert ist, sind nur die Befehle **für Zugriffslisten** und **Zugriffsgruppen** erforderlich, wenn keine Übersetzung durchgeführt wird.

Anwenden von ACLs auf Schnittstellen mit einem Befehl **access-group**. Dieser Befehl ordnet die ACL der Schnittstelle zu, um den Datenverkehr zu überprüfen, der in eine bestimmte Richtung fließt.

Im Gegensatz zu den **nat-** und **globalen** Befehlen, die interne Hosts erlauben, erstellt der **statische** Befehl eine bidirektionale Übersetzung, die es internen Hosts außerhalb und externen Hosts erlaubt, die richtigen ACLs/Gruppen hinzuzufügen.

Wenn ein externer Host in den in diesem Dokument gezeigten PAT-Konfigurationsbeispielen versucht, eine Verbindung zur globalen Adresse herzustellen, kann er von Tausenden von internen Hosts verwendet werden. Der **statische** Befehl erstellt eine Eins-zu-Eins-Zuordnung. Der Befehl **access-list** definiert, welcher Verbindungstyp für einen internen Host zulässig ist und wird immer benötigt, wenn ein Host mit niedrigerer Sicherheit eine Verbindung zu einem Host mit höherer Sicherheit herstellt. Der Befehl **access-list** basiert sowohl auf Port als auch auf Protokoll

und kann sehr permissiv oder sehr restriktiv sein, je nachdem, was der Systemadministrator erreichen möchte.

Das [Netzwerkdiagramm](#) in diesem Dokument veranschaulicht die Verwendung dieser Befehle, um das PIX so zu konfigurieren, dass alle nicht vertrauenswürdigen Hosts eine Verbindung zum internen Webserver herstellen können und nicht vertrauenswürdigen Host 192.168.1.1 den Zugriff auf einen FTP-Dienst auf demselben Computer ermöglichen.

## [Verwenden von ACLs auf PIX 7.0 und höher](#)

Führen Sie diese Schritte für die PIX-Softwareversion 7.0 und höher durch, und verwenden Sie ACLs.

1. Wenn die NAT-Kontrolle aktiviert ist, definieren Sie eine statische Adressumwandlung für den internen Webserver in eine externe/globale Adresse.

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

2. Legen Sie fest, welche Hosts eine Verbindung zu welchen Ports zu Ihrem Web/FTP-Server herstellen können.

```
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. Wenden Sie die ACL auf die externe Schnittstelle an.

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

4. Wählen Sie **Configuration > Features > NAT** und klicken Sie auf **Add**, um diese statische Übersetzung mit ASDM zu erstellen.
5. Wählen Sie **als** Ausgangsschnittstelle aus, und geben Sie die interne Adresse ein, für die Sie eine statische Übersetzung erstellen möchten.
6. Wählen Sie **Statisch**, und geben Sie die externe Adresse, in die übersetzt werden soll, in das IP-Adressfeld ein. Klicken Sie auf **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

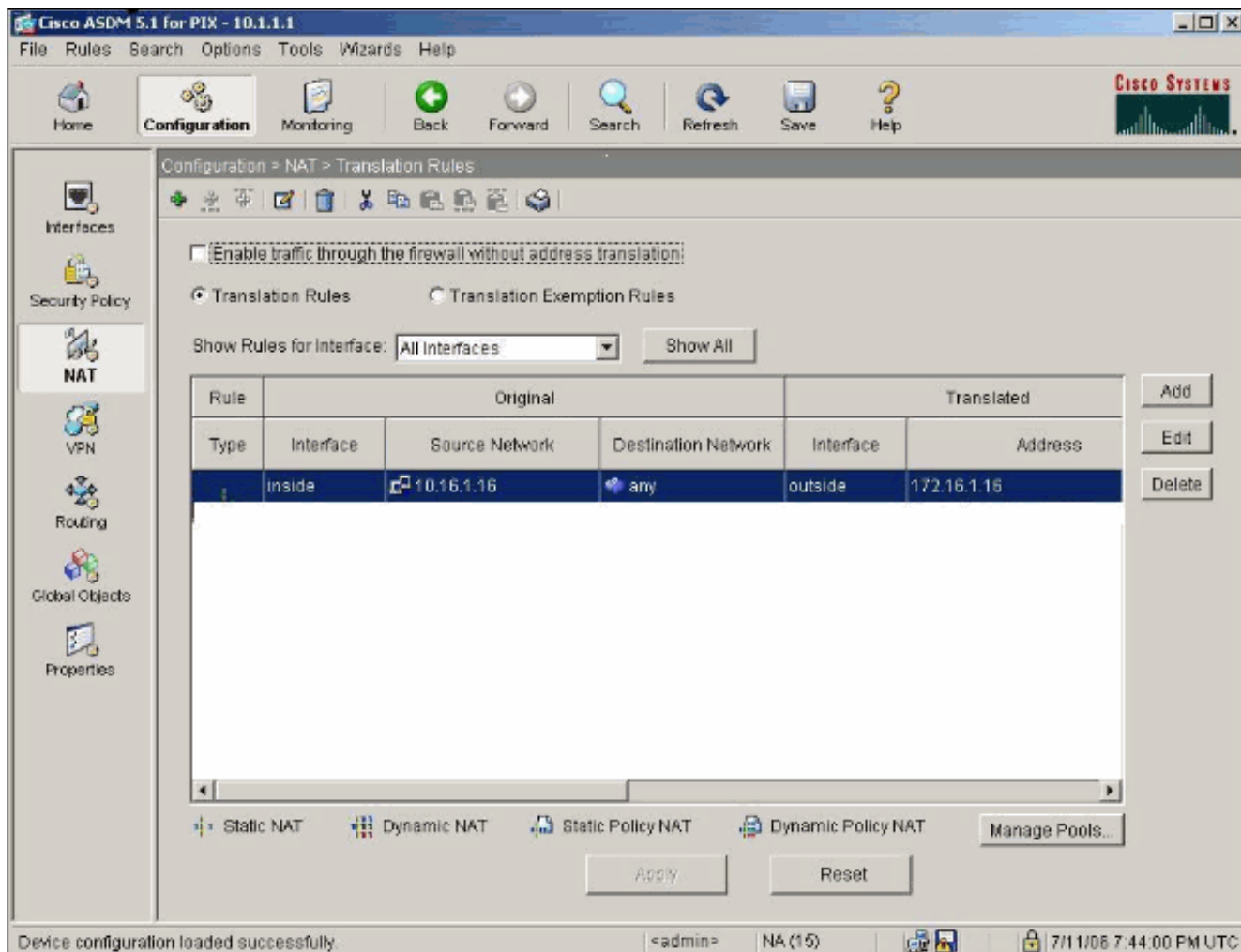
TCP     Original port:      Translated port:   
 UDP

 Dynamic     Address Pool:     

Pool ID	Address

7. Die Übersetzung wird in den Übersetzungsregeln angezeigt, wenn Sie **Configuration > Features > NAT > Translation Rules** auswählen.



8. Verwenden Sie die Prozedur [Restrict Inside Hosts Access to Outside Networks \(Zugriff auf externe Netzwerke einschränken\)](#), um die **Zugriffslisteneinträge** einzugeben. **Hinweis:** Seien Sie vorsichtig, wenn Sie diese Befehle implementieren. Wenn Sie die **Zugriffsliste 101 permit ip any** command implementieren, kann jeder Host im nicht vertrauenswürdigen Netzwerk mit IP auf jeden Host im vertrauenswürdigen Netzwerk zugreifen, sofern eine aktive Übersetzung vorliegt.

## Deaktivieren von NAT für bestimmte Hosts/Netzwerke

Wenn Sie die NAT-Kontrolle verwenden und im internen Netzwerk über einige öffentliche Adressen verfügen und diese spezifischen internen Hosts ohne Übersetzung nach außen gehen sollen, können Sie NAT für diese Hosts mit **nat 0-** oder **statischen** Befehlen deaktivieren.

Dies ist ein Beispiel für den Befehl **nat**:

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

Führen Sie diese Schritte aus, um NAT für bestimmte Hosts/Netzwerke unter Verwendung von ASDM zu deaktivieren.

1. Wählen Sie **Konfiguration > Funktionen > NAT** aus, und klicken Sie auf **Hinzufügen**.
2. Wählen Sie als Ausgangsschnittstelle aus, und geben Sie die interne Adresse bzw. das interne Netzwerk ein, für die Sie eine statische Übersetzung erstellen möchten.
3. Wählen Sie **Dynamic (Dynamisch)** aus, und wählen Sie die gleiche Adresse für den

Adresspool aus. Klicken Sie auf OK.

Use NAT  Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static

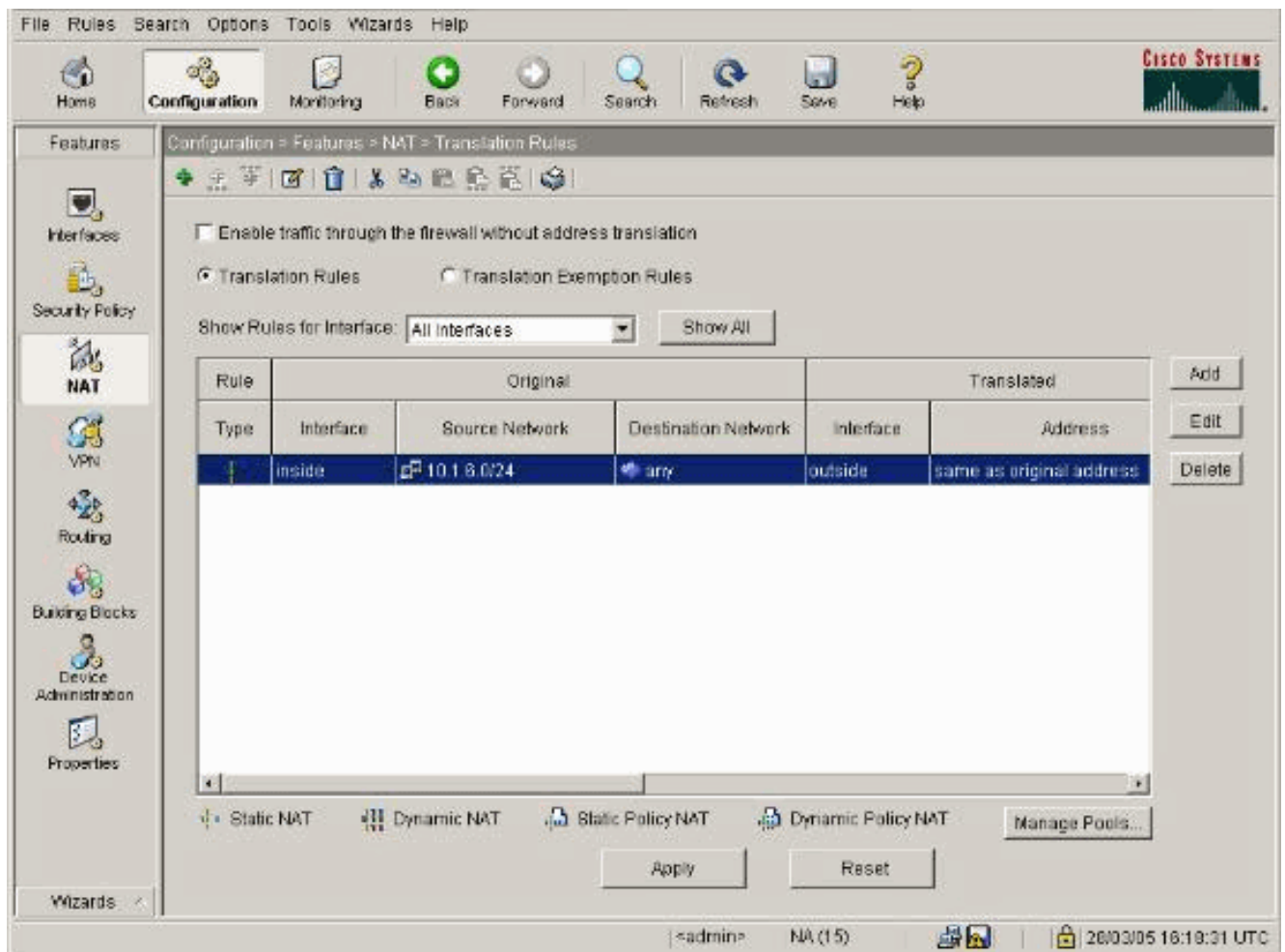
Redirect port

TCP    
 UDP

Dynamic

Pool ID	Address
N/A	No address pool defined

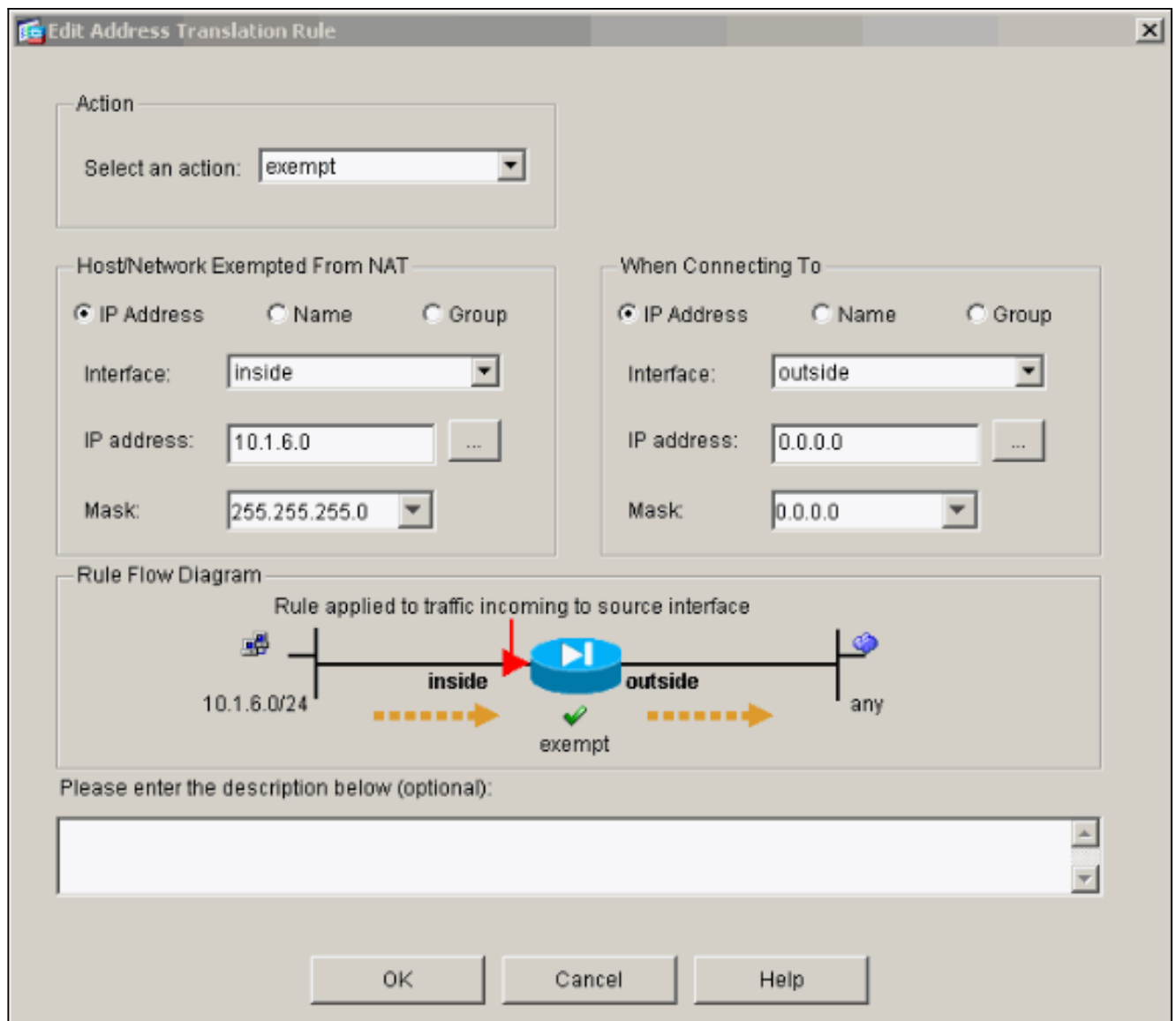
- Die neue Regel wird in den Übersetzungsregeln angezeigt, wenn Sie **Configuration > Features > NAT > Translation Rules** auswählen.



5. Wenn Sie ACLs verwenden, die eine präzisere Kontrolle des Datenverkehrs ermöglichen, den Sie nicht übersetzen sollten (basierend auf Quelle/Ziel), verwenden Sie diese Befehle.

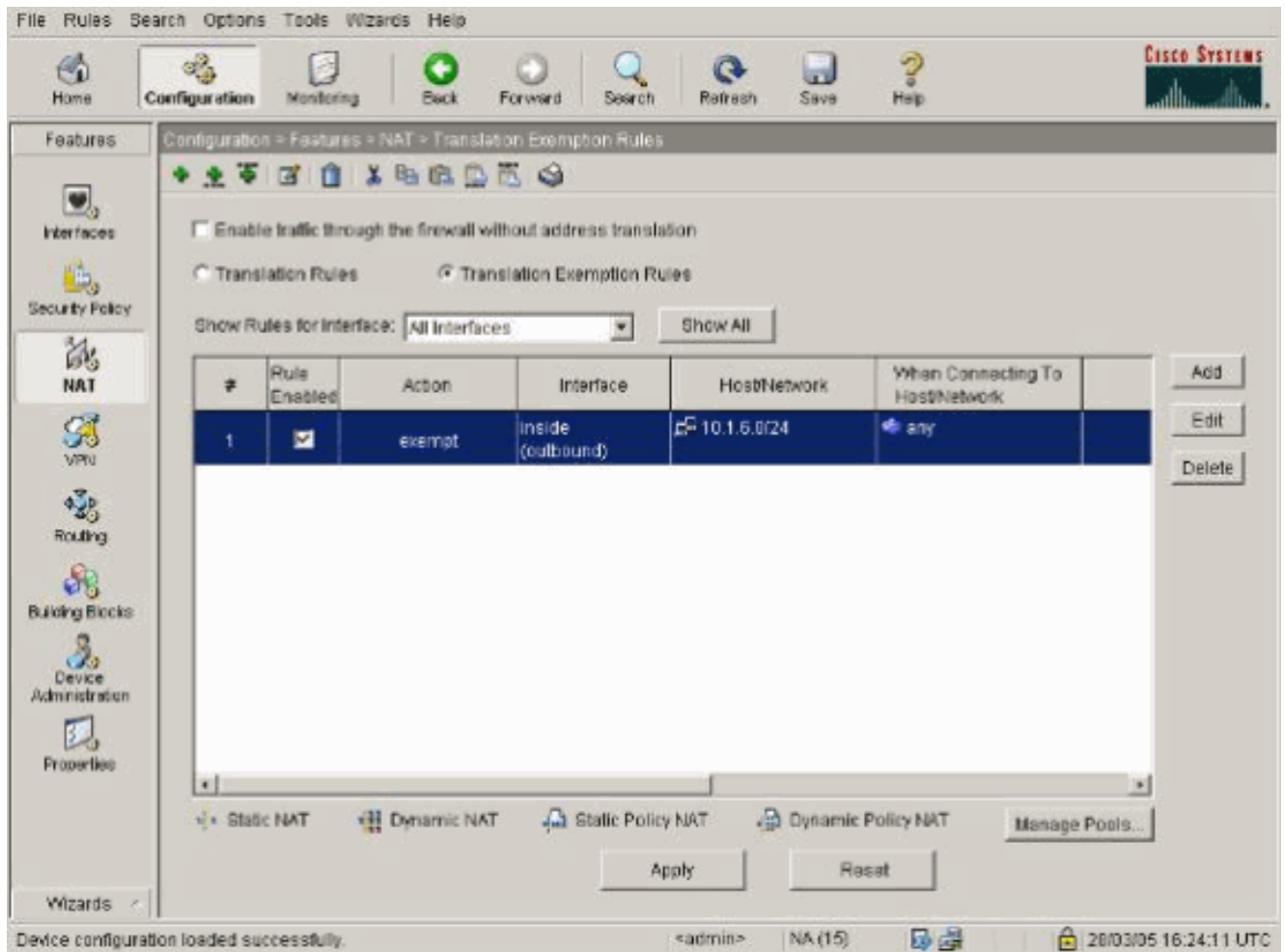
```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

6. Wählen Sie unter ASDM **Configuration > Features > NAT > Translation Rules** aus.
7. Wählen Sie **Übersetzungsfreistellungsregeln** aus und klicken Sie auf **Hinzufügen**. In diesem Beispiel wird veranschaulicht, wie der Datenverkehr aus dem Netzwerk 10.1.6.0/24 an einen beliebigen Ort von der Übersetzung ausgenommen wird.



8. Wählen Sie **Konfiguration > Funktionen > NAT > Übersetzungsfreistellungsregeln**, um die neuen Regeln anzuzeigen.





9. Der **statische** Befehl für den Webserver ändert sich, wie im folgenden Beispiel gezeigt.

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

10. Wählen Sie im ASDM **Configuration > Features > NAT > Translation Rules** aus.

11. Wählen Sie **Übersetzungsregeln aus**, und klicken Sie auf **Hinzufügen**. Geben Sie die Quelladressinformationen ein, und wählen Sie **Statisch** aus. Geben Sie dieselbe Adresse in das Feld IP-Adresse ein.



**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:

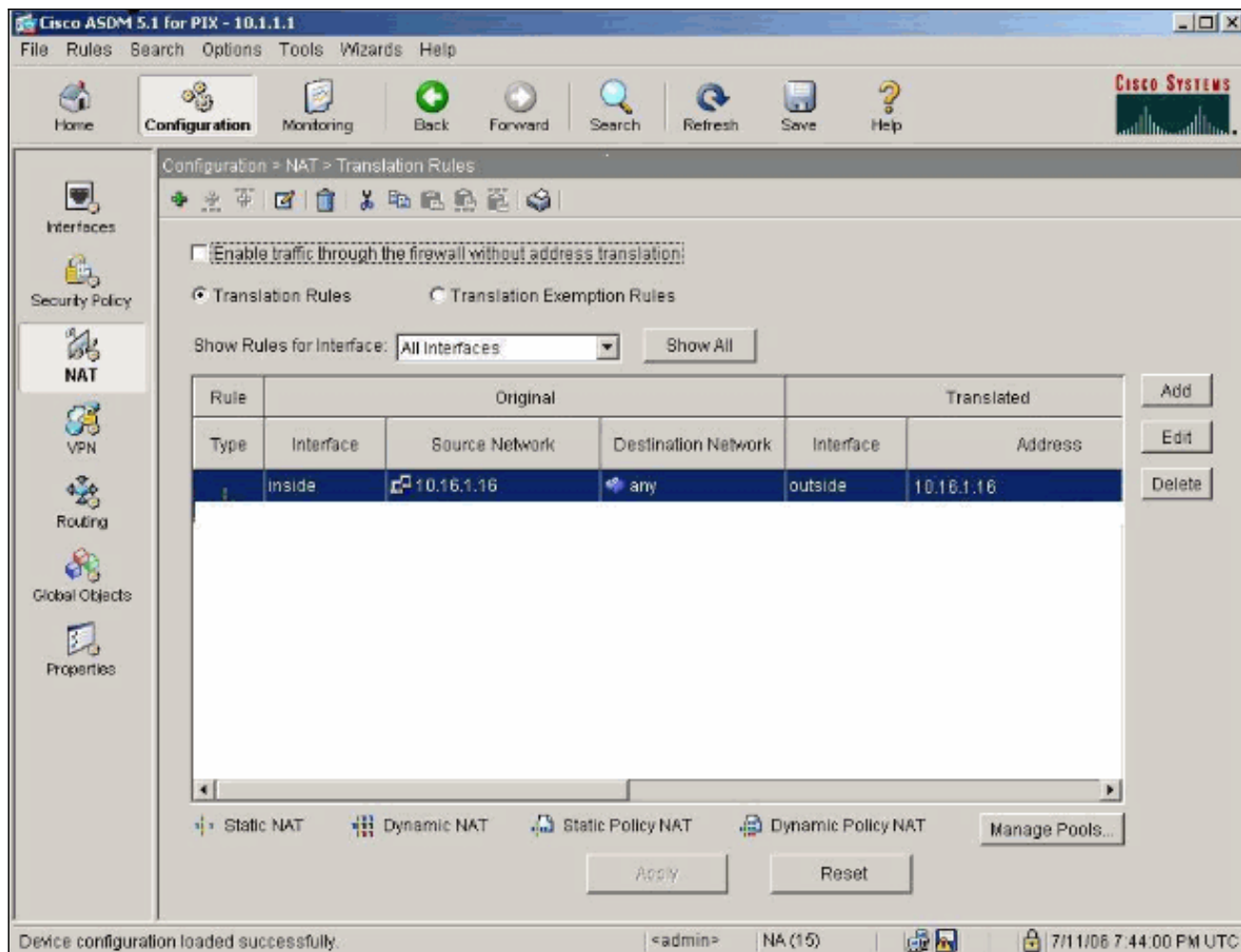
UDP

 Dynamic     Address Pool:     

Pool ID	Address

12. Die Übersetzung wird in den Übersetzungsregeln angezeigt, wenn Sie **Configuration > Features > NAT > Translation Rules** auswählen.



13. Wenn Sie ACLs verwenden, verwenden Sie diese Befehle.

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

Weitere Informationen zur Konfiguration von ACLs in ASDM finden Sie im Abschnitt [Einschränken von Gastgebern für den Zugriff auf externe Netzwerke](#) in diesem Dokument. Beachten Sie den Unterschied zwischen der Verwendung von **nat 0** bei Angabe von Netzwerk/Maske im Gegensatz zu der Verwendung einer ACL, die ein Netzwerk/eine Maske verwendet, die nur die Initiierung von Verbindungen von innen ermöglicht. Die Verwendung von ACLs mit **nat 0** ermöglicht die Initiierung von Verbindungen durch eingehenden oder ausgehenden Datenverkehr. Die PIX-Schnittstellen müssen sich in unterschiedlichen Subnetzen befinden, um Probleme mit der Erreichbarkeit zu vermeiden.

## [Port Redirection \(Forwarding\) mit Statistiken](#)

In PIX 6.0 wurde die Funktion "Port Redirection (Forwarding)" (Weiterleitung) hinzugefügt, um externen Benutzern die Verbindung mit einer bestimmten IP-Adresse bzw. einem bestimmten Port zu ermöglichen und den PIX-Datenverkehr an den entsprechenden internen Server bzw. Port umzuleiten. Der **statische** Befehl wurde geändert. Bei der freigegebenen Adresse kann es sich um eine eindeutige Adresse, eine gemeinsam genutzte PAT-Adresse für ausgehende Anrufe oder um eine mit der externen Schnittstelle gemeinsam genutzte Adresse handeln. Diese Funktion ist in PIX 7.0 verfügbar.

**Hinweis:** Aufgrund von Platzbeschränkungen werden Befehle in zwei Zeilen angezeigt.

```
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]]]
```

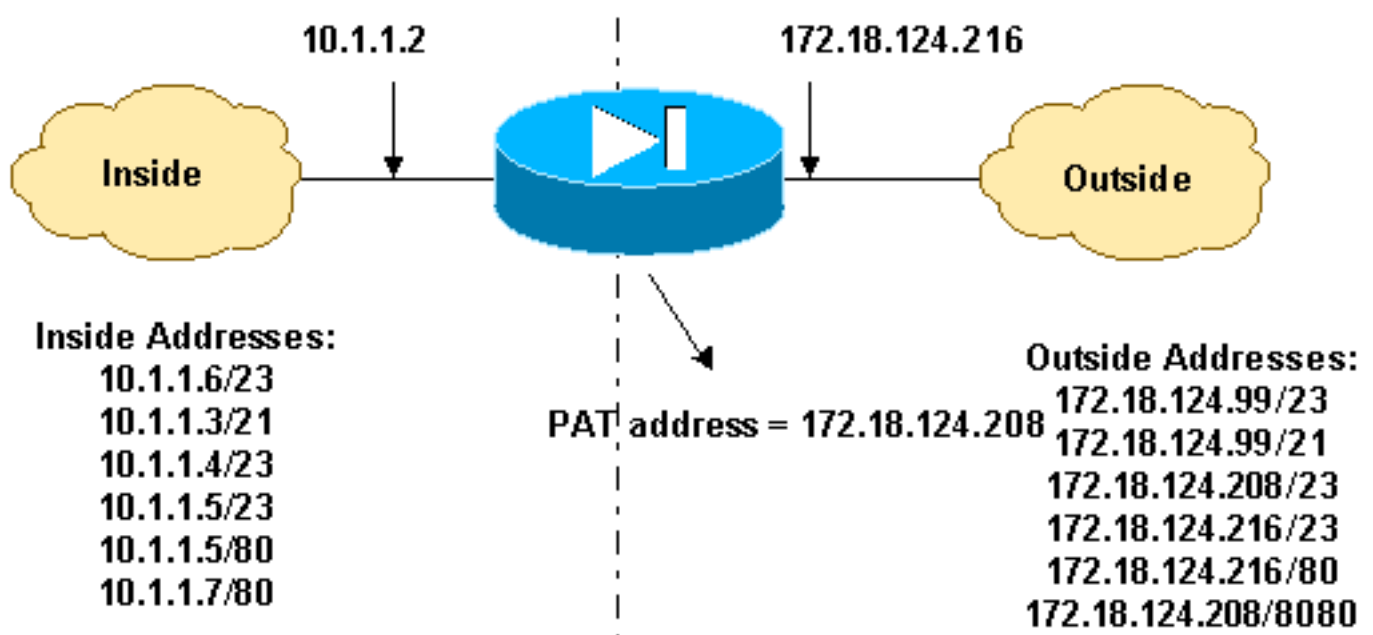
**Hinweis:** Wenn die statische NAT die externe IP-Adresse (global\_IP) für die Übersetzung verwendet, kann dies zu einer Übersetzung führen. Verwenden Sie daher in der statischen Übersetzung das Schlüsselwort **interface** anstelle der IP-Adresse.

Diese Portumleitungen (Weiterleitungen) sind in diesem Netzwerkbeispiel enthalten:

- Externe Benutzer leiten Telnet-Anfragen an die eindeutige IP-Adresse 172.18.124.99 weiter, die PIX an 10.1.1.6 umleitet.
- Externe Benutzer leiten FTP-Anfragen an die eindeutige IP-Adresse 172.18.124.99 weiter, die PIX an 10.1.1.3 umleitet.
- Externe Benutzer leiten Telnet-Anfragen an die PAT-Adresse 172.18.124.208 weiter, die PIX an 10.1.1.4 umleitet.
- Externe Benutzer leiten Telnet-Anfragen an PIX außerhalb der IP-Adresse 172.18.124.216 weiter, die PIX an 10.1.1.5 umleitet.
- Externe Benutzer leiten HTTP-Anfragen an PIX außerhalb der IP-Adresse 172.18.124.216 weiter, die PIX an 10.1.1.5 umleitet.
- Externe Benutzer leiten HTTP-Port 8080-Anforderungen an die PAT-Adresse 172.18.124.208 weiter, die PIX an 10.1.1.7-Port 80 umleitet.

In diesem Beispiel wird auch der Zugriff einiger Benutzer von innen nach außen mit ACL 100 blockiert. Dieser Schritt ist optional. Der gesamte ausgehende Datenverkehr ist ohne die vorhandene ACL zulässig.

### Netzwerkdiagramm - Port Redirection (Forwarding)



### Partielle PIX-Konfiguration - Port-Umleitung

Diese Teilkonfiguration veranschaulicht die Verwendung von Static Port Redirection (Weiterleitung). Siehe [Netzwerkdiagramm](#) für die [Port-Umleitung\(Weiterleitung\)](#).

### Partielle PIX 7.x-Konfiguration - Port Redirection(Forwarding)

```
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
```

**Hinweis:** Wenn PIX/ASA mit dem Befehl `sysopt noproxyarp outside` konfiguriert ist, erlaubt es der Firewall nicht, die Proxys und statische NAT-Übersetzungen in PIX/ASA auszuführen. Um dieses Problem zu beheben, entfernen Sie den Befehl `sysopt noproxyarp outside` in der PIX/ASA-Konfiguration und aktualisieren Sie dann die ARP-Einträge mithilfe von freiem ARP. Dadurch können statische NAT-Einträge einwandfrei funktionieren.

Dieses Verfahren ist ein Beispiel für die Konfiguration der Port Redirection (Forwarding), die externen Benutzern ermöglicht, Telnet-Anfragen an eine eindeutige IP-Adresse 172.18.124.99 weiterzuleiten, die von PIX zu 10.1.1.6 umgeleitet wird.

1. Wählen Sie unter **ASDM Configuration > Features > NAT > Translation Rules** aus.
2. Wählen Sie **Übersetzungsregeln** aus, und klicken Sie auf **Hinzufügen**.
3. Geben Sie als Quellhost/Netzwerk die Informationen für die interne IP-Adresse ein.
4. Wählen Sie als Übersetzen der Adresse in die Option **Statisch** aus, geben Sie die externe IP-Adresse ein, und aktivieren Sie **Redirect port**.
5. Geben Sie die Informationen für den Port vor und nach der Übersetzung ein (in diesem Beispiel wird Port 23 verwaltet). Klicken Sie auf **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

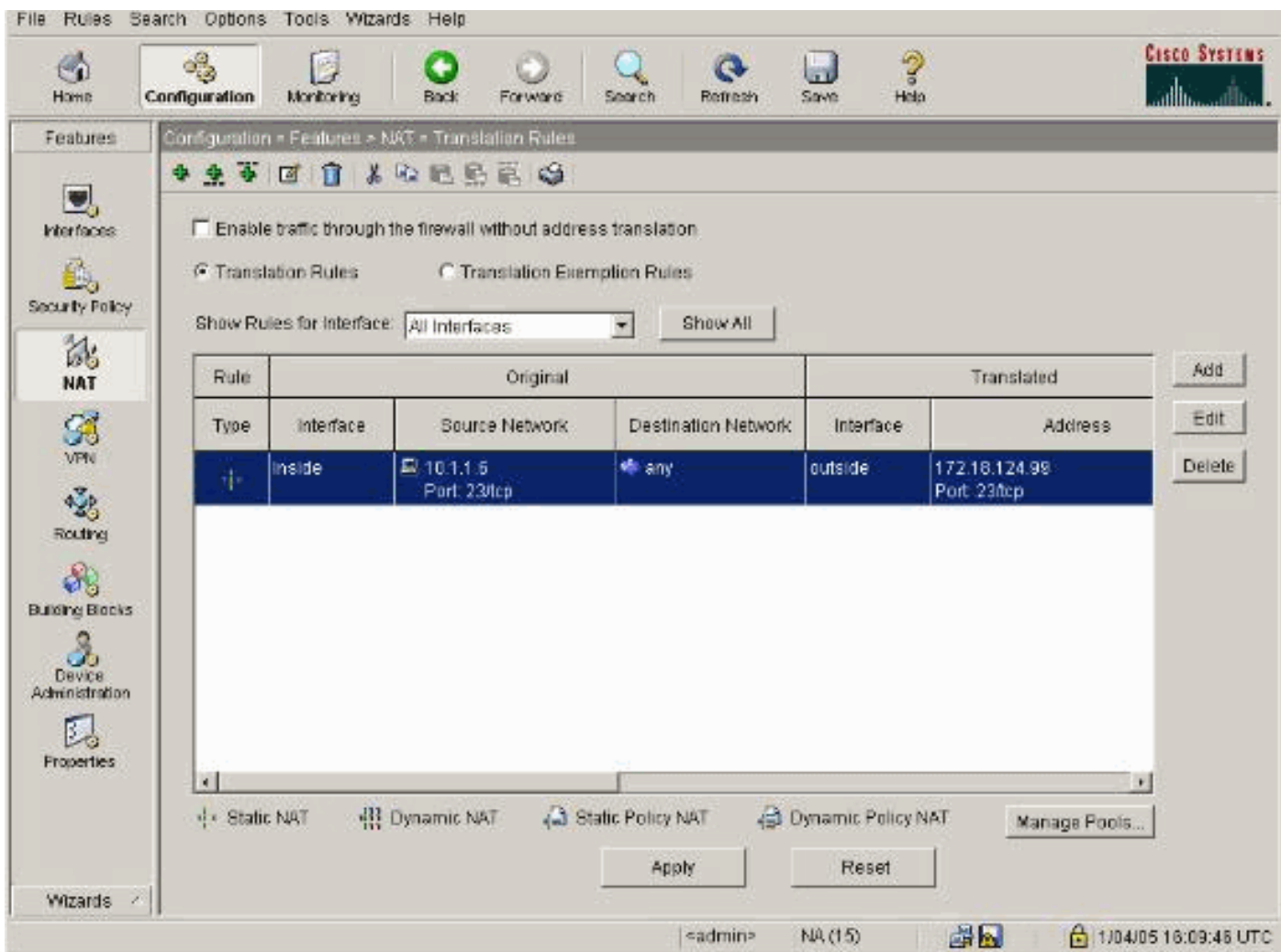
TCP    
 UDP    
Original port:     
Translated port:

 Dynamic    
Address Pool:     

Pool ID	Address

Die Übersetzung wird in den Übersetzungsregeln angezeigt, wenn Sie **Configuration > Features > NAT > Translation Rules** auswählen.



## Einschränkung der TCP/UDP-Sitzung mithilfe von Static

Wenn Sie die TCP- oder UDP-Sitzungen auf den internen Server in PIX/ASA beschränken möchten, verwenden Sie den **statischen** Befehl.

Gibt die maximale Anzahl gleichzeitiger TCP- und UDP-Verbindungen für das gesamte Subnetz an. Der Standardwert ist 0, d. h. unbegrenzte Verbindungen (Inaktive Verbindungen werden geschlossen, nachdem die Leerlaufzeitüberschreitung durch den Befehl **timeout conn** angegeben wurde.) Diese Option gilt nicht für externe NAT. Die Sicherheits-Appliance verfolgt nur Verbindungen von einer höheren Sicherheitsschnittstelle zu einer niedrigeren Sicherheitsschnittstelle.

Die Beschränkung der Anzahl an embryonalen Verbindungen schützt Sie vor einem DoS-Angriff. Die Sicherheits-Appliance verwendet das embryonale Limit, um TCP Intercept auszulösen, das interne Systeme vor einem DoS-Angriff schützt, der durch Überflutung einer Schnittstelle mit TCP-SYN-Paketen erfolgt. Eine embryonale Verbindung ist eine Verbindungsanforderung, die den erforderlichen Handshake zwischen Quelle und Ziel noch nicht beendet hat. Diese Option gilt nicht für externe NAT. Die TCP-Abhörungsfunktion gilt nur für Hosts oder Server mit einer höheren Sicherheitsstufe. Wenn Sie den Embryonalgrenzwert für eine externe NAT festlegen, wird der Embryonalgrenzwert ignoriert.

Beispiel:



```
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-3-201002: Zu viele Verbindungen auf {static|xlate} global\_address! Verbindungen

Dies ist eine verbindungsbezogene Nachricht. Diese Meldung wird protokolliert, wenn die maximale Anzahl von Verbindungen mit der angegebenen statischen Adresse überschritten wurde. Die econns-Variable ist die maximale Anzahl an embryonalen Verbindungen und nconns ist die maximale Anzahl von Verbindungen, die für die statische oder Xlate zulässig ist.

Es wird empfohlen, den Befehl **show static** zu verwenden, um die Beschränkung für Verbindungen mit einer statischen Adresse zu überprüfen. Das Limit ist konfigurierbar.

## %ASA-3-2011: Die Verbindungsgrenze für eingehende Pakete überschreitet 1000/1000 von 10.1.26.51/2393 bis 10.0.86.155/135 für die externe Schnittstelle.

Diese Fehlermeldung beruht auf der Cisco Bug ID [CSCsg52106](#) (nur [registrierte](#) Kunden) . Weitere Informationen finden Sie in diesem Bug.

## Zeitbasierte Zugriffsliste

Die Erstellung eines Zeitbereichs schränkt den Zugriff auf das Gerät nicht ein. Der Befehl **für die Zeitspanne** definiert nur den Zeitbereich. Nachdem ein Zeitraum definiert wurde, können Sie ihn an Verkehrsregeln oder eine Aktion anhängen.

Verwenden Sie zum Implementieren einer zeitbasierten Zugriffskontrollliste den Befehl **Time Range (Zeitbereich)**, um bestimmte Zeiten für Tag und Woche festzulegen. Verwenden Sie dann den Befehl **mit dem Befehl access-list extended time-range**, um den Zeitbereich an eine ACL zu binden.

Der Zeitraum hängt von der Systemuhr der Sicherheits-Appliance ab. Diese Funktion funktioniert jedoch am besten bei der NTP-Synchronisierung.

Nachdem Sie einen Zeitbereich erstellt und den Konfigurationsmodus für den Zeitbereich eingegeben haben, können Sie Zeitbereichsparameter mit den **absoluten** und **periodischen** Befehlen definieren. Um die Standardeinstellungen für absolute und periodische Schlüsselwörter für **Zeitbereichsbefehle** wiederherzustellen, verwenden Sie den **standardmäßigen** Befehl im Zeitbereichskonfigurationsmodus.

Verwenden Sie zum Implementieren einer zeitbasierten Zugriffskontrollliste den Befehl **Time Range (Zeitbereich)**, um bestimmte Zeiten für Tag und Woche festzulegen. Verwenden Sie dann den Befehl **mit dem Befehl access-list extended**, um den Zeitbereich an eine ACL zu binden. Im nächsten Beispiel wird eine ACL mit dem Namen "Sales" (Vertrieb) an einen Zeitbereich mit der Bezeichnung "New York Minute" gebunden:

In diesem Beispiel wird ein Zeitbereich mit dem Namen "New York Minute" erstellt und in den Zeitbereichskonfigurationsmodus gewechselt:

```
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
```

## Informationen zum Sammeln, wenn Sie ein technisches Support-Ticket öffnen

Wenn Sie weiterhin Hilfe benötigen und ein Ticket beim technischen Support von Cisco eröffnen möchten, geben Sie zur Fehlerbehebung für Ihre PIX Security Appliance diese Informationen an.

- Problembeschreibung und relevante Topologiedetails.
- Die Schritte zur Fehlerbehebung, die Sie vor dem Öffnen des Gehäuses durchgeführt haben.
- Ausgabe über den Befehl **show tech-support**.
- Ausgabe über den Befehl **show log** nach dem Ausführen des Befehls **logging buffered debugging** oder Konsolenerfassung, die das Problem (falls verfügbar) demonstrieren.

Hängen Sie die erfassten Daten im unverzipten Textformat (.txt) an Ihren Fall an. Sie können Informationen zu Ihrem Ticket im [TAC Service Request Tool](#) hinzufügen (nur [registrierte](#) Kunden). Wenn Sie nicht auf das [TAC Service Request Tool](#) zugreifen können (nur [registrierte](#) Kunden), können Sie die Informationen in einem E-Mail-Anhang an [attach@cisco.com](mailto:attach@cisco.com) mit Ihrer Fallnummer in der Betreffzeile Ihrer Nachricht senden.

## Zugehörige Informationen

- [Support-Seite für PIX Security Appliance](#)
- [PIX-Befehlsreferenzen](#)
- [Fehlerbehebung und Warnmeldungen mit dem Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)